Středoškolská odborná činnost

Obor č. 1: Matematika a statistika

p-adická čísla

Adéla Heroudková

Brno 2021

Středoškolská odborná činnost
Obor č. 1: Matematika a statistika

p-adická čísla

p-adic Numbers

Autor	Adéla Heroudková
Škola	Gymnázium Brno, třída Kapitána Jaroše 14., p. o.
Kraj	Jihomoravský
Obor	Matematika a statistika
Konzultant	prof. RNDr. Radan Kučera, DSc.

Brno 2021

Prohlášení

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

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

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

V _____ dne _____ podpis _____

Poděkování

Chtěla bych poděkovat panu profesorovi Radanu Kučerovi za skvělé vedení, cenné rady a za hodiny strávené nad opravami mé práce.

Dále bych chtěla poděkovat Tomášovi Perutkovi za pomoc v krizových situacích a skvělý nápad s aplikací Hasse-Minkowského věty.

Tato práce byla vypracována za finanční podpory JMK.

Abstrakt

Hlavním cílem této práce je uvést čtenáře do světa p-adických čísel. Ukázat, jak tato čísla sestrojit, jak se s nimi pracuje a čím se liší od reálných čísel. V druhé polovině práce popíšeme pomocí poznatků z p-adické analýzy jednotky v okruhu celých p-adických čísel. Tímto zjistíme, jak vypadají druhé mocniny p-adických čísel, což využijeme v poslední kapitole o lokálním-globálním principu. Na závěr sestavíme vlastní důkaz Fermatovy věty o součtu dvou druhých mocnin a Lagrangeovy věty o čtyřech čtvercích.

Klíčová slova

p-adická čísla, absolutní hodnoty, mocninné řady, druhé mocniny, lokální-globální princip, kvadratické formy

Abstract

The main goal of this thesis is to introduce the reader to the world of p-adic numbers. We show how to construct them, how to work with them and how they differ from real numbers. In the second half of the thesis we describe units in the ring of p-adic integers. This allows us to describe squares of p-adic numbers, which we use in the last chapter about Local-Global principle. There we show our own proof of Fermat's theorem on sum of two squares and Lagrange four squares theorem.

Key words

p-adic numbers, absolute values, power series, squares, Local-Global principle, quadratic forms

Obsah

Kapitola 1

Úvod

Těleso p-adických čísel je zúplněním tělesa racionálních čísel, stejně jako těleso reálných čísel, ovšem s jinou absolutní hodnotou. Pro každé prvočíslo p takto dostaneme unikátní metrický prostor $\mathbb{Q}_p$, který můžeme zkoumat.

V jedné knize o teorii čísel [7] jsem našla odstavec, který krásně vystihuje podstatu p-adických čísel: „In the long history of mathematics a number meant a real number, and it is only relatively recently that we realized that there is a world of p-adic numbers. It is as if those who had seen the sky only during the day are marvelling at the night sky. The mathematical scenery is completely different. $\mathbb{Q}_p$ emits "the light of prime number p" in the night sky as if it were a star that we could not see because of the sun, or the real number field $\mathbb{R}$, which emits "the light of real numbers" during the day. Just as there are countless stars in the night sky, there is one $\mathbb{Q}_p$ for each p. What each star is to the sun is what each $\mathbb{Q}_p$ is to $\mathbb{R}$. Just as we can see space objects better at night, we began to see the profound mathematical universe through the p-adic numbers."

V této práci se nejprve zaměříme na p-adickou absolutní hodnotu a na konstrukci těles p-adických čísel pomocí zmíněného zúplnění racionálních čísel.

V další kapitole se podíváme na to, jak vlastně p-adická čísla vypadají a co jsou to celá p-adická čísla. Též si představíme a dokážeme Henselovo lemma, což je poměrně silný nástroj při hledání kořenů p-adických polynomů.

Následuje kapitola o p-adické analýze, kde se budeme hlavně zabývat teorií p-adických mocninných řad, které mají spoustu užitečných vlastností, které využijeme v následující kapitole.

V páté kapitole se totiž budeme zabývat jednotkami v p-adických číslech. A na jejich popsání využijeme p-adický logaritmus a exponenciální funkci, které definujeme pomocí mocninných řad. Též se podíváme, které netriviální odmocniny z jedné leží v jednotlivých $\mathbb{Q}_p$, což nám dohromady dá způsob, jak můžeme popsat druhé mocniny v těchto tělesech.

V poslední kapitole se podíváme na využití p-adických čísel při zjišťovaní, zda má nějaká kvadratická forma řešení v racionálních číslech, na což nám slouží takzvaná Hasse-Minkowského věta. Tu následně použijeme při vlastním důkaze Fermatovy věty o součtu dvou druhých mocnin a Lagrangeovy věty o čtyřech čtvercích.

U čtenáře se předpokládá základní znalost reálné analýzy - základy limitních procesů, derivací, teorie nekonečných a mocninných řad reálných čísel přibližně v rozsahu stran 291-345 z knihy [10]. Též se předpokládá základní znalost teorie grup - grupy, faktor grupy, okruhy, ideály, tělesa a homomorfismy těles, Malá Fermatova věta.

1.1 Stručná historie p-adických čísel

Jako první představil p-adická čísla Kurt Hensel v roce 1897 s myšlenkou přivést metody mocninných řad do teorie čísel. Ale i před ním můžeme u některých matematiků vidět používání p-adických metod, například u Kummera, Dedekinda či Webera.

Henselovy myšlenky byly v některých ohledech ze začátku zmatené, například jeho představy o konvergenci. Ovšem i tak spousta jeho nápadů našla okamžité uplatnění v algebraické teorii čísel, například známé Henselovo lemma.

V roce 1910 vydal Ernst Steinitz článek o abstraktní teorii těles (jeden z prvních článků o abstraktní algebře), kde napsal, že jednou z hlavních motivací k této nové teorii jsou právě p-adická čísla. Od tohoto okamžiku se p-adická čísla začala objevovat i v běžných článcích o algebře.

Okolo roku 1912 začal Josef Kürschák přemýšlet o valuacích, aby bylo jednodušší p-adická čísla definovat, a dal základ celé teorii valuací (která má dnes spoustu dalších využití). To umožnilo popsat p-adická čísla jako metrický prostor.

Postupně se zájem o p-adická čísla začal zvyšovat. Roku 1917 přišel se svojí větou Alexander Ostrowski. Roku 1922 objevil Helmut Hasse lokální a globální princip. Mezi lety 1920-1926 Max Deuring, Erhard Schmidt, Wolfgang Krull a mnozí další dokončili teorii o valuacích, se kterou začal J. Kürschák. V roce 1926 se Reinhold Strassman začal zajímat o funkce definované mocninnými řadami.

Všechna tato data nejsou pro moji další práci nijak zvlášť důležitá, ale vzhledem k tomu, že spoustu ze zmíněných vět a jmen se v mé práci objeví, přijde mi zajímavé si uvědomit, v jakém pořadí se objevily.

Matematickému světu trvalo dlouho, než p-adická čísla akceptoval, ale dnes již hrají hlavní roli v moderní teorii čísel.

Dokonce můžeme najít jejich uplatnění i v jiných oborech, ve fyzice například v teorii strun či kvantové mechanice, ale ještě více překvapující je použití v biologii či geologii. Podrobnější informace o těchto využití můžete najít v [8].

Kapitola 2

Konstrukce p-adických čísel

Jak jsem již říkala v úvodu, p-adická čísla jsou zúplněním racionálních čísel, stejně jako reálná čísla, jenom s jinou absolutní hodnotou.

Ale, co je to vlastně to zúplnění? Abychom to mohli pochopit, musíme si nejprve připomenout definici cauchyovské posloupnosti a úplného prostoru:

Definice 2.0.1. ***Cauchyovská posloupnost***
Uvažujme posloupnost reálných čísel $(a_0, a_1, a_2, \dots)$ *takovou, že pro jakékoli kladné pevně dané* $\varepsilon > 0$ *existuje index* N *tak, že následující nerovnost platí pro všechna* $i > N, j > N$*:*

$$|a_i - a_j| < \varepsilon.$$

Tedy pro libovolně malou vzdálenost existuje hranice, za kterou jsou již všechny členy posloupnosti navzájem blíž než tato vzdálenost. Takovou posloupnost nazveme cauchyovskou.

Abychom mohli zavést, co je to úplný prostor, potřebuje vědět, co je to metrický prostor. Jeho definice je uvedena v definici 2.2.1. Nám prozatím postačí si metrický prostor představit jako množinu bodů s nějakou metrikou. Pod metrikou si můžeme představit například vzdálenost bodů - pokud si vezmeme prostor reálných čísel, je vzdáleností dvou čísel absolutní hodnota jejich rozdílu.

Definice 2.0.2. *Metrický prostor nazveme úplným, pokud každá cauchyovská posloupnost prvků tohoto metrického prostoru konverguje k nějakému prvku tohoto metrického prostoru.*

Příkladem úplného metrického prostoru můžou být množina všech celých čísel a právě množina všech reálných čísel.

Naopak metrický prostor všech racionálních čísel úplný není, protože můžeme například mít cauchyovskou posloupnost racionálních čísel konvergujících k π: (3,14; 3,1415; 3,14159; 3,1415926; ...). Pomocí racionálních čísel se můžeme π libovolně přiblížit, ale π není racionální, takže $\mathbb{Q}$ s absolutní hodnotou nemůže být úplný metrický prostor.

Před tím, než vysvětlím, co je to zúplnění, si musíme ještě definovat několik pojmů:

Definice 2.0.3. *Otevřenou koulí* $B(a, \epsilon)$ *se středem* a *a poloměrem* ϵ *rozumíme množinu všech bodů metrického prostoru* X*, které mají od bodu* a *vzdálenost menší než* ϵ*.*

Definice 2.0.4. *Podmnožinu* A *metrického prostoru* X *nazveme hustou, pokud pro každé* $x \in X$ *a každé* $\varepsilon > 0$ *platí:*

$$B(x, \varepsilon) \cap A \neq \emptyset.$$

Zúplněním racionálních čísel s normální absolutní hodnotou je pak metrický prostor, ve kterém jsou racionální čísla hustou podmnožinou a zároveň v něm konvergují všechny cauchyovské posloupnosti - je úplná. A tuto množinu nazýváme reálnými čísly.

Na konci této kapitoly si stejným způsobem vytvoříme p-adická čísla, ale nejprve si musíme definovat p-adickou absolutní hodnotu.

2.1 Valuace a absolutní hodnoty

2.1.1 Valuace

Abychom mohli popsat p-adickou absolutní hodnotu, musíme si nejprve zavést pojem p-adické valuace:

Definice 2.1.1. *Pro pevně dané prvočíslo p je p-adická valuace funkce:*

$$v_p : \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{Z}$$

definovaná následovně: pro každé $n \in \mathbb{Z}$, $n \neq 0$, je $v_p(n)$ unikátní celé nezáporné číslo splňující:

$$n = p^{v_p(n)} m, \quad m \in \mathbb{Z}, \quad p \nmid m.$$

Valuaci rozšíříme na racionální čísla následovně: jestliže $x = \frac{a}{b} \in \mathbb{Q} \setminus \{0\}$, $a, b \in \mathbb{Z}$, $(a, b) = 1$, potom:

$$v_p(x) = v_p(a) - v_p(b).$$

Poznámka. *Pokud $n = 0$, zavedeme $v_p(0) = \infty$.*

Jinak řečeno p-adickou valuaci libovolného nenulového racionálního čísla dostaneme, když si toto číslo rozepíšeme jako $x = p^n \frac{a}{b}$, kde a, b jsou celá nesoudělná čísla, která nejsou dělitelná p a n je celé, pak $v_p(x) = n$.

Příklady: $v_3(9) = 2$, $v_3(\frac{4}{54}) = -3$, $v_5(\frac{3}{22}) = 0$.

Valuace má několik zajímavých vlastností, které nám pak umožní vytvořit pomocí ní novou absolutní hodnotu.

Lemma 2.1.1. *Pro všechna $x, y \in \mathbb{Q}$, platí:*

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

ii) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

Důkaz: Nejprve si vezměme případ, kdy je jedno z čísel nulové. Součtem celého čísla a nekonečna rozumíme nekonečno a nekonečno považujeme za větší než libovolné celé číslo. Potom je pro tento případ jasné, že tvrzení platí.

Čísla x, y si zapíšeme jako: $x = p^a \frac{x'}{x''}$, $y = p^b \frac{y'}{y''}$, $p \nmid x'x''y'y''$ a $x', x'', y', y'' \in \mathbb{Z}$.

První vlastnost dokážeme následovně:

$$v_p(xy) = v_p\left(p^a \frac{x'}{x''} p^b \frac{y'}{y''}\right) = v_p\left(p^{a+b} \frac{x'}{x''} \frac{y'}{y''}\right) = a + b = v_p(x) + v_p(y).$$

Nyní se podívejme na druhou vlastnost a řekněme bez újmy na obecnosti, že platí, že $\min\{v_p(x), v_p(y)\} = \min\{a, b\} = a$:

$$v_p(x+y) = v_p\left(p^a\frac{x'}{x''} + p^b\frac{y'}{y''}\right) = v_p\left(p^a\left(\frac{x'}{x''} + p^{b-a}\frac{y'}{y''}\right)\right) =$$

$$= a + v_p\left(\frac{x'}{x''} + p^{b-a}\frac{y'}{y''}\right) \geq \min\{a, b\}.$$

Poslední nerovnost musí platit, protože, když si převedeme zlomek na stejného jmenovatele, dostaneme

$$v_p\left(\frac{x'y'' + p^{b-a}y'x''}{x''y''}\right) \geq 0,$$

neboť p může dělit $x'y'' + p^{b-a}y'x''$, ale nemůže dělit $x''y''$.

Levá strana je tudíž rovna a, pokud je $b > a$, protože pak $p \nmid (x'y'' + p^{b-a}y'x'')$.

Naopak pokud je $a = b$, tak pak součet $x + y$ může mít jinou valuaci než $\min\{a, b\}$. Prvočíslo p totiž může dělit $x'y'' + y'x''$.

Poznámka. *Všimněte si, že buď je levá strana nerovnosti rovna té pravé, nebo jsou si rovny valuace x a y.* □

2.1.2 Absolutní hodnoty

Jak jsem již dřív zmiňovala, v této části si zavedeme jinou absolutní hodnotu, než známe ze školy. Ve škole se totiž málokdy zmiňuje, že to, čemu říkáme absolutní hodnota, je jen nejpřirozenější funkce splňující následující vlastnosti:

Definice 2.1.2. *Absolutní hodnota na tělese $\mathbb{F}$ je funkce:*

$$|\ |: \mathbb{F} \longrightarrow \mathbb{R}^0_+,$$

kde $\mathbb{R}^0_+$ je množina nezáporných reálných čísel, splňující následující podmínky pro všechna $x, y \in \mathbb{F}$:

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

ii) $|xy| = |x||y|$,

iii) $|x + y| \leq |x| + |y|$,

iv) Pokud platí ještě následující doplňující podmínka, budeme říkat, že je absolutní hodnota ne-archimédovská: $|x + y| \leq \max\{|x|, |y|\}$.

Pokud splní první tři podmínky, ale tuto čtvrtou podmínku nesplňuje, tak o ní budeme mluvit jako o archimédovské absolutní hodnotě.

Všimněme si, že pokud funkce splňuje čtvrtou podmínku, musí automaticky splňovat i třetí. Ne-archimédovská podmínka je pouze silnější verze trojúhelníkové nerovnosti (třetí podmínky).

Tato definice má několik jednoduchých důsledků. Z toho, že $|1| > 0$ a $|1| = |1| \cdot |1|$ plyne, že $|1| = 1$. Z čehož dostáváme, že $|\frac{1}{x}| = \frac{1}{|x|}$, pro každé nenulové $x \in \mathbb{F}$.

PŘÍKLADY: Příkladem archimédovské absolutní hodnoty je klasická absolutní hodnota: $|x| = x$, pro $x \in \mathbb{Q}$ a zároveň $x \geq 0$, $|x| = -x$ pro $x \in \mathbb{Q}$ a zároveň $x < 0$. Již z definice je vidět, že první tři podmínky skutečně splňuje. Na dokázání, že čtvrtá podmínka neplatí, si stačí vzít například: $|3 + 5| = 8 > \max\{|3|, |5|\} = 5$. Tato absolutní hodnota je taky někdy zařazována do těch p-adických, které si definujeme za chvíli. V takových chvílích se značí $|\ |_\infty$ a říká se jí nekonečná absolutní hodnota nebo absolutní hodnota v nekonečnu.

Příkladem ne-archimédovské absolutní hodnoty je takzvaná triviální absolutní hodnota: $|x| = 0$ pro $x = 0$, $|x| = 1$ pro $x \in \mathbb{Q} \setminus \{0\}$. Je vidět, že první dvě podmínky splňuje a pojďme se podívat na čtvrtou - pokud je alespoň jeden ze sčítanců nenulový, tak $\max\{|x|, |y|\} = 1$, což je maximální možná hodnota této absolutní hodnoty, tím je podmínka splněna. Pokud jsou oba sčítanci nula, tak je součet nula i maximum nula.

Nyní pojďme spojit poslední dvě strany dohromady a vytvořme p-adickou absolutní hodnotu. Určitě jste si všimli podobnosti druhé vlastnosti z lemmatu 2.1.1 a ne-archimédovské vlastnosti v definici 2.1.2. Akorát valuace součtu je větší než minimum a absolutní hodnota součtu je menší než maximum. Takže chceme využít valuace na vytvoření absolutní hodnoty s přesně opačnou vlastností. Což vytvoříme následovně:

Definice 2.1.3. *Pro každé nenulové $x \in \mathbb{Q}$ definujeme jeho p-adickou absolutní hodnotu jako:*

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

Pokud $x = 0$, pak $|x|_p = 0$.

Všimněte si, že $|x|_p = 0$ pro $x = 0$, odpovídá tomu, že jsme definovali $v_p(0) = \infty$.

Ověřme, že tato funkce skutečně splňuje podmínky pro to být absolutní hodnotou. Většina plyne z lemmatu 2.1.1.

i) $|x| = 0$ právě tehdy když $x = 0$ – To určitě platí, protože pro $x \neq 0$, je $|x|_p = p^{-n}, n \in \mathbb{Z}$, což je větší než nula.

ii) $|xy| = |x||y|$ – Což platí díky první vlastnosti p-adických valuací z lemmatu 2.1.1 : $|xy|_p = p^{-v_p(xy)} = p^{-v_p(x)}p^{-v_p(y)} = |x|_p|y|_p$.

iii) ne-archimédovská absolutní hodnota: $|x + y| \leq \max\{|x|, |y|\}$ – Dokážeme pomocí druhé vlastnosti p-adických valuací z lemmatu 2.1.1:
$|x + y| = p^{-v_p(x+y)} \leq p^{-(\min\{v_p(x), v_p(y)\})} = \max\{p^{-v_p(x)}, p^{-v_p(y)}\} = \max\{|x|, |y|\}$.

Takže nejen, že je to skutečně absolutní hodnota, ale je to dokonce ne-archimédovská absolutní hodnota. Což, jak uvidíme za chvíli, dá metrickému prostoru s p-adickou absolutní hodnotou jednu zajímavou vlastnost.

2.2 Tvorba $\mathbb{Q}_p$

Nejprve si definujme, co je to metrický prostor, o kterém jsem se zmínila na začátku při vysvětlování zúplnění.

Definice 2.2.1. *Metrický prostor je neprázdná množina M spolu s metrikou ρ (vzdáleností), funkcí definovanou jako:*

$$\rho : M \times M \longrightarrow \mathbb{R}^0_+$$

kde pro libovolná $x, y, z \in M$ platí:

i) $\rho(x,y) = 0$ *právě tehdy, když* $x = y$,

ii) $\rho(x,y) = \rho(y,x)$,

iii) trojúhelníková nerovnost: $\rho(x,z) \leq \rho(x,y) + \rho(y,z)$.

Nyní již můžeme korektně definovat zúplnění.

Definice 2.2.2. *Metrický prostor M nazveme zúplněním metrického prostoru X, je-li M úplný metrický prostor a X je jeho hustým podprostorem.*

Když definujeme p-adickou metriku na $\mathbb{Q}$ předpisem $\rho(x,y) = |x-y|_p$, je z definice p-adické absolutní hodnoty jasné, že spolu s racionálními čísly tvoří metrický prostor.

Pokud metrika splňuje podmínku

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

říkáme jí ultrametrika. Příkladem může být naše p-adická metrika, protože p-adická absolutní hodnota je ne-archimédovská. Pro všechny ultrametriky platí následující tvrzení.

Lemma 2.2.1. *V ultrametrickém prostoru jsou všechny trojúhelníky rovnoramenné.*

Důkaz: Dokonce platí, že pokud se nejedná o rovnostranný trojúhelník, tak jsou ramena tohoto rovnoramenného trojúhelníka delší než základna. Mějme prvky x, y, z našeho ultrametrického metrického prostoru. Ukážeme, že pokud $\rho(x,y) \neq \rho(y,z)$, tak platí:

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

Díky symetrii mezi x a z můžeme bez újmy na obecnosti předpokládat, že $\rho(x,y) < \rho(y,z)$. Z ultrametrické nerovnosti plyne $\rho(x,z) \leq \max\{\rho(x,y), \rho(y,z)\} = \rho(y,z)$. Podobně $\rho(y,z) \leq \max\{\rho(y,x), \rho(x,z)\} = \max\{\rho(x,y), \rho(x,z)\}$. Maximum vpravo nemůže být $\rho(x,y)$, protože $\rho(x,y) < \rho(y,z)$. Je to tedy $\rho(x,z)$. Z čehož dostaneme $\rho(x,z) = \rho(y,z)$, což jsme chtěli dokázat. □

Vzhledem k tomu, že $\mathbb{Q}$ s p-adickou absolutní hodnotou je ultrametrický prostor se vzdálenostní funkcí $|\ |_p$, jsou v tomto prostoru všechny trojúhelníky rovnoramenné. Povšimněme si, že to odpovídá tomu, co jsme dostali v lemmatu 2.1.1. Této vlastnosti využijeme několikrát již v této kapitole.

Pro tento metrický prostor lze užít definice cauchyovské posloupnosti, úplnosti, otevřených koulí a husté podmnožiny tak, jak jsme je definovali na začátku kapitoly, jenom je všude místo normální absolutní hodnoty ta p-adická. Pro cauchyovské posloupnosti s p-adickou absolutní hodnotou ovšem platí silnější podmínka.

Lemma 2.2.2. *Posloupnost (x_n) racionálních čísel je cauchyovská vzhledem k ne-archimédovské absolutní hodnotě $|\ |_p$, právě tehdy, když:*

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

Důkaz: Jestliže $m = n + r > n$, dostaneme z ne-archimédovské vlastnosti:

$$|x_m - x_n|_p = |x_{n+r} - x_{n+r-1} \cdots + x_{n+1} - x_n|_p \leq \max\{|x_{n+r} - x_{n+r-1}|_p, \ldots, |x_{n+1} - x_n|_p\}.$$

Ze zadání víme, že pro každé $\varepsilon > 0$ existuje N takové, že pro každé $a > N$ je splněna rovnost $|x_{a+1} - x_a|_p < \varepsilon$. Pokud je $n > N$, je toto maximum menší než ε.

Takže nám počáteční podmínka $\lim_{n\to\infty} |x_{n+1} - x_n|_p = 0$ skutečně stačí k tomu, aby byla posloupnost cauchyovská. □

Nyní je potřeba ukázat, že $\mathbb{Q}$ není s p-adickou absolutní hodnotou úplný prostor. Musíme najít posloupnost racionálních čísel, která je cauchyovská vzhledem k p-adické absolutní hodnotě, ale nekonverguje p-adicky v $\mathbb{Q}$.

Příklad: Posloupnost, na které si nyní ukážeme neúplnost tohoto prostoru, je docela zajímavá. V tělese, které později dostaneme zúplněním $\mathbb{Q}$ s p-adickou absolutní hodnotou, bude konvergovat k netriviální $(p-1)$-ní odmocnině z jedné. Dokazovat, že v tomto tělese takové číslo skutečně leží, budeme v páté kapitole. Nicméně z toho plyne, že těleso, které budeme po tomto příkladu sestrojovat, není podmnožinou reálných čísel.

Mějme $p > 3$ a $a \in \mathbb{Z}$, pro které platí $1 < a < p-1$. Následně si vezmeme cauchyovskou posloupnost (x_n), kde $x_n = a^{p^n}$. Samozřejmě nejdříve musíme ukázat, že se skutečně jedná o cauchyovskou posloupnost. Díky lemmatu 2.2.2 nám stačí dokázat, že:

$$\lim_{n\to\infty} |a^{p^{n+1}} - a^{p^n}|_p = 0.$$

Indukcí dokážeme, že $p^n | (a^{p^{n+1}} - a^{p^n})$:

1. Ukažme, že dokazované platí pro $n = 0$. Jistě $p^0 = 1 \mid (a^p - a)$.

2. Pro $n \geq 0$ ukažme, že pokud $p^n | (a^{p^{n+1}} - a^{p^n})$, pak $p^{n+1} | (a^{p^{n+2}} - a^{p^{n+1}})$:

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

Z Malé Fermatovy věty víme, že $a^p \equiv a \pmod p$ pro libovolné a. Když využijeme této vlastnosti, můžeme odvodit, že $a^{p^n} \equiv (a^{p^{n-1}})^p \equiv a^{p^{n-1}} \equiv a^{p^{n-2}} \equiv a^p \equiv a \pmod p$ pro libovolné nezáporné celé n. Z toho je vidět, že:

$$((a^{p^{n+1}})^{p-1} + (a^{p^{n+1}})^{p-2}(a^{p^n}) + \cdots + (a^{p^n})^p) \equiv a^{p-1} + a^{p-2}a + \cdots + a^{p-1} = (pa^{p-1}) \equiv 0 \pmod p$$

$$\Rightarrow p | ((a^{p^{n+1}})^{p-1} + (a^{p^{n+1}})^{p-2}(a^{p^n}) + \ldots (a^{p^n})^{p-1}) \Rightarrow p^{n+1} | (a^{p^{n+2}} - a^{p^{n+1}}).$$

Z toho, že rozdíl po sobě jdoucích čísel naší posloupnosti dělí čím dál větší mocnina p, plyne, že absolutní hodnota tohoto rozdílu je čím dál menší, tudíž

$$\lim_{n\to\infty} |a^{p^{n+1}} - a^{p^n}|_p = 0.$$

Nyní tedy máme cauchyovskou posloupnost a musíme ukázat, že nekonverguje v $\mathbb{Q}$.

Nechť x je limita naší posloupnosti $(x_n) = (a^{p^n})$. Tato limita ovšem není reálná, jedná se o p-adickou limitu. Později v textu budeme s p-adickými limitami pracovat a uvidíme, že i vůči p-adické metrice je limita součinu posloupností součin jejich limit. Proto pro tuto limitu x bude platit:

$$x = \lim_{n\to\infty} x_n = \lim_{n\to\infty} x_{n+1} = \lim_{n\to\infty} x_n^p = (\lim_{n\to\infty} x_n)^p = x^p.$$

Pokud by $x \in \mathbb{Q}$, pak by $x = \pm 1$ (p je liché, takže -1 to též splňuje) nebo $x = 0$, protože pro žádné jiné racionální číslo neplatí, že $x^p = x$.

Nejprve ukážeme, že $|x - a|_p < 1$. Jak jsem psala před chvílí, pro libovolné $y \in \mathbb{Z}$ a n platí $y^{p^n} \equiv y \pmod p$ a tudíž z toho, jak je definovaná naše posloupnost, by muselo i x

být kongruentní s a, pokud by leželo v $\mathbb{Q}$. Proto $|x-a|_p < 1$, z čehož plyne, že $p|(x-a)$. Což ovšem neplatí ani pro nulu ani pro $x = \pm 1$, protože $1 < a < p-1$.

Z čehož plyne, že $\mathbb{Q}$ není úplné vzhledem k p-adické absolutní metrice, protože existuje cauchyovská posloupnost racionálních čísel, která p-adicky nekonverguje v $\mathbb{Q}$.

Z vlastností této posloupnosti je vidět, že by skutečně mohla konvergovat k nějaké netriviální $(p-1)$-ní odmocnině z jedné, jak jsem zmiňovala na začátku. Limita této posloupnosti splňuje $x^{p-1} = 1$. Víme, že to není nula, takže jsme $x^p = x$ mohli podělit. □

Když už víme, že těleso racionálních čísel není úplné vzhledem k p-adické absolutní hodnotě, pojďme vytvořit těleso, které bude obsahovat $\mathbb{Q}$ a bude úplné vzhledem k absolutní hodnotě, která na $\mathbb{Q}$ bude splývat s p-adickou metrikou.

Jak jsem říkala na začátku, zúplnění je jednoduše přidání limit cauchyovských posloupností. Jenže není snadné určit, co jsou ty limity, takže to musíme udělat jinak. Nejdříve vytvoříme okruh cauchyovských posloupností.

Definice 2.2.3. *Zvolme pevně prvočíslo p a uvažme ne-archimédovskou absolutní hodnotu $|\ |_p$ na $\mathbb{Q}$. Potom $\mathcal{C}$ označme množinu všech cauchyovských posloupností prvků z $\mathbb{Q}$:*

$$\mathcal{C} = \{(x_n) | (x_n) \text{ je posloupnost racionálních čísel cauchyovská vzhledem k } |\ |_p\}$$

Lemma 2.2.3. *Mějme dvě cauchyovské posloupnosti, potom pro jejich součet a součin definován následovně:*

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

platí, že taky leží v $\mathcal{C}$, jinými slovy jsou to cauchyovské posloupnosti.

Důkaz: Součet dokážeme jednoduše:

$$\lim_{n\to\infty} |(x_n + y_n) - (x_{n+1} + y_{n+1})|_p = \lim_{n\to\infty} |(x_n - x_{n+1})|_p + \lim_{n\to\infty} |(y_n - y_{n+1})|_p = 0.$$

Součin je trochu trikovější:

$$\lim_{n\to\infty} |(x_n y_n) - (x_{n+1} y_{n+1})|_p = \lim_{n\to\infty} |x_n(y_n - y_{n+1})|_p + \lim_{n\to\infty} |y_{n+1}(x_n - x_{n+1})|_p.$$

Víme, že rozdíly v závorkách se blíží k nule. Vzhledem k tomu, že obě posloupnosti jsou cauchyovské, tak je velikost jejich členů ohraničená. Proto musí platit, že:

$$\lim_{n\to\infty} |x_n(y_n - y_{n+1})|_p + \lim_{n\to\infty} |y_{n+1}(x_n - x_{n+1})|_p = 0.$$

Takže i součin dvou cauchyovských posloupností je cauchyovská posloupnost. □

Důsledek 2.2.1. *$\mathcal{C}$ spolu s násobením a sčítáním tvoří komutativní okruh.*

Důkaz: Díky lemmatu 2.2.3 je vidět, že na členech posloupnosti provádíme klasické sčítání a násobení racionálních čísel. Racionální čísla se sčítáním a násobením tvoří komutativní okruh a tedy vše plyne z toho. Nulou v tomto okruhu je cauchyovská posloupnost z nul a jedničkou v tomto okruhu je cauchyovská posloupnost ze samých jedniček. □

Pomocí tohoto okruhu budeme chtít popsat p-adická čísla. Aby tento okruh mohl být zúplněním racionálních čísel, musí v něm prvně ležet racionální čísla. Každé racionální

číslo x proto ztotožníme s cauchyovskou posloupností skládající se ze samých x, tj. s konstantní posloupností (x).

Bohužel tento okruh nemůže být naším zúplněním, protože za prvé můžeme mít více cauchyovských posloupností konvergujících ke stejnému číslu a za druhé to není těleso (můžeme mít dvě nenulové cauchyovské posloupnosti, jejichž součin bude 0). Oba tyto problémy můžeme vyřešit faktorizací pomocí vhodného maximálního ideálu.

Definice 2.2.4. *Definujeme ideál $\mathcal{N} \subset \mathcal{C}$:*

$$\mathcal{N} = \{(x_n) | \lim_{n\to\infty} |x_n|_p = 0\}.$$

Jedná se o množinu všech cauchyovských posloupností konvergujících p-adicky k nule.

Než ukážeme, že je tento ideál skutečně maximální, musíme dokázat následující pomocné lemma, které se nám později bude hodit i v p-adické analýze.

Lemma 2.2.4. *Mějme $(x_n) \in \mathcal{C}, (x_n) \notin \mathcal{N}$. Pro takovou posloupnost platí, že existuje N takové, že $|x_n|_p = |x_m|_p$,* kdykoli platí, že $m \geq N, n \geq N$.

Důkaz: Protože $(x_n) \notin \mathcal{N}$, existuje $c > 0$ tak, že pro každé N existuje $n > N$ s vlastností $|x_n|_p \geq c$. Vzhledem k tomu, že (x_n) je cauchyovská, pro číslo c existuje M takové, že pro všechna $i > M$, $j > M$ je $|x_i - x_j|_p < c$. Ovšem i pro M existuje $n > M$ tak, že $|x_n|_p \geq c$. Potom ale $|x_j|_p \geq c$ pro všechna $j > M$. Kdyby $|x_j|_p < c$, dostali bychom:

$$c \leq |x_n|_p = |x_j + (x_n - x_j)|_p \leq \max\{|x_j|_p, |x_n - x_j|_p\} < c,$$

což je spor.

Ovšem potom platí

$$i > M, j > M \Rightarrow |x_i - x_j|_p < \max\{|x_i|_p, |x_j|_p\}.$$

A z lemmatu 2.2.1 víme, že v ne-archimédovském metrickém prostoru jsou všechny trojúhelníky rovnoramenné, a proto musí být $|x_i|_p = |x_j|_p$ pro všechna $i > M$, $j > M$. □

Lemma 2.2.5. *$\mathcal{N}$ je maximální ideál v $\mathcal{C}$.*

Důkaz: $\mathcal{N}$ je určitě ideál, protože rozdíl dvou cauchyovských posloupností konvergujících k 0 je určitě opět cauchyovská posloupnost konvergující k nule. A díky tomu, že velikost členů libovolné cauchyovské posloupnosti (y_n) je ohraničená, tak když $(x_n) \in \mathcal{N}$, pak $(y_n)(x_n) \in \mathcal{N}$.

Abychom dokázali, že je to maximální ideál, přidáme k němu libovolnou posloupnost $(z_n) \in \mathcal{C}$, $(z_n) \notin \mathcal{N}$. Pak musíme ukázat, že v ideálu $\mathcal{I}$, generovaném $\mathcal{N}$ a (z_n), musí ležet 1, a proto už je to celý okruh a původní ideál byl maximální.

Z předchozího lemma 2.2.4 víme, že existuje kladné ε a k němu přirozené číslo M takové, že pro všechna $i \geq M$, platí, že $|z_i|_p \geq \varepsilon$. Nyní můžeme definovat y_n jako 0 pro $n < M$ a jako $\frac{1}{z_n}$ pro $n \geq M$. Dokažme, že tato posloupnost (y_n) leží v $\mathcal{C}$.

Pro každé $i \geq M$, $j \geq M$ platí $y_i - y_j = \frac{z_i - z_j}{z_i z_j}$, a tedy $|y_i - y_j|_p = \frac{|z_i - z_j|_p}{|z_i z_j|_p} \leq \frac{|z_i - z_j|_p}{\varepsilon^2}$. Protože ε je kladná konstanta a posloupnost (z_n) je cauchyovská, tak odtud plyne, že i posloupnost (y_n) je cauchyovská.

Jestliže posloupnost (z_n) vynásobíme cauchyovskou posloupností (y_n), dostaneme posloupnost, která bude mít na $M - 1$ místech nuly a pak již samé jedničky. Pak platí:

$$1 \in \mathcal{I}, \text{ protože } 1 - (z_n)(y_n) \in \mathcal{N}.$$

Proto je ideál $\mathcal{N}$ maximální. □

A protože faktorizací komutativního okruhu podle maximálního ideálu dostaneme těleso, můžeme již definovat p-adická čísla.

Definice 2.2.5. *Těleso p-adických číslel definujeme jako faktorokruh komutativního okruhu $\mathcal{C}$ podle maximálního ideálu $\mathcal{N}$:*

$$\mathbb{Q}_p = \mathcal{C}/\mathcal{N}.$$

Touto faktorizací jsme ztotožnili všechny cauchyovské posloupnosti, které měly stejnou limitu. Takže $\mathbb{Q}_p$ je skutečně $\mathbb{Q}$ zvětšené o limity cauchyovských posloupností.

Racionální číslo a ztotožníme s třídou obsahující konstantní posloupnost (a). Různá racionální čísla ztotožníme s různými třídami, protože kdyby byla nějaká dvě racionální čísla ve stejné třídě, musela by konstantní posloupnost, jejíž každý člen je roven rozdílu těchto racionálních čísel, ležet v $\mathcal{N}$, což neleží.

Nyní potřebujeme rozšířit p-adickou absolutní hodnotu i na čísla z $\mathbb{Q}_p$, která nejsou racionální. Na to se nám bude opět hodit lemma 2.2.4.

Definice 2.2.6. *Mějme $\lambda \in \mathbb{Q}_p$. Vezměme si libovolnou cauchyovskou posloupnost (x_n), z této levé třídy rozkladu λ. Potom definujeme absolutní hodnotu $|\lambda|_p$ následovně:*

$$|\lambda|_p = \lim_{n\to\infty} |x_n|_p.$$

Ještě si musíme uvědomit, že je tato definice korektní. Tedy, že dvě posloupnosti ze stejné levé třídy mají tuto limitu stejnou.

Nejprve se podívejme na případ, kdy λ je $\mathcal{N}$. Pak pro každou posloupnost $(x_n) \in \mathcal{N}$ platí z definice $\lim_{n\to\infty} |x_n|_p = 0$ a tudíž mají skutečně limitu absolutních hodnot všechny stejnou.

Pokud naopak λ není $\mathcal{N}$, pak pro libovolné $(x_n) \in \lambda$, $(y_n) \in \lambda$ podle lemmatu 2.2.4 existuje N takové, že pro každé $m \geq N$ hodnota $|x_m|_p$ nezávisí na m, řekněme $|x_m|_p = a > 0$. Stejně tak existuje M takové, že pro každé $m \geq M$ hodnota $|y_m|_p$ nezávisí na m, řekněme $|y_m|_p = b > 0$. Pak jistě $\lim_{n\to\infty} |x_n|_p = a$ a $\lim_{n\to\infty} |y_n|_p = b$.

Důkaz povedeme sporem. Bez újmy na obecnosti předpokládejme, že $a > b$. Protože (x_n) a (y_n) leží v téže třídě, platí $(x_n - y_n) \in \mathcal{N}$ a pro toto $b > 0$ existuje K takové, že pro každé $n > K$ platí $|x_n - y_n|_p < b$. Pak ovšem pro libovolné $n > \max\{N, M, K\}$ platí $a = |x_n|_p = |y_n + (x_n - y_n)|_p \leq \max\{|y_n|_p, |x_n - y_n|_p\} = b$, což je spor.

Abychom mohli prohlásit $\mathbb{Q}_p$ s p-adickou absolutní hodnotou za zúplnění $\mathbb{Q}$, musíme ještě pár věcí dokázat.

Nejprve vůbec musíme ověřit, že absolutní hodnota, jak jsme ji nyní definovali, splňuje podmínky absolutní hodnoty z definice 2.1.2. Při dokazování, že definice 2.2.6 je korektní, jsme zjistili, že absolutní hodnota třídy $\mathcal{N}$ je nula a absolutní hodnota jakékoli jiné třídy je kladná, takže $|x|_p = 0$, právě tehdy, když $x \in \mathcal{N}$. Vzhledem k tomu, že z lemmatu 2.2.3 víme, že $(x_n)(y_n) = (x_n y_n)$, platí i $|x|_p|y|_p = |xy|_p$, kde $x, y \in \mathbb{Q}_p$. Ukažme, že vzhledem k tomu, že $\mathbb{Q}$ s p-adickou metrikou je ultrametrický prostor, splňuje tato absolutní hodnota i bod iv) z definice 2.1.2. Pokud je x, y nebo $x+y$ nulové, je tato podmínka jistě splněna. A jestliže jsou nenulové, můžeme si zvolit posloupnosti (x_n) z x a (y_n) z y. Podle lemmatu 2.2.4 jsou posloupnosti $(|x_n|_p)$, $(|y_n|_p)$ a $(|x_n + y_n|_p)$ od určitého koeficientu konstantní. Potom pro všechna j větší než dostatečně velké N platí, že $|x_j|_p = |x|_p$, $|y_j|_p = |y|_p$ a $|x_j + y_j|_p = |x + y|_p$.

Jediné, co je ještě potřeba si uvědomit je, že tato absolutní hodnota je na $\mathbb{Q}$ stejná jako p-adická absolutní hodnota definovaná v 2.1.3.

Následně je potřeba dokázat, že $\mathbb{Q}$ je v tomto prostoru hustou množinou. A následně ukázat, že je tento metrický prostor úplný. Tak jsme to definovali na začátku této kapitoly.

Věta 2.2.1. *Obraz $\mathbb{Q}$ v zobrazení $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ je hustou množinou $\mathbb{Q}_p$.*

Důkaz: Zobrazení, o kterém se ve větě mluví, je zobrazení racionálních čísel na třídu obsahující jejich konstantní posloupnost.

Musíme dokázat, že pokud máme prvek z $\lambda \in \mathbb{Q}_p$, tak pak v libovolně malé otevřené kouli s poloměrem ε, $B(\lambda, \varepsilon)$, leží racionální číslo - třída rozkladu obsahující konstantní posloupnost.

Vezměme si cauchyovskou posloupnost $(x_n) \in \lambda$. Potom musí platit, že od určitého indexu N je $|x_n - x_m|_p < \varepsilon$ pro všechna $m, n \geq N$.

Můžeme si nyní vzít racionální číslo $y = x_N$. Což je jakožto prvek $\mathbb{Q}_p$ levá třída obsahující konstantní posloupnost (y). Dokažme, že y leží v otevřené kouli $B(\lambda, \varepsilon)$, tj. $|\lambda - y|_p < \varepsilon$.

Vzhledem k tomu, že $\lambda - y$ je levá třída obsahující posloupnost $(x_n - y)$, platí

$$|\lambda - y|_p = \lim_{n\to\infty} |x_n - y|_p.$$

Ale my víme, že pro $n \geq N$

$$|x_n - y|_p = |x_n - x_N|_p < \varepsilon.$$

Potom v limitě dostaneme

$$\lim_{n\to\infty} |x_n - y|_p < \varepsilon.$$

Tudíž (y) skutečně leží otevřené kouli $B(\lambda, \varepsilon)$.

S reálnou absolutní hodnotou by poslední nerovnost neplatila, protože by se mohlo stát, že všechny prvky posloupnosti jsou menší než ε a přitom limita by byla v absolutní hodnotě rovna ε. My ale z rozboru za definicí 2.2.6 víme, že tato situace nikdy v p-adickém případě nastat nemůže, protože posloupnost p-adických absolutních hodnot je buď od jistého místa konstantní nebo konverguje k nule. □

Abychom nyní dokázali poslední bod, a to, že je $\mathbb{Q}_p$ s p-adickou absolutní hodnotou úplný prostor, musíme ukázat, že v něm leží všechny limity cauchyovských posloupností prvků z $\mathbb{Q}_p$, tedy cauchyovských posloupností těchto levých tříd cauchyovských posloupností.

Věta 2.2.2. *$\mathbb{Q}_p$ tvoří s p-adickou metrikou úplný prostor.*

Důkaz: Nechť $\lambda_1, \lambda_2, \ldots, \lambda_n, \ldots$ jsou prvky z $\mathbb{Q}_p$, tvořící cauchyovskou posloupnost. Označme $N_0 = 1$. Pro každé $k \in \mathbb{N}$ zvolme $N_k > N_{k-1}$ takové, aby pro všechna $m \geq N_k$, $n \geq N_k$ platilo $|\lambda_n - \lambda_m|_p < \frac{1}{p^k}$. Takové N_k existovat musí, protože tyto prvky tvoří cauchyovskou posloupnost.

Z předchozí věty 2.2.1 plyne, že musí existovat i $y_k \in \mathbb{Q}$ takové, že pro něj bude platit $|y_k - \lambda_{N_k}|_p < \frac{1}{p^k}$. Ukažme, že posloupnost (y_k) těchto racionálních čísel je cauchyovská vzhledem k p-adické metrice. Pro $n \geq k$, $m \geq k$ platí

$$|y_m - y_n|_p = |(y_m - \lambda_{N_m}) - (y_n - \lambda_{N_n}) + (\lambda_{N_m} - \lambda_{N_n})|_p$$
$$\leq \max\{|y_m - \lambda_{N_m}|_p, |y_n - \lambda_{N_n}|_p, |\lambda_{N_m} - \lambda_{N_n}|_p\} < \frac{1}{p^k}.$$

Takže je posloupnost (y_k) skutečně cauchyovská.

Označme $\gamma \in \mathbb{Q}_p$ levou třídu obsahující (y_k) a ukažme, že γ je limitou posloupnosti $\lambda_1, \lambda_2, \ldots, \lambda_n, \ldots$. Pro libovolné $k \in \mathbb{N}$ platí, že pro každé $m \geq N_k$ je $|\lambda_m - \lambda_{N_k}|_p < \frac{1}{p^k}$ a zároveň $|y_k - \lambda_{N_k}|_p < \frac{1}{p^k}$, vzhledem k tomu, jak jsme tato čísla definovali. Též platí

$$|\gamma - y_k|_p = \lim_{n\to\infty} |y_n - y_k|_p \leq \frac{1}{p^k}.$$

Z čehož dostaneme pro všechna $n \geq N_k$

$$|\lambda_n - \gamma|_p = |(\lambda_n - \lambda_{N_k}) - (y_k - \lambda_{N_k}) - (\gamma - y_k)|_p \leq \max\{|\lambda_n - \lambda_{N_k}|_p, |y_k - \lambda_{N_k}|_p, |\gamma - y_k|_p\} \leq \frac{1}{p^k}.$$

A protože poslední nerovnost platí pro všechna $k \in \mathbb{N}$, je γ limitou posloupnosti $\lambda_1, \lambda_2, \ldots$. Proto každá cauchyovská posloupnost prvků z $\mathbb{Q}_p$ má v $\mathbb{Q}_p$ limitu, takže tento prostor je úplný. □

Způsob, jakým jsme v této kapitole sestrojili $\mathbb{Q}_p$, není jediným způsobem, jak toto těleso vytvořit.

V matematice se často využívá výstavba celých p-adických čísel, o kterých si budeme povídat v příští kapitole, pomocí takzvané inverzní limity. A následně se pak $\mathbb{Q}_p$ definuje jako podílové těleso tohoto oboru integrity. Podrobněji se tímto případem zabývají například v [7] či v [9].

Dalším možným způsobem je definovat p-adická čísla jako

$$\mathbb{Q}_p = \Big\{ \sum_{n=n_0}^{\infty} c_n p^n \;\Big|\; n_0 \in \mathbb{Z}, c_n \in \{0, 1, \ldots, p-1\} \Big\}.$$

Tento způsob je sice nejméně abstraktní, nicméně se příliš nevyužívá, protože například definovat zde násobení a sčítaní explicitně je trochu obtížné a nepřehledné.

O výhodách či nevýhodách těchto postupů si můžete přečíst například v [6] či v [7].

Důvodem, proč jsem zvolila tento způsob výstavby $\mathbb{Q}_p$, je, že krásně ukazuje korespondenci s $\mathbb{R}$. Navíc v p-adické analýze budeme stejně potřebovat pracovat s $\mathbb{Q}_p$ jako s metrickým prostorem.

Kapitola 3

Vlastnosti p-adických čísel

3.1 Celá p-adická čísla

Stejně jako množina racionálních čísel obsahuje podmnožinu celých čísel, obsahuje i množina p-adických čísel podmnožinu takzvaných celých p-adických čísel.

Definice 3.1.1. *Množinu celých p-adických čísel definujeme jako*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}.$$

Jedná se o podmnožinu $\mathbb{Q}_p$, která je uzavřená na sčítání a násobení. Vezměme si $x, y \in \mathbb{Z}_p$, potom $|x+y|_p \leq \max\{|x|_p, |y|_p\} \leq 1$ a $|xy|_p = |x|_p \cdot |y|_p \leq 1$, tudíž $x+y$ i xy leží v $\mathbb{Z}_p$. Celá p-adická čísla tedy tvoří podokruh okruhu p-adických čísel.

Je vidět, že tato množina obsahuje všechna celá čísla (respektive třídy, které obsahují konstantní posloupnosti celých čísel), protože všechna celá čísla jsou v p-adické absolutní hodnotě menší nebo rovny jedné.

Pojďme si ale ukázat, že se nejedná jen o podmnožinu $\mathbb{Q}_p$ obsahující celá čísla, ale že je to dokonce zúplnění $\mathbb{Z}$ s p-adickou absolutní hodnotou.

Na to ovšem nejprve potřebujeme dokázat následující dvě lemmata.

Lemma 3.1.1. *$\mathbb{Z}$ je hustou množinou v $\mathbb{Z}_p$. Mějme $x \in \mathbb{Z}_p$, potom pro každé $n \in \mathbb{N}$ existuje jediné $\alpha \in \mathbb{Z}$ takové, že $0 \leq \alpha \leq p^n - 1$ a $|x - \alpha|_p \leq p^{-n}$.*

Důkaz: Mějme $x \in \mathbb{Z}_p$. Protože $\mathbb{Q}$ je hustou podmnožinou v $\mathbb{Q}_p$, víme, že pro každé $x \in \mathbb{Z}_p$ a $n \in \mathbb{N}$ existuje racionální číslo (v základním tvaru) $\frac{a}{b}$, $a, b \in \mathbb{Z}$, takové, že

$$\left|x - \frac{a}{b}\right|_p \leq p^{-n} < 1.$$

Abychom lemma dokázali, musíme ukázat, že vždy existuje celé číslo, které tuto podmínku splňuje.

Z předchozí nerovnosti plyne

$$\left|\frac{a}{b}\right|_p \leq \max\left\{|x|_p, \left|\frac{a}{b} - x\right|_p\right\} \leq 1.$$

Což znamená, že $\frac{a}{b} \in \mathbb{Z}_p$, tedy $p \nmid b$. Proto pro b existuje $b' \in \mathbb{Z}$ takové, že $bb' \equiv 1 \pmod{p^n}$. Potom platí

$$\left|\frac{a}{b} - ab'\right|_p = \left|\frac{a(1-bb')}{b}\right|_p \leq p^{-n},$$

protože z definice b' plyne, že $p^n|(1-bb')$. Z čehož dostaneme, že

$$|x-ab'|_p = \left|\left(x-\frac{a}{b}\right)-\left(ab'-\frac{a}{b}\right)\right|_p \leq \max\left\{\left|x-\frac{a}{b}\right|_p, \left|ab'-\frac{a}{b}\right|_p\right\} \leq p^{-n}.$$

Nyní je potřeba ukázat, že jde vybrat ab' takové, že $0 \leq ab' \leq p^n-1$. A ukázat jeho jednoznačnost. Vezměme si $0 \leq \alpha \leq p^n-1$ takové, že $\alpha \equiv ab' \pmod{p^n}$. Potom

$$|x-\alpha|_p = |x-ab'+ab'-\alpha|_p \leq \max\{|x-ab'|_p, |ab'-\alpha|_p\} \leq p^{-n}.$$

Tudíž takové α skutečně splňuje podmínku. Jestliže také $\beta \in \mathbb{Z}$ splní podmínku $|x-\beta|_p \leq p^{-n}$, pak $|\alpha-\beta|_p = |(x-\beta)-(x-\alpha)|_p \leq \max\{|x-\alpha|_p, |x-\beta|_p\} \leq p^{-n}$ a tedy $\alpha \equiv \beta \pmod{p^n}$, a proto α s požadovanými vlastnostmi existuje jediné.

Takže $\mathbb{Z}$ je skutečně hustou podmnožinou v $\mathbb{Z}_p$. □

Lemma 3.1.2. *Pro každé $x \in \mathbb{Z}_p$ existuje cauchyovská posloupnost (α_n) convergující k x, vypadající následovně:*

- *pro každé $n \in \mathbb{N}$: $\alpha_n \in \mathbb{Z}$ splňuje $0 \leq \alpha_n \leq p^n-1$,*
- *pro všechna $n \geq 2$ platí $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$.*

Taková posloupnost je pro každé $x \in \mathbb{Z}_p$ jedinečná.

Důkaz: V minulém lemmatu jsme dokázali, že tyto α_n existují a jsou jedinečná, pokud splňují navíc ještě podmínku $|x-\alpha_n|_p \leq p^{-n}$. Pojďme dokázat, že to musí splňovat i α_n z tohoto lemma.

Pokud taková celá čísla α_n mají existovat, z toho, že limita α_n je x, plyne, že pro každé $n \in \mathbb{N}$ existuje M takové, že pro každé $m \geq M$ platí $|x-\alpha_m|_p \leq p^{-n}$. Je-li $n \geq M$, máme potřebnou nerovnost, je-li naopak $n < M$, z kongruencí plyne $|\alpha_n - \alpha_M|_p \leq p^{-n}$, odkud potřebná nerovnost plyne. Proto pro dané x a libovolné přirozené číslo n zvolíme α_n jako to jediné číslo, které splňuje podmínky lemmatu 3.1.1 pro tato x, n.

Každá taková posloupnost α_n musí z definice konvergovat k x.

V předchozím důkaze jsme též ukázali, že v množině $\{0,1,\ldots,p^{n-1}-1\}$ leží pouze jediné α_{n-1} splňující $|x-\alpha_{n-1}|_p \leq p^{-(n-1)}$. Což znamená, že pokud $|x-\alpha_n|_p \leq p^{-n}$, musí být $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$. □

Věta 3.1.1. *$\mathbb{Z}_p$ je zúplnění $\mathbb{Z}$ s p-adickou absolutní hodnotou.*

Důkaz: Jak jsem již psala, celá čísla leží v této množině. Musí zde ležet i všechny p-adicky cauchyovské posloupnosti celých čísel, protože limita λ libovolné z těchto posloupností bude splňovat $|\lambda|_p \leq 1$. Pokud se jedná o posloupnost, která nekonverguje k nule, musí mít podle lemmatu 2.2.4 od jistého indexu N platit $|x_n|_p = |x_m|_p$, pro všechna $n \geq N$, $m \geq N$. Potom je $|\lambda|_p = |x_n|_p$, ale x_n je celé číslo, takže skutečně $|\lambda|_p \leq 1$. Pokud se jedná o posloupnost konvergující k nule, je $\lambda = 0 \in \mathbb{Z}_p$.

$\mathbb{Z}_p$ je skutečně zúplnění $\mathbb{Z}$ s p-adickou absolutní hodnotou. □

To, že máme takovéto zúplnění $\mathbb{Z}$ s p-adickou absolutní hodnotou, je další věc, která odlišuje $\mathbb{Q}_p$ od $\mathbb{R}$.

3.1.1 Jednoduší způsob, jak si představovat prvky $\mathbb{Z}_p$

Zatím jsme pracovali s prvky $\mathbb{Z}_p$ a $\mathbb{Q}_p$ jako s třídami rozkladu. Což je poměrně abstraktní a špatně se to představuje.

Způsob, jakým jsme vybírali cauchyovské posloupnosti (α_n), nám pomůže ve zjednodušení představy, jak vlastně takový prvek $x \in \mathbb{Q}_p$ vypadá.

V následující větě budeme pracovat s nekonečnými řadami. Pod takovou nekonečnou řadou si budeme představovat její součet, tedy limitu konvergentní posloupnosti částečných součtů. Na začátku důkazu si dokážeme, že skutečně všechny posloupnosti částečných součtů pro tyto konkrétní nekonečné řady jsou p-adicky cauchyovské, a tedy mají limitu v p-adických číslech.

Věta 3.1.2. *Pro celá p-adická čísla platí*

$$\mathbb{Z}_p = \Big\{ \sum_{n=0}^{\infty} a_n p^n \mid a_n \in \{0, 1, \ldots, p-1\} \Big\}.$$

Každé celé p-adické číslo je součtem řady $\sum_{n=0}^{\infty} a_n p^n$ pro právě jednu posloupnost (a_n) takovou, že každý její prvek patří do množiny $\{0, 1, ..., p-1\}$.

Důkaz: Dokazujeme, že množina všech celých p-adických čísel je rovna množině limit částečných posloupností těchto nekonečných řad. Přesněji řečeno každé z celých p-adických čísel je rovno součtu právě jedné z těchto nekonečných řad.

Máme-li libovolnou posloupnost (a_n) takovou, že každý její prvek patří do množiny $\{0, 1, ..., p-1\}$, platí, že položíme-li $\alpha_n = \sum_{i=0}^{n-1} a_i p^i$ pro každé $n \geq 1$, tak posloupnost (α_n) splňuje obě podmínky lemmatu 3.1.2. Což znamená, že se jedná o cauchyovskou posloupnost, tudíž musí konvergovat k nějakému p-adickému číslu. Navíc žádné dvě řady nemůžou konvergovat ke stejnému číslu, protože pro každé p-adické číslo existuje pouze jedna posloupnost splňující podmínky z lemmatu 3.1.2, která k němu konverguje.

Dále, pro libovolné $x \in \mathbb{Z}_p$ máme posloupnost (α_n) sestrojenou v lemmatu 3.1.2. Z této posloupnosti vyrobíme posloupnost (a_n) takto:

$$\begin{aligned} a_0 &= \alpha_1, \\ a_n &= (\alpha_{n+1} - \alpha_n)/p^n \text{ pro } n > 0. \end{aligned}$$

Pak $a_n \in \{0, 1, ..., p-1\}$ pro každé $n \geq 0$, a současně $\alpha_n = \sum_{i=0}^{n-1} a_i p^i$ pro každé $m \geq 0$, a proto $\sum_{n=0}^{\infty} a_n p^n = \lim_{n\to\infty} \alpha_n = x$. Protože podle lemmatu 3.1.2 je číslem x určena posloupnost α_n jednoznačně, určuje x také posloupnost a_n jednoznačně.

Tedy každé p-adické číslo je rovno součtu právě jedné z těchto nekonečných řad. □

Nyní si můžeme celá p-adická čísla představovat jako takovéto nekonečné řady.

Navíc tato myšlenka jde rozvést na celé $\mathbb{Q}_p$.

Věta 3.1.3. *Každý nenulový prvek $x \in \mathbb{Q}_p$ můžeme zapsat jako řadu*

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

kde $n_0 \in \mathbb{Z}$ splňuje $p^{-n_0} = |x|_p$ a $0 \leq a_n \leq p-1$ pro každé $n \geq n_0$ a $a_{n_0} \neq 0$.

Důkaz: Prvně si ukažme, že každý nenulový prvek $x \in \mathbb{Q}_p$ si můžeme napsat jako $x = p^{n_0}z$, kde $n_0 \in \mathbb{Z}$, $z \in \mathbb{Z}_p$ a $|z|_p = 1$.

Vezměme si tedy $x \in \mathbb{Q}_p$, $x \neq 0$, pak obsahuje toto x cauchyovskou posloupnost (x_n) a $|x|_p = \lim_{n\to\infty} |x_n|_p$. A protože je x nenulové, je $|x_m|_p$ podle lemmatu 2.2.4 od jistého místa konstantní - existuje N takové, že $|x_j| = |x_N|$, pro všechna $j \geq N$. Potom $|x|_p = |x_N|_p$, což je celočíselná mocnina p, $|x|_p = p^{-n_0}$. Pak $|p^{-n_0}x|_p = 1$, a tudíž $z = p^{-n_0}x \in \mathbb{Z}_p$ a $x = p^{n_0}z$.

Protože $z \in \mathbb{Z}_p$, $|z|_p = 1$, a tedy $z = \sum_{n=0}^{\infty} b_n p^n$, kde $b_n \in \{0, 1, \ldots, p-1\}$, $b_0 \neq 0$. Pak stačí položit $a_n = b_{n-n_0}$, pro každé $n \geq n_0$. □

$\mathbb{Z}_p$ a $\mathbb{Q}_p$ v prostoru

Sice si už p-adická čísla umíme představit lépe, ale pořád si je úplně neumíme představit v prostoru - respektive nějak si je rozvrhnout, abychom mohli říct, která dvě p-adická čísla leží blízko sebe. Tato vlastnost se nám bude hodit v příští kapitole, kdy budeme řešit konvergenci nekonečných p-adických řad.

Reálná čísla můžeme uspořádat za sebe na reálnou osu, ale u p-adických čísel není na první pohled jasné, jak by se něco takového dalo udělat.

Definice 3.1.2. *Těleso $\mathcal{F}$ s lineárním uspořádáním $<$ (tranzitivní, asymetrická, trichotomická relace) nazveme uspořádaným tělesem, pokud pro libovolné $a, b, c \in \mathcal{F}$ platí:*

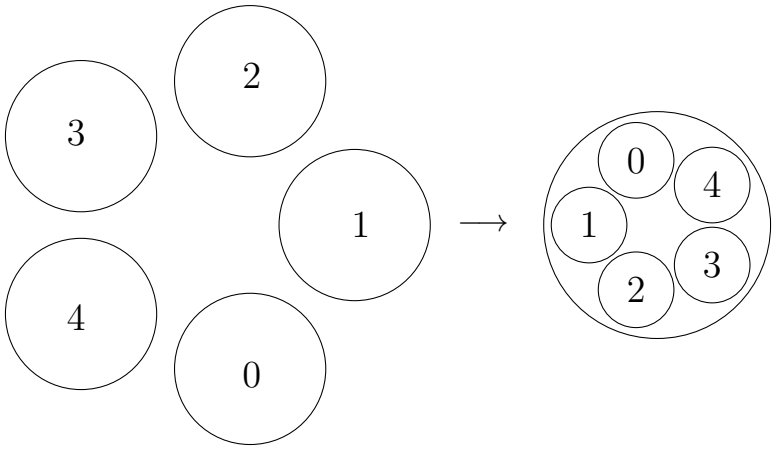
- *pokud $a < b$, potom $a + c < b + c$,*
- *pokud $0 < a$ a $0 < b$, pak $0 < a \cdot b$.*

Jak vidíme, reálná a racionální čísla jsou uspořádanými tělesy.

Zajímavostí je, že pro libovolné těleso existuje lineární uspořádání splňující předchozí definici právě tehdy, když 0 nejde napsat jako součet druhých mocnin nenulových prvků. U reálných a racionálních to zřejmě nejde, naopak v komplexních číslech můžeme napsat $0 = i^2 + 1^2$, takže žádným lineárním uspořádáním nelze z tělesa komplexních čísel vytvořit uspořádané těleso.

Druhým mocninám v tělese p-adických čísel se budeme věnovat v páté kapitole, takže si nyní můžeme dokázat, jak je to s uspořádáním p-adických čísel. Z věty 5.3.2 z konce páté kapitoly plyne, že pro $p \geq 3$ leží v $\mathbb{Q}_p$ druhá odmocnina z $1 - p$, tudíž můžeme psát $0 = (p-1)1^2 + (\sqrt{1-p})^2$. Pro $p = 2$ můžeme naopak využít buď Henselovo lemma, jež definujeme za chvíli, nebo větu 5.3.2 k určení, že v $\mathbb{Q}_2$ leží odmocnina z -7, takže můžeme psát $0 = 1^2 + 1^2 + 1^2 + 2^2 + (\sqrt{-7})^2$. Z čehož tedy plyne, že žádným lineárním uspořádáním nelze z p-adických čísel vytvořit uspořádané těleso.

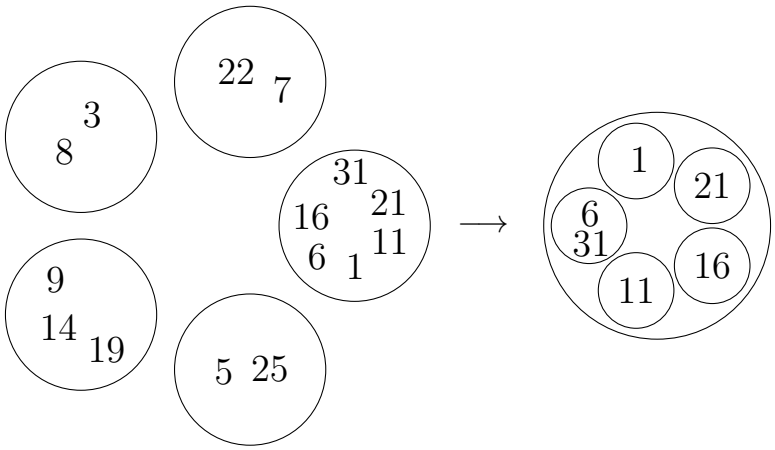
Nicméně posloupnosti (α_n) nám umožňují si celá p-adická čísla představovat následovně. Máme p koleček, v každém z nich p menších koleček a tak to pokračuje dál. Na obrázku vidíme případ, kdy $p = 5$.



Celé p-adické číslo nejprve vyjádříme sumou z věty 3.1.2, a pak je umístíme do kolečka, které odpovídá jeho koeficientu u p^0, v tomto kolečku ho dáme do kolečka (znázorněno vpravo), které odpovídá jeho koeficientu u p^1 atd.

Pro p-adická čísla platí, že čím menší kolečko spolu sdílejí, tím jsou si p-adicky blíže.

Ukažme si to na konkrétních číslech, mějme 5-adická čísla: 1, 3, 5, 6, 7, 8, 11, 14, 16, 19, 21, 22, 25, 31:



Z toho plyne, že 5-adicky jsou si blíže 6 a 11 než 6 a 19. A 31 a 6 jsou si 5-adicky blíže než 31 a 1.

Je vidět, že tento způsob je skutečně praktický a přehledný.

Pro celé $\mathbb{Q}_p$ tato představa funguje stejně, jenom nejde takto nakreslit, protože neexistuje nejmenší možná mocnina p, u které bychom se dívali na koeficienty. Nicméně si to můžeme představit jako, že těchto našich p koleček je v jednom z p stejně velkých koleček množiny $\frac{1}{p}\mathbb{Z}_p$, a to je zase jedno z p ještě větších koleček množiny $\frac{1}{p^2}\mathbb{Z}_p$ atd.

3.2 Henselovo lemma

Henselovo lemma, o kterém jsem mluvila již v úvodu, je velice užitečný nástroj při práci s p-adickými čísly. Pomáhá nám zjistit existenci p-adických kořenů u p-adických polynomů daleko rychleji, než jak to umíme u reálných čísel. Jeho druhá varianta, která je též uvedena níže, nám naopak pomáhá zjistit, zda umíme polynom rozložit v p-adických číslech na lineární činitele.

Vzhledem k tomu, že v této části budeme pracovat s kongruencemi celých p-adických čísel, měli bychom si vysvětlit, jak to funguje.

Mějme celá p-adická čísla α a β, potom $\alpha \equiv \beta \pmod{p^n}$ znamená totéž, co $|\alpha - \beta|_p \leq p^{-n}$. Tedy existuje celé p-adické číslo γ splňující $\alpha - \beta = p^n\gamma$.

Než se pustíme do Henselova lemmatu, dokážeme si ještě následující pomocné lemma.

Lemma 3.2.1. *Pro libovolný polynom f s koeficienty ze $\mathbb{Z}_p$ a libovolná $\alpha, \beta \in \mathbb{Z}_p$ platí, že z $\alpha \equiv \beta \pmod{p^n}$ plyne $f(\alpha) \equiv f(\beta) \pmod{p^n}$.*

Důkaz: Napišme si $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Víme, že $f(\alpha) \equiv f(\beta) \pmod{p^n}$ je to samé jako $|f(\alpha) - f(\beta)|_p \leq p^{-n}$. Ale vzhledem k tomu, že $|\alpha - \beta|_p \leq p^{-n}$, platí, že $|f(\alpha) - f(\beta)|_p = |a_n(\alpha^n - \beta^n) + a_{n-1}(\alpha^{n-1} - \beta^{n-1}) + \cdots + a_1(\alpha - \beta)|_p \leq p^{-n}$, protože ze všech sčítanců můžeme vytknou $(\alpha - \beta)$ a zůstane nám součet prvků ze $\mathbb{Z}_p$, který je v absolutní hodnotě menší nebo roven jedné. □

V následující větě budeme pomocí $f'(x)$ značit formální derivaci polynomu $f(x)$ danou vzorcem, jakým počítáme derivace v okruhu polynomů nad libovolným okruhem.

Věta 3.2.1. ***Henselovo lemma***
Pokud $f(x) \in \mathbb{Z}_p[X]$ a $a \in \mathbb{Z}_p$ splňuje:

$$f(a) \equiv 0 \pmod{p}, \quad f'(a) \not\equiv 0 \pmod{p},$$

potom existuje jedinečné $\alpha \in \mathbb{Z}_p$ takové, že $f(\alpha) = 0$ a $\alpha \equiv a \pmod{p}$.

Důkaz: Zvolme a_0 jakkoli, například $a_0 = 0$ Nejprve indukcí vůči n dokážeme, že pro každé $n \geq 1$, existuje $a_n \in \mathbb{Z}_p$ takové, že

$$f(a_n) \equiv 0 \pmod{p^n}, \quad a_n \equiv a_{n-1} \pmod{p^{n-1}}.$$

Jestliže podmínka platí pro každé $n = 1, 2, \ldots, m$, pak $a_m \equiv a_{m-1} \equiv \cdots \equiv a_1 \pmod{p}$.

Pro $n = 1$ to platí, protože si jednoduše vezmeme $a_1 = a$.

Nyní předpokládejme, že pro nějaké $n \geq 1$ to platí, a dokažme, že potom existuje $a_{n+1} \in \mathbb{Z}_p$ takové, že

$$f(a_{n+1}) \equiv 0 \pmod{p^{n+1}}, \quad a_{n+1} \equiv a_n \pmod{p^n}.$$

Takovéto a_{n+1}, můžeme napsat jako

$$a_{n+1} = a_n + p^n t_n,$$

kde $t_n \in \mathbb{Z}_p$, protože $a_{n+1} \equiv a_n \pmod{p^n}$. Takže nyní hledáme takovéto t_n, které bude splňovat $f(a_n + p^n t_n) \equiv 0 \pmod{p^{n+1}}$.

K tomu budeme nejprve potřebovat dokázat, že platí

$$f(X + Y) = f(X) + f'(X)Y + g(X, Y)Y^2$$

pro vhodné $g(X, Y) \in \mathbb{Z}_p[X, Y]$.

Vzhledem k tomu, že se jedná o polynom, můžeme ho psát jako: $f(X) = \sum_{i=0}^{d} c_i X^i$, kde $c_i \in \mathbb{Z}_p$. Z čehož dostaneme

$$f(X + Y) = \sum_{i=0}^{d} c_i (X + Y)^i = c_0 + \sum_{i=1}^{d} c_i (X^i + iX^{i-1}Y + g_i(X, Y)Y^2),$$

kde pro vhodné polynomy $g_i(X,Y) \in \mathbb{Z}_p[X,Y]$. Takže, když si vezmeme $g(X,Y) = \sum_{i=1}^{d} c_i g_i(X,Y)Y^2$, dostaneme to, co jsme chtěli

$$f(X+Y) = \sum_{i=0}^{d} c_i X^i + \sum_{i=1}^{d} i c_i X^{i-1} Y + \sum_{i=1}^{d} c_i g_i(X,Y) Y^2 = f(X) + f'(X)Y + g(X,Y)Y^2.$$

Nyní dosadíme a_n za X a $p^n t_n$ za Y a označíme $z = g(a_n, p^n t_n) \in \mathbb{Z}_p$. Platí

$$f(a_n + p^n t_n) = f(a_n) + f'(a_n) p^n t_n + z(p^n t_n)^2.$$

Z toho plyne

$$f(a_{n+1}) = f(a_n + p^n t_n) = f(a_n) + f'(a_n) p^n t_n + z p^{2n} t_n^2 \equiv f(a_n) + f'(a_n) p^n t_n \pmod{p^{n+1}}.$$

Vzhledem k tomu, že $f'(a_n) \in \mathbb{Z}_p$, je $f'(a_n)p^n t_n$ dělitelné p^n, a my pracujeme modulo p^{n+1}, zajímá nás proto $f'(a_n)$ pouze modulo p. Z pomocného lemmatu 3.2.1 víme, že z toho, že $a_n \equiv a \pmod{p}$, plyne $f'(a_n) \equiv f'(a) \pmod{p}$. Tedy platí, že $f'(a_n)p^n t_n \equiv f'(a)p^n t_n \pmod{p^{n+1}}$, z čehož dostaneme

$$f(a_n + p^n t_n) \equiv 0 \pmod{p^{n+1}} \iff f(a_n) + f'(a) p^n t_n \equiv 0 \pmod{p^{n+1}}$$

Nyní si musíme uvědomit, že $f(a_n) \equiv 0 \pmod{p^n}$, takže platí $\frac{f(a_n)}{p^n} \in \mathbb{Z}_p$.

$$f(a_n) + f'(a) p^n t_n \equiv 0 \pmod{p^{n+1}} \iff f'(a) t_n \equiv \frac{-f(a_n)}{p^n} \pmod{p}.$$

Vzhledem k tomu, že $f'(a) \not\equiv 0 \pmod{p}$, existuje jediné řešení $t_n \in \mathbb{Z}_p$ modulo p. Tím je naše indukce dokázaná.

Tímto jsme dostali posloupnost $a_1, a_2, a_3, \ldots a_n, \ldots$ prvků $\mathbb{Z}_p$, která je cauchyovská, protože $a_n \equiv a_{n+1} \pmod{p^n}$.

Mějme limitu této posloupnosti α a ukažme, že $f(\alpha) = 0$.

Takové α určitě splňuje $\alpha \equiv a_n \pmod{p^n}$ pro všechna $n \in \mathbb{N}$. Z toho díky pomocnému lemmatu 3.2.1 dostaneme

$$f(\alpha) \equiv f(a_n) \equiv 0 \pmod{p^n} \Rightarrow |f(\alpha)|_p \leq \frac{1}{p^n},$$

pro všechna $n \in \mathbb{N}$, tudíž $f(\alpha) = 0$.

Poslední, co je nyní ještě potřeba ověřit, je, že takové α je jediné.

Předpokládejme, že existuje kořen β polynomu $f(X)$ takový, že $\beta \equiv a \pmod{p}$. Nyní indukcí dokážeme, že $\beta \equiv \alpha \pmod{p^n}$ pro všechna $n \in \mathbb{N}$.

Už víme, že pro $n = 1$ platí $\alpha \equiv \beta \pmod{p}$. Nyní předpokládejme, že pro nějaké n platí $\alpha \equiv \beta \pmod{p^n}$. Tudíž $\beta = \alpha + p^n r_n$, kde $r_n \in \mathbb{Z}_p$. A z minulé indukce již víme, že potom platí

$$f(\beta) = f(\alpha + p^n r_n) \equiv f(\alpha) + f'(\alpha) p^n r_n \pmod{p^{n+1}}.$$

Vzhledem k tomu, že α i β jsou kořeny polynomu $f(X)$, je $0 \equiv f'(\alpha)p^n r_n \pmod{p^{n+1}}$. Tudíž $f'(\alpha)r_n \equiv 0 \pmod{p}$, a protože $f'(\alpha) \not\equiv 0 \pmod{p}$, dostaneme $r_n \equiv 0 \pmod{p}$. Z čehož plyne, že $\beta \equiv \alpha \pmod{p^{n+1}}$.

To znamená $|\beta - \alpha|_p \leq p^{-n}$ pro každé $n > 0$. Proto $|\beta - \alpha|_p = 0$ a tedy $\alpha = \beta$. □

Henselovo lemma, tak jak jsme ho nyní formulovali, nám může odhalit maximálně p kořenů. Pojďme si nyní představit silnější verzi. Ta řeší případy, kdy je $f'(a) \equiv 0 \pmod{p}$, tedy případy, kdy je nutné najít přesnější aproximaci hledaného kořene.

Věta 3.2.2. ***Silnější Henselovo lemma***
Mějme $f(X) \in \mathbb{Z}_p[X]$ a číslo $a \in \mathbb{Z}_p$, které splňuje

$$|f(a)|_p < |f'(a)|_p^2.$$

Potom existuje jedinečný kořen $\alpha \in \mathbb{Z}_p$ polynomu $f(X)$ takový, že $|\alpha - a|_p < |f'(a)|_p$. Pro tento kořen platí, že

- $|\alpha - a|_p = \left|\frac{f(a)}{f'(a)}\right|_p < |f'(a)|_p$,
- $|f'(\alpha)|_p = |f'(a)|_p$.

Na důkaz této věty se dají použít podobné myšlenky jako v důkazu Henselova lemmatu. Celý důkaz najdete v [2].

Henselovo lemma platí i mimo p-adická čísla. Mějme těleso $\mathcal{K}$, které je úplné vzhledem k ne-archimédovské absolutní hodnotě. Když si vezmeme okruh $\mathcal{O} = \{x \in \mathcal{K} : |x| \leq 1\}$, platí pro něj Henselovo lemma, stejně jako platí pro okruh $\mathbb{Z}_p$ v tělese $\mathbb{Q}_p$.

Henselovo lemma, jak jsme ho formulovali na začátku, je ve skutečnosti pouze konkrétním případem následující verze Henselova lemmatu. Tuto konkrétní verzi jsem uvedla jako první z důvodu, že se na ni budu v následujících kapitolách hodně odkazovat.

Myšlenku Henselova lemmatu totiž můžeme rozšířit z hledání kořenů polynomu na hledání polynomů, které tento polynom dělí. Hledání kořenů totiž není nic jiného, než hledání dělitelů stupně jedna.

Než se pustíme do definice, musíme si uvědomit, že faktorokruhy $\mathbb{Z}/p\mathbb{Z}$ a $\mathbb{Z}_p/p\mathbb{Z}_p$ jsou izomorfní p-prvková tělesa. Těleso $\mathbb{Z}_p/p\mathbb{Z}_p$ budeme značit jako $\mathbb{F}_p$.

Definice 3.2.1. *Mějme polynomy $g(X), h(X) \in \mathbb{Z}_p[X]$. Nechť $\overline{g}(X)$ a $\overline{h}(X)$ jsou polynomy v $\mathbb{F}_p$ vzniklé z polynomů $g(X)$, $h(X)$tak, že každý koeficient původního polynomu nahradíme jeho zbytkovou třídou modulo p. Řekneme, že $g(X)$ a $h(X)$ jsou nesoudělné modulo p, pokud $nsd(\overline{h}, \overline{g}) = 1$ nad $\mathbb{F}_p$.*

Věta 3.2.3. ***Henselovo lemma - druhá verze***
Nechť $f(X) \in \mathbb{Z}_p[X]$ a předpokládejme, že existují polynomy $g_1(X)$ a $h_1(X)$ v $\mathbb{Z}_p[X]$ takové, že

- *$g_1(X)$ je normovaný polynom,*
- *$g_1(X)$ a $h_1(X)$ jsou nesoudělné modulo p,*
- *$\overline{f}(X) = \overline{g_1}(X)\overline{h_1}(X)$.*

Potom existují polynomy $g(X), h(X) \in \mathbb{Z}_p[X]$ takové, že

- *$g(X)$ je normovaný,*
- *$\overline{g}(X) = \overline{g_1}(X)$ a $\overline{h}(X) = \overline{h_1}(X)$,*
- *$f(X) = g(X)h(X)$.*

I důkaz této věty jde provést pomocí indukce a můžete ho nalézt v [4].

Pojďme si nyní ukázat nějaké příklady.

Příklad: Mějme polynom $f(x) = x^4 - 1$ a ukažme, že všechny jeho kořeny leží v $\mathbb{Z}_5$. Použijeme Henselovo lemma 3.2.1:

- $1^4 - 1 \equiv 0 \pmod 5$ a $f'(1) = 4 \cdot 1^3 = 4 \not\equiv 0 \pmod 5$,
- $2^4 - 1 = 15 \equiv 0 \pmod 5$ a $f'(2) = 4 \cdot 2^3 = 32 \not\equiv 0 \pmod 5$,
- $3^4 - 1 = 80 \equiv 0 \pmod 5$ a $f'(3) = 4 \cdot 3^3 = 108 \not\equiv 0 \pmod 5$,
- $4^4 - 1 = 255 \equiv 0 \pmod 5$ a $f'(4) = 4 \cdot 4^3 = 256 \not\equiv 0 \pmod 5$.

Jak vidíme, v $\mathbb{Q}_5$ leží čtyři různé kořeny polynomu $f(x)$ a vzhledem k tomu, že se jedná o polynom čtvrtého stupně, jsou to všechny jeho kořeny. □

Příklad: Pojďme si ukázat, že v $\mathbb{Z}_2$ leží druhá odmocnina z -7.

Musíme ukázat, že polynom $g(x) = x^2 + 7$ má v $\mathbb{Z}_2$ kořen. Nemůžeme použít větu 3.2.1, protože $g'(x) = 2x \equiv 0 \pmod 2$, pro všechna $x \in \mathbb{Z}_2$. Nicméně můžeme zkusit použít větu 3.2.2.

$$|g(1)|_2 = |8|_2 = \frac{1}{2^3}, \;\; |g'(1)|_p = |2|_2 = \frac{1}{2} \Longrightarrow |g(1)|_2 < |g'(1)|_2^2.$$

Podmínka z věty 3.2.2 byla splněna, takže víme, že má polynom $g(x)$ kořen v $\mathbb{Z}_2$, a tedy v $\mathbb{Z}_2$ leží druhá odmocnina z -7. □

Kapitola 4

Analýza v $\mathbb{Q}_p$

Cílem této kapitoly je představit analýzu na tělesech $\mathbb{Q}_p$, ukázat podobnosti a naopak rozdílnosti s reálnou analýzou.

Bohužel není možné v tak krátké kapitole popsat všechno, tudíž se budeme zabývat hlavně p-adickými nekonečnými řadami, mocninnými řadami a následně funkcemi definovanými mocninnými řadami, protože tahle část p-adické analýzy je velice užitečná, jak si ukážeme v následující kapitole.

4.1 Nekonečné řady

Nekonečné p-adické řady fungují trochu jednodušeji než v reálné analýze, protože máme silnější podmínku pro cauchyovské posloupnosti (lemma 2.2.2).

Též můžeme formulovat lemma 2.2.4 pro všechny p-adické cauchyovské posloupnosti.

Lemma 4.1.1. *Mějme cauchyovskou posloupnost p-adických čísel (x_n), která nekonverguje k nule. Pro takovou posloupnost platí, že existuje N takové, že $|x_n|_p = |x_m|_p$ kdykoli platí, že $m \geq N, n \geq N$.*

Důkaz: Lemma dokážeme stejně jako lemma 2.2.4. □

Díky těmto vlastnostem p-adických cauchyovských posloupností platí pro p-adické nekonečné řady následující věta.

Věta 4.1.1. *Nekonečná řada $\sum a_n$ s členy $a_n \in \mathbb{Q}_p$ konverguje právě tehdy, když*

$$\lim_{n\to\infty} a_n = 0.$$

Jedná se o limitu v $\mathbb{Q}_p$. Ekvivalentně lze tuto podmínku formulovat tak, že platí $\lim_{n\to\infty} |a_n|_p = 0$ v $\mathbb{R}$.

V takovém případě platí, že

$$\Big|\sum_{n=0}^{\infty} a_n\Big|_p \leq \max_{n\geq 0} |a_n|_p.$$

Důkaz: Z lemmatu 2.2.2 víme, že posloupnost je cauchyovská (tedy v případě $\mathbb{Q}_p$ konvergentní) právě tehdy, když absolutní hodnoty rozdílů po sobě jdoucích členů jdou k nule. Tudíž v případě nekonečných řad musí jít k nule absolutní hodnoty rozdílů po

sobě jdoucích částečných součtů. Ovšem rozdíl po sobě jdoucích částečných součtů s_n a s_{n+1} je sčítanec a_{n+1}, tudíž musí jít k nule absolutní hodnoty sčítanců.

Zaměřme se nyní na dokazovanou nerovnost.

Pokud $\sum_{n=0}^{\infty} a_n = 0$, nerovnost určitě platí. Pokud $\sum_{n=0}^{\infty} a_n \neq 0$, z ne-archimédovské vlastnosti plyne $|\sum_{n=0}^{N} a_n|_p \leq \max_{0\leq n\leq N} |a_n|_p$ pro všechny částečné součty. Pokud si vezmeme dostatečně veliké N, dostaneme $\max_{0\leq n\leq N} |a_n|_p = \max_{0\leq n} |a_n|_p$, protože absolutní hodnoty a_n jdou k nule.

Vzhledem k tomu, že posloupnost částečných součtů nejde k nule, můžeme použít lemma 4.1.1, které nám říká, že členy této posloupnosti budou mít od určitého $N \in \mathbb{N}$ pořád stejnou absolutní hodnotu

$$\Big|\sum_{n=0}^{\infty} a_n\Big|_p = \Big|\sum_{n=0}^{N} a_n\Big|_p \leq \max_{0\leq n\leq N} |a_n|_p = \max_{0\leq n} |a_n|_p.$$

Z čehož jsme dostali požadovanou nerovnost. □

Díky těmto vlastnostem p-adických nekonečných řad, plynoucích z ne-archimédovské vlastnosti p-adické absolutní hodnoty, platí následující věta. Celý důkaz můžete najít v [4].

Definice 4.1.1. *Pro každá nezáporná celá i, j mějme $b_{ij} \in \mathbb{Q}_p$. Řekneme, že*

$$\lim_{i\to\infty} b_{ij} = 0 \quad \textit{stejnoměrně v } j,$$

pokud pro dané $\varepsilon > 0$ vždy existuje $N \in \mathbb{N}$, které nezáleží na j, takové, že pro všechna i, j platí

$$i \geq N \Longrightarrow |b_{ij}|_p < \varepsilon.$$

Věta 4.1.2. *Pro každá nezáporná celá i, j mějme $b_{ij} \in \mathbb{Q}_p$. Předpokládejme, že*

- *pro každé i, $\lim_{j\to\infty} b_{ij} = 0$,*
- *$\lim_{i\to\infty} b_{ij} = 0$ stejnoměrně v j.*

Potom obě nekonečné řady

$$\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) \quad a \quad \sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)$$

konvergují a jejich součty jsou stejné.

Vzhledem k tomu, že v důkazu je klíčová ne-archimédovská vlastnost p-adické absolutní hodnoty, tato věta v reálné analýze neplatí. Existují podobná tvrzení, ale nikdy tak silná jako v p-adické analýze.

Poslední věc, co nám chybí ověřit, je chování součtů a součinů dvou nekonečných řad v p-adické analýze.

Věta 4.1.3. *Mějme dvě konvergentní nekonečné řady $S = \sum_{n=0}^{\infty} a_n$ a $T = \sum_{n=0}^{\infty} b_n$, kde $a_n, b_n \in \mathbb{Q}_p$. Potom platí*

$$S + T = \sum_{n=0}^{\infty} a_n + \sum_{n=0}^{\infty} b_n = \sum_{n=0}^{\infty}(a_n + b_n),$$

$$S \cdot T = \left(\sum_{n=0}^{\infty} a_n\right) \cdot \left(\sum_{n=0}^{\infty} b_n\right) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}(a_{n-k}b_k)\right).$$

Důkaz: Pokud si ovšem vzpomeneme na důkazy, čemu se rovná součet dvou nekonečných řad v reálné analýze, zjistíme, že k důkazu nevyužíváme nic, co by v p-adické analýze neplatilo - sčítání čísel, násobení čísel a vlastnosti archimedovské absolutní hodnoty (pokud si potřebujete důkazy připomenout můžete se podívat například do [10], Kapitola 5).

Na násobení dvou řad nám reálná analýza nepostačí. Tato rovnost pro součin platí v reálné analýze pouze pro absolutně konvergentní řady.

Zvolme libovolné $\varepsilon > 0$, potom existuje $N \in \mathbb{N}$ takové, že pro každé $n \geq N$ platí $|a_n|_p < \varepsilon$, $|b_n|_p < \varepsilon$.

Navíc existuje $\delta > 0$ tak, že pro každé $n \in \mathbb{N}$ je $|a_n|_p < \delta$, $|b_n|_p < \delta$.

Pro libovolné $n \in \mathbb{N}$, $n > 2N$ platí

$$\left|\sum_{k=0}^{n} a_k b_{n-k}\right|_p \leq \max_{0\leq k\leq n} |a_k b_{n-k}|_p = \max\{\max_{0\leq k\leq \frac{n}{2}} |a_k b_{n-k}|_p, \max_{\frac{n}{2}\leq k\leq n} |a_k b_{n-k}|_p\} < \varepsilon\delta,$$

protože

$$k < \frac{n}{2} \Rightarrow n-k > N \Rightarrow |b_{n-k}|_p < \varepsilon, \text{ a } |a_k|_p < \delta \Rightarrow |a_k b_{n-k}|_p < \varepsilon\delta,$$

$$k \geq \frac{n}{2} > N \Rightarrow |b_{n-k}|_p < \delta, \text{ a } |a_k|_p < \varepsilon \Rightarrow |a_k b_{n-k}|_p < \varepsilon\delta.$$

Pro každé $\rho > 0$ zvolíme $\varepsilon = \frac{\rho}{\delta} > 0$. K tomuto ε zvolíme N stejně jako výše a dostaneme, že pro každé $n > 2N$ platí

$$\left|\sum_{k=0}^{n} a_k b_{n-k}\right|_p < \varepsilon\delta = \rho.$$

Což znamená, že řada $\sum_{n=0}^{\infty}(\sum_{k=0}^{n} a_k b_{n-k})$ je konvergentní. Pro její součet C navíc platí, že

$$\left|C - \sum_{n=0}^{2N}\left(\sum_{k=0}^{n} a_k b_{n-k}\right)\right|_p < \rho.$$

Navíc $|a_k b_l| < \rho$ vždy, když je $k + l > 2N$. Proto

$$\left|C - \left(\sum_{k=0}^{2N} a_k\right)\left(\sum_{l=0}^{2N} b_l\right)\right|_p < \rho.$$

Platí, že $|S| < \delta$, $|T| < \delta$ a $|S - \sum_{k=0}^{2N} a_k|_p < \varepsilon$,$|T - \sum_{l=0}^{2N} b_l|_p < \varepsilon$.

$$AB - \left(\sum_{k=0}^{2N} a_k\right)\left(\sum_{l=0}^{2N} b_l\right) = A\left(B - \sum_{l=0}^{2N} b_l\right) + \left(A - \sum_{k=0}^{2N} a_k\right) \cdot \sum_{l=0}^{2N} b_l,$$

$$\left|AB - \left(\sum_{k=0}^{2N} a_k\right)\left(\sum_{l=0}^{2N} b_l\right)\right|_p \leq \max\left\{\left|A\left(B - \sum_{l=0}^{2N} b_l\right)\right|_p, \left|\left(A - \sum_{k=0}^{2N} a_k\right) \cdot \sum_{l=0}^{2N} b_l\right|_p\right\} < \varepsilon\delta = \rho.$$

Proto $|AB - C|_p < \rho$. A protože je toto ρ libovolné, platí $AB = C$.

4.2 Mocninné řady

Nyní můžeme zavést p-adické mocninné řady. Budeme je značit tak, jak jsme zvyklí z reálné analýzy

$$f(X) = \sum_{n=0}^{\infty} a_n X^n,$$

kde $a_n \in \mathbb{Q}_p$.

A stejně jako v reálné analýze nás bude zajímat poloměr konvergence.

Věta 4.2.1. *Nechť $f(X) = \sum_{n=0}^{\infty} a_n X^n$ a definujme*

$$\rho = \frac{1}{\limsup \sqrt[n]{|a_n|_p}}.$$

Potom platí:

- *Pokud $\rho = 0$, $f(x)$ konverguje pouze pro $x = 0$.*
- *Pokud $\rho = \infty$, $f(x)$ konverguje pro všechna $x \in \mathbb{Q}_p$.*
- *Pokud $0 < \rho < \infty$ a $\lim_{n\to\infty} |a_n|_p \rho^n = 0$, potom $f(x)$ konverguje právě tehdy, když $|x|_p \leq \rho$.*
- *Pokud $0 < \rho < \infty$ a $\lim_{n\to\infty} |a_n|_p \rho^n \neq 0$, potom $f(x)$ konverguje právě tehdy, když $|x|_p < \rho$*

Důkaz: Vše plyne z toho, že p-adická nekonečná řada konverguje právě tehdy, když jdou absolutní hodnoty jejích sčítanců k nule. Tudíž mocninná řada konverguje právě tehdy, když x splňuje podmínky, které jsou napsané ve formulaci věty, protože pak $\lim_{n\to\infty} |a_n x^n|_p = 0$. □

Nyní definujme některé operace na mocninných řadách, tak aby to odpovídalo výsledkům z věty 4.1.3.

Definice 4.2.1. *Mějme dvě mocninné řady $S(X) = \sum_{n=0}^{\infty} a_n X^n$ a $T(X) = \sum_{n=0}^{\infty} b_n X^n$, kde $a_n, b_n \in \mathbb{Q}_p$. Potom definujeme součet a součin těchto řad takto*

$$(S+T)(X) = \sum_{n=0}^{\infty} a_n X^n + \sum_{n=0}^{\infty} b_n X^n = \sum_{n=0}^{\infty} (a_n + b_n) X^n,$$

$$(S \cdot T)(X) = \left(\sum_{n=0}^{\infty} a_n X^n\right) \cdot \left(\sum_{n=0}^{\infty} b_n X^n\right) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} (a_{n-k} b_k)\right) X^n.$$

A v případě, kdy $b_0 = 0$, definujme ještě skládání mocninných řad:

$$S(T(X)) = \sum_{n=0}^{\infty} a_n \left(\sum_{m=1}^{\infty} b_m X^m\right)^n.$$

Uvědomme si, že výsledné řady z definice jsou skutečně definované jednoznačně, tj. můžeme spočítat libovolný koeficient. U součtu a součinu to plyne z věty 4.1.3. Pro složení platí, že mocninná řada $S(T(X))$ a polynom $\sum_{n=0}^{k} a_n(\sum_{m=1}^{k} b_m X^m)^n$ mají stejné koeficienty u mocnin X^r pro všechna $r = 1, 2, \ldots, k$.

Nicméně p-adické analýza trochu liší od reálné analýzy v podmínkách, za kterých je funkce určená složením mocninných řad stejná jako složení jimi určených funkcí.

Věta 4.2.2. *Nechť $f(X) = \sum_{n=0}^{\infty} a_n X^n$ a $g(X) = \sum_{n=0}^{\infty} b_n X^n$, $b_0 = 0$, jsou formální mocninné řady s koeficienty z $\mathbb{Q}_p$ a nechť $h(X) = f(g(X))$ je jejich formální složení. Předpokládejme, že pro $x \in \mathbb{Q}_p$ platí*

1. *dosadíme-li x do $g(X)$, bude $g(x)$ konvergentní řada,*
2. *stejně tak, dosadíme-li číslo $g(x)$ do $f(X)$, bude $f(g(x))$ konvergentní řada,*
3. *pro všechna $n \in \mathbb{N}$ platí $|b_n x^n|_p \leq |g(x)|_p$.*

Potom $h(x)$ taky konverguje a platí $f(g(x)) = h(x)$.

V reálné analýze stačí, aby $|g(x)|_p < \rho$, kde ρ je poloměr konvergence $f(X)$. Nicméně v p-adické analýze je třetí podmínka skutečně potřeba - protipříklad můžete najít v [4], Problem 148, spolu s důkazem této věty.

4.3 Funkce definované mocninnými řadami

Jedním z problémů p-adické analýzy je, že zde nemůžeme využít derivaci tak hezky jako v reálné analýze. Nemáme zde totiž analogii Lagrangeovy věty o střední hodnotě, neboť zde neexistuje nic podobného intervalům.

Navíc pro dvě funkce se stejnou derivací obecně nemusí platit, že se liší pouze o konstantu.

Nicméně funkce definované mocninnými řadami mají v p-adické analýze spoustu hezkých vlastností a chovají se zde velice podobně tomu, jak jsme zvyklí z reálné analýzy. Například jsou spojité uvnitř kruhu konvergence (důkaz je stejný jako v reálné analýze, najít ho můžete například v [10] v části 6.3). A dokonce i jejich derivování funguje podobně jako v reálné analýze.

Definice 4.3.1. *Mějme otevřenou množinu $U \subset \mathbb{Q}_p$ a funkci $f : U \longrightarrow \mathbb{Q}_p$. Potom řekneme, že f je diferencovatelná v bodě $x \in U$, pokud limita*

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$

existuje a tuto hodnotu nazveme derivací funkce f v bodě x. Pokud $f'(x)$ existuje pro každé $x \in U$, řekneme, že f je diferencovatelná na U, a definujeme funkci $f' : U \longrightarrow \mathbb{Q}_p$, $x \mapsto f'(x)$.

Věta 4.3.1. *Nechť $f(X) = \sum_{n=0}^{\infty} a_n X^n$ je mocninná řada s koeficienty z $\mathbb{Q}_p$ mající nenulový poloměr konvergence. Nechť*

$$f'(X) = \sum_{n=1}^{\infty} n a_n X^{n-1}$$

je formální derivace této mocninné řady. Pak pro každé $x \in \mathbb{Q}_p$ takové, že $f(X)$ konverguje v bodě $X = x$, platí, že také $f'(X)$ konverguje v bodě $X = x$. Navíc platí, že funkce zadaná mocninnou řadou $f(X)$ má v bodě x derivaci a tato derivace je rovna hodnotě mocninné řady $f'(X)$ v bodě $X = x$.

Z toho dostaneme, že i vícenásobné derivace mocninných řad vypadají v p-adické analýze stejně jako v reálné analýze:

$$f^{(k)}(X) = k! \sum_{n \geq k}^{\infty} \binom{n}{k} a_n (X)^{n-k}.$$

Před tím, než si dokážeme, že pro dvě p-adické mocninné řady platí, že pokud se rovnají jejich derivace, pak se liší pouze v absolutním členu, pojďme si představit ještě jednu jejich vlastnost.

Věta 4.3.2. *Mějme dvě mocninné řady $f(X)$, $g(X)$ a $\rho > 0$ a předpokládejme, že obě konvergují pro $|x| < \rho$. Nyní předpokládejme, že existuje posloupnost prvků $x_m \in \mathbb{Q}_p$ ležících v kruhu konvergence, která má na nekonečně mnoho místech nenulové prvky, konverguje k nule a splňuje $f(x_m) = g(x_m)$ pro všechna m. Potom $f(X) = g(X)$.*

Důkazy obou vět opět můžete nalézt v [4] (Kapitola 4, strany 105-107) .
Nyní se podívejme na slibovanou větu.

Věta 4.3.3. *Mějme dvě mocninné řady $f(X)$, $g(X)$ a $\rho > 0$. Dále předpokládejme, že obě konvergují pro $|x| < \rho$. Pokud funkce mají funkce $f(x)$ a $g(x)$ definované mocninnými řadami $f(X)$ a $g(X)$ mají na množině $\{x \in \mathbb{Q}_p \mid |x|_p < \rho\}$ stejné derivace, potom existuje konstanta $c \in \mathbb{Q}_p$ taková, že $f(X) = g(X) + c$.*

Důkaz: Nechť $f(X) = \sum a_n X^n$ a $g(X) = \sum b_n X^n$. Pokud se rovnají derivace těchto funkcí, dostaneme z věty 4.3.1, že platí

$$\sum_{n=1}^{\infty} n a_n x^{n-1} = f'(x) = g'(x) = \sum_{n=1}^{\infty} n b_n x^{n-1}$$

pro všechna $|x| < \rho$. Potom ale z věty 4.3.2 plyne, že $a_n = b_n$ pro všechna $n \geq 1$. Tudíž jediné, v čem se můžou mocninné řady $f(X)$ a $g(X)$ lišit, jsou jejich absolutní členy, tudíž se můžou lišit pouze o konstantu. □

Výhodou p-adických mocninných řad je, že umíme říct daleko více o jejich kořenech. Strassmanova věta je pouze jedno z několika tvrzení, které bylo o kořenech p-adických funkcí definovaných mocninnými řadami dokázáno.

Věta 4.3.4. ***Strassmanova věta***
Nechť

$$f(X) = \sum_{n=0}^{\infty} a_n X^n = a_0 + a_1 X + a_2 X^2 + \dots$$

je nenulová mocninná řada s koeficienty z $\mathbb{Q}_p$ a předpokládejme, že $\lim_{n \to \infty} a_n = 0$, takže $f(x)$ konverguje pro všechna $x \in \mathbb{Z}_p$. Nechť N je takové nezáporné celé číslo, že

$$|a_N|_p = \max_{n \geq 0} |a_n|_p \text{ a } |a_n|_p < |a_N|_p \text{ pro } n > N.$$

Potom funkce $f : \mathbb{Z}_p \to \mathbb{Q}_p$, definovaná $x \mapsto f(x)$, má nejvýše N kořenů.

Důkaz: Důkaz povedeme indukcí vůči N. Nejprve si musíme uvědomit, že takové N skutečně vždy existuje, neboť $|a_n|_p$ jde k nule.

- Pokud $N = 0$, platí $|a_0|_p > |a_n|_p$ pro všechna $n \geq 1$. Chceme dokázat, že v takovém případě nemá tato mocninná řada žádný kořen. Tedy neexistuje žádné $x \in \mathbb{Z}_p$ takové, že $f(x) = 0$.

  Předpokládejme nyní, že takové x existuje, tudíž platí

  $$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots = 0,$$

  $$-a_0 = a_1 x + a_2 x^2 + a_3 x^3 + \ldots.$$

  Vzhledem k tomu, že p-adická absolutní hodnota opačných prvků je stejná, dostaneme pomocí věty 4.1.1

  $$|a_0|_p = |a_1 x + a_2 x^2 + a_3 x^3 + \ldots|_p \leq \max_{n\geq 1} |a_n x^n|_p \leq \max_{n\geq 1} |a_n|_p,$$

  protože $x \in \mathbb{Z}_p$, tudíž $|x|_p \leq 1$.

  To je však spor s předpokladem, že $|a_0|_p > |a_n|_p$ pro všechna $n \geq 1$.

- Předpokládejme, že je dáno přirozené číslo N takové, že pro všechny mocninné řady, jejichž koeficienty konvergují k nule, takové, že koeficient s indexem $N - 1 \geq 0$, má maximální absolutní hodnotu a zároveň všechny koeficienty s větším indexem mají menší absolutní hodnotu, platí, že mají nejvýše $N - 1$ kořenů v $\mathbb{Z}_p$.

  Nyní mějme mocninnou řadu $\sum_{n=0}^{\infty} a_n X^n$ s vlastností $\lim_{n\to\infty} a_n = 0$, pro kterou číslo N splňuje $|a_N|_p = \max_{n\geq 0} |a_n|_p$ a $|a_n|_p < |a_N|_p$ pro všechna $n > N$.

  Pokud by tato řada neměla žádný kořen v $\mathbb{Z}_p$, větu by automaticky splňovala. Proto předpokládejme, že existuje $\alpha \in \mathbb{Z}_p$ takové, že $f(\alpha) = 0$. Z toho dostaneme

  $$f(x) = f(x) - f(\alpha) = \sum_{n=1}^{\infty} a_n (x^n - \alpha^n) = (x - \alpha) \sum_{n=1}^{\infty} \sum_{j=0}^{n-1} a_n x^j \alpha^{n-1-j}.$$

  Nyní si zavedeme označení

  $$c_{jn} = \begin{cases} a_n x^j \alpha^{n-1-j} & \text{je-li } j < n, \\ 0 & \text{je-li } j \geq n. \end{cases}$$

  Pak pro každé n platí $\lim_{j\to\infty} c_{jn} = 0$, protože tato posloupnost má jen konečně mnoho nenulových členů. Protože $\alpha \in \mathbb{Z}_p$, $x \in \mathbb{Z}_p$, platí $|\alpha|_p \leq 1$, $|x|_p \leq 1$, a proto $|c_{jn}|_p \leq |a_n|_p$. Což znamená, že $\lim_{n\to\infty} c_{jn} = 0$ konverguje stejnoměrně v j. Podle věty 4.1.2 můžeme provést záměnu a dostaneme

  $$\sum_{n=1}^{\infty} \sum_{j=0}^{n-1} a_n x^j \alpha^{n-1-j} = \sum_{j=0}^{\infty} \sum_{n=j+1}^{\infty} a_n x^j \alpha^{n-1-j} = \sum_{j=0}^{\infty} x^j \sum_{k=0}^{\infty} a_{k+j+1} \alpha^k.$$

  Funkci $f(x)$ si proto můžeme napsat jako

  $$f(x) = (x - \alpha) \sum_{j=0}^{\infty} b_j x^j = (x - \alpha) g(x),$$

kde $g(x)$ je funkce definovaná mocninnou řadou s koeficienty

$$b_j = \sum_{k=0}^{\infty} a_{j+1+k}\alpha^k.$$

Řada definující b_j skutečně konverguje podle věty 4.1.1, neboť $|\alpha| \leq 1$ a platí $\lim_{k\to\infty} a_{j+1+k} = 0$. Z toho též dostaneme

$$|b_j|_p \leq \max_{k\geq 0} |a_{j+1+k}|_p \leq |a_N|_p$$

pro všechna j. A zároveň

$$|b_{N-1}|_p = |a_N + a_{N+1}\alpha + a_{N+2}\alpha^2 + \ldots|_p = |a_N|_p.$$

A proto, pokud $j \geq N$,

$$|b_j|_p \leq \max_{k\geq 0} |a_{j+1+k}|_p \leq \max_{j\geq N+1} |a_j|_p < |a_N|_p = |b_{N-1}|_p.$$

Tudíž má funkce $g(x)$ z indukčního předpokladu nejvýše $N-1$ kořenů v $\mathbb{Z}_p$. Ovšem naše funkce $f(x)$ má pouze o jeden kořen víc, α, které jsme si vzali na začátku. Funkce $f(x)$ má proto maximálně N kořenů v $\mathbb{Z}_p$.

□

Kapitola 5

Grupa $\mathbb{Z}_p^\times$

Množina invertibilních prvků v okruhu celých p-adických čísel je zajímavá z několika důvodů. Můžeme totiž pomocí ní vyjádřit všechny prvky $\mathbb{Q}_p^\times$ a popsat druhé mocniny p-adických čísel. Též v ní leží netriviální odmocniny z jedné, jak později dokážeme.

Prvně se podívejme na to, které prvky $\mathbb{Q}_p$ jsou invertibilní.

Věta 5.0.1. $\mathbb{Z}_p^\times = \{z \in \mathbb{Z}_p |\ |z|_p = 1\}$.

Důkaz: Vzhledem k tomu, že $|ab|_p = |a|_p|b|_p$, je jasné, že pokud $|a|_p < 1$, tak nemůže a^{-1} ležet v $\mathbb{Z}_p$, protože $|a^{-1}|_p > 1$.

Nyní ukažme, že pro každé číslo $|a|_p = 1$ existuje $a^{-1} \in \mathbb{Z}_p$. Protože je a nenulový prvek $\mathbb{Q}_p$, má v $\mathbb{Q}_p$ inverzní prvek. Pro tento inverzní prvek platí $|a^{-1}|_p = |a|_p^{-1} = 1$. A proto $a^{-1} \in \mathbb{Z}_p$, a a je tedy invertibilním prvkem $\mathbb{Z}_p$. □

Nyní pojďme ukázat, že každý nenulový prvek $\mathbb{Q}_p$ lze zapsat následujícím způsobem:

Věta 5.0.2. *Mějme $x \in \mathbb{Q}_p^\times$, potom existuje jediné $n \in \mathbb{Z}$ a $z \in \mathbb{Z}_p^\times$ tak, že platí:*

$$x = p^n z.$$

Důkaz: Podle definice 2.2.6 (s přihlédnutím k lemmatu 2.2.4) je absolutní hodnota libovolného nenulového p-adického čísla x tvaru p^k, kde $k \in \mathbb{Z}$. Položme $z = xp^k$, pak platí $|z|_p = |x|_p|p^k|_p = p^k p^{-k} = 1$, a tedy $z \in \mathbb{Z}_p^\times$. Proto pokud položíme $n = -k$, můžeme psát $x = p^n z$.

Nyní předpokládejme, že existují $n_1 \in \mathbb{Z}$, $n_2 \in \mathbb{Z}$ a k nim $z_1 \in \mathbb{Z}_p^\times$, $z_2 \in \mathbb{Z}_p^\times$ tak, že $x = p^{n_1} z_1$ a $x = p^{n_2} z_2$. Vzhledem k tomu, že $p^k = |x|_p = |p^{n_1}|_p|z_1| = p^{-n_1}$ a $p^k = |x|_p = |p^{n_2}|_p|z_1| = p^{-n_2}$, musí platit $k = -n_1 = -n_2$. Tedy dostaneme $xp^k = z_1$ a $xp^k = z_2$. Je tedy $n_1 = n_2$ a $z_1 = z_2$. □

5.1 Logaritmus a exponenciální funkce

V minulé kapitole jsme se bavili o p-adických funkcích definovaných pomocí mocninných řad a o jejich vlastnostech. Jedny z funkcí z reálné analýzy, které umíme napsat pomocí mocninné řady, jsou exponenciální funkce a logaritmus (ten tedy umíme takto vyjádřit pouze pro x z určitého intervalu). Navíc jsou tyto funkce navzájem inverzní bijekce, a proto zadávají izomorfismus mezi grupou reálných čísel se sčítáním a mezi grupou kladných reálných čísel s násobením:

$$x \in \langle \mathbb{R}; + \rangle \mapsto e^x \in \langle \mathbb{R}_+; \cdot \rangle; \quad t \in \langle \mathbb{R}_+; \cdot \rangle \mapsto \log(t) \in \langle \mathbb{R}; + \rangle.$$

V této sekci budeme definovat p-adický logaritmus a exponenciální funkci za pomoci jejich mocninných řad, které pro připomenutí vypadají následovně:

$$\log(X) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(X-1)^n}{n},$$

$$\exp(X) = e^x = \sum_{n=0}^{\infty} \frac{X^n}{n!}.$$

A podíváme se, jak se tyto mocninné řady chovají v p-adické analýze.

5.1.1 p-adický logaritmus

Nejdříve bychom měli zjistit poloměr konvergence mocninné řady pro náš potencionální logaritmus.

Věta 5.1.1. *Mocninná řada*

$$S(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(x-1)^n}{n}$$

konverguje p-adicky pouze pro $x - 1 \in p\mathbb{Z}_p$, *tj.* $x \in 1 + p\mathbb{Z}_p$. *Jinými slovy* $x \in B(1,1) = \{x \in \mathbb{Z}_p, |x-1|_p < 1\}$.

Důkaz: Nejprve se podíváme na poloměr konvergence:

$$|a_n|_p = |\tfrac{1}{n}|_p = p^{v_p(n)},$$

$$\sqrt[n]{|a_n|_p} = p^{\frac{v_p(n)}{n}}.$$

Nyní musíme ukázat, čemu se rovná $\lim_{n\to\infty} p^{\frac{v_p(n)}{n}}$. Víme, že $v_p(n)$ je největší m, takové, že $p^m | n$, z čehož plyne, že

$$v_p(n) = m = \frac{\log(p^m)}{\log(p)} \leq \frac{\log(n)}{\log(p)}.$$

A z toho již odvodíme, že

$$\frac{v_p(n)}{n} \leq \frac{\log(n)}{n\log(p)}.$$

Tedy $\frac{v_p(n)}{n}$ konverguje k nule, jak jde n do nekonečna, protože $0 \leq \frac{v_p(n)}{n} \leq \frac{\log(n)}{n\log(p)}$ a obě krajní posloupnosti konvergují k nule, jak jde n do nekonečna. Z čehož plyne

$$\lim_{n\to\infty} p^{\frac{v_p(n)}{n}} = 1.$$

Nyní tedy musíme ukázat, zda leží jednička v kruhu konvergence nebo ne. Když dosadíme $(x-1) = 1$:

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}.$$

Podle věty 4.1.1 řada konverguje, právě tehdy, když její členy jdou k nule. Což v tomto případě nenastává, protože když máme například $n = p^m$, je absolutní hodnota n-tého členu $|\frac{1}{n}|_p = m$.

Takže jednička neleží v poloměru konvergence a dostáváme to, co jsme chtěli. Řada ze zadání konverguje pro $(x-1) \in B(0,1)$, tedy pro $x \in B(1,1)$, tj. $x \in 1 + p\mathbb{Z}_p$. □

Nyní definujme p-adický logaritmus.

Definice 5.1.1. *Na množině $1 + p\mathbb{Z}_p$ definujeme p-adický logaritmus jako funkci $\log_p(x)$ danou mocninnou řadou $\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}(X-1)^n$, tedy pro každé $x \in 1 + p\mathbb{Z}_p$ klademe*

$$\log_p(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(x-1)^n}{n}.$$

Pojďme dokázat, že tato funkce má velice podobné vlastnosti jako v reálné analýze:

Věta 5.1.2. *Funkce $\log_p(x)$ má na množině $1 + p\mathbb{Z}_p$ derivaci, přičemž platí*

$$(\log_p(x))' = \frac{1}{x} \text{ pro každé } x \in 1 + p\mathbb{Z}_p.$$

Důkaz: Funkce $\log_p(1+x)$ je na množině $p\mathbb{Z}_p$ zadaná mocninnou řadou

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} X^n$$

Nyní můžeme využít věty 4.3.1 a součet geometrické řady. Pro libovolné $x \in p\mathbb{Z}_p$ platí

$$(log(x))' = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}n}{n} x^{n-1} = \sum_{n=1}^{\infty} (-1)^{n-1} x^{n-1} = \frac{1}{1-(-x)} = \frac{1}{1+x}.$$

Odtud již plyne požadované tvrzení. □

Věta 5.1.3. *Pro všechna $x, y \in 1 + p\mathbb{Z}_p$ platí*

$$\log_p(xy) = \log_p(x) + \log_p(y).$$

Důkaz: Dokážeme ekvivalentní tvrzení: pro každé $x, y \in p\mathbb{Z}_p$ platí

$$\log_p((1+x)(1+y)) = \log_p(1+x) + \log_p(1+y).$$

Budeme postupovat tak, že zafixujeme $y \in p\mathbb{Z}_p$ a ukážeme, že obě strany předchozí rovnosti jako funkce $x \in p\mathbb{Z}_p$ je možné zadat jako součet mocninné řady, abychom mohli využít větu 4.3.3. Platí $(1+y)(1+x) = 1 + y + (1+y)x \in 1 + \mathbb{Z}_p$, a tedy

$$\log_p((1+y)(1+x)) = \sum_{n=01}^{\infty} \frac{(-1)^{n-1}}{n}((1+y)x+y)^n = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} \sum_{k=0}^{n} \binom{n}{k} (1+y)^k x^k y^{n-k}.$$

Pro libovolné $n, k \in \mathbb{N} \cup \{0\}$ položme

$$b_{nk} = \begin{cases} \frac{(-1)^{n-1}}{n} \sum_{k=0}^{n} \binom{n}{k} (1+y)^k x^k y^{n-k}, & \text{je-li } k \leq n \text{ a } n \geq 1, \\ 0, & \text{je-li } k > n \text{ nebo } n = 0. \end{cases}$$

Pak tedy

$$\log_p((1+y)(1+x)) = \sum_{n=0}^{\infty} \sum_{k=0}^{\infty} b_{nk}.$$

Protože $|y| \leq \frac{1}{p}$, $|1+y|_p = 1$ a $|x|_p \leq \frac{1}{p}$ platí $|b_{nk}|_p \leq |\frac{1}{n}|_p \cdot \frac{1}{p^n}$, a tedy $\lim_{n\to\infty} b_{nk} = 0$ konverguje stejnoměrně v k. Jistě také platí $\lim_{k\to\infty} b_{nk} = 0$ pro každé n. Podle věty 4.1.2 platí

$$\log_p((1+y)(1+x)) = \sum_{k=0}^{\infty} \sum_{n=0}^{\infty} b_{nk} = \sum_{n=0}^{\infty} b_{n0} + \sum_{k=1}^{\infty} \sum_{n=k}^{\infty} \frac{(-1)^{n-1}}{n} \binom{n}{k} (1+y)^k x^k y^{n-k}.$$

Označme $g_0 = \sum_{n=0}^{\infty} b_{n0}$, $g_k = \sum_{k=1}^{\infty} \sum_{n=k}^{\infty} \frac{(-1)^{n-1}}{n} \binom{n}{k} (1+y)^k y^{n-k}$ pro každé $k \in \mathbb{N}$. Předchozí rovnost znamená, že mocninná řada $\sum_{k=0}^{\infty} g_k X^k$ konverguje na množině $p\mathbb{Z}_p$ a že pro každé $x \in p\mathbb{Z}_p$ platí

$$\sum_{k=0}^{\infty} g_k x^k = \log_p((1+y)(1+x)).$$

Protože $\log_p(1+x)$ je součtem mocninné řady konvergující pro $x \in p\mathbb{Z}_p$ a $\log_p(1+y)$ je konstanta, dostali jsme, že obě strany rovnosti, kterou chceme dokázat, jsou dány mocninnými řadami konvergujícími pro $x \in p\mathbb{Z}_p$.

Nyní můžeme využít faktu, že $\log_p((1+y)(1+x))$ je složenou funkcí a můžeme její derivaci spočítat jako derivaci složené funkce. Pravidlo pro derivování složené funkce je v p-adické analýze totožné s tím v reálné analýze a také se stejně dokazuje. Derivaci podle proměnné x dostaneme užitím věty 5.1.2 dostáváme

$$((1+y)(1+x))' = \frac{1}{(1+y)(1+x)} \cdot (1+y) = \frac{1}{1+x}.$$

Také platí

$$(\log_p(1+x) + \log(1+y))' = (\log_p(1+x))' = \frac{1}{1+x}.$$

Podle věty 4.3.3 existuje $c \in \mathbb{Q}_p$ takové, že $\log_p((1+x)(1+y)) = \log_p(1+x) + \log_p(1+y) + c$.

Volbou $x = 0$ odvodíme $c = 0$, a tím jsme dokázali požadovanou rovnost. □

5.1.2 p-adická exponenciální funkce

Stejně jako u logaritmu začneme tím, že zjistíme, pro jaký poloměr konvergence mocninná řada pro exponenciální funkci konverguje p-adicky.

Věta 5.1.4. *Mocninná řada*

$$R(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

konverguje v $\mathbb{Q}_p$ právě pro $x \in p\mathbb{Z}_p$ v případě, že $p \neq 2$. Pokud je $p = 2$, řada $R(x)$ konverguje v $\mathbb{Q}_p$ právě pro $x \in 4\mathbb{Z}_2$.

Důkaz: Podívejme se tedy na poloměr konvergence:

$$|a_n|_p = |\tfrac{1}{n!}|_p = p^{v_p(n!)},$$

$$\sqrt[n]{|a_n|_p} = p^{\frac{v_p(n!)}{n}}.$$

Abychom určili poloměr konvergence, musíme zjistit, jak vyjádřit $v_p(n!)$. Potřebujeme zjistit, kolik je přirozených čísel $m \leq n$ takových, že $p|m$. Toto množství dostaneme, když si vezmeme $\left\lfloor \frac{n}{p} \right\rfloor$, což je největší celé číslo, které je menší nebo rovno podílu $\frac{n}{p}$. Toto číslo nám bohužel nestačí, protože některá čísla můžou být dělitelná p^2. Kolik takových čísel existuje dostaneme opět, když si vezmeme $\left\lfloor \frac{n}{p^2} \right\rfloor$. Ale samozřejmě může být některé číslo dělitelné i vyšší mocninou p, proto

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Tato řada určitě konverguje, protože od určitého i bude $\left\lfloor \frac{n}{p^j} \right\rfloor = 0$ pro všechna $j \geq i$. Pomocí následující řady jsme schopni $v_p(n!)$ shora odhadnout.

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor < \sum_{i=1}^{\infty} \frac{n}{p^i} = \frac{n}{p-1}.$$

Poslední rovnost plyne z vlastnosti geometrických řad.

Z toho dostáváme, že

$$\limsup_{n\to\infty} \sqrt[n]{|a_n|_p} = \limsup_{n\to\infty} p^{\frac{v_p(n!)}{n}} \leq p^{\frac{1}{p-1}},$$

a tedy poloměr konvergence je větší nebo roven $p^{\frac{-1}{p-1}}$.

A řada tedy konverguje pro $|x|_p < p^{\frac{-1}{p-1}}$. Nyní zkusme dosadit $|x|_p \geq p^{\frac{-1}{p-1}}$ a podívejme se, zda řada může konvergovat i pro takové x. Vezměme si $n = p^m$, kde m je libovolné přirozené číslo, potom

$$v_p(n!) = p^{m-1} + p^{m-2} + \cdots + 1 = \frac{p^m - 1}{p-1}.$$

Ale vzhledem k tomu, že $|x|_p \geq p^{\frac{-1}{p-1}}$, dostaneme pro libovolné m:

$$\left|\frac{x^n}{n!}\right|_p = \left|\frac{x^{p^m}}{p^m!}\right|_p = \frac{|x|_p^{p^m}}{|p^m!|_p} \geq p^{\frac{-p^m}{p-1}} \cdot p^{\frac{p^m-1}{p-1}} = p^{\frac{-1}{p-1}}.$$

Z čehož plyne, že $\frac{x^n}{n!}$ nemůže jít k nule pro $|x|_p \geq p^{\frac{-1}{p-1}}$. Takže $R(x)$ konverguje na $B(0, p^{\frac{-1}{p-1}})$. Tudíž skutečně pro všechna $p \neq 2$ řada $R(x)$ v $\mathbb{Q}_p$ konverguje právě pro $x \in p\mathbb{Z}_p$. Pro $p = 2$ řada $R(x)$ konverguje v $\mathbb{Q}_p$ právě pro všechna $x \in 4\mathbb{Z}_2$, protože $2 - 1 = 1$, a proto $R(x)$ konverguje na $B(0, 2^{-1})$. □

Nyní definujme p-adickou exponenciální funkci.

Definice 5.1.2. *Nechť* $D = B(0, p^{\frac{-1}{(p-1)}}) = \{x \in \mathbb{Z}_p |\ |x|_p < p^{\frac{-1}{(p-1)}}\}$. *Potom p-adickou exponenciální funkci definujeme jako:*

$$\exp_p : D \longrightarrow \mathbb{Q}_p,$$

$$\exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

A ověřme, že i v p-adické analýze má podobné vlastnosti jako v reálné analýze.

Věta 5.1.5. *Mějme x, y ležící v množině konvergence* $\exp_p(x)$. *Potom platí:*

$$\exp_p(x+y) = \exp_p(x)\exp_p(y).$$

Důkaz: Vzhledem k tomu, že i $x + y$ leží v množině konvergence pro dané p, můžeme si to rozepsat jako:

$$\begin{aligned}\exp_p(x+y) &= \sum_{n=0}^{\infty} \frac{(x+y)^n}{n!} = \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k \\ &= \sum_{n=0}^{\infty}\sum_{k=0}^{n} \frac{1}{n!}\frac{n!}{(n-k)!k!}x^{n-k}y^k = \sum_{n=0}^{\infty}\sum_{k=0}^{n}\frac{x^{n-k}}{(n-k)!}\frac{y^k}{k!} \\ &= \left(\sum_{m=0}^{\infty}\frac{x^m}{m!}\right)\left(\sum_{k=0}^{\infty}\frac{y^k}{k!}\right).\end{aligned}$$

Poslední rovnost plyne z věty 4.1.3. □

Nyní nám již nic nebrání v definování p-adické exponenciální funkce.

5.1.3 $\log_p$ a $\exp_p$ jako inverzní funkce

Důležitou vlastností logaritmu a exponenciální funkce v reálné analýze je, že jsou navzájem inverzními funkcemi. Nyní si ukážeme, že i p-adické alternativy těchto funkcí jsou si na daných množinách inverzní.

Věta 5.1.6. *Mějme $x \in \mathbb{Z}_p$ takové, že $|x|_p < p^{\frac{-1}{p-1}}$. Potom*

$$\log_p(\exp_p(x)) = x.$$

Mějme x takové, že $x \in 1 + p\mathbb{Z}_p$ (pro $p = 2$ mějme $x \in 1 + 4\mathbb{Z}_2$). Potom

$$\exp_p(\log_p(x)) = x.$$

Důkaz: Abychom toto mohli dokázat, musíme ukázat, že funkce splňují všechny vlastnosti z věty 4.2.2 z předchozí kapitoly.

Nejprve pojďme na první rovnost. Vzhledem k tomu, že x leží v definičním oboru $\exp_p$, tak $\exp_p(x)$ konverguje. Nyní je potřeba ukázat, že konverguje k něčemu, co je v definičním oboru funkce $\log_p(x)$. Respektive musíme ukázat, že $\exp_p(x) \in 1 + p\mathbb{Z}_p$.

Ve větě 5.1.4 jsme ukázali, že $\sum_{n=0}^{\infty} \frac{x^n}{n!}$ konverguje právě pro $|x|_p < p^{\frac{-1}{p-1}}$. Nyní ukážeme, že pro všechny takové x a $n \geq 1$ platí:

$$\frac{|x|_p^n}{|n!|_p} \leq |x|_p.$$

Vzhledem k tomu, že $|n!|_p > p^{\frac{-n}{p-1}}$ a celé číslo menší než $\frac{n}{p-1}$ nemůže být větší než $\frac{n-1}{p-1}$, víme, že $|n!|_p \geq p^{-\frac{n-1}{p-1}}$. Tudíž

$$\frac{|x|_p^n}{|n!|_p|x|_p} \leq \frac{|x|_p^{n-1}}{p^{\frac{-(n-1)}{p-1}}} \leq \left(\frac{|x|_p}{p^{\frac{-1}{p-1}}}\right)^{n-1} \leq 1,$$

$$\frac{|x|_p^n}{|n!|_p} \leq |x|_p.$$

Vzhledem k tomu, že pro $n = 0$ je $\frac{x^0}{0!} = 1$, platí $\exp_p(x) \in 1 + p\mathbb{Z}_p$. Dokonce můžeme říct, že pro $x \in p^m\mathbb{Z}_p$, platí $\exp_p(x) \in 1 + p^m\mathbb{Z}_p$.

A zároveň z toho víme, že platí i třetí podmínka z věty 4.2.2 - $|b_n x^n|_p \leq |g(x)|_p$, v našem případě $|\frac{x^n}{n!}|_p \leq |\exp_p(x)|_p = 1$. Takže pro $|x|_p < p^{\frac{-1}{p-1}}$ můžeme psát

$$\log_p(\exp_p(x)) = x.$$

Nyní se podívejme na druhé složení funkcí. Máme $x \in 1 + p\mathbb{Z}_p$, takže leží v definičním oboru p-adického logaritmu. Nyní musíme dokázat, že i $\log_p(x)$ leží v definičním oboru $\exp_p$ a že i $\log(x)$ splňuje třetí podmínku z věty 4.2.2.

Nejprve si rozšiřme definici p-adické valuace na všechna p-adická čísla. Mějme $x \in \mathbb{Q}_p$. Nechť c je číslo takové, že $|x|_p = p^{-c}$, potom definujeme $v_p(x) = c$.

Vezměme si $x \in 1 + p^m\mathbb{Z}_p$ (kde pro $p = 2$ musí být $m \geq 2$, pro $p \neq 2$ se jedná o libovolné přirozené číslo). Potom pro $n > 1$

$$v_p\left(\frac{(-1)^{n-1}(x-1)^n}{n}\right) = nv_p(x-1) - v_p(n) > v_p(x-1),$$

protože

$$v_p(x-1) > \frac{v_p(n)}{n-1}.$$

Tato nerovnost musí platit, neboť $v_p(x-1)$ je kladné celé číslo a $\frac{v_p(n)}{n-1}$ je pro $n > 1$ menší než 1. Výjimkou je případ, kdy $p = 2$ a $n = 2$, kdy je zlomek roven jedné, ovšem pro $p = 2$ je vždy $v_2(x-1) \geq 2$.

Z toho dostáváme, že pro $n > 1$

$$\left|\frac{(-1)^{n-1}(x-1)^n}{n}\right|_p < |x-1|_p.$$

A pro $n = 1$ je $|\frac{(-1)^0(x-1)}{1}|_p = |x-1|_p$.

Z toho dostáváme, že $|\log_p(x)|_p = |x-1|_p$ a odtud plyne $\log_p(x) \in p^m\mathbb{Z}_p$, tedy $\log_p(x)$ leží v definičním oboru funkce $\exp_p$. A navíc z toho plyne, že je splněna i třetí podmínka věty 4.2.2, $|\frac{(-1)^{n-1}(x-1)^n}{n}|_p \leq |\log_p(x)|_p = |x-1|_p$. Takže už můžeme psát

$$\exp_p(\log_p(x)) = x.$$

□

Z této věty a díky důkazu, kde jsme dokázali trochu silnější tvrzení, plyne následující věta.

Věta 5.1.7. *Pro každé celé $m > \frac{1}{p-1}$ je aditivní grupa $p^m\mathbb{Z}_p$ izomorfní s multiplikativní grupou $1 + p^m\mathbb{Z}_p$*

Důkaz: Tímto izomorfismem jsou funkce $\log_p$ a $\exp_p$, jak jsme již dokázali. □

Obzvlášť důležitá věc plynoucí z této věty je, že pro $p \neq 2$ platí

$$\text{aditivní grupa } p\mathbb{Z}_p \cong \text{multiplikativní grupa } 1 + p\mathbb{Z}_p.$$

V případě $p = 2$ musíme, kvůli počátečním podmínkám, dát p v druhé mocnině

$$\text{aditivní grupa } 4\mathbb{Z}_2 \cong \text{multiplikativní grupa } 1 + 4\mathbb{Z}_2.$$

5.2 $\mathbb{Z}_p^\times$ a netriviální odmocniny z jedné

Cílem této části bude ukázat, že $\mathbb{Z}_p \cong G \times (1 + p^m\mathbb{Z}_p)$, kde G je grupa všech odmocnin z jedné, které leží v $\mathbb{Z}_p$, a m je nejmenší celé číslo takové, že $m > \frac{1}{p-1}$. Jak víme z předchozí části, je $m = 1$ pro všechna $p \neq 2$ a $m = 2$ pro $p = 2$.

Nejprve začneme zjišťováním, jaké n-té odmocniny z jedné v $\mathbb{Q}_p$ leží. Vzhledem k tomu, že pro ně platí $|x|_p^n = |x^n|_p = |1| = 1$, musí všechny odmocniny z jedné, které leží v $\mathbb{Q}_p$, ležet v $\mathbb{Z}_p^\times$.

Připomeňme, že odmocninu z jedné ζ nazveme primitivní n-tou odmocninou z jedné, pokud n je nejmenší přirozené číslo splňující $\zeta^n = 1$.

Věta 5.2.1. *Pro $p \neq 2$, $\mathbb{Z}_p^\times$ obsahuje všechny n-té primitivní odmocniny z jedné právě tehdy, když $n|(p-1)$. Odmocniny z jedné ležící v $\mathbb{Z}_p$ tvoří grupu izomorfní s $(\mathbb{Z}_p/p\mathbb{Z}_p)^\times$.*

Důkaz: Nejprve dokážeme, že v $\mathbb{Z}_p^\times$ leží všechny kořeny polynomu $f(X) = X^{p-1} - 1$. Z malé Fermatovy věty víme, že pro $a \in \{1, \ldots, p-1\}$ platí $a^{p-1} \equiv 1 \pmod{p}$. Též pro ně platí, že $f'(a) = (p-1)a^{p-2} \not\equiv 0 \pmod{p}$. Tudíž podle Henselova lemmatu každý z těchto prvků nám zadá jeden kořen polynomu $f(x)$, tento polynom má stupeň $(p-1)$, tudíž má $(p-1)$ kořenů a my našli všechny. Tyto odmocniny z jedné budeme značit jako ζ_a, kde $a \in \{1, \ldots, p-1\}$, podle toho, s jakým a jsou kongruentní modulo p.

Dokázali jsme, že v $\mathbb{Z}_p^\times$ leží všechny primitivní n-té odmocniny pro $n|(p-1)$. Nyní musíme ukázat, že jiné zde neleží.

Dokažme nyní, že pokud nějaké $\zeta \in \mathbb{Z}_p^\times$ splňuje $\zeta^m = 1$ pro m nedělitelné p, musí to být jedno ze ζ_a definovaných před chvílí. Pro takové ζ existuje $b \in \{1, \ldots, p-1\}$ takové, že platí $\zeta \equiv b \pmod{p}$ a $\zeta\zeta_b^{-1} \equiv 1 \pmod{p}$. A označme $\beta = \zeta\zeta_b^{-1}$, potom je β kořenem polynomu $g(x) = x^{(p-1)m} - 1$. Platí $\beta \equiv 1 \pmod{p}$ a jednička splňuje $g(1) \equiv 0 \pmod{p}$ a $g'(1) \not\equiv 0 \pmod{p}$, tudíž podle Henselova lemmatu existuje jediný kořen polynomu $g(x)$, který je kongruentní s 1 modulo p. Ovšem 1 je kořenem tohoto polynomu, tudíž platí $\beta = 1$. Tudíž $1 = \zeta\zeta_b^{-1}$ a tedy $\zeta = \zeta_b$.

Kdyby v $\mathbb{Z}_p^\times$ existovala primitivní n-tá odmocnina z jedné pro nějaké n dělitelné p, pak by její $\frac{n}{p}$-odmocnina byla primitivní p-tá odmocnina z jedné. Ukážeme, že p-tá odmocnina z jedné v $\mathbb{Z}_p^\times$ neexistuje.

Pojďme se tedy podívat na variantu, kdy $n = p$, na kterou jsme nemohli použít Henselovo lemma, protože $f_p'(x) = px^{p-1} \equiv 0 \pmod{p}$.

Nejprve se podívejme na funkci $\log_p$:

$$\log_p(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(x-1)^n}{n}.$$

Použijeme Strassmanovu větu 4.3.4 na počet kořenů. Bohužel tuto větu nemůžeme použít přímo, ale musíme vytvořit novou funkci $f(x) = \log_p(1+px)$, která konverguje pro všechna $x \in \mathbb{Z}_p$:

$$f(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}p^n x^n}{n}.$$

Jak víme z druhé části věty 5.1.6 pro libovolné $n > 1$ platí $v_p(n) < n-1$. Označme $a_n = (-1)^{n-1}\frac{p^n}{n}$. Uvědomme si, že $|a_1|_p = \frac{1}{p}$ a pro $n > 1$ je $|a_n|_p = p^{v_p(n)-n} < p^{-1}$. Proto N takové, že $|a_N|_p = \max|a_n|_p$ a $|a_n|_p < |a_N|_p$ pro $n > N$, je $N = 1$. Takže podle věty 4.3.4 má funkce $f(x)$ na $\mathbb{Z}_p$ nejvýše jeden kořen, kterým je zřejmě $x = 0$. Což znamená, že $\log_p$ má v $1 + p\mathbb{Z}_p$ pouze jeden kořen, $x = 1$.

Když si vezmeme x takové, že $x^p = 1$, znamená to, že $x \equiv 1 \pmod p$. Tudíž platí $x \in 1 + p\mathbb{Z}_p$. Ovšem když $x^p = 1$, pak

$$0 = \log_p(1) = \log_p(x^p) = p\log(x) \Rightarrow \log_p(x) = 0.$$

Což znamená, že x musí být 1, protože $\log_p$ má v $1 + p\mathbb{Z}_p$ pouze jeden kořen.

Taky to znamená, že odmocniny z jedné tvoří v $\mathbb{Z}_p^\times$ grupu izomorfní s $(\mathbb{Z}/p\mathbb{Z})^\times$. □

Poznámka. *Než půjdeme dál, podívejme se na případ $p = 2$. Grupa jednotek v $\mathbb{Z}_2$ je $1 + \mathbb{Z}_2$, tedy každá odmocnina z jedné v $\mathbb{Z}_2^\times$ má nulový 2-adický logaritmus. Podívejme se na $\log_2$ a opět použijme Strassmanovu větu 4.3.4, v tomto případě je hledané $N = 2$, takže $\log_p$ může mít až dva kořeny v $1 + 2\mathbb{Z}_2$. Ale my již známe dva kořeny: 1 a -1.*

Odmocninami z jedné v $\mathbb{Z}_2$ jsou tudíž pouze ± 1, které tvoří multiplikativní grupu izomorfní $\mathbb{Z}/(4\mathbb{Z})^\times$.

Nyní, když už víme, že odmocniny v jednotlivých $\mathbb{Z}_p^\times$ tvoří grupu, a dokonce i víme, jak tato grupa vypadá, můžeme dokázat následující větu.

Věta 5.2.2. *Označme $q = p$, když $p \neq 2$, a $q = 4$, když $p = 2$. Potom každou jednotku okruhu $\mathbb{Z}_p$ můžeme napsat jako součin odmocniny z jedné ze $\mathbb{Z}_p$ a jednotky z $1 + q\mathbb{Z}_p$, a to jediným způsobem.*

Důkaz: Vezměme nějaké číslo $u \in \mathbb{Z}_p^\times$. Víme, že v každé zbytkové třídě modulo q nedělitelné p leží právě jedna odmocnina z jedné ζ. Pro $p = 2$ to možná není vidět na první pohled, ale uvědomme si, že $-1 = 3 + 4 \cdot (-1)$ a $-1 \in \mathbb{Z}_2$, tudíž $-1 \in 3 + 4\mathbb{Z}_p$.

Potom $t = u\zeta^{-1} \in 1 + q\mathbb{Z}_p$. Takže $u = t\zeta$. □

Čímž mimo jiné také dostáváme izomorfismus mezi $\mathbb{Z}_p^\times$ a $G \times (1 + q\mathbb{Z}_p)$, kde G je množina odmocnin z jedné ležících v $\mathbb{Z}_p$. Jak víme, tato množina G je izomorfní s $(\mathbb{Z}/q\mathbb{Z})^\times$.

5.3 Druhé mocniny v $\mathbb{Q}_p^\times$

Abychom pochopili, k čemu nám může být, že víme, že je $\mathbb{Z}_p^\times \cong G \times (1 + q\mathbb{Z}_p)$, pojďme se podívat, co nám to řekne o druhých mocninách v $\mathbb{Q}_p^\times$.

Nejprve se podívejme, co díky části 5.2 víme o $\mathbb{Q}_p^\times$.

Věta 5.3.1. *Pokud $p \neq 2$:*

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times (1 + p\mathbb{Z}_p).$$

V případě, že $p = 2$:

$$\mathbb{Q}_2^\times \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times (1 + 4\mathbb{Z}_p).$$

Důkaz: Z věty 5.0.2 víme, že $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times$, protože každé $x \in \mathbb{Q}_p^\times$, můžeme napsat jediným způsobem jako $p^n u$, kde $u \in \mathbb{Z}_p^\times$.

Z věty 5.2.2 ale víme, že $\mathbb{Z}_p^\times \cong G \times (1 + q\mathbb{Z}_p)$. Zde $G \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$, pro $p \neq 2$. Pro $p = 2$ je $G \cong (\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$. □

Tento izomorfismus nám pomůže odhalit, jak vypadají druhé mocniny v $\mathbb{Q}_p$, respektive čísla, jejichž druhá odmocnina leží v $\mathbb{Q}_p$.

Věta 5.3.2. *Mějme prvek $a \in \mathbb{Q}_p^\times$ vyjádřen jako $p^n u$, kde $n \in \mathbb{Z}$ a $u \in \mathbb{Z}_p^\times$ potom a je druhou mocninou právě tehdy, když jsou splněny obě následující podmínky:*

1. *n je sudé*
2. *pokud $p \neq 2$, $u \pmod{p\mathbb{Z}_p}$ je druhou mocninou v $(\mathbb{Z}/p\mathbb{Z})^\times$, pokud $p = 2$, $u \equiv 1 \pmod{8\mathbb{Z}_2}$.*

Důkaz: Aby bylo a druhou mocninou v $\mathbb{Q}_p$, musí být n sudé a u musí být druhou mocninou v $\mathbb{Z}_p^\times$. Nejprve se podívejme na případ $p \neq 2$, protože v tomto případě můžeme udělat:

$$1 + p\mathbb{Z}_p = \exp_p(p\mathbb{Z}_p) = \exp_p(2p\mathbb{Z}_p) = (\exp_p(p\mathbb{Z}_p))^2.$$

Takže každý prvek z $1 + p\mathbb{Z}_p$ je druhou mocninou v $\mathbb{Z}_p^\times$. Z věty 5.2.2 víme, že $\mathbb{Z}_p^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (1+p\mathbb{Z}_p)$, takže $\mathbb{Z}_p^\times/(1+p\mathbb{Z}_p) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Z čehož plyne, že aby bylo u druhou mocninou v $\mathbb{Z}_p^\times$, musí být $u \pmod{p\mathbb{Z}_p}$ druhou mocninou v $(\mathbb{Z}/p\mathbb{Z})^\times$.

Když $p = 2$:

$$1 + 8\mathbb{Z}_2 = \exp_2(8\mathbb{Z}_2) = \exp_2(2 \cdot 4\mathbb{Z}_2) = (\exp_2(4\mathbb{Z}_2))^2.$$

Nyní si musíme uvědomit, že $\mathbb{Z}_2^\times/(1 + 8\mathbb{Z}_2) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}/8\mathbb{Z})^\times$. Ale jedinou druhou mocninou v $(\mathbb{Z}/8\mathbb{Z})^\times$ je jednička, takže máme vyřešen i případ $p = 2$. □

Takto jsme popsali, jak vypadají druhé mocniny v $\mathbb{Q}_p^\times$, což je velmi užitečné, jak si ukážeme v následující kapitole.

Kapitola 6

Využití p-adických čísel v teorii čísel

6.1 Kvadratické zbytky

Na konci minulé kapitoly jsme popsali druhé mocniny v $\mathbb{Q}_p$ pomocí druhých mocnin v určitých $(\mathbb{Z}/n\mathbb{Z})^\times$. Vzhledem k tomu, že v této kapitole se budeme s druhými mocninami pracovat, měli bychom si připomenout, co o těchto druhých mocninách v $(\mathbb{Z}/n\mathbb{Z})^\times$ víme.

Definice 6.1.1. ***Kvadratické zbytky:*** *Mějme dvě nesoudělná čísla a, n. Potom řekneme, že a je kvadratický zbytek modulo n, pokud existuje $c \in \mathbb{Z}$ takové, že $a \equiv c^2 \pmod{n}$. V opačném případě řekneme, že a je kvadratický nezbytek modulo n.*

Druhými mocninami v $(\mathbb{Z}/n\mathbb{Z})^\times$ jsou tedy třídy obsahující kvadratické zbytky modulo n.

O kvadratických zbytcích víme několik užitečných tvrzení:

Věta 6.1.1. *Nechť p je liché prvočíslo. Potom existuje právě $\frac{p-1}{2}$ kvadratických zbytků modulo p a právě $\frac{p-1}{2}$ kvadratických nezbytků modulo p.*

Věta 6.1.2. *Nechť p je liché prvočíslo. Potom platí, že součin dvou kvadratických zbytků i dvou nezbytků modulo p je kvadratický zbytek modulo p. Naopak součin kvadratického zbytku a nezbytku modulo p je kvadratický nezbytek modulo p.*

Věta 6.1.3. *Platí, že -1 je kvadratický zbytek modulo p právě tehdy, když je $p \equiv 1 \pmod{4}$.*

Když dáme dohromady věty 6.1.2 a 6.1.3 dostaneme, že pro $p \equiv 1 \pmod{4}$ platí, že pokud je a kvadratický zbytek modulo p, pak je i $-a$ kvadratický zbytek modulo p.

Naopak pro $p \equiv 3 \pmod{4}$ neexistuje žádný kvadratický zbytek a modulo p takový, že $-a$ je kvadratický zbytek modulo p.

6.2 Lokální-globální princip

Jedním z důvodů, proč jsou p-adická čísla důležitou součástí moderní matematiky, je takzvaný lokální-globální princip, o kterém si za chvíli řekneme více. Nejdříve se ovšem pojďme podívat zpátky na absolutní hodnoty na $\mathbb{Q}$.

Už víme, že na $\mathbb{Q}$ existuje klasická absolutní hodnota, které se též někdy říká absolutní hodnota v nekonečnu $|\ |_\infty$. Taky máme triviální absolutní hodnotu a ostatní p-adické absolutní hodnoty. Otázka zní jaké další existují.

Roku 1917 přišel A. Ostrowski s následujícím tvrzením, která tuto otázku vyřešila.

Definice 6.2.1. *Dvě absolutní hodnoty* $|\ |_1$ *a* $|\ |_2$ *na tělese* $\mathbf{k}$ *jsou ekvivalentní, pokud definují stejnou topologii na* $\mathbf{k}$*. Což znamená, že každá množina, která je otevřená i vzhledem k jedné absolutní hodnotě, je otevřená vzhledem k té druhé.*

Věta 6.2.1. ***Ostrowského věta***
Každá netriviální absolutní hodnota na $\mathbb{Q}$ *je ekvivalentní s nějakou absolutní hodnou* $|\ |_p$*, kde* p *je prvočíslo nebo nekonečno.*

Platí, že dvě absolutní hodnoty jsou ekvivalentní na $\mathbf{k}$ právě tehdy, když pro každé $x \in \mathbf{k}$ platí, že $|x|_1 < 1$, právě tehdy když je i $|x|_2 < 1$. Též platí, že dvě absolutní hodnoty jsou ekvivalentní na $\mathbf{k}$ právě tehdy, když existuje $\alpha \in \mathbb{R}_+$ tak, že pro každé $x \in \mathbf{k}$ platí $|x|_1^\alpha = |x|_2$. Uvádím to zde spíše jako zajímavost, ale důkaz tohoto tvrzení můžete nalézt v [4].

Příkladem takové absolutní hodnoty ekvivalentní p-adické absolutní hodnotě může být funkce:

$$|\ |_* : \mathbb{Q} \to \mathbb{R}_+,$$

$$|x|_* \to c^{-v_p(x)}, \text{ pro pevně zvolenou konstantu } c > 1.$$

Kdybychom se vrátili zpátky k definici 2.1.2, je snadné ověřit, že se skutečně jedná o absolutní hodnotu. Každá množina, která je otevřená vzhledem k p-adické absolutní hodnotě pro konkrétní p, bude otevřená vzhledem k této absolutní hodnotě. Tyto dvě absolutní hodnoty jsou proto ekvivalentní. Můžeme si všimnou, že tyto dvě absolutní hodnoty splňují: $|x|_p < 1 \Leftrightarrow |x|_* < 1$, protože $|x|_*^\alpha = |x_p|$, pro α splňující $c^\alpha = p$.

Pokud jsou dvě absolutní hodnoty ekvivalentní, tedy zadávají stejnou topologii, platí, že posloupnosti, které jsou cauchyovské vzhledem k jedné absolutní hodnotě, jsou cauchyovské i vzhledem k druhé. To platí samozřejmě i o konvergentních posloupnostech, z čehož plyne, že dvě ekvivalentní absolutní hodnoty na $\mathbb{Q}$, nám dají stejné zúplnění na $\mathbb{Q}$.

Což znamená, že už tedy známe všechna zúplnění $\mathbb{Q}$ a umíme s nimi pracovat.

Ve dvacátých letech dvacátého století se začal německý matematik Helmut Hasse zabývat myšlenkou studování problému v $\mathbb{Q}$ pomocí studování těchto problémů v $\mathbb{R}$ a ve všech $\mathbb{Q}_p$.

Lokální-globální princip: Řekněme, že lokální-globální princip je splněn pro danou vlastnost nějakého matematického objektu definovaného nad $\mathbb{Q}$, jestliže platí následující: objekt má tuto vlastnost v $\mathbb{Q}$, právě když ji má v $\mathbb{R}$ a současně ve všech $\mathbb{Q}_p$.

O $\mathbb{Q}$ mluvíme jako o globálním tělese a o $\mathbb{R}$ a $\mathbb{Q}_p$ mluvíme jako o lokálních tělesech. Nejedná se o větu, ale spíše o filozofii. Nicméně má tato myšlenka využití jak v teorii čísel, tak v geometrii.

Například nemůžeme říct, že pokud má polynom s racionálními koeficienty kořen ve všech lokálních tělesech, má ho i v $\mathbb{Q}$ (za chvíli si ukážeme příklad). Nicméně, pokud polynom nemá kořen v nějakém z lokálních těles, určitě ho nemůže mít ani v $\mathbb{Q}$.

Příklad: Mějme rovnici

$$(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0.$$

Rovnice má zřejmě řešení v $\mathbb{R}$. Též má zřejmě řešení ve všech $\mathbb{Q}_p$, kde $p \neq 2, 17$, protože z věty 5.3.2 víme, jak vypadají čtverce v $\mathbb{Q}_p$. Pokud není čtvercem v $\mathbb{Q}_p$ 2 ani 17, znamená

to, že se nejedná o kvadratické zbytky modulo p, v takovém případě je pak druhou mocninou 34, protože součin dvou kvadratických nezbytků je kvadratický zbytek. Pro $p = 2$ je 17 podle věty 5.3.2 druhou mocninou v $\mathbb{Q}_2$, pro $p = 17$ je 2 kvadratický zbytek, protože $6^2 \equiv 2 \pmod{17}$.

Rovnice má tedy řešení ve všech lokálních tělesech, ale přitom ho nemá v $\mathbb{Q}$.

Jak vidíme, myšlenka lokálního-globálního principu skutečně vždycky neplatí, pojďme se ale podívat na pěkný příklad, kdy tato myšlenka naopak platí.

Věta 6.2.2. *Racionální číslo $x \in \mathbb{Q}$ je druhou mocninou právě tehdy, když je druhou mocninou v $\mathbb{R}$ a ve všech $\mathbb{Q}_p$.*

Důkaz: Číslo $x \in \mathbb{Q}$ můžeme napsat jako:

$$x = \pm \prod_{p \text{ je prvočíslo}} p^{v_p(x)}.$$

Pokud se jedná o druhou mocninu v $\mathbb{R}$, zaručuje nám to, že se jedná o nezáporné číslo. Pokud se jedná o druhou mocninu v $\mathbb{Q}_p$, je $v_p(x)$ sudé číslo. Tudíž je x druhou mocninou v $\mathbb{Q}$ právě tehdy, když je druhou mocninou ve všech lokálních tělesech. □

A myšlenka lokálního-globálního principu nemá využití pouze, co se týče druhých mocnin, ale všeobecně u kvadratických forem.

Věta 6.2.3. ***Hasse-Minkowského věta***
Nechť $\mathcal{Q}(x_1, \ldots, x_n)$ je kvadratická forma s racionálními koeficienty. Potom

- *pro $c \in \mathbb{Q}^\times$ má rovnice $\mathcal{Q}(x_1, \ldots, x_n) = c$ řešení v $\mathbb{Q}$ právě tehdy, když ho má v $\mathbb{R}$ a ve všech $\mathbb{Q}_p$ a*
- *rovnice $\mathcal{Q}(x_1, \ldots, x_n) = 0$ má řešení $\mathbb{Q}$ různé od $(0, \ldots, 0)$ právě tehdy, když má řešení různé od $(0, \ldots, 0)$ v $\mathbb{R}$ a ve všech $\mathbb{Q}_p$.*

Může se zdát, že se nám touto větou práce s kvadratickými formami moc neulehčí, protože potřebuje zkontrolovat nekonečně mnoho možností. Nicméně jde ukázat, že nám ve skutečnosti stačí ověřit řešení pouze v konečně mnoha $\mathbb{Q}_p$.

Jak si za chvíli ukážeme, je tato věta opravdu užitečná.

6.3 Aplikace Hasse-Minkowského věty

V této poslední části svojí práce bych chtěla ukázat užitečnost Hasse-Minkowského věty tím, že ji aplikujeme na některé známé kvadratické formy.

Hasse-Minkowského věta nám ovšem pouze říká, kdy má daná kvadratická forma řešení v $\mathbb{Q}$. V teorii čísel nás ale daleko častěji zajímá, kdy má daná kvadratická forma řešení v $\mathbb{Z}$. Proto si nejdříve formulujme následující větu, jejíž důkaz můžete nalézt v [9] na straně 45.

Věta 6.3.1. ***Davenport-Casselsova věta***
Mějme kvadratickou formu $q(X_1, X_2, \ldots, X_n) = \sum_{i,j} a_{ij} X_i X_j$ s celočíselnými koeficienty, kde $a_{ij} = a_{ji}$. Navíc pro tuto kvadratickou formu platí, že pro každou n-tici x racionálních čísel existuje n-tice a celých čísel taková, že $|q(x - a)| < 1$. Potom pokud tato kvadratická forma vyjadřuje nějaké $n \in \mathbb{Z}$ v racionálních číslech, vyjadřuje toto n i v celých číslech.

6.3.1 Součet dvou, tří a čtyř druhých mocnin

V této části budeme aplikovat Hasse-Minkowského větu na známé problémy, které trápily matematiky několik desetiletí na přelomu sedmnáctého a osmnáctého století. Jedná se o Fermatovu větu o součtu dvou druhých mocnin a Lagrangeovu větu o čtyřech čtvercích.

Tyto dvě věty mají skutečně zajímavou historii. Vše začalo již ve třetím století našeho letopočtu, když Diophantus z Alexandrie publikoval sérii knih nazvaných Aritmetika. Bohužel většina těchto knih se nedochovala. Ovšem roku 1621 Claude Bachet de Mézirac vzal zbývající knihy, udělal jejich latinský překlad a s rozsáhlými komentáři je vydal. Ukázalo se, že Diophantus v několika svých větách předpokládal, že každé přirozené číslo jde napsat jako součet čtyř druhých mocnin, ale důkaz se nikde nenašel (je možné, že Diophantus důkaz ani neměl, jenom nenašel číslo, pro které by to neplatilo a tak předpokládal pravdivost tohoto tvrzení). Od vydání Bachetova překladu Aritmetiky matematici pracovaly na důkazu tohoto tvrzení. Nicméně se to povedlo až Josephu-Louisovi Lagrangeovi v roce 1770 (tedy o více než století později). Více o tom, jakým způsobem toto tvrzení Lagrange dokázal, se můžete dozvědět v [1].

Diophantova Aritmetika ovlivnila zásadním způsobem matematiku, když se dostala do rukou Pierre de Fermata v roce 1636, čímž začala Fermatovo nadšení pro teorii čísel. Během svého života Fermat napsal na okraje této knihy 48 poznámek, ve kterých byly tvrzení, které Fermat tvrdil, že dokázal, ovšem náznak důkazu v poznámkách mělo pouze jediné z těchto tvrzení. Po Fermatově smrti jeho syn vydal Aritmetiku s poznámkami svého otce a matematici se následně snažili dokázat zbylých 47 tvrzení. Některé tvrzení se ukázala nepravdivými a poslední nevyřešené tvrzení, známé jako Velká Fermatova věta, bylo dokázáno až v roce 1994.

A právě jedním z těchto 48 tvrzení byla věta dnes známá jako Fermatova věta o součtu dvou druhých mocnin. Není jasné, jestli Fermat skutečně měl důkaz nebo si to pouze myslel, nicméně skutečný důkaz vymyslel až Leonard Euler v roce 1749 (opět o skoro století později). Eulerova práce na tomto důkazu dala základ pro dnes již známý Zákon kvadratické reciprocity, pracující s kvadratickými zbytky, které budeme používat na důkaz částečně i my.

Cílem následujícího textu je ukázat, jak mocným nástrojem je Hasse-Minkowského věta. Díky ní jsem vytvořila poměrně krátké elegantní důkazy těchto dvou tvrzení, které jsou pochopitelné i pro středoškolské studenty.

Předtím, než se pustíme do důkazů, dokažme si toto lemma, které nám později usnadní práci.

Lemma 6.3.1. *Nechť p je liché prvočíslo. Mějme nulu a dalších $\frac{p-1}{2}$ různých nenulových prvků grupy $\mathbb{Z}/p\mathbb{Z}$. Potom libovolný prvek množiny $\mathbb{Z}/p\mathbb{Z}$ můžeme dostat jako součet dvou, ne nutně různých čísel, z této množiny $\frac{p-1}{2}+1$ čísel.*

Důkaz: Důkaz povedeme sporem. Předpokládejme, že máme množinu těchto $\frac{p-1}{2}$ čísel a nulu a prvek $a \in \mathbb{Z}/p\mathbb{Z}$, který nejde napsat jako součet dvou, ne nutně různých čísel z této množiny.

Potom tato množina neobsahuje ani a ani $\frac{a}{2}$. Tedy těch $\frac{p-1}{2}$ nenulových čísel bylo vybráno z množiny zbylých $p-3$ čísel ($\mathbb{Z}/p\mathbb{Z}$ bez nuly, a a $\frac{a}{2}$).

Číslo a jde napsat jako součet dvou ne nutně různých prvků $\mathbb{Z}/p\mathbb{Z}$ právě $\frac{p+1}{2}$ způsoby. Vyřadili jsme možnosti $a = a+0 = \frac{a}{2}+\frac{a}{2}$. Ovšem, ze zbývajících $p-3$ čísel jsme pořád schopni udělat $\frac{p-3}{2}$ možných dvojic, které dávají v součtu a. Pokud a nejde napsat jako součet některé z dvojic v naší množině, znamená to, že v této množině je nejvýše jeden

prvek z každé z $\frac{p-3}{2}$ dvojic, které dávají za součet a. Tudíž by naše množina mohla mít nanejvýš $\frac{p-3}{2}+1$ čísel, což je spor, protože naše množina má $\frac{p-1}{2}+1$ prvků, což je více. □

Důsledek 6.3.1. *Vzhledem k tomu, že víme, že kvadratických zbytků modulo liché prvočíslo p je $\frac{p-1}{2}$, znamená to, že každý nenulový prvek $\mathbb{Z}/p\mathbb{Z}$ je buď kvadratický zbytek, nebo jde napsat jako součet dvou kvadratických zbytků.*

Nyní se již můžeme pustit do prvního slibovaného důkazu.

Věta 6.3.2. ***Fermatova věta o součtu dvou druhých mocnin***
Nechť p je liché prvočíslo. Potom rovnice $x^2 + y^2 = p$ má celočíselné řešení právě tehdy, když $p \equiv 1 \pmod 4$.

Důkaz: Z Hasse-Minkowského věty plyne, že pokud existuje řešení v $\mathbb{Q}_q$ pro každé q a v $\mathbb{R}$, potom existuje řešení v $\mathbb{Q}$.

Kvadratická forma $x^2 + y^2$ splňuje podmínky z věty 6.3.1. Protože pro libovolné racionální číslo x jsme schopni najít celé číslo a takové, že $|x-a| \leq \frac{1}{2} \Rightarrow (x-a)^2 \leq \frac{1}{4}$. Tudíž pro libovolné $x, y \in \mathbb{Q}$ jsme schopni najít $a, b \in \mathbb{Z}$ takové, že $(x-a)^2 + (y-b)^2 < 1$. Tedy z věty 6.3.1 víme, že pokud tato forma vyjadřuje nějaké $n \in \mathbb{Z}$ v racionálních číslech, vyjadřuje ho i v celých číslech.

Nejprve se podívejme na řešení v $\mathbb{Q}_q$, kde $q \neq p$ a $q \neq 2$. V takovém případě $p \in \mathbb{Z}_q^\times$. Z lemma 6.3.1 víme, že, buď je p samo kvadratickým zbytkem modulo q, nebo existují dva kvadratické zbytky x, y modulo q, $0 < x \leq y \leq q-1$, takové, že $x + y \equiv p \pmod q$. V případě, kdy je p kvadratickým zbytkem, stačí vzít $x = 0$ a $y = p$. Pak $p - x \equiv y \pmod q$ je kvadratický zbytek modulo q, a tedy podle věty 5.3.2 jsou x i $p - x$ druhé mocniny v $\mathbb{Q}_q$, jejichž součtem je p.

Nyní se podívejme na řešení v $\mathbb{Q}_p$. Vzhledem k tomu, že p není druhou mocninou v $\mathbb{Q}_p$, musíme ho dostat jako součet dvou nenulových druhých mocnin. V případě, kdy $p \equiv 1 \pmod 4$, nám stačí vzít 1 a $p-1$, $p-1 \equiv -1 \pmod p$, protože pro tato p se jedná o druhé mocniny podle věty 5.3.2. V druhém případě, kdy $p \equiv 3 \pmod 4$, není -1 druhou mocninou, tudíž tuto možnost nemáme. Pojďme sporem dokázat, že pro tato p neexistuje v $\mathbb{Q}_p$ řešení. Předpokládejme, že p jde napsat jako součet dvou druhých mocnin v $\mathbb{Q}_p$. Nyní vezmeme nejmenší mocninu p takovou, že po vynásobení touto mocninou se tyto prvky stanou celými p-adickými čísly - tudíž alespoň jeden z těchto dvou prvků nebude dělitelný p. Označme tato celá p-adická čísla x a y. Tímto dostaneme vyjádření liché mocniny p jako součet dvou druhých mocnin ze $\mathbb{Z}_p$. Tedy určitě musí platit $x + y \equiv 0 \pmod p$, přičemž alespoň jedno z čísel x, y není dělitelné číslem p, a tedy žádné z nich. Pak by ovšem pro nějaký kvadratický zbytek a modulo p existoval kvadratický zbytek $-a$ modulo p, což je spor s tím, že $p \equiv 3 \pmod 4$, pro které žádné takové a neexistuje. Tudíž v případě $p \equiv 3 \pmod 4$ řešení v $\mathbb{Q}_p$ neexistuje nikdy.

Nyní se podívejme na poslední případ, řešení v $\mathbb{Q}_2$. V minulém odstavci jsme vyloučili možnost, že by šlo $p \equiv 3 \pmod 4$ napsat jako součet dvou druhých mocnin, proto nyní budeme pouze dokazovat, že jde prvočíslo $p \equiv 1 \pmod 4$ napsat jako součet dvou druhých mocnin i v $\mathbb{Q}_2$. Platí, že $p \equiv 1 \pmod 8$ nebo $p \equiv 5 \pmod 8$. V prvním případě je prvočíslo podle věty 5.3.2 samo o sobě druhou mocninou v $\mathbb{Q}_2$. V druhém případě můžeme napsat toto prvočíslo jako $p = 4 + u$, kde $u \equiv 1 \pmod 8$, tudíž jde skutečně napsat jako součet dvou druhých mocnin. □

Přirozenou otázkou nyní je: které další přirozená čísla jdou napsat jako součet dvou druhých mocnin celých čísel?

Věta 6.3.3. *Nechť n je přirozené číslo. Potom $n = x^2 + y^2$ pro nějaké $x, y \in \mathbb{Z}$ právě tehdy, když každé prvočíslo $p \equiv 3 \pmod 4$ se v prvočíselném rozkladu n objevuje v sudé mocnině.*

Důkaz: Vzhledem k tomu, že se jedná pořád o stejnou kvadratickou formu jako v minulé větě, opět pro ni platí Davenport-Casselsova věta, tudíž stačí ověřit, že pro každé takové n existuje řešení v $\mathbb{Q}$.

Začneme hledáním řešením v $\mathbb{Q}_p$ pro $p \nmid n$ a $p \neq 2$. V tomto případě je důkaz stejný jako v minulé větě pro $\mathbb{Q}_q$, kde $q \neq p$ a $q \neq 2$. Stačí nám opět pouze lemma 6.3.1, protože $n \in \mathbb{Z}_p^\times$.

Nyní se podívejme na všechna $p \mid n$ takové, že $p \equiv 1 \pmod 4$ a hledejme řešení v těchto $\mathbb{Q}_p$. V případě, že p dělí n v sudé mocnině, je $n = p^{2k}u$, kde $u \in \mathbb{Z}_p^\times$. Z předchozího odstavce víme, že u umíme napsat jako součet dvou druhých mocnin, řekněme $a^2 + b^2 = u$, kde $a, b \in \mathbb{Q}_p$, a proto $p^{2k}a^2 + p^{2k}b^2 = n$. Pokud p dělí n v liché mocnině, je $n = p^{2k}pu$, kde $u \in \mathbb{Z}_p^\times$, řekněme $u = a + z$, kde $0 < a \leq p - 1$ a $z \in p\mathbb{Z}_p$. Víme, že umíme napsat p jako součet dvou druhých mocnin, řekněme $c + d = p$, kde c, d jsou druhé mocniny v $\mathbb{Q}_p$. Potom $pu = pa + pz = (c + (a-1)p + zp) + d$, vzhledem k tomu, že $(a-1)p + pz \in p\mathbb{Z}_p$, je $c + (a-1)p + zp$ druhou mocninou, tudíž umíme vyjádřit n jako součet dvou druhých mocnin v $\mathbb{Q}_p$.

Přejděme na $p \mid n$, $p \equiv 3 \pmod 4$. Pokud p dělí n v sudé mocnině, umíme toto n napsat jako součet dvou druhých mocnin v $\mathbb{Q}_p$, ze stejného důvodu jako pro p nedělící n. Pokud p dělí n v liché mocnině, platí $n = p^{2k+1}u$, kde $u \in \mathbb{Z}_p^\times$. Předpokládejme, že $n = a + b$, pro nějaké druhé mocniny $a, b \in \mathbb{Q}_p$. Opět vynásobme a, b mocninou p takovou, že dostaneme celá p-adická čísla, kde alespoň jedno z nich nebude dělitelné p, tyto nové druhé mocniny označme c, d. Potom musí platit $np^a = c + d$, kde a je sudé celé číslo, pro které platí $-a < 2k + 1$. Vzhledem k tomu, že p dělí n v liché mocnině, dostaneme ekvivalenci $np^a \equiv 0 \equiv c + d \pmod p$, což je, stejně jako v důkaze minulé věty, spor s tím, že $p \equiv 3 \pmod 4$, protože pro tato p neexistují dva kvadratické zbytky, které by v součtu dávaly nulu.

A poslední nám zbývá ověřit existenci řešení v $\mathbb{Q}_2$. Mějme naše $n = 2^k u$, kde $u \in \mathbb{Z}_2^\times$. Možnost, kde $p \equiv 3 \pmod 4$ dělí n v liché mocnině jsme již vyloučili, tudíž $u \equiv 1 \pmod 4$ (protože $3^2 \equiv 1 \pmod 4$). V případě, kdy je k sudé, už víme, že n jde napsat jako součet dvou druhých mocnin, protože u už umíme napsat jako součet dvou druhých mocnin. Pokud je k liché, musíme zjistit, jestli umíme napsat jako součet dvou druhých mocnin i $2u$. Ovšem $u \equiv 1 \pmod 8$ nebo $u \equiv 5 \pmod 8$, a v obou případech $2u \equiv 2 \pmod 8$. Ovšem to znamená, že $2u - 1 \equiv 1 \pmod 8$, a tedy se jedná o druhou mocninu v $\mathbb{Q}_2$. A rovnost $2u - 1 + 1 = 2u$ nám dává vyjádření $2u$ jako součet dvou druhých mocnin v $\mathbb{Q}_2$. □

Abychom dokázali, že jde každé přirozené číslo napsat jako součet čtyř druhých mocnin, pomůžeme si tím, že dokážeme, že ve skutečnosti většinu přirozených čísel je možné napsat jako součet tří druhých mocnin.

Lemma 6.3.2. *Přirozené číslo n jde napsat jako součet tří druhých mocnin celých čísel právě tehdy, když n není tvaru $4^l(7 + 8k)$, pro žádná $l, k \in \mathbb{Z}_+^0$.*

Důkaz: Všechna čísla, která mají ve svém prvočíselném rozkladu všechna prvočísla $p \equiv 3 \pmod 4$ v sudé mocnině, jdou napsat jako součet dvou druhých mocnin, tudíž i jako součet tří druhých mocnin. Proto se budeme zabývat pouze případem, kdy je v rozkladu čísla n některé takové prvočíslo v liché mocnině.

Nejprve ověřme, že na i na tuto kvadratickou formu platí Davenport-Casselsova věta. Jak jsme již říkali v důkazu Fermatovy věty o součtu dvou druhých mocnin, pro každé $x \in \mathbb{Q}$ umíme najít $a \in \mathbb{Z}$ taková, že $|x-a| \leq \frac{1}{2}$. Tedy pro každá $x, y, z \in \mathbb{Q}$ umíme najít $a, b, c \in \mathbb{Z}$ takové, že $(x-a)^2 + (y-b)^2 + (z-c)^2 \leq \frac{3}{4} < 1$. Tudíž nám opět stačí ověřit řešení v $\mathbb{Q}$.

Pro $p \nmid n$ jsme již ověřili existenci řešení v $\mathbb{Q}_p$ pro součet dvou druhých mocnin, proto musí existovat i řešení pro součet tří druhých mocnin.

Stejně tak pro $p \mid n$, $p \equiv 1 \pmod 4$ a pro $p \equiv 3 \pmod 4$, které n dělí v sudé mocnině, jsme ověřili, že vždy existuje řešení v $\mathbb{Q}_p$ pro součet dvou druhých mocnin, tudíž určitě zde najdeme i tři druhé mocniny, které mají za součet n.

Nyní se podívejme na $p \equiv 3 \pmod 4$, které dělí n v liché mocnině. V takovém případě $n = p^{2k}pu$, kde $u \in \mathbb{Z}_p^\times$, pojďme dokázat, že umíme napsat pu jako součet tří druhých mocnin v $\mathbb{Q}_p$. Vezměme si kvadratický zbytek $0 < a \leq p-1$. Z věty 6.1.3 víme, že $-a$ není kvadratický zbytek, ale potom z důsledku 6.3.1 plyne, že nyní existují kvadratické zbytky b, c, $0 < b \leq c \leq p-1$ takové, že $b+c \equiv -a \pmod p$. Tedy $a+b+c \equiv 0 \pmod p$. A proto určitě existuje $k \in \mathbb{Z}_p$ tak, že $a+b+(c+pk) = pu$, ovšem každý ze sčítanců a, b, $c+pk$ je druhou mocninou v $\mathbb{Q}_p$.

Tudíž pro všechna lichá p má rovnice $x^2+y^2+z^2 = n$ řešení v $\mathbb{Q}_p$. Problém tedy nastane až pro $p = 2$.

Pojďme se podívat na řešení v $\mathbb{Q}_2$. Napišme si $n = 4^l u$, kde l je celé nezáporné a 4 nedělí u. Potom $u-1$ dává po dává po dělení osmi jeden ze zbytků 0, 1, 2, 4, 5, 6. S výjimkou čísla 6 umíme každý z těchto zbytků napsat jako součet dvou sčítanců $a, b \in \{0, 1, 4\}$, což jsou druhé mocniny. Vzhledem k tomu, že je $u-a-b \equiv 1 \pmod 8$, dostáváme požadované vyjádření u jako součtu tří druhých mocnin: $(u-a-b)+a+b = u$.

Zbývá nám možnost $u \equiv 7 \pmod 8$, tj $u = 7+8k$ Pro tuto možnost sporem dokážeme, že vyjádření pro n neexistuje. Předpokládejme, že $n = 4^l(7+8k) = x^2+y^2+z^2$, kde $x, y, z \in \mathbb{Q}_2^\times$, případem, kde je některé z čísel x, y nebo z nulové, se budeme zabývat později. Přepišme si tento součet na $4^r a^2 + 4^s b^2 + 4^t c^2 = 4^l(7+8k)$, kde $2 \nmid a$, $2 \nmid b$, $2 \nmid c$. Bez újmy na obecnosti předpokládejme, že $r \geq s \geq t$. Vzhledem k tomu, že se nemuselo jednat o celá p-adická čísla, můžou být tyto exponenty i nekladné, ale to náš výpočet nijak neovlivní. Zřejmě $l \geq t$. Můžeme tedy rovnici vydělit 4^t: $4^{r-t}a^2 + 4^{s-t}b^2 + c^2 = 4^{l-t}(7+8k)$. Pokud by bylo $l-t = 0$ a $r-t \geq s-t > 0$, muselo by platit $c^2 \equiv 3 \pmod 4$, což nelze. Odtud je vidět, že musí být $s = t$. Tedy dostáváme $4^{r-t}a^2 + b^2 + c^2 = 4^{l-t}(7+8k)$. Pokud je $r-t > 0$ a $l-t > 0$, musí $b^2+c^2 \equiv 0 \pmod 4$, ale druhé mocniny v $\mathbb{Z}_2^\times$ jsou vždy kongruentní s jedničkou modulo 8, tudíž to není možné. Což znamená, že buď $r-t = 0$ nebo $l-t = 0$. V prvním případě dostaneme rovnost $a^2+b^2+c^2 = 4^{l-t}(7+8k)$. Potom by musela jedna z rovností $a^2+b^2+c^2 \equiv 0 \pmod 4$ nebo $a^2+b^2+c^2 \equiv 7 \pmod 8$ a ani jedna není možná. Poslední neprozkoumanou možností je $l-t = 0$ a $r-t > 0$, ale v tomto případě dostáváme rovnost $a^2+b^2 \equiv 3 \pmod 4$, což opět nejde. Dostáváme tedy spor s tím, že by šlo napsat $n = 4^l(7+8k)$, kde $l \in \mathbb{N}$, $k \in \mathbb{N}$, jako součet tří nenulových druhých mocnin v $\mathbb{Q}_2$.

Nyní se podívejme na možnost, kdy je jedna z druhých mocnin v součtu nulová, kterou jsme v minulém odstavci nebrali v úvahu. V takovém případě umíme vyjádřit n jako součet dvou druhých mocnin z $\mathbb{Q}_2$: $n = x^2+y^2$. Naše n není druhou mocninou z $\mathbb{Q}_2$, tudíž x i y jsou určitě nenulové. Stejně jako v minulém případě si napišme $n = 4^l(7+8k) = 4^r a^2 + 4^s b^2$, kde $2 \nmid a$, $2 \nmid b$ a $l \geq s$, $r \geq s$. Nyní vydělíme 4^s a dostaneme $n = 4^{l-s}(7+8k) = 4^{r-s}a^2 + b^2$. Nyní můžou nastat tři situace. Pokud je $r-s = 0$ a $l-s > 0$, musí platit $a^2+b^2 \equiv 0 \pmod 4$, což už víme, že nejde. Dále může nastat situace opačná: $r-s > 0$ a $l-s = 0$.

Potom by muselo platit $3 \equiv a^2 \pmod 4$, což opět nastat nemůže. Třetí možností je $r = s = l$, pak by muselo platit $7 \equiv a^2 + b^2 \pmod 8$, což též nelze.

Proto právě čísla tvaru $n = 4^l(7 + 8k)$ nejdou napsat jako součet tří druhých mocnin v $\mathbb{Q}_2$ a tudíž ani v $\mathbb{Q}$. □

Věta 6.3.4. ***Lagrangeova věta o čtyřech čtvercích***
Každé přirozené číslo jde napsat jako součet čtyř druhých mocnin celých čísel.

Důkaz: Vzhledem k tomu, že na tuto kvadratickou formu nemůžeme použít Davenport-Casselsovu větu, pomůžeme si předchozím lemmatem. Jediná přirozená čísla, která nejdou napsat jako součet tří druhých mocnin, jsou čísla tvaru $n = 4^l(7 + 8k)$. Ovšem tato čísla si můžeme rozepsat na $4^l(7 + 8k) = 4^l + 4^l(6 + 8k)$ a z předchozího lemmatu víme, že číslo $4^l(6 + 8k)$ jde napsat jako součet tří druhých mocnin. Všechna přirozená čísla jdou napsat jako součet čtyř druhých mocnin celých čísel. □

Jak vidíme, p-adická čísla a Hasse-Minkowského věta jsou opravdu silným matematickým nástrojem. Díky nim jsme schopni vyřešit problémy, které matematici řešili celé století, pouze pomocí základních znalostí sčítání, kongruencí a kvadratických zbytků.

Kapitola 7

Závěr

Doufám, že z mé práce bylo poznat, že p-adická čísla jsou krásnou oblastí matematiky propojující algebru, analýzu a teorii čísel. Navíc jsou opravdu užitečná, poslední kapitola ukazovala pouze jednu z mnoha věcí, na kterou se p-adická čísla používají. Jejich aplikaci můžeme najít například i ve známém důkazu Velké Fermatovy věty.

Svět p-adických čísel se může zdát ze začátku zvláštní a nepředstavitelný, nicméně nás donutí zamyslet se nad některými matematickými pojmy více dopodrobna. Například, co je to vlastně vzdálenost mezi dvěma čísly a že to nemusí být pouze něco, co jde změřit pravítkem. Ještě zajímavější je následná práce s touto vzdáleností v p-adické analýze. V reálné analýze se dá spousta věcí vysvětlit obrázkem, ale množinu p-adických čísel neumíme tak jednoduše nakreslit. Na druhou stranu nám ne-archimédovská vlastnost p-adické absolutní hodnoty spoustu věcí usnadnila, například jsme díky ní mohli formulovat Strassmanovu větu o kořenech funkcí definovaných mocninnými řadami, kdežto v reálné analýze nic podobného neplatí. Ovšem úplně nejkrásnější je, jak následně můžeme znalosti z p-adické analýzy využít na zkoumání algebraických struktur na $\mathbb{Q}_p$.

Tato práce má hlavně sloužit jako úvod do problematiky p-adických čísel. Já jsem se na konci rozhodla zaměřit na druhé mocniny v $\mathbb{Q}_p$ a využití při řešení kvadratických forem nad $\mathbb{Q}$, protože mi byla tato oblast nejblíže. Nicméně je to pouze jedna z mnoha oblastí, která by se dala zkoumat. Zajímavé by určitě mohlo být podívat se na další p-adické funkce definované mocninnými řadami či na algebraický uzávěr tělesa p-adických čísel.

Literatura

[1] BARRIOS, Alexander J., *Introduction to Modular Forms - Lecture notes*, dostupné online na adrese: https://www.math.arizona.edu/ swc/

[2] CONRAD, Keith, *Hensel's lemma*, dostupné online na adrese: https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf

[3] CONRAD, Keith, *The Local-Global Principle*, dostupné online na adrese: https://kconrad.math.uconn.edu/blurbs/gradnumthy/localglobal.pdf

[4] GOUVÊA, Fernando Q., *p-adic Numbers*, Springer, New York, druhá edice, 1997

[5] GOUVÊA, Fernando Q., *Hensel's p-adic Numbers: early history*, 1999, dostupné online na adrese: https://www-fourier.ujf-grenoble.fr/ panchish/Mag2009L3/GouveaHensel2.pdf

[6] GUPTA, Arushi, *The P-adic Integers, Analytically and Algebraically*, 2018, dostupné online na adrese: http://math.uchicago.edu/ may/REU2018/REUPapers/Gupta.pdf

[7] KAZUYA, K., NOBUSHIGE K., AND TAKESHI S., *Number Theory 1: Fermat's Dream*, Translations of Mathematical Monographs, volume 186, 2000

[8] KHRENNIKOV A., LOPÉZ C., OLESCHKO K., *Applications of p-adic numbers: from physics to geology*, Contemporary mathematics, volume 665, 2016

[9] SERRE, Jean-Pierre, *A Course in Aritmetics*, Springer, Paris, 1973

[10] SLOVÁK, Jan a kol., *Brisk Guide to Mathematics*, Masarykova univerzita, Brno, 2018