The p-adic numbers and Hensel's lemma

Justyna Dabrowska

Bachelor's thesis
2023:K24

Lund University

Faculty of Science
Centre for Mathematical Sciences
Mathematics

THE p-ADIC NUMBERS AND HENSEL'S LEMMA

JUSTYNA DĄBROWSKA

Date: May 2023.

Popular scientific summary

As the stereotype states, mathematicians tend to think of yet nonexistent problems and seek solution to them as a challenge. Such a rich and still expanding world of the p-adics, the main focus of this thesis, have arisen in this exact manner - with a question: what if one change 10 in decimal representation of a number into a prime? This simple idea led to the discovery of completely new mathematics, that, although follows the same schemes, produces some surprising twists.

Here, the reader shall gain knowledge about the basic laws of mathematics redefined in the p-adic setting. We will begin by introducing the necessary different branches of mathematics, starting from basic arithmetic properties, through topology and absolute values, finishing on the power series.

Therefore if the reader is looking for the answers to how is it possible that there are more p-adic numbers than the ones with base of 10, or why do only isosceles triangles exist in the p-adic space, this reading should not come as a disappointment.

Abstract

The thesis consists of four chapters, each focused on developing the knowledge and drawing new connections with the p-adic numbers and the notions that are well known from the usual analysis on the real topology.

In the first chapter, we introduce the basic structure of the p-adics, in connection to the conergent series and field axioms. Following that, in chapter two we focus on the defining the distance in the p-adic world, recalling the definition of the absolute value, valuation and exploring the metric space defined by them. After introducing the distance, we will introduce the p-adic topology connected to it, recall some of the notions from the topology and explore more the p-adic field structure. Our considerations will be rewarded by introducing the Hensel's lemma, centered on polynomials and solving congruence equations with their help.

Contents

1. Introduction

The p-adic numbers were developed more than a hundred years ago by Kurt Hensel, who based his deliberations on the work of Ernst Kummer. Their arisal was mainly influenced by an urge to extend the meaning of the power series in the subject of number theory. Hensel, basing his ideas on some structures proposed by his predecessor, made an attempt to connect the p-adics with the rational numbers, and thus introducing a new way of tackling the power series in the broader sense.

The revolutionary algorithms he defined implied the beginning of the very new field of p-adic numbers, $\mathbb{Q}_p$. The potential within this newly emerged number structure was quickly noticed, and thus the expanding of its calculus began. Hensel's analogy describes the relation that was also a motivation for the p-adics to get developed; it recounted the direct similarities between the known structure of the real numbers and complex polynomials with the p-adic numbers. The similarities noticed by Hensel led to defining completely analogous operations on the p-adic numbers as for real arithmetic, where various methods were evaluated based on the basic operations, such as addition and finding inverses.

In this thesis, we shall follow the steps of Hensel to slowly develop understanding and, most importantly, an intuition of the p-adic numbers. The considerations dating back to the nineteenth century will be interposed by some notes from the author, with many useful examples, and some drawings in order to give the most complete picture of the p-adic numbers as possible. We shall give a concise outline of the work, so the fluency of reading will not be interrupted by questions such as "why do we care about that?" or "what does it have to do with the subject?", as it often might be the case with mathematical texts.

Although, the introduction of the numbers themselves was not such an extraordinary contrivance, but the development of the completely new form of calculus definitely was. In the p-adic sense, Hensel has redefined the meaning of the metric, giving the foundations of the p-adic analysis. Ensuing the metric, we will follow the steps of Hensel's journey and present more detailed considerations about the absolute value function, and we will eventually introduce the connection between the importance of the absolute values and valuations in the p-adic calculus.

Thereafter we will take a closer look into the topology, exposing the variety of differences between the usual rational field and the p-adic fields. We will take a deep dive into the different rings and fields among the p-adics, and elaborate on their relations. Also, using the theory provided in the previous chapter, we will derive numerous advanced proofs of all the properties we manage to introduce.

The above considerations will sum up with the most important piece of the theory in this work: Hensel's Lemma. When stating the lemma, the intuition, as well as the alternative formulation drawing connection with Hensel's analogy will be given. Furthermore, numerous examples will develop the reader's intuition and give an idea of the proof of the lemma, that follows the same pattern.

The p-adic numbers, after the development discussed above was done, have found applications in various number theory proofs and types of the equations. Probably the most important result was the use of the p-adics in famous proof of Fermat's Last Theorem by Andrew Wiles.

2. Introduction to the p-adic world

2.1. **Hensel's analogy and construction of the p-adics.**

The historically accurate description of the p-adic numbers begins with Kurt Hensel, who at the turn of the 19th and 20th century described what we now call Hensel's analogy. He proposed an analogy between the already well-known field of complex polynomials and the newly defined p-adic numbers.

The ring of integers $\mathbb{Z}$ and the field of rationals $\mathbb{Q}$ are related to each other by the fact that any $x \in \mathbb{Q}$ is a quotient of $a, b \in \mathbb{Z}$: $x = \frac{a}{b}$.

Analogously, the ring of complex polynomials $\mathbb{C}[X]$ and the field of quotients on such are related to each other by the fact that for $f(X) \in \mathbb{C}(X)$ we have $p(X), q(X) \in \mathbb{C}[X]$ such that $f(X) = \frac{p(X)}{q(X)} \in \mathbb{C}(X)$, where $\mathbb{C}(X)$ is a field of quotients; compare Theorem 2.1.2 below.

Moreover, all elements of both $\mathbb{Z}$ and $\mathbb{C}[X]$ have unique factorizations, where primes $p \in \mathbb{Z}$ are analogous to the linear polynomials $(X - \alpha) \in \mathbb{C}[X]$.

Definition 2.1.1. *The ring of quotients of the complex polynomials* is

$$\mathbb{C}(X) = \left\{ \frac{g(X)}{h(X)} : \ g(X), h(X) \in \mathbb{C}[X] \text{ with } h(X) \neq 0 \right\}.$$

Theorem 2.1.2. *The ring of quotients of the complex polynomials $\mathbb{C}(X)$ is a field.*

Proof. As the ring of polynomials $\mathbb{C}[X]$ already satisfies associativity, commutativity, distributivity and identity axioms for both addition and multiplication, and has an additive inverse, it remains to show that any element $0 \neq f_1(X) \in \mathbb{C}(X)$ has a multiplicative inverse. Therefore let $g(X), h(X) \in \mathbb{C}[X]$ be such that

$$f_1(X) = \frac{g(X)}{h(X)} \in \mathbb{C}(X).$$

Observe that $g(X), h(X) \neq 0$. Then there exists

$$f_2(X) = \frac{h(X)}{g(X)} \in \mathbb{C}(X)$$

giving $f_1(X) \cdot f_2(X) = 1$. □

From now on, $\mathbb{C}(X)$ will be referred to simply as the *field of quotients*.

Furthermore, for a given prime p, any positive integer m can be written as

$$m = a_0 + a_1 p + \cdots + a_n p^n = \sum_{i=0}^{n} a_i p^i$$

for some $n \geq 0$ and a sequence (a_i) with elements in the set $\{0, 1, \ldots, p-1\}$.
Let us give a draft of the comparison between the usual integer and the p-adic number below.

We can write every integer in the usual base of 10, which can be decomposed into

$$327 = 7 \times 10^0 + 2 \times 10^1 + 3 \times 10^2.$$

Although note, that this element does not have an inverse in $\mathbb{Z}$! If we let $p = 7$ and consider the 7-adic expansion of 327, namely

$$327 = 5 \times 7^0 + 4 \times 7^1 + 6 \times 7^2$$

we will later show, that we can indeed find its inverse among 7-adic numbers.

Similarly, any complex polynomial can be written with the use of Taylor's expansion as follows:

$$f(X) = a_0 + a_1(X-\alpha) + \cdots + a_n(X-\alpha)^n = \sum_{i=0}^{n} a_i(X-\alpha)^i,$$

where n is the degree of $f(X)$, the quantity α is an arbitrary integer, and (a_i) a sequence derived from Taylor's formula, that we do not focus on; all we intend to emphasize is that it is always possible to use such representation.

More formally speaking, the map

$$f(X) \longmapsto \text{expansion around } (X-\alpha)$$

defines an inclusion of fields $\mathbb{C}(X) \hookrightarrow \mathbb{C}((X-\alpha))$, where $\mathbb{C}((X-\alpha))$ represents all expansions:

$$\begin{aligned} f(X) = \frac{p(X)}{q(X)} &= a_{n_0}(X-\alpha)^{n_0} + a_{n_0+1}(X-\alpha)^{n_0+1} + \cdots \\ &= \sum_{i \geq n_0} a_i(X-\alpha)^i. \end{aligned}$$

Analogously, any positive rational number $x = \frac{c}{d}$ can be written as formal power series

$$x = \sum_{n \geq n_0} a_n p^n \quad \text{where} \quad x = p^{n_0}\frac{\tilde{c}}{\tilde{d}} \quad \text{with} \quad p \nmid \tilde{c}\tilde{d}$$

with no usual notion of convergence with respect to the usual absolute value. Here n_0 reflects the multiplicity, that will be discussed in detail later, namely in Definition 3.1.4, and the discussion of the convergence (with respect to a different absolute value) will follow. This shows the main idea behind the construction of the p-adic numbers, and one to be considered the most formal.

Let us consider a simple example on how to compute a p-adic expansion.

Example 2.1.3. [Gou65, p.13, p.14] Consider a 5-adic expansion of $\frac{1}{2}$. First, we divide $\frac{1}{2}$ by 5 as follows

$$\frac{1}{2} = -\frac{1}{2} \cdot 5 + 3,$$

so that last digit is 3. Now, taking $-\frac{1}{2}$ and dividing by 5, we get

$$-\frac{1}{2} = -\frac{1}{2} \cdot 5 + 2.$$

Since the new quotient is equal to $-\frac{1}{2}$, we obtain 2 in the expansion forever, yielding

$$\frac{1}{2} = (\ldots 2223)_5.$$

As a check, we can multiply both sides by 2 and notice that the identity agrees (on the right hands side, taking modulo 5 of each digit).

We remark that in the above example we take uniqueness for granted; this matter will reappear in the later part of this thesis.

Definition 2.1.4. For a positive rational x, the formal power series

$$x = a_{n_0}p^{n_0} + a_{n_0+1}p^{n_0+1} + \cdots = \sum_{n \geq n_0} a_n p^n, \tag{2.1}$$

is called the *p-adic expansion* of x, where (a_i) is an arbitrary sequence of numbers taking values between 0 and $p-1$, and n_0 is the multiplicity of x with respect to p. More generally, we consider

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

for $n_0 \in \mathbb{Z}$ and $a_i = \{0, 1, \cdots, p-1\}$. Such an expression is called a *p-adic number*.

It turns out that the set of all series in the powers of p (i.e. p-adic expansions) form a field, just as $\mathbb{C}(X-\alpha)$ is a field, which we have shown in the Theorem 2.1.2. With some additional tools introduced in this chapter, we will prove that fact in detail in Theorem 2.2.9. Although from this point, we will refer to $\mathbb{Q}_p$ as the *field of p-adic numbers*.

The function taking x to its p-adic expansion gives the inclusion of fields $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$, analogous to the inclusion for complex polynomials.

Before we formulate algorithms for the basic operations on the p-adic numbers, and we consider an example of the usefulness of the construction we have introduced.

Example 2.1.5. Show that if the p-adic number has a periodic expansion then it is rational.
To solve such a problem in the intuitive way, we would use the trick similar to proving that $0.999\cdots = 1$:

$$x = 0.999\cdots \iff 10x = 9.999\cdots \implies 10x - x = 9 \iff x = 1.$$

Thus the idea is that if the expansion in the p-adic sense is periodic, then multiplying by the right power of p and subtracting will give a finite expression. The general formulation goes as follows:

$$\begin{aligned} x &= a_0 + a_1 p + \cdots + a_{k-1}p^{k-1} + a_0 p^k + \cdots + a_{k-1}p^{2k-1} + \cdots \\ \iff p^k x &= a_0 p^k + a_1 p^{k+1} + \cdots + a_{k-1}p^{2k-1} + a_0 p^{2k} + \cdots + a_{k-1}p^{3k-1} + \cdots \end{aligned}$$

and now

$$x - p^k x = a_0 + \cdots + a_{k-1}p^{k-1} \iff x = \frac{a_0 p + \cdots + a_{k-1}p^{k-1}}{1-p^k}$$

therefore $x \in \mathbb{Q}$ given that x has periodic expansion.

Note that now we have shown that the periodic expansion implies that the number is rational, but we can also aim for the reverse. The fact that the expansion is in fact unique for any number would give us the desired result, and the reverse claim will hold as well. That fact is proved later on, in Chapter 5.

2.2. **The p-adic digit, the p-adic integer and the p-adic number.** From the very formal construction, we now consider a more intuitive approach for the p-adic numbers. In order to make a connection between the theory and the calculations, we define different objects in the p-adic sense and construct addition and multiplication algorithms on such; we will also focus on some basic properties of them.

Clearly, similarly as in the base of 10, the p-adic number will be an integer (a p-adic integer in that sense) if its p-adic expansion will contain only non-negative powers of p. Although, there is much more than that to see; thus we define p-adic integers will more detail below.

Definition 2.2.1. [Gou65, p.17, p.84] The *p-adic digit* is a natural number d such that $0 \leq d < p$, where p is prime.

We call a sequence of p-adic digits $(d_i)_{i\in\mathbb{N}}$ a *p-adic integer*, which corresponds to the formal sum and informal notation

$$\sum_{i=0}^{\infty} d_i p^i = \cdots d_i \cdots d_1 d_0.$$

We define $\mathbb{Z}_p$ as the set of *p-adic integers*:

$$\mathbb{Z}_p := \{(d_i)_{i\in\mathbb{N}} : d_i \text{ is a } p\text{-adic digit}\} = \{\cdots d_i \cdots d_1 d_0 : d_i \text{ is a } p\text{-adic digit}\},$$

that relates to the p-adic numbers such that

$$x \in \mathbb{Z}_p \iff x = \sum_{n\geq 0} a_n p^n.$$

Before we draw any conclusions, let us consider some simple example of the p-adic integer.

Example 2.2.2. Consider an integer 583, then its 5-adic expansion is

$$583 = 3 \times 5^0 + 1 \times 5^1 + 3 \times 5^2 + 4 \times 5^3,$$

what translates into $(583)_{10} = (4313)_5$ by the formulation given above. Note that similarly to the notion of the usual integers, the p-adic integers allow only non-negative powers of p in the expansion (so the lowest power appearing in the expansion is 0).

We can clearly see that $\mathbb{Z}_p$ is not a field, since similarly to $\mathbb{Z}$ it does not contain inverses of some of its elements. Thus we want to show that apart from that condition, the set $\mathbb{Z}_p$ fulfills all the other axioms, and is therefore an integral domain.

Proposition 2.2.3. *[Che18, Proposition 1.2] The set $\mathbb{Z}_p$ is an integral domain.*

Proof. By the construction we know that $\mathbb{Z}_p$ is a commutative ring with unity (containing identity element), so we only need to show it has no zero divisors. Suppose we have two p-adic integers

$$\alpha = \sum_i \alpha_i p^i \text{ and } \beta = \sum_j \beta_j p^j, \text{ with } \alpha, \beta \neq 0, \ \ 0 \leq \alpha_i, \beta_j \leq p-1 \ \forall i, j.$$

Then take some elements of the sums α_n, β_m that are both non-zero, and we know they exist since α and β are non-zero. Consider $\alpha\beta =: \gamma$ and write $\gamma = \sum_l \gamma_l p^l$. It follows that an arbitrary element of the sequence γ_k can be expressed as

$$\sum_{n+m=k} \alpha_n \beta_m \equiv \gamma_k \pmod{p},$$

and for ν, μ minimal such that $\alpha_\nu \neq 0$, $\beta_\mu \neq 0$, then $\gamma_\kappa \neq 0$, which implies $\gamma \neq 0$. Therefore $\mathbb{Z}_p$ has no zero divisors and is an integral domain. □

The integral domain $\mathbb{Z}_p$ does not contain all inverses as we have mentioned above, thus we consider if there is some condition on which we can easily determine, whether the element has an inverse.

Lemma 2.2.4. *[Che18, Lemma 1.3] A p-adic integer is invertible if and only if $d_0 \neq 0$.*

Proof. Define reduction modulo p as the map

$$\varphi : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p\mathbb{Z} \text{ by } (d_i)_{i\in\mathbb{N}} = \sum_{i=0}^{\infty} d_i p^i \mapsto d_0 \pmod{p},$$

i.e. mapping a p-adic integer to its last digit. It is easy to see that this is a ring homomorphism.

($\Longrightarrow$) Suppose $(d_i)_{i\in\mathbb{N}}$ is invertible, then $\varphi((d_i)_{i\in\mathbb{N}}) = d_0$ is as well, since φ maps one element of the sequence to the other. This means d_0 has an inverse in $\mathbb{Z}/p\mathbb{Z}$ and $d_0 \neq 0$.

($\Longleftarrow$) Suppose $d_0 \neq 0$, we want to show (d_i) is invertible by proposing a general method to find such an inverse. By assumption, we can always find an inverse

$$a_0 = d_0^{-1} \in (\mathbb{Z}/p\mathbb{Z})^\times \quad \text{such that} \quad a_0 d_0 \equiv 1 \pmod{p}.$$

Then

$$(d_i)_{i\in\mathbb{N}} = \sum_{i=0}^{\infty} d_i p^i = d_0 + d_1 p + d_2 p^2 + \cdots = d_0 + p\delta,$$

where $\delta = d_1 + d_2 p + \cdots$, which yields

$$\begin{aligned}(d_i)_{i\in\mathbb{N}} a_0 &= d_0 a_0 + d_1 a_0 p + d_2 a_0 p^2 + \cdots \\ &= 1 + p a_0 (d_1 + d_2 p + \cdots) \\ &= 1 + p a_0 \delta \equiv 1 \pmod{p}.\end{aligned}$$

We also note that for some $t \in \mathbb{Q}_p$

$$(d_i)_{i\in\mathbb{N}}\ a_0 (1 + pt)^{-1} = 1 \iff (d_i)_{i\in\mathbb{N}}^{-1} = a_0 (1 + pt)^{-1},$$

thus we only need to prove that $(1 + tp)$ is invertible. By the Taylor expansion we can write

$$(1 + tp)^{-1} = 1 - tp + (tp)^2 - (tp)^3 + \ \cdots = 1 + b_1 p + b_2 p^2 + \ \cdots \in \mathbb{Z}_p,$$

with $(d_i)_{i\in\mathbb{N}}$ the p-adic digits. We see that constant term 1 is never eliminated, thus $(1 + tp)^{-1} \neq 0$ and $(d_i)_{i\in\mathbb{N}}$ has an inverse. □

We shall summarise with defining the relation between the p-adic integers $\mathbb{Z}_p$ and the p-adic numbers $\mathbb{Q}_p$ introduced above.

Proposition 2.2.5. *The ring $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$.*

Proof. For $\mathbb{Z}_p$ to be a subring of $\mathbb{Q}_p$, we need it to be non-empty (which is obvious to see), closed under subtraction, multiplication and containing all additive inverses, by the subring definition.

The last part is obvious, as we can define an isomorphism that takes $a \mapsto -a$, which by definition of the ring is also in $\mathbb{Z}_p$, and thus all additive inverses are included.

Let us consider two elements of $\mathbb{Z}_p$,

$$a = \sum_i a_i p^i \ \text{ and } \ b = \sum_j b_j p^j, \ \text{ with } a, b \neq 0.$$

We know that all i, j are greater or equal to 0, thus we consider

$$\begin{aligned}a - b &= (a_0 + a_1 p + a_2 p^2 + \cdots) - b_0 - b_1 p - b_2 p^2 - \cdots \\ &= (a_0 - b_0) + (a_1 - b_1) p + (a_2 - b_2) p^2 + \cdots \\ &= c_0 + c_1 p + c_2 p^2 + \cdots,\end{aligned}$$

and we obtain some new p-adic number $c = a - b$. Now, it is left to show that $c \in \mathbb{Z}_p$. For that we claim that any $c_k \in \{0, 1, \ldots, p-1\}$, but we know that it might be the case that $a_k - b_k < 0$. Therefore, if that would be the case, we consider the nearby coefficients as below:

$$\begin{aligned}
&\cdots + (a_k - b_k)p^k + (a_{k+1} - b_{k+1})p^{k+1} + \cdots \\
&= \cdots + (-c_k)p^k + (a_{k+1} - b_{k+1})p^{k+1} + \cdots \\
&= \cdots + p^k((a_{k+1} - b_{k+1}) \cdot p - c_k) + \cdots \\
&= \cdots + d_k p^k + d_{k+1} p^{k+1} + \cdots ,
\end{aligned}$$

where we expand the higher term with the given scheme, and produce new coefficients $d_k, d_{k+1} \in \{0, 1, \ldots, p-1\}$ that imply the result of the subtraction is indeed a p-adic integer.

Lastly, we check if the multiplication of two p-adic integers also belongs to $\mathbb{Z}_p$. Considering the same two elements as above, with $i, j \geq 0$, while performing the multiplication we sum up the powers of p from the numbers a and b, thus the resulting powers are also always greater or equal to zero. Moreover, any multiplication of non-zero coefficients a_i and b_j results in something non-divisible by p, but it might be the case that the sum of a few such terms is indeed divisible by p or that is greater than $p-1$, and thus cannot be a coefficient of a p-adic number. In order to cover those cases, we refer the reader to the *Multiplication algorithm* part of this section. Hence we are done. □

After summarising the structural properties, we shall establish some basic operations and illustrate them with examples.

Addition algorithm. Based on the formulation above, we can define addition on the p-adic integers (and therefore, the p-adic numbers in general) as follows; if

$$\cdots c_{n_0+2}\ c_{n_0+1}\ c_{n_0} = \cdots a_{n_0+2}\ a_{n_0+1}\ a_{n_0} + \cdots b_{n_0+2}\ b_{n_0+1}\ b_{n_0},$$

where n_0 is the minimal power of p appearing in a and b. Note, that if the minimal power is higher in one of the terms, the rest can be just zeros. Let us look at an arbitrary part of the algorithm. Then we consider the addition as

$$\begin{array}{ccccc}
 & \epsilon_k & \epsilon_{k-1} & & \\
\cdots & a_{k+1} & a_k & a_{k-1} & \cdots \\
\cdots & b_{k+1} & b_k & b_{k-1} & \cdots \\
\hline
\cdots & (a_{k+1} + b_{k+1} + \epsilon_k) & (a_k + b_k + \epsilon_{k-1}) & (a_{k-1} + b_{k-1} + \epsilon_{k-2}) & \cdots
\end{array}$$

where $a_{k-1} + b_{k-1} = \epsilon_{k-1} p + c_{k-1}$, with ϵ_{k-1} is either 0 or 1. Thus we consider two cases:

$$c_{k-1} \equiv \begin{cases} a_{k-1} + b_{k-1} & \text{if } \ \epsilon_{k-1} = 0, \\ a_{k-1} + b_{k-1} - p & \text{if } \ \epsilon_{k-1} = 1, \end{cases}$$

then ϵ_i is called a carry digit, and we continue the scheme in the analogous manner, resulting in some number $\cdots c_{n_0+2}\ c_{n_0+1}\ c_{n_0}$.

We note numerous similarities with the addition defined on the real numbers: we also start the algorithm "from the end" and continue with adding multiples of the higher powers of p, same as with base 10. Also, the idea of the carry digit is identical to the one we have in the real sense. For focusing our attention on the differences though, we consider the example below.

Example 2.2.6. Recalling what we have introduced before, we want to show that the 5-adic expansion of -1 can be written as

$$-1 = \sum_{k=0}^{\infty} 4 \cdot 5^k = 4 + 4 \cdot 5 + 4 \cdot 5^2 + \cdots .$$

Consider expansion of $1 = 1 + 0 \cdot 5^1 + 0 \cdot 5^2$. Then the sum of the expressions for 1 and -1 should equal to 0. We check this with the algorithm proposed above using the carry digits.

$$\begin{array}{r} {\scriptstyle 1\,1\,\,} \\ \cdots 444 \\ 1 \\ \hline \cdots 000 \end{array}$$

The addition, same as multiplication, is defined for both $\mathbb{Z}_p$ and $\mathbb{Q}_p$.

Multiplication algorithm. Let $\sum a_k p^k, \sum b_k p^k$ be elements in $\mathbb{Q}_p$. Note, that we can always bring out the lowest power of p in any element to obtain some expansion with only powers of p more or equal zero. To find the c_i term of the result of the multiplication we need to collect the terms from the corresponding multipliers, for example:

$$\begin{aligned} c_0 &= a_0 b_0 \\ c_1 &= a_0 b_1 + a_1 b_0 \\ c_2 &= a_0 b_2 + a_1 b_1 + a_2 b_0 \end{aligned}$$

and so on. Although it is not trivial to see anymore as in the addition case, the multiplication also follows the scheme from real arithmetic. Here, each c_i represents the sum "below the line", as we perform the usual multiplication. Therefore we see, that as we move to the left, the more numbers we should add together.

Example 2.2.7. We want to prove that $\sqrt{-1}$ exists in $\mathbb{Z}_5$, so let $\sqrt{-1} = \sum_i a_i p^i$. Then we consider

$$\begin{array}{lrrr} \cdots & a_2 & a_1 & a_0 \\ \cdots & a_2 & a_1 & a_0 \\ \hline \cdots & a_0 a_2 & a_0 a_1 & a_0^2 \\ \cdots & a_1^2 & a_0 a_1 & \\ \cdots & a_0 a_2 & & \\ \hline \cdots & a_1^2 + 2a_0 a_2 & 2a_0 a_1 & a_0^2 \end{array}$$

that has to equal $\cdots 444$. We obtain

$$a_0^2 \equiv 4 \pmod 5 \iff a_0 \equiv 2 \text{ or } 3 \pmod 5.$$

If we choose $a_0 \equiv 3$, then we carry $+1$ to the next term (since $a_0^2 = 9 = 4 + 1 \cdot 5$) and

$$\begin{aligned} & 2a_0 a_1 + 1 \equiv 4 \pmod 5 \\ \iff\ & 6a_1 + 1 \equiv 4 \pmod 5 \\ \iff\ & a_1 + 1 \equiv 4 \pmod 5 \\ \iff\ & a_1 \equiv 3 \pmod 5. \end{aligned}$$

Now we get $2a_0a_1 + 1 = 4 \cdot 5 + 4$ from the first equation, thus we carry over $+4$ and get

$$\begin{aligned} a_1^2 + 2a_0a_2 + 4 \equiv 4 \pmod 5 &\iff 9 + 6a_2 \equiv 0 \pmod 5) \\ &\iff a_2 \equiv 1 \pmod 5). \end{aligned}$$

Carrying the algorithm over we would get more coefficients, but for now we obtain $\cdots 133$. We also note, that choosing $a_0 \equiv 2$, we would get different representation of $\sqrt{-1}$.

That is correct, we will obtain two different representations of $\sqrt{-1}$, but it doesn't contradict the uniqueness proposed above! Indeed, also in the usual $\mathbb{C}$, we have two different representations of $\sqrt{-1}$: i and $-i$, and the reason is that square root will always give two different results.

Example 2.2.8. We want to find the 5-adic expansion of $\frac{7}{15}$. Let

$$7 = \sum_i a_i 5^i = 2 \cdot 5^0 + 1 \cdot 5^1,$$

and

$$15 = \sum_j b_j 5^j = 0 \cdot 5^0 + 3 \cdot 5^1.$$

Thus in $\mathbb{Q}_5$, the number $\frac{7}{15}$ corresponds to

$$\frac{\alpha}{\beta} = \frac{2 \cdot 5^0 + 1 \cdot 5^1}{0 \cdot 5^0 + 3 \cdot 5^1}.$$

We notice that while α is coprime with 5, the number β is not, thus we need to manipulate the fraction a bit to obtain

$$\beta = 5 \sum_j b_j 5^{j-1} = 5(3 + 0 \cdot 5 + 0 \cdot 5^2 + \cdots).$$

Then

$$\frac{\alpha}{\beta} = 5^{-1}(2 \cdot 5^0 + 1 \cdot 5^1 + \cdots)(3 + 0 \cdot 5 + 0 \cdot 5^2 + \cdots)^{-1},$$

so we are looking for an inverse of $(\cdots 003)_5$.

We look for an integer that multiplied by $(\cdots 003)_5$ would give $(\cdots 001)_5$, so we are actually looking for what we are multiplying by (second row of the multiplication). Therefore we carry the multiplication digit by digit, again, by guessing and checking. We start from "what we have to multiply 3 with to get 1 under the line, what gives us the obvious answer 2, and the first row to be 6, or in the 5-adic $(\cdots 0011)_5$. Now, we look for a digit x such that $3 \cdot x + 1 \equiv 0$, so the guess is 3, and we continue in the similar manner to obtain $(\cdots 003)^{-1}$; see the left computation below. Finally, we multiply $\alpha \cdot (\cdots 003)^{-1}$ in the right computation.

$$\begin{array}{l} \cdots 00003 \\ \cdots 13132 \\ \hline \cdots 00011 \\ \cdots 0014 \\ \cdots 003 \\ \cdots 14 \\ \cdots \\ \hline \cdots 00001 \end{array} \qquad\qquad \begin{array}{l} \cdots 13132 \\ \cdots 00012 \\ \hline \cdots 31314 \\ \cdots 3132 \\ \cdots 000 \\ \cdots 00 \\ \cdots \\ \hline \cdots 13134 \end{array}$$

Hence $(\cdots 003)^{-1} = (\cdots 13132)_5$, and

$$\begin{aligned}\frac{\alpha}{\beta} &= 5^{-1}(\cdots 13134)_5 \\ &= 4\cdot 5^{-1} + 3\cdot 5^0 + 1\cdot 5^1 + 3\cdot 5^2 + 1\cdot 5^3 + \cdots = (\cdots 1313.4)_5.\end{aligned}$$

Finally we are able to prove that $\mathbb{Q}_p$ is indeed a field.

Theorem 2.2.9. *[Gou65, Chapter 3] The set $\mathbb{Q}_p$ is a field.*

Proof. Consider two p-adic numbers

$$x = \sum_{n\geq n_0} a_n p^n, \quad y = \sum_{n\geq n_1} b_n p^n.$$

Suppose without loss of generality that $n_1 \geq n_0$, and thus $n_1 = n_0 + k$. Then the addition is performed as

$$\begin{aligned}x + y &= a_{n_0}p^{n_0} + a_{n_0+1}p^{n_0+1} + \cdots + b_{n_1}p^{n_1} + b_{n_1+1}p^{n_1+1} + \cdots \\ &= a_{n_0}p^{n_0} + \cdots + a_{n_0+k-1}p^{n_0+k-1} + a_{n_0+k}p^{n_0+k} + \cdots + \\ &\quad b_{n_0+k}p^{n_0+k} + b_{n_0+k+1}p^{n_0+k+1} + \cdots \\ &= a_{n_0}p^{n_0} + \cdots + a_{n_0+k-1}p^{n_0+k-1} + (a_{n_0+k} + b_{n_1})p^{n_0+k} + \cdots .\end{aligned}$$

By assumption, we have $a_i, b_j < p$, but $a_i + b_j$ might not be less than p anymore. In that case, consider an arbitrary term from the second part of the sum with the property $a_{n_0+k+l} + b_{n_1+l} > p$, then

$$(a_{n_0+k+l} + b_{n_1+l})p^{n_0+k+l} = (c_1p + d_1)p^{n_0+k+l} = d_1p^{n_0+k+l} + c_1p^{n_0+k+l+1}. \tag{2.2}$$

Note that the term $c_1p^{n_0+k+l+1}$ will get included in the next element of the expansion, and thus addition is defined on $\mathbb{Q}_p$.

Multiplication is defined analogously as

$$\begin{aligned}xy &= (a_{n_0}p^{n_0} + a_{n_0+1}p^{n_0+1} + \cdots)(b_{n_1}p^{n_1} + b_{n_1+1}p^{n_1+1} + \cdots) \\ &= a_{n_0}b_{n_1}p^{n_0+n_1} + (a_{n_0}b_{n_1+1} + a_{n_0+1}b_{n_1})p^{n_0+n_1+1} + \cdots ,\end{aligned}$$

then we can rename the given sequence as

$$\begin{aligned}c_{n_2} &= a_{n_0}b_{n_1}, \\ c_{n_2+1} &= a_{n_0}b_{n_1+1} + a_{n_0+1}b_{n_1}, \\ &\vdots\end{aligned}$$

where

$$xy = z = \sum_{n\geq n_2} c_n p^n.$$

Lastly, we check if all the non-zero elements of $\mathbb{Q}_p$ indeed have inverses. Let x and y as above, with $xy = z$. We want to show that we can always find y such that $z = 1$, the identity element, given some x in $\mathbb{Q}_p$. If $z = 1$, then the coefficient $c_0 = 1$ and all other $c_n = 0$, for $n \geq n_2$, $n \neq 0$. Now compare it to the coefficients given above: all of $c_{n_2+1}, c_{n_2+2}, ...$ can be solved to be equal to zero, as they are defined as sums of elements in modulo p. Only c_{n_2} cannot be equal to zero, as neither a_{n_0} nor b_{n_1} are zeros by assumption. But it can be equal to 1: given x and thus a_{n_0}, which is an element modulo p, is always had an inverse modulo p, so we let $b_{n_1} = a_{n_0}^{-1}$. Therefore solving the system of equations

$$\begin{aligned} c_{n_2} &= a_{n_0} b_{n_1} = 1, \\ c_{n_2+1} &= a_{n_0} b_{n_1+1} + a_{n_0+1} b_{n_1} = 0, \\ &\vdots \end{aligned}$$

will give the desired result, that will be a well defined element of $\mathbb{Q}_p$, just as z is. The fact that the solution will be indeed unique will be proven in the next chapter, after introducing less tedious notation.

The above shows that $\mathbb{Q}_p$ is indeed a field. □

As the derivation of the p-adic numbers, together with basic operations on them, has been introduced in detail, we switch our focus onto the construction of the absolute value functions. The next chapter will require a bit more of patience, as we will slowly explore the type of such functions, and smoothly move into the p-adic setting.

3. Absolute value functions

3.1. **Valuations.** After introducing the main idea of the p-adics, we begin this section with recalling some basic terms, and the mathematical meaning behind them, that will appear regularly in regards to the general idea of the p-adic numbers.

A *space* is a set with some added structure. By *p-adic space* we mean the set of p-adic numbers along with the valuation and absolute value structures, that we will define soon.

The reason of introducing the term is to draw an analogy between the p-adic space and the usual real space.

This chapter will focus on developing the structure of the field $\mathbb{Q}_p$ of the p-adic numbers. In order to give more intuition behind $\mathbb{Q}_p$, we define the notion of distance, which is well defined on the set of real numbers, in a more detail manner.

Therefore we start this section by redefining the absolute value function, or in other words, expanding its definition in the p-adic sense. We will draw a connection between both, and mark the differences, which will also give more understanding of the distinctions between the fields. Lastly, we will give some intuitive examples on how to approach the valuations.

In order to not lose generality yet, we present the definitions with the use of some arbitrary field $\daleth$.

Definition 3.1.1. [Gou65, Definition 2.1.1] An *absolute value* on a field $\daleth$ is a function

$$|\cdot| : \daleth \longrightarrow \mathbb{R}_+$$

such that it satisfies

(1) $|x| = 0 \iff x = 0$,

(2) $|xy| = |x||y|$ for all $x, y \in \daleth$,

(3) $|x + y| \leq |x| + |y|$ for all $x, y \in \daleth$.

Moreover, the absolute value is called *non-archimedian* if it satisfies

$(3)^*$ $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in \daleth$.

The above inequality is often referred to as an *ultrametric inequality.*

We note that the condition $(3)^*$ is much stronger than (3), thus we have just created a new subset of absolute values. We shall consider two easy examples of functions that respectively do and do not satisfy the condition $(3)^*$ to give the intuition behind their behaviour.

Example 3.1.2. The infinite absolute value is defined as we know it from basic calculus:

$$|x| = \begin{cases} -x & \text{if } x < 0, \\ x & \text{if } x \geq 0. \end{cases}$$

It is easy to notice (for example, by taking $x = y = 1$) that the condition $(3)^*$ does not hold for this absolute value, thus we refer to it as *archimedian.* Also, for the reasons described later, we call it the infinite absolute value, denoted as $|\cdot|_\infty$.

Example 3.1.3. The trivial absolute value is defined as

$$|x| = \begin{cases} 1 & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

This absolute value works on every given field, and is the easiest example of a non-archimedian absolute value. Even though it plays an important role in general, we will not be referring to it in this text.

After stating in detail what the absolute value functions are, and dividing them into two main groups by their properties, we shall focus on relating them to the p-adic numbers. In order to further study the p-adic numbers, we want to introduce the notion of distances on $\mathbb{Q}_p$ - that is the main reason we have shifted our attention to the absolute values. The goal is to introduce a function measuring any object with the relation to our prime p, therefore we should consider defining a map measuring "how much the given object is divisible by p".

Definition 3.1.4. [Gou65, Definition 2.1.2] The *p-adic valuation* on $\mathbb{Z}$ is the function

$$v_p : \mathbb{Z} - \{0\} \longrightarrow \mathbb{R}$$

defined as follows: for an integer $n \in \mathbb{Z} - \{0\}$, let $v_p(n)$ be the unique integer satisfying

$$n = p^{v_p(n)} n' \text{ where } p \nmid n'.$$

We extend the map v_p to the field of rationals as follows. If

$$x = \frac{a}{b} \in \mathbb{Q} \text{ then } v_p(x) = v_p(a) - v_p(b).$$

By the construction we get $v_p(0) = \infty$.

Notice the similarity with the general real case here as well. The usual absolute value measures how many units we are from the origin, thus here the equivalent units are the powers of p.

As in general now we are dealing with some exponents, it is rather easy to see that the computational rules for the p-adic valuation will follow the ones for exponents from the real analysis.

Lemma 3.1.5. *[Gou65, Lemma 2.1.3] For all $x, y \in \mathbb{Q}$ we have*

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

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

Proof. (1) Let

$$x = p^{v_p(x)} x', \quad y = p^{v_p(y)} y' \text{ where } p \nmid x', p \nmid y'$$

by definition. Then we have

$$xy = p^{v_p(x)} x' p^{v_p(y)} y' = p^{v_p(x)+v_p(y)} x'y' \text{ where } p \nmid x'y'$$
$$\Longrightarrow v_p(xy) = v_p(x) + v_p(y).$$

(2) Consider a similar set-up for x and y, then

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

By picking the smaller power of both, we let

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

where one of the powers in the parenthesis is equal to zero. Without loss of generality, we let

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

and thus we see

$$p \nmid (p^{v_p(x)-\min\{v_p(x),v_p(y)\}}x' + y')$$

as $p \mid p^{v_p(x)-\min\{v_p(x),v_p(y)\}}x'$ but $p \nmid y'$ by assumption. Hence

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

Finally, we make the connection between a valuation and an absolute value function, by defining the p-adic absolute value as below.

Definition 3.1.6. [Gou65, Definition 2.1.4] For any $x \in \mathbb{Q}$, we define the *p-adic absolute value of x* by

$$|x|_p = p^{-v_p(x)} \text{ if } x \neq 0,$$

and set $|0|_p = 0$ for all p.

Theorem 3.1.7. *The p-adic absolute value is an absolute value function.*

Proof. To check if the introduced function is an absolute value function, one needs to check if it satisfies Definition 3.1.1 for the absolute values and is well-define; the latter comes later in the chapter, and we focus of the first part below.

By definition, $|x|_p = p^{-v_p(x)}$ and since there exists no finite power of p that would give 0, the only case when $|x|_p = 0$ is $x = 0$. For the second condition, we have

$$|xy|_p = p^{-v_p(xy)} \overset{*}{=} p^{-v_p(x)}p^{-v_p(y)} = |x|_p|y|_p,$$

where $*$ holds from Lemma 3.1.5(1). Finally, recall that from Lemma 3.1.5(2) we know that

$$|x+y|_p = p^{-v_p(x+y)} \leq p^{-\min\{v_p(x),v_p(y)\}}.$$

Then we have

$$\begin{aligned}|x|_p + |y|_p &= p^{-v_p(x)} + p^{-v_p(y)} \\ &= p^{-\min\{v_p(x),v_p(y)\}} + p^{-\max\{v_p(x),v_p(y)\}} \\ &\overset{**}{\geq} p^{-\min\{v_p(x),v_p(y)\}} \geq p^{-v_p(x+y)} = |x+y|_p,\end{aligned}$$

where $**$ is true since any valuation is always greater or equal to 0. This shows the p-adic absolute value satisfies all conditions from the definition. $\square$

Intuitively, as we increase "the divisibility" by p, i.e. we will have a higher valuation, the p-adic absolute value will tend to zero. Speaking more simply, the more a number is divisible by p, the lower its p-adic absolute value.

Proposition 3.1.8. *[Gou65, Proposition 2.1.5] The p-adic absolute value is non-archimedian.*

Proof. Consider two arbitrary elements $x, y \in \mathbb{Q}$ such that $|x|_p = n$, $|y|_p = m$. In other words we have $x = p^{-n}a$ and $y = p^{-m}b$ for $a, b \in \mathbb{Q}$ where $p \nmid a, b$. Without loss of generality let $m < n$, then

$$\begin{aligned}|x+y|_p &= |p^{-n}a + p^{-m}b|_p = |p^{-n}(a + p^{-m+n}b)|_p = \\ &= |p^{-n}|_p|a + p^{-m+n}b|_p = n|a + p^{-m+n}b|_p = n\end{aligned}$$

since $a + p^{-m+n}b$ is not divisible by p from the assumption. Thus

$$|x+y|_p = n = \max\{|x|_p, |y|_p\}$$

and the $|\cdot|_p$ is non-archimedean. □

Note that if we only concentrate on the non-negative integers for a moment, their valuations are the natural numbers together with infinity, thus the p-adic absolute values will all be contained between 0 and 1.

To visualise that simple concept, we consider two basic examples below.

Example 3.1.9.

$$|123|_5 = |123 \cdot 5^0|_5 = 5^{-0} = 1,$$

$$|75|_5 = |3 \cdot 5^2|_5 = 5^{-2} = \frac{1}{25},$$

$$\left|\frac{375}{1010}\right|_5 = \left|\frac{3 \cdot 5^3}{202 \cdot 5^1}\right|_5 = 5^{-3-(-1)} = 5^{-2} = \frac{1}{25}.$$

To further develop our intuition, we consider a small exercise. Referring back to the very first section, we conclude that according to Hensel's analogy we should be able to derive a similar notion for the field of quotients of complex polynomials. For a field $\daleth$, define

$$\daleth(t) =: \left\{\frac{f(t)}{g(t)} : f(t), g(t) \in \daleth[t],\ g(t) \neq 0\right\}.$$

For $f(t) \in \daleth[t]$, set $v_\infty(f(t)) = -\deg(f(t))$, such that we have

$$v_\infty\left(\frac{f(t)}{g(t)}\right) = v_\infty(f(t)) - v_\infty(g(t)) = \deg(g(t)) - \deg(f(t)).$$

The properties satisfied by this construction should also be analogous to the p-adic valuation. If $v_\infty(\frac{f}{g}) = 0$, we have no dependence on t, and thus the function is constant, analogically to the number being coprime with p.
The first zero condition is obvious, thus we consider

$$v_\infty(f(t)g(t)) = -\deg(f(t)) - \deg(g(t)) = v_\infty(f(t)) + v_\infty(g(t)),$$

which is the second condition from the Definition 3.1.4. Now, for the third and last one, we have

$$v_\infty(f(t)+g(t)) = -\deg(f(t)+g(t)) \leq -\max\{\deg(f(t)), \deg(g(t))\},$$

which is not so obvious to see. Generally, if we have two polynomials of different degree that we aim to add, the resulting polynomial will have the degree same as the higher degree of one of the adding polynomials. However it might be the case that $f(t)$ and $g(t)$ have the same degrees and additionally when we add them together, the first term (or terms) cancel out, then the degree of the resulting polynomial will be lower than the maximum degree of $f(t)$ and $g(t)$. This shows the construction on polynomials also makes sense with the introduced definition of the absolute value.

3.2. **Properties of the absolute value functions.** Before we move on to discuss the absolute value functions in more detail, we should consider an alternative formulation of the definition. Recall that the non-archimedean and archimedean properties, respectively, are stated as

(3) $|x+y| \leq |x| + |y|$ for all $x, y \in \daleth$,

(3)* $|x+y| \leq \max\{|x|,|y|\}$ for all $x, y \in \daleth$.

In order to take into account all the possibilities, we aim to rephrase the above into a single condition written as

(3) there exists $C \in \daleth$ such that $|b| \leq 1 \Longrightarrow |1+b| \leq C$.

For this purpose, we introduce the following lemmas.

Lemma 3.2.1. *[Cas86, Lemma 1.2] A necessary and sufficient condition for a valuation to satisfy the inequality* (3) *is when $C = 2$ in* **(3)**.

Proof. We prove the above by considering broader and broader cases, and expanding the argument from $|b| \leq 1$ to the general statement.

If the triangle inequality is true and $|a| \leq 1$, then $|1+a| \leq |1| + |a| \leq 2$.

Suppose **(3)** holds with $C = 2$. Consider $a_1, a_2 \in \daleth$ such that $|a_1| \geq |a_2|$. Then, without loss of generality, we have $a_2 = a \cdot a_1$ with $|a| \leq 1$. Hence

$$|a_1 + a_2| = |a_1 + aa_1| = |a_1||1+a| \leq 2|a_1| \iff |a_1+a_2| \leq 2\max\{|a_1|,|a_2|\}.$$

Similarly, without loss of generality, we can assume that for $a_1, a_2, a_3, a_4 \in \daleth$ we have $|a_1 + a_2| \geq |a_3 + a_4|$ and $|a_1| \geq |a_2|$. Then, for some $b \in \daleth$ with $|b| \leq 1$ we have $a_3 + a_4 = b(a_1 + a_2)$ and hence

$$|a_1+a_2+a_3+a_4| = |a_1+a_2+b(a_1+a_2)| = |a_1+a_2||1+b| \leq 2|a_1+a_2| \leq 2^2|a_1|$$

and hence $|a_1+a_2+a_3+a_4| \leq 2^2 \max\{|a_1|,|a_2|,|a_3|,|a_4|\}$. Repeating the process, we obtain

$$|a_1 + \cdots + a_{2^n}| \leq 2^n \max\{|a_i| : 1 \leq i \leq 2^n\} \text{ for } n \in \mathbb{Z}_+.$$

Next, consider an arbitrarily long sequence $a_1, \ldots, a_N \in \daleth$, and N such that

$$2^{n-1} < N \leq 2^n.$$

Let $a_{N+1} = \cdots = a_{2^n} = 0$, so that

$$\begin{aligned} |a_1 + \cdots + a_N + a_{N+1} + \cdots + a_{2^n}| = |a_1 + \cdots + a_N| &\leq 2^n \max|a_i| \\ &= 2 \cdot 2^{n-1} \max|a_i| \leq 2N \max|a_i| \end{aligned}$$

and observe, that letting $a_i = 1$ for all $1 \leq i \leq N$ we obtain $|N| \leq 2N$. (Note that this is far from the best we can do, although it is sufficient for our proof; improved version of this inequality can be found under the proof of 4.0.9.) Observe that we now have

$$|a_1 + \cdots + a_N| \leq 2N \max|a_i|. \quad (*)$$

Finally, let $b, c \in \daleth$ and $n \in \mathbb{Z}_+$. Then

$$|b+c|^n = |(b+c)^n| = \left|\sum_{r=0}^{n} \binom{n}{r} b^r c^{n-r}\right|,$$

where the sum has $n+1$ summands, thus referring to $(*)$ and letting $N = n+1$, we obtain

$$\left|\sum_{r=0}^{n} \binom{n}{r} b^r c^{n-r}\right| \overset{*}{\leq} 2(n+1) \max_r \left\{\left|\binom{n}{r} b^r c^{n-r}\right|\right\}.$$

Now, from $|N| \leq 2N$, we observe that

$$\left|\binom{n}{r}\right| \leq 2\binom{n}{r},$$

which then yields

$$2(n+1)\max_r\left\{\left|\binom{n}{r}b^r c^{n-r}\right|\right\} \leq 4(n+1)\max_r\left\{\binom{n}{r}|b|^r|c|^{n-r}\right\}.$$

Moreover, considering $\max_r\left\{\binom{n}{r}|b|^r|c|^{n-r}\right\}$ we have a single term for some r, and it is trivial to say that a sum including that term and multiple positive terms will be greater, i.e.

$$\max_r\left\{\binom{n}{r}|b|^r|c|^{n-r}\right\} \leq \sum_r\binom{n}{r}|b|^r|c|^{n-r},$$

which gives

$$4(n+1)\max_r\left\{\binom{n}{r}|b|^r|c|^{n-r}\right\} \leq 4(n+1)\sum_r\binom{n}{r}|b|^r|c|^{n-r} = 4(n+1)(|b|+|c|)^n.$$

Thus by taking the n'th root on both sides we obtain

$$|b+c|^n \leq 4(n+1)(|b|+|c|)^n \iff |b+c| \leq \sqrt[n]{4(n+1)}(|b|+|c|).$$

and by letting $n \longrightarrow \infty$, by the standard argument $\frac{1}{n}$ tends to zero faster than $4n+4$ goes to ∞, which yields

$$\lim_{n\to\infty}(4n+4)^{\frac{1}{n}} = 1.$$

Hence we finally have

$$|b+c| \leq |b|+|c|. \qquad \square$$

Next, we obtain the condition for the ultrametric inequality.

Lemma 3.2.2. *[Cas86] A valuation $|\cdot|$ on $\daleth$ is non-archimedian if and only if one can take $C = 1$ in* **(3)***.*

Proof. If $|b| \leq |a|$ then $|ba^{-1}| \leq 1$, and thus we can write that $|ba^{-1}+1| \leq 1$. That gives

$$|a+b||a^{-1}| \leq 1 \iff |a+b| \leq |a| = \max\{|a|,|b|\}.$$

On the other hand, if $C = 1$ in **(3)**, the definition reads

$$|b| \leq 1 \quad \longrightarrow \quad |1+b| \leq 1,$$

which can be rephrased as

$$|1+b| \leq \max\{|1|,|b|\},$$

which follows directly from definition. □

Since we have now introduced two types of absolute value functions and have shown that it is possible to merge their definitions together, it is worth continuing this idea to show the similarities between them. Therefore we establish some properties holding for both archimedian and non-archimedian absolute values.

Lemma 3.2.3. *[Gou65, Lemma 2.2.1] For any absolute value on a field $\daleth$ we have:*

1. *$|1| = 1$,*
2. *if $|x^n| = 1$, then $|x| = 1$,*
3. *$|-1| = 1$,*
4. *$|-x| = |x|$ for any $x \in \daleth$,*
5. *if $\daleth$ is a finite field, then $|\cdot|$ is trivial.*

Proof. Using the definition of the valuation, we have

(1) $|1| = |1 \cdot 1| = |1||1| \implies |1| = |1|^2$, so we have either $|1| = 1$ or $|1| = 0$, but since the second one contradicts the definition, we obtain $|1| = 1$;
(2) $|x^n| = |x \cdot x^{n-1}| = \cdots = |x|^n \implies |x|^n = 1$, which gives $|x| = 1$ or $|x| = -1$, but since the absolute value is positive by definition we have $|x| = 1$;
(3) $|1| = |(-1) \cdot (-1)| = |-1||-1| = |-1|^2 = 1$ so that $|-1| = -1$ or $|-1| = 1$, but by the same argument as above we have $|-1| = 1$;
(4) $|-x| = |-1||x| = 1 \cdot |x| = |x|$;
(5) suppose the contrary, i.e. for some finite field $\daleth$ there exists an element $0 \neq x \in \daleth$ such that $|x| = L \neq 0, 1$. Then since x needs to have a finite order, let the order equal to m, we have $x = x^{m+1}$ and from the definition $|x| = |x^{m+1}| = |x|^{m+1}$, which gives that
$$L = L^{m+1} \iff L(L^m - 1) = 0 \iff L = 0 \text{ or } L = 1,$$
which yields a contradiction. □

After drawing the connection between all the absolute value functions, we shall consider the main condition that would separate the archimedian absolute values from the non-archimedian ones. Recall that by the first definition introduced we have noted that the non-archimedian condition, referred to as $(3)^*$, was more strict than the archimedian one, denoted as condition (3). Now we give a condition that determines if the absolute value is non-archimedian.

Theorem 3.2.4. *[Gou65, Theorem 2.2.4] Let $A \subset \daleth$ be the image of $\mathbb{Z}$ in $\daleth$. An absolute value on $\daleth$ is non-archimedian if and only if*
$$|a| \leq 1 \text{ for all } a \in A.$$
In particular, an absolute value on $\mathbb{Q}$ is non-archimedian if and only if
$$|n| \leq 1 \text{ for all } n \in \mathbb{Z}.$$

Proof. ($\Longrightarrow$) If $|\cdot|$ is non-archimedian, we get
$$|2| = |1 + 1| \leq \max\{|1|, |1|\} = 1$$
and we repeat the argument by induction. Suppose $|a - 1| \leq 1$, then
$$|a| = |(a-1) + 1| \leq \max\{|a-1|, |1|\} = 1,$$
obtaining $|a| \leq 1$ for all $a \in A$, with a being the image of a positive integer. Symmetrically, if we let $\alpha = -a$, for $a > 0$, we can argue
$$|\alpha - 1| = |-a-1| = |-1||a+1| = |a+1| \leq \max\{|a|, 1\} = 1$$
and so
$$|\alpha| = |(\alpha - 1) + 1| \leq \max\{|\alpha - 1|, 1\} \leq \max\{1, 1\} = 1,$$
thus the statement holds for the negative integers.

($\Longleftarrow$) Suppose $|a| \leq 1$ for all $a \in A$, then we want to show that
$$|x + y| \leq \max\{|x|, |y|\} \text{ for all } x, y \in \daleth.$$
If $y = 0$ we have
$$|x| \leq \max\{|x|, 0\} = |x| \text{ since } |x| \geq 0.$$
Thus we multiply both sides by y^{-1}, assuming $y \neq 0$, and obtain the equivalent inequality
$$|xy^{-1} + 1| \leq \max\{|xy^{-1}|, |1|\},$$

so we only need to prove the inequality when one of the terms is 1.

We want to prove

$$|x+1| \leq \max\{|x|, 1\}.$$

Let $m \in \mathbb{Z}_+$, then

$$|x+1|^m = \left|\sum_{k=0}^{m} \binom{m}{k} x^k\right| \leq \sum_{k=0}^{m} \left|\binom{m}{k}\right| |x^k| \leq \sum_{k=0}^{m} |x^k| = \sum_{k=0}^{m} |x|^k,$$

since the valuation of $\binom{m}{k}$, an integer, is at most $|1|$.

Note:

- If $|x| \geq 1$, then $\max\{|x|^k : 0 \leq k \leq m\} = |x|^m$.
- If $|x| < 1$, $\max\{|x|^k : 0 \leq k \leq m\} = 1$.

Therefore we have

$$\sum_{k=0}^{m} |x|^k \leq (m+1)\max\{1, |x|^m\} \Longrightarrow |x+1| \leq \sqrt[m]{m+1}\ \max\{1, |x|\}.$$

It only remains to show that $\sqrt[m]{m+1} \longrightarrow 1$ as $m \longrightarrow \infty$. This holds since

$$\begin{aligned}\lim_{m\to\infty}(m+1)^{\frac{1}{m}} &= \lim_{m\to\infty}\left(e^{\ln(1+m)}\right)^{\frac{1}{m}} = \lim_{m\to\infty} e^{\frac{\ln(m+1)}{m}} \\ &= e^{(\lim_{m\to\infty}\frac{\ln(m+1)}{m})} = e^0 = 1,\end{aligned}$$

which finally yields

$$|x+1| \leq \max\{1, |x|\}. \qquad \square$$

The section will be concluded with the focus on the functions that are the most interesting for us, the p-adic absolute values. We have already given some properties of such, thus the last step will be to show that they actually define a function on $\mathbb{Q}_p$ together with its convergence for each prime p, using all the tools introduced in the chapter.

Let us focus on the p-adic expansion of an arbitrary element $X \in \mathbb{Q}_p$. Recall that by definition

$$x = \sum_{i \geq n_0} a_i p^i = a_{n_0}p^{n_0} + a_{n_0+1}p^{n_0+1} + \dots$$

for some sequence a_i with elements modulo p.

When dealing with such expansions, we are not always interested in all terms of the expansion, especially when the expansion is infinite. Although when dealing with such expansion we know that further terms "matter less", can we be sure that this will also be true for the p-adic expansion?

As it turns out, yes! To see it, let us consider an infinite p-adic expansion of X, $(a_{n_0}, a_{n_0+1}, \dots)$ and let us introduce the appropriate notation of each expansion:

$$\begin{aligned}x_1 &= a_{n_0}p^{n_0} \\ x_2 &= a_{n_0}p^{n_0} + a_{n_0+1}p^{n_0+1}\end{aligned}$$

and so on. Consider two such elements x_l and x_m, and without loss of generality say $l > m$. Now we obtain

$$\begin{aligned} x_l = \sum_{i \geq n_0}^{n_0+l-1} a_i p^i &= a_{n_0} p^{n_0} + a_{n_0+1} p^{n_0+1} + \cdots + a_{n_0+m-1} p^{n_0+m-1} \\ &+ a_{n_0+m} p^{n_0+m} + \cdots + a_{n_0+l-1} p^{n_0+l-1}, \\ x_m = \sum_{j \geq n_0}^{n_0+m-1} a_j p^j &= a_{n_0} p^{n_0} + a_{n_0+1} p^{n_0+1} + \cdots + a_{n_0+m-1} p^{n_0+m-1}, \end{aligned}$$

that we compare in terms of p-adic absolute value, just as we compare the distance between two elements in reals. Observe that

$$x_l - x_m = a_{n_0+m} p^{n_0+m} + \cdots + a_{n_0+l-1} p^{n_0+l-1}.$$

Indeed, let $r \geq 1$ such that $a_{n_0+m} = a_{n_0+m+1} = \cdots = a_{n_0+m+r-1} = 0$, and $a_{n_0+m+r} \neq 0$. Then

$$\begin{aligned} |x_l - x_m|_p &= |a_{n_0+m} p^{n_0+m} + \cdots + a_{n_0+l-1} p^{n_0+l-1}|_p \\ &= |a_{n_0+m+r} p^{n_0+m+r} + \cdots + a_{n_0+l-1} p^{n_0+l-1}|_p \\ &= |p^{n_0+m+r}(a_{n_0+m+r} + a_{n_0+m+r+1} p + \cdots + a_{n_0+l-1} p^{l-m-r-1})|_p \\ &= |p^{n_0+m+r}|_p |a_{n_0+m+r} + a_{n_0+m+r+1} p + \cdots + a_{n_0+l-1} p^{l-m-r-1}|_p \\ &= p^{-(n_0+m+r)} \cdot 1 = \frac{1}{p^{n_0+m+r}}, \end{aligned}$$

that tends to zero as m tends to infinity, which shows that the expansions really are relatively close to each other.

The above consideration naturally points toward the notion of the Cauchy sequence.

Definition 3.2.5. A sequence of elements $x_n \in \rceil$ is called a *Cauchy sequence* if, for every $\epsilon > 0$, one can find a bound M such that $|x_n - x_m| < \epsilon$ whenever $m, n \geq M$. Moreover, for a p-adic number

$$x = \sum_{i \geq n_0} a_i p^i$$

the x_n defined above is a *Cauchy representation of* x.

Finally, after introducing the notion of the Cauchy sequence and its interpretation in the p-adics, we consider the fundamental connection between the set and p-adic absolute value.

Definition 3.2.6. [Che18, Definition 1.14] For $X \in \mathbb{Q}_p$, we define

$$|X|_p : \mathbb{Q}_p \longmapsto [0, \infty) \quad \text{by} \quad |X|_p = \lim_{n \to \infty} |x_n|_p,$$

where $(x_n)_{n=1}^{\infty}$ is a Cauchy sequence representation of X.

We shall check if the definition satisfies all required properties of the absolute value.

(1) $|X|_p = 0 \iff X = 0$: Let $|X|_p = 0$, then $\lim_{n\to\infty} |x_n|_p = 0$. Since x_n is a sum of n positive numbers (see expressions for x_l and x_m above), all of them have to be equal to 0, which yields $X = 0$. On the other hand, if $X = 0$, then $|X|_p = 0$

holds trivially.

(2) $|XY|_p = |X|_p|Y|_p$: This follows directly from definition

$$|XY|_p = \lim_{n\to\infty} |x_n \cdot y_n|_p = \lim_{n\to\infty} |x_n|_p \cdot \lim_{n\to\infty} |y_n|_p = |X|_p|Y|_p.$$

(3) $|X+Y|_p \leq |X|_p + |Y|_p$: Similarly, we follow the definition and the property of the limits

$$|X+Y|_p = \lim_{n\to\infty} |x_n + y_n|_p \leq \lim_{n\to\infty} |x_n|_p + \lim_{n\to\infty} |y_n|_p = |X|_p + |Y|_p.$$

Note that in the similar fashion one can show that the ultrametric inequality holds as well, using the established properties of $|\cdot|_p$ function.

Proposition 3.2.7. *[Che18, Proposition 1.15] The absolute value $|\cdot|_p$ is well defined on the field $\mathbb{Q}_p$.*

Proof. Since all elements of $\mathbb{Q}_p$ have their representation as a Cauchy sequence by Definition 3.2.6, in order to show the absolute value on the field $\mathbb{Q}_p$ is well defined, we show that for $X = (x_n) \in \mathbb{Q}_p$ the limit $\lim_{n\to\infty} |x_n|_p$ exists and is unique.
(Existence) Here, we only need to show that the limit introduced in the Definition 3.2.6 is convergent. Using the calculation from the page before, we show that

$$||x_l|_p - |x_m|_p|_p = \frac{1}{p^{n_0+m+r}}$$

follows from analogical reasoning:

$$\begin{aligned}
||x_l|_p - |x_m|_p|_p &= ||a_{n_0}p^{n_0} + a_{n_0+1}p^{n_0+1} + \cdots + a_{n_0+m-1}p^{n_0+m-1}|_p \\
&- |a_{n_0}p^{n_0} + a_{n_0+1}p^{n_0+1} + \cdots + a_{n_0+m-1}p^{n_0+m-1}|_p|_p \\
&\leq ||a_{n_0}p^{n_0}|_p + |a_{n_0+1}p^{n_0+1}|_p + |\ldots|_p + |a_{n_0+m-1}p^{n_0+m-1}|_p \\
&- |a_{n_0}p^{n_0} + a_{n_0+1}p^{n_0+1}|_p - |\ldots|_p - |a_{n_0+m-1}p^{n_0+m-1}|_p|_p \\
&= ||a_{n_0+m+r}p^{n_0+m+r}|_p + |\ldots|_p + |a_{n_0+l-1}p^{n_0+l-1}|_p|_p \\
&= ||p^{n_0+m+r}|_p|(a_{n_0+m+r} + a_{n_0+m+r+1}p + \cdots + a_{n_0+l-1}p^{l-m-r-1})|_p|_p \\
&= |p^{n_0+m+r}|_p|a_{n_0+m+r} + a_{n_0+m+r+1}p + \cdots + a_{n_0+l-1}p^{l-m-r-1}|_p \\
&= p^{-(n_0+m+r)} \cdot 1 = \frac{1}{p^{n_0+m+r}},
\end{aligned}$$

Therefore for n_0 being multiplicity and $r \geq 1$ such that $a_{n_0+m} = a_{n_0+m+1} = \cdots = a_{n_0+m+r-1} = 0$, and $a_{n_0+m+r} \neq 0$, we obtain

$$\forall \epsilon > 0,\ \exists\, l, m > N \ \text{ such that } \ ||x_l|_p - |x_m|_p|_p < \epsilon,$$

and thus the function is convergent.
(Uniqueness) To prove the representation is unique, we let (y_n) be a different Cauchy sequence representation of the same element. Then

$$\lim |y_n|_p \leq \lim |y_n - x_n|_p + \lim |x_n|_p = \lim |x_n|_p$$

by the ultrametric property, and the fact that as (x_n) and (y_n) both represent X we have

$$\begin{aligned}
\lim_{n\to\infty} |y_n - x_n|_p &= \lim_{n\to\infty} |y_n - X + X - x_n|_p \\
&\leq \lim_{n\to\infty} |y_n - X|_p + \lim_{n\to\infty} |X - x_n|_p = 0 + 0 = 0
\end{aligned}$$

so $\lim_{n\to\infty}|y_n - x_n|_p = 0$. Symmetrically we obtain

$$\lim|x_n|_p \leq \lim|x_n - y_n|_p + \lim|y_n|_p = \lim|y_n|_p$$

which implies $\lim|x_n|_p = \lim|y_n|_p$. □

3.3. **Introduction to the metric spaces.** As we have already discussed the similarities between various notions on $\mathbb{R}$ and $\mathbb{Q}_p$, such as valuations, we shall remind ourselves of the differences underlying in these structures.
We begin by introducing the main phrase, that will allow us to discuss the sets (including fields) together with the metric functions derived in detail in the chapter.

Definition 3.3.1. [Sut09, p.37] The *metric space* is a set X together with the notion of a distance between its elements. The distance is measured by a function called a *metric* or a *distance function*

$$d: \; X \times X \longmapsto \mathbb{R}.$$

It has to satisfy following properties, for $x, y, z \in X$:

(1) $d(x, y) \geq 0$,
(2) $d(x, y) = 0 \iff x = y$,
(3) $d(x, y) = d(y, x)$,
(4) $d(x, z) \leq d(x, y) + d(y, z)$.

An obvious choice, as we have considered absolute values before, would be to define the notion of the distance in the broad meaning of valuations.

Definition 3.3.2. [Gou65, Definition 2.3.1] Let $\daleth$ be a field and $|\cdot|$ an absolute value on $\daleth$. We define the *distance* $d(x, y)$ between two elements $x, y \in \daleth$ by $d(x, y) = |x - y|$.
We call $d(x, y)$ a *metric induced by the absolute value.*

Indeed, one can verify this directly with the use of Definition 3.1.1.

(1) Consider $\alpha = x - y$, then we want to show that any $|\alpha| \geq 0$. We have $|-\alpha| = |-1||\alpha| = |\alpha|$, and we assume the contrary: we have α such that $|\alpha| < 0$ and thus also $|-\alpha| < 0$. But then

$$|0| = |\alpha + (-\alpha)| \leq |\alpha| + |-\alpha| = 2|\alpha| < 0,$$

which yields contradiction.
(2) $d(x, y) = |x - y| = 0 \iff x - y = 0 \iff x = y$.
(3) $d(x, y) = |x - y| = |-(y - x)| = |y - x| = d(y, x)$.
(4) $d(x, z) = |x - z| = |(x - y) + (y - z)| \leq |x - y| + |y - z| = d(x, y) + d(y, z)$.

Example 3.3.3. The set $\mathbb{R}$ together with the infinite absolute value (or the usual absolute value $|\cdot|$) comprise a real metric space.

Let us now make a two small remarks in connection to what we have introduced by now.

$\mathbb{R}$ is an "ordered field", i.e. it has a well-defined order of the elements and thus notions of bigger-than and less-than; this is not the case for $\mathbb{Q}_p$.

The infinite absolute value on $\mathbb{R}$ is archimedian; all p-adic absolute values on $\mathbb{Q}_p$ are non-archimedian - compare with Proposition 3.3.5.

The metric induced by the absolute value can be used in surprisingly broad contexts. It not only gives us basic intuition to the geometry, but can be also a useful tool in proving some results in arithmetic, seemingly not related to the metric in a field $\daleth$.

Since the introduction of the valuation was motivated by redefining the notion of distance in the p-adic sense, and we know already that all the p-adic valuations are non-archimedian, we limit our focus to the distances in the non-archimedian cases. We should remember though, that the distance functions have no reasonable geometrical sense - both with respect to the non-archimedian absolute value, and to the p-adic absolute value, which we will show soon with the use of some basic topology.

The following step for understanding the metric function in connection to the valuation is rather intuitive, and follows from our previous reasonings.

Lemma 3.3.4. *[Gou65, Lemma 2.3.3] Let $|\cdot|$ be an absolute value on a field $\daleth$, and define the metric as $d(x, y) = |x-y|$ for $x, y \in \daleth$. Then $|\cdot|$ is non-archimedian if and only if for all $x, y, z \in \daleth$ we have*

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

Proof. ($\Longrightarrow$) We have

$$|x-y| = |(x-z)+(z-y)| \leq \max\{|x-z|, |z-y|\} = \max\{d(x, z), d(z, y)\}.$$

($\Longleftarrow$) We have $d(x, y) \leq \max\{d(x, z), d(z, y)\}$. Consider $y = -y'$, then

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

By the assumption and the property $d(a, b) = d(-a, b)$, we have

$$|x+y'| \leq \max\{d(x, z), d(z, y)\} = \max\{d(x, z), d(z, y')\}.$$

Now take $z = 0$, so that

$$|x+y'| \leq \max\{|x-0|, |0-y'|\} = \max\{|x|, |y'|\}. \qquad \square$$

Analogous to the absolute value definition, we shall mention the condition distinguishing the archimedian and non-archimedian distance.

Proposition 3.3.5. *[Gou65, Proposition 2.3.4] Let $\daleth$ be a field and let $|\cdot|$ be a non-archimedian absolute value on $\daleth$. If $x, y \in \daleth$ and $|x| \neq |y|$, then $|x+y| = \max\{|x|, |y|\}$.*

Proof. By symmetry, without loss of generality, suppose that $|x| \geq |y|$. Then

$$|x+y| \leq \max\{|x|, |y|\} = |x|.$$

On the other hand,

$$|x| = |(x+y)-y| \leq \max\{|x+y|, |y|\}.$$

If we take $\max\{|x+y|, |y|\} = |y|$ we obtain contradiction, thus we need to have $\max\{|x+y|, |y|\} = |x+y|$ and therefore $|x| = |x+y|$. $\square$

This result is rather surprising. In terms of distances, we obtain that the sum of any two vectors is equal to one of the vectors being summed. In the non-archimedian setting, we can therefore develop a small result on how the geometrical consequences can be expressed.

Corollary 3.3.6. *[Gou65, Corollary 2.3.5] In a space with on non-archimedian absolute value, all triangles are isosceles.*

Proof. Let $x, y, z \in \mathbb{Q}_p$. We certainly have $(x-y)+(y-z) = x-z$. If $|x-y| = |y-z|$, we are done. Otherwise, given $|x-y| \neq |y-z|$, by Proposition 3.3.10 we have

$$|x-z| = \max\{|x-y|, |y-z|\}. \qquad \square$$

The analogous properties hold for the p-adic absolute values, as all of them are non-archimedian. To shortly illustrate how the distance behaves in the p-adic setting, consider $x = p^n x', y = p^m y'$ with $p \nmid x', y'$ and corresponding p-adic absolute values $|x|_p = p^{-n}$, $|y|_p = p^{-m}$. Moreover, suppose $|x|_p \neq |y|_p$. Then, without loss of generality suppose $|x|_p < |y|_p$. Then it implies we have $n > m$ and let $n = m + \epsilon$. Therefore

$$x + y = p^n x' + p^m y' = p^{m+\epsilon} x' + p^m y' = p^m (p^\epsilon x' + y')$$

with $p \nmid (p^\epsilon x' + y')$. Thus

$$|x+y|_p = p^{-m} = |y|_p.$$

Finally, we complete the notion of space by examining the construction of balls in the p-adic setting. For the purpose of the following section, we introduce some of the basic notions used later in the text.

Definition 3.3.7. Let X be a metric space with distance function d. We call $B(a,r) \in X$ an *open ball* centered at a with radius r, i.e. the set of all points of distance less than r from a. We write

$$x \in B(a,r) \iff d(x,a) < r.$$

Similarly, a *closed ball* is centered at a with radius r, i.e. the set of all points of distance less than or equal to r from a. We write

$$x \in \bar{B}(a,r) \iff d(x,a) \leq r.$$

Moreover, an open ball $B_p(a,r)$ is a *p-adic (open) ball* when it is defined according to the p-adic absolute value, i.e. the set of all points of distance less than or equal to r from a defined by the p-adic absolute value. We write

$$x \in B_p(a,r) \iff |x-a|_p < r.$$

For the purpose of the following section, we only consider open p-adic balls, although the reader should be aware that closed p-adic balls also exist.

Furthermore, a few rather surprising properties of the p-adic balls are given and explored in detail in the proofs.

Proposition 3.3.8. *[Gou65, Proposition 2.3.7] Let $\daleth$ be a field with a non-archimedian absolute value.*

1. *If b belongs to the ball with a center a and a radius r, i.e. $b \in B(a,r)$, then $B(a,r) = B(b,r)$, i.e. every point contained in the ball is also its center.*
2. *The set $B(a,r)$ is both open and closed.*
3. *Any two open balls are either disjoint or contained in one another.*

Proof. (1) By definition, we have $b \in B(a,r)$ if $|b-a| < r$. Now, taking any x such that $|x-a| < r$, we get

$$|x-b| = |x-a+a-b| \leq \max\{|x-a|, |b-a|\} < r$$
$$\implies x \in B(b,r) \implies B(a,r) \subseteq B(b,r).$$

Repeating the argument symmetrically we obtain

$$B(b,r) \subseteq B(a,r) \implies B(b,r) = B(a,r).$$

(2) Consider x on the boundary of the open ball $B(a,r)$, then any open ball centered at x contains points from $B(a,r)$. Take $s < r$, then there exists $y \in \daleth$ such that $y \in B(a,r) \cap B(x,s)$ and hence

$$\begin{cases} |y-a| < r, \\ |y-x| < s \leq r. \end{cases}$$

Now we have the following implication:

$$\begin{aligned} |x-a| \leq \max\{|x-y|, |y-a|\} \leq \max\{s,r\} = r \implies |x-a| \leq r \\ \iff x \in B(a,r), \end{aligned}$$

which shows that any boundary point of $B(a,r)$ belongs to that ball.
(3) Suppose $s \leq r$. For arbitrary centers a and b, we have either

$$B(a,r) \cap B(b,s) = \emptyset \text{ or } \exists\, c \in B(a,r) \cap B(b,s).$$

Then, in the latter, using (1),

$$\begin{cases} B(a,r) = B(c,r) \\ B(b,s) = B(c,s) \end{cases} \implies B(c,s) = B(b,s) \subseteq B(a,r) = B(c,r). \qquad \square$$

The geometrical understanding of the p-adic valuations is the fundamental consideration to have before beginning to discuss the p-adic topology. Although we should note that some of the above considerations will not influence the upcoming content, and was presented for interest and to show the reader how little we have changed, and how greatly it has impacted some basic properties of space.

After introducing the basic properties of some of the objects in the non-archimedian setting, the focus in the next chapter will shift to the construction of the entire set of the absolute value functions, their properties and connections between each other.

4. The p-adic topology

Subsequent to giving the basic properties of the absolute value functions and distinguishing the two different types of them, we shall move on to more details about their topological meaning. The main reason for the consideration of the valuations in this thesis about p-adic numbers in the first place was to redefine the "usual" topology in the p-adic setting by drawing the connection with the p-adic distance function.

This chapter will therefore tell more about the different topological concepts and finally introduce the connection between the p-adics and cardinality of non-archimedian absolute functions. Therefore we begin by introducing what equivalent topology means, and we consider which properties it satisfies.

Let us start with defining the p-adic space with respect to the topology.

Definition 4.0.1. [Sut09, Definition 7.1] Let X be a set and τ be a family of subsets of X. Then τ is called a *topology* of X if:

- Both the empty set and X are elements of τ.
- Any union of elements of τ is also an element of τ.
- Any intersection of finitely many elements of τ is also an element of τ.

Every element of τ is called an *open set.*

Example 4.0.2. Let $X = \mathbb{R}$ and τ be the set of arbitrary unions of half-open intervals $[a, b)$, for $a < b$. Then the union of no intervals gives the empty set, and the union of all intervals gives the whole set, thus $\emptyset, \mathbb{R} \in \tau$. It is clear that for any arbitrary $\tau_1, \tau_2 \in \tau$ their union and intersection also belong to τ by basic interval properties. Therefore τ gives a topology on the set $\mathbb{R}$.

Proposition 4.0.3. *The field $\mathbb{Q}_p$ is a topological space with topology τ given by the set of arbitrary unions of the p-adic open balls.*

Proof. Similarly as in the above example, the union of no balls gives the empty set, while the union of all balls gives the entire set, therefore $\emptyset, \mathbb{Q}_p \in \tau$.

Consider an arbitrary union and intersection of two sets of such balls. Note that by Proposition 3.3.8 we have that two balls are either disjoint or contained in one another.

Let $B(a, r_1)$ and $B(b, r_2)$ be two arbitrary p-adic balls in τ. If $B(a, r_1) \subseteq B(b, r_2)$, the result is trivial as their intersection is just $B(a, r_1)$, and their union is $B(b, r_2)$, therefore both intersection and union are in τ. In the case when they are disjoint, both union and intersection (which is the empty set) are still some arbitrary unions of p-adic balls, thus τ is a topology. □

Definition 4.0.4. [Gou65, Definition 3.1.1] The absolute values $| \cdot |_1$ and $| \cdot |_2$ on a field $\daleth$ are *equivalent* if they define the same topology on $\daleth$, i.e. every set that is open with respect to one of them is also open with respect to the other.

Example 4.0.5. Consider two topologies on the real line. Let τ_0 be the topology generated by the arbitrary unions of open intervals (a, b) where $a < b$, and τ_1 be the topology generated by the arbitrary unions of half-open intervals $[a, b)$ where $a < b$. Then every nonempty set in τ_0 contains a nonempty set in τ_1 and vice versa, thus τ_0 and τ_1 are equivalent.

Proposition 4.0.6. *[Gou65, Proposition 3.1.3] The following statements are equivalent.*

(1) $|\cdot|_1$ *and* $|\cdot|_2$ *are equivalent,*
(2) *for any* $x \in \daleth$ *we have*

$$|x|_1 < 1 \iff |x|_2 < 1,$$

(3) $\exists\, \alpha \in \mathbb{R}_+$ *such that for all* $x \in \daleth$ *we have* $|x|_1 = |x|_2^\alpha$.

Proof. The statements will be proven in the circular order: first that (1) implies (2), then that (2) implies (3) and finally (3) implies (1).

(1) $\implies$ (2). If any sequence converges with respect to $|\cdot|_1$, then it also converges with respect to $|\cdot|_2$. Given $x \in \daleth$, if $|x|_1 < 1$ then

$$\lim_{n\to\infty} |x^n|_1 = \lim_{n\to\infty} |x|_1^n = 0.$$

Hence we have

$$\lim_{n\to\infty} |x|_2^n = 0,$$

which gives $|x|_2 < 1$. The reverse implication follows symmetrically.

(2) $\implies$ (3). Choose $x_0 \in \daleth$ so that $|x_0|_1 < 1$, equivalently $|x_0|_2 < 1$. Let $\alpha \in \mathbb{R}$ be such that

$$|x_0|_1 = |x_0|_2^\alpha,$$

and taking logarithms on both sides and simplifying we obtain

$$\log|x_0|_1 = \alpha \log|x_0|_2 \iff \alpha = \frac{\log|x_0|_1}{\log|x_0|_2}.$$

Note that $\log|x_0|_1 < 0$ and $\log|x_0|_2 < 0$.

Consider any other $x \in \daleth$, $x \neq 0$. Then there is some β such that

$$|x|_1 = |x|_2^\beta \iff \beta = \frac{\log|x|_1}{\log|x|_2}.$$

Now our aim is to show that $\alpha = \beta$.

If $|x|_1 = |x_0|_1$, then $|\frac{x}{x_0}|_1 = 1$. By (2) we have $|\frac{x}{x_0}|_2 \geq 1$. Also $|\frac{x_0}{x}|_1 = 1$ implies $|\frac{x_0}{x}|_2 \geq 1$. Equivalently, we have

$$|x|_2 \geq |x_0|_2$$
$$|x_0|_2 \geq |x|_2$$

and thus $|x|_2 = |x_0|_2$. Putting this together, we obtain

$$\alpha = \frac{\log|x_0|_1}{\log|x_0|_2} = \frac{\log|x|_1}{\log|x|_2} = \beta.$$

If $|x|_1 = 1$, then $|x|_2 \geq 1$ by (2). Then we have $|\frac{1}{x}|_2 \leq 1$. If we would have $|\frac{1}{x}|_2 < 1$, then $|\frac{1}{x}|_1 < 1$ and $|x|_2 > 1$, which gives $|x|_1 > 1$, contradiction. Therefore $|x|_2 = |x|_1 = 1$ and we can pick $\alpha = \beta$.

Thus the only case remaining for us to consider is $|x|_i \neq 1$ and $|x|_i \neq |x_0|_i$ for $i = 1, 2$. We can safely assume $|x|_1 < 1$, equivalently $|x|_2 < 1$, as the case $|x|_1 > 1$ will follow by the argument applied to $|\frac{1}{x}|_1 < 1$.

Let $m, n \in \mathbb{N}$. Then

$$|x|_1^n < |x_0|_1^m \iff \left|\frac{x^n}{x_0^m}\right|_1 < 1 \iff \left|\frac{x^n}{x_0^m}\right|_2 < 1 \iff |x|_2^n < |x_0|_2^m$$

and taking logarithm on both sides yields

$$n \log |x|_1 < m \log |x_0|_1 \iff n \log |x|_2 < m \log |x_0|_2$$
$$\frac{n}{m} > \frac{\log |x_0|_1}{\log |x|_1} \iff \frac{n}{m} > \frac{\log |x_0|_2}{\log |x|_2};$$

recall that by assumption $\log |x|_1 < 0$ and hence $\log |x|_2 < 0$. Now, let us justify why this means that the two logarithmic fractions are equal. Indeed, suppose that

$$\frac{\log |x_0|_1}{\log |x|_1} > \frac{\log |x_0|_2}{\log |x|_2}.$$

So we can find positive integers m, m', n, n' such that

$$\frac{n}{m} > \frac{\log |x_0|_1}{\log |x|_1} \quad \text{and} \quad \frac{\log |x_0|_1}{\log |x|_1} \geq \frac{n'}{m'} > \frac{\log |x_0|_2}{\log |x|_2}.$$

However, then

$$\frac{n'}{m'} > \frac{\log |x_0|_2}{\log |x|_2} \quad \text{but} \quad \frac{n'}{m'} \not> \frac{\log |x_0|_1}{\log |x|_1},$$

a contradiction. Symmetrically, we obtain

$$\frac{\log |x_0|_1}{\log |x|_1} = \frac{\log |x_0|_2}{\log |x|_2}.$$

If we were to consider the case when $|x_0|_1 > 1$, equivalently $|x_0|_2 > 1$, it is trivial to see that $\frac{1}{|x_0|_1} < 1$, equivalently $\frac{1}{|x_0|_2} < 1$, so we can choose $x_0' = \frac{1}{x_0}$, and proceed as before. For the case where $|x_0|_1 = 1$, we have that $|x_0|_2 = 1$. Indeed, if $|x_0|_2 < 1$, then by (2) we have $|x_0|_1 < 1$, a contradiction. If $|x_0|_2 > 1$ we have $|\frac{1}{x_0}|_2 < 1$ and again by (2) we have $|\frac{1}{x_0}|_1 < 1$, which is not true since $|x_0|_1 = |\frac{1}{x_0}|_1 = 1$. Therefore we have $|x_0|_1 = |x_0|_2 = 1$, and clearly we can take $\beta = \alpha$.

(3) $\implies$ (1). For $x \in B(a, r)$, we have

$$|x - a|_1 < r \iff |x - a|_2^\alpha < r \iff |x - a|_2 < r^{\frac{1}{\alpha}},$$

and both are open balls, which by definition implies they are equivalent. □

As of now the various properties of the absolute values with connection to the p-adics have been introduced, and therefore we narrow down our considerations to how many of them actually exist, i.e. if there is a chance that they might align for different primes p and q.

Corollary 4.0.7. *If p, q are different primes, then p-adic and q-adic absolute values are not equivalent.*

Proof. Consider $x \in$ ⅂ such that

$$x = p^n q^m x' \implies \begin{cases} |x|_p = p^{-n} \\ |x|_q = q^{-m}, \end{cases}$$

with $p \nmid x'$ and $q \nmid x'$, and m, n being the maximum powers of p and q in x, respectively. Since $\gcd(p, q) = 1$, we know that there exists no $\alpha \in \mathbb{R}_+$ such that $|x|_p^\alpha = |x|_q$ since $p^{-n\alpha} \neq q^{-m}$ are still coprime and cannot be equal. □

Finally, we connect the above theory with the cardinality of the set of absolute value functions. The following theorem describes the relation between the

p-adic valuations and the entire set of the absolute values, and proves that the non-archimedian absolute value function on $\mathbb{Q}$ defines exactly the set of p-adic absolute values.

Theorem 4.0.8 (Ostrowski's Theorem)**.** *[Gou65, Theorem 3.1.4] Over $\mathbb{Q}$, every non-trivial absolute value is equivalent either to the p-adic absolute value, or to the usual absolute value (referred to as "infinite absolute value").*

Proving the theorem is quite a challenging task, hence we divide it into two steps: introducing the estimation lemma and using it to prove Ostrowski's Theorem.

Lemma 4.0.9. *[pla13] If $m, n > 1$ are integers and $|\cdot|$ is any non-trivial absolute value on $\mathbb{Q}$, then*

$$|m| \leq \max\{1, |n|\}^{\frac{\log(m)}{\log(n)}}.$$

Proof. If $m = n$, then the result is clear, since $\log m = \log n$, and $|m| = |n|$. Otherwise suppose that $m \neq n$. Then we consider m to be a composition in the n-adic meaning (similar to the p-adic, but with less remarkable properties), so that we have

$$m = a_0 + a_1 n + \cdots + a_r n^r \text{ for some } (a_i)_{i=1}^{r} \in \mathbb{Z}_n, \quad 0 \leq a_i \leq n-1, \quad a_r \neq 0.$$

Then, by the triangle inequality, we get

$$|a_i| = |1 + \cdots + 1| \leq a_i|1| = a_i \leq n - 1 \implies |a_i| \leq n.$$

Also,

$$n^r \leq m \iff r\log(n) \leq \log(m) \iff r \leq \frac{\log(m)}{\log(n)}.$$

Summing up all of the above, we have $r+1$ summands, we bound each $|a_i|$ with n, and since

- $|n| > 1 \implies \max\{1, |n|, \ldots,\ |n|^r\} = |n|^r$,
- $|n| \leq 1 \implies \max\{1, |n|, \ldots,\ |n|^r\} = 1$,

this gives us

$$|m| = |a_0 + a_1 n + \cdots + a_r n^r| \leq |a_0| + |a_1||n| + \cdots + |a_r||n^r|.$$

Thus we have $(r+1)$ expressions of form $|a_i||n^i| = |a_i||n|^i$, where from above we know $|a_i| \leq n$ and $|n^i| \leq \max\{1, |n|^r\} = \max\{1, |n|\}^r$. Replacing r with the bound obtained above we get

$$|m| \leq \left(1 + \frac{\log(m)}{\log(n)}\right) n \cdot \max\{1, |n|\}^r.$$

Now the trick is to replace m by m_0^t for $t \in \mathbb{Z}$, and take the t'th root, resulting in

$$\begin{aligned}
|m_0^t| &\leq \left(1 + \frac{\log(m_0^t)}{\log(n)}\right) n \cdot \max\{1, |n|\}^{\frac{\log(m_0^t)}{\log(n)}} \\
&= \left(1 + \frac{t\log(m_0)}{\log(n)}\right) n \cdot \max\{1, |n|\}^{\frac{t\log(m_0)}{\log(n)}} \\
\implies |m_0| &\leq \left(1 + \frac{t\log(m_0)}{\log(n)}\right)^{1/t} n^{1/t} \cdot \max\{1, |n|\}^{\frac{\log(m_0)}{\log(n)}}
\end{aligned}$$

and as $t \longrightarrow \infty$ we have $\lim_{t\to\infty} n^{1/t} = 1$ and

$$\lim_{t\to\infty}\left(1+\frac{\log(m_0)}{\log(n)}t\right)^{1/t} = \lim_{t\to\infty}(1+at)^{1/t} = \lim_{u\to 0}\left(1+\frac{a}{u}\right)^{u},$$

for constant a, so consider logarithm of the limit. By the continuity

$$\log\lim_{u\to 0}\left(1+\frac{a}{u}\right)^{u} = \lim_{u\to 0}\log\left(1+\frac{a}{u}\right)^{u} = \lim_{u\to 0} u\log\left(1+\frac{a}{u}\right) = 0\cdot\log(1) = 0,$$

and since $e^0 = 1$, we have that the entire limit is 1, which proves the lemma. □

Proof of Ostrowski's Theorem. Case 1. Suppose that for all $n > 1$ we have $|n| > 1$. Then by the Estimation Lemma we have

$$|m| \leq |n|^{\frac{\log(m)}{\log(n)}} \iff |m|^{\frac{1}{\log(m)}} \leq |n|^{\frac{1}{\log(n)}}$$

for all $m, n > 1$. By switching places for m and n we get the reverse, thus $|m|^{\frac{1}{\log(m)}}$ is constant for every element in the set. Therefore we have

$$|m|^{\frac{1}{\log(m)}} = c \iff |m| = c^{\log(m)}$$

which is equivalent to $|m|_\infty = e^{\log(m)}$.

Case 2. If instead for some $n > 1$ we have $|n| < 1$, then the Estimation Lemma gives $|m| \leq 1$ and by Theorem 3.2.4, the absolute value is non-archimedian. We define the region of interest as the ring of $A = \{x \in \mathbb{Q} : |x| \leq 1\}$ where the maximal ideal (an ideal such that there is no other ideal contained between the ring and the maximal ideal) is $A_M = \{x \in \mathbb{Q} : |x| < 1\}$.

Considering the valuation on $\mathbb{Z}$, we notice that

$$|n| \leq 1 \ \ \forall n \in \mathbb{Z} \implies \mathbb{Z} \subseteq A \ \text{ and } \ \mathbb{Z} \cap A_M \neq \emptyset$$

(since then the valuation would be trivial). Note that we have $\mathbb{Z} \cap A_M = p\mathbb{Z}$ for some prime p; that is since A_M contains elements divisible by p at least once, and its intersection with integers give integers divisible by p at least once, or integers times p. For any element $a \in \mathbb{Z}$ such that $p \nmid a$ we have

$$|a| = 1 \implies a \in A - A_M.$$

So for $x = \frac{p^t a}{b}$, where $p \nmid a, b$,

$$|x| = \left|\frac{p^t a}{b}\right| = |p^t|\frac{|a|}{|b|} = |p|^t$$

which gives a valuation equivalent to the p-adic valuation. □

The theorem summarises our discourse about the absolute value functions, and begins the discussion about the topology induced by their properties. We have made a proper connection between the p-adic numbers and non-archimedian valuations, therefore the next chapter will go in detail into the properties implied by their behaviour.

5. Hensel's Lemma

After exploring the field of $\mathbb{Q}_p$, Hensel moved on to formulating probably one of the most significant results in number theory. Using the structure provided by the Cauchy sequences, he proposed an algorithm for finding solutions of equations modulo p^n.

Assuming that consecutive solutions, as we increase n, will follow the scheme of a Cauchy sequence, we can construct the idea of how to obtain the solutions. In order to introduce the reader to that concept, we first introduce a definition used in a single step in that algorithm, that of a lift.

Definition 5.0.1. [Che18, Definition 3.1] Let $f(X)$ be a polynomial with integer coefficients and let p be a prime. Suppose there exists a solution to $f(x_1) \equiv 0 \pmod{p}$. Then a solution x_n to

$$f(x_n) \equiv 0 \pmod{p^n} \text{ where } x_n \equiv x_1 \pmod{p}$$

is called a *lift* of $x_1 \pmod{p^n}$ for some given $n > 0$.

Example 5.0.2. [Che18, Example 3.2] Consider $f(X) = X^2 + 1$. We can see that $f(2) \equiv 0 \pmod{5}$, and we have

$$x_1 \equiv 2 \pmod{5} \iff x = 5t + 2 \text{ for some } t \in \mathbb{Z}.$$

We find a lift by trial-and-error that $t = 1$ is a solution to:

$$(5t + 2)^2 + 1 \equiv 0 \pmod{25},$$

which gives $x_2 = 7$. We also have $f(3) \equiv 0 \pmod{5}$, so we could take $x_1 = 3$. Writing $x_2 = 5t + 3$ we see that $t = 3$ is a solution to

$$(5t + 3)^2 + 1 \equiv 0 \pmod{25},$$

thus $x_2 = 18$.

Following this introduction of what will be a single step in the algorithm, we now have all the tools to introduce Hensel's Lemma in its entirety.

Lemma 5.0.3 (Hensel's Lemma)**.** *[Gou65, Theorem 6.5.2] Let*

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$$

be a non-zero polynomial with coefficients being p-adic digits. Suppose there exists a p-adic integer $\alpha_1 \in \mathbb{Z}_p$ such that

$$f(\alpha_1) \equiv 0 \pmod{p} \text{ and } f'(\alpha_1) \not\equiv 0 \pmod{p}.$$

Then there exists a unique p-adic integer $\alpha \in \mathbb{Z}_p$ such that

$$\alpha \equiv \alpha_1 \pmod{p} \text{ and } f(\alpha) = 0.$$

The next lemma is an equivalent formulation of Hensel's Lemma.

Lemma 5.0.4 (Hensel's Lemma, alternative formulation)**.** *[Gou65, Theorem 6.5.2] Consider a non-zero polynomial $f(X) \in \mathbb{Z}[X]$ and suppose*

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

for some $a \in \mathbb{Z}$ and p prime. Then we have solutions modulo p^{n+1} for all $n \geq 0$:

$$f(a_n) \equiv 0 \pmod{p^{n+1}} \text{ such that } a_{n+1} \equiv a_n \pmod{p^{n+1}}.$$

In other words, we obtain sequences $(a_0, a_1, \dots)$ as a solution. Each element of the sequence is unique modulo p^{n+1}.

Example 5.0.5 (continued)**.** We claim that by following our previous calculations, we can construct a sequence representing one of the solutions of the polynomial $f(X) = X^2 + 1 \pmod{5^n}$.

Recall the first two solutions we had were $a_0 = 2, a_1 = 7$. Therefore by Hensel's Lemma we have $a_2 = 25t + 7$, and from

$$(25t + 7)^2 + 1 \equiv 0 \pmod{125}$$

we see that we can take $t = 2$, and so $a_2 = 57$ is a solution. Hence the 5-adic expansion of $\sqrt{-1}$, the solution of the polynomial has a Cauchy sequence solution $(2, 7, 57, \dots)$.

The motivation behind giving an example prior to proving the lemma is that the scheme of the proof follows the exact same algorithm as the numerical example considered above. Therefore it is worth to present the easy-to-follow example first, and then "expand" our considerations into the general case.

Proof of Lemma 5.0.3. Following the idea from the example, we construct a Cauchy sequence (α_n) of integers converging to α and satisfying

$$f(\alpha_n) \equiv 0 \pmod{p^n},$$
$$\alpha_n \equiv \alpha_{n+1} \pmod{p^n}.$$

The sequence is Cauchy and convergent by how we have introduced it before, and its limit α will satisfy $f(\alpha) = 0$ (by continuity) and $\alpha \equiv \alpha_1 \pmod{p}$ (by construction). Thus once we establish that polynomials are continuous and the existence of the α_n, we will be done.

Recall that for some

$$x_l = \alpha_0 + \alpha_1 p + \cdots + \alpha_m p^m + \alpha_{m+1} p^{m+1} + \cdots + \alpha_l p^l,$$
$$x_m = \alpha_0 + \alpha_1 p + \cdots + \alpha_m p^m,$$

letting $r \geq 1$ such that $a_{n_0+m} = a_{n_0+m+1} = \cdots = a_{n_0+m+r-1} = 0$, and $a_{n_0+m+r} \neq 0$, we have

$$|x_l - x_m|_p = \frac{1}{p^{n_0+m+r}},$$

thus as we increase l and m, we can make their difference relatively small. Indeed, let $x = x_l$ some Cauchy sequence representation, and an arbitrarily close point $a = x_m$, then for some polynomial function $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ we have

$$\begin{aligned} |f(x_l) - f(x_m)|_p &= |a_0 + a_1 x_l + \cdots + a_n x_l^n - a_0 - a_1 x_m - \cdots - a_n x_m^n|_p \\ &\leq |a_1|_p |x_l - x_m|_p + \cdots + |a_n|_p |x_l^n - x_m^n|_p \\ &\leq |x_l - x_m|_p + \cdots + |x_l^n - x_m^n|_p \end{aligned}$$

since each a_i is an integer. Looking at the first difference, we see

$$\begin{aligned} x_l^2 &= (x_m + \alpha_{m+1} p^{m+1} + \cdots + \alpha_l p^l)^2 \\ &= x_m^2 + 2x_m(\alpha_{m+1} p^{m+1} + \cdots + \alpha_l p^l) + (\alpha_{m+1} p^{m+1} + \cdots + \alpha_l p^l)^2 \\ &\implies |x_l^2 - x_m^2|_p \leq |2x_m(\alpha_{m+1} p^{m+1} + \cdots + \alpha_l p^l)|_p + |\alpha_{m+1} p^{m+1} + \cdots + \alpha_l p^l|_p^2 \\ &= |\alpha_{m+1} p^{m+1} + \cdots + \alpha_l p^l|_p |2x_m + \alpha_{m+1} p^{m+1} + \cdots + \alpha_l p^l|_p \\ &= \frac{1}{p^{m+1}} + \frac{1}{p^m} < \frac{2}{p^m}. \end{aligned}$$

By induction we argue that in fact

$$|x_l^n - x_m^n|_p < \frac{n}{p^m},$$

and thus each such summand will be bound by respective ϵ_n. Finally, we claim that

$$|f(x_l) - f(x_m)|_p \leq \epsilon_1 + \cdots + \epsilon_n < \epsilon$$

with l, m being large enough.

The argument is, if we can take a step from α_1 to α_2, we can repeat the procedure to recursively obtain α_{n+1} from α_n - therefore we only consider the first step. Let $\alpha_2 = \alpha_1 + b_1 p$, then, using the Taylor's series,

$$\begin{aligned} f(\alpha_2) &= f(\alpha_1 + b_1 p) \\ &\equiv f(\alpha_1) + f'(\alpha_1) b_1 p + \text{terms in } \ p^2 \\ &\equiv f(\alpha_1) + f'(\alpha_1) b_1 p \pmod{p^2}, \end{aligned}$$

which gives

$$f(\alpha_1) + f'(\alpha_1) b_1 p \equiv 0 \pmod{p^2}.$$

Since $f(\alpha_1) \equiv 0 \pmod p$, or equivalently $f(\alpha_1) = p\lambda$ for some λ, then

$$\begin{aligned} p\lambda + f'(\alpha_1) p b_1 \equiv 0 \pmod{p^2} &\iff \lambda + f'(\alpha_1) b_1 \equiv 0 \pmod p \\ &\iff b_1 \equiv -\lambda (f'(\alpha_1))^{-1} \pmod p \end{aligned}$$

with $0 \leq b_1 \leq p-1$. Then we repeat the procedure to obtain the result.

We show that the p-adic integer solution is unique.

Let $\alpha = \alpha_0' + \alpha_1' p + \cdots$ be another representation of $\alpha \in \mathbb{Z}_p$, and let n be the first position where $\alpha_n \neq \alpha_n'$, without loss of generality let $\alpha_n < \alpha_n'$.

Similarly define

$$\beta_n = a_0 + a_1 p + \cdots + a_n p^n, \ \ \beta_n' = a_0' + a_1' p + \cdots + a_n' p^n$$

with finite expansions, where

$$(a_i)_{i=0}^{n-1} = (a_i')_{i=0}^{n-1} \ \text{ and } \ a_n \neq a_n'.$$

Then

$$\beta_n' - \beta_n = (a_n' - a_n) p^n.$$

We know that $p \nmid (a_n' - a_n)$ since if $a_n' \equiv a_n \pmod p$ we get an immediate contradiction.

As $a_n' \not\equiv a_n \pmod p$, then we can have $a_n' > p$ and by Hensel's Lemma a_{n+1}' would increase, but we know $a_{n+1}' \equiv 0 \pmod p$ since n was the last element of the Cauchy sequence, thus we get contradiction. Therefore

$$|(a_n' - a_n) p^n|_p = |(a_n' - a_n)|_p |p^n|_p = \frac{1}{p^n},$$

since $p \nmid (a_n' - a_n)$. But by the ultrametric inequality

$$|\beta_n' - \beta_n|_p = |(\beta_n' - \alpha) + (\alpha - \beta_n)|_p \leq \max\{|\beta_n' - \alpha|_p, |\alpha - \beta_n|_p\},$$

where

$$\begin{aligned}|\beta'_n-\alpha|_p &= |a'_0+a'_1p+\cdots+a'_np^n-a'_0-a'_1p-\cdots-a'_np^n-a'_{n+1}p^{n+1}-\cdots|_p\\ &= |-a'_{n+1}p^{n+1}-\cdots|_p=\frac{1}{p^{n+1}},\\ |\alpha-\beta_n|_p &= |a_0+a_1p+\cdots+a_np^n+a_{n+1}p^{n+1}+\cdots-a_0-a_1p-\cdots-a_np^n|_p\\ &= |a_{n+1}p^{n+1}+\cdots|_p=\frac{1}{p^{n+1}}.\end{aligned}$$

Then we obtain a contradiction and thus the representation is unique. □

Remark 5.0.6. The reader might also recognize the proof from a completely other reason: it follows the same scheme as the Newton's algorithm, used in the optimization theory.

Hensel's Lemma contributes hugely towards connecting p-adic fields with solving power series problems, including solving congruence power equations, and proving various topological concepts on the p-adics.

6. Conclusion

The p-adic numbers make a large contribution to connecting number theory with analysis, and present a completely new approach in tackling some of the functions and its power series convergence (provided for example by Taylor polynomials), that might not be obtained in the real case. This thesis presents a small portion of treating such questions and rather gives the tools and their detailed background to develop such intuition for the future reading. The non-archimedian absolute value has been present in string theory and dynamics. Therefore once more, the p-adic numbers were a type of purely abstract mathematical structure, that later began to take part in numerous real-life developments.

It feels like this work has implemented all sorts of mathematical theory, but all of those considerations lay the foundations of the completely new structure: the p-adic numbers.

My hope is the reader has found the order of those considerations easy enough to follow to not lose interest too early and has found the topic intuitive and engaging. Most of the examples provided in the thesis were developed by myself, as well as some of the easier proofs of corollaries or propositions.

Thank you for the time spent on reading my thesis. I hope that this rather brief introduction to the p-adic world will arouse your curiosity about this topic.

References

[Cas86] John W. S. Cassels. *Local Fields*. The Pitt Building, Trumpington Street, Cambridge CB2 1RP: Press Syndicate of the University of Cambridge, 1986. ISBN: 0-521-30484-9.

[Che18] Yuchen Chen. *p-adics, Hensel's Lemma and Strassman's Theorem*. University of Chicago, 2018.

[Gou65] Fernando Q. Gouvea. *p-adic Numbers, An Introduction*. Departament of Mathematics and Computer Science, Colby College: Springer-Verlag Berlin Heidelberg, 1965. ISBN: 3-540-56844-1.

[Ngu14] Lam Nguyen. *The p-adic Numbers*. University of Utah, 2014.

[pla13] planetmath.org. *Proof of Ostrowski's Valuation Theorem*. online, 2013. (accessed: 03.05.2022).

[Sut09] Wilson A. Sutherland. *Introduction to Metric and Topological Spaces*. Oxford University Press, 2009.

Bachelor’s Theses in Mathematical Sciences 2023:K24
ISSN 1654-6229

LUNFMA-4150-2023

Mathematics
Centre for Mathematical Sciences
Lund University
Box 118, SE-221 00 Lund, Sweden

http://www.maths.lu.se/