The p-adic Numbers

De p-adiske tal

An introduction to the theory of p-adic numbers
with comparisons to the real numbers

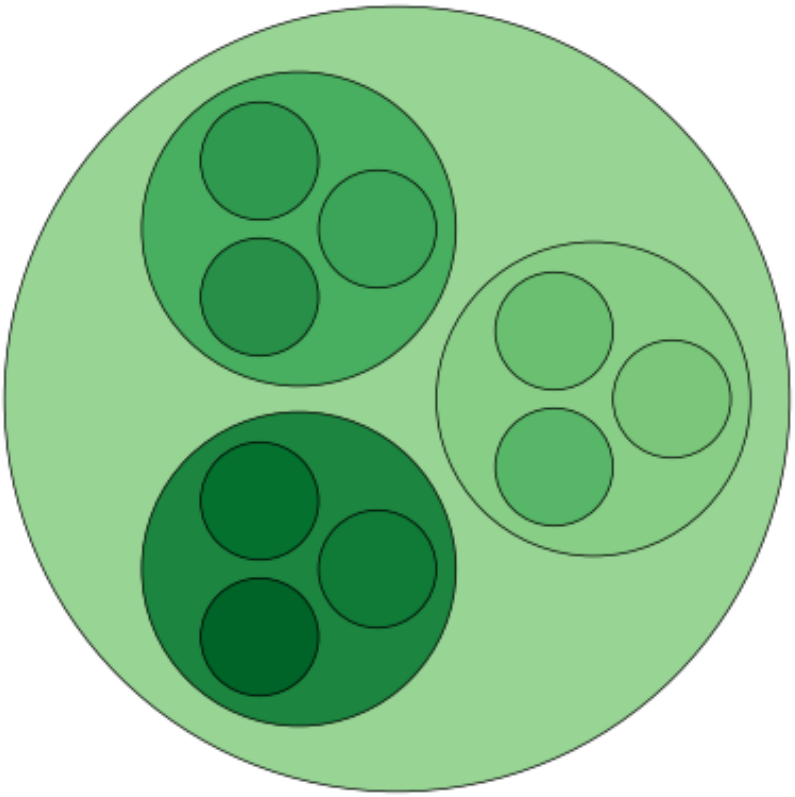

Figure: A visualization of the first digits of $\mathbb{Z}_3$.

Bachelor's Thesis in Mathematics

Department of Mathematics
Aarhus University
Supervisor: Corina Ciobotaru
Turned in March 16, 2026

Abstract

This thesis gives a brief introduction to the p-adic numbers, constructed via completion of $\mathbb{Q}$ with respect to the p-adic norm. A key result is Ostrowski's Theorem, justifying the p-adic norm as the only alternative to the usual absolute value. Topological and algebraic properties of $\mathbb{Q}_p$ are explored, including Hensel's Lemma and finite extensions, with a focus on quadratic cases. The p-adic exponential and logarithm functions are also examined. Throughout, comparisons to the real numbers highlight the unique nature of the p-adic setting.

Resumé

Denne opgave giver en kort introduktion til de p-adiske tal, konstrueret via fuldstændiggørelse af $\mathbb{Q}$ med hensyn til den p-adiske norm. Et centralt resultat er Ostrowski's Theorem, som viser, at den p-adiske norm er det eneste alternativ til den sædvanlige norm. Topologiske og algebraiske egenskaber af $\mathbb{Q}_p$ udforskes samt Hensel's Lemma og endelige udvidelser, med fokus på de kvadratiske udvidelser. Til sidst ses der på den p-adiske eksponential- og logaritmefunktion. Gennem opgaven sammenlignes der med de reelle tal for at illustrere den særlige karakter af de p-adiske tal.

Contents

1 Introduction

During the process of writing this thesis, I've often been asked by non-mathematicians what the project is about. My answer has typically reflected how far along I was in the research. A few months ago, when someone asked "What are... p-adics?", I might have offered the rather non-conclusive response:

> "The p-adics are a different version of the numbers we use. Since mathematics is built from definitions and theorems, if we take the usual properties of distance but tweak them, we can redefine how we measure numbers. The p-adics have a distance function that makes very large numbers very small."

At the time, I was referring, loosely, to Ostrowski's Theorem, one of the central results in this paper. It states that, up to equivalence, there are only two types of absolute values on $\mathbb{Q}$: the usual absolute value, and the p-adic absolute value. Since the p-adic numbers, $\mathbb{Q}_p$, are defined as the completion of $\mathbb{Q}$ with respect to the p-adic norm, this explanation felt quite fitting.

Later in my process, I began exploring the quadratic extensions of $\mathbb{Q}_p$. The topic of extending $\mathbb{Q}_p$ to an algebraically closed field turns out to be strikingly different from the case of $\mathbb{R}$, where extending to $\mathbb{C}$ completes the picture. My answer to the same question evolved:

> "Mathematicians are always trying to improve our number systems. We started with the natural numbers, then added negatives to get integers, then fractions. But fractions were still missing numbers like π and $\sqrt{2}$, so we introduced the real numbers. Then, the equation $x^2 + 1 = 0$ had no solution in $\mathbb{R}$, so we added its solution and created the complex numbers. The p-adics take a different starting point. I'm exploring whether they can be extended in similar ways, and if so, what that looks like."

This often led to a follow-up question: *"So are they better?"*. To which I could only reply: *"Well, they're pretty hard to visualize..."*. That very question of comparing $\mathbb{Q}_p$ and $\mathbb{R}$ ended up becoming a recurring theme throughout the thesis.

Thus, these notes begin with the definition of $\mathbb{Q}_p$, explore its key properties, and gradually build toward the construction of a field $\mathbb{C}_p$ that plays a similar role for $\mathbb{Q}_p$ as $\mathbb{C}$ does for $\mathbb{R}$. Along the way, I examine Ostrowski's Theorem, which classifies all absolute values on $\mathbb{Q}$; study Hensel's Lemma, a fundamental tool for finding roots of polynomials over $\mathbb{Q}_p$; and eventually construct an algebraically closed and complete field, $\mathbb{C}_p$.

Since my work focuses on understanding the differences between p-adic and real numbers, the thesis concludes with a brief exploration of the p-adic exponential and logarithmic functions. These power series behave quite differently from their real counterparts due to the nature of the p-adic norm, where, for instance, large numbers can become "small."

I hope this thesis sparks interest in the topic for readers unfamiliar with $\mathbb{Q}_p$, and provides a clear path into the curious and rich world of p-adic numbers.

2 Construction of the p-adic numbers

This chapter will act as the building blocks of $\mathbb{Q}_p$. The construction may initially seem unintuitive; after all, the size in the p-adic world allows large numbers to be small. This transformation arises naturally from defining a norm $|\cdot|_p$ with respect to each prime p. With this norm, the rest will follow from techniques in analysis and algebra applied to our new metric space.

The material in this chapter is based on [Bak]. Many proofs follow the outlines provided in the article, whilst others are self-drafted.

2.1 Norms and the p-adic Norm

We begin by recalling the notion of a norm.

Definition 2.1. Let R be a ring. A function $N : R \to \mathbb{R}^+$ is called a *norm* if the following properties hold:

$$(N1)\ \ N(x) = 0 \text{ if and only if } x = 0$$

$$(N2)\ \ N(xy) = N(x)N(y),\ \forall x, y \in R$$

$$(N3)\ \ N(x+y) \leq N(x) + N(y),\ \forall x, y \in R.$$

A norm is called *non – Archimedean* if $(N3)$ can be replaced by the *ultrametric inequality*:

$$(N4)\ \ N(x+y) \leq \max\{N(x), N(y)\},\ \forall x, y \in R.$$

If $(N4)$ does not hold, the norm is called *Archimedean.*

Let $p \in \mathbb{N}$ be a prime number. Now we introduce the p-adic norm, that will define the structure of the p-adic numbers. First we define the p-adic ordinal.

Definition 2.2. The p-adic ordinal $ord_p(x)$ of $0 \neq x \in \mathbb{Z}$, as well as the ordinal for $\frac{a}{b} \in \mathbb{Q}$, are given by

$$ord_p(x) = \max\{r \mid p^r \text{ divides } x\}, \quad ord_p(\frac{a}{b}) = ord_p(a) - ord_p(b).$$

We use the convention $ord_p(0) = \infty$.

Definition 2.3. The p-adic norm of x, for $x \in \mathbb{Q}$ is given by

$$|\, x \,|_p := \begin{cases} p^{-ord_p(x)} & \text{for } x \neq 0 \\ p^{-\infty} = 0 & \text{for } x = 0. \end{cases}$$

It is clear, that $|\cdot|_p$ is a discrete norm, and we will now show that it is non-Archimedean.

Proposition 2.4. *$|\cdot|_p$ is a non-Archimedean norm on $\mathbb{Q}$.*

Proof. We want to verify each property of a norm from Definition 2.1.
$(N1)$: if $x \neq 0$, then $ord_p(x) < \infty$ so $|x|_p = 1/p^{ord_p(x)} > 0$. Conversely if $x = 0$, then $|x|_p = 0$ by definition.

$(N2)$: let $x, y \in \mathbb{Q}$ given by $x = \frac{a}{b}, y = \frac{c}{d}$ with $a, b, c, d \in \mathbb{Z}$ and $b, d \neq 0$. First we will explicitly see, that the ordinal of products of integers is the sum of their ordinals. Let $a = p^{r_1}h$ and $b = p^{r_2}k$, where $p \nmid h$, $p \nmid k$, and $r_1, r_2 \in \mathbb{N}$.

$$ord_p(ab) = \max\{r : p^r \mid ab\} = \max\{r : p^r \mid p^{r_1+r_2}hk\} = r_1 + r_2 = ord_p(a) + ord_p(b).$$

We can easily apply this to the product of rationals, so $ord_p(xy) = ord_p(x) + ord_p(y)$. For $x, y \neq 0$

$$|xy|_p = p^{-ord_p(xy)} = p^{-ord_p(x)-ord_p(y)} = |x|_p|y|_p.$$

$(N4)$: lastly we will show the ultra metric inequality by showing that $ord_p(x+y) \geq \min\{ord_p(x), ord_p(y)\}$. Let $x, y \in \mathbb{Q} \setminus \{0\}$ given by $x = p^{r_1}\frac{a}{b}$ and $y = p^{r_2}\frac{c}{d}$, where p and a, b, respectively c, d, are pairwise relatively prime. When $r_1 = r_2$, then $x+y = p^{r_1}\frac{ad+bc}{bd}$, and since $p \nmid bd$ it follows that $ord_p(x+y) \geq r_1$. Now WLOG assume $r_1 < r_2$, so

$$x + y = p^{r_1}\left(\frac{a}{b} + p^{r_2-r_1}\frac{c}{d}\right) = p^{r_1}\left(\frac{ad + p^{r_2-r_1}bc}{bd}\right),$$

since $r_2 - r_1 > 0$ and $p \nmid bd$ then $ord_p(x + y) \geq \min\{r_1, r_2\}$. This gives us the following:

$$|x + y|_p = p^{-ord_p(x+y)} \leq \max\{|x|_p, |y|_p\},$$

so the p-adic norm is a non-Archimedean norm on $\mathbb{Q}$.

□

Notation: We have seen that for every prime p, the p-adic norm $|\cdot|_p$ gives another way to measure the size of the elements of $\mathbb{Q}$. It will be necessary to be on the same page with notation with a few additional central norms. First, we have the *trivial norm*, $|\cdot|_{\text{tr}}$, defined by:

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

Second, we have the standard absolute value on $\mathbb{R}$, also known as the Euclidean, or Archimedean, norm. This will also be relevant and will be denoted by $|\cdot|_\infty$, analogously to the p-adic norms. That is,

$$|x|_\infty = \sqrt{x^2}.$$

Example: Let p be a prime number. The number p^{100} is, by most, considered very large in $\mathbb{R}$. If $p = 3$, then 3^{100} has 48 digits, and if $p = 11$ then 11^{100} has approximately 104 digits. Contrarily p^{100} is very small in $\mathbb{Q}_p$. We see this by computing the p-adic norm

$$|p^{100}|_p = \frac{1}{p^{100}}.$$

Depending on choice of p, this norm will have roughly as many zeroes after the decimal point as digits in p^{100}. This goes to illustrate that very large numbers in $\mathbb{R}$ can be very small in $\mathbb{Q}_p$.

2.2 The Completion of $\mathbb{Q}_p$

Just as $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$, the field $\mathbb{Q}_p$ arises as the completion of $\mathbb{Q}$ under the p-adic norm $|\cdot|_p$.
In other words, $\mathbb{Q}_p$ is defined as the quotient set

$$\mathbb{Q}_p := CS(\mathbb{Q}, |\cdot|_p)/Null(\mathbb{Q}, |\cdot|_p), \tag{1}$$

where:

$$\begin{aligned} CS(\mathbb{Q}, |\cdot|_p) &= \{\text{Cauchy sequences in } \mathbb{Q} \text{ with respect to } |\cdot|_p\}, \\ Null(\mathbb{Q}, |\cdot|_p) &= \{\text{null sequences in } \mathbb{Q} \text{ with respect to } |\cdot|_p\} \\ &= \left\{(a_n) \in \mathrm{CS}(\mathbb{Q}, |\cdot|p) : \lim_{n\to\infty} |a_n|_p = 0\right\}. \end{aligned}$$

Thus two Cauchy sequences (a_n) and (b_n) in $CS(\mathbb{Q}, |\cdot|_p)$ are equivalent if their difference $(a_n - b_n)$ is a null-sequence i.e,

$$(a_n) \sim (b_n) \iff \lim_{n\to\infty} |a_n - b_n|_p = 0.$$

We denote the equivalence class of a Cauchy sequence (a_n) by $[(a_n)]$, and so $[(a_n)] \in \mathbb{Q}_p$ (see [Bak] page 20). It is this equivalence that turns the quotient set $\mathbb{Q}_p$ into a field, a fact which is verified in Theorem 2.6 below.

Definition 2.5. The ring of p-adic numbers, denoted by $\mathbb{Q}_p$, is the completion of $\mathbb{Q}$ with respect to the p-adic norm $|\cdot|_p$.
Furthermore, the p-adic integers $\mathbb{Z}_p$ are defined to be the unit disc about $0 \in \mathbb{Q}_p$,

$$\mathbb{Z}_p := \{\alpha \in \mathbb{Q}_p : |\alpha|_p \leq 1\}.$$

In order to see that $\mathbb{Q}_p$ is a field, we first need to define its addition and multiplication. Let $\alpha = [(a_n)], \beta = [(b_n])] \in \mathbb{Q}_p$. Then the sum and product of elements in $\mathbb{Q}_p$ is defined by

$$\alpha + \beta = [(a_n + b_n)], \quad \alpha \cdot \beta = [(a_n b_n)]. \tag{2}$$

These relations are easily checked to be well defined. Given these operations, we can now show that $\mathbb{Q}_p$ is indeed a field.

Theorem 2.6. $\mathbb{Q}_p$ is a field.

Proof. First, it is easy to see that $CS(\mathbb{Q}, |\cdot|_p)$ with the addition and multiplication from (2.2), and with $0, 1 \in \mathbb{Q}$, form a commutative ring, since $\mathbb{Q}$ is commutative.
Next, given that $CS(\mathbb{Q}, |\cdot|_p)$ is a commutative ring, we want to verify that $Null(\mathbb{Q}, |\cdot|_p)$ is a two-sided ideal. By the known theory on rings and ideals, it will imply that the quotient set $\mathbb{Q}_p$ is a field.

To show that $Null(\mathbb{Q}, |\cdot|_p)$ is a two-sided ideal, let $(a_n) \in CS(\mathbb{Q}, |\cdot|_p)$ and $(b_n) \in Null(\mathbb{Q}, |\cdot|_p)$. Then $(a_n b_n), (b_n a_n) \in Null(\mathbb{Q}, |\cdot|_p)$. We see this using the product defined in equation (2.2),

$$\lim_{n\to\infty} |a_n b_n|_p = \lim_{n\to\infty} (|a_n|_p |b_n|_p) = \lim_{n\to\infty} |a_n|_p \cdot 0 = 0,$$

and equivalently for $(b_n a_n)$. Hence $Null(\mathbb{Q}, |\cdot|_p)$ is a two-sided ideal.

Lastly, we need to show that every element different from 0 has a multiplicative inverse. Let $[(a_n)] \in \mathbb{Q}_p$ and assume $[(a_n)] \neq [0]$. Define $l := \lim_{n\to\infty} |a_n|_p$. We know that $l > 0$, since otherwise we get

$$\lim_{n\to\infty} |a_n|_p = 0 \Leftrightarrow (a_n) \in Null(\mathbb{Q}, |\cdot|_p)$$
$$\Leftrightarrow [(a_n)] = [0]. \quad \lightning$$

We can then find for any $\epsilon > 0$ an $N \in \mathbb{N}$, so that $\left| |a_n|_p - l \right| < \epsilon$, whenever $n > N$. Choose $\epsilon = \frac{l}{2}$.

$$-\frac{l}{2} < |a_n|_p - l < \frac{l}{2} \quad \Rightarrow \quad 0 < \frac{l}{2} < |a_n|_p \quad \Rightarrow a_n \neq 0.$$

Since $\mathbb{Q}$ is a field, a_n has a well defined inverse when $n > N$, allowing us to define the sequence $\{b_n\}$ as following

$$b_n = \begin{cases} 1, & \text{when } n \leq N, \\ a_n^{-1}, & \text{when } n > N. \end{cases}$$

Note that (b_n) is Cauchy since for $n, m > N$

$$|b_n - b_m|_p = |a_n^{-1} - a_m^{-1}|_p = |\frac{a_m - a_n}{a_n a_m}|_p = \frac{|a_m - a_n|_p}{|a_n|_p |a_m|_p} < \frac{\epsilon}{(\frac{l}{2})^2}$$

for any $\epsilon > 0$, since $\{a_n\}$ is Cauchy. It follows from construction that $\lim_{n\to\infty} |a_n b_n|_p = 1$, so $[(a_n)][(b_n)] = 1$, showing that all non-zero elements have an inverse in $\mathbb{Q}_p$.

□

2.3 The p-adic Expansion

This section will be focusing on how numbers are represented in $\mathbb{Q}_p$. First we notice that we can always write a finite p-adic expansion of any integer $s \in \mathbb{Z}$:

$$s = s_0 + s_1 p + s_2 p^2 + \cdots + s_l p^l, \quad 0 \leq s_0, ..., s_l \leq p - 1$$

for some $l \in \mathbb{N}$. This follows from repeatedly doing Euclidean division. This will be useful in the proof of the next proposition.

Proposition 2.7. ([Bak] Thm. 2.28) *$\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$. Every element of $\mathbb{Z}_p$ is the limit of a sequence of non-negative integers from $\mathbb{Z}$. Conversely, every sequence of integers that is Cauchy with respect to the p-adic norm $|\cdot|_p$ has a limit in $\mathbb{Z}_p$.*

Proof. First we prove that $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$, so we want to show that it is a subgroup of $(\mathbb{Q}_p, +)$ and closed under multiplication in $(\mathbb{Q}_p, \cdot)$, as well as $1 \in \mathbb{Z}_p$. Indeed, the latter mentioned fact follows, since $|0|_p = 0 \leq 1$ and $|1|_p = 1 \leq 1$, so $0, 1 \in \mathbb{Z}_p$. The former mentioned fact follows immediately from the definition of $|\cdot|_p$: let $a, b \in \mathbb{Z}_p$, then $\mathbb{Z}_p$ is closed under addition, since $|a + b|_p \leq \max\{|a|_p, |b|_p\} \leq 1$, and it is also closed under multiplication, since $|a \cdot b|_p = |a|_p |b|_p \leq 1$. This shows that $(\mathbb{Z}_p, \cdot)$ is a subring of $(\mathbb{Q}_p, \cdot)$.

As a side remark, notice that any negative integer in $\mathbb{Z}$ is a limit of a sequence of positive integers from $\mathbb{Z}$ with respect to the p-adic norm. One just needs to write the p-adic decomposition of -1:

$$-1 = p - 1 + (p-1)p + (p-1)p^2 + \cdots = \sum_{i=0}^{\infty} (p-1)p^i.$$

Moving on, our goal is to find a sequence of integers that converges to a given p-adic integer. Using the definition of $\mathbb{Q}_p$, i.e. elements in $\mathbb{Q}_p$ are limits of Cauchy sequences in the rational numbers, along with some number theory, we will create this sequence of integers.
Let $\alpha \in \mathbb{Z}_p$, so by definition $\alpha = [(a_n)]$ is a Cauchy sequence with $a_n \in \mathbb{Q}$. Since $|\cdot|_p$ is a non-Archimedean norm, thus taking discrete values, the Cauchy sequences $|a_n|_p$ will eventually be constant, so $|a_n|_p = c$ for some $c \in \mathbb{Q}$ for all $n > M$ using a suitable M. As a consequence $|\alpha|_p = c \leq 1$ by definition of $\mathbb{Z}_p$. Without loss of generality, assume $|a_n|_p \leq 1$ for all n.
Let $a_n = \frac{r_n}{s_n}$ with $r_n, s_n \in \mathbb{Z}$, co-prime, and $r_n, s_n \neq 0$. It follows, that $ord_p(r_n) - ord_p(s_n) \geq 0$ since

$$1 \geq |a_n|_p = \frac{|r_n|_p}{|s_n|_p} \quad \Rightarrow \quad |s_n|_p \geq |r_n|_p \quad \Rightarrow \quad ord_p s_n \leq ord_p r_n$$

It then follows that $s_n \not\equiv 0 \pmod{p}$, since otherwise

$$s_n = p \cdot l(\text{ for } l \in \mathbb{Z}) \quad \Rightarrow \quad |s_n|_p < 1 \text{ and } p \nmid r_n \quad \Rightarrow \quad |r_n|_p = 1 \quad \Rightarrow \quad \frac{|r_n|_p}{|s_n|_p} > 1 \quad \lightning.$$

Using some number theory results, for each m we can solve the equation $s_n x \equiv 1 \pmod{p^m}$ with solutions in $\mathbb{Z}$, i.e. finding the inverse of s_n modulo p^m. This loosely follows from s_n and p being co-prime, so by Bezous' identity we can find an inverse modulo p. Using induction this can be extended to being able to find an inverse modulo p^m. Let u_{nm} be that solution. By the possibility of adding multiples of p^m we can assume $1 \leq u_{nm} \leq p^m - 1$. For all m we now have $|s_n u_{nm} - 1|_p \leq \frac{1}{p^m}$, since

$$s_n u_{nm} - 1 \equiv 0 \pmod{p^m} \quad \Rightarrow \quad s_n u_{nm} - 1 = p^m \cdot j, \text{ for a suitable } j \quad \Rightarrow \quad ord_p(s_n u_{nm} - 1) \geq m.$$

We want to use these integers to construct our sequence that converges to α, hence we need to start finding some upper limits. For all m

$$|\frac{r_n}{s_n} - r_n u_{nm}|_p = |\frac{r_n}{s_n}|_p |1 - s_n u_{nm}|_p \leq \frac{1}{p^m}.$$

Very nice!
Since $\alpha = [(a_n)]$ is a Cauchy sequence and from the above inequality, for every m we can find an integer $z_{k_m} \in \mathbb{Z}$ such that $|\alpha - z_{k_m}|_p \leq \frac{1}{p^m}$. Indeed, combining everything, we get

$$\begin{aligned} |\alpha - r_{k_m} u_{k_m(m+1)}|_p &= |\alpha - a_{k_m} + a_{k_m} - r_{k_m} u_{k_m(m+1)}|_p \\ &\leq max\{|\alpha - a_{k_m}|_p, |a_{k_m} - r_{k_m} u_{k_m(m+1)}|_p\} \\ &< \frac{1}{p^m}, \end{aligned}$$

showing $\lim_{n\to\infty}(\alpha - r_{k_n} u_{k_n(n+1)}) = 0$, so $\alpha \in \mathbb{Z}_p$ is the limit of a sequence of integers.

Finally we want to show that every sequence of integers that is Cauchy with respect to the p-adic norm has a limit in $\mathbb{Z}_p$. Let $(a_n)_n$ with $a_n \in \mathbb{Z}$ be a Cauchy sequence with respect to $|\cdot|_p$, thus there exists an element $\alpha \in \mathbb{Q}_p$ which is the p-adic limit of $(a_n)_n$. Being a Cauchy sequence we have $|\alpha - a_n|_p < \frac{1}{p}$ for some $n \in \mathbb{N}$. Then

$$|\alpha|_p = |\alpha - a_n + a_n|_p \leq \max\{|\alpha - a_n|_p, |a_n|_p\} \leq 1,$$

since $a_n \in \mathbb{Z} \subseteq \mathbb{Z}_p$. Thus $\alpha \in \mathbb{Z}_p$ which concludes the proof.

□

Now we will describe the *p-adic digit expansion*, which characterizes the elements of $\mathbb{Q}_p$. Our goal is to express the p-adic integers as infinite sums.

Lemma 2.8. *Let $\alpha \in \mathbb{Z}_p$. Then α has a p-adic expansion*

$$\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots = \sum_{i=0}^{\infty} \alpha_i p^i \qquad \text{with } \alpha_i \in \{0, ..., p-1\}.$$

Proof. Let $\alpha \in \mathbb{Z}_p$, by Proposition 2.7 and its proof, we claim there exists an $\alpha_0 \in \mathbb{Z}$ such that

$$|\alpha - \alpha_0|_p \leq \frac{1}{p}, \quad 0 \leq \alpha_0 \leq p-1.$$

Indeed, fix some $m \geq 1$. Then one can take α_0 to be the term corresponding to p^0 of the p-adic expansion of the integer $r_{k_m} u_{k_m(m+1)}$. Thus we have

$$r_{k_m} u_{k_m(m+1)} = \alpha_0 + p(\cdots), \quad 0 \leq \alpha_0 \leq p-1$$

since it then follows

$$\begin{aligned} |\alpha - \alpha_0|_p &= |\alpha - r_{k_m} u_{k_m(m+1)} + r_{k_m} u_{k_m(m+1)} - \alpha_0|_p \\ &\leq max\{|\alpha - r_{k_m} u_{k_m(m+1)}|_p, |r_{k_m} u_{k_m(m+1)} - \alpha_0|_p\} \\ &\leq \frac{1}{p}. \end{aligned}$$

We can consider

$$|\frac{\alpha - \alpha_0}{p}|_p = |\frac{1}{p}|_p \cdot |\alpha - \alpha_0|_p \leq p \cdot \frac{1}{p} = 1,$$

which gives us the p-adic number $\frac{\alpha-\alpha_0}{p} \in \mathbb{Z}_p$. Again by Proposition 2.7 applied to $\frac{\alpha-\alpha_0}{p}$, we can find $\alpha_1 \in \mathbb{Z}_p$ such that

$$|\frac{\alpha - \alpha_0}{p} - \alpha_1|_p < 1, \quad 0 \leq \alpha_1 \leq p-1 \quad \Rightarrow \quad |\alpha - (\alpha_0 + \alpha_1 p)|_p < \frac{1}{p}, \quad 0 \leq \alpha_1 \leq p-1.$$

Repeating this, we get a sequence of positive integers $\{\alpha_n\}$ such that

$$|\alpha - (\alpha_0 + \alpha_1 p + \cdots + \alpha_n p^n)|_p < \frac{1}{p^n}, \quad 0 \leq \alpha_n \leq p-1.$$

The sequence (β_n) given by $\beta_n := \alpha_0 + \alpha_1 p + \cdots + \alpha_n p^n$ is Cauchy with respect to the p-norm, since for any $k \in \mathbb{N}$

$$\begin{aligned} |\beta_{n+k} - \beta_n|_p &= |\alpha_{n+1} p^{n-1} + \alpha_{n+2} p^{n+2} + \cdots + \alpha_{n+k} p^{n+k}|_p \\ &= |p^n|_p \cdot |\alpha_{n+1} p + \cdots + \alpha_{n+k} p^k|_p \\ &\leq \frac{1}{p^n}, \end{aligned}$$

where we for any $\epsilon > 0$ can choose an $M \in N$ such that $p^M \geq \frac{1}{\epsilon}$, so for $n > M$

$$|\beta_{n+k} - \beta_n|_p < \frac{1}{p^M} \leq \epsilon.$$

The limit is of course α. This gives us the desired expansion of α by $\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \cdots$. □

Although this looks very similar to decimal expansion, a very nice property with the p-adic integers is that they are unique, unlike in $\mathbb{R}$, where it is known that $0,999... = 1$. Now let us expand this notion to all p-adic numbers.

Theorem 2.9. ([Bak] Thm. 2.29) Every p-adic number $\alpha \in \mathbb{Q}_p$ has a unique expansion given by

$$\alpha = \alpha_{-r}p^{-r} + \alpha_{1-r}p^{1-r} + \cdots + \alpha_{-1}p^{-1} + \alpha_0 + \alpha_1 p + \cdots = \sum_{i=-r}^{\infty} \alpha_i p^i,$$

where $\alpha_n \in \mathbb{Z}$ with $0 \leq \alpha_n \leq p-1$.

Proof. We have shown the expansion for p-adic integers in Lemma 2.8. Our goal is to find an expansion for elements $\alpha \notin \mathbb{Z}_p$.
Let $\alpha \in \mathbb{Q}_p$ and assume $|\alpha|_p > 1$, hence $|\alpha|_p = p^k$ for some $k \geq 1$. We know the expansion for the p-adic integer $p^k\alpha =: \beta$, since $|\beta|_p = 1$, so we can write $\beta = \beta_0 + \beta_1 p + \beta_2 p^2 + \cdots$. Then

$$\alpha = \frac{\beta_0}{p^k} + \frac{\beta_1}{p^{k-1}} + \cdots + \frac{\beta_{k-1}}{p} + \beta_k + \beta_{k+1}p + \beta_{k+2}p^2, \qquad 0 \leq \beta_n \leq p-1.$$

Now let us prove uniqueness. Assume $\alpha = \alpha'_0 + \alpha'_2 p + \cdots$ is another p-adic expansion of α and denote the coefficients (β'_n). Let d be the first integer such that $\alpha_d \neq \alpha'_d$, and assume WLOG $\alpha_d < \alpha'_d$ so $1 \leq \alpha'_d - \alpha_d \leq p-1$. This implies

$$|\beta'_d - \beta_d|_p = |(\alpha'_d - \alpha_d)p^d|_p = \frac{1}{p^d}.$$

But contradictorily, we also get

$$|\beta'_d - \beta_d|_p = |\beta'_d - \alpha + \alpha - \beta_d|_p \leq max\{|\beta'_d - \alpha|_p, |\alpha - \beta_d|_p\} < \frac{1}{p^d}.$$

Letting us conclude that the expansion is unique, since such d cannot exist.

□

3 Topological and Algebraic Structure of $\mathbb{Q}_p$

The topological and algebraic structure of $\mathbb{Q}_p$ is interesting to look at, since the p-adic norm is discrete, whilst the usual norm on $\mathbb{R}$ is not. This leads to open balls also being closed in $\mathbb{Q}_p$. Moreover, unlike $\mathbb{Z} \subseteq \mathbb{R}$ being a discrete unbounded subset, the ring of p-adic integers $\mathbb{Z}_p$ is compact in $\mathbb{Q}_p$. This highlights some central differences between $\mathbb{Q}_p$ and $\mathbb{R}$.

Definition 3.1. The open ball centered at $\alpha \in \mathbb{Q}_p$ with radius $\delta > 0$ is given by

$$B(\alpha, \delta) = \{\gamma \in \mathbb{Q}_p : |\gamma - \alpha|_p < \delta\}.$$

Proposition 3.2. *If $\beta \in B(\alpha, \delta)$ then $B(\beta, \delta) = B(\alpha, \delta)$.*

Proof. Let $a \in B(\alpha, \delta)$.

$$|a - \beta|_p = |(a - \alpha) + (\alpha - \beta)|_p \leq \max\{|a - \alpha|_p, |\alpha - \beta|_p\} < \delta,$$

thus $B(\alpha, \delta) \subseteq B(\beta, \delta)$. The same calculation can be used to prove the equality. □

Notice that Proposition 3.2 states that in the p-adic world the center of an open ball is not unique, and in fact every element of an open ball is a center of it.

Proposition 3.3. ([Kat] Prop. 2.3) *The open balls in $\mathbb{Q}_p$ are open and closed.*

Proof. Let $B(a, r)$ be an open ball. Then $B(a, r)$ is open by definition. We want to show that the complement of the ball $B(a, r)$ is an open set. Let the complement be denoted by $C := \{x \in \mathbb{Q}_p : |x - a|_p \geq r\}$, and see that

$$C = \{x \in \mathbb{Q}_p : |x - a|_p = r\} \cup \{x \in \mathbb{Q}_p : |x - a|_p > r\}.$$

We know that $\{x \in \mathbb{Q}_p : |x - a|_p > r\}$ is open, being the complement of the closed ball $\{x \in \mathbb{Q}_p : |x - a|_p \leq r\}$. Therefore, we just need to show that the sphere $S(a, r) := \{x \in \mathbb{Q}_p : |x - a|_p = r\}$ is also open. To see this, let $x \in S(a, r)$ and $0 < \epsilon < r$ be given. We want to show that $B(x, \epsilon) \subset S(a, r)$. Let $y \in B(x, \epsilon)$. We have

$$r = |x - a|_p = |x - y + y - a|_p \leq \max\{|x - y|_p, |y - a|_p\} = |y - a|_p,$$

since, if we assumed $|y - a|_p \leq |x - y|_p < \epsilon < r$, we would get a contradiction. Moreover, we have

$$|y - a|_p \leq \max\{|y - x|_p, |x - a|_p\} = r,$$

which proves that $|y - a|_p = r$. Thus, indeed $B(x, \epsilon) \subset S(a, r)$, so the sphere $S(a, r)$ is open. This finishes the proof that the open ball $B(a, r)$ is closed. □

Proposition 3.4. *$\mathbb{Z}_p$ is compact.*

Proof. Since $\mathbb{Z}_p$ is a metric space with the p-adic norm (induced by $\mathbb{Q}_p$), proving compactness is equivalent to proving sequential compactness.

Take a sequence $(x_n)_{n\in\mathbb{N}}$ in $\mathbb{Z}_p$ and, by Theorem 2.9, write each element x_n in it's p-adic decomposition

$$x_n = a_{n_0} + a_{n_1}p + a_{n_2}p^2 + \cdots, \tag{3}$$

with $a_i \in \{0, ..., p-1\}$. Now, for each element of the sequence $(x_n)_{n\in\mathbb{N}}$, consider the corresponding first digit a_{n_0} from (3) and select a digit $d_0 \in \{0, ..., p-1\}$ that appears as the first digit for infinitely many elements in $(x_n)_{n\in\mathbb{N}}$. Select the subsequence $(x_{k_j})_{j\in\mathbb{N}}$ of elements having as first digit d_0. This subsequence is infinite by construction.
Consider the second digit in the p-adic decomposition (3) of the elements in the subsequence (x_{k_j}), i.e. the corresponding a_{n_1} in (3). Select a digit $d_1 \in \{0, ..., p-1\}$ that appears as the second digit for infinitely many elements in (x_{k_j}) and construct a subsequence $(x_{k_{j_i}})_{i\in\mathbb{N}}$ of (x_{k_j}) with d_1 as a second digit. It is again infinite by construction, and all elements in the subsubsequence $(x_{k_{j_i}})$ share the first two digits, and thus are of the form

$$x_{k_{j_i}} = d_0 + d_1 p + p^2(\cdots).$$

Inductively, if we continue, then at step $k+1$ we will have a subsequence where the elements agree on the first k digits, $d_0, ..., d_{k-1}$. Again by construction and by the pigeon hole principal we can look at the $(k+1)^{\text{th}}$ digit, corresponding to a_{n_k} in (3), and choose a d_k such that there are infinitely many elements with this as the$(k+1)^{\text{th}}$ digit. We will denote this subsequence that agrees on the first $k+1$ digits by $(x_{n_k})_{k\in\mathbb{N}}$.

All that remains is to show that there is a convergence subsequence in our original sequence $(x_n)_{n\in\mathbb{N}}$. Let $x := \sum_{i=0}^{\infty} d_i p^i$, which by Proposition 2.7 is a well-defined element in $\mathbb{Z}_p$. Let $\epsilon > 0$ and choose k such that $\frac{1}{p^k} < \epsilon$. By construction, (x_{n_k}) and x agree at least on the first k digits, so

$$|x - x_{n_k}|_p \leq \frac{1}{p^k} < \epsilon,$$

so $\lim_{k\to\infty} x_{n_k} = x$. showing that $\mathbb{Z}_p$ is sequentially compact and thus compact.

□

Recall that a Hausdorff topological space X is called *locally compact*, if for every $x \in X$ there exists a compact neighborhood of x with respect to the given topology on X.

Theorem 3.5. $\mathbb{Q}_p$ is locally compact.

Proof. Since $\mathbb{Q}_p$ is a metric space, it is also Hausdorff. Let $\alpha \in \mathbb{Q}_p$. Since by Proposition 3.3 $\mathbb{Z}_p$ is compact and open in $\mathbb{Q}_p$, and translation is a homeomorphism, then $\alpha + \mathbb{Z}_p$ is a compact neighborhood of α, which proves the theorem. □

Proposition 3.6. *The ball $p\mathbb{Z}_p = B(0,1) = \{x \in \mathbb{Q}_p : |x|_p < 1\}$ is a maximal ideal of $\mathbb{Z}_p$.*

Proof. It is clear that $p\mathbb{Z}_p$ is an ideal in $\mathbb{Z}_p$, so why is it maximal? If I is an ideal of $\mathbb{Z}_p$, we say that $p\mathbb{Z}_p$ is maximal if $p\mathbb{Z}_p \subseteq I$ then $p\mathbb{Z}_p = I$ or $I = \mathbb{Z}_p$.
Suppose I is an ideal of $\mathbb{Z}_p$, and assume $p\mathbb{Z}_p \subseteq I$. Note that we can write

$$\mathbb{Z}_p = \bigcup_{i=0}^{p-1} \{i + p\mathbb{Z}_p\}, \quad x = x_0 + p\mathbb{Z}_p \text{ when } x \in \mathbb{Z}_p.$$

Let $a \in I$ and $a \notin p\mathbb{Z}_p$, so $a = a_0 + p\mathbb{Z}_p$ with $a_0 \neq 0$. Note, since I is a group, then $ma_0 \in I$ for all $m \in \mathbb{Z}$. Our goal is to show that $I = \mathbb{Z}_p$, and to do this we will prove that

$$\{ma_o \mid n \in \mathbb{Z}\} \overset{\text{mod } p}{=} \{0, 1, ..., p-1\}.$$

Since $a_0 \in \{0, 1, ..., p-1\}$, with $a_0 \neq 0$, we have $\gcd(p, a_0) = 1$. By Bezout's we can find $s, t \in \mathbb{Z}$ such that $sp + ta_0 = 1$. Thus $ta_0 \equiv 1 \pmod{p}$ and $1 \in I$, since I is a group. Since $1 \in I$, we are done, since 1 generates $\{0, ..., p-1\}$ modulo p.

□

4 Ostrowski's Theorem: Classification of Absolute Values on $\mathbb{Q}$

Before we state Ostrowski's Lemma, it is helpful to understand how absolute values on $\mathbb{Q}$ can differ, and in what sense they are essentially unique. Ostrowski's Theorem provides a complete classification of all absolute values on $\mathbb{Q}$: up to equivalence, every nontrivial absolute value is either the usual absolute value $|\cdot|_\infty$ which leads to the completion $\mathbb{R}$, or a p-adic absolute value $|\cdot|_p$ for some prime p, leading to the field $\mathbb{Q}_p$. This striking result highlights that $\mathbb{Q}_p$ is not just an exotic number system. In a sense, it is the only natural alternative to the real numbers arising from $\mathbb{Q}$. This chapter is largely based on chapter 3.1 in [Gou].

Definition 4.1. Let D be a field. An *absolute value* $|\cdot| : D \to \mathbb{R}$ on D is a function satisfying

$$
\begin{aligned}
&(A1)\ |x| \geq 0, && \text{(non-negativity)}\\
&(A2)\ |x| = 0 \Leftrightarrow x = 0, && \text{(positive definiteness)}\\
&(A3)\ |xy| = |x||y|, && \text{(multiplicativity)}\\
&(A4)\ |x+y| \leq |x| + |y|, && \text{(triangle inequality).}
\end{aligned}
$$

If an absolute value satisfies the stronger triangle inequality, $(A4)'$: $|x+y| \leq \max\{|x|, |y|\}$, we say $|\cdot|$ is *non-Archimedean.*

The field $\mathbb{Q}$ yields the absolute values we have already touched upon, $|\cdot|_{tr}$, $|\cdot|_\infty$ and $|\cdot|_p$ for every prime p.
Remark: Absolute values induce a metric $d(x,y) = |x-y|$, and hence a topology on a given field $\boldsymbol{F}$.

Definition 4.2. ([Gou] Def. 3.1.1) Given two absolute values, $|\cdot|_1$ and $|\cdot|_2$, on a field $\boldsymbol{F}$, we say they are *equivalent* if they define the same topology on $\boldsymbol{F}$, i.e every open set with respect to the one absolute value must also be open with respect to the other.

This sounds very nice, but it is hard to prove. So, we will instead use the following criteria:

Definition 4.3. Let $|\cdot|_1$ and $|\cdot|_2$ be absolute values on $\boldsymbol{F}$. We say that they are *equivalent* (or λ-equivalent) if there exist a real number $\lambda > 0$ such that for all $x \in \boldsymbol{F}$ we have $|x|_1 = |x|_2^\lambda$.

Lemma 4.4. *The λ-equivalence in Definition 4.3 defines an equivalence relation on absolute values.*

Proof. Reflexitivity: let $\lambda = 1$. Then for any absolute value on $\boldsymbol{F}$, $|x| = |x|^1$ for all $x \in \boldsymbol{F}$ proving reflexitivity.
To prove symmetry, assume $|\cdot|_1$ is equivalent to $|\cdot|_2$, so there exists a $\lambda > 0$ such that

$$
|x|_1 = |x|_2^\lambda \quad \Rightarrow \quad |x|_1^{1/\lambda} = |x|_2, \qquad \text{where } \frac{1}{\lambda} > 0,
$$

so $|\cdot|_2$ is equivalent to $|\cdot|_1$.
Assume $|\cdot|_3$ is another non-trivial absolute value on $\boldsymbol{F}$ and assume $|x|_1 = |x|_2^{\lambda_1}$ and $|x|_2 = |x|_3^{\lambda_2}$. Substituting the equations, it follows that

$$
|x|_1 = (|x|_3^{\lambda_2})^{\lambda_1} = |x|_3^{\lambda_1\lambda_2},
$$

hence it defines an equivalence relation. □

The next lemma will show that this λ-equivalence corresponds to topological equivalence, i.e. inducing the same topology.

Lemma 4.5. *Let $|\cdot|_1$ and $|\cdot|_2$ be non-trivial absolute values on a field $\boldsymbol{F}$. They define the same topology on $\boldsymbol{F}$ if and only if they are λ-equivalent.*

Proof. The metrics induced by the absolute values are respectively $d_1(x,a) = |x-a|_1$ and $d_2(x,a) = |x-a|_2$. Assume $|x|_1 = |x|_2^\lambda$ for some $\lambda > 0$, so

$$d_1(x,a) = |x-a|_1 = |x-a|_2^\lambda.$$

We want to show that the same open balls are created. Let $a \in \boldsymbol{F}$. We will show that $B_1(a,r) = B_2(a,r^{1/\lambda})$ where $B_1(a,r) = \{x \in \mathbf{F} : d_1(x,a) < r\}$ and $B_2(a,r) = \{x \in \mathbf{F} : d_2(x,a) < r\}$. First, let $x \in B_1(a,r)$, then

$$|x-a|_1 < r \quad \Rightarrow \quad |x-a|_2^\lambda < r \quad \Rightarrow \quad |x-a|_2 < r^{1/\lambda},$$

so $B_1(a,r) \subseteq B_2(a,r^{1/\lambda})$ hence it will also be an open ball with respect to $|\cdot|_2$. By the same logic, it is easy to see, that we can conclude that $B_1(a,r) = B_2(a,r^{1/\lambda})$.

□

Our goal is of course to characterize the absolute values on $\mathbb{Q}$. In order to do so, this next Proposition will be very useful.

Proposition 4.6. ([Kat] Prop. 1.14) *An absolute value, $|\cdot|$, on $\mathbb{Q}$ is non-Archimedean if and only if $|n| \leq 1$ for all integers n.*

Proof. First assume $|\cdot|$ is a non-archimedean norm on $\mathbb{Q}$. We want to inductively prove that $|n| \leq 1$ for all $n \in \mathbb{Z}$. Since $|\pm 1| = 1 \leq 1$ is clear, assume $|n| \leq 1$ for some $n \in \mathbb{N}$. Then, by the ultra metric inequality,

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

so $|n| \leq 1$ for natural n. If $n = 0$ the inquality is clear. To cover the negative integers, let $m \in \mathbb{Z}_-$. Then $|m| = |-1||m| = |-m| \leq 1$, by the proof for positive integers, proving the one implication.

Assume $|n| \leq 1$ for all $n \in \mathbb{Z}$. We want to prove that $|x+y| \leq \max\{|x|, |y|\}$ for all $x, y \in \mathbb{Q}$. Assume $x, y \neq 0$, since it follows that if $y = 0$, then $|x+0| = |x| \leq \max\{|x|, 0\}$. Note that it is sufficient to show that $|x+1| \leq \max\{|x|, y\}$. This is the case since, if $|\cdot|$ is archimedean and if $|x| \leq |y|$, then $|\frac{x}{y}| \leq 1$ and

$$|x+y| = |y||\frac{x}{y} + 1| \leq |y| \cdot 1 = \max\{|x|, |y|\}.$$

Correspondingly, this is the case for $|y| \leq |x|$.
Let $m \in \mathbb{N}$ and x be a non-zero rational number. Then we have

$$\begin{aligned} |x+1|^m = |\sum_{k=0}^{m} \binom{m}{k} x^k| &\leq \sum_{k=0}^{m} |\binom{m}{k} x^k| \\ &\leq \sum_{k=0}^{m} |x|^k \qquad (i) \\ &\leq (m+1)\max\{|x|^m, 1\}, \qquad (ii) \end{aligned}$$

where (i) follows since $\binom{m}{k}$ is an integer, and thus $|\binom{m}{k}| \leq 1$ by assumption. To argue (ii), first look at the case where $|x| \leq 1$. It follows that $|x|^k \leq 1$ for all $0 \leq k \leq m$, so

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

Now if $|x|^k > 1$, then $|x|^k \leq |x|^m$ for $0 \leq k \leq m$, so

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

We can now take the m'th root of our inequality, so

$$|x+1| \leq \sqrt[m]{(m+1)} \max\{|x|, 1\}.$$

This yields the desired inequality. Indeed, since m was chosen arbitrarily, we can take the limit

$$|x+1| \leq \lim_{m \to \infty} \sqrt[m]{(m+1)} \max\{|x|, 1\} = \max\{|x|, 1\}.$$

□

This next proof is based on Theorem 3.1.3 in [Gou].

Theorem 4.7. (Ostrowski's Theorem) Let $|\cdot|$ be a non-trivial absolute value on $\mathbb{Q}$. Then $|\cdot|$ is equivalent to either $|\cdot|_\infty$ or $|\cdot|_p$ for some p.

Proof. We will show for the two cases where $|\cdot|$ is either Archimedean or non-Archimedean.

Case 1: Assume $|\cdot|$ is non-Archimedean. By Proposition 4.6, $|n| \leq 1$ for all $n \in \mathbb{Z}$. Since the absolute value is assumed to be nontrivial, we can find n_0 such that $|n_0| < 1$, and we choose the smallest of such.

Notice, it is sufficient to look for $n_0 \in \mathbb{N}$, since $|x| = |-x|$ for any absolute value on $\mathbb{Q}$.
Our goal now is to show that n_0 is a prime number. With $n = p_0^{r_0} p_1^{r_1} \cdots p_m^{r_m}$, with $r_i \in \mathbb{N}_{>0}$, we must have for some i a p_i such that $|p_i| < 1$, call this prime number p. Assume, for contradiction, q is another prime with $|q| < 1$. Find $k \in \mathbb{N}$ such that $|p^k|, |q^k| < \frac{1}{2}$. Also, by the Euclidean algorithm, we can find $s, t \in \mathbb{Z}$ so $sp^k + tq^k = 1$. Combining this we get

$$1 = |sp^k + tq^k| \leq max\{|sp^k|, |tq^k|\}.$$

Without loss of generality, let $|tq^k| \leq |sp^k|$,

$$max\{|sp^k|, |tq^k|\} = |sp^k| = |s||p^k| < \frac{1}{2}, \qquad \lightning$$

since $|s| \leq 1$. This shows that p is the only prime with $|p| < 1$. Since n_0 was chosen to be the smallest, then it can't be a power of p, so $n_0 = p$. We want to show that $|\cdot|$ is equivalent to $|\cdot|_p$ with the just found p.
We now want to show that for any $n \in \mathbb{Z}$ where $p \nmid n$, then $|n| = 1$. Since p doesn't divide n we will have a remainder when dividing, so write

$$n = qp + r, \qquad 1 \leq r \leq p-1.$$

Since $r < p$, we must have $|r| \geq 1$ since p is the smallest integer with absolute value strictly less than 1. Thus $|r| = 1$, since r is an integer. We also have $|qp| = |q||p| < 1$. Using (prop. 2.3.3 [Gou]), it then

follows that $|n| = |qp + r| = max\{|qp|, |r|\} = 1$.

We are now ready to show the equivalence. Let $n \in \mathbb{Z}$ and write $n = p^v n'$ where $p \nmid n'$, then

$$|n| = |p^v||n'| = |p|^v = c^{-v} = (p^a)^{-v} = (p^{-v})^a = |n|_p^a$$

where $0 < c^{-1} := |p| < 1$. Then $c > 1$, and so we can find some $a \in \mathbb{R}$, $a > 0$ such that $c = p^a$. So the absolute value also depends on p-powers up to a power, which shows the equivalence by 4.5. So any Archimedean absolute value is equivalent to the p-adic absolute value for some p.

Case 2: Suppose $|\cdot|$ is Archimedean. We want to show, that the absolute value is then equivalent to the usual absolute value, $|\cdot|_\infty$. Since $|\cdot|$ is Archimedean we can again by proposition 4.6 find a smallest positive integer n_0 such that $|n_0| > 1$ and again write $|n_0| = n_0^\alpha$, for $\alpha = \frac{\ln|n_0|}{\ln n_0} \in \mathbb{R}_+$. Since absolute values work nicely with multiplication, and $|-1| = 1$, it will be enough to show the equivalence for all positive integers (not just n_0 ☺).
Let n be an arbitrary positive integer, and write it in base n_0,

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + \cdots + a_k n_0^k, \qquad a_k \neq 0, \;\; 0 \leq a_i < n_o \text{ for } i = 0, 1, ..., k. \tag{4}$$

Taking the absolute value, we get

$$|n| \leq |a_o| + |a_1 n_0| + |a_2 n_0^2| + \cdots + |a_k n_0^k| = |a_0| + |a_1|n_0^\alpha + |a_2|n_0^{2\alpha} + \cdots + |a_k|n_0^{k\alpha}.$$

With all the coefficients being less that n_0, and the way n_0 was chosen, this forces $|a_i| \leq 1$, so

$$\begin{aligned}
|n| &\leq 1 + n_0^\alpha + n_0^{2\alpha} + \cdots + n_0^{k\alpha} \\
&= n_0^{k\alpha}(1 + n_0^{-\alpha} + n_0^{-2\alpha} + \cdots + n_0^{-ka}) \\
&\leq n_0^{k\alpha} \sum_{i=0}^{\infty} (\frac{1}{n_0^\alpha})^i \\
&= n_0^{k\alpha}(\frac{1}{1 - \frac{1}{n_0^\alpha}}) = n_0^{k\alpha}(\frac{n_0^\alpha}{n_0^\alpha - 1}),
\end{aligned}$$

since $0 < \frac{1}{n_0^\alpha} < 1$. Notice that the series is independent of choice of n, so we will call it $C := \frac{n_0^\alpha}{n_0^\alpha - 1}$. So we have shown $|n| \leq C n_0^{k\alpha} \leq C n^\alpha$ because $n_0^k \leq n$. Since this applies to any positive integer, we use it for the positive integer n^N,

$$|n^N| \leq C n^{\alpha N} \quad \Rightarrow \quad |n| \leq \sqrt[N]{C}\, n^\alpha.$$

Now, since we could choose any N, for a fixed n, we will let $N \to \infty$, and so we obtain

$$|n| \leq n^\alpha, \tag{5}$$

showing (only) inequality.
To gain equality we will look at the n_0 expansion, from equation (2) for some positive integer n, and note that $n_0^{k+1} > n \geq n_0^k$ which implies that:

$$n_0^{\alpha(k+1)} = |n_0^{k+1}| = |n + n_0^{k+1} - n| \leq |n| + |n_0^{k+1} - n|.$$

Using the previously achieved formula (5), we get $|n_0^{k+1} - n| \leq (n_0^{k+1} - n)^\alpha$, so $n_0^{\alpha(k+1)} - (n_0^{k+1} - n)^\alpha \leq |n|$. Our goal is to find a lower bound for $|n|$ given by $C' n^\alpha$, where C' once again doesn't depend on n,

so we can apply the smart trick of using inequality on n^N.

$$\begin{aligned}
|n| &\geq n_0^{\alpha(k+1)} - (n_0^{k+1} - n)^\alpha \\
&\geq n_0^{\alpha(k+1)} - (n_0^{k+1} - n_0^k)^\alpha, && n \geq n_0^k \\
&= n_0^{\alpha(k+1)} - n_0^{\alpha k}(n_0 - 1)^\alpha = n_0^{\alpha(k+1)}(1 - (\frac{n_0 - 1}{n_0})^\alpha) \\
&= n_0^{\alpha(k+1)}(1 - (1 - \frac{1}{n_0})^\alpha) \\
&= C' n_0^{\alpha(k+1)} \\
&\geq C' n^\alpha, && n_0^{k+1} > n,
\end{aligned}$$

showing $|n| \geq C' n^\alpha$ where $C' \coloneqq 1 - (\frac{n_0 - 1}{n_0})^\alpha > 0$ doesn't depend on n, so we can use the inequality on n^N and take the limit, like we did showing the other inequality,

$$C' n^{N\alpha} \leq |n|^N \quad \Rightarrow \quad \sqrt[N]{C'}\, n^\alpha \leq |n|,$$

where $\lim_{N\to\infty} \sqrt[N]{C'}$, so $n^\alpha \leq |n|$.
Thus we have shown that $|n| = n^\alpha = |n|_\infty^\alpha$. So, any Archimedean absolute value is equivalent to the absolute value $|\cdot|_\infty$ by Lemma 4.5.

□

5 Hensel's Lemma

Of course there are differences between $\mathbb{Z}$ and $\mathbb{Z}_p$. We have already seen in Proposition 2.7 that $\mathbb{Z}_p$ forms a subring of $\mathbb{Q}_p$. Interestingly, $\mathbb{Z}_p$ retains many of the algebraic properties familiar from $\mathbb{Z}$, such as being an integral domain with well-behaved ideals and a form of unique factorization. In this chapter, we focus on the problem of finding roots of polynomials over $\mathbb{Z}_p$. A central result in this context is *Hensel's Lemma*, which allows us to lift solutions modulo p to genuine p-adic roots. We will present the lemma, prove it, and explore some of its important consequences. The Proof of Hensel's Lemma is based on Theorem 3.4.1 in [Gou].

Theorem 5.1. (Hensel's Lemma) Let $F(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ be a polynomial with coefficiants in $\mathbb{Z}_p$ and let $F'(X) = a_1 + 2a_2X + \cdots + na_nX^{n-1}$ be its derivative. Assume $\alpha_1 \in \mathbb{Z}_p$ satisfies

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

Then there exists a unique p-adic integer $\alpha \in \mathbb{Z}_p$ such that $F(\alpha) = 0$ and $\alpha \equiv \alpha_1 \pmod{p}$.

Proof. The idea of the proof is to construct some $\alpha \in \mathbb{Z}_p$ such that $F(\alpha) \equiv 0 \pmod{p^n}$, for all $n \in \mathbb{N}$, which forces $F(\alpha) = 0$. This is intuitively clear if we imagine the p-adic expansion of $F(\alpha)$. We will do this by constructing a sequence $(\alpha_n)_n \subset \mathbb{Z}_p$ having the following properties:

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

Moreover, in construction of the sequence $(\alpha_n)_n$, we will see that we can claim uniqueness. In addition, this procedure should yield that the sequence (α_n) has a limit $\alpha \in \mathbb{Z}_p$. Then we will use $|F(\alpha)|_p \leq \frac{1}{p^n}$ to show that $F(\alpha) = 0$ and $\alpha \equiv \alpha_1 \pmod{p^n}$ by construction. Thus α is a root of $F(X)$ with the desired properties.

We will be creating the sequence inductively. Since our assumption gives us α_1, we need to use this to create α_2. For this we want to use the Taylor expansion identity. First, see that for $f \in \mathbb{Z}_p[X]$ given by $f(X) = \sum_{i=0}^{d} c_iX^i$ and using the binomial theorem, we get

$$f(X+Y) = \sum_{i=0}^{d} c_i(X+Y)^i = \sum_{i=0}^{d} c_i \sum_{j=0}^{d} \binom{i}{j} X^{i-j}Y^j.$$

When $j = 0$ we obtain $\sum_{i=0}^{d} c_iX^i = f(X)$. When $j = 1$ we obtain

$$\sum_{i=0}^{d} c_i \binom{i}{1} X^{i-1}Y = \sum_{i=1}^{d} c_i i X^{i-1}Y = f'(X)Y.$$

When $j \geq 2$ the terms have order at least Y^2.
Since we want to have $\alpha_1 \equiv \alpha_2 \pmod{p}$, let $\alpha_2 = \alpha_1 + b_1p$ for some $b_1 \in \mathbb{Z}_p$.Thus setting $X = \alpha_1$ and $Y = b_1p$

$$\begin{aligned} F(\alpha_2) &= F(\alpha_1 + b_1p) \\ &= F(\alpha_1) + F'(\alpha_1)b_1p + p^2(\cdots) \\ &\equiv F(\alpha_1) + F'(\alpha_1)b_1p \pmod{p^2}. \end{aligned}$$

Our goal now is to find b_1 such that $F(\alpha_2) \equiv 0 \pmod{p^2}$. Note that since $F(\alpha_1) \equiv 0 \pmod{p}$ this implies $F(\alpha_1) = c_1p$ for some $c \in \mathbb{Z}_p$. We will use this to find b_1 such that (i) holds for α_2:

$$\begin{aligned} & c_1p + F'(\alpha_1)b_1p = F(\alpha_1) + F'(\alpha_1)b_1p = F(\alpha_2) \equiv 0 \pmod{p^2} \\ \Leftrightarrow \quad & c_1 + F'(\alpha_1)b_1 \equiv 0 \pmod{p}. \end{aligned}$$

By assumption $b_1F'(\alpha_1) \equiv -c_1 \not\equiv 0 \pmod{p}$ and $p \nmid F'(\alpha_1)$, so $F'(\alpha_1)$ has an inverse in $\mathbb{Z}_p$, since it is different from 0, and $\mathbb{Z}_p$ is a subring. Thus

$$b_1 \equiv -c_1(F'(\alpha_1))^{-1} \pmod{p},$$

and by construction we can choose b_1 uniquely in $\mathbb{Z}$ with $0 \leq b_1 < p$. With this b_1 we have constructed α_2 for which (i) and (ii) holds. To be able to inductively deduce the sequence $\{\alpha_n\}$, we need to check that the derivative $F'(\alpha_2)$ remains different from 0 modulo p:

$$F'(\alpha_2) = F'(\alpha_1) + b_1pF''(\alpha_1) + \cdots \equiv F'(\alpha_1) \not\equiv 0 \pmod{p}.$$

As an induction step for $n > 2$, we can easily show the desired construction with the same calculations for α_{n+1} using α_n. Hence we have created a sequence $\{\alpha_n\}$ with a lot of very nice properties. Note that this sequence is Cauchy, since for any $m > n$

$$\alpha_n \equiv \alpha_m \pmod{p^n} \quad \Rightarrow \quad |\alpha_n - \alpha_m|_p \leq \frac{1}{p^n}.$$

Setting $\alpha := \lim_{n\to\infty} \alpha_n$ we see that this fulfills the wanted properties in the theorem, since the previous calculation using $n = 1$ and taking the limit of m gives us $\alpha_1 \equiv \alpha \pmod{p}$. Now since $\alpha \equiv \alpha_n \pmod{p^n}$ we know that $\alpha = \alpha_n + p^n b_n$ for suitable b_n, yielding

$$F(\alpha) = F(\alpha_n) + F'(\alpha_n)b_np^n + p^{n+1}(\cdots) \equiv 0 \pmod{p^n},$$

so for all n we get

$$|F(\alpha)|_p \leq \frac{1}{p^n} \quad \Rightarrow \quad |F(\alpha)|_p = 0 \quad \Rightarrow \quad F(\alpha) = 0.$$

□

This next Theorem is another version of Hensel's Lemma, which we will state without proof, since it will be used later in the topic of finite field extensions. A proof can be found in [Gou] page 74.

Theorem 5.2. (Hensel's Lemma, Second Form)
Let $f(X) \in \mathbb{Z}_p[X]$. If there exists polynomials $g_1(X), h_1(X) \in \mathbb{Z}_p[X]$ such that:

- (i) $g_1(X)$ is monic,
- (ii) $g_1(X)$ and $h_1(X)$ are relatively prime modulo p,
- (iii) and $f(X) \equiv g_1(X)h_1(X) \pmod{p}$.

Then there exists polynomials $g(X), h(X) \in \mathbb{Z}_p[X]$ such that:

- (i) $g(X)$ is monic,
- (ii) $g(X) \equiv g_1(X) \pmod{p}$ and $h(X) \equiv h_1(X) \pmod{p}$ and
- (iii) $f(X) = g(X)h(X)$.

5.1 Roots of unity

First we will use Hensel's Lemma on the polynomial $F(X) = X^m - 1$ to look for m'th roots of unity, where $m \in \mathbb{N}$. An element $x \in \mathbb{Q}_p$ is called a root of unity if there is some $m \in \mathbb{N}$ such that $x^m = 1$.

Let us first give some thoughts on the units of $\mathbb{Z}_p$ which we denote by $\mathbb{Z}_p^*$, i.e. $x \in \mathbb{Z}_p$ is called a unit of $\mathbb{Z}_p$ if there is $y \in \mathbb{Z}_p$ with $xy = 1$. Let $x \in \mathbb{Z}_p$ be given by $x = p^r l$, where $r \in \mathbb{N}$, $l \in \mathbb{Z}_p \backslash p\mathbb{Z}_p$ and $p \nmid l$. By definition $x \in \mathbb{Z}_p^*$ if and only if $\frac{1}{x} \in \mathbb{Z}_p^*$, so

$$\frac{1}{p^r} = |x|_p \leq 1 \text{ and } 1 \geq |\frac{1}{x}|_p = p^r,$$

yielding $\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p : \exists y \in \mathbb{Z}_p \text{ with } xy = 1\} = \{x \in \mathbb{Z}_p : |x|_p = 1\}$. It is also useful to be aware that if $\xi \in \mathbb{Q}_p$ is an m'th root of unity, then $1 = |\xi^m|_p = \frac{1}{p^{km}}$, for some $k \in \mathbb{Z}$, implying that $k = 0$, so $\xi \in \mathbb{Z}_p^*$.

Corollary 5.3. ([Rob] p. 51) *For $p > 2$ the set of roots of unity in $\mathbb{Q}_p$ is a subgroup of $(\mathbb{Z}_p^*, \cdot)$. Furthermore the set of $(p-1)$-roots of unity in $\mathbb{Q}_p$ is a cyclic group of order $p-1$.*

Proof. To be clear, we know $(\mathbb{Z}_p^*, \cdot)$ is an (abelian) group since $\mathbb{Q}_p$ is a field. Knowing that roots of unity lie in $\mathbb{Z}_p^*$, it is then quick to show that the set of roots of unity in $\mathbb{Q}_p$ form a group with multiplication.
Next we will show that $\mathbb{Z}_p$ has $p-1$ distinct $(p-1)$'th roots of unity.
Look at the polynomial $f(X) = X^{p-1} - 1 \in \mathbb{Q}_p$. We know f has at most $p-1$ roots, since $\mathbb{Q}_p$ is a field. Let $1 \leq a < p$. Since $p \nmid a$ we can use Fermat's little theorem, $a^p \equiv a \pmod{p}$, to get

$$f(a) = a^{p-1} - 1 \equiv 0 \pmod{p} \quad \text{and} \quad f'(a) = (p-1)a^{p-2} \not\equiv 0 \pmod{p}.$$

Using Hensel's Lemma (first version) we can conclude, that there is a unique $(p-1)$-root in $\mathbb{Z}_p$ for every $a = 1, ..., p-1$.
By Gauss (Thm. 4.5.3 in [Lau]), since $\mathbb{Q}_p$ is a field and the group of $(p-1)$-roots in $\mathbb{Q}_p$ is a finite subgroup of $\mathbb{Z}_p^*$, then the group of $(p-1)$-roots of unity is cyclic. □

5.2 Local to Global

The fields $\mathbb{R}$ and $\mathbb{Q}_p$ are completions of $\mathbb{Q}$ with respect to the Archimedean and p-adic absolute values, respectively. Although each of these completions gives valuable local information, we are often interested in whether local information can determine global properties. This is the essence of the *local-to-global principle* (or Hasse principle).

Both $\mathbb{R}$ and $\mathbb{Q}_p$ are not algebraically closed. For example, consider the polynomial $f(X) = X^2 - p$ for some prime $p > 2$. This equation has no root in $\mathbb{Q}_p$, as can be seen from the fact that if $\alpha^2 = p$, then $|\alpha|_p^2 = \frac{1}{p}$, and hence $|\alpha|_p = \frac{1}{\sqrt{p}}$, which is not a valid p-adic norm since $1/2 \notin \mathbb{Z}$. Later we will extend $\mathbb{Q}_p$, so such elements are well defined.

However, even though individual completions may lack some algebraic properties, collectively they can determine important arithmetic information about $\mathbb{Q}$. The following result illustrates this:

Proposition 5.4. ([Gou] Prop. 3.5.1) *$x \in \mathbb{Q}$ is a square if and only if it is a square in every $\mathbb{Q}_p$ for $p \leq \infty$.*

Proof. Assume $x \in \mathbb{Q}$ is a square in $\mathbb{Q}_p$ for every $p \leq \infty$. Since $\mathbb{Q} \subset \mathbb{Q}_\infty := \mathbb{R}$, and x a square in $\mathbb{R}$, it follows that x is positive, but not necessarily a square in $\mathbb{Q}$. So write $x = \prod_{p \text{ prime}} p^{ord_p(x)} \in \mathbb{Q}$. Then since x is a square in $\mathbb{Q}_p$, for every p, we deduce that $ord_p(x)$ must be even or zero, for every prime p. And so x is a square in $\mathbb{Q}$ as well.
Now assume $x \in \mathbb{Q}$ is a square in $\mathbb{Q}$. This means that we can find some $k \in \mathbb{Q}$ such that $x = k^2$. Then $k = \pm \prod_{p \text{ prime}} p^{ord_p(k)} \in \mathbb{Q} \subseteq \mathbb{Q}_p$ for any p. This implies that $k^2 = x \in \mathbb{Q}_p$ is a square for all primes p. □

6 Finite Extensions of $\mathbb{Q}_p$

We have seen $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ similarly to $\mathbb{R}$. Since they share common properties, we are led to ask what the analogue to $\mathbb{C}$, an algebraically closed and complete field, is for $\mathbb{Q}_p$. This turns out to be a bit more fiddly than in $\mathbb{R}$, where adding i is sufficient.

In contrast to $\mathbb{R}$, which only has the algebraic extension $\mathbb{C}$, it turns out that $\mathbb{Q}_p$ has algebraic extensions of degree n for every n ([Sal, page 22]), we will only look at finite extensions of $\mathbb{Q}_p$ that are of degree 2. Thus, we shall look at extensions of the form $\mathbb{Q}_p(\sqrt{d})$, where $d \in \mathbb{Q}_p$ is not a square root in $\mathbb{Q}_p$.
The following definitions are from [Moy].

Definition 6.1. Let F be a field and K be a vector space over F. If K is moreover a field, thus containing the subfield F, we call K a *field extension* of F, and this is denoted by K/F. The *degree* of the field extension K/F is denoted by $[K : F]$ and is defined as the dimension of the vector space K over F. If $[K : F]$ is finite, then the extension is said to be *finite*, and it is called *infinite* if otherwise.

We will be interested in finite field extensions K of $\mathbb{Q}_p$. We will be extending $\mathbb{Q}_p$ by using irreducible polynomials, as defined in the next theorem, which will be stated without proof.

Theorem 6.2. Let F be a field and $q(X) \in F[X]$ an irreducible polynomial. Let K be a field extension containing a root α of $q(X)$, so $q(\alpha) = 0$. Let $F(\alpha)$ be the subfield of K generated by α over F, i.e. the smallest subfield of K containing F and α. Then

$$F(\alpha) \cong F[X]/q(X).$$

For the proof, see Theorem 3.19 in [Moy].

Definition 6.3. A field extension K/F is said to be *algebraic*, if every element $\alpha \in K$ is a root of a non-zero polynomial $q[X] \in F[X]$.

We still want to consider the absolute values on the field extensions of $\mathbb{Q}_p$. We will require that such an absolute value extends $|\cdot|_p$. Let K be a finite algebraic extension of $\mathbb{Q}_p$ of degree n, then by definition, K is an n-dimensional vector space over $\mathbb{Q}_p$, so $K \cong \mathbb{Q}_p^n$. We can identify elements $x \in \mathbb{Q}_p$ with $x = (r_1, r_2, ..., r_n)$ with $r_i \in \mathbb{Q}_p$.
Let $a \in K$ and define the linear map $\varphi_a : \mathbb{Q}_p^n \to \mathbb{Q}_p^n$ given by $x \mapsto ax$. Now, choosing a basis B_1 for $\mathbb{Q}_p^n$ we represent the linear map as a matrix $\mathcal{M}_a^{B_1} \in \mathrm{Mat}_n(\mathbb{Q}_p)$, so $\varphi_a = \mathcal{M}_a^{B_1}$. Define a map $\mathrm{Norm}_K : K \to \mathbb{Q}_p$ by $a \mapsto \det(\varphi_a)$. We see that this map is independent of choice of basis, i.e. if we take another basis B_2 for $\mathbb{Q}_p$, so $\varphi_a = \mathcal{M}_a^{B_2}$, we know we can find a coordinate transformation matrix A such that $\mathcal{M}_a^{B_1} = A\mathcal{M}_a^{B_2}A^{-1}$, (see Corollary 8.18 in [Tho]). Using the multiplicativity of the determinant, we see that

$$\det(\mathcal{M}_a^{B_1}) = \det(A\mathcal{M}_a^{B_2}A^{-1}) = \det(A)\det(\mathcal{M}_a^{B_2})\det(A^{-1}) = \det(\mathcal{M}_a^{B_2}).$$

Note that for an element $\alpha \in K$, the determinant $\det(\varphi_\alpha)$ lies in $\mathbb{Q}_p$.
We define the absolute value $|\cdot|_K$ on K as following:

$$|a|_K := \sqrt[n]{|\det(\varphi_a)|_p}.$$

This extends $|\cdot|_p$, since for $x \in \mathbb{Q}_p$, the matrix φ_x is a diagonal $n \times n$ matrix with x in each non-zero entry, and thus $|x|_K = \sqrt[n]{|\det(\varphi_x)|_p} = \sqrt[n]{|x^n|_p} = |x|_p$ (see [Sal, page 23]).

Theorem 6.4. Let $K/\mathbb{Q}_p$ be an n-dimensional field extension. The function $|\cdot|_K\colon K \to \mathbb{R}_+$ defined by

$$|x|_K = \sqrt[n]{|\det(\varphi_x)|_p}$$

is a non-Archimedean absolute value over K.

Proof. This proof is based on the proof of Thm. 5.3.5 in [Gou]. Let $x \in K$. By the construction of $|\cdot|_K$ we get $|x|_K \geq 0$, since $\det(\varphi_x)$ is a map into $\mathbb{Q}_p$, and $|\cdot|_p$ is a norm.
For definiteness, first assume $x = 0$. Then φ_0 is the zero-linear map, and the matrix representation is thus the zero-matrix, so $\det(\varphi_0) = 0$, and thus $|0|_K = 0$. Now assume $x \neq 0$ with $|x|_K = 0$, and we want to show this is not possible. Indeed,

$$\sqrt[n]{|\det(\varphi_x)|_p} = 0 \quad \Rightarrow \quad |\det(\varphi_x)|_p = 0 \quad \Rightarrow \quad \det(\varphi_x) = 0 \quad \Rightarrow \quad \varphi_x \notin GL(\mathbb{Q}_p).$$

Since φ_x isn't invertible, it's kernel is non trivial, so there must exist a $t \in K$ with $t \neq 0$ such that the linear transformation $\varphi_x(t) = xt = 0$. But since K is a field, we can conclude that this is the case only of $x = 0$.
Again, by construction, it is clear that multiplicativity holds, since $\varphi_{xy}(z) = xyz = x\varphi_y(z) = (\varphi_x \circ \varphi_y)(z)$ and so

$$\det(\varphi_{xy}) = \det(\varphi_x\varphi_y) = \det(\varphi_x)\det(\varphi_y).$$

Finally, we must prove the non-Archimedean inequality. Unfortunately, this is not a trivial claim, and we will need to take some algebraic results for granted.
We can assume that that $x, y \in K$ are non-zero elements, since this case is trivial. As in the proof of Proposition 4.6, it is sufficient to prove that

$$|x+1|_K \leq \max\{|x|_K, 1\}. \tag{6}$$

This will follow from

$$|x|_K \leq 1 \Rightarrow |x-1|_K \leq 1. \tag{$\star$}$$

First, we see that ($\star$) is sufficient. Assume the implication is true, then

$$|x|_K = |-x|_K \leq 1 \quad \Longrightarrow \quad |-x-1|_K = |x+1|_K \leq 1 = \max\{|x|, 1\}.$$

If $|x|_K \leq 1$, then (6) holds. If $|x|_K > 1$, then

$$|\frac{1}{x}|_K < 1 \quad \overset{(\star)}{\Longrightarrow} \quad |\frac{1}{x}+1|_K = |\frac{x+1}{x}|_K \leq 1 \quad \Longrightarrow \quad |x+1|_K \leq |x| = \max\{|x|, 1\},$$

as wanted. So it is sufficient to show that ($\star$) hold for all $x \in K$.

Let $x \in K$ with $|x|_K \leq 1$. This is the case when $|\det(\varphi_x)|_p \leq 1$, hence we need to show

$$|\det(\varphi_x)|_p \leq 1 \quad \Longrightarrow \quad |\det(\varphi_{x-1})|_p \leq 1,$$

or, in other words,

$$\det(\varphi_x) \in \mathbb{Z}_p \quad \Longrightarrow \quad \det(\varphi_{x-1}) \in \mathbb{Z}_p.$$

The norm can be defined in many ways, and for this proof the following definition will be useful: x has a minimal polynomial f with coefficients in $\mathbb{Q}_p$ such that

$$f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0, \quad \text{with } f(x) = 0,$$

then the norm is defined to be

$$\det(\varphi_x) = (-1)^{mr} a_o^r,$$

where $[K : \mathbb{Q}_p] = n$, $[K : \mathbb{Q}_p(x)] = r$ and $n = mr$. With this definition we get

$$\det(\varphi_x) = (-1)^n a_0^r \in \mathbb{Z}_p \quad \Rightarrow \quad a_0 \in \mathbb{Z}_p.$$

Our goal is, of course, to show that it then follows, that the corresponding coefficient, from the minimal polynomial with $x - 1$ as a root, also lies in $\mathbb{Z}_p$.

Since $\mathbb{Q}_p(x) = \mathbb{Q}_p(x-1)$, the minimal polynomial for $x - 1$ clearly is

$$g(X) := f(X+1) = X^m + (1 + a_{m-1})X^{m-1} + \cdots + (1 + a_{n-1} + \cdots + a_1 + a_0),$$

so we need to show that $1 + a_m - 1 + \cdots + a_1 + a_0 \in \mathbb{Z}_p$, or equivalently, that all of the coefficients lie in $\mathbb{Z}_p$.

To show this, we will prove it more generally for any monic, irreducible polynomial $F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ with coefficients in $\mathbb{Q}_p$ and $a_0 \in \mathbb{Z}_p$, that then all coefficients must lie in $\mathbb{Z}_p$. For this, we will use the second form of Hensel's Lemma, Theorem 5.2, to prove by contradiction, that if some coefficients do not lie in $\mathbb{Z}_p$, then F must be reducible.
Assume some $a_i \notin \mathbb{Z}_p$. Choose the smallest m such that $p^m a_i \in \mathbb{Z}_p$ for all non p-adic integers a_i. Define

$$G(X) = p^m F(X) = b_n X^n + \cdots b_1 X + b_0, \quad b_i = p^m a_i.$$

Since F is monic and $a_0 \in \mathbb{Z}_p$, we know that $b_n = p^m$ and $b_0 = p^m a_0$ are divisible by p. Since m was chosen to be the smallest power such that $p^m a_i \in \mathbb{Z}_p$ for all i, then at least one term is not divisible by p. Set k to be the smallest i such that p does not divide b_i. Then

$$G(X) \equiv (b_n X^{n-k} + \cdots + b_k)X^k \pmod{p},$$

where the factors X^k and $b_n X^{n-k} + \cdots + b_k$ are relatively prime, since no divisor of X^k will divide b_k, since $b_k \not\equiv 0 \pmod{p}$. Then by the second form of Hensel's Lemma, Theorem 5.2, $G(X) = p^m F(X)$ is irreducible, which is a contradiction to $F(X)$ being irreducible. Hence if we have a minimal polynomial with coefficients in $\mathbb{Q}_p$ and $a_0 \in \mathbb{Z}_p$, then all coefficients must belong to $\mathbb{Z}_p$.

Hence, we can conclude, that $\det(\varphi_{x-1}) = (-1)^n(1 + a_{m-1} + \cdots + a_0) \in \mathbb{Z}_p$, since all coefficients of the minimal polynomial f for x must lie in $\mathbb{Z}_p$. We have now shown that $|\cdot|_K$ is a non-Archimedean absolute value over K. □

6.1 Quadratic extensions

In order to study the quadratic extensions of $\mathbb{Q}_p$, we will first need to decompose $\mathbb{Q}_p^* = \mathbb{Q}_p \backslash \{0\}$. We already know that we can represent $x \in \mathbb{Q}_P^*$ as $x = p^k u$, with $u \in U = \{y \in \mathbb{Q}_p : |y|_p = 1\}$, and $k \in \mathbb{Z}$, so $\mathbb{Q}_p^* \cong p^{\mathbb{Z}} U$. For further decomposition, see that for $u \in U$, $u = a_0 + a_1 p + \cdots = a_0(1 + \frac{a_1}{a_0} p + \cdots)$, so

$$U = \{1, \ldots, p-1\} \times (1 + p\mathbb{Z}_p),$$

so we denote $U_1 := \{1 + p\mathbb{Z}_p\}$. We can also see the decomposition as $\mathbb{Q}_p^* \cong p^{\mathbb{Z}} \times \mathbb{F}_p^* \times U_1$, where $\mathbb{F}_p^*$ is a cyclic group of order $p - 1$.
This section is based on [Sal, Chapter 3].

Proposition 6.5. *If p is odd, then $U_1^2 = U_1$*

Proof. To show $U_1^2 \subset U_1$, let $x \in U_1^2$. We can write x in the form $x = (1+u)^2 = 1 + u^2 + 2u$ with $u \in p\mathbb{Z}_p$, where $u^2 + 2u = u(u+2) \in p\mathbb{Z}_p$ since $p\mathbb{Z}_p$ is an ideal by Proposition 3.6. Thus $U_1^2 \subset U_1$.
Now to show the other inclusion, let $\alpha \in U_1$. We wish to find $\beta \in U_1$ such that $\beta^2 = \alpha$, or, in other words, we wish to find a root of the polynomial $f(X) = X^2 - \alpha$. We will not use Hensel's Lemma directly, but instead apply the p-adic analogue of Newton's method. Define a sequence $(a_n)_{n\in\mathbb{N}_0}$ by setting $a_0 = 1 \in U_1$ and $a_{i+1} = a_i - \frac{f(a_i)}{f'(a_i)}$, where our goal is to inductively show that this sequence converges to a root whilst still being in U_1.
Since $\alpha \in U_1$, write $\alpha = 1 + pu$ with $u \in \mathbb{Z}_p$. Now see that $a_2 = 1 - \frac{1^2-\alpha}{2} = 1 - \frac{1-(1-pu)}{2} = 1 - \frac{pu}{2}$, where $-\frac{pu}{2} \in p\mathbb{Z}_p$ since p is odd, so $a_2 \in U_1$.
Now assume $a_n \in U_1$, so $a_n = 1 + pu_n$ with $u_n \in \mathbb{Z}_p$. So $|a_n|_p = 1$ and $f'(a_n) = 2a_n$ is a unit, since p is odd. Then, looking at the denominator,

$$f(a_n) = a_n^2 - \alpha = (1 + p^2u_n^2 + 2pu_n) - (1 + pu) = p(2u_n - u + pu_n^2) \in p\mathbb{Z}_p,$$

hence we get that the fraction $\frac{f(a_n)}{f'(a_n)}$ is something in $p\mathbb{Z}_p$ divided by the unit $f'(a_n) = 2a_n$. So the whole fraction $\frac{a_n^2-\alpha}{2a_n} \in p\mathbb{Z}_p$. Now $a_{n+1} = a_n - \frac{f(a_n)}{a_n} = (1 + \text{something in } p\mathbb{Z}_p) - \text{something in } p\mathbb{Z}_p \in U_1$.
The sequence (a_n) is Cauchy, since Newton's Method has a quadratic convergence. This can be seen by taking the Taylor expansion as in the proof for Hensel's lemma. Thus, if $|f(a_n)|_p = |a_n^2 - \alpha|_p \leq \frac{1}{p^k}$ for some $k \in \mathbb{N}$, then $|f(a_{n+1})|_p \leq \frac{1}{p^{2k}}$. So

$$|a_{n+1} - a_n|_p = |-\frac{f(a_n)}{f'(a_n)}|_p \leq \frac{1}{p^k},$$

where $k \to \infty$ when $n \to \infty$. Thus (a_n) is a Cauchy sequence converging to some element β. Since $a_n \in U_1$ for all n and since $U_1 = \{1 + p\mathbb{Z}_p\}$ is closed, the limit $\beta \in U_1$. And, as argued, we know $f(a_n) = a_n^2 - \alpha \underset{n\to\infty}{\longrightarrow} 0$. So by sequential continuity with respect to the p-adic norm, $\beta^2 = \alpha$. Hence we can conclude that all elements in U_1 are squares, i.e. $U_1 = U_1^2$.

□

Since we are looking at quadratic extensions, we are interested in extensions of the form $\mathbb{Q}_p(\sqrt{d})$, where $d \in \mathbb{Q}_p^*\backslash(\mathbb{Q}_p^*)^2$, cf. Theorem 6.2, so d is determined by its class in $\mathbb{Q}_p^*\backslash(\mathbb{Q}_p^*)^2$. Now, with the knowledge of Proposition 6.5, we get that $\mathbb{Q}_p^2 \cong p^{2\mathbb{Z}} \times (\mathbb{F}_p)^2 \times U_1$, where $(\mathbb{F}_p)^2 \subseteq \mathbb{F}_p$. So

$$\mathbb{Q}_p^*\backslash(\mathbb{Q}_p^*)^2 \cong \mathbb{Z}\backslash 2\mathbb{Z} \times \mathbb{F}_p\backslash(\mathbb{F}_p)^2.$$

By [Sal, page 9], $[\mathbb{Q}_p^* : (\mathbb{Q}_p^*)^2] = 4$ when p is odd. Note: the case for $p = 2$ is much more complicated, since $U_1 \neq U_1^2$ yielding $[\mathbb{Q}_p^* : (\mathbb{Q}_p^*)^2] = 8$. We are only interested in non-trivial classes, so we will ignore the class of all squares. Hence for p odd, there are 3 quadratic extensions represented by $\mathbb{Q}_p(\sqrt{p})$, $\mathbb{Q}_p(\sqrt{\epsilon})$ and $\mathbb{Q}_p(\sqrt{\epsilon p})$, where $\epsilon \in \mathbb{Z}_p^*\backslash(\mathbb{Z}_p^*)^2$ is a non-square unit.

Let $q \in \{p, \epsilon, p\epsilon\}$ and consider $\mathbb{Q}_p(\sqrt{q})$. Let us see what the corresponding norm $|\cdot|_{\mathbb{Q}_p(\sqrt{q})}$ looks like. The linear map $\varphi_x : \mathbb{Q}_p(\sqrt{q}) \to \mathbb{Q}_p(\sqrt{q})$ is given by $y \mapsto xy$. In addition, for $x, y \in \mathbb{Q}_p(\sqrt{q})$ we can write $x = x_1 + \sqrt{q}x_2$, $y = y_1 + \sqrt{q}y_2$ with $x_1, x_2, y_1, y_2 \in \mathbb{Q}_p$, and so

$$\varphi_x(y) = xy = (x_1 + \sqrt{q}x_2)(y_1 + \sqrt{q}y_2) = x_1y_1 + qx_2y_2 + \sqrt{q}(x_1y_2 + x_2y_1). \tag{7}$$

We know that $\mathbb{Q}_p(\sqrt{q}) \cong \mathbb{Q}_p \times \mathbb{Q}_p$ since $\mathbb{Q}_p(\sqrt{q})$ is a vector space over $\mathbb{Q}_p$. Using the basis $B = (\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\\sqrt{q}\end{pmatrix})$, we see that the linear map is represented by the matrix $\mathcal{M}_x^B \in \mathrm{Mat}_2(\mathbb{Q}_p)$ given by

$$\mathcal{M}_x^B = \begin{pmatrix} x_1 & qx_2 \\ x_2 & x_1 \end{pmatrix},$$

using equation (7). Thus, following Theorem 6.4, we get

$$|y|_{\mathbb{Q}_p(\sqrt{q})} = \sqrt{|\det(\mathcal{M}_x^B)|_p} = \sqrt{|x_1^2 - qx_2^2|_p} = \sqrt{|x\bar{x}|_p},$$

where $\bar{x} = x_1 - \sqrt{q}x_2$.

Since we, for example, have $\sqrt{p} \in \mathbb{Q}_p(\sqrt{p})$, but $ord_p(\sqrt{p}) = 1/2 \notin \mathbb{Z}$, we are interested in understanding the p-adic ordinal in our extensions field. For this, we introduce the concept of ramification.

Let K be a finite extension of $\mathbb{Q}_p$. Define the following subspaces

$$\mathcal{R} = \{x \in K : |x| \leq 1\}, \quad \mathcal{P} = \{x \in K : |x| < 1\}, \quad \mathcal{O} = \{x \in K : |x| = 1\}$$

The quotient group $k = \mathcal{R}/\mathcal{P}$ is a finite extension of $\mathbb{F}_p$. If $f = [k : \mathbb{F}_p] = \dim_{\mathbb{F}_p}(k)$ then k is isomorphic to $\mathbb{F}_q$ where $q = \#(k) = p^f$. Since $\mathcal{P}$ is an ideal, we can find $\omega \in K$ such that $\mathcal{P} = \langle\omega\rangle$. We call ω the *uniformizer* of $\mathcal{P}$.

Definition 6.6. ([Sal] pages 23-24) The *residue degree* of K of $\mathbb{Q}_p$ is the the integer

$$f = [k : \mathbb{F}_p] = \dim_{\mathbb{F}_p}(k).$$

The *ramification index* of K over $\mathbb{Q}_p$ is the integer $e \geq 1$ such that $p = \omega^e u$, where $u \in \mathcal{O}$. We say that $K/\mathbb{Q}_p$ is *unramified* if $e = 1$, *ramified* if $e > 1$ and *totally ramified* if $e = n$. Also, $n = e \cdot f$.

We will now show that $\mathbb{Q}_p(\sqrt{q})$ is a ramified extension for $q \in \{p, \epsilon p\}$ and an unramified extension when $q = \epsilon$. This topic has a lot of theory to support it, but here we will just refer to some results. Claim: if $\mathbb{Q}_p(\sqrt{q})$ is a ramified extension, then a uniformizer ω will satisfy $|\omega|_{\mathbb{Q}_p(\sqrt{q})} = p^{-1/e}$, (Thm. 4.14 in [Tur]). Furthermore the the residue field $\mathcal{R}/\mathcal{P} = \mathcal{R}/\omega\mathcal{R} \cong \mathbb{F}_{p^f}$, (Prop. 9.4 in [MIT]).

Let $q \in \{p, p\epsilon\}$ and $\mathbb{Q}_p(\sqrt{q})$ a quadratic extension of $\mathbb{Q}_p$. A good guess for a uniformizer is $\omega = \sqrt{q}$. First we see that

$$|\omega|_{\mathbb{Q}_p(\sqrt{q})} = \sqrt{|q|_p} = p^{-1/2},$$

so, if we assume that $\mathbb{Q}_p(\sqrt{q})$ is totally ramified, it aligns with the previous claim with $e = 2$.

Now we want to describe the digits of $\mathbb{Q}_p(\sqrt{q})$ and see if it makes sense that $f = 1$. Take $x \in \mathbb{Q}_p(\sqrt{q})$, so $x = x_1 + x_2\sqrt{q}$ with $x_1, x_2 \in \mathbb{Q}_p$ and $x_1 = a_k p^k + a_{k+1}p^{k+1} + \cdots$, $x_2 = b_l p^l + b_{l+1}p^{l+1} + \cdots$ with $a_i, b_i \in \{0, ..., p-1\}$. With uniformizer $\omega = \sqrt{q}$. Since $\omega^2 = q$, we can write

$$x = a'_k\omega^{2k} + a'_{k+1}\omega^{2(k+1)} + \cdots + \omega\left(b'_l\omega^{2l} + b'_{l+1}\omega^{2(l+1)}\right) = c_r\omega^r + c_{r+1}\omega^{r+1} + \cdots, \tag{8}$$

for some fitting r and $c_r \in \{0, ..., p-1\}$ and a'_i, b'_i being the same, if $q = p$, and otherwise chosen to fit. Thus the digits used in $\mathbb{Q}_p(\sqrt{q})$ with $q \in \{p, p\epsilon\}$ are isomorphic to $\mathbb{F}_{p^1}$, so $f = 1$.

Now let $q = \epsilon$. Choose the uniformizer $\omega = p$. With the same digit expansion as (8), we get for $x \in \mathbb{Q}_p(\sqrt{\epsilon})$:

$$x = a_k p^k + \cdots + (b_l p^l + \cdots)\sqrt{\epsilon} = (c_r + d_r\sqrt{\epsilon})p^r + (c_{r+1} + d_{r+1}\sqrt{\epsilon})p^{r+1} + \cdots,$$

where $c_i + d_i\sqrt{\epsilon} \in \mathbb{F}_p(\sqrt{\epsilon}) \cong \mathbb{F}_{p^2}$. Thus the residue degree $f = 2$. Since $n = 2$ and $n = ef$, we can conclude that $e = 1$ making $\mathbb{Q}_p(\sqrt{\epsilon})$ an unramified extension of $\mathbb{Q}_p$.

6.2 The Complex p-adic numbers

In the case of the real numbers $\mathbb{R}$, the process of forming an algebraic closure is simple and elegant: by adjoining the imaginary unit i, we obtain the complex numbers $\mathbb{C}$, which is both algebraically closed and complete. It is natural to ask whether a similar construction exists in the context of p-adic numbers.
However, the situation over $\mathbb{Q}_p$ is significantly more intricate. Even at the level of quadratic extensions, there are already multiple distinct types, as seen: unramified and totally ramified extensions, just depending on the choice of polynomial. This diversity appears for all primes p, illustrating that the algebraic structure of $\mathbb{Q}_p$ is much richer than that of $\mathbb{R}$.

To build an analogue of the complex numbers in the p-adic setting, a first step is to consider the algebraic closure of $\mathbb{Q}_p$, denoted $\mathbb{Q}_p^{alg}$. This field contains all algebraic extensions of $\mathbb{Q}_p$, thus accounting for roots of all polynomials of arbitrary degree. One might hope that $\mathbb{Q}_p^{\text{alg}}$ is sufficient, but unfortunately the field is not complete with respect to $|\cdot|_p$.
To fix this, we must take the completion of $\mathbb{Q}_p^{alg}$ with respect to its extended p-adic norm. This yields the field $\mathbb{C}_p$, defined as:

$$\mathbb{C}_p := \widehat{\mathbb{Q}_p^{\text{alg}}}.$$

This field $\mathbb{C}_p$ is both algebraically closed and complete with respect to a p-adic absolute value, and plays the role in p-adic analysis that $\mathbb{C}$ plays in real and complex analysis. It is a fact that as sets $\mathbb{C}$ and $\mathbb{C}_p$ are the same, still they are endowed with different topologies.

This section was based on Chapter 5 in [Bak].

7 The p-adic Exponential and Logarithm

In this chapter, we will continue our quest of finding similarities and differences between the p-adic and the real numbers. Here we only make a quick visit to some elementary functions: the exponential and logarithm. Thus the topic of derivatives, continuity and power seires will not be explicit.
It can be noted that the general theory concerning the p-adics in many ways remains unchanged. But since $\mathbb{Q}_p$ is not an ordered field, since $|\cdot|_p$ is discrete and non-Archimedean, this leads to other challenges and differences; think of the *mean value theorem*, and re-centering the ball of convergence for series using Proposition 3.2. For more details, see Chapter 4 in [Gou].

We will find that the p-adic exponential and logarithm differ from the real counterparts by not being defined on all of $\mathbb{Q}_p$, but on smaller balls.
The region of convergence for a power series $\sum_{n=0}^{\infty} a_n X^n$ is a ball, and elements $x \in \mathbb{Q}_p$ lie in the ball if and only if $|a_n x^n|_p \to 0$. Remember, the radius of convergence ρ is given by

$$\rho = \frac{1}{\limsup_{n\to\infty} |a_n|_p^{1/n}}.$$

If $0 < \rho < \infty$ and $\lim_{n\to\infty} |a_n|_p p^n = 0$, the series converges if and only if $|a_n| < \rho$. ([Gou] Prop. 4.3.1).

7.1 The p-adic Exponential

Lemma 7.1. *Let $n \in \mathbb{N}$, and write $n = a_0 + a_1 p + \cdots + a_k p^k$ then*

$$ord_p(n!) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor = \frac{n-s}{p-1} \leq \frac{n}{p-1},$$

where $s = a_0 + a_1 + \cdots + a_k$.

Proof. Based on Euclidean division, we know that the number of elements divisible by p in $\{1, 2, ..., n\}$ is $\lfloor \frac{n}{p} \rfloor$. We are interested in finding the largest k such that $p^k \mid n! = n(n-1)\cdots 2 \cdot 1$. So first count the number factors in $n!$ divisible by p, $\lfloor \frac{n}{p} \rfloor$. Assuming a factor is divisible by p^2 we count the added powers $\lfloor \frac{n}{p^2} \rfloor$, so $\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor$ will be the total contribution to powers in elements divisible by p and p^2. Thus

$$ord_p(n!) = \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor \leq \sum_{i=1} \frac{n}{p^i} = \frac{n}{p-1},$$

since $\lfloor x \rfloor \leq x$.
For the second equality, we see that $\lfloor \frac{n}{p} \rfloor = a_1 + a_2 p + \cdots + a_k p^{k-1}$, $\lfloor \frac{n}{p^2} \rfloor = a_2 + a_3 p + \cdots + a_k p^{k-2}$ and $\lfloor \frac{n}{p^k} \rfloor = a_k$. For $i > k$, we get $\lfloor \frac{n}{p^i} \rfloor = 0$, so

$$\sum_{i=0}^{\infty} \lfloor \frac{n}{p^i} \rfloor = a_1 + a_2(p+1) + \cdots + a_k(p^{k-1} + \cdots + p + 1).$$

On the other hand,

$$n - s = \sum_{i=0}^{k} a_i (p^i - 1) \quad \Rightarrow \quad \frac{n-s}{p-1} = \sum_{i=0}^{k} a_i \frac{p^i - 1}{p-1} = \sum_{i=0}^{k} a_i \sum_{j=0}^{i-1} p^j,$$

which exactly gives us

$$\sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor = \frac{n-s}{p-1}.$$

□

Theorem 7.2. ([Gou] Lem. 4.5.5) The p-adic exponential function $\exp_p(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}$ has convergence radius $p^{-1/(p-1)}$.

Proof. Using the previous lemma, we know that $|\frac{1}{n!}|_p = p^{ord_p(n!)} \leq p^{n/(p-1)}$, so $|\frac{1}{n!}|_p^{1/n} \leq p^{1/(p-1)}$ and thus

$$\rho = \frac{1}{\limsup_{n\to\infty} |\frac{1}{n!}|_p^{1/n}} \geq p^{-1/(p-1)}.$$

Knowing that the series at least converges for $|x|_p < p^{-1/(p-1)}$, we want to show that the inequality is strict. Let $x \in \mathbb{Q}_p$ such that $|x|_p = p^{-1/(p-1)}$ and let n be a power of p, so $n = p^m$. By Lemma 7.1,

$$ord_p(n!) = ord_p(p^m!) = \frac{p^m - 1}{p-1}.$$

Since $ord_p(x) = \frac{1}{p-1}$, we get

$$ord_p(\frac{x^n}{n!}) = ord_p(\frac{x^{p^m}}{p^m!}) = \frac{p^m}{p-1} - \frac{p^m-1}{p-1} = \frac{1}{p-1} \quad \xrightarrow[n\to\infty]{} \quad \frac{1}{p-1} \neq 0.$$

Thus the series does not converge for $|x|_p = p^{-1/(p-1)}$, and the convergence radius is $p^{-1/(p-1)}$.

□

Proposition 7.3. ([Gou] Prop. 4.5.7) *For $x, y \in B(0, p^{-1/(p-1)})$ we have*

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

Proof.

$$\begin{aligned}
\exp_p(x+y) &= \sum_{n=0}^{\infty} \frac{(x+y)^n}{n!} = \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j \\
&= \sum_{n=0}^{\infty} \sum_{j=0}^{n} \frac{1}{n!} \frac{n!}{(n-j)!j!} x^{n-j} y^j = \sum_{n=0}^{\infty} \sum_{j=0}^{n} \frac{x^{n-j}}{(n-j)!} \frac{y^j}{j!} \\
&= \Big(\sum_{k=0}^{\infty} \frac{x^k}{k!}\Big)\Big(\sum_{j=0}^{\infty} \frac{y^j}{j!}\Big), \qquad k = n-j \\
&= \exp_p(x)\exp_p(y),
\end{aligned}$$

where we use the absolute convergence of the series on the ball $B(0, p^{-1/(p-1)})$ to rearrange the double sum. □

7.2 The p-adic Logarithm

We want to understand the corresponding inverse function of $\exp_p$. Note that unless noted as a function explicitly in the real numbers ($\log^{\mathbb{R}}$), log just defines a series.

Lemma 7.4. *The series $\log(1+X) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} X^n$ converges for $|x|_p < 1$.*

Proof. Checking the definition, we get the radius of convergence ρ given by

$$\rho = \frac{1}{\limsup_{n\to\infty} |a_n|_p^{1/n}} = \frac{1}{\limsup_{n\to\infty} |\frac{1}{n}|_p^{1/n}} = \frac{1}{\limsup_{n\to\infty} p^{ord_p(n)/n}} = 1.$$

This is the case, since $ord_p(n)/n$ tends towards 0, and we see this by making the confusing introduction of the real valued, commonly known logarithm, but denoting it $\log^{\mathbb{R}}$, so

$$p^{ord_p(n)} \leq n \quad \Rightarrow \quad ord_p(n) \leq \log_p^{\mathbb{R}}(n) = \frac{\log^{\mathbb{R}}(n)}{\log \mathbb{R}(p)} \quad \Rightarrow \quad \frac{ord_p(n)}{n} \leq \frac{\log^{\mathbb{R}}(n)}{n \log^{\mathbb{R}}(p)} \quad \underset{n\to\infty}{\longrightarrow} 0.$$

□

Definition 7.5. We define the p-adic logarithm of $x \in B(1,1) = 1 + p\mathbb{Z}_p$ as

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

Lemma 7.6. ([Gou] Prop. 4.5.3) *For $x, y \in B(1,1)$ we have*

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

Proof. To begin with, note that the expression makes sense, so let $x = 1 + a,\ y = 1 + b$ with $a, b \in p\mathbb{Z}_p$. Then $xy = (1+a)(1+b) = 1 + (a + b + ab) \in 1 + p\mathbb{Z}_p$ since $p\mathbb{Z}_p$ is an ideal.

We will be using term-wise differentiation to get the derivative $\frac{\mathrm{d}}{\mathrm{d}s} \log_p(s) = \sum_{n=1}^{\infty} (-1)^{n+1} s^{n-1} = \frac{1}{s}$. Define $g(x) = \log_p(xy) - \log_p(x) - \log_p(y)$. Taking the derivative, we get

$$g'(x) = \frac{1}{xy} y - \frac{1}{x} = 0,$$

so g is a constant function. We see that $g = 0$, since $g(1) = \log_p(y) - \log_p(1) - \log_p(y) = 0$, and thus proving $\log_p(xy) = \log_p(x) + \log_p(y)$.

□

We see that $\exp_p$ and $\log_p$ make great candidates for the p-adic analogues of the real exponential and logarithm. However, the significant difference in their radii of convergence raises concerns about whether they can truly function as inverses of each other.

Proposition 7.7. *Let $\rho_{\exp} := p^{-1/(p-1)}$. The maps*

$$\exp_p :\ B(0, \rho_{\exp}) \to B(1, \rho_{\exp}), \quad \log_p :\ B(1, \rho_{\exp}) \to B(0, \rho_{\exp})$$

are inverse to each other, i.e for $x \in B(0, \rho_{\exp})$,

$$(1)\ \log_p(\exp_p(x)) = x \quad \text{and} \quad (2)\ \exp_p(\log_p(1+x)) = 1 + x.$$

Proof. The relations (1) and (2) follow from their power series, so we need to check for convergence. We can assume $x \neq 0$, since the relations clearly are true when this is the case. We will check that the ranges of $\exp_p$ and $\log_p$ are respectively $B(1, \rho_{\exp})$ and $B(0, \rho_{\exp})$.
Let $x \in B(0, \rho_{\exp})$. We wish to show that $\exp_p(x) \in B(1, \rho_{\exp})$. Since $\exp_p(x) = 1 + \sum_{n=1}^{\infty} \frac{x^n}{n!}$, we get

$$|\exp_p(x) - 1|_p = |\sum_{n=1}^{\infty} \frac{x^n}{n!}|_p \leq \max_{n \geq 1} \left\{ |\frac{x^n}{n!}|_p \right\},$$

by the ultrametric inequality. Looking at each $n \geq 1$,

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

using Lemma 7.1. Since $x \in B(0, \rho_{\exp})$, we can estimate $|x|_p p^{1/(p-1)} < p^{-1/(p-1)} p^{1/(p-1)} = 1$. So we can conclude that $|\exp_p(x) - 1|_p \to 0$ for n tends toward infinity, with maximal value at $n = 1$. Thus

$$|\exp_p(x) - 1|_p \leq |x|_p < \rho_{\exp},$$

so $\exp_p(x) \in B(1, \rho_{\exp})$ as hoped for.

Now to show $\log_p(1 + x) \in B(0, \rho_{\exp})$, let $x \in B(0, \rho_{\exp})$. Then

$$|\log_p(1 + x)|_p = |\sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}|_p \leq \max_{n \geq 1} \left\{ |\frac{x^n}{n}|_p \right\}.$$

Let $n \geq 1$, and thus $|\frac{1}{n}|_p \leq 1$, then

$$|\frac{x^n}{n}|_p = |x^n|_p |\frac{1}{n}|_p \leq |x|_p^n \leq |x| < \rho_{\exp}.$$

Using this we can conclude that $\log_p(1 + x) \in B(0, \rho_{\exp})$, proving the proposition.

□

Bibliography

[Bak] Baker, Andrew; *An Introduction to p-adic Numbers and p-adic Analysis*, Department of Mathematics, University of Glasgow, 2010. Available at: https://www.ams.org/open-math-notes/files/course-material/OMN-202003-110818-1-Course_notes-v1.pdf

[Gou] Gouvêa, Fernando Q.; *p-adic Numbers, An Introduction*, 2nd edition, Universitext, Springer-Verlag, Berlin, 1997.

[Kat] Katok, Svetlana; *p-adic Analysis Compared with Real*, Student Mathematical Library, vol. 37, 2nd edition, American Mathematical Society, 2007.

[Lau] Lauritzen, Niels; *Concrete Abstract Algebra: From Numbers to Gröbner Bases*, Cambridge University Press, 2003.

[MIT] MIT Department of Mathematics; *Local Fields and Hensel's Lemmas (Lecture 9)*, 18.785 Algebraic Number Theory, Fall 2015. Available at: https://math.mit.edu/classes/18.785/2015fa/LectureNotes9.pdf

[Moy] Moy, Samuel; *An Introduction to the Theory of Field Extensions*, University of Chicago Department of Mathematics, 2009. Available at: https://www.math.uchicago.edu/~may/VIGRE/VIGRE2009/REUPapers/Moy.pdf

[Rob] Robert, Alain M.; *A Course in p-adic Analysis*, Graduate Texts in Mathematics, vol. 198, Springer-Verlag, New York, 2000.

[Sal] Sally, Paul J. Jr.; *An Introduction to p-adic Fields, Harmonic Analysis and the Representation Theory of SL_2*, [publication details missing — please add if known].

[Tho] Thomsen, Jesper F.; *Interactive Linear Algebra*, 2020. Available at: https://data.math.au.dk/interactive/linalg/2020/index.html

[Tur] Turner, Evan; *An Introduction to p-adic Numbers and p-adic Analysis*, University of Chicago REU, 2011. Available at: https://www.math.uchicago.edu/~may/VIGRE/VIGRE2011/REUPapers/Turner.pdf