2013

Comparing the algebraic and analytical properties of p-adic numbers with real numbers

Joseph Colton Wilson

Comparing the Algebraic and Analytical Properties of p-adic Numbers with Real Numbers

---

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Mathematics

---

by

Joseph Colton Wilson III

June 2013

Comparing the Algebraic and Analytical Properties of p-adic Numbers with Real Numbers

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

by

Joseph Colton Wilson III

June 2013

Approved by:

[redacted]

Shawnee McMurran, Committee Chair

6/14/13

Date

[redacted]

Davida Fischman, Committee Member

[redacted]

John Sarli, Committee Member

[redacted]

Peter Williams, Chair,
Department of Mathematics

[redacted]

Charles Stanton
Graduate Coordinator,
Department of Mathematics

Abstract

This paper provides a glimpse into the world of p-adic numbers, which encompasses a different way to measure the distance between rational numbers. Defining a new non-Archimedean norm on the field $\mathbb{Q}$ allows us to form a new completion as a metric space, which we call $\mathbb{Q}_p$, the field of p-adic numbers. This paper will explicitly construct and define $\mathbb{Q}_p$ along with other relevant, unfamiliar topics that arise. Simple calculations and surprising results are examined to help familiarize the reader to the new space. Standard algebraic and analytical exercises are performed and discussed in the new setting, such as kth roots of unity, Hensel's Lemma, which is the p-adic analog of Newton's Method, Cauchy Sequences, Convergence, the Mean Value Theorem, the Intermediate Value Theorem and the Chain Rule. This paper then relates these results to their more familiar real counterparts.

Acknowledgements

I wish to thank Dr. Davida Fischman and Dr. John Sarli for their valuable input and suggestions. I would like to thank Dr. Shawnee McMurran for agreeing to be my graduate advisor. Additionally, I thank her for all of the time, patience and assistance she provided with my studies and my writing.

Table of Contents

Chapter 1

Introduction

1.1 Non-Archimedean Norms

The concept of p-adic numbers arises from the fact that there exists more than one way to (naturally) measure the distance between rational numbers. The Euclidean distance, or the standard absolute value, allows us to form a completion of $\mathbb{Q}$ as a metric space, which is $\mathbb{R}$. Defining a new norm on $\mathbb{Q}$, particularly a non-Archimedean norm, forms a new completion of $\mathbb{Q}$, which we call $\mathbb{Q}_p$, that is distinct for each prime p. This norm considers two numbers "close" if their difference is a power of p; the higher the power of p, the "closer" the numbers are considered to be.

We start with the definition of a non-Archimedean norm, which is a fourth condition added to the definition of a standard norm on a field. Refer to [Kat07] (page 6) for the definition of a norm. Refer to [Fra67] (page 259) for the definition of a field.

Definition 1. *Let $|\cdot|$ be a norm on a field, F. Then $|\cdot|$ is **non-Archimedean** if*

$$|x+y| \leq \max(|x|, |y|) \textit{ for all } x, y \in F.$$

This fourth condition that makes a norm non-Archimedean is referred to as the the "strong triangle inequality". We also say that a metric space endowed with a non-Archimedean norm is an *ultrametric* space.

Working with a non-Archimedean norm yields surprising results in our new space.

Exercise 2. *If $|\cdot|$ is a non-Archimedean norm on a field, F, then any point of an open ball*

$$B(a,r) = \{x : |x-a| < r\}$$

in F is its center, i.e., if b is in $B(a,r)$, then $B(b,r) = B(a,r)$. The same is true for closed balls.

Proof. Let $|\cdot|$ be a non-Archimedean norm on an ultrametric space, M. Let $B(a,r) \subset M$ be the open ball of radius r with center a, and let $b \in B(a,r)$. Additionally, let $x \in B(b,r)$. Then $|x-b| < r$ and $|b-a| < r$ by assumption. It follows that

$$|x-a| = |(x-b)+(b-a)| \leq \max(|x-b|, |b-a|)$$

by the strong triangle inequality. Since $\max(|x-b|, |b-a|) < r$, we have $|x-a| < r$. Thus, we have shown that $x \in B(a,r)$.

Since $x \in B(b,r)$ was arbitrary, we conclude that $B(b,r) \subset B(a,r)$. However, since $|b-a| < r$, then $a \in B(b,r)$. Now, we choose a point $y \in B(a,r)$ and by the same argument we can show that $y \in B(b,r)$. It follows that $B(a,r) \subset B(b,r)$. Therefore, $B(a,r) = B(b,r)$. Since b was arbitrary, we have established that any point in an open ball in an ultrametric space is its center.

Note that the same argument holds for closed balls when we replace "$<$" with "$\leq$". □

We can use the result of Exercise 2, particularly the case of closed balls, to prove another suprising result. However, we need to introduce a definition.

Definition 3. *The **sphere** of radius r and center a in a metric space M is the set*

$$S(a,r) = \{x \in M \mid |x-a| = r\}.$$

Exercise 4. *In an ultrametric space, every triangle is isosceles and the length of the two equal sides is greater than or equal to the length of the third side.*

Proof. Let $\triangle ABC$ be a triangle in an ultrametric space, M. Consider the longest side and label the endpoints A and B. Construct the closed ball with center A with radius equal to the length of side AB. Since we have assumed that $AB \geq AC$, we know that

$C \in B[A, AB]$. By our previous result that all points included in a closed ball are its center, we have $B[A, AB] = B[C, AB]$. Since B is contained in the sphere of $B[C, AB]$, then $\overline{BC}$ is the radius of $B[C, AB]$. Since $\overline{AB}$ is also the radius of the ball, we conclude that $AB = BC$. Thus, our arbitrary triangle is isosceles. The second part is immediate from our assumption, that $AB \geq AC$. If AC was indeed the longer side, we would construct the closed ball with center A with that length as its radius and obtain the same result. □

1.2 The Construction of $\mathbb{Q}_p$ - The Underlying Structure

We now begin the construction the new space we will examine in this study, the field $\mathbb{Q}_p$. To do this, we will begin working with general elements in order to build our structure. Once our structure is complete and sound, we will rename our players and prove that they indeed fit our mold. The following procedure outlines the completion of a field with respect to any norm, not necessarily a non-Archimedean norm.

Let F be a field and let $|\cdot|$ be a norm on F. We denote $\{F\}$ as the set of all Cauchy sequences with elements in F. For the definition of a Cauchy sequence, see [Abb01] (page 39). We say that two Cauchy sequences are equivalent, $\{a_n\} \sim \{b_n\}$, if $d(a_n, b_n) \to 0$.

Lemma 5. *The equivalence of Cauchy sequences is an equivalence relation.*

Proof. The properties follow easily from the definition of the equivalence of Cauchy sequences. Let $\{a_n\}, \{b_n\}$ and $\{c_n\}$ be Cauchy sequences.
Since $d(a_n, a_n) \to 0$, then $\{a_n\} \sim \{a_n\}$. Thus, the relation is reflexive.
Assume $\{a_n\} \sim \{b_n\}$. Then, $d(a_n, b_n) \to 0$. Clearly, $d(b_n, a_n) \to 0$, and thus, $\{b_n\} \sim \{a_n\}$. Thus, the relation is symmetric.
Assume $\{a_n\} \sim \{b_n\}$ and $\{b_n\} \sim \{c_n\}$. Then, $d(a_n, b_n) \to 0$ and $d(b_n, c_n) \to 0$. Then,

$$\lim_{n\to\infty} d(a_n, c_n) \leq \lim_{n\to\infty} \left(d(a_n, b_n) + d(b_n, c_n)\right) = 0$$

by the triangle inequality and the properties of real limits. Thus, $d(a_n, c_n) \to 0$ and $\{a_n\} \sim \{c_n\}$. Thus, the relation is transitive. □

Let $\hat{F}$ be the set of equivalence classes of all Cauchy sequences in F. Our goal at this juncture is to prove that $\hat{F}$ is a field. Before we prove this, we must carefully consider the elements and operations in $\hat{F}$. The addition and multiplication of Cauchy sequences are defined pointwise. Let $\{a_n\}$ and $\{b_n\}$ be Cauchy sequences in F.

$$\text{If } \{a_n\} = \{a_0, a_1, a_2, \dots\} \text{ and } \{b_n\} = \{b_0, b_1, b_2, \dots\},$$

$$\text{then define } \{a_n + b_n\} = \{a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots\}$$

$$\text{and } \{a_n \cdot b_n\} = \{a_0 \cdot b_0, a_1 \cdot b_1, a_2 \cdot b_2, \dots\}.$$

Lemma 6. *If $\{a_n\}$ and $\{b_n\}$ are Cauchy sequences, then $\{a_n+b_n\}, \{a_n-b_n\}$ and $\{a_n \cdot b_n\}$ are Cauchy sequences.*

Proof. Since $\{a_n\}$ and $\{b_n\}$ are Cauchy sequences, fix $\varepsilon > 0$. For that value of ε, there exist integers N_1 and N_2 such that $m, n > N_1$ implies $|a_n - a_m| < \frac{\varepsilon}{2}$ and $m, n > N_2$ implies $|b_n - b_m| < \frac{\varepsilon}{2}$. Let $N = \max\{N_1, N_2\}$. Then, $m, n > N$ implies

$$\begin{aligned} |(a_n + b_n) - (a_m + b_m)| &= |(a_n - a_m) + (b_n - b_m)| \\ &\leq |a_n - a_m| + |b_n - b_m| \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\ &= \varepsilon. \end{aligned}$$

Thus, $\{a_n + b_n\}$ is a Cauchy sequence. We use a similar argument to show $\{a_n - b_n\}$ is a Cauchy sequence.

Finally, to show that $\{a_n \cdot b_n\}$ is a Cauchy sequence, we use the fact that all Cauchy sequences are bounded, or if $\{a_n\}$ is a Cauchy sequence, then $|a_n| \leq C$ for all n and some $C > 0$. Choose positive constants C_1 and C_2 such that $|a_n| \leq C_1$ and $|b_n| \leq C_2$ for all n. Given $\varepsilon > 0$, There exist integers N_1 nad N_2 such that $n, m > N_1$ implies $|a_n - a_m| < \frac{\varepsilon}{2C_2}$ and $n, m > N_2$ implies $|b_n - b_m| < \frac{\varepsilon}{2C_1}$. Let $N = \max\{N_1, N_2\}$. Then, $m, n > N$ implies

$$\begin{aligned} |a_m \cdot b_m - a_n \cdot b_n| &= |a_m \cdot b_m - a_m \cdot b_n + a_m \cdot b_n - a_n \cdot b_n| \\ &= |a_m \cdot (b_n - b_m) - b_n \cdot (a_n - a_m)| \\ &\leq |a_m| \cdot |b_n - b_m| + |b_n| \cdot |a_n - a_m| \\ &< C_1 \cdot \left(\frac{\varepsilon}{2C_1}\right) + C_2 \cdot \left(\frac{\varepsilon}{2C_2}\right) \\ &= \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\ &= \varepsilon. \end{aligned}$$

Thus, $\{a_n \cdot b_n\}$ is a Cauchy sequence. [Fai13] □

We now show that our operations in $\hat{F}$ are well-defined. The elements of $\hat{F}$ are equivalence classes of Cauchy sequences. We need to define what it means to add and multiply equivalence classes.

We now introduce the notation that we use for equivalence classes. We denote equivalence classes of Cauchy sequences by capital letters: A. We may also refer to an equivalence class of a particular Cauchy sequence by placing parentheses around the Cauchy sequence: $(\{a_n\})$.

Let A and B be equivalence classes of Cauchy sequences with representative Cauchy sequences $\{a_n\}$ and $\{b_n\}$, respectively. Now, we define addition and multiplication of equivalence classes as the addition and multiplication of their representative Cauchy sequences:

$$A + B = (\{a_n + b_n\}) \text{ and } A \cdot B = (\{a_n \cdot b_n\})$$

We now need to show that the addition and multiplication of equivalence classes do not depend on the representatives.

Lemma 7. *If $\{a_n\} \sim \{a'_n\}$ and $\{b_n\} \sim \{b'_n\}$ are two pairs of equivalent Cauchy sequences, then $\{a_n \pm b_n\} \sim \{a'_n \pm b'_n\}$ and $\{a_n \cdot b_n\} \sim \{a'_n \cdot b'_n\}$.*

Proof. From the definition of the equivalence of Cauchy sequences, we know that

$$\lim_{n\to\infty} d(a_n, a'_n) = 0 \text{ and } \lim_{n\to\infty} d(b_n, b'_n) = 0.$$

By the triangle inequality and the properties of real limits, we know

$$\lim_{n\to\infty} d(a_n \pm b_n, a'_n \pm b'_n) \leq \lim_{n\to\infty} d(a_n, a'_n) + \lim_{n\to\infty} d(b_n, b'_n) = 0.$$

To show that the multiplication of equivalence classes of Cauchy sequences does not depend on the representatives, we have

$$\begin{aligned} d(a_n \cdot b_n, a'_n \cdot b'_n) &= |a_n \cdot b_n - a'_n \cdot b'_n| \\ &= |a_n \cdot b_n - a'_n \cdot b_n + a'_n \cdot b'_n - a'_n \cdot b'_n| \\ &\leq |b_n||a_n - a'_n| + |a'_n||b_n - b'_n|. \end{aligned}$$

Taking the limit as n approaches infinity, we have

$$\lim_{n\to\infty} |b_n||a_n - a'_n| + |a'_n||b_n - b'_n| = \lim_{n\to\infty} |b_n| \cdot 0 + \lim_{n\to\infty} |a'_n| \cdot 0.$$

Since $\{b_n\}$ and $\{a'_n\}$ are Cauchy sequences, by definition, their limits exist. We also use the fact that all Cauchy sequences are bounded to say that the entire limit is zero. $\square$

This establishes that our operations in $\hat{F}$ are well-defined and we are now ready to prove that $\hat{F}$ is a field. Many of our properties of a field will follow immediately from the fact that each individual element of any Cauchy sequence belongs to the field F. We will begin by showing that $\hat{F}$ is a commutative ring with unity under addition and multiplication of equivalence classes of Cauchy sequences. Finally, we will show the existance of multiplicative inverses, which will complete the proof.

Theorem 8. $\left\langle \hat{F}, +, \cdot \right\rangle$ *is a field.*

Proof. Let A, B and C be equivalence classes of Cauchy sequences in $\hat{F}$ with the addition and multiplication operations defined above, and let $\{a_n\}, \{b_n\}$ and $\{c_n\}$ be the representative Cauchy sequences, respectively.

- We have shown that $\hat{F}$ is closed under the addition of equivalence classes of Cauchy sequences. $A + B \in \hat{F}$: closure under addition is satisfied.

- We next need to show that the addition of equivalence classes of Cauchy sequences is commutative, saving us work in later steps. Since we add the representative Cauchy sequences pointwise and each element of each Cauchy sequence is from the field F where commutative addition is established, we know that the addition of equivalence classes of Cauchy sequences is commutative. $A+B = B+A$: commutative addition is satisfied.

- Similarly, we know that the addition of equivalence classes of Cauchy sequences is associative. $(A + B) + C = A + (B + C)$: associative addition is satisfied.

- Consider the constant sequence $\{0, 0, 0, \dots\}$ where 0 is the additive identity in F. Clearly, this is a Cauchy sequence. Adding this sequence pointwise to a representative Cauchy sequence $\{a_n\} = \{a_0, a_1, a_2 \dots\}$ for the equivalence class A will yield $\{a_0 + 0, a_1 + 0, a_2 + 0, \dots\} = \{a_0, a_1, a_2, \dots\} = \{a_n\}$. Thus, our additive identity in $\hat{F}$ is the equivalence class containing the constant squence $\{0, 0, 0, \dots\}$, which we will denote as $(\hat{0})$. $A + (\hat{0}) = A$: the existence of an additive identity in $\hat{F}$ is satisfied. We also say that any sequence $\{z_n\} \in (\hat{0})$ is a *null sequence* because $\lim_{n\to\infty} |z_n| = 0$.

- If $\{a_n\} = \{a_0, a_1, a_2 \dots\}$ is a Cauchy sequence, then it is clear there exists a sequence $\{-a_0, -a_1, -a_2 \dots\}$ made up of the addititive inverses of each a_n. Each $-a_n$ exists because it is in the field F. Call this sequence $\{-a_n\}$ where

  $$\{a_n\} + \{-a_n\} = \{0, 0, 0 \dots\}.$$

  We already know that the constant sequence $\{0, 0, \dots\}$ a Cauchy sequence. We need to show that $\{-a_n\}$ is a Cauchy sequence. Since $\{a_n\}$ is a Cauchy sequence, we know that for any $\varepsilon > 0$, there exists an integer N such that for integers

  $$n, m > N, \;\; d(a_n, a_m) < \varepsilon.$$

  Then, it is clear that for the same n, m that $d(-a_n, -a_m) < \varepsilon$ and $\{-a_n\}$ is a Cauchy sequence. Let A' be the equivalence class containing the Cauchy sequence, $\{-a_n\}$, and we have that $A + A' = (\hat{0})$: The existence of additive inverses is satisfied.

- We have shown that $\hat{F}$ is closed under the multiplication of equivalence classes of Cauchy sequences: $A \cdot B \in \hat{F}$: closure under multiplication is satisfied.

- The commutivity of multiplication follows from the addition case. $A \cdot B = B \cdot A$: commutative multiplcation is satisfied.

- The associativity of multiplication follows from the addition case.
  $(A \cdot B) \cdot C = A \cdot (B \cdot C)$: associative multiplication is satisfied.

- The distributive property of multiplication and addition follows similarly because the operations are computed pointwise and the elements of the representative Cauchy sequences are from the field F where the distributive property is established.
  $A \cdot (B + C) = A \cdot B + A \cdot C$: the distributive property is satisfied.

- Consider the constant sequence $\{1, 1, 1, \dots\}$, where 1 is the multiplicative identity in F. This is clearly a Cauchy sequence. Multiplying this sequence pointwise to a representative Cauchy sequence $\{a_n\} = \{a_0, a_1, a_2 \dots\}$ for the equivalence class A will yield $\{a_0 \cdot 1, a_1 \cdot 1, a_2 \cdot 1, \dots\} = \{a_0, a_1, a_2, \dots\} = \{a_n\}$. Thus, our multiplicative identity in $\hat{F}$ is the equivalence class containing the constant sequence $\{1, 1, 1, \dots\}$, which we will denote as $(\hat{1})$. $A \cdot (\hat{1}) = A$: the existence of a multiplicative identity in $\hat{F}$ is satisfied.

In order to complete the proof that $\hat{F}$ is a field, we need to show the existence of multiplicative inverses. That is, for an equivalence class $A \in \hat{F}$ that is not the zero class, $(\hat{0})$, there exists an equivalence class $A^{-1} \in \hat{F}$ such that $A \cdot A^{-1} = (\hat{1})$. To begin, we need to prove a lemma. Since our arbitrary equivalence class, A is not the zero class, $(\hat{0})$, its representative Cauchy sequence $\{a_n\}$ is not a null sequence. However, $\{a_n\}$ still could contain one or more zero elements. Nonetheless, we can show at some point in the sequence that there must be no more zero elements.

Lemma 9. *Let $\{a_n\}$ be a Cauchy sequence, but not a null sequence. Then, there exist a number $c > 0$ and a positive integer N such that for all $n > N, |a_n| > c$.*

Proof. Let $\{a_n\}$ be a Cauchy sequence, but not a null sequence. Then there exists $\varepsilon > 0$ such that for all N, there exists $n > N$ such that $|a_n| \geq \varepsilon$. Thus, for $N = 1$, there exists an element a_{n_1} such that $|a_{n_1}| \geq \varepsilon$. For $N = 2$ there exists an element a_{n_2} such that $|a_{n_2}| \geq \varepsilon$ and $n_2 > n_1$. It is clear that we can construct a subsequence $\{a_{n_i}\}$ where $|a_{n_i}| \geq \varepsilon$ for all i.

Since $\{a_n\}$ is a Cauchy sequence, there exists an N such that $n_i > N$ and $n > N$ imply $|a_n - a_{n_i}| < \frac{\varepsilon}{3}$. Using the following property of a norm: $|x-y| \geq \big||x| - |y|\big| \geq |x| - |y|$ for all $x, y \in F$, we have that

$$\begin{aligned} |a_n| &= |a_{n_i} - (a_{n_i} - a_n)| \\ &\geq |a_{n_i}| - |a_n - a_{n_i}| \\ &\geq \varepsilon - \frac{\varepsilon}{3} \\ &> \frac{\varepsilon}{2}. \end{aligned}$$

Thus, we can choose $c = \frac{\varepsilon}{2}$ and the statement is proven. □

We have what we need to show the existence of multiplicative inverses in $\hat{F}$. Let $A \in \hat{F}$ and $A \neq (\hat{0})$. Let $\{a_n\}$ be the representative sequence for A. Since $A \neq (\hat{0})$, that implies $\{a_n\}$ is not a null sequence. Define a new sequence, $\{a_n^*\}$, by

$$a_n^* = \begin{cases} 0 & \text{if } 1 \leq n \leq N-1, \\ \frac{1}{a_n} & \text{if } n \geq N. \end{cases}$$

Lemma 10. *Let $\{a_n\}$ be a Cauchy sequence that is not a null sequence. Let $\{a_n^*\}$ be as defined above. Then $\{a_n^*\}$ is a Cauchy sequence.*

Proof. It follows from Lemma 9, there exist a number $c > 0$ and a positive integer N such that $|a_n| > c$ for all $n \geq N$. Let $\varepsilon > 0$ be fixed. Since $\{a_n\}$ is a Cauchy sequence, there exists a positive integer N such that $n, m > N$ implies $|a_n - a_m| < c^2\varepsilon$. Then,

$$\begin{aligned} |a_n^* - a_m^*| &= \left|\frac{1}{a_n} - \frac{1}{a_m}\right| \\ &= \frac{|a_n - a_m|}{|a_n| \cdot |a_m|} \\ &\leq \frac{1}{c} \cdot \frac{1}{c} \cdot |a_n - a_m| \\ &< \frac{1}{c^2} \cdot c^2\varepsilon \\ &= \varepsilon. \end{aligned}$$

Thus, $\{a_n^*\}$ is a Cauchy sequence. □

Let the equivalence class with representative Cauchy sequence $\{a_n^*\}$ be A^{-1}. Now we perform the needed multiplication, $A \cdot A^{-1}$. To do this, we multiply our representative Cauchy sequences pointwise:

$$\{a_n\} \cdot \{a_n^*\} = \{0, 0, 0, \ldots, 0, 1, 1, 1, \ldots\},$$

where the first $N - 1$ terms are each 0 and each nth term is 1 for $n \geq N$. It is clear that $\{0, 0, 0, \ldots, 1, 1, 1, \ldots\}$ is a representative for the equivalence class $(\hat{1})$. Thus, $A \cdot A^{-1} = (\hat{1})$: the existence of multiplicative inverses is satisfied.

We have previously shown that $\left\langle \hat{F}, +, \cdot \right\rangle$ is a commutative ring with identity. Now, we have shown that every nonzero element of $\hat{F}$ has a multiplicative inverse. Therefore, we have shown that $\left\langle \hat{F}, +, \cdot \right\rangle$ is a field. □

Our next step is to extend the norm $|\cdot|$ from F to $\hat{F}$.

Definition 11. *Let $A \in \hat{F}$ and let $\{a_n\}$ be a representative Cauchy sequence for A. Define $||\cdot||$ by*

$$||A|| = \lim_{n\to\infty} |a_n|.$$

To show that $||\cdot||$ is well-defined, we must show that $||\cdot||$ also does not depend on the choice of representative of the equivalence class. We use this property of a normed field: $\big||x| - |y|\big| \leq |x - y|$ for all $x, y \in F$. By this fact, we can say that

$$\big||a_n| - |a_m|\big| \leq |a_n - a_m|,$$

and thus the sequence of real numbers $\{|a_n|\}$ is a Cauchy sequence with respect to the usual norm on $\mathbb{Q}$, which is the standard absolute value. Since $\mathbb{R}$ is complete, then the limit defining $||\cdot||$ exists, and thus, $||\cdot||$ is well defined. Now take a different representative sequence of A, call it $\{a'_n\}$. By the same inequality above, we get that

$$0 \leq \lim_{n\to\infty} \left| |a_n| - |a'_n| \right| \leq \lim_{n\to\infty} |a_n - a'_n| = 0$$

and thus, $\lim_{n\to\infty} |a'_n| = \lim_{n\to\infty} |a_n| = ||A||$. Therefore, $||\cdot||$ does not depend on the choice of representative of the equivalence class.

Theorem 12. *$||\cdot||$ is a norm on $\hat{F}$.*

Proof. We need to verify the three properties of a norm. Let A and B be equivalence classes of Cauchy sequences and let $\{a_n\}$ and $\{b_n\}$ be the representative Cauchy sequences, respectively.

Property 1: We need to show:

$||A|| = 0$ if and only if $A = (\hat{0})$, and $||A|| > 0$ if and only if $A \neq (\hat{0})$.

If $||A|| = 0$, then $\lim_{n\to\infty} |a_n| = 0$ and $\{a_n\}$ is a null sequence. Thus, $A = (\hat{0})$. Similarly, if $A = (\hat{0})$, then $\{a_n\}$ is a null sequence and $||A|| = \lim_{n\to\infty} |a_n| = 0$.

If $||A|| > 0$, then $\{a_n\}$ is not a null sequence and $A \neq (\hat{0})$. If $A \neq (\hat{0})$, then there exist positive numbers c and N such that for all $n > N$, we have $|a_n| \geq c > 0$. Thus, $||A|| > 0$.

Property 2: We need to show: $||A \cdot B|| = ||A|| \cdot ||B||$

Since $||\cdot||$ yields a positive real number, we use the properties of real limits and the fact that $|\cdot|$ is a norm.

$$||A \cdot B|| = \lim_{n\to\infty} |a_n \cdot b_n| = \lim_{n\to\infty} |a_n| \cdot |b_n| = \lim_{n\to\infty} |a_n| \cdot \lim_{n\to\infty} |b_n| = ||A|| \cdot ||B||.$$

Property 3: We need to show: $||A + B|| \leq ||A|| + ||B||$.

Again, we use the properties of real limits, the fact that $|\cdot|$ is a norm.

$$||A + B|| = \lim_{n\to\infty} |a_n + b_n| \leq \lim_{n\to\infty} \left(|a_n| + |b_n|\right) = \lim_{n\to\infty} |a_n| + \lim_{n\to\infty} |b_n| = ||A|| + ||B||.$$

□

Theorem 13. *F is a dense subset of $\hat{F}$ and $\hat{F}$ is complete with respect to the norm $||\cdot||$.*

Proof. It is clear that there is a subset of $\hat{F}$ that is isomorphic to F. This is the set of equivalence classes that have a representative of a constant Cauchy sequence, which we will denote by $\{(\{\hat{a}_n\})\}$. To show that F is a dense subset of $\hat{F}$, we will show that this set of equivalence classes contains a representative constant Cauchy sequence is dense in $\hat{F}$ or for any $A \in \hat{F}$, there exists a constant Cauchy sequence $\{\hat{a}_n\}$ such that

$$\lim_{n\to\infty} ||A - (\hat{a}_n)|| = 0.$$

Let $A \in \hat{F}$ and let $\{a_m\}$ be a representative Cauchy sequence of A. For each $a_n \in \{a_m\}$, construct the constant sequence $\{\hat{a}_n\}$ For each fixed positive integer n, consider the sequence $\{a_m - a_n\}_{m=1}^{\infty}$. This is a Cauchy sequence because $\{a_m\}$ is a Cauchy sequence and a_n is a constant. We denote the equivalence class of $\{\hat{a}_n\}$ as $(\hat{a}_n)$. Hence, the equivalence class for the Cauchy sequence, $\{a_m - a_n\}_{m=1}^{\infty}$ is $A - (\hat{a}_n)$ by the definition of our operations on equivalence classes of Cauchy sequences. From the definition of the extension of $|\cdot|$ to $\hat{F}$, we have

$$\lim_{n\to\infty} ||A - (\hat{a}_n)|| = \lim_{n,m\to\infty} |a_m - a_n| = 0.$$

To show completeness, we need to show that any Cauchy sequence in $\hat{F}$ has a limit in $\hat{F}$. Let $\{A_n\}$ be a Cauchy sequence in $\hat{F}$. Since we have shown that F is a dense subset of $\hat{F}$, we can say that for any $A_n \in \{A_n\}$, there exists an element $a_n \in F$ such that $||A_n - (\hat{a}_n)|| < \frac{1}{n}$. So, $\{A_n - (\hat{a}_n)\}$ is by definition a null sequence, and thus, a Cauchy sequence in $\hat{F}$. Now, $\{(\hat{a}_n)\} = \{A_n\} - \{A_n - (\hat{a}_n)\}$ and $\{(\hat{a}_n)\}$ is the difference between two Cauchy sequences which we have already shown is a Cauchy sequence. Since all of the elements of $\{A_n - (\hat{a}_n)\}$ are members of F (or the subset of $\hat{F}$ isomorphic to F), then we can say that $\{a_n\}$ is a Cauchy sequence in F. Let A be the equivalence class of $\{a_n\}$ in $\hat{F}$. From our earlier results, we can say that $\{A_n - (\hat{a}_n)\}$ and $\{A - (\hat{a}_n)\}$ are both null sequences in $\hat{F}$, and it is clear that the difference of two null sequence is also a null sequence. Since

$$\{A - A_n\} = \{A - (\hat{a}_n)\} - \{A_n - (\hat{a}_n)\},$$

it follows that $\{A - A_n\}$ is a null sequence. This implies that $\lim_{n\to\infty} ||A - A_n|| = 0$, or that the limit of a Cauchy sequence $\{A_n\}$ in $\hat{F}$ has limit A in $\hat{F}$. Thus, $\hat{F}$ is complete with respect to the norm $||\cdot||$. □

Finally, we have shown that every element of $A \in \hat{F}$ contains a representative that is a constant sequence $\{\hat{a}_n\}$. Thus, we can say that the operations in $\hat{F}$ are extended from F by continuity.

Theorem 14.

$$\textit{If } A = \lim_{n\to\infty}(\hat{a}_n) \textit{ and } B = \lim_{n\to\infty}(\hat{b}_n)$$
$$\textit{then } A + B = \lim_{n\to\infty}(\hat{a}_n + \hat{b}_n) \textit{ and } A \cdot B = \lim_{n\to\infty}(\hat{a}_n \cdot \hat{b}_n).$$

Proof. Let $A = \lim_{n\to\infty}(\hat{a}_n)$ and $B = \lim_{n\to\infty}(\hat{b}_n)$. Fix $\varepsilon > 0$. Since there exists a positive integer N such that $n > N$ implies that $||A - (\hat{a}_n)|| < \frac{\varepsilon}{2}$ and $||B - (\hat{b}_n)|| < \frac{\varepsilon}{2}$. Then,

$$\begin{aligned} ||A + B - (\{\hat{a}_n + \hat{b}_n\})|| &= ||(A - (\hat{a}_n)) + (B - (\hat{b}_n))|| \\ &\leq ||A - (\hat{a}_n)|| + ||B - (\hat{b}_n)|| \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\ &= \varepsilon. \end{aligned}$$

Thus,

$$A + B = \lim_{n\to\infty}(\hat{a}_n + \hat{b}_n).$$

We now show that multiplication is extended.

Fix $\varepsilon > 0$. Then there exists a positive integer N such that $n > N$ implies that

$$||A - (\hat{a}_n)|| < \varepsilon \text{ and } ||B - (\hat{b}_n)|| < \varepsilon.$$

Hence, we can say that $\lim_{n\to\infty} ||A - (\hat{a}_n)|| = 0$ and $\lim_{n\to\infty} ||B - (\hat{b}_n)|| = 0$. Thus,

$$\begin{aligned} \lim_{n\to\infty} ||A \cdot B - (\{\hat{a}_n \cdot \hat{b}_n\})|| &= \lim_{n\to\infty} ||A \cdot B - A \cdot (\hat{b}_n) + A \cdot (\hat{b}_n) - (\{\hat{a}_n \cdot \hat{b}_n\})|| \\ &\leq \lim_{n\to\infty} ||A|| \cdot ||B - (\hat{b}_n)|| + \lim_{n\to\infty} ||(\hat{b}_n)|| \cdot ||A - (\hat{a}_n)|| \\ &= \lim_{n\to\infty} ||A|| \cdot 0 + \lim_{n\to\infty} ||(\hat{b}_n)|| \cdot 0. \end{aligned}$$

Since A and $(\hat{b}_n)$ are equivalence classes of Cauchy sequences, their limits exist and are bounded. Thus, the entire limit is zero and we have that

$$A \cdot B = \lim_{n\to\infty}(\hat{a}_n \cdot \hat{b}_n).$$

□

1.3 The Construction of $\mathbb{Q}_p$ - Naming Our Elements

As expected, our field F is the field of rational numbers $\mathbb{Q}$ under usual addition and multiplication. If we take our norm to be the standard absolute value, $|\cdot|$, we can form the completion of $\mathbb{Q}$ with respect to that norm, which is $\mathbb{R}$. However, we can endow $\mathbb{Q}$ with many different norms, resulting in many different completed fields. We begin this section by stating the definition of the norm that will create the field of p-adic numbers $\mathbb{Q}_p$ as a different completion of $\mathbb{Q}$.

It is a fact that $\mathbb{Q}$ is not complete with respect to any nontrivial norm, that is, we can construct a Cauchy sequence of rational numbers that converges to an element not in $\mathbb{Q}$ with respect to any nontrivial norm. We will prove in Chapter 3 that $\mathbb{Q}$ is not complete with respect to the p-adic norm as defined below when we are more familiar with Cauchy sequences featuring our new norm.

Definition 15. *Let $p \in \mathbb{N}$ be any prime number. Define a map $|\cdot|_p$ on $\mathbb{Q}$ by:*

$$|x|_p = \begin{cases} p^{-\mathrm{ord}_p x} & \text{if } \; x \neq 0, \\ 0 & \text{if } \; x = 0. \end{cases}$$

Define $\mathrm{ord}_p\, x$ (the p-adic order) as the highest power of p which divides x if $x \in \mathbb{Z}$, or $\mathrm{ord}_p\, x = \mathrm{ord}_p\, a - \mathrm{ord}_p\, b$, if $x = \frac{a}{b}$, where $a, b \in \mathbb{Z}$, $b \neq 0$.

Note that $|x|_p \leq 1$ for all $x \in \mathbb{Z}$, as the integers will play a large role in this study.

Theorem 16. *$|\cdot|_p$ is a non-Archimedean norm on $\mathbb{Q}$.*

Proof. We need to verify the four properties of a non-Archimedean norm. Let $|\cdot|_p$ be as defined above.

Property 1 : We need to show that:

$|x|_p = 0$ if and only if $x = 0$, and $|x|_p > 0$ if and only if $x \neq 0$.

This property follows immediately from the definition of $|\cdot|_p$. If $x \in \mathbb{Q}$ and $x \neq 0$, then it is clear that $|x|_p > 0$.

Property 2 : We need to show that:

$|xy|_p = |x|_p|y|_p$ for all $x, y \in \mathbb{Q}$.

If $x = 0$ or $y = 0$, the result is trivial. Let $x = \frac{a}{b}$ and $y = \frac{c}{d}$, where $a, b, c, d \in \mathbb{Z}$, $b \neq 0, d \neq 0$. Then, $|xy|_p = |\frac{ac}{bd}|_p = p^{-\text{ord}_p\,(\frac{ac}{bd})}$. Note that $\text{ord}_p\,(ac)$ is the highest power of p that divides ac. Suppose that the highest power of p that divides a is n and the highest power of p that divides b is m, then it is clear that the highest power of p that divides ac is $n + m$. Thus, we can say that $\text{ord}_p\,(ac) = \text{ord}_p\,a + \text{ord}_p\,c$. Then

$$\begin{aligned}
|xy|_p &= \left|\frac{ac}{bd}\right|_p \\
&= p^{-(\text{ord}_p\,ac - \text{ord}_p\,bd)} \\
&= p^{-(\text{ord}_p\,a + \text{ord}_p\,c - (\text{ord}_p\,b + \text{ord}_p\,d))} \\
&= p^{-((\text{ord}_p\,a - \text{ord}_p\,b) + (\text{ord}_p\,c - \text{ord}_p\,d))} \\
&= p^{-\text{ord}_p\,\frac{a}{b}} \cdot p^{-\text{ord}_p\,\frac{c}{d}} \\
&= |x|_p|y|_p.
\end{aligned}$$

Property 3 : We need to show that:

$|x + y|_p \leq |x|_p + |y|_p$ for all $x, y \in \mathbb{Q}$. Again, if $x = 0$ or $y = 0$, the result is trivial. Let $x = \frac{a}{b}$ and $y = \frac{c}{d}$, where $a, b, c, d \in \mathbb{Z}$, $b \neq 0, d \neq 0$. Then

$$\begin{aligned}
|x + y|_p &= p^{-\text{ord}_p\,(x+y)} \\
&= p^{-\text{ord}_p\,(\frac{ad+bc}{bd})} \\
&= p^{-(\text{ord}_p\,(ad+bc) - \text{ord}_p\,(bd))}
\end{aligned}$$

We claim that $\text{ord}_p\,(ad+bc) \geq \min\{\text{ord}_p(ad), \text{ord}_p(bc)\}$. Let n be the highest power of p that divides ad and let m be the highest power of p that divides bc. Then, if we factor out the highest power of p that divides $ad + bc$, we can see that it is at least the minimum of n and m.

Thus, we know

$$p^{-(\text{ord}_p\,(ad+bc) - \text{ord}_p\,(bd))} \leq p^{-[\min\{\text{ord}_p(ad), \text{ord}_p(bc)\} - \text{ord}_p b - \text{ord}_p d]}.$$

Suppose that $\min\{\text{ord}_p(ad), \text{ord}_p(bc)\} = \text{ord}_p(ad)$. Then,

$$\begin{aligned}
\min\{\text{ord}_p(ad), \text{ord}_p(bc)\} - \text{ord}_p b - \text{ord}_p d &= \text{ord}_p a + \text{ord}_p d + \text{ord}_p b - \text{ord}_p d \\
&= \text{ord}_p a - \text{ord}_p b.
\end{aligned}$$

Similarly, suppose that $\min\{\mathrm{ord}_p(ad), \mathrm{ord}_p(bc)\} = \mathrm{ord}_p(bc)$. Then,

$$\begin{aligned} \min\{\mathrm{ord}_p(ad), \mathrm{ord}_p(bc)\} - \mathrm{ord}_p b - \mathrm{ord}_p d &= \mathrm{ord}_p b + \mathrm{ord}_p c - \mathrm{ord}_p b - \mathrm{ord}_p d \\ &= \mathrm{ord}_p c - \mathrm{ord}_p d. \end{aligned}$$

Thus,

$$\min\{\mathrm{ord}_p(ad), \mathrm{ord}_p(bc)\} - \mathrm{ord}_p b - \mathrm{ord}_p d = \min\{(\mathrm{ord}_p a - \mathrm{ord}_p b), (\mathrm{ord}_p c - \mathrm{ord}_p d)\}.$$

Finally, we have that

$$\begin{aligned} p^{-[\min\{\mathrm{ord}_p(ad), \mathrm{ord}_p(bc)\} - \mathrm{ord}_p b - \mathrm{ord}_p d]} &= p^{-\min\{(\mathrm{ord}_p a - \mathrm{ord}_p b), (\mathrm{ord}_p c - \mathrm{ord}_p d)\}} \\ &= p^{-\min\{\mathrm{ord}_p x, \mathrm{ord}_p y\}} \\ &= \max\{p^{-\mathrm{ord}_p x}, p^{-\mathrm{ord}_p y}\} \\ &= \max\{|x|_p, |y|_p\} \\ &\leq |x|_p + |y|_p. \end{aligned}$$

This proves the triangle inequality, that $|x+y|_p \leq |x|_p + |y|_p$. Additionally, we have proven the fourth condition, the strong triangle inequality: $|x+y|_p \leq \max\{|x|_p, |y|_p\}$. Thus, we have shown that $|\cdot|_p$ is a non-Archimedean norm on $\mathbb{Q}$. □

Finally, we define $\mathbb{Q}_p$ (which is our $\hat{F}$ in Section 1.2) as the completion of $\mathbb{Q}$ with respect to the p-adic norm, $|\cdot|_p$. As earlier, we extend the p-adic norm to $\mathbb{Q}_p$. Let $a \in \mathbb{Q}_p$. Then,

$$|a|_p = \lim_{n\to\infty} |a_n|_p$$

where $\{a_n\}$ is a Cauchy sequence in $\mathbb{Q}$ representing a. Note that $|\cdot|_p$ can take on only a discrete set of values. We see that if $x \in \mathbb{Q}$, then $|x|_p \in \{0\} \cup \{p^n,\ n \in \mathbb{Z}\}$, and the sequence of norms, $\{|a_n|_p\}$ will converge as $n \to \infty$.

Now, consider the series:

$$\frac{d_{-m}}{p^m} + \frac{d_{-m+1}}{p^{m-1}} + \cdots + d_0 + d_1 p + d_2 p^2 + \cdots,$$

where each d_k is an integer in the set $\{0, 1, 2, \ldots, p-1\}$ and $d_{-m} \neq 0$.

Theorem 17. *Any partial sum of the above series is a Cauchy sequence.*

Proof. Fix an $\varepsilon > 0$ and choose an N such that $p^{-N} < \varepsilon$. Let $k > n > N$. Then,

$$\left| \sum_{i=-m}^{k} d_i p^i - \sum_{i=-m}^{n} d_i p^i \right|_p = \left| \sum_{i=n+1}^{k} d_i p^i \right|_p \leq \max_{n<i\leq k} \{|d_i p^i|_p\} \leq p^{-N} < \varepsilon.$$

So, each partial sum of the series above represents an element of $\mathbb{Q}_p$. □

The converse of the statement is also true. Each equivalence class of Cauchy sequences in $\mathbb{Q}$ contains a unique canonical representative Cauchy sequence, which can be expressed by the sequence of partial sums of the series above.

Theorem 18. *Every equivalence class a in $\mathbb{Q}_p$ satisfying $|a|_p \leq 1$ has a unique representative Cauchy sequence $\{a_i\}$ such that*

(1) $a_i \in \mathbb{Z}$, $0 \leq a_i < p^i$ for $i = 1, 2, \ldots,$ and

(2) $a_i \equiv a_{i+1} \pmod{p^i}$ for $i = 1, 2, \ldots$.

Proof. Let $\{b_i\}$ be a Cauchy sequence representing $a \in \mathbb{Q}$. We want to find an equivalent sequence satisfying the two properties. Since $|b_i|_p \to |a|_p$ as i gets larger, we can disregard a finite number of initial terms if necessary. Then, given $\varepsilon > 0$, we can say that $|b_i|_p \leq 1+\varepsilon$ for i large enough. Since $\{b_i\}$ is a Cauchy sequence, for every $j \in \mathbb{N}$, let $N(j)$ be a positive integer such that $|b_i - b_{i'}|_p \leq p^{-j}$, for all $i, i' \geq N(j)$. We may take the sequence of numbers, $N(j)$, to be strictly increasing with j, so we can say that $N(j) \geq j$. At this point, we need a lemma.

Lemma 19. *If $x \in \mathbb{Q}$ and $|x|_p \leq 1$, then for any i there exists an integer α such that $|\alpha - x|_p \leq p^{-i}$. α can be chosen from the set $\{0, 1, 2, \ldots, p^i - 1\}$ and is unique if chosen in this range.*

Proof. Let $x = \frac{a}{b}$ where $\gcd(a, b) = 1$. Since $|x|_p \leq 1$, we know that

$$p^{-(\mathrm{ord}_p a - \mathrm{ord}_p b)} = p^{-\mathrm{ord}_p a} p^{\mathrm{ord}_p b} \leq 1.$$

Note that if p divides b, then $\mathrm{ord}_p b \geq 1$, and since $\gcd(a, b) = 1$, then $\mathrm{ord}_p\, a = 0$. Thus, if p divides b, then $p^{-\mathrm{ord}_p a} p^{\mathrm{ord}_p} = p^0 p^k$ for some $k \in \mathbb{N}$, which is clearly greater than 1. Thus, we know that p does not divide b and we can say that $\gcd(b, p^i) = 1$. Hence, we can find integers m and n such that $mb + np^i = 1$. Let $\alpha = am$. Then,

$$|\alpha - x|_p = \left| am - \frac{a}{b} \right|_p = \left| \frac{a}{b} \right|_p |mb - 1|_p \leq |mb - 1|_p = |np^i|_p = |n|_p p^{-i} \leq p^{-i}.$$

Using the strong triangle inequality, $|\alpha - x|_p \leq \max\{|\alpha|_p, |x|_p\}$, we can add or subtract a multiple of p^i for which the above inequality still holds and obtain an integer in the set $\{0, 1, 2, \ldots, p-1\}$. □

So, from Lemma 19, we can find integers a_j, where $0 \leq a_j < p^j$, such that

$$|a_j - b_{N(j)}|_p \leq p^{-j}.$$

We claim that $a_j \equiv a_{j+1} \mod p^j$ and $(b_i) \sim (a_i)$.

The first assertion is true because

$$\begin{aligned} |a_{j+1} - a_j|_p &= |a_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} - (a_j - b_{N(j)})|_p \\ &\leq \max\{|a_{j+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{N(j)}|_p, |a_j - b_{N(j)}|_p \\ &\leq \max\left\{\frac{1}{p^{j+1}}, \frac{1}{p^j}, \frac{1}{p^j}\right\} \\ &= \frac{1}{p^j}. \end{aligned}$$

Thus, $a_j \equiv a_{j+1} \pmod{p^j}$.

Now, we show that $(b_i) \sim (a_i)$. Fix any j. Then, for $i \geq N(j)$ we have

$$\begin{aligned} |a_i - b_i|_p &= |a_i - a_j + a_j - b_{N(j)} - (b_i - b_{N(j)})|_p \\ &\leq \max\{|a_i - b_i|_p, |a_j - b_{N(j)}|_p, |b_i - b_{N(j)}|_p\} \\ &= \max\left\{\frac{1}{p^j}, \frac{1}{p^j}, \frac{1}{p^j}\right\} \\ &= \frac{1}{p^j}. \end{aligned}$$

Thus, $|a_i - b_i|_p \longrightarrow 0$ as $i \to \infty$ and $(b_i) \sim (a_i)$.

Finally, we prove that $\{a_n\} \in \{\mathbb{Q}\}$ is the unique Cauchy sequence representing $a \in \mathbb{Q}_p$. Let $\{a'_i\}$ be a Cauchy sequence such that $\{a'_i\} \neq \{a_i\}$ and let $\{a'_i\}$ satisfy the two requirements of the theorem. Thus, $a_{i_0} \neq a'_{i_0}$ for some i_0. Then, we have $a_{i_0} \not\equiv a'_{i_0} \mod p^{i_0}$ since both a_{i_0} and a'_{i_0} are between 0 and p^{i_0}. Then from requirement (2), for $i > i_0$,

$$a_i \equiv a_{i_0} \not\equiv a'_{i_0} \equiv a'_i \mod p^{i_0}.$$

Therefore, $a_i \not\equiv a'_i \mod p^{i_0}$. However, this means that $|a_i - a'_i|_p > \frac{1}{p^{i_0}}$ for all $i \geq i_0$, which implies that $(a_i) \not\sim (a'_i)$, and thus $\{a_i\}$ is unique. □

By Theorem 18, if $a \in \mathbb{Q}_p$ and $|a|_p \leq 1$, then each a_i of the sequence can be expressed by

$$a_i = d_0 + d_1 p + \cdots + d_{i-1} p^{i-1}$$

where each d_i is from the set $\{0, 1, 2, \ldots, p-1\}$. The condition that $a_i \equiv a_{i+1} (\text{mod } p^i)$ gives us

$$a_{i+1} = d_0 + d_1 p + \cdots + d_{i-1} p^{i-1} + d_i p^i$$

where each of the p-adic digits up to d_{i-1} are the same for each expansion. Then we can see that $a \in \mathbb{Q}_p$ is the following series, which is convergent in the p-adic norm:

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

This can be thought of as a number written in base p with the p-adic digits expanding infinitely far to the left, and we can write this number in the more convenient form:

$$a = \ldots d_n d_{n-1} \ldots d_2 d_1 d_0.$$

We call this the *canonical form* of a, and we can see that this form mimics our usual decimal form in $\mathbb{R}$. Instead of our numbers being closer together as the decimal form extends to the right, we can see that the p-adic norm makes our numbers closer together by higher powers of p extending to the left. That is why our ellipses replace our higher powers of p as they replace our "less significant" digits, just as they replace the digits to the right in the infinite decimal expansion of the elements of $\mathbb{R}$.

We can also see that the cardinality of $\mathbb{Q}_p$ is the same as *the continuum* or the same cardinality as $\mathbb{R}$. We can mimic Cantor's proof for showing that the set of real numbers from $[0, 1]$ is uncountable to show that $\mathbb{Q}_p$ is uncountable. We use the "diagonalization method" to attempt to create a one-to-one map from $\mathbb{N}$ to $\mathbb{Q}_p$. However, just as in the real case, we create a new element that is not on the list that is the diagonal of the list of numbers. Thus, we conclude that $\mathbb{Q}_p$ is uncountable.

In the cases when $|a|_p > 1$, we can multiply a by a high power of p, to obtain a new p-adic number $a' = ap^m$ that satisfies $|a'|_p = 1$, and we can apply Theorem 18.

Thus,

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

where $d_{-m} \neq 0$ and our canonical form becomes

$$\ldots d_n \ldots d_2 d_1 d_0 . d_{-1} \ldots d_{-m}.$$

We note that the canonical form can never have infinitely many digits to the right because if $x \in \mathbb{Q}$, then the highest power of p that divides the denominator of x must be some finite integer m that will translate to a p-adic canonical form ending with d_{-m} and terminating.

In the next chapter, we will explore our new space $\mathbb{Q}_p$, perform arithmetic and examine some of the algebraic properties.

Chapter 2

Algebra of $\mathbb{Q}_p$

2.1 Arithmetic

Let us begin by showing some examples of expressing numbers in canonical form. For example, in $\mathbb{Q}_5$, let us write the canonical form of 37, -1 and -37. To do this, we will need to find the coefficients d_i in the series

$$\frac{d_{-m}}{5^m} + \frac{d_{m-1}}{5^{m-1}} + \cdots + d_0 + d_1 \cdot 5 + d_2 \cdot 5^2 + \cdots .$$

Exercise 20. *Find the canonical forms of* 37, -1 *and* -37 *in* $\mathbb{Q}_5$.

Since we are working in $\mathbb{Q}_5$, we know that each $d_i \in \{0, 1, 2, 3, 4\}$. We see that

$$37 = 1 \cdot 5^2 + 2 \cdot 5^1 + 2 \cdot 5^0.$$

Thus, our canonical form of 37 in $\mathbb{Q}_5$ is $\ldots 0122$.

To find the canonical form of -1, we need to think about what we really seek. Clearly, our series above is the sum of positive powers of p, all of whose coefficients are either positive or zero. However, we know that $\mathbb{Q}_5$ is a field, so we know that every element has an additive inverse. Thus, instead of "-1", what we really seek is the additive inverse of 1. Thus, we would like to find the d_i's such that

$$\ldots 0001 + \ldots d_3 d_2 d_1 d_0 . d_{-1} \ldots d_{-m} = \ldots 0000.$$

Clearly the d's with a negative index are all zeros since 0 and 1 have all zeros in those positions. Now, we see that $1 + d_0 \equiv 0 \pmod 5$, and since $d_0 \in \{0, 1, 2, 3, 4\}$, the only choice that we have is 4, noting that we will have to regroup a 1 into the d_1 term because 4+1 creates an extra multiple of 5^1. Now, we need to find d_1 such that

$$0 + (d_1 + 1) \equiv 0 \text{ (mod 5)}.$$

Again, d_1 must be 4, carrying another 1 into the d_2 term, which continues infinitely to the left. Thus,

$$-1 \text{ in } \mathbb{Q}_5 = \ldots 4444.$$

Similarly, to find -37, we seek the additive inverse of 37 in $\mathbb{Q}_5$, or the additive inverse of $\ldots 0122$. We start with d_0 first. Noting that $2 + d_0 \equiv 0 \pmod 5$, we find that $d_0 = 3$, regrouping a 1 to the d_1 term. Solving for d_1, we have

$$2 + (d_1 + 1) \equiv 0 \text{ (mod 5)} \;\Rightarrow\; d_1 = 2,$$

regrouping a 1 to the d_2 term. Solving for d_2, we have

$$1 + (d_2 + 1) \equiv 0 \text{ (mod 5)} \;\Rightarrow\; d_2 = 3,$$

regrouping a 1 to the d_3 term. Solving for d_3, we have

$$0 + (1 + d_3) \equiv 0 \text{ (mod 5)} \Rightarrow d_3 = 4,$$

regrouping a 1 to the d_4 term. Just as in the case with finding the canonical form of -1, the digit 4 will now repeat, so $d_i = 4$ for $i > 2$. Thus,

$$-37 \text{ in } \mathbb{Q}_5 = \ldots 444323.$$

We perform arithmetic in $\mathbb{Q}_p$ in the expected way. We use the canonical form of our elements and perform arithmetic base p, regrouping when needed. Here are some examples of addition and multiplication in $\mathbb{Q}_5$.

$$\begin{array}{rcr} & \ldots & 4104 \\ + & \ldots & 1432 \\ \hline & \ldots & 1041 \end{array}$$

$$\begin{array}{rcr} & \ldots & 4104 \\ \times & \ldots & 1432 \\ \hline & \ldots & 3213 \\ & \ldots & 23120 \\ & \ldots & 143100 \\ & \ldots & 4104000 \\ \hline & \ldots & 3433 \end{array}$$

Exercise 21. *Find the canonical forms of $\frac{1}{3}$ and $\frac{1}{7}$ in $\mathbb{Q}_5$.*

This is similar to the method to find $-1 \in \mathbb{Q}_5$, as we have no fractions in our canonical form. So we again use the fact that $\mathbb{Q}_5$ is a field. We know that we seek the multiplicative inverses of 3 and 7 in $\mathbb{Q}_5$. Again, we find that we do not need the negative indexes of d. Let the canonical form of the multiplicative inverse of 3 in $\mathbb{Q}_5$ be $\ldots d_3d_2d_1d_0$. Then, we know that

$$\begin{array}{ccc} & \ldots & d_3d_2d_1d_0 \\ \times & \ldots & 0\ 0\ 0\ 3 \\ \hline & \ldots & 0\ 0\ 0\ 1 \end{array}$$

Solving for d_0, we know that $3d_0 \equiv 1 \pmod 5$, and since $d_0 \in \{0,1,2,3,4\}$, the only choice will be $d_0 = 2$, and we will have to regroup a 1 to the d_1 digit. Solving for d_1, we have $3d_1 + 1 \equiv 0 \pmod 5 \Rightarrow 3d_1 \equiv 4 \pmod 5 \Rightarrow d_1 = 3$. Now, we'll have to regroup a 2 to the d_2 digit. Solving for d_2, we have $3d_2+2 \equiv 0 \pmod 5 \Rightarrow 3d_2 \equiv 3 \pmod 5 \Rightarrow d_2 = 1$. We regroup a 1 to the d_3 digit. We see that the digits will repeat, in a way analagous to the infinite decimal expansion of some fractions in $\mathbb{R}$. Thus,

$$\frac{1}{3} \text{ in } \mathbb{Q}_5 \text{ is } \ldots 1313132.$$

Finding $\frac{1}{7}$ in $\mathbb{Q}_5$ is slightly more difficult. We seek the multiplicative inverse of 7 in $\mathbb{Q}_5$, or the multiplicative inverse of $\ldots 0012$. Now, the computation will require regrouping from multiplication and addition.

$$\begin{array}{cccccc} & \ldots & d_3 & d_2 & d_1 & d_0 \\ \times & \ldots & 0 & 0 & 1 & 2 \\ \hline & \ldots & 2d_3 & 2d_2 & 2d_1 & 2d_0 \\ & \ldots & d_2 & d_1 & d_0 & 0 \\ \hline & \ldots & 0 & 0 & 0 & 1 \end{array}$$

We begin solving for our p-adic digits on the right. $2d_0 \equiv 1 \pmod 5 \Rightarrow d_0 = 3$. Solving for d_1, we have a regrouping of 1 from the multiplication of $2 \cdot d_0$. Thus we get

$$(2d_1 + 1) + 3 \equiv 0 \ (\text{ mod } 5) \Rightarrow 2d_1 \equiv 1 \ (\text{ mod } 5) \Rightarrow d_1 = 3.$$

So far, our multiplication looks like

$$\begin{array}{cccccc} & \ldots & d_3 & d_2 & 3 & 3 \\ \times & \ldots & 0 & 0 & 1 & 2 \\ \hline & \ldots & 2d_3 & 2d_2 & 2 & 1 \\ & \ldots & d_2 & 3 & 3 & 0 \\ \hline & \ldots & 0 & 0 & 0 & 1 \end{array}$$

Solving for d_2, we have a regrouping from the multiplication and addition.

$((2d_2+1)+1)+3 \equiv 0 \ (\bmod 5) \Rightarrow 2d_2+5 \equiv 0 \ (\bmod 5) \Rightarrow 2d_2 \equiv 0 \ (\bmod 5) \Rightarrow d_2 = 0.$

We continue to solve for our p-adic digits in this way, and we find that

$$\frac{1}{7} \text{ in } \mathbb{Q}_5 \text{ is } \ldots 412032412032412032.$$

There are six repeating digits, just as there are six repeating digits in the infinite decimal expansion of $\frac{1}{7}$ in $\mathbb{R}$. Later in this chapter, we pose the question, "Is $\mathbb{Q}_p$ isomorphic to $\mathbb{R}$?"

2.2 Polynomials in $\mathbb{Q}_p$

Now, we begin to see that $\mathbb{Q}_p$ contains elements not in $\mathbb{Q}$. We know that $\mathbb{Q}_p$ contains every element in $\mathbb{Q}$ because we can construct a constant Cauchy sequence for any $x \in \mathbb{Q}$, which we know has a representative in $\mathbb{Q}_p$. We know that $\mathbb{Q}$ with respect to the standard absolute yields a completion, $\mathbb{R}$ that properly contains $\mathbb{Q}$. Similarly, we will see that $\mathbb{Q}_p$ properly contains $\mathbb{Q}$.

Exercise 22. *Find $\sqrt{6}$ and $\sqrt{7}$ in $\mathbb{Q}_5$.*

Note that the canonical form of 6 in $\mathbb{Q}_5$ is ...0011. Now, let us consider this in polynomial form, or that we are looking for roots of the equation $x^2 - 6 = 0$ in $\mathbb{Q}_5$. Let a be such that $a^2 = ...0011 = 1 + 1 \cdot 5 + 0 \cdot 5^2 + \cdots$. Let the canonical form of a be $\ldots d_2 d_1 d_0$. We solve for our d_i's by equating coefficients in corresponding terms of the expansion. We know that $d_0^2 \equiv 1 \pmod 5$. We must examine the two cases, $d_0 = 1$ and $d_0 = 4$.

Case 1 : $d_0 = 1$. When expanding the square of a, we see that our "5" term is $d_0 d_1 + d_0 d_1 = 2d_0 d_1 = 2d_1$. Setting this equal to the coefficient of 5 in the canonical form of 6, we get that $2d_1 \equiv 1 \pmod 5 \Rightarrow d_1 = 3$.

Now, we solve for d_2. We know that $(1 + 3 \cdot 5 + d_2 \cdot 5^2 + \ldots)^2 = 1 + 1 \cdot 5 + 0 \cdot 5^2 + \ldots$. Now, we will have a regrouping into the 5^2 term:

$$\begin{aligned}(1+3\cdot 5+d_2\cdot 5^2+\cdots)^2 &= 1+(3+3)5+((1)d_2+3\cdot 3+(1)d_2)5^2+\cdots \\ &= 1+6\cdot 5+(2d_2+9)5^2+c\ldots \\ &= 1+1\cdot 5+5\cdot 5+(2d_2+9)5^2+\cdots \\ &= 1+1\cdot 5+(2d_2+10)5^2+\cdots.\end{aligned}$$

Equating coefficients, we get that

$$2d_2 + 10 \equiv 0 \mod 5 \Rightarrow 2d_2 \equiv 0 \pmod 5 \Rightarrow d_2 = 0.$$

Proceeding on, we find $d_3 = 4$. Thus, $a = \ldots 4031$.

We see that there will be regrouping of terms for each d_i and each one would have to be found separately. As we solve for more terms, the question arises of the form of the canonical expansions square roots in $\mathbb{Q}_p$. We saw that some canonical expansions of fractions (multiplicative inverses) had repeating digits and infinite expansions to the left in their respective canonical expansions. Finding the first three terms of the canonical expansion of $\sqrt{6}$ in $\mathbb{Q}_5$ and noticing that further regroupings are present for each term, we suspect that square roots in $\mathbb{Q}_p$ have infinite nonrepeating canonical expansions to the left. We will approach this subject in a future study.

Case 2 : $d_0 = 4$. Let a' denote this expansion of $\sqrt{6}$. Note that in this case, we have a regrouping of 3 to the d_1 term:

$$\begin{aligned}(4 + d_1 \cdot 5 + \cdots)^2 &= 16 + (4d_1 + 4d_1) \cdot 5 + \cdots \\ &= 1 + 3 \cdot 5 + (8d_1)5 + \cdots \\ &= 1 + (8d_1 + 3)5 + \cdots .\end{aligned}$$

Equating coefficients, we get that

$$8d_1 + 3 \equiv 1 \pmod 5 \Rightarrow 3d_1 \equiv 3 \pmod 5 \Rightarrow d_1 = 1.$$

Solving for d_2, we have several terms to regroup:

$$\begin{aligned}(4 + 1 \cdot 5 + d_2 \cdot 5^2 + \ldots)^2 &= 16 + (4 + 4) \cdot 5 + (4d_2 + 1 \cdot 1 + 4d_2) \cdot 5^2 + \cdots \\ &= 1 + 3 \cdot 5 + 8 \cdot 5 + (8d_2 + 1) \cdot 5^2 + \cdots \\ &= 1 + 1 \cdot 5 + 2 \cdot 5^2 + (8d_2 + 1) \cdot 5^2 + \cdots \\ &= 1 + 1 \cdot 5 + (8d_2 + 3) \cdot 5^2 + \cdots .\end{aligned}$$

Equating coefficients, we get $8d_2 + 3 \equiv 0 \pmod 5 \Rightarrow 3d_2 \equiv 2 \pmod 5 \Rightarrow d_2 = 4$. Solving for d_3 in a similar way, we get $d_3 = 0$.

Thus, $a' = \ldots 0414$. It is no surprise that a' is the additive inverse of a in $\mathbb{Q}_5$, so we can think of a as $\sqrt{6}$ and a' as $-\sqrt{6}$ just as the additive inverses $\sqrt{6}$ and $-\sqrt{6}$ are both roots of the equation $x^2 - 6 = 0$.

Now, we must find $\sqrt{7}$ in $\mathbb{Q}_5$. Note that 7 in $\mathbb{Q}_5$ is $\ldots 0012$. Thus, if $a = \sqrt{7}$, and the canonical form of a is $\ldots d_3d_2d_1d_0$, then

$$(d_0 + d_1 \cdot 5 + d_2 \cdot 5^2 + \cdots)^2 = 2 + 1 \cdot 5 + 0 \cdot 5^2 + \cdots .$$

We continue in the same way as before, equating coefficients, but when we solve for our first digit, d_0, we get that $d_0^2 \equiv 2 \pmod 5$. However, there is no 5-adic digit whose square is equivalent to 2 (mod 5). Thus, we say that $\sqrt{7} \notin \mathbb{Q}_5$, and we have that

$$\sqrt{12}, \sqrt{17}, \sqrt{22}, \cdots \notin \mathbb{Q}_5 \text{ and } \sqrt{-3}, \sqrt{-8}, \sqrt{-13}, \cdots \notin \mathbb{Q}_5$$

because we similarly cannot solve for d_0 in their respective expansions.

Note that in $\mathbb{Q}_p$ where p is an odd prime, once we solve for d_0 in the expansion of an irrational square root from the set $\{1, \ldots, p-1\}$, we will always be able to solve for the subsequent digits. This is because the equations to solve for the subsequent digits are always of the form $2d_0d_k + m \equiv n \pmod p$ where m is a combination of previously solved p-adic digits and $n \in \{0, 1, 2, \ldots, p-1\}$. It is clear that these equations can be solved for each d_k since we know that $d_0 \neq 0$. This is not the case in $\mathbb{Q}_2$. The $2d_0d_k$ term will always be supressed because it is equivalent to 0 (mod 2) and we will be left with

$$m \equiv n \ (\text{ mod } 2)$$

which may lead to a contradiction.

Exercise 23. *Find a polynomial with integer coefficients that has a root modulo 2 but has no roots in $\mathbb{Q}_2$.*

Working in $\mathbb{Q}_2$, we find that the first integer that does not have a square root in $\mathbb{Q}_2$ is 3. The canonical form of 3 in $\mathbb{Q}_2$ is $\ldots 0011$. Letting a be such that $a^2 = 3$ in $\mathbb{Q}_2$, and letting the canonical form of a be $\ldots d_3d_2d_1d_0$ we get that

$$(d_0 + d_1 \cdot 2 + d_2 \cdot 2^2 + \cdots)(d_0 + d_1 \cdot 2 + d_2 \cdot 2^2 + \cdots) = 1 + 1 \cdot 2 + 0 \cdot 2^2 + \cdots .$$

We have $d_0^2 \equiv 1 \pmod 2 \Rightarrow d_0 = 1$, but we cannot solve for d_1:

$$d_0d_1 + d_0d_1 \equiv 1 \ (\text{ mod } 2) \Rightarrow 2d_1 \equiv 1 \ (\text{ mod } 2).$$

Thus, $\sqrt{3} \notin \mathbb{Q}_2$ and $x^2 - 3 = 0$ does not have a solution in $\mathbb{Q}_2$. Clearly, 1 is a root modulo 2 because $1^2 - 3 = -2 \equiv 0 \pmod 2$.

Now, we will see that $\mathbb{Q}_p$ contains a representative element that is not in $\mathbb{R}$. Since we have no negative numbers in $\mathbb{Q}_p$, we interpret negative numbers as additive inverses.

Exercise 24. *Show that $\sqrt{1-p} \in \mathbb{Q}_p$ where p is an odd prime.*

Working in $\mathbb{Q}_p$ where p is an odd prime, we see that $1 - p$ is the additive inverse of $p - 1$, which has a canonical form of $\ldots 000(p-1)$. Thus, the canonical form $1 - p$ is $\ldots(p-1)(p-1)(p-1)1$. We claim that the equation $d_0^2 \equiv 1 \pmod p$ always has a solution in the set $\{0, 1, 2, \ldots, p-1\}$. Clearly 1 is a solution. Also, $p - 1$ will always be a solution since $(p-1)^2 = p^2 - 2p + 1 \equiv 1 \pmod p$. As we solve for each d_k, we have seen that all equations to solve for subsequent coefficients will be of the form

$$2d_k + m \equiv n \ (\bmod p), \ \ m, n \in \{0, 1, 2, \ldots, p-1\},$$

which can always be solved as long as p is an odd prime. The ability to solve for subsequent terms is not guaranteed when $p = 2$. We saw in Exercise 22 that the ability to solve for d_0 does not guarantee that we can solve for later terms in $\mathbb{Q}_2$. Note that in $\mathbb{Q}_2$, $\sqrt{1-p} = \sqrt{-1}$. The canonical form of -1 is $\ldots 1111$. We can easily solve for d_0 because

$$d_0^2 \equiv 1 \ (\bmod 2) \Rightarrow d_0 = 1.$$

However, the problem arises when we attempt to solve for d_1:

$$2d_1 \equiv 1 \ (\bmod 2)$$

which has no solutions.

We now introduce a theorem that will play an important role in the solvability of polynomials in $\mathbb{Q}_p$.

Theorem 25. *(Hensel's Lemma) Let $F(x) = c_0 + c_1 x + \cdots + c_n x^n$ be a polynomial whose coefficients are p-adic integers. Let*

$$F'(x) = c_1 + 2c_2 x + 3c_3 x^2 + \ldots n c_n x^{n-1}$$

be the derivative of $F(x)$. Suppose $\bar{a}_0$ is a p-adic integer that satisfies $F(\bar{a}_0) \equiv 0 \pmod{p}$ and $F'(\bar{a}_0) \not\equiv 0 \pmod{p}$. Then there exists a unique p-adic integer a such that $F(a) = 0$ and $a \equiv \bar{a}_0 \pmod{p}$.

Proof. We prove the theorem by induction on k in the statement, "There exists a p-adic integer of the form

$$a_k = b_0 + b_1 p + b_2 p^2 + \cdots + b_k p^k,$$

where each $b_k \in \{0, 1, 2, \ldots, p-1\}$, such that $F(a_k) \equiv 0 \pmod{p^{k+1}}$ and $a_k \equiv \bar{a}_0 \pmod{p}$."

Initial step : We take b_0 equal to the first p-adic digit of $\bar{a}_0$. Then $a_0 \equiv \bar{a}_0 \pmod{p}$ and $F(a_0) \equiv 0 \pmod{p}$.

Induction step : Assume that $a_{k-1} = b_0 + b_1 p + b_2 p^2 + \cdots + b_{k-1} p^{k-1}$ is such that $F(a_{k-1}) \equiv 0 \pmod{p^{k+1}}$ and $a_{k-1} \equiv \bar{a}_0 \pmod{p}$. Let $a_k = a_{k-1} + b_k p^k$ for some $b_k \in \{0, 1, 2, \ldots, p-1\}$ to be determined. We expand $F(a_k)$ ignoring the terms divisible by p^{k+1} because we only need to consider the terms that are not congruent to zero modulo p^{k+1}.

$$\begin{aligned} F(a_k) &= F(a_{k-1} + b_k p^k) \\ &= \sum_{i=0}^{n} c_i (a_{k-1} + b_k p^k)^i \\ &= c_0 + \sum_{i=1}^{n} c_i (a_{k-1}^i + i a_{k-1}^{i-1} b_k p^k + \cdots) \\ &\equiv F(a_{k-1} + b_k p^k) F'(a_{k-1}) \; (\bmod\ p^{k+1}). \end{aligned}$$

Since $F(a_{k-1}) \equiv 0 \pmod{p^k}$ by the assumption, we can say that

$$F(a_k) \equiv \alpha_k p^k + b_k p^k F'(a_{k-1}) \; (\bmod\ p^{k+1})$$

for some integer $\alpha_k \in \{0, 1, 2, \ldots, p-1\}$. Thus, we come to the following equation, which we can solve for b_k:

$$\alpha_k + b_k F'(a_{k-1}) \equiv 0 \; (\bmod\ p).$$

Since $a_{k-1} \equiv \bar{a}_0 \pmod{p}$ from the assumption, we know $F'(a_{k-1}) \not\equiv 0 \pmod{p}$. Therefore, we can divide by $F'(a_{k-1})$. Thus,

$$b_k = \frac{-\alpha_k}{F'(a_{k-1})} \; (\bmod\ p).$$

Substituting our value for b_k in our earlier equation for the equivalence of $F(a_k)$ mod p^{k+1}, we get $F(a_k) \equiv 0 \pmod{p^{k+1}}$, which concludes the induction step.

To prove that the p-adic integer a is unique, let

$$a = b_0 + b_1 p + b_2 p^2 + \cdots$$

Then $F(a) = 0$ since for all k we have $F(a) \equiv F(a_k) \equiv 0 \pmod{p^{k+1}}$. It immediately follows that a is unique because the sequence $\{a_k\}$ is unique from Theorem 18. □

Hensel's Lemma allows us to construct a Cauchy sequence where finding each term is analagous to approximating a root of a polynomial. This method of approximation is the p-adic analog to Newton's method of finding a root of a polynomial with real coefficients. In Newton's method, having a particular approximation, a_{n-1}, we solve for the next approximation, a_n by

$$a_n = a_{n-1} - \frac{f(a_{n-1})}{f'(a_{n-1})}.$$

The value $\frac{f(a_{n-1})}{f'(a_{n-1})}$ is very similar to the "correction term" in the proof of Hensel's Lemma when we solve for b_k in the induction step. However, the initial conditions on the approximate solution $\bar{a}_0$ guarantee that the Cauchy sequence $\{a_k\}$ will converge to a root, a, while the initial guess of Newton's method must be "sufficiently close" to an actual root for the sequence of approximations, $\{a_n\}$ to converge to that root.

2.3 Algebraic Structure of $\mathbb{Q}_p$

We can also consider the algebraic properties of a particular subset of $\mathbb{Q}_p$, called the p-adic integers, which we will denote $\mathbb{Z}_p$.

Definition 26. *The* ***p-adic integers*** *or $\mathbb{Z}_p$ are the set of all $a \in \mathbb{Q}_p$ where the canonical form of a contains only nonnegative powers of p. Thus,*

$$\mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i \right\}.$$

From our earlier arithmetical computations, we can see that $\mathbb{Z}_p$ is still closed under addition and multiplication. All other proprties of a commutative ring with unity are inherited from $\mathbb{Q}_p$. Clearly, $\mathbb{Z}_p$ has no zero divisors because it is a subset of $\mathbb{Q}_p$, which also has no zero divisors. However, $\mathbb{Z}_p$ is not a field because it has nonzero elements that do not have multiplicative inverses. In fact, any $a \in \mathbb{Z}_p$ where $a_0 = 0$ does not have a multiplicative inverse because in this case,

$$\begin{array}{crr} & \dots & d_3d_2d_1d_0 \\ \times & \dots & a_3a_2a_1\;0 \\ \hline & \dots & 0\;0\;0\;1 \end{array}$$

we cannot solve for d_0. Thus, we have that $\mathbb{Z}_p$ is an integral doman, just as $\mathbb{Z}$ is an integral domain. We can also say that $\mathbb{Z}_p = \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\}$ because, by definition of $\mathbb{Z}_p$, we know that the canonical form of a cannot contain any negative powers of p. Thus, $\text{ord}_p\, a \geq 0$ and $|a|_p \leq 1$. Reverse containment follows.

Since we know that $\mathbb{Z}_p$ has some elements that do have multiplicative inverses, we can form a new set of just the elements of Z_p that are invertible.

Definition 27. *The set of invertible elements of $\mathbb{Z}_p$, denoted by $\mathbb{Z}_p^\times$, is the set*

$$\mathbb{Z}_p^\times = \Big\{ \sum_{i=0}^{\infty} a_i p^i \mid a_0 \neq 0 \Big\}.$$

It is clear that $\mathbb{Z}_p \ncong \mathbb{Z}$. We see that $\mathbb{Z}_p$ has infinitely many units, while $\mathbb{Z}$ only has two, 1 and -1. We also see that $\mathbb{Z}_p^\times$ is an Abelian group under multiplication. The multiplicative identity, 1, is clearly in $\mathbb{Q}_p^\times$. Associativity and commutivity are inherited from $\mathbb{Q}_p$ and inverses are included by the definition of the set. Finally, the set must be closed under multiplication because we know that two elements of $\mathbb{Z}_p^\times$, say a and b, will have p-adic digits a_0 and b_0 from the set $\{1, 2, \dots, p-1\}$. Since p is prime, we know that $a_0 b_0 \not\equiv 0 \mod p$ and $ab \in \mathbb{Z}_p^\times$. The set $\mathbb{Z}_p^\times$ is referred to as the group of p-adic units.

We know that $\mathbb{Q}_p$ is a field, as is $\mathbb{R}$. It is natural to check if the two fields are isomorphic. We expect that they are not isomorphic, as we have shown that $\sqrt{7} \notin \mathbb{Q}_5$ and $\sqrt{-4} \in \mathbb{Q}_5$. If $\mathbb{R}$ and $\mathbb{Q}_p$ were isomorphic, the study of p-adic numbers would be trivial. We will begin by assuming that the two fields are isomorphic and hope to reach a contradiction.

Exercise 28. *Show that $\mathbb{R}$ and $\mathbb{Q}_p$ are not isomorphic.*

Proof. Assume that $\mathbb{R}$ and $\mathbb{Q}_p$ are isomorphic. Then there exists a field isomorphism $\varphi : \mathbb{R} \longrightarrow \mathbb{Q}_p$ such that

$$\varphi(a + b) = \varphi(a) + \varphi(b) \text{ for all } a, b \in \mathbb{R},$$

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \text{ for all } a, b \in \mathbb{R},$$

$$\varphi(0) = 0 \text{ and } \varphi(1) = 1.$$

Note that

$$\varphi(p) = \varphi(\underbrace{1 + 1 + \cdots + 1}_{p \text{ addends}}) = \underbrace{\varphi(1) + \varphi(1) + \cdots + \varphi(1)}_{p \text{ addends}} = \underbrace{1 + 1 + \cdots + 1}_{p \text{ addends}} = p.$$

Let us consider $\varphi(\sqrt{p})$. Clearly $\sqrt{p} \in \mathbb{R}$. By the properties of isomorphisms, we know that $\varphi(\sqrt{p}) = \sqrt{\varphi(p)}$. Thus, we need to find the element $a \in \mathbb{Q}_p$ such that $a^2 = p$. Let $\ldots d_2 d_1 d_0 . d_{-1} \ldots d_{-m}$ be the canonical expansion of a. Then,

$$\begin{array}{rl} \ldots & d_3 d_2 d_1 d_0 . d_{-1} \ldots d_{-m} \\ \times \quad \ldots & d_3 d_2 d_1 d_0 . d_{-1} \ldots d_{-m} \\ \hline \ldots & 0\ 0\ 1\ 0\ .\ 0\ \ldots\ 0 \end{array}$$

We know that each $d_i \in \{0, 1, 2, \ldots, p-1\}$. We start from the right, solving for d_{-m}. The only way we can get $d_{-m} \cdot d_{-m} = 0$ is to have $d_{-m} = 0$. Since p is prime, no digit from the set $\{0, 1, 2, \ldots, p-1\}$ squared can be a multiple of p. We continue in this manner, finding each p-adic digit is zero until we get to d_1. By equating coefficients, we see that

$$d_0 d_1 + d_0 d_1 \equiv 1(\bmod p) \quad \Rightarrow \quad 0 d_1 + 0 d_1 \equiv 1(\bmod p) \quad \Rightarrow \quad 0 \equiv 1(\bmod p),$$

which is a contradiction. Thus, $\sqrt{p} \notin \mathbb{Q}_p$ and $\mathbb{R}$ is not isomorphic to $\mathbb{Q}_p$. □

We next show that $\mathbb{Q}_p$ is not isomorphic to $\mathbb{Q}_q$ for any two distinct primes, p and q. The proof will require the following lemma.

Lemma 29. *For any prime p and any positive integer m that is relatively prime to p, there exists a primitive m^{th} root of unity in $\mathbb{Q}_p$ if and only if $m \mid (p-1)$.*

Proof. Let $m \mid (p-1)$. Then $p - 1 = km$ for some $k \geq 1$. Thus, every m^{th} root of unity is also a $(p-1)^{\text{th}}$ root of unity. Let $f(x) = x^{p-1} - 1$, so $f'(x) = (p-1)x^{p-2}$. Choose $x_0 \in \mathbb{Q}_p^\times$ to be any integer in the set $\{1, 2, \ldots, p-1\}$. Then $f(x_0) \equiv 0(\bmod p)$. (Using the usual notation of $\mathbb{Z}_p$ being the field of the integers from 0 to $p-1$, we know that $a^{p-1} \equiv 1(\bmod p)$ for all $a \in \mathbb{Z}_p$ because $\mathbb{Z}_p$ is cyclic.) Also, $f'(x_0) \not\equiv 0(\bmod p)$ because $|f'(x_0)|_p = 1$. These are exactly the condtions that we stated for Hensel's Lemma, Theorem 25. Thus $f(x)$ has exactly $p-1$ solutions, the $(p-1)$ roots of 1, which we have seen are also m^{th} roots of 1. We know that at least one of the m^{th} roots of 1 will be a primitive root because the roots will be in the form $e^{2\pi i \frac{k}{m}}$, $k = 1, \ldots, m$. We know that the case for $k = 1$ or any k relatively prime to m will be a primitive m^{th} root of 1.

Conversely, let α be a primitive mth root of unity in $\mathbb{Q}_p$. Thus $\alpha^m = 1$ and by the properties of a norm, $|\alpha|_p = 1$, which tells us that $\alpha \in \mathbb{Z}_p$. Let α_0 be the terminating digit on the right in the canonical form of α. Then, $\alpha_0^m \equiv 1 \pmod{p}$. However, we also know that $\alpha_0^{p-1} \equiv 1 \pmod{p}$ for any choice of α_0. It follows that $m \mid (p-1)$. □

Theorem 30. *$\mathbb{Q}_p$ and $\mathbb{Q}_q$ are not isomorphic for any two distinct primes, p and q.*

Proof. We will proceed by assuming $\mathbb{Q}_p \cong \mathbb{Q}_q$ for two distinct primes p and q, then we constuct an isomorphism $\varphi : \mathbb{Q}_p \longrightarrow \mathbb{Q}_q$ as in Exercise 28. Let us choose an m such that m divides $p - 1$ and m does not divide $q - 1$. We claim that there always exists an m such that the previous statement is true for distinct primes p and q.

Choose $m = p-1$, then m clearly divides $p-1$. (If we find that our chosen m also divides $q - 1$, then we choose m instead to be $q - 1$ without loss of generality. Since $p \neq q$, then we know that $m = q - 1$ does not divide $p - 1$.)

By Lemma 29, we know that there exists a primitive m^{th} root of unity in $\mathbb{Q}_p$, which we will denote as α. We have that $\alpha \in \mathbb{Q}_p$ and we have shown that $\alpha \in \mathbb{Z}_p$. Thus,

$$\varphi(\alpha) = \varphi(\underbrace{1 + 1 + \cdots + 1}_{\alpha \text{ addends}}) = \underbrace{\varphi(1) + \varphi(1) + \ldots \varphi(1)}_{\alpha \text{ addends}} = \underbrace{1 + 1 + \cdots + 1}_{\alpha \text{ addends}} = \alpha.$$

We know that $\alpha^m = 1$ in $\mathbb{Q}_p$. It follows that $\varphi(\alpha^m) = 1$ in $\mathbb{Q}_q$. By the properties of an isomorphism, we know that $(\varphi(\alpha))^m = 1$ in $\mathbb{Q}_q$ and finally $\alpha^m = 1$ in $\mathbb{Q}_q$. However this means that α is an m^{th} root of unity in $\mathbb{Q}_q$. Since we know that α is a primitive m^{th} root of unity in $\mathbb{Q}_p$, that implies α is also a primitive m^{th} root of unity in $\mathbb{Q}_q$ by the properties of an isomorphism. Thus, by Lemma 21, $m \mid q - 1$, which is a contradiction. Thus, $\mathbb{Q}_p$ is not isomorphic to $\mathbb{Q}_q$. □

Chapter 3

Analysis in $\mathbb{Q}_p$

3.1 Convergence and Cauchy Sequences

We recall that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic norm. Thus, $\mathbb{Q}_p$ is a complete metric space, and by definition, every Cauchy sequence in $\mathbb{Q}_p$ converges to some element in $\mathbb{Q}_p$. Thus, we need to characterize Cauchy sequences in $\mathbb{Q}_p$ in order to study convergence.

Theorem 31. *A sequence $\{a_n\}$ in $\mathbb{Q}_p$ is a Cauchy sequence if and only if it satisfies*

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

Proof. We assume that $\{a_n\}$ is a Cauchy sequence in $\mathbb{Q}_p$, then, by definition,

$$\lim_{m,n\to\infty} |a_m - a_n|_p = 0.$$

Thus, we obtain the desired result for $m = n + 1$.

Conversely, we assume that $\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0$. Then we know that for any $\varepsilon > 0$, there exists a positive integer N such that for any $n > N$, $|a_{n+1} - a_n|_p < \varepsilon$. Now, taking $m > n > N$, consider $|a_m - a_n|_p$. Using the strong triangle inequality of a non-Archimedean norm, we have

$$\begin{aligned}|a_m - a_n|_p &= |a_m - a_{m-1} + a_{m-1} - a_{m-2} + a_{m-2} - a_{m-3} + \cdots + a_{n+1} - a_n|_p \\ &\le \max\{|a_m - a_{m-1}|_p, |a_{m-1} - a_{m-2}|_p, \ldots, |a_{n+1} - a_n|_p\} < \varepsilon\end{aligned}$$

Thus, $\{a_n\}$ is a Cauchy sequence in $\mathbb{Q}_p$. □

We are now ready to prove our assertion from Chapter 1 that $\mathbb{Q}$ is not complete with respect to the p-adic norm, $|\cdot|_p$. To accomplish this, we will construct a Cauchy sequence of rational numbers that will converge to an element not in $\mathbb{Q}$, namely the square root of some integer, a, which is not a perfect square. We will need to do this proof twice, once for $|\cdot|_p$ where p is an odd prime and once for $|\cdot|_2$. The reason we need two cases follows from the results of Exercise 22. When p is an odd prime, we know that if we can solve for d_0 in the canonical form of a square root, we are guaranteed to be able to solve for each subsequent d_i. However, this result will not hold in $\mathbb{Q}_2$. Solving for d_1 will yield an equation of the form $2d_0d_1 + m \equiv n \pmod 2$ which may not have a solution.

First, we prove a lemma that establishes the existence of the sequence we need.

Lemma 32. *A p-adic integer*

$$x = a_0 + a_1p + a_2p^2 + \cdots$$

is a solution in $\mathbb{Q}_p$ of an equation $X^2 = m$ if and only if the sequence

$$(a_0,\ a_0 + a_1p,\ a_0 + a_1p + a_2p^2, \ldots)$$

is a coherent sequence of solutions of the congruences $x^2 \equiv m(\bmod p^n)$.

Proof. Assume that $x \in \mathbb{Z}_p$ is a solution in $\mathbb{Q}_p$ of an equation $X^2 = m$. Then

$$m = a_0^2 + (2a_0a_1)p + (2a_0a_2 + a_1^2)p^2 + \cdots .$$

We prove the statement via mathematical induction.

Initial Step: $n = 1$. The first solution of our sequence is $x_0 = a_0$. Note

$$x_0^2 = a_0^2 \equiv m(\bmod p).$$

Induction Step: Assume that $x_{n-1} = a_0 + a_1p + a_2p^2 + \cdots + a_{n-1}p^{n-1}$. Then

$$\begin{aligned} x_{n-1}^2 &= (a_0 + a_1p + a_2p^2 + \cdots + a_{n-1}p^{n-1})^2 \\ &= a_0^2 + (2a_0a_1)p + \cdots + (2a_0a_{n-2} + 2a_1a_{n-3} + \cdots)p^{n-2} + \cdots . \\ &\equiv m(\bmod p^{n-1}). \end{aligned}$$

Let $x_n = a_0 + a_1p + a_2p^2 + \cdots + a_np^n$. Then

$$\begin{aligned} x_n^2 &= a_0^2 + (2a_0a_1)p + \cdots + (2a_0a_{n-2} + 2a_1a_{n-3} + \cdots)p^{n-2} \\ &\quad +(2a_0a_{n-1} + 2a_1a_{n-2} + \cdots)p^{n-1} + \cdots \\ &\equiv x_{n-1}^2 + (2a_0a_{n-1} + 2a_1a_{n-2} + \cdots)p^{n-1}(\bmod p^n) \\ &\equiv m(\bmod p^n) \end{aligned}$$

Conversely, let $x = a_0 + a_1p + a_2p^2 + \cdots$ and let $(a_0,\ a_0 + a_1p,\ a_0 + a_1p + a_2p^2, \ldots)$ be a coherent sequence of solutions of the congruences $x^2 \equiv m(\text{mod } p^n)$. Then, we have

$$\lim_{n\to\infty} x_n \equiv m(\bmod p^n)$$

implies x is a solution to $X^2 = m$ in $\mathbb{Q}_p$. □

Theorem 33. *$\mathbb{Q}$ is not complete with respect to the p-adic norm, $|\cdot|_p$.*

Proof. Let p be an odd prime. Let $a \in \mathbb{Z}$ be such that $\sqrt{a} \notin \mathbb{Q}$, p does not divide a, and a is a quadratic residue modulo p, or there is an integer solution to the equation $x^2 \equiv a \mod p$. In other words, if we choose a such that a is not a perfect square but a is some multiple of p plus some perfect square, that will satisfy the above conditions. Now, we will construct a Cauchy sequence, $\{d_n\}$, with respect to the p-adic norm that will converge to a number that is not in $\mathbb{Q}$, namely $\sqrt{a}$.

By the way we chose a, we are guaranteed to find at least one solution the equation

$$x^2 \equiv a(\bmod p).$$

We choose $x \in \mathbb{Q}_p$ to be any solution to that equation. Then, we construct the sequence $\{d_n\}$ of coherent solutions in Lemma 32. We saw in Exercise 22 that if p is an odd prime, we are guaranteed to be able to solve for subsequent digits of the canonical form of square roots once we solve for the initial digit, d_0. The construction of this sequence is done in a similar way because once we know that d_0 is a solution to $x^2 \equiv a(\bmod p)$. We choose each subsequent d_n, noting that

$$d_n \equiv d_{n-1}(\bmod p^n) \text{ and } d_n^2 \equiv a(\bmod p^{n+1}).$$

Now, we need to show that $\{d_n\}$ is a Cauchy sequence with respect to the p-adic norm. From the way that we constructed our sequence, we have

$$|d_n - d_{n-1}|_p = |k_n p^n|_p \leq p^{-n} \text{ for some } k_n \in \mathbb{Z}$$

and

$$\lim_{n\to\infty} p^{-n} = 0.$$

Thus, $\{d_n\}$ is a Cauchy sequence. However, we also know that

$$|d_n^2 - a|_p = |\kappa_n p^{n+1}|_p \leq p^{-(n+1)} \text{ for some } \kappa_n \in \mathbb{Z}$$

and

$$\lim_{n\to\infty} p^{-(n+1)} = 0.$$

This implies that the sequence $\{d_n\}$ converges to $\sqrt{a}$, which is not in $\mathbb{Q}$, and thus, we have shown that $\mathbb{Q}$ is not complete with respect to the p-adic norm where p is an odd prime.

To show that $\mathbb{Q}$ is not complete with respect to the 2-adic norm, we mimic the above proof to construct a Cauchy sequence with elements in $\mathbb{Q}$ that converge to $\sqrt[3]{3}$ with respect to $|\cdot|_2$. In Exercise 22, we saw that finding square roots of elements in $\mathbb{Q}_2$ lead to problems when we tried to find d_1 in the canonical form. When finding a cube root, we will not have have coefficients disappear that are congruent to 0 (mod 2). Thus, we will be able to find the needed sequence.

We choose $a = 3$ and note that $3 \equiv 1 \pmod 2$. We can certainly find an $x \in \mathbb{Q}_2$ such that $x^3 \equiv 1 \pmod 2$. Considering the p-adic expansion of x, we have

$$x^3 = a_0^3 + (3a_0^2 a_1) \cdot 2 + (3a_0^2 a_2 + 3a_0 a_1^2) \cdot 2^2 + \cdots .$$

As in the case where p is an odd prime, we have a sequence of coherent solutions to $x^3 \equiv 3 \pmod{2^n}$,

$$(a_0^3,\ a_0^3 + (3a_0^2 a_1) \cdot 2,\ a_0^3 + (3a_0^2 a_1) \cdot 2 + (3a_0^2 a_2 + 3a_0 a_1^2) \cdot 2^2, \ldots)$$

This sequence satisfies

$$d_n \equiv d_{n-1}(\bmod 2^n) \text{ and } d_n^3 \equiv 3(\bmod 2^{n+1}).$$

We next show that this sequence is a Cauchy sequence with respect to the 2-adic norm.

$$|d_n - d_{n-1}|_2 = |k_n 2^n|_2 \leq 2^{-n} \text{ for some } k_n \in \mathbb{Z}$$

and

$$\lim_{n\to\infty} 2^{-n} = 0.$$

Thus, $\{d_n\}$ is a Cauchy sequence. However, we also know that

$$|d_n^3 - 3|_2 = |\kappa_n 2^{n+1}|_2 \leq 2^{-(n+1)} \text{ for some } \kappa_n \in \mathbb{Z}$$

and

$$\lim_{n\to\infty} 2^{-(n+1)} = 0.$$

Thus, $\mathbb{Q}$ is also not complete with respect to the $|\cdot|_p$ and $\mathbb{Q}$ is not complete with respect to $|\cdot|_p$ for any prime, p. □

It is now clear why we had to construct $\mathbb{Q}_p$ as the completion of $\mathbb{Q}$ with respect to the p-adic norm in the way that we did. We know that there exist Cauchy sequences with elements in $\mathbb{Q}$ that do not converge to an element in $\mathbb{Q}$ with respect to the p-adic norm. Thus, to form the compeltion of $\mathbb{Q}$ with respect to the p-adic norm, we must consider all sequences that are Cauchy with respect to that norm and form the new field that contains all of $\mathbb{Q}$ together with all the limits of Cauchy sequences.

We continue with a closer analysis of Cauchy sequences in $\mathbb{Q}_p$.

Exercise 34. *Decide if the following sequences converge in $\mathbb{Q}_p$, and find the limit of those that do.*

a. $a_n = n!$

b. $a_n = n$

c. $a_n = p^n$

d. $a_n = \dfrac{1}{n}$

a. The sequence $a_n = n!$ will converge. Note

$$|(n+1)! - n!|_p = |n!(n+1-1)|_p = |n! \cdot n|_p.$$

As n gets larger, $n! \cdot n$ will be divisible by a very high power of p and thus $|n! \cdot n|_p$ will converge to zero, thus the sequence converges. We see that $\lim_{n\to\infty} |n!|_p = 0$.

b. The sequence $a_n = n$ will diverge. We notice that for any n,

$$|(n+1) - n|_p = |1|_p = p^0 = 1.$$

In order for the sequence to converge, we need $\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0$. Thus, $a_n = n$ will diverge.

c. The sequence $a_n = p^n$ will converge. Note

$$\left|p^{n+1} - p^n\right|_p = \left|p^n(p+1)\right|_p = |p^n|_p|p+1|_p = |p^n|_p \cdot 1.$$

Clearly, $|p^n|$ approaches zero as n gets larger, thus the sequence converges to zero.

d. The sequence $\frac{1}{n}$ will diverge. Note

$$\begin{aligned} \left|\frac{1}{n+1} - \frac{1}{n}\right|_p &= \left|\frac{n}{n(n+1)} - \frac{n+1}{n(n+1)}\right|_p \\ &= \left|\frac{n-(n+1)}{n(n+1)}\right|_p \\ &= \left|\frac{-1}{n(n+1)}\right|_p \end{aligned}$$

Note that as $n \to \infty$,

$$\left|\frac{-1}{n(n+1)}\right|_p$$

could be large if $p^k|n$ or $p^k|n+1$ for large k. Thus, the sequence diverges.

3.2 Convergence of Series

We now look at the convergence of series in $\mathbb{Q}_p$ and see that a particular series that is clearly divergent in $\mathbb{R}$ is convergent in $\mathbb{Q}$.

Definition 35. *We say that the series $\sum_{i=1}^{\infty} a_i \in \mathbb{Q}_p$* ***converges in $\mathbb{Q}_p$*** *if the sequence of partial sums, $S_n = \sum_{i=1}^{n} a_i$ converges in $\mathbb{Q}_p$. The series converges* absolutely *if $\sum_{i=1}^{\infty} |a_i|_p$ converges in $\mathbb{R}$.*

Theorem 36. *If a series $\sum |a_i|_p$ converges in $\mathbb{R}$, then $\sum a_i$ converges in $\mathbb{Q}_p$.*

Proof. Assuming that $\sum |a_i|_p$ converges in $\mathbb{R}$, then by definition, the sequence of its partial sums converges and, thus, is a Cauchy sequence. Therefore, for any $\varepsilon > 0$, there exists an integer N such that for all n, m with $m > n > N$, we have

$$\sum_{i=n+1}^{m} |a_i|_p < \varepsilon.$$

Now, we want to show that $\{S_n\}$ is a Cauchy sequence in $\mathbb{Q}_p$. We use the triangle inequality property of a norm to see that

$$|S_m - S_n| = \left| \sum_{i=n+1}^{m} a_i \right|_p \leq \sum_{i=n+1}^{m} |a_i|_p < \varepsilon.$$

Thus, $\{S_n\}$ is a Cauchy sequence in $\mathbb{Q}_p$ and $\sum a_i$ converges in $\mathbb{Q}_p$. □

Exercise 37. *Prove that* $\sum\limits_{n=1}^{\infty} n^2 \cdot (n+1)! = 2$ *in $\mathbb{Q}_p$ for any p.*

Proof. Fix a prime, p. In order to show that the series converges, we will show that

$$\sum_{n=1}^{\infty} \left| n^2 \cdot (n+1)! \right|_p$$

converges in $\mathbb{R}$.

Fix $\varepsilon > 0$. Let $\{S_n\}$ be a sequence of partial sums of the above sequence. Choose $m \in \mathbb{N}$ such that $\frac{1}{p^m} < \varepsilon$. Then, for all $n > p^m$ we will have

$$|S_n - S_{n-1}|_p = |n^2 \cdot (n+1)!|_p < \frac{1}{p^m}.$$

Thus, $\{S_n\}$ is a Cauchy sequence and $\sum_{n=1}^{\infty} |n^2(n+1)!|_p$ converges in $\mathbb{R}$. Thus, by Theorem 33, we know that that $\sum_{n=1}^{\infty} n^2 \cdot (n+1)!$ converges in $\mathbb{Q}_p$.

Note that

$$\sum_{n=1}^{\infty} n^2 \cdot (n+1)! = 2 + \sum_{n=2}^{\infty} n^2 \cdot (n+1)!.$$

We claim

$$\sum_{n=2}^{N} n^2 \cdot (n+1)! = (N+2)!(N-1).$$

We prove this via mathematical induction.

Initial Step : When $N = 2$, we have

$$\sum_{n=2}^{2} n^2 \cdot (n+1)! = 2^2 \cdot (3!) = 4! \cdot (1) = (2+2)! \cdot (2-1).$$

Induction Step : Assume

$$\sum_{n=2}^{N-1} n^2 \cdot (n+1)! = ((N-1)+2)! \cdot ((N-1)-1) = (N+1)! \cdot (N-1).$$

Then,

$$\begin{aligned}\sum_{n=2}^{N} n^2 \cdot (n+1)! &= (N+1)! \cdot (N-2) + N^2 \cdot (N+1)! \\ &= (N+1)! \cdot (N^2 + N - 2) \\ &= (N+1)! \cdot (N+2) \cdot (N-1) \\ &= (N+2)! \cdot (N-1).\end{aligned}$$

It now follows that for $N \geq p^m$,

$$\begin{aligned}\left| \sum_{n=1}^{N} n^2 \cdot (n+1)! - 2 \right|_p &= \left| 2 + \sum_{n=2}^{N} n^2 \cdot (n+1)! - 2 \right|_p \\ &= \left| (N+2)! \cdot (N-1) \right|_p \\ &\leq \left| N^2 \cdot (N+1)! \right|_p \\ &< \frac{1}{p^m} \\ &< \varepsilon.\end{aligned}$$

which we can guarantee choosing N large enough.

Thus, we have

$$\lim_{N\to\infty}\left|\sum_{n=1}^{N} n^2\cdot(n+1)!-2\right|_p = 0, \text{ and}$$

$$\sum_{n=1}^{\infty} n^2\cdot(n+1)! = 2 \text{ in } \mathbb{Q}_p \text{ for any } p.$$

□

3.3 Functions and Derivatives

In this section, we consider such topics from Real Analysis such as the Intermediate Value Theorem, the Mean Value Theorem and the Chain Rule, and examine if these results hold in $\mathbb{Q}_p$. We will begin with the Intermediate Value Theorem, but it will be helpful to first look at additional topological properties of $\mathbb{Q}_p$ as a complete metric space.

We will begin by showing that open balls in $\mathbb{Q}_p$ are both open and closed. The proof will require the following lemmas.

Lemma 38. *If* $|x-a|_p < |a|_p$, *then* $|x|_p = |a|_p$.

Proof. Let $|x-a|_p < |a|_p$. Using the strong triangle inequality of the p-adic norm, we have that

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

Now, to prove the inequality in the other direction, we have that

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

We want to show that $\max\{|x-a|_p, |x|_p\} = |x|_p$. Assume that $|x-a|_p > |x|_p$. One property that holds for all norms is $|x-a|_p \leq |x|_p + |a|_p$. (This is true from the triangle inequality $|x+a|_p \leq |x|_p + |a|_p$ and the fact that $|-a|_p = |a|_p$.) Then, if we have $|x-a|_p > |x|_p$, that would imply that $|a|_p \leq |x-a|_p$. However, this contradicts our assumption that $|x-a|_p < |a|_p$. Thus, we know that

$$\begin{aligned} |x-a|_p \leq |x|_p &\Rightarrow \max\{|x-a|_p, |x|_p\} = |x|_p \\ &\Rightarrow |a|_p \leq |x|_p. \end{aligned}$$

Since we have shown $|a|_p \geq |x|_p$ and $|a|_p \leq |x|_p$, we conclude that $|a|_p = |x|_p$. □

Lemma 39. *The sphere $S(a,r)$ in $\mathbb{Q}_p$ is an open set.*

Proof. Let $x \in S(a,r)$ and let $\varepsilon < r$. In order to show that $S(a,r)$ is open, we will show that $B(x,\varepsilon) \subset S(a,r)$. Let $y \in B(x,\varepsilon)$. Then, $|x-y|_p < |x-a|_p = r$ because $\varepsilon < r$. Then, $|x-y+a-a|_p < |x-a|_p$ and $|(x-a)-(y-a)|_p < |x-a|_p$. By Lemma 38, this implies $|y-a|_p = |x-a|_p = r$. But this implies $y \in S(a,r)$ and we have that the sphere, $S(a,r)$ is an open set in $\mathbb{Q}_p$. (This is certainly not true in $\mathbb{R}$, where any sphere is closed.) □

Theorem 40. *Open balls in $\mathbb{Q}_p$ are both open and closed.*

Proof. Let $B(a,r)$ be an open ball in $\mathbb{Q}_p$. In order to prove that $B(a,r)$ is also closed, we will show that its complement is open. By definition, $B(a,r) = \{x \in \mathbb{Q}_p \mid |x-a|_p < r\}$. Let C be the complement of $B(a,r)$. Then, we have that C is the union of the sphere $S(a,r)$ and the set $D = \{x \in \mathbb{Q}_p \mid |x-a|_p > r\}$. We have shown that $S(a,r)$ is open. Now, we need to show that D is open.

Let $y \in D$. Then $|y-a|_p = r_1 > r$. Now construct the open ball, $B\Big(y, \frac{r_1-r}{2}\Big)$. We claim that $B\Big(y, \frac{r_1-r}{2}\Big)$ is open in D. Let $z \in B\Big(y, \frac{r_1-r}{2}\Big)$. By the triangle in equality, we have that $|y-a|_p \le |z-a|_p + |z-y|_p < |z-a|_p + \Big(\frac{r_1-r}{2}\Big)$. Thus,

$$\begin{aligned} |z-a|_p &> |y-a|_p - \Big(\frac{r_1-r}{2}\Big) \\ &= r - \Big(\frac{r_1-r}{2}\Big) \\ &= \frac{r}{2} + \frac{r_1}{2} \\ &> \frac{r}{2} + \frac{r}{2} \\ &= r. \end{aligned}$$

Thus, $z \in D$ by the definition of D and $B\Big(y, \frac{r_1-r}{2}\Big)$ is open in D. Hence, D is open. This is what we needed to show that C is open, as the finite union of open sets in any metric space is open. Finally, we have that the complement of $B(a,r) \in \mathbb{Q}_p$ is open, and thus $B(a,r)$ is both open and closed. □

This is a surprising result, as there are no nonempty proper subsets in $\mathbb{R}$ that are both open and closed.

Now, in order to approach the subject of the Intermediate Value Theorem in the p-adic context, we need to examine what it means for points and sets to be connected in $\mathbb{Q}_p$.

Definition 41. *A set S is said to be* ***disconnected*** *if there exist two open sets U_1 and U_2 such that*

(1) $U_1 \cap U_2 = \varnothing$,

(2) $S = \{S \cap U_1\} \cup \{S \cap U_2\}$,

(3) $S \cap U_1 \neq \varnothing$ *and* $S \cap U_2 \neq \varnothing$.

Theorem 42. $\mathbb{Q}_p$ *is a* ***totally disconnected*** *set. That is, the connected component of any point $x \in \mathbb{Q}_p$ is the set consisting of only x.*

Proof. Let x, $y \in \mathbb{Q}_p$ and let $|x - y|_p = r$. We seek the sets U_1 and U_2 from Definition 39. Let $U_1 = B(x, \frac{r}{2})$ and let U_2 be the complement of U_1. Clearly U_1 is open, and therefore also closed. Thus, U_2 is open. By definition of a complement, $U_1 \cap U_2 = \varnothing$. Also, we know that $\mathbb{Q}_p = U_1 \cup U_2 = \{\mathbb{Q}_p \cap U_1\} \cup \{\mathbb{Q}_p \cap U_2\}$. Finally, since $x \in \mathbb{Q}_p \cap U_1$ and $y \in \mathbb{Q}_p \cap U_2$, neither set is empty, which satisfies our three conditions. Since $x \notin U_2$ and $y \notin U_1$ we have that $\mathbb{Q}_p$ is a totally disconnected set. □

Now, we are finally ready to approach the subject of the Intermediate Value Theorem in the p-adic context. The Intermediate Value Theorem states that the image of an interval under a continuous function $f : \mathbb{R} \longrightarrow \mathbb{R}$ is an interval. This is actually just a special case of a broader version of the theorem that is true in any metric space: the image of a connected set under a continuous function is a connected set. Since $\mathbb{Q}_p$ is a metric space, this theorem also applies, but the only connected sets in $\mathbb{Q}_p$ are the sets consisting of only one point. Thus, the Intermediate Value Theorem for $\mathbb{Q}_p$ would be: "The image of a point under a continuous function is a point!"

However, we will see that the Mean Value Theorem in the p-adic context does not hold, even in a trivial sense.

Proposition 43. *It is not the case that:*
If a function $f(X)$ is differentiable with continuous derivative on $\mathbb{Q}_p$ then for any two numbers a, $b \in \mathbb{Q}_p$, there exists an element, $\xi \in \mathbb{Q}_p$ of the form $\xi = at + b(1-t)$ for some

t, where $|t|_p \leq 1$ for which we have $f(b) - f(a) = f'(\xi)(b-a)$.
In other words, the p-adic Mean Value Theorem is false.

Proof. Let $x \in \mathbb{Q}_p$ and let $f(x) = x^p - x$. In addition, let $a = 0$ and $b = 1$. We defined the derivative of a function in $\mathbb{Q}_p$ in Theorem 22 (Hensel's Lemma), which is what we would expect the derivative to be. Thus $f'(x) = px^{p-1} - 1$ and $f(a) = f(b) = 0$. So, for the theorem to be true, we would need to find a ξ such that $p\xi^{p-1} - 1 = 0$. We know that $\xi = at + b(1-t) = 1 - t$ for some $|t|_p \leq 1$. This means precisely that $t \in \mathbb{Z}_p$. Thus, we have seen from our arithmetic that ξ itself must belong to $\mathbb{Z}_p$. We consider the canonical form of $p\xi^{p-1} - 1$. Since this number is one less than some multiple of p, we know that the p-adic digit $a_0 \neq 0$. Thus, from Definition 24 of $\mathbb{Z}_p^\times$ from Chapter 2, we know that $p\xi^{p-1} - 1$ is in the group of p-adic units, and clearly $p\xi^{p-1} - 1 \neq 0$ for any $\xi \in \mathbb{Q}_p$. □

This counterexample is heavily dependent on the choice of f. We found a function whose derivative resulted in values that are one less than a multiple of p, and we found that those numbers were in a multiplicative subgroup of our field that does not contain zero.

Now, we consider the Chain Rule in $\mathbb{Q}_p$ to see if we see similar problems when computing derivatives.

Theorem 44. *Let $f, g : \mathbb{Q}_p \longrightarrow \mathbb{Q}_p$ be two functions where g is differentiable at a point x and f is differentiable at a point $y = g(x)$. Then $(f \circ g)' = f'(g(x)) \cdot g'(x)$.*

It is clear that the standard proof of the Chain Rule in $\mathbb{R}$ will hold in $\mathbb{Q}_p$ because the Chain Rule is dependent on the limit definition of the derivative and the facts that f and g are differentiable at those particular points. We see that the problem function from our Mean Value Theorem, $f(x) = x^p - x$, is certainly differentiable at any point $x \in \mathbb{Q}_p$ because $f'(x) \in \mathbb{Q}_p$.

We have seen different results in analytical properties of $\mathbb{Q}_p$. We have examined standard results of Real Analysis and found that one result held, one result was entirely false, and one was only true in a trivial sense. In a future study, we will examine more closely how the p-adic norm affects analysis.

Chapter 4

Conclusion

In this study, we examined some of the fundamentals of the space $\mathbb{Q}_p$. We defined a non-Archimedean norm and looked at how the strong triangle inequality affects our new space. We found that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ as a metric space with respect to the p-adic norm. We constructed the completion of $\mathbb{Q}$ with respect to a norm. When constructing Cauchy sequences of rational numbers, we can see that most Cauchy sequences with respect to the standard absolute value will not be Cauchy sequences with respect to the p-adic norm and vice versa.

The algebraic structure of $\mathbb{Q}_p$ does hold silimarities to its real counterpart. We have seen that $\mathbb{Q}_p$ and $\mathbb{R}$ are nonisomorphic fields while $\mathbb{Z}$ and $\mathbb{Z}_p$ are nonisomorphic integral domains. There are differences, however. For example. we saw that there exists a nontrivial subset of $\mathbb{Z}_p$ that is an Abelian group under multiplication, which is certainly not true for $\mathbb{Z}$.

In the study of the analysis of $\mathbb{Q}_p$, we saw large differences in comparison with real analysis. This is because the p-adic norm is a much different way to measure the distance between two points than the standard absolute value. This creates open sets in $\mathbb{Q}_p$ that are also closed, which is not the case in the topology of $\mathbb{R}$. In fact, since we have seen that $\mathbb{Q}_p$ is a totally disconnected set, topologically, the only useful balls to consider would be those with radii that are powers of p.

The study of p-adic numbers does provide a deeper understanding into the fields of analysis and algebra. It provides new and complex examples of familiar topics and structures, allowing for deeper learning from a different perspective.

Bibliography

[Abb01} Stephen Abbott. *Understanding analysis.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2001.

[Fai13] Jane Fairfax. Cauchy sequences of rational numbers, January 2013.

[Fra67] John B. Fraleigh. *A first course in abstract algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1967.

[Gou97] Fernando Q. Gouvêa. *p-adic numbers.* Universitext. Springer-Verlag, Berlin, second edition, 1997. An introduction.

[Kat07] Svetlana Katok. *p-adic analysis compared with real,* volume 37 of *Student Mathematical Library.* American Mathematical Society, Providence, RI, 2007.