6-2011

An Introduction to the p-adic Numbers

Charles I. Harrington
Union College - Schenectady, NY

AN INTRODUCTION TO

THE p-adic NUMBERS

By

Charles Irving Harrington

****

Submitted in partial fulfillment

of the requirements for

Honors in the Department of Mathematics

UNION COLLEGE

June, 2011

Abstract

HARRINGTON, CHARLES An Introduction to the p-adic Numbers. Department of Mathematics, June 2011.

ADVISOR: DR. KARL ZIMMERMANN

One way to construct the real numbers involves creating equivalence classes of Cauchy sequences of rational numbers with respect to the usual absolute value. But, with a different absolute value we construct a completely different set of numbers called the p-adic numbers, and denoted $\mathbb{Q}_p$. First, we take an intuitive approach to discussing $\mathbb{Q}_p$ by building the p-adic version of $\sqrt{7}$. Then, we take a more rigorous approach and introduce this unusual p-adic absolute value, $|\ |_p$, on the rationals to the lay the foundations for rigor in $\mathbb{Q}_p$. Before starting the construction of $\mathbb{Q}_p$, we arrive at the surprising result that all triangles are isosceles under $|\ |_p$. Then, we quickly construct $\mathbb{Q}_p$ and extend $|\ |_p$ from the rationals. Next, we leave equivalence classes of Cauchy sequences behind and introduce a more understandable view of numbers in $\mathbb{Q}_p$. With this view, we compute some p-adic numbers and observe that these computations are similar to analogous computations in the real numbers. Then, we end our tour of $\mathbb{Q}_p$ with a proof of Hensel's Lemma—a result describing a general approach to building p-adic numbers. Lastly, we move to finite field extensions of $\mathbb{Q}_p$. We extend $|\ |_p$ to these field extensions with the help of the norm function, and end the paper with two important propositions that characterize most finite field extensions of $\mathbb{Q}_p$.

Contents

1 Introduction

At an early age we are only exposed to certain numbers, the integers and rationals, restricting our grasp of mathematical concepts to only part of the number line. Later, armed with our new favorite tool, the calculator, we take on the irrationals and fully explore the real numbers while rumors of numbers existing illegally by taking the square root of a negative number float around the outskirts of our developing mathematical minds. The boundaries of manipulating numbers with sophisticated laws and axioms do not stop with the complex numbers and keep disturbing our comfort with numbers. In this paper, we go one step further, and introduce another such disturbance: the p-adic numbers.

Observe the familiar base-10 expansion of a real number, $\sqrt{7}$:

$$\sqrt{7} = 2.645\ldots = 2(10)^0 + 6(10)^{-1} + 4(10)^{-2} + 5(10)^{-3} + \cdots .$$

But, if we use a different perspective, viewing the 2-adic expansion of -1 leads to a similar looking expansion which challenges our comfort with numbers and raises interesting questions:

$$-1 = 1(2)^0 + 1(2)^1 + 1(2)^2 + 1(2)^3 + \cdots .$$

This admittedly seems suspicious, however, if we add 1 to both sides of the equation,

we have

$$\begin{aligned}
-1+1 &= 1+1+1(2)+1(2^2)+1(2^3)+\cdots \\
0 &= 0+1(2)+1(2)+1(2^2)+1(2^3)+\cdots \\
&= 0+2(2)+1(2^2)+1(2^3)+\cdots \\
&= 0+0+1(2^2)+1(2^2)+1(2^3)+\cdots \\
&= 0+0+2(2^2)+1(2^3)+\cdots \\
&= 0+0+0+2(2^3)+\cdots \\
&= 0+0+\cdots+0+\cdots .
\end{aligned}$$

Now, we are in fact simply shuffling powers of 2 farther to the right of the equation, but in the world of p-adic numbers, $p^n \to 0$ as $n \to \infty$. So, our goal is to describe a scenario in which we view 2^n as a small number when n is large. In doing so, we are really talking about "2-adic" numbers.

A more interesting number, such as $\sqrt{7}$, has an analogous representation in the 3-adic numbers (see Example 2.2 for the derivation). For now, consider

$$\sqrt{7} = 1(3)^0 + 1(3)^1 + 1(3)^2 + 0(3)^3 + 2(3)^4 + \cdots .$$

Note again the positive exponents, a signature of p-adic integers. Also, just as our familiar $\sqrt{7} \notin \mathbb{Q}$ but $\sqrt{7} \in \mathbb{R}$, this $\sqrt{7}$ is an element in a different field extending $\mathbb{Q}$: the field of 3-adic numbers $\mathbb{Q}_3$. Recall from real analysis, one way to construct the real numbers involves creating equivalence classes of Cauchy sequences of rational numbers, relative to the "usual" absolute value. Analogously, the field of p-adic numbers, $\mathbb{Q}_p$, may be constructed from the rationals with Cauchy sequences by the same procedure with a different absolute value. Whereas the familiar $|\ |$ ignores the sign of a number, the p-adic absolute value, $|\ |_p$, unintuitively measures the divisibility

of a number by a fixed prime p. We will make sense of our p-adic expansions using the fact that p^n is very small in terms of this absolute value. Now, we present other concrete properties of the p-adics and show how we formed the 3-adic expansion of $\sqrt{7}$. Our first approach is to intuitively explain the behavior of the p-adic numbers, and then we will take a more mathematically rigorous approach.

2 Foundations

2.1 p-adic Expansions: An Intuitive Approach

Before diving into an example, we define a useful property underlying our p-adic expansions.

Definition 2.1. Let p be a prime. We say a sequence (α_n) of integers with $0 \leq \alpha_n \leq p^{n+1} - 1$ is *coherent* if, for every $n \geq 0$, we have

$$\alpha_{n+1} \equiv \alpha_n \pmod{p^{n+1}}.$$

First, we examine a number less intimidating than the irrational $\sqrt{7}$. Take $58 \in \mathbb{Q}_5$, as 5 is a comfortable base to use. We will soon see that every p-adic number can be represented in base-p, or more precisely a Laurent series [1]

$$\mathbb{Q}_p = \{a_{-n}p^{-n} + \cdots + a_0 + a_1 p + a_2 p^2 + \cdots \mid 0 \leq a_i \leq p-1\}. \tag{2.1}$$

We see below that the 5-adic expansion of 58 works the same as expanding plain, old $58 \in \mathbb{Z}$ into base-5.

Example 2.1. The 5-adic expansion of 58 is as expected, $58 = 3 + 1(5) + 2(5)^2$. The elements α_0, α_1, α_2 of the sequence (α_n) are

$$\alpha_0 = a_0 = 3$$
$$\alpha_1 = a_0 + a_1 p = 3 + 1(5) = 8$$
$$\alpha_2 = a_0 + a_1 p + a_2 p^2 = 3 + 1(5) + 2(5)^2 = 58.$$

Note that the rest of the elements in (α_n) are equal to 58, or $58 = \alpha_3 = \alpha_4 = \cdots$. Since we constructed the expansion around powers of 5, the elements 3, 8, and 58 are related by reducing modulo powers of 5. That is $58 \equiv 8 \pmod{5^2}$ and $8 \equiv 3 \pmod{5}$.

Introducing coherent sequences for integers does not seem particularly helpful, but now we use additional information to unlock the sequence for the more complicated $\sqrt{7}$.

Example 2.2. To find the 3-adic expansion of $\sqrt{7}$, we must build the expression—rather than dismantle it as in Example 2.1—by using Definition 2.1 in reverse. We want to start with the bottom term α_0 and build to $\alpha = \lim_{n\to\infty} \alpha_n = a_0 + a_1 p + a_2 p^2 + \cdots$. So, keeping some number theory in mind, we begin with

$$\alpha \equiv \alpha_0 \pmod{3}$$
$$\alpha_0 \equiv \alpha \pmod{3}$$
$$(\alpha_0)^2 \equiv (\alpha)^2 \pmod{3}.$$

Then, note we may replace $(\alpha)^2$ with 7, and

$$(\alpha_0)^2 \equiv 7 \pmod 3$$
$$(\alpha_0)^2 \equiv 1 + 2(3) \pmod 3$$
$$(\alpha_0)^2 \equiv 1 \pmod 3,$$

implying α_0 equals 1 or 2. Semi-surprisingly, the 2 begins a second 3-adic expansion that we represent with the other root to the equation $x^2 - 7 = 0$, $-\sqrt{7}$. Let us concentrate on $\alpha_0 = a_0 = 1$. We continue building our expansion and arrive at an expression for the next term in our sequence,

$$(\alpha_1)^2 \equiv (\alpha)^2 \pmod{3^2}.$$

Now, $\alpha_1 = a_0 + a_1(3) = 1 + a_1(3)$ since we must have $\alpha_1 \equiv \alpha_0 \pmod 3$, and so

$$(1 + a_1(3))^2 \equiv 7 \pmod{3^2}$$
$$1 + 2a_1(3) + (a_1)^2 3^2 = 1 + 2(3) \pmod{3^2}$$
$$2a_1(3) = 2(3) \pmod{3^2}$$
$$a_1 \equiv 1 \pmod 3,$$

meaning $a_1 = 1$ since $0 \leq a_1 \leq 2$. Next, since our coefficients are to be taken from $\{0, 1, \ldots, p-1\}$ note that $\alpha_2 = a_0 + a_1 p + a_2 p^2 = 1 + (3) + a_2(3^2)$ as $\alpha_2 \equiv \alpha_1 \pmod{3^2}$.

We show the steps for one more term;

$$\begin{aligned}
(1 + (3) + a_2(3^2))^2 &\equiv 7 \pmod{3^3} \\
1 + 2(3) + (2a_2 + 1)3^2 + 2a_2 3^3 + (a_2)^2 3^4 &\equiv 1 + 2(3) \pmod{3^3} \\
(2a_2 + 1)3^2 &= 0 \pmod{3^3} \\
2a_2 + 1 &\equiv 0 \pmod{3} \\
\Rightarrow a_2 &= 1.
\end{aligned}$$

Continuing further, we obtain our result: the aforementioned 3-adic expansion $+\sqrt{7} = 1 + 1(3) + 1(3^2) + 0(3^3) + 2(3^4) + \cdots$. Had we continued the example with $a_0 = 2$, we would get $-\sqrt{7} = 2 + 1(3) + 1(3^2) + 2(3^3) + 0(3^4) + \cdots$, the negative version of our first expansion. Just as $+\sqrt{7}$ and $-\sqrt{7}$ are related in the real numbers, we relate these numbers in the 3-adics. Observe that

$$\begin{aligned}
-(+\sqrt{7}) &= -(1 + 1(3) + 1(3^2) + 0(3^3) + 2(3^4) + \cdots) \\
&= -1 - 1(3) - 1(3^2) - 2(3^4) + \cdots \\
&= (2 - 3) + (2 - 3)(3) + (2 - 3)(3^2) + (1 - 3)(3^4) + \cdots \\
&= 2 + (2 - 1)(3) + (2 - 1)(3^2) - 1(3^3) + 1(3^4) + \cdots \\
&= 2 + 1(3) + 1(3^2) + (2 - 3)(3^3) + 1(3^4) + \cdots \\
&= 2 + 1(3) + 1(3^2) + 2(3^3) + 0(3^4) + \cdots \\
&= -\sqrt{7}.
\end{aligned}$$

With an intuitive understanding of p-adic expansions, we now turn our attention to the p-adic absolute value, $|\ |_p$, to make our argument more rigorous.

2.2 Absolute Values

The absolute value lays the groundwork for the rigor required to construct the p-adics. We define it as follows. To set notation, let $\mathbb{R}_+ = \{r \in \mathbb{R} \mid r \geq 0\}$.

Definition 2.2. An *absolute value* on a field F is a function

$$|\ | : F \to \mathbb{R}_+$$

that satisfies the following conditions:

i) $|x| = 0$ if and only if $x = 0$

ii) $|xy| = |x||y|$ for all $x, y \in F$

iii) $|x + y| \leq |x| + |y|$ for all $x, y \in F$.

We will say an absolute value on F is *non-archimedean* if it satisfies the additional condition:

iv) $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in F$;

otherwise, we will say that the absolute value is *archimedean*.

Condition iv) of the definition is a bit unusual and will be explored after an example.

Example 2.3. Let $F = \mathbb{Q}$ and let $|\ |$ be the usual absolute value defined by

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

This absolute value is archimedean, as taking $x = y = 1$ for example, violates condition iv).

For comparison, $|\ |$ defined by

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

is non-archimedean, and is called the trivial absolute value.

The absolute value has the following properties.

Lemma 2.1. *For any absolute value $|\ |$ on a field F, we have for all $x \in F$:*

i) $|1| = 1$

ii) $|x^n| = 1 \Rightarrow |x| = 1$, *for* $n \in \mathbb{Z}$

iii) $|-1| = 1$

iv) $|-x| = |x|$

Proof. This proof follows [2, p. 27]. For the first statement, note that $|1| = |1 \cdot 1| \overset{Def 2.2}{=} |1| \cdot |1| = |1|^2$. Since $|1| = r$, a positive real number, and $r = r^2 \Rightarrow r = 1$, and we get our result. Next, $|x^n| = 1 \Rightarrow |x|^n = 1$, and once again since $|x| \in \mathbb{R}_+$ we get $|x| = 1$. For iii), see that $|-1|^2 = |(-1)^2| = |1| \overset{i)}{=} 1 \overset{ii)}{\Rightarrow} |-1| = 1$. Finally, $|-x| = |-1| \cdot |x| \overset{iii)}{=} |x|$. □

Now, we reach a critical point in our groundwork, as the next definition is tied to the p-adic absolute value.

Definition 2.3. Fix a prime number $p \in \mathbb{Z}$. The p-*adic valuation* on $\mathbb{Z}$ is the function

$$v_p : \mathbb{Z} \setminus \{0\} \to \mathbb{R}$$

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

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

We extend v_p to the field of rational numbers as follows: if $x = a/b \in \mathbb{Q} \setminus \{0\}$, then

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

and if $x = 0$, then $v_p(0) = +\infty$, treating infinity with the usual conventions.

Since v_p is an exponent, it makes sense to extend it to the rationals as the difference between the p-adic valuation of the numerator and the p-adic valuation of the denominator of a rational number. Let us compute an example for this seemingly random number.

Example 2.4. Take $v_5(3/35)$. First, $3 = 5^0(3)$ and $35 = 5^1(7)$. So, $v_5(3) = 0$ and $v_5(35) = 1$, meaning $v_5(3/35) = 0 - 1 = -1$. Now, think back to Example 2.2. We haven't defined what this p-adic valuation means in the field extending $\mathbb{Q}$, our desired field $\mathbb{Q}_p$ (this definition will come much later). But, since we conveniently have an element from $\mathbb{Q}_3$, $\sqrt{7}$, we may as well ponder $v_3(\sqrt{7})$. Recall from Example 2.2 that $\sqrt{7} = 1 + 1(3) + 1(3^2) + 0(3^3) + 2(3^4) + \cdots$. We will see that for elements of $\mathbb{Q}_p$, v_p will be determined as it is for elements of $\mathbb{Q}$. So, since $a_0 = 1 \neq 0$, we cannot factor out any powers of 3 and $\sqrt{7} = 3^0\alpha'$ where $\alpha' \in \mathbb{Q}_3$ (clearly $\alpha' = \sqrt{7}$), meaning $v_3(\sqrt{7}) = 0$.

More generally, recall from Equation (2.1) that a p-adic number may be represented as a Laurent series. So, imagine some p-adic number α, given by the expansion $\alpha = a_2p^2 + a_3p^3 + \cdots$. Then, $\alpha = p^2(a_2 + a_3p + \cdots) = p^2\alpha'$ for $\alpha' \in \mathbb{Q}_p$, and so $v_p(\alpha) = 2$. Also, as we will see in Lemma 2.2, since $v_p(ab) = v_p(a) + v_p(b)$, $v_p(\alpha) = v_p(p^2) + v_p(a_2 + a_3p + \cdots) = 2 + 0 = 2$. For expansions with negative powers, take $\lambda \in \mathbb{Q}_p$ given by $\lambda = a_{-2}p^{-2} + a_{-1}p^{-1} + a_0 + a_1p + \cdots = \frac{1}{p^2}(a_{-2} + a_{-1}p + a_0p^2 + a_1p^3 + \cdots)$. Then, λ is analogous to a rational number where $\lambda = \alpha/\beta$ with $\alpha, \beta \in \mathbb{Z}_p \subseteq \mathbb{Q}_p$, the field of p-adic integers. So, as with a rational number, $v_p(\lambda) = v_p(\alpha) - v_p(\beta) = v_p(a_{-2} + a_{-1}p + a_0p^2 + a_1p^3 + \cdots) - v_p(p^2) = 0 - 2 = -2$.

We will confirm these p-adic musings later.

Example 2.4 suggests a nice interpretation of the p-adic valuation. If we expand a number (taken from $\mathbb{Q}$ or $\mathbb{Q}_p$), v_p gives the power of the p multiplying the first non-zero number in the expansion. We will observe later that this is, in fact, the case.

Now, back to firm footing, we examine some suggestive properties of the p-adic valuation v_p on $\mathbb{Q}$ in the form of a lemma.

Lemma 2.2. *For all $x, y \in \mathbb{Q}$, we have*

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

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

Proof. i) First, let $a, b \in \mathbb{Z}$ and write $a = p^{v_p(a)}a'$ and $b = p^{v_p(b)}b'$ where $p \nmid a'$ and $p \nmid b'$, and note that since p is prime $p \nmid a'b'$. Then, $ab = p^{v_p(a)+v_p(b)}a'b' = p^{v_p(ab)}n$ for some $n \in \mathbb{Z}$, $p \nmid n$, and the result follows for v_p on $\mathbb{Z}$. So, if $x, y \in \mathbb{Q}$, $x = \frac{r}{s}$ and $y = \frac{t}{z}$ with $s, z \neq 0$, and $r, s, t, z \in \mathbb{Z}$, we see $v_p(x) = v_p(\frac{r}{s}) = v_p(r) - v_p(s)$ and $v_p(y) = v_p(\frac{t}{z}) = v_p(t) - v_p(z)$. Thus, $v_p(x) + v_p(y) = (v_p(r) + v_p(t)) - (v_p(s) + v_p(z)) = v_p(rt) - v_p(sz) = v_p(\frac{rt}{sz}) = v_p(xy)$, establishing the result for v_p on $\mathbb{Q}$.

ii) Assume $v_p(a) < v_p(b)$. Then, $a+b = p^{v_p(a)}a' + p^{v_p(b)}b' = p^{v_p(a)}(a' + p^{v_p(b)-v_p(a)}b')$, showing $v_p(a+b) = v_p(a) \geq v_p(a)$. An analogous argument works if $v_p(b) < v_p(a)$. Now, let $x, y \in \mathbb{Q}$ be as above and assume $v_p(x) < v_p(y)$. Then, $v_p(r) - v_p(s) <$

$v_p(t) - v_p(z) \Rightarrow v_p(r) + v_p(z) < v_p(t) + v_p(s) \Rightarrow v_p(rz) < v_p(ts)$. So,

$$\begin{aligned} v_p(x+y) &= v_p\left(\frac{rz+ts}{sz}\right) \\ &= v_p(rz+ts) - v_p(sz) \\ &\geq \min\{v_p(rz), v_p(ts)\} - (v_p(s) + v_p(z)) \\ &= v_p(rz) - (v_p(s) + v_p(z)) \\ &= v_p(r) - v_p(s) \\ &= v_p(x), \end{aligned}$$

and a similar argument works if we assume $v_p(y) < v_p(x)$. □

Sneakily, Lemma 2.2 suggests defining an absolute value based on the p-adic valuation. Looking back at the absolute value Definition 2.2, condition ii) and the non-archimedean condition iv) slightly resemble the above observed properties of v_p. In fact, if we make v_p an exponent and negate it, Lemma 2.2 clauses i) and ii) fulfill Definition 2.2 ii) and iv), respectively, bringing us to the p-adic absolute value.

Definition 2.4. For any $x \in \mathbb{Q} \setminus \{0\}$, we define the p-*adic absolute value* of x by

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

and we set $|0|_p = 0$.

Note that this matches our definition of v_p when $v_p(0) = +\infty$, as $|0|_p = p^{-v_p(0)} = p^{-\infty} = 0$, if we continue to treat ∞ as usual. As established in the preceding paragraph, this new absolute value is non-archimedean, making $|\ |_p$ very unfamiliar.

Example 2.5. To become more familiar, we calculate some p-adic absolute values. From Example 2.4, $|3/35|_5 = 5^{-v_5(3/35)} = 5^{-(-1)} = 5$. Also, we will see that $|\ |_p$ extends to the p-adic numbers and using $v_3(\sqrt{7}) = 0$ from the example, we find

$|\sqrt{7}|_3 = 3^0 = 1$. For the number crunchers, we try $|4243686|_{29}$. To start, $4243686 = 29^4(6)$, meaning $v_{29}(4243686) = 4$, and $|4243686|_{29} = 29^{-4} = \dfrac{1}{707281}$. In the end, we are just calculating friendly rational numbers since $|\ |_p$ is an absolute value after all.

As revealed in the introduction, numbers divisible by a high power of p are small under the p-adic absolute value. Looking to Example 2.1 for $|58|_5$, although 58 is pretty close to $50 = 2(5^2)$, 58 is not divisible by 5, and $|58|_5 = 1$. Then, while 50 is divisible by 5, $|50|_5 = \dfrac{1}{25}$ is not so small compared to $\dfrac{1}{707281}$, for example. But, take p^n (as in $\sqrt{7} = 1(3)^0 + 1(3)^1 + 1(3)^2 + 0(3)^3 + 2(3)^4 + \cdots + a_n(3^n) + \cdots$ for $p = 3$). Then, as $n \to \infty$, $|p^n|_p \to 0$ because $|p^n|_p = \dfrac{1}{p^n}$, meaning p^n becomes more divisible by p as $n \to \infty$.

To end this section, we introduce some topology to fully ensure the oddities of the p-adic absolute value (or any non-archimedean absolute value in general) sink in before leaving behind such concrete mathematics for more abstract grounds.

Definition 2.5. Let F be a field and $|\ |$ an absolute value on F. The *metric* induced by $|\ |$ is the distance $d(x, y)$ between some $x, y \in F$ and is given by

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

The set F on which the metric $d(x, y)$ is defined is called a *metric space*.

A metric, for our lowly intent and purpose, is a fancy synonym for a distance function, but distance-function-space fails to match the allure of metric space. A non-archimedean metric space—a place where $|\ |_p$ could live—measures distance strangely, as seen below.

Proposition 2.1. *Let F be a field and let $|\ |$ be a non-archimedean absolute value on F. If $x, y \in F$ and $|x| \neq |y|$, then*

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

Proof. Assume $x, y \in F$ and $|x| > |y|$, meaning $\max\{|x|, |y|\} = |x|$. We will show $|x+y| \leq |x|$ and $|x| \leq |x+y|$ to arrive at our desired equality. We get the first inequality directly from the non-archimedean condition, i.e., $|x+y| \leq \max\{|x|, |y|\} = |x|$. Next, note again by the special condition that $|x| = |(x+y)+(-y)| \leq \max\{|x+y|, |y|\}$ since $|-y| = |y|$ by Lemma 2.1. Then, either $|x| \leq |x+y|$ or $|x| \leq |y|$. But, the second relation contradicts our assumption that $|x| > |y|$, and so $|x| \leq |x+y|$. Therefore, $|x+y| = |x| = \max\{|x|, |y|\}$. Assuming $|y| > |x|$ gives an analogous result. □

It is strange that the absolute value of a sum equals the absolute value of a summand, but, applied to distances and our concept of geometry involving triangles and circles, it is even stranger.

Corollary 2.1. *Let F be as above. Then, all "triangles" in F are isosceles.*

Proof. Let $x, y, z \in F$, a non-archimedean metric space, be the vertices of our "triangle." Then, the lengths of the sides of the "triangle" are: $d(x,y) = |x-y|$, $d(y,z) = |y-z|$, and $d(x,z) = |x-z|$. Assume, for example, $d(x,y) \neq d(y,z)$. Then, $|x-y| \neq |y-z|$ and we use Proposition 2.1 to see that $d(x,z) = |x-z| = |(x-y)+(y-z)| = \max\{|x-y|, |y-z|\} = \max\{d(x,y), d(y,z)\}$. Thus, two of the sides are equal and we have an "isosceles triangle." □

We look to a concrete example to see that a non-isosceles triangle in the rationals may be isosceles in the p-adics.

Example 2.6. First, let $F = \mathbb{Q}$ with $|\ |_5$ and let $x, y, z \in \mathbb{Q}$ be vertices of a triangle. Then, for example let $x = 200$, $y = 185$, and $z = 85$. By our p-adic metric, $d(x,y) = |15|_5 = \frac{1}{5}$ and $d(y,z) = |100|_5 = \frac{1}{25}$. Since $d(x,y) \neq d(y,z)$ we know by Corollary 2.1, $d(x,z) = |x-y+y-z|_5 = |15+100|_5 = \max\{d(x,y), d(y,z)\} = \frac{1}{5}$. A simple calculation of $|115|_5$ confirms this result that $d(x,z) = d(x,y)$ and we are in fact dealing with some sort of isosceles triangle.

Next, we think intuitively again and let $F = \mathbb{Q}_p$ with $|\ |_p$ and examine the p-adic metric on the field of p-adic numbers, recalling Example 2.4 if necessary. Also, recall from Equation 2.1 that we may use a Laurent series to represent elements in $\mathbb{Q}_p$. So, let $\lambda, \mu, \nu \in \mathbb{Q}_p$ be vertices of a triangle with $\lambda - \mu = a_{-1}p^{-1} + a_0 + a_1 p + a_2 p^2 + \cdots$ and $\mu - \nu = b_1 p + b_2 p^2 + \cdots$. Then, $d(\lambda, \mu) = p \neq d(\mu, \nu) = \dfrac{1}{p}$ and the corollary says $d(\lambda, \nu) = \max\{p, \dfrac{1}{p}\} = p$, which is true, as $d(\lambda, \nu) = |\lambda - \nu|_p = |a_{-1}p^{-1} + a_0 + (a_1 + b_1)p + (a_2 + b_2)p^2 + \cdots|_p = p$.

Now, we move to circles, or balls, in this strange metric space. First, a quick definition.

Definition 2.6. Let F be a field with an absolute value $|\ |$. Let $a \in F$ and $r \in \mathbb{R}_+$. Then, the *open ball* of radius r and center a is the set

$$B(a, r) = \{x \in F \mid d(x, a) < r\} = \{x \in F \mid |x - a| < r\}.$$

The *closed ball* of radius r and center a is the set

$$\overline{B}(a, r) = \{x \in F \mid d(x, a) \leq r\} = \{x \in F \mid |x - a| \leq r\}.$$

Once again, we consider a non-archimedean metric space which includes our $|\ |_p$.

Proposition 2.2. *Let F be a field with a non-archimedean absolute value $|\ |$. Then, every point in an open or closed ball is a center of the ball.*

Proof. This proof follows [2, p.34]. Consider the open ball $B(a, r)$ with center $a \in F$ and radius $r \in \mathbb{R}_+$, and let $b \in F$ be an arbitrary point in $B(a, r)$. We will show $B(b, r) = B(a, r)$. To that end, let $x \in B(b, r)$. Then, by Definition 2.6, $|x - b| < r$. But, also since $b \in B(a, r)$, $|b - a| < r$. Thus, by the non-archimedean property, $|x - a| = |(x - b) + (b - a)| \leq \max\{|x - b|, |b - a|\} < r$, meaning $x \in B(a, r)$, and

so $B(b,r) \subseteq B(a,r)$. Similarly, we find $B(a,r) \subseteq B(b,r)$, and therefore $B(b,r) = B(a,r)$. Replace $<$ with $\leq$ to get the result for a closed ball. $\square$

As with the isosceles triangle, we discuss the open ball in $\mathbb{Q}$ and $\mathbb{Q}_p$ with $|\ |_p$ in one last example.

Example 2.7. We describe $B(3, \frac{1}{7})$ in $\mathbb{Q}$ with $|\ |_7$ by first describing the ball in the integers and then informally describing it in the rationals. The ball contains elements $a \in \mathbb{Z}$ such that $|a-3|_7 < \frac{1}{7}$, meaning $v_7(a-3) > 1$. So, if we expand $a-3$ base-7, it must equal an expansion with all powers of 7 greater than 1. Therefore, since the expansion of $a-3$ cannot contain $\ldots, 7^{-1}, 7^0, 7$ but may contain $7^2, 7^3, 7^4, \ldots$ then $7^2|(a-3) \Rightarrow a \equiv 3 \pmod{7^2} \Rightarrow a \in \{\ldots -95, -46, 3, 52, 101, \ldots\} \supseteq B(3, \frac{1}{7}) \cap \mathbb{Z}$. Or, from an expansion point of view, integers in $B(3, \frac{1}{7})$ include $3+2(7^2) = 101$, $3-4(7^3) = -1369$, $3+6(7^4)+1(7^{17})+3(7^{88})$, etc. Then for determining $x \in \mathbb{Q} \cap B(3, \frac{1}{7})$, we take a purely expansionist view. Since $v_7(x-3) > 1$, for $x-3$ the p-adic valuation of the numerator must be at least two greater than that of the denominator so the difference is greater than 1. These elements include $3 + \dfrac{5(7^3)+5(7^4)}{2+1(7)+4(7^2)+6(7^5)} = 3 + \dfrac{13720}{101047}$, etc.

Now, we look at the same ball and absolute value in $\mathbb{Q}_7$. Note that elements of $\mathbb{Q}$ have finite expansions, but are nonetheless Laurent series, and so it is intuitively clear that $\mathbb{Q}_7$ extends $\mathbb{Q}$. Therefore, the ball in $\mathbb{Q}_7$ includes the above elements, yet also contains elements following the same rules established above but with infinite expansions. That is, $\alpha \in B(3,1)$, $\alpha = 3 + a_2(7^2) + a_3(7^3) + a_4(7^4) + \cdots$, where $0 \leq a_i \leq 6$. These elements cannot be pictured as easily as the rationals, and we will work to interpret the p-adic numbers.

Now that we have defined and dissected the p-adic absolute value, we are ready to construct the mysterious field of p-adic numbers $\mathbb{Q}_p$ that we have increasingly hinted at in examples.

3 The p-adic Numbers

3.1 Construction

As the main goal of this paper is to introduce the p-adic numbers, we construct the field $\mathbb{Q}_p$ without providing much proof so as not to distract the reader. We are more concerned with providing a concrete understanding of the numbers than constructing them. By the end of this section we will be able to forget parts of the construction, but then can continue to extensions knowing that the p-adic numbers actually exist.

As stated in the introduction, the construction of $\mathbb{Q}_p$ is similar to that of $\mathbb{R}$. As the real numbers complete the rationals with respect to the usual $|\ |$, the p-adics complete the rational numbers with respect to the p-adic absolute value $|\ |_p$. In fact, $\mathbb{R}$ and $\mathbb{Q}_p$ are the only fields which complete $\mathbb{Q}$ in this manner because no other absolute values exist as asserted in the following theorem.

For convenience, $|\ |_\infty$, called the prime at infinity, represents the "usual absolute value".

Theorem 3.1. (Ostrowski's Theorem) *Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to one of the absolute values $|\ |_p$, where either p is a prime number or $p = \infty$ [2, p.43].*

A nice application of Theorem 3.1 comes in the form of a product formula for absolute values seen below.

Proposition 3.1. *For any $x \in \mathbb{Q} \setminus \{0\}$, we have*

$$\prod_{p \leq \infty} |x|_p = 1,$$

where $p \leq \infty$ means we take the product of all the primes of $\mathbb{Q}$ [2, p.46].

With this formula and all but one of the absolute values of a rational number,

we can determine the missing absolute value. We provide essentially a sketch of the proof in an example.

Example 3.1. This argument follows [2, p.46]. Let $x \in \mathbb{Z} \setminus \{0\}$ with prime factorization $x = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$ (think back to factor trees). Then,

$$\begin{cases} |x|_q = 1 & \text{if } q \neq p_i \\ |x|_{p_i} = p_i^{-a_i} & \text{if } i = 1, 2, \ldots, k \\ |x|_\infty = x = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k} \end{cases},$$

and so $|x|_q \cdot |x|_{p_1} \cdot |x|_{p_2} \cdots |x|_{p_k} \cdot |x|_\infty = 1$. Reinforcing our analysis, take $18928 \in \mathbb{Z}$. This number breaks down to $18928 = 2^4 \cdot 7 \cdot 13^2$. So, for unused primes such as 3, $|18928|_3 = \dfrac{1}{3^0} = 1$. For primes included in the factorization like 2, $|18928|_2 = \dfrac{1}{2^4}$ and clearly $|18928|_\infty = 18928$. Therefore, $\prod\limits_{p \leq \infty} |18928|_p = \dfrac{1}{2^4} \cdot \dfrac{1}{7} \cdot \dfrac{1}{13^2} \cdot 18928 = 1$.

Now, we recall important definitions from real analysis which will guide us to the p-adic numbers.

Definition 3.1. Let F be a field and let $|\ |$ be an absolute value on F.

i) A sequence of elements $x_n \in F$ is called a *Cauchy sequence* if for all $\varepsilon > 0$, there exists a bound $N \in \mathbb{N}$ such that $|x_m - x_n| < \varepsilon$ whenever $m, n \geq N$.

ii) The field F is called *complete* with respect to $|\ |$ if every Cauchy sequence of elements of F has a limit in F.

iii) A subset $S \subset F$ is called *dense* in F if for every $x \in F$ and for every $\varepsilon > 0$ we have $B(x, \varepsilon) \cap S \neq \emptyset$.

Note, part iii) of the definition can also be worded as S is dense in F if every open ball around every element of F contains an element of S. We remind ourselves of these terms with an example.

Example 3.2. Consider the first real number introduced in this paper, $\sqrt{7} = 2.645\ldots$, and form the sequence $(a_n) = \{2, 2.6, 2.64, 2.645, \ldots\}$. This is certainly Cauchy. Let $\varepsilon > 0$ and pick $N \in \mathbb{N}$ such that $\frac{1}{10^N} < \varepsilon$. Then if $m, n \geq N$, $|a_m - a_n| < \frac{1}{10^{\min\{m,n\}}} \leq \frac{1}{10^N} < \varepsilon$. Next, by construction we know $\lim_{n\to\infty}(a_n) = \sqrt{7}$. Similarly, every limit of Cauchy sequences in $\mathbb{R}$ lives in $\mathbb{R}$, and therefore the real numbers are complete with respect to $|\ |_\infty$. Unfortunately, since the elements of (a_n) are rational numbers, but $\sqrt{7} \notin \mathbb{Q}$, $\mathbb{Q}$ is not complete with respect to $|\ |_\infty$. Finally, the rational numbers are dense in the real numbers. For example, $\sqrt{7} \in \mathbb{R}$ is surrounded by the two rationals 2.645 and 2.646, and we may use (a_n) to find even closer numbers if need be.

Analogously, and thinking intuitively again (for another page or so) with $\sqrt{7} = 1 + 1(3) + 1(3)^2 + 0(3)^3 + 2(3)^4 + \cdots$ and the sequence $(\alpha_n) = \{1, 1+1(3), 1+1(3)+1(3)^2, 1+1(3)+1(3)^2+0(3)^3, 1+1(3)+1(3)^2+0(3)^3+2(3)^4 \ldots\} = \{1, 4, 13, 13, 175, \ldots\}$ we find $\mathbb{Q}$ is not complete with respect to $|\ |_3$.

From the above two examples and Theorem 3.1, we surmise the following lemma.

Lemma 3.1. *The field $\mathbb{Q}$ of rational numbers is not complete with respect to any of its nontrivial absolute values [2, p.49].*

So, let us construct a completion of $\mathbb{Q}$ with respect to $|\ |_p$. This entails adding all the limits of $|\ |_p$-Cauchy sequences to $\mathbb{Q}$. We constructed something that represents a limit to $\sqrt{7} \in \mathbb{Q}_3$ in Section 2. But, we clearly do not have any other limits and cannot possibly conceive what they look like. Thus, our approach will be to replace the limits we do not have with the equivalence classes of limits of Cauchy sequences we do [2, p.52]. We start this process with some set notation.

Let $\mathcal{C} = \{(x_n) \mid (x_n) \text{ is a Cauchy sequence with respect to } |\ |_p\}$ be the set of all Cauchy sequences of elements of $\mathbb{Q}$ with respect to $|\ |_p$. This set has a ring structure

as shown,

$$(x_n) + (y_n) = (x_n + y_n)$$
$$(x_n) \cdot (y_n) = (x_n \cdot y_n).$$

Clearly, $\mathcal{C}$ is a commutative ring with identity. Define $f : \mathbb{Q} \to \mathcal{C}$ by the constant sequence $f(x) = \{x, x, x, \ldots\}$ denoted by (x). Now, note that f is 1-1 and $f(\mathbb{Q}) \subseteq \mathcal{C}$. So, we say there is an inclusion of $\mathbb{Q}$ into $\mathcal{C}$ denoted $\mathbb{Q} \hookrightarrow \mathcal{C}$.

Unfortunately, $\mathcal{C}$ is not a field because not all non-zero elements are invertible. Let $(x_n) \in \mathcal{C}$ where $(x_n) \neq 0 = \{0, 0, 0, \ldots\}$. If any term in (x_n) equals zero (e.g. $\{1, 0, 1, 0, \ldots\}$), then $(x_n) \cdot (y_n) \neq 1 = \{1, 1, 1, \ldots\}$ for any $(y_n) \in \mathcal{C}$ since 0 is not invertible, and so $(x_n)^{-1}$ does not exist. Moreover $\mathcal{C}$ is not a field, as it contains zero divisors. The product of the non-zero two sequences in $\mathcal{C}$, $\{0, 1, 1, 1, \ldots\}$ and $\{1, 0, 0, 0, \ldots\}$, is clearly $\{0, 0, 0, \ldots\}$.

Naturally, some Cauchy sequences share the same limit. Since it is the limits we are after for the construction, the limits dictate how we treat the elements in $\mathcal{C}$, and so we define an equivalence relation that groups together sequences in $\mathcal{C}$ that have the same limit. That is, we say two Cauchy sequences are equivalent when they share the same limit and we define a set $\mathcal{N} \subset \mathcal{C}$ of sequences that tend to zero with respect to the absolute value $|\ |_p$, or $\mathcal{N} = \{(x_n) \mid \lim_{n\to\infty} |x_n|_p = 0\}$. Clearly, $\mathcal{N}$ is an ideal since for $(x_n) \in \mathcal{C}$ and $(y_n) \in \mathcal{N}$, $\lim_{n\to\infty} |x_n y_n|_p = \lim_{n\to\infty} |x_n|_p \cdot 0 = 0$ and so $(x_n) \cdot (y_n) \in \mathcal{N}$, and for $(z_n), (y_n) \in \mathcal{N}$ $(z_n) + (y_n) \in \mathcal{N}$. The next result is less obvious.

Lemma 3.2. *$\mathcal{N}$ is a maximal ideal of $\mathcal{C}$ [2, p.52].*

Thus, recall from abstract algebra that the quotient ring of a maximal ideal is a field, and we finally define the field of p-adic numbers.

Definition 3.2. We define the field of p-adic numbers to be the quotient of the ring

$\mathcal{C}$ by its maximal ideal $\mathcal{N}$:

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

Now, we must consider the p-adic absolute value in our new field. By [2, p.54], a sequence of real numbers $(|x_n|_p)$ is eventually stationary provided (x_n) is Cauchy and so we define $|\ |_p$ as expected.

Definition 3.3. If $\lambda \in \mathbb{Q}_p$ and (α_n) is any Cauchy sequence representing λ, we define

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

Without proof, we claim that the rationals are in fact dense in the field of p-adic numbers and this field is complete. To summarize, we have the following.

Theorem 3.2. *For each prime $p \in \mathbb{Z}$ there exists a field $\mathbb{Q}_p$ with a non-archimedean absolute value $|\ |_p$, such that:*

i) there exists an inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ (defined via constant Cauchy sequences), and the absolute value on $\mathbb{Q}_p$ induced by $|\ |_p$, as defined in Definition 3.3, is the p-adic absolute value;

ii) $f(\mathbb{Q})$ is dense in $\mathbb{Q}_p$ with respect to $|\ |_p$; and

iii) $\mathbb{Q}_p$ is complete with respect to $|\ |_p$.

The field $\mathbb{Q}_p$ satisfying (i), (ii), and (iii) is unique up to unique isomorphism preserving the absolute values [2, p.57].

As promised, the last part of Theorem 3.2 allows us to continue without paying attention to the details of the completion. The field of p-adic numbers is unique, meaning no other field shares its established properties, and so we concentrate on these properties to give a concrete description of a p-adic number (as a Laurent series) in the next section.

3.2 Interpreting $\mathbb{Q}_p$

First, we check that the p-adic valuation v_p from Section 2 makes sense in $\mathbb{Q}_p$. Property i) from Theorem 3.2 and Definition 3.3 implies that $|\ |_p$ returns the same values for elements of $\mathbb{Q}$ and $\mathbb{Q}_p$, namely $\{\ldots, \frac{1}{p^2}, \frac{1}{p}, 1, p, p^2, \ldots\}$. So in that regard, v_p behaves the same in $\mathbb{Q}_p$ as it does in $\mathbb{Q}$ a la Definition 2.3.

Lemma 3.3. *For each $\lambda \in \mathbb{Q}_p \setminus \{0\}$, there exists an integer $v_p(\lambda)$ such that $|\lambda|_p = p^{-v_p(\lambda)}$, meaning the* p*-adic valuation v_p extends to $\mathbb{Q}_p$ [2, p.58].*

We first met the valuation in Example 2.4 and interpreted v_p as the power of the p multiplying the first non-zero number in an expansion of a rational or p-adic number. Now, we return to this concrete interpretation of p-adic numbers as expansions that has only been proposed in examples, and solidify it. Consider the following important theorem.

Theorem 3.3. *Every equivalence class $[\alpha]$ in $\mathbb{Q}_p$ for which $|\alpha|_p \leq 1$, has exactly one representative Cauchy sequence of the form (α_n) for which:*

i) $0 \leq \alpha_n \leq p^{n+1} - 1$ for $n = 0, 1, 2, \ldots$

ii) $\alpha_{n+1} \equiv \alpha_n \pmod{p^{n+1}}$ for $n = 0, 1, 2, \ldots$ [3, p.11].

Using this theorem, we finally confirm the concrete interpretation of p-adic numbers we have only portrayed in examples. The properties of Theorem 3.3 mirror Definition 2.1, the definition of coherent sequences defined back in Section 2. We understand how these sequences work, remembering Example 2.1 and the famous $\sqrt{7}$ Example 2.2. So, we satisfy conditions i) and ii) with the familiar sequence

$(\alpha_n) = \{\alpha_0, \alpha_1, \alpha_2, \ldots\}$ given by

$$\begin{aligned}
\alpha_0 &= a_0 \\
\alpha_1 &= a_0 + a_1 p \\
\alpha_2 &= a_0 + a_1 p + a_2 p^2 \\
&\vdots \\
\alpha_n &= a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n \\
\alpha_{n+1} &= a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + a_{n+1} p^{n+1} \\
&\vdots
\end{aligned}$$

Then, since $\mathbb{Q}_p$ is complete by Theorem 3.2, we take the limit of this sequence to produce an element α in $\mathbb{Q}_p$. That is, $\alpha = \lim_{n\to\infty}(\alpha_n) = a_0 + a_1 p + a_2 p^2 + \cdots$ where $0 \leq a_i \leq p-1$ and $|\alpha|_p \leq 1$. We make these numbers a special subset of the p-adic numbers, called the p-adic integers, defined by $\mathbb{Z}_p = \{\lambda \in \mathbb{Q}_p \mid |\lambda|_p \leq 1\}$. We briefly discussed p-adic integers in Example 2.4 and saw $\sqrt{7} \in \mathbb{Z}_3$, and we see in an example that these numbers indeed have no negative powers of p and that the p-adic valuation is the first power of p multiplied by a non-zero coefficient.

Example 3.3. Let $\beta \in \mathbb{Q}_7$ such that $\beta = 6(7^2) + 4(7^3) + 1(7^4) + \cdots$. Then, $(\beta_n) = \{\beta_0, \beta_1, \beta_2, \ldots\}$ is a Cauchy sequence representing β given by

$$\begin{aligned}
\beta_0 &= 0 \\
\beta_1 &= 0 \\
\beta_2 &= 6(7^2) \\
\beta_3 &= 6(7^2) + 4(7^3) \\
\beta_4 &= 6(7^2) + 4(7^3) + 1(7^4) \\
&\vdots
\end{aligned}$$

Clearly, after the first couple zero terms in the sequence (β_n), the valuations of the proceeding terms $\beta_2, \beta_3, \beta_4, \ldots$ do not change. That is, since each new term β_{n+1} adds on to the preceding term β_n, $v_7(\beta_2) = v_7(\beta_3) = v_7(\beta_4) \cdots = 2$, or $v_7(\beta) = \lim_{n\to\infty} v_7(\beta_n) = 2$. Therefore, the 7-adic valuation is indeed the first power of 7 multiplied by a non-zero coefficient. Then, by Definition 3.3, $|\beta|_7 = \lim_{n\to\infty}(\beta_n) = \lim_{n\to\infty} \frac{1}{7^{v_7(\beta_n)}} = \frac{1}{7^2} \leq 1$, and $\beta \in \mathbb{Z}_7$.

Now, Theorem 3.3 does not address $\lambda \in \mathbb{Q}_p$ where $|\lambda|_p > 1$. But, we remedy this simply by multiplying by a power of p. Assume $\mu \in \mathbb{Q}_p$ with $|\mu|_p = p^m$. Then, multiply μ by p^m to get $|p^m\mu|_p = |p^m|_p|\mu|_p = \frac{1}{p^m}p^m = 1$ and so $p^m\mu \in \mathbb{Z}_p$. Then, since $p^m\mu$ is a p-adic integer, it is given by $p^m\mu = a_0 + a_1p + a_2p^2 + \cdots + a_mp^m + \cdots$ where $0 \leq a_i \leq p-1$. Dividing by p^m, we arrive at the expression $\mu = \frac{a_0}{p^m} + \frac{a_1}{p^{m-1}} + \frac{a_2}{p^{m-2}} + \cdots + a_m + a_{m+1}p + a_{m+2}p^2 + \cdots$. Since we assumed $|\mu|_p = p^m = \frac{1}{p^{-m}} \Rightarrow v_p(\mu) = -m$, agreeing with our established visualization of the p-adic valuation.

Thus, every $\lambda \in \mathbb{Q}_p$ can be written as a Laurent series

$$\lambda = \frac{a_{-n}}{p^n} + \frac{a_{-n+1}}{p^{n-1}} + \cdots + \frac{a_{-1}}{p} + a_0 + a_1p + a_2p^2 + \cdots$$

where $0 \leq a_n \leq p-1$ (we shuffled the subscripts to conveniently match the power of p). Interestingly, note that the p-adic numbers extend infinitely to the right, but finitely to the left. We compare this attribute to the real numbers in an example.

Example 3.4. Look at $\frac{7}{6} \in \mathbb{R}$ and $\frac{7}{6} \in \mathbb{Q}_3$. In $\mathbb{R}$, $\frac{7}{6} = 1(10^0) + 1(10^{-1}) + 6(10^{-2}) + 6(10^{-3}) + \cdots = 1.166\ldots$. So, according to our familiar notation, the coefficients of the negative powers of 10 in a decimal expansion are the digits to the right of the decimal place. Then in $\mathbb{Q}_3$, $\frac{7}{6} = \frac{2}{3} + 2 + 1(3) + 1(3^2) + \cdots = \cdots + 1(3^2) + 1(3) + 2(3^0) + 2(3^{-1}) = \ldots 112.2$.

Also of interest is the uniqueness of a p-adic expansion asserted by Theorem

3.3. Whereas in $\mathbb{R}$, $0.999\ldots$ and 1 are interchangeable, in $\mathbb{Q}_p$ any two p-adic which converge to the same p-adic number have the same digits.

So, in a sense the p-adic numbers are opposite the real numbers. While the reals are finite to the left and infinite to the right, the p-adics are finite to the right and infinite to the left. This makes arithmetic in $\mathbb{Q}_p$ just slightly different from that in $\mathbb{R}$.

3.3 Calculations in $\mathbb{Q}_p$

Calculations in $\mathbb{Q}_p$ are similar to our usual mode of operating in $\mathbb{R}$ except here we "borrow" and "carry" numbers from left to right, rather than right to left. First, we show an example of p-adic multiplication and then we will divide two p-adic numbers.

Example 3.5. Multiply $2+3(5)+1(5^2)+3(5^3)+\cdots$ and $4+2(5)+2(5^2)+1(5^3)+\cdots$ in $\mathbb{Q}_5$. We start at the left and move right.

$$\begin{array}{rl} & 2+3^{\mathit{1}}(5)+1^{\mathit{2}}(5^2)+3^{\mathit{1}}(5^3)+\cdots \\ \times & 4+2(5)+2(5^2)+1(5^3)+\cdots \\ \hline & 3+3(5)+1(5^2)+3(5^3)+\cdots \end{array}$$

The italicized numbers in the top multiplier are the carried terms. We have

$$\begin{aligned} 4(2+3(5)+1(5^2)+3(5^3)+\cdots) &= 8+12(5)+4(5^2)+12(5^3)+\cdots \\ &= (3+\mathit{1}(5))+12(5)+4(5^2)+12(5^3)+\cdots \\ &= 3+(3+\mathit{2}(5))(5)+4(5^2)+12(5^3)+\cdots \\ &= 3+3(5)+(1+\mathit{1}(5))(5^2)+12(5^3)+\cdots \\ &= 3+3(5)+1(5^2)+3(5^3)+\cdots. \end{aligned}$$

We continue and note that adding p-adic numbers is similar to adding polynomials.

$$
\begin{array}{rr}
 & 2+3(5)+1(5^2)+3(5^3)+\cdots \\
\times & 4+2(5)+2(5^2)+1(5^3)+\cdots \\
\hline
 & 3+3(5)+1(5^2)+3(5^3)+\cdots \\
 & \quad 4(5)+1(5^2)+3(5^3)+\cdots \\
 & \qquad\quad 4(5^2)+1(5^3)+\cdots \\
+ & \qquad\qquad\quad 2(5^3)+\cdots \\
\hline
 & 3+2(5)+2(5^2)+0(5^3)+\cdots
\end{array}
$$

Now, we provide an example of division in $\mathbb{Q}_7$.

Example 3.6. Calculate $\dfrac{1+6(7)+3(7^2)+5(7^3)+\cdots}{2+5(7)+1(7^2)+4(7^3)+\cdots}$ in $\mathbb{Q}_7$.

$$
\begin{array}{rr|l}
 & & 4 \\
\hline
2+5(7)+1(7^2)+4(7^3)+\cdots & & 1+6(7)+3(7^2)+5(7^3)+\cdots \\
 & - & \underline{8+20(7)+4(7^2)+16(7^3)+\cdots}
\end{array}
$$

Then,

$$
\begin{aligned}
8+20(7)+4(7^2)+16(7^3)+\cdots &= (1+7)+(6+2(7))(7)+4(7^2)+(2+2(7))(7^3)+\cdots \\
&= 1+1(7)+6(7)+2(7^2)+4(7^2)+2(7^3)+\cdots \\
&= 1+7(7)+6(7^2)+2(7^3)+\cdots \\
&= 1+3(7^3)+\cdots .
\end{aligned}
$$

So,

$$
\begin{array}{rr|l}
 & & 4+3(7)+1(7^2)+3(7^3)+\cdots \\
\cline{2-3}
2+5(7)+1(7^2)+4(7^3)+\cdots & & 1+6(7)+3(7^2)+5(7^3)+\cdots \\
 & - & 1+0(7)+0(7^2)+3(7^3)+\cdots \\
\cline{2-3}
 & & 6(7)+3(7^2)+2(7^3)+\cdots \\
 & - & 6(7)+1(7^2)+5(7^3)+\cdots \qquad (=6(7)+15(7^2)+3(7^3)+\cdot \\
\cline{2-3}
 & & 2(7^2)-3(7^3)+\cdots \\
 & - & 2(7^2)+5(7^3)+\cdots \\
\cline{2-3}
 & & 6(7^3)+\cdots \qquad (=-8(7^3)+\cdots)
\end{array}
$$

Consider a number in $\mathbb{Q}_p$ such as $\lambda = \dfrac{a_1p + a_2p^2 + a_3p^3 + \cdots}{b_3p^3 + b_4p^4 + b_5p^5 + \cdots}$. If we solve for λ as in our example, we need to multiply b_3p^3 by some cp^{-2} to subtract off a_1p. So, the quotient λ starts its expansion at p^{-2}, meaning λ is not a p-adic integer. We easily confirm this by recalling $v_p(\lambda) = 1 - 3 = -2$, the power of the first p in λ.

Now, we will find the invertible elements of $\mathbb{Z}_p$, i.e., the p-adic units. So, we use the above analysis and keep quotients in mind. Let $\alpha \in \mathbb{Z}_p$ and we require $\dfrac{1}{\alpha} \in \mathbb{Z}_p$. Then, $\alpha \in \mathbb{Z}_p \Rightarrow |\alpha|_p \leq 1 \Rightarrow v_p(\alpha) \geq 0$, and so $v_p(\alpha^{-1}) \leq 0$. But, $v_p(\alpha^{-1}) < 0 \Rightarrow |\alpha^{-1}|_p > 1 \Rightarrow \alpha^{-1} \notin \mathbb{Z}_p$, meaning $|\alpha|_p = 1 \Rightarrow \alpha^{-1} \in \mathbb{Z}_p$. Thus, the set of p-adic units is defined by $\mathbb{Z}_p^\times = \{\alpha \in \mathbb{Z}_p \mid |\alpha|_p = 1\}$. Or equivalently, $\alpha = a_0 + a_1p + a_2p^2 + \cdots$ where $a_0 \neq 0$ which implies $\alpha \not\equiv 0 \pmod{p}$, and $\mathbb{Z}_p^\times = \{\alpha \in \mathbb{Z}_p \mid \alpha \not\equiv 0 \pmod{p}\}$.

With a concrete representation of the p-adic numbers and a grasp on calculations, we conclude this section with the proof of an important abstract algebra result.

3.4 Hensel's Lemma

With this theorem we test whether a polynomial has roots in $\mathbb{Z}_p$, which, recalling some abstract algebra, is necessary to find irreducible polynomials and create field extensions.

Theorem 3.4. (Hensel's Lemma) *Let* $f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$ *be a polynomial with coefficients in* $\mathbb{Z}_p$ *and suppose that there exists* $\alpha_0 \in \mathbb{Z}_p$ *such that*

$$f(\alpha_0) \equiv 0 \pmod{p} \text{ and}$$
$$f'(\alpha_0) \not\equiv 0 \pmod{p},$$

where $f'(x)$ *is the derivative of* $f(x)$*. Then, there exists* $\alpha \in \mathbb{Z}_p$ *such that* $\alpha \equiv \alpha_0 \pmod{p}$ *and* $f(\alpha) = 0$*.*

Proof. We will construct a Cauchy sequence of rational integers which converges to a root α to show it exists. We have built many of these sequences already so this proof will not be too unusual. First, we claim there exists a sequence of non-p-adic integers $\{\alpha_0, \alpha_1, \alpha_2, \ldots\}$ such that for all $n \geq 0$:

i) $f(\alpha_n) \equiv 0 \pmod{p^{n+1}}$ and

ii) $\alpha_{n+1} \equiv \alpha_n \pmod{p^{n+1}}$.

We proceed by induction to show for all $n \geq 0$, we can construct α_n satisfying these properties.

Base Case: First, we show i) and ii) hold when $n = 0$. For i), let $a_0 \in \{0, \ldots, p-1\}$ satisfy $\alpha_0 \equiv a_0 \pmod{p}$. Then, $f(\alpha_0) \equiv f(a_0) \pmod{p}$ and $f(\alpha_0) \equiv 0 \pmod{p}$. Next, for any $0 \leq a_1 \leq p-1$ we need to find $\alpha_1 = a_0 + a_1p$, satisfying condition ii). Then, we show a_1 exists by solving for it using the given polynomial $f(x)$ and the fact that

$$f(\alpha_1) \equiv f(a_0 + a_1p) \pmod{p^2}.$$

To continue we will use a Taylor series of $f(x)$ centered around a_0. Recall $f(x) =$

$f(a_0) + f'(a_0)(x - a_0) + \frac{1}{2}f''(a_0)(x - a_0)^2 + \cdots$. Now, we plug in for α_1 and simplify,

$$\begin{aligned} f(\alpha_1) &= f(a_0 + a_1 p) \\ &= f(a_0) + f'(a_0)(a_1 p) + \frac{1}{2}f''(a_0)(a_1 p)^2 + \cdots \\ &\equiv f(a_0) + f'(a_0)(a_1 p) \pmod{p^2}. \end{aligned}$$

If we are to have α_1, it should satisfy condition i). That is

$$f(a_0) + f'(a_0)(a_1 p) \equiv 0 \pmod{p^2}.$$

Next, $f(a_0) \equiv f(\alpha_0) \equiv 0 \pmod{p} \Rightarrow f(a_0) = \beta p$ for some $\beta \in \mathbb{Z}_p$, and this implies $f(a_0) \equiv b_1 p \pmod{p^2}$ where $0 \leq b_1 \leq p - 1$. So,

$$\begin{aligned} b_1 p + f'(a_0)(a_1 p) &\equiv 0 \pmod{p^2} \\ b_1 + f'(a_0)(a_1) &\equiv 0 \pmod{p}. \end{aligned}$$

But, by assumption $f'(a_0) \equiv f'(\alpha_0) \not\equiv 0 \pmod{p}$, and thus we may divide by $f'(a_0)$ to get $a_1 \equiv -b_1[f'(a_0)]^{-1} \pmod{p}$, showing a_1 exists. So, we have established the base case and move to the inductive hypothesis.

Inductive Step: Assume we have the stated properties for $a_0, \alpha_1, \ldots, \alpha_n$. Similar to our base step, we let $\alpha_{n+1} = \alpha_n + \alpha_{n+1} p^{n+1}$ where $0 \leq \alpha_{n+1} \leq p - 1$ and try to determine α_{n+1} using the fact that α_{n+1} must satisfy

$$\begin{aligned} f(\alpha_{n+1}) &= f(\alpha_n + a_{n+1} p^{n+1}) \\ &= f(\alpha_n) + f'(\alpha_n)(a_{n+1} p^{n+1}) + \frac{1}{2}f''(\alpha_n)(a_{n+1} p^{n+1})^2 + \cdots \\ &\equiv f(\alpha_n) + f'(\alpha_n)(a_{n+1} p^{n+1}) \pmod{p^{n+2}}. \end{aligned}$$

We want α_{n+1} to satisfy i), so $f(\alpha_{n+1}) \equiv 0 \pmod{p^{n+2}}$. Also by the inductive assumption, $f(\alpha_n) \equiv 0 \pmod{p^{n+1}} \Rightarrow f(\alpha_n) \equiv b_{n+1}p^{n+1} \pmod{p^{n+2}}$ for some $0 \leq b_{n+1} \leq p-1$ and

$$\begin{aligned} f(\alpha_n) + f'(\alpha_n)(a_{n+1}p^{n+1}) &\equiv 0 \pmod{p^{n+2}} \\ b_{n+1}p^{n+1} + f'(\alpha_n)(a_{n+1}p^{n+1}) &\equiv 0 \pmod{p^{n+2}} \\ b_{n+1} + f'(\alpha_n)(a_{n+1}) &\equiv 0 \pmod{p}. \end{aligned}$$

Then, since $\alpha_n \equiv \alpha_0 \pmod{p} \Rightarrow f'(\alpha_n) \equiv f'(\alpha_0) \not\equiv 0 \pmod{p}$, we get $a_{n+1} \equiv -b_{n+1}[f'(\alpha_n)]^{-1} \pmod{p}$. Therefore, $\alpha_{n+1} = \alpha_n + a_{n+1}p^{n+1}$ satisfies condition ii), and we have proved our claim with induction.

So, we have constructed the sequence $(\alpha_n) = \{a_0, \alpha_1, \alpha_2, \ldots\}$ with our desired properties. As expected, let $\alpha = a_0 + a_1p + a_2p^2 + \cdots$. Clearly, $\alpha = a_0 + a_1p + a_2p^2 + \cdots \equiv a_0 \equiv \alpha_0 \pmod{p}$ and since we have $f(\alpha) \equiv f(\alpha_n) \equiv 0 \pmod{p^{n+1}}$ for all $n \geq 0$, then $f(\alpha) = 0$. Also, note that the choice at each step was unique, so the root constructed is unique. □

We end this section with a final example using Hensel's Lemma.

Example 3.7. We determine whether three polynomials have roots in $\mathbb{Z}_p$ using Hensel's Lemma (Theorem 3.4). According to the theorem, we need $f(\alpha_0) \equiv 0 \pmod{p}$ and $f'(\alpha_0) \not\equiv 0 \pmod{p}$ where $\alpha_0 \in \mathbb{Z}_p$. Since we require these congruences mod p, then only the first coefficient in the p-adic expansion of α_0 matters, that is the digit multiplying p^0. Clearly, this digit can be taken from the set $\{0, \ldots, p-1\}$.

First, we use our relentless example and confirm $\sqrt{7} \in \mathbb{Z}_3$. Then, let $f(x) = x^2 - 7$

and $f'(x) = 2x$ with $\alpha_0 \in \{0, 1, 2\}$. We test the possible α_0

$\underline{\alpha_0}$	$\underline{f(\alpha_0)}$	$\underline{f'(\alpha_0)}$
0	$-7 \equiv 1 \not\equiv 0 \pmod 3$	
1	$-6 \equiv 0 \pmod 3$	$2 \not\equiv 0 \pmod 3$
2	$-3 \equiv 0 \pmod 3$	$4 \equiv 1 \not\equiv 0 \pmod 3$

Since the degree of $f(x)$ is two, we expect at most two roots, and according to our chart, there exists $\alpha \in \mathbb{Z}_3$ such that $\alpha \equiv \alpha_0 \equiv 1 \pmod p$ and $\alpha \equiv 2 \pmod p$ with $f(\alpha) = 0$. We have seen these α_0 already in Example 2.2. But, these simple calculations using Hensel's Lemma quickly reveal 7 is a 3-adic square. To actually build the 3-adic expansion of $\sqrt{7}$ refer back to the old example.

Next, we take a mildly more interesting polynomial, letting $f(x) = x^2 + x - 6$ which clearly has roots -3 and 2 in $\mathbb{Z}$. We will check for roots in $\mathbb{Z}_3$ and $\mathbb{Z}_5$. So, we need $\alpha_0 \in \mathbb{Z}_3$ and $\beta_0 \in \mathbb{Z}_5$ satisfying the input of Theorem 3.4 where $\alpha_0 \in \{0, 1, 2\}$ and $\beta_0 \in \{0, 1, 2, 3, 4\}$. Then, recalling $f(x) = 2x + 1$,

$\alpha_0 \in \mathbb{Z}_3$	$f(\alpha_0)$	$f'(\alpha_0)$
0	0	1
1	2	
2	0	2

and

$\beta_0 \in \mathbb{Z}_5$	$f(\beta_0)$	$f'(\beta_0)$
0	4	
1	1	
2	0	0
3	4	
4	1	

Since $\mathbb{Z}_3$ and $\mathbb{Z}_5$ extend $\mathbb{Z}$, then 2 is certainly a root in both fields. So, note that while all $\beta_0 \in \mathbb{Z}_5$ fail Hensel's Lemma, this does not imply that $f(x)$ has no roots in $\mathbb{Z}_5$. Rather, this implies that we cannot definitively use Hensel's Lemma to conclude that $f(x)$ has roots in $\mathbb{Z}_5$. To compute 5-adic expansion of the second root, simply

compute the 5-adic expansion of -3.

Now, consider a more interesting polynomial in $\mathbb{Z}_3$ that does not have roots in $\mathbb{Z}$ such as $f(x) = \sqrt{7}x^2 - 3x + 2$. We are allowed to use Hensel's Lemma because $\sqrt{7} \in \mathbb{Z}_3$, meaning $\sqrt{7}$ is equivalent to an integer in the set $\{0, 1, 2\}$ mod 3. That is, we know from Example 2.2 (and above) that $\sqrt{7} \equiv 1 \pmod 3$ and $\sqrt{7} \equiv 2 \pmod 3$. But we cannot have both, so we establish the convention that $+\sqrt{7} \equiv 1 \pmod 3$ and $-\sqrt{7} \equiv 2 \pmod 3$. Then,

$\underline{\alpha_0}$	$\underline{f(\alpha_0)}$	$\underline{f'(\alpha_0)}$
0	2	
1	0	2
2	0	1

and this polynomial has roots in $\mathbb{Z}_3$, and we would build these 3-adic integers using Hensel or some 3-adic quadratic formula. For amusement, since we use the notation $\pm\sqrt{7}$ to represent the 3-adic expansions of the roots of $x^2 - 7$ in $\mathbb{Z}_3$, we could represent the roots of $\sqrt{7}x^2 - 3x + 2$ with the notation $\dfrac{3 \pm \sqrt{9 - 8\sqrt{7}}}{2\sqrt{7}}$.

Now that we have lightly studied roots of polynomials, it makes sense to transition to field extensions. While, we saw that the construction and calculations in $\mathbb{Q}_p$ are quite similar to those in $\mathbb{R}$, the two fields are not so similar. One glaring difference is each field's algebraic closure. The field of p-adic numbers is complete, but turns out to not be algebraically closed. This is true for the real numbers as well, but there is no easy analogous field of complex numbers (both complete and algebraically closed) for $\mathbb{Q}_p$. Whereas it takes one step to go from $\mathbb{R}$ to $\mathbb{C}$, it takes two steps to go from $\mathbb{Q}_p$ to a complete and algebraically closed field containing $\mathbb{Q}_p$. So, we now introduce some important properties of finite field extensions of $\mathbb{Q}_p$ to assist in determining its algebraic closure.

4 Finite Extensions

4.1 Preliminaries

This section heavily relies on concepts from abstract algebra, and the reader may want to refer to [3, p.52] for a quick review on the subject or [4] for more detail. $\mathbb{Q}_p$ is not algebraically closed, and so in this section we categorize some of its field extensions to help find the algebraic closure. Field extensions of $\mathbb{Q}_p$ are simply fields K that contain $\mathbb{Q}_p$. This also means K is a vector space over $\mathbb{Q}_p$, and we write $K/\mathbb{Q}_p$ to denote a field extension K over $\mathbb{Q}_p$. In this section, we only consider finite extensions $K/\mathbb{Q}_p$, that is, fields that are finite dimensional over $\mathbb{Q}_p$.

Just as we extended the p-adic absolute value $|\ |_p$ from $\mathbb{Q}$ to $\mathbb{Q}_p$, we now look to extend $|\ |_p$ from $\mathbb{Q}_p$ to K. Denote this new absolute value by $|\ |$. We require $|\ |$ to satisfy the usual properties of a non-archimedean absolute value from Definition 2.2, and additionally the property that $|\lambda| = |\lambda|_p$ for $\lambda \in \mathbb{Q}_p$. Without proof, we note the following.

Proposition 4.1. *There is at most one absolute value on K extending the p-adic absolute value on $\mathbb{Q}_p$ [2, p.129].*

This proposition will help us later. Next, the following function will help us define this new absolute value.

Definition 4.1. The *norm from K to F* is a function $\mathbf{N}_{K/F} : K \to F$ and can be defined in several (equivalent) ways. Here, are three definitions:

i) Take $\alpha \in K$, a finite-dimensional F-vector space, and consider the F-linear map from K to K given by multiplication by α. Since this is a linear transformation of vector spaces, it corresponds to a matrix. Then we define $\mathbf{N}_{K/F}(\alpha)$ to be the determinant of this matrix.

ii) Let $\alpha \in K$, and consider the subfield $F(\alpha)$. Then, let $r = [K : F(\alpha)]$ be the

degree of K as an extension of $F(\alpha)$. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in F[x]$$

be the minimal polynomial of α over F such that $f(\alpha) = 0$. Then we define $\mathbf{N}_{K/F}(\alpha) = (-1)^{nr}a_0^r$.

iii) Let K/F be a finite, normal extension. Then, $\mathbf{N}_{K/F}(\alpha) = \prod_{\sigma}\sigma(\alpha)$ where σ is an F-automorphism of K.

We will use each definition depending on which one makes most sense in context. The definitions can be proven equivalent (see [2, p.132]), but we settle with an example instead.

Example 4.1. This argument follows [2, p.133]. Consider the field $K = \mathbb{Q}_5(\sqrt{2})$ over $F = \mathbb{Q}_5$. Note that $\sqrt{2} \notin \mathbb{Q}_5$. We calculate the norm of $\alpha = a + b\sqrt{2} \in \mathbb{Q}_5(\sqrt{2})$ using all three interpretations:

i) A basis for $\mathbb{Q}_5(\sqrt{2})$ over $\mathbb{Q}_5$ is $\{1, \sqrt{2}\}$. Let $T_{a+b\sqrt{2}} : \mathbb{Q}_5(\sqrt{2}) \to \mathbb{Q}_5(\sqrt{2})$ be defined by $T_{a+b\sqrt{2}}(x) = (a + b\sqrt{2})(x)$. Then, $T(1) = a + b\sqrt{2}$ and $T(\sqrt{2}) = 2b + a\sqrt{2}$. So, the corresponding matrix with respect to our basis is

$$\begin{bmatrix} a & 2b \\ b & a \end{bmatrix},$$

which has determinant $a^2 - 2b^2$. Therefore, $\mathbf{N}_{\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5}(a + b\sqrt{2}) = a^2 - 2b^2$.

ii) We look at two cases. First, if $b = 0$, then $\alpha = a$ and we consider the subfield $\mathbb{Q}_5(a) \subseteq \mathbb{Q}_5(\sqrt{2})$. Since $a \in \mathbb{Q}_5$, then $\mathbb{Q}_5(a) = \mathbb{Q}_5$. Thus, the minimal polynomial of a is just $f(x) = x - a$, meaning $n = [\mathbb{Q}_5(a) : \mathbb{Q}_5] = \deg(f) = 1$, and these fields are equal. So, $r = [\mathbb{Q}_5(\sqrt{2}) : \mathbb{Q}_5(a)] = [\mathbb{Q}_5(\sqrt{2}) : \mathbb{Q}_5]$ and since $g(x) = x^2 - 2$ is the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}_5$, $r = \deg(g) = 2$. Therefore, $\mathbf{N}_{\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5}(a) = (-1)^{nr}a_0^r = (-1)^{(1)(2)}(a)^2 = a^2$. Next, in the second case $b \neq 0$ and $\alpha = a + b\sqrt{2}$,

and we consider $\mathbb{Q}_5(a+b\sqrt{2}) \subseteq \mathbb{Q}_5(\sqrt{2})$. Let $h(x)$ be the minimal polynomial of $a+b\sqrt{2}$ over $\mathbb{Q}_5$. The degree of $h(x)$ cannot be 1 because that would imply $h(x) = x-(a+b\sqrt{2}) \Rightarrow \sqrt{2} \in \mathbb{Q}_5$, a contradiction. Then, $h(x) = x^2 - 2ax + (a^2 - 2b^2)$ because we note that $(a+b\sqrt{2})^2 = a^2+2ab\sqrt{2}+2b^2$ and working backwards find that

$$\begin{aligned} 0 &= (a+b\sqrt{2})^2 - a^2 - 2ab\sqrt{2} - 2b^2 \\ &= (a+b\sqrt{2})^2 - 2a(a+b\sqrt{2}) + (a^2-2b^2) \\ &= h(a+b\sqrt{2}). \end{aligned}$$

Therefore $n = [\mathbb{Q}_5(a+b\sqrt{2}) : \mathbb{Q}_5] = \deg(h) = 2$. But, from above we know that $[\mathbb{Q}_5(\sqrt{2}) : \mathbb{Q}_5] = \deg(x^2-2) = 2$, implying that $\mathbb{Q}_5(a+b\sqrt{2}) = \mathbb{Q}_5(\sqrt{2})$. Thus $r = [\mathbb{Q}_5(\sqrt{2}) : \mathbb{Q}_5(a+b\sqrt{2})] = [\mathbb{Q}_5(\sqrt{2}) : \mathbb{Q}_5(\sqrt{2})] = 1$, and so $\mathbf{N}_{\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5}(a+b\sqrt{2}) = (-1)^{(2)(1)}(a^2-2b^2)^1 = a^2-2b^2$, which agrees with our calculation from i). Also, if we set $b=0$, we get our first result, namely $a^2 - 2(0)^2 = a^2$.

iii) The $\mathbb{Q}_5$-automorphisms of $\mathbb{Q}_5(\sqrt{2})$ map roots of the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}_5$ to each other and leave elements of $\mathbb{Q}_5$ unchanged. There are two roots of x^2-2, meaning there are two automorphisms, the identity ι and τ. That is, ι and τ map $a \mapsto a$ and $b \mapsto b$, while $\iota(\sqrt{2}) = \sqrt{2}$ and $\tau(\sqrt{2}) = -\sqrt{2}$. So, $\tau(a+b\sqrt{2}) = \tau(a) + \tau(b)\tau(\sqrt{2}) = a - b\sqrt{2}$ and as expected $\iota(a+b\sqrt{2}) = a+b\sqrt{2}$. Therefore, $\mathbf{N}_{K/F}(a+b\sqrt{2}) = \prod_{\sigma}\sigma(a+b\sqrt{2}) = \iota(a+b\sqrt{2}) \cdot \tau(a+b\sqrt{2}) = (a+b\sqrt{2})(a-b\sqrt{2}) = a^2-2b^2$.

From part i) of Definition 4.1, it is clear that the norm is multiplicative since determinants are multiplicative. Next, to see what the extended absolute value must be, assume K is normal. Then, let $|\ |' : K \to \mathbb{R}_+$ be defined by $|x|' = |\sigma(x)|$ where σ is a K-automorphism. This is clearly an absolute value, but by Proposition 4.1 there is only one $|\ |$ extending $|\ |_p$, and so $|x| = |x|' = |\sigma(x)|$. Now, recall that if $K/\mathbb{Q}_p$ is normal, there are $n = [K : \mathbb{Q}_p]$ K-automorphisms, namely $\sigma_1, \ldots, \sigma_n$.

So, $|x|^n = |\prod_\sigma \sigma(x)|$ and using part iii) of the definition for a norm, we see that $|x|^n = |x|\cdots|x| = |\sigma_1(x)||\sigma_2(x)|\cdots|\sigma_n(x)| = |\sigma_1(x)\cdots\sigma_n(x)| = |\mathbf{N}_{K/\mathbb{Q}_p}(x)|$. But, the norm lies in $\mathbb{Q}_p$, and therefore $|x| = \sqrt[n]{|\mathbf{N}_{K/\mathbb{Q}_p}(x)|_p}$. We formally put this into a theorem.

Theorem 4.1. *Let $K/\mathbb{Q}_p$ be a finite extension of degree n. The function $|\ |: K \to \mathbb{R}_+$ defined by*

$$|x| = \sqrt[n]{|\mathbf{N}_{K/\mathbb{Q}_p}(x)|_p}$$

is a non-archimedean absolute value on K which extends the p-adic absolute value on $\mathbb{Q}_p$ [2, p.135].

Note that the extension K does not need to be normal. Also, this new $|\ |$ is clearly an absolute value, as it satisfies Definition 2.2 (to get multiplication, recall the norm is multiplicative). Also, $|\ |$ satisfies our requirement that $|\lambda| = |\lambda|_p$ for $\lambda \in \mathbb{Q}_p$. Use part ii) of Definition 4.1 and remember that the minimal polynomial over $\mathbb{Q}_p$ for any $\lambda \in \mathbb{Q}_p$ is simply $x - \lambda$. Now, we calculate two easy examples.

Example 4.2. First, we calculate the absolute value of $10+5\sqrt{2}$ in $\mathbb{Q}_5(\sqrt{2})$. From Example 4.1 ii) we know that $n = [\mathbb{Q}_5(\sqrt{2}) : \mathbb{Q}_5] = 2$ and $\mathbf{N}_{\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5}(10+5\sqrt{2}) = (10)^2 - 2(5)^2 = 50$. Then, $|50|_5 = |2(5^2)|_5 = \frac{1}{5^2}$. Therefore, $|10+5\sqrt{2}| = \sqrt[n]{|\mathbf{N}_{\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5}(10+5\sqrt{2})|_5} = \sqrt{|50|_5} = \sqrt{\frac{1}{5^2}} = \frac{1}{5}$.

Next, we calculate $|2\sqrt{7}+\sqrt{3}|$ in $\mathbb{Q}_3(\sqrt{3})$ (recall that $\sqrt{7} \in \mathbb{Q}_3$). Similar to the calculation in Example 4.1 iii), we see that $\mathbf{N}_{\mathbb{Q}_3(\sqrt{3})/\mathbb{Q}_3}(a+b\sqrt{3}) = a^2 - 3b^2$. Also, again $n = [\mathbb{Q}_3(\sqrt{3}) : \mathbb{Q}_3] = 2$, and so $|2\sqrt{7}+\sqrt{3}| = \sqrt{|25|_3} = \sqrt{\frac{1}{3^0}} = 1$.

Before we begin examining field extensions of $\mathbb{Q}_p$, we introduce one last familiar proposition.

Proposition 4.2. (Eisenstein Irreducibility Criterion) *Let*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}_p[x]$$

be a polynomial satisfying the conditions

i) $|a_n|_p = 1$,

ii) $|a_i|_p < 1$ *for* $0 \leq i < n$, *and*

iii) $|a_0|_p = \dfrac{1}{p}$.

Then $f(x)$ *is irreducible over* $\mathbb{Q}_p$ *[2, p.140].*

This is an extremely useful result and we provide an example.

Example 4.3. Here we show that $x^2 - 3$ is irreducible over $\mathbb{Q}_3$. For the first two conditions, $|1|_3 = 1$ and $|0|_3 = 0 < 1$. Then, $|-3|_3 = \dfrac{1}{3}$, and this polynomial is irreducible by Eisenstein. Furthermore, we can adjoin a root of $x^2 - 3$ to $\mathbb{Q}_3$ to gain the extension $\mathbb{Q}_3(\sqrt{3})$ that we dealt with in Example 4.2.

4.2 Properties

Now, we are ready to present some information about finite extensions of $\mathbb{Q}_p$. First, we note that the p-adic valuation extends to finite extensions and is defined, as expected, in the usual way.

Definition 4.2. Let K be a finite extension of $\mathbb{Q}_p$, and let $|\ |$ be the p-adic absolute value on K. For any $x \in K \setminus \{0\}$, we define the p-adic valuation $v_p(x)$ to be the unique rational number satisfying

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

and we set $v_p(0) = \infty$.

Next, combining this definition and Theorem 4.1, we can solve for the p-adic valuation, and get $v_p(x) = \dfrac{1}{n} v_p(\mathbf{N}_{K/\mathbb{Q}_p}(x))$ for any $x \in K \setminus \{0\}$. Now, an example.

Example 4.4. Let $10 + 5\sqrt{2} \in \mathbb{Q}_5(\sqrt{2})$; we will calculate its 5-adic valuation. From Example 4.2, $\mathbf{N}_{\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5}(10 + 5\sqrt{2}) = 50$ and $n = [\mathbb{Q}_5(\sqrt{2}) : \mathbb{Q}_5] = 2$. So, $v_5(10 +$

$5\sqrt{2}) = \frac{1}{n} v_5(\mathbf{N}_{\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5}(10+5\sqrt{2})) = \frac{1}{2} v_5(50) = 1$ which agrees with our previous result that $|10+5\sqrt{2}| = \frac{1}{5}$.

Now, let $2\sqrt{7}+\sqrt{3} \in \mathbb{Q}_3(\sqrt{3})$. Then, using Example 4.2 again, we find $v_3(2\sqrt{7}+\sqrt{3}) = \frac{1}{2} v_3(25) = 0$.

Clearly, the image of v_p is contained in $\frac{1}{n}\mathbb{Z} = \{x \in \mathbb{Q} \mid nx \in \mathbb{Z}\}$. More precisely, this image is a non-trivial additive subgroup of $\frac{1}{n}\mathbb{Z}$ that contains $\mathbb{Z}$, and therefore, it must equal $\frac{1}{e}\mathbb{Z}$ for some positive integer e dividing n [3, p.66]. We give this e a special name, as it will help us sort out some properties of finite field extensions of $\mathbb{Q}_p$.

Definition 4.3. Let $K/\mathbb{Q}_p$ be a finite extension, and let e be the unique positive integer dividing $n = [K : \mathbb{Q}_p]$ defined by

$$v_p(K \setminus \{0\}) = \frac{1}{e}\mathbb{Z} = \{x \in \mathbb{Q} \mid ex \in \mathbb{Z}\}.$$

We call e the *ramification index* of K over $\mathbb{Q}_p$. We say the extension $K/\mathbb{Q}_p$ is *unramified* if $e = 1$. We say the extension is *ramified* if $e > 1$, and *totally ramified* if $e = n$. Finally, we write $f = \frac{n}{e}$.

Soon, we will see that f corresponds to something much more important than simply the quotient of two integers. Intuitively, we want $\frac{1}{e}$ to play the same role in finite field extensions of $\mathbb{Q}_p$ as $v_p(p)$ plays in $\mathbb{Q}_p$. That is, since $v_p(p) = 1$, any $\lambda \in \mathbb{Z}_p$ can be written as $\lambda = p^{v_p(\lambda)}u$ where u is a p-adic unit, or $v_p(u) = 0$. So, we define such a number analogous to p with valuation equal to $\frac{1}{e}$.

Definition 4.4. Let $K/\mathbb{Q}_p$ be a finite extension, and let e be the ramification index. We say an element $\pi \in K$ is a *uniformizer* if $v_p(\pi) = \frac{1}{e}$.

Note that there are many $\alpha \in \mathbb{Z}_p$ with $v_p(\alpha) = 1$, and similarly there are many uniformizers for a field K. Also, in the unramified case where $e = 1$, we can set

$\pi = p$. Finally, notice that if $v_p(K \setminus \{0\}) = \frac{1}{e}\mathbb{Z}$, then there exists $\pi \in K \setminus \{0\}$ such that $v_p(\pi) = \frac{1}{e}$, meaning $v_p(\pi^e) = 1$. So rather than expansions of p as in $\mathbb{Z}_p$, we have expansions of π in K. Now, we make the above definitions concrete through calculation.

Example 4.5. In this example we find the ramification index e and uniformizer π of $\mathbb{Q}_3(\sqrt{3})$. From Example 4.2, we know $n = 2$, and from Definition 4.3, e must divide 2. Therefore, $e = 1$ or $e = 2$. Now since the valuation extends $\mathbb{Q}_3$ to $\mathbb{Q}_3(\sqrt{3})$, $v_3(\mathbb{Q}_3 \setminus \{0\}) = \mathbb{Z} \subseteq v_3(\mathbb{Q}_3(\sqrt{3}) \setminus \{0\}) = \frac{1}{e}\mathbb{Z}$ (and remember $\frac{1}{e}\mathbb{Z} \subseteq \frac{1}{n}\mathbb{Z} = \frac{1}{2}\mathbb{Z}$). That is, if $e = 1$, $v_3(\mathbb{Q}_3(\sqrt{3}) \setminus \{0\}) = \frac{1}{e}\mathbb{Z} = \frac{1}{1}\mathbb{Z} = \mathbb{Z}$, and 3 (for example) would be a uniformizer of $\mathbb{Q}_3(\sqrt{3})$. So to show $e = 2$, we just need to find an element whose valuation is not simply contained in $\mathbb{Z}$, but contained in $\frac{1}{e}\mathbb{Z} = \frac{1}{2}\mathbb{Z} = \{\ldots, -\frac{3}{2}, -1, -\frac{1}{2}, 0, \frac{1}{2}, 1, \frac{3}{2}, \ldots\}$. Well, recall from Example 4.2 that for $a + b\sqrt{3} \in \mathbb{Q}_3(\sqrt{3})$, $\mathbf{N}_{\mathbb{Q}_3(\sqrt{3})/\mathbb{Q}_3}(a + b\sqrt{3}) = a^2 - 3b^2$, meaning $v_3(a+b\sqrt{3}) = \frac{1}{2}v_3(a^2-3b^2)$. Thus, we do not want $v_3(a^2-3b^2)$ to be a multiple of 2. Take $\sqrt{3} \in \mathbb{Q}_3(\sqrt{3})$. Then, $v_3(\sqrt{3}) = \frac{1}{2}v_3((0)^2 - 3(1)^2) = \frac{1}{2}v_3(-3) = \frac{1}{2}$. So, the ramification index of $\mathbb{Q}_3(\sqrt{3})$ is $e = 2$ and $\pi = \sqrt{3}$ is a uniformizer (another easy uniformizer to find is $3 + \sqrt{3}$).

Now, we set up the algebraic structure of K.

Proposition 4.3. *Let K be a finite extension of $\mathbb{Q}_p$ of degree n, and let*

$$\begin{aligned} A &= \{x \in K \mid |x| \leq 1\} = \{x \in K \mid v_p(x) \geq 0\}, \\ M &= \{x \in K \mid |x| < 1\} = \{x \in K \mid v_p(x) > 0\}. \end{aligned}$$

Then, A is a ring, M is its unique maximal ideal, and A/M is a finite extension of $\mathbb{F}_p$ of degree at most n [3, p.64].

The field A/M is called the residue field of K, and $[A/M : \mathbb{F}_p] = f$. The ring A is called the valuation ring of $|\ |_p$ in K. This is the f that we revealed in Definition

4.3, and it indeed has the property $f = \frac{n}{e}$.

Proposition 4.4. *Let $K/\mathbb{Q}_p$ be a finite extension with $[K : \mathbb{Q}_p] = n$ and ramification index e. Then, the degree of the finite field with p^f elements over the finite field of p elements is $[A/M : \mathbb{F}_p] = \frac{n}{e}$. In other words, $A/M = \mathbb{F}_{p^f}$ [2, p.146].*

Now, we are ready to give our first description of a field extension of $\mathbb{Q}_p$. Recall that we may find an extension of a field F by adjoining the root of an irreducible polynomial. With totally ramified extensions, we can specify this polynomial.

Proposition 4.5. *Let $K/\mathbb{Q}_p$ be a totally ramified finite extension of $\mathbb{Q}_p$ of degree n. Then, $K = \mathbb{Q}_p(\pi)$, where π is a uniformizer. Furthermore, π is a root of a polynomial*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

which satisfies the conditions of the Eisenstein criterion.

Proof. Let π be a uniformizer (Definition 4.4). Then, $v_p(\pi) = \frac{1}{e}$, and since $K/\mathbb{Q}_p$ is totally ramified, $e = n = [K : \mathbb{Q}_p]$ so that $v_p(\pi) = \frac{1}{n}$. Or equivalently, $|\pi| = p^{-v_p(\pi)} = p^{-1/n}$. But also, using the definition (Theorem 4.1) of absolute value in a finite extension of $\mathbb{Q}_p$, $|\pi| = \sqrt[n]{|\mathbf{N}_{K/\mathbb{Q}_p}(\pi)|_p}$.

Now, let $f(x)$ be the minimal polynomial of π over $\mathbb{Q}_p$ with degree s where $s|n$ such that $n = [K : \mathbb{Q}_p] = [K : \mathbb{Q}_p(\pi)] \cdot [\mathbb{Q}_p(\pi) : \mathbb{Q}_p] = r \cdot s$. Then, $f(x) = x^s + a_{s-1}x^{s-1} + \cdots + a_1 x + a_0$ where $a_i \in \mathbb{Q}_p$ and $f(\pi) = 0$. Using definition ii) of the norm (Definition 4.1), we have $\mathbf{N}_{K/\mathbb{Q}_p}(\pi) = (-1)^{nr} a_0^r$.

Then, using our absolute values defined above, $p^{-1/n} = |\pi| = (|(-1)^{nr} a_0^r|_p)^{1/n} = |a_0^r|_p{}^{1/n} = |a_0|_p{}^{r/n} = |a_0|_p{}^{1/s}$. Now, note that $|a_0|_p \in \{\ldots, p^{-2}, p^{-1}, 1, p, p^2, \ldots\}$ since $a_0 \in \mathbb{Q}_p$. Let $|a_0|_p = p^z$ for some $z \in \mathbb{Z}$. Then, $p^{-1/n} = |a_0|_p{}^{1/s} = (p^z)^{1/s} = p^{z/s}$. So, $\frac{z}{s} = \frac{-1}{n} \Rightarrow zn = -s$, meaning $s \geq n$. But, we know $n = rs \Rightarrow s \leq n$, and so $s = n$. Thus, $z = -1$ and $|a_0|_p = p^{-1}$.

Thus since $f(x)$, the minimal polynomial of π over $\mathbb{Q}_p$, is of degree $s = n = [K : \mathbb{Q}_p]$, $K = \mathbb{Q}_p(\pi)$ as desired. Next, we have $|a_0|_p = p^{-1}$, condition iii) of the Eisenstein criterion (Proposition 4.2), and we also clearly have $|a_n|_p = 1$, condition i). For condition ii), let $\pi_1, \pi_2, \ldots, \pi_n$ be roots of $f(x)$. Since the roots have the same minimal polynomial $f(x)$, they have the same norm by definition ii), and thus $|\pi_1| = |\pi_2| = \cdots = |\pi_n| = p^{-1/n} < 1$. The coefficients a_i of $f(x)$ are combinations of the roots, that is $f(x) = (x - \pi_1)(x - \pi_2)\cdots(x - \pi_n)$, and it follows that $|a_i|_p < 1$ for $0 \leq i < n$ by the non-archimedean principle. There, conditions i), ii), and iii) hold and $f(x)$ is an Eisenstein polynomial. □

In the next proof, we describe the unramified extensions of $\mathbb{Q}_p$. Here, we use a bar represent an element in a finite field. Also in a field F, $F^\times$ denotes the multiplicative group of non-zero elements of F.

Proposition 4.6. *There is exactly one unramified extension K_f^{unram} of $\mathbb{Q}_p$ of degree f, and it can be obtained by adjoining a primitive $(p^f - 1)$th root of unity. If K is an extension of $\mathbb{Q}_p$ of degree n, index of ramification e, and residue field degree f (so that $n = ef$ as in Proposition 4.4), then $K = K_f^{\text{unram}}(\pi)$, where π satisfies an Eisenstein polynomial with coefficients in K_f^{unram}.*

Proof. This proof follows [3, p.67]. Let $\overline{\alpha}$ be a generator of the multiplicative group $\mathbb{F}_{p^f}^\times$ so that $\mathbb{F}_{p^f}^\times = \{\overline{\alpha}, \overline{\alpha}^2, \ldots, \overline{\alpha}^{p^f-1}\}$, and let $\overline{P}(x) = x^f + \overline{a}_{f-1}x^{f-1} + \cdots + \overline{a}_0$, $\overline{a}_i \in \mathbb{F}_p$ be its minimal polynomial over $\mathbb{F}_p$. That is, $\deg(\overline{P}) = [\mathbb{F}_p(\overline{\alpha}) : \mathbb{F}_p] = [\mathbb{F}_{p^f} : \mathbb{F}_p] = f$. For each i, let $a_i \in \mathbb{Z}_p$ be any element such that $a_i \equiv \overline{a}_i \pmod{p}$, and let $P(x) = x^f + a_{f-1}x^{f-1} + \cdots + a_0$. Clearly, $P(x)$ is monic. Now, if $P(x)$ were reducible it would be the product of two polynomials, $P(x) = (x^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0)(x^l + c_{l-1}x^{l-1} + \cdots + c_1x + c_0)$ where $m + l = f$, $m, l \geq 1$, and coefficients $b_i, c_i \in \mathbb{Z}_p$ could be reduced (mod p) to coefficients in $\mathbb{F}_p$. But, this new product would equal $\overline{P}(x)$, contradicting that $\overline{P}(x)$ is irreducible. Therefore, $P(x)$ is irreducible. So, take a root

α of $P(x)$ and adjoin this to $\mathbb{Q}_p$ to get $\mathbb{Q}_p(\alpha) = K$, and let $A = \{x \in K \mid |x| \leq 1\}$ and $M = \{x \in K \mid |x| < 1\}$ as in Proposition 4.3. Then, $n = [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = f$, while the coset $\alpha + M$ has the degree f minimal polynomial $\overline{P}(x)$ over $\mathbb{F}_p$. Thus, $[A/M : \mathbb{F}_p] = f$ and using the relation $f = \dfrac{n}{e}$ from Proposition 4.4 shows $e = 1$, meaning $\mathbb{Q}_p(\alpha)$ is an unramified extension of $\mathbb{Q}_p$ of degree f.

For uniqueness, let $\widetilde{K}$ be another finite extension of $\mathbb{Q}_p$ of degree n, index of ramification e, and residue field degree f. Also, let $\widetilde{A} = \{x \in \widetilde{K} \mid |x| \leq 1\}$ and $\widetilde{M} = \{x \in \widetilde{K} \mid |x| < 1\}$, so that $\widetilde{A}/\widetilde{M} = \mathbb{F}_{p^f}$. Then, let $\overline{\beta} \in \mathbb{F}_{p^f}$ be a generator of the multiplicative group $\mathbb{F}_{p^f}^{\times}$. Let $\beta_0 \in \widetilde{A}$ be any element that reduces to $\overline{\beta}$ mod $\widetilde{M}$. Finally, let $\pi \in \widetilde{K}$ be any element with $v_p(\pi) = \dfrac{1}{e}$.

We claim that there exists $\beta \equiv \beta_0 \pmod{\pi}$ where $\beta \in \widetilde{K}$ such that $\beta^{p^f-1} - 1 = 0$, i.e., we want β to be a $(p^f - 1)$th root of unity. The technique used to prove this claim is very similar to that used to prove Hensel's Lemma (Theorem 3.4). That is, we write $\beta \equiv \beta_0 + \beta_1\pi \pmod{\pi^2}$. Then, we want $\beta^{p^f-1} - 1 = 0 \Rightarrow (\beta_0 + \beta_1\pi)^{p^f-1} - 1 \equiv 0 \pmod{\pi^2}$. Next, recall the binomial theorem which says, $(x+y)^n = \binom{n}{0}x^n y^0 + \binom{n}{1}x^{n-1}y^1 + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-1}x^1 y^{n-1} + \binom{n}{n}x^0 y^n$. So, we expand $(\beta_0+\beta_1\pi)^{p^f-1} = \beta_0^{p^f-1} + (p^f-1)\beta_0^{p^f-2}\beta_1\pi + \binom{p^f-1}{2}\beta_0^{p^f-3}(\beta_1\pi)^2 + \cdots$, but $\pi^2 \equiv \pi^3 \equiv \cdots \equiv \pi^{p^f-1} \equiv 0 \pmod{\pi^2}$, and we may ignore these higher terms. Also, since p^f is the order of $\widetilde{A}/\widetilde{M}$, $p^f \equiv 0 \pmod{\pi}$, and so we reduce our equation to $\beta_0^{p^f-1} - \beta_0^{p^f-2}\beta_1\pi - 1 \equiv 0 \pmod{\pi^2}$. Solving, we get $\beta_1 \equiv (\beta_0^{p^f-1} - 1)/(\pi\beta_0^{p^f-2}) \pmod{\pi}$. Continuing in this way, we find a solution $\beta = \beta_0 + \beta_1\pi + \beta_2\pi^2 + \cdots$ to the equation $\beta^{p^f-1} = 1$. Finally, since the elements $\overline{\beta}, \overline{\beta}^2, \ldots, \overline{\beta}^{p^f-1}$ of $\mathbb{F}_{p^f}$ are all distinct, $\beta, \beta^2, \ldots, \beta^{p^f-1}$ are distinct, meaning β is indeed a primitive $(p^f - 1)$th root of unity. Note that $[\mathbb{Q}_p(\beta) : \mathbb{Q}_p] \geq f = [\widetilde{A}/\widetilde{M} : \mathbb{F}_p] = [\mathbb{F}_{p^f} : \mathbb{F}_p]$ by Proposition 4.3.

Now, the above construction of β also applies to our α from the first paragraph. Therefore, $\beta \in \mathbb{Q}_p(\alpha)$ and $\mathbb{Q}_p(\beta) \subset \mathbb{Q}_p(\alpha)$, where we just showed β is a primitive $(p^f - 1)$th root of unity. But, we saw $f = [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] \geq [\mathbb{Q}_p(\beta) : \mathbb{Q}_p] \geq f$, which

implies $\mathbb{Q}_p(\alpha) = \mathbb{Q}_p(\beta)$. Thus, the unramified extension of degree f is unique, and we denote it K_f^{unram}.

For the last part of the proof, we must show $K = K_f^{\text{unram}}(\pi)$, where π is a uniformizer of K over $\mathbb{Q}_p$ and satisfies an Eisenstein polynomial. This is similar to our argument in Proposition 4.5. So, let $E(x)$ be the minimal polynomial with degree d of π over K_f^{unram} such that $E(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_1 x + c_0 = (x-\pi_1)(x-\pi_2)\cdots(x-\pi_d)$. This polynomial is clearly monic ($|c_d|_p = |1|_p = 1$). Then, by Definition 4.1 each π_i has the same norm, and so $|\pi_1| = |\pi_2| = \cdots = |\pi_d| = p^{-1/e} < 1$. Now, since the coefficients c_i are combinations of the roots π_i, it follows by the non-archimedean property that $|c_i|_p < 1$. Finally, observe that the constant term is $c_0 = (-1)^d \pi_1 \cdot \pi_2 \cdot \cdots \cdot \pi_d$. Then, $v_p(c_0) = v_p(\pi_1) + v_p(\pi_2) + \cdots + v_p(\pi_d) = d(\frac{1}{e})$. But since $ef = n = [K : \mathbb{Q}_p] = [K : K_f^{\text{unram}}] \cdot [K_f^{\text{unram}} : \mathbb{Q}_p] = [K : K_f^{\text{unram}}] \cdot f \Rightarrow e = [K : K_f^{\text{unram}}]$, it follows that $d \leq e$. Then since $c_0 \in K_f^{\text{unram}}$, $v_p(c_0)$ is an integer, and we conclude that $d = e$ with $v_p(c_0) = 1 \Rightarrow |c_0|_p = \dfrac{1}{p}$. Therefore, $E(x)$ is an Eisenstein polynomial and $K = K_f^{\text{unram}}(\pi)$. □

By classifying the totally ramified and unramified extensions, these last two propositions do a good job of categorizing arbitrary finite extensions of $\mathbb{Q}_p$ because it turns out any extension is obtained by adjoining a combination of the two [3]. So, with a basic description of finite extensions of $\mathbb{Q}_p$ in hand, the reader can move on to describe the algebraic closure of the field of p-adic numbers. This field is not complete, so an additional step is necessary to find a field containing $\mathbb{Q}_p$ that is both complete and algebraically closed. Then, with such a field, many options, including analysis of the p-adic numbers, are open to the reader.

References

[1] C.C. MacDuffee. *The p-Adic Numbers of Hensel. The American Mathematical Monthly*, Vol. 45, No. 8 (Oct., 1938), pp. 500-508.

[2] F.Q. Gouvêa. *p-adic Numbers: An Introduction*. Springer-Verlag, New York, Berlin, Heidelberg, first edition, 1993.

[3] N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-functions*. Springer-Verlag, New York, Berlin, Heidelberg, second edition, 1984.

[4] J. Howie. *Fields and Galois Theory*. Springer-Verlag, London, New York, first edition, 2005.