THE P-ADIC COMPLETION OF $\mathbb{Q}$ AND HENSEL'S LEMMA

THEODOR CHRISTIAN HERWIG

Abstract. We provide an introduction to the p-adic metric and its applications to algebra, analysis, topology, and number theory. We begin by emphasizing the properties of a non-archimedean norm and exploring the topology it induces. From there, we follow the process of completing $\mathbb{Q}$ with respect to this norm, obtaining $\mathbb{Q}_p$ and examining the algebraic structure of this new field. Finally, our discussion culminates with the proof of Hensel's Lemma, a number theoretic result stating the ability to 'lift' roots of polynomials mod p to obtain unique roots modulo any higher power of p. We assume a basic knowledge of group and ring theory.

Contents

Introduction 1
1. The p-adic Metric 2
2. The Topology of Non-Archimedean Spaces 4
3. The Completion of $\mathbb{Q}$ to $\mathbb{Q}_p$ 6
4. Algebra on $\mathbb{Q}_p$ 9
5. Hensel's Lemma 10
Acknowledgments 13
References 13

Introduction

The p-adics present a particularly rich subject; they cut across many disciplines in mathematics, largely beginning in analysis, and expanding from there to topology, algebra, and number theory. Our consideration of the p-adics is born out of analysis; the p-norm (denoted $|x|_p$) is a non-standard way to define absolute value based upon prime factors p contained in the number x. At first glance, this new norm may seem arbitrary, but a theorem due to Ostrowski proves that, in fact, the only possible constructions of absolute value on the rationals are these p-norms and the conventional absolute value.

Theorem 0.1 (Ostrowski)**.** *Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to either one of the absolute values $|\cdot|_p$ or the standard absolute value.*

For a proof, see [Go]. Because we go on to use this norm in defining a completion of $\mathbb{Q}$ alternate to $\mathbb{R}$, Ostrowski's result tells us of its importance: in effect, real analysis and p-adic analysis are the only two options for discussing the Cauchy-completion of the field of rational numbers.

We will detail exactly how this completion is constructed and go on to examine how algebra on this field interacts with its topology. Once equipped with these tools, we will have the power to prove Hensel's Lemma, a result from number theory. Our proof, adopted from techniques of [Go], will draw on the analytic and algebraic results we will develop as we go. Hensel's Lemma allows us to find roots to polynomials in $\mathbb{Z}_p$ with integer coefficients by looking for roots modulo

Date: August 26, 2011.

p, using a process akin to Newton's method for finding roots of equations through approximation by derivatives.

1. The p-adic Metric

To begin, we define the notion of an absolute value. This type of function is familiar from calculus and analysis and satisfies three important conditions.

Definition 1.1. An *absolute value* on a field $\mathbb{K}$ is a function

$$|\cdot| : \mathbb{K} \to \mathbb{R}_+$$

(where $\mathbb{R}_+ = \{x \text{ in } \mathbb{R} : x \geq 0\}$) that satisfies the following conditions:

i) $|x| = 0$ if and only if $x = 0$
ii) $|xy| = |x||y|$ for all x, y in $\mathbb{K}$
iii) $|x + y| \leq |x| + |y|$ for all x, y in $\mathbb{K}$

We will say that an absolute value on $\mathbb{K}$ is *non-archimedean* if it also satisfies the condition that

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

for all x, y in $\mathbb{K}$. Otherwise, we will say that the absolute value is *archimedean.*

One may recall another definition of an archimedean norm on a metric space in which, for any $\varepsilon > 0$, there exists an integer N such that $1/N < \varepsilon$. This, in effect, is saying that we can have 'arbitrarily large' integers.

However, using the definition of a non-archimedean norm we have laid out above, we can show these ideas are equivalent. Take the non-archimedean triangle inequality $|x+y| \leq \max\{|x|, |y|\}$ and apply it to $x = N$, a large integer, and $y = 1$. Then since $N > 1$ we obtain $|N + 1| \leq |N|$. So with this norm we cannot always keep adding units indefinitely to progress from some N to some $1/\varepsilon$, as in the archimedean case. Thus, our two seemingly different notions of the archimedean property are in fact equivalent.

We will soon revisit the idea of the non-archimedean property and the unique type of topology it induces on a space. First, however, we must develop language that we can use in constructing and describing the p-adic metric.

Definition 1.2. Fix a prime number p in $\mathbb{Z}$. The *p-adic valuation* on $\mathbb{Z}$ is the function

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

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

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

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

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

We further define $v_p(0)$ to be $+\infty$.

We see in the following lemma that the p-adic valuation exhibits properties curiously similar to the log of the absolute value. Perhaps our intuition will lead us to search for some connection between the two.

Proposition 1.3. *For all x, y in $\mathbb{Q}$, we have*

i) $v_p(xy) = v_p(x) + v_p(y)$,
ii) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$;

with the obvious conventions with respect to $v_p = +\infty$.

Proof. (1) The proof follows easily from Definition 1.2 and the laws of logarithmic addition.
(2) Let $x = a/b$ and let $y = c/d$. Fix a prime p. Write $x + y = p^{v_p(x)}a'/b' + p^{v_p(y)}c'/d'$. Assume without loss of generality that $v_p(x) \leq v_p(y)$ and write $v_p(x) + n = v_p(y)$ from some n in $\mathbb{N}$. Then

$$x + y = p^{v_p(x)}(a'/b' + p^n c'/d') = p^{v_p(x)}\frac{a'd' + p^n b'c'}{b'd'}. \tag{1.4}$$

Notice that we have already imposed the condition that $b'd'$ has no factors of p in it, but we cannot say with certainty whether the numerator $(a'd' + p^n b'c')$ of the final fraction in Equation 1.4 will introduce any new prime factors. Clearly then, since we have assumed that $v_p(x) = \min\{v_p(x), v_p(y)\}$, we have that $v_p(x + y) \geq v_p(x)$ proving the lemma. □

We find that our intuition was in fact correct and formalize the connection between p-adic valuations and absolute values in the following definition.

Definition 1.5. For any x in $\mathbb{Q}$, we define the *p-adic absolute value* of x by

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

if $x \neq 0$, and we set $|0|_p = 0$.

Notice that this definition is consistent with our definition that $v_p(0) = +\infty$. Also observe that by the previous lemma, we have defined a non-archimedean absolute value on $\mathbb{Q}$. We can check that this is in fact an absolute value by verifying the three criteria laid out in Definition 1.1.

Lemma 1.6. *We have rightly defined a non-archimedean absolute value on $\mathbb{Q}$.*

Proof. The first criterion ($|x| = 0$ if and only if $x = 0$) is satisfied one way because we define $|0|_p = 0$ and the other way because for nonzero x we can never have $p^{-v_p(x)}$ equal to zero since p is never zero. For the second criterion ($|xy| = |x||y|$ for all x, y in a field $\mathbb{K}$), take x, y in $\mathbb{Q}$ so $|x|_p = p^{-v_p(x)}$ and $|y|_p = p^{-v_p(y)}$ so that $|x|_p|y|_p = p^{-v_p(x)-v_p(y)}$. The Fundamental Theorem of Arithmetic tells us that the number of prime factors p in xy is the same as the sum of the factors in x and y individually ($v_p(x) + v_p(y)$), so $|xy|_p = p^{-v_p(x)-v_p(y)}$ as desired. The non-archimedean property follows directly from parts (i) and (ii) of Proposition 1.3. □

Before we move on, let us observe for a moment exactly how this p-norm behaves with a few brief computational examples.

Exercise 1.7. Arrange the following elements of $\mathbb{Q}$ in order of increasing 3-adic magnitude:

$$63, 1/27, 686, 13929, 243/3879$$

(Hint: Notice $63 = 3^2 \times 7, 1/27 = 3^{-3}, 686 = 2 \times 7^3, 13929 = 3 \times 4643, 243/3879 = 27/431 = 3^3 \times 1/431$)

Exercise 1.8. Find a sequence of rational numbers that converges to zero, 7-adically. (Hint: $|7^n|_7 = 1/7^n$).

Exercise 1.9. Find a sequence of rational numbers that converges to 32, 7-adically.

Exercise 1.10. Find a sequence of rational numbers that converges to $\sqrt{7}$, 7-adically.

Remark 1.11. The first two examples are trivial and pertinent solely to get used to thinking of 'distance' in the non-archimedean way, especially as it relates to convergence of sequences. The third requires more careful thought but is certainly within reach. The fourth is a bit trickier and to determine what exactly this question is asking will require concepts developed more fully in Section 3.

2. The Topology of Non-Archimedean Spaces

Now that we have defined a metric, the obvious next step is to apply it to a space and see what we get. It turns out that by modifying the triangle inequality, with which we are all-too-familiar, into the stronger non-archimedean property, we induce non-intuitive conditions that are responsible for much of the interesting behavior we encounter in this section. For a more extensive look at these results, the interested reader may refer to [Sa]. First we formally define distances.

Definition 2.1. Let $\mathbb{K}$ be a field and $|\cdot|$ an absolute value on $\mathbb{K}$. We define the distance $d(x, y)$ between two elements x, y in $\mathbb{K}$ by

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

The function $d(x, y)$ is called the *metric* induced by the absolute value.

Lemma 2.2. *Let $|\cdot|$ be an absolute value on a field $\mathbb{K}$ and define a metric by $d(x, y) = |x - y|$. Then $|\cdot|$ is non-archimedean if and only if for any x, y, z in $\mathbb{K}$, we have*

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

Proof. This follows immediately from the non-archimedean property and Definition 2.1. □

So far this looks very much like the definitions we encountered in the previous section and feels intuitive if unfamiliar. Now, however, we have the tools to take this concept farther and develop some truly bizarre results.

Proposition 2.3. *Let $\mathbb{K}$ be a field and let $|\cdot|$ be a non-archimedean absolute value on $\mathbb{K}$. If x, y in $\mathbb{K}$ and $|x| \neq |y|$, then*

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

Proof. If x and y are in $\mathbb{K}$, then without losing generality we assume $|x| > |y|$. Then Lemma 2.2 tells us

$$|x + y| \leq |x| = \max\{|x|, |y|\}. \tag{2.4}$$

On the other hand, $x = (x + y) - y$, so by application of the same lemma

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

Since we know that $|x| > |y|$, this inequality can hold only if

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

This gives the reverse inequality $|x| \leq |x + y|$. But since we also know $|x| \geq |x + y|$ (Equation 2.4), we can conclude that $|x| = |x + y|$. □

This paves the way for a result which will be fundamental to all following results regarding the topology of non-archimedean metric spaces.

Corollary 2.5. *In a space with a non-archimedean metric, all 'triangles' are isosceles.*

Proof. Let x, y, z be three elements of our space (i.e., the vertices of our 'triangle'). The lengths of the sides of this 'triangle' are the three distances

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

Now, of course,

$$(x - y) + (y - z) = (x - z),$$

so that we can invoke Proposition 2.3. Now, without loss of generality, we can have $|x - y| \neq |y - z|$, and then we may say that $|x - z|$ is equal to $\max\{|x - y|, |y - z|\}$. In any case, two of the 'sides' are equal. □

Exercise 2.6. We now know that in a space with a non-archimedean metric, all triangles are isosceles. Can we make a further generalization about equilateral triangles?

At this point, we recall some basic definitions from topology necessary in our discussion of spaces.

Definition 2.7. In a metric space

i) A set U is *open* if any element in U belongs to an open ball that is contained in U.
ii) A set is *closed* if its complement is an open set.
iii) A point x is a *boundary point* of a set S if any open ball with center x contains points that are in S and points that are not in S.

S is closed exactly when it contains all of its boundary points.

Definition 2.8. Let $\mathbb{K}$ be a field with an absolute value $|\cdot|$. Let a be an element of $\mathbb{K}$ and let r be a positive real number. The *open ball* of radius r and center a is the set

$$B(a,r) = \{x \text{ in } \mathbb{K} : d(x,a) < r\} = \{x \text{ in } \mathbb{K} : |x-a| < r\}.$$

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

$$\overline{B}(a,r) = \{x \text{ in } \mathbb{K} : d(x,a) \leq r\} = \{x \text{ in } \mathbb{K} : |x-a| \leq r\}.$$

Given this, we are ready to discuss the topology of our p-normed space in earnest. We now present *three* startling and non-intuitive results describing these balls and the topology surrounding them. First, any point in the interior of a ball, open or closed, is a center for that ball. Second, each ball, open or closed, is an open *and* closed set. Third, if two balls intersect, one must be contained within the other.

Proposition 2.9. *Let $\mathbb{K}$ be a field with a non-archimedean absolute value.*

i) *If b is in $B(a,r)$, then $B(a,r) = B(b,r)$.*
ii) *The set $B(a,r)$ is open and closed.*
iii) *If a, b are in $\mathbb{K}$ and r, s are in $\mathbb{R}_+^\times$, we have $B(a,r) \cap B(b,s) \neq \emptyset$ if and only if $B(a,r) \subset B(b,s)$ or $B(a,r) \supset B(b,s)$.*

Proof. *i*) Definition 2.8 tells that if b in $B(a,r)$, then $|b-a| < r$. Now we apply the non-archimedean property (Lemma 2.2) to any other x for which $|x-a| < r$ so that

$$|x-b| \leq \max(|x-a|, |b-a|) < r$$

which gives that x in $B(b,r)$ by Definition 2.8, giving us that $B(a,r) \subset B(b,r)$. Switching a and b, we get the opposite inclusion so the two balls are the same.

ii) Clearly the open ball $B(a,r)$ is an open set, regardless of the chosen metric space. To show that is it also closed, we pick some x which is a boundary point of $B(a,r)$, so that any open ball centered at x must contain points that are in $B(a,r)$. Choose some number $s \leq r$ and examine the open ball $B(x,s)$. Since x is a boundary point we know that $B(a,r) \cap B(x,s) \neq \emptyset$, so that there exists an element y in $B(a,r) \cap B(x,s)$.

In reference to our definition of the respective balls, this means that $|y-a| < r$ and $|y-x| < s \leq r$. Again by Lemma 2.2 we get the non-archimedean result

$$|x-a| \leq \max(|x-y|, |y-a|) < \max(s,r) \leq r$$

so that x is in $B(a,r)$. Thus because $B(a,r)$ contains each of its boundary points, Definition 2.7 tells us that $B(a,r)$ is a closed set.

iii) Assume without loss of generality that $r \leq s$. If the intersection is non-empty then there exists a c in $B(a,r) \cap B(b,s)$. Then we know, from (i), that $B(a,r) = B(c,r)$ and $B(b,s) = B(c,s)$. Hence

$$B(a,r) = B(c,r) \subset B(c,s) = B(b,s)$$

as claimed. □

Exercise 2.10. Prove these three results for the closed ball $\overline{B}(a, r)$.

These results will serve to conclude our elementary discussion of the topological structure of p-adic normed metric spaces. Presently, we will turn back to the question posed in Exercise 1.10, explore the limits of the p-norm applied to rational numbers only, and how it might make sense to talk about the absolute value of numbers outside of $\mathbb{Q}$.

3. The Completion of $\mathbb{Q}$ to $\mathbb{Q}_p$

When evaluating limits of sequences earlier in Section 1, we had had to pause before attacking the question of a sequence approaching $\sqrt{7}$. While we could easily create a sequence of rational numbers converging to $\sqrt{7}$ in the usual sense (for example: $2, 2.6, 2.64, 2.645, \ldots$) this doesn't necessarily interest us. The whole idea of a converging sequence is that the terms get 'closer' and 'closer' over time but we don't really know how to interpret that in this context. (Our intuition of course tells us by now that "close" is a loaded word, so we must wait and define it in this new context.) The reason this particular exercise interests us is that it presents a problem with our metric space. It is not complete. That is, not all Cauchy sequences of rational numbers converge to rational numbers, but something else altogether. Recall that when one completes $\mathbb{Q}$ with respect to the usual absolute value, we arrive at $\mathbb{R}$, the familiar reals. However, in this section we will develop a completion of $\mathbb{Q}$ based instead upon the p-adic absolute value, leading us to the complete metric space $\mathbb{Q}_p$.

We begin this formal completion by recalling the precise definition of a Cauchy sequence and what it means with respect to the p-adic norm.

Definition 3.1. Let $\mathbb{K}$ be a field and let $|\cdot|$ be an absolute value on $\mathbb{K}$.

i) A sequence of elements x_n in $\mathbb{K}$ is called a *Cauchy sequence* if for every $\epsilon > 0$ one can find an M such that we have $|x_n - x_m| < \epsilon$ for every $n, m \geq M$.

ii) The field $\mathbb{K}$ is called *complete* with respect to $|\cdot|$ if every Cauchy sequence of elements of $\mathbb{K}$ has a limit.

iii) A subset $S \subset \mathbb{K}$ is called *dense* in $\mathbb{K}$ if every open ball around every element of $\mathbb{K}$ contains an element of S.

It is easy to show that $\mathbb{Q}$ is not complete by constructing a Cauchy sequence whose limit is not in $\mathbb{Q}$: for example, a Cauchy sequence in $\mathbb{Q}$ converging to $\sqrt{7}$. We will remedy this by completing $\mathbb{Q}$ with respect to the p-adic metric, to $\mathbb{Q}_p$.

It will be helpful through this process to keep in mind the more familiar completion of $\mathbb{Q}$ to $\mathbb{R}$. The idea is the same in that we seek to modify the rationals by adding in the limits of all Cauchy sequences and then create equivalence classes of sequences, i.e., sequences converging to the same limit. In fact, the only difference from the completion to $\mathbb{R}$ is how we define the norm on the limit.

We will proceed with the goal of defining numbers in our new field, $\mathbb{Q}_p$ as sequences in $\mathbb{Q}$. With this definition we arrive at a set $\mathcal{C}$, which is a formal analytic completion of $\mathbb{Q}$, since all sequences in this set will converge to a member of $\mathcal{C}$.

Definition 3.2. Let $|\cdot| = |\cdot|_p$ be a non-archimedean absolute value on $\mathbb{Q}$. We denote by $\mathcal{C}$, or $\mathcal{C}_p(\mathbb{Q})$ if we want to emphasize p and $\mathbb{Q}$, the set of all Cauchy sequences of elements of $\mathbb{Q}$:

$$\mathcal{C} = \mathcal{C}_p(\mathbb{Q}) = \{(x_n) : (x_n) \text{ is a Cauchy sequence with respect to } |\cdot|_p\}.$$

However, though this set is a formal completion of $\mathbb{Q}$, it leaves still something to be desired. We would like to impose the condition that all sequences converging to the same value in $\mathcal{C}$ be equivalent to one another (just as we do in the completion to $\mathbb{R}$). We will use the tools of algebra to achieve this by 'modding out' these extraneous sequences, all converging to a single value,

effectively creating classes of sequences whose members we will consider equivalent. Using the machinery of the quotient ring to achieve this, we must first clarify how we will treat $\mathcal{C}$ as a ring, specifically choosing to add and multiply sequences term-by-term.

Exercise 3.3. Check that $\mathbb{Q}$ is a commutative ring with identity.

We check that $\mathcal{C}$ has the natural ring structure, using the above definitions of product and sum.

Proposition 3.4. *Defining*

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

makes $\mathcal{C}$ a commutative ring with unity.

Proof. The conditions that addition and multiplication be commutative and associative as well as distributive, follow immediately from the fact that $\mathbb{Q}$ is a ring itself. The identity is clearly just the class of sequences converging to 1 (take the constant sequence $x_n = 1$, for example). We simply must check that the sum and product of two Cauchy sequences is also a Cauchy sequence.

This is simple. If we know that (x_n) is bounded by $\epsilon/2$, for all $n > M$, and (y_n) is bounded by $\epsilon/2$, for all $n > N$, then clearly $(x_n + y_n)$ is bounded by ϵ for all $n > \max\{M, N\}$. For the multiplicative case we use the definition of a Cauchy sequence and note that

$$\begin{aligned} |x_n y_n - x_m y_m| &= |x_n y_n - x_m y_n + x_m y_n - x_m y_m| \\ &= |y_n(x_n - x_m) + x_m(y_n - y_m)|. \end{aligned}$$

And of course we may bound x_n and y_n (say by some large positive constants A and B, respectively) by definition and also the differences $(x_n - x_m)$ and $(y_n - y_m)$ (choosing $\epsilon/2B$ and $\epsilon/2A$, respectively). Thus we get

$$|x_n y_n - x_m y_m| < \left| B\left(\frac{\epsilon}{2B}\right) + A\left(\frac{\epsilon}{2A}\right) \right| = \epsilon$$

completing the proof. □

Furthermore, it is easy to notice that $\mathbb{Q}$ is included within $\mathcal{C}$ simply by considering the map from some rational x to a corresponding constant sequence (x) in $\mathcal{C}$.

Now we define exactly how we propose to 'mod out' equivalent sequences by constructing classes that will become the elements of our final goal, $\mathbb{Q}_p$.

Definition 3.5. We define $\mathcal{N} \subset \mathcal{C}$ to be the ideal

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

of sequences that tend to zero with respect to the absolute value $|\cdot|_p$.

Exercise 3.6. Check that $\mathcal{N}$ is indeed an ideal.

This is the obvious choice of ideal because now we can compare different Cauchy sequences and call them equivalent if their difference is in $\mathcal{N}$.

Note further that $\mathcal{N}$ must be maximal. Too see this, suppose that we add another element to our ideal not already in $\mathcal{N}$, i.e., some sequence (z_n) where $\lim_{n\to\infty} |z_n|_p \neq 0$. This sequence will become a unit in the ideal, necessitating the inclusion of other elements in accordance with the rules we have established for sequence arithmetic. We leave it as an exercise to show why this ideal we have constructed is $\mathcal{C}$ itself. This at last brings us to what we have sought all along: what we propose as a completion of $\mathbb{Q}$.

Definition 3.7. We define the field of p-adic numbers to be the quotient of the ring $\mathcal{C}$ by its maximal ideal $\mathcal{N}$:

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

Here we have constructed a new ring $\mathbb{Q}_p$, based upon the non-archimedean norm $|\cdot|_p$ but actually, we still do not 'know how to use it' on the majority of numbers in $\mathbb{Q}_p$, i.e., those not corresponding to the classes of constant sequences of rational numbers. In other words, we have clearly defined $|x|_p$ for x in $\mathbb{Q}$ but don't yet know how to interpret it for x in $\mathbb{Q}_p$. We want to show that this absolute value intuitively extends to $\mathbb{Q}_p$. To do so, we prove the following helpful lemma.

Lemma 3.8. *Let (x_n) be a member of $\mathcal{C}$, not in the ideal $\mathcal{N}$. The sequence of rational numbers $(|x_n|_p)$ is eventually stationary, that is, there exists an integer N such that $|x_n|_p = |x_m|_p$ whenever $m, n \geq N$.*

Proof. Since (x_n) is a Cauchy sequence which does not tend to zero, we can find c and N_1 such that

$$n \geq N_1 \Longrightarrow |x_n|_p \geq c > 0.$$

On the other hand, there also exists an integer N_2 for which

$$n, m \geq N_2 \Longrightarrow |x_n - x_m|_p < c.$$

Set $N = \max\{N_1, N_2\}$ so that we then have, by Lemma 2.2,

$$n, m \geq N_2 \Longrightarrow |x_n - x_m|_p < \max\{|x_n|_p, |x_m|_p\}$$

and so $|x_n|_p = |x_m|_p$ by Corollary 2.5 ('all triangles are isosceles'). □

It then makes sense to accept this limiting value as the norm. It is both intuitive and consistent with our previous definition of a norm for the rational numbers, so we have checked that the following definition makes sense.

Definition 3.9. If λ is an element of $\mathbb{Q}_p$ and (x_n) is any Cauchy sequence representing λ, we define

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

It is trivial to see that $|\lambda|_p$ is well-defined. Simply consider two sequences x_n and y_n converging to the same limit. Then we have $x_i - y_i = 0$, which tells us that the sequence is in $\mathcal{N}$ and $\lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n$.

Finally, there is one last question to address on the subject of this completion. We know that $\mathbb{Q}$ is a field, and we know that $\mathbb{Q}_p$ is an analytically complete ring, as we have just completed it, but we have not verified that it is in fact also a field. We dispatch with that now.

Proposition 3.10. *$\mathbb{Q}_p$ is a field.*

Proof. We already know that $\mathbb{Q}_p$ is a commutative ring with unity, so the only thing left to prove is that all non-zero elements have inverses in $\mathbb{Q}_p$. To do so, it suffices to check that elements which are not in $\mathcal{N}$ have inverses in $\mathcal{C}$, or rather that $\mathcal{N}$ is a maximal ideal of $\mathcal{C}$. Because $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, we know that we can describe any member of $\mathbb{Q}_p$ as a sequence x_n of rational numbers (stipulating each $x_n \neq 0$, since $\lim_{n\to\infty} x_n \neq 0$). We can then take the inverse of each member of that sequence $(1/x_n)$, which we claim represents the inverse of the original member of $\mathbb{Q}_p$. To realize this, multiply the two sequences together (term-by-term, as defined above), to see that we are left with the sequence (1), which of course corresponds to the multiplicative identity in $\mathbb{Q}_p$. But how do we know that $(1/x_n)$ is Cauchy? Simply consider $|1/x_n - 1/x_m|_p = \dfrac{|x_m - x_n|_p}{|x_m x_n|_p}$. The limit of the numerator of this fraction is zero because (x_n) is Cauchy and the denominator is a nonzero constant by Lemma 3.8 and our stipulation that $x_n \neq 0$, so the entire fraction tends to zero. Thus, all 'non-zero' sequences (i.e. those not in $\mathcal{N}$) have inverses modulo $\mathcal{N}$, proving that $\mathbb{Q}_p$ is indeed a field. □

Finally, we have a formal completion of the rationals to $\mathbb{Q}_p$, which is confirmed to be a field, leaving us with the opportunity to move on and to arrive at more interesting results. Our ultimate goal will be to construct special polynomials with coefficients in $\mathbb{Q}_p$ and examine their roots over varying conditions. Before we get there, however, we would be remiss to introduce algebraic structure solely for the purposes of completion. Perhaps the most interesting aspect of the p-adics is the interaction between the topology and algebra on the field, which is far different from anything that occurs on the reals. In the next section we delve a bit deeper into this structure, albeit briefly, making connections to the topology we discussed in Section 2 and preparing for a discussion of polynomials in $\mathbb{Q}_p$ with Hensel's Lemma on the horizon.

4. Algebra on $\mathbb{Q}_p$

Remark 4.1. In this section, basic knowledge of group and ring theory is assumed. For reference or further reading on related topics, see [DF].

Taking a second look at concepts introduced more generally in Section 2, we now specifically revisit the closed unit ball, through a new lens.

Definition 4.2. The *ring of p-adic integers* is the ring

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

Note that according to this definition, all of the integers (in the traditional sense) are members of $\mathbb{Z}_p$. Further, in the following discussions it may be useful to refer to another set $\mathbb{Q} \cap \mathbb{Z}_p$, the *localization of* $\mathbb{Z}$ *at* p. This set is clearly dense in $\mathbb{Z}_p$ and consists of elements of the form a/b, where p may divide a, but not b. Often this set will be easier to work with than $\mathbb{Z}_p$, and several theorems that we prove in the localization will hold for $\mathbb{Z}_p$ as well, for reasons that should be obvious to the reader at this point.

Now, when we are working in rings and seek to manipulate equations it will become very important to decide which elements are invertible, or not invertible. As the name implies, an element is invertible if its inverse is also an element of the given ring. Therefore, 26 is not invertible in the ring of even numbers because its multiplicative inverse $1/26$ is not even. Perhaps more in our vein, 26 is not invertible in the ring of 13-adic integers $\mathbb{Z}_{13}$ since, though $|26|_{13} = 1/13 < 1$, there exists no element 26^{-1} in $\mathbb{Z}_{13}$. This is because such an element would necessarily have $|26^{-1}| = 13 > 1$. The intuition from this second example leads to the following proposition.

Proposition 4.3. *The ring $\mathbb{Z}_p$ of p-adic integers is a ring whose maximal ideal is the principal ideal $p\mathbb{Z}_p = \{x \text{ in } \mathbb{Q}_p : |x| < 1\}$. Furthermore, every element of the complement $\mathbb{Z}_p - p\mathbb{Z}_p$ is invertible in $\mathbb{Z}_p$.*

Proof. To show that $p\mathbb{Z}_p$ is an ideal, we need to check that it is closed under addition, that it contains 0, and that if x is in $\mathbb{Z}_p$ and y is in $p\mathbb{Z}_p$, then xy is in $p\mathbb{Z}_p$. Closure under addition follows directly from the non-archimedean property. This closure also implies the existence of a zero element. The two assumptions for x and y say that $|x| < 1$ and $|y| \leq 1$. Since $|xy| = |x||y|$ it follows that $|xy| < 1$ so that xy is in $p\mathbb{Z}_p$.

If x is in $\mathbb{Z}_p$ but not in $\mathbb{Z}_p$ then we clearly have $|x| = 1$. Thus $|1/x| = 1$ so that x^{-1} is in $\mathbb{Z}_p$ and x is invertible in $\mathbb{Z}_p$. Finally, any ideal strictly containing $p\mathbb{Z}_p$ would have to contain an invertible element and would therefore be all of $\mathbb{Z}_p$. This shows $p\mathbb{Z}_p$ is maximal. □

Proposition 4.4. *If an element of the localization of $\mathbb{Z}$ at p is not divisible by p, then it is invertible.*

Proof. We claim the invertible elements are the set

$$\mathbb{Q} \cap \mathbb{Z}_p - \mathbb{Q} \cap p\mathbb{Z}_p = \{x \in \mathbb{Q} : |x|_p = 1\} = \{a/b \text{ such that } a, b \text{ in } \mathbb{Z} \text{ and } p \text{ does not divide } a \text{ or } b\}$$

and the non-invertible elements are the set

$$\mathbb{Q} \cap p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p < 1\} = \{a/b \text{ such that } a, b \text{ in } \mathbb{Z} \text{ and } p \text{ divides } a\}$$

where fractions a/b are in simplest form (perhaps now our motivation for labeling $p\mathbb{Z}_p$ as such is clear). That elements of $\mathbb{Q} \cap \mathbb{Z}_p - \mathbb{Q} \cap p\mathbb{Z}_p$ are invertible is trivial. However, when we inspect the inverse of an element of $\mathbb{Q} \cap p\mathbb{Z}_p$, clearly it does not fall in $\mathbb{Q} \cap p\mathbb{Z}_p$ for much the same reason why 26 was not found to be invertible in the example above. □

The *p-adic units* are the invertible elements of $\mathbb{Z}_p$. We will denote the set of all such elements by $\mathbb{Z}_p^\times$. Since x in $\mathbb{Z}_p$ means $|x|_p \leq 1$ and x^{-1} in $\mathbb{Z}_p$ means $|x^{-1}|_p = |x|_p^{-1} \leq 1$, we see that

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : |x|_p = 1\}.$$

It is also easy to see that

$$\mathbb{Z}_p^\times \cap \mathbb{Q} = \left\{ \frac{a}{b} \in \mathbb{Q} : p \text{ does not divide } ab \right\}$$

is the set of invertible elements of the localization of $\mathbb{Z}$ at p.

Recall an interesting result from Section 2, Proposition 2.9 *(ii): the set $B(a, r)$ is both open and closed*. While we have already proved this result, the following proposition should give the reader a better idea of exactly what is going on at the boundary points in such a ball. The key lies in the equality

$$p\mathbb{Z}_p = \{x \in \mathbb{Z}_p : |x|_p < 1\} = \{x \in \mathbb{Z}_p : |x|_p \leq 1/p\},$$

specifically in the notion that the conditions $|x|_p < 1$ and $|x|_p \leq 1/p$ become equivalent in this case. It is this 'shelled' structure that is fundamental in the p-adic structure, tying together topology, analysis, and algebra.

Proposition 4.5. *We claim*

$$\mathbb{Z}_p = \bigcup_{0 \leq k \leq p-1} k + p\mathbb{Z}_p.$$

Proof. Let x be in $\mathbb{Z}_p$. If $|x|_p < 1$ then x in $p\mathbb{Z}_p$. Suppose $|x|_p = 1$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, there is some r in $\mathbb{Q}$ such that $r = a/b$ with a, b in $\mathbb{Z}$, p does not divide a or b, and $|r - x|_p < 1$. Hence, from Proposition 2.9 (every point in the interior of a ball is its center) $x + p\mathbb{Z}_p = r + p\mathbb{Z}_p$. A basic result from number theory (see [Sa]) tells us that since p and b are coprime, there exists an integer k with $0 < k \leq p - 1$ such that p divides $a - kb$. Hence, $|a - kb|_p < 1$, and also $|\frac{a-kb}{b}|_p < 1$, since p does not divide b. Thus, $|k - \frac{a}{b}|_p < 1$. It follows then that

$$k + p\mathbb{Z}_p = r + p\mathbb{Z}_p = x + p\mathbb{Z}_p,$$

so that x is in $k + p\mathbb{Z}_p$. □

This result (which would certainly startle those unaccustomed to working in non-archimedean spaces) tells us that we can take the union of p distinct open balls and be left with a closed ball. Each of these open balls represents a different equivalence class of elements of $\mathbb{Z}_p$, for a total of p different equivalence classes, as one would expect.

5. Hensel's Lemma

After discussing such topics as p-adic metrics, topologies, completions, and algebraic structures, we finally have enough mathematical dexterity to dispatch with a proof of Hensel's Lemma. Hensel's Lemma is a powerful tool which relates the roots of a given polynomial to its solution modulo a prime. The lemma and its proof both rely on iterative procedures that return an agreeable solution if supplied with a well-behaved seed. In this manner it may be useful to think about the Lemma as an analogue to Newton's Method.

Recall Newton's Method from calculus as a means of finding roots to a polynomial by choosing a seed and then making better and better approximations based on the polynomial's derivative at that point. As long as the seed is 'nice enough', one can come as close as desired to the actual solution. In the case of Newton's method, the condition on the seed is that the derivative at that point be non-zero, otherwise it supplies no useful information for improving at each iteration.

Hensel's Lemma is similar. It takes instead a polynomial with coefficients in $\mathbb{Z}_p$ and instead of requiring a 'guess' at a possible root, it requires a p-adic integer that is a root mod p, i.e. some α such that the polynomial ($F(X)$, let us say) evaluated at α is

$$F(\alpha) \equiv 0 \pmod{p\mathbb{Z}_p}.$$

This method will then return roots mod $p, p^2, p^3, \ldots$ until the desired root of the equation is found 'mod ∞'. This is the true root, which we were after in the first place.

Furthermore, for this very reason, Hensel's Lemma provides a method to find traditional roots of a polynomial even when we don't otherwise care about its behavior mod p. Because it is often easier to find the root of an equation mod p than it is to find the actual root itself, Hensel's Lemma is helpful not only in that it ensures the existence of true root, but also a method for obtaining that root numerically.

Theorem 5.1 (Hensel's Lemma)**.** *Let $F(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ be a polynomial whose coefficients are in $\mathbb{Z}_p$. Suppose that there exists a p-adic integer α_1 in $\mathbb{Z}_p$ such that*

$$F(\alpha_1) \equiv 0 \pmod{p\mathbb{Z}_p}$$

and

$$F'(\alpha_1) \not\equiv 0 \pmod{p\mathbb{Z}_p}$$

where $F'(X)$ is the formal derivative of $F(X)$. Then there exists a unique p-adic integer α in $\mathbb{Z}_p$ such that $\alpha \equiv \alpha_1 \pmod{p\mathbb{Z}_p}$ and $F(\alpha) = 0$.

Remark 5.2. At this point, the author must admit that we will abuse notation a bit in the following proof, though with the best of intentions. We will at times refer to an equivalence modulo p^n. This would be correct if we were discussing the rational elements of $\mathbb{Z}_p$, but in fact we are proving Hensel's Lemma for coefficients in $\mathbb{Z}_p$, so we take 'mod p^n' to mean that the difference of the two terms is in the set $p^n\mathbb{Z}_p$.

Proof. We will show that the root α exists by constructing a Cauchy sequence of p-adic integers converging to it. We construct the sequence $\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots$ such that, for all $n \geq 1$, we have

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

It is easy to see that such a sequence will be Cauchy. From our second rule we know that $\alpha_1 \equiv \alpha_2 \pmod{p}$ so we may write

$$\begin{aligned}
\alpha_1 &= c_0 + \text{ (terms in } p\mathbb{Z}_p, p^2\mathbb{Z}_p, p^3\mathbb{Z}_p, \ldots) \\
\alpha_2 &= c_0 + c_1p + \text{ (terms in } p^2\mathbb{Z}_p, p^3\mathbb{Z}_p, p^4\mathbb{Z}_p, \ldots) \\
\alpha_n &= c_0 + \ldots + c_np^n + \text{ (terms in } p^n\mathbb{Z}_p, p^{n+1}\mathbb{Z}_p, p^{n+2}\mathbb{Z}_p, \ldots).
\end{aligned}$$

Then we may choose an N such that for any $m, n > N$ we will have

$$\alpha_n - \alpha_m = 0 \cdot p + 0 \cdot p^2 + \ldots + 0 \cdot p^N + b_{N+1}p^{N+1} + b_{N+2}p^{N+2} + \ldots$$

where the coefficients b_n for $n > N$ may be nonzero. This ensures

$$|\alpha_n - \alpha_m|_p \leq \frac{1}{p^N}$$

so a sufficiently large N will make this difference arbitrarily small.

Furthermore, the sequence's limit α will satisfy $F(\alpha) = 0$ (this is given by the fact that the sequence is Cauchy and the polynomial is a continuous function: a routine $\epsilon - \delta$ argument) and $\alpha = \alpha_1 \pmod{p}$ (by construction). Thus once we have the α_n the theorem will be proved.

The main assumption in the theorem is that α_1 exists. To find α_2, we note that condition (ii) requires that

$$\alpha_2 = \alpha_1 + b_1 p$$

for some b_1 in $\mathbb{Z}_p$, much in the same manner that we initially proved our sequence Cauchy. Plugging this expression into the polynomial $F(X)$ and expanding, we get

$$\begin{aligned} F(\alpha_2) &= F(\alpha_1 + b_1 p) \\ &= F(\alpha_1) + F'(\alpha_1) b_1 p + \text{ terms in } p^n\mathbb{Z}_p, n \geq 2 \\ &\equiv F(\alpha_1) + F'(\alpha_1) b_1 p \pmod{p^2}. \end{aligned}$$

One way to view how we arrive at the second equality is to examine the polynomial as a Taylor series expanded about the point α_1. In reality though, because F is a polynomial, we are simply expanding it and regrouping according to powers of $p^n\mathbb{Z}_p$. This gives us terms in successively higher power of p, which we have proceeded to 'mod out' in the third line.

To show that one can find α_2, it suffices to show that we can find b_1 so that

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

Now we know that $F(\alpha_1) \equiv 0 \pmod{p}$, so that $F(\alpha_1) = px$ for some x in $\mathbb{Z}_p$. The equation then becomes

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

Note that we could write this equivalently as the product of two terms

$$p \cdot (x + F'(\alpha_1) b_1) \equiv 0 \pmod{p^2}$$

so because $p \equiv 0 \pmod{p}$ we must then have

$$x + F'(\alpha_1) b_1 \equiv 0 \pmod{p},$$

in effect, 'dividing both sides by p'. To solve this, recall that our assumptions tell us $F'(\alpha_1)$ is not divisible by p, and thus, by Proposition 4.4, is invertible in $\mathbb{Z}_p$, so that we can take

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

In fact, we can choose such a b_1 in $\mathbb{Z}$, with $0 \leq b_1 \leq p-1$, and then b_1 is uniquely determined. For this choice of b_1, we set $\alpha_2 = \alpha_1 + b_1 p$, which will have the stated properties.

This shows that one can take the first step, given α_1, find α_2. But a careful inspection shows that exactly the same calculation works to get α_{n+1} from α_n.

So, using condition (ii) once more we write

$$\alpha_{n+1} = \alpha_n + b_n p^{n+1}$$

with b_{n+1} in $\mathbb{Z}_p$. This gives us that

$$\begin{aligned} F(\alpha_{n+1}) &= F(\alpha_n + b_n p^{n+1}) \\ &= F(\alpha_n) + F'(\alpha_n) b_n p^{n+1} + \text{ terms in } p^{2n+2}\mathbb{Z}_p, p^{3n+3}\mathbb{Z}_p, \ldots \\ &\equiv F(\alpha_n) + F'(\alpha_n) b_n p^{n+1} \pmod{p^{n+2}}. \end{aligned}$$

We proceed to prove that we can find this b_n so that

$$F(\alpha_n) + F'(\alpha_n) b_n p^{n+1} \equiv 0 \pmod{p^{n+2}}.$$

We know that $F(\alpha_n) \equiv 0 \pmod{p}^n$, so that $F(\alpha_n) = p^n x$ for some x. So then

$$p^n x + F'(\alpha_n) b_n p^n \equiv 0 \pmod{p^{n+1}}$$

'dividing' by p^n we obtain

$$x + F'(\alpha_n) b_n \equiv 0 \pmod{p}.$$

Thus, for the same reasons as above we know $b_n \equiv -x(F'(\alpha_n))^{-1} \pmod{p^n}$ and also that we may choose a specific one in the same manner.

Hence, we can construct the whole sequence, and it is uniquely determined at each step. This proves the theorem. □

Acknowledgments. First, I would like to thank Peter May for his work in putting together this opportunity for undergraduates; it has been an enlightening experience that has taught eager students how true mathematics works. In addition, the success of this program demands thanks for the support of the VIGRE grant, the NSF, and the generous instructors from the Department of Mathematics. Finally, thank you to Daphne Kao and Max Engelstein for their indispensable help with this paper. Daphne, you motivated me from the beginning and provided the support and guidance necessary to do so much math for 5-plus weeks. Max, your attention to detail in editing my drafts and high expectations paid dividends for my paper and gave me an appreciation for how *real* mathematicians think.

References

[Go] Fernando Q. Gouvêa, p-adic Numbers: An Introduction, 2nd ed. *Springer.* (1997).

[DF] David S. Dummit and Richard M. Foote, Abstract Algebra, 3rd ed. *John Wiley and Sons, Inc.* (2004).

[Fr] John B. Fraleigh, A First Course in Abstract Algebra, 7th ed. *Addison Wesley.* (2002).

[Sa] Paul J. Sally, Tools of the Trade. *American Mathematical Society.* (2008).