THE P-ADIC NUMBERS AND FINITE FIELD EXTENSIONS OF $\mathbf{Q_p}$

EVAN TURNER

Abstract. This paper will focus on the p-adic numbers and their properties. First, we will examine the p-adic norm and look at some of the more interesting properties that result from it being non-Archimedean. We will then try to understand the structure of the p-adic numbers and look at Hensel's Lemma. Finally, we will extend the norm to finite extensions of $\mathbf{Q_p}$ and try to understand some of the structure behind totally ramified extensions.

Contents

1. Introduction 1
2. The P-Adic Norm 2
3. The P-Adic Numbers 3
4. Extension Fields of $\mathbf{Q_p}$ 6
Acknowledgments 10
References 10

1. Introduction

The construction of the real numbers from the rationals relies very much on the usual absolute value. Furthermore, until one has constructed the p-adic numbers, it is not clear how important a role this norm plays in determining the properties of the real numbers. The p-adic norm behaves much differently than our usual concept of distance. For fixed prime p, two numbers are close together if their difference is divisible by a high power of p. The p-adic norm is also non-Archimedean, and many unusual properties result from this fact.

The completion of $\mathbf{Q}$ under the p-adic norm yields an interesting field $\mathbf{Q_p}$. We can think of elements in this field simply as infinite sequences of the form

$$a = \frac{b_{-m}}{p^m} + \frac{b_{-m-1}}{p^{m-1}} + ... + b_0 + b_1 p + ... + b_n p^n + ...$$

where $0 \leq b_i \leq p-1$. It's clear $\mathbf{Q}$ and $\mathbf{Z}$ lie in $\mathbf{Q_p}$, and elements of both $\mathbf{Q}$ and $\mathbf{Z}$, when expanded p-adically, take on a particular form in $\mathbf{Q_p}$. We will explore the p-adic numbers and will be aided in this endeavor by Hensel's Lemma, which simplifies the task of finding roots to polynomials in $\mathbf{Z_p}[x]$.

Our final task will be to examine extension fields of $\mathbf{Q_p}$. We will first have to extend the p-adic norm to these fields. It turns out there is a unique way to do this, and, for $\alpha \in K$, where K is a finite extension, the extended p-adic norm will

Date: August 26, 2011.

only depend on the constant term in the monic irreducible polynomial of α over $\mathbf{Q_p}$. With these tools, it will not be difficult to characterize how one constructs totally ramified extension fields K of $\mathbf{Q_p}$

I will assume fairly basic knowledge of field theory in this paper. For questions on that, any introductory algebra text will do. See, for instance, *A First Course in Abstract Algebra* by John Fraleigh.

2. The P-Adic Norm

Definition 2.1. For a prime number p and integer a, $\text{ord}_p\ a$ (the order of p at a) is the highest power of p that divides a, i.e. the greatest integer m such that $a \equiv 0 \mod p^m$.

So $\text{ord}_5\ 25 = 2$, while $\text{ord}_5\ 35 = 1$ and $\text{ord}_3\ 25 = 0$. It is a simple exercise to see that $\text{ord}_p\,(a_1a_2) = \text{ord}_p\ a_1 + \text{ord}_p\ a_2$. Another useful fact is that $\text{ord}_p\,(ad+bc) \geq \min\left(\text{ord}_p\,(ad), \text{ord}_p\,(bc)\right)$ simply because if the minimum order is r, then $p^r | ad$ and bc as well as their sum. For x rational, i.e. for $x = \dfrac{a}{b}$, it makes sense to define $\text{ord}_p\ x = \text{ord}_p\ a - \text{ord}_p\ b$. Now we introduce the p-adic norm on $\mathbf{Q}$, which has many different properties from the usual absolute value.

$$|x|_p = \begin{cases} \dfrac{1}{p^{\text{ord}_p\ x}}, & x \neq 0 \\ 0, & x = 0 \end{cases}$$

It is relatively straightforward to prove that the p-adic norm is in fact a norm. However, while every norm must satisfy the triangle inequality, the p-adic norm satisfies an even stronger property that leads to some interesting results.

Definition 2.2. A norm $||\ ||$ is *non-Archimedean* if $||x+y|| \leq \max\left(||x||, ||y||\right)$.

Theorem 2.3. *$|x|_p$ is a non-Archimedean norm.*

Proof. If $x = 0$, $y = 0$, or $x + y = 0$, then it's obvious.
For $x = \dfrac{a}{b}$ and $y = \dfrac{c}{d}$, $x + y = \dfrac{ad+bc}{bd}$ and

$$\begin{aligned} \text{ord}_p\,(x+y) &= \text{ord}_p\,(ad+bc) - \text{ord}_p\ b - \text{ord}_p\ d \\ &\geq \min\left(\text{ord}_p\,(ad), \text{ord}_p\,(bc)\right) - \text{ord}_p\ b - \text{ord}_p\ d \\ &= \min\left(\text{ord}_p\ a + \text{ord}_p\ d, \text{ord}_p\ b + \text{ord}_p\ c\right) - \text{ord}_p\ b - \text{ord}_p\ d \\ &= \min\left(\text{ord}_p\ a - \text{ord}_p\ b, \text{ord}_p\ c - \text{ord}_p\ d\right) \\ &= \min\left(\text{ord}_p\ x, \text{ord}_p\ y\right) \end{aligned}$$

So

$$\begin{aligned} |x+y|_p &= \frac{1}{p^{\text{ord}_p\,(x+y)}} \\ &\leq \frac{1}{p^{\min(\text{ord}_p\ x, \text{ord}_p\ y)}} \\ &= \max\left(|x|_p, |y|_p\right) \end{aligned}$$

□

One peculiar result of this fact is that, under a non-Archimedean norm $||\ ||$, every triangle must be isosceles. If we suppose $||x|| < ||y||$, then

$$\begin{aligned} ||x-y|| &\leq \max(||x||, ||y||) \\ &= ||y|| \end{aligned}$$

But

$$\begin{aligned} ||y|| &= ||x-(x-y)\,|| \\ &\leq \max(||x||, ||x-y||) \\ &= ||x-y|| \end{aligned}$$

and $||y|| = ||x-y||$.

3. The P-Adic Numbers

Building up the p-adic field $\mathbf{Q_p}$ from the rational numbers is an interesting task and is quite similar to the way one constructs the real numbers from $\mathbf{Q}$. However, as I would like to talk more about properties of the p-adic numbers, I will skip over this. For more information, see [1]. It turns out, though, that each p-adic number can be thought of as an infinite sequence of the form

$$a = \frac{b_{-m}}{p^m} + \frac{b_{-m-1}}{p^{m-1}} + ... + b_0 + b_1 p + ... + b_n p^n + ...$$

where $0 \leq b_i \leq p-1$. Furthermore, this construction is unique.

Theorem 3.1. *A series converges in $\mathbf{Q_p}$ if and only if its terms approach zero.*

Proof. Note that $\mathbf{Q_p}$ is complete. I will not prove this fact but it is a straightforward result of the construction of the p-adic field. Suppose $\{a_i\}$ is a sequence in $\mathbf{Q_p}$ such that $|a_i|_p \to 0$ as $i \to \infty$. Then its partial sums $S_n = a_0 + ... + a_n$ are Cauchy since for $n > m$

$$\begin{aligned} |S_n - S_m|_p &= |a_{m+1} + ... + a_n|_p \\ &\leq \max(|a_{m+1}|_p, ..., |a_n|_p) \\ &\to 0 \qquad \text{as } n, m \to \infty \text{ by assumption.} \end{aligned}$$

$\mathbf{Q_p}$ is complete so this implies convergence.

Now suppose then that we have a series that converges in $\mathbf{Q_p}$. Then it is Cauchy as well, and given $\epsilon > 0$, there exists N such that for $n, m > N$, $|S_n - S_m|_p < \epsilon$, where S_n denotes the nth partial sum. In particular, $|S_{n+1} - S_n|_p = |a_{n+1}|_p < \epsilon$. Thus, the terms approach zero as $n \to \infty$.

□

We define the p-adic integers to be the subring

$$\mathbf{Z_p} = \{x \in \mathbf{Q_p} |\, |x|_p \leq 1\}$$

If $a \in \mathbf{Z_p}$, then clearly

$$a = a_0 + a_1 p + a_2 p^2 + ...$$

since $ord_p\, a \geq 0$. Note that in this paper, I will use the word integer to mean elements of $\mathbf{Z}$, while elements of $\mathbf{Z_p}$ will always be specified as p-adic integers. Similarly, we define the set of p-adic units

$$\begin{aligned}\mathbf{Z_p^*} &= \{a \in \mathbf{Z_p} | 1/a \in \mathbf{Z_p}\} \\ &= \{a \in \mathbf{Z_p} |\, |a|_p = 1\}\end{aligned}$$

The equivalence of these two sets is easy to see since if $|a|_p = 1$, then $|1/a|_p = 1$ so $1/a \in \mathbf{Z_p^*}$. We now turn to a very important and useful result that will greatly simplify the task of finding roots in $\mathbf{Z_p}$ for polynomials in $\mathbf{Z_p}[x]$.

Theorem 3.2. *(Hensel's Lemma) Let $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$ be a polynomial in $\mathbf{Z_p}[x]$ with formal derivative $f'(x) = nx^{n-1} + ... + a_1$. Let c_0 be a p-adic integer such that $f(c_0) \equiv 0 \mod p$ and $f'(c_0) \not\equiv 0 \mod p$. Then there exists a unique p-adic integer c such that $f(c) = 0$ and $c_0 \equiv c \mod p$*

Proof. The idea behind the proof is to construct a p-adic number c such that $f(c) \equiv 0 \mod p^n$ for all n, which then clearly implies $f(c) = 0$. We will do this by first constructing a unique sequence of integers $\{b_i\}$ in $\mathbf{Z}$ such that the following conditions hold for all $n \geq 1$:
1) $f(b_n) \equiv 0 \mod p^{n+1}$
2) $b_n \equiv b_{n-1} \mod p^n$
3) $0 \leq b_n < p^{n+1}$

We will prove this by induction on n. We begin with the case $n = 1$. There is clearly a unique integer, b_0, s.t. $b_0 \equiv c_0 \mod p$ and $0 \leq b_0 < p$. By 2) and 3), we need $b_1 \equiv b_0 \mod p$ and $0 \leq b_1 < p^2$; thus, $b_1 = b_0 + c_1 p$ for some $0 \leq c_1 < p$. Now we must check 1).

$$\begin{aligned}f(b_1) = f(b_0 + c_1 p) &= \sum_{i=0}^{n} a_i (b_0 + c_1 p)^i \\ &= \sum_{i=0}^{n} (a_i b_0^i + i a_i b_0^{i-1} c_1 p + \text{terms divisible by } p^2) \\ &\equiv \sum_{i=0}^{n} (a_i b_0^i + i a_i b_0^{i-1} c_1 p) \mod p^2 \\ &= f(b_0) + f'(b_0) c_1 p\end{aligned}$$

We chose $b_0 \equiv c_0 \mod p$, and since $f(x)$ is a polynomial it follows that $f(b_0) \equiv f(c_0) \equiv 0 \mod p$. Thus, $f(b_0) \equiv \beta p \mod p^2$ for some $0 \leq \beta < p$. Similarly, since $f'(b_0) \equiv f'(c_0) \not\equiv 0 \mod p$, we can uniquely solve for c_1 in the equation $\beta p + f'(b_0) c_1 p \equiv 0 \mod p^2$ so that $0 \leq c_1 < p$. This is equivalent to solving $\beta + f'(b_0) c_1 \equiv 0 \mod p$. c_1 is then the unique integer between 0 and $p-1$ such that $c_1 \equiv \dfrac{-\beta}{f'(b_0)} \mod p$, and, for this choice of c_1, $b_1 = b_0 + c_1 p$ satisfies properties 1), 2), and 3).
Now we continue the induction step and assume that we have found $b_1, ..., b_{n-1}$ which satisfy 1), 2), and 3). We need $b_n \equiv b_{n-1} \mod p^n$ and $0 \leq b_n < p^{n+1}$, so $b_n = b_{n-1} + c_n p^n$ for some c_n satisfying $0 \leq c_n < p$. We will now solve for c_n so

that 1) is satisfied as well.

$$\begin{aligned} f(b_n) = f(b_{n-1} + c_n p^n) &= \sum_{i=0}^{n} a_i (b_{n-1} + c_n p^n)^i \\ &= \sum_{i=0}^{n} (a_i b_{n-1}^i + i a_i b_{n-1}^{i-1} c_n p^n + \text{terms divisible by } p^{n+1}) \\ &\equiv \sum_{i=0}^{n} (a_i b_{n-1}^i + i a_i b_{n-1}^{i-1} c_n p^n) \mod p^{n+1} \\ &= f(b_{n-1}) + f'(b_{n-1}) c_n p^n \end{aligned}$$

We know that $f(b_{n-1}) \equiv 0 \mod p^n$ by the inductive assumption, so we can write $f(b_{n-1}) \equiv \alpha p^n \mod p^{n+1}$. Our equation then becomes

$$\alpha p^n + f'(b_{n-1}) c_n p^n \equiv 0 \mod p^{n+1} \quad \text{or} \quad \alpha + f'(b_{n-1}) c_n \equiv 0 \mod p$$

We constructed b_{n-1} so that $b_{n-1} \equiv b_0 \equiv c_0 \mod p$ so, as we argued before, $f'(b_{n-1}) \equiv f'(c_0) \not\equiv 0 \mod p$. As before then, we can solve for c_n uniquely so that $0 \leq c_n < p$. With this c_n, b_n satisfies 1), 2), and 3), and our claim is proved. Now we let

$$c = b_0 + c_1 p + c_2 p^2 + ...$$

Note that $c \equiv b_n \mod p^{n+1}$ so that

$$f(c) \equiv f(b_n) \equiv 0 \mod p^{n+1} \text{ for all } n \geq 1$$

which implies that $f(c) = 0$. The uniqueness of c follows from the uniqueness of the $\{b_i\}$. □

Hensel's Lemma has many useful applications, one of which is the existence of square roots. Suppose $a \in \mathbf{Z_p}$, then a has a square root in $\mathbf{Q_p}$ if and only if there exists $b \in \mathbf{Z_p}$ such that $f(b) = b^2 - a \equiv 0 \mod p$. So if

$$a = a_0 + a_1 p + a_2 p^2 + ... \text{ and } b = b_0 + b_1 p + b_2 p^2 + ...$$

then $b^2 \equiv a \mod p$ iff. $b_0^2 \equiv a_0 \mod p$. Thus, we really just need to check if there exists an integer b_0 with $0 \leq b_0 < p$ such $b_0^2 \equiv a_0 \mod p$. This makes the problem much simpler. The other $\{b_i\}$ can all be solved for once b_0 is found, and the process is similar to that used in the proof of the lemma.

Example 3.3. Let's examine 9 in $\mathbf{Z_5}$. $9 = 4 + 1 * 5$ and $2^2 \equiv 4 \mod 5$ so we can immediately see that 9 has a square root in $\mathbf{Q_5}$. $7 = 2 + 1 * 5$ does not however, since $2 \not\equiv a^2 \mod 5$ for $a \in \{0, 1, 2, 3, 4\}$.

It is also an interesting exercise to examine the p-adic expansion of rational x.

Proposition 3.4. *The p-adic expansion of $a \in \mathbf{Q_p}$ has repeating digits if and only if $a \in \mathbf{Q}$*

Proof. Suppose $a \in \mathbf{Q_p}$ has repeating digits, i.e.,

$$a = \frac{a_{-m}}{p^m} + ... + a_0 + ... \left(a_i p^i + a_{i+1} p^{i+1} + ... + a_{i+r-1} p^{i+r-1}\right) \left(1 + p^r + p^{2r} + ...\right)$$

First we need to show that $\left(1+p^r+p^{2r}+...\right)$ converges to $\dfrac{1}{1-p^r}$ under the p-adic norm.

$$\begin{aligned}\left|\frac{1}{1-p^r}-\left(1+p^r+p^{2r}+...+p^{nr}\right)\right|_p &= \left|\frac{p^{(n+1)r}}{1-p^r}\right|_p \\ &\leq \frac{1}{p^{n+1}}\end{aligned}$$

which goes to zero as $n \to \infty$.

So we have

$$a=\frac{a_{-m}}{p^m}+...+a_0+...\left(a_ip^i+a_{i+1}p^{i+1}+...+a_{i+r-1}p^{i+r-1}\right)\left(\frac{1}{1-p^r}\right)$$

which can be evaluated under our normal rules for addition and multiplication to get an element of $\mathbf{Q}$.

Now suppose $x \in \mathbf{Q}$. We really just need to show that any rational number $x=\frac{a}{b}$ can be put in some form

$$x=c+\frac{d}{1-p^r}$$

for c, d positive integers and some $r \in \mathbf{Z}$. It is not difficult to see that the p-adic expansion of any positive integer is the same as its base p expansion. Thus, any integer will have a finite p-adic expansion. With that in mind, if we can show that x is of this form, then $x=\frac{a}{b}$ will have a p-adic expansion with repeating digits once we expand c,d, and $\dfrac{1}{1-p^r}$ p-adically.

We can reduce to the situation where p does not divide b since if it does and $b=p^rb_0$, we simply examine a/b_0 and the extra $1/p^r$ term will not change the fact that there are repeating digits. Finally, we let $x=a/b$ be between -1 and 0, since if it's not, we can add a constant term that will not change the fact that there are repeating digits.

We look at $\mathbf{Z}/b\mathbf{Z} \cong \{0,1,2,...,b-1\}$. Clearly for some $m, n \geq 0$, $p^m \equiv p^n(\mod b)$ since there are only b equivalence classes. It is fine to assume $m>n$, then $p^{m-n} \equiv 1(\mod b)$, which implies that there exists c such that $cb=p^{m-n}-1$. Thus, we write

$$x=\frac{a}{b}=\frac{ac}{bc}=\frac{-ac}{1-p^{m-n}}$$

and we have our repeating expansion. □

4. Extension Fields of $\mathbf{Q_p}$

Definition 4.1. Let V be a finite-dimensional vector space over a field F. A field norm on V is a map $||\,||_v$ satisfying 1) $||x||_v=0$ if and only if $x=0$, 2) $||ax||_v=||a||*||x||_v$ for $a \in F$, $x \in V$, and $||\,||$ the norm on F, and 3) $||x+y||_v \leq ||x||_v+||y||_v$.

If K is a finite extension field of F, K is an n-dimensional vector space over F. Thus, the concept of a field norm applies here. Before we can discuss extensions fields though, we must first extend the p-adic norm to these fields. First, however, we will define a different kind of "norm."

Definition 4.2. Let $K = F(\alpha)$ be a finite extension of a field F and suppose α has monic irreducible polynomial $f(x) = x^n + ... + a_0$ for $a_i \in F$. The *norm of* α *from* K *to* F

$$\mathbf{N}_{K/F}(\alpha) = \det(A_\alpha)$$

where A_α is the corresponding matrix for the F-linear map $\sigma : K \to K$ given by $\sigma(x) = \alpha x$.

Notation 4.3. The monic irreducible polynomial for α over $\mathbf{Q_p}$ will be denoted irred(α), if the polynomial exists.

Proposition 4.4. *The definition given above for* $\mathbf{N}_{K/F}(\alpha)$ *is equivalent to the following:*
1) $\mathbf{N}_{K/F}(\alpha) = (-1)^n a_0$*, where* n *is the degree of irred(*α*) and* a_0 *is its constant term.*
2) $\mathbf{N}_{K/F}(\alpha) = \prod_{i=1}^{n} \alpha_i$*, where the* α_i *are the conjugates of* $\alpha = \alpha_1$ *over* F*.*

Proof. We choose a convenient basis for K, an n-dimensional vector space over F, namely the set {1, α, ... , α^{n-1}}. With this basis, the matrix A_α has the following form, which shows that $\det(A_\alpha) = (-1)^n a_0$

$$\begin{pmatrix} 0 & 0 & 0 & ... & 0 & -a_0 \\ 1 & 0 & 0 & ... & 0 & -a_1 \\ 0 & 1 & 0 & ... & 0 & -a_2 \\ . & . & 1 & ... & . & . \\ . & . & . & ... & . & . \\ . & . & . & ... & 1 & -a_{n-1} \end{pmatrix}$$

Once factored,

$$\text{irred}(\alpha) = x^n + a_{n-1}x^{n-1} ... + a_0 = \prod_{i=1}^{n}(x - \alpha_i)$$

Thus, it is clear that

$$\prod_{i=1}^{n} \alpha_i = (-1)^n a_0$$

□

One can prove that there can only be one extension of the p-adic norm to any finite extension field K of $\mathbf{Q_p}$. For the interested reader, see [1]. I will motivate the extension, but I will not prove that the extended norm is a field norm nor that it is the unique extension.

Remarks 4.5. Note that Proposition 4.4 implies $\mathbf{N}_{K/F}(\alpha) \in \mathbf{Q_p}$. We can also see that $\mathbf{N}_{K/F}(\alpha)\mathbf{N}_{K/F}(\beta) = \mathbf{N}_{K/F}(\alpha\beta)$ simply because the determinant map satisfies this multiplicative property.

Construction 4.6. Suppose irred(α)= $x^n + a_{n-1}x^{n-1} + ... + a_0$. Let K be the finite extension field of $\mathbf{Q_p}$ containing α and all its conjugates. Then K is a Galois extension. Let σ be an automorphism of K fixing $\mathbf{Q_p}$ sending α to a conjugate α_i. If $||\,||$ is the unique field norm extending $|\,|_p$ to K, then let $||\,||' : K \to \mathbf{R}$ be given by $||x||' = ||\sigma(x)||$. It is not difficult to show that $||\,||'$ satisfies a field norm as well.

But this means $||\alpha|| = ||\alpha||' = ||\sigma(\alpha)|| = ||\alpha_i||$, so conjugates have the same norm. By Remarks 4.5 and Proposition 4.4,

$$\begin{aligned} |\mathbf{N}_{\mathbf{Q_p}(\alpha)/\mathbf{Q_p}}(\alpha)|_p &= ||\mathbf{N}_{\mathbf{Q_p}(\alpha)/\mathbf{Q_p}}(\alpha)|| \\ &= ||\prod_{i=1}^{n} \alpha_i|| \\ &= \prod_{i=1}^{n} ||\alpha_i|| \\ &= ||\alpha||^n \end{aligned}$$

So we see that $||\alpha|| = |\mathbf{N}_{\mathbf{Q_p}(\alpha)/\mathbf{Q_p}}(\alpha)|_p^{1/n}$.

If K is a finite extension of $\mathbf{Q_p}$ containing α, then $||\alpha|| = |\mathbf{N}_{K/\mathbf{Q_p}}(\alpha)|^{1/[K:\mathbf{Q_p}]}$. This follows from the fact that we can form a basis for K over $\mathbf{Q_p}$ from the product of $\{1, \alpha, ..., \alpha^{n-1}\}$ and $\{x_1, x_2, ..., x_m\}$ where $\{\alpha^i\}$ form a basis for $\mathbf{Q_p}(\alpha)$ over $\mathbf{Q_p}$, $\{x_j\}$ form a basis for K over $\mathbf{Q_p}(\alpha)$, and $m = [K : \mathbf{Q_p}(\alpha)]$. The linear map given by multiplication by α then yields a matrix with m blocks along the diagonal given by the matrix A_α given in Proposition 4.4. The determinant of this block matrix is then $\det(A_\alpha)^m$. Thus,

$$\mathbf{N}_{K/\mathbf{Q_p}(\alpha)} = \left(\mathbf{N}_{\mathbf{Q_p}(\alpha)/\mathbf{Q_p}}\right)^{[K:\mathbf{Q_p}(\alpha)]}$$

So

$$\begin{aligned} \left(\mathbf{N}_{K/\mathbf{Q_p}(\alpha)}\right)^{1/[K:\mathbf{Q_p}]} &= \left(\mathbf{N}_{\mathbf{Q_p}(\alpha)/\mathbf{Q_p}}\right)^{\frac{[K:\mathbf{Q_p}(\alpha)]}{[K:\mathbf{Q_p}]}} \\ &= \left(\mathbf{N}_{\mathbf{Q_p}(\alpha)/\mathbf{Q_p}}\right)^{1/[\mathbf{Q_p}(\alpha):\mathbf{Q_p}]} \\ &= \left(\mathbf{N}_{\mathbf{Q_p}(\alpha)/\mathbf{Q_p}}\right)^{1/n} \end{aligned}$$

Note that the extension of the p-adic norm will still be non-Archimedean.

Notation 4.7. From now on, we will denote the extension of the p-adic norm by $|\,|_p$ too.

Definition 4.8. Let K be a finite extension of $\mathbf{Q_p}$, and let A be the set of all $\alpha \in K$ such that α is a root of a polynomial in $\mathbf{Z_p}[x]$, i.e.,

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + ... + a_0 = 0, \quad a_i \in \mathbf{Z_p}$$

Then A is called the *integral closure of* $\mathbf{Z_p}$ *in* K.

Theorem 4.9. *Let K be a finite extension of $\mathbf{Q_p}$ of degree n, and let*

$$\begin{aligned} A &= \{x \in K |\ |x|_p \leq 1\} \\ M &= \{x \in K |\ |x|_p < 1\} \end{aligned}$$

Then A is a ring, the integral closure of $\mathbf{Z_p}$ in K. M is its unique maximal ideal, and A/M is a finite extension of $\mathbf{F_p}$ of degree at most n.

Proof. A inherits the structure of K so we just need to check that it's closed under addition and multiplication. Clearly if $x, y \in A$, then $|xy|_p \leq 1$, so $xy \in A$. Also,$|x + y|_p \leq \max(|x|_p, |y|p) \leq 1$, so $x + y \in A$, and A is a ring. For $a \in A$ and $m \in M$, $|am|_p = |a|_p|m|_p < 1$, so $am \in M$. M is an additive subgroup of A, so M is an ideal.

Now we want to show that A is the integral closure of $\mathbf{Z_p}$ in K. Suppose $\alpha \in A$, then $|\alpha|_p \leq 1$. Since $\alpha \in K$, α is algebraic over $\mathbf{Q_p}$ with

$$\text{irred}(\alpha) = x^m + a_{m-1}x^{m-1} + ... + a_0 = \prod_{i=1}^{m}(x - \alpha_i)$$

where the α_i are conjugates of α. We know that all conjugates of α have the same norm, i.e. $|\alpha_i| \leq 1$ and $\alpha_i \in A$. But the coefficients a_i of irred(α) are sums and products of the α_i, which implies that $|a_i|_p \leq 1$ as well. Since the $a_i \in \mathbf{Q_p}$ already, the a_i are actually in $\mathbf{Z_p}$ and we see that irred(α) $\in \mathbf{Z_p}[x]$.

If $\alpha \in K$ is the root of a polynomial in $\mathbf{Z_p}[x]$, it's pretty clear that irred(α)$\in \mathbf{Z_p}[x]$ too. Let the degree of irred(α) be m so that $\alpha^m + a_{m-1}\alpha^{m-1} + ... + a_0 = 0$. Suppose $|\alpha|_p > 1$. Then

$$\begin{aligned} |\alpha^m|_p = |\alpha|_p^m &= |-a_{m-1}\alpha^{m-1} - ... - a_0|_p \\ &\leq \max(|a_{m-1}\alpha^{m-1}|_p, ..., |a_0|_p) \\ &\leq \max(|\alpha^{m-1}|_p, ..., 1) \ \text{ since } |a_i|_p \leq 1 \\ &= |\alpha^{m-1}|_p \end{aligned}$$

but this is a contradiction since $|\alpha|_p > 1$. Thus, $|\alpha|_p \leq 1$, and $\alpha \in A$. The set A defined in the theorem is then the integral closure of $\mathbf{Z_p}$ in K.

Let's now turn to M being a maximal ideal. Suppose N is an ideal such that $M < N < A$ (this is a strict inequality). So there exists $\alpha \in A$ such that $\alpha \in N$ but $\alpha \notin M$. This implies $|\alpha|_p = 1$ so that $|1/\alpha|_p = 1$ and $1/\alpha \in A$. But then $\frac{1}{\alpha} * \alpha = 1 \in N$, which is a contradiction since $N \neq A$. So M is maximal in A.
Since M is maximal and A is a ring, we know that A/M is a field. It's not difficult to see that $M \cap \mathbf{Z_p} = p\mathbf{Z_p}$. Clearly if $a \in \mathbf{Z_p}$, then $a \in A$ since $|a|_p \leq 1$. If $a, b \in \mathbf{Z_p}$, then $a + M$ and $b + M$ represent the same coset iff. $a - b \in M \cap \mathbf{Z_p} = p\mathbf{Z_p}$. But this means that for $a + p\mathbf{Z_p} \in \mathbf{Z_p}/p\mathbf{Z_p}$, there exists a corresponding $a + M \in A/M$. Or equivalently, that $\mathbf{F_p} = \mathbf{Z_p}/p\mathbf{Z_p}$ lies in A/M. Thus, A/M is an extension field of $\mathbf{F_p}$.

To show that $[A/M : \mathbf{F_p}] \leq n$, we show that any linear combination of $n + 1$ elements over $\mathbf{F_p}$ is linearly dependent. So we take

$$a_1 + M, a_2 + M, ..., a_{n+1} + M \in A/M \text{ for } a_i \in A$$

The a_i are clearly linearly dependent over $\mathbf{Q_p}$ since each $a_i \in K$. Thus,

$$b_1a_1 + ... + b_{n+1}a_{n+1} = 0 \text{ for } b_i \in \mathbf{Q_p} \tag{4.10}$$

If we let $m = \min(ord_p b_1, ..., ord_p b_{n+1})$, then we can multiply 4.10 by p^{-m} and obtain a similar equation with all coefficients in $\mathbf{Z_p}$ and at least one is not in p$\mathbf{Z_p}$ (Just to make sure notation is clear, note that if $m < 0$, then we'll be multiplying by $p^{|m|}$). Thus, if we map 4.10 into A/M, we get an equation of the form

$$b_1a_1 + ... + b_{n+1}a_{n+1} + M = 0 + M \text{ for } b_i \in \mathbf{F_p} \tag{4.11}$$

Any $b_i \in p\mathbf{Z_p}$ is mapped to $0 + M$ in A/M, but we know this isn't the case for all the b_i. This shows that the $\{a_i\}$ are linearly dependent and the claim is proved. □

Definition 4.12. The field A/M described in the preceding theorem is called the *residue field* of K.

We can extend the p-adic norm even further, to the algebraic closure of $\mathbf{Q_p}$, denoted $\bar{\mathbf{Q}}_p$. For $\alpha \in \bar{\mathbf{Q}}_p$, the norm itself depends only on the constant term in irred(α), so this is fine intuitively.

Let K be an extension of $\mathbf{Q_p}$ of degree n, and let $\alpha \in K$. Then we define

$$ord_p\alpha = -\log_p |\alpha|_p = -\log_p |\mathbf{N}_{K/\mathbf{Q_p}}(\alpha)|_p^{1/n} = -\frac{1}{n}\log_p |\mathbf{N}_{K/\mathbf{Q_p}}(\alpha)|_p$$

For $\alpha \in \mathbf{Q_p}$, this agrees with the earlier definition, and has the same multiplicative property. The image of K under the ord_p map is contained in

$$(1/n)\,\mathbf{Z} = \{x \in \mathbf{Q} |\, nx \in \mathbf{Z}\}$$

The image is an additive subgroup of $(1/n)\,\mathbf{Z}$ so it's of the form $1/e$ for some integer e dividing n.

Definition 4.13. This integer e is called the *index of ramification* of K over $\mathbf{Q_p}$. If $e = 1$, K is called an *unramified extension* of $\mathbf{Q_p}$, while if $e = n$, the extension K is called *totally ramified*.

Theorem 4.14. *If K is totally ramified and $\alpha \in K$ is such that $ord_p\alpha = 1/e$, then α satisfies an Eisenstein equation*

$$x^e + a_{e-1}x^{e-1} + ... + a_0 = 0, \text{ for } a_i \in \mathbf{Z_p}$$

where $a_i \equiv 0(\mod p)$ for all i, but $a_0 \not\equiv 0(\mod p^2)$. Conversely, if α is a root of an Eisenstein polynomial of degree e over $\mathbf{Q_p}$, then $\mathbf{Q_p}(\alpha)$ is totally ramified over $\mathbf{Q_p}$ of degree e.

Proof. If $ord_p\alpha = 1/e$, then irred(α) over $\mathbf{Q_p}$ has degree e based on the definition of $ord_p\alpha$. Thus, we need to show that the coefficients a_i are in $\mathbf{Z_p}$. In $\bar{\mathbf{Q}}_p[x]$,

$$\text{irred}(\alpha) = \prod_{i=1}^{e}(x - \alpha_i)$$

where α_i are conjugates of α. Thus, we see that the a_i are symmetric in α_i, which implies $|a_i|_p \leq 1$. Also, $|a_0|_p = |\alpha|_p^e = 1/p$ so we see that $a_0 \not\equiv 0(\mod p^2)$.

Now suppose α is a root of an Eisenstein polynomial. It is well-known that an Eisenstein polynomial is irreducible over $\mathbf{Q}$, and the same applies in $\mathbf{Q_p}$, although I will not prove it. Thus, irred(α) has degree e and $[\mathbf{Q_p}(\alpha) : \mathbf{Q_p}] = e$. $ord_p a_0 = 1$ by assumption, so

$$ord_p\alpha = -\log_p |\alpha|_p = -\frac{1}{e}\log_p |a_0|_p = 1/e$$

so $\mathbf{Q_p}(\alpha)$ is totally ramified over $\mathbf{Q_p}$. □

Acknowledgments. I want to thank my mentors, Shawn Drenning and Casey Rodriguez, for their time in helping me with this paper. They were great to work with and excellent resources. I also want to thank the REU program in general for giving me the opportunity to work on math this summer and to study a topic that I may not have been able to experience otherwise.

References

[1] Neal Koblitz p-adic numbers, p-adic analysis, and Zeta-Functions, 2nd ed. Springer-Verlag. 1984.