$\mathbb{Q}_p$ and its Extensions
Math 129 Final Project

William Fithian

18 May 2005

1 Introduction

This paper is intended as an introduction to the field $\mathbb{Q}_p$ of p-adic numbers, and some of the ways in which it relates to the theory we have been building up over the course of the semester. We will leave a few small facts unproven, in the interest of being able to attack larger things without getting bogged down in all the gory details of norms and topology. The content of the paper is divided into three sections, the first of which will introduce the reader to the p-adic numbers and motivate their further study, and the next two of which are intended give the reader some perspective on how some the topics we studied this semester about Number Fields relate to the p-adics, and what similar theory we can build up around $\mathbb{Q}_p$.

Much of this paper, and in particular the construction of $\mathbb{Q}_p$, Hensel's Lemma, and the sections on extensions of norms and the generalized ring of integers, follows more or less loosely the presentation in Koblitz [3]. The section on viewing $\mathbb{Z}_p$ as a tree is from Holly [1]. Some of the random little facts such as $e^p \in \mathbb{Q}_p$ and the generalization of $|\cdot|_p$ in Section 3.4 came from [5].

2 The p-adic Numbers

There are various ways to construct the p-adic numbers. One very intuitive one involves defining $\mathbb{Z}_p$ to be the projective limit of $\mathbb{Z}/p^n\mathbb{Z}$ for a prime p with n going to infinity, and then taking $\mathbb{Q}_p$ to be the fraction field of that limit, which is an integral domain. We choose to construct them here by defining $\mathbb{Q}_p$ to be the completion of $\mathbb{Q}$ with respect to the p-adic norm (which we will define soon), because the concept of the non-archimedean norm will ultimately prove useful in proving things about the extension fields of $\mathbb{Q}_p$. Still, it is useful to know the alternate definitions of $\mathbb{Z}_p$ and $\mathbb{Q}_p$, which is closely related to the p-ary representation of $\mathbb{Q}_p$ that we will discuss below.

2.1 Non-Archimedean Norms

In the same way that the real numbers are typically constructed as the completion of the rationals with respect to the usual, intuitive Euclidean metric, we will construct $\mathbb{Q}_p$ by taking the completion of $\mathbb{Q}$ with respect to a metric induced by a more exotic norm, which we will denote $|\cdot|_p$, and refer to as the *p-adic norm* on $\mathbb{Q}$. We begin with the definition of a norm on a field.

Definition 2.1.1 (Norm on a Field). A *norm* $|\cdot|$ on the field F is a map from F to $\mathbb{R}_{\geq 0}$ such that for all $x, y \in F$:

1. $|x| = 0$ *iff* $x = 0$.

2. $|x \cdot y| = |x| \cdot |y|$.

3. *(triangle inequality)* $|x + y| \leq |x| + |y|$.

The usual absolute value (which we will denote $|\cdot|_\infty$) is one example of a norm on $\mathbb{Q}$ with which we are all familiar. However, there are other possible norms on $\mathbb{Q}$, for instance the "trivial norm" which sends 0 to 0 and everything else to 1. The trivial norm thus defined is a norm on every field F.

As another example, if we fix some prime p, we can define a norm $|\cdot|_p$ as follows: If $x = \frac{a}{b} \neq 0$ in lowest terms, we can alternately write $x = p^n \frac{a'}{b'}$ for some $n \in \mathbb{Z}$ and with a' and b' relatively prime to p, by dividing out the highest power of p dividing either a or b. Then we just define $|x|_p = p^{-n}$ ($|0|_p = 0$). n here can also be written as $\mathrm{ord}_p(x)$. This is an odd norm, so to give it concreteness we evaluate some examples below:

$$\begin{aligned}
|7|_7 &= \frac{1}{7} \\
\left|\frac{1}{49}\right|_7 &= 49 \\
|5|_7 &= 1 \\
|21|_7 &= \frac{1}{7} \\
\left|\frac{51}{35}\right|_7 &= 7
\end{aligned}$$

So that, in general, a rational number is p-adically "larger" when higher powers of p divide its denominator, and p-adically "smaller" when higher powers divide its numerator. Note in particular that $|n|_p \leq 1$ for all $n \in \mathbb{Z}$.

Proposition 2.1.2. $|\cdot|_p$ *is a norm on* $\mathbb{Q}$.

Proof. It is trivial that $|\cdot|_p$ satisfies conditions 1 and 2 of the definition of a norm, and we can actually prove an even stronger version of the triangle inequality, the equation

$$|x+y|_p \leq \max(|x|_p, |y|_p)$$

The above is trivial when x or y is 0, so assume that both are nonzero and assume that $|x|_p \geq |y|_p$. Then $x = p^n \frac{a}{b}$ and $y = p^m \frac{c}{d}$ with $n \leq m$ and a, b, c, d all relatively prime to p, so that we have

$$\begin{aligned} |x+y|_p &= |p^n \frac{ad + bcp^{m-n}}{bd}|_p \\ &= |p^n| \cdot |\frac{1}{bd}| \cdot |ad + bcp^{m-n}| \\ &\leq p^{-n} \\ &= |x|_p \\ &= \max(|x|_p, |y|_p) \end{aligned}$$

where the inequality step comes from the fact that bd is relatively prime to p and $ad+bcp^{m-n}$ is an integer. □

We have a natural metric $d_p(x, y) = |x - y|_p$ induced by the p-adic norm, which in turn induces a metric topology on $\mathbb{Q}$.

Norms which satisfy the stronger triangle inequality above are called *non-archimedean* norms. Norms that do not are called, unsurprisingly, *archimedean.* There is a nice theorem by Ostrowski, which we will not prove here, classifying all nontrivial norms on $\mathbb{Q}$.

Theorem 2.1.3 (Ostrowski). *Every nontrivial norm on $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for $p = \infty$ or p some prime.*

where two norms $|\cdot|_1$ and $|\cdot|_2$ are defined to be *equivalent* if they induce the same topology, or alternately if there exists $\alpha \in \mathbb{R}$ such that, $\forall x \in \mathbb{Q}$, $|x|_1 = |x|_2^\alpha$.

2.2 $\mathbb{Q}_p$

Now we are ready to define $\mathbb{Q}_p$ to be the set of all equivalence classes of Cauchy sequences of rational numbers $\{a_n\}_{n=1}^\infty$ with the relation

$$\{a_n\} \sim \{b_n\} \Leftrightarrow \{a_n - b_n\} \longrightarrow 0$$

We further define the operations $\{a_n\} \cdot \{b_n\} = \{a_n \cdot b_n\}$, $\{a_n\} + \{b_n\} = \{a_n + b_n\}$, $\frac{1}{\{a_n\}} = \{\frac{1}{a_n}\}$, $-\{a_n\} = \{-a_n\}$, and $|\{a_n\}|_p = \lim_{n\to\infty} |a_n|_p$. It is not difficult to prove the continuity of these operations with respect to the p-adic norm, though we will not do so here. Neither will we prove that $\mathbb{Q}_p$ is complete, though that is also true. It follows easily from these definitions that the extension of $|\cdot|_p$ is a non-archimedean norm on $\mathbb{Q}_p$.

At this point, we may want to ask whether or not $\mathbb{Q}$ was already complete with respect to the p-adic norm. In fact it is not; we can see this by considering the number 6, which has a unique square root n_i modulo every positive power 5^i of 5 (we can show this using Hensel's Lemma, which we introduce later, in Section 2.6). Thus, if the sequence $(n_i)_{i=1}^{\infty}$ converges to $x \in \mathbb{Q}$, we would have $|6 - x^2|_p = \lim_{i\to\infty} |6 - n_i^2|_p$, but $6 - n_i^2 \equiv 0 \pmod{p^i}$, $\forall i$, so this limit is 0 and consequently $x^2 = 6$. In other words, we would have constructed a rational square root of 6. Since this is impossible, it must be that the sequence of n_i has no limit in $\mathbb{Q}$.

Though we can construct $\mathbb{Q}_p$ with the p-adic norm, there are much better ways to think about its elements in practice. It can be shown, for instance, that any Cauchy sequence in $\mathbb{Q}_p$ that does not converge to 0 is equivalent to a unique sequence of the form

$$\left(\sum_{i=k}^{n} a_i \cdot p^i \right)_{n=k}^{\infty}$$

with $0 \leq a_i < p \; \forall i$, $k \in \mathbb{Z}$, and $a_k > 0$. This is the sequence of partial sums of the infinite sum $\sum_{i=k}^{\infty} a_i \cdot p^i$, so we may as well think of x as being "equal" to that infinite sum, and think of $\mathbb{Q}_p$ as the set of infinite sums of that form. Note that these sums converge because the norms of the sums of remaining terms get p-adically smaller and smaller as the powers of p that divide them get higher and higher. We can also use the multiplicative and additive properties of our non-archimedean norm $|\cdot|_p$ to deduce that $|x|_p = p^{-k}$.

Alternately, we can divide out x by p^k and note that any nonzero p-adic number x may be expressed as

$$x = \sum_{i=k}^{\infty} a_i \cdot p^i = p^k \cdot \sum_{i=0}^{\infty} a_{i+k} \cdot p^i = p^k \cdot u$$

where we use the letter u because the p-adic numbers of the form $u = \sum_{i=0}^{\infty} a_i \cdot p^i$ with $a_0 \neq 0$ are exactly those for which $|u|_p = 1$, which we will see later are the units of the ring of p-adic integers $\mathbb{Z}_p$.

Note that this is equivalent to the idea that a real number may be represented by an infinite decimal expansion, which can be understood as an infinite sum of digits times smaller and smaller powers of 10, except that the decimal representation is not unique; for instance, $1.\overline{0} = 0.\overline{9}$. This comparison inspires the idea of a representation of a p-adic as a "p-ary" expansion that is finite on the *right* and goes off to infinity on the *left*. For instance, the 5-ary representation of $17 = 2 + 3 \cdot 5$ would be $\ldots 00032$. We will see more of this representation in the next section.

2.3 Arithmetic in $\mathbb{Q}_p$

We can add, subtract, and multiply in the p-adics with the p-ary representations just like we do in the reals with decimal notation, with the same notions of carrying and borrowing. For instance, in $\mathbb{Q}_5$,

$$\begin{array}{rl} & \ldots 131.23 \\ + & \ldots 442.122 \\ = & \ldots 123.402 \end{array}$$

There are repeating decimals in $\mathbb{Q}_p$ just like in $\mathbb{R}$. For instance, consider $1/3 = 0.333\ldots$ in $\mathbb{R}$. By comparison, the 2-ary representation in $\mathbb{Q}_2$ is $1/3 = \ldots 0101011.0$, which we can compute by solving $3X - 1 \equiv 0$ modulo successively higher and higher powers of 2 (3 has inverse 1 mod 2, 3 mod 4 and mod 8, 11 mod 16 and mod 32, 43 mod 64 and mod 128, and so on).

2.4 $\mathbb{Z}_p$

We now introduce the concept of $\mathbb{Z}_p$, the set of p-adic integers. $\mathbb{Z}_p$ is just the set of p-adic numbers x with $|x|_p \leq 1$ (or equivalently, 0 and those whose p-ary representations terminate to the left of the decimal point). Since $|\cdot|_p$ is multiplicative, the group of units $\mathbb{Z}_p^\times$ are exactly the x for which $|x|_p = 1$ (or equivalently, those whose p-ary representations have their rightmost nonzero digit in the "ones" place). Since we have for all $x \neq 0$ that $x = p^m \cdot u$, we can alternately say that the nonzero p-adic integers are those for which $m \geq 0$ and the units are those for which $m = 0$. That $\mathbb{Z}_p$ is a ring follows from the properties of the non-archimedean norm, and the ideals of $\mathbb{Z}_p$ are the powers of $p\mathbb{Z}_p$, $\mathbb{Z}_p$'s only ideal. We will see generalizations of these concepts later in Section 3.2.

Note that $\mathbb{Z}_p \cap \mathbb{Q}$ is not just $\mathbb{Z}$, though it does contain $\mathbb{Z}$: for instance, $1/2 = \ldots 1112.0$ in $\mathbb{Q}_3$ is not only an integer but a unit (this is not surprising since $2 = \ldots 0002.0$ is also a *unit*). In fact, $\mathbb{Z}_p \cap \mathbb{Q}$ consists of all rational numbers whose denominators in lowest terms are not divisible by p, and $\mathbb{Z}_p^\times \cap \mathbb{Q}$ is those whose numerators *and* denomators in lowest terms are *both* not divisible by p.

2.5 Fun with the p-adic Topology

The p-adic topology is an exotic one with some strange consequences, and requires us to forget all of the geometric intuition we have from working with $|\cdot|_\infty$. To illustrate this, we will consider the differences between non-archimedean and archimedean geometry.

First, note that in the proof of Proposition 2.1.2, if n is strictly less than m, we actually have *equality*, i.e.

$$|x + y|_p = \max(|x|_p, |y|_p) \tag{1}$$

because then we have

$$p|bcp^{m-n} \Rightarrow p \not| (ad + bcp^{m-n}) \Rightarrow |ad + bcp^{m-n}|_p = 1$$

This is known as the "isosceles triangle principle," because it implies, with our stronger triangle inequality, that for any three points x, y, and z, the larger two of $d_p(x,y)$, $d_p(y,z)$, and $d_p(x,z)$ must be the same: in other words, every triangle is isosceles!

A further implication of this fact is that if $y, z \in B(x,r)$, the ball of radius r centered at x, then $d_p(y,z) \leq \max(d_p(x,y), d_p(x,z)) < r \Rightarrow z \in B(y,r)$. Thus we see that $z \in B(x,r) \Leftrightarrow z \in B(y,r)$, so that we have

$$\forall y \in B(x,r),\ B(y,r) = B(x,r)$$

in other words, that every point in a ball is the center of that ball!

Another nice corollary of this fact is that if two balls intersect, they are concentric, sharing a center at their point of intersection; therefore one is entirely contained in the other.

These facts seem completely counterintuitive if we make any attempt to analogize $\mathbb{Q}_p$ to $\mathbb{R}$; however, Holly suggests another model which can be of help in this matter. She suggests we think of a p-ary "tree" of infinite depth, with each p-adic number being a "leaf" infinitely far down on the tree, essentially the limit of a path down the tree, where at the n^{th} step, we choose the a_n^{th} child to go to next. Then, the "distance" between two p-adic numbers is inversely proportional to how far down the tree is their lowest common ancestor. To generalize this to $\mathbb{Q}_p$ is more difficult; we must imagine a tree that extends infinitely up *and* down, with some depth 0 in the middle of the tree. This is not as easy to picture, so since we know any finite set of numbers must all be contained in some $p^k\mathbb{Z}_p$, which is topologically the same as $\mathbb{Z}_p$, we will only consider $\mathbb{Z}_p$ for now.

Now, we can easily see that the right way to re-envision a ball in this analogy is to let $B(x,r)$ be the set of all descendants of any sufficiently low ancestor of x, which is the same as saying all descendants of the highest sufficiently low ancestor. In other words, a ball is the set of all common ancestors of any node of the tree with finite depth. It becomes clear with this definition of a ball why all points in a ball are centers of that ball; any descendant of the node defining the ball is clearly a center of that ball. Furthermore, if two balls intersect, the node defining one ball must be a descendant of the node defining the other ball. Thus, the ball of the descendant node is totally contained in the ball of the ancestor node.

The isosceles triangle principle also becomes obvious when we consider that given three points, x, y, and z, either their paths all split at the same depth in the tree (in which case the triangle is equilateral), or (w.l.o.g.) x splits off from the others earlier and the other two split off later, in which case x is equally far from the other two, which are closer to each other than they are to x, and the triangle is isosceles.

This topological analogy of $\mathbb{Z}_p$ is closely related to the fact that $\mathbb{Z}_p$ has the topology of the Cantor Set as a subspace of $\mathbb{R}$.

2.6 Hensel's Lemma: the p-adic Newton's Method

One question which naturally arises with the p-adics is, how can we tell if a given polynomial has a root in the p-adics? In most cases, as we will see, the answer is not actually too difficult to arrive at. Since any polynomial equation with coefficients in the p-adic numbers can become a polynomial equation with coefficients in the p-adic integers by multiplying all the coefficients by a suitable power of p, we will consider the limited case of whether such equations have solutions in $\mathbb{Z}_p$ (we can easily generalize this to ask whether the same polynomial has roots in $p^k\mathbb{Z}_p$, by replacing every X in the polynomial with p^kX and asking whether the resulting polynomial has roots in $\mathbb{Z}_p$).

We can see without too much difficulty that if the reduction of a polynomial has no root in $\mathbb{Z}_p/p\mathbb{Z}_p$, then it has no root in $\mathbb{Z}_p$, but it is not immediately clear that the converse is true. In fact, we can prove the converse if we add an additional hypothesis. The following theorem was proven by Hensel and is very useful.

Theorem 2.6.1 (Hensel's Lemma). *Let $f(X) = \sum_{j=0}^{m} c_jX^j$ be a polynomial with coefficients in $\mathbb{Z}_p$, and let $f'(X) = \sum_{j=0}^{m} jc_jX^{j-1}$ be its derivative. Suppose $f(a_0) \equiv 0$ (mod p) and $f'(a_0) \not\equiv 0$ (mod p). Then a_0 lifts to a unique p-adic integer root of $f(X)$.*

Proof. We will prove this by showing (by induction) that there is a unique sequence of integers $\{a_n\}_{n=0}^{\infty}$ beginning with a_0 (considered now as an integer between 0 and $p-1$) such that for all n,

- $f(\sum_{i=0}^{n} a_ip^i) \equiv 0 \pmod{p_{n+1}}$
- $0 \leq a_n < p$

Note that this claim is equivalent to the theorem since we are essentially finding a unique infinite p-ary expansion $\dots a_3a_2a_1a_0.0$ for a root of $f(X)$ whose reduction modulo p is a_0 (more precisely, the partial sums are a Cauchy sequence in $\mathbb{Q}$ and any other solution must be equivalent as a Cauchy sequence to the sequence of partial sums).

Now, on to proving the claim. We have the claim for $n = 0$ by hypothesis, so we need only consider the inductive step. Suppose we have $a_0, \dots, a_{n-1}$, for some n, which all satisfy the claim. Let $S = f(\sum_{i=0}^{n-1} a_ip^i)$. Then we have, for any a_n which could possibly satisfy the claim, working modulo p^{n+1}

$$\begin{aligned}
f(\sum_{i=0}^{n} a_ip^i) &= f(S + a_np^n) \\
&= \sum_{j=0}^{m} c_j\left(S + a_np^n\right)^j \\
&= \sum_{j=0}^{m} \left(c_jS^j + jc_jS^{j-1}a_np^n + \text{termsdivisibleby}\, p^{n+1}\right) \\
&\equiv \sum_{j=0}^{m} c_jS^j + \left(\sum_{j=0}^{m} jc_jS^{j-1}\right) a_np^n \\
&= f(S) + f'(S)a_np^n \\
&\equiv 0
\end{aligned}$$

Now, we have that $f(S) \equiv 0 \pmod{p^n}$ by our induction hypothesis, so we may divide both sides of the congruence by p^n to obtain the congruence $\frac{-f(S)}{p^n} \equiv f'(S)a_n \pmod{p}$. Since $f'(S) \equiv f'(a_0) \not\equiv 0 \pmod{p}$, this congruence has a unique solution a_n. So the claim is proved and the theorem follows. □

Note that the converse is not true; for instance $f(X) = X^2$ does not satisfy the hypotheses of Theorem 2.6.1, but it certainly has a root, 0, in $\mathbb{Z}_p$ for every p. Roots modulo p which also give nonzero derivative modulo p are called *nonsingular* roots.

Now we can see how to find a root of $f(X) = X^2 - 6$ in $\mathbb{Z}_5$. Just observing that $f(X)$ has nonsingular roots at 1 and 4, modulo 5, is enough to prove that $f(X)$ has exactly two roots in $\mathbb{Z}_5$. Furthermore, we can actually approximate these with arbitrary precision by solving the equation modulo 5^n, or by finding the a_i with the iterative procedure given for Theorem 2.6.1. Let's work this as an example, approximating the root which is congruent to 4 modulo 5. Note that $f'(X) = 2X$. For the first step we have, modulo 25

$$f(4 + 5a_1) \equiv f(4) + f'(4) \cdot 5a_1 \equiv 0(\mod 25)$$

or in other words

$$a_1 \equiv -\frac{f(4)/5}{f'(4)}(\mod 5)$$

Since $f(4) = 10$ and $f'(4) = 8 \equiv 3$, we have $a_1 \equiv 1$. For the next step, $S = 9$, so we have

$$a_2 \equiv -\frac{f(9)/25}{f'(9)}(\mod 5)$$

$f(9) = 75$ and $f'(9) \equiv f'(4) \equiv 3$, so we get $a_3 \equiv 4$. Now, we notice we can just replace $-\frac{1}{f'(S)}$ with 3, since it is always congruent to 3 modulo 5. To continue, we get

$$\begin{aligned} a_3 &\equiv 3f(109)/125 \equiv & 0; S = 109 \\ a_4 &\equiv 3f(109)/625 \equiv & 2; S = 1359 \\ a_5 &\equiv 3f(1359)/3125 \equiv & 3; S = 10734 \end{aligned}$$

and with very little work we have found a solution to $X^2 - 6 = 0(\mod 15625)$, which is a pretty good approximation (within a ball of radius 1/15625) to a known square root of 6 in $\mathbb{Z}_5$! We can actually write, using our 5-ary representation,

$$\sqrt{11.0} = \ldots 32041.0$$

Approximation using Hensel's Lemma is frequently referred to as the "p-adic Newton's Method" because it is very similar in that it iteratively computes $-\frac{f(x_n)}{f'(x_n)}$ to approximate a real root of a polynomial equation. This gives an algorithm for approximating any polynomial within precision ϵ in $O((\log \epsilon)^2)$ time, where one log factor comes from the number of repetitions of the procedure and the other comes from the size of the numbers the computer must do arithmetic on.

3 Extensions of $\mathbb{Q}_p$

Recall that though $\mathbb{R}$ may be complete, it is not algebraically closed. We need to adjoin some complex element to it before we get $\mathbb{C}$, the algebraic closure.

It is also true that $\mathbb{Q}_p$ is not actually algebraically closed; that is $\mathbb{Q}_p \neq \overline{\mathbb{Q}}_p$. To see this fact, consider the polynomial $f(X) = X^2 - n$ for some prime $p > 2$ and $0 < n < p$ not a square in $\mathbb{Z}/p\mathbb{Z}$. That polynomial may only be satisfied by a square root of n, but none may exist because if $x^2 = (p^m \cdot u)^2 = n$ then $m = 0$ and therefore

$$x^2 = u^2 = (a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots)^2 \in a_0^2 + p\mathbb{Z}_p$$

but $n \not\equiv a_0^2$ so $x^2 \neq n$.

Just like we can adjoin roots of irreducible polynomials with coefficients in $\mathbb{Q}$ to get finite extensions of $\mathbb{Q}$, which we call number fields, we can similarly adjoin roots of irreducible polynomials with coefficients in $\mathbb{Q}_p$ to $\mathbb{Q}_p$ to get finite extensions of $\mathbb{Q}_p$. In this section we will examine some of the properties of the fields that result from this process.

3.1 Extending the p-adic Norm

We will say that a norm on an extension $K_p \supset \mathbb{Q}_p$ *extends* $|\cdot|_p$ if its restriction to $\mathbb{Q}_p$ is just $|\cdot|_p$. First, note that $\mathbb{Q}_p$ has characteristic 0, so extensions of it have many of the same useful properties that extensions of $\mathbb{Q}$ have, for instance, all are separable and all are generated by a primitive element. One thing that we will find useful when dealing with an algebraic number field is being able to extend our non-archimedean norm $|\cdot|_p$ to an arbitrary finite extension K_p (and in general to $\overline{\mathbb{Q}}_p$).

We will ultimately prove in this section that there is a unique way to extend $|\cdot|_p$ to any finite extension K_p, which actually gives us a unique extension to $\overline{\mathbb{Q}}_p$. To do this, we will first show that there is no more than one way to extend the norm to any given finite extension, then we will prove a proposition about how the extended norm must be defined if it exists, and culminate with a proof that it *does* exist.

It will be helpful here to introduce the concept of a norm on a vector space.

Definition 3.1.1 (Norm on a Vector Space). *A* norm *Let F be a field with norm $|\cdot|$, and let V be a vector space over F. A* norm *on V is a map $\|\cdot\|$ from V to $\mathbb{R}_{\geq 0}$ such that for all $x \in F$, $u, v \in V$:*

1. $\|v\| = 0$ *iff* $v = 0$.

2. $\|xv\| = |x| \cdot \|v\|$.

3. *(triangle inequality)* $\|u + v\| \leq \|u\| + \|v\|$.

We say that two norms on a vector space V, $\|v\|_1$ and $\|v\|_2$, are *equivalent* if there exist two real numbers $c_1, c_2 > 0$ such that $\forall v \in V$,

$$c_1 \|v\|_1 \leq \|v\|_2 \leq c_2 \|v\|_1$$

Like the definition of equivalence for the field, this definition of equivalence comes from the fact that two norms induce the same topology on V if and only if they are equivalent.

We will first show that all *vector space norms* on V over $\mathbb{Q}_p$ are equivalent, and then that unequal but equivalent vector space norms cannot both be *field norms* on $V = K$ which actually extend F's norm (it follows from the definition of a vector space norm that if V is actually a field, then a field norm which extends the norm on F is also trivially a vector space norm).

We will need to use the fact here that $\mathbb{Q}_p$ is locally compact. This follows from observing that $\mathbb{Z}_p$ is compact, so for all $k \in \mathbb{Z}$, $p^k\mathbb{Z}_p$ is compact, and every point in $\mathbb{Q}_p$ lies in some $p^k\mathbb{Z}_p$. $\mathbb{Z}_p$ is compact because it has the same topology of the Cantor set, which, as a subspace of $\mathbb{R}$, is closed (a complement of a union of open itervals) and bounded.

Theorem 3.1.2. *Let V be a vector space over F, and let F be locally compact and with norm $|\cdot|$. Then all norms on V are equivalent.*

Proof. Fix the basis $\{v_1, \ldots, v_n\}$ for V and consider the "sup-norm", which is defined by

$$\|a_1v_1 + \cdots + a_nv_n\|_{\text{sup}} = \max_i(|a_i|)$$

Now, it is not too hard to check that the sup-norm is a norm, so we need only to show that any other norm $\|\cdot\|$ on V is equivalent to the sup-norm.

To obtain an upper bound for $\|\cdot\|$ in terms of the sup-norm, we choose the constant $C = n\max_i(\|v_i\|)$ and we can observe that

$$\begin{aligned}\|a_1v_1 + \cdots + a_nv_n\| &\leq \|a_1\|\|v_1\| + \cdots + \|a_n\|\|v_n\| \\ &\leq n\max_i(\|v_i\|)\max_i(\|a_i\|) \\ &\leq C\|a_1v_1 + \cdots + a_nv_n\|_{\text{sup}}\end{aligned}$$

To show the lower bound we need the following lemma.

Lemma 3.1.3. *Let $U = \{v \in V : \|v\|_{\text{sup}} = 1\}$. For any norm $\|\cdot\|$ on V, $\|\cdot\|$ is bounded away from 0 on the subset U; that is, there exists a positive number ϵ such that $\epsilon \leq \|u\|$, $\forall v \in U$*

This lemma is not too interesting, but it is proved in Koblitz [3], and it is the step for which we need local compactness of F.

Using the lemma, the rest of the proof follows easily, since we then have, on U, $\epsilon\|v\|_{\text{sup}} \leq \|v\|_{\text{sup}}$. But then we have it for all $v = (a_1, \ldots, a_n) \in V$, since $\frac{v}{\max(a_i)} \in U$ and therefore $\epsilon\left\|\frac{v}{\max(a_i)}\right\|_{\text{sup}} \leq \left\|\frac{v}{\max(a_i)}\right\|$ and multiplying by $|\max(a_i)|_p$ gives the desired result.

So on all of V we have $\epsilon\|v\|_{\text{sup}} \leq \|v\| \leq n\max_i(\|v_i\|)\|v\|_{\text{sup}}$ and the theorem is proved. □

Corollary 3.1.4. *Let K be a finite extension of a locally compact field F, where $|\cdot|_F$ is a norm on F. There is at most one norm on K which extends $|\cdot|_F$.*

Proof. Suppose we had two field norms $\| \cdot \|_1$ and $\| \cdot \|_2$ which are not identical, i.e. $\exists \alpha \in K$ such that $\|\alpha\|_1 < \|\alpha\|_2$. They are equivalent in the vector space sense so there is a positive constant c such that for all $x \in K$, $\|x\|_1 \geq c\|x\|_2$. But after fixing c, we may choose N sufficiently large to get $\|\alpha\|_1^N < c\|\alpha\|_2^N$. This is a contradiction, so the two were not both field norms. □

Now, let $\mathbb{N}_{K/F}(\alpha)$ be the old "norm" from K down to F (note this notion of norm is different from the field norm we seek; the shared nomenclature is just an unhappy coincidence).

Proposition 3.1.5. *If K_p is a finite extension of $\mathbb{Q}_p$, with norm $\|\cdot\|$ that extends $|\cdot|_p$, and $\alpha \in K_p$ is nonzero, then $\|\alpha\| = |\mathbb{N}_{K_p/\mathbb{Q}_p}(\alpha)|_p^{1/[K_p:\mathbb{Q}_p]}$.*

Proof. Consider some element α in some *Galois* extension K_p of $\mathbb{Q}_p$, and suppose we have a correct extension $\|\cdot\|_p$ of $|\cdot|_p$ to K_p. Now let σ be some $\mathbb{Q}_p$-automorphism of K_p, and consider the map $\|\cdot\|_p' = \|\cdot\|_p \circ \sigma$, which is, of course, also a field norm on K_p which also extends $|\cdot|_p$.

Now we get to apply Corollary 3.1.4 to conclude that in fact $\|\cdot\|_p' = \|\cdot\|_p$, allowing us to conclude that all conjugates of α must have the same norm as α. Noting that $\mathbb{N}_{K/\mathbb{Q}_p}(\alpha)$ is an element of $\mathbb{Q}_p$, we have, if α has n conjugates (including itself),

$$\begin{aligned}
|\mathbb{N}_{K/\mathbb{Q}_p}(\alpha)|_p &= \left\|\mathbb{N}_{K/\mathbb{Q}_p}(\alpha)\right\|_p \\
&= \left\| \prod_{\sigma \in Gal(K/\mathbb{Q}_p)} \sigma(\alpha) \right\|_p \\
&= \prod \|\sigma(\alpha)\| \\
&= \|\alpha\|^{[K:\mathbb{Q}_p]}
\end{aligned}$$

Note that $\|\alpha\|_p$ is independent of what extension field we take its norm in, since if L extends K extends F and $\alpha \in K$ we have $\mathbb{N}_{L/F}(\alpha) = \left(\mathbb{N}_{K/F}(\alpha)\right)^{[L:K]}$. This is a good thing, since if a norm on L extends F, the restriction of that norm to K had also better extend F. Thus, we can drop the condition that K is Galois (since for any K we could extend to K's splitting field, which is an extension of K, and prove the fact for the splitting field).

□

Now, we have shown exactly what form the extension of $|\cdot|_p$ must take, but we still do not know for sure whether what we have is even a norm at all.

Theorem 3.1.6. *Let K be a finite extension of $\mathbb{Q}_p$. The function $|\cdot|_p$ given by Proposition 3.1.5 is the unique non-archimedean field norm on K which extends the p-adic norm on $\mathbb{Q}_p$.*

Proof. To begin with, we can dispense with the following easy-to-check facts:

- The restriction to $\mathbb{Q}_p$ is the p-adic norm.
- If $|\cdot|_p$ is a norm, it is the unique one that extends $\mathbb{Q}_p$.
- $|\alpha|_p = 0 \Leftrightarrow \alpha = 0$.
- $|\cdot|_p$ is multiplicative.

Now, what remains, which is the difficult part, is to show the non-archimedean triangle inequality, namely that

$$|\alpha + \beta|_p \leq \max(|\alpha|_p, |\beta|_p)$$

This takes some doing, and we will not prove it here, but there is a relatively succinct proof in Koblitz [3]. □

3.2 The Ring of Integers, the Unit Group, and the Maximal Ideal

Now it makes sense to consider the analog of the ring of integers of a number field. In fact, we do have something called the ring of integers in an algebraic extension of $\mathbb{Q}_p$. The reader will recall that our definition of the integers of a number field came from the notion of the *integral closure* of $\mathbb{Z}$ in a number field K, which was in turn integrally closed in K, its field of fractions. We can then very naturally define the *ring of integers* A in $K \supset \mathbb{Q}_p$ to be the integral closure of $\mathbb{Z}_p$ in K. In fact, it turns out that there is a very simple condition for the integral closure of K, similar to the condition for membership in $\mathbb{Z}_p$.

Proposition 3.2.1. *Let K be a finite extension of $\mathbb{Q}_p$. Then the ring of integers of K is*

$$A = \{x \in K : |x|_p \leq 1\}$$

Proof. A is clearly a subring of K, from the additive and multiplicative properties of the non-archimedean norm. We must show that everything in A is an integer, and conversely, there are no integers outside of A.

First, consider $\alpha \in A$. Then α's conjugates are all in A (since they have the same norm as α), and since all the coefficients of α's minimal polynomial over $\mathbb{Q}_p$ are sums of products of conjugates of α, they also must lie in the ring A, but since they are all p-adic numbers, they lie in $A \cap \mathbb{Q}_p = \mathbb{Z}_p$, so α is an integer.

Conversely, consider any integer α whose monic irreducible polynomial is $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, with coefficients in $\mathbb{Z}_p$ (i.e., the coefficients all have norm less than or equal to 1). Then we have the following expression:

$$\alpha^n = a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$$

from which, using the properties of the non-archimedean norm, we derive

$$|\alpha|_p^n \leq \max_{i<m}(|a_i\alpha^i|_p) \leq \max_{i<m}(|\alpha|_p^i)$$

which would not be possible if $|\alpha|_p$ were larger than 1 □

Proposition 3.2.2. *Let K_p be a finite extension of $\mathbb{Q}_p$. Then the group of units of A is*

$$A^\times = \{x \in K_p : |x|_p = 1\}$$

Proof. Since $|x^{-1}|_p = |x|_p^{-1}$, we have that for integers x, $x^{-1} \in A \Leftrightarrow |x|_p \geq 1 \Leftrightarrow |x|_p = 1$ □

A is also sometimes known as the *valuation ring* of $|\cdot|_p$ in K.

Proposition 3.2.3. *Let K_p be a finite extension of $\mathbb{Q}_p$. Then the ring of integers has a unique maximal ideal, which is*

$$M = \{x \in K_p : |x|_p < 1\}$$

Furthermore, A/M is a finite extension of $\mathbb{F}_p$ of degree at most $[K : \mathbb{Q}_p]$.

Proof. The first statement follows from the fact that, because every single element of A that is not a unit is an element of M, M contains every ideal of A except for the unit ideal. Note that $M \cap \mathbb{Z}_p = p\mathbb{Z}_p$.

To prove the second statement, first observe that we have a natural inclusion $\mathbb{F}_p \approx \mathbb{Z}_p/p\mathbb{Z}_p \hookrightarrow A/M$ given by $a + p\mathbb{Z}_p \mapsto a + M$. This is well-defined and injective since for $a, a' \in \mathbb{Z}_p$, $a - a' \in \mathbb{Z}_p \Leftrightarrow a - a' \in M$. Therefore, A/M is an extension of $\mathbb{F}_p$.

Furthermore, the degree must be finite and no greater than $n = [K : \mathbb{Q}_p]$, since given $n+1$ elements of A/M, we can lift them to $n+1$ elements in $A \subset K$, which must be linearly dependent over $\mathbb{Q}_p$.

If p^k is the largest power of p dividing all the coefficients of the dependence relation, then if we multiply all coefficients by p^{-k}, we have another dependence relation whose coefficients are all in $\mathbb{Z}_p$ but are *not* all in $p\mathbb{Z}_p$. Projecting all the lifts and the coefficients back into A/M, we have a dependence relation on the original elements whose coefficients are all in $\mathbb{Z}_p/p\mathbb{Z}_p$ and are not all 0. Thus, the dimension of A/M as a vector space over $\mathbb{Z}_p/p\mathbb{Z}_p \approx \mathbb{F}_p$ does not exceed $[K : \mathbb{Q}_p]$.

□

We call A/M the *residue field* of K. Note that as a finite extension of $\mathbb{F}_p$, it has order p^f for $f < n$ and its unit group is cyclic of order $p^f - 1$. Further, note that the unit group $A^\times$ consists of the elements of the $p^f - 1$ nonzero cosets $u + M$ in A/M, so in a sense "most" elements of A are units.

3.3 Finite Extensions of $\mathbb{Q}_p$ Are Complete

It is a nice fact that finite extensions of the p-adic numbers are complete. To continue our analogy with the real numbers, note that this is trivially true of the reals, since the only algebraic extension of $\mathbb{R}$ is $\mathbb{C}$. This is because $\mathbb{C}$ is a 2-dimensional vector space over $\mathbb{R}$, and hence the only subspaces of $\mathbb{C}$ containing $\mathbb{R}$ are $\mathbb{C}$ and $\mathbb{R}$ themselves.

Theorem 3.3.1. *Let K be a finite extension of $\mathbb{Q}_p$ of degree m, and let $|\cdot|_p$ be the uniquely defined norm on K which extends the p-adic norm. Then K is complete with respect to $|\cdot|_p$.*

Proof. This is true because K has the product topology as a finite-dimensional vector space over $\mathbb{Q}_p$; that is, if we fix a basis and map the sequence $\{v_n\}_{n=1}^{\infty}$ to $\{(x_{1,n}, x_{2,n}, \ldots x_{m,n})\}_{n=1}^{\infty}$. Each of the sequences of projections $\{\pi_i(v_n)\}_{n=1}^{\infty} = \{x_{i,n}\}_{n=1}^{\infty}$ converges to some x_i^* by completeness of $\mathbb{Q}_p$, so the v_n converge to $v^* = (x_1^*, \ldots, x_m^*)$.

The fact that K has the product topology follows from Theorem 3.1.2, which implies that the the extended norm $\|\cdot\|_p$ is equivalent to the sup-norm, which yeilds the product topology on K. □

Unfortunately this is not the case for infinite extensions; in particular, $\overline{\mathbb{Q}}_p$, the algebraic closure of $\mathbb{Q}_p$, is not complete with respect to the extended norm, which arises from setting $|\alpha|_p$ to be the norm of α in $\mathbb{Q}_p(\alpha)$. (We can easily check that this is a norm by observing that any two given elements α, β of $\overline{\mathbb{Q}}_p$ both lie in the finite extension $\mathbb{Q}_p(\alpha, \beta)$ and have the same norms, so it is sufficient to know that the three conditions for norm hold in all the finite extensions between $\mathbb{Q}_p$ and $\overline{\mathbb{Q}}_p$). However, if we take the completion of $\overline{\mathbb{Q}}_p$, which we denote Ω_p, then finally we get something that is complete *and* algebraically closed. For this reason, Ω_p is frequently called "the p-adic analog of $\mathbb{C}$."

Amazingly, the Axiom of Choice implies that Ω_p is actually *isomorphic* to $\mathbb{C}$, but there is no known explicit isomorphism between the two.

Again, the situation is much cleaner if we replace $\mathbb{Q}_p$ with $\mathbb{R}$, since the algebraic closure of $\mathbb{R}$, $\mathbb{C}$, is just a *quadratic* extension and is complete with respect to the archimedean norm on the $\mathbb{C}$ that extends $|\cdot|_\infty$, which is just the complex modulus.

3.4 $\mathfrak{p}$-adic Norms of Number Fields

Thus far, we have only considered the perspective of completing $\mathbb{Q}$ with respect to a non-archimedean norm and then taking algebraic extensions. But what if we turned this order backwards: that is, what if we started with a number field K and then took its completion with respect to any non-archimedean norm? This is a more complicated case, but the result of this process is in fact a finite extension of $\mathbb{Q}_p$.

To generalize the definition of our p-adic norm, consider any Dedekind domain D (for instance the ring of integers of a number field K) and let K be it's field of fractions. Then if $\mathfrak{p}$ is a nonzero prime ideal of D, for any nonzero $x \in K$, xD is then a fractional ideal with some unique prime ideal factorization. We may define $|x|_\mathfrak{p} = ([D : \mathfrak{p}])^{-\operatorname{ord}_\mathfrak{p}(x)}$, where $\operatorname{ord}_\mathfrak{p}(x)$ is the exponent of $\mathfrak{p}$ in the prime factorization of (x). If we then complete K with respect to $|\cdot|_\mathfrak{p}$, we get a field $K_\mathfrak{p}$, the correct generalization of the p-adic numbers. When K is a number field, this does turn out to be a finite extension of $\mathbb{Q}_p$, where $\mathfrak{p}$ lies over p.

3.5 Examples

To cap off our journey, we might like to consider some examples of finite extensions of $\mathbb{Q}_p$ and work with them a bit.

First, we may consider an extension which exists for every single p. This is $\mathbb{Q}_p(\sqrt{p})$, a quadratic extension. Since $|\sqrt{p}|_p = 1/\sqrt{p}$ and $\mathbb{Q}_p$ has no elements of norm not equal to an integral power of p, $\sqrt{p}$ must not be an element of $\mathbb{Q}_p$.

There is another extension of the p-adic numbers that we might be surprised to find at first: $\mathbb{Q}_p(e)$, where e is the base of the natural logarithm. This is because $e^p \in \mathbb{Q}_p$ for $p > 2$, which is clear from the expansion of e^p:

$$e^p = 1 + p/1! + p^2/2! + p^3/3! + \cdots$$

Note that the denominator keeps acquiring higher powers of p at a rate of $1/p + 1/p^2 + 1/p^3 + \cdots = 1/(p-1)$, but this is absorbed by the numerator, which gains 1 power of p per term, so the terms still get smaller and smaller and the series still converges. For $p = 2$, $e^4\mathbb{Q}_2$. Thus e is actually algebraic over $\mathbb{Q}_p$ for all p.

It is a fact, which is not easy to prove, that there are only finitely many extension fields of $\mathbb{Q}_p$ of any given degree n. We will attempt to make this fact at least plausible by proving it for quadratic extensions and finding all quadratic extensions of $\mathbb{Q}_3$.

First, we consider all quadratic extensions of $\mathbb{Q}_p$ for general p and note that the quadratic formula applies in any field of characteristic 0; that is, given any quadratic polynomial $aX^2 + bX + c = 0$ (with $a \neq 0$), solving the equation for X is equivalent to finding a square root of $b^2 - 4ac$:

$$\begin{aligned} aX^2 + bX + c = 0 \quad &\Leftrightarrow \quad 4a^2X^2 + 4abX + b^2 = b^2 - 4ac \\ &\Leftrightarrow \quad (2aX + b)^2 = b^2 - 4ac \end{aligned}$$

And the last equation can be solved whenever a square root of $b^2 - 4ac$ exists.

Thus, we have reduced to the polynomials of the form $f(X) = X^2 - a$. The quadratic extensions of $\mathbb{Q}_p$ are exactly the fields obtained by adjoining square roots of elements for which no square root exists in $\mathbb{Q}_p$. We may further note that $b^2 = a \Leftrightarrow (p^k b)^2 = p^{2k}a$ for any $k \in \mathbb{Z}$, and therefore adjoining a square root of $p^{2k}a$ gives the same field as adjoining a square root of a. Thus, any quadratic extension of $\mathbb{Q}_p$ is equivalent to one obtained by adjoining a square root of some $a \in \mathbb{Z}_p - p^2\mathbb{Z}_p$.

Now we must use something called Krasner's Lemma:

Theorem 3.5.1 (Krasner's Lemma). *Suppose that α and β are elements of $\overline{\mathbb{Q}}_p$, the algebraic closure of $\mathbb{Q}_p$ with the canonical non-archimedean extension norm. Then if β is closer to α than any of α's conjugates, then $K(\alpha) \subset K(\beta)$.*

Proof. This proof closely follows that in [2]. First, let $L = \mathbb{Q}_p(\beta)$ and suppose that $\alpha \notin L$, so that $[L(\alpha) : L] > 1$. Then, there is at least one L-automorphism of $\overline{\mathbb{Q}}_p$ σ which does not fix α. We know that all conjugates of an element in $\overline{\mathbb{Q}}_p$ have the same p-adic norm, so we have

$$|\sigma(\beta) - \sigma(\alpha)|_p = |\sigma(\beta - \alpha)|_p = |\beta - \alpha|_p$$

But since σ is an L-automorphism, $\sigma(\beta) = \beta$ and we have

$$|\beta - \sigma(\alpha)|_p = |\beta - \alpha|_p$$

But then we have, by our strong triangle inequality, that

$$|\alpha - \sigma(\alpha)|_p \leq \max(|\beta - \alpha|_p, |\beta - \sigma(\alpha)|_p) = |\beta - \alpha|_p$$

Which contradicts our initial assumption, that β was closer to α than any of α's conjugates! Thus our assumption must have been false and the theorem is proved. □

Note that if both $K(\alpha)$ and $K(\beta)$ are extensions of the same degree over $\mathbb{Q}_p$, then the conclusion implies further that $K(\alpha) = K(\beta)$.

Krasner's Lemma is a step in showing the fact that in general that there are only finitely many extensions of $\mathbb{Q}_p$ of degree n, but for now we will just use it in the special case we are considering.

Now, we are equipped to show the following corollary:

Corollary 3.5.2. *Let $p > 2$, and let α and β be square roots of elements of $\mathbb{Z}_p - p^2\mathbb{Z}_p$. If $\alpha^2 \equiv \beta^2(\mod p|\alpha^2|_p)$, then $K(\alpha) = K(\beta)$.*

Proof. Assume the opposite; then $[K : \mathbb{Q}_p] = 4$ and $\text{Gal}(K/\mathbb{Q}_p)$ consists of the four maps which send $\alpha + \beta$ to $\alpha + \beta$, $-\alpha + \beta$, $\alpha - \beta$, and $-\alpha - \beta$. Since α's only conjugate is $-\alpha$, we have that the closest distance between conjugates is

$$|\alpha - (-\alpha)|_p = |2\alpha|_p = |\alpha|_p$$

since 2 is a unit in $\mathbb{Z}_p$. But the distance between α and β is

$$\begin{aligned} |\alpha - \beta|_p &= |\mathbb{N}(\alpha - \beta)|_p^{1/4} \\ &= |(\alpha - \beta)(\alpha + \beta)(-\alpha - \beta)(-\alpha + \beta)|_p \\ &= |(\alpha^2 - \beta^2)^2|_p^{1/4} \\ &= |\alpha^2 - \beta^2|_p^{1/2} \\ &\leq \left(\frac{1}{p}|\alpha^2|_p\right)^{1/2} \\ &= |\alpha|_p/(\sqrt{p}) \\ &< |\alpha - (-\alpha)|_p \end{aligned}$$

Therefore, Krasner's Lemma applies and the two extensions must be the same after all, contradicting our assumption. □

Note that this corollary implies that there are only finitely many quadratic extensions of $\mathbb{Q}_p$ for odd p. This proof can be generalized to $p = 2$ if we tighten the hypothesis so that $\alpha^2 \equiv \beta^2(\mod p^3|\alpha^2|_p)$.

To apply the corollary above for $p = 3$, note that an element of $\mathbb{Z}_3 - 9\mathbb{Z}_3$ is either a unit (in which case its norm, and its square root's norm, are 1) or three times a unit (in which case the norm of its square root is $1/\sqrt{(3)}$). In the first case, it means we need only consider one unit from each congruence class modulo 3; in the second case, we need only consider one element from each congruence class modulo 9. In other words, since we have square roots of 1 and 0 already in $\mathbb{Q}_3$ we have shown that there are finitely many quadratic extensions of $\mathbb{Q}_3$, and in fact that a complete list (with possible repetition) is $\mathbb{Q}_3(\sqrt{2})$, $\mathbb{Q}_3(\sqrt{3})$, and $\mathbb{Q}_3(\sqrt{6})$. Note that either all of these are equal or all three are distinct, since $\sqrt{2}\cdot\sqrt{3} = \sqrt{6}$.

In fact, it must be the case that all three are distinct because $\mathbb{Q}_3(\sqrt{2})$ has no elements of norm $1/\sqrt{3} = |\sqrt{3}|_3$ in it. To see this observe that

$$\begin{aligned} |a+b\sqrt{2}|_3^2 &= |\mathbb{N}(a+b\sqrt{2})|_3 \\ &= |(a+b\sqrt{2})(a-b\sqrt{2})|_3 \\ &= |a^2-2b^2|_3 \\ &\leq \max(|a|_3^2, |b|_3^2) \end{aligned}$$

since 2 is a unit. We want to show that the above is an *even* power of 3.

If $|a|_3 \neq |b|_3$, then the isosceles triangle principle implies that

$$|a+b\sqrt{2}|_3 = \max(|a|_3, |b|_3)$$

and we are done. If $|a|_3 = |b|_3 = 3^k$ then we have, for some $a_0, b_0 \in \{1, -1\}$ and some $u, v \in U$, $a = 3^{-k}(a_0+3u)$ and $b = 3^{-k}(b_0+3v)$, so that we have

$$\begin{aligned} |a+b\sqrt{2}|_3^2 &= |a^2-2b^2|_3 \\ &= |3^{-2k}\left((a_0+3u)^2 - 2(b_0+3v)^2\right)|_3 \\ &= 3^{2k}|a_0^2 - 2b_0^2 + 3(2a_0u+3u^2-4b_0+3v^2)|_3 \\ &= 3^{2k}|-1+3(\cdots)|_3 \\ &= 3^{2k} \end{aligned}$$

and we are done.

References

[1] Holly, Jan. "Pictures of Ultrametric Spaces, the p-adic Numbers, and Valued Fields." *The Mathematical Association of America Monthly*, October 2001.

[2] KimJ. "p-adics, part deux." Elementary lecture on topics in p-adics. Transcript online at

`br.endernet.org/~loner/basicnumbertheory/kimjp-adicsdeux.txt`

[3] Koblitz, Neal. *p-adic Numbers, p-adic Analysis, and Zeta-Functions.* New York: Springer-Verlag, 1977.

[4] Stein, William. *A Brief Introduction to Classical and Adelic Number Theory*. Notes for Math 129, Spring 2004.

[5] "*p*-adic Number." Absolute Astronomy Reference. Online at

`www.absoluteastronomy.com/encyclopedia/P/P/P-adic_number.htm`