University of Nevada, Reno

Finite Field Extensions of the p-adic Numbers

A thesis submitted in partial fulfillment of the
requirements for the degree of
Master of Science in Mathematics.

by

Annalee Helen Wiswell Gomm

Dr. Bruce E. Blackadar/Thesis Advisor

May 2011

University of Nevada, Reno

THE GRADUATE SCHOOL

We recommend that the thesis
prepared under our supervision by

ANNALEE HELEN WISWELL GOMM

entitled

Finite Field Extensions of the p-adic Numbers

be accepted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE

Bruce E. Blackadar, Ph.D., Advisor

Valentin Deaconu, Ph.D., Committee Member

W. Patrick Arnott, Ph.D., Graduate School Representative

Marsha H. Read, Ph.D., Associate Dean, Graduate School

May 2011

Abstract

When we complete the rational numbers $\mathbb{Q}$ with respect to the usual absolute value, we obtain the real numbers $\mathbb{R}$. If we complete $\mathbb{Q}$ with respect to the so-called p-adic absolute value, we get a new field, $\mathbb{Q}_p$. In this paper, we demonstrate a method for finding finite field extensions of $\mathbb{Q}_p$ by determining all extensions of $\mathbb{Q}_p$ of degree five in the case $p = 5$.

Acknowledgements

First and foremost I offer my sincerest gratitude to my advisor, Dr. Bruce Blackadar, who has supported me throughout my thesis with his patience and knowledge whilst allowing me the freedom to work on a project of my own choosing. I attribute the level of my master's degree to his encouragement and effort. One simply could not wish for a better or friendlier advisor.

The informal support and optimism of many teachers, friends, and family members has also been indispensable. My husband Jeffrey has sustained me mentally, emotionally, and physically, and I thank him.

Contents

Chapter 1

Construction of $\mathbb{Z}_p$ and $\mathbb{Q}_p$

1.1 Introduction

First year analysis students should all be familiar with the process of constructing the field $\mathbb{R}$ of real numbers from the rational numbers $\mathbb{Q}$. In Cantor's construction of $\mathbb{R}$, each real number is defined to be an equivalence class of Cauchy sequences of rational numbers. Since Cauchy sequences are defined using the notion of distance, induced by the absolute value function, the way in which we define absolute value determines the field that results from the completion of $\mathbb{Q}$. If we measure distance between rational numbers using an absolute value other than the traditional one, we obtain an entirely different field after completing $\mathbb{Q}$ by Cantor's process.

In this chapter we will introduce a new class of absolute value functions, each of which corresponds to a prime number p. As it turns out, every possible absolute value on $\mathbb{Q}$ is equivalent either to one of these, to the traditional absolute value, or to the discrete absolute value. For each p, we will complete $\mathbb{Q}$ with respect to the absolute value

associated to it and obtain a new field, the p-adic numbers $\mathbb{Q}_p$.

1.2 The p-adic Absolute Value

We begin this section by defining the p-adic ordinal.

Definition. Let $p \in \mathbb{Z}$ be prime. For any nonzero integer a, define

$$\mathrm{ord}_p(a) = \text{the largest power of } p \text{ which divides } a$$

to be the *p-adic ordinal of a*. More formally, $\mathrm{ord}_p(a)$ is the unique positive integer which satisfies

$$a = p^{\mathrm{ord}_p(a)} \cdot b \qquad \text{and} \qquad p \nmid b$$

for some integer b.

Examples. We have $-423 = 3^2 \cdot -47$ and $3 \nmid -47$, so $\mathrm{ord}_3(-423) = 2$. Since $5 \nmid 24$, we have $\mathrm{ord}_5(24) = 0$.

We can extend the definition of ord_p to $\mathbb{Q}$ by writing a rational number x as a/b for integers a and b and putting

$$\mathrm{ord}_p(x) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b).$$

By convention we say that $\mathrm{ord}_p(0) = \infty$ for any p.

Examples. The following examples illustrate the extended definition of the p-adic

ordinal:

$$\begin{aligned}
&\mathrm{ord}_2\left(\frac{4}{7}\right) = \mathrm{ord}_2\left(2^2\right) - \mathrm{ord}_2\left(7\right) = 2 - 0 = 2;\\
&\mathrm{ord}_3\left(-\frac{1}{81}\right) = \mathrm{ord}_3\left(-1\right) - \mathrm{ord}_3\left(3^4\right) = 0 - 4 = -4;\\
&\mathrm{ord}_5\left(\frac{2620}{1500}\right) = \mathrm{ord}_5\left(5 \cdot 524\right) - \mathrm{ord}_5\left(5^3 \cdot 12\right) = 1 - 3 = -2.
\end{aligned}$$

Now for any integers a and c, the highest power of p that divides the product ac is just the sum of the power of p dividing a and the power dividing c. In terms of the p-adic ordinal, this means that $\mathrm{ord}_p(ac) = \mathrm{ord}_p(a) + \mathrm{ord}_p(c)$. Observe that

$$\begin{aligned}
\mathrm{ord}_p\left(\frac{ac}{bc}\right) &= \left(\mathrm{ord}_p(a) + \mathrm{ord}_p(c)\right) - \left(\mathrm{ord}_p(b) + \mathrm{ord}_p(c)\right)\\
&= \mathrm{ord}_p(a) - \mathrm{ord}_p(b))\\
&= \mathrm{ord}_p(a/b).
\end{aligned}$$

Therefore, even if $x = a/b$ is not written in lowest terms, $\mathrm{ord}_p(x)$ is still well defined. In the third example above, we could have calculated the 5-adic ordinal of 2620/1500 as follows:

$$\mathrm{ord}_5\left(\frac{2620}{1500}\right) = \mathrm{ord}_5\left(\frac{131}{75}\right) = \mathrm{ord}_5\left(131\right) - \mathrm{ord}_5\left(5^2 \cdot 3\right) = 0 - 2 = -2.$$

Now that we have defined the ordinal, we will use it to define a new absolute value on the rational numbers. First we need to know precisely what is meant by an absolute value.

Definition. A function $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ is said to be an absolute value on $\mathbb{Q}$ if the following are true for all $x, y \in \mathbb{Q}$:

1. $|x|_p \geq 0$ and $|x|_p = 0$ iff $x = 0$;

2. $|xy|_p = |x|_p \, |y|_p$; and

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

The reader is no doubt familiar with the traditional absolute value on the rational numbers, which is given by

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

The following definition gives another absolute value on $\mathbb{Q}$.

Definition. Let $p \in \mathbb{Z}$ be prime. For any rational number x, define

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

The function $|\cdot|_p$ is said to be the *p-adic absolute value*.

Examples. We can use the p-adic ordinals that we calculated above to find absolute values in the following examples:

$$|-423|_3 = 3^{-2} = \frac{1}{9}; \qquad |24|_5 = 5^0 = 1;$$

$$\left|\frac{4}{7}\right|_2 = 2^{-2} = \frac{1}{4}; \qquad \left|-\frac{1}{81}\right|_3 = 3^4 = 81; \qquad \left|\frac{2620}{1500}\right|_5 = 5^2 = 25.$$

It is straightforward to verify that the p-adic absolute value satisfies the first two of the defining properties of an absolute value. In order to establish the third property,

we will prove the stronger claim that $|\cdot|_p$ is *non-archimedean*.

Definition. An absolute value $|\cdot|$ on a field $\mathbb{F}$ is said to be *non-archimedean* if for all $x, y \in \mathbb{F}$,

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

Clearly the non-archimedean property implies the triangle inequality, so by proving that this holds we will have shown that $|\cdot|_p$ is a non-archimedean absolute value.

Proposition. The function $|\cdot|_p$ on $\mathbb{Q}$ is a non-archimedean absolute value.

Proof. We need only to show that the non-archimedean property holds. Let $x, y \in \mathbb{Q}$. The proof is trivial if any of x, y, or $x+y$ are equal to zero, so we assume that all three are nonzero. Write $x = a/b$ and $y = c/d$, where the fractions are in lowest terms. Then $x+y = (ad+bc)/bd$, and so we have $\mathrm{ord}_p(x+y) = \mathrm{ord}_p(ad+bc) - \mathrm{ord}_p(bd)$. Note that any power of p which divides both ad and bc will also divide the sum $ad + bc$; thus $\mathrm{ord}_p(ad + bc) \geq \min\{\mathrm{ord}_p(ad), \mathrm{ord}_p(bc)\}$. Therefore, we have

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

It follows that $-\mathrm{ord}_p(x + y) \leq \max\{-\mathrm{ord}_p(x), -\mathrm{ord}_p(y)\}$. Incorporating this result

into the definition of $|\cdot|_p$ gives

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

which is what we wanted to prove. □

In section 1.5, we will see that several interesting results about the p-adic numbers can be derived from the non-archimedean property.

Since $|\cdot|_p$ is indeed an absolute value on $\mathbb{Q}$, it makes sense to talk about the notion of a Cauchy sequence under the induced metric.

Definition. A sequence $\{a_n\}$ of rational numbers is said to be *Cauchy with respect to* $|\cdot|_p$ if for every $\epsilon > 0$ there is a positive integer N such that $|a_n - a_m|_p < \epsilon$ whenever $n > N$ and $m > N$.

We say that two absolute value functions are *equivalent* if any sequence of rational numbers is Cauchy with respect to the first absolute value if and only if it is Cauchy with respect to the second absolute value. At this point it is natural to ask whether there are any other absolute values on the rational numbers. The following theorem, due to Ostrowski, answers this question. It states that we have found essentially all absolute value functions on $\mathbb{Q}$.

Theorem (Ostrowski's Theorem). Every absolute value function on $\mathbb{Q}$ is equivalent to one of the following:

1. the discrete absolute value:

$$|x|_0 = \begin{cases} 1, & \text{if } x \neq 0 \\ 0, & \text{if } x = 0 \end{cases};$$

2. the traditional absolute value, sometimes denoted $|\cdot|_\infty$:

$$|x|_\infty = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \end{cases}; \text{ or}$$

3. $|\cdot|_p$ for some prime number p.

There is a nice proof of this theorem in [6].

1.3 The Field $\mathbb{Q}_p$

We are now ready to construct a new field, $\mathbb{Q}_p$. We will do this by completing $\mathbb{Q}$ as a metric space with respect to the metric induced by $|\cdot|_p$ for a fixed prime number p. The method that we will use is analogous to the one Cantor used to construct $\mathbb{R}$ from $\mathbb{Q}$. Our construction will rely on the notion of Cauchy sequences and equivalence classes of Cauchy sequences.

Recall from the previous section that a sequence $\{a_n\}$ of rational numbers is Cauchy with respect to $|\cdot|_p$ if for every $\epsilon > 0$ there is a positive integer N such that $|a_n - a_m|_p < \epsilon$ whenever $n > N$ and $m > N$. This definition is also valid if we replace "p" with "∞". It is important to keep in mind that since $|\cdot|_p$ and $|\cdot|_\infty$ mea-

sure distance between rational numbers differently, sequences in $\mathbb{Q}$ which are Cauchy with respect to $|\cdot|_p$ may not be Cauchy with respect to the traditional absolute value and vice versa.

Let $\mathcal{C}_p$ denote the set of all sequences of rational numbers which are Cauchy with respect to $|\cdot|_p$. We can add, subtract, and multiply elements of $\mathcal{C}_p$ by defining

$$\{a_n\} + \{b_n\} = \{a_n + b_n\}; \qquad \{a_n\} - \{b_n\} = \{a_n - b_n\}; \qquad \{a_n\} \cdot \{b_n\} = \{a_n \cdot b_n\},$$

so $\mathcal{C}_p$ is a commutative ring. The identity element under addition is the sequence $\{0, 0, 0, \ldots\}$, and the identity element under multiplication is $\{1, 1, 1, \ldots\}$. For every rational number x, the sequence $\{x, x, x, \ldots\}$ is clearly Cauchy. By identifying x with the sequence $\{x, x, x, \ldots\}$, we see that $\mathcal{C}_p$ contains a subring isomorphic to $\mathbb{Q}$. However, $\mathcal{C}_p$ itself is not a field. We can see this by noting that it contains zero divisors: for example,

$$\{1, 0, 0, 0, \ldots\} \cdot \{0, 1, 0, 0, \ldots\} = \{0, 0, 0, \ldots\}.$$

This "problem" arises because two different Cauchy sequences can have the same limit even though they are distinct elements of $\mathcal{C}_n$. The following definition will help us remedy this.

Definition. Let $\{a_n\}$ and $\{b_n\}$ be sequences of rational numbers which are Cauchy with respect to $|\cdot|_p$. We say that they are *equivalent Cauchy sequences* if

$$\lim_{n\to\infty} |a_n - b_n|_p = 0.$$

Instead of working with elements of $\mathcal{C}_p$, we would like to instead work with the set of

equivalence classes. Let

$$\mathcal{I} = \left\{ \{a_n\} \in \mathcal{C}_n : \lim_{n\to\infty} |x_n|_p = 0 \right\}$$

denote sequences which tend to zero with respect to $|\cdot|_p$. So two elements of $\mathcal{C}_p$ are equivalent if and only if their difference is in $\mathcal{I}$. It is not difficult to show that $\mathcal{I}$ is an ideal of $\mathcal{C}_p$, and it can be proved that it is in fact a maximal ideal (see [5]). The set of equivalence classes of Cauchy sequences in $\mathcal{C}_p$ is the quotient $\mathcal{C}_p/\mathcal{I}$. The quotient of a commutative ring by a maximal ideal is a field, so this gives us the new field that we were seeking.

Definition. The field of *p-adic numbers* is defined to be the set of equivalence classes of Cauchy sequences of rational numbers with respect to $|\cdot|_p$. We denote this field $\mathbb{Q}_p$.

If x and y are distinct rational numbers, then the sequences

$$\{x, x, x, \ldots\} \quad \text{and} \quad \{y, y, y, \ldots\}$$

are clearly not equivalent, so they represent different elements of $\mathbb{Q}_p$. This means that the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ is injective, so $\mathbb{Q}_p$ contains a subfield isomorphic to $\mathbb{Q}$.

We can take the absolute value of an element of $\mathbb{Q}_p$ by choosing a representative sequence $\{a_n\}$ for an equivalence class A and letting $|A|_p = \lim_{n\to\infty} |a_n|_p$. Since $|a_n|_p$ is a rational — hence real — number for each n, this is a limit of real numbers.

In order to see that this absolute value on $\mathbb{Q}_p$ is well defined, we must show that the limit exists and that it does not depend on the choice of the representative $\{a_n\}$.

From the triangle inequality for $|\cdot|_p$ we can deduce that

$$\Big||x|_p - |y|_p\Big|_\infty \leq |x-y|_p$$

for all $x, y \in \mathbb{Q}$. Applying this to two terms $|a_n|_p$ and $|a_m|_p$ of the sequence $\{|a_n|_p\}$ of real numbers,

$$\Big||a_n|_p - |a_m|_p\Big|_\infty \leq |a_n - a_m|_p\,,$$

shows that $\{|a_n|_p\}$ is Cauchy with respect to $|\cdot|_\infty$ since $\{a_n\}$ is Cauchy with respect to $|\cdot|_p$. Therefore $\lim_{n\to\infty}|a_n|_p$ exists. If $\{a'_n\}$ is a second sequence in the equivalence class a, the same inequality gives

$$0 \leq \lim_{n\to\infty}\Big||a_n|_p - |a'_n|_p\Big|_\infty \leq |a_n - a'_n|_p = 0.$$

Hence $\lim_{n\to\infty}|a_n|_p = \lim_{n\to\infty}|a'_n|_p$.

Recall that for each nonzero rational number a_n, $|a_n|_p$ is a rational number of the form p^k. Therefore, since the sequence of norms $\{|a_n|_p\}$ converges, either it tends to zero or is eventually constant. Moreover, each p-adic number has an absolute of the form p^k. Even though the set of p-adic numbers is strictly bigger than the set $\mathbb{Q}$, the set of absolute values of p-adic numbers is the same as the set of absolute values of rational numbers. That is,

$$\{|x|_p : x \in \mathbb{Q}_p\} = \{|x|_p : x \in \mathbb{Q}\}.$$

Now for the punchline of this discussion: it turns out that $\mathbb{Q}_p$ is complete, and that the isomorphic image of $\mathbb{Q}$ in $\mathbb{Q}_p$ is dense.

Proposition. The field $\mathbb{Q}_p$ is complete with respect to the absolute value $|\cdot|_p$, and the image of $\mathbb{Q}$ under the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ is a dense subset of $\mathbb{Q}_p$.

Proof. We'll prove the second part first. Fix $\epsilon > 0$, and let $A \in \mathbb{Q}_p$ be represented by the sequence $\{a_n\}$. What needs to be shown is that the open ball of radius ϵ around A contains an element of the image of $\mathbb{Q}$, that is, the equivalence class of a constant sequence. By the Cauchy property, we can find an integer N such that $|a_n - a_m|_p < \epsilon/2$ whenever $n > N$ and $m > N$. Consider the equivalence class B of the constant sequence $\{a_{N+1}\}$. The sequence $\{a_n - a_{N+1}\}$ represents $A - B$. We claim that $|A - B|_p < \epsilon$. Indeed, for any $n > N$ we have

$$|a_n - a_{N+1}|_p < \epsilon/2,$$

so that in the limit we obtain

$$|A - B|_p = \lim_{n\to\infty} |a_n - a_{N+1}|_p \leq \epsilon/2 < \epsilon.$$

This shows that B belongs to the open ball of radius ϵ around a, so we are done with the first part of the proof.

Proving the second part is not difficult, but we must be careful with our notation since we will be considering Cauchy sequences of equivalence classes of Cauchy sequences. Suppose $\{A_n\}$ is a Cauchy sequence in $\mathbb{Q}_p$. By what we just proved, for any A_n there exists an equivalence class B_n containing a constant sequence $\{a_n, a_n, a_n, \cdots\}$ such that $a_n \in \mathbb{Q}$ and

$$|A_n - B_n|_p < 1/n.$$

This shows that $|A_n - B_n|_p$ approaches zero, so the sequence $\{A_n - B_n\}$ in $\mathbb{Q}_p$ ap-

proaches the equivalence class of $\{0, 0, 0, \ldots\}$. In particular, $\{A_n - B_n\}$ converges, so it is a Cauchy sequence in $\mathbb{Q}_p$. Since $\{B_n\} = \{A_n\} - \{A_n - B_n\}$ is the difference of two Cauchy sequences, it too is a Cauchy sequence in $\mathbb{Q}_p$. Each term B_n in the sequence $\{B_n\}$ is the image of a rational number a_n, and so $\{a_n\}$ is a Cauchy sequence of rational numbers. Let A denote the equivalence class of $\{a_n\}$ and note that each term in the sequence $\{A - B_n\}$ is equivalent to $\{0, 0, 0, \ldots\}$. We use the fact that

$$\{A - A_n\} = \{A - B_n\} - \{A_n - B_n\}$$

is the difference of two sequences approaching the equivalence class of $\{0, 0, 0, \ldots\}$ to conclude that $\{A - A_n\}$ approaches the equivalence class of $\{0, 0, 0, \ldots\}$, and therefore

$$\lim_{n\to\infty} |A - A_n|_p = 0.$$

This means that $\lim_{n\to\infty} A_n = A$, so that $\{A_n\}$ converges, and $\mathbb{Q}_p$ is complete. $\square$

Thinking of the field elements as equivalence classes is an abstruse way to visualize the p-adic numbers. One of the standard ways to define the real numbers is as equivalence classes of Cauchy sequences of rational numbers (with respect to $|\cdot|_\infty$), but each real number has a standard decimal representation, and it is more concrete to think of $\mathbb{R}$ in these terms. Similarly, there is a more concrete way to think of the p-adic numbers. Each $a \in \mathbb{Q}_p$ can be represented uniquely by an infinite sum of the form

$$a = a_{-k}p^{-k} + a_{-(k-1)}p^{-(k-1)} + \cdots + a_{-1}p^{-1} + a_0 + a_1 p + a_2 p^2 + \cdots,$$

where each coefficient a_n is in the set $\{0, 1, \ldots, p-1\}$ and a_{-k} is nonzero. This can be shown systematically, as in [6], but here we will just give some examples. We call this representation of a its p-adic expansion (note that it resembles a Laurent series

expansion in p). The p-adic absolute value is easily determined when a is written in this form: it is just $\left|a_{-k}p^{-k}\right|_p = p^k$.

Examples. The 7-adic expansion of the rational number 47474 is:

$$47474 = 6 \cdot 7 + 2 \cdot 7^2 + 5 \cdot 7^3 + 5 \cdot 7^4 + 2 \cdot 7^5.$$

The 5-adic expansion of $96.904 = 12113/125$ is:

$$96.904 = 3 \cdot 5^{-3} + 2 \cdot 5^{-2} + 4 \cdot 5^{-1} + 1 + 4 \cdot 5 + 3 \cdot 5^2.$$

The p-adic expansion allows us to perform the field operations of addition and multiplication in $\mathbb{Q}_p$ in a way very similar to that in $\mathbb{R}$. In fact, addition and multiplication just amount to a straightforward generalization of the usual algorithms for adding and multiplying positive integers expressed in base p. In order to illustrate the addition algorithm, and to give another example of p-adic expansions, let us find the p-adic expansion of -2 in $\mathbb{Q}_5$. Since $|-2|_5 = |2|_5 = 1 = p^0$, the first nonzero coefficient in the 5-adic expansion of -2 is a_0. Thus we have

$$-2 = a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \cdots,$$

where $a_n \in \{0, 1, 2, 3, 4\}$ for each n and $a_0 \neq 0$. We also know that $-2 + 2 = 0$:

$$\begin{array}{rl} & a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \cdots \\ + & 2 \\ \hline & 0 \end{array}$$

From this we see that we must have $a_0 + 2 = 0$, but since $a_0 \in \{0, 1, 2, 3, 4\}$, the only

way to achieve this is to have $a_0 + 2 = 5$ and carry 1 to the right. Thus $a_0 = 3$. The sum of a_1 and the carried 1 must also be 0, so $a_1 = 4$, and we again carry 1 to the right. Continuing in this fashion, we see that

$$-2 = 3 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + \cdots .$$

Multiplication can be performed in a similar way; we just need to remember to multiply and carry from the left to the right rather than from the right to the left as we do in $\mathbb{R}$. This is natural, since the expansions are written opposite to the way they are in $\mathbb{R}$. For example, in $\mathbb{Q}_{11}$ we have:

$$\begin{array}{rl}
 & 2 + 2 \cdot 11 + 1 \cdot 11^2 \\
\times & 3 + 3 \cdot 11 + 5 \cdot 11^2 + 9 \cdot 11^3 \\
\hline
 & 6 + 6 \cdot 11 + 3 \cdot 11^2 \\
 & \quad 6 \cdot 11 + 6 \cdot 11^2 + 3 \cdot 11^3 \\
 & \qquad 10 \cdot 11^2 + 10 \cdot 11^3 + 5 \cdot 11^4 \\
 & \qquad\qquad 7 \cdot 11^3 + 8 \cdot 11^4 + 10 \cdot 11^5 \\
\hline
 & 6 + 1 \cdot 11 + 9 \cdot 11^2 + 10 \cdot 11^3 + 3 \cdot 11^4 + 0 \cdot 11^5 + 1 \cdot 11^6
\end{array}$$

Definition. Elements of $\mathbb{Q}_p$ with absolute value less than or equal to one form a ring known as the *p-adic integers* and denoted $\mathbb{Z}_p$. The *set of units* of $\mathbb{Z}_p$, written $\mathbb{Z}_p^\times$, consists of the elements of $\mathbb{Z}_p$ with absolute value exactly one.

The fact that $\mathbb{Z}_p^\times$ as defined above coincides with the units of the ring $\mathbb{Z}_p$ in the algebraic sense is given by the following proposition.

Proposition. A p-adic integer a has a multiplicative inverse in $\mathbb{Z}_p$ if and only if $|a|_p = 1$.

Proof. An element $a \in \mathbb{Z}_p$ is invertible if and only if $a^{-1} \in \mathbb{Z}_p$. This is equivalent to saying that $|a|_p \leq 1$ and $|a^{-1}|_p = |a|_p^{-1} \leq 1$, that is, $|a|_p = 1$. □

Algebraists will notice that the p-adic integers are defined as a *valuation ring*. It can also be shown that $\mathbb{Q}_p$ is the field of fractions of $\mathbb{Z}_p$. This provides a nice analogy between $\mathbb{Q}_p$ and $\mathbb{Q}$, which is the field of fractions of the rational integers $\mathbb{Z}$.

Examples. The number 225 is a 5-adic integer because its absolute value is $|225|_5 = 5^{-2} < 1$. Its 5-adic expansion is:

$$225 = 4 \cdot 5^2 + 1 \cdot 5^3.$$

Actually, any rational integer is also a p-adic integer. Nevertheless, there are some numbers which are p-adic integers but not rational integers. For example, $1/8$ is a 7-adic integer—in fact, it is a 7-adic unit—since $|1/8|_7 = 1$. The 7-adic expansion of $1/8$ is:

$$\frac{1}{8} = 1 + 6 \cdot 7 + 0 \cdot 7^2 + 6 \cdot 7^3 + 0 \cdot 7^4 + 6 \cdot 7^5 + \cdots .$$

To see why this is the case, multiply this expansion by 8:

$$\begin{aligned}
8 \times (1 + 6 \cdot 7 + 0 \cdot 7^2 + 6 \cdot 7^3 + 0 \cdot 7^4 + 6 \cdot 7^5 + \cdots) & \\
&= (1 + 1 \cdot 7)(1 + 6 \cdot 7 + 0 \cdot 7^2 + 6 \cdot 7^3 + 0 \cdot 7^4 + 6 \cdot 7^5 + \cdots) \\
&= (1 + 6 \cdot 7 + 0 \cdot 7^2 + 6 \cdot 7^3 + 0 \cdot 7^4 + 6 \cdot 7^5 + \cdots) \\
&\qquad + (1 \cdot 7 + 6 \cdot 7^2 + 0 \cdot 7^3 + 6 \cdot 7^4 + 0 \cdot 7^5 + 6 \cdot 7^6 + \cdots) \\
&= 1 + (6 + 1) \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 + 6 \cdot 7^4 + 6 \cdot 7^5 + 6 \cdot 7^6 + \cdots \\
&= 1 + \underbrace{7 \cdot 7 + 6 \cdot 7^2}\, + 6 \cdot 7^3 + 6 \cdot 7^4 + 6 \cdot 7^5 + 6 \cdot 7^6 + \cdots \\
&= 1 + (1 + 6) \cdot 7^2 + 6 \cdot 7^3 + 6 \cdot 7^4 + 6 \cdot 7^5 + 6 \cdot 7^6 + \cdots
\end{aligned}$$

$$
\begin{aligned}
&= 1 + \underbrace{7 \cdot 7^2 + 6 \cdot 7^3} + 6 \cdot 7^4 + 6 \cdot 7^5 + 6 \cdot 7^6 + \cdots \\
&= 1 + (1+6) \cdot 7^3 + 6 \cdot 7^4 + 6 \cdot 7^5 + 6 \cdot 7^6 + \cdots \\
&= 1 + \underbrace{7 \cdot 7^3 + 6 \cdot 7^4} + 6 \cdot 7^5 + 6 \cdot 7^6 + \cdots \\
&\cdots \\
&= 1.
\end{aligned}
$$

We note that the p-adic expansion of any p-adic integer is of the form

$$a = a_k p^k + a_{k+1} p^{k+1} + a_{k+2} p^{k+2} + \cdots ,$$

with k nonnegative. In fact, an alternate way to define the p-adic integers is to say that an element a of $\mathbb{Q}_p$ is a p-adic integer if and only if in its p-adic expansion the coefficients of negative powers of p are all zero. The units of $\mathbb{Z}_p$ are all of the form

$$a = a_0 + a_1 p + a_2 p^2 + \cdots ,$$

with $a_0 \neq 0$.

Now suppose

$$a = a_{-k} p^{-k} + a_{-(k-1)} p^{-(k-1)} + \cdots + a_{-1} p^{-1} + a_o + a_1 p + a_2 p^2 + \cdots$$

is an arbitrary p-adic number. By factoring out p^{-k}, we get $a = p^{-k} u$, where

$$u = a_{-k} + a_{-(k-1)} p + \cdots + a_{-1} p^{-1+k} + a_0 p^k + a_1 p^{k+1} + a_2 p^{k+2} + \cdots$$

is a unit. This illustrates an important point: any element of $\mathbb{Q}_p$ can be written

uniquely as the product of a power of p and a p-adic unit. The p-adic integers which are not units form a maximal ideal of $\mathbb{Z}_p$.

Proposition. The ring $\mathbb{Z}_p$ has a unique maximal ideal, $p\mathbb{Z}_p = \mathbb{Z}_p \setminus \mathbb{Z}_p^\times$.

Proof. There is a natural ring homomorphism from $\mathbb{Z}_p$ to the finite field containing p elements, $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$, given by reduction modulo p:

$$a = a_0 + a_1 p + a_2 p^2 + \cdots \mapsto a_0$$

This homomorphism is surjective, and its kernel is

$$\{a \in \mathbb{Z}_p : a_0 = 0\} = p\mathbb{Z}_p = \mathbb{Z}_p \setminus \mathbb{Z}_p^\times.$$

Since the quotient is a field, the kernel $p\mathbb{Z}_p$ is a maximal ideal. To show that it is the unique maximal ideal of $\mathbb{Z}_p$, suppose that I is another maximal ideal. Since $p\mathbb{Z}_p$ is maximal, it is not entirely contained in I. Therefore I contains some element of $\mathbb{Z}_p^\times$, the complement of $p\mathbb{Z}_p$. But then I contains a unit, so we must actually have $I = \mathbb{Z}_p$. This is a contradiction, so we conclude that $p\mathbb{Z}_p$ is the unique maximal ideal of the p-adic integers. □

We end this section with a cautionary note. Some algebraists use $\mathbb{Z}_p$ to denote the field $\mathbb{Z}/p\mathbb{Z}$. In this paper, $\mathbb{Z}_p$ and $\mathbb{Z}/p\mathbb{Z}$ are completely different and should not be confused with one another.

1.4 $\mathbb{Z}_p$ as the Inverse Limit of $\{\mathbb{Z}/p^n\mathbb{Z}\}$

There is another formulation of the p-adic numbers which deserves mention. We begin with a proposition.

Proposition. The image of $\mathbb{Z}$ under the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ is a dense subset of $\mathbb{Z}_p$. In particular, for each $a \in \mathbb{Z}_p$ and $n \geq 1$, there is a unique rational integer α such that $0 \leq \alpha \leq p^n - 1$ and $|x - \alpha|_p \leq p^{-n}$.

Proof. Fix $a \in \mathbb{Z}_p$ and $n \geq 1$. Let $a = a_0 + a_1 p + a_2 p^2 + \cdots$ be the p-adic expansion of a and set

$$\alpha = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}.$$

Then $\alpha \in \mathbb{Z}$ and satisfies $0 \leq \alpha \leq p^n - 1$. Also,

$$a - \alpha = a_n p^n + a_{n+1} p^{n+1} + a_{n+2} p^{n+2} + \cdots$$

is divisible by p^n, so $|a - \alpha|_p \leq p^{-n}$. It remains to show that α is the unique rational integer satisfying these conditions. Indeed, if $\beta \in \mathbb{Z}$ with $0 \leq \alpha \leq p^n - 1$, then β has a p-adic expansion of the form

$$\beta = b_0 + b_1 p + b_2 p^2 + \cdots + b_{n-1} p^{n-1}.$$

We have

$$a - \beta = (a_0 - b_0) + (a_1 - b_1)p + \cdots + (a_{n-1} - b_{n-1})p^{n-1} + a_n p^n + a_{n+1} p^{n+1} + \cdots,$$

so $a - \beta$ is divisible by p^n if and only if $a_k = b_k$ for $0 \leq k \leq n - 1$. Therefore, if

$|a-\beta|_p \leq p^n$ then we have

$$\beta = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1} = \alpha,$$

showing that α is indeed unique. □

An immediate consequence of this proposition is that for any $a \in \mathbb{Z}_p$, we can obtain a unique Cauchy sequence $\{\alpha_n\}$ converging to a in which each term α_n is a rational integer satisfying $0 \leq \alpha_n \leq p^n - 1$, and for each n we have $|x-\alpha|_p \leq p^{-n}$. Note that if $n \leq m$, we have

$$|\alpha_n - \alpha_m|_p \leq \max\left\{|x-\alpha_n|_p, |x-\alpha_m|_p\right\} \leq p^{-n},$$

so p^n divides $\alpha_m - \alpha_n$, that is, $\alpha_n \equiv \alpha_m \pmod{p^n}$.

On the other hand, if $\{\alpha_n\}$ is a sequence of rational integers satisfying $0 \leq \alpha_n \leq p^n - 1$ for $n \geq 1$ and $\alpha_n \equiv \alpha_m \pmod{p^n}$ for $n \leq m$, then we claim that $\lim_{n\to\infty} \alpha_n$ exists and is in $\mathbb{Z}_p$. Indeed, the condition $\alpha_n \equiv \alpha_m \pmod{p^n}$ is equivalent to $|\alpha_n - \alpha_m|_p \leq p^{-n}$, so the sequence is Cauchy and therefore has a limit. If $a = \lim_{n\to\infty} \alpha_n$, by definition we have

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

Since $|\alpha_n|_p \leq 1$ for each n (because $\alpha_n \in \mathbb{Z} \subset \mathbb{Z}_p$), we must also have $|a|_p \leq 1$. Thus $a \in \mathbb{Z}_p$.

What follows is that we can identify the elements of $\mathbb{Z}_p$ with sequences $\{\alpha_n\}$ satisfying the conditions given in the previous paragraph. That is, we can define $\mathbb{Z}_p$ to be the set of such sequences. Equivalently, we can consider sequences of the form $\{r_1, r_2, r_3, \ldots\}$, where r_n is an element of the ring $\mathbb{Z}/p^n\mathbb{Z}$ for each $n \geq 1$, since there is an obvious

correspondence between integers α with $0 \leq \alpha \leq p^n - 1$ and the elements of $\mathbb{Z}/p^n\mathbb{Z}$. We can summarize this using the concept of an inverse limit.

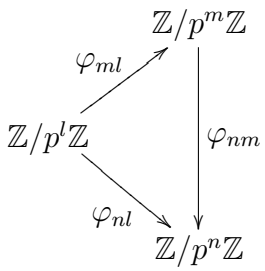
In the following definition, recall that the cartesian product of a sequence $\{S_n\}$ of sets, denoted $\prod_{n=1}^{\infty} S_n$, is the set of sequences $\{s_1, s_2, s_3, \ldots\}$ where $s_n \in S_n$ for each $n \geq 1$.

Definition. Let $\{S_n\}$ be a sequence of sets, and suppose that there are surjective maps $\varphi_{nm} : S_m \to S_n$, defined whenever $n \leq m$, such that φ_{nn} is the identity on S_n and $\varphi_{nl} = \varphi_{nm} \circ \varphi_{ml}$ for all $n \leq m \leq l$. The sets together with the homomorphisms form what is known as an *inverse system*. We define the *inverse limit* of the inverse system to be the subset of the cartesian product $\prod_{n=0}^{\infty} S_n$ defined by

$$\varprojlim S_n = \left\{ \{s_1, s_2, s_3, \ldots\} \in \prod_{n=1}^{\infty} S_n : s_n = \varphi_{nm}(r_m) \text{ for all } n \leq m \right\}.$$

The existence and uniqueness of the inverse limit of an inverse system is proved in [12]. That author also shows that when an inverse system is formed of topological spaces and continuous maps, then the inverse limit is a topological space. Similarly, the inverse limit of an inverse system of rings and ring homomorphisms is a ring.

Now consider the sequence $\{\mathbb{Z}/p^n\mathbb{Z}\}$ of rings. These rings are equipped with natural homomorphisms $\varphi_{nm} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, whenever $n \leq m$, given by reduction modulo p^n, and each φ_{nm} is surjective. For $n \leq m \leq l$, reducing elements of $\mathbb{Z}/p^l\mathbb{Z}$ modulo m and then reducing modulo n is the same as reducing modulo n by itself. That is, the following diagram commutes:



This means that $\varphi_{nl} = \varphi_{nm} \circ \varphi_{ml}$ for all $n \leq m \leq l$. Clearly φ_{nn} is the identity on $\mathbb{Z}/p^n\mathbb{Z}$, so $\{\mathbb{Z}/p^n\mathbb{Z}\}$ together with the (continuous) ring homomorphisms $\{\varphi_{nm}\}$ is an inverse system. The inverse limit $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ consists of sequences of the form $\{a_1, a_2, a_3, \ldots\}$ where $a_n \in \mathbb{Z}/p^n\mathbb{Z}$ for each n and a_n is equal to $a_m \pmod{p^n}$ whenever $n \leq m$. Our discussion above proves that

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p.$$

It is possible to begin the theory of the field of p-adic numbers by first defining $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ and then letting $\mathbb{Q}_p$ be the field of fractions of $\mathbb{Z}_p$. Our work in this section shows that this formulation of $\mathbb{Q}_p$ is equivalent to the formulation given in section 1.3.

1.5 Topological Properties of $\mathbb{Q}_p$

We saw in the previous section that $\mathbb{Q}_p$ is a complete metric space, and that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. As a topological space, this means that $\mathbb{Q}_p$ is *separable*: it has a countable dense subset. In this respect, $\mathbb{R}$ and $\mathbb{Q}_p$ are quite analogous. However, as we will show in this section, there are many differences between $\mathbb{R}$ and $\mathbb{Q}_p$ as topological spaces.

An important topological property of the real numbers is local compactness, that is, that every point of $\mathbb{R}$ has a compact neighborhood. It turns out that $\mathbb{Q}_p$ has this property in common with $\mathbb{R}$. Moreover, the p-adic integers form a compact subset of $\mathbb{Q}_p$.

Proposition. The set $\mathbb{Z}_p$ is compact, and $\mathbb{Q}_p$ is locally compact.

Proof. Since we are working in a metric space, showing that $\mathbb{Z}_p$ is compact is equivalent to showing that it is *sequentially compact*, i.e., that every infinite sequence of p-adic integers has a convergent subsequence. Let $\{x_n\}$ be a sequence in $\mathbb{Z}_p$, and for each $n \geq 1$, let

$$x_n = a_{n,0} + a_{n,1}p + a_{n,2}p^2 + a_{n,3}p^3 + \cdots$$

be the p-adic expansion of x_n. Each of the coefficients $a_{n,0}$ must be in the finite set $\{0, 1, \ldots, p-1\}$, so we can find $b_0 \in \{0, 1, \ldots, p-1\}$ and an infinite subsequence of $\{x_n\}$, which we will denote by $\{x_k^0\}$, such that $a_{n,0}$ is equal to b_0 for each of the terms in $\{x_k^0\}$. In the same manner, we can find $b_1 \in \{0, 1, \ldots, p-1\}$ and an infinite subsequence $\{x_k^1\}$ of $\{x_k^0\}$ such that $a_{n,1} = b_1$ for each term in $\{x_k^1\}$. By iterating this process, we will obtain $b_0, b_1, b_2, \ldots$ together with a sequence of sequences $\{x_k^0\}, \{x_k^1\}, \{x_k^2\}, \ldots$ in which the p-adic expansion of each term of $\{x_k^j\}$ begins with

$$b_0 + b_1 p + b_2 p^2 + \cdots + b_j p^j.$$

The diagonal sequence, given by $x_1^1, x_2^2, x_3^3, \ldots$, is a subsequence of $\{x_n\}$ which converges to the p-adic integer

$$b_0 + b_1 p + b_2 p^2 + \cdots .$$

This proves that $\mathbb{Z}_p$ is sequentially compact, and hence compact. For any point $a \in \mathbb{Q}_p$, the set $\{x + a : x \in \mathbb{Z}_p\}$ is the image of the compact set $\mathbb{Z}_p$ under the continuous map $x \mapsto x + a$, so it is a compact neighborhood of a. Therefore $\mathbb{Q}_p$ is locally compact. □

It is well known that $\mathbb{R}$ is a connected set, as is any open or closed interval of $\mathbb{R}$; but the p-adic numbers form a totally disconnected set, that is, the only connected subsets of $\mathbb{Q}_p$ are the empty set and sets consisting of a single point.

Proposition. The p-adic numbers form a totally disconnected set.

Proof. We must show that any subset of $\mathbb{Q}_p$ containing at least two elements is a disconnected set. Therefore, suppose that $A \subset \mathbb{Q}_p$ and that a and b are distinct elements of A. For any positive integer n, the set

$$U_n(a) = \left\{x \in \mathbb{Q}_p : |x - a|_p \leq p^{-n}\right\} = \left\{x \in \mathbb{Q}_p : |x - a|_p < p^{-n+1}\right\}$$

is both open and closed. For sufficiently large values of n, $b \notin U_n(a)$. The sets $V_1 = U_n(a) \cap A$ and $V_2 = (\mathbb{Q}_p \setminus U_n(a)) \cap A$ are disjoint since $b \in V_2$ but $b \notin V_1$. Note that V_1 is open in A, and V_2 is open in A since its complement in A is closed. Also, V_1 and V_2 are both nonempty. We have $A = V_1 \cup V_2$, so A is the disjoint union of nonempty open sets. This means that A is disconnected, completing the proof. □

Recall from section 1.2 that the p-adic absolute value is non-archimedean. That is, for all $x, y \in \mathbb{Q}_p$, we have $|x + y|_p \leq \max\left\{|x|_p, |y|_p\right\}$. Surprisingly, it turns out that if $|x_p| \neq |y|_p$, then this becomes an equality: $|x + y|_p = \max\left\{|x|_p, |y|_p\right\}$. To see this, assume without loss of generality that $|x|_p > |y|_p$, so that $|x|_p = \max\left\{|x|_p, |y|_p\right\}$.

This gives

$$|x+y|_p \leq |x|_p.$$

On the other hand, we can write x as $(x+y)+(-y)$. By the non-archimedean property, $|x|_p = |(x+y)+(-y)|_p \leq \max\left\{|x+y|_p, |y|_p\right\}$. By assumption $|x|_p$ is strictly greater than $|y|_p$, so we must have

$$|x|_p \leq |x+y|_p .$$

Combining these two inequalities gives us our result.

The fact that $|x_p| \neq |y|_p$ implies that $|x+y|_p = \max\left\{|x|_p, |y|_p\right\}$ seems unintuitive at first, but it makes sense if we think about what the p-adic absolute value means. This statement simply says that if two numbers are divisible by different powers of p (i.e. they have different absolute values), then their sum is divisible by the smaller power of p (which means it is the same size as the larger of the two numbers).

There are several unexpected results that follow from the non-archimedean property that are true of the p-adic numbers as well as of any metric space with a non-archimedean absolute value. We will present some of the most interesting results here.

Proposition. Every triangle in $\mathbb{Q}_p$ is an isosceles triangle. That is, given $x, y, z \in \mathbb{Q}_p$, at least two of the following distances are equal:

$$|x-y|_p, \qquad |y-z|_p, \qquad |z-x|_p.$$

Proof. This is a simple proof, given what we know about the p-adic absolute value.

Suppose that $|x-y|_p \neq |y-z|_p$. Then by the argument given above, we have

$$|(x-y)+(y-z)|_p = \max\left\{|x-y|_p, |y-z|_p\right\}.$$

But the left-hand side simplifies to $|x-z|_p = |z-x|_p$, so the third distance is equal to one of the first two. □

Proposition. Open balls in $\mathbb{Q}_p$ are closed sets, and closed balls in $\mathbb{Q}_p$ are open sets.

Proof. Let a be a p-adic number, and let $r > 0$ be a real number. To show that the open ball $B_r(a) = \left\{x \in \mathbb{Q}_p : |x-a|_p < r\right\}$ is a closed set, we will show that it contains its boundary. Take any b in the boundary of $B_r(a)$; this means that any open ball around b must contain points that are in $B_r(a)$. In particular, the open ball $B_r(b)$ must have a nonempty intersection with $B_r(a)$. Therefore, we choose some $x \in B_r(a) \cap B_r(b)$, and we have $|x-a|_p < r$ and $|b-x|_p = |x-b|_p < r$. Note that we can write $b-a$ as $(b-x)+(x-a)$. So by the non-archimedean property,

$$\begin{aligned} |b-a|_p &\leq \max\left\{|b-x|_p, |x-a|_p\right\} \\ &< r. \end{aligned}$$

Thus by definition, $b \in B_r(a)$. It follows that $B_r(a)$ is closed.

Next we show that the closed ball $\overline{B_r(a)} = \left\{x \in \mathbb{Q}_p : |x-a|_p \leq r\right\}$ is an open set. Given any $x \in \overline{B_r(a)}$, we must find an open ball around x that is completely contained in $\overline{B_r(a)}$. The open ball $B_r(x)$ will do. For an arbitrary $y \in B_r(x)$, we have $|y-x|_p < r$; and, since $x \in \overline{B_r(a)}$, we have $|x-a|_p \leq r$. We write $y-a$ as $(y-x)+(x-a)$

and apply the non-archimedean property to get

$$\begin{aligned} |y-a|_p &\leq \max\left\{|y-x|_p, |x-a|_p\right\} \\ &\leq r. \end{aligned}$$

This means that $y \in \overline{B_r(a)}$, and so $B_r(x) \subset \overline{B_r(a)}$. We conclude that $\overline{B_r(a)}$ is open. □

Proposition. Every point in a ball is a center of that ball.

Proof. We will prove the proposition for open balls only, since the proof for closed balls is almost identical. Let a be a p-adic number, let $r > 0$ be a real number, and let x be any point in the ball $B_r(a)$. We wish to show that $B_r(x) = B_r(a)$.

For any $y \in B_r(x)$, we have $|y-x|_p < r$. We also have $|x-a|_p < r$, because $x \in B_r(a)$ by assumption. Since we can write $y-a$ as $(y-x)+(y-a)$, we have

$$\begin{aligned} |y-a|_p &\leq \max\left\{|y-x|_p, |x-a|_p\right\} \\ &< r. \end{aligned}$$

This means that $y \in B_r(a)$, and so $B_r(x) \subset B_r(a)$.

The reverse containment is just as easy to show. For $y \in B_r(a)$, we have $|y-a|_p < r$. By assumption, we also have $|a-x|_p = |x-a|_p < r$. We write $y-x$ as $(y-a)+(a-x)$ and get

$$\begin{aligned} |y-x|_p &\leq \max\left\{|y-a|_p, |a-x|_p\right\} \\ &< r. \end{aligned}$$

Thus $y \in B_r(x)$, and so $B_r(a) \subset B_r(x)$. We conclude that $B_r(x) = B_r(a)$. $\square$

Proposition. Given two balls in $\mathbb{Q}_p$, they are either disjoint, or else one contains the other.

Proof. Let a and b be p-adic numbers, and let $r, s > 0$ be real. Suppose that the balls $B_r(a)$ and $B_s(b)$ are not disjoint. Assuming without loss of generality that $r \leq s$, we will show that $B_r(a) \subset B_s(b)$.

Since the intersection of $B_r(a)$ and $B_s(b)$ is nonempty, we choose some $x \in B_r(a) \cap B_s(b)$. The previous proposition tells us that x is a center of $B_r(a)$ and a center of $B_s(b)$. That is, $B_r(x) = B_r(a)$ and $B_s(x) = B_s(b)$. Since $r \leq s$, we have $B_r(x) \subset B_s(x)$. Therefore, we have

$$B_r(a) = B_r(x) \subset B_s(x) = B_s(a),$$

as desired.

A nearly identical proof shows that the proposition is true for closed balls as well. $\square$

To end this section, we will prove a surprising result concerning infinite series in $\mathbb{Q}_p$.

Proposition. Any infinite series of p-adic numbers whose terms approach 0 is convergent, and vice versa. That is,

$$\sum_{n=0}^{\infty} a_n \text{ converges} \qquad \text{iff} \qquad \lim_{n\to\infty} |a_n|_p = 0.$$

Proof. The proof that a series of p-adic numbers is convergent only if its terms approach 0 is analogous to the proof of a similar result in the real numbers. Thus we

will only prove the converse. We must show that if $\{a_n\}$ is a sequence of p-adic numbers such that $\lim_{n\to\infty} |a_n|_p = 0$, then $\sum_{n=0}^{\infty} a_n$ converges. In other words, we must show that the sequence $\{S_n\}$ of partial sums, defined by $S_n = \sum_{k=0}^{n} a_k$, converges. Since $\mathbb{Q}_p$ is a complete metric space by construction, it is enough to show that $\{S_n\}$ is Cauchy. To this end, we fix $\epsilon > 0$ and find a positive integer N such that $|a_k|_p < \epsilon$ whenever $k > N$. We are guaranteed the existence of N since $\lim_{n\to\infty} |a_n|_p = 0$. Now suppose $n \geq m > N$. Then using the non-archimedean property we obtain

$$\begin{aligned} |S_m - S_n|_p &= |a_{n+1} + a_{n+2} + \cdots + a_m| \\ &\leq \max\left\{ |a_{n+1}|_p , |a_{n+2}|_p , \cdots , |a_m|_p \right\} \\ &< \epsilon, \end{aligned}$$

which implies that $\{S_n\}$ is Cauchy and hence convergent. □

This is an interesting result since in calculus of real numbers, the implication is only true in the forward direction.

1.6 Hensel's Lemma

Now let us examine some of the algebraic properties of $\mathbb{Q}_p$. Consider the polynomial $f(x) = x^2 + 7$ in $\mathbb{Q}_{11}$. We would like to know whether f has any roots in $\mathbb{Q}_{11}$. That is, we want to find an element $a \in \mathbb{Q}_{11}$ such that $a^2 = -7$. Since $|-7|_{11} = 1$, we know that -7 is a unit; so since the absolute value is multiplicative, if a exists it will be a unit as well. Thus the 11-adic expansion of a is of the form $a = a_0 + a_1 \cdot 11 + a_2 \cdot 11^2 + \cdots$

with $a_0 \neq 0$. We claim that the 11-adic expansion of -7 is

$$-7 = 4 + 10 \cdot 11 + 10 \cdot 11^2 + 10 \cdot 11^3 + 10 \cdot 11^4 + \cdots .$$

To see why, we add 7 to this expansion to get

$$\begin{aligned}
7 + (-7) &= 7 + (4 + 10 \cdot 11 + 10 \cdot 11^2 + 10 \cdot 11^3 + 10 \cdot 11^4 + \cdots) \\
&= \underbrace{11 + 10 \cdot 11}\, + 10 \cdot 11^2 + 10 \cdot 11^3 + 10 \cdot 11^4 + \cdots \\
&= (1 + 10) \cdot 11 + 10 \cdot 11^2 + 10 \cdot 11^3 + 10 \cdot 11^4 + \cdots \\
&= \underbrace{11 \cdot 11 + 10 \cdot 11^2}\, + 10 \cdot 11^3 + 10 \cdot 11^4 + \cdots \\
&= (1 + 10) \cdot 11^2 + 10 \cdot 11^3 + 10 \cdot 11^4 + \cdots \\
&= \underbrace{11 \cdot 11^2 + 10 \cdot 11^3}\, + 10 \cdot 11^4 + \cdots \\
&\cdots \\
&= 0.
\end{aligned}$$

Thus we are trying to solve the following equation:

$$(a_0 + a_1 \cdot 11 + a_2 \cdot 11^2 + \cdots)^2 = 4 + 10 \cdot 11 + 10 \cdot 11^2 + 10 \cdot 11^3 + \cdots . \qquad (1.1)$$

Let us start by examining (1.1) as a congruence modulo 11. We have

$$a_0^2 \equiv 4 \pmod{11},$$

and so $a_0 = 2$ or 9. Let us take $a_0 = 2$. Now we solve (1.1) as a congruence modulo

11^2:

$$(a_0 + a_1 \cdot 11)^2 \equiv 4 + 10 \cdot 11 \pmod{11^2}$$
$$a_0^2 + 2a_0a_1 \cdot 11 \equiv 4 + 10 \cdot 11 \pmod{11^2}$$
$$4 + 4a_1 \cdot 11 \equiv 4 + 10 \cdot 11 \pmod{11^2}$$
$$4a_1 \cdot 11 \equiv 10 \cdot 11 \pmod{11^2}$$
$$4a_1 \equiv 10 \pmod{11}$$

We multiply both sides by 3 since it is the multiplicative inverse of 4 modulo 11. This gives

$$(3 \cdot 4)a_1 \equiv 3 \cdot 10 \pmod{11}$$
$$a_1 \equiv 30 \equiv 8 \pmod{11}.$$

We now have $a_1 = 8$. Continuing modulo 11^3 gives

$$(a_0 + a_1 \cdot 11 + a_2 \cdot 11^2)^2 \equiv 4 + 10 \cdot 11 + 10 \cdot 11^2 \pmod{11^3}$$
$$a_0^2 + 2a_0a_1 \cdot 11 + (2a_0a_2 + a_1^2) \cdot 11^2 \equiv 4 + 10 \cdot 11 + 10 \cdot 11^2 \pmod{11^3}$$
$$4 + 32 \cdot 11 + (4a_2 + 64) \cdot 11^2 \equiv 4 + 10 \cdot 11 + 10 \cdot 11^2 \pmod{11^3}$$
$$22 \cdot 11 + (4a_2 + 64) \cdot 11^2 \equiv 10 \cdot 11^2 \pmod{11^3}$$
$$2 \cdot 11^2 + 4a_2 \cdot 11^2 + 64 \cdot 11^2 \equiv 10 \cdot 11^2 \pmod{11^3}$$
$$4a_2 \cdot 11^2 \equiv -56 \cdot 11^2 \pmod{11^3}$$
$$4a_2 \equiv -56 \equiv 10 \pmod{11}.$$

Once again we multiply by 3.

$$(3 \cdot 4)a_2 \equiv 3 \cdot 10 \pmod{11}$$
$$a_2 \equiv 30 \equiv 8 \pmod{11}.$$

Therefore $a_2 = 8$.

By continuing in this fashion, we can find each coefficient in the 11-adic expansion of a. If we had chosen $a_0 = 9$ in the first step, we would have obtained another root of f. This other root is the additive inverse of the root a which we just found.

Unfortunately, this procedure does not always work. Consider the polynomial $g(x) = x^2 - 2$ in $\mathbb{Q}_5$. In order to find a root, we must solve the following equation:

$$(a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \cdots)^2 = 2. \tag{1.2}$$

To solve (1.2) modulo 5, we would need to find a_0 such that $a_0^2 \equiv 2 \pmod{5}$. Since 2 is not a quadratic residue modulo 5, there is no such a_0. Thus g has no roots in $\mathbb{Q}_5$.

The method that we have just demonstrated can be used in a more general fashion. Let $\hat{a}_0$ denote the canonical lift of an element of $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Q}_p$. If there is no $a_0 \in \mathbb{Z}/p\mathbb{Z}$ such that $f(\hat{a}_0) \equiv 0 \pmod{p}$, then f has no roots in $\mathbb{Q}_p$. Even more powerful than this fact is the following theorem, one of the most fundamental algebraic results about the p-adic numbers. It states that when certain conditions are met, we can guarantee that a polynomial has roots in $\mathbb{Q}_p$.

Theorem (Hensel's Lemma). Let $f(x) = c_0 + c_1x + c_2x^2 + \cdots c_nx^n$ be a polynomial whose coefficients are p-adic integers, and let $f'(x) = c_1 + 2c_2x + 3c_3x^2 + \cdots + nc_nx^{n-1}$

be the formal derivative of f. Suppose that there exists a p-adic integer a_0 such that

$$f(a_0) \equiv 0 \pmod{p}$$

and

$$f'(a_0) \not\equiv 0 \pmod{p}.$$

Then there exists a unique $a \in \mathbb{Z}_p$ such that

$$f(a) = 0 \qquad \text{and} \qquad a \equiv a_0 \pmod{p}.$$

The proof of this theorem shows that $a \in \mathbb{Z}_p$ exists by constructing a Cauchy sequence of integers which converges to it.

At the beginning of this section we were trying to find a root of $f(x) = x^2 + 7$ in $\mathbb{Q}_{11}$. The 11-adic integer $a_0 = 2$ gave us

$$f(2) = 2^2 + 7 \equiv 0 \pmod{11}$$

and

$$f'(2) = 2 \cdot 2 \not\equiv 0 \pmod{11},$$

guaranteeing the existence of a root a via Hensel's Lemma.

Chapter 2

Extensions of the Field $\mathbb{Q}_p$

2.1 Introduction

In this section we will discuss algebraic extensions of the field $\mathbb{Q}_p$. Our objective is to find an algebraic closure of $\mathbb{Q}_p$ which is also topologically complete. Such a field will be analogous to the algebraic closure $\mathbb{C}$ of the real numbers. We also introduce some properties of finite extensions of $\mathbb{Q}_p$. The reader should be prepared to encounter quite a bit of algebraic terminology, but we will try to introduce the necessary concepts as we go along.

2.2 Extending $|\cdot|_p$

The first thing we need to know is that any field K containing another field F is called a *field extension* of F, and we write K/F. If K is an extension of F, then K may be viewed as a vector space over F, and the *degree* of K/F, denoted $[K : F]$, is

the dimension of the vector space. In this paper we will primarily be concerned with *finite* field extensions, that is, field extensions of finite degree.

Example. Every element of the complex numbers $\mathbb{C}$ can be expressed as $a + bi$ for some real numbers a and b, so $\mathbb{C}$ can be viewed as a real vector space with basis $\{1, i\}$. Therefore $\mathbb{C}$ is an extension of $\mathbb{R}$ of degree two.

The notion of a vector space norm is closely related to the notion of an absolute value.

Definition. Let F be a field equipped with the absolute value $|\cdot|$, and let V be a vector space over F. A *norm* on V is a map $\|\cdot\| : V \to \mathbb{R}$ such that for any $x, y \in V$ and any scalar $a \in F$, the following properties hold:

1. $\|x\| \geq 0$ and $\|x\| = 0$ iff $x = 0$;
2. $\|ax\| = |a| \, \|x\|$; and
3. $\|x + y\| \leq \|x\| + \|y\|$ (the triangle inequality).

A norm induces a metric on its vector space in the same way that an absolute value induces a metric on its field. Therefore we can consider Cauchy sequences of vectors, which leads to the notion of equivalence of norms. We say that two norms are *equivalent* if any sequence of vectors is Cauchy with respect to the first norm if and only if it is Cauchy with respect to the second norm. Another characterization of equivalent norms is given by the following proposition.

Proposition. The norms $|\cdot|$ and $\|\cdot\|$ on a vector space V are equivalent if and only if there exist positive constants C_1 and C_2 such that

$$C_1 \, |x| \leq \|x\| \leq C_2 \, |x|$$

for each vector $x \in V$.

This is a standard result, the proof of which can be found, for example, in [4].

If F is a field equipped with the absolute value $|\cdot|$ and K is a finite extension of F, then any absolute value on K which coincides with $|\cdot|$ on elements of F is also a norm on K/F as a vector space.

Example. The standard absolute value on the field of complex numbers is defined by

$$|a + bi| = \sqrt{a^2 + b^2}.$$

For any real number $x \in \mathbb{C}$, we have $|x| = \sqrt{x^2} = |x|_\infty$. That is, the restriction of the norm $|\cdot|$ to $\mathbb{R}$ is just the usual absolute value on $\mathbb{R}$. Therefore $|\cdot|$ can also be viewed as a vector space norm on the vector space $\mathbb{C}/\mathbb{R}$.

The example above shows that the absolute value $|\cdot|$ on $\mathbb{R}$ extends to an absolute value on the larger field $\mathbb{C}$. We would like to know if we can similarly extend $|\cdot|_p$ to finite extensions of $\mathbb{Q}_p$. Moreover, we would like to know whether a given extension of the absolute value $|\cdot|_p$ is unique.

We will address the question of uniqueness first. Let $K/\mathbb{Q}_p$ be a finite field extension. An extension of $|\cdot|_p$ to K will be a norm on K as a $\mathbb{Q}_p$ vector space. It is well known (see, for example, [2]) that any two norms on a finite-dimensional vector space over a complete field are equivalent; we can use this result to arrive at the following proposition.

Proposition. If K is a finite field extension of $\mathbb{Q}_p$, then there is at most one absolute value on K extending the p-adic absolute value.

Proof. Suppose that $|\cdot|$ and $\|\cdot\|$ are two absolute values on K which extend the p-adic absolute value on $\mathbb{Q}_p$. Then $|\cdot|$ and $\|\cdot\|$ are both norms on K when it is considered as a vector space over $\mathbb{Q}_p$, and moreover they are equivalent as norms. There exist positive constants C_1 and C_2 such that

$$C_1 |x| \leq \|x\| \leq C_2 |x|$$

for each $x \in K$. But $x^n \in K$ for each positive integer n since K is a field. So we can replace x with x^n in the preceding inequality to obtain

$$C_1 |x^n| \leq \|x^n\| \leq C_2 |x^n| .$$

Since $|\cdot|$ and $\|\cdot\|$ are absolute values, they are multiplicative, and the inequality becomes

$$C_1 |x|^n \leq \|x\|^n \leq C_2 |x|^n ,$$

or

$$C_1^{1/n} |x| \leq \|x\| \leq C_2^{1/n} |x| .$$

This inequality holds for all values of n. As n approaches ∞, we have $C_1^{1/n} \to 1$ and $C_2^{1/n} \to 1$, so that

$$|x| \leq \|x\| \leq |x| .$$

This proves that $|x| = \|x\|$ for each $x \in K$, so the two absolute values are equal. $\square$

Establishing the existence of an absolute value extending $|\cdot|_p$ on a finite field extension $K/\mathbb{Q}_p$ is more difficult, and we will only outline the process here. The crucial fact that we will need is that there is a function $\mathbf{N}_{K/\mathbb{Q}_p} : K \to \mathbb{Q}_p$ called the *norm from K to $\mathbb{Q}_p$*. The term "norm" in this context is completely different from the vector

space norm; hopefully there will be no confusion. There are three equivalent ways to define the function $\mathbf{N}_{K/\mathbb{Q}_p}$, but we will stick to one of these definitions.

In what follows, we will need to know a few more facts about field extensions. First, an element $\alpha \in K$ is said to be *algebraic* over $\mathbb{Q}_p$ if it is a root of a nonzero polynomial with coefficients in $\mathbb{Q}_p$. In this case, there is a unique monic irreducible polynomial $f(x)$ with coefficients in $\mathbb{Q}_p$ which has α as a root. We call $f(x)$ the *minimal polynomial* of α over $\mathbb{Q}_p$, and $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]$ is equal to the degree of $f(x)$. In a finite field extension, every element is algebraic, so it makes sense to talk about the minimal polynomial of each of the elements. If $f(x)$ is the minimal polynomial for an element $\alpha \in K$, then all of the roots of $f(x)$ are known as the *conjugates* of α.

The *characteristic* of a field is the smallest positive integer n for which adding the multiplicative identity 1 to itself n times will yield the multiplicative identity 0, if such a number exists; otherwise the characteristic is zero. The field of p-adic numbers has characteristic zero since we can never obtain 0 by adding 1 to itself. Similarly, any field K containing $\mathbb{Q}_p$ has characteristic zero. Any extension of a field of characteristic zero is *separable*, that is, the minimal polynomial of any element has distinct roots. Therefore, if $K/\mathbb{Q}_p$ is a finite extension and $\alpha \in K$, the number of conjugates of α is equal to the degree of its minimal polynomial, which is $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p]$.

Any automorphism of K which induces the identity on the subfield $\mathbb{Q}_p$ is known as an *automorphism of the extension* $K/\mathbb{Q}_p$. If K is an algebraic closure of $\mathbb{Q}_p$ (i.e., if K contains all the roots of polynomials with coefficients in $\mathbb{Q}_p$), then any automorphism of $K/\mathbb{Q}_p$ will send an element $\alpha \in K$ to one of its conjugates. If $K/\mathbb{Q}_p$ is a *normal* extension, that is, if K contains the conjugates of each of its elements, then this along with the fact that $K/\mathbb{Q}_p$ is separable implies that the set of automorphisms of $K/\mathbb{Q}_p$ forms a group of order $[K : \mathbb{Q}_p]$, where the group operation is composition.

Definition. Let K be a finite normal field extension of $\mathbb{Q}_p$ and x an element of K. We define the *norm of x from K to $\mathbb{Q}_p$* by

$$\mathbf{N}_{K/\mathbb{Q}_p}(x) = \prod_{k=1}^{n} \sigma_k(x),$$

where the σ_k are the automorphisms of $K/\mathbb{Q}_p$ and $n = [K : \mathbb{Q}_p]$.

Note that the definition above requires that the extension $K/\mathbb{Q}_p$ is normal. If the extension is not normal, we can still define the norm by considering a larger field L such that $[L : \mathbb{Q}_p]$ is normal and taking the product over the distinct embeddings of K in L; there will turn out to be exactly n such embeddings.

A useful thing to note here is that if we have a finite normal extension $K/\mathbb{Q}_p$ and an element $a \in \mathbb{Q}_p$, then $\sigma(a) = a$ for any automorphism of $K/\mathbb{Q}_p$. Therefore $\mathbf{N}_{K/\mathbb{Q}_p}(a) = a^n$, where n is the degree of the extension. It is also useful to note that for any $\alpha \in K$, $\mathbf{N}_{K/\mathbb{Q}_p}(\alpha)$ will belong to $\mathbb{Q}_p$. This is not immediately obvious from the definition, but recall that the automorphisms of $K/\mathbb{Q}_p$ permute the roots of the minimal polynomial of α. It follows that $\mathbf{N}_{K/\mathbb{Q}_p}(\alpha)$ is some power of the product of the roots of the minimal polynomial of x. That is, $\mathbf{N}_{K/\mathbb{Q}_p}(\alpha) = \left((-1)^m a_0\right)^r$ for some positive integer r, where m is the degree of the minimal polynomial of x and a_0 is its constant term. It turns out (see [5]) that $r = [K : F(\alpha)]$ is the degree of K as an extension of $F(\alpha)$. Since $a_0 \in \mathbb{Q}_p$, it follows that $\mathbf{N}_{K/\mathbb{Q}_p}(\alpha) \in \mathbb{Q}_p$ as well.

Example. We showed in section 1.6 that the polynomial $g(x) = x^2 - 2$ has no roots in $\mathbb{Q}_5$. The two roots of $g(x)$ exist in a larger field which contains $\mathbb{Q}_5$; let us call them $\sqrt{2}$ and $-\sqrt{2}$. The extension $\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5$ is normal of degree two, and $g(x)$ is the minimal polynomial of $\sqrt{2}$. There are two automorphisms of $\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5$, and each is completely determined by the image of $\sqrt{2}$. Moreover, $\sqrt{2}$ must be sent to one of

its conjugates, which are itself and $-\sqrt{2}$. Now $\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5$ is a vector space over $\mathbb{Q}_5$ with basis $\{1, \sqrt{2}\}$, so any element of $\mathbb{Q}_5(\sqrt{2})$ can be written uniquely as $a + b\sqrt{2}$. The two automorphisms of $\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5$ are given by

$$a + b\sqrt{2} \mapsto a + b\sqrt{2} \quad \text{and} \quad a + b\sqrt{2} \mapsto a - b\sqrt{2}.$$

The norm of $a + b\sqrt{2}$ from $\mathbb{Q}_5(\sqrt{2})$ to $\mathbb{Q}_5$ is therefore given by

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

Recall that we are looking for an absolute value extending $|\cdot|_p$ on a finite field extension $K/\mathbb{Q}_p$. We can use the norm of an extension of $\mathbb{Q}_p$ to figure out how to define such an absolute value. Consider a normal extension $K/\mathbb{Q}_p$ and an element $\alpha \in K$. If $|\cdot|$ is an absolute value on K which extends $|\cdot|$, then so is $|\sigma(\cdot)|$, where σ is an automorphism of $K/\mathbb{Q}_p$. Indeed, the properties of an absolute value are easily verified: for any $x \in K$,

1. $|\sigma(x)| \geq 0$ (since $|\cdot|$ is an absolute value) and $|\sigma(x)| = 0$ iff $\sigma(x) = 0$ iff $x = 0$;
2. $|\sigma(xy)| = |\sigma(x)\sigma(y)| = |\sigma(x)|\,|\sigma(y)|$; and
3. $|\sigma(x + y)| = |\sigma(x) + \sigma(y)| \leq |\sigma(x)| + |\sigma(y)|$.

Moreover, since σ induces the identity on the subfield $\mathbb{Q}_p$, $|\sigma(a)| = |a| = |a|_p$ for any $a \in \mathbb{Q}_p$. We showed that there can only be one absolute value on K which extends $|\cdot|_p$, so we must have $|\sigma(\cdot)| = |\cdot|$. Now suppose $x \in K$ and note that $\left|\mathbf{N}_{K/\mathbb{Q}_p}(x)\right|_p$ is well defined since $\mathbf{N}_{K/\mathbb{Q}_p}(x) \in \mathbb{Q}_p$. We have

$$\left|\mathbf{N}_{K/\mathbb{Q}_p}(x)\right|_p = \left|\mathbf{N}_{K/\mathbb{Q}_p}(x)\right|$$

$$
\begin{aligned}
&= \left| \prod_{k=1}^{n} \sigma_k(x) \right| \\
&= \prod_{k=1}^{n} |\sigma_k(x)| \\
&= \prod_{k=1}^{n} |x| \\
&= |x|^n .
\end{aligned}
$$

Therefore, if an extension $|\cdot|$ of the p-adic absolute value exists on a field extension $K/\mathbb{Q}_p$, it must be given by

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

The next step would be to show that $\sqrt[n]{\left|\mathbf{N}_{K/\mathbb{Q}_p}(\,\cdot\,)\right|_p}$ really does define an absolute value on K. We will not go through the details here, but instead refer the reader to [7] or [12].

2.3 $\overline{\mathbb{Q}}_p$ and $\mathbb{C}_p$

A field F is said to be *algebraically closed* if every polynomial with coefficients in F has a root in F. The completion of $\mathbb{Q}$ with respect to the standard absolute value is $\mathbb{R}$, but $\mathbb{R}$ is not algebraically closed since, for example, the polynomial $f(x) = x^2 + 1$ has no roots in $\mathbb{R}$. If we adjoin $\sqrt{-1} = i$ we obtain $\mathbb{R}(i) = \mathbb{C}$, which turns out to be the algebraic closure of $\mathbb{R}$. The extension $\mathbb{C}/\mathbb{R}$ is finite (of degree two), and $\mathbb{C}$ is complete.

We want to find an analogue of $\mathbb{C}$ for the p-adic numbers. We begin by completing $\mathbb{Q}$ with respect to the p-adic absolute value to obtain $\mathbb{Q}_p$. It is easy to find examples

which prove that $\mathbb{Q}_p$ is not algebraically closed. For a given value of p, we can find a rational integer a which is not a square modulo p. By Hensel's Lemma it follows that a is not a square in $\mathbb{Q}_p$; thus the polynomial $f(x) = x^2 - a$ has no roots in $\mathbb{Q}_p$. For example, $g(x) = x^2 - 2$ has no roots in $\mathbb{Q}_5$ (cf. 1.6).

Recall that $|\cdot|_p$ has a unique extension to any finite field extension of $\mathbb{Q}_p$. The algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ is the union of all finite extensions, so it follows that $|\cdot|_p$ extends uniquely to $\overline{\mathbb{Q}}_p$ as well. As it turns out, $\overline{\mathbb{Q}}_p$ has infinite degree over $\mathbb{Q}_p$. Moreover, $\overline{\mathbb{Q}}_p$ is not complete, so it does not give us an analogue of $\mathbb{C}$. We won't prove these facts, but we should mention that the proof that $\overline{\mathbb{Q}}_p$ is not complete uses an important result called Krasner's Lemma. It says that if an element b is "close enough" to an element a (closer to a than any of a's conjugates) then a belongs to the field generated by b.

Theorem (Krasner's Lemma). Let a and b be elements of $\overline{\mathbb{Q}}_p$, and let $a_1, a_2, \ldots, a_n$ be the conjugates of a over $\overline{\mathbb{Q}}_p$ which are not equal to a itself. If b is closer to a than a_i for $1 \leq i \leq n$, that is if

$$|b - a|_p < |a_i - a|_p, \quad 1 \leq i \leq n,$$

then $\mathbb{Q}_p(a) \subset \mathbb{Q}_p(b)$.

Proof. In order to make the notation easier, let $K = \mathbb{Q}_p(b)$. We suppose for the sake of contradiction that $a \notin K$ and consider the extension $K(a)$. The degree $[K(a) : K]$ must be strictly larger than one, so a has at least one conjugate $a_i \neq a$ which is not contained in K. Thus there is an automorphism σ of the extension $\overline{K}/K$ which sends a to a_i. Since $b \in K$, $\sigma(b) = b$. We know, by the uniqueness of the extension of the

absolute value $|\cdot|_p$, that $|x|_p = |\sigma(x)|_p$ for all $x \in K(a)$. In particular,

$$|b-a|_p = |\sigma(b-a)|_p = |\sigma(b)-\sigma(a)|_p = |b-a_i|_p = |a_i-b|_p .$$

Therefore,

$$\begin{aligned} |a_i - a|_p &\leq \max\left\{|a_i-b|_p, |b-a|_p\right\} \\ &= |b-a|_p \\ &< |a_i-a|_p . \end{aligned}$$

This contradicts our hypothesis, so we conclude that $a \in K = \mathbb{Q}_p(b)$. This shows that $\mathbb{Q}_p(a) \subset \mathbb{Q}_p(b)$. □

We will rely on this same result later, in chapter 3.

At this point one might begin to worry whether a p-adic analogue of $\mathbb{C}$ exists. If we take the completion of $\overline{\mathbb{Q}}_p$, it is possible that the new field will not be algebraically closed. Potentially, the process of taking algebraic closures and topological completions could continue indefinitely, without us ever obtaining a field which is both closed and complete. However, this is not the case: when we complete $\overline{\mathbb{Q}}_p$ we obtain a field that is both algebraically closed and complete, and denote it $\mathbb{C}_p$.

The results presented in this section are worked out in detail in [7]. The diagram below provides a summary.

$\mathbb{C}_p$ algebraically closed and topologically complete

| *completion*

$\overline{\mathbb{Q}}_p$ algebraically closed but not complete

| *algebraic closure*

$\mathbb{Q}_p$ complete but not algebraically closed

| *completion*

$\mathbb{Q}$ neither algebraically closed nor complete

2.4 Properties of Finite Extensions

Let K be a finite extension of $\mathbb{Q}_p$ of degree n. By abuse of notation, we let $|\cdot|_p$ denote both the p-adic absolute value and its unique extension to an absolute value on K, given by the formula

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

Recall that the p-adic absolute value of a nonzero element of $\mathbb{Q}_p$ is of the form p^k for some $k \in \mathbb{Z}$. It follows immediately that the absolute value of a nonzero element of K is of the form $p^{k/n}$ for some $k \in \mathbb{Z}$. If $x \in \mathbb{Q}$ and $|x|_p = p^k$, then $-k$ is the p-adic ordinal of x. We can use this to extend the definition of ordinal to $\mathbb{Q}_p$ and to K.

Definition. Let K be a finite extension of the field $\mathbb{Q}_p$. For any nonzero $x \in K$, we define the p-adic ordinal of x, denoted $\mathrm{ord}_p(x)$, to be the unique rational number satisfying

$$|x|_p = p^{-\mathrm{ord}_p(x)}.$$

By convention we say that $\mathrm{ord}_p(0) = \infty$. Equivalently, we can use the formula

$$\mathrm{ord}_p(x) = \frac{1}{n} \mathrm{ord}_p \left(\mathbf{N}_{K/\mathbb{Q}_p}(x) \right),$$

where n is the degree $[K : \mathbb{Q}_p]$.

Example. Let us compute $\mathrm{ord}_5(1 + 4\sqrt{2})$ in $\mathbb{Q}_5(\sqrt{2})$. Recall from our example in section 2.2 that $[\mathbb{Q}_5(\sqrt{2}) : \mathbb{Q}_5] = 2$ and that the norm of $a + b\sqrt{2} \in \mathbb{Q}_5(\sqrt{2})$ is given by

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

We have

$$\mathbf{N}_{\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5}(1 + 4\sqrt{2}) = 1 - 2 \cdot 4 = -7,$$

hence, since $\mathrm{ord}_5(-7) = 0$,

$$\mathrm{ord}_5(1 + 4\sqrt{2}) = \frac{1}{2} \mathrm{ord}_5(-7) = 0.$$

For any $x \in K$, $|x|_p$ is the n^{th} root of the absolute value of some element of $\mathbb{Q}_p$. Therefore the image of $K^\times$, the nonzero elements of K, is contained in $\frac{1}{n}\mathbb{Z}$. The next proposition gives a better description of this image.

Proposition. Let K be a finite extension of $\mathbb{Q}_p$ of degree n. The image of $K^\times$ under the map ord_p is of the form $\frac{1}{e}\mathbb{Z}$, where e is a rational integer which divides n.

Proof. It is clear from our definition of ord_p that

$$\mathrm{ord}_p(xy) = \mathrm{ord}_p(x) + \mathrm{ord}_p(y)$$

for any $x, y \in K$. Therefore ord_p is a group homomorphism from the multiplicative group $K^\times$ to the additive group $\frac{1}{n}\mathbb{Z}$. We know that the image contains all of $\mathbb{Z}$, since the image of $\mathbb{Q}_p^\times$ does, and that it is a subgroup of $\frac{1}{n}\mathbb{Z}$. The nontrivial subgroups of $\frac{1}{n}\mathbb{Z}$ are of the form $\frac{1}{e}\mathbb{Z}$, where e divides n, so it follows immediately that the image of $K^\times$ is of this form. □

The integer e as given in the preceding proposition is important enough to deserve its own name.

Definition. Let K be a finite extension of $\mathbb{Q}_p$ of degree n, and let e be the unique integer satisfying

$$\mathrm{ord}_p(K^\times) = \frac{1}{e}\mathbb{Z}.$$

We say that e is the *ramification index* of K over $\mathbb{Q}_p$. The extension $K/\mathbb{Q}_p$ is said to be *unramified* if $e = 1$, and it is *ramified* if $e > 1$. If $e = n$ then the extension is said to be *totally ramified*.

Example. Suppose we want to compute the ramification index of $\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5$, which the reader will recall is an extension of degree two. We need to determine what values $\mathrm{ord}_5(a + b\sqrt{2})$ can have for $a + b\sqrt{2} \in \mathbb{Q}_5(\sqrt{2})$. We have

$$\mathrm{ord}_5(a + b\sqrt{2}) = \frac{1}{2}\,\mathrm{ord}_5\left(\mathbf{N}_{\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5}(a + b\sqrt{2})\right) = \frac{1}{2}\,\mathrm{ord}_5(a^2 - 2b^2).$$

Because of the squared terms in the quantity $a^2 - 2b^2$, it is clear that the highest power of 5 which divides $a^2 - 2b^2$ must be even. Therefore $\mathrm{ord}_5(a + b\sqrt{2})$ is an integer, and we conclude that the ramification index of $\mathbb{Q}_5(\sqrt{2})/\mathbb{Q}_5$ is $e = 1$. In other words, it is an unramified extension.

In section 1.3 we observed that any element of $\mathbb{Q}_p$ can be expressed as some power

of p times a p-adic unit: we can write any p-adic number a as $p^{\mathrm{ord}_p(a)}u$ for some $u \in \mathbb{Z}_p^\times$. The number p plays a special role since it is an element of $\mathbb{Q}_p$ with the smallest possible positive ordinal, $\mathrm{ord}_p(p) = 1$. To do something similar in a finite extension K of $\mathbb{Q}_p$, we need an element whose valuation is $\frac{1}{e}$.

Definition. Let $K/\mathbb{Q}_p$ be a finite extension with ramification index e. We say an element $\pi \in K$ is a *uniformizer* if $\mathrm{ord}_p(\pi) = \frac{1}{e}$.

We can describe the algebraic structure of the extension $K/\mathbb{Q}_p$ by defining an analogue to the p-adic integers. Let $\mathcal{O}$ denote the valuation ring consisting of elements of K with absolute value less than or equal to one. The units of $\mathcal{O}$, denoted $\mathcal{O}^\times$ are elements with absolute value equal to one. The unique maximal ideal of $\mathcal{O}$ is

$$\mathfrak{P} = \{x \in K : |x| < 1\}.$$

So if π is a uniformizer in K, then we can write any element $x \in K$ as $\pi^k u$ for some rational number k and $u \in \mathcal{O}^\times$. The quotient $\mathcal{O}/\mathfrak{P}$ is a field, and it is given a special name.

Definition. Let $K/\mathbb{Q}_p$ be a finite extension with valuation ring $\mathcal{O}$, and let $\mathfrak{P}$ be the unique maximal ideal of $\mathcal{O}$. The field $\mathcal{O}/\mathfrak{P}$ is known as the *residue field* of K.

It turns out that the residue field of a finite extension K of $\mathbb{Q}_p$ is always the finite field with p^f elements, denoted $\mathbb{F}_{p^f}$, where f is the integer defined by $ef = n$.

In studying the finite extensions of $\mathbb{Q}_p$, it is useful to look at irreducible polynomials over $\mathbb{Q}_p$. There is a standard result in field theory (given, for example, in [3]) which tells us that any extension of a field of characteristic zero can be obtained by adjoining the root of an irreducible polynomial. In the case of totally ramified extensions of

$\mathbb{Q}_p$, it is enough to consider only polynomials of a certain type.

Definition. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with coefficients in $\mathbb{Z}_p$. If $\text{ord}_p(a_k) \geq 1$ for $k \geq 0$ and $\text{ord}_p(a_0) = 1$, then we say that $f(x)$ is an *Eisenstein polynomial*.

It is well known (again, see [3]), that Eisenstein polynomials are irreducible.

Theorem (Totally Ramified Extensions of $\mathbb{Q}_p$). If $K/\mathbb{Q}_p$ is a totally ramified finite extension of $\mathbb{Q}_p$ of degree n and $\pi \in K$ is a uniformizer, then $K = \mathbb{Q}_p(\pi)$. Moreover, π is a root of an Eisenstein polynomial. In other words, the totally ramified finite extensions of $\mathbb{Q}_p$ are generated by Eisenstein polynomials.

Proof. Let π be a uniformizer, so that $\text{ord}_p(\pi) = \frac{1}{e} = \frac{1}{n}$. In other words, we have $|\pi|_p = p^{-1/n}$. Let $f(x)$ be the minimal polynomial for π over $\mathbb{Q}_p$, and suppose $f(x)$ has degree m. Recall that the absolute value of p is, by definition, given in terms of the norm $\mathbf{N}_{K/\mathbb{Q}_p}(\pi)$. Recall also, from our discussion in section 2.2, that $\mathbf{N}_{K/\mathbb{Q}_p}(\pi) = \big((-1)^m a_0\big)^r$, where $r = [K : \mathbb{Q}_p(\pi)]$. Therefore,

$$p^{-1/n} = |\pi|_p = \sqrt[n]{\left|\mathbf{N}_{K/\mathbb{Q}_p}(\pi)\right|_p} = |a_0|_p^{r/n}$$

Since a_0 is a p-adic number, its absolute value is an integer power of p. So looking at the equation above, we see that we must have $r = 1$ and $|a_0|_p = p^{-1}$. Standard field theory tells us that the degrees of field extensions are in a sense multiplicative, so we have

$$n = [K : \mathbb{Q}_p] = [K : \mathbb{Q}_p(\pi)][\mathbb{Q}_p(\pi) : \mathbb{Q}_p] = rm.$$

It follows that the degree of $f(x)$ is n, and the fact that $[K : \mathbb{Q}_p] = [\mathbb{Q}_p(\pi) : \mathbb{Q}_p]$ proves that $K = \mathbb{Q}_p(\pi)$. In order to prove that $f(x)$ is an Eisenstein polynomial, all that

remains is to show that $\text{ord}_p(a_i) \geq 1$ for each i and $\text{ord}_p(a_0) = 1$. Actually, since we showed that $|a_0|_p = p^{-1}$, it is immediate that $\text{ord}_p(a_0) = 1$. Now each conjugate $\sigma(\pi)$ of π is a root of $f(x)$, and it has the same absolute value as π. In particular, we have $|\sigma(\pi)|_p = p^{-1/n} < 1$. Since each of the coefficients of $f(x)$ are given by symmetric sums and products of its roots, we must have $|a_k|_p < 1$ for $k \geq 1$. Thus $\text{ord}_p(a_k) \geq 1$ for $k \geq 0$, and the proof is complete. □

The converse to this theorem is true as well. That is, if π is the root of an Eisenstein polynomial of degree n, then $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is an extension of degree n (since Eisenstein polynomials are irreducible), and by applying the definition of absolute value using $\mathbf{N}_{K/\mathbb{Q}_p}(\pi)$ we see that $|\pi|_p = p^{-1/n}$.

It turns out that the description of unramified extensions is even simpler.

Theorem (Unramified Extensions of $\mathbb{Q}_p$). For each positive integer n, there is exactly one unramified extension K of $\mathbb{Q}_p$ of degree n. If $\overline{f}(x)$ is an irreducible polynomial of degree n over the residue field $\mathbb{Z}/p\mathbb{Z}$ of $\mathbb{Q}_p$, and if $f(x)$ is a polynomial of degree n over $\mathbb{Q}_p$ which maps canonically onto $\overline{f}(x)$, then $f(x)$ generates K.

For the proof of the theorem, see [1]. It is interesting to note that the proof relies on Hensel's Lemma, which we introduced in section 1.6.

The two preceding theorems will both be useful in the next chapter.

Chapter 3

Extensions of $\mathbb{Q}_5$ of Degree Five

3.1 Introduction

In this chapter we present the main result of the paper. The aim is to illustrate a way to find all possible field extensions of $\mathbb{Q}_p$ of a given finite degree by doing so in a particular case. Here we will find the degree five extensions of $\mathbb{Q}_5$. Some of the techniques that we will use are well known in general, but they are perspicuously represented in our example.

3.2 Known Results

For a fixed prime number p, it is well known (see [9], for example) that there are only finitely many field extensions of $\mathbb{Q}_p$ of a given finite degree. The problem of determining the number of such extensions has been studied at length.

Krasner gives a formula for the number of extensions of $\mathbb{Q}_p$ of a given finite degree in [8], wherein he uses his famous lemma as a main tool. More generally, if $K/\mathbb{Q}_p$ is a finite extension, the formula gives the number of extensions of K of a given finite degree. Serre arrives at the same result using a different method in [13].

Providing a classification of all extensions of $\mathbb{Q}_p$ of a given degree is in general a complex problem, but in theory there exist methods for doing so. In the next section, we will present a classification in a particular case: the degree five extensions of $\mathbb{Q}_5$.

3.3 Degree Five Extensions of $\mathbb{Q}_5$

The goal of this section is to describe all of the extensions of $\mathbb{Q}_5$ of degree five. We will do so by finding a polynomial over $\mathbb{Q}_5$ which generates each extension. According to Krasner's formula, as described in [11], there are a total of 106 such extensions. Actually, the formula is broken down into several cases, according to the so called *discriminant* of the extension. The discriminant of a field is a numerical invariant that, loosely speaking, measures the size of the ring of integers of field.

Throughout this section, let $\overline{a}$ denote the canonical image of a 5-adic integer a in the finite field $\mathbb{Z}/5\mathbb{Z}$.

Let K be an extension of $\mathbb{Q}_5$ of degree five. Since the ramification index e must divide the degree, either we have $e = 1$, in which case the extension is unramified, or $e = 5$, in which case the extension is totally ramified.

Let us deal with the unramified case first. According to the last theorem of the previous chapter, there is only one unramified extension of degree five, and we can

find a polynomial which generates it by first finding polynomial over $\mathbb{Z}/5\mathbb{Z}$ of degree five which is irreducible. The following proposition shows that $x^5 + \overline{4}x + \overline{1}$ is such a polynomial.

Proposition. The polynomial $x^p - x + \overline{1}$ over $\mathbb{Z}/p\mathbb{Z}$ is irreducible.

Proof. Let α be a root of $x^p - x + \overline{1}$. In $\mathbb{Z}/p\mathbb{Z}$, we have $(\alpha + \overline{1})^p = \alpha^p + \overline{1}^p = \alpha^p + \overline{1}$. Therefore,

$$(\alpha + \overline{1})^p - (\alpha + \overline{1}) + \overline{1} = \alpha^p + \overline{1} - \alpha - \overline{1} + \overline{1} = \alpha^p - \alpha + \overline{1} = \overline{0},$$

showing that $\alpha + \overline{1}$ is also a root of $x^p - x + \overline{1}$. By iterating this argument, we find that $\alpha, \alpha + \overline{1}, \alpha + \overline{2}, \ldots, \alpha + \overline{p-1}$ are the p roots. Since the extensions of $\mathbb{Z}/p\mathbb{Z}$ obtained by adjoining each of these roots are clearly equal, these roots all have the same degree over $\mathbb{Z}/p\mathbb{Z}$. In particular, the minimal polynomials of these roots all have the same degree. Now $x^p - x + \overline{1}$ is the product of the minimal polynomials, and the degrees of the minimal polynomials add up to p. Thus the degree of each minimal — and therefore the degree of each root — is a divisor of p. There are two possibilities: either each root has degree one over $\mathbb{Z}/p\mathbb{Z}$, or else each root has degree p over $\mathbb{Z}/p\mathbb{Z}$. In the first case, each root would actually be an element of $\mathbb{Z}/p\mathbb{Z}$, which is impossible since $x^p - x + \overline{1}$ has no roots in $\mathbb{Z}/p\mathbb{Z}$. Indeed, for any $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ we have $\overline{a}^p = \overline{a}$, so

$$\overline{a}^p - \overline{a} + \overline{1} = \overline{a} - \overline{a} + \overline{1} = \overline{1} \neq \overline{0}.$$

Therefore, it must be the case that each root has degree p and that $x^p - x + \overline{1}$ is its minimal polynomial. We conclude that $x^p - x + \overline{1}$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$. □

Since $x^5 - x + \overline{1} = x^5 + \overline{4}x + \overline{1}$ is irreducible over $\mathbb{Z}/p\mathbb{Z}$, it follows that $x^5 + 4x + 1$ is

irreducible over $\mathbb{Q}_5$ and that it generates the unramified extension of $\mathbb{Q}_5$.

Now we turn to the totally ramified case. Per the theorem in section 2.4 about totally ramified extensions, it is sufficient to study Eisenstein polynomials. There are infinitely many Eisenstein polynomials, so we would like to start by finding sufficient conditions for two distinct polynomials to generate the same extension of $\mathbb{Q}_5$. The following original theorem provides such a condition.

Theorem. Suppose $f(x) = x^5 + ax^4 + bx^3 + cx^2 + dx + e$ and $g(x)$ are Eisenstein polynomials of degree five over $\mathbb{Q}_5$. Let $\pi_1, \pi_2, \pi_3, \pi_4, \pi_5$ denote the five roots of $f(x)$, and let β be a root of $g(x)$. Define

$$\sigma = \min\left\{\frac{9}{5},\ \frac{3}{5} + \mathrm{ord}_5(a),\ \frac{2}{5} + \mathrm{ord}_5(b),\ \frac{1}{5} + \mathrm{ord}_5(c),\ \mathrm{ord}_5(d)\right\}.$$

If $\mathrm{ord}_5\left(f(\beta)\right) > \frac{5}{4}\sigma$, then $\mathbb{Q}_5(\beta) = \mathbb{Q}_5(\pi_i)$ for some $i \in \{1, 2, 3, 4, 5\}$.

Proof. The product

$$(\pi_1 - \pi_2)(\pi_1 - \pi_3)(\pi_1 - \pi_4)(\pi_1 - \pi_5)$$

is equal to the derivative of $f(x)$ evaluated at π_1. Therefore, we have

$$\begin{aligned}\mathrm{ord}_5(\pi_1 - \pi_2) + \mathrm{ord}_5(\pi_1 - \pi_3) + \mathrm{ord}_5(\pi_1 - \pi_4) + \mathrm{ord}_5(\pi_1 - \pi_5)& \\ = \mathrm{ord}_5\left((\pi_1 - \pi_2)(\pi_1 - \pi_3)(\pi_1 - \pi_4)(\pi_1 - \pi_5)\right)& \\ = \mathrm{ord}_5(5\pi_1^4 + 4a\pi_1^3 + 3b\pi_1^2 + 2c\pi_1 + d).&\end{aligned}$$

Now we know that in general the ordinal of a sum is at least as large as the minimum

of the ordinals of each term, but in this case the expression is actually equal to

$$\begin{aligned}
&\min\left\{\mathrm{ord}_5(5\pi_1^4),\, \mathrm{ord}_5(4a\pi_1^3),\, \mathrm{ord}_5(3b\pi_1^2),\, \mathrm{ord}_5(2c\pi_1),\, \mathrm{ord}_5(d)\right\} \\
&\quad = \min\left\{\frac{9}{5},\, \frac{3}{5} + \mathrm{ord}_5(a),\, \frac{2}{5} + \mathrm{ord}_5(b),\, \frac{1}{5} + \mathrm{ord}_5(c),\, \mathrm{ord}_5(d)\right\} \\
&\quad = \sigma
\end{aligned}$$

This follows from the fact that, since $f(x)$ is an Eisenstein polynomial, π_1 is a uniformizer, i.e., an element of ordinal $\frac{1}{5}$. Each term of the sum contains a different power of π_1, hence when we factor out from the sum the largest possible power of π_1 — this power is equal to 5σ — we are left with a unit. Next we claim that

$$\mathrm{ord}_5(\pi_1 - \pi_2) = \mathrm{ord}_5(\pi_1 - \pi_3) = \mathrm{ord}_5(\pi_1 - \pi_4) = \mathrm{ord}_5(\pi_1 - \pi_5).$$

We arrive at this result by noting that the expressions

$$\begin{gathered}
(\pi_1 - \pi_2)(\pi_1 - \pi_3)(\pi_1 - \pi_4)(\pi_1 - \pi_5), \\
(\pi_2 - \pi_1)(\pi_2 - \pi_3)(\pi_2 - \pi_4)(\pi_2 - \pi_5), \\
(\pi_3 - \pi_1)(\pi_3 - \pi_2)(\pi_3 - \pi_4)(\pi_3 - \pi_5), \\
(\pi_4 - \pi_1)(\pi_4 - \pi_2)(\pi_4 - \pi_3)(\pi_4 - \pi_5), \\
(\pi_5 - \pi_1)(\pi_5 - \pi_2)(\pi_5 - \pi_3)(\pi_5 - \pi_4)
\end{gathered}$$

all have the same ordinal, and that $\mathrm{ord}(\pi_i - \pi_j) = \mathrm{ord}(\pi_j - \pi_i)$ for each i and j. This implies that $\mathrm{ord}_5(\pi_1 - \pi_2) = \frac{1}{4}\sigma$. Clearly we have $\mathrm{ord}_5(\pi_i - \pi_j) = \frac{1}{4}\sigma$ for any indices $i \neq j$. Now Krasner's Lemma (see section 2.3), implies that $\mathbb{Q}_5(\beta) \subset \mathbb{Q}_5(\pi_i)$ whenever $\mathrm{ord}_5(\beta - \pi_i) > \frac{1}{4}\sigma$. Since $\mathbb{Q}_5(\beta)$ and $\mathbb{Q}_5(\pi_i)$ have the same degree in our

case, the two field extensions will actually be equal. We have

$$\mathrm{ord}_5\left(f(\beta)\right) = \mathrm{ord}_5(\beta-\pi_1)+\mathrm{ord}_5(\beta-\pi_2)+\mathrm{ord}_5(\beta-\pi_3)+\mathrm{ord}_5(\beta-\pi_4)+\mathrm{ord}_5(\beta-\pi_5),$$

so if $\mathrm{ord}_5\left(f(\beta)\right) > \frac{5}{4}\sigma$, then at least one of the terms on the right-hand side of the above equation must be greater than $\frac{1}{4}s$. This completes the proof. □

Let us divide all degree five Eisenstein polynomials into five sets as follows:

$$E_1 = \left\{x^5 + ax^4 + bx^3 + cx^2 + dx + e : \mathrm{ord}_5(d) = 1\right\}$$
$$E_2 = \left\{x^5 + ax^4 + bx^3 + cx^2 + dx + e : \mathrm{ord}_5(c) = 1; \mathrm{ord}_5(d) \geq 2\right\}$$
$$E_3 = \left\{x^5 + ax^4 + bx^3 + cx^2 + dx + e : \mathrm{ord}_5(b) = 1; \mathrm{ord}_5(c), \mathrm{ord}_5(d) \geq 2\right\}$$
$$E_4 = \left\{x^5 + ax^4 + bx^3 + cx^2 + dx + e : \mathrm{ord}_5(a) = 1; \mathrm{ord}_5(b), \mathrm{ord}_5(c), \mathrm{ord}_5(d) \geq 2\right\}$$
$$E_5 = \left\{x^5 + ax^4 + bx^3 + cx^2 + dx + e : \mathrm{ord}_5(a), \mathrm{ord}_5(b), \mathrm{ord}_5(c), \mathrm{ord}_5(d) \geq 2\right\}$$

For each $i \in \{1, 2, 3, 4, 5\}$, we will use the theorem above to find a finite subset A_i of E_i such that each polynomial in E_i is equivalent to one of the polynomials in A_i, in the sense that they generate the same extension of $\mathbb{Q}_5$.

Consider first the set E_1. For each polynomial in E_1 we have

$$\sigma = \min\left\{\frac{9}{5},\ \frac{3}{5} + \mathrm{ord}_5(a),\ \frac{2}{5} + \mathrm{ord}_5(b),\ \frac{1}{5} + \mathrm{ord}_5(c),\ 1\right\} = 1.$$

Suppose

$$f(x) = x^5 + a_1x^4 + b_1x^3 + c_1x^2 + d_1x + e_1$$

and

$$g(x) = x^5 + a_2x^4 + b_2x^3 + c_2x^2 + d_2x + e_2$$

are both in E_1, and let β be any root of $g(x)$. According to the theorem above, if $\mathrm{ord}_5\big(f(\beta)\big) > \frac{5}{4}s = \frac{5}{4}$, then there is a root of $f(x)$ which generates the same extension of $\mathbb{Q}_5$ as β does. Now

$$\begin{aligned} f(\beta) &= (f-g)(\beta) \\ &= (a_1-a_2)\beta^4 + (b_1-b_2)\beta^3 + (c_1-c_2)\beta^2 + (d_1-d_2)\beta + (e_1-e_2), \end{aligned}$$

hence $\mathrm{ord}_5\big(f(\beta)\big)$ is at least as great as the minimum of

$$\tfrac{4}{5}+\mathrm{ord}_5(a_1-a_2),\ \tfrac{3}{5}+\mathrm{ord}_5(b_1-b_2),\ \tfrac{2}{5}+\mathrm{ord}_5(c_1-c_2),\ \tfrac{1}{5}+\mathrm{ord}_5(d_1-d_2),\ \mathrm{ord}_5(e_1-e_2).$$

Therefore, whenever each of these quantities is greater than $\frac{5}{4}$, $f(x)$ and $g(x)$ will generate the same extension. Equivalently, if

$$\begin{cases} \mathrm{ord}_5(a_1-a_2) \geq 1 \\ \mathrm{ord}_5(b_1-b_2) \geq 1 \\ \mathrm{ord}_5(c_1-c_2) \geq 1 \\ \mathrm{ord}_5(d_1-d_2) \geq 2 \\ \mathrm{ord}_5(e_1-e_2) \geq 2 \end{cases}$$

is fulfilled, i.e., if

$$\begin{cases} a_1 \equiv a_2 \pmod 5 \\ b_1 \equiv b_2 \pmod 5 \\ c_1 \equiv c_2 \pmod 5 \\ d_1 \equiv d_2 \pmod{5^2} \\ e_1 \equiv e_2 \pmod{5^2} \end{cases},$$

then $f(x)$ and $g(x)$ are equivalent. We know that the first three congruences always hold since the non-leading coefficients of an Eisenstein polynomial are all divisible by 5. We also know that polynomials in E_1 satisfy $\text{ord}_5(d) = 1$ and $\text{ord}_5(e) = 1$. Hence every polynomial in E_1 is equivalent to one in A_1, where

$$A_1 = \left\{x^5 + 5ux + 5v : u, v \in \{1, 2, 3, 4\}\right\}.$$

Now suppose $f(x)$ and $g(x)$ are in E_2. Polynomials in E_2 each give $\sigma = \frac{6}{5}$, so if $\text{ord}_5\left(f(\beta)\right) > \frac{5}{4}s = \frac{3}{2}$, then $f(x)$ and $g(x)$ generate the same extension of $\mathbb{Q}_5$. The condition $\text{ord}_5\left(f(\beta)\right) > \frac{3}{2}$ is equivalent to saying that

$$\begin{cases} \text{ord}_5(a_1 - a_2) \geq 1 \\ \text{ord}_5(b_1 - b_2) \geq 1 \\ \text{ord}_5(c_1 - c_2) \geq 2 \\ \text{ord}_5(d_1 - d_2) \geq 2 \\ \text{ord}_5(e_1 - e_2) \geq 2 \end{cases},$$

or

$$\begin{cases} a_1 \equiv a_2 \pmod 5 \\ b_1 \equiv b_2 \pmod 5 \\ c_1 \equiv c_2 \pmod{5^2} \\ d_1 \equiv d_2 \pmod{5^2} \\ e_1 \equiv e_2 \pmod{5^2} \end{cases}.$$

The first and second congruences always hold, and the fourth congruence is satisfied for all polynomials in E_2 since $\text{ord}_5(d) \geq 2$ in this case. We have $\text{ord}_5(c) = 1$ and

$\text{ord}_5(e) = 1$, so it follows that polynomials in E_2 are each equivalent to a polynomial in

$$A_2 = \left\{x^5 + 5ux^2 + 5v : u, v \in \{1, 2, 3, 4\}\right\}.$$

For polynomials in E_3 we have $\sigma = \frac{7}{5}$. Following the same scheme as above, we find that polynomials $f(x)$ and $g(x)$ in E_3 are equivalent if

$$\begin{cases} a_1 \equiv a_2 \pmod 5 \\ b_1 \equiv b_2 \pmod{5^2} \\ c_1 \equiv c_2 \pmod{5^2} \\ d_1 \equiv d_2 \pmod{5^2} \\ e_1 \equiv e_2 \pmod{5^2} \end{cases}$$

and that each member of E_3 is equivalent to a member of

$$A_3 = \left\{x^5 + 5ux^3 + 5v : u, v \in \{1, 2, 3, 4\}\right\}.$$

We find the sets A_4 and A_5 in a similar fashion, ultimately obtaining

$$A_4 = \left\{x^5 + 5ux^4 + 5v : u \in \{1, 2, 3, 4\} \text{ and } 1 \leq v \leq 24, 5 \nmid v\right\}$$

and

$$A_5 = \left\{x^5 + 5^2ux + 5v : u \in \{0, 1, 2, 3, 4\} \text{ and } 1 \leq v \leq 24, 5 \nmid v\right\}.$$

We now have a finite list of polynomials which generate all possible totally ramified degree five extensions of $\mathbb{Q}_5$, namely $A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$. By using some of the results given in [11], we find that the five groups A_1, A_2, A_3, A_4, A_5 contain polynomials of

different discriminants, and therefore two polynomials which are members of different groups cannot be equivalent. In particular, the polynomials in A_1 correspond to extensions of discriminant 5^5, those in A_2 correspond to extensions of discriminant 5^6, and those in A_3, A_4, and A_5 correspond to extensions of discriminant 5^7, 5^8, and 5^9, respectively.

However, it is possible that many of the polynomials in each of five groups still generate the same extension; this does in fact turn out to be the case. In order to eliminate the redundancies on our list, we turn to a method described in [11] for determining whether a polynomial has any roots in a given field. It utilizes Peter Panayi's root finding algorithm, [10].

We start with a polynomial $f(x)$ and let π be one of its roots. To determine whether another polynomial $g(x)$ has a root in $K = \mathbb{Q}_5(\pi)$, we apply the following algorithm. First let $g_0(x) = g(x)$, then define $g_0^{\#}(x) = g_0(x)/\pi^{5m}$, where m is the minimum of the ordinals of the coefficients of $g_0(x)$. In other words, to obtain $g_0^{\#}(x)$ we divide $g_0(x)$ by the largest power of π which divides them all: the greatest common divisor of the coefficients. Then reduce $g_0^{\#}(x)$ modulo π and let $\overline{g_0^{\#}}(x)$ denote its image as a polynomial over the residue field of K. Recall that the residue field is the field with p^f elements, where f is defined by $ef = 5$. Each of the cases that we will be working with are totally ramified extensions, so $e = 5$ and $f = 1$. That is, the residue field is just $\mathbb{Z}/5\mathbb{Z}$. At this point, we look for the roots of $\overline{g_0^{\#}}(x)$ in $\mathbb{Z}/5\mathbb{Z}$. If $g(x)$ has a root in K, then clearly there will exist a root of $\overline{g_0^{\#}}(x)$ in $\mathbb{Z}/5\mathbb{Z}$. So if $\overline{g_0^{\#}}(x)$ has no roots, then we conclude that $f(x)$ and $g(x)$ generate distinct extensions of $\mathbb{Q}_5$. Otherwise, for each root β_0 of $\overline{g_0^{\#}}(x)$ we define a new polynomial $g_1(x) = g_0^{\#}(\pi x + \hat{\beta}_0)$, where $\hat{\beta}_0$ denotes a lift of β_0 to the valuation ring $\mathcal{O}$ of K. We then repeat this procedure with $g_1(x)$ in place of $g_0(x)$. If we reach a point at which $\overline{g_k^{\#}}(x)$ is a nonconstant linear

polynomial, then we conclude that $g(x)$ has a root in K. It is possible through this same algorithm to obtain an approximation for each root.

Let us apply Panayi's algorithm to determine which of the polynomials in A_1 are equivalent. Set $f(x) = x^5 + 5hx + 5$, where h is equal to one of $1, 2, 3, 4$, and let π be a root of $f(x)$. This implies that $\pi^5 + 5h\pi + 5 = 0$, or $5 = \dfrac{-\pi^5}{h\pi + 1}$. Let $g(x) = x^5 + 5ux + 5v$ be another polynomial in A_1. We proceed as follows:

- Set $g_0(x) = g(x) = x^5 + 5ux + 5v = x^5 - \dfrac{u\pi^5}{h\pi + 1}x - \dfrac{v\pi^5}{h\pi + 1}$.
- Divide out the highest possible power of π (we can only divide out $\pi^0 = 1$ in this case) to get $g_0^{\#}(x) = x^5 - \dfrac{u\pi^5}{h\pi + 1}x - \dfrac{v\pi^5}{h\pi + 1}$.
- Reduce to $\mathbb{Z}/5\mathbb{Z}$ to obtain $\overline{g_0^{\#}}(x) = x^5$.
- There is only one root of $\overline{g_0^{\#}}(x) = x^5$, namely $\beta_0 = \overline{0}$.
- Define $g_1(x) = g_0^{\#}(\pi x + \hat{\beta}_0) = g_0^{\#}(\pi x) = \pi^5 x^5 - \dfrac{u\pi^6}{h\pi + 1}x - \dfrac{v\pi^5}{h\pi + 1}$.
- Divide out π^5, yielding $g_1^{\#}(x) = x^5 - \dfrac{u\pi}{h\pi + 1}x - \dfrac{v}{h\pi + 1}$.
- Reduce to $\mathbb{Z}/5\mathbb{Z}$ to get $\overline{g_1^{\#}}(x) = x^5 - \overline{v}$.
- The only root of $\overline{g_1^{\#}}(x)$ is $\beta_1 = \overline{v}$.
- Define $g_2(x) = g_1^{\#}(\pi x + \hat{\beta}_1) = g_1^{\#}(\pi x + v) = (\pi x + v)^5 - \dfrac{u\pi}{h\pi + 1}(\pi x + v) - \dfrac{v}{h\pi + 1}$. A little algebra allows us to rewrite this as

$$g_2(x) = \pi^5 x^5 - \frac{v\pi^9}{h\pi + 1}x^4 - \frac{2v^2\pi^8}{h\pi + 1}x^3 - \frac{2v^3\pi^7}{h\pi + 1}x^2 - \left(\frac{v^4\pi^6}{h\pi + 1} + \frac{u\pi^2}{h\pi + 1}\right)x - \left(\frac{(uv - hv^5)\pi}{h\pi + 1} + \frac{v - v^5}{h\pi + 1}\right).$$

Performing the next step will require a little more thought, because it is not immediately evident what power of π we can divide out of each of the terms of $g_2(x)$. Looking at the linear term indicates that we can divide out, at most, π^2, and each of the higher degree terms contain π^2 as well. Therefore, we focus on the constant term. Now $v - v^5$ is divisible by π^5 since it is divisible by 5: every element of $\mathbb{Z}/5\mathbb{Z}$ is congruent to its fifth power. So it boils down to whether or not $uv - hv^5$ is divisible by π. Actually, since u, v, h are all integers, we ask whether or not $uv - hv^5$ is divisible by 5. If so, then we divide out π^2 to get $g_2^{\#}(x)$, and when we reduce to the residue field in the next step of the algorithm we end up with a linear polynomial. This leads to the conclusion that if $uv - hv^5$ is divisible by 5, then $g(x)$ has one root in the field $\mathbb{Q}_5(\pi)$. If, on the other hand, $uv - hv^5$ is not divisible by 5, then we can only divide out π. Reducing to the residue field in this case yields a nonzero constant polynomial, i.e., a polynomial with no roots, and we conclude that $g(x)$ is not equivalent to $f(x)$. By examining the quantity $uv - hv^5$ for the various values of u, v, h, we see that

$$\begin{aligned}
x^5 + 5x + 5 \quad &\text{is equivalent to} \quad x^5 + 5ux + 5v \text{ iff } u = v; \\
x^5 + 10x + 5 \quad &\text{is equivalent to} \quad x^5 + 5ux + 5v \text{ iff } u = 2v; \\
x^5 + 15x + 5 \quad &\text{is equivalent to} \quad x^5 + 5ux + 5v \text{ iff } u = 3v; \\
x^5 + 20x + 5 \quad &\text{is equivalent to} \quad x^5 + 5ux + 5v \text{ iff } u = 4v.
\end{aligned}$$

Therefore, the four polynomials

$$x^5 + 5x + 5, \quad x^5 + 10x + 5, \quad x^5 + 15x + 5, \quad x^5 + 20x + 5$$

generate distinct extensions of $\mathbb{Q}_5$, and the field generated by any member of A_1 is equal to one of them. The algorithm also tells us that, for example, $x^5 + 5x + 5$ only has a single root in the field generated by one of its roots. In other words, it does

not generate a normal extension. This means that each of the four polynomials listed above generates five distinct but isomorphic extensions.

Applying Panayi's algorithm to the polynomials in A_2 and in A_3 works out to be nearly identical to the case we just did, so we will not recount the tedious details here. Instead, we will simply state the results. It turns out that every member of A_2 is equivalent to one of

$$x^5 + 5x^2 + 5, \quad x^5 + 10x^2 + 5, \quad x^5 + 15x^2 + 5, \quad x^5 + 20x^2 + 5.$$

Moreover, these polynomials are not equivalent to one another, and each one generates five isomorphic extensions of $\mathbb{Q}_5$. Similarly, every member of A_3 is equivalent to one of

$$x^5 + 5x^3 + 5, \quad x^5 + 10x^3 + 5, \quad x^5 + 15x^3 + 5, \quad x^5 + 20x^3 + 5.$$

Once again, these four polynomials are not equivalent to one another, and each one generates five isomorphic extensions of $\mathbb{Q}_5$.

We now turn to the group A_4. Applying Panayi's algorithm here turns out to be more difficult than in the previous cases. Set $f(x) = x^5 + 5hx^4 + 5$, where h is equal to one of $1, 2, 3, 4$, and let π be a root of $f(x)$. This implies that $\pi^5 + 5h\pi^4 + 5 = 0$, or $5 = \dfrac{-\pi^5}{h\pi^4 + 1}$. Let $g(x) = x^5 + 5ux^4 + 5v$ be another polynomial in A_4. The steps of the algorithm are as follows:

- $g_0(x) = g(x) = x^5 + 5ux^4 + 5v = x^5 - \dfrac{u\pi^5}{h\pi^4 + 1}x - \dfrac{v\pi^5}{h\pi^4 + 1}$.
- $g_0^{\#}(x) = x^5 - \dfrac{u\pi^5}{h\pi^4 + 1}x^4 - \dfrac{v\pi^5}{h\pi^4 + 1}$.
- $\overline{g_0^{\#}}(x) = x^5$.

- $\beta_0 = \overline{0}$.
- $g_1(x) = g_0^{\#}(\pi x + \hat{\beta}_0) = g_0^{\#}(\pi x) = \pi^5 x^5 - \dfrac{u\pi^9}{h\pi^4+1}x - \dfrac{v\pi^5}{h\pi^4+1}$.
- $g_1^{\#}(x) = x^5 - \dfrac{u\pi^4}{h\pi^4+1}x - \dfrac{v}{h\pi^4+1}$.
- $\overline{g_1^{\#}}(x) = x^5 - \overline{v}$.
- $\beta_1 = \overline{v}$.
- $g_2(x) = g_1^{\#}(\pi x + \hat{\beta}_1) = g_1^{\#}(\pi x + v)$
$$= \pi^5 x^5 - \left(\frac{v\pi^9}{h\pi^4+1} + \frac{u\pi^8}{h\pi^4+1}\right)x^4 - \left(\frac{2v^2\pi^8}{h\pi^4+1} + \frac{4uv\pi^7}{h\pi^4+1}\right)x^3$$
$$- \left(\frac{2v^3\pi^7}{h\pi^4+1} + \frac{6uv^2\pi^6}{h\pi^4+1}\right)x^2 - \left(\frac{v^4\pi^6}{h\pi^4+1} + \frac{4uv^3\pi^5}{h\pi^4+1}\right)x$$
$$- \left(\frac{(uv^4 - hv^5)\pi}{h\pi^4+1} + \frac{v - v^5}{h\pi+1}\right).$$

At this point we find that if $uv^4 - hv^5$ is not divisible by 5, then $g(x)$ is not equivalent to $f(x)$. If $uv^4 - hv^5$ is divisible by 5, then we define s and t by $5s = v - v^5$ and $5t = uv^4 - hv^5$ and continue the algorithm by dividing out π^5:

- $g_2^{\#}(x) = x^5 - \left(\dfrac{v\pi^4}{h\pi^4+1} + \dfrac{u\pi^3}{h\pi^4+1}\right)x^4 - \left(\dfrac{2v^2\pi^3}{h\pi^4+1} + \dfrac{4uv\pi^2}{h\pi^4+1}\right)x^3$
$$- \left(\frac{2v^3\pi^2}{h\pi^4+1} + \frac{6uv^2\pi}{h\pi^4+1}\right)x^2 - \left(\frac{v^4\pi}{h\pi^4+1} + \frac{4uv^3}{h\pi^4+1}\right)x$$
$$+ \left(\frac{t\pi^4}{h\pi^4+1} + \frac{s}{h\pi+1}\right).$$
- $\overline{g_2^{\#}}(x) = x^5 - \overline{4}\overline{u}\overline{v}^3 x + \overline{s}$.

The root(s) of $\overline{g_2^{\#}}(x)$ depend on the value of h. We define $j = 2$ if $k = 1$, $j = 3$ if $k = 2$, or $j = 1$ if $k = 3$. Then for k equal to 1, 2, or 3, there is a single root to $\overline{g_2^{\#}}(x)$ given by $\beta_2 = \overline{j}\overline{s}$. Resuming the algorithm in these three cases produces a lengthy expression for $g_3(x)$ in which the highest power of π present in the nonconstant terms

is just π. The constant term of $g_3(x)$ is

$$-\frac{s - j^5 s^5 + 4uvjs}{(h\pi^4 + 1)^2}$$

plus a number of other expressions which all contain at least one power of π. It turns out that $g(x)$ is equivalent to $f(x)$ if and only if $s - j^5 s^5 + 4uvjs$ is divisible by 5.

For $k = 4$, we have an entirely different situation. In this case, $\overline{g_2^{\#}}(x)$ has no root if $\overline{s} \neq 0$, and if $\overline{s} = 0$ then each element of $\mathbb{Z}/5\mathbb{Z}$ is a root. This means that we must continue the algorithm for each of the five possible values of β_2. In doing so, we find five members of A_4 which are equivalent to $x^5 + 20x + 5$. Each polynomial has all five roots in the field K, so the extension generated by one of these polynomials is normal. We say that the extension is *cyclic* since the group of automorphisms of $K/\mathbb{Q}_5$ is isomorphic to the cyclic group $\mathbb{Z}/5\mathbb{Z}$ in this case. However, this still leaves us with several members of A_4 that are not equivalent to any of the polynomials identified up to this point. Therefore, we need to restart the algorithm from the beginning with $f(x) = x^5 + 20x^4 + 5k$, where k is one of the integers satisfying $1 \leq k \leq 24$ and $5 \nmid k$. We will omit the tedious steps of the algorithm and present the result.

The polynomials in A_4 are each equivalent to one of the following:

$$x^5 + 5x^4 + 5, \quad x^5 + 10x^4 + 5, \quad x^5 + 15x^4 + 5,$$
$$x^5 + 20x^4 + 5, \quad x^5 + 20x^4 + 30, \quad x^5 + 20x^4 + 55,$$
$$x^5 + 20x^4 + 80, \quad x^5 + 20x^4 + 105.$$

Moreover, each of these polynomials generates a different extension of $\mathbb{Q}_5$. The polynomials in the first row each generate five isomorphic extensions of $\mathbb{Q}_5$, while the polynomials in the second and third rows each generate a single cyclic extension.

For the polynomials in A_5, performing Panayi's algorithm is again tedious, and therefore we omit the calculations. What the algorithm shows is that the each member of A_5 is equivalent to one of

$$x^5 + 5, \quad x^5 + 25x + 5, \quad x^5 + 50x + 5, \quad x^5 + 75x + 5, \quad x^5 + 100x + 5,$$

that these polynomials are all distinct from one another, and that each one generates five isomorphic extensions of $\mathbb{Q}_5$.

To end this section, we point out that the number of extensions we found in each case is consistent with the numbers given by Krasner's formula: there are 20 extensions each of discriminant 5^5, 5^6, 5^7, and 5^8, and there are 25 extensions of discriminant 5^9.

3.4 Summary

We now summarize the results of the previous section.

There are a total of 106 field extensions of $\mathbb{Q}_5$ of degree five; up to isomorphism there are a total of 26 extensions. The polynomials which generate these extensions can be chosen as follows:

$$x^5 + 4x + 1, \tag{3.1}$$

$$x^5 + 5x + 5, \quad x^5 + 10x + 5, \quad x^5 + 15x + 5, \quad x^5 + 20x + 5 \tag{3.2}$$

$$x^5 + 5x^2 + 5, \quad x^5 + 10x^2 + 5, \quad x^5 + 15x^2 + 5, \quad x^5 + 20x^2 + 5 \tag{3.3}$$

$$x^5 + 5x^3 + 5, \quad x^5 + 10x^3 + 5, \quad x^5 + 15x^3 + 5, \quad x^5 + 20x^3 + 5 \tag{3.4}$$

$$x^5 + 5x^4 + 5, \quad x^5 + 10x^4 + 5, \quad x^5 + 15x^4 + 5, \tag{3.5}$$

$$x^5 + 20x^4 + 5, \quad x^5 + 20x^4 + 30, \quad x^5 + 20x^4 + 55, \tag{3.6}$$

$$x^5 + 20x^4 + 80, \quad x^5 + 20x^4 + 105 \tag{3.7}$$

$$x^5 + 5, \quad x^5 + 25x + 5, \quad x^5 + 50x + 5, \quad x^5 + 75x + 5, \quad x^5 + 100x + 5 \tag{3.8}$$

There is one unramified extension, given by the polynomial in 3.1. There are 20 totally ramified extensions of discriminant 5^5, given by the polynomials in 3.2. Each of these polynomials generates five isomorphic extensions. Similarly, there are 20 totally ramified extensions of discriminant 5^6, given by the polynomials in 3.3, and 20 extensions of discriminant 5^7, given by the polynomials in 3.4. The totally ramified extensions of discriminant 5^8 are of two types: 15 of the extensions, given by the polynomials in 3.5, are not normal; and five of the extensions, given by the polynomials in 3.6 and 3.7, are cyclic. Finally, there are 25 totally ramified extensions of discriminant 5^9, given by the polynomials in 3.8.

Bibliography

[1] Emil Artin. *Algebraic numbers and algebraic functions*. AMS Chelsea Publishing, Providence, RI, 2006. Reprint of the 1967 original.

[2] J. W. S. Cassels. *Local fields*, volume 3 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1986.

[3] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[4] Mariano Giaquinta and Giuseppe Modica. *Mathematical analysis*. Birkhäuser Boston Inc., Boston, MA, 2007. Linear and metric structures and continuity.

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

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

[7] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1984.

[8] Marc Krasner. Nombre des extensions d'un degré donné d'un corps p-adique. In *Les Tendances Géom. en Algèbre et Théorie des Nombres*, pages 143–169. Editions du Centre National de la Recherche Scientifique, Paris, 1966.

[9] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[10] Peter Panayi. *Computation of Leopoldt's p-adic Regulator*. PhD thesis, University of East Anglia, 1995. http://www.mth.uea.ac.uk/~h090/.

[11] Sebastian Pauli and Xavier-François Roblot. On the computation of all extensions of a p-adic field of a given degree. *Math. Comp.*, 70(236):1641–1659 (electronic), 2001.

[12] Alain M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[13] Jean-Pierre Serre. Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local. *C. R. Acad. Sci. Paris Sér. A-B*, 286(22):A1031–A1036, 1978.

[14] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.