APPLICATIONS OF PRIME FACTORIZATION OF IDEALS IN NUMBER FIELDS

BRIAN MCDONALD

CONTENTS

1. INTRODUCTION

For a number field K, that is, a finite extension of $\mathbb{Q}$, and a prime number p, a fundamental theorem of algebraic number theory implies that the ideal $(p) \subseteq \mathcal{O}_K$ factors uniquely into prime ideals as $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$. In this paper we explore different interpretations of this using the factorization of polynomials in finite and p-adic fields and Galois theory. In particular, we present some concrete applications for which these different interpretations are useful:

- We use the Cebotarev Density Theorem to prove Dirichlet's Theorem by computing the Frobenius element in a cyclotomic field in Section 3.1.
- We prove quadratic reciprocity in Section 3.2 by using two different methods to determine how a prime splits in a particular number field.
- We will also investigate in Section 3.3 under what conditions the existence of a rational root to a polynomial is guaranteed given a real root and a root in $\mathbb{Q}_p$ for each prime. This is known as the Hasse Principle, and we will show that it holds for irreducible polynomials in one variable, and also construct a counterexample to show that it doesn't hold for every polynomial in one variable.

Date: December 8, 2015.
2010 *Mathematics Subject Classification.* 11B39 (primary) 65Q30, 60B10 (secondary).

- Lastly, since many of our methods are made easier by working in a monogenic ring of integers, that is when $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α, in section 3.4 we will construct an example of a non-monogenic ring of integers to show that we can't hope to always be working in the simpler monogenic case.

Before getting to these applications we first collect some facts about the relationship between factorizations of polynomials over finite and p-adic fields and factorizations of a prime in a ring of integers in sections 2.1 and 2.2. We also build some machinery which we need to do arithmetic in the p-adic numbers, such as Hensel's lemma. Finally we discuss (in the Galois case) how Gal$(K/\mathbb{Q})$ acts on the primes lying above p in section 2.3, before moving on to the aforementioned applications.

2. Some Interpretations of a Prime Factorization

2.1. Number Fields and Ring of Integers.

Definition 2.1. *A **number field** K is a finite extension of $\mathbb{Q}$. Its **ring of integers**, $\mathcal{O}_K$, is the set of roots in K of monic polynomials in $\mathbb{Z}[x]$.*

As the name suggests, $\mathcal{O}_K$ is a ring (Theorem 2.1 of [2]). The motivation for calling $\mathcal{O}_K$ the ring of integers is that its relationship with K is similar to the relationship that $\mathbb{Z}$ has with $\mathbb{Q}$. In particular, $\mathbb{Z}$ is the ring of integers of $\mathbb{Q}$, and K is the field of fractions of $\mathcal{O}_K$.

Definition 2.2. *An integral domain that is not a field is called a* Dedekind domain *if every nonzero proper ideal I factors into prime ideals*

$$I = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_g^{e_g} \tag{2.1}$$

Theorem 2.3. *$\mathcal{O}_K$ is a Dedekind domain (Theorem 3.29 of* [2]*)*

Corollary 2.4. *For a number field K and a rational prime p, there is a unique factorization of (p) into prime ideals in $\mathcal{O}_K$ of the form*

$$(p) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_g^{e_g} \tag{2.2}$$

Definition 2.5. *In the notation of Theorem 2.4, we say that p* ramifies *in K if $e_j > 1$ for some j. Otherwise, we say p is* unramified*. Also, the* inertial degree *of $\mathfrak{p}_j$ is $[\mathcal{O}_K/\mathfrak{p}_j : \mathbb{Z}/p\mathbb{Z}]$*

As is suggested by the definition for inertial degree, $\mathcal{O}_K/\mathfrak{p}_j$ is a field, and is a finite extension of $\mathbb{Z}/p\mathbb{Z}$. We will address a few different ways to consider the factorization given by Corollary 2.4, as well as the relationship between them. We first consider the case when $\mathcal{O}_K = \mathbb{Z}[x]/f(x)$ for some $f(x)$ irreducible over $\mathbb{Q}$. That is, $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some α. We call such a ring monogenic. This begs the question: How often is the ring of integers of a number field monogenic? In sections 3.1 and 3.2 we will discuss a few problems in which it is useful to work in $K = \mathbb{Q}(\zeta_n)$, a cyclotomic field, in which case the ring of integers is monogenic, generated by a primitive nth root of unity. We also will deal with a few examples involving quadratic number fields, which are monogenic. One might ask whether there even exist any non-monogenic examples. It turns out that they do exist, and we will construct an example in section 3.4. In the monogenic case, there is a direct correspondence to the factorization of (p) in $\mathcal{O}_K$, and the factorization of $f(x)$ modulo p.

Theorem 2.6. *Suppose that $O_K = \mathbb{Z}[x]/f(x)$. If*

$$\begin{aligned} (p) &= \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_g^{e_g}, \\ f(x) &\equiv f_1(x)^{E_1} f_2(x)^{E_2}\cdots f_G(x)^{E_G} \ (\mathit{mod}\, p) \end{aligned} \tag{2.3}$$

are the factorizations of (p) and $f(x)$ in $\mathcal{O}_K$ and $\mathbb{F}_p$ respectively, then $g = G$, and up to some permutation we have $E_j = e_j$ and $\deg f_j$ is the inertial degree of $\mathfrak{p}_j$.

Proof. We prove our claim by directly constructing a prime factorization of (p), which then must be equal to the factorization in our hypothesis by the uniqueness of prime factorizations. Let $\mathfrak{q}_j = (p) + (F_j(\alpha))$, where α is a root of $f(x)$ and $F_j(x) \in \mathbb{Z}[x]$ reduces to $f_j(x)$ modulo p. These are prime ideals, as $\mathcal{O}_K/(p, F_j(\alpha)) \cong \mathbb{F}_p[x]/f_j(x)$, and the latter is a field since $f_j(x)$ is irreducible over $\mathbb{F}_p$. We see that the $\mathfrak{q}_j$ are the only primes lying above (p) by considering the correspondence between primes lying above (p) in $\mathcal{O}_K$ and primes in $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_p[x]/(f(x))$, and noting that the only maximal ideals in $\mathbb{F}_p[x]/(f(x))$, and hence the only prime ideals since in a finite ring all prime ideals are maximal, are $(f_j(x))$. Therefore we have, where S_r is the set of subsets of $\{1, 2, ..., k\}$ of size r,

$$\begin{aligned} \prod_j \mathfrak{q}_j^{e_j} &= \sum_{r=1}^{k}\left((p)^{k-r}\sum_{S\in S_r}\prod_{j\in S} F_j(\alpha)^{e_j}\right) \\ &= (p)\sum_{r=1}^{k-1}\left((p)^{k-r-1}\sum_{S\in S_r}\prod_{j\in S} F_j(\alpha)^{e_j}\right) + (F_1(\alpha)^{e_1}F_2(\alpha)^{e_2}\cdots F_G(\alpha)^{e_G}) \end{aligned} \tag{2.4}$$

Since the $\mathfrak{q}_j$ are the only primes lying above (p), we must have $\mathfrak{q}_j = \mathfrak{p}_j$ up to some permutation. Also, the coefficients e_j are the minimal integers such that (p) divides $(F_1(\alpha)^{E_1}\cdots F_G(\alpha)^{E_G})$. This gives $e_j = E_j$, since in $\mathbb{F}_p[x]/f(x)$ we have $\prod(f_j(x)^{E_j}) = 0$, and the E_j are minimal with that property. It only remains to show that the inertial degree of $\mathfrak{p}_j$ is $\deg f_j$. This is trivial, as $\deg f_j = [\mathbb{F}_p[x]/f_j(x) : \mathbb{Z}/p\mathbb{Z}] = [\mathcal{O}_K/\mathfrak{p}_j : \mathbb{Z}/p\mathbb{Z}]$. □

Another way to look at this factorization is to consider the canonical map $\mathcal{O}_K \to \mathcal{O}_K/p\mathcal{O}_K$. Since this map is surjective, there is a one-to-one correspondence between prime ideals in $\mathcal{O}_K$ containing (p) and prime ideals in $\mathcal{O}_K/p\mathcal{O}_K$. This correspondence is what motivates our choice of $(p)+(F_j(x))$ as a candidate for $\mathfrak{p}_j$.

Although this theorem only applies to the monogenic case, all hope is not lost in the non-monogenic case. Instead of factoring over $\mathbb{F}_p$, we will work in the field of p-adic numbers, $\mathbb{Q}_p$.

2.2. p-adic Numbers.

Definition 2.7. *If $m, n \in \mathbb{Z}$ are not divisible by p, and $x = p^k\frac{m}{n}$, then we can define a norm $|x| = p^{-k}$. We define the field of p-adic numbers, $\mathbb{Q}_p$, to be the completion of $\mathbb{Q}$ with respect to the metric induced by $|\cdot|$.*

We also give an alternate definition that is often used for $\mathbb{Z}_p$, and as before let $\mathbb{Q}_p$ be its field of fractions. First, we must define inverse limits for a sequence of ring homomorphisms.

Definition 2.8. *Suppose we have a sequence of rings with homomorphisms*

$$\cdots \to R_{n+1} \to R_n \to \cdots \to R_2 \to R_1 \tag{2.5}$$

*where $f_n : R_{n+1} \to R_n$. Then the **inverse limit** is the ring*

$$\lim_{\leftarrow} R_n := \left\{ (x_n)_n \in \prod_n R_n : f_n(x_{n+1}) = x_n \textit{ for all } n \right\} \tag{2.6}$$

with addition and multiplication defined as in $\prod_n R_n$.

Definition 2.9. *$\mathbb{Z}_p$ is the inverse limit*

$$\mathbb{Z}_p = \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z} \tag{2.7}$$

with the map $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ given by mapping each element to its residue modulo p^n.

We give both of these equivalent definitions because in some of our applications it will be useful to use them interchangeably. They are equivalent since the natural map $\mathbb{Z} \to \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$ can be extended to the completion of $\mathbb{Z}$ with respect to the p-adic metric because for any cauchy sequence in $\mathbb{Z}$, and for any n, from an index up every term of the sequence will have the same residue modulo p^n. Another useful way of thinking of a p-adic number $x \in \mathbb{Q}_p$ is by its unique representation as a formal power series

$$x = \sum_{j=-\infty}^{\infty} a_j p^j \tag{2.8}$$

where $a_j \in \{0, 1, ..., p-1\}$ and there exists some $n \in \mathbb{Z}$ such that $a_j = 0$ for all $j < n$.

In the following theorem, the inverse limit definition will be the most useful.

Theorem 2.10. *Let $K = \mathbb{Q}[x]/f(x)$. If $p\mathcal{O}_K = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_g^{e_g}$, and $f(x)$ factors over $\mathbb{Q}_p$ as $f(x) = f_1(x)\cdots f_G(x)$, then $g = G$, and up to a permutation $\deg f_j$ is the product of e_j and the inertial degree of $\mathfrak{p}_j$.*

Before proving this, we define a notion similar to $\mathbb{Q}_p$ for a number field K.

Definition 2.11. *For a number field K and a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, we define $K_\mathfrak{p}$ as the field of fractions of the inverse limit*

$$\lim_{\leftarrow} \mathcal{O}_K/\mathfrak{p}^n \tag{2.9}$$

We now prove the theorem.

Proof. (Theorem 2.10) Our proof boils down to writing $K \otimes \mathbb{Q}_p$ in two different ways. We first note that

$$K \otimes_\mathbb{Q} \mathbb{Q}_p = \mathbb{Q}[x]/f(x) \otimes_\mathbb{Q} \mathbb{Q}_p = \mathbb{Q}_p[x]/f(x) = \prod \mathbb{Q}_p[x]/f_i(x) \tag{2.10}$$

We may also write

$$\begin{aligned} K \otimes_{\mathbb{Q}} \mathbb{Q}_p &= (\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p)[1/p] = (\mathcal{O}_K \otimes_{\mathbb{Z}} \varprojlim \mathbb{Z}/p^n\mathbb{Z})[1/p] = (\varprojlim (\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z}))[1/p] \\ &= \varprojlim (\mathcal{O}_K/p^n\mathcal{O}_K)[1/p] = \left(\varprojlim \prod_{j=1}^{g} \mathcal{O}_K/\mathfrak{p}_j^n\right)[1/p] = \left(\prod_{j=1}^{g} \varprojlim \mathcal{O}_K/\mathfrak{p}_j^n\right)[1/p] \\ &= \prod_{j=1}^{g} K_{\mathfrak{p}_j} \end{aligned} \tag{2.11}$$

To see the third equality, consider the isomorphism

$$(\mathcal{O}_K \otimes_{\mathbb{Z}} \varprojlim \mathbb{Z}/p^n\mathbb{Z}) \to \varprojlim (\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z}) \tag{2.12}$$

given by mapping $x \otimes_{\mathbb{Z}} (a_n)_n$ to $(x \otimes_{\mathbb{Z}} a_n)_n$. This works because $\mathcal{O}_K$ is a $\mathbb{Z}$ module of finite rank. Now suppose that for fields F_j, E_j, we have $\prod_{j=1}^m F_j \cong \prod_{j=1}^n E_j$. Then considering the surjective map

$$\varphi : \prod_{j=1}^{m} F_j \to E_k \tag{2.13}$$

we note that its kernel must be a maximal ideal, hence for some ℓ it is $\prod_{j \neq \ell} F_j$, and thus we find $E_k \cong F_\ell$. Repeating this argument, we find that in fact $m = n$ and up to some permutation $F_j \cong E_j$. Applying this fact to the products

$$\prod \mathbb{Q}_p[x]/f_i(x) \cong \prod K_{\mathfrak{p}} \tag{2.14}$$

we conclude that $K_{\mathfrak{p}_j} \cong \mathbb{Q}_p[x]/f_j(x)$ up to some permutation. The conclusion about $\deg f_j$ follows from a more careful analysis of the relation between $\mathcal{O}_K$ and its completion at $\mathfrak{p}_j$, which we omit. □

2.3. **Galois Theory.** We now move on to a different perspective on these factorizations. Let $G = \text{Gal}(K/\mathbb{Q})$ for a Galois number field K, and recall that G acts transitively on the primes lying over p in $\mathcal{O}_K$. For such a prime $\mathfrak{p}$, we define the following subgroup of G:

Definition 2.12. *The* ***decomposition group*** *$D_{\mathfrak{p}}$ of $\mathfrak{p}$ is the group*

$$D_{\mathfrak{p}} = \{\sigma \in G : \sigma(\mathfrak{p}) = \mathfrak{p}\} \tag{2.15}$$

The crucial observation about this group is that since $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$ is a finite field of characteristic p, there is a natural homomorphism

$$\varphi : D_{\mathfrak{p}} \to \text{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p) \tag{2.16}$$

Since galois groups of finite extensions of finite fields are cyclic and generated by the frobenius map $x \mapsto x^p$, a lot of information about $D_{\mathfrak{p}}$, and hence a lot of information about the factorization of (p), can be obtained by knowing which elements of $D_{\mathfrak{p}}$ corresponds to the frobenius under the above natural map. We have a name for these elements:

Definition 2.13. *A* ***Frobenius Element*** *is any element of $D_{\mathfrak{p}}$ that maps to the frobenius under φ.*

Note that $\mathrm{Frob}_{\mathfrak{p}}$ has the property that $\mathrm{Frob}_{\mathfrak{p}}(x) - x^p \in \mathfrak{p}$ for all x. Another interesting thing to note about the map $\varphi : D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$ is that in the case where p is unramified, it is actually an isomorphism (Corollary 9.3.7 of [4]).

In an abuse of notation, we will use the term Frobenius element to mean what we specified above, as well as the following:

Definition 2.14. *For a prime p of $\mathbb{Z}$, The **Frobenius Element** $Frob_p$ is defined to be any element of the set*

$$Frob_p = \{Frob_{\mathfrak{p}} : \mathfrak{p}|(p)\} \tag{2.17}$$

Lemma 2.15. *If p is unramified, then $Frob_p$ is a conjugacy class in G*

Proof. This is a result of the fact that the Galois group acts transitively on the primes lying above p. It suffices to show that $\mathrm{Frob}_{\sigma(\mathfrak{p})} = \sigma \mathrm{Frob}_{\mathfrak{p}} \sigma^{-1}$. This is straightforward; for any $x \in \mathcal{O}_K$, we have

$$\mathrm{Frob}_{\mathfrak{p}}(\sigma^{-1}(x)) - \sigma^{-1}(x)^p \in \mathfrak{p} \tag{2.18}$$

And thus

$$\sigma \mathrm{Frob}_{\mathfrak{p}}(\sigma^{-1}(x)) - x^p \in \sigma\mathfrak{p} \tag{2.19}$$

And thus Frob_p is a conjugacy class in G. □

3. Applications

3.1. Dirichlet's Theorem is a Special Case of Cebotarev's Density Theorem.

For a number field K with $G := \mathrm{Gal}(K/\mathbb{Q})$, there is a theorem by Cebotarev concerning the distribution of the Frobenius element in G over the set of primes. First, we define a notion of the density of a subset of ther primes.

Definition 3.1. *We say that the set of primes $S \subseteq P$ has density δ if*

$$\lim_{n \to \infty} \frac{\# S \cap [1, n]}{\# P \cap [1, n]} = \delta \tag{3.1}$$

Theorem 3.2 (Cebotarev Density Theorem)**.** *For any conjugacy class $C \subseteq G$, the density of the set of primes whose Frobenius element is C is $\frac{|C|}{|G|}$.*

Proof. See Theorem 3.21 of [1]. □

This has a close relationship with Dirichlet's Theorem:

Corollary 3.3 (Dirichlet's Theorem)**.** *If $(m, n) = 1$, then the density of the set of primes p with $p \equiv m\ (mod\, n)$ is $1/\varphi(n)$.*

In fact, Dirichlet's Theorem is a special case of the Cebotarev Density Theorem corresponding to $K = \mathbb{Q}(\zeta_n)$.

Proof. Our first observation is that in the case $K = \mathbb{Q}(\zeta_n)$ of the Cebotarev Density Theorem, we have $G \cong (\mathbb{Z}/n\mathbb{Z})^*$, by identifying $a \in (\mathbb{Z}/n\mathbb{Z})^*$ with the map σ_a, the unique map sending ζ_n to ζ_n^a. As this group is abelian, each of its conjugacy classes is a single element. Hence, there are $\varphi(n)$ conjugacy classes, each with the same number of elements, so we are done if we can show that $p \equiv a \pmod{n}$ if and only if $\mathrm{Frob}_p = \{a\}$. Note that since we aim to prove a result about density in the set of primes, we may disregard what happens in any finite set, and thus we may safely assume that $(p, n) = 1$.

Now consider the map $\sigma_p \in G$ mapping ζ_n to ζ_n^p, and note that since $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$[3], any element can be written as $\sum_{j=0}^{\varphi(n)-1} \alpha_j \zeta_n^j$ for $\alpha_n \in \mathbb{Z}$, so modulo p we have

$$\sigma_p\left(\sum_{j=1}^{\varphi(n)-1} \alpha_j \zeta_n^j\right) \equiv \sum_{j=1}^{\varphi(n)-1} \alpha_j \zeta_n^{pj} \equiv \sum_{j=1}^{\varphi(n)-1} \alpha_j^p \zeta_n^{pj} \equiv \left(\sum_{j=1}^{\varphi(n)-1} \alpha_j \zeta_n^j\right)^p \tag{3.2}$$

The second congruence is because $\alpha_j^p \equiv \alpha_j \pmod{p}$ for any integer α_j, while the first and third congruences follow from the fact that $(a+b)^p = a^p + b^p$ in characteristic p. So by definition, σ_p must be the Frobenius element, and thus we are done. □

Corollary 3.4. *σ_p is the Frobenius element for p in K.*

3.2. A Proof of Quadratic Reciprocity.

Some facts we have proved about the Frobenius element can be used to prove in a very natural way the classic result of Quadratic Reciprocity, originally due to Gauss. To simplify notation, for p, q odd primes we set

$$p' = \begin{cases} p & p \equiv 3 \pmod{4} \\ -p & p \equiv 1 \pmod{4} \end{cases} \tag{3.3}$$

Note that this ensures $p' \equiv 3 \pmod{4}$. We will also define the Legendre symbol.

Definition 3.5. *The **Legendre Symbol** for an odd prime p is the function mapping an integer a to*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & : a \textit{ is a quadratic residue modulo } p \\ -1 & : a \textit{ is a quadratic non-residue modulo } p \\ 0 & : a \equiv 0 \ (\textit{mod}\ p) \end{cases} \tag{3.4}$$

A quadratic residue modulo p is an integer y such that for some x, we have $x^2 \equiv y$ (mod p).

An important property of the Legendre Symbol is that it is multiplicative in a. With this notation, quadratic reciprocity can be stated very succintly.

Theorem 3.6 (Quadratic Reciprocity)**.** *For any odd primes p, q, we have*

$$\left(\frac{q}{p}\right)\left(\frac{p'}{q}\right) = 1 \tag{3.5}$$

Proof. The key idea of this proof is to consider whether q splits in $\mathbb{Q}(\sqrt{p'})$ in two different ways. The first way is to compute the frobenius element for q in K.

First consider $\mathbb{Q}(\zeta_p)$, whose Galois group G over $\mathbb{Q}$ is cyclic of order $p-1$, and is generated by the map σ_a, the unique map sending ζ to ζ^a, where a is a primitive root modulo p. Then the squares in G form a subgroup of index 2, $H := \left\{\sigma_k : \left(\frac{k}{p}\right) = 1\right\}$. Let K be the fixed field of H, and note that by Galois theory it is a quadratic extension of $\mathbb{Q}$. Also,

$$P := \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/K}(\zeta) = \zeta + \zeta^4 + \zeta^9 + \cdots \tag{3.6}$$

is in K, where the sum is over the quadratic residues modulo p. Let

$$P' = \sum_{j \text{ nonresidue}} \zeta^j \tag{3.7}$$

and combining these sums we get a geometric series,

$$P + P' = \zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1 \tag{3.8}$$

Therefore, $P - P' \in K$. We also have

$$(P-P')^2 = \left(\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta^n\right)^2 = \sum_{m,n=1}^{p-1} \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \zeta^{m+n} \tag{3.9}$$

For a fixed m, as t ranges over $\{1, 2, ..., p-1\}$ so does mt (modulo p). Thus, we may replace n with mt in the above sum, obtaining

$$\begin{aligned}(P-P')^2 &= \sum_{m=1}^{p-1}\sum_{t=1}^{p-1} \left(\frac{m^2 t}{p}\right) \zeta^{m(1+t)} = \sum_{m=1}^{p-1}\sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \zeta^{m(1+t)} \\ &= \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \sum_{m=1}^{p-1} \zeta^{m(1+t)} \end{aligned} \tag{3.10}$$

But

$$\sum_{m=1}^{p-1} \zeta^{m(1+t)} = \begin{cases} -1 & : t \neq p-1 \\ p-1 & : t = p-1 \end{cases} \tag{3.11}$$

Thus

$$(P-P')^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{t=1}^{p-2} \left(\frac{t}{p}\right) = \left(\frac{-1}{p}\right) p = p' \tag{3.12}$$

And thus $\sqrt{p'} \in K$, so since K is a quadratic extension we may conclude that $K = \mathbb{Q}(\sqrt{p'})$. Therefore,

$$\left(\frac{q}{p}\right) = 1 \iff \sigma_q \in H \iff \sigma \text{ fixes } K = \mathbb{Q}(\sqrt{p'}) \tag{3.13}$$

By Corollary 3.4, σ_q is the Frobenius element of q in $\mathbb{Q}(\zeta_p)$. Then for any $x \in K$, since we have $\sigma_q(x) \equiv x^q \pmod{\mathfrak{q}}$ for any prime $\mathfrak{q}$ in $\mathbb{Z}[\zeta]$ lying above q, we see that for any prime $\mathfrak{q}'$ in $\mathcal{O}_K$ lying above q, we must similarly have $\sigma_q|_K(x) \equiv x^q \pmod{\mathfrak{q}'}$, and thus $\sigma_q|_K$ is the Frobenius element for q in K. Then $\sigma_q|_K$ has order $[\mathcal{O}_K/\mathfrak{q}' : \mathbb{Z}/q\mathbb{Z}]$, where $\mathfrak{q}'$ was any prime in $\mathcal{O}_K$ lying above q. Therefore, σ_q fixes K if and only if q splits completely in K.

Therefore, we are done if we can show that q splits completely in K if and only if $\left(\frac{p'}{q}\right) = 1$. Before we characterized whether q splits using the frobenius element, and now we will do it by factoring the minimal polynomial for $\frac{1+\sqrt{p'}}{2}$. Note that $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{p'}}{2}\right]$, since $p' \equiv 3 \pmod 4$. The minimal polynomial for $\frac{1+\sqrt{p'}}{2}$ is $f(x) = x^2 - x + \frac{1-p'}{4}$. We know from the correspondence established by Theorem 2.4 that q splits in K if and only if $f(x)$ factors modulo q, but the discriminant of $f(x)$ is p', so $f(x)$ factors modulo q exactly when $\left(\frac{p'}{q}\right) = 1$.

Through this chain of equivalences, we have thus established that $\left(\frac{q}{p}\right) = 1 \Leftrightarrow \left(\frac{p'}{q}\right) = 1$, thus quadratic reciprocity is proved.

□

3.3. **The Hasse Principle.**

The Hasse Principle says that for nice enough polynomials one can construct a solution over the rationals using solutions in the p-adics for every prime, as well as a real solution. This cannot be done for all polynomials.

Theorem 3.7. *The polynomial*

$$f(x) = (x^2 - 2)(x^2 + 7)(x^2 + 14) \tag{3.14}$$

has solutions in $\mathbb{Q}_p$ for every p, and also a real solution, yet no solutions in $\mathbb{Q}$.

Proof. Clearly it has real solutions and no rational ones, so it remains to show that it has a solution in the p-adic numbers $\mathbb{Q}_p$ for every p.

First consider any prime $p \neq 2, 7$ and note that there is a solution to $f(x)$ in $\mathbb{F}_p$ because if there is no solution to $x^2 - 2$ or $x^2 + 7$, that means that $\left(\frac{2}{p}\right) = \left(\frac{-7}{p}\right) = -1$, and thus $\left(\frac{-14}{p}\right) = 1$, so there is a solution to $x^2 + 14$ modulo p. We will use a version of Hensel's Lemma which will allow us to lift such a solution to a solution in $\mathbb{Q}_p$.

Lemma 3.8 (Hensel's Lemma). *For $f(x) \in \mathbb{Z}[x]$, if for some $a \in \mathbb{Z}_p$ we have $|f(a)| < |f'(a)|^2$, where $|\cdot|$ denotes the p-adic metric, then there exists some $\alpha \in \mathbb{Q}_p$ with $f(\alpha) = 0$ and $|\alpha - a| = |f(a)/f'(a)| < |f'(a)|$.*

Applying this lemma to each of the quadratic factors of $f(x)$, we know that $f(x)$ has a root in $\mathbb{Q}_p$, since at least one of $x^2 - 2$, $x^2 + 7$, and $x^2 + 14$ has a solution modulo p, and it will satisfy the hypotheses of Hensel's lemma for $p \neq 2, 7$. We now need only check $2, 7$. Since -7 is a square modulo 8, say $g(x) = x^2 + 7$, then we have $|g(1)| < 1/8 < 1/4 = |g'(1)|^2$. This ensures that there is a solution to $g(x)$, and hence a solution to $f(x)$ in $\mathbb{Q}_2$. Lastly we consider $\mathbb{Q}_7$. But for $h(x) = x^2 - 2$, note that $h(3) = 7$ and $h'(3) = 6$, so we easily see that there is a solution in $\mathbb{Q}_7$. □

Therefore, the Hasse Principle does not hold for $f(x)$, so we will have to be more picky than just hoping for it to hold for all polynomials. We now prove Hensel's Lemma.

Proof. (of Lemma 3.8) Recall Newton's method of approximation from calculus: with starting point a_0, we recursively define the sequence $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$. Unfortunately this won't always converge, but we know that when it does converge, its limit is a root of f. The analogous sequence in the setting of $\mathbb{Q}_p$ will always converge under our hypotheses, as we will see, thus we will be able to construct a root.

Set $a_0 = a$, and define the sequence $\{a_n\}_n$ in the same way as above. Set $t = \left|\frac{f(a_0)}{f'(a_0)^2}\right|$, and by hypothesis we have $t < 1$. We claim that for all n, we have that $a_n \in \mathbb{Z}_p$, $|f'(a_n)| = |f'(a_0)|$, and $|f(a_n)| \leq |f'(a_0)|^2 t^{2^n}$. We proceed by induction, noting that it is clear for the base case $t = 0$. Assuming that these facts are true for n, we see that

$$\left|\frac{f(a_n)}{f'(a_n)}\right| = |f(a_n)|/|f'(a_0)| \leq |f'(a_0)|t^{2^n} \leq 1 \tag{3.15}$$

and thus $f(a_n)/f'(a_n) \in \mathbb{Z}_p$, so $a_{n+1} \in \mathbb{Z}_p$ as well. To show that $|f'(a_n)|$ is constant, we note that for any polynomial $p(x)$, $x - y$ divides $p(x) - p(y)$, and thus for some $F(x, y) \in \mathbb{Z}_p$ we have

$$\begin{aligned}|f'(a_{n+1}) - f'(a_n)| &= |a_{n+1} - a_n||F(x,y)| \leq |a_{n+1} - a_n| = \frac{|f(a_n)|}{|f'(a_n)|} \\ &= \frac{|f(a_n)|}{|f(a_0)|} \leq |f'(a_0)|t^{2^n} < |f'(a_0)| = |f'(a_n)|\end{aligned} \tag{3.16}$$

Since $|x| < |y|$ implies $|y| = |x - y|$, we may conclude that in fact $|f'(a_{n+1})| = |f'(a_n)| = |f'(a_0)|$. Lastly, we need to prove that $|f(a_{n+1})| \leq |f'(a_0)|^2 t^{2^{n+1}}$. To see this, observe that for $f(x) = c_0 + c_1 x + \cdots + c_d x^d$, we have

$$\begin{aligned}f(x+y) &= c_0 + \sum_{j=1}^{d} c_j (x+y)^j = c_0 + \sum_{j=1}^{d} c_j (x^j + jx^{j-1}y + g(x,y)y^2) \\ &= f(x) + f'(x)y + g(x,y)y^2\end{aligned} \tag{3.17}$$

Thus,

$$\begin{aligned}f(a_{n+1}) &= f\left(a_n - \frac{f(a_n)}{f'(a_n)}\right) = f(a_n) - f'(a_n)\left(\frac{f(a_n)}{f'(a_n)}\right) + r\left(\frac{f(a_n)}{f'(a_n)}\right)^2 \\ &= r\left(\frac{f(a_n)}{f'(a_n)}\right)^2\end{aligned} \tag{3.18}$$

for some $r \in \mathbb{Z}_p$. Then we have

$$|f'(a_{n+1})| \leq \frac{|f(a_n)|^2}{|f'(a_n)|^2} = \frac{|f(a_n)|^2}{|f'(a_0)|^2} \leq |f(a_0)|^2 t^{2^{n+1}} \tag{3.19}$$

Thus by induction we have proved all three of our initial claims. Now all we need to do is prove the convergence of a_n. But with the above facts this is easy, as

$$|a_{n+1} - a_n| = \frac{|f(a_n)|}{|f'(a_n)|} = \frac{|f(a_n)|}{|f'(a_0)|} \leq |f'(a_0)| t^{2^n} \tag{3.20}$$

Thus we may conclude that $\{a_n\}$ is Cauchy and hence convergent, since

$$\sum_{j=m}^{n} t^{2^j} \leq \sum_{j=m}^{\infty} t^{2^j} \tag{3.21}$$

which can of course be made arbitrarily small by choosing m large enough, as it is the tail of a convergent series. Thus the sequence converges, and its limit $\alpha \in \mathbb{Q}_p$ must then be a root of $f(x)$. It remains to show that $|\alpha - a| = |f(a)/f'(a)| < |f'(a)|$. Note that $|a_1 - a| = |f(a)/f'(a)|$. For $n \geq 1$, we have by Eq 3.20 that

$$|a_{n+1} - a_n| \leq |f'(a)| t^{2^n} < |f'(a)| t = |f(a)/f'(a)| \tag{3.22}$$

If $|a_n - a| = |f(a)/f'(a)|$, then $|a_{n+1} - a| = |a_n - a| = |f(a)/f'(a)|$ since $|a_{n+1} - a_n| < |f(a)/f'(a)| = |a_n - a|$. By induction we conclude that $|a_n - a| = |f(a)/f'(a)|$ for all n, thus by taking limits we see that $|\alpha - a| = |f(a)/f'(a)| < |f'(a)|$. □

However, the Hasse Principle can be shown to hold for certain classes of polynomials.

Theorem 3.9 (Hasse Principle for Irreducibles). *If $f(x) \in \mathbb{Q}[x]$ is irreducible, has solutions in $\mathbb{Q}_p$ for each p, and has a real solution, then it must have a rational solution, hence must be linear.*

This theorem tells us that there are no nontrivial examples of irreducible polynomials with local solutions everywhere.

Proof. Let $\alpha \in \mathbb{R}$ be a root of $f(x)$. We will first prove the theorem assuming that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is Galois, that is $K := \mathbb{Q}(\alpha)$ is the splitting field of f over $\mathbb{Q}$. Note that viewing the Galois group G as a subgroup of S_n, where $n = \deg f$, the conjugacy classes of G are exactly the cycle types. If $K \neq \mathbb{Q}$, then G is nontrivial, so there is some nontrivial cycle cycle type in G, and thus by the Cebotarev density theorem there are infinitely many primes p which don't totally split in $\mathcal{O}_K$. In particular there is one such prime p, but this contradicts that $f(x)$ has a root in $\mathbb{Q}_p$.

Now we extend to the case where $\mathbb{Q}(\alpha)/\mathbb{Q}$ isn't Galois. Let L be the splitting field of $f(x)$, and $H = \text{Gal}(L/K) \subseteq G$. We note that if $f(x)$ has a root in $\mathbb{Q}_p$, this corresponds to a prime $\mathfrak{p}_j$ above p in K with $e_j = f_j = 1$. This implies that $\text{Frob}_{\mathfrak{p}_j} \in H$. But by Cebotarev Density Theorem, every conjugacy class in G is the Frobenius element for some prime, and thus every conjugacy class in G intersects H. But since G is a finite group, we get a contradiction by a counting argument, since this implies that $G = \bigcup_g gHg^{-1}$ where the union is taken over a set of coset representatives for G/H.

This is a union of $|G|/|H|$ sets, each of which has H elements, so since the union has $|G|$ elements, it must be a union of disjoint sets. However, the identity is in all of them, so this is not the case.

□

3.4. **Monogenic Rings of Integers.**

We now return to the problem of proving that there exist non-monogenic rings of integers. We first prove the following lemma:

Lemma 3.10. *If $\mathcal{O}_K$ is monogenic, say $\mathcal{O}_K = \mathbb{Z}[\alpha]$, and p splits completely in $\mathcal{O}_K$, then $[K : \mathbb{Q}] \leq p$.*

Proof. For each degree 1 prime $\mathfrak{p}$ lying above p we obtain the map $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p} = \mathbb{F}_p$, so the number of such maps is at least the number of primes lying above p, since they are all distinct as the map corresponding to $\mathfrak{p}$ has kernel $\mathfrak{p}$. But since each map is uniquely determined by its value at α, there are at most p such maps, hence there are at most p primes above (p). If p splits completely, then the number of primes above it is $[K : \mathbb{Q}]$, which then must be at most p. □

Therefore, if we can find a degree 3 extension in which 2 splits completely, then we know that it is not monogenic.

Theorem 3.11. *The number field $K = \mathbb{Q}[x]/g(x)$ is not monogenic, where*

$$g(x) = x^3 - 6x^2 + 27x - 6. \tag{3.23}$$

Proof. This is indeed a field, as $g(x)$ is irreducible by Eisenstein's criterion at 3. Also, it satisfies the hypotheses of Hensel's lemma with $p = 2$ and $a \in \{1, 2, 3\}$, so we may conclude that it has roots $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}_2$ with $|\alpha_k - k| < |g'(k)|$. We compute $|g'(1)| = |18| = 1/2$, $|g'(2)| = |15| = 1$, $|g'(3)| = |18| = 1/2$. Suppose $\alpha_i = \alpha_j$ for some $i \neq j$. Then we get

$$|i - j| = \max(|\alpha_i - i|, |\alpha_i - j|) = \max(|\alpha_i - i|, |\alpha_j - j|) < \max(|g'(i)|, |g'(j)|) \leq 1 \tag{3.24}$$

Since $|i - j| < 1$ and $i, j \in \{1, 2, 3\}$, i and j must be 1 and 3. Then

$$1/2 = |3 - 1| = |i - j| < \max(|g'(1)|, |g'(3)|) = 1/2 \tag{3.25}$$

This is a contradiction, so we may conclude that $\alpha_i = \alpha_j$ implies $i = j$, so $g(x)$ has 3 distinct roots in $\mathbb{Q}_2$. Therefore K is a degree 3 extension of $\mathbb{Q}$ in which 2 splits completely, so it isn't monogenic. □

The motivation for constructing $g(x)$ was to start with

$$f(x) = (x - 1)(x - 2)(x - 3) = x^3 - 6x^2 + 11x - 6 \tag{3.26}$$

and to perturb the coefficients by small amounts with respect to the 2-adic metric, while simultaneously obtaining a polynomial that is irreducible over $\mathbb{Q}$. One way to do this is to consider polynomials of the form $f(x) + 2^n x$, since Eisenstein's criterion applies whenever n is even.

Acknowledgments. It is my pleasure to thank my mentors, Sean Howe and Abigail Ward, for guiding me in finding a nice project this summer and for helping me learn some really pleasant mathematics. I would also like to thank Peter May for ensuring that the REU ran as smoothly as it did.

REFERENCES

[1] Milne, J.S. Ch. 5 in *Class Field Theory*. 1997
[2] Milne, J.S. Ch. 2,3 in *Algebraic Number Theory*.
[3] Neukirch, J. *Algebraic Number Theory*. Springer, 1999
[4] Stein, W. Ch. 9 in *Algebraic Number Theory, A Computational Approach*. 2012.