THE THEORY OF NUMBERS IN DEDEKIND RINGS

JOHN KOPPER

Abstract. This paper explores some foundational results of algebraic number theory. We focus on Dedekind rings and unique factorization of prime ideals, as well as some celebrated consequences such as a partial proof of Fermat's last theorem due to Kummer, and the law of quadratic reciprocity.

Contents

1. Introduction

It is not clear that the methods of algebra necessarily lend themselves to solving the problems of number theory. There are a few examples, though, that will serve as motivation for the rest of this paper, and indeed historically motivated a significant amount of the developments of algebraic number theory. These examples will exhibit some of the power of algebraic abstraction when applied to the ring $\mathbb{Z}$. Our first example is known as the *two squares theorem.*

Theorem 1.1. *(Two squares)A prime number p is the sum of two squares if and only if $p \equiv 1 \pmod 4$.*

In other words, we have a statement about solutions to the Diophantine equation $x^2 + y^2 = z$. In general, Diophantine equations are difficult to solve not because they involve multiplication, and not because they involve addition, but because they involve both. So in order to deal with this equation we may wish to factor the left side using complex numbers: $(x + iy)(x - iy) = z$. We are thus led to consider the ring $\mathbb{Z}[i]$. It is a fact that this ring, called the *Gaussian integers* is a principal ideal domain; in fact it is a Euclidean domain, and this is not difficult to prove: for any Gaussian integers z, w we may calculate z/w first in the field of complex numbers. Now it is easy to see geometrically that any complex number is within a distance of $\sqrt{2}/2$ from some Gaussian integer. Let y be a Gaussian integer within $\sqrt{2}/2$ of z/w. Then wy is a Gaussian integer such that $|z - wy| < w$.

Date: Aug 24, 2011.

Now let (p) denote the ideal generated by a prime integer p within the ring $\mathbb{Z}[i]$. Then $(p) = (q_1)(q_2)$ for prime ideals (q_1) and (q_2) if and only if

$$\begin{aligned} \mathbb{Z}[i]/(p) &= \mathbb{Z}[i]/((q_1)(q_2)) \\ &\cong \mathbb{Z}[i]/(q_1) \times \mathbb{Z}[i]/(q_2) \end{aligned}$$

is the product of two fields. But rewriting $\mathbb{Z}[i]$ as $\mathbb{Z}[X]/(X^2+1)$ we see that $\mathbb{Z}[i]/(p) = \mathbb{F}_p[X]/(X^2+1)$ is a product of fields if and only if X^2+1 has a root (mod p). Now $(\mathbb{F}_p)^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$, so -1 is a square in $\mathbb{F}_p$ if and only if $-1 \equiv (p-1)/2$ (mod $p-1$) is even. But this occurs if and only if $4 \mid (p-1) \iff p \equiv 1 \pmod 4$.

Assume $p \equiv 1 \pmod 4$. We can take norms so that $p^2 = N(p) = N(q_1)N(q_2)$. Then since p is prime and $N(q_1) > 1$, we have $p = N(q_1)$. But q_1 is a Gaussian integer $q_1 = x + iy$, and $N(q_1) = x^2 + y^2$, so p is the sum of two squares. This proves the theorem.

One may wish to prove similar theorems about solutions to Diophantine equations of the form $x^2 + ny^2 = p$ for primes p. It would be natural to apply a similar method and consider the ring $\mathbb{Z}[\sqrt{-n}]$. To do so, we need to characterize those primes which split into two distinct principal prime ideals. It is easy to characterize those which split into two prime ideals using the same method as above: it depends only on whether $-n$ is a square (mod p). Using the law of quadratic reciprocity (5.14) this becomes a congruence condition (mod $4n$). However, it can be very difficult to characterize those primes which split into *principal* prime ideals.

In the example of the two squares theorem it was easy because $\mathbb{Z}[i]$ is a Euclidean domain, hence a principal ideal domain. Thus the same argument will work for $x^2 + 2y^2 = p$ because $\mathbb{Z}[\sqrt{-2}]$ is also Euclidean. Unfortunately, this is not generally the case with $\mathbb{Z}[\sqrt{-n}]$. In fact, there is no guarantee that $\mathbb{Z}[\sqrt{-n}]$ is a unique factorization domain, much less a principal ideal domain, as we shall see in Section (2). The question of which primes are of the form $x^2 + ny^2$ then becomes quite difficult. We will not be able to solve this problem in this paper. Nevertheless, many of the methods used in solving the $x^2 + y^2 = z^2$ case—especially the use of ideals—will inform much of our discussion.

Another example, and a particularly salient motivation in the historical development of algebraic number theory is the diophantine equation

$$x^n + y^n = z^n$$

and the question, *for which n are there integer solutions for x, y and z?* The answer is Fermat's last theorem (1.2), a theorem which requires little introduction and less motivation. The theorem itself provides surprisingly little insight into other problems, even Diophantine problems. Much more valuable are the proof and the attempts to prove it. Essentially all of the mathematics in this paper, including the modern definitions, are somehow inspired by 20th century attempts to prove Fermat's last theorem.

In Section (2) we will introduce the notion of Dedekind rings and unique factorization of ideals. This leads naturally to the definition of the ideal class group and Kummer's partial proof of Fermat's last theorem in Section (3). Section (4) will be another application of the theory of Dedekind rings in the context of ramification theory. We will then use the abstraction of ramification combined with Galois theory to prove the law of quadratic reciprocity in Section (5). To begin, however, we will first introduce some of the historical background of Fermat's last theorem and elementary methods of trying to prove it.

Theorem 1.2. *The equation $x^n + y^n = z^n$ has no nontrivial integer solutions for $n \geq 3$.*

The first thing that should be noted when trying to prove this is that x, y, and z may be assumed to be relatively prime, since if d is a common divisor and $x^n + y^n = z^n$ then $(x/d)^n + (y/d)^n = (z/d)^n$.

Second, we may assume n is prime or a power of 2. To see this, suppose $n = pq$ is composite and $x^n + y^n = z^n$. Then $x^{pq} + y^{pq} = z^{pq}$, so x^q, y^q, and z^q solve the Fermat equation for $n = p$. It follows that we need only consider the cases where n is an odd prime or $n = 4$. Fermat himself is purported to have solved at least the $n = 3$ and $n = 4$ cases. In Section (3) we will prove a significantly weaker version of Fermat's last theorem; first, however we will need a great deal of algebraic machinery.

One of the more tantalizing aspects of Fermat's last theorem is Fermat's claim to have found a "marvelous" proof. It is generally considered unlikely that Fermat knew an actual proof because a complete proof wasn't published until a few years ago. Nevertheless, it's reasonable to assume that Fermat had discovered a partial proof. Siegel writes,

> "[Fermat] might have conceived the idea...of working in the ring of integers of the field containing the nth roots of unity; he may have believed that such a ring is always a principal ideal ring... For n prime, this ring is a principal ideal ring only for finitely many values of n."—C. L. Siegel (cf. Samuel [3] p. 15)

In particular, Fermat may have thought about cyclotomic extensions of $\mathbb{Q}$, and not without good reason. We may factor Fermat's equation as

$$\prod_{i=0}^{p-1}(x + \zeta_p^i y) = z^p \tag{1.3}$$

where ζ_p is a primitive pth root of unity. We will now suppress the subscript p. We shall soon see that the terms on the left side of Equation (1.3) are pair-wise relatively prime. Supposing $\mathbb{Z}[\zeta]$ were a unique factorization domain, we would have that $(x + \zeta^i y)$ is a pth power. From this we can derive a contradiction. Unfortunately, $\mathbb{Z}[\zeta]$ is not, in general, a unique factorization domain. In fact, the first prime p for which $\mathbb{Z}[\zeta_p]$ is not a unique factorization domain is $p = 23$.

2. Dedekind Rings

Consider the ring $\mathbb{Z}[\sqrt{-6}]$, and the element 6:

$$-3 \cdot 2 = -6 = \sqrt{-6} \cdot \sqrt{-6}.$$

But in $\mathbb{Z}[\sqrt{-6}]$, $\sqrt{-6}$ doesn't divide 3 or 2. We see that $\mathbb{Z}[\sqrt{-6}]$ is not a unique factorization domain. This discovery was sufficiently disturbing to Kummer and Dedekind who each sought ways to rectify it. Dedekind's ideas are the ones which are more closely adhered to today; he introduced the notion of ideals, which in many cases retain the property of unique factorization into primes. It is the object of this section to pursue the question of when specifically we can say that ideals in

a ring will factor uniquely into primes. But before we get to answer this question, we need some preliminary definitions and propositions.

Definition 2.1. Let R be a ring and K a field containing R. Then $\alpha \in K$ is *integral over* R if there exists a monic polynomial $P \in R[X]$ such that $P(\alpha) = 0$.

This paper will assume some familiarity with integrality and integral extensions. In particular, we shall assume without proof several facts about integral closures. The following proposition provides an alternate definition of integrality which will be useful in proving the main theorem of this section.

Proposition 2.2. *Let R be a ring and K a field containing R. Then $\alpha \in K$ is integral over R if and only if $R[\alpha]$ is finitely generated as an $R-$module.*

Proof. Clear. □

We ultimately wish to show that under the correct conditions ideals can be uniquely factored into prime ideals. These next two propositions provide relatively weak statements about containing products of ideals, and will be essential in proving unique factorization.

Proposition 2.3. *Let R be a Noetherian integral domain. If $\mathfrak{a}$ is a non-zero ideal of R, then it contains a product of non-zero prime ideals.*

Proof. Suppose not. Let $\mathscr{C}$ be the collection of non-zero ideals of R which do not contain a product of non-zero prime ideals. By assumption, $\mathscr{C}$ is not empty. Since R is Noetherian, there must be a maximal element $\mathfrak{m}$ of $\mathscr{C}$ with respect to set inclusion. Clearly $\mathfrak{m}$ is not prime. Thus there exist $a, b \in R - \mathfrak{m}$ such that $ab \in \mathfrak{m}$.

Now $\mathfrak{m} \subset \mathfrak{m} + Ra$ and $\mathfrak{m} \subset \mathfrak{m} + Rb$. By the maximality of $\mathfrak{m}$, there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{q}_1, \ldots, \mathfrak{q}_k$ such that

$$\mathfrak{m} + Ra \supset \mathfrak{p}_1 \cdots \mathfrak{p}_n$$
$$\mathfrak{m} + Rb \supset \mathfrak{q}_1 \cdots \mathfrak{q}_k$$

But $ab \in \mathfrak{m}$ implies $(\mathfrak{m} + Ra)(\mathfrak{m} + Rb) \subset \mathfrak{m}$, thus $\mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{q}_1 \cdots \mathfrak{q}_k \subset \mathfrak{m}$, a contradiction. □

Proposition 2.4. *Let R be a ring and $\mathfrak{p}$ a prime ideal of R. Suppose $\mathfrak{p}$ contains a product $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ of ideals. Then there is some i such that $\mathfrak{a}_i \subset \mathfrak{p}$.*

Proof. Suppose not. Then for each i there exists $a_i \in \mathfrak{a}_i - \mathfrak{p}$. Since $\mathfrak{p}$ is prime, it follows that $a_1 a_2 \cdots a_n \notin \mathfrak{p}$. But $a_1 a_2 \cdots a_n \in \mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_n \subset \mathfrak{p}$, a contradiction. □

To prove that ideals factor uniquely into prime ideals we need some assumptions on the ring in which the ideals reside; it is certainly not true in general that ideals can be uniquely factored. For example, consider the ring $\mathbb{Z}[\sqrt{-3}]$. Then the ideal (4) can be factored as $(2)(2)$ and $(1+\sqrt{-3})(1-\sqrt{-3})$. But these factorizations are distinct. The correct set of assumptions for unique factoriation of ideals are those of a *Dedekind ring*, defined below.

Definition 2.5. Let R be an integral domain and K its field of fractions. Then R is a *Dedekind ring* (or *Dedekind domain*) if the following properties hold.

(i) R is Noetherian.
(ii) R is integrally closed in K.
(iii) If $\mathfrak{p}$ is a non-zero prime ideal of R then $\mathfrak{p}$ is maximal.

It can be shown that any principal ideal domain is a Dedeking ring, but the converse is not true. However, we will see in the next section that most rings we are concerned with are Dedekind (cf. Proposition (3.2)). We require one last definition.

Definition 2.6. Let R be an integral domain and K its field of fractions. Then if $\mathfrak{a}$ is an $R-$submodule of K, it is called a *fractional ideal of* R if there exists a non-zero $r \in R$ such that $r\mathfrak{a} \subset R$. If $\mathfrak{a}$ and $\mathfrak{b}$ are both fractional ideals of R then we define the product $\mathfrak{ab}$ to be the set of all finite sums of the form $\sum a_i b_i$ such that $a_i \in \mathfrak{a}$ and $b_i \in \mathfrak{b}$.

Alternatively, one can define fractional ideals as an product $\mathfrak{a}k$ where $\mathfrak{a}$ is an ideal of R and $k \in K$. Note that fractional ideals aren't necessarily ideals, but all ideals of R are fractional ideals. Fractional ideals will be essential in proving the main theorem of this section, Theorem (2.9), as well as in defining the ideal class group which will be a valuable tool in later sections. We would like to show that fractional ideals form a group under multiplication with identity R.

Lemma 2.7. *Let R be a Dedekind ring which is not a field and K its field of fractions. Then for every maximal ideal $\mathfrak{m}$ of R there exists a fractional ideal $\mathfrak{m}^{-1}$ of R such that $\mathfrak{m}\mathfrak{m}^{-1} = R$.*

Proof. Since R is not a field, $\mathfrak{m} \neq (0)$. Define

$$\mathfrak{m}^{-1} = \{\alpha \in K : \alpha\mathfrak{m} \subset R\}. \tag{2.8}$$

Clearly $\mathfrak{m}^{-1}$ is an $R-$submodule, and if $0 \neq m \in \mathfrak{m}$ then $m\alpha \in R$ for all $\alpha \in \mathfrak{m}^{-1}$. Thus $\mathfrak{m}^{-1}$ is a fractional ideal. It remains to show $\mathfrak{m}\mathfrak{m}^{-1} = R$.

It is clear that $\mathfrak{m}\mathfrak{m}^{-1} \subset R$, and that $R \subset \mathfrak{m}^{-1}$, so $\mathfrak{m} \subset \mathfrak{m}\mathfrak{m}^{-1} \subset R$. But $\mathfrak{m}$ is maximal, so either (1) $\mathfrak{m}\mathfrak{m}^{-1} = R$, or (2) $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$. It therefore remains to show that (2) is impossible.

Suppose, for a contradiction, $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$. It follows that for all $\alpha \in \mathfrak{m}^{-1}$ and all $n \in \mathbb{N}$,

$$\begin{aligned} \alpha\mathfrak{m} &\subset \mathfrak{m} \\ \alpha^2\mathfrak{m} &\subset \mathfrak{m} \\ &\vdots \\ \alpha^n\mathfrak{m} &\subset \mathfrak{m}. \end{aligned}$$

Thus if r is a non-zero element of $\mathfrak{m}$, we have $r\alpha^n \in \mathfrak{m} \subset R$. That is, $R[\alpha]$ is a fractional ideal. Since R is Dedekind and therefore Noetherian, it follows that $R[\alpha]$ is finitely generated as an $R-$module. Thus α is integral over R by Proposition (2.2). But R is integrally closed, so $\alpha \in R$. Since $R \subset \mathfrak{m}^{-1}$, this implies $\mathfrak{m}^{-1} = R$.

Now let a be a non-zero element of $\mathfrak{m}$. Then by Proposition (2.3) there exist non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ such that

$$Ra \supset \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k.$$

Further, we may assume k is minimal. Then $\mathfrak{m} \supset Ra \supset \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_k$, so there is some index i such that $\mathfrak{m} \supset \mathfrak{p}_i$ by Proposition (2.4). Without loss of generality, assume $i = 1$. Since R is Dedekind, all prime ideals are maximal. Thus $\mathfrak{m} = \mathfrak{p}_1$. We now have

$$Ra \supset \mathfrak{m}\mathfrak{p}_2\mathfrak{p}_3 \cdots \mathfrak{p}_k.$$

Since k is minimal, $Ra \not\supset \mathfrak{p}_2\mathfrak{p}_3\cdots\mathfrak{p}_k$. Therefore there exists some $b \in \mathfrak{p}_2\mathfrak{p}_3\cdots\mathfrak{p}_k$ such that $b \notin Ra$. But clearly $\mathfrak{m}b \subset Ra$, so $\mathfrak{m}ba^{-1} \subset R$. By definition of $\mathfrak{m}^{-1}$ we see that $ba^{-1} \in \mathfrak{m}^{-1}$. But $b \notin Ra$ implies $ba^{-1} \notin R$, which contradicts $\mathfrak{m}^{-1} = R$. □

Theorem 2.9. *(Unique factorization of prime ideals) Let R be a Dedekind ring, $\mathfrak{a}$ a non-zero fractional ideal of R, and P the collection of non-zero prime ideals of R. Then $\mathfrak{a}$ can be uniquely factored into prime ideals as*

$$\mathfrak{a} = \prod_{\mathfrak{p}\in P} \mathfrak{p}^{n_\mathfrak{p}} \tag{2.10}$$

where the $n_\mathfrak{p}$ are integers and all but finitely many are zero.

Proof. Let $\mathfrak{a}$ be a non-zero fractional ideal of R. Then there is some non-zero $d \in R$ such that $d\mathfrak{a} \subset R$. Clearly $d\mathfrak{a}$ is an ideal of R. Since $\mathfrak{a} = (d\mathfrak{a})(Rd)^{-1}$, it suffices to prove the theorem for ideals of R rather than all fractional ideals.

Let $\mathscr{C}$ denote the set of all non-zero ideals of R which are not products of prime ideals. Suppose $\mathscr{C}$ is not empty. Since R is Noetherian, $\mathscr{C}$ has a maximal element $\mathfrak{m}$. Note that $\mathfrak{m} = R$ is impossible since R is the empty product of prime ideals. Thus $\mathfrak{m}$ is contained in a maximal ideal $\mathfrak{p}$. By the lemma, $\mathfrak{p}$ has an inverse $\mathfrak{p}^{-1}$ such that $\mathfrak{p}\mathfrak{p}^{-1} = R$.

Now $\mathfrak{m} \subset \mathfrak{p}$, so $\mathfrak{m}\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} = R$. By the definition of $\mathfrak{p}^{-1}$ in Equation (2.8), $\mathfrak{p}^{-1} \supset R$. Thus $\mathfrak{m}\mathfrak{p}^{-1} \supset \mathfrak{m}R = \mathfrak{m}$. Suppose $\mathfrak{m}\mathfrak{p}^{-1} = \mathfrak{m}$. Then if $\alpha \in \mathfrak{p}^{-1}$ we have

$$\alpha\mathfrak{m} \subset \mathfrak{m}, \ldots, \alpha^n\mathfrak{m} \subset \mathfrak{m}$$

for all $n \in \mathbb{N}$. As in the proof of the lemma, this implies $R[\alpha]$ is finitely generated as an $R-$module, thus α is integral over R, thus an element of R since R is integrally closed. Then $\mathfrak{p}^{-1} = R$. But this is impossible since $\mathfrak{p}\mathfrak{p}^{-1} = R$, but $\mathfrak{p}R = \mathfrak{p} \neq R$. This proves that $\mathfrak{m}\mathfrak{p}^{-1} \neq \mathfrak{m}$.

Since $\mathfrak{m} \subset \mathfrak{m}\mathfrak{p}^{-1}$, and $\mathfrak{m}$ is maximal in $\mathscr{C}$, we see that $\mathfrak{m}\mathfrak{p}^{-1} \notin \mathscr{C}$. Thus there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ such that $\mathfrak{m}\mathfrak{p}^{-1} = \mathfrak{p}_1\cdots\mathfrak{p}_n$. That is, $\mathfrak{m} = \mathfrak{p}\mathfrak{p}_1\cdots\mathfrak{p}_n$. It remains to show uniqueness.

Recall that P is the collection of all non-zero prime ideals of R. Suppose we have two equivalent products of prime ideals,

$$\prod_{\mathfrak{p}\in P} \mathfrak{p}^{n_\mathfrak{p}} = \prod_{\mathfrak{p}\in P} \mathfrak{p}^{m_\mathfrak{p}}. \tag{2.11}$$

We would like to show $n_\mathfrak{p} = m_\mathfrak{p}$ for all $\mathfrak{p}$. We may rewrite (2.11) as

$$\prod_{\mathfrak{p}\in P} \mathfrak{p}^{n_\mathfrak{p} - m_\mathfrak{p}} = R.$$

Suppose there are some prime ideals $\{\mathfrak{p}_i\}$ for which $n_{\mathfrak{p}_i} - m_{\mathfrak{p}_i} \neq 0$. Then we can separate positive and negative exponents so that

$$\mathfrak{p}_1^{k_1}\cdots\mathfrak{p}_r^{k_r} = \mathfrak{q}_1^{j_1}\cdots\mathfrak{q}_s^{j_s},$$

where all exponents are positive and $\mathfrak{q}_i \neq \mathfrak{p}_l$ for all indices i, l. Clearly the left hand side is contained in $\mathfrak{p}_1$, so the right hand side is as well. By Proposition (2.4), there is some i such that $\mathfrak{p}_1 \supset \mathfrak{q}_i$. Since R is Dedekind, both $\mathfrak{p}_1$ and $\mathfrak{q}_i$ are maximal. Thus $\mathfrak{p}_1 = \mathfrak{q}_i$, a contradiction. □

In the course of the proof the theorem we showed that if $\mathfrak{a}$ is an integral ideal then the exponents $n_{\mathfrak{p}}$ in Equation (2.10) are non-negative. That is, $\mathfrak{a}$ can be written as a unique product of prime ideals of R. This is not necessarily the case if $\mathfrak{a}$ is a fractional ideal in the field of fractions of R.

Corollary 2.12. *The set* $\{\mathfrak{a} : \mathfrak{a}$ *is a non-zero fractional ideal of* $R\}$ *is a group under multiplication.*

Let $F(R)$ denote the group of non-zero fractional ideals of R. It is easy to show that $I(R) = \{\mathfrak{a} : \mathfrak{a}$ is a principal fractional ideal of $R\}$ is a subgroup of $F(R)$.

Definition 2.13. With $F(R)$ and $I(R)$ as above, define $C(R) = F(R)/I(R)$ to be the *ideal class group of* R. We will use the letter h to denote the order of $C(A)$. The number h is called the *class number of* R.

An intuitive notion of the class number h is the extent to which the ring R fails to be a principal ideal domain. Indeed since R has the property that every nonzero prime ideal is maximal, R is a unique factorization domain if and only if it is a principal ideal domain.

Proposition 2.14. *Let* R *be a Dedekind ring. Then* R *is a principal ideal domain if and only if it is a unique factorization domain.*

Proof. It is well known that all principal ideal domains are unique factorization domains. We therefore need only show that UFD implies PID. Let I be an ideal of R. We may assume I is prime since any ideal is a product of primes and a product of principal ideals is principal. Let $a \in I$. Then there is some irreducible $r \mid a$ such that $r \in I$. Thus (r) is prime. We have $(0) \subset (r) \subset I$. But (r) is maximal, so $(r) = I$. □

Corollary 2.15. *The ideal class group* $C(R)$ *is trivial if and only if* R *is a unique factorization domain.*

It is not immediately clear what the order of the ideal class group is. However, in many circumstances it is enough to know that it is finite. This next theorem provides sufficient conditions for this.

Theorem 2.16. *Let* K *be a finite extension of* $\mathbb{Q}$ *and* $\mathcal{O}_K$ *the corresponding ring of integers. Then* $C(\mathcal{O}_K)$ *is finite.*

Proof. The proof uses Minkowski's geometry of numbers. For the details, see Stewart and Tall [4] p. 157. □

3. Fermat's Last Theorem

The attempted proof of Fermat's last theorem discussed in the introduction will serve as our inspiration for a partial proof due to Kummer. If we can show that $\mathbb{Z}[\zeta]$ is a Dedekind domain, we will be able to pass to ideals in Equation (1.3) and derive a contradiction. In this section the symbol ζ_n will always denote an nth root of unity.

Proposition 3.1. *Let* ζ *be a primitive pth root of unity. Then* $\mathbb{Z}[\zeta]$ *is the ring of integers in* $\mathbb{Q}(\zeta)$.

Proof. See Washington [5] pp. 1–2. □

Proposition 3.2. *Let K be a number field and $\mathcal{O}_K$ its ring of integers. Then $\mathcal{O}_K$ is a Dedekind ring.*

Proof. We must verify properties (i)-(iii) in Definition (2.5). Let $n = [K : \mathbb{Q}]$. By the classification of finitely generated abelian groups, the ring $\mathcal{O}_K$ is a $\mathbb{Z}-$submodule of a free $\mathbb{Z}-$module of rank n which is obviously torsion-free. Then if $\mathfrak{a}$ is a non-zero ideal of $\mathcal{O}_K$, and $\alpha \in \mathfrak{a}$, let f be the $\mathbb{Z}-$minimal polynomial for α. Then $\alpha \mid f(0)$ so $\alpha \in \mathfrak{a} \cap \mathbb{Z}$. Now let $a \in \mathfrak{a} \cap \mathbb{Z}$. Then $\mathcal{O}_K/\mathfrak{a}$ is a quotient of $\mathcal{O}_K/(a)$. Since $\mathcal{O}_K$ is a free $\mathbb{Z}-$module, there is a $\mathbb{Z}-$module isomorphism $\mathcal{O}_K/(a) \to (\mathbb{Z}/a\mathbb{Z})^n$. Thus $\mathcal{O}_K/\mathfrak{a}$ is finite.

Now suppose $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$ is a chain of ideals of $\mathcal{O}_K$. The set of ideals containing $\mathfrak{a}_1$ is in bijection with the ideals of $\mathcal{O}_K/\mathfrak{a}_1$, which is finite. Thus the chain has a maximal element, so $\mathcal{O}_K$ is Noetherian. This proves (i). Further, $\mathcal{O}_\mathcal{K}/\mathfrak{a}$ is an integral domain. A finite integral domain is a field, and $\mathfrak{a}$ is therefore maximal, proving property (ii).

Finally, it follows from the transitivity of integrality that the ring of integers is integrally closed in its field of fractions, thus property (iii). □

For more details see Stewart and Tall [4] p. 43. Proposition (3.2) can technically be made more general by considering an arbitrary ring R such that the field of fractions of R has characteristic zero, and any finite extension K of its field of fractions. For our purposes, however, number fields will suffice. The next two lemmas will also be essential and are reasonably easy to prove. The proofs can be found in Washington [5] chapter 1.

Lemma 3.3. *Let $u \in \mathbb{Z}[\zeta]^\times$ be a unit. Then there exists some $r \in \mathbb{Q}(\zeta + \zeta^{-1})$ and $n \in \mathbb{Z}$ such that $u = r\zeta^n$.*

Lemma 3.4. *Let $\alpha \in \mathbb{Z}[\zeta]$. Then there exists an integer a such that $\alpha^p \equiv a \pmod{p}$.*

Finally, we need one last definition. Kummer's partial proof of Fermat's last theorem requires a particular property of the exponent p.

Definition 3.5. A prime p is called *regular* if it does not divide the class number of $\mathbb{Q}(\zeta_p)$.

Many regular primes are known. For example, 2, 3, 5, 7, are all regular; in fact, 37 is the first *irregular* prime. It is not known, however, whether there are infinitely many regular primes. Nevertheless, Kummer proved Fermat's last theorem for all regular primes, which is certainly an improvement on the case when the class number is 1, as discussed in the introduction. In fact, Kummer discovered a criterion for the regularity of primes, related to the divisibility of Bernoulli numbers by p. This gives a reasonably fast way to check regularity.

Theorem 3.6. *(Kummer) Let p be an odd, regular prime. Then there are no nontrivial integer solutions to $x^p + y^p = z^p$.*

Proof. Recall that x, y, and z may be assumed to be relatively prime. First we shall assume $p \neq 3$, then deal with the case $p = 3$ explicitly. Further, it is impossible for $x \equiv y \equiv -z \pmod{p}$ to hold since then $z^p \equiv -2z^p$, and $-3z^p \equiv 0$. But $p \nmid 3z$, so this cannot be. Now if $x \equiv y$ we therefore know that $x \not\equiv -z$. Thus we may rewrite the Fermat equation as $x^p + (-z)^p = (-y)^p$. We see that if there is a solution where

the first term is congruent to the second term, there is one where it is not. We thus assume $x \not\equiv y \pmod{p}$.

Suppose, for a contradiction, that there exist integers such that $x^p + y^p = z^p$. There are now two cases: when p divides xyz, and when it does not. In this paper we will tackle only the latter case. Begin by rewriting $x^p + y^p = z^p$ and passing to ideals:

$$\prod_{i=0}^{p-1}(x + \zeta^i y) = (z)^p. \tag{3.7}$$

We first show that the ideals $(x + \zeta^i y)$ are pairwise relatively prime. Let $\mathfrak{p}$ be a prime ideal which contains $(x + \zeta^i y)$ and $(x + \zeta^j y)$ for $i > j$. Then $\mathfrak{p}$ contains $(x+\zeta^i y) - (x+\zeta^j y) = y\zeta^j(1-\zeta^{i-j})$. Now ζ^j is a unit, and $1-\zeta^{i-j} = u(1-\zeta)$ for some unit u, so $\mathfrak{p}$ contains y or $1-\zeta$. An identical argument shows that $\mathfrak{p}$ contains x or $1-\zeta$. Since x and y are assumed to be relatively prime, it follows that $\mathfrak{p}$ must contain $(1-\zeta)$. But $1-\zeta$ is prime, so $\mathfrak{p} = (1-\zeta)$.

Then $x + y = x + \zeta^i y + (1-\zeta^i)y \equiv x + \zeta^i y \equiv 0$ in $\mathbb{Z}[\zeta]/\mathfrak{p}$, since $x + y \in \mathbb{Z}$. Now consider the polynomial $f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$, which factors as $(X-\zeta)(X-\zeta^2)\cdots(X-\zeta^{p-1})$. Clearly $f(1) = p$, thus $p \in \mathfrak{p}$. Since $\mathfrak{p} \cap \mathbb{Z}$ must also be prime, we see that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Since x and y are integers, and $x + y \in \mathfrak{p}$, we have $x + y \in p\mathbb{Z}$. Then $\pmod{p}$ we have

$$0 \equiv (x+y)^p \equiv x^p + y^p \equiv z^p$$

So p divides z^p, contradicting $p \nmid z$. Therefore the terms $(x + \zeta^i y)$ are pairwise relatively prime.

Consider again Equation (3.7): both sides must factor into the same product of prime ideals. On the right hand side we see that any factor $\mathfrak{p}$ of $(z)^p$ must have ramification index a multiple of p. Since the ideals $(x+\zeta^i y)$ are pairwise relatively prime, each must be a pth power of some ideal $\mathfrak{a}_i$. That is, for each i we have

$$(x + \zeta^i y) = \mathfrak{a}_i^p.$$

In particular, $\mathfrak{a}_i^p$ is principal. Consider $\mathfrak{a}_i$ as an element of the ideal class group; the equivalence class of the ideal $\mathfrak{a}_i^p$ is the identity. But the class group is finite, and p is assumed to not divide its order, so $\mathfrak{a}_i$ itself must be the identity. That is, $\mathfrak{a}_i$ is principal. Write $\mathfrak{a}_i = (\alpha_i)$. Since $(x + \zeta^i y) = (\alpha_i^p)$, it is clear that $x + \zeta^i y$ and α_i^p are equal up to some unit $u = r\zeta^n$ as in Lemma (3.3). Assume $i = 1$.

Now there is some integer a such that $\alpha_1^p \equiv a \pmod{p}$, so $x+\zeta y \equiv r\zeta^n a \pmod{p}$. Further, $x + \zeta^{-1}y = r\zeta^{-n}\bar{\alpha}^p$ by taking complex conjugates. So $x + \zeta^{-1}y \equiv r\zeta^{-n}\bar{a} \pmod{\bar{p}}$. But of course $\bar{a} = a$ and $\bar{p} = p$. Thus,

$$\zeta^{-n}(x + \zeta y) \equiv \zeta^n(x + \zeta^{-1}y) \pmod{p},$$

or

$$x + \zeta y - \zeta^{2n}x - \zeta^{2n-1}y \equiv 0 \pmod{p}.$$

We wish to show that $1, \zeta, \zeta^{2n}, \zeta^{2n-1}$ cannot be distinct. We have

$$kp = x + \zeta y - \zeta^{2n}x - \zeta^{2n-1}y$$

for some integer k. Note that $\{1, \zeta, \zeta^{2n}, \zeta^{2n-1}\}$ may be extended to a basis for $\mathbb{Z}[\zeta]$ as a $\mathbb{Z}-$module, so long as $p > 3$. Thus $x + \zeta y - \zeta^{2n}x - \zeta^{2n-1}y$ is an expression of kp in terms of a basis. It follows that p divides $x, \zeta y, \ldots$ But this contradicts our

assumption. Thus $1, \zeta, \zeta^{2n}, \zeta^{2n-1}$ cannot be distinct. Now $1 \neq \zeta$, and $\zeta^{2n} \neq \zeta^{2n-1}$. We are thus left with three cases.

(i) Suppose $1 = \zeta^{2n}$. Then $x + \zeta y - x - \zeta^{-1} y \equiv 0 \pmod{p}$, or $y(\zeta - \zeta^{-1}) \equiv 0 \pmod{p}$. This implies p divides y, a contradiction.

(ii) Suppose $1 = \zeta^{2n-1}$. Then $\zeta = \zeta^{2n}$. We then have $(x-y) - (y-x)\zeta \equiv 0 \pmod{p}$, so $(x-y) - (y-x)\zeta = \alpha p$ for some integer $\alpha \in \mathbb{Z}[\zeta]$. We see that $(x-y)$ and $(y-x)$ are coefficients for αp with respect to a basis for $\mathbb{Z}[\zeta]$ as a $\mathbb{Z}-$module. Thus p divides $x-y$, so $x \equiv y \pmod{p}$, contrary to assumption.

(iii) Suppose $\zeta = \zeta^{2n-1}$. Then $x - \zeta^2 x \equiv 0 \pmod{p}$. Then $x \equiv 0 \pmod{p}$, a contradiction.

It now remains to show that the case $p = 3$ is impossible. All cubes mod 9 are ± 1 or 0. Since $3 \nmid x$ it follows that $x^3 \equiv \pm 1 \pmod{9}$. The same holds for y and z. But then $x^3 + y^3 \equiv 2, 0, -2 \not\equiv \pm 1 \pmod{9}$. Thus z^3 cannot be a cube, which is a contradiction. □

4. Ramification

Consider a Dedekind ring R and its field of fractions K. Assume the characteristic of K is zero. Recall from Theorem (2.9) that any $\mathfrak{a}$ of R may be written as a unique product of prime ideals as in Equation (2.10). We wish to now consider what happens to $\mathfrak{a}$ in the integral closure $\mathcal{O}_L$ of R in a finite extension L of K. In the remarks following Proposition (3.2) we noted that $\mathcal{O}_L$ is in fact a Dedekind ring itself. Thus if $\mathfrak{p}$ is a prime ideal of R, then $\mathcal{O}_L\mathfrak{p}$ is an ideal of $\mathcal{O}_L$ and has a unique factorization

$$\mathcal{O}_L\mathfrak{p} = \prod_{i=1}^{n} \mathfrak{P}_i^{e_i} \tag{4.1}$$

where each $\mathfrak{P}_i$ is prime in $\mathcal{O}_L$, and the e_i are all positive integers. It is not difficult to characterize the $\mathfrak{P}_i$ completely.

Proposition 4.2. *With notation as above, the $\mathfrak{P}_i$ are precisely the prime ideals of $\mathcal{O}_L$ whose intersection with R is $\mathfrak{p}$. The $\mathfrak{P}_i$ are commonly said to* lie over $\mathfrak{p}$.

Proof. Suppose first that $\mathfrak{P}$ is a prime factor of $\mathcal{O}_L\mathfrak{p}$. Then $\mathcal{O}_L\mathfrak{p} \subset \mathfrak{P}_i$, so $\mathfrak{P}_i \cap R$ is an ideal of R containing $\mathfrak{p}$. But it is obvious that $\mathfrak{P}_i \cap R$ is prime, and so must be identically $\mathfrak{p}$. On the other hand, if $\mathfrak{P}$ has the property that $\mathfrak{P} \cap R = \mathfrak{p}$, then $\mathfrak{p} \subset \mathfrak{P}$. Thus $\mathfrak{P}$ is a factor of $\mathfrak{p}$; by uniqueness of factorization, it must appear in the factorization. □

Definition 4.3. With notation as above, the integer e_i in Equation (4.1) is the *ramification index of $\mathfrak{P}_i$ over R*. If $e_i > 1$ for some i then $\mathfrak{p}$ is said to *ramify in $\mathcal{O}_L$ and L*.

If $\mathfrak{p}$ is a prime and $\mathfrak{P}_i$ lies above $\mathfrak{p}$, then it is clear that, with notation as above, $\mathcal{O}_L/\mathfrak{P}$ is a finite field extension of $R/\mathfrak{p}$. We call degree of this extension, f_i, the *residual degree* of $\mathfrak{P}_i$ over R.

Theorem 4.4. *Let $R, K, \mathcal{O}_L, L$ be as above, and $\mathfrak{p}$ a prime ideal of R. Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ be the primes of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Then*

$$\sum_{i=1}^{m} e_i f_i = [L : K]. \tag{4.5}$$

Proof. The ring $\mathcal{O}_L/\mathcal{O}_L\mathfrak{p}$ is certainly a finitely generated $R/\mathfrak{p}-$vector space of dimension $n = [L : K]$. By the Chinese remainder theorem, we have

$$(R/\mathfrak{p})^n \cong \mathcal{O}_L/\mathcal{O}_L\mathfrak{p} \cong \prod_i \mathcal{O}_L/\mathfrak{P}_i^{e_i}.$$

Now $\mathcal{O}_L/\mathfrak{P}_i$ is a field extension of $R/\mathfrak{p}$ of degree f_i isomorphic to $\mathbb{F}_q$ for some q. Thus $\mathcal{O}_L/\mathfrak{P}_i^{e_i} \cong \mathbb{F}_q[X]/X^{e_i}$, which is thus (isomorphic to) an $R-$module of rank $e_i f_i$. □

We wish to focus our attention on number fields. In this particular example, we will consider quadratic extensions. Let d be a square-free integer, p an odd prime and let S denote the ring of integers in $\mathbb{Q}(\sqrt{d})$. We first calculate S explicitly.

Proposition 4.6. *Let d be a square-free integer. Then the ring of integers S in $\mathbb{Q}(\sqrt{d})$ is*

$$\begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod 4 \\ \mathbb{Z}\left[\frac{1}{2}(1+\sqrt{d})\right] & d \equiv 1 \pmod 4. \end{cases} \tag{4.7}$$

Proof. Suppose $w \in S$ is integral over $\mathbb{Z}$. Then $w = a + b\sqrt{d}$ for some $a, b \in \mathbb{Q}$. Then w is a root of the polynomial $(X - w)(X - \sigma(w)) = (X - a - b\sqrt{d})(X - a + b\sqrt{d})$ where σ is the nontrivial element of $Gal(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. This polynomial must have integer coefficients. Thus,

$$2a \in \mathbb{Z}$$
$$a^2 - b^2 d \in \mathbb{Z}$$

Suppose first that $a \notin \mathbb{Z}$. Then $a = n/2$ for some integer n. We have that

$$n^2 - 4db^2 \in 4\mathbb{Z}.$$

Since $n^2 \equiv 0$ or $1 \pmod 4$, it follows that $4db^2 \equiv 0$ or $1 \pmod 4$ respectively. The second case occurs if and only if b^2 is not an integer. But b^2 is not an integer because this would imply a^2 is an integer, contrary to assumption. However, d is square-free so if $4b^2$ is not an integer then $4b^2 d$ is not either. Thus $4b^2 \in \mathbb{Z}$. Evidently $2b$ is an integer. Thus $2a$ and $2b$ are integers, so $S = \mathbb{Z}\left[\frac{1}{2}(1+\sqrt{d})\right]$. Further, since this is the case if and only if $4db^2 \equiv 1 \pmod 4$, we necessarily have $d \equiv 1 \pmod 4$.

On the other hand, if $a \in \mathbb{Z}$ then $db^2 \in \mathbb{Z}$. But d is square-free, so $b \in \mathbb{Z}$. Thus in this case $S = \mathbb{Z}[\sqrt{d}]$, and d is necessarily congruent to 2 or 3 (mod 4). We may now revisit the proof and see that all implications are actually double implications, thus proving the proposition. □

Equipped with this knowledge, we can now characterize precisely those primes which ramify in quadratic extensions.

Example 4.8. Let d be a square-free integer and S be the ring of integers in $\mathbb{Q}(\sqrt{d})$ and p an odd prime. Then consider the quotient $S/(p)$. Note first that if $S = \mathbb{Z}\left[\frac{1}{2}(1+\sqrt{d})\right]$ then the image of $a + \frac{b}{2}(1+\sqrt{d}) \bmod (p)$ is an element of $\mathbb{Z}[\sqrt{d}]/(p)$. We can thus assume the case $S = \mathbb{Z}[\sqrt{d}]$.

Now $\mathbb{Z}[\sqrt{d}]/(p) \cong \mathbb{Z}[X]/(X^2 - d, p) \cong (\mathbb{Z}/p\mathbb{Z}[X])/(X^2 - d)$. If $X^2 - d$ is irreducible in $\mathbb{F}_p[X]$ then the ideal it generates is prime, hence maximal. That is, $S/(p)$

is a field if and only if d is not a quadratic residue mod p, and also if and only if (p) is prime in S. It is clear that the residual degree of (p) over $\mathbb{Z}$ is 2. Another possibility is that $X^2 - d$ has two distinct roots $\pm\omega$ in $\mathbb{F}_p$. Then

$$S/(p) \cong \mathbb{F}_p/(X-\omega) \times \mathbb{F}_p/(X+\omega).$$

It is clear that this occurs if and only if (p) splits in S. That is, if (p) is the product of two *distinct* primes P_1, P_2 of S. Then $f_1 = f_2 = e_1 = e_2 = 1$. Finally, if $X^2 - d$ is a square mod p, which occurs precisely when $p \mid d$ or $p = 2$, then $S/(p) \cong \mathbb{F}_p/(X^2)$. This is the last remaining possibility: $f = 1, e = 2$. That is, p ramifies in S.

5. Galois Theory Applied to Ramification

This section assumes some familiarity with Galois theory. Our aim is to take the theory of ramification we have developed and interpret it in the context of Galois extensions. The methods of Galois theory lead to several applications, including a proof of quadratic reciprocity which is given at the end of the section.

Proposition 5.1. *Let R be a Dedekind ring, K its field of fractions, and suppose K has characteristic zero. Further, let L be a Galois extension of K. Define $\mathcal{O}_L$ to be the integral closure of R in L. Then $\sigma(\mathcal{O}_L) = \mathcal{O}_L$ for all $\sigma \in Gal(L/K)$.*

Proof. Suppose $\alpha \in \mathcal{O}_L$ and σ is a Galois automorphism. Then α is a root of some polynomial $X^n + a_1X^{n-1} + \cdots + a_n$ with coefficients in R. We see that $\sigma(\alpha)$ must also be a root of this polynomial, hence $\sigma(\mathcal{O}_L) \subset \mathcal{O}_L$. On the other hand, $\sigma^{-1}(\mathcal{O}_L) \subset \mathcal{O}_L$ for the same reason. □

Proposition 5.2. *With notation as above, let $\mathfrak{p}$ be a prime of R and $\mathscr{P}$ the collection of primes lying over $\mathfrak{p}$. Then the Galois group $Gal(L/K)$ acts transitively on $\mathscr{P}$.*

Corollary 5.3. *Let $R, K, L, \mathcal{O}_L$ be as above. Then if $\mathfrak{p}$ is a maximal ideal of R, each of the primes $\mathfrak{P}$ lying over $\mathfrak{p}$ have the same ramifications indices e and same residual degrees f.*

Definition 5.4. With notation as above, then for any prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ we have a subgroup $D_\mathfrak{P}$ of the Galois group given by $D_\mathfrak{P} = \{\sigma \in Gal(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$. We call $D_\mathfrak{P}$ the *decomposition group of* $\mathfrak{P}$.

Because the Galois group acts transitively on primes lying over $\mathfrak{p}$, we see that the index of $D_\mathfrak{P}$ in $Gal(L/K)$ is equal to the number of primes lying over $\mathfrak{p}$. Further, since R is Dedekind, and therefore so is its integral closure $\mathcal{O}_L$, it follows from Proposition (3.2) that $\mathfrak{P}$ is maximal, hence $\mathcal{O}_L/\mathfrak{P}$ is a field. Similarly, so is $R/\mathfrak{p}$. Suppose $\sigma \in D_\mathfrak{P}$, thus $\sigma(\mathfrak{P}) = \mathfrak{P}$. Then σ restricts to an automorphism of $\mathcal{O}_L$ such that there is an induced automorphism $\bar{\sigma}$ on $\mathcal{O}_L/\mathfrak{P}$ and the following diagram commutes.

$$\begin{array}{ccc} R & \xrightarrow{\sigma|_R} & R \\ \downarrow & & \downarrow \\ R/\mathfrak{p} & \xrightarrow{\bar{\sigma}|_{R/\mathfrak{p}}} & R/\mathfrak{p} \end{array}$$

Clearly $R/\mathfrak{p}$ is fixed by each $\bar{\sigma}$. Thus there is a map $\varphi : D_\mathfrak{P} \to G$ with $\sigma \mapsto \bar{\sigma}$ and where G is the set of automorphisms of $\mathcal{O}_L/\mathfrak{P}$ which fix $R/\mathfrak{p}$. Since $\mathcal{O}_L/\mathfrak{P}$ / $R/\mathfrak{p}$ is

a finite extension of finite fields it is a Galois extension. Thus φ is a homomorphism $D_{\mathfrak{P}} \to Gal(\mathcal{O}_L/\mathfrak{P} \,/\, R/\mathfrak{p})$.

Definition 5.5. Assume the above notation and that $\mathcal{O}_L/\mathfrak{P}$ is a Galois extension of $R/\mathfrak{p}$. Let $I_{\mathfrak{P}}$ denote the kernel of φ. The group $I_{\mathfrak{P}}$ is called the *inertia subgroup of* $\mathfrak{P}$.

By definition, $I_{\mathfrak{P}}$ is a normal subgroup of $D_{\mathfrak{P}}$. In fact, $D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong Gal(\mathcal{O}_L/\mathfrak{P} \,/\, R/\mathfrak{p})$. For a proof, see Marcus [1] p. 101.

Proposition 5.6. *A prime $\mathfrak{p}$ of R ramifies in $\mathcal{O}_L$ if and only if $I_{\mathfrak{P}}$ is not trivial for any $\mathfrak{P}$ which lies over $\mathfrak{p}$.*

Proof. By definition, $[\mathcal{O}_L/\mathfrak{P} : R/\mathfrak{p}] = f$, where f is the residual degree of $\mathfrak{P}$ over $\mathfrak{p}$. Since $\mathcal{O}_L/\mathfrak{P}$ is a Galois extension of $R/\mathfrak{p}$, the Galois group G has order f. Thus $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ has order f.

On the other hand, G has order equal to ref where r is the number of primes lying over $\mathfrak{p}$ and e is the ramification index. The Galois group G acts transitively on the primes lying over $\mathfrak{p}$ so we have $r = [G : D_{\mathfrak{P}}]$. Thus $|D_{\mathfrak{P}}| = ref/r = ef$. Then $[D_{\mathfrak{P}} : I_{\mathfrak{P}}] = f$ implies $I_{\mathfrak{P}}$ has order e. □

We will now apply the above theory to the specific case of number fields—that is, to finite extensions of $\mathbb{Q}$. Suppose K and L are number fields with L a Galois extension of K. Let $\mathcal{O}_K$ and $\mathcal{O}_L$ denote the ring of integers in K and L, respectively. Then $K/\mathcal{O}_K \cong \mathbb{F}_q$ for some $q = p^n$ with p prime, and $L/\mathcal{O}_L \cong \mathbb{F}_{q^m}$ for some integer m. In particular, $Gal(L/K)$ is cyclic with generator $\mathcal{F}$ defined by $\mathcal{F}(x) = x^q$.

Suppose now $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ such that $\mathfrak{p}$ does not ramify in $\mathcal{O}_L$. By Corollary (5.6) we see that $D_{\mathfrak{P}} \cong Gal(\mathcal{O}_L/\mathfrak{P}\,/\mathcal{O}_K/\mathfrak{p}\,)$ for all primes $\mathfrak{P}$ lying over $\mathfrak{p}$. Thus $D_{\mathfrak{P}}$ is cyclic with generator σ. We see that $\sigma(x) = x^q \pmod{\mathfrak{P}}$.

Definition 5.7. With notation as above, the generator σ of $D_{\mathfrak{P}}$ is called the *Frobenius automorphism of* $\mathfrak{P}$. We can define the Frobenius automorphism for ramified primes as the coset of $I_{\mathfrak{P}}$ which is mapped to the generator of $Gal(\mathcal{O}_L/\mathfrak{P}\,/\mathcal{O}_K/\mathfrak{p}\,)$

Since the Frobenius automorphism σ generates the Galois group, it follows from Proposition (5.6) that σ has order f in $D_{\mathfrak{P}}$. In the context of a quadratic extension, using Theorem (4.4) we see that σ must have order 1 or 2. This is a particularly important example and motivates the remainder of this paper. We will conclude with a proof of the law of quadratic reciprocity, but first we need some definitions.

Definition 5.8. Let p be a prime and n an integer such that $p \nmid n$. Then we define the *Legendre symbol* $(\frac{n}{p})$ by

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & n \text{ is a quadratic residue } (\text{mod } p) \\ -1 & n \text{ is not a quadratic residue } (\text{mod } p). \end{cases}.$$

With this notation we can rewrite the results of Example (4.8).

Proposition 5.9. *Let d be a squarefree integer, p an odd prime, and S the ring of integers in $\mathbb{Q}(\sqrt{d})$. Then*

$$\begin{cases} p \text{ ramifies in S} & \text{iff } p \mid d \\ p \text{ splits in S} & \text{iff } \left(\frac{d}{p}\right) = 1 \\ p \text{ remains prime in S} & \text{iff } \left(\frac{d}{p}\right) = -1 \end{cases}$$

For a prime $p \in \mathbb{Z}$ which does not ramify in some number field K, write σ_p for the associated Frobenius automorphism. Since σ_p must have order f, we see that σ_p is trivial if and only if $e = 2$, (cf. Theorem (4.4)) so p must split in K. On the other hand, if σ_p is the nontrivial automorphism, then $f = 2$, so p necessarily remains prime in K. Identifying $Gal(K/\mathbb{Q})$ with $\{1, -1\}$ and by appealing to the above proposition, we may write $\sigma_p = (\frac{d}{p})$.

That the Legendre symbol is multiplicative in the numerator follows from Proposition (5.18). Therefore to calculate $(\frac{a}{p})$ it suffices to calculate $(\frac{q}{p})$ for primes q dividing a. Making this calculation is essentially the content of the law of quadratic reciprocity. However, to prove the law we will require some facts about cyclotomic fields.

Proposition 5.10. *Let ζ be a primitive nth root of unity. Then $\mathbb{Q}(\zeta)$ is a Galois extension of $\mathbb{Q}$ and there exists a canonical isomorphism $\varphi : Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$. Further, if p is a prime not dividing n and $\mathfrak{P}$ is a prime lying over p with corresponding Frobenius automorphism σ, then $\varphi(\sigma) \equiv p \pmod{n}$.*

Proof. By defintion of σ we have that $\sigma(x) \equiv x^p \pmod{\mathfrak{P}}$ for all $x \in \mathcal{O}_{\mathbb{Q}(\zeta)}$. Now σ is an automorphism of a cyclotomic extension. Therefore $\sigma(\zeta) = \zeta^i$, where $i = \varphi(\sigma)$. We thus have:

$$\zeta^{\varphi(\sigma)} \equiv \zeta^p \pmod{\mathfrak{P}}.$$

We wish to show $\varphi(\sigma) \equiv p \pmod{n}$. Suppose not. Assume p and $\varphi(\sigma)$ have already been reduced (mod n). Then we may rewrite the above as $\zeta^p(1 - \zeta^{\varphi(\sigma)-p}) \in \mathfrak{P}$. Since $\mathfrak{P}$ is prime and ζ^p is a unit, it follows that $(1 - \zeta^{\varphi(\sigma)-p}) \in \mathfrak{P}$. But consider the polynomial $F(X) = (X^n)/(X - 1) = X^{n-1} + X^{n-2} + \cdots + 1$, which factors as $(X - \zeta)(X - \zeta^2) \cdots (X - \zeta^{n-1})$. We see that $F(1) = n$. It follows that $(1 - \zeta) \cdots (1 - \zeta^{n-1}) \in \mathfrak{P}$. But $p \nmid n$, so $n \notin \mathfrak{P} \cap \mathbb{Z}$, a contradiction.

It is clear that $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ since each Galois automorphism τ is determined by the power to which it raises ζ. On the other hand, if q and p are primes and σ_q, σ_p are the corresponding Frobenius automorphisms, $\varphi(\sigma_q \circ \sigma_p) = pq$. So if $m \in \mathbb{Z}/n\mathbb{Z}$ and m has the prime factorization (in $\mathbb{Z}$) $p_1 \cdots p_n$, then $\varphi(\sigma_{p_1} \circ \cdots \circ \sigma_{p_n}) = m$. Thus φ is surjective. □

Theorem 5.11. *Let ζ be a primitive nth root of unity. Then for all primes p which ramify in $\mathbb{Q}(\zeta)$, we have $p \mid n$.*

Proof. Suppose $p \nmid n$. Then using the above proposition we see that the Frobenius automorphism corresponding to p is well defined. That is, $I_{\mathfrak{P}}$ is trivial and $e = 1$. □

In Proposition (5.9) we saw that we can relate the Legendre symbol to ramification in quadratic extensions. In order to prove the law of quadratic reciprocity we will use the following classification of quadratic extensions which are subfields of cyclotomic extensions.

Proposition 5.12. *Let p be an odd prime and let ζ be a primitive pth root of unity. Then the field $\mathbb{Q}(\zeta)$ has a unique quadratic subfield F, where*

$$F = \begin{cases} \mathbb{Q}(\sqrt{p}) & p \equiv 1 \pmod{4} \\ \mathbb{Q}(\sqrt{-p}) & p \equiv 3 \pmod{4} \end{cases}. \tag{5.13}$$

Proof. We have seen that the Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/q\mathbb{Z})^\times$. This group has a unique subgroup of index 2, corresponding via isomorphism to a unique index 2 subgroup H of the Galois group. The fixed field $\mathbb{Q}(\zeta)^H$ is therefore a quadratic extension of $\mathbb{Q}$. For the remainder of the proof see Samuel [3] p. 75. □

Theorem 5.14. *(Law of Quadratic Reciprocity) Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right) \tag{5.15}$$

Proof. Let $L = \mathbb{Q}(\zeta)$ where ζ is a primitive qth root of unity. Then L has a unique quadratic subfield K. By Proposition (5.12), $K = \mathbb{Q}(\sqrt{q})$ or $K = \mathbb{Q}(\sqrt{-q})$. Now $p \neq q$, so p does not ramify in L, hence does not ramify in K. Thus corresponding to p we have a Frobenius automorphism $\sigma \in Gal(L/\mathbb{Q})$. By definition, for all $x \in K$, $\sigma(x) \equiv x^q \pmod{\mathcal{O}_L p}$, thus $\sigma(x) \equiv x^q \pmod{\mathcal{O}_K p}$. Further, $\sigma(\mathcal{O}_K p) = \sigma(\mathcal{O}_L p \cap K) = \mathcal{O}_K p$, so σ is in the decomposition group. This proves that $\sigma|_K$ is the Frobenius automorphism of p for $K/\mathbb{Q}$.

Now $Gal(L/\mathbb{Q}) \cong \mathbb{F}_q^\times$, and $Gal(K/\mathbb{Q}) \cong \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2$, so $\sigma|_K$ is trivial if and only if it is in the subgroup of $Gal(L/\mathbb{Q})$ corresponding to $(\mathbb{F}_q^\times)^2$. We have seen in Proposition (5.10) that σ corresponds to $p \pmod q$ in $\mathbb{F}_q^\times$. Thus $\sigma|_K$ is trivial if and only if p is a square in $\mathbb{F}_q$. We can identify $Gal(K/\mathbb{Q})$ with the group $\{-1, 1\}$. We see that

$$\sigma|_K = \left(\frac{p}{q}\right). \tag{5.16}$$

Now if f denotes the residual degree of p in K, we know that necessarily f is the order of $\sigma|_K$ in $Gal(K/\mathbb{Q})$ (cf. the remarks following Definition (5.7)). Thus $\sigma|_K$ is trivial if and only if p remains prime in K, and $\sigma|_K$ is nontrivial if and only if p splits in K. Using Proposition (5.9) we have,

$$\begin{cases} \sigma|_K = \left(\frac{q}{p}\right) & \text{if } q \equiv 1 \pmod 4 \\ \sigma|_K = \left(\frac{-q}{p}\right) & \text{if } q \equiv 3 \pmod 4. \end{cases} \tag{5.17}$$

Combining Equations (5.16) and (5.17) we have

$$\begin{aligned} \left(\frac{p}{q}\right) &= \sigma|_K = \left(\frac{\pm q}{p}\right) \\ &= \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) \\ &= \left(\frac{q}{p}\right)\left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \\ &= \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \end{aligned}$$

□

Finding $(\frac{p}{q})$ when $q = 2$ is trivial. However, there is a rather glaring omission in the theorem: we have not accounted for the case $p = 2$. We will solve this problem using slightly more elementary methods. The only required proposition is Euler's Criterion.

Proposition 5.18. *(Euler's Criterion) Let p be a prime and a an integer such that $p \nmid a$. Then*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Proof. By definition $(\frac{a}{p}) = 1$ if and only if there exists some $n \in \mathbb{F}_p^\times$ such that $n^2 = a$. Now $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$, so equivalently there exists some $m \in \mathbb{Z}/(p-1)\mathbb{Z}$ such that $2m = a$. That is, $\frac{p-1}{2}a = 0$. Writing this as an equation in $\mathbb{F}_p$ we have $a^{\frac{p-1}{2}} = 1$. On the other hand, $(\frac{a}{p}) = -1$ then $a^{p-1} = 1$, and $a^{\frac{p-1}{2}}$ is a square root of 1. But we have seen that $a^{\frac{p-1}{2}} = 1 \iff (\frac{a}{p}) = 1$, thus $(\frac{a}{p}) = -1$. □

Theorem 5.19. *(Legendre Symbol for 2) If p is an odd prime then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8. \end{cases}$$

Proof. We have that $(1+i)^2 = 2i$, so

$$2^{\frac{p-1}{2}} = \frac{(1+i)^p}{1+i} i^{\frac{p-1}{2}}.$$

Then

$$2^{\frac{p-1}{2}} \equiv \frac{1+i^p}{1+i} i^{\frac{p-1}{2}}.$$

The result follows. □

Acknowledgments. It is my pleasure to thank my mentor, Dan Le, for his patience and guidance. I'd also like to thank Nick Ramsey for putting ideas in my head.

References

[1] Daniel Marcus. Number Fields. Springer-Verlag New York, Inc. 1977
[2] Serge Lang. Algebraic Number Theory. Second Edition. Springer-Verlag New York, Inc. 1999
[3] Pierre Samuel. Algebraic Theory of Numbers. Translated by Allan J. Silberger. Kershaw Publishing Company Ltd. 1971
[4] Ian Stewart and David Tall. Algebraic Number Theory and Fermat's Last Theorem. Third Edition. A K Peters, Ltd. 2002
[5] Lawrence C. Washington Introduction to Cyclotomic Fields. Springer-Verlag New York, Inc. 1982