Cyclotomic Fields and Fermat's Last Theorem

Samuel Runyeon Odeberg

Advisor: Prof. Arne Meurman

September 17, 2021

Popular Scientific Summary

Number theory is in a sense among the oldest disciplines of mathematics. A running theme is that many number theoretic problems are very easy to state and understand. However, actually solving these problems often requires much work or some very clever trick. An extreme case of this would be Fermat's last theorem: originally a conjecture by French lawyer Pierre de Fermat whose statement is understandable to anyone who knows how to add and take powers; however, it took over three and a half centuries to prove, despite many of history's greatest mathematicians giving it their best efforts.

During the 17^{th} century Fermat made a note in a copy of Diophantus's Arithmetica of a statement for which he famously claimed to have a marvelous proof; this is the very same note where he famously wrote that the margins of the book were too small for said proof. The statement he wrote down was simply that the equation

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

has no solutions such that x, y and z are all non-zero integers when n is an integer strictly greater than 2. This is the statement that would eventually became known as Fermat's last conjecture. For centuries this conjecture remained uncracked until the matter was finally settled by Andrew Wiles toward the end of the 20^{th} century. Wiles managed to prove that the conjecture was in fact true, earning it the title it is currently known by: Fermat's last theorem.

Before yielding to Wiles, Fermat's last theorem was highly sought after. Many a great mathematician attempted to prove the statement long before Wiles, including the likes of Euler and Gauss, but they were only ever able to establish special cases. Among these was French mathematician Gabriel Lamé. In fact, Lamé was convinced that he had essentially found a proof for the statement [2]. The trick was, according to Lamé, to look at a certain factorization of $x^n + y^n$ as a *cyclotomic integer*. He thought that he could use the uniqueness of this factorization to prove Fermat's last theorem. However, his proof turned out to have a fatal flaw.

Cyclotomic integers are essentially a collection of complex numbers with an arithmetic very similar to that of the integers. For instance, much like integers, cyclotomic integers have irreducible numbers that all cyclotomic integers factor into. Here irreducible essentially means that there are no "meaningful" cyclotomic integers dividing the factor and that the number itself is "meaningful" as a divisor; some cyclotomic integers divide all other cyclotomic and in this sense behave very much like ± 1, since knowing that they divide a given number tells us nothing about that number. The collection of cyclotomic integers can be different depending on what specific cyclotomic integers we are talking about. Each collection of cyclotomic integers corresponds to the complex number $\omega = e^{\frac{2\pi i}{m}}$ for some integer m, and can be constructed by extending the integers to also include ω and all possible finite sums and products of integers and ω, with repetition of numbers allowed.

On the 4^{th} of January 1847, Lamé proposed to use the cyclotomic integers corresponding to n to factorize $x^n + y^n$. Where he went wrong was in assuming that factorization into irreducible cyclotomic integers was in fact unique. That this was not always the case had in fact been proven in a paper by German mathematician Ernst Kummer three years prior to Lamé presenting his supposed proof [2]. One integer n such that unique factorization fails for the corresponding cycltomic integers is $n = 23$, as is shown in this paper.

While Kummer's paper was a death-blow to Lamé's arguments, Kummer was convinced that unique factorization into irreducible numbers was in fact valid for cyclotomic integers if one also considered what he called *ideal numbers*. Using these he was able to use Lamé's factorization to prove Fermat's last theorem for special primes that are known as *regular primes*, although his proof was much more complicated than that which Lamé had proposed. A proof of Fermat's last theorem for regular primes can be found in the last section of this paper.

Abstract

The two main aims of this paper are to show that there are rings of cyclotomic rings which are not UFD's and to prove Fermat's last theorem for regular primes, assuming the statement of Kummer's lemma holds.

This work is dedicated to my wife, Robin, and our cat, Percival.

Acknowledgements

I would here like to thank my supervisor Arne Meurman for introducing me to such a wonderful topic and for his invaluable help and guidance throughout the project.

Contents

1 Introduction

On the January 4 1847, French mathematician Gabriel Lamé published a proof of Fermat's last theorem, which made use of an infinite descent in rings of cyclotomic integers [3]. The main idea was to factor the equation $x^p + y^p = z^p$ into $\prod_{k=0}^{p-1}(x + {\omega_p}^k y) = z^p$ in the ring $\mathbb{Z}[\omega_p] \cong \mathbb{Z}[x]/(\phi_p(x))$, where ω_p is a primitive p^{th} root of unity for a prime p and $\phi_p(x) = \frac{x^p-1}{x-1}$.

Set $\omega = \omega_p$. Under the assumptions that $\mathbb{Z}[\omega]$ is a UFD and that none of the factors $x + \omega^k y$ are units, this leads to an infinite descent in $\mathbb{Z}[\omega]$ as follows. We begin by assuming that x, y, z are pairwise relatively prime in $\mathbb{Z}$, which we may do since if any two of these numbers share a common factor, so does the third. Our next step is to change our factorization of $x^p + y^p$ slightly. For each k we can find an integer j such that $2j \equiv -k \bmod p$. It is clear that as k runs through the integers $0, \ldots, p-1$, then so does j. We therefore have the factorization

$$x^p + y^p = \omega^{-\frac{p(p-1)}{2}} \prod_0^{p-1}(x\omega^{-j} + y\omega^j) = \prod_0^{p-1}(x\omega^{-j} + y\omega^j)$$

in $\mathbb{Z}[\omega]$. Let us now define α_j to be the j^{th} factor in this factorization. Take n and m to be two distinct integers contained in the set $\{0, \ldots, p-1\}$. Lamé goes on to show that

$$\alpha_n + \alpha_m = x(\omega^{-n} + \omega^{-m}) + y(\omega^n + \omega^m) = c_d\alpha_s,$$

with $2d \equiv n - m \bmod p$ and $2s \equiv n + m \bmod p$, with $c_d := \omega^d + \omega^{-d}$. He then states that whenever a cyclotomic integer d is a common divisor of two factors α_i it is a common divisor of all of them and that c_d cannot divide any factor α_i without dividing every one of them.

While rational integers indeed factorize uniquely, this is unfortunately not the general case for cyclotomic integers. On March 1 1847, after Lamé had presented his proof during a meeting at the Paris Academy, Joseph Liouville criticized the assumption that factorization in rings of cyclotomic integers works like that of the rational integers [2]. Unique factorization into prime elements for cyclotomic integers was not obvious and more importantly not proven. The matter therefore required further motivation before Lamé's proof could possibly be considered complete.

In May the same year Liouville received a letter from German mathematican Ernst Eduard Kummer, where he not only assured Liouville that he was right to criticize Lamé's proof; Kummer also included a copy of a by then three-year-old paper he had written. He had in this very paper proven that there indeed exist primes such that unique factorization fails in its corresponding cyclotomic ring of integers.

However, Kummer himself was developing theory that might allow for one to circumvent the fact that the cyclotomic integers lack unique factorization; he was convinced that one could embed each ring of numbers into a ring of what he called ideal numbers, which had the desired unique factorization property [5]. Kummer's theory of ideal numbers was later further developed by Richard Dedekind into the theory of ideals that is now essential in the study of arbitrary rings.

Fermat's last theorem is often split into two cases: case I and case II. In case I one considers non-zero integral solutions of $x^p + y^p = z^p$ such that $p \nmid xyz$ and in case II non-zero integral solutions such that $p \mid xyz$. We may assume that x, y and z are relatively prime so that p divides only one of the variables, since any divisor of two of the variables is a divisor of all three. Which variable is divisible by p doesn't matter since p must be odd and thus rewriting the equation as $x^p + y^p + (-z)^p = 0$ makes it clear that the choice completely arbitrary. Both cases may be proven by starting out similarly to Lamé's proposed "proof" for a subclass of primes called **regular primes**. A prime p is called regular if it does not divide the **class number** of $\mathbb{Q}(\omega_p)$, which we will define later. For now, it suffices to know that this is euqivalent to the statement that for each ideal $\mathfrak{a}$ of $\mathbb{Z}[\omega_p]$, we have that $\mathfrak{a}$ is principal if and only if $\mathfrak{a}^p$ is principal.

If p is assumed a regular prime, then instead of what Lamé proposed one may consider the factorization

$$\prod_0^{p-1}(x + \omega^k y) = (z)^p,$$

where $\omega = \omega_p$, of principal ideals of $\mathbb{Z}[\omega_p]$. We will later prove that $\mathbb{Z}[\omega_p]$ is an example of a **Dedekind domain**, in which all ideals factor uniquely into prime ideals. Since this is the case, we may in case I show that $(x + \omega^i y)$ and $(x + \omega^j y)$ are relatively prime by assuming toward contradiction that there exists a prime ideal $\mathfrak{p}$ dividing both, where divisiblity of ideals $\mathfrak{a}$ and $\mathfrak{b}$ is defined by $\mathfrak{a} \mid \mathfrak{b} \iff \mathfrak{a} \supset \mathfrak{b}$. The importance of p being regular comes from that we can in fact show that $(x + \omega y) = \mathfrak{a}^p$, for some

non-trivial ideal $\mathfrak{a}$. Regularity ensures that $\mathfrak{a}$ is in fact also principal. Finishing the argument requires a bit more theory than is readily available to a student without any background in algebraic number theory and is therefore better saved for later. We will return to proving Fermat's last theorem for regular primes in Section 6.

Our inital goal in the following sections will be to prove that $\mathbb{Z}[\omega_{23}]$ is not necessarily a UFD. This can be easily done, albeit somewhat tediously, by first showing that 2 is irreducible in $\mathbb{Z}[\omega_{23}]$ and then considering the product

$$(1+\omega^2+\omega^4+\omega^5+\omega^6+\omega^{10}+\omega^{11})(1+\omega+\omega^5+\omega^6+\omega^7+\omega^9+\omega^{11}),$$

with $\omega = \omega_{23}$ which is divisible by 2 despite neither of its factors being divisible by 2, as is outlined in an exercise in Chapter 1 of [4]. The above factorization thus violates the notion of unique factorization required for $\mathbb{Z}[\omega_{23}]$ to be a UFD and the proof is complete. While this may prove the statement, it is not a very satisfying proof. For instance, it tells us very little about why such a product exists in $\mathbb{Z}[\omega_{23}]$ or under what conditions we could expect unique factorization to fail in other rings. Furthermore, the product seemingly comes from nowhere and as such the proof certainly doesn't feel very elegant. It will therefore be in our interest to develop more advanced theory in order to better understand what is going on in $\mathbb{Z}[\omega_{23}]$.

This paper assumes a basic knowledge of abstract algebra corresponding roughly to a one-semester introductory course in abstract algebra. In addition, the reader would do well to have some basic knowledge of Galois theory, module theory and commutative Algebra; these fields are not always touched upon in an introductory course. As is standard in algebraic number theory, all rings are assumed to be commutative with 1.

2 Algebraic Integers

2.1 Rings of Integers

Our first step in setting up the framework required in order to gain a satisfactory understanding of why Lamé's proof fails is to generalize the notion of an integer. The following definitions lay the foundations for this.

Definition 2.1. A number field is a finite extension $K|\mathbb{Q}$.

Definition 2.2. We say that an element a of K is an **algebraic integer** of K if a is the root of a monic polynomial in $\mathbb{Z}[x]$. The set of all algebraic integers of K by $\mathcal{O}_K$.

Definition 2.3. More generally, for a ring extension $A \subset B$ we say that $b \in B$ is **integral** over A if b is the root of some monic polynomial with coefficients in A. If all elements of B are integral over A, we simply say that B is **integral** over A.

The set $\mathcal{O}_K$ defined above is in fact a ring. A rather straightforward approach to this would be to show that $\mathcal{O}_K$ is a subring of K, which would essentially reduce to showing that given two elements $a, b \in \mathcal{O}_K$ we have that the difference and product $a - b, ab \in \mathcal{O}_K$. This is easier said than done with the tools currently available to us, as given monic polynomials with roots a and b it is not completely obvious as to how one would construct monic polynomials with roots $a-b$. It will therefore be of interest to find a condition on elements of K that is equivalent to being an algebraic integer.

Lemma 2.1. *Suppose we are given an extension of rings $A \subset B$. The elements of the finite subset $\{b_1, \dots, b_n\}$ of B is are algebraic over $A \iff$ the ring $A[b_1, \dots, b_n] = \{g(b_1, \dots, b_n) \mid g \in A[x_1, \dots, x_n]\}$ is finitely generated as an A-module.*

Proof. We begin by proving the $\implies$ part of the statement. Suppose first that b is an element of B that is integral over A. There must then exist some monic polynomial $f(x) \in A[x]$ such that $f(b) = 0$ for each by hypothesis. Now for any $g(x) \in A[x]$ the division algorithm may be applied to get $g(x) = f(x)q(x)+r(x)$, with $\deg r(x) < n$. Hence $g(b) = f(b)q(b) + r(b)$, and since $f(b) = 0$ this reduces to $g(b) = r(b)$, so that each element of $A[b]$ may be written on the form $\sum_0^{n-1} a_i b^i$, with $a_i \in A$. Hence $\{1, b, \dots, b^{n-1}$ is a set of genertors of $A[b]$ and thus it follows that $A[b]$ is finitely generated as an A-module.

Now assume instead that finitely many elements $b_1, \dots, b_n$ are integral over A. By the above we may then find a finite set of generators X_i for each A-module $A[b_i]$. The cardinality of the product $X = \prod_1^n X_i = \{\prod_1^n x_i \mid x_i \in X\}$ is clearly bounded by $\prod_1^n |X_i|$, which is finite. The set X generates $A[b_1, \dots, b_n]$ as an A-module, so $A[b_1, \dots, b_n]$ is a finitely generated A-module whenever the adjoined elements are integral over A.

For the converse implication $\impliedby$, consider some set of finitely many generators $\{e_1, \dots, e_n\}$ of $A[b_1, \dots, b_n]$ and let $b = b_i$ act on these as an A-linear transformation by multiplication. In terms of matrices, this takes the form

$$b \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix} = M_b \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix},$$

for some $n \times n$ matrix M_b with coefficients in A. If we rewrite this as the equivalent matrix equation

$$(bI - M_b) \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix}$$

it is immediate that $\det(bI - M_b) = 0$. This proves that b is a root of the characteristic polynomial $\det(xI - M_b)$ of M_b, i.e. a monic polynomial contained in $A[x]$ of degree n. Hence b_i is integral for each i. □

Corollary 2.1.1. *Suppose $A \subset B$ is a ring extension and that $b_1, b_2 \in B$ are integral over A. Then so are $b_1 - b_2$ and $b_1 b_2$.*

Proof. The elements $b_1 - b_2$ and b_1, b_2 are elements of $A[b_1, b_2]$, so that in fact

$$A[b_1, b_2, b_1 - b_2, b_1 b_2] = A[b_1, b_2],$$

from which the statement immediately follows. □

Corollary 2.1.2. *Integrality is transitive; if $A \subset B \subset C$, B is integral over A and C is integral over B, then C is integral over A.*

Proof. Let c be any element of C. Then $B[c]$ is a finitely generated B-module and c satisfies some monic polynomial of $B[x]$, so that $c^n + b_{n-1} + c^{n-1} \ldots + b_0 = 0$. Setting $R = A[b_{n-1}, \ldots, b_0]$, it is clear that $R[c]$ is finitely generated as an R-module. Since R is finitely generated as an A-module, this gives that $R[c]$ is actually also finitely generated as an A-module. In fact, $R[c] = A[b_{n-1}, \ldots, b_0; c]$, so c is therefore integral over A. □

Corollary 2.1.3. *The set $\mathcal{O}_K$ is a subring of K; we call it the **ring of integers** of K and in general we call rings of integers **number rings**.*

Definition 2.4. Given an extension of rings $A \subset B$, we call the ring $\overline{A} = \{b \in B \mid b \text{ is integral over } A\}$ the integral closure of A in B. In particualar, $\mathcal{O}_K$ is the algebraic closure of $\mathbb{Z}$ in K.

In consideration of the above, it might be tempting to try to prove that the cyclotomic integers $\mathbb{Z}[\omega_p]$ is the ring of integers of the corresponding cyclotomic field $\mathbb{Q}(\omega_p)$. While this is indeed the case, a proving this statement is better left for later, when we will have access to better tools for doing so. The ring of integers of $\mathbb{Q}(\sqrt{d})$, however, will not be much easier to determine later and will be of great importance to us. One could perhaps to be lead to think that this number ring is simply the ring $\mathbb{Z}[\sqrt{d}]$, but things turn out to be somewhat more interesting.

Theorem 2.2. *Let d be a squarefree integer and $K = \mathbb{Q}(\sqrt{d})$. Then $\mathcal{O}_K$ is $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ if $d \equiv 1 \bmod 4$ and $\mathbb{Z}[\sqrt{d}]$ otherwise.*

Proof. The field K consists of elements of the form $a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$, so finding the elements of $\mathcal{O}_K$ essentially reduces to figuring out when one of these is the root of a monic polynomial with integer coefficients. This is equivalent to the minimal polynomial $m(x)$ having integer coefficients.

Any $a+b\sqrt{d} \in K \backslash \mathbb{Q}$ has a minimal polynomial of degree 2. The polynomial $(x-a+b\sqrt{d})(x-a-b\sqrt{d}) = x^2 - 2ax + a^2 - b^2 d$ is a monic polynomial of degree 2 with $a+b\sqrt{d}$ as a root and is therefore its minimal polynomial $m(x)$. Hence $a + b\sqrt{d} \in \mathcal{O}_K$ if and only if both $-2a$ and $a^2 - b^2 d$ are integers.

Regardless of d, the only possibility for a to be something other than an integer is if $a = \frac{a'}{2}$ with a' an odd integer. Setting $b = \frac{b'}{2}$, with $b' \in \mathbb{Q}$, we get that the above has to coincide with

$$\frac{a'^2 - b'^2 d}{4} \in \mathbb{Z},$$

or equivalently

$$a'^2 - b'^2 d \equiv 0 \bmod 4,$$

which shows both that b' must be an integer and that a', b' can only be odd at the same time and that this is possible if and only if $d \equiv 1 \bmod 4$, from which the original statement immediately follows. □

2.2 Trace, Norm and Discriminant

We now define the trace and norm of a number field, which gives us two very potent tools to work with. The norm in particular will be of great importance in many proofs that lie ahead.

Definition 2.5. Let $L|K$ be a finite extension of fields and define T_α to be the endomorphism on L as a K-vector space given by sending β to $\alpha\beta$, for each $\beta \in L$. The functions

$$Tr_{L|K}(\alpha) = Tr(T_\alpha), \quad N_{L|K}(\alpha) = \det(T_\alpha)$$

are then called the **trace** and **norm** of $L|K$, respectively.

If the extension is separable, one may alternatively characterize them as follows.

Theorem 2.3. *Suppose $L|K$ is a separable extension of fields. Let $H = \mathrm{Hom}_K(L, \overline{K})$ be the set of K-embeddings of L into an algebraic closure $\overline{K}$ of K. Then the trace and norm can equivalently be defined by*

$$Tr_{L|K} : \alpha \mapsto \sum_{\sigma \in H} \sigma(\alpha), \quad N_{L|K} : \alpha \mapsto \prod_{\sigma \in H} \sigma(\alpha)$$

and the characteristic polynomial $f_\alpha(x)$ is a power of the minimal polynomial $m_\alpha(x)$.

Proof. Let $m_\alpha(x)$ be the minimal polynomial of α over K and set $d = \deg m_\alpha(x) = [K(\alpha) : K]$ and $n = [L : K(\alpha)]$. We clearly have that $1, \dots, \alpha^{d-1}$ is a basis of $K(\alpha)|K$ as a K-vector space, so given a basis $\beta_1, \dots, \beta_n$ of $L|K(\alpha)$ as a $K(\alpha)$-vectorspace, we have that

$$\beta_1, \dots, \beta_1\alpha^{d-1}; \dots; \beta_n, \dots, \beta_n\alpha^{d-1}$$

is a basis of $L|K$ as a K-vector space. The matrix for T_α with respect to this basis simply becomes a block diagonal matrix with n identical blocks whose characteristic polynomial are the minimal polynomial $m_\alpha(x)$ of α. It follows that $f_\alpha = m_\alpha^n$.

The set H is partitioned by the equivalence relation

$$\sigma \sim \tau \iff \sigma(\alpha) = \tau(\alpha)$$

into n different equivalence classes each containing d elements. Let S be a set of representatives. Then clearly

$$m_\alpha(x) = \prod_{\sigma \in S} (x - \sigma(\alpha))$$

and so $f_\alpha(x) = \left(\prod_{\sigma\in S}(x - \sigma(\alpha))\right)^n = \prod_{\sigma\in H}(x-\sigma(\alpha))$. Now let a_k denote the coefficient of the x^k-term in f_α. The trace is clearly equal to $-a_{nd-1}$ and the norm to $(-1)^{nd}a_0$, from which it now follows that

$$Tr_{L|K}(\alpha) = \sum_{\sigma\in H} \sigma(\alpha), \quad N_{L|K}(\alpha) = \prod_{\sigma\in H} \sigma(\alpha).$$

□

The trace and norm have some very useful properties. For instance, it is clear from either definition that $N_{L|K}(\alpha\beta) = N_{L|K}(\alpha)N_{L|K}(\beta)$. The norm in particular will be crucial in proving that $\mathbb{Z}[\omega_{23}]$ is not a UFD. We therefore state and prove a handful of results about the trace and norm below.

Theorem 2.4. *Let A be a ring, K its field of fractions, $L|K$ a separable extension, B the integral closure of A in L and b an element of B. Then*

$$Tr_{L|K}(b), N_{L|K}(b) \in A.$$

Proof. Let $m_b(x)$ be the minimal polynomial of b over K and d its degree. $-Tr_{L|K}(b)$ and $\pm N_{L|K}(b)$ are clearly the coefficient of x^{d-1} and the constant term, respectively, so they are therefore both contained in K. Each conjugate $\sigma(b)$ is algebraic over A due to being a root of $m_b(x)$, and as such of any polynomial in $K[x]$ having b as a root. By Corollary 2.1.1 the trace and norm of α are then both algebraic over A and contained in K. They are therefore in particular elements of B. □

Theorem 2.5. *Suppose that $K \subset L \subset M$ is a tower of finite separable extensions. We then have that*

$$N_{M|K} = N_{L|K} \circ N_{M|L}.$$

Proof. The relation

$$\sigma \sim \tau \iff \sigma|_L = \tau|_L$$

on the set $H = \mathrm{Hom}_K(L, \overline{K})$, with $\overline{K}$ an algebraic closure of K, is clearly an equivelence relation and as such it partitions G into $n = [L : K]$ equivalence classes, with representatives $\sigma_1, \dots, \sigma_n$. It follows that

$$Tr_{M|K}(\alpha) = \sum_{\sigma\in H} \sigma(\alpha) = \sum_1^n \sum_{\sigma\sim\sigma_i} \sigma(\alpha) = \sum_1^n \sigma_i(Tr_{M|L}(\alpha)) = Tr_{L_K} \circ Tr_{M|L}(\alpha),$$

where the last equality is due to $Tr_{M|L}(\alpha) \in L$. The proof for the norm is identical but with the sums replaced by products. □

Theorem 2.6. *Suppose $L|K$ is a finite separable extension, such that the extension of rings $A \subset B$ has the properties that B is the integral closure of A in L and that A, B have K, L as their respective field of fractions. Then $N_{L|K}(b)$ is a unit of A if and only if b is a unit of B.*

Proof. Suppose first that $N_{L|K}(b)$ is a unit of A and let $H = \mathrm{Hom}_K(L, \overline{K})$, with $\overline{K}$ being an algebraic closure of K. The element b is integral over A by hypothesis and therefore is the root of some polynomial $f(x) \in A[x]$. The minimal polynomial $m_\alpha(x) \in K[x]$ must divide this polynomial and as such $\sigma(b)$ is also integral over A, for each $\sigma \in H$.

Now $N_{L|K}(b)$ is a unit, so $aN_{L|K}(b) = 1$ for some $a \in A$. There exists at least one K-embedding $\sigma \in H$ that sends b to itself, so $ab^{-1}N_{L|K}(b) = ab^{-1}\prod_{\sigma\in H}\sigma(b)$ is an element of L that is a product of integral elements; it is therefore an element of B. In particular, this means that we have found an inverse of b in B, so b is a unit.

Conversely, if b is a unit of V, it is an immediate consequence that $N_{L|K}(b)$ is indeed a unit of A, as $N_{L|K}(b)N_{L|K}(b^{-1}) = N_{L|K}(1) = 1$. □

We are now done with establishing the properties of the trace and norm that we will need later on. Let us therefore introduce an important invariant of a number field, the discriminant.

Definition 2.6. Let $\alpha_1, \ldots, \alpha_n$ be a basis of a separable extension $L|K$. The **discriminant** of the basis is then defined by

$$d(\alpha_1, \ldots, \alpha_n) = \det((\sigma_i\alpha_j))^2,$$

where σ_i runs through the n K-embeddings of L into an algebraic closure of K and $(\sigma_i\alpha_j)$ denotes the $n \times n$ matrix with $\sigma_i\alpha_j$ as its ij entry.

The discriminant may be equivalently defined by $d(\alpha_1, \ldots, \alpha_n) = \det(Tr_{L|K}(\alpha_i\alpha_j))$. This is due to the identity $Tr_{L|K}(\alpha_i\alpha_j) = \sum_k(\sigma_k\alpha_i)(\sigma_k\alpha_j)$, which shows that the matrix $(Tr_{L|K}(\alpha_i\alpha_j)$ is in fact equal to the product $(\sigma_i\alpha_j)^t(\sigma_i\alpha_j)$, whose determinant is clearly equal to that of $((\sigma_i\alpha_j))^2$.

Let $A \subset B$ be a ring extension with corresponding extension $L|K$ for their respective field of fractions and B is the integral closure of A in L. One may wonder if there is any K-basis of $L|K$ that is also an A-basis of B. After proving a lemma below, we shall be able to establish that this is indeed the case when A is a PID.

Lemma 2.7. *Suppose $\alpha_1, \ldots, \alpha_n$ is a basis with discriminant d of $L|K$ that is contained in B. Then*

$$dB \subset A\alpha_1 + \ldots + A\alpha_n.$$

Proof. Let b be an arbitrary element of B, which may of course be written on the form

$$b = \sum_1^n a_k\alpha_k,$$

with $a_k \in K$. Multiplying by α_i and then applying the trace on both sides of the above equation gives

$$Tr_{L|K}(\alpha_i b) = \sum_{k=1}^n Tr_{L|K}(\alpha_i\alpha_k)a_k,$$

as each K-embedding of L fixes K and therefore a_k. Both α_k and b are elements of B and so $Tr_{L|K}(\alpha_i b)$ is contained in A. Solving for a_k by means of Cramer's rule shows that

$$a_k = \frac{d_k}{\det(Tr_{L|K}(\alpha_i\alpha_j))} = \frac{d_k}{d},$$

with d_k being the determinant of the matrix $(Tr_{L|K}(\alpha_i\alpha_j))$ but with the k^{th} column replaced with a column with entries $Tr_{L|K}(\alpha_i b)$. The matrix in question has entries in A and therefore its determinant d_k is also in A. Hence a_j is in fact the quotient of an element of A by d, or equivalently $db \in A\alpha_1 + \ldots + A\alpha_n$. Since b was taken to be an arbitrary element of B, we have that $db \in A\alpha_1 + \ldots + A\alpha_n$ for any $b \in B$, and so the desired statement follows. □

Theorem 2.8. *Suppose $L|K$ is separable and A a PID. Then every finitely generated B-submodule $M \neq 0$ of L is isomorphic to the free A-module A^n of rank n as an A-module, where $n = [L : K]$. The ring B therefore admits an integral basis over A.*

Proof. Suppose we are given a finitely generated B-submodule $M \neq 0$. Let $\alpha_1, \ldots, \alpha_n$ be a basis of $L|K$. Since each α_i is a root of its minimal polynomial $m_{\alpha_i}(x) \in K[x]$, we may assume that the basis is contained in B.

This can be seen by noting that α_i must be a root of its minimal polynomial $m_{\alpha_1}(x) \in K[x]$, whose degree we denote by d and mutliplying by a power of the product ℓ of the denominators of the coefficients of this polynomial. More precisely, if $a_0, \ldots, a_d$ are the coefficients, we have that

$$\sum_{j=0}^{d} a_j \ell^{d-j} (\ell \alpha_i)^j = 0,$$

so that $\ell\alpha_i$ is the root of the monic polynomial $\sum_{j=0}^{d} a_j \ell^{d-j} x^j \in A[x]$ and is therefore integral over A.

It therefore follows from Lemma 2.7 that

$$dB \subset A\alpha_1 + \ldots + A\alpha_n,$$

and hence $\operatorname{rank}(B) \leq n$. We need not settle for a bound of the rank, however; any basis of B as an A-module must span L as a K-vector space, and so $\operatorname{rank}(B) = n$.

Now let $\mu_1, \ldots, \mu_r$ be a basis of the given finitely generated B-submodule $M \neq 0$ of L. We may argue as we did above for the basis of L that there is some $a \in A \setminus \{0\}$ such that $aM \subset B$, so that

$$daM \subset dB \subset A\alpha_1 + \ldots, A\alpha_n.$$

As the right-most module in this series of inclusions is a free A-module, so is daM and therefore equivalently M, by the theory of modules over PID's. We therefore have

$$n = \operatorname{rank}(B) \leq \operatorname{rank}(M) = \operatorname{rank}(daM) \leq \operatorname{rank}(dB) = \operatorname{rank}(B) = n,$$

and so $\operatorname{rank}(M) = n$. □

The discriminant of a $\mathbb{Z}$-basis of $\mathcal{O}_K$ is simply called the discriminant of K. It is unique up to sign, since any matrix changing from one $\mathbb{Z}$-basis of $\mathcal{O}_K$ to another must have determinant ± 1, or the other basis would necessarily have to contain some element not in $\mathcal{O}_K$. Hence if $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ are two $\mathbb{Z}$-bases of $\mathcal{O}_K$ and T the matrix from $\alpha_1, \ldots, \alpha_n$ to $\beta_1, \ldots, \beta_n$, then

$$d(\alpha_1, \ldots, \alpha_n) = (\det T)^2 d(\beta_1, \ldots, \beta_n) = d(\beta_1, \ldots, \beta_n),$$

which shows that it is not misguided to talk about *the* discriminant of K.

We now round of this section by proving two results about the discriminant that will be used later.

Theorem 2.9. *Suppose the extension $L|K$ is separable and that $\alpha_1, \ldots, \alpha_n$ is a basis. Then*

$$(x, y) = Tr_{L|K}(xy)$$

is a non-degenerate bilinear form and

$$d(\alpha_1, \ldots, \alpha_n) \neq 0.$$

Proof. The second part of the statement clearly follows from the first, so it suffices to show that (x, y) is a non-degenerate bilinear form. $L|K$ is separable, so there exists a primitive element α, so that $1, \alpha, \ldots, \alpha^{n-1}$ is a K-basis of L. With respect to this basis, (x, y) takes the form

$$(x, y) = xMy,$$

where M is the $n \times n$ matrix given by $M = (Tr_{L|K}(\alpha^{i-1}\alpha^{j-1}))$. Now let $\sigma_1, \ldots, \sigma_n$ be the K-embeddings of L into an algebraic closure of K. Since

$$\det Tr_{L|K}(\alpha^{i-1}\alpha^{j-1}) = d(1, \alpha, \ldots, \alpha^{n-1}) = \det((\sigma_i \alpha^{j-1}))^2,$$

we have from the fact that $((\sigma_i \alpha^{j-1}))$ is a Vandermonde matrix that

$$\det M = \prod_{i<j} (\sigma_i \alpha - \sigma_j \alpha)^2 \neq 0,$$

where the inequality is due to the separability of $L|K$. □

Theorem 2.10. *Let $N \subset M$ be two non-zero finitely generated $\mathcal{O}_K$-submodules of K. Then*

$$d(N) = [M : N]^2 d(M).$$

Proof. The modules M and N are also finitely generated free $\mathbb{Z}$-modules. The index $[M : N]$ is simply equal to the absolute value of the determinant of any matrix representing the injection homomorphism $N \hookrightarrow M$, i.e. a change of base matrix that changes from a basis of N to a basis of M. Since M and N are isomorphic to $\mathbb{Z}^n$ as $\mathbb{Z}$-modules, with n equal to the degree $[K : \mathbb{Q}]$, by Theorem 2.8. Identifying M with a copy of $\mathbb{Z}^n$ and N with an embedding therein, we may consider any matrix A representing the injection map. This matrix A is invertible as a matrix over $\mathbb{Q}$ and therefore has a Smith normal form PAQ with no zeroes on the diagonal. The index $[M : N]$ is therefore given by $[M : N] = [\mathbb{Z}^n : A\mathbb{Z}^n] = [\mathbb{Z}^n : PAQ\mathbb{Z}^n] = \det D = |\det A|$ and thus the desired statement follows. □

We round off the section by proving that the ring of cyclotomic integers $\mathbb{Z}[\omega_p]$ is, as its name suggests, the ring of integers of the corresponding cyclotomic field $\mathbb{Q}(\omega_p)$.[1]

Theorem 2.11. *The ring $\mathbb{Z}[\omega_p]$ is the ring of integers of $\mathbb{Q}(\omega_p)$.*

Proof. Let ϕ_p denote the minimal polynomial of ω over $\mathbb{Q}$, $\omega := \omega_p$ and $\mathcal{O}$ the ring of integers of $\mathbb{Q}(\omega)$. The ring $\mathbb{Z}[\omega]$ is clearly a subring of $\mathcal{O}$. The discriminant of $1, \omega, \ldots, \omega^{p-1}$ is given by

$$d(1, \omega, \ldots, \omega^{p-1}) = \pm \prod_{i \neq j} (\omega^i - \omega^j) = \prod_{1}^{p-1} \phi_p'(\omega^i) = N_{K|\mathbb{Q}}(\phi_p'(\omega)).$$

Now differentiating on both sides of

$$(x-1)\phi_p(x) = x^p - 1$$

yields the polynomial equation

$$\phi_p(x) + (x-1)\phi_p'(x) = px^{p-1}$$

and evaluating at ω shows that

$$(\omega - 1)\phi_p'(\omega) = p\omega^{p-1}.$$

The element ω^{p-1} is a unit and therefore has a norm of ± 1. As for $\omega - 1$, its norm is the product $\prod_1^{p-1}(\omega^k - 1) = p$. Taking the norm and then dividing by p on both sides of the above equation therefore gives

$$d(1, \omega, \ldots, \omega^{p-1}) = \pm N_{K|\mathbb{Q}}(\phi_p'(\omega)) = \pm p^{p-2}.$$

Before proceeding, we show that $(\omega - 1)$ is a prime ideal of $\mathcal{O}$ lying over p of intertia degree 1. We have in terms of ideals that $\prod_1^{p-1}(\omega^k - 1)\mathcal{O} = p\mathcal{O}$, so it suffices to show that $(\omega^k - 1)\mathcal{O} = (\omega - 1)\mathcal{O}$. Now $\frac{\omega^k - 1}{\omega - 1} = \sum_0^{k-1} \omega^i$ is clearly an element of $\mathbb{Z}[\omega]$ and therefore $\mathcal{O}$, so $(\omega - 1)\mathcal{O} \supset (\omega^k - 1)\mathcal{O}$. Next, take j to be a positive integer such that $jk \equiv 1 \bmod p$. Then $\sum_{i=1}^{j-1} \omega^{ki} = \frac{(\omega^j)^k - 1}{\omega^k - 1} = \frac{\omega - 1}{\omega^k - 1}$ shows that in fact the reverse inclusion $(\omega - 1)\mathcal{O} \subset (\omega^k - 1)\mathcal{O}$ holds, so that the ramification index is $p - 1$ and therefore the inertia degree 1.

Now set $d = d(1, \omega, \ldots, \omega^{p-1})$. By Lemma 2.7 we then have that

$$p^{p-2}\mathcal{O} = d\mathcal{O} \subset \mathbb{Z} + \mathbb{Z}\omega + \ldots + \mathbb{Z}\omega^{p-1} = \mathbb{Z}[\omega] \subset \mathcal{O}.$$

The inertia degree of $(\omega - 1)$ over p is 1, i.e. $[\mathcal{O}/(\omega - 1) : \mathbb{Z}/(p)] = 1$, from which it follows that $\mathcal{O}/(\omega - 1) \cong \mathbb{Z}/(p)$. Hence $\mathcal{O} = \mathbb{Z} + (\omega - 1)\mathcal{O}$, which of course implies that

$$\mathcal{O} = \mathbb{Z}[\omega] + (\omega - 1)\mathcal{O}. \tag{1}$$

Multiplying by $\omega - 1$ give

$$(\omega - 1)\mathcal{O} = (1 - \omega)\mathbb{Z}[\omega] + (\omega - 1)^2\mathcal{O} \subset \mathbb{Z}[\omega] + (\omega - 1)^2\mathcal{O}$$

and substitution of $(\omega - 1)\mathcal{O}$ in (1) now yields

$$\mathcal{O} \subset \mathbb{Z}[\omega] + (\omega - 1)^2\mathcal{O}.$$

Repeating this argument $(p-2)^2 - 2$ times finally shows that

$$\mathcal{O} \subset \mathbb{Z}[\omega] + p^{p-2}\mathcal{O} = \mathbb{Z}[\omega] + d\mathcal{O} \subset \mathbb{Z}[\omega] + \mathbb{Z}[\omega] = \mathbb{Z}[\omega].$$

□

[1] The statement actually holds for arbitrary positive n. This is however not used in this paper and requires a bit more work; it is therefore omitted, but the interested reader may consult for instance [4] or [5].

3 Dedekind Domains

3.1 Unique Ideal Factorization

While unique factorization of elements generally fails for number rings, it turns out that ideals factor uniquely into a product of prime ideals. In fact, rings of integers are contained in a larger class of rings, called Dedekind domains, that all share the property of unique factorization of ideals into prime ideals.

Definition 3.1. A Dedekind domain is an integral domain that is noetherian and integrally closed whose prime ideals $\mathfrak{p} \neq 0$ are all maximal.

Theorem 3.1. *Every number ring $\mathcal{O}_K$ is a Dedekind domain.*

Proof. The ring $\mathcal{O}_K$ is clearly integrally closed, as it is the integral closure of $\mathbb{Z}$ in K.

Every ideal of $\mathcal{O}_K$ is contained in K. Hence they are all finitely generated free $\mathbb{Z}$-modules by Theorem 2.8, and must therefore also be finitely generated as a $\mathcal{O}_K$-modules. Hence $\mathcal{O}_K$ is noetherian.

An ideal $\mathfrak{a}$ of a ring A is maximal if and only if $A/\mathfrak{a}$ is a field and every finite integral domain is a field. It therefore suffices to show that $\mathcal{O}_K/\mathfrak{p}$ is finite for every prime ideal $\mathfrak{p} \neq 0$ of $\mathcal{O}_K$.

The set $\mathfrak{p} \cap \mathbb{Z}$ is clearly a prime ideal of $\mathbb{Z}$, as it is the contraction of $\mathfrak{p}$ via the unique[2] homorophism $\mathbb{Z} \hookrightarrow \mathcal{O}_K$. It is in fact also non-zero, which we may see by fixing an element $\pi \in \mathfrak{p} \setminus \{0\}$ and considering some monic polynomial with coefficients in $\mathbb{Z}$ with π, but not 0, as a root; we know such a polynomial must exist since π is an algebraic integer and since 0 cannot possibly be conjugate to π. Suppose this polynomial has coefficients $a_0, \ldots, a_{n-1}$, so that

$$\pi^n + a_{n-1}\pi^{n-1} + \ldots + a_0.$$

This shows that $a_0 \in \mathbb{Z} \cap \mathfrak{p}$, and so this ideal is non-zero. It is therefore equal to $p\mathbb{Z}$, for some rational prime p.

Note that $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module, as are both $\mathcal{O}_K/\mathfrak{p}$ and $\mathcal{O}_K/p\mathcal{O}_K$. In particular, it is clear that

$$|\mathcal{O}_K/\mathfrak{p}| \leq |\mathcal{O}_K/p\mathcal{O}_K|. \tag{2}$$

It follows from the $\mathbb{Z}$-module isomorphisms

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{Z}^n/p\mathbb{Z}^n \cong (\mathbb{Z}/p\mathbb{Z})^n$$

that the order of $\mathcal{O}_K/p\mathcal{O}_K$ is p^n. Hence it follows from (2) that $\mathcal{O}_K/\mathfrak{p}$ is also finite and therefore a field. □

With this basic fact established we now develop the theory of ideal factorization in the more general case of a Dedekind domain $\mathcal{O}$ with field of fractions K. As a natural generalization of the case of PID's, we say that an ideal $\mathfrak{a}$ divides another ideal $\mathfrak{b}$, denoted $\mathfrak{a} \mid \mathfrak{b}$, if $\mathfrak{a} \supset \mathfrak{b}$. The notion of a greatest common divisor and least common multiple are similarly defined by $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$ and $\operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$. The following definition, however, is in some sense more novel.

Definition 3.2. For any non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}$, we define a corresponding so-called **fractional ideal** $\mathfrak{p}^{-1}$ by $\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subset \mathcal{O}\}$.

Having set up the basic terminology, we may now start setting up the proof for unique factorization.

Lemma 3.2. *Suppose $\mathfrak{a} \neq 0$ is an ideal of $\mathcal{O}$. Then there exists a product $\prod_1^r \mathfrak{p}_i$ of non-zero prime ideals contained in $\mathfrak{a}$.*

Proof. Assume that the set S of ideals not satisfying this condition is non-empty. Dedekind domains are noetherian, so S must contain a maximal element $\mathfrak{m}$. This ideal cannot be prime, for it were then $\mathfrak{m}$ would be a prime product contained in $\mathfrak{m}$, contradicting $\mathfrak{m}$'s inclusion in S. We can must therefore be able to find elements $x_1, x_2 \in \mathcal{O}$ such that $x_1x_2 \notin \mathfrak{m}$ but $x_1, x_2 \notin \mathfrak{m}$. Now let $\mathfrak{m}_1 = (x_1) + \mathfrak{m}$ and similarly $\mathfrak{m}_2 = (x_2) + \mathfrak{m}$, which are both clearly not contained in S by the maximality of $\mathfrak{m}$. It is also clear that $\mathfrak{m} \subsetneq \mathfrak{m}_1, \mathfrak{m}_2$ and that $\mathfrak{m}_1\mathfrak{m}_2 \subset \mathfrak{m}$. Since neither $\mathfrak{m}_1$ nor $\mathfrak{m}_2$ are in S, they must both contain a product of primes, and so $\mathfrak{m}$ must contain the product of these products, which is also a product of primes. This is a contradiction; the set S must therefore be empty. □

[2] The homomorphism is unique since $\mathbb{Z}$ is initial in **Ring**.

Lemma 3.3. *Let $\mathfrak{a} \neq 0$ be an ideal of $\mathcal{O}$ and $\mathfrak{p}$ a prime ideal. Then*

$$\mathfrak{a}\mathfrak{p}^{-1} = \{\sum_{1}^{n} a_i x_i \mid a_i \in \mathfrak{a}, x_i \in \mathfrak{p}^{-1}, n \in \mathbb{Z}\} \neq \mathfrak{a}.$$

Proof. We begin by showing that for any prime ideal $\mathfrak{p}$ we have that $\mathfrak{p}^{-1} \neq \mathcal{O}$. Take a to be a non-zero element of $\mathfrak{p}$, and suppose we have $\mathfrak{p}_1 \dots \mathfrak{p}_r \subset (a) \subset \mathfrak{p}$, with r as small as possible. These ideals are all prime, so $\mathfrak{p}_1 \subset \mathfrak{p}$ after suitable re-indexing. In fact, since all non-zero prime ideals of Dedekind domains are maximal, we must actually have $\mathfrak{p}_1 = \mathfrak{p}$. We cannot have $\mathfrak{p}_2 \dots \mathfrak{p}_r \subset (a)$, for this would contradict the minimality of r. It is therefore possible to find an element b of $\mathfrak{p}_2 \dots \mathfrak{p}_r$ such that $b \notin (a) = a\mathcal{O}$. This is clearly equivalent to $a^{-1}b \notin \mathcal{O}$. Note also that $a^{-1}b\mathfrak{p} \subset a^{-1}\mathfrak{p}\mathfrak{p}_2 \dots \mathfrak{p}_r \subset a^{-1}(a) = (1) = \mathcal{O}$. This shows that $a^{-1}b$ is in fact an element of $\mathfrak{p}^{-1}$ not contained in $\mathcal{O}$. It therefore follows that $\mathfrak{p}^{-1} \neq \mathcal{O}$.

Now take $\mathfrak{a}$ to be any non-zero ideal of $\mathcal{O}$ generated by $\alpha_1, \dots, \alpha_n$. We assume, in order to get a contradiction, that $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}$. We can then for each $b \in \mathfrak{p}^{-1}$ write

$$b\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j,$$

with the a_{ij} being elements of $\mathcal{O}$. Denote the matrix $(b\delta_{ij} - a_{ij})$ by A and observe that by definition it must satisfy

$$A \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = 0.$$

We therefore have that $\det A = 0$, and so b is a zero of the monic polynomial $\det(x\delta_{ij} - a_{ij})$ with coefficients in $\mathcal{O}$, so that b is in fact integral over $\mathcal{O}$. But $\mathcal{O}$ is integrally closed in K, so b must be an element of $\mathcal{O}$, for every element b of $\mathfrak{p}^{-1}$. The fractional ideal $\mathfrak{p}^{-1}$ must therefore be equal to $\mathcal{O}$, which contradicts what we showed about $\mathfrak{p}^{-1}$ earlier. Hence it follows that $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$. □

Theorem 3.4. *Every non-zero proper ideal $\mathfrak{a}$ of $\mathcal{O}$ admits a factorization into non-zero prime ideals*

$$\mathfrak{a} = \prod_{1}^{r} \mathfrak{p}_i^{\nu_i},$$

which is unique up to permutation of factors if we require that the prime ideals $\mathfrak{p}_i$ be distinct.

Proof. We start by proving that each ideal has some factorzation. Once this has been established we show that it is also unique.

Let S be the set of non-zero proper ideals of $\mathcal{O}$ that do not factor into prime ideals. If it is non-empty, it must have a maximal element, say $\mathfrak{m}$, since $\mathcal{O}$ is noetherian. The fractional ideal $\mathfrak{p}^{-1}$ clearly properly contains all of $\mathcal{O}$ and $\mathfrak{p}\mathfrak{p}^{-1}$ must be equal to $\mathcal{O}$ by how $\mathfrak{p}^{-1}$ is defined, so

$$\mathfrak{m} \subsetneq \mathfrak{m}\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}.$$

In particular this shows that, $\mathfrak{m}\mathfrak{p}^{-1}$ is an ideal of $\mathcal{O}$ properly containing $\mathfrak{m}$. By $\mathfrak{m}$'s maximality, $\mathfrak{m}\mathfrak{p}^{-1}$ admits a prime factorization $\prod_i \mathfrak{p}_i$. The ideal $\mathfrak{m}$ must then, however, be equal to $\mathfrak{p}\prod_i \mathfrak{p}_i$, which contradicts $\mathfrak{m}$'s inclusion in S. The set S must therefore be empty, so that every non-zero proper ideal admits a prime factorization.

The proof for uniqueness is essentially the proof for the uniqueness part of the fundamental theorem of arithmetic but in the language of ideals and can be found in [5]. □

With the above theorem proven, let us now generalize the notion of a fractional ideal and prove a useful statement about these.

Definition 3.3. We call a subset of K a **fractional ideal** if it is a non-zero finitely generated $\mathcal{O}$-submodule of K. A fractional ideal is said to be **principal** if it is of the form $a\mathcal{O}$, with a a unit of K. We sometimes call the ideals of $\mathcal{O}$ **integral ideals**, to emphasize that fractional ideals are generally not ideals.

Theorem 3.5. *The set J_K of all fractional ideals is a free abelian group generated by the non-zero prime ideals of $\mathcal{O}$. The identity of J_K is $\mathcal{O}$ and the inverse of any fractional ideal $\mathfrak{a}$ is given by $\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subset \mathcal{O}\}$.*

Proof. Multiplication of fractional ideals is clearly an associative and commutative operation that J_K is closed under, $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$ for any fractional ideal $\mathfrak{a}$ and $\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subset \mathfrak{o}\}$ is clearly a fractional ideal whenever $\mathfrak{a}$ is.

The set $\mathfrak{a}\mathfrak{a}^{-1} = \{\sum_i a_i x_i \mid a_i \in \mathfrak{a}, x_i \in \mathfrak{a}^{-1}\}$ clearly contains 1, as $\mathfrak{a}$ is a finitely generated $\mathfrak{o}$-module and as such we may form the least common multiple ℓ and consider $\ell\mathfrak{a}$. Now $\ell\mathfrak{a}$ clearly has inverse $(\ell\mathfrak{a})^{-1} = \ell^{-1}\mathfrak{a}^{-1}$, so that in fact $\mathfrak{a}\mathfrak{a}^{-1} = (\ell\mathfrak{a})(\ell\mathfrak{a})^{-1} = \mathfrak{o}$. The set J_K is therefore an abelian group.

Every fractional ideal $\mathfrak{a}$ must by definition be of the form

$$\mathfrak{a} = \alpha_1\mathfrak{o} + \ldots + \alpha_n\mathfrak{o},$$

with each α_i an element of K. This can clearly be made into an integral ideal by multiplying by some element b of $\mathfrak{o}$, i.e. .

$$b\mathfrak{a} \subset \mathfrak{o}.$$

Both $(b)\mathfrak{a}$ and (b) have unique prime factorizations $(b)\mathfrak{a} = \prod_i \mathfrak{p}_i$ and $(b) = \prod_j \mathfrak{q}_j$. Multiplying $\mathfrak{a}$ by the fractional ideal $(b)^{-1} = \prod_j \mathfrak{q}_j^{-1}$ gives a unique prime factorization $\mathfrak{a} = \prod_i \mathfrak{p}_i \prod_j \mathfrak{q}_j^{-1}$ of $\mathfrak{a}$. □

The set P_K consisting of all principal fractional ideals is clearly a subgroup, as $(a\mathfrak{o})(b^{-1}\mathfrak{o}) = (ab^{-1})\mathfrak{o}$ is still principal. Quotienting J_K by P_K gives rise to a new abelian group

$$Cl_K = J_K/P_K.$$

If $\mathfrak{o}$ is a number ring it turns out that Cl_K is finite and that there is an upper bound for its order that depends on K. Its order is denoted h_K and clearly $h_K = 1$ is equivalent to that $\mathfrak{o}_K$ is a PID.

3.2 Splitting and Ramification of Primes

In this subsection $\mathfrak{o}$ is always taken to be a Dedekind extension and K its field of fractions. In the same vein, $L|K$ is a finite field extension and $\mathcal{O}$ the integral closure of $\mathfrak{o}$ in L. We furthermore assume that $L|K$ is separable. The main goal will be to understand how the prime ideals of $\mathfrak{o}$ and $\mathcal{O}$ are connected. This understanding will then be of great use to us in later sections.

Theorem 3.6. *The ring $\mathcal{O}$ is a Dedekind domain*[3].

Proof. The fact that $\mathcal{O}$ is integrally closed is trivial, as it is defined to be the integral closure of $\mathfrak{o}$ in L.

Let $\alpha_1, \ldots, \alpha_n$ be a K-basis of L contained in $\mathcal{O}$ of discriminant d. Then

$$\mathcal{O} \subset \mathfrak{o}\frac{\alpha_1}{d} + \ldots + \mathfrak{o}\frac{\alpha_n}{d},$$

and so in fact every ideal $\mathfrak{A}$ of $\mathcal{O}$ is contained in a finitely generated $\mathfrak{o}$-module and therefore themselves finitely generated $\mathfrak{o}$-submodules. Any set that generates $\mathfrak{A}$ as a $\mathfrak{o}$-module also generates $\mathfrak{A}$ as a $\mathcal{O}$-module and so each ideal of $\mathcal{O}$ is finitely generated and therefore $\mathcal{O}$ is noetherian.

Finally, we prove that each non-zero proper prime ideal of $\mathcal{O}$ is maximal. The contraction $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}$ of a non-zero proper prime ideal $\mathfrak{P}$ of $\mathcal{O}$ with respect to the containment injection is also a proper prime ideal. As $\mathcal{O}$ is integral over $\mathfrak{o}$, it is possible to select a non-zero element $b \in \mathfrak{P}$ such that $b^n + a_1 b^{n-1} + \ldots + a_n = 0$ (or else b would have to be a conjugate of and therefore equal to 0), from which it follows that a_n is a non-zero element of $\mathfrak{p}$. Hence $\mathfrak{p}$ is a non-zero proper prime ideal of $\mathfrak{o}$ and therefore $\mathfrak{o}/\mathfrak{p}$ is a field.

Now consider the map $\iota : \mathfrak{o}/\mathfrak{p} \to \mathcal{O}/\mathfrak{P}$ sending $a \bmod \mathfrak{p}$ to $a \bmod \mathfrak{P}$. This is a well-defined homorphism, since $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}$. Furthermore, it clearly has a trivial kernel, so $\mathfrak{o}/\mathfrak{p}$ may in fact be identified with a subring of the integral domain $\mathcal{O}/\mathfrak{P}$. Since $\mathcal{O}$ is integral over $\mathfrak{o}$ it is also algebraic over $\mathfrak{o}$, which extends to each element of $\overline{\mathcal{O}} = \mathcal{O}/\mathfrak{P}$ being algebraic over $k = \mathfrak{o}/\mathfrak{p}$. Each element $\bar{b}$ of $\overline{\mathcal{O}}$ is contained in the ring extension $k[\bar{b}]$, which is in turn contained in $\overline{\mathcal{O}}$; let $m_b(x)$ be the minimal polynomial of $\bar{b}$ over k. The extension $k[\bar{b}]$ is then isomorphic to $k[x]/m_b(x)$, which is in fact a field, so that each element $\bar{b}$ of $\overline{\mathcal{O}}$ has an inverse contained in $\overline{\mathcal{O}}$. The integral domain $\overline{\mathcal{O}}$ is therefore a field, from which it follows that $\mathfrak{P}$ is maximal. □

[3]It is actually true that $\mathcal{O}$ is a Dedekind domain even when $L|K$ is not separable [5], but this would require a more involved proof and is not a fact that will be used in this paper.

Theorem 3.6 in particular tells us that each each prime $\mathfrak{p}$ of $\mathcal{o}$ has a prime factorization in $\mathcal{O}$ in the sense that we can find primes $\mathfrak{P}_i$ of $\mathcal{O}$ such that

$$\mathfrak{p}\mathcal{O} = \prod_1^r \mathfrak{P}_i{}^{e_i}.$$

Given a factorization of the form above, we say that each $\mathfrak{P}_i$ lies over $\mathfrak{p}$, or equivalently that $\mathfrak{p}$ lies under $\mathfrak{P}_i$. A prime $\mathfrak{P}$ of $\mathcal{O}$ lies over exactly one prime $\mathfrak{p}$ of $\mathcal{o}$, since $\mathfrak{P} \cap \mathcal{o}$ is a non-zero proper prime ideal containing $\mathfrak{p}$ and must therefore equal $\mathfrak{p}$. The number e_i is called the **ramification index** of $\mathfrak{P}_i$ over $\mathfrak{p}$ and the number $f_i = [\mathcal{O}/\mathfrak{P}_i : \mathcal{o}/\mathfrak{p}]$ the **inertia degree**. When working with some specific primes lying over $\mathfrak{p}$ it may be convenient to denote the ramification index of a fixed prime $\mathfrak{P}$ over $\mathfrak{p}$ by $e(\mathfrak{P}|\mathfrak{p})$ and the corresponding inertia degree by $f(\mathfrak{P}|\mathfrak{p})$.

The ramification indices and inertia degrees of a given prime are intimitely related to each other and to the degree of the extension by an identity that we shall now endeavor to prove.

Theorem 3.7. *The ramification indices and inertia degrees satsify the identity*

$$\sum_1^r e_i f_i = [L : K].$$

Proof. The main idea of the proof is to use the isomorphism

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \bigoplus_1^r \mathcal{O}/\mathfrak{P}_i{}^{e_i}$$

from the Chinese remainder theorem and counting their dimensions as vector spaces over the field $k = \mathcal{o}/\mathfrak{p}$. These dimensions must be equal by the isomorphism as rings and therefore k-vector spaces; if we can then just show that the respective dimensions are equal to $n = [L : K]$ and $\sum_1^r e_i f_i$, we are done.

First, in order to show that $\dim_k \mathcal{O}/\mathfrak{p}\mathcal{O} = n$, take the elements $\alpha_1, \ldots, \alpha_m$ of $\mathcal{O}$ to be representatives of the k-basis $\bar{\alpha}_1, \ldots, \bar{\alpha}_m$ of $\mathcal{O}/\mathfrak{p}\mathcal{O}$. The current goal is to show that $\alpha_1, \ldots, \alpha_m$ is a basis of $L|K$, as this will immediately imply that $m = n$, as desired. Suppose now that on the contrary, the elements $\alpha_1, \ldots, \alpha_m$ are linearly dependent. Then it is possible to find $a_1, \ldots, a_m$ in K, and in particular in $\mathcal{o}$, that are not all zero such that

$$\sum_1^m a_i \alpha_i = 0.$$

Consider the ideal $\mathfrak{a}$ of $\mathcal{O}$ generated by $a_1, ..., a_m$. Due to the unique ideal factorization of Dedekind domains, the fractional ideals $\mathfrak{a}^{-1}$ and $\mathfrak{a}^{-1}\mathfrak{p}$ are not equal, so it is possible to find some $a \in \mathfrak{a}^{-1}$ that is not in $\mathfrak{a}^{-1}\mathfrak{p}$. Hence $a\mathfrak{a} \not\subset \mathfrak{p}$, and so $aa_i \notin \mathfrak{p}$, so the linear dependence of $\alpha_1, , \alpha_m$ in fact implies that $\bar{\alpha}_1, \ldots, \bar{\alpha}_m$ are linearly dependent by

$$\sum_1^m a a_i \alpha_i \equiv 0 \bmod \mathfrak{p}.$$

This is a clear contradiction, so $\alpha_1, \ldots, \alpha_m$ must be linearly independent.

With linear independence established, it only remains to show that $\alpha_1, \ldots, \alpha_m$ actually span the entirety of $L|K$. We therefore consider the $\mathcal{o}$-modules $M = \sum_1^m \mathcal{o}\alpha_i$ and $N = \mathcal{O}/M$. It follows from the definition of $\alpha_1, \ldots, \alpha_m$ that $\mathcal{O} = M + \mathfrak{p}\mathcal{O}$ and so $\mathfrak{p}N = N$; this is due to the fact that every element b of $\mathcal{O}$ can be written as a sum $m + ab'$, with $m \in M$, $a \in \mathfrak{p}$ and $b' \in \mathcal{O}$, so that in N it holds that $b \equiv m + ab' \equiv ab' \bmod M$. Due to the hypothesis that $L|K$ is separable, $\mathcal{O}$ is a finitely generated $\mathcal{o}$-module, as was established in the proof of Theorem 3.6; the $\mathcal{o}$-module N must therefore also be finitely generated. Now let $n_1, \ldots, n_k$ be elements that generate N. Then each of these may be written as a sum $n_i = \sum_j a_{ij} n_j$, where each a_{ij} is an element of $\mathfrak{p}$, since $\mathfrak{p}N = N$. This may be written in matrix form as

$$(A - I) \begin{bmatrix} n_1 \\ \vdots \\ n_k \end{bmatrix} = 0,$$

with A the $k \times k$ matrix (a_{ij}) and I the identity matrix. Let $(A - I)^a$ be the adjoint matrix of A and d the determinant of $A - I$. The determinant d is clearly non-zero, as otherwise 1 would have to be a root

of the polynomial $\det(A - xI)$, but all of the entries of A are contained in $\mathfrak{p}$ and 1 is not an element of $\mathfrak{p}$. It follows that

$$\begin{bmatrix} dn_1 \\ \vdots \\ dn_k \end{bmatrix} = dI \begin{bmatrix} n_1 \\ \vdots \\ n_k \end{bmatrix} (A-I)^a(A-I) \begin{bmatrix} n_1 \\ \vdots \\ n_k \end{bmatrix} = 0,$$

so that in particular $dN = 0$, and by equivalence $d\mathcal{O} \subset M = \sum_1^m \mathfrak{o}\alpha_i$. It follows that $L = dL \subset KM$ as K-vector spaces, and so $\alpha_1, \ldots, \alpha_m$ spans L and $\dim_k \mathcal{O}/\mathfrak{p}\mathcal{O} = n$.

Computing the remaining dimension is significantly less work. Fix some index i and set $\mathfrak{P} = \mathfrak{P}_i$, $e = e_i$ and $f = f_i$. Consider the ascending chain

$$(0) \subset \mathfrak{P}^{e-1}/\mathfrak{P}^e \subset \ldots \subset \mathfrak{P}/\mathfrak{P}^e \subset \mathcal{O}/\mathfrak{P}^e$$

of K-vector spaces. The quotients $\mathfrak{P}^\nu/\mathfrak{P}^{\nu+1}$ are all isomorphic to $\mathcal{O}/\mathfrak{P}$ since the surjective homomorphism $\mathcal{O} \twoheadrightarrow \mathfrak{P}^\nu/\mathfrak{P}^{\nu+1}$ mapping $b \in \mathcal{O}$ to $ab \in \mathfrak{P}^\nu/\mathfrak{P}^{\nu+1}$, with a some element of $\mathfrak{P}^\nu/\mathfrak{P}^{\nu+1}$, has kernel $\mathfrak{P}$; it is surjective because $\gcd(\mathfrak{P}^\nu, \mathfrak{P}^{\nu+1}) = \mathfrak{P}^\nu$, so that $\mathfrak{P}^\nu = a\mathcal{O} + \mathfrak{P}^{\nu+1}$. Therefore $\dim_k \mathfrak{P}^\nu/\mathfrak{P}^{\nu+1} = \dim_k \mathcal{O}/\mathfrak{P} = [\mathcal{O}/\mathfrak{P} : k] = f$. Now setting $\mathfrak{P}^0 = \mathcal{O}$, we have that $\mathcal{O}/\mathfrak{P}^e \cong \bigoplus_0^{e-1} \mathfrak{P}^\nu/\mathfrak{P}^{\nu+1}$, so $\dim_k \mathcal{O}/\mathfrak{P}^e = ef$. We may therefore finally conlude that

$$\dim_k \bigoplus_1^r \mathcal{O}/{\mathfrak{P}_i}^{e_i} = \sum_1^r e_i f_i,$$

as was to be shown. □

Since $L|K$ is assumed to be separable, we have that $L = K(\alpha)$ for some primitive element α. It may be assumed that α is an element of $\mathcal{O}$ and that its minimal polynomial is contained in $\mathfrak{o}[x]$, for if one or both of these do not hold then multiplying by a suitable element of $\mathcal{O}$ will force them to.

Definition 3.4. Let $A \subset B$ be an extension of rings. The **conductor** of A in B is the ideal

$$\mathfrak{F} = \mathrm{Ann}_B(B/A) = \{b \in B \mid bB \subset A\}$$

of B. In particular, the conductor is the largest ideal of B contained in A.

It turns out that given such a primitive element, the primes of $\mathcal{O}$ lying over some prime $\mathfrak{p}$ of $\mathfrak{o}$ are closely related to the minimal polynomial of α, given that $\mathfrak{p}$ is relatively prime to the conductor $\mathfrak{F}$ of $\mathfrak{o}[\alpha]$ in $\mathcal{O}$.

Theorem 3.8. *Suppose that α is a primitive element generating $L|K$ such that it is contained in $\mathcal{O}$ with a minimal polynomial contained in $\mathfrak{o}[x]$. Let $\mathfrak{p}$ be any prime of $\mathfrak{o}$ that is relatively prime to the conductor $\mathfrak{F} = \mathrm{Ann}_{\mathcal{O}}(\mathcal{O}/\mathfrak{o}[\alpha])$ of $\mathfrak{o}[\alpha]$ and $\overline{m}(x)$ be the minimal polynomial of α with coefficients reduced mod $\mathfrak{p}$, so that it is contained in $\overline{\mathfrak{o}}[x] = \mathfrak{o}/\mathfrak{p}[x]$. Suppose that the factorization of $\overline{m}(x)$ into monic irreducible polynomials of $\overline{\mathfrak{o}}[x]$ is*

$$\overline{m}(x) = \prod_1^r (\overline{m}_i(x))^{e_i}.$$

Then $\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + m_i(\alpha)\mathcal{O}$ are the primes of $\mathcal{O}$ lying over $\mathfrak{p}$ with ramification index e_i and inertia degree equal to $\deg p_i(x)$. That is,

$$\mathfrak{p}\mathcal{O} = \prod_1^r {\mathfrak{P}_i}^{e_i}$$

and $f_i = \deg p_i(x)$.

Proof. Set $A = \mathfrak{o}[\alpha]$. We aim to prove that

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong A/\mathfrak{p}A \cong \overline{\mathfrak{o}}[x]/(\overline{m}(x))$$

as rings. It will then follow from the Chinese remainder theorem that

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \cong \overline{\mathfrak{o}}[x]/(\overline{m}(x)) \cong \bigoplus_1^r \overline{\mathfrak{o}}[x]/(\overline{m}_i(x))^{e_i},$$

which implies that the prime ideals of $\overline{o}[x]/(\overline{m}(x))$ are simply those generated by $\overline{m}_i(x)$, which must then correspond to the prime ideals $\mathfrak{P}_i$. If we index the prime ideals of $\overline{\mathcal{O}} = \mathcal{O}/\mathfrak{p}\mathcal{O}$ such that the prime ideal $\overline{\mathfrak{P}}_i$ is mapped to $\overline{m}_i(x)$ by the isomorphism $\varphi : \mathcal{O}/\mathfrak{p}\mathcal{O} \xrightarrow{\sim} \overline{o}[x]/(\overline{m}(x))$ that sends $\overline{f}(\alpha)$ to $\overline{f}(x)$, then it follows immediately that

$$[\overline{\mathcal{O}}/\overline{\mathfrak{P}}_i : \overline{o}] = [\overline{o}[x]/(\overline{m}_i(x)) : \overline{o}] = \deg \overline{m}_i(x).$$

Setting $\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + m_i(\alpha)\mathcal{O}$, $\mathfrak{P}_i$ is then the inverse image of $\overline{\mathfrak{P}}_i$ with respect to the canonical projection $\mathcal{O} \twoheadrightarrow \overline{\mathcal{O}}$, in view of the isomorphism φ and the fact that $\mathcal{O} = \mathfrak{p}\mathcal{O} + \mathfrak{F} = \mathfrak{p}\mathcal{O} + A$; the latter is due to $\mathfrak{p}$ and $\mathfrak{F} \subset A$ being relatively prime. The inverse image of a prime ideal is again prime, so the $\mathfrak{P}_i$'s are prime ideals of $\mathcal{O}$ lying over $\mathfrak{p}$ and

$$f_i = [\mathcal{O}/\mathfrak{P}_i : o/\mathfrak{p}] = [\overline{\mathcal{O}}/\overline{\mathfrak{P}}_i : \overline{o}] = \deg \overline{m}_i(x).$$

The primality of the ideals $(\overline{m}_i(x))$ of $\overline{o}[x]/(\overline{m}(x))$ lets us conclude that

$$(0) = (\overline{m}(x)) = \prod_1^r (\overline{m}_i(x)) = \bigcap_1^r (\overline{m}_i(x))^{e_i},$$

so that we must likewise have

$$\bigcap_1^r \overline{\mathfrak{P}}_i{}^{e_i} = (0).$$

Since $\overline{\mathfrak{P}}_i{}^{e_i}$ is the image of $\mathfrak{P}_i{}^{e_i}$ and the inverse image of an ideal is again an ideal, the inverse image of $\overline{\mathfrak{P}}_i{}^{e_i}$ must be an ideal of $\mathcal{O}$ containing $\overline{\mathfrak{P}}_i{}^{e_i}$, so it must be of the form $\overline{\mathfrak{P}}_i{}^{\nu}$. However, ν must equal e_i, since for $\nu < e_i$ the given ideal has an image that is not contained in $\overline{\mathfrak{P}}_i{}^{e_i}$; the ideal $\mathfrak{P}_i{}^{e_i}$ is therefore the inverse image of $\overline{\mathfrak{P}}_i{}^{e_i}$. Hence $\mathfrak{p}\mathcal{O} \supset \bigcap_1^r \mathfrak{P}_i{}^{e_i} = \prod_1^r \mathfrak{P}_i{}^{e_i}$, and the given e_i's satisfy $\sum_1^r e_i f_i$, from which it follows that the e_i must in fact be the ramification indices and therefore equality must hold, so that we indeed have that

$$\mathfrak{p}\mathcal{O} = \prod_1^r \mathfrak{P}_i{}^{e_i}.$$

We now prove the two isomorphisms mentioned in the beginning of the proof. First consider the homomorphism $\psi : A \to \mathcal{O}/\mathfrak{p}\mathcal{O}$ that sends a to $a \bmod \mathfrak{p}\mathcal{O}$. This homomorphism is in fact surjective, since $\mathcal{O} = \mathfrak{p}\mathcal{O} + A$. Its kernel is clearly $A \cap \mathfrak{p}\mathcal{O}$, which by $\mathcal{O} = \mathfrak{p} + \mathfrak{F}$ implies that

$$A \cap \mathfrak{p}\mathcal{O} = (\mathfrak{p} + \mathfrak{F})(A \cap \mathfrak{p}\mathcal{O}) \subset (\mathfrak{p} + \mathfrak{F})A = \mathfrak{p}A$$

and the reverse inclusion is obvious since $\psi(\mathfrak{p}A) = (0)$. This establishes the isomorphism $A/\mathfrak{p}A \cong \mathcal{O}/\mathfrak{p}\mathcal{O}$. For the other isomorphism, it suffices to note that

$$\overline{o}[x]/(\overline{m}(x)) \cong o[x]/(\mathfrak{p}, m(x)) \cong A/(\mathfrak{p}) = A/\mathfrak{p}A.$$

□

If the number of factors r in the prime decomposition of $\mathfrak{p}$ in $\mathcal{O}$

$$\mathfrak{p} = \prod_1^r \mathfrak{P}_i{}^{e_i}$$

is greater than 1, then $\mathfrak{p}$ is said to **split** in L and if $e_i > 1$ for some i it is said to **ramify** in L. A prime that does not split is called **non-split** and one that does not ramify is similarly called **unramified**. If a prime on the other hand has $r = n$ factors or $e_i = 1$ for every i, it is said to be **totally split** or **totally ramified**, respectively. For a prime $\mathfrak{P}$ lying over $\mathfrak{p}$, we say that it **splits** over K whenever $\mathfrak{p}$ splits in L and that it **ramifies** over K if $\mathfrak{p}$ ramifies in L.

One may wonder how common each of these scenarios is; it turns out ramification is an exceptional case when $L|K$ is separable in that it can only ever happen to a finite amount of primes.

Theorem 3.9. *Only finitely many primes of K are ramified in L.*

Proof. There exists a primitive element α since $L|K$ is separable, so that $L = K(\alpha)$. We can take α to be in $\mathcal{O}$, as if it is not then multiplication by a suitable non-zero element of $\mathcal{O}$ will certainly make it so. Setting $\alpha_1, \ldots, \alpha_n$ to be the $n = [L : K]$ conjugates of α and $m(x)$ to be the minimal polynomial of α over $\mathfrak{o}$, we have that the discriminant d of $m(x)$ is

$$d = d(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Set $\overline{\mathfrak{o}} = \mathfrak{o}/\mathfrak{p}$ and suppose that $\mathfrak{p}$ is a prime of $\mathfrak{o}$ that both ramifies in L and is relatively prime to both $d\mathfrak{o}$ and the conductor $\mathfrak{F}$ of $\mathfrak{o}[\alpha]$. Then some prime $\mathfrak{P}_i$ of $\mathcal{O}$ lying over $\mathfrak{p}$ must ramify over $\mathfrak{o}$. Then there is a ramification index $e_i > 1$, which implies that $\overline{m}(x)$ has a double root so that in turn $\overline{d} = 0$. However, this contradicts the assumption that $\mathfrak{p} \nmid d\mathfrak{o}$, the ramification index e_i must be equal to 1 for each prime $\mathfrak{P}_i$ lying over $\mathfrak{p}$. Each field extension $\mathcal{O}/\mathfrak{P}_i|\mathfrak{o}/\mathfrak{p}$ is of the form $\mathcal{O}/\mathfrak{P}_i = \mathfrak{o}/\mathfrak{p}(\overline{\alpha})$, with $\overline{\alpha} = \alpha \bmod \mathfrak{P}_\mathfrak{i}$. The element $\overline{\alpha}$ is separable, for if it were not then neither would $\alpha \bmod \mathfrak{p}$, and so the corresponding extension is separable.

The statement is thus proven, as it has now been shown that any prime $\mathfrak{p}$ that is ramified in L must either divide $d\mathfrak{o}$ or $\mathfrak{F}$ and each of these have only a finite amount of prime divisors. □

The assumption of $L|K$ being separable is now restricted further and $L|K$ is assumed to be Galois. Its Galois group is denoted G. This assumption is particularly attractive due to the fact that $\mathbb{Q}(\omega_p)|\mathbb{Q}$ is in fact a Galois extension, for it is the splitting field of the polynomial $\frac{x^n-1}{x-1}$ over $\mathbb{Q}$.

Lemma 3.10. *Suppose that $L|K$ is Galois. Given a prime $\mathfrak{p}$ of $\mathfrak{o}$, the Galois group G acts transitively on the set of primes of $\mathcal{O}$ lying over $\mathfrak{P}$.*

Proof. Suppose that $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are primes lying over $\mathfrak{p}$ that are not conjugate. Then by the Chinese remainder theorem it is possible to find some element a of $\mathcal{O}$ such that

$$a \equiv 1 \bmod \sigma\mathfrak{P}_1, \quad a \equiv 0 \bmod \mathfrak{P}_2,$$

for all $\sigma \in G$. Hence a is not contained in any of the primes $\sigma\mathfrak{P}_1$ and equivalently $\sigma a \notin \mathfrak{P}_1$. Hence $N_{L|K}(a) = \prod_{\sigma \in G} \sigma a$ is contained in $\mathfrak{P}_2 \cap \mathfrak{o}$ but not in $\mathfrak{P}_1 \cap \mathfrak{o}$. But these primes of $\mathfrak{o}$ are both equal to $\mathfrak{p}$ and we cannot have both $a \in \mathfrak{p}$ and $a \notin \mathfrak{p}$. All primes lying over $\mathfrak{p}$ must therefore be conjugate. □

Theorem 3.11. *Let $\mathfrak{p}$ be a prime of $\mathfrak{o}$ and assume that $L|K$ is Galois with Galois group G. Then*

$$\mathfrak{p}\mathcal{O} = \prod_1^r \mathfrak{P}_i{}^e.$$

That is, the ramification indices are all equal; the same is true for the inertia degrees.

Proof. Set $\mathfrak{P} = \mathfrak{P}_1$. Then each $\mathfrak{P}_i$ is a conjugate of $\mathfrak{P}$, so that $\mathfrak{P}_i = \sigma\mathfrak{P}$ for some $\sigma \in G$. Now consider the following diagram.

$$\begin{array}{ccc} \mathcal{O} & \xrightarrow{\quad\sigma\quad} & \mathcal{O} \\ \downarrow & & \downarrow \\ \mathcal{O}/\mathfrak{P} & \xrightarrow{\quad\overline{\sigma}\quad} & \mathcal{O}/\sigma\mathfrak{P} \end{array}$$

The induced isomorphism $\overline{\sigma} : a \bmod \mathfrak{P} \mapsto \sigma a \bmod \sigma\mathfrak{P}$ shows that $\mathcal{O}/\mathfrak{P} \cong \mathcal{O}/\sigma\mathfrak{P}$. It follows that $[\mathcal{O}/\mathfrak{P} : \mathfrak{o}/\mathfrak{p}] = [\mathcal{O}/\sigma\mathfrak{P} : \mathfrak{o}/\mathfrak{p}]$, i.e. that the inertia degrees are equal.

Since the automorphisms $\sigma \in G$ fix K and therefore $\mathfrak{p}$, the ramification degrees are shown to be equal by simply considering the equivalence

$$\mathfrak{P}^\nu \mid \mathfrak{p}\mathcal{O} \iff \sigma\mathfrak{P}^\nu \mid \mathfrak{p}\mathcal{O}.$$

□

4 The Minkowski Bound and the Class Number

Throughout this section K is understood to be an arbitrary number field. The main aim throughout this subsection is to prove that Cl_K is always finite. In order to meet this end a basic knowledge of lattices will have to be acquired.

4.1 Lattices and Minkowski Theory

A **lattice** in an n-dimensional euclidean vector space V is an additive subgroup of the from

$$\Gamma = \bigoplus_1^m \mathbb{Z}v_i.$$

The set

$$\Phi = \{\sum_1^m x_i v_i \mid x_i \in [0,1) \subset \mathbb{R}\}$$

is called the **fundamental mesh** of Γ. When $m = n$, or equivalently when $\Gamma + \Phi$ covers the entirety of V, we call the lattice **complete**. A subset X of V is called **centrally symmetric** if $x \in X \implies -x \in X$ and **convex** if for any two points x_1 and x_2 of X, the line segment $\{tx_1+(1-t)x_2 \mid t \in [0,1]\}$ is contained in X.

Theorem 4.1 (Minkowski's Lattice Point Theorem)**.** *Suppose that Γ is a complete lattice in a euclidean vector space V and let X be a subset of V that is convex and centrally symmetric. Then X contains at least one non-zero lattice point provided that*

$$\mathrm{vol}(X) > 2^n \mathrm{vol}(\Gamma).$$

Proof. Suppose that we are able find two points, γ_1 and γ_2, in the lattice Γ, such that the intersection $(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2)$ is non-empty. Then it is possible to find two elements x_1 and x_2 of X such that $\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2$, or equivalently an element γ of Γ such that

$$\gamma = \gamma_2 - \gamma_1 = \frac{1}{2}(x_1 - x_2).$$

Hence it suffices to show that whenever all intersections of the form $(\frac{1}{2}X + \gamma_1) \cap (\frac{1}{2}X + \gamma_2)$ are empty, $\mathrm{vol}(X) \leq 2^n \mathrm{vol}(\Gamma)$.

Let us therefore equivalently assume that the sets of form $X_\gamma := \frac{1}{2}X + \gamma$ are pairwise disjoint. Then their intersections with Φ are also disjoint, so that

$$\sum_\gamma \mathrm{vol}(\Phi \cap X_\gamma) \leq \mathrm{vol}(\Phi).$$

Now X_γ has the same volume as its translate $X_\gamma - \gamma = \frac{1}{2}X$ and Γ is complete, so

$$\mathrm{vol}(\Gamma) \geq \sum_\gamma \mathrm{vol}\left((\Phi - \gamma) \cap \frac{1}{2}X\right) = \mathrm{vol}\left(\frac{1}{2}X\right) = \frac{1}{2^n}\,\mathrm{vol}(X).$$

Hence the pairwise disjointedness has enabled us to conclude that in fact

$$\mathrm{vol}(X) \leq 2^n\,\mathrm{vol}(\Gamma),$$

contrary to the hypothesis of the theorem. □

In order to apply this theory about lattices to a number field K, first map K to the complex vector space $K_\mathbb{C} := \prod_\tau \mathbb{C}$ by the map $j : K \to K_\mathbb{C}$, mapping each element a of K to the n-tuple $ja = (\tau a)$ consisting of the images of a with respect to each embedding $\tau : K \to \mathbb{C}$ of K into $\mathbb{C}$. If z is an element of $K_\mathbb{C}$, then by z_τ we mean the entry of z that corresponds to the embedding τ in the tuple. The sum

$$\langle x, y \rangle = \sum_\tau x_\tau \bar{y}_\tau$$

defines a Hermitian inner product as it is clear that it is linear with respect to the first variable and $\overline{\langle x, y\rangle} = \langle y, x\rangle$.

Taking elementwise complex conjugates defines an involution F on $K_{\mathbb{C}}$ by mapping (z_τ) to $(\bar{z}_{\bar{\tau}})$. Denote the set of points of $K_{\mathbb{C}}$ that are invariant under F by $K_{\mathbb{R}}$. The map j actually embeds K into $K_{\mathbb{R}}$; since $\bar{\sigma}$ is also an embeds K into $\mathbb{C}$ we have that $(\overline{\sigma a}_{\overline{\sigma}}) = (\sigma a_\sigma)$, so all elements ja are indeed F-invariant. This embedding will eventually let us use the theory of lattices to say things about K itself.

Let us now partition the set $\mathrm{Hom}(K, \mathbb{C})$ of embeddings $\tau : K \to \mathbb{C}$ by the equivalence relation

$$\tau_1 \sim \tau_2 \iff \tau_1 = \tau_2 \text{ or } \tau_1 = \bar{\tau}_2.$$

If $\rho(K) \subset \mathbb{R}$ we call ρ a **real** embedding; embeddings σ such that $\sigma(K) \cap (\mathbb{C} \setminus \mathbb{R}) \neq \emptyset$ we call **complex**. Embeddings of the latter kind always come in distinct pairs; if σa is not real, then it is distinct from $\overline{\sigma a}$, so that σ and $\bar{\sigma}$ are differ for at least one point a. The real embeddings, however, are clearly invariant under conjugation. Hence the equivalence relation partitions $\mathrm{Hom}(K, \mathbb{C})$ into r equivalence classes each consisting of a single real embedding and s equivalence classes each consisting of two complex embeddings. Setting $n = [K : \mathbb{Q}]$, we find that $n = r + 2s$.

Upon restriction to $K_{\mathbb{R}}$, the Hermitian inner product restricts to a positive-definite scalar product, which gives us a notion of volume of its lattices as follows: the volume of the lattice $\Gamma = \bigoplus_1^n \mathbb{Z} v_i$ of $K_{\mathbb{R}}$ is given by

$$\mathrm{vol}(\Gamma) = \mathrm{vol}(\Phi) = |\det(\langle v_i, v_j\rangle)|^{1/2}.$$

This defines a Haar measure which we shall call the **canonical measure**

Theorem 4.2. *Set S to be a set containing a system of representatives of the equivalence classes of the complex embeddings of* $\mathrm{Hom}(K, \mathbb{C})$. *There exists an isomorphism*

$$K_{\mathbb{R}} \xrightarrow{\sim} \prod_\tau \mathbb{R}$$

such that $(z_\tau) \mapsto (x_\tau)$, where $x_\rho = \mathrm{Re}(z_\rho)$, $x_\sigma = \mathrm{Re}(z_\sigma)$ and $x_{\overline{\sigma}} = \mathrm{Im}(z_\sigma)$ for all real embeddings ρ and $\sigma \in S$. Furthermore, the scalar product on $K_{\mathbb{R}}$ is taken to the scalar product $(x, y) = \sum_\tau \alpha_\tau x_\tau y_\tau$, with $\alpha_\rho = 1$ for real embeddings ρ and $\alpha_\sigma = 2$ for complex embeddings σ. Hence

$$\mathrm{vol}_{\mathrm{canonical}}(X) = 2^s \,\mathrm{vol}_{\mathrm{Lebesgue}}(\mathrm{im}\, X).$$

Proof. The map is clearly a bijective homomorphism of eucliden vector spaces, ergo an isomorphism of these. Setting $(z_\tau) = (x_\tau + iy_\tau)$ and $(z'_\tau) = (x'_\tau + iy'_\tau)$, it is easily seen that the product $\overline{z'}_\rho z_\rho$ is sent to $x'_\rho x_\rho$ and the sum of products $z'_\sigma \bar{z}_\sigma + z'_{\overline{\sigma}} \bar{z}_{\overline{\sigma}} = z'_\sigma \bar{z}_\sigma + \overline{z'_\sigma \bar{z}_\sigma}$ to $2\mathrm{Re}(z'_\sigma \bar{z}_\sigma) = 2(x'_\sigma x_\sigma + x'_{\overline{\sigma}} x_{\overline{\sigma}})$. The inner product and volume parts of the statement now follow. □

Lemma 4.3. *For any non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, $\Gamma = j\mathfrak{a}$ is a complete lattice in $K_{\mathbb{R}}$ with fundamental mesh of volume given by*

$$\mathrm{vol}(\Gamma) = \sqrt{|d_K|}[\mathcal{O} : \mathfrak{a}].$$

Proof. Set d_K to be the discriminant of K and let $\alpha_1, \ldots, \alpha_n$ to be a $\mathbb{Z}$-basis of $\mathfrak{a}$, so that one may write

$$\Gamma = \mathbb{Z} j\alpha_1 \oplus \ldots \oplus \mathbb{Z} j\alpha_n.$$

Let A be the matrix $(\tau_i \alpha_k)$. Now the discriminant $d(\mathfrak{a})$ of $\mathfrak{a}$ is given by

$$d(\mathfrak{a}) = (\det A)^2 = [\mathcal{O}_K : \mathfrak{a}]^2 d_K,$$

whereas

$$[\mathrm{vol}(\Gamma)]^2 = |\det(\langle j\alpha_i, j\alpha_k\rangle)| = |\det(AA^\dagger)| = |\det A|^2,$$

and from these two equations it follows that

$$\mathrm{vol}(\Gamma) = [\mathcal{O}_K : \mathfrak{a}]\sqrt{|d_K|}.$$

□

4.2 Finiteness of the Class Number

Now in possession of a method through which to identify K with a lattice, we are ready to prove the Minkowski bound. This bound in turn lets us show that the class number h_K of a separable number field is always finite. However, we first take a detour to define and study the norm and absolute norm of an ideal.

Definition 4.1. Define the **absolute norm** $\mathfrak{N}$ of a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ by the identity

$$\mathfrak{N}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}].$$

The **norm** $\mathfrak{N}_{L|K}$ of a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_L$, given a separable field extension $L|K$, is given by

$$\mathfrak{N}_{L|K}(\mathfrak{a}) = \prod_{\sigma} \sigma(\mathfrak{a}),$$

where σ runs through the K-embeddings of L into an algebraic closure of K.

Theorem 4.4. *Let $\mathfrak{a} = \prod_1^r \mathfrak{p}_i^{\nu_i}$ be the prime factorization of an ideal $\mathfrak{a}$ of $\mathcal{O}_K$. The absolute norm of $\mathfrak{a}$ is then multiplicative in the sense that we have the identity*

$$\mathfrak{N}(\mathfrak{a}) = \prod_1^r \mathfrak{N}(\mathfrak{p}_i)^{\nu_i}.$$

The norm is of course also multiplicative in the same sense, but this fact is so trivial that it needn't be properly stated and proven. We now show that the absolute norm essentially corresponds to applying the norm and then extracting the generator of the resulting principal ideal of $\mathbb{Z}$ when $K|\mathbb{Q}$ is Galois.

Lemma 4.5. *Suppose that $L|K$ is Galois. The image of a prime $\mathfrak{P}$ of $\mathcal{O}_L$ under the map $\mathfrak{N}_{L|K}$ is a power of the prime $\mathfrak{p}$ of $\mathcal{O}_K$ lying under $\mathfrak{P}$ in the sense that*

$$\mathfrak{N}_{L|K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})}\mathcal{O}_L.$$

Proof. Set $e = e(\mathfrak{P}|\mathfrak{p})$ and $f = f(\mathfrak{P}|\mathfrak{p})$. The primes lying over $\mathfrak{p}$ are all conjugates, so

$$\mathfrak{N}_{L|K}(\mathfrak{P}) = \prod_{\sigma \in G} \sigma\mathfrak{P} = \left(\prod_1^r \mathfrak{P}_i{}^e \right)^{\frac{n}{re}} = (\mathfrak{p}\mathcal{O}_L)^f = \mathfrak{p}^f \mathcal{O}_L.$$

□

Theorem 4.6. *For any non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ the following identity holds if $L|K$ is Galois.*

$$\mathfrak{N}_{K|\mathbb{Q}}(\mathfrak{a}) = \mathfrak{N}(\mathfrak{a})\mathbb{Z}$$

Proof. Due to the complete multiplicativity of both norms involved it suffices to prove the statement for prime ideals $\mathfrak{p}$. Since $\mathcal{O}_K/\mathfrak{p}$ is a finite field of prime characteristic its order is a prime power. In fact, if p is taken to be the prime of $\mathbb{Z}$ lying under $\mathfrak{p}$, it is easily seen that $|\mathcal{O}_K/\mathfrak{p}| = p^{[\mathcal{O}_K/\mathfrak{p}:\mathbb{Z}/(p)]} = p^f$, where $f = f(\mathfrak{p}|p)$. That $N_{K|\mathbb{Q}}(\mathfrak{p}) = p^f\mathbb{Z}$ follows from Lemma 4.5. □

Corollary 4.6.1. *Given a Galois*[4] *extension $K|\mathbb{Q}$, the principal integral ideal (a) of $\mathcal{O}_K$ satisfies*

$$\mathfrak{N}((a)) = |N_{K|\mathbb{Q}}(a)|.$$

Proof. It follows directly from Theorem 4.5 that $\mathfrak{N}((a)) = N_{K|\mathbb{Q}}((a))$, so that the latter is an ideal of $\mathbb{Z}$. Since $\mathbb{Z}$ is a PID and since a generates all of (a) in $\mathcal{O}_K$, it follows that $\mathfrak{N}((a))\mathbb{Z} = N_{K|\mathbb{Q}}(a)\mathbb{Z}$. The units of $\mathbb{Z}$ are simply ± 1, so we must then have $\mathfrak{N}((a)) = |N_{K|\mathbb{Q}}|$. □

With these facts about the absolute norm established, it is time to get back to stating and proving the Minkowski bound.

[4] The statement is actually true for separable extensions, but requires a bit more work to prove when $K|\mathbb{Q}$ is not normal. Since we only apply the theorem to the Galois case in the sequel, we do not prove this here. The interested reader may find a proof in [4].

Lemma 4.7. *The convex and centrally symmetric set*

$$X = \{(z_\tau) \in K_{\mathbb{R}} \mid \sum_\tau |z_\tau| < t\}$$

is of volume $\mathrm{vol}(X) = 2^r \pi^s \frac{t^n}{n!}$.

Proof. Consider instead an isomoprhic image $\mathrm{im}\, X = \left\{(x_\tau) \in \prod_\tau \mathbb{R} \;\middle|\; \sum_\rho |x_\rho| + 2\sum_\sigma \sqrt{{x_\sigma}^2 + {x_{\overline{\sigma}}}^2} < t\right\}$ of X in $\prod_\tau \mathbb{R}$. Now re-index the coordinates of elements in $\mathrm{im}\, X$ with numbers, so that the inequality that defines it may instead be written as

$$\sum_1^r |x_i| + 2\sum_1^s \sqrt{{y_j}^2 + {z_j}^2} < t.$$

Determining the volume of this set is simply done by integrating 1 over $\mathrm{im}\, X$. By symmetry we may consider only non-negative x_i when computing it and then multiply by 2^r in order to recover the original integral. Changing the y_j's and z_j's into polar coordinates such that $y_j = v_j \cos\theta_j$ and $z_j = v_j \sin\theta_j$ and then performing the change of variables $2v_j = w_j$ gives us a simpler domain

$$D(t) := \{(x_1, \ldots, x_r; w_1, \ldots, w_s; \theta_1, \ldots, \theta_s) \in \mathbb{R}^n \mid \sum_1^r x_i + \sum_1^s w_j < t,\, 0 \le x_i,\, 0 \le w_j,\, \theta_j \in [0, 2\pi],\}$$

to integrate over. Hence the integral we wish to compute is

$$I(t) = 2^r 4^s (2\pi)^s \int_{D(t)} w_1 \ldots w_s \, dx_1 \ldots dx_r dw_1 \ldots dw_s.$$

From the above it is clear that $I(t) = t^{r+2s} I(1) = t^n I(1)$. Let us therefore instead consider the integral

$$I_{r,s}(1) = \int_{D_{r,s}(1)} w_1 \ldots w_s \, dx_1 \ldots dx_r dw_1 \ldots dw_s,$$

with $D_{a,b}(t)$ being $D(t)$ but with a coordinates x_i and b coordinates w_j and θ_j. With this notation

$$I_{r,s}(1) = \int_0^1 I_{r-1,s}(1 - x_1)\, dx_1 = I_{r-1,s}(1) \int_0^1 (1 - x_1)^{n-1}\, dx_1 = \frac{I_{r-1,s}}{2s(2s-1)},$$

and so by induction it follows that

$$I_{r,s}(1) = \frac{I_{0,s}(1)}{\mathrm{P}_r^n}, \tag{3}$$

with P_r^n being the number of r-permutations of n elements, i.e. $\mathrm{P}_r^n = n(n-1)\ldots(n-r+1)$. In the same fashion

$$I_{0,s}(1) = \int_0^1 w_1 I_{0,s-1}(1 - w_1)\, dw_1 = I_{0,s-1}(1) \int_0^1 w_1 (1 - w_1)^{2(s-1)}\, dw_1 = \frac{I_{0,s-1}(1)}{2s},$$

and so again by induction $I_{0,s}(1) = \frac{1}{(2s)!}$, which combined with (3) yields

$$I_{r,s}(1) = \frac{1}{\mathrm{P}_r^n (2s)!} = \frac{1}{n!}$$

and by how $I_{r,s}(1)$ was define in relation to $I(t)$ it finally follows that

$$\mathrm{vol}(X) = 2^s \,\mathrm{vol}(\mathrm{im}\, X) = I(t) = 2^s \frac{2^r (2\pi)^s t^n}{4^s} I_{r,s}(1) = \frac{2^r \pi^s t^n}{n!}.$$

□

Theorem 4.8 (The Minkowski Bound)**.** *Every ideal* $\mathfrak{a} \neq 0$ *contains some element whose norm satisfies* $|N_{K|\mathbb{Q}}(a)| \le \lfloor M \mathfrak{N}(\mathfrak{a}) \rfloor$*, where* $M = \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|d_K|}$ *is the* ***Minkowski bound****.*

Proof. Consider the set X from Lemma 4.7. Suppose we are able to set t to be such that

$$\frac{2^r \pi^s t^n}{n!} = \operatorname{vol}(X) > 2^n \operatorname{vol}(\Gamma) = 2^n \mathfrak{N}(\mathfrak{a}) \sqrt{|d_K|}$$

and

$$\sum_\tau |z_\tau| < B(t),$$

with $B(t)$ some real number depending on t satisfying $\lfloor B(t) \rfloor < n \left(M\mathfrak{N}(\mathfrak{a})\right)^{1/n}$. Then we will have by AM-GM and Minkowski's lattice point theorem that there exists some $a \in \mathfrak{a}$ whose norm satisfies $|N_{K|\mathbb{Q}}(a)| < M\mathfrak{N}(\mathfrak{a})$, since then

$$N_{K|\mathbb{Q}}(a) = \prod_\tau |a_\tau| \leq \left(\frac{1}{n} \sum_\tau |a_\tau| \right)^n \leq \left(\frac{1}{n} \lfloor B(t) \rfloor \right)^n < M\mathfrak{N}(\mathfrak{a});$$

we may take the floor of $B(t)$ above since we know that $N_{K|\mathbb{Q}}(a)$ must be an integer. If we have that $M_0 := n(M\mathfrak{N}(\mathfrak{a}))^{1/n}$ is not an integer, then choosing t to be a real number such that $t \in (M_0, \lceil M_0 \rceil)$, we get that

$$\operatorname{vol}(X) > \frac{2^r \pi^s n^n M \mathfrak{N}(\mathfrak{a})}{n!} = 2^n \mathfrak{N}(\mathfrak{a}) \sqrt{|d_K|} = 2^n \operatorname{vol}(\Gamma)$$

and setting $B(t) = t$ finishes the proof. It therefore only remains to show that $M_0 \notin \mathbb{Z}$. If $s > 0$ this is immediate, as π is transcendental. In the case $s = 0$ either M_0 is not an integer and we may argue similarly, or if M_0 were somehow an integer the inequality

$$N_{K|\mathbb{Q}}(a) \leq M\mathfrak{N}(\mathfrak{a})$$

still arises from taking t to be a real number contained in the interval $(M_0, M_0 + 1)$ and $B(t) = t$, although it is not strict. In either case, the inequality $|N_{K|\mathbb{Q}}(a)| \leq \lfloor M\mathfrak{N}(\mathfrak{a}) \rfloor$ holds. □

Corollary 4.8.1. *Each ideal class of Cl_K contains an integral ideal whose absolute norm is bounded from above by the Minkowski bound M.*

Proof. Fix an integral ideal and consider its ideal class $\mathfrak{a}P_K$. It is a simple matter to see that all ideal classes are of this form; any fractional $\mathfrak{a}$ can be made integral by multiplying by the principal ideal (a) for any denominator present in any element of $\mathfrak{a}$. This can be forced to be a finite process by considering a finite[5] set of generators, since $\mathcal{O}_K$ is noetherian.

Now Cl_K is a group, so it is possible to find a class $\mathfrak{b}P_K$ such that $\mathfrak{a}\mathfrak{b}P_K = \mathcal{O}_K P_K$ and we may of course also assume that $\mathfrak{b}$ is integral. It contains an element b of norm bounded by the Minkowski bound through the inequality

$$|N_{K|\mathbb{Q}}(b)| \leq M\mathfrak{N}(\mathfrak{b}).$$

Now $\mathfrak{a}\mathfrak{b}P_K = (b)P_K$, so after suitable multiplication of prinipal ideals, we may write $\mathfrak{a}\mathfrak{b} = (b)$, and it follows that

$$\mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b}) = \mathfrak{N}(\mathfrak{a}\mathfrak{b}) = \mathfrak{N}((b)) = |N_{K|\mathbb{Q}}(b)| \leq M\mathfrak{N}(\mathfrak{b}),$$

and we are done after division by $\mathfrak{N}(\mathfrak{b})$ on both sides. □

Corollary 4.8.2. *The class number of any number field is finite.*

Proof. Each ideal class in Cl_K contains an ideal $\mathfrak{a}$ whose norm is bounded by the number field's Minkowski bound M. The absolute norm is multiplicative and thus

$$\mathfrak{N}(\mathfrak{a}) = \prod_1^r \mathfrak{N}(\mathfrak{p})^{\nu_i}.$$

As seen in the proof for Theorem 4.6, absolute norms of primes of $\mathcal{O}_K$ are prime powers of $\mathbb{Z}$ and there are only finitely many primes of $\mathcal{O}_K$ lying over any single prime of $\mathbb{Z}$. Hence there are only finitely many possible representatives for the ideal classes in Cl_K and therefore there can only be finitely many classes, so Cl_K must itself also be finite. □

[5] In fact, each ideal of a Dedekind domain can be generated by only two elements, since the quotient $\mathcal{O}_K/\mathfrak{a}$ can be shown to be a PID.

5 Failure of Unique Factorization

We are now in a position to give two different proofs of the failure of unique factorization in $\mathbb{Z}[\omega_2 3]$. The majority of the first proof was outlined by Prof. Arne Meurman for $p = 23$ early on in the project – in particular, all results in Subsection 5.1 appearing before Theorem 5.4 – and the second is essentially a solution to a series of problems from Chapter 3 of [4]. However, before delving into either proof, we prove that $\mathbb{Q}(\omega_p)$ contains a unique quadratic subfield. This subfield will play an important role in both proofs.

Theorem 5.1. *Let $L = \mathbb{Q}(\omega_p)$, with p a prime, and K its quadratic subfield. Then $K = \mathbb{Q}(\sqrt{a_p})$, with $a_p = (-1)^{\frac{p-1}{2}} p$.*

Proof. The field of cyclotomic integers L contains a unique quadratic subfield since $G := \mathrm{Gal}(L|\mathbb{Q}) \cong C_{p-1}$, which has a unique subgroup of order 2. Hence there exists one and only one subfield of L of index 2 over $\mathbb{Q}$ by the fundamental theorem of Galois theory. Set K to be the quadratic subfield of L and a_p to be the squarefree integer such that $K = \mathbb{Q}(\sqrt{a_p})$. Now $\sqrt{a_p} \in \mathcal{O}_K$, regardless of what exactly a_p might be, so

$$(\sqrt{a_p})^2 = (a_p) \tag{4}$$

in $\mathcal{O}_K$. The element $\sqrt{a_p}$ has a norm of either a_p if congruent to 3 mod 4 or $\frac{a_p}{4}$ if congruent to 1 mod 4; its norm can therefore never be 1 and $\sqrt{a_p}$ cannot be a unit of $\mathcal{O}_K$. Hence the ideal it generates is a non-trivial proper ideal and by unique ideal factorization this shows that some prime q dividing a_p must ramify in K and therefore also in L. But the discriminant of L is $\pm p^{p-2}$ and L is separable, so we may apply Theorem 3.9 in $\mathcal{O}_L$ with the conductor set to $\mathfrak{F} = \mathcal{O}_L$, so that it doesn't matter. Hence $q \mid p^{p-2}$, which forces $q = p$.

Now consider the equation of ideals

$$\mathfrak{a}^2 = \frac{a_p}{p}\mathcal{O}_K$$

which results from dividing by (p) on both sides of (4). Repeating the argument above for all primes dividing $\frac{a_p}{p}$, we get that they are all also equal to p and this in turn forces $a_p = \pm p$, since a_p was assumed to be squarefree. Finally, consider the prime 2 of $\mathbb{Z}$. It certainly does not divide p^{p-2} and can therefore not ramify in L. If $a_p \equiv 3 \bmod 4$, then clearly

$$2\mathcal{O}_K \supset (4, 2 + 2\sqrt{a_p}, 1 + 2\sqrt{a_p} + a_p) = (2, 1 + \sqrt{a_p})^2,$$

or in the language of prime factorization in Dedekind domains, $2\mathcal{O}_K \mid (2, 1 + \sqrt{a_p})^2$ Furthermore, $2 \nmid (2, 1 + \sqrt{a_p})$, so $2\mathcal{O}_K$ is not prime and must therefore split. The ideal $(2, 1 + \sqrt{a_p})$, howevever, is clearly a non-zero proper prime ideal, and so the only possiblity is

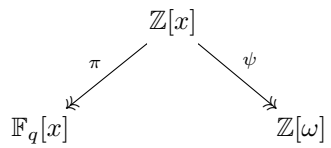
$$2\mathcal{O}_K = (2, 1 + \sqrt{a_p})^2.$$

But then 2 ramifies in K and therefore also in L, a clear contradiction. This tells us that $a_p \equiv 1 \bmod 4$, which forces a_p to be as was stated in the theorem. □

5.1 First Proof

Definition 5.1. A Sophie Germain prime is a prime p such that $q = 2p + 1$ is also a prime. The prime q is called the safe prime associated with p.

Let p be a Sophie Germain prime with safe prime q. We begin by considering the maps $\psi : f(x) \mapsto f(\omega_p)$ and $\pi : f(x) \mapsto f(x) \bmod (q)$ as is illustrated in the diagram



and the ideals $\mathfrak{m}_j = (q, x - j^2)$, for $2 \leq j \leq p$. The ideals $\mathfrak{m}_j$ are easily seen to be maximal, as

$$\mathbb{Z}[x]/\mathfrak{m}_j = \mathbb{Z}[x]/(q, x - j^2) \cong \mathbb{F}_q[x]/(x - j^2),$$

which is clearly a field, since $x - j^2$ is irreducible.

Lemma 5.2. *The minimal polynomial of ω_p, $\phi_p(x)$, is contained in the ideal $(q, x-n)$ if and only if n is a quadratic residue mod q incongruent to 1. In particular, $\phi_p(x) \in \mathfrak{m}_j$. These ideals have natural correspondents in $\mathbb{Z}[\omega]$, namely the ideals $\mathfrak{p}_j = (q, \omega - j^2)$. As we shall soon see, these are the prime factors of the ideal (q).*

Proof. It is equivalent to show that $\phi_p(x) \in (x-n) \subset \mathbb{F}_q[x]$, with $\phi_p(x)$ considered as a polynomial in $\mathbb{F}_q(x)$. Now $\phi_p(x) \in (x-n)$ is equivalent to $x-n \mid \phi_p(x)$, i.e. n is a root of $\phi_p(x)$. Since $\phi_p(1) \equiv p-1 \not\equiv 0 \bmod q$, it suffices to consider the case $n \not\equiv 1 \bmod q$. By the identity

$$\phi_p(x) = \frac{x^p - 1}{x - 1}$$

and the fact that $\varphi(q) = 2p$, where φ is Euler's totient function, we may now conclude that

$$\phi_p(n) \equiv 0 \iff n^p - 1 \equiv 0 \iff n \text{ is a quadratic residue mod } q,$$

since the quadratic residues mod q are precisely the elements whose orders are p. □

The above lemma can now be used to factorize the ideal $(q, \varphi_p(x))$ of $\mathbb{Z}[x]$ into a product of maximal ideals.

Theorem 5.3. *We have the ideal factorization $(q, \phi_p(x)) = \prod_2^p \mathfrak{m}_j$ in the ring $\mathbb{Z}[x]$.*

Proof. We have by the above lemma that the only divisors of $\phi_p(x)$ in $\mathbb{F}_q[x]$ are $x-n$, where n is a quadratic residue incongruent to 1 mod q. Now $\phi_p(x) = \sum_0^{p-1} x^i$ so its degree is $p-1$ and there are exactly $p-1$ quadratic resudues mod q, not counting 1. Hence $\phi_p(x) = \prod_2^p (x - j^2)$ in $\mathbb{F}_q[x]$, from which it indeed follows that

$$(q, \phi_p(x)) = \prod_2^p (q, x - j^2)$$

from the correspondence theorem. □

Corollary 5.3.1. *The ideal (q) factors into the product $\prod_2^p \mathfrak{p}_j$ of prime ideals in the ring $\mathbb{Z}[\omega_p]$.*

Proof. The surjective homomorphism ψ sends $\mathfrak{m}_j$ to $\mathfrak{p}_j$ and $(q, \phi_p(x))$ to (q). Since $\ker \psi$ is contained in the respective ideals of $\mathbb{Z}$, the $\mathfrak{p}_j$ are all prime. □

With the above facts established, we are now ready to prove our main result.

Theorem 5.4. *Suppose p is a Sophie Germain prime with safe prime q. Then unique factorization fails for $\mathbb{Z}[\omega_p]$ if there exists no integer solutions $(x, y) \in \mathbb{Z}^2$ to the equation $x^2 + (-1)^{\frac{p+1}{2}} p y^2 = \pm 4q$.*

Proof. Let $L = \mathbb{Q}(\omega_p)$ and suppose that $\mathcal{O}_L$ is a PID. By the corollary above we have that $\prod_2^p \mathfrak{p}_j$ is the unique decomposition of (q) as a product of prime ideals in $\mathbb{Z}[\omega_p]$, so if $q = \prod_2^p \pi_j$, with $(\pi_j) = \mathfrak{p}_j$. The number q has norm $N_{\mathbb{L}|\mathbb{Q}}(q) = q^{p-1}$. Hence it follows by multiplicativity of the norm that $N_{L|\mathbb{Q}}(\pi_j) = \pm q$, because any π_j having a norm of a higher power would force some other π_j to have a norm of 1, thus being a unit. If this were the case we would have $\mathfrak{p}_j = \mathcal{O}_L$. But the $\mathfrak{p}_j$ are all proper prime ideals, so this is impossible.

The field $\mathbb{Q}(\omega_p)$ contains the quadratic subfield $K = \mathbb{Q}(\sqrt{d})$, with $d = (-1)^{\frac{p-1}{2}} p$. It therefore follows from Theorem 2.5 that we may decompose the norm of $L|\mathbb{Q}$ as

$$N_{L|\mathbb{Q}} = N_{K|\mathbb{Q}} \circ N_{L|K}.$$

Since $d \equiv 3 \bmod 4$, it follows that K has $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ as its field of integers by Theorem 2.2. Now suppose $\alpha \in \mathbb{Z}[\omega_p]$. The ring $\mathbb{Z}[\omega_p]$ is the ring of integers of L, so $N_{L|K}(\alpha) \in \mathcal{O}_K$ and we may therefore write

$$N_{L|K}(\alpha) = \frac{a + b\sqrt{d}}{2},$$

for some pair of integers $a, b \in \mathbb{Z}$ such that $a \equiv b \bmod 2$. The conjugate of such an element is simply $\frac{a - b\sqrt{d}}{2}$ and so we finally arrive at

$$N_{L|\mathbb{Q}}(\alpha) = N_{K|\mathbb{Q}}\left(\frac{a + b\sqrt{d}}{2}\right) = \frac{a + b\sqrt{d}}{2}\frac{a - b\sqrt{d}}{2} = \frac{a^2 - b^2 d}{4} = \frac{a^2 + (-1)^{\frac{p+1}{2}} p b^2}{4}.$$

Hence we would in particular have to have

$$a^2 + (-1)^{\frac{p-1}{2}} pb^2 = 4N_{L|\mathbb{Q}}(\pi_j) = \pm 4q,$$

if L were a PID. Therefore $\mathbb{Z}[\omega_p]$ can only be a PID when it is possible to find $a, b \in \mathbb{Z}$ such that $a^2 + (-1)^{\frac{p+1}{2}} pb^2 = \pm 4q$. UFD $\iff$ PID for Dedekind domains, so $\mathbb{Z}[\omega_p]$ must satisfy the same condition if it is a UFD. □

The above theorem is particularly useful when $p \equiv 3 \bmod 4$, as we can then sometimes prove that $\mathbb{Z}[\omega_p]$ is not a UFD simply by showing that the two-element set $S(p) = \{4q - 4p, 4q - p\}$ does not contain any squares, as $a^2 + pb^2$ is always positive.

Corollary 5.4.1. *If p is a Sophie Germain prime congruent to 3 mod 4 and in the interval $[23, 1000]$, then $\mathbb{Z}[\omega_p]$ is not a UFD.*

Proof. Since the relevant primes are all congruent to 3 mod 4, it is suffient to show that no element of $S(p)$, as defined above, is a square. The relevant sets $S(p)$ are listed below.

$$S(23) = \{96, 165\}, \quad S(83) = \{336, 585\}, \quad S(131) = \{528, 921\},$$

$$S(179) = \{720, 1257\}, \quad S(191) = \{768, 1341\}, \quad S(239) = \{960, 1677\} \quad S(251) = \{1008, 1761\},$$

$$S(359) = \{1440, 2517\}, \quad S(419) = \{1680, 2937\}, \quad S(431) = \{1728, 3021\}, \quad S(443) = \{1776, 3105\},$$

$$S(491) = \{1968, 3441\}, \quad S(659) = \{2640, 4617\}, \quad S(683) = \{2736, 4785\}, \quad S(719) = \{2876, 5037\},$$

$$S(743) = \{2976, 5205\}, \quad S(911) = \{3648, 6381\}$$

None of the numbers contained in the above sets are squares and this covers all Sophie Germain primes in the interval $[23, 1000]$ as listed in OEIS [6]. Thus the proof is complete. □

5.2 Second Proof

The second proof only considers the case $p = 23$. If we are solely interested in whether $\mathbb{Z}[\omega_{23}]$ is a UFD or not, this proof will add nothing of interest. While this might seem redundant at first glance, this second proof will make up for its comparative lack of generality by requiring us to understand more about the quadratic subfield $\mathbb{Q}(\sqrt{-23})$ of $\mathbb{Q}(\omega_{23})$. In particular, we will have an added incentive to compute the class number of said quadratic subfield.

For the rest of this section, set $K = \mathbb{Q}(\sqrt{-23})$, $L = \mathbb{Q}(\omega_{23})$, $\alpha = \frac{1+\sqrt{-23}}{2}$ and lastly $\mathfrak{p}_1 = (2, \alpha)$ and $\mathfrak{p}_2 = (2, 1 - \alpha)$ to be ideals of $\mathcal{O}_K$.

Lemma 5.5. *The ideal $\mathfrak{p}_1$ is not principal.*

Proof. Set $\mathfrak{p} = \mathfrak{p}_1$. Had $\mathfrak{p}$ been principal, we would have $\mathfrak{p} = (\pi)$ for some $\pi \in \mathcal{O}_K$ and we would have by Corollary 4.6.1 that $2 = \mathfrak{N}(\mathfrak{p}) = N_{K|\mathbb{Q}}(\pi) = \frac{x^2+23y^2}{4}$, where $x, y \in \mathbb{Z}$. This, however, implies the existence of a pair $(x, y) \in \mathbb{Z}^2$ such that $x^2 + 23y^2 = 8$, which is clearly ridiculous. It follows that $\mathfrak{p}$ cannot be principal. □

Lemma 5.6. *Let $\mathbb{Q} \subset K \subset L$ be a tower of Galois extensions of $\mathbb{Q}$, $\mathfrak{p}$ a prime ideal of $\mathcal{O}_K$ and $\mathfrak{P}$ a prime ideal of $\mathcal{O}_L$ lying over $\mathfrak{p}$. The map $N : Cl_L \to Cl_K$ defined by mapping the ideal class of $\mathfrak{a}$ to the class of the ideal $\mathfrak{N}_{L|K}(\mathfrak{a}) \cap \mathcal{O}_K$ is then a group homomorphism that sends the class of $\mathfrak{P}$ to the class of $\mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})}$.*

Proof. Set $f = f(\mathfrak{P}|\mathfrak{p})$. By Lemma 4.5 we already have that $\mathfrak{N}_{L|K}(\mathfrak{P}) = \mathfrak{p}^f \mathcal{O}_L$. It is clear that the operations performed by N on an ideal are well-defined and it therefore suffices to show that $\mathfrak{a}\mathcal{O}_L \cap \mathcal{O}_K = \mathfrak{a}$, as then it will both follow that N is a homomorphism and that $N(\mathfrak{P}) = \mathfrak{p}^f$. It is clear that $\mathfrak{a}\mathcal{O}_L \cap \mathcal{O}_K$ is an ideal of $\mathcal{O}_K$ containing $\mathfrak{a}$, so the proof may be further reduced to showing the reverse containment $\mathfrak{a}\mathcal{O}_L \cap \mathcal{O}_K \subset \mathfrak{a}$.

The key to this is using the unique factorization into prime ideals; the ideal $\mathfrak{a}$ factorizes into

$$\mathfrak{a} = \prod_1^r \mathfrak{p}_i^{\nu_i}.$$

With this in mind, fix an index i and set $\mathfrak{p} = \mathfrak{p}_i$ and $\nu = \nu_i$. In view of the containment $\mathfrak{a} \cap \mathcal{O}_K \subset \mathfrak{p}^\nu \cap \mathcal{O}_K$, it suffices to show that $\mathfrak{p}^\nu \cap \mathcal{O}_K = \mathfrak{p}^\nu$ and it will then immediately follow that $\mathfrak{a} \mid \mathfrak{a}\mathcal{O}_L \cap \mathcal{O}_K$ and therefore that in fact $\mathfrak{a} = \mathfrak{a}\mathcal{O}_L \cap \mathcal{O}_K$. Now suppose that on the contrary, $\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_K \neq \mathfrak{p}^\nu$. This must imply that $\mathfrak{p}$ is in fact equal to $\mathfrak{p}^n$ for some integer n satisfying $1 \leq n < \nu$, as clearly $\mathfrak{p}^\nu\mathcal{O}_L \cap \mathcal{O}_K$ must contain $\mathfrak{p}^\nu$. However, if this were true, we would have

$$\mathfrak{p}^n\mathcal{O}_L = (\mathfrak{p}^\nu\mathcal{O}_L \cap \mathcal{O}_K)\mathcal{O}_L = \mathfrak{p}^\nu\mathcal{O}_L,$$

which stands in clear violation to the unique prime factorization of $\mathcal{O}_L$. To see that the latter equality above holds, simply observe that the middle expression is $\mathfrak{a}^{ece} = \mathfrak{a}^e$, with $\mathfrak{a} = \mathfrak{p}^\nu$ and $\mathfrak{a}^e = \mathfrak{a}\mathcal{O}_L$ and $\mathfrak{A}^c = \mathfrak{A} \cap \mathcal{O}_K$ the extension and contraction, respectively, with respect to the injection homomorphism $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$. □

Lemma 5.7. *The class number of* $\mathbb{Q}(\sqrt{-23})$ *is* 3.

Proof. Let $K = \mathbb{Q}(\sqrt{-23})$. The Minkowski bound for K is $M = \frac{2}{\pi}\sqrt{23}$ and it is easily seen that $M^2 < \frac{4}{9} \cdot 23 = \frac{92}{9} < \frac{144}{9} = 4^2$, so $M < 4$. The ideal class group of K is therefore generated by the primes lying over (2) and (3). Denote the non-trivial element of $\mathrm{Gal}(K|\mathbb{Q})$ by σ and set $\alpha = \frac{1+\sqrt{-23}}{2}$, $\mathfrak{p} = (2, \alpha)$ $\mathfrak{q} = (3, \alpha)$. In this notation

$$(2) = \mathfrak{p}(\sigma\mathfrak{p}), \quad (3) = \mathfrak{q}(\sigma\mathfrak{q}).$$

Now consider the principal ideal (α). It has norm $\mathfrak{N}((\alpha)) = 6$ and must therefore be divisible by exactly one prime lying over each of the ideals (2) and (3). As $(\alpha) \subset \mathfrak{p}, \mathfrak{q}$, the decomposition of (α) into a product of prime ideals must be $(\alpha) = \mathfrak{p}\mathfrak{q}$. It follows that $(\sigma\mathfrak{p})^{-1}P_K = \mathfrak{p}P_K = \mathfrak{q}^{-1}P_K = (\sigma\mathfrak{q})P_K$ and so Cl_K is generated by $\mathfrak{p}P_K$.

Finally, we consider what $\mathfrak{p}^2P_K$ could possibly be. We have by the Minkowski bound that $\mathfrak{p}^2P_K$ must contain some integral ideal of norm 1, 2 or 3. It suffices to consider $\mathcal{O}, \mathfrak{p}$ and $\sigma\mathfrak{p}$, since each of the primes lying over 3 are in the same ideal class as a prime lying over 2. If $\mathcal{O} \in \mathfrak{p}^2P_K$, we must have that $\mathfrak{p}^2$ principal, which would imply that it is generated by an element π of norm 2 or 4. This would further require that at least one of the equations

$$x^2 + 23y^2 = 8, \quad x^2 + 23y^2 = 16$$

would have to admit an integral solution. Under these conditions the left equation is clearly unsolvable and the right equation admits only the solutions $(x, y) = (\pm 4, 0)$, so then π would have to be 2, which is not even an element of $\mathfrak{p}^2$. On the other hand, $\mathfrak{p} \in \mathfrak{p}^2P_K$ would force $\mathcal{O} \in \mathfrak{p}^{-1}\mathfrak{p}^2P_K = \mathfrak{p}P_K$, which contradicts the fact that $\mathfrak{p}$ is non-principal. We must therefore have that $\sigma\mathfrak{p} \in \mathfrak{p}^2P_K$. In particular, this proves that

$$\mathfrak{p}^3P_K = \mathfrak{p}\mathfrak{p}^2P_K = \mathfrak{p}(\sigma\mathfrak{p})P_K = (2)P_K = P_K,$$

so the order of $\mathfrak{p}$, and consequently Cl_K, must be 3. □

Theorem 5.8. *The ring* $\mathbb{Z}[\omega_{23}]$ *is not a UFD.*

Proof. Set $\mathfrak{p} = \mathfrak{p}_1$ and $\mathfrak{P} = \mathfrak{p}\mathcal{O}_L$. We begin by showing that $\mathfrak{P}$ lies over $\mathfrak{p}$ with inertial degree $f = 11$.

The ideal (2) splits into two prime ideals in $\mathcal{O}_K$, as $(2, \alpha)(2, 1 - \alpha) = (2)$ is the unique factorization of (2) into prime ideals of $\mathcal{O}_K$. Hence its inertia degree is $f(\mathfrak{p}|(2)) = 1$.

Let us now consider $f(\mathfrak{P}|(2))$. We first prove that $\mathfrak{P}$ actually lies over (2). Of course $\mathbb{Z} \subset \mathcal{O}_K$, so $\mathfrak{P} \cap \mathbb{Z} = (\mathfrak{P} \cap \mathcal{O}_K) \cap \mathbb{Z} = \mathfrak{p} \cap \mathbb{Z} = (2)$, and so $\mathfrak{P}$ indeed lies over (2). Now consider the identity

$$f(\mathfrak{P}|(2)) = [\mathcal{O}_L/\mathfrak{P} : \mathbb{Z}/(2)] = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}][\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/(2)] = f \cdot 1 = f.$$

Theorem 3.7 tells us that the only possible alternatives are 1 and 11. However, 1 is impossible, since this would imply that 2 is completely ramified in $\mathbb{Z}[\omega_{23}]$, despite 2 not dividing the discriminant of $\mathbb{Z}[\omega_{23}]$. It follows that $f = 11$.

This tells us that the homomorphism N from Lemma 5.6 sends $\mathfrak{P}P_L$ to $\mathfrak{p}^{11}P_K$. We therefore have that the order $\mathfrak{p}^{11}P_K$ divides that of $\mathfrak{P}P_K$. The desired statement will therefore follow if we can show that the order of $\mathfrak{p}P_K$ is not a multiple of 11, as this will imply that $\mathfrak{p}^{11}P_K \neq P_K$. Fortunately, this is an immediate consequence of Lemma 5.7. UFD $\iff$ PID for Dedekind domains, so we have just shown that $\mathbb{Z}[\omega_{23}]$ cannot be a UFD. □

There is a bit more to be taken away from this proof than merely another way of proving something we already knew. Not only have we learned the class number of $\mathbb{Q}(\sqrt{-23})$ is 3; this number along with the non-triviality of the homomorphism N from Lemma 5.6 tells us that the class number of $\mathbb{Q}(\omega_{23})$ must be divisible by 3. Actually, equality to 3 is in fact the case [7], although showing this would require us to consider many more cases than we had to in $\mathbb{Q}(\sqrt{-23})$ if we were to use essentially the same method due to the sheer size of the Minkowski bound in the cyclotomic case.

6 Fermat's Last Theorem and Regular Primes

In the previous section we investigated a prime for which Lamé's proof did not work. Here we prove Fermat's last theorem for a subclass of primes called **regular primes**. We begin by dealing with case I; the proof for regular primes other than 3 is essentially follows a series of exercises from Chapter 1 of [4] whereas the case $p = 3$ is an argument found in [1]. When these two instances are dealt with we finish by showing case II for arbitrary regular primes, closely following the treatment of the proof given in [1]. Throughout this section, we set $\omega = \omega_p$ and let p be an arbitrary regular prime unless otherwise explicitly stated.

6.1 Case I for $p = 3$

Although Euler never published a correct proof, case I can be established for $p = 3$ using methods known to Euler, as is done in Sections 2.4–2.5 of [1]. Alternatively, if we are content with settling only case I for $p = 3$, we may observe that 3 is a Sophie Germain prime. We may therefore prove a more general statement that holds for arbitrary[6] Sophie Germain primes.

Theorem 6.1. *Let p be an odd Sophie Germain prime. Then any integral solution (x, y, z) to the equation*

$$x^p + y^p = z^p$$

has the property that $p \mid xyz$.

Proof. We assume without loss of generality that the involved variables are relatively prime and begin by rewriting the equation on the symmetric form

$$x^p + y^p + z^p = 0$$

by changing the sign of z. It may now be observed that

$$-z^p = (x + y) \sum_0^{p-1} x^i (-y)^{p-1-i}$$

and clearly the same holds for any permutation of the order of the entries of (x, y, z) by symmetry. Now fix a prime r and suppose that r divides $x + y$. Then $x \equiv -y \bmod r$, so that

$$\sum_0^{p-1} x^i (-y)^{p-1-i} \equiv p x^{p-1}.$$

This forces either $r = p$, in which case we are done, or $r \mid x$. The latter case would imply that x and y are not coprime, contrary to hypothesis, since it was assumed that r also divides $x + y$.

Since the factors $x + y$ and $\sum_0^{p-1} x^i (-y)^{p-1-j}$ were shown to be coprime, we have by the original eqution and symmetry that

$$\begin{array}{lll} x + y = a^p, & \sum_0^{p-1} x^i (-y)^{p-1-i} = A^p, & z = -aA, \\ y + z = b^p, & \sum_0^{p-1} y^i (-z)^{p-1-i} = B^p, & x = -bB, \\ z + x = c^p, & \sum_0^{p-1} z^i (-x)^{p-1-i} = C^p, & y = -cC. \end{array}$$

However, if φ is taken to denote Euler's totient function, we have that $\varphi(q) = 2p$, and so the only p^{th} powers mod q are 0 and ± 1. Hence the only way for the equation

$$x^p + y^p + z^p \equiv 0 \bmod q$$

is for at least one variable, say x, to be divisible by q. We may easily deduce that

$$2x = b^p + c^p + (-a)^p$$

by the equations involving sums of two of the variables above and so at least one of the numbers b, c and a must be divisble by q. However, if a or c is divisible by q then either y or z is also divisible by q,

[6] In fact, even for $p = 2$, as is easily seen by considering the equation $x^2 + y^2 = z^2$ in $\mathbb{F}_2$; however, since this is hardly relevant, we only properly state and prove the statement for Sophie Germain primes $p \geq 3$.

contradicting the assumption of the entries of (x, y, z) being coprime. It must therefore be the number b that is divisible by q, but then $y \equiv -z \bmod q$, so that in fact

$$B^p \equiv py^{p-1} \bmod q.$$

Since x was assumed to be divisible by q, it may also be seen that $y^{p-1} \equiv A^p \bmod q$, so that in fact

$$B^p \equiv pA^p.$$

Since the p^{th} powers mod q were precisely 0 and ± 1 the only way for this to happen is $B \equiv A \equiv 0 \bmod q$, in which case q is a common divisor of x and y. This is yet another contradiction of the assumption that the entries of (x, y, z) are relatively prime and this finally yields the desired divisibility $p \mid xyz$. □

Before moving on to other primes, we show that $\mathbb{Z}[\omega_3]$ is in fact a UFD. One way to prove this is to show that it is a Euclidean domain, but let us instead see if we can do this by determining the class number of $\mathbb{Z}[\omega_3]$. Set $\omega = \omega_3$ and $K = \mathbb{Q}(\omega)$. The Minkowski bound M satisfies

$$M = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)^1 \sqrt{3^2} = \frac{6}{\pi} < 3,$$

so every ideal class of K contains an ideal of absolute norm 2. Therefore Cl_K is generated by the prime ideals of $\mathbb{Z}[\omega]$ lying over 2. It is well-known that the polynomial $x^2 + x + 1$ in $\mathbb{F}_2[x]$ is irreducible, so by Theorem 3.8 it follows that

$$2\mathcal{O} = (2, \omega^2 + \omega + 1) = (2, 0) = (2),$$

and so 2 splits into just one principal ideal of intertia degree 2. Since every ideal class contains a prime ideal lying over 2 and as there is only one such ideal there can be only one ideal class and thus $h_K = 1$. The foundational arguments of Lamé's idea for a proof therefore hold.

Now set $K = \mathbb{Q}[\omega_p]$ for an arbitrary prime p. Then it can in fact be shown that $h_K = 1 \iff p \leq 19$, which was done independently by Montgomery and Uchida [7]. For the reader interested in a proof, this can be found in Chapter 11 of [7], although it should be noted that understanding this proof requires any things that are neither a prerequisite for understanding this paper nor covered within it. In particular, one will need some knowledge in complex analysis, Dirichlet characters and Dirichlet L-series. Fortunately, the latter two of the three are in fact covered in earlier chapters of [7].

6.2 Case I for $p > 3$

The proof for case I essentially begins like the incomplete proof proposed by Lamé but makes use of unique ideal factorization rather than unique factorization of elements. Recall the factorization of ideals proposed in the introduction, namely

$$\prod_0^{p-1}(x + \omega^k y) = (z)^p. \tag{5}$$

For the remainder of this subsection, set $\mathfrak{a}_k = (x + \omega^k y)$, so that in this notation $(z)^p$ factorizes as

$$\prod_0^{p-1} \mathfrak{a}_k = (z)^p.$$

Lemma 6.2. *The factors $\mathfrak{a}_k$ above are relatively prime.*

Proof. If $\mathfrak{p}$ divides both $\mathfrak{a}_i$ and $\mathfrak{a}_j$, where $i < j$, then it divides their greatest common divisor $\mathfrak{a}_i + \mathfrak{a}_j$ and therefore in particular the principal ideal $(\omega^i y - \omega^j y) = (y - \omega^{j-i} y)$ contained therein. It follows from the identities

$$\sum_0^{p-1} x^i = \frac{x^p - 1}{x - 1} = \prod_1^{p-1}(x - \omega^k)$$

and by evaluating the middle and left-most expressions above at 1 that

$$p = \sum_0^{p-1} 1^i = \prod_1^{p-1}(1 - \omega^k).$$

Hence $\mathfrak{p} \mid (1-\omega^{j-i})(y)$ in fact implies that $\mathfrak{p}$ divides (py). In view of (5), $\mathfrak{p}$ must then also divide $(z)^p$. The fact that $\mathfrak{p}$ divides both (yp) and (z) is a contradiction, and we may conclude that the ideals $(x+\omega^k y)$ are relatively prime. □

Corollary 6.2.1. *For each factor $\mathfrak{a}_k$ there exists some non-zero non-unit a_k of $\mathbb{Z}[\omega]$ such that $\mathfrak{a}_k$ may be written on the form*

$$\mathfrak{a}_k = (a_k)^p.$$

Proof. Since the $\mathfrak{a}_k$ are relatively prime the unique prime factorization forces each $\mathfrak{a}_k$ to be a p^{th} power of some ideal, since their product $(z)^p$ is a p^{th} power. Now p was assumed to be regular, so the class number of $\mathbb{Q}(\omega)$ is not divisible by p; hence if $\mathfrak{a}_k = \mathfrak{b}^p$, we must have that $\mathfrak{b}$ is a principal ideal, say (a_k).

Now set $K = \mathbb{Q}(\omega)$ and suppose that a_k is a unit. Then so is $x+\omega^k y$ and for $k = 0$ it follows that

$$\pm\mathfrak{N}(\mathfrak{a}_0) = N_{K|\mathbb{Q}}(x+y) = (x+y)^{p-1} = \pm 1.$$

This forces one of x, y to be 0 and the other to be ± 1, but x, y were both assumed to be non-zero so this is a contradiction. When $k > 0$ is assumed we similarly get

$$\pm\mathfrak{N}(\mathfrak{a}_k) = N_{K|\mathbb{Q}}(x+\omega^k y) = \frac{x^p+y^p}{x+y},$$

so $x^p + y^p$ must be equal to $\pm(x+y)$. In case of $-$ this is equivalent to $x^p + x = y^p + y$ and since $f(t) = t^p + t$ is injective as a function defined on $\mathbb{R}$ it follows that $x = y$. These numbers may be assumed to be relatively prime, for if they are not then their greatest common divisor, say d, must also divide z and so dividing the equation $x^p + y^p = z^p$ by d gives a new equation where they are indeed relatively prime. Thus we have forced $x = y = \pm 1$ when $x^p + y^p = -(x+y)$, but neither 2 nor -2 is a p^{th} power of an integer, so $x^p + y^p \neq z^p$, contrary to hypothesis.

Consider now instead the possibility

$$x^p + y^p = x + y.$$

If we can show that it has no solutions such that both x and y are non-zero, we are done. We may assume without loss of generality that $x > 0$, for if this is not the case multiply both sides by -1 to get an equation where this is the case. Now if y is of the same sign as x, we may set $x = e^s$, $y = e^t$ for some pair of real numbers s and t. Substituting this into the equation we get

$$\begin{aligned} e^{ps} + e^{pt} &= e^s + e^t \\ \iff (e^s + e^t)(e^p - 1) &= 0, \end{aligned}$$

but there do not exist any real numbers s and t that satisfy equivalent equation. Finally, if x and y are of opposite sign, then setting $x = e^s$ and $y = -e^t$ similarly gives the equation

$$(e^s - e^t)(e^p - 1) = 0,$$

which is satisfied if and only if $s = t$ and therefore equivalently $x = -y$, but if this is the case then we may reach a contradiction by either noting that this implies that

$$z^p = x^p + y^p = x^p + (-x)^p = 0,$$

which contradict the fact that x, y and z were all assumed to be non-zero, or by noticing that $x = -y$ contradicts that x and y are relatively prime. Hence $x + \omega^k y$ cannot be a unit, since we assumed from the beginning that $(x, y, z) \in (\mathbb{Z} \setminus \{0\})^3$, and then neither can a_k. □

The isomorphism $\mathbb{Z}[\omega] \cong \mathbb{Z}[x]/(\phi_p)$ induced by mapping $f(x) \in \mathbb{Z}[x]$ to $f(\omega) \in \mathbb{Z}[\omega]$ tells us that each element a of $\mathbb{Z}[\omega]$ is uniquely representable on the form $a = \sum_0^{p-2} a_i \omega^i$ in the sense that the coefficients a_i are unique; furthermore, the identity

$$\phi_p(\omega) = \sum_0^{p-1} \omega^i = 0$$

is a direct consequence.

Theorem 6.3. *A rational integer m divides a in $\mathbb{Z}[\omega]$ if and only if the coefficients a_i in the sum $a = \sum_0^{p-1} a_i\omega^i$ are congruent to one another* mod m.

Proof. If the coefficients satisfy the congruence condition, adding a suitable multiple of $\phi_p(\omega)$ will clearly give a cyclotomic integer divisible by m. Conversely, if m divides a, consider the fact that we may find a polynomial f with integral coeffients of degree at most $p-2$ such that $a = f(\omega)$; in terms of ideals, this may be stated as $f(\omega) \in (m)$, which in turn implies that $f(x) \in (m, \phi_p(x))$ in the ring $\mathbb{Z}[x]$. It is now quite clear that the coefficients of f are congruent mod m. □

It is a well-known fact that in rings of characteristic p it holds that

$$\left(\sum_1^n x^i\right)^p = \sum_1^n {x_i}^p.$$

In view of this, we have that $a^p \equiv \left(\sum_0^{p-2} a_i\omega_i\right)^p \equiv \sum_0^{p-2}(a_i\omega)^p \equiv \sum_0^{p-2} {a_i}^p \bmod p\mathbb{Z}[\omega]$, which in particular shows that the image of a^p under the canonical projection $\mathbb{Z}[\omega] \twoheadrightarrow \mathbb{F}_p[\omega]$ can be represented with just an element of $\mathbb{F}_p$. Now the ideal factorization we did earlier tells us that $x + \omega y = \varepsilon a^p$, with ε a unit of $\mathbb{Z}[\omega]$. Let $\bar{\varepsilon}$ denote the complex conjugate of ε. We now prove a lemma that is due to Kummer [4].

Lemma 6.4 (Kummer)**.** *In $\mathbb{Z}[\omega]$, the quotient of units $u = \varepsilon/\bar{\varepsilon}$ is a power of ω.*

Proof. The element $\bar{\varepsilon}$ is a unit, for $\bar{\omega} = \omega^{p-1}$, so that $\bar{\varepsilon}$ is a conjugate of ε and therefore has the same norm. Another property ε and $\bar{\varepsilon}$ share is that they have the same modulus as complex numbers, so that their quotient has a modulus of 1, which means that it is of the form $e^{\frac{2\pi i}{x}}$, for some real x.

Now consider what algebraic integers could possibly have a modulus of 1. All of these occur as roots of monic polynomials with coefficients in $\mathbb{Z}$, so suppose $p(x)$ is such a polynomial of degree n. In view of the triangle inequality, each coefficient a_i of p, which is simply a sum of products of roots, must be bounded by some constant c_i, in such a way that $a_i \in [-c_i, c_i]$. We therefore see that there can only exist a finite amount of such polynomials for each degree n and therefore also only a finite amount of algebraic integers of modulus 1 whose minimal polynomial is of degree less than or equal to some fixed n. Now $\mathbb{Z}[\omega]$ is a field extension of degree $p-1$ over $\mathbb{Q}$ and can therefore not contain any algebraic integer whose minimal polynomial is of a higher degree. In particular, this means that x must be rational, as otherwise we would get an infinite amount of algebraic integers of modulus 1 by taking integral powers of u. This further shows that u must be a root of unity, leaving only the possibilities $u = \pm\omega^k$.

Suppose for now that the sign is negative, so that $u = -\omega^k$, and consider what this leads to in the ring $\mathbb{Z}[\omega]/(p)$. Then $\varepsilon = -\bar{\varepsilon}\omega^k$ implies that $\varepsilon^p = -\bar{\varepsilon}^p$, and in particular $\varepsilon^p \equiv -\bar{\varepsilon}^p \bmod p\mathbb{Z}[\omega]$. Complex conjugation does not change the real part of any number and $\varepsilon^p \bmod p$ is simply the sum of p^{th} powers of its integral coefficients when written out as a cycltomic integer, mod p. Hence it must be equal to its complex conjugate in $Z[\omega]/(p)$ and so we must in fact have that p divides ε^p, which is a unit of $\mathbb{Z}[\omega]$, despite not being a unit itself. □

Corollary 6.4.1. *Suppose that p is a regular prime strictly greater than 3. For the element $x + \omega$ from the factorization of $x^p + y^p = z^p$, it holds that*

$$x + \omega y \equiv \omega x + y \bmod p\mathbb{Z}[\omega].$$

Proof. The above lemma due to Kummer and our knowledge of binomial expansion in $\mathbb{F}_p[\omega]$ lets us conclude that for some integer k

$$\begin{aligned} x + \omega y &\equiv \varepsilon a^p \\ &\equiv \omega^k \bar{\varepsilon} a^p \\ &\equiv \omega^k \bar{\varepsilon} \bar{a}^p \\ &\equiv \omega^k \overline{(x + \omega y)} \\ &\equiv \omega^k (x + \omega^{p-1} y) \bmod p\mathbb{Z}[\omega]. \end{aligned}$$

But then we must have that $x + \omega y - \omega^k(x + \omega^{p-1}y) \equiv 0 \bmod p\mathbb{Z}[\omega]$, which implies that the set $\{1, \omega, \omega^k, \omega^{k+p-1}\} \subset \mathbb{F}_p[\omega]$ is linearly dependent. But $\{1, \omega, \ldots, \omega^{p-1}\}$ is a basis of $\mathbb{F}_p[\omega]$ as a vector

space over $\mathbb{F}_p$. Thus the linear dependence is only possible if k is either congruent to 0, 1 or 2 mod p, if $p \geq 5$, which is the case by hypothesis.

Out of the possibilites 0, 1 and 2 for the congruence class of k, let us first consider the former. If $k \equiv 0 \bmod p$, then $x+\omega y \equiv x+\omega^{p-1}y \bmod p\mathbb{Z}[\omega]$ and therefore p must divide the difference $\omega(1-\omega^{p-2})y$ so the norm p^{p-1} of p must divide the norm py^{p-1} of $\omega(1-\omega^{p-2})y$, but y was relatively prime to p so this cannot be. If $k \equiv 2 \bmod p$ we get a contradiction in the same way by observing that this implies that p then divides $(1-\omega^2)x$. Hence k must be congruent to 1 mod p and we arrive at

$$x + \omega y \equiv \omega x + y \bmod p\mathbb{Z}[\omega],$$

as was desired. □

With the above corollary established we are now in position to prove case I for regular primes other than 3.

Theorem 6.5. *Case I of Fermat's last theorem holds for all regular primes.*

Proof. Since $p = 3$ has already been dealt with in full generality, we focus on the situation where $p \geq 5$, in which case Corollary 6.4.1 gives that $x+\omega y \equiv \omega x+y \bmod p\mathbb{Z}[\omega]$, or equivalently that $p \mid (x-y)+(y-x)\omega$ in $\mathbb{Z}[\omega]$, This is in turn is equivalent to $x \equiv y \bmod p$ as rational integers. It follows from symmetry that also $x \equiv -z \bmod p$ by considering instead the equality $x^p + (-z)^p = (-y)^p$ and so we have from the original equality $x^p + y^p = z^p$ that

$$0 \equiv x^p + y^p - z^p \equiv 3x^p \bmod p,$$

which is a clear contradiction since p was assumed to be greater than 3. □

6.3 Case II

Case II for regular primes is a deeper result than that of the corresponding case I, as it requires the following lemma, which we state but do not prove.

Lemma 6.6 (Kummer's Lemma)**.** *Let p be a regular prime and suppose that ε is a unit of $\mathbb{Z}[\omega]$ such that*

$$\varepsilon \equiv n \bmod p\mathbb{Z}[\omega_p]$$

for some rational integer n. The unit ε is then a p^{th} power of some unit of $\mathbb{Z}[\omega]$.

This lemma is deeper than anything required to settle case I for regular primes in the sense that its proof involves concepts that this paper neither mentions nor assumes that its reader should know. The interested reader may find a proof near the end of Chapter 5 of [7].

Once again, consider the factorization (5) of $(z)^p$ into ideals and set $\mathfrak{a}_k = (x + \omega^k y)$. It is possible to find an integer z_0 coprime to p such that $(z) = (1-\omega)^\ell(z_0)$, by which we may rewrite (5) on the form

$$\prod_0^{p-1} \mathfrak{a}_k = (1-\omega)^{p\ell}(z_0)^p. \tag{6}$$

We begin the proof of the second case by proving an analogue to Lemma 6.2.

Lemma 6.7. *The factors $\mathfrak{a}_k$ are each divisible by $(1-\omega)$ and only $\mathfrak{a}_0$ is divisible by $(1-\omega)^2$. In particular, the ideals $\mathfrak{a}_k(1-\omega)^{-1}$ are pair-wise coprime.*

Proof. Following the arguments of Lemma 6.2 we again find that any prime ideal $\mathfrak{p}$ dividing two distinct factors $\mathfrak{a}_i$ and $\mathfrak{a}_j$ must also divide the ideal $(1-\omega)(y)$. Since $p \mid z$ we may no longer conclude that $\mathfrak{p} \nmid (1-\omega)$; in fact, this must be the case for at least one factor, say $\mathfrak{a}_k$. But

$$x + \omega^k y - \omega^k(1-\omega)y = x + \omega^{k+1}y,$$

which in terms of ideals translates into

$$(1-\omega) = \mathfrak{a}_k + (1-\omega) \supset \mathfrak{a}_{k+1},$$

which shows that $\mathfrak{a}_{k+1}$, is also divisible by $(1-\omega)$. Hence by repeating this argument for each successive index, it follows in a finite amount of steps that $(1-\omega) \mid \mathfrak{a}_k$ for every index k.

Let us now prove that at least one factor is divisible by $(1-\omega)^2$. Our first step towards this is to assume the contrary. Since all factors are divisible by $(1-\omega)$, this would mean that we can find p elements $a_k \in \mathbb{Z}[\omega]$ such that $a_k(1-\omega) = x + \omega^k y$ such that $1-\omega$ divides none of the a_k. But we have previously shown that $(1-\omega)$ is a prime lying over p of inertia degree 1, so that $\mathbb{Z}[\omega]/(1-\omega) \cong \mathbb{Z}/p\mathbb{Z}$, which in particular tells us that there can only be $p-1$ non-zero congruence classes mod $(1-\omega)$. Hence $a_i - a_j \equiv 0 \bmod (1-\omega)$, for some pair of distinct indices i and j, which would in turn imply that $(1-\omega)^2 \mid (1-\omega)(y)$, or equivalently that $(1-\omega) \mid (y)$ and we have thus reached a contradiction.

If there were two distinct factors $\mathfrak{a}_i$ and $\mathfrak{a}_j$ such that $(1-\omega)^2$ divides both we would then have again $(1-\omega)^2 \mid (1-\omega)(y)$ as an immediate consequence. There therefore exists only one factor $\mathfrak{a}_k$ divisible by $(1-\omega)^2$. This factor must be $\mathfrak{a}_0 = (x+y)$, as $x+y$ is an integer and so the ideal $\mathfrak{a}_0$ must be divisible by $(1-\omega)^{p-1}$ whenever it is divisible by $(1-\omega)$.

In view of what has been proven so far, it is now an immediate consequence that the ideals $\mathfrak{a}_k(1-\omega)^{-1}$ are pair-wise relatively prime; the ideals $\mathfrak{a}_k(1-\omega)^{-1}$ are coprime by arguing mutatis mutandis as we did for the factors $\mathfrak{a}_k$ in Lemma 6.2, since we have by dividing out factors $(1-\omega)$ from each $\mathfrak{a}_k$ forced all but one of them to be relatively prime to p. □

The above lemma essentially lets us instead consider the factorization

$$\prod_0^{p-1} \mathfrak{a}_k (1-\omega)^{-1} = (z)^p (1-\omega)^{-p}.$$

Arguing as in case I, we find that

$$\frac{x+\omega^k y}{1-\omega} = \varepsilon_k t_k^p,$$

for some unit ε_k and some cyclotomic integer t_k, for each index $k > 0$. For $k = 0$ we similarly find

$$\frac{x+y}{(1-\omega)^{p\ell-(p-1)}} = \varepsilon_0 t_0^p,$$

where the exponent in the denominator is found by considering the amount and distribution of factors $1-\omega$ in the product $\prod_0^{p-1}(x+\omega^k y)$. Multiplying by the denominator of the left-hand side on both sides of each equation and setting $s = (1-\omega)^{\ell-1} t_0$ gives rise to p equations, out of which we focus on the three in the system of equations below.

$$\begin{cases} x + y = (1-\omega)\varepsilon_0 s^p \\ x + \omega y = (1-\omega)\varepsilon_1 t_1^p \\ x + \omega^{p-1} y = (1-\omega)\varepsilon_{p-1} t_{p-1}^p \end{cases}$$

The variable x may be eliminated by subtracting the second equation from the first and the first from the third, which results in the new system below.

$$\begin{cases} (1-\omega)y = (1-\omega)\left(\varepsilon_0 s^p - \varepsilon_1 t_1^p\right) \\ (\omega^{p-1}-1)y = (1-\omega)\left(\varepsilon_{p-1} t_{p-1}^p - \varepsilon_0 s^p\right) \end{cases}$$

The variable y may be eliminated in a similar fashion by subtracting the first equation from the second multiplied by ω in the above system, which after division by $(1-\omega)$ yields the equation

$$0 = \omega\left(\varepsilon_0 s^p - \varepsilon_{p-1} t_{p-1}^p\right) - \left(\varepsilon_1 t_1^p - \varepsilon_0 s^p\right).$$

The above equation may then quite easily be algebraically manipulated to instead read

$$0 = (1+\omega)\varepsilon_0 s^p + (-\varepsilon_1) t_1^p + (-\omega\varepsilon_{p-1}) t_{p-1}^p.$$

Now $1+\omega = (1-\omega^2)(1-\omega)^{-1}$ and $1+\omega$ is therefore a cyclotomic unit. Hence the above equation may be written on an equivalent and simpler form by setting $E_0 = (1+\omega)\varepsilon_0 E_1^{-1}$, $E_1 = -\varepsilon_1$ and lastly $E_{p-1} = -\omega\varepsilon_{p-1}E_1^{-1}$. After substituting back from s to t_0 this gives us the much less cluttered equation

$$0 = E_0\left((1-\omega)^{p(\ell-1)} t_0\right)^p + t_1^p + E_{p-1} t_{p-1}^p$$

to work with. Now if $\ell > 1$, considering where the canonical projection $\pi : \mathbb{Z}[\omega] \twoheadrightarrow \mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$ sends each side of the above equation gives rise to the congruence relation

$$0 \equiv m_1 + E_{p-1}m_{p-1} \bmod p\mathbb{Z}[\omega],$$

with both m_1 and m_{p-1} being integers relatively prime to p. The unit E_{p-1} must therefore be congruent to an integer m such that $m \equiv -m_1 m_{p-1}^{-1} \bmod p\mathbb{Z}$, so that $E_{p-1} = e^p$ for some unit e of $\mathbb{Z}[\omega]$ by Kummer's lemma. We may therefore further simplify our equation, by setting $u = et_{p-1}$, yielding

$$0 = E_0 \left((1-\omega)^{\ell-1}\right)^p t_0^p + t_1^p + u^p.$$

This motivates the consideration of solutions of the more general equation

$$0 = x^p + y^p + \varepsilon \left((1-\omega)^\ell z\right)^p,$$

where x, y and z are pair-wise coprime cyclotomic integers relatively prime to $1-\omega$ such that $xyz \neq 0$ and ℓ a positive rational integer. If we can show that this more general equation has no such solutions then the special case where x, y, $(1-\omega)^\ell z$ and ε are rational integers will give us exactly what we want. We are now ready to put the final nail in the coffin.

Theorem 6.8. *Let ε be a cyclotomic unit and ℓ a positive rational integer. Furthermore, suppose that x, y and z are cyclotomic integers such that $xyz \neq 0$ and that x, y, z and $1-\omega$ are pair-wise relatively prime. Then the equation*

$$0 = x^p + y^p + \varepsilon \left((1-\omega)^\ell z\right)^p$$

is impossible.

Proof. An ideal factorization analogous to (6) is still applicable, namely

$$\prod_0^{p-1} \mathfrak{a}_k := \prod_0^{p-1} (x + \omega^k y) = (1-\omega)^{pl}(z)^p$$

and Lemma 6.7 still holds, although with the restriction that we can't necessarily argue that $\mathfrak{a}_0$ is the precise factor divisble by $(1-\omega)^2$ in the same way. This is due to us no longer being able to guarantee that $x+y$ is rational integer. However, if $(1-\omega)^2$ divides some other factor, say $\mathfrak{a}_m$, then multiplying y by a factor ω^{p-k} in the original equation gives a new equation which gives rise to an ideal factorization

$$\prod_0^{p-1} \mathfrak{b}_k := \prod_{k=0}^{p-1} \mathfrak{a}_{p+k-m}$$

where indeed $(1-\omega) \mid \mathfrak{b}_0$. Hence we may assume without loss of generality that in fact $(1-\omega)^2$ divides $\mathfrak{a}_0$. Repeating the arguments made after the proof of Lemma 6.7, we get an equation of the form

$$X^p + Y^p = E(1-\omega)^{(\ell-1)p} Z^p,$$

with X, Y and Z cyclotomoic integers relatively prime to each other and $1-\omega$ such that their product is non-zero and E a cyclotomic unit. Hence we can, starting out with any possible value for ℓ in the original equation and eventually reach an equation which is of the same type but with $\ell = 1$. But if we were to actually have $\ell = 1$, then each factor would be divisible by $(1-\omega)$ only once, since they are all divisble by $(1-\omega)$. However, we have also shown that there is always exactly one factor divisible by $(1-\omega)^2$, so $\ell = 1$ is impossible. In view of the reduction possible for any $\ell > 1$, it is therefore impossible for there to exist any value of ℓ such that the original equation holds. □

References

[1] Harold M. Edwards. *Fermat's Last Theorem: A Genetic Introdution to Algebraic Number Theory*. Springer-Verlag New York Heidelberg Berlin, 1999.

[2] Harold M. Edwards. "The Background of Kummer's Proof of Fermat's Last Theorem for Regular Primes". In: *Archive for History of Exact Sciences* 14.3 (1975), pp. 219–236. ISSN: 00039519, 14320657. URL: http://www.jstor.org/stable/41133432.

[3] Gabriel Lamé. "Démonstration générale du théorème de Fermat, sur l'impossibilité, en nombres entiers, de l'équation $x^n + y^n = z^n$". In: *Compte rendu des séances de l'académie des sciences* (1847), pp. 310–316.

[4] Daniel A. Marcus. *Number Fields*. Second Edition. Springer Verlag Inc., New York, 2018.

[5] Jürgen Neukirch. *Algebraic Number Theory*. Springer-Verlag Berlin Heidelberg, 1999.

[6] N. J. A. Sloane. *The On-Line Encyclopedia of Integer Sequences*. 2021. URL: https://oeis.org/A005384.

[7] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Second Edition. Springer Verlag Inc., New York, 1997.