University of Plymouth

PEARL **https://pearl.plymouth.ac.uk**

The Plymouth Student Scientist - Volume 11 - 2018 The Plymouth Student Scientist - Volume 11, No. 2 - 2018

2018

Algebraic Number Theory and Fermat's Last Theorem

Evans, E.

Evans, E. (2018) 'Algebraic Number Theory and Fermat's Last Theorem', The Plymouth Student Scientist, 11(2), p. 92-143.
http://hdl.handle.net/10026.1/14185

The Plymouth Student Scientist
University of Plymouth

All content in PEARL is protected by copyright law. Author manuscripts are made available in accordance with publisher policies. Please cite only the published version using the details provided on the item record or document. In the absence of an open licence (e.g. Creative Commons), permissions for further reuse of content should be sought from the publisher or author.

Algebraic Number Theory and Fermat's Last Theorem

Edward Evans

Project Advisor: Dr. Daniel Robertz, School of Computing, Electronics, and Mathematics, Plymouth University, Drake Circus, Plymouth, PL4 8AA

Abstract

The project aims to deliver sufficient mathematical background to understand a partial proof, due to Ernst Kummer, of Fermat's last theorem for a specific class of primes called regular primes. In doing so, we also develop some theory that is applicable to a wide range of scenarios in modern number theory, a few of which are discussed in somewhat more superficial detail in the final section.

Introduction

> *Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*
>
> — Pierre de Fermat [1]

Pierre de Fermat was a 17th century French lawyer and amateur mathematician, perhaps best known for his so-called *Last Theorem*. Fermat famously made annotations in his copy of Diophantus' *Arithmetica* (from which we take the name *Diophantine equation*), all of which were published posthumously by his son Samuel de Fermat as an appendix to a restored edition of Arithmetica. One-by-one, as the story goes, each of the unjustified annotations was proven. Finally, cl_1 problem 8 in Book II of Diophantus' Arithmetica asks [2, p.2]

> "Given a number which is a square, write it as a sum of two other squares."

Fermat's notorious annotation of this problem follows (a translation of the epigraph heading this section given in [2]):

> "On the other hand, it is impossible for a cube to be written as a sum of two cubes, or a fourth power to be written as a sum of two fourth powers or, in general, for any number which is a power greater than the second to be written as a sum of two like powers. I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain."

The symbolism we have today grants us a much more succinct expression of this annotation:

> "For any natural number $n > 2$, there exists no integer triple (x, y, z) with $xyz \neq 0$ such that $x^n + y^n = z^n$."

It is exactly this assertion that we refer to now as *Fermat's last theorem*[1], being the last of his annotations to be proven.

The aim of this project is to provide sufficient mathematical background in order to be able to understand a modernised version of a partial proof of Fermat's last theorem due to Ernst Kummer. By modernised, I mean that most of the modern algebraic language used in this project was not available to Kummer. Indeed, most of his original proof in [13] was given in terms of so-called ideal complex numbers and his regularity condition was given in terms of divisors of the numerators of Bernoulli numbers.

In the introductory section we shall provide some of the mathematical background and terminology required to launch into the main subject matter of the project. This includes a (very) brief exposition of groups, rings, and modules (including the special case of vector spaces).

In Section 1 we shall see some of the main results in field theory and the related Galois theory. In the first section we shall see a way of constructing field extensions, prove

[1] Of course, without proof this name was inaccurate; some texts published prior to Wiles' proof refer to the "theorem" as *Fermat's conjecture*, though these are by far in the minority.

that the degree of a field extension is the product of the degrees of intermediate extensions, and discuss the properties of separability and normality. The second section is reserved for the Galois theory of fields both of characteristic 0 and of characteristic p, which will be used extensively throughout the project.

Following Section 1 we specialise to the case of number fields in Section 2. We discuss some numerical invariants of number fields, in particular the norm, trace, and discriminant of a number field. By analogy with $\mathbb{Q}$, we define the ring of integers of a number field to be a subring of the number field with some properties analogous to $\mathbb{Z}$ as a subring of $\mathbb{Q}$. These rings are the main setting for the partial proof of Fermat's last theorem discussed in Section 4.

Section 3 gives a much closer look at the properties of rings of integers as discussed in Section 2. In general, the ring of integers of a number field fails to retain the unique factorisation properties that we enjoy in $\mathbb{Z}$. To replace this, we develop a notion of unique factorisation at the level of ideals, and this will coincide with the unique factorisation of elements if and only if the ring under consideration is a principal ideal domain. The section following this discusses the notion of prime factorisation in a number field. That is, we discuss the question "when is a prime of $\mathbb{Z}$ still a prime of the ring of integers of a number field, and if it is not, how does this prime factorise in this new setting?". To finish the section, we shall discuss a way of quantifying the failure of a given ring of integers to be a unique factorisation domain. To do this, we endow the set of fractional ideals with a group structure with the product of fractional ideals as the group operation. In particular, the set of all principal fractional ideals is a normal subgroup of this group, and so the quotient of the group of fractional ideals by this subgroup is well-defined. We call this the ideal class group of the number field and its order will be referred to as the class number of the number field.

Section 4 contains the proof of Fermat's last theorem for regular primes. After defining what it means for a prime to be regular, we state and prove a few lemmas (save Kummer's lemma, whose proof is beyond the scope of the content of this project) that will be used in the proof. As regards the actual proof, we shall split the statement into two cases depending on the divisibility of the solution (x, y, z) by the exponent p. Case 1 is the easier of the two and concerns the case where $p \nmid xyz$. In this case, we shall show that Fermat's equation factors into linear factors over the relevant field (called a cyclotomic field) and that, when considered as an equation of ideals, the regularity condition on p allows us to reduce the equation to an equation of elements, leading to a contradiction. Case 2, when $p \mid xyz$, is harder and requires us to reformulate the statement of Fermat's last theorem. In fact, we shall prove a stronger statement which can be reduced to the case of Fermat's last theorem. When written as an equation of ideals, that $p \mid xyz$ causes us to lose the coprimality condition on the relevant ideals that made Case 1 easier to prove. Fortunately we can go some way to restoring this by undertaking a closer inspection of these ideals. Inevitably, we shall also reach a contradiction by Fermat's beloved method of infinite descent.

To conclude the project, Section 5 gives a slightly superficial insight into some possible areas of future study. In particular, the 20th century saw the development of class field theory, which provides information on so-called Abelian extensions of number fields based on information intrinsic to the number field[2]. We discuss the decomposition and

[2] To be slightly more technical, class field theory provides an isomorphism between quotients of the ideal class group of a number field and the Galois group of an extension of a number field. This isomorphism provides a structural comparison between the ring of integers of a number field and the

inertia groups of a prime ideal in a Galois extension of a number field and see how a field extension can be decomposed into several intermediate extensions over which a prime ideal of the ground field splits in a very predictable fashion. To finish, we discuss the Artin map and the homomorphism it induces between the group of ideals of a number field and the Galois group of an extension. Class field theory tells us that when this extension is the Hilbert class field (for which the Section is named!), the homomorphism is surjective and that the kernel is exactly the subgroup of principal ideals, thus inducing an isomorphism between the ideal class group of the number field and the Galois group of the Hilbert class field.

Mathematical Background

We shall use this section to provide a short list of terminology that will be used throughout the project. Most of the relevant properties of the objects we discuss are assumed.

Group Theory

By *group* we shall mean a set G together with a binary operation $\cdot : G \times G \to G$ such that

(i) if $g, h \in G$ then $g \cdot h \in G$,
(ii) there is an element $e \in G$ with $g \cdot e = e \cdot g = g$ for all $g \in G$, called the identity of G,
(iii) for all $g \in G$ there is an element $g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$ called the inverse of the element g, and
(iv) for all $g, h, i \in G$, we have $g \cdot (h \cdot i) = (g \cdot h) \cdot i$, called associativity.

An *Abelian group*[3] is a group G with the additional property that $g \cdot h = h \cdot g$ for all $g, h \in G$, called *commutativity*.
By *subgroup* we shall mean a subset H of G such that H also forms a group under the same operation as G. The subgroup *generated* by an element of G, which we denote (g), is the smallest subgroup of G containing the element g. Given an element g of G and a subgroup H of G we call the set $gH = \{gh : h \in H\}$ a left coset of H in G, with a corresponding definition for right coset. The left/right cosets of H in G partition G. If $gH = Hg$ for all $g \in G$ then we call H a *normal subgroup* of G and write $H \trianglelefteq G$. In particular, if H is a normal subgroup of G then we may define a group operation $(g_1H)(g_2H) = (g_1 \cdot g_2H)$ on the set of cosets of H in G, which we call the *quotient of* G *by* H and write G/H, read G modulo H.
In most cases the notation will be relative to the objects under consideration. For instance, if $G = \mathbb{Z}$ and $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is addition we shall write $+$ instead of $\cdot$, as one might expect. In the context of multiplication or of function composition we shall often simply use juxtaposition to represent the binary operation (though this convention may occasionally be abandoned in the name of clarity).
An *action* of a group G on a set S is a function $\pi : G \times S \to S$ with

Galois group of the extension, and the Galois correspondence tells us what we need to know about the intermediate extensions. Unfortunately the more general scenario is far beyond the scope of this project and so we restrict ourselves to a discussion of the "easiest" class field.

[3] Named for Niels Henrik Abel, a Norwegian mathematician. Bearing his name is the Abel-Ruffini theorem, the proof that the general quintic is insoluble in radicals.

(i) $\pi(e, s) = s$ for all $s \in S$, where e is the identity of G, and
(ii) $\pi(g_1g_2, s) = \pi(g_1, \pi(g_2, s))$ where $g_1, g_2 \in G$ and $s \in S$.

To give a simple example, we may take for G the group $\mathrm{GL}_n(\mathbb{R})$ of $n \times n$ invertible matrices with coefficients in $\mathbb{R}$ and $S = \mathbb{R}^2$ the set of 2-vectors with coefficients in $\mathbb{R}$. Then $\pi(M, v) = Mv$ is a group action[4].

A *group homomorphism* between two groups G and H is a map $\varphi : G \to H$ with the property that $\varphi(gh) = \varphi(g)\varphi(h)$ for all $g, h \in G$. The usual Bourbaki nomenclature applies when describing such maps, as well as some more subject-specific naming conventions; a bijective group homomorphism is an isomorphism, for instance.

Ring Theory

A *ring* is a set R together with two binary operations, usually written $+ : R \times R \to R$ and $\cdot : R \times R \to R$ (or juxtaposition for the latter) such that

(i) R is an Abelian group under addition,
(ii) $a \cdot (r + s) = a \cdot r + a \cdot s$ for all $a, r, s \in R$, called left-distributivity,
(iii) $(r + s) \cdot a = r \cdot a + s \cdot a$ for all $a, r, s \in R$, called right-distributivity,
(iv) $\cdot$ is associative, and
(v) there is an element $1 \in R$ such that $1 \cdot r = r \cdot 1 = r$ for all $r \in R$, called the mulitplicative identity of R.

A *commutative ring* is a ring in which all elements of R commute with each other under the multiplication of R. If this is the case then properties (ii) and (iii) in the definition coincide (which will always be the case in this project!). A *subring* is, as one might expect, a non-empty subset S of R such that S is a ring with the same addition and multiplication as R.

An *ideal* of R is a non-empty subset $\mathfrak{a}$ of R satisfying the following properties:

(i) if $a, b \in \mathfrak{a}$ then $a - b \in \mathfrak{a}$, that is, $\mathfrak{a}$ is an additive subgroup of R, and
(ii) if $a \in \mathfrak{a}$ and $r \in R$ then $ra \in \mathfrak{a}$.

A similar dichotomy between left and right ideals occurs in the context of non-commutative rings, though this will not be an issue in this project.

An ideal generated by a single element $a \in R$ will be denoted (a) (just as the subgroup generated by an element is denoted (g) in the context of groups) and will be referred to as a *principal ideal*. A ring in which every ideal is principal is called a *principal ideal ring*.

When discussing divisibility of elements we write $a \mid b$ and say "a divides b". By this, we mean that there is an element $r \in R$ such that $b = ra$, as in $\mathbb{Z}$. An element $u \in R$ is called a *unit* of R if there exists an element $v \in R$ such that $uv = 1$; in other words, u has a multiplicative inverse in R. The set of all such elements forms a group called the *group of units* of R and is denoted $R^\times$. An element $\pi \in R$ is called *irreducible* if $\pi = ab$, for some $a, b \in R$, implies that $a \in R^\times$ or $b \in R^\times$. An element $p \in R$ is called *prime* if $p \mid ab$ implies $p \mid a$ or $p \mid b$. In a principal ideal ring, such as $\mathbb{Z}$, these properties coincide, though they are distinct in general.

If $a \in R$ is such that that $a \neq 0$ and there exists a non-zero $b \in R$ such that $ab = 0$, we call a a *zero-divisor*. A ring containing no zero-divisors is called an *integral domain*.

[4] Note that left-actions and right-actions do not coincide in general.

This name combines with principal ideal ring to give *principal ideal domain*, meaning a principal ideal ring which is also an integral domain.
A *unique factorisation domain* is an integral domain in which every element can be written uniquely as a product of irreducible elements of the ring up to ordering and multiplication by units.
A ring R is said to be *Noetherian* if all of its ideals satisfy the ascending chain condition. That is, if $\mathfrak{a}_i \subset R$ are ideals such that there is an infinite ascending chain of ideals

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \dots$$

then for some k we have $\mathfrak{a}_k = \mathfrak{a}_{k+1} = \dots$ for all subsequent ideals in the chain.
By *ring homomorphism* we mean a map $\varphi : R \to S$ such that $\varphi(r+s) = \varphi(r) + \varphi(s)$ and $\varphi(rs) = \varphi(r)\varphi(s)$ for all $r, s \in R$, and such that $\varphi(1_R) = 1_S$. As usual, a ring isomorphism is a ring homomorphism that is bijective.

Modules over a ring

By *left R-module* we shall mean an Abelian group M together an action $\cdot : R \times M \to M$ of the ring R on M with

(i) $r \cdot (m+n) = r \cdot m + r \cdot n$, for all $r \in R$ and $m, n \in M$,
(ii) $(r+s) \cdot m = r \cdot m + s \cdot m$, for all $r, s \in R$ and $m \in M$,
(iii) $(rs) \cdot m = r \cdot (s \cdot m)$ for all $r, s \in R$ and $m \in M$, and
(iv) $1_R \cdot m = m$.

Analogous properties hold for right R-modules. If we take R to be a field then this coincides with the definition of vector space from linear algebra.
An *R-submodule* is a subgroup N of M which is closed under the action of R on N, that is, $rn \in N$ for all $r \in R$ and $n \in N$. In particular, N is a submodule of M if and only if $N \neq \varnothing$ and $n_1 + rn_2 \in N$ for all $r \in R$ and $n_1, n_2 \in N$.
Every ring R is a module over itself, taking the multiplication of R as the R-action. In this case, ideals and submodules coincide. If M is an R-module and N is a submodule of M then we can make the quotient group M/N into an R-module by specifying the R-action $r(m+N) = rm+N$ for all $r \in R$ and $m \in M$ (noting that $m+N$ is an element of M/N).
If M_1, M_2 are R-modules then an R-module homomorphism is a map $\varphi : M_1 \to M_2$ such that $\varphi(m+n) = \varphi(m) + \varphi(n)$ and $\varphi(rm) = r\varphi(m)$ for all $r \in R$ and $m, n \in M_1$. As in the case of rings and groups, an R-module isomorphism is an R-module homomorphism that is bijective.
An R-module M *generated* by the subset A of M is the R-module

$$RA = \left\{ \sum_{i=1}^{m} r_i a_i : r_i \in R,\ a_i \in A \right\}.$$

If $A = \{a_1, \dots, a_n\}$ is some finite subset of M then we write $RA = Ra_1 + \cdots + Ra_n$. A submodule N of M is said to be *finitely generated* if a finite subset of M exists such that $N = Ra_1 + \cdots + Ra_n$. If $N = M$ then M is said to be a *finitely generated* R-module.
The *direct sum* of R-modules M_1 and M_2, written $M_1 \oplus M_2$, is the direct sum of Abelian groups with an R-action defined component-wise. A *free* R-module M is one that is R-module isomorphic to a direct sum of copies of R. The number of copies of R is

called the *rank* of M. If M is a free R-module of rank n then M possesses a basis, say $\{e_1, \ldots, e_n\} \subseteq M$ such that every element $x \in M$ can be written uniquely as

$$x = r_1 e_1 + \cdots + r_n e_n$$

with $r_i \in R$.

1 Fields and Galois Theory

The majority of the focus in this project is on the study of finite degree field extensions of $\mathbb{Q}$ and certain algebraic objects attached to, or contained within, them. As such, it will be useful to first give a short exposition on the theory of fields. In addition, it will be useful to study these extensions via the action of a group of automorphisms on them, which is the objective of Galois theory. Much of the subject matter in this Section is taken from exposition in [6], Chapters 13 and 14.

1.1 Field Theory

By field, we mean a set F together with an addition and a multiplication, such that F is an Abelian group under the addition, and such that $F \setminus \{0\}$ is an Abelian group under the multiplication.

Definition 1.1. *Let F be a field. The smallest positive integer p such that $p \cdot 1 = 0$ is called the **characteristic** of F, denoted $\mathrm{ch}(F)$. If no such integer exists, we say that the field has characteristic 0.*

Since F is a field, we must have that $\mathrm{ch}(F)$ is zero or prime. To see this, suppose that $n = \mathrm{ch}(F)$ but that $n = k\ell$ with $k \neq 1$ and $\ell \neq 1$. Then

$$n = (\underbrace{1 + 1 + \cdots + 1}_{k \text{ times}})(\underbrace{1 + 1 + \cdots + 1}_{\ell \text{ times}}) = 0.$$

But F is a field and this would imply the existence of zero divisors. Hence, either k or ℓ (or both) is 0, or one of k and ℓ is equal to 1, and the other is equal to n, i.e. n is prime. We may define for F the **ring** homomorphism $\varphi : \mathbb{Z} \to F$ by $n \mapsto n \cdot 1$. If $\mathrm{ch}(F) = 0$ then $\ker \varphi = \{0\}$, so that φ is an injection of $\mathbb{Z}$ into F. Since F is a field, this means that F contains a subfield isomorphic to $\mathbb{Q}$. If $\mathrm{ch}(F) = p$ then we have $\ker \varphi = p\mathbb{Z}$, so by the first isomorphism theorem for rings we have $\mathbb{Z}/p\mathbb{Z} \cong \mathrm{Im}\, \varphi \subseteq F$, so that F contains a subfield isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Definition 1.2. *Let F be a field. A **field extension** of F is a field K containing F. We write K/F (read K over F) for the extension K where context requires it. We call F the **ground field** of the extension.*

Since K is itself a field containing F, it is an Abelian group. In addition, there is a multiplication on K by elements of F that is compatible with the addition on K, and so we can make K into an F-vector space by letting F act on K by scalar multiplication.

Definition 1.3. *The **degree** of a field extension K/F, denoted $[K : F]$, is its dimension as an F-vector space. We say K/F is an infinite extension if $[K : F]$ is infinite, and call K/F finite otherwise.*

We shall be most interested in this project in studying finite extensions of $\mathbb{Q}$ and of finite fields by so-called *algebraic elements*.

Definition 1.4. *Let F be a field and $F[X]$ the ring of polynomials with coefficients in F. Let K be an extension of F. An element $\alpha \in K$ is said to be **algebraic** over F if there exists a non-zero polynomial $p(X) \in F[X]$ such that $p(\alpha) = 0$.*

Our first theorem guarantees the existence of a field K in which an irreducible polynomial $p(X) \in F[X]$ has a root. This shall be particularly important for us, since our main study of extensions of $\mathbb{Q}$ shall be through adjoining algebraic numbers.

Theorem 1.1. *Let F be a field and let $p(X) \in F[X]$ be irreducible. Then there is a field $K = F[X]/(p(X))$ containing F and in which $p(X)$ has a root.*

Proof. We use the fact that $F[X]$ is a principal ideal domain to conclude that $(p(X))$ is a maximal ideal in $F[X]$, and hence $F[X]/(p(X))$ is a field, which we call K. Denote by $\pi : F[X] \to K$ the projection sending $f(X)$ to the coset $f(X) + (p(X))$. Then the restriction of π to F gives a homomorphism $\pi|_F$. Since $\pi|_F(1) = 1 + p(X)$ we have that $\pi|_F$ is not identically zero. Thus, $\ker \pi|_F \neq F$, and so we must have that $\ker \pi|_F = \{0\}$, that is, that $\pi|_F$ is an injection, so there is an isomorphic copy of F inside K. We identify F with its image in K so that K is an extension of F. Denote by $\overline{X}$ the image of X under π. Then, since π is a homomorphism, we have $p(\overline{X}) = \overline{p(X)}$. But $\overline{p(X)} = p(X) + (p(X)) = 0 + (p(X))$, and so $p(\overline{X}) = 0$ in K. Hence, K is an extension of F containing a root $\overline{X}$ of $p(X)$. □

It was mentioned earlier that an extension K/F can be made into an F-vector space by letting F act on K by scalar multiplication. Since every vector space has a basis, it will be useful to know how such a basis looks.

Proposition 1.1. *Let F be a field, $p(X) \in F[X]$ a degree n irreducible polynomial, and $K = F[X]/(p(X))$. Denote by α the image of X in K. Then $\{1, \alpha, \dots, \alpha^{n-1}\}$ is a basis for K as an F-vector space. In particular, we have that $[K : F] = n$ and*

$$K \cong F(\alpha) = \{f_0 + f_1\alpha + \cdots + f_{n-1}\alpha^{n-1} : f_i \in F\}.$$

Proof. Without loss of generality, we may assume that $p(X)$ is monic, since F is a field. Write $p(X) = X^n + f_{n-1}X^{n-1} + \cdots + f_1X + f_0$. Since $p(X)$ is irreducible, we have a field $K = F[X]/(p(X))$ containing a root α of $p(X)$, so that

$$\alpha^n + f_{n-1}\alpha^{n-1} + \cdots + f_1\alpha + f_0 = 0$$

in K. Thus, since $\alpha^n = -(f_{n-1}\alpha^{n-1} + \cdots + f_1\alpha + f_0)$, we may reduce any expression in α with exponent higher than n to an expression in α with exponent less than or equal to $n-1$, so certainly $\{1, \dots, \alpha^{n-1}\}$ spans K/F. Now suppose that $\{1, \dots, \alpha^{n-1}\}$ is not a linearly independent set, so that there exist $a_0, \dots, a_{n-1} \in F$, not all zero, such that

$$a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Then we have

$$a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \equiv 0 \mod p(X),$$

or equivalently that $p(X)$ divides $a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. But $\deg p(X) = n > n-1$ and such a_i cannot exist unless $a_i = 0$ for all i.

To show that $K \cong F(\alpha)$, we note that there is a natural homomorphism $\varphi : F[X] \to F(\alpha)$ with $X \mapsto \alpha$ which is clearly surjective, and whose kernel is the ideal generated by the monic irreducible polynomial $p(X)$. By the first isomorphism theorem, we have

$$F[X]/(p(X)) \cong F(\alpha).$$

□

We shall call a field $K = F(\alpha)$ generated over another field F by a single algebraic element α a *simple extension*.

Definition 1.5. *Let F be a field and let $K = F(\alpha)$ where α is algebraic over F. The **minimal polynomial** of α over F, denoted $m_{\alpha,F}(X) \in F[X]$ is the unique monic irreducible polynomial of smallest degree over F satisfied by α. We refer to the degree of $m_{\alpha,F}(X)$ as the degree of α over F.*

Context permitting, we shall refer to $m_{\alpha,F}(X)$ simply as $m(X)$. In fact, it is not obvious that such a polynomial exists, though we shall show that it does exist. Suppose $m(X) \in F[X]$ is a monic polynomial of smallest degree satisfied by $\alpha \in K$ and suppose there exist non-constant $f(X), g(X) \in F[X]$ such that $m(X) = f(X)g(X)$. Then $\deg f$ and $\deg g$ are both smaller than $\deg m$, and $f(\alpha)g(\alpha) = 0$ in K. But since K is a field we must then have $f(\alpha) = 0$ or $g(\alpha) = 0$, contradicting the minimality of $m(X)$. Suppose now that there exists a polynomial $f(X) \in F[X]$ such that $f(\alpha) = 0$. By the Euclidean algorithm, we have

$$f(X) = q(X)m(X) + r(X), \ \ \deg r(X) < \deg m(X).$$

Since $f(\alpha) = 0$, this forces $r(\alpha) = 0$, and so $m(X) \mid f(X)$. Thus, given any other irreducible polynomial $p(X) \in F[X]$ satisfied by α we have $p(X) = km(X)$ where $k \in F$, and so $m(X)$ is the unique monic irreducible polynomial satisfied by α.

Example 1.1. *Examples of field extensions that will feature frequently throughout the project are so-called quadratic extensions, that is, extensions of degree 2. In particular, we let $F = \mathbb{Q}$ and fix a square-free $d \in \mathbb{Z}$. The polynomial $X^2 - d \in \mathbb{Q}[X]$ is Eisenstein with any prime p dividing d, and so the quotient $\mathbb{Q}[X]/(X^2 - d)$ is a field $K = \mathbb{Q}(\sqrt{d})$ containing $\mathbb{Q}$ such that $X^2 - d$ has a root.*

An element of $\mathbb{C}$ that is algebraic over $\mathbb{Q}$ is called an *algebraic number*. The title *algebraic number theory* may thus be interpreted both as the algebraic theory of numbers, and as the theory of algebraic numbers.
A particularly useful property of field extensions is the multiplicativity of their degrees, which we shall prove in the following theorem.

Theorem 1.2. *Let $L/K/F$ be a tower of extensions. Then $[L : F] = [L : K][K : F]$.*

Proof. Let $[L : K] = m$ and $[K : F] = n$ and let $\{\alpha_1, \dots, \alpha_m\}$ and $\{\beta_1, \dots, \beta_n\}$ be bases for L/K and K/F respectively. Let $\ell \in L$. Then

$$\ell = \sum_{i=1}^{m} k_i \alpha_i$$

with the $k_i \in K$. In addition, for any of the k_i we have

$$k_i = \sum_{j=1}^{n} f_{ij} \beta_j$$

for some $f_{ij} \in F$. Hence, we have

$$\ell = \sum_{i=1}^{m} \sum_{j=1}^{n} f_{ij} \alpha_i \beta_j.$$

Thus, every element of L can be written as a linear combination of elements of the set $\{\alpha_1\beta_1, \dots, \alpha_i\beta_j, \dots, \alpha_m\beta_n\}$ and so these span L as an F-vector space.
Suppose now that there is some linear dependence in this set. Then, defining the k_i as above, we would have

$$\ell = \sum_{i=1}^{m} k_i\alpha_i = 0$$

and so all of the k_i must be 0 since the α_i are a basis for L over K. Thus, this induces a linear dependence

$$k_i = \sum_{j=1}^{n} f_{ij}\beta_j = 0.$$

But the β_j are a basis for K over F, and so this forces $f_{ij} = 0$ for all i and j, and so $\{\alpha_1\beta_1, \dots, \alpha_i\beta_j, \dots, \alpha_m\beta_n\}$ is a basis for L as an F-vector space.
In conclusion, we have that $[L : F] = nm = [L : K][K : F]$ as desired. □

An interesting corollary of Theorem 1.2 is the lack of intermediate extensions between extensions of prime degree. For instance, since $\mathbb{Q}(\sqrt{2})$ has degree 2 over $\mathbb{Q}$, we may conclude that there are no extensions of $\mathbb{Q}$ lying between $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}$. Furthermore, Theorem 1.2 tells us that the only extensions lying between fields L and F are those whose degree divides $[L : F]$.
Since we know that for any irreducible polynomial $p(X) \in F[X]$ there is an extension of F containing a root of K, we may ask the question whether there exists an extension E of F containing all of the roots of $p(X)$.

Definition 1.6. *Let F be a field and let $p(X) \in F[X]$ be irreducible. An extension E of F is called a **splitting field** for $p(X)$ if $p(X)$ splits completely into linear factors in E, and in any proper subfield of E, $p(X)$ does not split.*

Since $F[X]$ is a principal ideal domain, it is a unique factorisation domain. If a polynomial $p(X)$ has a root α_1 then $X - \alpha_1 \mid p(X)$, and since linear factors are irreducible we may conclude that a polynomial of degree n has at most n roots (counted with multiplicity). Thus, if E is a splitting field for an irreducible polynomial of degree n then that polynomial has exactly n roots in E.

Theorem 1.3. *Let F be a field and let $p(X) \in F[X]$ be an irreducible polynomial of degree n. Then there exists an extension E over F which is a splitting field for $p(X)$. Furthermore, $[E : F] \leq n!$.*

Proof. We proceed by induction on the degree of $p(X)$. If $n = 1$ then $p(X)$ is linear and so a root for $p(X)$ lies in the ground field F, so we may assume that $n > 1$. By Theorem 1.1, we know that there exists an extension K_1 over F that contains a root of $p(X)$. The extension K_1 contains at least one root of $p(X)$, say α_1, so that $p(X) = (X-\alpha_1)f_1(X)$ in $K_1[X]$ with $\deg f_1 \leq n - 1$, so that $[K_1 : F] \leq n$. Thus, by induction, we may construct a tower of field extensions $F \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n = E$ such that in each intermediate extension we have the factorisation $p(X) = (X - \alpha_1)\cdots(X - \alpha_i)f_i(X)$ with $\deg f_i \leq n - i$ and $[K_i : F] \leq n(n - 1)\cdots(n - i + 1)$. Thus, in the final extension K_n we have

$$p(X) = \prod_{i=1}^{n}(X - \alpha_i).$$

By multiplicativity of degrees, we have $[E : F] \leq n!$. Equality occurs if and only if every root is distinct and the factor $f_i(X)$ is irreducible at every stage. $\square$

Consider the polynomial $p(X) = X^3 - 2$. Then $p(X)$ is irreducible by Eisenstein's criterion with prime 2, and so $\mathbb{Q}[X]/(p(X))$ is a field containing a root of $p(X)$. We know that $\alpha_1 = \sqrt[3]{2}$ is a root of $p(X)$ so we might write $K_1 = \mathbb{Q}(\alpha_1)$. Of course, we also have the roots $\alpha_2 = j\sqrt[3]{2}$ and $\alpha_3 = j^2\sqrt[3]{2}$ where $j \neq 1$ is a complex number such that $j^3 = 1$. Notice that every element of K_1 is a real number, and so $\alpha_2, \alpha_3 \notin K_1$. The problem is that the fields K_1, $\mathbb{Q}(\alpha_2)$, and $\mathbb{Q}(\alpha_3)$ are isomorphic and so α_1, α_2, and α_3 are what we refer to as *algebraically indistinguishable*. We shall show that this is always the case for distinct roots of an irreducible polynomial.

Proposition 1.2. *Let F_1 and F_2 be fields and let $p_1(X) \in F_1[X]$. Suppose there is an isomorphism $\varphi : F_1 \to F_2$ of fields. Then φ induces a ring isomorphism $\widetilde{\varphi} : F_1[X] \to F_2[X]$ and hence if $K_1 = F_1(\alpha)$ is an extension of F_1 containing the root α_1 of $p_1(X)$ then there is an extension $K_2 = F_2(\beta)$, such that β is a root of the polynomial $p_2(X) \in F_2[X]$, obtained by applying $\widetilde{\varphi}$ to $p_1(X)$ and such that $K_1 \cong K_2$.*

Proof. Let $\varphi : F_1 \to F_2$ be an isomorphism of fields and write

$$p_1(X) = X^n + f_{n-1}X^{n-1} + \cdots + f_1X + f_0 \in F_1[X].$$

Applying φ to $p_1(X)$ requires us to specify the image of X under φ. Indeed, since φ is a homomorphism, this gives

$$p_2(X) = \varphi(X)^n + \varphi(f_{n-1})\varphi(X)^{n-1} + \cdots + \varphi(f_1)\varphi(X) + \varphi(f_0).$$

Thus if we specify that $X \mapsto X$ under φ we have an isomorphism of rings $\widetilde{\varphi} : F_1[X] \to F_2[X]$.

If $p_1(X)$ is irreducible in F_1 then the ideal $(p_1(X))$ is a maximal ideal. We wish to show that $(p_2(X)) = (\widetilde{\varphi}(p_1(X)))$ is a maximal ideal by showing that the image of $p_1(X)$ under $\widetilde{\varphi}$ is an irreducible polynomial. Suppose $p_2(X)$ is reducible. Then

$$p_2(X) = a(X)b(X)$$

for some non-constant $a(X), b(X) \in F_2[X]$. Since $p_2(X) = \widetilde{\varphi}(p_1(X))$ we have

$$\widetilde{\varphi}(p_1(X)) = a(X)b(X) \iff p_1(X) = \widetilde{\varphi}^{-1}(a(X))\widetilde{\varphi}^{-1}(b(X))$$

and so $p_1(X)$ is reducible. By contraposition, if $p_1(X)$ is irreducible, then $p_2(X)$ is irreducible. Thus $(p_2(X))$ is a maximal ideal in $F_2[X]$. Thus, we have a commutative diagram

$$\begin{tikzcd}
F_1(\alpha) \arrow[r, "\widetilde{\psi}"] & F_2(\beta) \\
F_1[X] \arrow[u, "\pi_1"] \arrow[r, "\widetilde{\varphi}"] & F_2[X] \arrow[u, "\pi_2"]
\end{tikzcd}$$

where we have used Proposition 1.1 to write $F_1(\alpha) = F_1[X]/(p_1(X))$ and $F_2(\beta) = F_2[X]/(p_2(X))$. Thus in the diagram we have the canonical projections π_1, π_2, and an isomorphism $\widetilde{\psi}$ with $\widetilde{\psi}(\alpha) = \beta$ (noting that, since $F_1(\alpha)$ is generated over F_1 by α, the image of α under $\widetilde{\psi}$ determines the map completely). $\square$

We shall be interested in several corollaries of the above proposition. First, we note that, in the notation of Proposition 1.2, taking φ to be the identity gives an isomorphism $\widetilde{\psi}$ between any two fields generated by roots of the polynomial $p_1(X)$, resolving the problem we had with $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$, and $\mathbb{Q}(j^2\sqrt[3]{2})$. Furthermore, combining Proposition 1.2 with Theorem 1.3 tells us that any two splitting fields for an irreducible polynomial are isomorphic.

To conclude this section, we introduce two properties of field extensions that will be particularly useful for us.

Definition 1.7. *Let F be a field and let N be an extension of F with the property that every irreducible polynomial with a root in N splits completely into linear factors over N. Such an extension is called a **normal** extension of F.*

Example 1.2. *Let $N = \mathbb{Q}(\sqrt{2})$. Then N is normal over $\mathbb{Q}$ since the minimal polynomial of $\sqrt{2}$ is $m(X) = X^2 - 2$ and the two roots of $m(X)$ are $\pm\sqrt{2}$, both of which lie in N. An example of an extension of $\mathbb{Q}$ that is not normal is $\mathbb{Q}(\sqrt[3]{2})$; the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $X^3 - 2$, but we saw earlier that the other two roots, $j\sqrt[3]{2}$ and $j^2\sqrt[3]{2}$, were not elements of $\mathbb{Q}(\sqrt[3]{2})$ and so $\mathbb{Q}(\sqrt[3]{2})$ is not normal over $\mathbb{Q}$.*

Definition 1.8. *Let F be a field and let $p(X) \in F[X]$ be irreducible. We say that $p(X)$ is **separable** if $p(X)$ has no multiple roots. An extension K of F is said to be a **separable extension** if the minimal polynomial over F of every element of K is separable, and the extension is called **inseparable** otherwise.*

Our final theorem, from [14], will tell us when an extension is separable. Until now the results we have quoted have been general, in the sense that they did not depend on the characteristic of the fields discussed.

Theorem 1.4. *Let F be a field and let K be an extension of F. If $\mathrm{ch}(K) = 0$ then every irreducible polynomial in $F[X]$ is separable over K. If $\mathrm{ch}(K) = p$ then a polynomial $f(X) \in F[X]$ is separable over K if and only if $f(X)$ is not a polynomial in X^p.*

Proof. Let $f(X) \in F[X]$ be irreducible. We first prove that $f(X)$ is separable if and only if it is coprime to its derivative. Suppose that $f(X)$ is separable. Then there is some $\alpha \in K$ such that $f(X) = (X - \alpha)g(X)$ with $(X - \alpha) \nmid g(X)$. By the chain rule of differentiation, we have

$$f'(X) = g(X) + (X - \alpha)g'(X).$$

Since $f'(\alpha) = g(\alpha) \neq 0$, we have that $f(X)$ and $f'(X)$ have no common roots, and so they are coprime in $K[X]$. Suppose now that $f(X)$ is inseparable. Without loss of generality, we suppose that there is an $\alpha \in K$ with $f(X) = (X - \alpha)^2 g(X)$ such that $(X - \alpha) \nmid g(X)$. Then

$$f'(X) = 2(X - \alpha)g(X) + (X - \alpha)^2 g'(X).$$

Since $f(\alpha) = f'(\alpha) = 0$, the root α is common to $f(X)$ and $f'(X)$, and so $f(X)$ and $f'(X)$ are not coprime. By contraposition, we have that if $f(X)$ and $f'(X)$ are coprime, then $f(X)$ is separable.

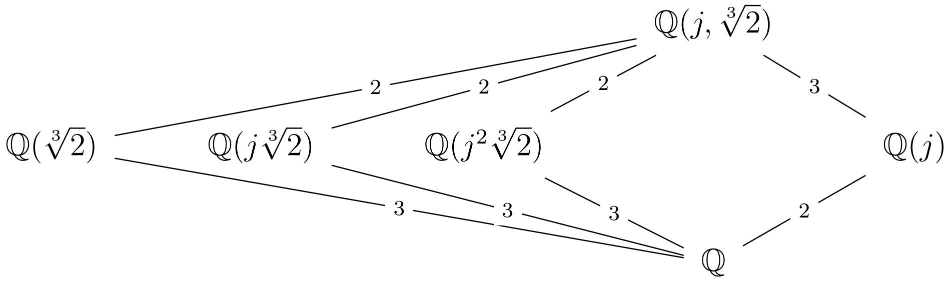
Now, suppose $f(X)$ is an inseparable irreducible polynomial in $F[X]$. Then, from above, we have that $f(X)$ and $f'(X)$ are not coprime. Since $f(X)$ is irreducible, we must have $f(X) \mid f'(X)$, but $\deg f' < \deg f$, and so this forces $f'(X) = 0$. On the other hand, if $f'(X) = 0$ then the greatest common divisor of $f(X)$ and $f'(X)$ is $f(X)$, and so $f(X)$ is separable by the previous argument. In both cases, contraposition gives us that $f(X)$ is separable if and only if $f'(X) \neq 0$.

Finally, in a field of characteristic 0, a non-constant polynomial always has non-zero derivative, and so every non-constant irreducible polynomial is separable. In a field of characteristic p, a non-constant polynomial has non-zero derivative if and only if it is not a polynomial in X^p, since if this were the case then every term of the derivative would be divisible by p, and thus equal to 0. □

Example 1.3. *The procedure discussed above to construct splitting fields requires one simply to successively adjoin roots of an irreducible polynomial to a field until a field E is reached in which the given polynomial splits into linear factors. We shall do this with the polynomial $m(X) = X^3 - 2$ over $\mathbb{Q}$ and analyse the extensions we obtain.*

By Eisenstein's criterion with prime 2 we have that $m(X)$ is irreducible over $\mathbb{Q}$. We know that $\sqrt[3]{2}$ is a root of $m(X)$ so we adjoin this to $\mathbb{Q}$ to obtain $K_1 = \mathbb{Q}(\sqrt[3]{2})$ and note that $[K_1 : \mathbb{Q}] = 3$. By Theorem 1.3 we know that $[E : \mathbb{Q}] \leq 3!$ and by Theorem 1.2 we know that the degree of any further extension of K_1 must be 2. Indeed, if we factor $X^3 - 2$ over $\mathbb{Q}(\sqrt[3]{2})$ we have $m(X) = (X - \sqrt[3]{2})(X^2 + X\sqrt[3]{2} + \sqrt[3]{4})$. Set $m_1(X) := X^2 + X\sqrt[3]{2} + \sqrt[3]{4}$ and notice that the discriminant of $m_1(X)$ is $\sqrt[3]{4} - 4\sqrt[3]{4} < 0$ so $m_1(X)$ has a pair of conjugate complex roots. Since $K_1 \subset \mathbb{R}$, we know that no such root can lie in K_1. Now, we know that $j\sqrt[3]{2}$ is a root of $m(X)$, and so since $(j\sqrt[3]{2})^2 + (j\sqrt[3]{2})\sqrt[3]{2} + \sqrt[3]{4} = 0$, we have the extension $E = \mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2})$, which has degree 2 over K_1 and hence degree 6 over $\mathbb{Q}$, and is thus a splitting field of $m(X)$ over $\mathbb{Q}$. Clearly $E \subseteq \mathbb{Q}(j, \sqrt[3]{2})$, and since $\frac{j\sqrt[3]{2}}{\sqrt[3]{2}} = j \in E$, we also have $\mathbb{Q}(j, \sqrt[3]{2}) \subseteq E$, and so we conclude finally that $E = \mathbb{Q}(j, \sqrt[3]{2})$ is the splitting field for $m(X)$.

We can now look at the intermediate extensions between $\mathbb{Q}$ and E, which are summarised in the following diagram of subfields:


$\mathbb{Q}(j, \sqrt[3]{2})$
2
2
2
3
$\mathbb{Q}(\sqrt[3]{2})$
$\mathbb{Q}(j\sqrt[3]{2})$
$\mathbb{Q}(j^2\sqrt[3]{2})$
$\mathbb{Q}(j)$
3
3
3
2
$\mathbb{Q}$

where the numbers between each extension denote the degree of the extension. Each of the extensions of degree 3 over $\mathbb{Q}$ is not normal, as we discussed above. The degree 2 extension is normal, since the minimal polynomial of j over $\mathbb{Q}$ is $X^2 + X + 1$ and the roots of this polynomial are j and $j^2 = -(j + 1)$, both of which lie in $\mathbb{Q}(j)$. The multiplicativity of degrees discussed in Theorem 1.2 gives us a basis for $\mathbb{Q}(j, \sqrt[3]{2})$ as a $\mathbb{Q}$-vector space; namely, $\{1, \sqrt[3]{2}, \sqrt[3]{4}, j, j\sqrt[3]{2}, j\sqrt[3]{4}\}$, which we obtained simply by taking bases for $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(j)$ over $\mathbb{Q}$ and taking products of their elements (which was the entire premise of Theorem 1.2).

1.2 Galois Theory

The main objective of Galois theory is to establish a correspondence between field extensions and certain groups of automorphisms attached to these extensions. In later

Sections, we shall see that this correspondence allows us to easily study the behaviour of prime ideals in special subrings of extensions of $\mathbb{Q}$, as well as being generally useful in studying towers of extensions. We begin by introducing the automorphisms of interest.

Definition 1.9. *Let F be a field and let K, K' be extensions of F. A field homomorphism $\sigma : K \to K'$ that fixes the ground field F point-wise is called an F-**homomorphism**.*

The usual variants of homomorphism apply in this case, for instance, we shall be mainly interested in studying F-*automorphisms* of an extension K of F. We denote by $\mathrm{Aut}(K/F)$ the group of F-automorphisms of K and note that this is a subgroup of the group $\mathrm{Aut}(K)$ of *all* automorphisms of K; clearly $\mathrm{id} \in \mathrm{Aut}(K/F)$ so it is non-empty, and if $\sigma, \tau \in \mathrm{Aut}(K/F)$ then since $\sigma(F) = \tau(F) = F$ we have $\tau^{-1} \circ \sigma(F) = F$, so that $\tau^{-1} \circ \sigma \in \mathrm{Aut}(K/F)$.

Definition 1.10. *Let $H \leq \mathrm{Aut}(K/F)$. The field $K^H := \{x \in K : \sigma(x) = x$ for all $\sigma \in H\}$ is called the **fixed field** of H.*

As an example, we have the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ and a $\mathbb{Q}$-automorphism σ such that $\sqrt{2} \mapsto \sqrt{2}$ and $\sqrt{3} \mapsto -\sqrt{3}$. Notice that $\sigma^2 = \mathrm{id}$ so we have a subgroup

$$H_1 = \{\mathrm{id}, \sigma\} \leq \mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}).$$

Since $\sqrt{2}$ is fixed by every element of H_1, we have $K^{H_1} = \mathbb{Q}(\sqrt{2})$. Similarly, we have a $\mathbb{Q}$-automorphism τ with $\sqrt{2} \mapsto -\sqrt{2}$ and $\sqrt{3} \mapsto \sqrt{3}$ so that $H_2 = \{1, \tau\} \leq \mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ and a $\mathbb{Q}$-automorphism $\sigma\tau$ sending both roots to their negatives and so that there is a subgroup $H_3 = \{1, \sigma\tau\} \leq \mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$. We have $K^{H_2} = \mathbb{Q}(\sqrt{3})$ and $K^{H_3} = \mathbb{Q}(\sqrt{6})$, and hence a lattice of subgroups

$$\begin{tikzcd}
& \{\mathrm{id}\} \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
H_1 \arrow[dr, dash, "2"'] & H_2 \arrow[d, dash, "2"] & H_3 . \arrow[dl, dash, "2"] \\
& \mathrm{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) &
\end{tikzcd}$$

Compare this with the diagram:

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash, "2"] & \mathbb{Q}(\sqrt{6}) . \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

Both diagrams are exceptionally similar, with the only difference being that the inclusions are reversed (that is, in the lattice of subgroups we have a "large" group at the bottom of the diagram and a "small" group at the top of the diagram, while the opposite is true of the fields in the lattice of subfields). This is easy to see; let $K^{H_1} \subset K^{H_2}$ be the respective fixed fields of the groups H_1 and H_2. Any element $\sigma \in H_2$ also fixes all of K^{H_1}, so that $\sigma \in H_1$, while the reverse is not true, and hence $H_2 \leq H_1$. Conversely, if $H_2 \leq H_1$ have respective fixed fields K^{H_2} and K^{H_1} and if $k \in K^{H_1}$ then for any $\sigma \in H_1$ we have $\sigma(k) = k$, and since $H_2 \leq H_1$, the same holds for any $\sigma' \in H_2$, so that $k \in K^{H_2}$, and hence $K^{H_1} \subset K^{H_2}$.

Proposition 1.3. *Let F be a field and let E be a splitting field of an irreducible polynomial $p(X) \in F[X]$. Then the F-automorphisms of E permute the roots of $p(X)$. In particular, we have*

$$|\mathrm{Aut}(E/F)| \leq [E : F]$$

with equality if and only if E is separable over F.

Proof. Suppose $\alpha \in E$ is a root of $p(X)$. Then

$$p(\alpha) = \alpha^n + f_{n-1}\alpha^{n-1} + \cdots + f_1\alpha + f_0 = 0.$$

Since any $\sigma \in \mathrm{Aut}(E/F)$ is an F-automorphism, we have

$$\begin{aligned}\sigma(p(\alpha)) &= \sigma(\alpha^n + f_{n-1}\alpha^{n-1} + \cdots + f_1\alpha + f_0)\\ &= \sigma(\alpha)^n + f_{n-1}\sigma(\alpha)^{n-1} + \cdots + f_1\sigma(\alpha) + f_0\\ &= 0\end{aligned}$$

so that $\sigma(\alpha)$ is another root of $p(X)$ in E. This means that any F-automorphism of E must send a root of an irreducible polynomial over F to another root, and so it follows that the number of F-automorphisms of E is exactly the number of distinct roots of $p(X)$. Thus, we have $|\mathrm{Aut}(E/F)| \leq [E : F]$. If $p(X)$ is separable then $[E : F] = \deg p = |\mathrm{Aut}(E/F)|$. □

Definition 1.11. *Let F be a field and K a finite extension of F. We say that K is **Galois** over F if $|\mathrm{Aut}(K/F)| = [K : F]$. In this case, we write $\mathrm{Gal}(K/F) := \mathrm{Aut}(K/F)$ and call this the **Galois group** of K/F.*

We now quote the main theorem of Galois theory, whose proof can be found in [6, p.554]. This will provide us with a dictionary between subgroups of Galois groups and intermediate field extensions, as was described at the start of the section.

Theorem 1.5. *Let F be a field and let K be a Galois extension of F. Let $\mathcal{E}$ be the set of subfields of K containing F and let $\mathcal{G}$ be the set of subgroups of $\mathrm{Gal}(K/F)$. Then,*

(i) there is a bijection $\varphi : \mathcal{E} \to \mathcal{G}$, which is decreasing for the inclusion relation, sending $E \in \mathcal{E}$ to the element $H \in \mathcal{G}$ that fixes E, while $\varphi^{-1} : \mathcal{G} \to \mathcal{E}$ sends an element $H \in \mathcal{G}$ to the subfield K^H of K fixed by H,

(ii) $[K : E] = |H|$ and $[E : F] = [\mathrm{Gal}(K/F) : H]$,

(iii) K/E is always a Galois extension with $\mathrm{Gal}(K/E) = H$,

(iv) E/F is Galois if and only if $H \trianglelefteq \mathrm{Gal}(K/F)$, in which case

$$\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\,\mathrm{Gal}(K/E),$$

(v) if E/F is not Galois then $\mathrm{Gal}(K/E) \ntrianglelefteq \mathrm{Gal}(K/F)$ by the previous property, but even in this case we have $\mathrm{Aut}(E/F)$ equal to the coset space $\mathrm{Gal}(K/F)/\,\mathrm{Gal}(K/E)$.

Proof. Found in [6, p.554, 555, 556]. □

1.2.1 Galois Theory of Finite Fields

Since in Theorem 1.5 we didn't specify the characteristic of the fields under examination, the results also hold for finite fields, and so there is a Galois theory of finite fields. Fortunately, the Galois groups of finite fields are especially easy to describe.

Proposition 1.4. *Let* $m(X) \in \mathbb{F}_p[X]$ *be irreducible and suppose* $\deg m(X) = n$*. Then* $\mathbb{F}_p[X]/(m(X)) \cong \mathbb{F}_{p^n}$ *so that* $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$*.*

Proof. Since $\deg m(X) = n$, every element of the quotient is represented by a polynomial of degree less than or equal to $n-1$. Thus, we have

$$a_0 + a_1X + \cdots + a_{n-1}X^{n-1},\ a_i \in \mathbb{F}_p.$$

Since each coefficient is equal to one of the p elements of $\{0, \ldots, p-1\}$ and there are p such coefficients, the number of elements in the quotient is p^n. For the same reason that we discussed in Proposition 1.1, we have that $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Finally, this is a field because $m(X)$ is irreducible, so that $(m(X))$ is a maximal ideal in $\mathbb{F}_p[X]$. □

Proposition 1.5. *Let* $p \in \mathbb{Z}$ *be prime and denote by* $\mathbb{F}_{p^n}$ *a finite field of order* p^n*. Then* $\mathbb{F}_{p^n}$ *is the splitting field of* $X^{p^n} - X \in \mathbb{F}_p[X]$*.*

Proof. By Fermat's Little Theorem from elementary number theory, we have

$$a^p \equiv a \bmod p$$

for all $X \in \mathbb{Z}$, which is equivalent to $a^p - a = 0$ in $\mathbb{F}_p$. Since $\mathbb{F}_{p^n}$ is a field of characteristic p, this also holds in $\mathbb{F}_{p^n}$ and so $a^{p^n} = (a^{p^{n-1}})^p \equiv a \bmod p$ for all $a \in \mathbb{Z}$, and equivalently $a^{p^n} - a = 0$ for every element of $\mathbb{F}_{p^n}$. Hence $X^{p^n} - X$ splits completely into linear factors over $\mathbb{F}_{p^n}$. □

Since $\mathbb{F}_{p^n}$ is the splitting field for $X^{p^n} - X \in \mathbb{F}_p[X]$, it is a Galois extension, and so $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = n$. In addition, we have a field homomorphism[5]

$$\sigma : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$$

with $\sigma(a) = a^p$. Successively applying σ gives us $\sigma \circ \sigma(a) = (a^p)^p = a^{p^2}$ and so on. Since $a^{p^n} = a$, we have that σ has order n in $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ and so $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/(n)$, after observing that $a^{p^k} = a$ for all $a \in \mathbb{F}_{p^n}$ cannot occur for any $k < n$, since $a^{p^k} - a = 0$ has only $p^k < p^n$ solutions. This automorphism is called the *Frobenius automorphism* and is denoted Frob_p.
We shall use these results in Section 5 to discuss the splitting properties of prime ideals in Galois extensions of certain fields.

2 Number Fields

The majority of the project will be spent studying the arithmetic of so-called *number fields*. We shall spend the first two Sections studying the structure of number fields and their rings of integers, with the aim of applying the theory to the proof of Fermat's last theorem for regular primes. With this in mind, a good place to begin would be in developing a definition of *number field*.

[5] It is perhaps non-obvious that this is a homomorphism until one considers that p is prime and so by the so-called "Freshman's dream" the map is additive. Multiplicativity is obvious.

2.1 Number Fields

In this section we begin by defining number fields, and then introduce some useful numerical invariants.

Definition 2.1. *A **number field** is an extension of $\mathbb{Q}$ obtained by adjoining finitely many algebraic numbers to $\mathbb{Q}$.*

As discussed in Section 1, quadratic number fields[6] are particularly simple examples of number fields obtained by adjoining the square root of a square-free integer to $\mathbb{Q}$. In general, one might be interested in how a field K embeds into an algebraically closed field. In this case, we study how number fields embed into $\mathbb{C}$.

Proposition 2.1. *Let K be a number field of degree n over $\mathbb{Q}$ and, using the primitive element theorem, let $\alpha \in \mathbb{C}$ be an algebraic number such that $K = \mathbb{Q}(\alpha)$. Let $p(X) \in \mathbb{Q}[X]$ be the minimal polynomial of α over $\mathbb{Q}$ and let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be the conjugates of α. Then there are exactly n distinct field homomorphisms $\sigma_k : K \hookrightarrow \mathbb{C}$ such that $\sigma_k(\alpha) = \alpha_k$.*

Proof. By Proposition 1.2 from Section 1, each of the embeddings σ_k induces an isomorphism $\sigma_k : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha_k)$. Since there are exactly n conjugates of α, this proves the proposition. □

Each of the σ_k is referred to as a *complex embedding* of K into $\mathbb{C}$, and if the image of K under σ_k is contained in $\mathbb{R}$ then we refer to σ_k as a *real embedding* of K into $\mathbb{R}$. The fields $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\alpha_k)$ are referred to as *conjugate fields*.

Definition 2.2. *Let K be a number field of degree n over $\mathbb{Q}$ such that $K = \mathbb{Q}(\alpha)$ for some algebraic number $\alpha \in \mathbb{C}$. Let $\sigma_k : K \hookrightarrow \mathbb{C}$ be the n distinct embeddings of K into $\mathbb{C}$. The **discriminant** of a set of elements $\theta_1, \ldots, \theta_n \in K$ is the number*

$$d(\theta_1, \ldots, \theta_n) := \begin{vmatrix} \sigma_1(\theta_1) & \sigma_2(\theta_1) & \cdots & \sigma_n(\theta_1) \\ \sigma_1(\theta_2) & \sigma_2(\theta_2) & \cdots & \sigma_n(\theta_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\theta_n) & \sigma_2(\theta_n) & \cdots & \sigma_n(\theta_n) \end{vmatrix}^2 .$$

Example 2.1. *Let $K = \mathbb{Q}(\sqrt{2})$ and consider the set $\{1, \sqrt{2}\}$. We have two embeddings of K into $\mathbb{C}$, namely $\mathrm{id} : \sqrt{2} \mapsto \sqrt{2}$, and $\sigma : \sqrt{2} \mapsto -\sqrt{2}$. Thus, the discriminant of the set $\{1, \sqrt{2}\}$ is*

$$d(1, \sqrt{2}) = \begin{vmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{vmatrix}^2 = 8.$$

The main reason for introducing discriminants will become clear in Section 2.2 when we introduce *integral bases*.

Definition 2.3. *Let K be a number field of degree n over $\mathbb{Q}$, let $\theta \in K$, and let $\sigma_k : K \hookrightarrow \mathbb{C}$ be the n distinct embeddings of K into $\mathbb{C}$. The **norm** of θ is the product*

$$N_{K/\mathbb{Q}}(\theta) = \prod_{k=1}^{n} \sigma_k(\theta).$$

[6] We will often refer to these simply as quadratic fields, though in general a quadratic field is simply an extension of degree 2 over the relevant ground field.

If $K/\mathbb{Q}$ is Galois then this coincides with

$$N_{K/\mathbb{Q}}(\theta) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(\theta),$$

though in general a number field is not always a normal extension of $\mathbb{Q}$. Take, for example, the number field $K = \mathbb{Q}(\sqrt[3]{2})$. Then K is not a normal extension of $\mathbb{Q}$, and in fact there are no non-trivial $\mathbb{Q}$-automorphisms of K, so that $\mathrm{Aut}(K/\mathbb{Q}) = \{\mathrm{id}\}$. There are, however, three embeddings of K into $\mathbb{C}$; one real embedding and two complex embeddings. Thus, the norm of the element $\sqrt[3]{2}$ is

$$N_{K/\mathbb{Q}}(\sqrt[3]{2}) = (\sqrt[3]{2}) \times (j\sqrt[3]{2}) \times (j^2\sqrt[3]{2}) = 2$$

where j is a primitive cube root of unity.
Another observation to make is that any embedding of a number field into $\mathbb{C}$ fixes $\mathbb{Q}$, and so $N_{K/\mathbb{Q}}(a) = a^n$ if $a \in \mathbb{Q}$.

Definition 2.4. *Let K be a number field of degree n over $\mathbb{Q}$, let $\theta \in K$, and let $\sigma_k : K \hookrightarrow \mathbb{C}$ be the n distinct embeddings of K into $\mathbb{C}$. The **trace** of θ is the sum*

$$\mathrm{tr}_{K/\mathbb{Q}}(\theta) = \sum_{k=1}^{n} \sigma_k(\theta).$$

In the same way that $N_{K/\mathbb{Q}}(\theta)$ is a product running over the elements of $\mathrm{Gal}(K/\mathbb{Q})$ when K is Galois, so too is $\mathrm{tr}_{K/\mathbb{Q}}(\theta)$ a sum over the elements of $\mathrm{Gal}(K/\mathbb{Q})$ when K is Galois. Interestingly, the norm and trace of an element give elements of $\mathbb{Q}$. To see this, note that $N_{K/\mathbb{Q}}(\theta)$ is a product running over *all* possible embeddings of K into $\mathbb{C}$, and so the image of $N_{K/\mathbb{Q}}(\theta)$ under such an embedding must be $N_{K/\mathbb{Q}}(\theta)$, that is, $N_{K/\mathbb{Q}}(\theta)$ is fixed by an embedding, and so must lie in $\mathbb{Q}$. An identical argument applies to $\mathrm{tr}_{K/\mathbb{Q}}(\theta)$, replacing every instance of the word “product” with “sum”.

2.2 Rings of Integers

In the same way that $\mathbb{Z}$ is an interesting subring of $\mathbb{Q}$, in a more general number field we are interested in the collections of *integral elements* over subrings of the field.

Definition 2.5. *Let K be a field and let R be an integral domain contained in K. An element $k \in K$ is said to be **integral** over R if there exist $r_i \in R$ such that*

$$k^n + r_{n-1}k^{n-1} + \cdots + r_1 k + r_0 = 0.$$

*The collection of elements of K that are integral over R is called the **integral closure** of R in K.*

Most of our efforts will be aimed at studying substructures of number fields, and so applying Definition 2.5 to the case when K is a finite degree extension of $\mathbb{Q}$ gives us the following interesting subring.

Definition 2.6. *The integral closure of $\mathbb{Z}$ in a number field K is called the **ring of integers** of K and is denoted $\mathcal{O}_K$.*

That the *set* $\mathcal{O}_K$ is a ring is a non-trivial statement which we will now prove following a proof given in [5, p.27].

Proposition 2.2. *Let K be a field and R an integral domain contained in K. An element $\alpha \in K$ is integral over R if and only if there exists a non-zero finitely generated R-submodule of K, say M, such that $\alpha M \subseteq M$.*

Proof. For the first direction, if $\alpha \in K$ is integral over R then there exist $r_i \in R$ such that $\alpha^n + r_{n_1}\alpha^{n-1} + \cdots + r_1\alpha + r_0 = 0$, and so we have

$$\alpha^n = -(r_{n_1}\alpha^{n-1} + \cdots + r_1\alpha + r_0).$$

In particular, if we take the R-module M generated by $\{1, \alpha, \ldots, \alpha^{n-1}\}$ then

$$M = R + R\alpha + \cdots + R\alpha^{n-1}$$

and

$$\begin{aligned}\alpha M &= R\alpha + R\alpha^2 + \cdots + R\alpha^n \\ &= R\alpha + R\alpha^2 + \cdots + R\alpha^{n-1} \\ &\subseteq M.\end{aligned}$$

For the second direction, we apply a ring theoretic analogue of Cramer's rule from linear algebra. Recalling this, let $Ax = b$ be a system of linear equations with $A = (a_{ij})$ an $m \times m$ matrix such that $\det A \neq 0$, and $x = (x_1, \ldots, x_m)^\mathsf{T}$ a vector of variables. Then

$$x_i = \frac{\det A_i}{\det A}$$

where A_i is the matrix whose ith column has been replaced with the column vector b. Rewriting this as $x_i \det A = \det A_i$ gives us a statement which can be utilised over any ring. Returning to the proof, suppose M is a finitely generated non-zero R-module in K such that $\alpha M \subseteq M$ (where $\alpha \in K$) and suppose $v_1, \ldots, v_n$ are a set of generators for M. Then for every i we have

$$\alpha v_i = \sum_{j=1}^{n} r_{ij} v_j.$$

Rewriting this as a system of equations we have

$$\begin{aligned}(\alpha - r_{11})v_1 - r_{12}v_2 - \cdots - r_{1n}v_n &= 0 \\ -r_{21}v_1 + (\alpha - r_{22})v_2 - \cdots - r_{2n}v_n &= 0 \\ &\vdots \\ -r_{n1}v_n - r_{n2}v_2 - \cdots + (\alpha - r_{nn})v_n &= 0.\end{aligned}$$

Let A be the matrix of coefficients on the left hand side of the above system, let $v = (v_1, \ldots, v_n)^\mathsf{T}$, and let $b = (0, \ldots, 0)^\mathsf{T}$ so that $Av = b$. Then Cramer's rule says that $v_i \det A = 0$. Since M is assumed to be a non-zero finitely generated R-module, at least one of the v_i is non-zero, and so we must have that $\det A = 0$ (since we are working in K, a field). Thus, upon expanding out the determinant of A, we have

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0$$

with the $c_i \in R$, i.e. that α is integral over R. □

If we choose K to be a number field and $R = \mathbb{Z}$ then we obtain the statement for rings of integers. The crucial logical step uses Proposition 2.2 to argue that for any two elements $\alpha, \beta \in K$ that are integral over $\mathbb{Z}$, there exist non-zero finitely generated $\mathbb{Z}$-submodules M, N of K such that $\alpha M \subseteq M$ and $\beta N \subseteq N$. Now, define the set

$$MN = \left\{ \sum_i m_i n_i : m_i \in M,\ n_i \in N \right\}.$$

It is easily shown that MN is a $\mathbb{Z}$-module. In addition, if $\{m_1, \ldots, m_k\}$ and $\{n_1, \ldots, n_l\}$ are finite sets of generators for M and N respectively, then the set $\{m_1n_1, \ldots, m_in_j, \ldots, m_kn_l\}$ is a finite set of generators for MN, so it is finitely generated as a $\mathbb{Z}$-module. Finally, if $\alpha, \beta \in K$ are integral over $\mathbb{Z}$ then the $\mathbb{Z}$-modules M and N generated by $\{1, \ldots, \alpha^{n-1}\}$ and $\{1, \ldots, \beta^{m-1}\}$ give us the $\mathbb{Z}$-module

$$MN = \mathbb{Z} + \cdots + \mathbb{Z}\alpha^i\beta^j + \cdots + \mathbb{Z}\alpha^{n-1}\beta^{m-1}.$$

That $\alpha\beta MN \subseteq MN$ and $(\alpha \pm \beta)MN \subseteq MN$ confirms that $\mathcal{O}_K$ is a ring.

We now quote one of the most important properties of $\mathcal{O}_K$, coming from [6, p.670], which will pave the way to developing several important structural invariants of $\mathcal{O}_K$, as well as defining the most basic numerical invariant of a number field.

Theorem 2.1. *Let K be a number field of degree n over $\mathbb{Q}$. Then*

(i) K is the field of fractions of $\mathcal{O}_K$,

(ii) $\mathcal{O}_K$ is Noetherian and is a free $\mathbb{Z}$-module of rank n, and

(iii) given any basis $\{b_1, \ldots, b_n\}$ for K as a $\mathbb{Q}$-vector space there is an integer $d \in \mathbb{Z}$ such that $\{db_1, \ldots, db_n\}$ is a basis for a free $\mathbb{Z}$-submodule of $\mathcal{O}_K$ with rank n. In particular, any basis for $\mathcal{O}_K$ as a free $\mathbb{Z}$-module is also a basis for K as a $\mathbb{Q}$-vector space.

Proof. Found in [6, p.670]. □

Definition 2.7. *Let K be a number field of degree n over $\mathbb{Q}$ with ring of integers $\mathcal{O}_K$. A basis $\{b_1, \ldots, b_n\}$ for $\mathcal{O}_K$ as a free $\mathbb{Z}$-module is called an **integral basis** for K.*

To finish this section, we define the *discriminant* of a number field, a numerical invariant which will be of particular importance throughout the remainder of the project, and relate this to the ring of integers of quadratic fields.

Definition 2.8. *Let K be a number field of degree n over $\mathbb{Q}$ with ring of integers $\mathcal{O}_K$. Fix an integral basis $\{b_1, \ldots, b_n\}$ for K and let $\sigma_k : K \hookrightarrow \mathbb{C}$ be the n distinct embeddings of K into $\mathbb{C}$. The **discriminant** of K is the discriminant*

$$d_K := d(b_1, \ldots, b_n) = \begin{vmatrix} \sigma_1(b_1) & \sigma_2(b_1) & \cdots & \sigma_n(b_1) \\ \sigma_1(b_2) & \sigma_2(b_2) & \cdots & \sigma_n(b_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(b_n) & \sigma_2(b_n) & \cdots & \sigma_n(b_n) \end{vmatrix}^2.$$

In fact, we have a characterisation for the rings of integers of quadratic fields K based on the discriminant of K.

Proposition 2.3. *Let $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ square-free. Then*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \bmod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

Proof. The inclusion

$$\mathcal{O}_K \supseteq \begin{cases} \mathbb{Z}[\sqrt{d}] \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \end{cases}$$

is clear; in the first case, $X^2 - d$ is an integer polynomial satisfied by $\sqrt{d}$, and so every element of $\mathbb{Z}[\sqrt{d}]$ is an algebraic integer. In the second case, since $d \equiv 1 \bmod 4$, we have that $X^2 - X + (1-d)/4$ is an integer polynomial satisfied by $(1+\sqrt{d})/2$.
The reverse inclusion requires a touch more effort. Every element $\alpha \in K$ can be written $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$. Suppose that $\alpha \in \mathcal{O}_K$. If $b = 0$ then $\alpha \in \mathbb{Q}$ and so $a \in \mathbb{Z}$ (we knew that $\mathbb{Z} \subseteq \mathcal{O}_K$ anyway). More interesting is the case when $b \neq 0$. First we need to find the minimal polynomial of α over $\mathbb{Z}$. We do this by taking linear combinations of successive powers of α and taking the first linear combination that provides a $\mathbb{Q}$-linear dependence of the powers of α. Indeed, $\alpha^2 = a^2 + 2ab\sqrt{d} + b^2$ so

$$\alpha^2 - 2a\alpha + (a^2 - b^2 d) = 0. \tag{1}$$

Note that since α was assumed to be an algebraic integer and (1) is its minimal polynomial, this means that $2a$ and $a^2 - b^2 d$ are rational integers. Now clearly $4(a^2 - b^2 d)$ is an integer, and so it follows that $4b^2 d \in \mathbb{Z}$. Since d was assumed square-free, it follows that $2b \in \mathbb{Z}$. We now know that $2a, 2b \in \mathbb{Z}$, so let $a = x/2$ and $b = y/2$ for some $x, y \in \mathbb{Z}$. Then $x^2 - y^2 d \equiv 0 \bmod 4$ by the way x and y were chosen. This means in particular that $x^2 \equiv y^2 d \bmod 4$ so that $y^2 d$ is a square modulo 4. The only squares modulo 4 are 0 and 1, so we have either that $y^2 d \equiv 0 \bmod 4$ or that $y^2 d \equiv 1 \bmod 4$. In the first case, since $4 \nmid d$, we must have $y^2 \equiv 0 \bmod 4$, and so both x and y must be even and $d \equiv 1, 2,$ or $3 \bmod 4$. In the second case, we have $y^2 d - 4u = 1$, with $u \in \mathbb{Z}$. If y is even then this equation has no integral solutions, so y must be odd. Let $y = 2v + 1$, with $v \in \mathbb{Z}$. Then $y^2 = 4v^2 + 4v + 1$, and so $d \equiv 1 \bmod 4$. Since this means that $x^2 \equiv y^2 \bmod 4$ and $y^2 \equiv 1 \bmod 4$, we also have that x is odd. In summary, we have

(i) $d \equiv 2, 3 \bmod 4$ and x, y are both even;
(ii) $d \equiv 1 \bmod 4$ and x, y are either both even or both odd.

In case (i), both a and b are integers and so $\alpha \in \mathbb{Z}[\sqrt{d}]$. In case (ii), we may write $a + b\sqrt{d} = r + s(1+\sqrt{d})/2$, with $r = (x-y)/2$ and $s = y$, so that $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. In both cases, this shows that the desired inclusion holds. □

3 Dedekind Domains

We showed in the previous Section that the ring $\mathcal{O}_K$ has the property of being Noetherian, and that $\mathcal{O}_K$ is integrally closed in its field of fractions K. We now show that every non-zero prime ideal in $\mathcal{O}_K$ is maximal. To do so, we shall require a few lemmas. The first lemma was proven as part of an exercise in [3].

Lemma 3.1. *Let K be a number field of degree n and let $\mathcal{O}_K$ be its ring of integers. For a non-zero rational integer a we have*

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

as $\mathbb{Z}$-modules.

Proof. Recall that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n, so that it has a basis, say $\{b_1, \dots, b_n\}$, ensuring that every element $\alpha \in \mathcal{O}_K$ has a unique representation as a $\mathbb{Z}$-linear combination of the b_i. Let $a\mathcal{O}_K \subset \mathcal{O}_K$ be the ideal in $\mathcal{O}_K$ generated by the rational integer a and let $\alpha = c_1b_1 + \cdots + c_nb_n$ where $c_i \in \mathbb{Z}$ for all i. Then $a \mid \alpha$ if and only if $a \mid c_i$ for all i. To see this, suppose $\alpha = ar$ with $r \in \mathcal{O}_K$. Then r has a unique representation as a $\mathbb{Z}$-linear combination of the b_i, say $r = d_1b_1 + \cdots + d_nb_n$. We bring ar to the left hand side so that

$$c_1b_1 + c_2b_2 + \cdots + c_nb_n - ad_1b_1 - ad_2b_2 - \cdots - ad_nb_n = 0.$$

After “collecting like terms” and invoking the linear independence of the b_i as basis elements, we have that $c_i - ad_i = 0$ for all $i = 1, \dots, n$, and hence that $a \mid c_i$ for all i. This is particularly useful, because this means that $\alpha \in a\mathcal{O}_K$ only if $c_i \in a\mathcal{O}_K$ for all i, and hence, in the quotient $\mathcal{O}_K/a\mathcal{O}_K$, we have that $c_1b_1+\cdots+c_nb_n+a\mathcal{O}_K = 0+a\mathcal{O}_K$ only if $c_i + a\mathcal{O}_K = 0 + a\mathcal{O}_K$ for all i. Equivalently, we have a $\mathbb{Z}/a\mathbb{Z}$-linearly independent set $\{b_1+a\mathcal{O}_K, \dots, b_n+a\mathcal{O}_K\}$. Finally, that these span $\mathcal{O}_K/a\mathcal{O}_K$ comes from the surjectivity of the natural projection homomorphism $\mathcal{O}_K \to \mathcal{O}_K/a\mathcal{O}_K$ that sends $\alpha \mapsto \alpha + a\mathcal{O}_K$. Hence $\mathcal{O}_K/a\mathcal{O}_K \cong (\mathbb{Z}/a\mathbb{Z})^n$ as asserted. □

Since we have just seen that $\mathcal{O}_K/a\mathcal{O}_K$ is isomorphic to a finitely generated free module over a finite ring, it has finite cardinality. We use this to show that $\mathcal{O}_K/\mathfrak{I}$ has finite cardinality for any non-zero ideal $\mathfrak{I} \subseteq \mathcal{O}_K$.

Lemma 3.2. *Let K be a number field of degree n and let $\mathcal{O}_K$ be its ring of integers. For any non-zero ideal $\mathfrak{I} \subseteq \mathcal{O}_K$, the quotient $\mathcal{O}_K/\mathfrak{I}$ is finite.*

Proof. Every ideal $\mathfrak{I} \subseteq \mathcal{O}_K$ contains a non-zero rational integer. To see this, note that $\mathcal{O}_K$ consists of all elements of K that are integral over $\mathbb{Z}$. Let $\alpha \in \mathfrak{I}$ be non-zero and let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of α over $\mathbb{Z}$. Then clearly $\alpha \mid f(\alpha) - f(0)$ and since $f(\alpha) = 0$, we have a non-zero integer $-f(0) \in \mathfrak{I} \cap \mathbb{Z}$. Let a be a non-zero rational integer in $\mathfrak{I}$. Then we have the sequence of inclusions $a\mathcal{O}_K \subseteq \mathfrak{I} \subseteq \mathcal{O}_K$. By the third isomorphism theorem,

$$\frac{\mathcal{O}_K/a\mathcal{O}_K}{\mathfrak{I}/a\mathcal{O}_K} \cong \mathcal{O}_K/\mathfrak{I}.$$

In Lemma 3.1 we showed that $\mathcal{O}_K/a\mathcal{O}_K$ was finite. Hence, since $\mathfrak{I}/a\mathcal{O}_K$ is an ideal of $\mathcal{O}_K/a\mathcal{O}_K$, the quotient $\mathcal{O}_K/\mathfrak{I}$ is finite. □

The first theorem of this Section comes as a simple corollary of Lemma 3.2.

Theorem 3.1. *Let K be a number field and let $\mathfrak{p} \subset \mathcal{O}_K$ be a non-zero prime ideal in its ring of integers. Then $\mathfrak{p}$ is a maximal ideal.*

Proof. By Lemma 3.2, we have that $\mathcal{O}_K/\mathfrak{p}$ is finite. Since $\mathfrak{p}$ is a prime ideal, this means that $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain, but finite integral domains are fields, and $\mathcal{O}_K/\mathfrak{p}$ is a field if and only if $\mathfrak{p}$ is maximal. □

The properties of $\mathcal{O}_K$ that we have built up until now are those of so-called *Dedekind domains*.

Definition 3.1. *A **Dedekind domain** is an integral domain D satisfying the following properties:*

(i) D is a Noetherian domain,
(ii) D is integrally closed in its field of fractions, that is, if $\alpha \in K$ is integral over D then $\alpha \in D$, and
(iii) every non-zero prime ideal of D is a maximal ideal.

If K is a number field then, as we have shown, $\mathcal{O}_K$ is always a Dedekind domain. There are examples of rings which appear at first sight to be the ring of integers of a number field, but which are in fact not, and we can use the characterisation of rings of integers as Dedekind domains to prove that they are not, as in the following example.

Example 3.1. *Let $K = \mathbb{Q}(\sqrt{5})$ and let $D = \mathbb{Z}[\sqrt{5}]$. One might naïvely assume that $D = \mathcal{O}_K$. Property (ii) of Definition 3.1 says that $\mathcal{O}_K$ is integrally closed, meaning that an element $\alpha \in K$ that satisfies a monic polynomial over $\mathcal{O}_K$ is in fact an element of $\mathcal{O}_K$. It's easy to find an element of K that violates this property for D; let $\alpha = \frac{1+\sqrt{5}}{2}$. Then $\alpha^2 - \alpha - 1 = 0$, but $\alpha \notin D$, so D cannot be the ring of integers of K.*

The introduction of Dedekind domains begs the following question; why does it matter that $\mathcal{O}_K$ has these seemingly arbitrary properties? Indeed, for the most part, the motivation for their introduction seems somewhat unfounded, with the only reason being that $\mathcal{O}_K$ might be interesting for studying properties of integers by analogy. Fortunately, there is a much more important reason for introducing Dedekind domains. In the integers, we have the *Fundamental Theorem of Arithmetic*. That is, every integer can be written uniquely as a product of prime numbers up to ordering, or equivalently, into a unique product of irreducibles up to ordering. Does a similar property hold in general? Unfortunately, the answer is no, and counter-examples are disconcertingly easy to find. In the ring $\mathbb{Z}[\sqrt{-5}]$ we have $9 = 3^2 = (2+\sqrt{-5})(2-\sqrt{-5})$. Each of these factors is irreducible; since $N(3) = 9 = N(\alpha)N(\beta)$ we only have the possibilities $N(\alpha) = 1, 3, 9$. If $N(\alpha) = 1$ then α is a unit so this doesn't help. There is no element of norm 3 in $\mathbb{Z}[\sqrt{-5}]$ since this would correspond to an integer solution to $a^2+5b^2 = 3$, and if $N(\alpha) = 9$ then β must be a unit. The same argument applies to both $2+\sqrt{-5}$ and $2-\sqrt{-5}$, and so we have found two distinct factorisations into irreducibles of $\mathbb{Z}[\sqrt{-5}]$. Notice that we have been careful to refer to these as factorisations into *irreducibles*. In general, the definitions of prime and irreducible are distinct, though they coincide in $\mathbb{Z}$ since $\mathbb{Z}$ is a unique factorisation domain. In the example given above, $(2+\sqrt{-5}) \mid 9$ but $(2+\sqrt{-5}) \nmid 3$.

The failure of this property to hold in general rings of integers was the Achilles' heel in Lamé's proposed proof of Fermat's Last Theorem. According to [2, p.76-77], Lamé had announced to the Paris Academy a proof of Fermat's Last Theorem based on the factorisation

$$x^n + y^n = (x+y)(x+ry)\dots(x+r^{n-1}y)$$

with $r \neq 1$ a complex number such that $r^n = 1$ (and, of course, $n \neq 2$) . He made the claim that

> ... if x and y are such that the factors $x+y, x+ry, \ldots, x+r^{n-1}y$ are relatively prime then $x^n + y^n = z^n$ implies that each of the factors $x+y, x+ry, \ldots$ must itself be an nth power.

Liouville lacked the same enthusiasm that Lamé had for his proposed proof and was quick to point out that Lamé was making some bold assumptions about the factorisation of complex numbers. It was not until around 2 months later that Liouville was able to confirm to the Academy that Kummer had written to him from Wrocław, and that the content of the letter was damning for Lamé's proof. It was indeed the case that Lamé had erroneously been assuming unique factorisation, and this led his proof to break down.

How do we get around this? The answer is exactly the reason we introduced Dedekind domains; unique factorisation at the level of **elements** may fail, but in a Dedekind domain, unique factorisation is restored at the level of **ideals**.

3.1 Unique Prime Factorisation

In order to study the factorisation of an ideal into a product of prime ideals, we shall make some local arguments about the rings of interest. In particular, this means taking a short detour into commutative algebra to construct *local rings* and *discrete valuation rings*. What follows is taken from exposition in [6, §15.4].

Proposition 3.1. *Let R be a commutative ring with unity and let D be a multiplicatively closed subset of R containing 1. Then there is a commutative ring $D^{-1}R$ and a ring homomorphism $\pi : R \to D^{-1}R$ satisfying the following universal property: for any homomorphism $\psi : R \to S$ of commutative rings sending 1 to 1 such that $\psi(d)$ is a unit in S for every $d \in D$ there is a unique homomorphism $\Psi : D^{-1}R \to S$ that makes the following diagram commute:*

$$\begin{tikzcd}
R \arrow[r, "\pi"] \arrow[dr, "\psi"'] & D^{-1}R \arrow[d, dashed, "\Psi"] \\
& S
\end{tikzcd}$$

Proof. First we define an equivalence relation on $R \times D$ as follows: $(r,d) \sim (s,e)$ if and only if there exists an $x \in D$ such that $x(er - ds) = 0$. This is clearly reflexive; any $x \in D$ will do for this. It is also symmetric, since if such an x exists then there exists a $y \in D$ such that $y(ds - er) = 0$, namely $y = -x$. For transitivity, we suppose that $(r,d) \sim (s,e)$ and $(s,e) \sim (t,f)$, so that $x(er - ds) = 0$ and $y(fs - et) = 0$ for some $x, y \in D$. Then, multiplying the first of these by fy, the second by dx, and adding, we obtain

$$\begin{aligned} fxy(er - ds) + dxy(fs - et) &= xy(fer - fds + fds - det) \\ &= exy(fr - dt) \\ &= 0. \end{aligned}$$

Since D was assumed to be multiplicatively closed, $exy \in D$ and so $(r,d) \sim (t,f)$.

We denote by $D^{-1}R$ the quotient set $(R \times D)/\sim$ and write r/d for the equivalence class of a pair (r,d). The addition and multiplication are easily shown to be well-defined, and they make $D^{-1}R$ into a commutative ring with $1 = 1/1$, and every $d \in D$ becomes a unit in $d/1 \in D^{-1}R$. Define the ring homomorphism $\pi : R \to D^{-1}R$ by $\pi(r) = r/1$

and suppose that $\psi : R \to S$ is a homomorphism of rings sending 1 to 1 such that $\psi(d)$ is a unit in S for every $d \in D$. Define $\Psi : D^{-1}R \to S$ by $\Psi(r/d) = \psi(r)\psi(d)^{-1}$. This map is well-defined since if $r/d = s/e$ then $x(er - ds) = 0$ for some $x \in D$ and so $\psi(x)(\psi(er) - \psi(ds)) = 0$ and so $\psi(r)\psi(d)^{-1} = \psi(s)\psi(e)^{-1}$ ($\psi(x)$ is a unit and $0 \cdot \psi(x)^{-1} = 0$). Hence, it follows that Ψ is a ring homomorphism and that $\Psi \circ \pi = \psi$. To show that Ψ is unique, suppose that Ψ' is another ring homomorphism with $\Psi' \circ \pi = \psi$. Let $x = r/d \in D^{-1}R$. Then $(d/1)x = r/1$ and hence $\pi(d)x = \pi(r)$. Precomposing with Ψ we have $\Psi \circ \pi(d)\Psi(x) = \Psi \circ \pi(r)$ and hence $\psi(d)\Psi(x) = \psi(r)$. In the same way we can obtain $\psi(d)\Psi'(x) = \psi(r)$, and so we have that $\psi(d)\Psi(x) = \psi(d)\Psi'(x)$. Since $d \in D$, $\psi(d)$ is a unit in S and so can be inverted, giving us that $\Psi(x) = \Psi'(x)$. As $x \in D^{-1}R$ was arbitrary, this shows that Ψ was unique to begin with. □

The ring $D^{-1}R$ we constructed above is called the *ring of fractions* of R with respect to D, or alternatively the *localisation* of R at D. It is necessary to specify the D under consideration, since in general there is more than one multiplicatively closed subset of a ring R. In fact, for the purposes of this document, the D under consideration will always be the complement of a prime ideal in R.

Definition 3.2. *A* ***local ring*** *is a ring with a unique maximal ideal.*

Suppose R is a ring with a prime ideal $\mathfrak{p}$. Let $D = R \setminus \mathfrak{p}$. Then the ring $R_{\mathfrak{p}} := D^{-1}R$ is a local ring with the unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. In passing from R to $R_{\mathfrak{p}}$ we discard a lot of structure; the construction ensures that every element of R that is not in $\mathfrak{p}$ becomes a unit, and this gives us a way to focus in on $\mathfrak{p}$, hence the name *local* ring.

Example 3.2. *Let $R = \mathbb{Z}$ and let $D = \mathbb{Z} \setminus (p)$, with p a rational prime. The localisation of $\mathbb{Z}$ at (p), denoted $\mathbb{Z}_{(p)}$, is comprised of all elements of $\mathbb{Q}$ of the form*

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \right\}.$$

Note that since (p) is a prime ideal, if $r \notin (p)$ and $s \notin (p)$ then $rs \notin (p)$, and so D is multiplicatively closed. In addition, the ideal $(p)\mathbb{Z}_{(p)}$ is the unique maximal ideal in $\mathbb{Z}_{(p)}$, and the quotient $\mathbb{Z}_{(p)}/(p)\mathbb{Z}_{(p)}$ is a field of characteristic p, isomorphic to $\mathbb{Z}/(p)$.

Having defined a local ring and given a way to construct them, we define discrete valuation rings following the rather condensed discussion given in [5, p.45]. Their uncomplicated ideal structure will give us what we need to show that ideals in Dedekind domains factorise uniquely into products of prime ideals.

Definition 3.3. *A* ***discrete valuation ring*** *is a local principal ideal domain which is not a field. Equivalently, a discrete valuation ring has a unique non-zero prime ideal. Since a discrete valuation ring is a principal ideal domain, this means that there is exactly one prime element, up to associates.*

Example 3.2 was an example of a discrete valuation ring; the unique non-zero prime ideal is $(p)\mathbb{Z}_{(p)}$ and is generated by the element unique prime element p.
The utility in introducing discrete valuation rings is, as mentioned above, their uncomplicated ideal structure. This is reflected in the following proposition from [5, p.46]:

Proposition 3.2. *An integral domain A is a discrete valuation ring if and only if*

(i) A is Noetherian,

(ii) A is integrally closed, and
(iii) A has exactly one non-zero prime ideal.

Proof. If A is a discrete valuation ring then A is an integral domain by definition so we need only prove one direction.
Suppose then that A is an integral domain satisfying the three conditions above. First we show that every ideal of A is principal. Let c be a non-zero, non-unit element of A and let $M := A/(c)$. For every non-zero $m \in M$ we have the annihilator ideal

$$\mathrm{Ann}(m) = \{a \in A : am = 0\}.$$

By property (i), A is Noetherian, and so we can choose $m \in M$ to be such that $\mathrm{Ann}(m)$ is maximal among all such ideals. Let $m = b + (c)$ for some $b \in A$ and write $\mathfrak{p} = \mathrm{Ann}(b + (c))$. Note that $ab + (c) = 0 + (c)$ when $c \mid ab$, so $\mathfrak{p} = \{a \in A : c \mid ab\}$. We show that $\mathfrak{p}$ is a prime ideal (hence the notation). Suppose not, and let $x, y \in A$ such that $xy \in \mathfrak{p}$ but $x \notin \mathfrak{p}$ and $y \notin \mathfrak{p}$. Then $yb + (c)$ is non-zero in M since $y \notin \mathfrak{p}$. Now consider the ideal $\mathrm{Ann}(yb + (c))$. This ideal is the set of $a \in A$ such that $c \mid ayb$, and so taking $y = 1$ gives the ideal $\mathfrak{p}$. In particular, this means that $\mathfrak{p} \subset \mathrm{Ann}(yb + (c))$, contradicting the maximality of $\mathfrak{p}$, and so $\mathfrak{p}$ must be prime. We claim now that $\mathfrak{p} = (cb^{-1})$. Firstly, we cannot have $bc^{-1} \in A$, since if this were the case then $b = c \cdot bc^{-1} \in (c)$ and so $m = b + (c) = 0 + (c)$ in M. By the way $\mathfrak{p}$ was defined, we have $\mathfrak{p}b \subseteq (c)$, and so $\mathfrak{p}bc^{-1} \subseteq A$ and $\mathfrak{p}bc^{-1}$ is an ideal. If $\mathfrak{p}bc^{-1} \subseteq \mathfrak{p}$ then bc^{-1} would be integral over A, since $\mathfrak{p}$ is a finitely generated A-module (being that it is an ideal in a Noetherian ring) and Proposition 2.2 guarantees that bc^{-1} is integral over A. However, if bc^{-1} is integral over A then property (ii) says that $bc^{-1} \in A$, which we know is untrue, so $\mathfrak{p} \subsetneq \mathfrak{p}bc^{-1} \subseteq A$, and since $\mathfrak{p}$ is maximal, we have that $\mathfrak{p}bc^{-1} = A$. In other words, we have $\mathfrak{p} = (cb^{-1})$
Finally, we show that this implies that every ideal is principal. Let $\pi = cb^{-1}$, so that $\mathfrak{p} = (\pi)$. Let $\mathfrak{a} \subsetneq A$ be an ideal and consider the sequence of inclusions

$$\mathfrak{a} \subset \mathfrak{a}\pi^{-1} \subset \mathfrak{a}\pi^{-2} \subset \dots$$

If there is some r for which $\mathfrak{a}\pi^{-r} = \mathfrak{a}\pi^{-r-1}$ then $\pi^{-1}(\mathfrak{a}\pi^{-r}) = \mathfrak{a}\pi^{-r}$, and by Proposition 2.2 once again, we have that π^{-1} is integral over A and so $\pi^{-1} \in A$, but of course $\pi^{-1} = bc^{-1} \notin A$, so the sequence of inclusions is a strictly increasing sequence. Since A is Noetherian, this cannot be completely contained in A. Let m be the smallest integer such that $\mathfrak{a}\pi^{-m} \subseteq A$ but $\mathfrak{a}\pi^{-m-1} \not\subseteq A$. Then $\mathfrak{a}\pi^{-m} \not\subseteq \mathfrak{p}$, since if this were the case then $\pi^{-1}\mathfrak{a}\pi^{-m} = \mathfrak{a}\pi^{-m-1} \subset \pi^{-1}\mathfrak{p} = A$, a possibility we excluded in the way we chose m. Hence, we must have $\mathfrak{a}\pi^{-m} = A$, and so $\mathfrak{a} = (\pi^m)$. Since $\mathfrak{a}$ was arbitrary, we have that A is a principal ideal domain.
To conclude, since A has been shown to be a principal ideal domain with a unique non-zero prime ideal, we have that A is a discrete valuation ring. □

In light of the above discussion, we are now able to introduce the main property of Dedekind domains that we are interested in.

Theorem 3.2. *Let D be a Dedekind domain. Then every proper non-zero ideal $\mathfrak{a} \subset D$ can be written*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\dots\mathfrak{p}_n^{r_n}$$

where the $\mathfrak{p}_i$ are distinct non-zero prime ideals of D and the $r_i \in \mathbb{N}$ are uniquely determined.

We shall need a few lemmas in order to prove the statement.

Lemma 3.3. *Let D be a Noetherian ring. Then every non-zero ideal $\mathfrak{a}$ of D contains a product of non-zero prime ideals.*

Proof. Suppose to the contrary that there exists a non-zero ideal $\mathfrak{a}$ that does not contain a product of prime ideals, and choose $\mathfrak{a}$ to be maximal among such counterexamples. Then $\mathfrak{a}$ is, of course, itself not prime, so there exist $x, y \in D$ such that $xy \in \mathfrak{a}$ but $x \notin \mathfrak{a}$ and $y \notin \mathfrak{a}$. Now $\mathfrak{a} \subset \mathfrak{a} + (x)$ and $\mathfrak{a} \subset \mathfrak{a} + (y)$, but the product of $\mathfrak{a} + (x)$ and $\mathfrak{a} + (y)$ is contained in $\mathfrak{a}$. Since $\mathfrak{a}$ was chosen to be a maximal counterexample to the statement, it must be that $\mathfrak{a} + (x)$ and $\mathfrak{a} + (y)$ contain products of prime ideals, but then so, too, does their product, and so it follows that $\mathfrak{a}$ must contain a product of prime ideals. Hence there exists no non-zero ideal $\mathfrak{a}$ that does not contain a product of non-zero prime ideals. □

Lemma 3.4. *Let D be a ring and let $\mathfrak{a}$ and $\mathfrak{b}$ be coprime ideals in D. For all $m, n \in \mathbb{N}$, the ideals $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are coprime.*

Proof. Suppose, to the contrary, $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are not coprime. Then $\mathfrak{a}^m + \mathfrak{b}^n \neq D$ so $\mathfrak{a}^m + \mathfrak{b}^n \subset \mathfrak{p}$ for some maximal (hence prime) ideal $\mathfrak{p}$. As such, we have $\mathfrak{a}^m \subset \mathfrak{p}$ and $\mathfrak{b}^n \subset \mathfrak{p}$, but since $\mathfrak{p}$ is prime this implies that $\mathfrak{a} \subset \mathfrak{p}$ and $\mathfrak{b} \subset \mathfrak{p}$, a contradiction. □

Lemma 3.5. *Let D be an integral domain with a maximal ideal $\mathfrak{p}$. Let $\mathfrak{q}$ be the ideal generated by $\mathfrak{p}$ in the localisation $D_\mathfrak{p}$ of D at $\mathfrak{p}$ (that is, $\mathfrak{q} = \mathfrak{p}D_\mathfrak{p}$). Then the map*

$$\varphi : D/\mathfrak{p}^m \to D_\mathfrak{p}/\mathfrak{q}^m, \quad m \in \mathbb{N}$$

sending $a + \mathfrak{p}^m$ to $a + \mathfrak{q}^m$ is an isomorphism for all $m \in \mathbb{N}$.

Proof. First we show that the map is injective. To do this, we show that the kernel of φ is $\mathfrak{p}^m$. This is equivalent to showing that $\mathfrak{q}^m \cap D = \mathfrak{p}^m$. Since $D_\mathfrak{p} = S^{-1}D$, with $S^{-1} = D \setminus \mathfrak{p}$, we have to show that $(S^{-1}\mathfrak{p}^m) \cap D = \mathfrak{p}^m$. Given an arbitrary element $a \in (S^{-1}\mathfrak{p}^m) \cap D$ we can write $a = b/s$ with $b \in \mathfrak{p}^m$, $s \in S$, and $a \in D$. But then $sa = b$, and so $sa \in \mathfrak{p}^m$, which in turn means that $sa = 0$ in $D/\mathfrak{p}^m$. The only maximal ideal containing $\mathfrak{p}^m$ is $\mathfrak{p}$, so the only maximal ideal of $D/\mathfrak{p}^m$ is $\mathfrak{p}/\mathfrak{p}^m$, and so $D/\mathfrak{p}^m$ is a local ring. Now, since $s \in S = D \setminus \mathfrak{p}$, we have that $s + \mathfrak{p}^m \notin \mathfrak{p}/\mathfrak{p}^m$, and so $s + \mathfrak{p}^m$ is a unit in $D/\mathfrak{p}^m$. Hence, $sa = 0$ in $D/\mathfrak{p}^m$ implies that $a = 0$ in $D/\mathfrak{p}^m$ and hence that $a \in \mathfrak{p}^m$. The arbitrariness of a allows us to conclude that $\mathfrak{p}^m = \mathfrak{q}^m \cap D$, and so φ is injective.
To prove that φ is surjective, we take an element $as^{-1} \in D_\mathfrak{p}$. Since $s \notin \mathfrak{p}$, we have $\mathfrak{p} \subset (s) + \mathfrak{p} \subseteq D$ and since $\mathfrak{p}$ is maximal, we have $(s) + \mathfrak{p} = D$, that is, (s) and $\mathfrak{p}$ are coprime. Hence, there exist $b \in D$ and $q \in \mathfrak{p}^m$ such that $bs + q = 1$, and so $b \mapsto s^{-1}$ in $D_\mathfrak{p}/\mathfrak{q}^m$ and $ba \mapsto as^{-1}$ under φ. Since for any $a \in D$ we have an image under φ, the result is proven. □

We now have what we need to prove that every non-zero ideal in a Dedekind domain factors uniquely into a product of prime ideals. Let D be a Dedekind domain and let $\mathfrak{a}$ be a non-zero ideal. By Lemma 3.3 we have that every non-zero ideal contains a product of prime ideals. Let $\mathfrak{b}$ be this product, so that $\mathfrak{b} \subset \mathfrak{a}$ and $\mathfrak{b} = \mathfrak{p}_1^{r_1} \dots \mathfrak{p}_m^{r_m}$. Supposing that the $\mathfrak{p}_i$ are distinct, we have that

$$D/\mathfrak{b} \cong \prod_{i=1}^{m} D/\mathfrak{p}_i^{r_i} \cong \prod_{i=1}^{m} D_{\mathfrak{p}_i}/\mathfrak{q}_i^{r_i}$$

where $\mathfrak{q}_i = \mathfrak{p}_i D_{\mathfrak{p}_i}$ is the unique maximal ideal of $D_{\mathfrak{p}_i}$ as given in Lemma 3.5. The first isomorphism follows from the Chinese Remainder Theorem, since the $\mathfrak{p}_i$ are pairwise distinct, and coprime by Lemma 3.4. The second isomorphism follows from Lemma 3.5. Now we consider the ideal $\mathfrak{a} \subset D$. Since $\mathfrak{b} = \mathfrak{p}_1^{r_1} \dots \mathfrak{p}_m^{r_m} \subset \mathfrak{a}$, in the quotient $D/\mathfrak{b}$ we have

$$\mathfrak{a}/\mathfrak{b} \cong \prod_{i=1}^{m} \mathfrak{a}/\mathfrak{p}_i^{r_i} \cong \prod_{i=1}^{m} \mathfrak{a}/\mathfrak{q}_i^{r_i}$$

where, in the second isomorphism, $\mathfrak{a}$ is considered as an ideal of the local ring $D_{\mathfrak{p}_i}$ for each i. Now, since the $D_{\mathfrak{p}_i}$ are local rings, they are discrete valuation rings, and so any ideal of $D_{\mathfrak{p}_i}$ has the form $\mathfrak{a} = \mathfrak{q}_i^{s_i}$ where $\mathfrak{q}_i = \mathfrak{p}_i D_{\mathfrak{p}_i}$ as in Lemma 3.5. In the second isomorphism above, we then have

$$\prod_{i=1}^{m} \mathfrak{a}/\mathfrak{q}_i^{r_i} \cong \prod_{i=1}^{m} \mathfrak{q}_i^{s_i}/\mathfrak{q}_i^{r_i}$$

for some $s_i \leq r_i$. In particular, under this isomorphism, this is also the image of a product of prime ideals $\mathfrak{p}_1^{s_1} \dots \mathfrak{p}_m^{s_m} \subset D$, so that $\mathfrak{a} = \mathfrak{p}_1^{s_1} \dots \mathfrak{p}_m^{s_m}$ in $D/\mathfrak{b}$. Finally, since there is a one-to-one correspondence between ideals of $D/\mathfrak{b}$ and ideals of D containing $\mathfrak{b}$, we have that $\mathfrak{a} = \mathfrak{p}_1^{s_1} \dots \mathfrak{p}_m^{s_m}$ in D. For the uniqueness, note that if $\mathfrak{a} = \mathfrak{p}_1^{s_1} \dots \mathfrak{p}_m^{s_m} = \mathfrak{p}_1^{t_1} \dots \mathfrak{p}_m^{t_m}$ then $s_i = t_i$ for all i, since in the above proof we showed that $\mathfrak{q}_i^{s_i} = \mathfrak{a} D_{\mathfrak{p}_i} = \mathfrak{q}_i^{t_i}$.

Thus, we see that, while a ring may not possess unique factorisation of elements, if that ring is a Dedekind domain, it always possesses unique factorisation of ideals. We revisit our example in the previous section.

Example 3.3. *Let $D = \mathbb{Z}[\sqrt{-5}]$. We saw in the first section that $9 = 3^2 = (2+\sqrt{-5})(2-\sqrt{-5})$ and that each of these numbers was prime, so that unique factorisation in $\mathbb{Z}[\sqrt{-5}]$ fails. Now we consider the ideal $(9) \subset \mathbb{Z}[\sqrt{-5}]$. Immediately, we may write $(9) = (3)^2$ but note that (3) is not a prime ideal in $\mathbb{Z}[\sqrt{-5}]$. In fact, the ideal (3) factorises as $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$, and each of these is a prime ideal since, for example*

$$\mathbb{Z}[\sqrt{-5}]/(3, 1+\sqrt{-5}) \cong \mathbb{Z}[X]/(3, 1+X) \cong \mathbb{F}_3$$

which is an integral domain. We write $\mathfrak{p}_1 = (3, 1+\sqrt{-5})$ and $\mathfrak{p}_2 = (3, 1-\sqrt{-5})$. Then $9 = \mathfrak{p}_1^2\mathfrak{p}_2^2$. We can see that $(2-\sqrt{-5}) = \mathfrak{p}_1^2$ and $(2+\sqrt{-5}) = \mathfrak{p}_2^2$, so the factorisation $(9) = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_1\mathfrak{p}_2) = \mathfrak{p}_1^2\mathfrak{p}_2^2$ is unique.

3.2 Factorisation in Number Fields

In the last section we saw that every ideal in a Dedekind domain factorises uniquely into a product of prime ideals. In the same way that we have divisibility for elements of rings, we also have a concept of divisibility for ideals. If $\mathfrak{a}$ is an ideal in a Dedekind domain with prime ideal factorisation $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$ then we say that the $\mathfrak{p}_i^{e_i}$ are divisors of $\mathfrak{a}$ and write $\mathfrak{p}_i^{e_i} \mid \mathfrak{a}$ in analogy with the notation we have for elements. In the context of number fields and their rings of integers, we wish to study the splitting properties of primes in extensions of $\mathbb{Q}$. In the previous section, we saw that $(3) \subset \mathbb{Z}[\sqrt{-5}]$ was not a prime ideal, but that it split into the product $(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$ and that each of these was a prime ideal. We call this property *splitting*, which we discuss now along with other important properties such as *ramification* and *inertia*. The following definitions come from [3, ch.10].

Definition 3.4. *Let K be a number field and $\mathcal{O}_K$ its ring of integers. Let $\mathfrak{p}$ be a prime ideal in $\mathbb{Z}$. Since $\mathcal{O}_K$ is a Dedekind domain, the ideal $\mathfrak{p}\mathcal{O}_K$ can be written*

$$\mathfrak{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$$

where each of the $\mathfrak{P}_i$ is a prime ideal in $\mathcal{O}_K$. The primes $\mathfrak{P}_i$ are called primes ***lying above*** *$\mathfrak{p}$ (or equivalently that $\mathfrak{p}$ lies below the $\mathfrak{P}_i$.) We say that $\mathfrak{p}$* ***ramifies*** *in $\mathcal{O}_K$ if any of the e_i is greater than 1. If $e_i = 1$ for all i then $\mathfrak{p}$ is said to be* ***unramified****. For each of the $\mathfrak{P}_i$ the index e_i is called the* ***ramification index*** *of $\mathfrak{P}_i$ and the number g is called the* ***decomposition number*** *of the prime $\mathfrak{p}$ in $\mathcal{O}_K$. If $g = 1$ there is a single prime ideal with ramification index e. If, in addition, $e = 1$ then we say that $\mathfrak{p}$ is* ***inert*** *in $\mathcal{O}_K$. Finally, if $e_i = 1$ for all i and $g = [K : \mathbb{Q}]$, we say that $\mathfrak{p}$* ***splits completely*** *in $\mathcal{O}_K$.*

The primes $\mathfrak{P}_i$ uniquely determine the prime $\mathfrak{p}$ above which they lie. If $\mathfrak{p} \subset \mathbb{Z}$ is a prime ideal then $\mathfrak{p} = (p)$. If there were another prime ideal (q) lying below the $\mathfrak{P}_i$ then $(p) \subseteq \mathfrak{P}_i$ and $(q) \subseteq \mathfrak{P}_i$ so that $(p, q) \subseteq \mathfrak{P}_i$, which is impossible, since, as p and q are prime, the ideals (p) and (q) are coprime, so that $(p, q) = (p) + (q) = \mathcal{O}_K$.

Definition 3.5. *Let K be a number field and $\mathcal{O}_K$ its ring of integers. Let $\mathfrak{I}$ be an ideal in $\mathcal{O}_K$. The* ***norm*** *of $\mathfrak{I}$ is defined as $N(\mathfrak{I}) = |\mathcal{O}_K/\mathfrak{I}|$, which is a natural number by Lemma 3.2.*

We saw at the beginning of the Section that $\mathcal{O}_K/\mathfrak{P}_i$ is a finite field of characteristic p (when $\mathfrak{P}_i$ is a prime ideal, of course). Recall from Lemma 3.1 that $\mathcal{O}_K/p\mathcal{O}_K \cong (\mathbb{Z}/p\mathbb{Z})^n$, where $n = [K : \mathbb{Q}]$, so that $N(p\mathcal{O}_K) = p^n$. Now let $\mathfrak{P}_i \supseteq p\mathcal{O}_K$ be a prime lying above p. Since $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$ and $\mathbb{Z}$ is a principal ideal domain, $\mathfrak{P}_i$ is a free $\mathbb{Z}$-submodule of $\mathcal{O}_K$ and has rank less than or equal to n, say m, so that $|\mathfrak{P}_i/p\mathcal{O}_K| = p^m$, and hence, by Lemma 3.2,

$$\mathcal{O}_K/\mathfrak{P}_i \cong \frac{(\mathbb{Z}/p\mathbb{Z})^n}{(\mathbb{Z}/p\mathbb{Z})^m} \cong (\mathbb{Z}/p\mathbb{Z})^{f_i}$$

where $f_i = n - m$. To complete Definition 3.4, we define the positive integer f_i as the *inertial degree* of the prime $\mathfrak{P}_i$ in $\mathcal{O}_K$. It is the degree of the field extension $[\mathcal{O}_K/\mathfrak{P}_i : \mathbb{Z}/p\mathbb{Z}]$, so that if $f_i = 1$, we have $\mathcal{O}_K/\mathfrak{P}_i \cong \mathbb{Z}/p\mathbb{Z}$.
The splitting behaviour of primes in number fields is controlled by these properties, as can be seen in the following theorem from [5, p.58]. The theorem is proven for general field extensions, and can be specialised to the case of number fields.

Theorem 3.3. *Let K be a number field of degree n, let p be a rational prime and suppose $p\mathcal{O}_K$ has the factorisation*

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}.$$

Then

$$e_1 f_1 + e_2 f_2 + \dots + e_g f_g = n,$$

where the e_i and f_i are respectively the ramification indices and inertial degrees of the primes $\mathfrak{P}_i$.

Proof. From Lemma 2.2., we have that $\mathcal{O}_K/p\mathcal{O}_K \cong (\mathbb{Z}/p\mathbb{Z})^n$, so that $\mathcal{O}_K/p\mathcal{O}_K$ is an n-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$. Additionally, by the Chinese remainder theorem, we have that

$$\mathcal{O}_K/p\mathcal{O}_K \cong \bigoplus_{i=1}^{g} \mathcal{O}_K/\mathfrak{P}_i^{e_i},$$

so that

$$(\mathbb{Z}/p\mathbb{Z})^n \cong \bigoplus_{i=1}^{g} \mathcal{O}_K/\mathfrak{P}_i^{e_i}$$

as $\mathbb{Z}/p\mathbb{Z}$-vector spaces. Finally, since $[\mathcal{O}_K : \mathfrak{I}] = N(\mathfrak{I})$ for ideals $\mathfrak{I} \subset \mathcal{O}_K$, and since the norm of an ideal is multiplicative, we have that $[\mathcal{O}_K : \mathfrak{P}_i^{e_i}] = [\mathcal{O}_K : \mathfrak{P}_i]^{e_i} = p^{e_i f_i}$ by definition, showing that each of the summands $\mathcal{O}_K/\mathfrak{P}_i^{e_i}$ is an $e_i f_i$-dimensional $\mathbb{Z}/p\mathbb{Z}$-vector space, whose direct sum is an n-dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$. We conclude that $\sum e_i f_i = n$ by the well-definedness of vector space dimension. □

Theorem 3.3 places a restriction on the way that a rational prime can decompose in a number field, as in the following example.

Example 3.4. *Let $K = \mathbb{Q}(\sqrt{d})$, that is, K is a quadratic extension. That $[K : \mathbb{Q}] = 2$ massively restricts the possible ways that a prime can decompose in K. If $(p) = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$ (assuming each of the e_i is non-zero), then we must have $g \leq 2$, so that $g = 1$ or 2. If $g = 2$, Theorem $3.1.$ says that $e_1 f_1 + e_2 f_2 = 2$, which forces $e_1 = e_2 = f_1 = f_2 = 1$. If $g = 1$, then $e_1 f_1 = 2$, so either $e_1 = 1$ and $f_1 = 2$, or vice-versa. Equivalently, a rational prime p can only decompose in K in the following ways*

$$\begin{aligned} &p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2, \text{ where } f_1 = f_2 = 1, \text{ and } \mathfrak{P}_1 \neq \mathfrak{P}_2 \\ &p\mathcal{O}_K = \mathfrak{P}^2, \text{ where } f_1 = 1, \\ &p\mathcal{O}_K = \mathfrak{P}, \text{ where } f_1 = 2. \end{aligned}$$

In the first case, $p\mathcal{O}_K$ splits into a product of distinct prime ideals. In the second case, $p\mathcal{O}_K$ ramifies and $\mathfrak{P}$ is a prime ideal in $\mathcal{O}_K$ with ramification index 2. In the third case, $p\mathcal{O}_K$ is inert. These behaviours are linked to the solubility of the congruence $X^2 \equiv d \bmod p$, and so can be studied via the law of quadratic reciprocity, as is shown in Theorem 10.2.1. in [3, p.242-245].

Example 3.4 shows the behaviour of primes in a Galois extension. In this case, all of the ramification indices are the same and all of the inertial degrees are the same, and so the statement of Theorem 3.3 undergoes a slight modification.

Theorem 3.4. *Let K be a number field of degree n and suppose K is Galois over $\mathbb{Q}$. Let p be a rational prime and suppose that $p\mathbb{Z}$ has the $\mathcal{O}_K$-factorisation*

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}.$$

Then $e_i = e_j$ and $f_i = f_j$ for all $i, j \in \{1, \dots, g\}$ and so $efg = n$.

Proof. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Then $\sigma(\mathcal{O}_K) = \mathcal{O}_K$. To see this, note that $\mathcal{O}_K$ consists of all elements of K that are integral over $\mathbb{Z}$, and $\mathbb{Z}$ is fixed by $\mathrm{Gal}(K/\mathbb{Q})$. Additionally, if $\mathfrak{P}_i$ is prime then $\sigma(\mathfrak{P}_i)$ is prime; if $xy \in \sigma(\mathfrak{P}_i)$ then $\sigma(x)^{-1}\sigma(y)^{-1} \in \mathfrak{P}_i$, and so $x \in \sigma(\mathfrak{P}_i)$ or

$y \in \sigma(\mathfrak{P}_i)$. If $\mathfrak{P}_i$ lies over p then $\sigma(\mathfrak{P}_i)$ lies over p, since it also occurs in the factorisation of $p\mathcal{O}_K$. Consider the factorisation

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}.$$

Then $\sigma(p\mathcal{O}_K) = p\mathcal{O}_K$ so that

$$p\mathcal{O}_K = \sigma(\mathfrak{P}_1)^{e_1} \dots \sigma(\mathfrak{P}_g)^{e_g}$$

and so the ramification indices of $\mathfrak{P}_i$ and $\sigma(\mathfrak{P}_i)$ coincide. Finally, if $a+\mathfrak{P}_i$ is an element of $\mathcal{O}_K/\mathfrak{P}_i$ then $\sigma(a)+\sigma(\mathfrak{P}_i)$ is an element of $\mathcal{O}_K/\sigma(\mathfrak{P}_i)$. Since $a \in \mathcal{O}_K$, and $\sigma(\mathcal{O}_K) = \mathcal{O}_K$, the degrees of $\mathcal{O}_K/\mathfrak{P}_i$ and $\mathcal{O}_K/\sigma(\mathfrak{P}_i)$ over $\mathbb{Z}/p\mathbb{Z}$ are both f_i. It remains now to prove that σ acts transitively on the set of primes of $\mathcal{O}_K$ that lie above p. Suppose $\mathfrak{P}_i$ and $\mathfrak{P}_j$ both divide $p\mathcal{O}_K$ but that $\mathfrak{P}_i$ and $\mathfrak{P}_j$ are not conjugate, so that for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ we have $\sigma(\mathfrak{P}_i) \neq \mathfrak{P}_j$. Then, by the Chinese remainder theorem, we can find a $\beta \in \mathfrak{P}_j$ such that $\beta \notin \mathfrak{P}_i$ for any other i. Let $b = N(\beta) = \prod \sigma(\beta)$. Then $b \in \mathbb{Z}$, and since $\beta \in \mathfrak{P}_j$, we also have $b \in \mathfrak{P}_j$. Hence, $b \in \mathfrak{P}_j \cap \mathbb{Z} = p\mathcal{O}_K$. Now, for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, we have $\beta \notin \sigma^{-1}(\mathfrak{P}_i)$ and so $\sigma(\beta) \notin \mathfrak{P}_i$, but we showed that $b = \prod \sigma(\beta) \in p\mathcal{O}_K \subset \mathfrak{P}_i$, so this contradicts that $\mathfrak{P}_i$ is a prime ideal. □

Example 3.5. *Let $K = \mathbb{Q}(\sqrt{78})$. Since $78 \equiv 2 \bmod 4$ we have $\mathcal{O}_K = \mathbb{Z}[\sqrt{78}]$. The minimal polynomial of $\sqrt{78}$ over $\mathbb{Q}$ is $X^2 - 78$, and the factorisation of a prime in $\mathcal{O}_K$ is mirrored by the factorisation of $X^2 - 78 \bmod p$, since $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{Z}[X]/(p, X^2-78)$ and $\mathbb{Z}[X]/(p, X^2-78) \cong \mathbb{F}_p[X]/(X^2 - \overline{78})$ where $\bar{\cdot}$ denotes reduction modulo p. Let $p = 3$. Then, since $3 \mid 78$, we have $X^2 - 78 \equiv X^2 \bmod 3$, and so $(3) = (3, \sqrt{78})^2$ in $\mathcal{O}_K$. That is, the prime 3 ramifies in this extension. When $p = 5$, we have $X^2 - 78 \equiv X^2 + 2 \bmod 5$, and this is irreducible, so that $\mathbb{F}_p[X]/(X^2+2)$ is a finite field, and so (5) is prime in $\mathcal{O}_K$.*

3.3 The Ideal Class Group

Before we begin to talk about the ideal class group, we first need to introduce *fractional ideals*.

Definition 3.6. *Let D be a Dedekind domain with field of fractions K. A **fractional ideal** is a non-empty subset $\mathfrak{F} \subset K$ with the following properties:*

(i) if $\alpha \in \mathfrak{F}$ and $\beta \in \mathfrak{F}$ then $\alpha + \beta \in \mathfrak{F}$,
(ii) if $\alpha \in \mathfrak{F}$ and $r \in D$ then $r\alpha \in \mathfrak{F}$, and
(iii) there exists a non-zero $\gamma \in D$ such that $\gamma\mathfrak{F} \subseteq D$.

These fractional ideals closely resemble what we, to avoid confusion, now refer to as *integral ideals*. Indeed, the class of fractional ideals subsumes that of integral ideals, in that such a γ always exists for integral ideals; just take $\gamma = 1$ and $\mathfrak{F}$ an integral ideal. We stress the use of the indefinite article when referring to γ; if γ is such as described then so is any integral multiple of γ. We can think of these γ as common denominators for fractional ideals. If D is the ring of integers of a number field K (whose field of fractions is then, of course, the number field), we can find alternative definitions for fractional ideals, as in Theorem 2.3 of [4, p.2, 3]. For instance, we can always improve on a common denominator $\gamma \in \mathcal{O}_K \setminus \{0\}$ by replacing it with $N(\gamma) \in \mathbb{Z} \setminus \{0\}$, which is guaranteed to exist and falls within the description “integral multiple of γ”. Additionally, fractional ideals are finitely generated $\mathcal{O}_K$-modules in K, with the $\mathcal{O}_K$-action given by multiplication. This gives us another way to check if a non-empty subset of K is a fractional ideal. This is particularly useful when we define the *inverse* of a fractional ideal.

Definition 3.7. *For each fractional ideal $\mathfrak{F}$ of a Dedekind domain D we define the set*

$$\widetilde{\mathfrak{F}} = \{\gamma \in K : \gamma\mathfrak{F} \subseteq D\}.$$

Notice here that $\gamma \in K$, so this is slightly more than just the common denominators for a fractional ideal $\mathfrak{F}$.
It turns out that $\widetilde{\mathfrak{F}}$ is itself a fractional ideal, the proof of which makes use of the equivalent characterisations mentioned earlier. Indeed, $\widetilde{\mathfrak{F}}$ is non-empty because $\mathfrak{F}$ has non-zero common denominators. It is easy to show that left multiplication makes $\widetilde{\mathfrak{F}}$ into an $\mathcal{O}_K$-module. To show that it is finitely generated as an $\mathcal{O}_K$-module, let $x \in \mathfrak{F} \setminus \{0\}$. For any $\alpha \in \widetilde{\mathfrak{F}}$ we have $\alpha\mathfrak{F} \subset \mathcal{O}_K$, so that $x\alpha \in \mathcal{O}_K$ for any $\alpha \in \widetilde{\mathfrak{F}}$, and hence $x\widetilde{\mathfrak{F}} \subset \mathcal{O}_K$. In particular, since x is invertible, we have $\widetilde{\mathfrak{F}} \subset \frac{1}{x}\mathcal{O}_K$. Now, recall that $\mathcal{O}_K$ is a finitely generated free $\mathbb{Z}$-module. Since $\widetilde{\mathfrak{F}} \subset \frac{1}{x}\mathcal{O}_K$ it is a submodule of a finitely generated free $\mathbb{Z}$-module, and so itself is finitely generated as a $\mathbb{Z}$-module, hence also as an $\mathcal{O}_K$-module. Hence, $\widetilde{\mathfrak{F}}$ is a fractional ideal.
As with any ideal, we can take sums and products of ideals to obtain new ideals.

Proposition 3.3. *Let K be a number field and let $\mathfrak{F}$ be a fractional ideal of $\mathcal{O}_K$. Then*

$$\mathfrak{F}\widetilde{\mathfrak{F}} = \mathcal{O}_K.$$

Proof. Suppose there is an ideal $\mathfrak{I}$ such that $\mathfrak{F}\mathfrak{I} = \mathcal{O}_K$. For any $x \in \mathfrak{I}$ we have $x\mathfrak{F} \subseteq \mathfrak{I}\mathfrak{F} = \mathfrak{F}\mathfrak{I} = \mathcal{O}_K$, so certainly we have $\mathfrak{I} \subseteq \widetilde{\mathfrak{F}}$. Then $\mathfrak{F}\mathfrak{I} = \mathcal{O}_K \subseteq \mathfrak{F}\widetilde{\mathfrak{F}}$. On the other hand, if $x \in \widetilde{\mathfrak{F}}$ then $x\mathfrak{F} \subset \mathcal{O}_K$ by definition, and so $\mathfrak{F}\widetilde{\mathfrak{F}} \subseteq \mathcal{O}_K$. Hence, $\mathfrak{F}\widetilde{\mathfrak{F}} = \mathcal{O}_K$. □

Proposition 3.3 suggests we have a multiplicative inverse for multiplication of ideals. Indeed, we can place a group structure on the set of all fractional ideals of a number field, since the product of any two fractional ideals is again a fractional ideal, we exhibited the existence of an inverse, and the ideal $(1) = \mathcal{O}_K$ is a suitable candidate for the identity of the group.

Proposition 3.4. *Let K be a number field and let I_K denote the group of fractional ideals of $\mathcal{O}_K$. Let P_K denote the set of principal ideals of $\mathcal{O}_K$. Then $P_K \trianglelefteq I_K$.*

Proof. I_K is an Abelian group, so in fact we need only show that P_K is a subgroup of I_K and normality follows immediately. Indeed, the ideal (1) is principal, so there is an identity in P_K. If $\alpha \in \mathcal{O}_K$ then the principal ideal (α) has inverse $(1/\alpha)$. Finally, a product of principal ideals is again principal, so $P_K \leq I_K$. □

Since P_K is normal in I_K we can form a well-defined quotient from them, and this is the main definition of this section.

Definition 3.8. *Let K be a number field and let I_K be the group of fractional ideals of $\mathcal{O}_K$ with the subgroup P_K of principal fractional ideals. We define the **ideal class group** as the quotient $\mathrm{Cl}(K) := I_K/P_K$. The **class number** of K, denoted h_K, is the order of $\mathrm{Cl}(K)$.*

Notice that, if $P_K = I_K$ then $h_K = 1$ and $\mathcal{O}_K$ is a principal ideal domain.

Proposition 3.5. *Let K be a number field with ring of integers $\mathcal{O}_K$. Then*

$$\begin{aligned} h_K = 1 &\iff \mathcal{O}_K \textit{ is a principal ideal domain} \\ &\iff \mathcal{O}_K \textit{ is a unique factorisation domain.} \end{aligned}$$

Proof. If $h_K = 1$ then every ideal is principal so $\mathcal{O}_K$ is a principal ideal domain and every principal ideal domain is a unique factorisation domain.
For the other direction, suppose that D is a unique factorisation domain and let $\mathfrak{p} \subset D$ be a non-zero prime ideal. Let $x \in \mathfrak{p}$ be non-zero. Since D is a unique factorisation domain, we have $x = p_1^{r_1} \dots p_n^{r_n}$ where the $r_i \in \mathbb{N}$ and the p_i are irreducible elements of D. Now, as $\mathfrak{p}$ is a prime ideal and $x \in \mathfrak{p}$, we must have one of the $p_i \in \mathfrak{p}$, so that $(p_i) \subseteq \mathfrak{p}$. But any ideal generated by an irreducible element in a unique factorisation domain is prime, so that (p_i) is a prime ideal, and since any prime ideal in a Dedekind domain is a maximal ideal, we must have that $(p_i) = \mathfrak{p}$. Finally, note that every ideal in a Dedekind domain is built from products of prime ideals, and so since we have just shown that every prime ideal is principal, we must have that every ideal is principal, i.e. D is a principal ideal domain, and hence $h_K = 1$. □

It is not immediately clear that h_K should even be finite, however in the case of $\mathcal{O}_K$ for some number field K, this is true, which we quote from [8].

Theorem 3.5. *Let K be a number field of degree n and let $\mathcal{O}_K$ be its ring of integers. Then $\mathrm{Cl}(K)$ is a finite group.*

Proof. We begin by showing that there is a constant $C > 0$ such that for an ideal $\mathfrak{a} \subset \mathcal{O}_K$ there is an $\alpha \in \mathfrak{a}$ such that $|N(\alpha)| \leq CN(\mathfrak{a})$.
Since $\mathcal{O}_K$ is a free $\mathbb{Z}$-module we have a basis, say $\{b_1, \dots, b_n\}$. We shall use the n complex embeddings $\sigma_1, \dots, \sigma_n : K \to \mathbb{C}$. The norm of an element $x \in K$ was defined in Section 2 as

$$N(x) = \prod_{i=1}^{n} \sigma_i(x).$$

Since $x = c_1 b_1 + c_2 b_2 + \cdots + c_n b_n$, with the $c_i \in \mathbb{Q}$, we have

$$\begin{aligned} |N(x)| &= \prod_{i=1}^{n} |\sigma_i(x)| \\ &= \prod_{j=1}^{n} \left| \sum_{i=1}^{n} c_i \sigma_j(b_i) \right| \\ &\leq \prod_{j=1}^{n} \sum_{i=1}^{n} |c_i||\sigma_j(b_i)| \\ &\leq (\max|c_i|)^n \underbrace{\prod_{j=1}^{n} \left(\sum_{i=1}^{n} |\sigma_j(b_i)| \right)}_{\text{call this } C}. \end{aligned}$$

For any ideal $\mathfrak{a} \subseteq \mathcal{O}_K$ we have $k^n \leq N(\mathfrak{a}) < (k+1)^n$ for some $k \in \mathbb{Z}$. Consider the set

$$S = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in \mathbb{Z},\ 0 \leq a_i \leq k. \right\}.$$

Then $|S| = (k+1)^n$ and so

$$\sum_{i=1}^{n} a_i b_i \equiv \sum_{i=1}^{n} a_i' b_i \bmod \mathfrak{a}$$

with $a_i \neq a_i'$ for some i and $0 \leq a_i, a_i' \leq k$, by the pigeonhole principle. Hence, we have

$$\sum_{i=1}^{n}(a_i - a_i')b_i \equiv 0 \bmod \mathfrak{a}.$$

Letting $c_i = a_i - a_i'$ we have

$$\sum_{i=1}^{n} c_i b_i \in \mathfrak{a}.$$

Let $\alpha = \sum_{i=1}^{n} c_i b_i$. Then $\alpha \neq 0$ and

$$|N(\alpha)| \leq (\max|c_i|)^n C \leq k^n C \leq CN(\mathfrak{a}).$$

Now we prove that the ideal class group is finite. First, we show that there are only finitely many integral ideals $\mathfrak{a} \subset \mathcal{O}_K$ with $N(\mathfrak{a}) = k$ for some $k \in \mathbb{Z}^+$. First, note that $N(\mathfrak{a}) = k = |\mathcal{O}_K/\mathfrak{a}|$, so by Lagrange's theorem from group theory, we have $k \in \mathfrak{a}$, and thus $(k) \subset \mathfrak{a}$, that is, $\mathfrak{a} \mid (k)$. Since $\mathcal{O}_K$ is a Dedekind domain we have prime ideals $\mathfrak{p}_i$ such that

$$(k) = \mathfrak{p}_1^{r_1} \dots \mathfrak{p}_n^{r_n}$$

and since $\mathfrak{a} \mid (k)$ we have

$$\mathfrak{a} = \mathfrak{p}_1^{s_1} \dots \mathfrak{p}_n^{s_n}$$

with $s_i \in \{0, \dots, r_i\}$ for $i = 1, \dots, n$. Hence, there are at most $(r_1+1)(r_2+1)\dots(r_n+1)$ possibilities for $\mathfrak{a}$. That is, there are at most $(r_1 + 1)\dots(r_n + 1)$ integral ideals $\mathfrak{a}$ that have norm k. We combine these two results to prove that $\mathrm{Cl}(K)$ is finite.

Denote by $[\mathfrak{b}]$ the class of the ideal $\mathfrak{b}$ in $\mathrm{Cl}(K)$ and let $\mathfrak{a}$ be an ideal in $[\mathfrak{b}]^{-1}$ so that $\mathfrak{a}^{-1} \in [\mathfrak{b}]$. Take an element $\alpha \in \mathfrak{a}$ so that $(\alpha) \subseteq \mathfrak{a}$ and hence $\mathfrak{a} \mid (\alpha)$. Thus, $\mathfrak{b} = (\alpha)\mathfrak{a}^{-1}$ is an integral ideal in the class $[\mathfrak{b}]$, and $N(\mathfrak{b}) = N((\alpha)\mathfrak{a}^{-1}) = |N(\alpha)|N(\mathfrak{a})^{-1} \leq C$, where C is the bound given in the first part of the proof. It follows, then, that each ideal class $[\mathfrak{b}]$ is represented by an integral ideal of $\mathcal{O}_K$ with norm less than C, and so there are only finitely many ideal classes, and so the ideal class group is finite. □

Thus, we have shown that there can only be finitely many representatives for a given ideal class. To conclude, note that every ideal in a Dedekind domain is a product of prime ideals, and so it suffices for the generation of the ideal class group to only look at prime ideals of norm at most C, as given in Theorem 3.5.

The main use for the bound C in Theorem 3.5 was showing that the ideal class group is finite. In practice, we use a much tighter bound called the *Minkowski bound*, whose derivation is a little more involved and is presented in [3, p.300-310].

Definition 3.9. *Let K be a number field of degree $n = r_1 + 2r_2$, where r_1 is the number of real embeddings of K and r_2 the number of pairs of complex embeddings. Let d_K be the discriminant of K. We define the **Minkowski bound** to be the real number*

$$M_K = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}.$$

The bound M_K functions the same way as the bound C in Theorem 3.5, but drastically reduces the number of ideals we need to check to determine the structure of $\mathrm{Cl}(K)$. As an example, if $K = \mathbb{Q}(\sqrt{-5})$ then $C = (1 + \sqrt{5})^2 \approx 10.47$, while $M_K \approx 2.85$. In the first case, we would have to check prime ideals lying above $2, 3, 5$, and 7, while in the second case we need only check prime ideals lying above 2. We present some ideal class group computations using the Minkowski bound.

Example 3.6. *Let $K = \mathbb{Q}(\sqrt{78})$. As $78 \equiv 2 \bmod 4$, the full ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\sqrt{78}]$. We now compute the ideal class group of K using the Minkowski bound.*
First we need to calculate some invariants of K. Since K is quadratic, we have $[K : \mathbb{Q}] = 2$, and the discriminant of K is $d_K = 4 \cdot 78$. Hence, the Minkowski bound for K is $M_K \approx 8.83...$ and so $\mathrm{Cl}(K)$ is at most generated by primes of K lying above $2, 3, 5$, and 7. In order to determine how these primes look in $\mathrm{Cl}(K)$, we need to find the prime ideal factorisation of the ideals $(2), (3), (5)$, and (7) in $\mathcal{O}_K$. These are easily found in analogy with the factorisation of the minimal polynomial of $\sqrt{78}$ modulo each of these primes. The following table summarises these factorisations:

p	*Factorisation* $\mathrm{mod} p$	*Result*	*Norms*
2	X^2	$(2) = \mathfrak{p}_2^2$	$N(\mathfrak{p}_2) = 2$
3	X^2	$(3) = \mathfrak{p}_3^2$	$N(\mathfrak{p}_3) = 3$
5	$X^2 + 2$	$(5) = \mathfrak{p}_5$	$N(\mathfrak{p}_5) = 25$
7	$(X-1)(X+1)$	$(7) = \mathfrak{p}_7\overline{\mathfrak{p}}_7$	$N(\mathfrak{p}_7) = N(\overline{\mathfrak{p}}_7) = 7$

.

In order to determine the structure of $\mathrm{Cl}(K)$ we need to establish relations between each of the primes in the table. Firstly, note that since (5) remains prime in $\mathcal{O}_K$, the ideal class of $\mathfrak{p}_5$ is trivial. Next, we have the relations $\mathfrak{p}_2^2 \sim 1$, $\mathfrak{p}_3^2 \sim 1$, and $\mathfrak{p}_7\overline{\mathfrak{p}}_7 \sim 1$. The element $\alpha = 8 + \sqrt{78}$ has norm $N(\alpha) = -14 = -(2 \cdot 7)$ we have that $N((8 + \sqrt{78})) = N(\mathfrak{p}_2)N(\mathfrak{p}_7)$ and so $(8 + \sqrt{78}) = \mathfrak{p}_2\mathfrak{p}_7$. Since this is principal, we obtain the relation $\mathfrak{p}_2 \sim \mathfrak{p}_7^{-1}$, and so we may eliminate $[\mathfrak{p}_7]$ and $[\overline{\mathfrak{p}}_7]$ from the generating set of $\mathrm{Cl}(K)$. Now, notice that there is an element of norm 3 in $\mathcal{O}_K$, namely, $N(9 + \sqrt{78}) = 3$, so that $\mathfrak{p}_3$ is principal. Finally, notice that the norm equation $a^2 - 78b^2 = 2$ has no solutions in $\mathbb{Z}$, since $a^2 \equiv 2 \bmod 78$ has no solutions, and so $\mathfrak{p}_2$ is non-principal. Hence, we conclude that $\mathrm{Cl}(K) = \langle [\mathfrak{p}_2] \rangle \cong \mathbb{Z}/(2)$.

4 Fermat's Last Theorem for Regular Primes

In this Section we present a partial proof of Fermat's Last Theorem. The proof uses the ideas of Kummer, albeit in more modern language. Indeed, when Kummer first came up with his proof the language of ideals did not exist, and he instead used the language of *ideal numbers*. A more detailed account of Kummer's original ideas can be found in [2]. We first introduce the crucial property of regularity, for which regular primes are named.

Definition 4.1. *Let p be a rational prime and let $K = \mathbb{Q}(\zeta_p)$, where $\zeta_p \neq 1$ is a pth root of unity. Then p is said to be a **regular prime** if $p \nmid h_K$.*

Here, we follow a proof given in [9]. We first require a few lemmas.

Lemma 4.1. *In $\mathbb{Z}[\zeta_p]$, the numbers $1 - \zeta_p, 1 - \zeta_p^2, \ldots, 1 - \zeta_p^{p-1}$ differ only by a unit, and $1 + \zeta_p$ is a unit. Also, $p = u(1 - \zeta_p)^{p-1}$ for some unit u and $(1 - \zeta_p)$ is the only prime ideal of $\mathbb{Z}[\zeta_p]$ lying above p.*

Proof. For any $1 \leq j \leq p-1$ we have

$$\frac{1-\zeta_p^j}{1-\zeta_p} = 1 + \zeta_p + \cdots + \zeta_p^{j-1} \in \mathbb{Z}[\zeta_p].$$

In addition, since $p \nmid j$, we may write $jj' \equiv 1 \bmod p$, and hence

$$\frac{1-\zeta_p}{1-\zeta_p^j} = \frac{1-\zeta_p^{jj'}}{1-\zeta_p^j} \in \mathbb{Z}[\zeta_p^j]$$

and since $\mathbb{Z}[\zeta_p^j] = \mathbb{Z}[\zeta_p]$, we have that the inverse of $\frac{1-\zeta_p^j}{1-\zeta_p}$ is also in $\mathbb{Z}[\zeta_p]$, so the two are units. Thus, writing $\frac{1-\zeta_p^j}{1-\zeta_p}(1-\zeta_p)$ we see that $1-\zeta_p^j$ is a unit multiple of $1-\zeta_p$ for any $1 \leq j \leq p-1$. Letting $j=2$ gives us that $1+\zeta_p$ is a unit.
The minimal polynomial of ζ_p over $\mathbb{Q}$ is $\Phi_p(X) = 1 + X + \cdots + X^{p-1}$, so in $\mathbb{Q}(\zeta_p)$ (the splitting field of $\Phi_p(X)$) we have

$$\Phi_p(X) = 1 + X + \cdots + X^{p-1} = \prod_{i=1}^{p-1}(X - \zeta_p^i).$$

Setting $X=1$ gives

$$\Phi_p(1) = p = \prod_{i=1}^{p-1}(1 - \zeta_p^i)$$

and so the previous argument shows that $p = u(1-\zeta_p)^{p-1}$. Thus, as ideals, we have $(p) = (1-\zeta_p)^{p-1}$. The properties of prime splitting that we discussed in the previous Section show that, since $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$, this must be a prime decomposition, and so $(1-\zeta_p)$ is a prime ideal, and is the only prime ideal dividing p. □

Lemma 4.2. *Let $\alpha \in \mathbb{C}$ be an algebraic number such that all of the conjugates of α have absolute value 1. Then α is a root of unity.*

Proof. Let $T(X) \in \mathbb{Z}[X]$ be an irreducible polynomial such that

$$T(X) = \prod_{i=1}^{n}(X - \alpha_i)$$

in some splitting field of $T(X)$. Consider, for $k \geq 1$, the polynomials

$$T_k(X) = \prod_{i=1}^{n}(X - \alpha_i^k).$$

Then the coefficients of $T_k(X)$ are symmetric polynomials in the α_i with integer coefficients. Since $|\alpha_i^k| = |\alpha_i|^k = 1$, the triangle inequality gives us a bound on the coefficient of X^{n-m} in $T_k(X)$, namely $\binom{n}{m}$. Hence, since the coefficients are integers, there are only finitely many $T_k(X)$ and so there are only finitely many distinct values for α_i^k, so there exists i and $k_1 \neq k_2$ such that

$$\alpha_i^{k_1} = \alpha_i^{k_2}$$

and so $\alpha_i^{k_1-k_2} = 1$. Thus, α_i is a root of unity, and it follows that all the conjugates of α_i are roots of unity. □

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and denote by $\bar{\cdot}$ complex conjugation (which is also an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$). Then, since $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is Abelian, we have $\sigma(\overline{u}) = \overline{\sigma(u)}$. Given any $u \in \mathbb{Z}[\zeta_p]^\times$, we have that $u/\overline{u}$ has absolute value 1, and so if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, we have that $\sigma(u)/\sigma(\overline{u}) = \sigma(u)/\overline{\sigma(u)}$ has absolute value 1. Since these are exactly the $\mathbb{Q}$-conjugates of $u/\overline{u}$, Lemma 4.2 tells us that $u/\overline{u}$ is a root of unity, and so $u/\overline{u} = \pm\zeta_p^k$ for some $k \in \mathbb{Z}$. We now show that the sign is actually $+$. Suppose $u \in \mathbb{Z}[\zeta_p]^\times$ and write $u = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$. Since $\zeta_p \equiv 1 \bmod (1-\zeta_p)$ we must have

$$u \equiv a_0 + a_1 + \cdots + a_{p-2} \bmod (1-\zeta_p).$$

In the same way, since we showed above that $1-\zeta_p$ and $1-\zeta_p^{p-1} = 1-\overline{\zeta_p}$ are associates, we must have

$$\overline{u} \equiv a_0 + a_1 + \cdots + a_{p-2} \bmod (1-\zeta_p).$$

Thus, if $u \equiv -\zeta_p^k\overline{u}$ then we have

$$\overline{u} \equiv u \equiv -\zeta_p^k\overline{u} \equiv -\overline{u} \bmod (1-\zeta_p).$$

But then $2\overline{u} \in (1-\zeta_p)$, a prime ideal, and since neither $p \neq 2$, $2 \notin (1-\zeta_p)$ and $\overline{u}$ is a unit so certainly $\overline{u} \notin (1-\zeta_p)$, this is a contradiction.

Lemma 4.3 (Kummer's Lemma)**.** *Let u be a unit in $\mathbb{Z}[\zeta_p]$. If $u \equiv k \bmod p$ for some rational integer k and p a regular prime then in fact $u = v^p$ for some other $v \in \mathbb{Z}[\zeta_p]^\times$.*

Proof. The proof of this requires a lot of machinery from p-adic analysis, and thus won't be discussed here. A proof can be found in [10] □

We are now ready to prove Fermat's Last Theorem for regular primes. The proof will be divided into two cases. In the first case, we shall assume that $p \nmid xyz$, while in the second case we shall relax this assumption.

4.1 The First Case

Theorem 4.1. *Let p be a regular prime. Then the equation $x^p + y^p = z^p$ has no solutions in integers with $p \nmid xyz$.*

Proof. First, note that we may assume for any solution that $x \not\equiv y \bmod p$. If not, that is, if $x \equiv y \bmod p$, then $z^p \equiv z \equiv x^p + y^p \equiv 2x \bmod p$, so $z \equiv 2x \bmod p$. Now, take a new solution $x' = x$, $y' = -z$ and $z' = -y$. Then $y' = -z \equiv -2x \bmod p$, so if $x' \equiv y'$ then $x \equiv -2x \bmod p$ so that $p \mid 3x$. But $p \geq 5$ and $p \nmid xyz$, so this cannot happen. Hence, given any solution (x, y, z) we may transform to a solution for which $x \not\equiv y \bmod p$.
We now look to the factorisation of $x^p + y^p$ in $\mathbb{Z}[\zeta_p]$. We have

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

We shall show that any pair of ideals $(x + \zeta_p^i y)$ and $(x + \zeta_p^j y)$ are coprime. Suppose that $\mathfrak{p} \subset \mathbb{Z}[\zeta_p]$ is a prime ideal dividing both $(x + \zeta_p^i y)$ and $(x + \zeta_p^j y)$. Then $\mathfrak{p}$ also divides the ideals

$$((x + \zeta_p^j y) - (x + \zeta_p^i y)) = ((\zeta_p^j - \zeta_p^i)y)$$

and

$$((x+\zeta_p^j y)-\zeta_p^{j-i}(x+\zeta_p^i y))=((1-\zeta_p^{j-i})x).$$

Now, notice that $\zeta_p^j-\zeta_p^i=\zeta_p^j(1-\zeta_p^{i-j})$ and $1-\zeta_p^{j-i}$ are both a unit away from $1-\zeta_p$. Hence, we have that $\mathfrak{p}$ divides the ideals $(1-\zeta_p)(x)$ and $(1-\zeta_p)(y)$. Since x and y were assumed coprime, we must have that $\mathfrak{p}\mid(1-\zeta_p)$, but $(1-\zeta_p)$ is prime, and so we conclude that $\mathfrak{p}=(1-\zeta_p)$. Suppose then that $(1-\zeta_p)\mid(x+\zeta_p^i y)$ and $(1-\zeta_p)\mid(x+\zeta_p^j y)$ as ideals. Then, since these are principal ideals, we must have

$$x+\zeta_p^i y\equiv 0 \bmod 1-\zeta_p.$$

Notice, in addition, that $1-\zeta_p\mid 1-\zeta_p^i$ (as elements), and so $\zeta_p^i\equiv 1 \bmod 1-\zeta_p$, allowing us to conclude that

$$x+y\equiv 0 \bmod 1-\zeta_p$$

and hence that $x+y\in(1-\zeta_p)$. Now, since $(1-\zeta_p)$ is a prime ideal lying above the prime ideal $p\mathbb{Z}$, we have $(1-\zeta_p)\mathbb{Z}[\zeta_p]\cap\mathbb{Z}=p\mathbb{Z}$, and since $x+y\in\mathbb{Z}$ we have $x+y\in p\mathbb{Z}$, so that $p\mid x+y$. But $x+y\equiv x^p+y^p\equiv z^p \bmod p$, and so $p\mid z^p$, and as a result we have $p\mid z$, contradicting that $p\nmid xyz$. Hence, $(x+\zeta_p^i y)$ and $(x+\zeta_p^j y)$ are coprime ideals for $i\neq j$.

We now use the fact that $\mathbb{Z}[\zeta_p]$ is the ring of integers of the number field $\mathbb{Q}(\zeta_p)$ to note that, since $\mathbb{Z}[\zeta_p]$ is a Dedekind domain, every ideal has a unique factorisation into a product of prime ideals. Consider the factorisation

$$(z)=\mathfrak{p}_1^{e_1}\dots\mathfrak{p}_g^{e_g}$$

where the $\mathfrak{p}_i$ are pairwise distinct prime ideals in $\mathbb{Z}[\zeta_p]$ and the $e_i\in\mathbb{N}$. Then

$$(z)^p=\mathfrak{p}_1^{pe_1}\dots\mathfrak{p}_g^{pe_g}$$

and so

$$(x+y)(x+\zeta_p y)\dots(x+\zeta_p^{p-1}y)=\mathfrak{p}_1^{pe_1}\dots\mathfrak{p}_g^{pe_g}.$$

Now, since the ideals on the left-hand side are pairwise coprime, each prime factor on the right-hand side can occur in the prime factorisation of exactly one of the ideals on the left hand side, so that, for example

$$(x+\zeta_p^i y)=\mathfrak{p}_1^{pe_1}\dots\mathfrak{p}_s^{pe_s}=(\mathfrak{p}_1^{e_1}\dots\mathfrak{p}_s^{e_s})^p=\mathfrak{a}_i^p$$

with $s<g$. Hence $(x+\zeta_p^i y)$ is the pth power of some ideal $\mathfrak{a}_i\subset\mathbb{Z}[\zeta_p]$ with $(z)=\mathfrak{a}_1\dots\mathfrak{a}_r$. This is where the regularity assumption on p is used; since $p\nmid h_K$, there are no ideal classes of order p in $\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ and so the fact that $\mathfrak{a}_i^p$ is principal implies that $\mathfrak{a}_i$ is itself principal. Let $\mathfrak{a}_i=(\alpha_i)$ with $\alpha_i\in\mathbb{Z}[\zeta_p]$, so that

$$(x+\zeta_p^i y)=(\alpha_i)^p.$$

Then we may pass to elements and write $x+\zeta_p^i y=u\alpha_i^p$ for some $u\in\mathbb{Z}[\zeta_p]^\times$.

We now show that α_i^p is congruent to a rational integer modulo p. Since $\{1,\zeta_p,\dots,\zeta_p^{p-2}\}$ is an integral basis for $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$ we have

$$\alpha_i^p=(a_0+a_1\zeta_p+\dots+a_{p-2}\zeta_p^{p-2})^p$$

for some $a_i \in \mathbb{Z}$. Now, since p divides all of the binomial coefficients $\binom{p}{k}$ with $k \neq 0, p$, we have

$$\alpha_i^p \equiv a_0^p + a_1^p\zeta_p^p + \cdots + a_{p-2}^p\zeta_p^{p(p-2)} \bmod p$$

and since $\zeta_p^{jp} = 1$, we have

$$\alpha_i^p \equiv a_0^p + a_1^p + \cdots + a_{p-2}^p \bmod p.$$

In particular, $\alpha_i^p \equiv \overline{\alpha_i}^p \bmod p$ since rational integers are fixed by complex conjugation. We know that $u/\overline{u} = \zeta_p^j$ for some $0 \leq j \leq p-1$. Thus, we have

$$x + \zeta_p y = u\alpha_1^p = \zeta_p^j\overline{u}\alpha_i^p \equiv \zeta_p^j\overline{u\alpha_i}^p \bmod p \equiv \zeta_p^j(x + \zeta_p^{p-1}y) \bmod p.$$

In summary, since $\zeta_p^{p-1} = \zeta_p^{-1}$, we have

$$x + \zeta_p y - \zeta_p^{j-1}y - \zeta_p^j x \equiv 0 \bmod p$$

when $u/\overline{u} = \zeta_p^j$. We wish to show that this congruence cannot hold. At the start of Section 3 we showed that $\mathcal{O}_{\mathbb{Q}(\zeta_p)}/p\mathcal{O}_{\mathbb{Q}(\zeta_p)} \cong (\mathbb{Z}/p\mathbb{Z})^{p-1}$ by showing that, given a basis $\{b_1, \ldots, b_{p-1}\}$, we could construct a set $\{b_1 + p\mathcal{O}_{\mathbb{Q}(\zeta_p)}, \ldots, b_{p-1} + p\mathcal{O}_{\mathbb{Q}(\zeta_p)}\}$ of $\mathbb{Z}/p\mathbb{Z}$-linearly independent elements which spanned $\mathcal{O}_{\mathbb{Q}(\zeta_p)}/p\mathcal{O}_{\mathbb{Q}(\zeta_p)}$. Since $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$ are a basis for $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$, this shows that $\{1 + p\mathcal{O}_{\mathbb{Q}(\zeta_p)}, \zeta_p + p\mathcal{O}_{\mathbb{Q}(\zeta_p)}, \ldots, \zeta_p^{p-2} + p\mathcal{O}_{\mathbb{Q}(\zeta_p)}\}$ is a $\mathbb{Z}/p\mathbb{Z}$-linearly independent set, and so neither of the congruences from above can hold if $0, 1, j-1$ and j are all distinct. If $j = 0, 1, 2,$ or $p-1$ then this can break down, since, for example, if $j = 1$ then $0 = j - 1$. We shall account for all of these possibilities and show that, in every case, we reach a contradiction.

$\underline{j = 0}$: If $j = 0$ then we have

$$x + \zeta_p y - \zeta_p^{-1}y - x \equiv y(\zeta_p - \zeta_p^{-1}) \bmod p.$$

Since $p \nmid y$ we may divide by y to obtain

$$\zeta_p \equiv \zeta_p^{-1} \bmod p$$

and hence $\zeta_p^2 - 1 \equiv 0 \bmod p$, contradicting the $\mathbb{Z}/p\mathbb{Z}$-linear independence of 1 and ζ_p^2.

$\underline{j = 1}$: If $j = 1$ then we have

$$x(1 - \zeta_p) \equiv y(1 - \zeta_p) \bmod p.$$

Writing $p = u(1 - \zeta_p)^{p-1}$ for some unit u, we thus have

$$x \equiv y \bmod (1 - \zeta_p)^{p-2}$$

so that $(1 - \zeta_p)^{p-2} \mid x - y$, and so certainly $1 - \zeta_p \mid x - y$ and hence $x - y \in (1 - \zeta_p)$. But $x - y \in \mathbb{Z}$ and $(1 - \zeta_p) \cap \mathbb{Z} = (p)$, so $x \equiv y \bmod p$, a possibility that we ruled out at the start of the proof.

$\underline{j = 2}$: If $j = 2$ then we have

$$x + \zeta_p y - \zeta_p y - \zeta_p^2 x \equiv x - \zeta_p^2 x \equiv 0 \bmod p$$

and this, again, contradicts the linear independence of 1 and ζ_p^2.

$\underline{j = p-1}$: If $j = p-1$ then

$$x + \zeta_p y - \zeta_p^{p-2} y - \zeta_p^{p-1} x \equiv 0 \bmod p.$$

Now notice that $\zeta_p^{p-1} = -(1 + \zeta_p + \cdots + \zeta_p^{p-2})$ so

$$x + \zeta_p y - \zeta_p^{p-2} y + (1 + \zeta_p + \cdots + \zeta_p^{p-2}) x \equiv 0 \bmod p$$

which contradicts the $\mathbb{Z}/p\mathbb{Z}$-linear independence of the ζ_p^i.

Thus, we have dealt with all possibilities and have shown that no solution to $x^p + y^p = z^p$ can exist in integers prime to p. □

4.2 The Second Case

Theorem 4.2. *Let p be a regular prime. Then the equation*

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

has no solutions $x, y, z \in \mathbb{Z}$ with $p \mid z$.

Proof. Since p is an odd prime (Fermat's equation is true for $p = 2$!), for any solution $(x, y, z) \in \mathbb{Z}^3$ we also have

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

and so under $z \mapsto -z$, we make use of this symmetry and instead prove a statement similar to

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

First, note that we may assume that $p \mid z$ but $p \nmid x, y$, since if $p \mid z$ and $p \mid x$, say, then since $x^p + z^p = -y^p$, we have $p \mid y$, and so we may expel this factor of p. We prove, instead, the following stronger statement:

> *Let p be a regular prime. Then the equation*
>
> $$\alpha^p + \beta^p + u(1 - \zeta_p)^{np} \gamma^p = 0$$
>
> *has no solutions with $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta_p]$ all prime to $1 - \zeta_p$ and $u \in \mathbb{Z}[\zeta_p]^\times$.*

The strategy will be similar to that of the first case, but in this case we note that the ideals $(\alpha + \beta), (\alpha + \zeta_p \beta), \ldots, (\alpha + \zeta_p^{p-1} \beta)$ will no longer be coprime, and so a closer examination of their prime decomposition will be necessary. In the same vain as in the first case, we make the following observation: given a solution (α, β, γ), we have the ideal equation

$$\prod_{i=0}^{p-1} (\alpha + \zeta_p^i \beta) = (1 - \zeta_p)^{pn} (\gamma)^p.$$

Now, since $\zeta_p \equiv 1 \bmod 1 - \zeta_p$, we have that $\alpha + \zeta_p^i \beta \equiv \alpha + \beta \bmod 1 - \zeta_p$, so that all of the $\alpha + \zeta_p^i \beta$ are congruent modulo $1 - \zeta_p$. Hence, if one of the $\alpha + \zeta_p^i \beta$ is divisible by $1 - \zeta_p$ then all of them are. Indeed, by the ideal equation above, since α, β, γ are pairwise coprime, we must have that all of the $\alpha + \zeta_p^i \beta$ are divisible by $1 - \zeta_p$.

Suppose now that there exist i, i' with $i' > i$ such that $\alpha + \zeta_p^i \beta \equiv \alpha + \zeta_p^{i'} \beta \bmod (1 - \zeta_p)^2$. Then $\zeta_p^i \beta (1 - \zeta_p^{i'-i}) \equiv 0 \bmod (1 - \zeta_p)^2$. Now, ζ_p^i is a unit and $1 - \zeta_p^{i'-i}$ is an associate of $1 - \zeta_p$, so this must imply that $(1 - \zeta_p)^2 \mid \beta$, and hence that $(1 - \zeta_p) \mid \beta$, contradicting the assumption that β is prime to $1 - \zeta_p$. Given any number $\delta(1 - \zeta_p)$, considered modulo $(1 - \zeta_p)^2$, we care about δ only up to multiples of $1 - \zeta_p$, since if $1 - \zeta_p \mid \delta$ then $\delta(1 - \zeta_p) \equiv 0 \bmod (1 - \zeta_p)^2$. Recalling that $(p) = (1 - \zeta_p)^{p-1}$ as ideals, we have that $N(p) = p^{p-1} = N(1 - \zeta_p)^{p-1}$, and so $N(1 - \zeta_p) = p$, so that the inertial degree of $(1 - \zeta_p)$ over (p) is 1, and we conclude that $\mathbb{Z}[\zeta_p]/(1 - \zeta_p) \cong \mathbb{Z}/(p)$, and hence that there are only p multiples of $1 - \zeta_p$ modulo $(1 - \zeta_p)^2$. From above, we saw that all of the $\alpha + \zeta_p^i \beta$ are distinct modulo $(1 - \zeta_p)^2$, and so we must have that one of these is congruent to 0 modulo $(1 - \zeta_p)^2$. Hence, we have that all of the terms on the left-hand side of the ideal equation above are divisible by $1 - \zeta_p$, and exactly one of them is divisible by $(1 - \zeta_p)^2$, and so $n \neq 1$.

We wish then to prove the statement for some $n > 1$. The strategy is to take n to be minimal for the solution (α, β, γ), and to then construct a new solution $(\alpha', \beta', \gamma')$ in such a way that

$$(\alpha')^p + (\beta')^p + v(1 - \zeta_p)^{p(n-1)}(\gamma')^p = 0,$$

with α', β', γ' prime to $1 - \zeta_p$ and $v \in \mathbb{Z}[\zeta_p]^\times$. This new solution contradicts the minimality that we built into n and thus proves that no solution can exist.

If $\alpha + \zeta_p^i \beta$ is the term on the left hand side of the ideal equation above then we may replace $\zeta_p^i \beta$ with β (since $\zeta_p \equiv 1 \bmod 1 - \zeta_p$) and so we may safely assume that $\alpha + \beta \equiv 0 \bmod (1 - \zeta_p)^2$ and that $\alpha + \zeta_p^i \beta \not\equiv 0 \bmod (1 - \zeta_p)^2$ for any $1 \leq j \leq p - 1$. Let $\mathfrak{d} = (\alpha, \beta)$, that is, the ideal generated by α and β. Then certainly $\mathfrak{d} \mid (\alpha + \zeta_p^i \beta)$ for any i, since $\mathfrak{d} = \{r_1 \alpha + r_2 \beta : r_1, r_2 \in \mathbb{Z}[\zeta_p]\}$, and so taking $r_1 = 1$ and $r_2 = \zeta_p^i$, we have that $\alpha + \zeta_p^i \beta \in \mathfrak{d}$ and hence $(\alpha + \zeta_p^i \beta) \subseteq \mathfrak{d}$. Finally, since $(1 - \zeta_p) \mid (\alpha + \zeta_p^i \beta)$ (as ideals) but $(1 - \zeta_p)^2 \mid (\alpha + \beta)$ only, we have that $\mathfrak{d}(1 - \zeta_p)$ is the smallest ideal containing all of the ideals $(\alpha + \zeta_p^i \beta)$, and hence this is the greatest common divisor of all of the $(\alpha + \zeta_p^i \beta)$. Furthermore, we make the observation that

$$(1 - \zeta_p)^{np} \mid \prod_{i=0}^{p-1} (\alpha + \zeta_p^i \beta)$$

and since $(1 - \zeta_p)$ divides each of the $(\alpha + \zeta_p^i \beta)$, with $i > 0$, only once, we have that

$$(1 - \zeta_p)^{p-1} \mid \prod_{i=1}^{p-1} (\alpha + \zeta_p^i \beta).$$

We conclude, thus, that $(1 - \zeta_p)^{np-(p-1)} \mid (\alpha + \beta)$. Hence, we write

$$\begin{aligned} (\alpha + \beta) &= \mathfrak{d}(1 - \zeta_p)^{np-p+1}\mathfrak{I}_0 \\ (\alpha + \zeta_p \beta) &= \mathfrak{d}(1 - \zeta_p)\mathfrak{I}_1 \\ &\vdots \\ (\alpha + \zeta_p^{p-1} \beta) &= \mathfrak{d}(1 - \zeta_p)\mathfrak{I}_{p-1} \end{aligned}$$

where the $\mathfrak{I}_i$ are pairwise coprime (since $\mathfrak{d}(1 - \zeta_p)$ is the greatest common divisor of any two $(\alpha + \zeta_p^i \beta)$). Thus, the ideal equation gives us that each of the $\mathfrak{I}_i$ is the pth power of some ideal, say $\mathfrak{I}_i = \mathfrak{a}_i^p$. Suppose then that we take the ratio of $(\alpha + \zeta_p^i \beta)$ and $(\alpha + \beta)$. Then we have the (fractional) ideal equation

$$(\alpha + \zeta_p^i \beta)(\alpha + \beta)^{-1} = (1 - \zeta_p)^{p(1-n)} \mathfrak{a}_i^p \mathfrak{a}_0^{-p}$$

and hence

$$\left(\frac{(\alpha + \zeta_p^i \beta)(1 - \zeta_p)^{p(n-1)}}{\alpha + \beta} \right) = \mathfrak{a}_i^p \mathfrak{a}_0^{-p}$$

showing that $\mathfrak{a}_i^p \mathfrak{a}_0^{-p}$ is a principal fractional ideal. Thus, by the regularity of p, we must have that $\mathfrak{a}_i \mathfrak{a}_0^{-1}$ is itself a principal fractional ideal. Choose $x_i \in \mathbb{Q}(\zeta_p)$ such that $(x_i) = \mathfrak{a}_i \mathfrak{a}_0^{-1}$. By the way the $\mathfrak{a}_i$ were defined, we have that $(1 - \zeta_p) \nmid (x_i)$. Hence, we have the ideal equation

$$\left(\frac{(\alpha + \zeta_p^i \beta)(1 - \zeta_p)^{p(n-1)}}{\alpha + \beta} \right) = (x_i).$$

This is an equality of principal ideals, so there exists some unit $u_i \in \mathbb{Z}[\zeta_p]^\times$ such that we may pass to the equation of elements

$$\frac{\alpha + \zeta_p^i \beta}{\alpha + \beta} = \frac{u_i x_i}{(1 - \zeta_p)^{p(n-1)}}.$$

Consider now the relation

$$\zeta_p(\alpha + \zeta_p^{p-1}\beta) + (\alpha + \zeta_p \beta) - (1 + \zeta_p)(\alpha + \beta) = 0.$$

Dividing by $\alpha + \beta$ and using the elemental equation from above we have

$$\frac{\zeta_p u_{p-1} x_{p-1}^p}{(1 - \zeta_p)^{p(n-1)}} + \frac{u_1 x_1^p}{(1 - \zeta_p)^{p(n-1)}} - (1 + \zeta_p) = 0.$$

Clearing denominators, we obtain

$$\zeta_p u_{p-1} x_{p-1}^p + u_1 x_1^p - (1 + \zeta_p)(1 - \zeta_p)^{p(n-1)} = 0.$$

Now, since the $x_i \in \mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_p)$ is the field of fractions of $\mathbb{Z}[\zeta_p]$, we can write x_i as the ratio of a pair of elements from $\mathbb{Z}[\zeta_p]$, with the additional property that $1 - \zeta_p$ not divide either of these elements (since x_i was itself prime to $1 - \zeta_p$). Thus, we write $x_{p-1} = a_{p-1}/b_{p-1}$ and $x_1 = a_1/b_1$ (where, of course, $b_{p-1}, b_1 \neq 0$). Dividing by $\zeta_p u_{p-1}$ and clearing denominators we have

$$(a_{p-1}b_1)^p + \frac{u_1}{\zeta_p u_{p-1}}(a_1 b_{p-1})^p - \frac{1 + \zeta_p}{\zeta_p u_{p-1}}(1 - \zeta_p)^{p(n-1)}(b_1 b_{p-1})^p = 0.$$

Since $a_1, a_{p-1}, b_1, b_{p-1} \in \mathbb{Z}[\zeta_p]$, the product of any pair is also an element of $\mathbb{Z}[\zeta_p]$. Rather suggestively, we let $\alpha' := a_{p-1}b_1$, $\beta' := a_1 b_{p-1}$, and $\gamma' := b_1 b_{p-1}$, so that the equation reads

$$(\alpha')^p + \frac{u_1}{\zeta_p u_{p-1}}(\beta')^p - \frac{1 + \zeta_p}{\zeta_p u_{p-1}}(1 - \zeta_p)^{p(n-1)}(\gamma')^p = 0$$

where α', β', and γ' have been chosen such that none of them is divisible by $1 - \zeta_p$. The coefficients in front of $(\beta'_p)^p$ and $(1 - \zeta_p)^{p(n-1)}(\gamma')^p$ are units, but they aren't quite as we'd like them; in particular, the coefficient of $(\beta'_p)^p$ is not 1, so this is not quite

the equation that we're looking for. We recall from Case 1 that the pth power of a cyclotomic integer is congruent modulo p to a rational integer, and appeal to Kummer's Lemma to rewrite this.
Considered modulo p, there exist non-zero rational integers m_1 and m_2 such that

$$(\alpha')^p \equiv m_1 \bmod p \text{ and } (\beta')^p \equiv m_2 \bmod p.$$

In addition, since we proved that $n > 1$, and using the fact that $p = U(1-\zeta_p)^{p-1}$, the last term in our equation is 0 modulo p, and so we have

$$(\alpha')^p + \frac{u_1}{\zeta_p u_{p-1}}(\beta')^p - \frac{1+\zeta_p}{\zeta_p u_{p-1}}(1-\zeta_p)^{p(n-1)}(\gamma')^p = 0 \equiv m_1 + \frac{u_1}{\zeta_p u_{p-1}} \bmod p.$$

Since m_1, m_2 are non-zero in $\mathbb{Z}/(p)$, and m_2 is invertible modulo p, we have

$$\frac{u_1}{\zeta_p u_{p-1}} \equiv -m_1 m_2' \bmod p.$$

But the left-hand side of this congruence is a unit, and $-m_1 m_2'$ is a rational integer, and so Kummer's Lemma says that $\frac{u_1}{\zeta_{p-1}}$ is in fact equal to the pth power of some unit, say $u \in \mathbb{Z}[\zeta_p]^\times$, so that $\frac{u_1}{\zeta_p u_{p-1}} = u^p$. Thus, we may replace β' with $u\beta'$ to obtain

$$\alpha'^p + \beta'^p + V(1-\zeta_p)^{p(n-1)}\gamma'^p = 0$$

where V is the unit $V = -\frac{(1+\zeta_p)}{\zeta_p u_{p-1}}$. Thus, we have constructed a solution such that α', β', γ' are all prime to $1-\zeta_p$ and we have replaced n by $n-1$. By descent, we conclude that no solution (α, β, γ) could have existed to begin with. Finally, note that if $p \mid z$ then we can write $z = p^k z_0$ where $p \nmid z_0$, and so Fermat's equation becomes

$$x^p + y^p + U(1-\zeta_p)^{kp(p-1)} z_0^p = 0,$$

for some $U \in \mathbb{Z}[\zeta_p]^\times$ and x, y, z_0 prime to $(1-\zeta_p)$, so the proof of the theorem for $\alpha, \beta, \gamma \in \mathbb{Z}[\zeta_p]$ applies in this case. □

Combining the two theorems, we have shown that there exist no integers x, y, z such that

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

where p is a regular prime, hence concluding this Section.

5 The Hilbert Class Field

In this Section we shall deepen our study of factorisation in number fields, as introduced in Section 3. In particular, we shall link this to the Galois theory studied in Section 1 to study some properties of the properties of an Abelian extension H over a number field K such that H is unramified at all primes of K by linking the ideal structure of $\mathcal{O}_K$ to the Galois group $\mathrm{Gal}(H/K)$. First, we introduce some Galois theory specific to number fields. The exposition in this Section follows [7] and [11].

5.1 Decomposition and Inertia Groups

Definition 5.1. *Let K be a number field and L an extension of K. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a non-zero prime ideal and $\mathfrak{P} \subset \mathcal{O}_L$ a non-zero prime ideal such that $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. The **decomposition group** of $\mathfrak{P}$ is the set $Z_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}$.*

It is easy to see that $Z_{\mathfrak{P}} \leq \mathrm{Gal}(L/K)$; if $\sigma, \tau \in Z_{\mathfrak{P}}$ then $\sigma(\mathfrak{P}) = \mathfrak{P}$ and $\tau(\mathfrak{P}) = \mathfrak{P}$, so $\sigma(\mathfrak{P}) = \tau(\mathfrak{P})$, and hence $\tau^{-1} \circ \sigma(\mathfrak{P}) = \mathfrak{P}$, i.e. $\tau^{-1} \circ \sigma \in Z_{\mathfrak{P}}$.
We saw in Section 3 that $\mathrm{Gal}(L/K)$ acts transitively on the primes of $\mathcal{O}_L$ lying over a given prime $\mathfrak{p} \subset \mathcal{O}_K$. The group $Z_{\mathfrak{P}}$ is the stabiliser of the prime $\mathfrak{P}$ under this action. Thus, if there are g primes of $\mathcal{O}_L$ lying over $\mathfrak{p}$ then, by the Orbit-Stabiliser theorem, we have

$$[\mathrm{Gal}(L/K) : Z_{\mathfrak{P}}] = g$$

and so $|\mathrm{Gal}(L/K)| = g|Z_{\mathfrak{P}}|$. Finally, we have $|\mathrm{Gal}(L/K)| = [L : K]$, and we saw in Section 3 that $[L : K] = efg$ where e is the ramification index, f the inertial degree, and g the decomposition number, of the primes $\mathfrak{P}$ of $\mathcal{O}_L$ lying above the prime $\mathfrak{p}$ of $\mathcal{O}_K$. Thus, we conclude that

$$|Z_{\mathfrak{P}}| = ef.$$

Proposition 5.1. *Let L/K be a Galois extension of number fields, let $\mathfrak{P}, \mathfrak{P}' \subset \mathcal{O}_L$ be two primes of $\mathcal{O}_L$ lying above the prime $\mathfrak{p} \subset \mathcal{O}_K$. Then the decomposition groups $Z_{\mathfrak{P}}$ and $Z_{\mathfrak{P}'}$ are conjugate.*

Proof. Let $\sigma, \tau \in \mathrm{Gal}(L/K)$. Then $\tau^{-1}(\sigma(\tau(\mathfrak{P}))) = \mathfrak{P}$ if and only if $\sigma(\tau(\mathfrak{P})) = \tau(\mathfrak{P})$. Thus $\tau^{-1}\sigma\tau \in Z_{\mathfrak{P}}$ if and only if $\sigma \in Z_{\tau(\mathfrak{P})}$. Hence, $\tau^{-1}Z_{\mathfrak{P}}\tau = Z_{\tau(\mathfrak{P})}$. That $\mathrm{Gal}(L/K)$ acts transitively on the primes of $\mathcal{O}_L$ lying over $\mathfrak{p}$ gives us the result. □

Proposition 5.2. *Let L/K be an extension of number fields and let $\mathfrak{P}$ and $\mathfrak{p}$ be non-zero primes of $\mathcal{O}_L$ and $\mathcal{O}_K$ respectively and such that $\mathfrak{P}$ lies over $\mathfrak{p}$. Denote by $\mathbb{F}_{\mathfrak{P}}$ the finite field $\mathcal{O}_L/\mathfrak{P}$ and by $\mathbb{F}_{\mathfrak{p}}$ the finite field $\mathcal{O}_K/\mathfrak{p}$, and recall that the degree of this extension is the natural number $f(\mathfrak{P}/\mathfrak{p})$; the inertial degree of $\mathfrak{P}$ over $\mathfrak{p}$. We have*

(i) $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ is a Galois extension,

(ii) $\sigma(\mathcal{O}_L) = \mathcal{O}_L$ for all $\sigma \in \mathrm{Gal}(L/K)$, and

(iii) for all $\sigma \in Z_{\mathfrak{P}}$ there is a natural action of σ on $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ that fixes $\mathbb{F}_{\mathfrak{p}}$.

Proof. For (i), we note that $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p$ is a finite field of order $p^{f(\mathfrak{P}/p)}$, and so it is the splitting field of the polynomial $X^{p^{f(\mathfrak{P}/p)}} - X \in \mathbb{F}_p[X]$, and is hence Galois. Since $\mathbb{F}_p \subset \mathbb{F}_{\mathfrak{p}} \subset \mathbb{F}_{\mathfrak{P}}$, Galois theory says that $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ is a Galois extension of degree $f(\mathfrak{P}/\mathfrak{p})$ over $\mathbb{F}_{\mathfrak{p}}$.
For (ii), we recall that any element of $\mathcal{O}_L$ satisfies a monic polynomial over $\mathbb{Z}$, so that if $\ell \in \mathcal{O}_L$ we have

$$\ell^n + a_{n-1}\ell^{n-1} + \cdots + a_1\ell + a_0 = 0$$

with the $a_i \in \mathbb{Z}$. Since $\mathrm{Gal}(L/K)$ fixes all of K and $\mathbb{Z} \subset K$, we have

$$\sigma(\ell)^n + a_{n-1}\sigma(\ell)^{n-1} + \cdots + a_1\sigma(\ell) + a_0 = 0$$

and conclude that $\sigma(\ell) \in \mathcal{O}_L$. Thus $\sigma(\mathcal{O}_L) = \mathcal{O}_L$.
For (iii), the elements of $\mathbb{F}_{\mathfrak{P}}$ are cosets $\ell + \mathfrak{P}$ with $\ell \in \mathcal{O}_L$ so if $\sigma \in Z_{\mathfrak{P}}$ then $\sigma(\ell + \mathfrak{P}) = \sigma(\ell) + \mathfrak{P}$, and by (ii) $\sigma(\ell) \in \mathcal{O}_L$. Since $\sigma(\mathfrak{P}) = \mathfrak{P}$ and $\mathfrak{p} \subset \mathcal{O}_K$, we also have $\sigma(\mathfrak{p}) = \mathfrak{p}$. Thus, as the elements of $\mathbb{F}_{\mathfrak{p}}$ are cosets $k + \mathfrak{p}$ with $k \in \mathcal{O}_K$ and $\sigma \in \mathrm{Gal}(L/K)$, we also have that $\sigma(k + \mathfrak{p}) = k + \mathfrak{p}$ and so σ fixes $\mathbb{F}_{\mathfrak{p}}$. □

Part (iii) of Proposition 5.2 tells us that $\sigma \in Z_{\mathfrak{P}}$ induces an $\mathbb{F}_{\mathfrak{p}}$-automorphism $\tilde{\sigma}$, so we may conjecture the existence of a map $Z_{\mathfrak{P}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ with $\sigma \mapsto \tilde{\sigma}$. Indeed, such a map exists, which we will now show with the following theorem from [7, p.15], with suitable specialisation to the case of extensions of number fields.

Theorem 5.1. *Let L/K be an extension of number fields. Let $\mathfrak{P} \subset \mathcal{O}_L$ be a non-zero prime ideal lying above a non-zero prime ideal $\mathfrak{p} \subset \mathcal{O}_K$. Let $\sigma \in Z_{\mathfrak{P}}$. Then there is a surjective homomorphism of groups*

$$\begin{aligned} \varphi : Z_{\mathfrak{P}} &\to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) \\ \sigma &\mapsto \tilde{\sigma}. \end{aligned}$$

The kernel of φ is $T_{\mathfrak{P}} = \{\sigma \in Z_{\mathfrak{P}} : \sigma(\alpha) \equiv \alpha \bmod \mathfrak{P},\ \forall \alpha \in \mathcal{O}_L\}$. In particular, we have that $Z_{\mathfrak{P}}/T_{\mathfrak{P}} \cong \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$.

Proof. We shall first reduce to the case where there is exactly one prime ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$. To do this, we first show that the fixed field of $Z_{\mathfrak{P}}$ is the smallest field in which $\mathfrak{P}$ is the unique prime ideal lying above $\mathfrak{p}$. Following this, we look at the integral closure of $\mathcal{O}_K$ in this field, which we denote $\mathcal{O}_K^{Z_{\mathfrak{P}}}$, and show that $\mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_K^{Z_{\mathfrak{P}}}/\mathfrak{q}$, where $\mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_K^{Z_{\mathfrak{P}}}$. In doing so, we may take $K = K^{Z_{\mathfrak{P}}}$ and $\mathfrak{q} = \mathfrak{p}$.
Let E be a subfield of L such that $K \subset K^{Z_{\mathfrak{P}}} \subset E \subset L$ and such that $\mathfrak{P}$ is the unique prime of L lying above $\mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_E$. Then, by Theorem 3.4, since the primes of L lying above $\mathfrak{q}$ are conjugate under the action of $\mathrm{Gal}(L/E)$, we must have that $\mathfrak{P}$ is fixed under this action, and so $\mathrm{Gal}(L/E) \leq Z_{\mathfrak{P}}$. By the Galois correspondence, this means that $E \supset K^{Z_{\mathfrak{P}}}$, and since E was arbitrary, this proves that $K^{Z_{\mathfrak{P}}}$ is the smallest subfield of L containing K with the desired property.
To show that $\mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_K^{Z_{\mathfrak{P}}}/\mathfrak{q}$, we note that the map $a + \mathfrak{p} \mapsto a + \mathfrak{q}$ is an injection (since $\mathcal{O}_K \subset \mathcal{O}_K^{Z_{\mathfrak{P}}}$ and $\mathfrak{p} \subset \mathfrak{q}$) so it remains only to prove that this map is also a surjection. Suppose that $\sigma \notin Z_{\mathfrak{P}}$ so that $\sigma(\mathfrak{P}) \neq \mathfrak{P}$ and $\sigma^{-1}(\mathfrak{P}) \neq \mathfrak{P}$, and let $\mathfrak{q}_\sigma = \sigma^{-1}(\mathfrak{P}) \cap \mathcal{O}_K^{Z_{\mathfrak{P}}}$. Then $\mathfrak{q} \neq \mathfrak{q}_\sigma$, so the Chinese remainder theorem allows us to find $x, y \in \mathcal{O}_K^{Z_{\mathfrak{P}}}$ such that

$$\begin{aligned} y &\equiv x \bmod \mathfrak{q} \\ y &\equiv 1 \bmod \mathfrak{q}_\sigma \end{aligned}$$

for every $\sigma \notin Z_{\mathfrak{P}}$. Thus, we also have the congruences

$$\begin{aligned} y &\equiv x \bmod \mathfrak{P} \\ y &\equiv 1 \bmod \sigma^{-1}(\mathfrak{P}). \end{aligned}$$

Hence, we also have $\sigma(y) \equiv 1 \bmod \mathfrak{P}$ for every $\sigma \notin Z_{\mathfrak{P}}$. Considering the norm function $N_{K^{Z_{\mathfrak{P}}}/K} : K^{Z_{\mathfrak{P}}} \to K$, since $\mathrm{Aut}(K^{Z_{\mathfrak{P}}}/K) \cap Z_{\mathfrak{P}} = \{\mathrm{id}\}$ (note this extension is not Galois in general), we have that the norm of an element of $K^{Z_{\mathfrak{P}}}/K$ is a product of $\sigma(y)$ with $\sigma \notin Z_{\mathfrak{P}}$, and so

$$N_{K^{Z_{\mathfrak{P}}}/K}(y) \equiv x \bmod \mathfrak{P}.$$

However, since $y \in \mathcal{O}_K^{Z_{\mathfrak{P}}}$, the norm of y is an element of $\mathcal{O}_K \subset \mathcal{O}_K^{Z_{\mathfrak{P}}}$ so $x, N_{K^{Z_{\mathfrak{P}}}/K}(y)$ are both elements of $\mathcal{O}_K^{Z_{\mathfrak{P}}}$. Thus, $N_{K^{Z_{\mathfrak{P}}}/K}(y) - x \in \mathfrak{P} \cap \mathcal{O}_K^{Z_{\mathfrak{P}}} = \mathfrak{q}$, so the last congruence holds modulo $\mathfrak{q}$. To clarify, we have given a way of constructing an element of $\mathcal{O}_K$ to which x is congruent modulo $\mathfrak{q}$, which is what we wanted.

At this point, we have the desired case reduction. Indeed, since $\mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_K^{Z_\mathfrak{P}}/\mathfrak{q}$ we may replace $\mathbb{F}_\mathfrak{p}$ in the statement of the theorem with $\mathbb{F}_\mathfrak{q} := \mathcal{O}_K^{Z_\mathfrak{P}}/\mathfrak{q}$. Following this, we replace K with $K^{Z_\mathfrak{P}}$ so that $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/K^{Z_\mathfrak{P}}) = Z_\mathfrak{P}$.
Finally, take an element $\tilde{\alpha} := \alpha + \mathfrak{P} \in \mathbb{F}_\mathfrak{P}$ such that $\mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{q}(\tilde{\alpha})$ and lift this to an element $\alpha \in \mathcal{O}_L$. Letting $f(X) \in K^{Z_\mathfrak{P}}[X]$ be the minimal polynomial of α over $K^{Z_\mathfrak{P}}$, we note that any automorphism of $\mathbb{F}_\mathfrak{P}$ is determined by its effect on $\tilde{\alpha}$ and sends $\tilde{\alpha}$ to a root of $\tilde{f}(X) := f(X) \bmod \mathfrak{P}$. Suppose $\alpha = \alpha_1$. Then, given any other root α_i of $f(X)$, we have an element $\sigma \in Z_\mathfrak{P}$ such that $\sigma(\alpha) = \alpha_i$ and so $\tilde{\sigma}(\tilde{\alpha}) = \tilde{\alpha}_i$. Since the action of $\mathrm{Gal}(L/K^{Z_\mathfrak{P}})$ on the roots of $f(X)$ is transitive, the automorphisms $\tilde{\sigma} \in \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{q})$ induced by elements of $\mathrm{Gal}(L/K^{Z_\mathfrak{P}})$ act transitively on the roots of $\overline{f}(X)$ and so we obtain every automorphism of $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{q}$ in this way. We conclude then that $\varphi : Z_\mathfrak{P} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{q})$ is a surjection, and since $\mathbb{F}_\mathfrak{q} = \mathbb{F}_\mathfrak{p}$, the result is proven. The kernel of this action is the set of $\sigma \in Z_\mathfrak{P}$ such that $\sigma(\alpha) \equiv \alpha \bmod \mathfrak{P}$ for all $\alpha \in \mathcal{O}_L$. In other words, this is the set of $\sigma \in Z_\mathfrak{P}$ such that σ is the identity map on $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$, which we denote $T_\mathfrak{P}$. By the first isomorphism theorem, $Z_\mathfrak{P}/T_\mathfrak{P} \cong \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$. □

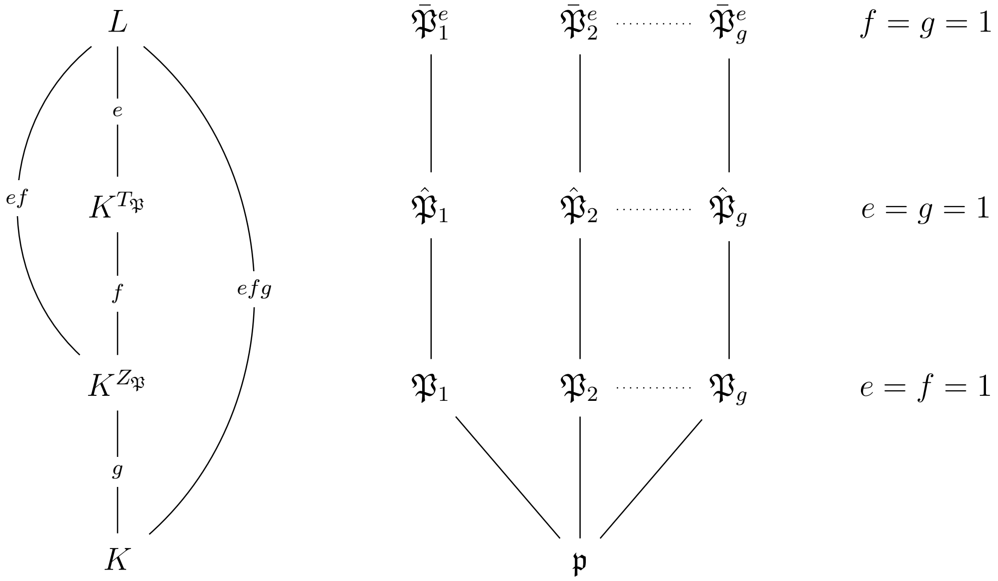
Definition 5.2. *Let $\varphi : Z_\mathfrak{P} \to \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ be the surjective group homomorphism discussed in Theorem 5.1. The kernel of φ is called the **inertia group** of the prime ideal $\mathfrak{P}$, denoted $T_\mathfrak{P}$. The fixed field of $T_\mathfrak{P}$, being that it is a subgroup of a Galois group, is denoted $K^{T_\mathfrak{P}}$.*

We saw earlier that $|Z_\mathfrak{P}| = ef$ where $e = e(\mathfrak{P}/\mathfrak{p})$ is the ramification index of $\mathfrak{P}$ over $\mathfrak{p}$ and $f = f(\mathfrak{P}/\mathfrak{p})$ is the inertial degree of $\mathfrak{P}$ over $\mathfrak{p}$. Additionally, we know from Galois theory that $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}) = [\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}] = f$, and so Theorem 5.1 tells us that

$$|Z_\mathfrak{P}/T_\mathfrak{P}| = f.$$

We conclude that $|T_\mathfrak{P}| = e$, and so, in particular, if $\mathfrak{p}$ is unramified in $\mathcal{O}_L$ then $e = 1$ and so $Z_\mathfrak{P} \cong \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$.

The point of this discussion of decomposition and inertia groups is to illustrate the splitting properties of primes in Galois extensions of number fields. In particular, in each intermediate extension the prime ideals under consideration behave in a very predictable way. We have the following situation for a Galois extension L of a number field K:



where $\mathfrak{P}_i$ is understood to be *the* prime of its decomposition field lying above $\mathfrak{p}$, $\hat{\mathfrak{P}}_i$ a prime of its inertia field lying above $\mathfrak{p}$, and $\bar{\mathfrak{P}}_i$ a prime of L. Intuitively, we see that $K^{Z_\mathfrak{P}}/K$ is responsible for all of the splitting of $\mathfrak{p}$, $K^{T_\mathfrak{P}}/K^{Z_\mathfrak{P}}$ is responsible for all of the inertial degree of the primes lying above $\mathfrak{p}$, and $L/K^{T_\mathfrak{P}}$ for all of the ramification of $\mathfrak{p}$ in L.

5.2 The Hilbert Class Field

We shall need to introduce some terminology before we begin taking steps to construct the Hilbert class field. Firstly, we distinguish between *finite* and *infinite* primes; an infinite prime is an embedding of K into $\mathbb{C}$, while a finite prime is a prime ideal[7]. As well as discussing the ramification of finite primes as discussed previously in the project, we shall also discuss the ramification of infinite primes. An infinite prime σ of K will be called ramified in an extension L if $\sigma : K \hookrightarrow \mathbb{R}$ is a real embedding, but whose extension to L is a complex embedding.

Definition 5.3. *Let K be a number field other than $\mathbb{Q}$. There is an extension H/K such that H is Abelian, unramified, and such that every other unramified Abelian extension of K is contained in H. We call H the **Hilbert class field** of K and it is the unique extension of K with these properties.*

We shall show that the Hilbert class field also has the interesting property that its Galois group is isomorphic to the ideal class group of the ground field it extends. In order to do so, we shall first need to introduce the so-called Artin symbol.

Proposition 5.3. *Let L/K be a Galois extension of number fields, let $\mathfrak{p}$ be a prime of K which is unramified in L, and let $\mathfrak{P}$ be a prime of L lying above $\mathfrak{p}$. There is a unique element $\sigma \in \mathrm{Gal}(L/K)$ with*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}$$

for all $\alpha \in \mathcal{O}_L$.

Proof. The assumption that $\mathfrak{p}$ be unramified in L is crucial; the order of $T_\mathfrak{P}$ is 1 when $\mathfrak{p}$ is unramified and so Theorem 5.1 gives us an isomorphism

$$Z_\mathfrak{P} \cong \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}).$$

Being that $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$ is a finite field, its Galois group is a cyclic group generated by a Frobenius element $\mathrm{Frob}_\mathfrak{p} : x \mapsto x^{|\mathbb{F}_\mathfrak{p}|}$. Since $|\mathbb{F}_\mathfrak{p}| = N(\mathfrak{p})$ by definition, this proves the existence of such an element of $\mathrm{Gal}(L/K)$ (since $Z_\mathfrak{P} \leq \mathrm{Gal}(L/K)$). For uniqueness, suppose $\sigma' \in Z_\mathfrak{P}$ and $x \in \mathfrak{P}$, so that $\sigma'(x) \equiv x^{N(\mathfrak{p})} \equiv 0 \bmod \mathfrak{P}$. Then $\sigma'(x) \in \mathfrak{P}$, and so $\sigma'(\mathfrak{P}) = \mathfrak{P}$. Thus, $\sigma' \in Z_\mathfrak{P}$ and both σ and σ' are mapped to $\mathrm{Frob}_\mathfrak{p}$ by the isomorphism. The injectivity of an isomorphism ensures that $\sigma = \sigma'$. □

This element of $\mathrm{Gal}(L/K)$ is called the *Artin symbol*[8] and is written

$$\left(\frac{L/K}{\mathfrak{P}}\right)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \bmod \mathfrak{P}.$$

[7] In fact, in a more modern view of algebraic number theory, infinite primes are identified with so-called archimedean valuations, and finite primes with non-archimedean valuations. We shan't discuss this here.

[8] Named for Emil Artin, a famous expositor of Galois theory.

We list a few interesting properties of the Artin symbol. Let $\mathfrak{p}$ be unramified in L and let $\mathfrak{P}$ be a prime of L lying over $\mathfrak{p}$. Firstly, by the uniqueness of the Artin symbol, we have

$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1}$$

for some $\sigma \in \mathrm{Gal}(L/K)$. This follows from the fact that decomposition groups are conjugate by elements of $\mathrm{Gal}(L/K)$. Secondly, the order of $((L/K)/\mathfrak{P}))$ is exactly the inertial degree of $\mathfrak{P}$ over $\mathfrak{p}$. This follows immediately from the fact that the Artin symbol maps to a generator of $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ under the isomorphism in Proposition 5.3, and the order of $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is the inertial degree of $\mathfrak{P}$ over $\mathfrak{p}$. Finally, we note that $\mathfrak{p}$ splits completely in L if and only if $((L/K)/\mathfrak{P}) = \mathrm{id}$. Since we are already assuming that $\mathfrak{p}$ is unramified, we have $e(\mathfrak{P}/\mathfrak{p}) = 1$, and so for $\mathfrak{p}$ to split completely we need only that $f(\mathfrak{P}/\mathfrak{p}) = 1$, which is exactly the statement that the Artin symbol is the identity.

Particularly interesting is the case when L/K is an Abelian extension. Indeed, in this case, the previous paragraph shows that the Artin symbol depends only on the prime $\mathfrak{p}$ of K lying below $\mathfrak{P}$. To see this, recall that the action $\mathrm{Gal}(L/K)$ on the primes of L is transitive, and so for any two primes $\mathfrak{P}, \mathfrak{P}'$ of L there is an element $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Thus, we have

$$\left(\frac{L/K}{\mathfrak{P}'}\right) = \left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma\left(\frac{L/K}{\mathfrak{P}}\right)\sigma^{-1} = \left(\frac{L/K}{\mathfrak{P}}\right).$$

Instead of writing $((L/K)/\mathfrak{P})$, since the dependence is only on $\mathfrak{p}$, we write $((L/K)/\mathfrak{p})$. Since L/K is an unramified extension, the Artin symbol is defined for all primes of L, and so we can extend the Artin symbol to all ideals of $\mathcal{O}_L$. That is, given an ideal $\mathfrak{a} \subset \mathcal{O}_L$, we have a unique factorisation into primes of $\mathcal{O}_L$ (by Section 3). We write

$$\mathfrak{a} = \mathfrak{P}_1^{a_1} \ldots \mathfrak{P}_r^{a_r}$$

where $\mathfrak{P}_i$ are such that $\mathfrak{p}_i = \mathfrak{P}_i \cap \mathcal{O}_K$ is a prime of $\mathcal{O}_K$ lying below $\mathfrak{P}_i$. We specify the Artin symbol on $\mathfrak{a}$ to be the map

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{i=1}^{r}\left(\frac{L/K}{\mathfrak{p}_i}\right)^{a_i}.$$

As a consequence of this, the Artin symbol induces a homomorphism $I_K \to \mathrm{Gal}(L/K)$ called the *Artin map*. We write

$$\left(\frac{L/K}{\cdot}\right) : I_K \to \mathrm{Gal}(L/K).$$

When L is the Hilbert class field of K then the Artin map is surjective[9] and the kernel is exactly the subgroup P_K of principal ideals of I_K. Consequently, by the first isomorphism theorem, the Artin map induces an isomorphism

$$I_K/P_K = \mathrm{Cl}(\mathcal{O}_K) \cong \mathrm{Gal}(L/K)$$

which is what we set out to show.

[9] The proof of both of these facts requires the heavy machinery of class field theory and so will not be presented here.

In fact, the Artin map is in some sense a generalisation of quadratic reciprocity to higher powers. For instance, we can re-obtain the Legendre symbol from the Artin symbol as follows: in the notation of the preceding discussion, let $K = \mathbb{Q}$ and let $L = \mathbb{Q}(\sqrt{2})$. Then, as the Artin map is a $\mathbb{Q}$-automorphism of L, we only need know the image of $\sqrt{2}$ under this map. Indeed, we have

$$\left(\frac{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}{p}\right)(\sqrt{2}) \equiv \sqrt{2}^{N(p)} \equiv 2^{\frac{p-1}{2}}\sqrt{2} \equiv \left(\frac{2}{p}\right)(\sqrt{2}) \bmod p$$

where $(2/p)$ is the usual Legendre symbol. Note that we only defined the Artin symbol for unramified primes of the ground field. Indeed, this goes some way to explaining why there is a supplementary law for the case where $p = 2$; if $K = \mathbb{Q}(\sqrt{d})$ is such that $d \equiv 2, 3 \bmod 4$ then 2 always ramifies in K (since $2 \mid d_k$ in this case!).
Pending the proof of a few lemmas, we shall construct the Hilbert class field of $K = \mathbb{Q}(\sqrt{-17})$ (Exercise 5.25 in [11]).

Lemma 5.1. *Let K be a number field and L a Galois extension of K such that $L = K(\alpha)$ for some $\alpha \in \mathcal{O}_L$ and such that $\mathcal{O}_L = \mathcal{O}_K[\alpha]$. Let $m(X)$ be the minimal polynomial of α over K so that $m(X) \in \mathcal{O}_K[X]$. If $\mathfrak{p}$ is a prime of K and $m(X)$ is separable modulo $\mathfrak{p}$ then*

(i) the factorisation of $\mathfrak{p}$ in L depends on the factorisation $m(X) \equiv \pi_1(X)\dots\pi_g(X) \bmod \mathfrak{p}$ where the $\pi_i(X)$ are distinct irreducible factors of $m(X)$. In particular, $\mathfrak{P}_i = \mathfrak{p}\mathcal{O}_L + \pi_i(\alpha)\mathcal{O}_L$ is a prime ideal in $\mathcal{O}_L$ and $\mathfrak{p} = \mathfrak{P}_1\dots\mathfrak{P}_g$. In addition, all of the $\pi_i(X)$ have the same degree and this is equal to the inertial degree f,
(ii) $\mathfrak{p}$ is unramified in L,
(iii) $\mathfrak{p}$ splits completely in L if and only if $m(X) \equiv 0 \bmod \mathfrak{p}$ has a solution in $\mathcal{O}_K$.

Proof. For (i), the reader is referred to [5, p.63, 64] for a proof. For (ii), we note that if $m(X)$ is separable modulo $\mathfrak{p}$ then there are no repeated factors in the factorisation of $m(X)$ modulo $\mathfrak{p}$ and so by (i) this implies that $\mathfrak{p}$ is unramified in L. For (iii), if $m(X)$ has a root in $\mathcal{O}_K$ then one of the $\pi_i(X)$ has degree 1, and so by (i), all of the $\pi_i(X)$ have degree 1. Since this corresponds to the inertial degree f of the $\mathfrak{P}_i$ in the factorisation of $\mathfrak{p}$ and the ramification indices of each of the $\mathfrak{P}_i$ is 1, we have $g = [L : K]$, i.e. $\mathfrak{p}$ splits completely in L. □

Lemma 5.2. *Let $L = K(\sqrt{u})$ and let $\mathfrak{p} \subset \mathcal{O}_K$ be a non-zero prime ideal. Then*

(i) if $2u \notin \mathfrak{p}$ then $\mathfrak{p}$ is unramified in L, and
(ii) if $2 \in \mathfrak{p}$ but $u \notin \mathfrak{p}$ and $u = b^2 - 4c$ for some $b, c \in \mathcal{O}_K$ then $\mathfrak{p}$ is unramified in L.

Proof. The discriminant of $X^2 - u \in \mathcal{O}_K[X]$ is $4u$. By assumption we have that $2u \notin \mathfrak{p}$ and hence[10] $4u \notin \mathfrak{p}$. Lemma 5.1 says that $X^2 - u$ is separable modulo $\mathfrak{p}$ and so it is unramified in L.
For (ii), note that we can write $L = K(\alpha)$ where $\alpha = \frac{-b+\sqrt{u}}{2}$ is a root of the polynomial $X^2 + bX + c \in \mathcal{O}_K[X]$. Thus, if $u = b^2 - 4c$, the discriminant of this polynomial, and $u \notin \mathfrak{p}$, then again by Lemma 5.1 we have that $\mathfrak{p}$ is unramified in L. □

[10] If $4u \in \mathfrak{p}$ then $2 \in \mathfrak{p}$ or $2u \in \mathfrak{p}$ because $\mathfrak{p}$ is a prime ideal. But $2u \notin \mathfrak{p}$ by assumption so $2 \in \mathfrak{p}$, which is a contradiction since $2u \notin \mathfrak{p}$ implies that $2 \notin \mathfrak{p}$.

Example 5.1. *Let $K = \mathbb{Q}(\sqrt{-17})$. We shall show that the Hilbert class field H of K is $H = K(\alpha)$ where $\alpha = \sqrt{\frac{1+\sqrt{17}}{2}}$.*

We first begin by showing that $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/(4)$, since this tells us that $\mathrm{Gal}(H/K) \cong \mathbb{Z}/(4)$ and hence that H has degree 4 over K. The discriminant of K is $d_K = -68$, the degree of $K/\mathbb{Q}$ is 2 and there is exactly one pair of complex embeddings of K into $\mathbb{C}$, namely complex conjugation. Thus, we have the Minkowski bound

$$M_K = \frac{2!}{2^2}\left(\frac{4}{\pi}\right)\sqrt{|-68|} \approx 5.25\ldots$$

and so we need only check primes of $\mathcal{O}_K$ lying above $2, 3,$ and 5. Indeed, we have $X^2 + 68 \equiv X^2 \bmod 2$, so $2\mathbb{Z}$ ramifies in $\mathcal{O}_K$, $X^2 + 68 \equiv X^2 + 2 \equiv (X-1)(X+1) \bmod 3$ so $3\mathbb{Z}$ splits in $\mathcal{O}_K$, and $X^2 + 68 \equiv X^2 + 3 \bmod 5$, which has no solutions so $5\mathbb{Z}$ is inert in $\mathcal{O}_K$. Let $2\mathcal{O}_K = \mathfrak{p}_2^2$, $3\mathcal{O}_K = \mathfrak{p}_3\bar{\mathfrak{p}}_3$, and $5\mathcal{O}_K = \mathfrak{p}_5$, so that $N(\mathfrak{p}_2) = 2$, $N(\mathfrak{p}_3) = N(\bar{\mathfrak{p}}_3) = 3$, and $N(\mathfrak{p}_5) = 25$. Thus, we have[11] $\mathfrak{p}_2 \sim \mathfrak{p}_2^{-1}$, $\mathfrak{p}_3 \sim \bar{\mathfrak{p}}_3^{-1}$, and $\mathfrak{p}_5 \sim 1$ in $\mathrm{Cl}(\mathcal{O}_K)$. The norm of $1 + \sqrt{-17}$ is $N(1 + \sqrt{-17}) = 18 = 2 \times 3^2$ so the we have a principal ideal $(1 + \sqrt{-17}) = \mathfrak{p}_2\mathfrak{p}_3^2$ and hence that $\mathfrak{p}_3^2 \sim \mathfrak{p}_2$, so we may eliminate $\mathfrak{p}_2$ from the generating set of $\mathrm{Cl}(\mathcal{O}_K)$ and focus on determining the order of $\mathfrak{p}_3$ in $\mathrm{Cl}(\mathcal{O}_K)$. Since $a^2 + 17b^2 = 3$ has no solutions with $a, b \in \mathbb{Z}$, we know at least that $\mathfrak{p}_3$ is itself non-principal. Since we just showed that $\mathfrak{p}_3^2 \sim \mathfrak{p}_2$ and $a^2 + 17b^2 = 2$ has no integral solutions, we also have that $\mathfrak{p}_3^2 \not\sim 1$. Additionally, $a^2 + 17b^2 = 3^3 = 27$ has no solutions, since if this were the case then $a^2 \equiv 10 \bmod 17$ would have solutions, which is easily checked to be false by calculation, and so $\mathfrak{p}_3^3$ is non-principal. Finally, we have $N(8 + \sqrt{-17}) = 81 = 3^4$ and so $(8 + \sqrt{-17}) = \mathfrak{p}_3^4$, showing that $\mathfrak{p}_3^4 \sim 1$, and hence that $\mathrm{Cl}(\mathcal{O}_K)$ is the cyclic group of order 4 generated by the ideal class of $\mathfrak{p}_3$.

We have now shown that $\mathrm{Cl}(\mathcal{O}_K) \cong \mathbb{Z}/(4)$ and so $\mathrm{Gal}(H/K) \cong \mathbb{Z}/(4)$, so that H is a degree 4 Abelian extension of K. Following this, we shall show that there is a tower of extensions $K \subset K_1 \subset H$ such that K_1 is unramified over K and H is unramified over K_1. Clearly the multiplicativity of the exponents of prime ideals means then that H is unramified over K, so this shall be an easier route.

Since $\alpha = \sqrt{\frac{1+\sqrt{17}}{2}}$ we have $2\alpha^2 - 1 = \sqrt{17} \in H$ and so we first show that the extension $K_1 = K(\sqrt{17})$ is unramified[12] over K. Let $\mathfrak{p}$ be a prime of K and suppose $2 \in \mathfrak{p}$. Then certainly $17 \notin \mathfrak{p}$ since $17 - 8 \cdot 2 = 1 \notin \mathfrak{p}$ (since it is a prime ideal) and since $17 = 1^2 - 4 \cdot (-4)$, Lemma 5.2 says that $\mathfrak{p}$ is unramified in K_1. Now, notice that $\sqrt{17} \in K_1$ and $\sqrt{-17} \in K$ so that $\sqrt{17}/\sqrt{-17} = \sqrt{-1} \in K_1$ so that $K_1 = K(\sqrt{-1})$. Thus, $u = -1$ is certainly not an element of $\mathfrak{p}$ and if $2 \notin \mathfrak{p}$ then $2u \notin \mathfrak{p}$ and so $\mathfrak{p}$ is unramified in K_1. We now move on to showing that $H = K_1(\sqrt{u})$ is an unramified extension, where $u = \frac{1+\sqrt{17}}{2}$. Let $u' = \frac{1-\sqrt{17}}{2}$. Then $uu' = \frac{-16}{4} = -4$ so that $\sqrt{uu'} = 2\sqrt{-1} \in K_1$. Thus, since $\sqrt{u'} = \frac{2\sqrt{-1}}{\sqrt{u}} \in H$, we have $H = K_1(\sqrt{u}) = K_1(\sqrt{u'})$. Following this, let $\mathfrak{P}$ be a prime of K_1. It must always be the case that either u or u' is in $\mathfrak{P}$, but never both, since $u + u' = 1$. Thus, if $2 \notin \mathfrak{P}$ then either $u \notin \mathfrak{P}$ or $u' \notin \mathfrak{P}$ and the fact that $K_1(\sqrt{u}) = K_1(\sqrt{u'})$ gives us that $\mathfrak{P}$ is unramified in H. Now, note that u and u' both

[11] Note the abuse of notation; we mean of course that the **ideal classes** of $\mathfrak{p}_2$ and $\mathfrak{p}_2^{-1}$ are equivalent, though the notation $[\mathfrak{p}_2]$ quickly becomes cumbersome.

[12] Note that since K is an imaginary quadratic field, and $2 = r_1 + 2r_2$ where r_1 is the number of real embeddings of K into $\mathbb{C}$ and r_2 the number of pairs of complex embeddings, we have $r_2 = 1$ and $r_1 = 0$ so there are no real infinite primes to ramify!

satisfy $X^2 - X - 4 \in \mathcal{O}_{K_1}[X]$ and so since $u \notin \mathfrak{P}$ or $u' \notin \mathfrak{P}$, we have $u = \left(\frac{1+\sqrt{17}}{2}\right)^2 - 4\cdot 1$, and so $\mathfrak{P}$ is unramified in H by Lemma 5.2.
Putting these results together, we have that K_1 is an unramified extension of K and that H is an unramified extension of K_1. Thus, H is an unramified extension of K. Additionally, we showed that H is an Abelian extension of K whose Galois group is isomorphic to the ideal class group of K, and so H is the Hilbert class field of K.

6 Conclusions

To conclude I'd like to discuss some of the implications of the ideas discussed in sections 4 and 5 and how they might lead to future study and/or research.
Firstly, let us recall some of the main issues with Kummer's proof discussed in Section 4. The most important step in the proof of both cases was in factoring the left hand side of the equation $x^p + y^p = z^p$ over $\mathbb{Z}[\zeta_p]$, translating this into the language of ideals, and obtaining information about the prime decomposition of such ideals (possible because $\mathbb{Z}[\zeta_p]$ is a Dedekind domain, which we know courtesy of Section 3!). In both cases we were able to conclude that the factors of $x^p + y^p$, as ideals, were equal to the pth power of some ideal in $\mathcal{O}_{\mathbb{Z}[\zeta_p]}$ and that, due to the lack of p-torsion in the ideal class group of $\mathcal{O}_{\mathbb{Z}[\zeta_p]}$ (given by the regularity assumption on p), this meant that these factors must be principal. The main obstruction, then, to a full proof of Fermat's last theorem is in the potential p-torsion in the ideal class group of $\mathbb{Z}[\zeta_p]$. For example, when $p = 37$, we have that $\mathrm{Cl}(\mathbb{Q}(\zeta_{37})) \cong \mathbb{Z}/37\mathbb{Z}$ and so there is 37-torsion in the ideal class group of $\mathbb{Z}[\zeta_{37}]$. Of course, this means that, in Kummer's proof, we can no longer make the assumption that for an ideal $\mathfrak{a} \subset \mathbb{Z}[\zeta_{37}]$, if $\mathfrak{a}^{37}$ is principal then $\mathfrak{a}$ is principal. In future it would be interesting to look into *Iwasawa Theory*[13]. In particular, if p is not a regular prime (i.e. $p \mid h_{\mathbb{Q}(\zeta_p)}$), Iwasawa theory aims to get information on the p-part of the ideal class group of $\mathbb{Z}[\zeta_p]$ by constructing infinite extensions over $\mathbb{Q}$ called $\mathbb{Z}_p$-extensions (extensions whose Galois group is isomorphic to the additive group of p-adic integers). This requires the study of infinite Galois theory [14], the theory of local fields (of which $\mathbb{Q}_p$, whose ring of integers is $\mathbb{Z}[\zeta_p]$, is an example), and some analytic theory.
Secondly, Section 5 discusses the Hilbert class field. This was described as the maximal unramified Abelian extension of a number field, its Galois group was seen to be isomorphic to the ideal class group of the ring of integers of the base number field, and it was the unique field satisfying these properties. We might instead be interested in describing the maximal Abelian extension A of a number field K (this time dropping the unramified property). In this case, things become much harder. This extension has infinite degree over K and so its Galois group is (as in the footnote) a profinite group. The open subgroups (with respect to the *restricted product topology*) of finite index are associated, by the Galois correspondence, to finite Abelian extensions of K, and such extensions are called *class fields*, for which the theory is named. One very explicit outcome of class field theory is the *Kronecker-Weber* theorem, which says that every Abelian extension of $\mathbb{Q}$ is contained in some cyclotomic extension. The study of class field theory requires, among other things, more study of topological groups, and local field theory (as above).

[13] Named for Kenkichi Iwasawa.

[14] The Galois groups of infinite towers of field extensions are called profinite groups. These are topological groups that are isomorphic to the projective limit of some inverse system of groups (in particular the Galois groups of the intermediate extensions!).

Acknowledgements

I should very much like to thank Dr. Daniel Robertz for his supervision of this project, whose time, expertise, and relentless tutoring have been invaluable in my completion of the project. I should also like to thank Dr. Nathan Broomhead, Dr. Colin Christopher, and Dr. Marina Logares for several discussions related to the subject matter, all of whom have at some point given up their time to help me.

References

[1] Andrew J. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics, **141** (1995), 443-551

[2] Harold M. Edwards, *Fermat's Last Theorem*, Springer-Verlag

[3] Ş. Alaca, K. S. Williams. *Introductory Algebraic Number Theory*. Cambridge University Press, Cambridge, United Kingdom, 2004.

[4] K. Conrad, *Ideal Factorization*, `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/idealfactor.pdf`

[5] J.S. Milne, *Algebraic Number Theory*, `http://jmilne.org/math/CourseNotes/ANT.pdf`

[6] D. S. Dummit, R. M. Foote, *Abstract Algebra*, Prentice Hall, New Jersey, 1999.

[7] Serge Lang, *Algebraic Number Theory*, Springer, New York, 1994.

[8] K. Conrad, *Ideal Classes and the Kronecker Bound*, `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/classgroupKronecker.pdf`

[9] K. Conrad, *Fermat's Last Theorem for Regular Primes*, `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/fltreg.pdf`

[10] K. Conrad, *Kummer's Lemma*, `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/kummer.pdf`

[11] D. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication, 2nd Edition*, Wiley, New Jersey, 2013.

[12] J. Escofier, *Galois Theory*, Springer, New York, 2001.

[13] E. Kummer, *Allgemeiner Beweis des Fermatschen Satzes, daß die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in den Zählern der ersten $\frac{1}{2}(\lambda - 3)$ Bernoullischen Zahlen als Factoren nicht vorkommen.*, Journal für die reine und angewandte Mathematik , Göttingen, n.d.

[14] K. Conrad, *Separability*, `http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/separable1.pdf`

[15] J. Neukirch, *Algebraic Number Theory*, Springer, Berlin, 1999.