Kummer's Theory of Regular Primes

Malthe Fog Sporring

s1745523
Project UG771

Year 5 MMath Dissertation
School of Mathematics
University of Edinburgh
May 22, 2022

Abstract

Fermat's Last Theorem says that the equation $x^n + y^n = z^n$ has no integer solutions for $n > 2$. In 1847, Ernst Kummer proved the theorem for a certain type of prime exponents, called *regular primes*. We give a historically motivated account of his proof in the modern language of ideals. In particular, we show how Fermat's Last Theorem can be reformulated as a multiplicative problem in the ring $\mathbb{Z}[\omega]$ where $\omega = e^{2\pi i/p}$, for a prime p. The result is then reduced to proving that (I) the ideals of $\mathbb{Z}[\omega]$ factorise uniquely into *prime ideals*, and (II) the equivalence classes of ideals under a certain equivalence relation is a finite abelian group. These properties are shown to follow from the fact that $\mathbb{Z}[\omega]$ is (I) a *Dedekind domain* and (II) a *number ring*.

Declaration

I declare that this thesis was composed by myself and that the work contained therein is my own, except where explicitly stated otherwise in the text.

(*Malthe Fog Sporring*)

To Phoebe.

Contents

Acknowledgements

I want to thank my supervisor, Professor James Wright, for his guidance and advice throughout this project. I also wish to express my gratitude to my parents and friends for their constant encouragement and support.

Chapter 1

Introduction

One of the most infamous theorems of number theory is Fermat's Last Theorem. This theorem was first stated in 1637 by Pierre de Fermat, written in the margins of his copy of *Arithmetica* with the note that he had discovered "a truly marvelous proof of this, which however the margin is not large enough to contain" [6]. Fermat never gave a full proof of the theorem, and despite their best efforts, the proof eluded many mathematicians through the centuries until a complete proof was finally published in 1995 by Sir Andrew Wiles. Simon Singh's *Fermat's Last Theorem* [10] gives an excellent historical account of the efforts to prove the theorem, in a manner accessible to the non-mathematician.

Despite the infamous difficulty of its proof, Fermat's Last Theorem is brief to state.

Theorem 1.0.1 (Fermat's Last Theorem)**.** *The equation*

$$x^n + y^n = z^n \tag{1.1}$$

has no integer solutions for $n \in \mathbb{N}, n > 2$.

When $n = 2$, the equation is Pythagoras' Theorem, which is known to have integer solutions. For example, $(x,y,z) = (3,4,5)$ works.

We now give some reductions of Fermat's Last Theorem, inspired by [13]. We may reduce the proof of Fermat's Last Theorem to the case where n is an odd prime, as a counter-example for a composite power $n = pm$ divisible by p also gives a counter-example for the power p:

$$(x^m)^p + (y^m)^p = (z^m)^p.$$

Note this will not take care of powers of the form $n = 2^n$, so we should additionally prove the theorem for the $n = 4$. Luckily, Fermat himself proved this case - in fact it is the only surviving contribution of his to the proof [4]. As an additional reduction, we may assume that in a counter-example (x,y,z), x, y and z are all coprime. Firstly, note that if two of the three integers are divisible by an integer m, then the third must also be divisible by m, as otherwise the theorem will not hold $\mod m$. Additionally, letting $g := gcd(x,y,z)$, any counter-example (x,y,z) gives a counter-example $(\frac{x}{g}, \frac{y}{g}, \frac{z}{g})$ where all three integers are jointly coprime, hence pairwise coprime by the previous remark. We make a final reduction by classifying the counterexamples for exponent p as one of two types:

- (Type I): p does not divide either of x,y,z.

- (Type II): p divides exactly one of x, y, z.

We will focus exclusively on Type I solutions in this text. The case $p = 3$ can be proven using simple modular arithmetic. It is easy to check exhaustively that the cube of any integer not divisible by 3 is congruent to $\pm 1 \mod 9$, so it follows that

$$x^3 + y^3 \neq z^3 (\mod 9).$$

We may therefore assume $p > 5$. We will start by turning $Eq.$ (1.1) into a multiplicative equation. Let $\omega = e^{2\pi i/p}$, and recall $\omega, \omega^2, \ldots, \omega^n = 1$ are the p distinct p-th roots of unity. Since each solve $t^p - 1 = 0$, and $\mathbb{C}$ is algebraically closed,

$$t^p - 1 = (t-1)(t-\omega)\ldots(t-\omega^{p-1}). \tag{1.2}$$

Letting $t = \frac{-x}{y}$ gives

$$z^p = x^p + y^p = (x+y)(x+\omega y)\ldots(x+\omega^{p-1}y) \tag{1.3}$$

as required. This turns Fermat's Last Theorem into an algebraic problem in the ring $\mathbb{Z}[\omega]$ of polynomials in ω with integer coefficients. In 1847, Gabriel Lamé gave a proof which relied on the assumption that the ring of polynomials $\mathbb{Z}[\omega]$ is a unique factorisation domain (UFD). An integral domain is said to be a UFD if every non-zero, non-unit (that is, non-invertible) element $r \in R$ has a unique decomposition as a finite product of irreducibles $r = r_1 r_2 \ldots r_n$, where an element s is irreducible if

$$s = ab \implies a \text{ or } b \text{ is a unit.}$$

Unfortunately, this assumption turns out to be false in general. Nonetheless, let us make the assumption that $\mathbb{Z}[\omega]$ is a UFD and briefly outline Lamé's false proof.

1.1 Lamé's false proof for Type I solutions

We follow the account in [13]. The proof splits into two parts.

Part I: By the assumption that $\mathbb{Z}[\omega]$ is a UFD, we can factorise

$$z = r_1 r_2 \ldots r_n$$

such that

$$z^p = r_1^p r_2^p \ldots r_n^p.$$

Similarly, write

$$(x+\omega^j y) = r_{1j} r_{2j} \ldots r_{n_j j}.$$

Since this factorisation is assumed to be unique, Eq. (1.3) implies that for each $1 \leq j \leq n, 1 \leq s \leq n_j$, we have $r_{sj} = v r_i$ for some $1 \leq i \leq n$ and unit v. We will additionally show that $x + \omega y$ does not share any irreducibles with $x + \omega^j y$ for all $1 < j \leq p$. Indeed, if r is an irreducible dividing both, then

$$r | (x+\omega y) - (x+\omega^j y) = \omega y (1 - \omega^{j-1}).$$

Since ω is a unit with inverse ω^{p-1}, it follows that

$$r|y(1-\omega^{j-1})|y\prod_j(1-\omega^j).$$

We show that $\prod_j(1-\omega^j)=p$ in Lemma 3.4.11, so it follows that $r|py$. Since p,y and z are pairwise coprime, py and z also coprime. By the extended Euclidean algorithm, there exist integers m,n such that

$$mpy+nz=1.$$

Then r divides the left-hand side but not the right-hand side, a contradiction.

It follows that no irreducibles divide both $(x-\omega y)$ and $(x-\omega^j y)$ for each $1<j\leq n$. Since the irreducible factors of the $(x-\omega^j y)$'s multiply to give $z^p=r_1^p\dots r_n^p$, the irreducible factors of $(x-\omega y)$ must also appear as powers of p. In fact, we are about to show that It follows that

$$(x-\omega y)=ur_{\alpha(1)}^p\dots r_{\alpha(i)}^p=:u\alpha^p \tag{1.4}$$

for some unit u and $\alpha\in\mathbb{Z}[\omega]$. Note we have assumed here that $(x-\omega y)$ has at least one irreducible factor, but of course if it is a unit we may still write $(x-\omega y)=u\alpha^p$ for $\alpha=1$. Part II will in fact show this is impossible.

Part II: Under the assumption that $(x-\omega y)=u\alpha^p$, we finish the proof of Theorem 1.0.1. We note this part does not use the false assumption that $\mathbb{Z}[\omega]$ is a UFD. We will take the following lemma as given – proving it is surprisingly tricky and requires some sophisticated Galois theory.

Lemma 1.1.1. *For any unit $u\in\mathbb{Z}[\omega]$,*

$$\frac{u}{\overline{u}}=\omega^k$$

for some $k\in\mathbb{Z}$.

Proof. Omitted. See [9]. □

Writing $\alpha=a_0+a_1\omega+\dots+a_{p-1}\omega^{p-1}$, for $a_i\in\mathbb{Z}$ we find by multinomial expansion that $\alpha^p=a_0^p+\dots+a_{p-1}^p \mod p\mathbb{Z}[\omega]$, since every other term in the expansion is a multiple of p. Note by equality $\mod p\mathbb{Z}[\omega]$ we mean they are mapped to the same element under the projection $\mathbb{Z}[\omega]\to\mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$. It follows that

$$(x+\omega y)=ua \mod p\mathbb{Z}[\omega]$$

for some $a\in\mathbb{Z}$. By Lemma 1.1.1,

$$(x+\omega y)=\omega^k\overline{(x+\omega y)}=\omega^k(x+\omega^{-1}y) \mod p\mathbb{Z}[\omega]$$

for some $k\in\mathbb{Z}$. By equating coefficients as polynomials in ω, we find $k=1$, so

$$x+\omega y=x\omega+y \mod p\mathbb{Z}[\omega] \implies x=y \mod p.$$

Rewriting Fermat's Last Theorem as $x^p + (-z)^p = (-y)^p$ then also gives

$$x = -z \mod p.$$

By Fermat's little theorem, Theorem 1.0.1 reduces to

$$x + y = z \mod p.$$

By what we have shown, this implies

$$3x = 0 \mod p.$$

This is a contradiction since $p > 3$ and does not divide x by assumption.

1.2 Kummer's partial rectification

Kummer discovered the critical flaw in Part I of Lamé's proof, by showing that $\mathbb{Z}[\omega]$ is **not** a UFD in general. For example he showed that $\mathbb{Z}[e^{2\pi i/23}]$ is not a UFD [13]. Every element of $\mathbb{Z}[\omega]$ **does** factor as a product of irreducibles, as we will later show by proving $\mathbb{Z}[\omega]$ is **Noetherian**. However, this factorisation is not unique in general. This is a subtle point - in Part I of Lamé's proof we were only able to deduce that $x + \omega y = u\alpha^p$ by arguing that if r is in the decomposition of $x + \omega y$ then it must be in the decomposition of z^p as well. Kummer realised that there was a strictly stronger[1] condition to the UFD condition which would make Lamé's Part I proof work. This condition is best explained in the framework of ideals, an invention of Dedekind [13]. Dedekind showed that the **ideals** of $\mathbb{Z}[\omega]$ factorise uniquely into **prime ideals**. Prime ideals are proper ideals I of R such that $xy \in I \implies x \in I$ or $y \in I$ where $x, y \in R$. We now show that Part I of Lamé's proof can be rewritten in terms of ideals. From Eq. (1.3), we can take the **ideal generated** by both sides (see Chapter 2) to get

$$\langle z^p \rangle = \langle z \rangle^p = \langle (x+y)(x+\omega y)\dots(x+\omega^{p-1}y) \rangle = \langle x+y \rangle \dots \langle x+\omega^{p-1}y \rangle \tag{1.5}$$

where we have defined multiplication of ideals as $IJ = \langle ij : i \in I, j \in J \rangle$. Then decomposing $\langle x + \omega y \rangle$ into prime ideals $P_1 P_2 \dots P_n$ we can use (now correctly) the unique factorisation property to see $\langle x + \omega y \rangle = I^p$ for some ideal I, as long as we can establish that $x + \omega y$ does not share any prime ideals with the $x + \omega^j y$ (see Remark 4.3.6).

The final step will be to show that I is principal: $I = \langle \alpha \rangle$. Then $I^p = \langle \alpha \rangle^p = \langle \alpha^p \rangle$. Now note

$$x + \omega y \in \langle \alpha^p \rangle \implies x + \omega y = s\alpha^p \text{ for some } s \in \mathbb{Z}[\omega],$$

and conversely

$$\alpha^p \in \langle x + \omega y \rangle \implies \alpha^p = r(x + \omega y) \text{ for some } r \in \mathbb{Z}[\omega].$$

Then $\alpha^p = rs\alpha^p \implies 1 = rs \implies s$ is a unit . Note this implication is valid because $\mathbb{Z}[\omega]$ is an integral domain. Therefore, $x + y\omega = u\alpha^p$ for a unit u, completing Step I.

[1] See Remark 5.1.3.

When is I principal? Let us define an equivalence relation on ideals I of $\mathbb{Z}[\omega]$ by

$$I \sim J \iff \alpha I = \beta J \text{ for some } \alpha, \beta \in \mathbb{Z}[\omega]$$

This equivalence relation is clearly reflexive and symmetric. It is also transitive: if $\alpha I = \beta J$ and $\gamma J = \zeta K$ then $\alpha\gamma I = \alpha\gamma J = \alpha\zeta K$. As we will show, the set of equivalence classes is a finite abelian group $Cl(\mathbb{Z}[\omega])$, thus we can define **class number** h_p of $\mathbb{Z}[\omega], \omega = e^{2\pi i/p}$ by $h_p = |l(\mathbb{Z}[\omega])|$. We then define

Definition 1.2.1. A prime p is **regular** if $p \not| h_p$.

If p is regular, then by Lagrange's Theorem, $Cl(\mathbb{Z}[\omega])$ has no elements of order p. In particular, $[I]$ does not have order p where I is the ideal s.t. $x + \omega y = I^p$. As we will show, the identity element in $Cl(\mathbb{Z}[\omega])$ is the equivalence class of principal ideals. It follows that $e = [\langle x + \omega y \rangle] = [I^p] = [I]^p$, and since $[I]$ does not have order p, it must be the identity element. In particular, I is principal.

If we can fill in the missing gaps we will have, just as Kummer did in 1847, proved Fermat's Last Theorem for Type I solutions and regular exponents. Kummer also managed to prove that Type 2 solutions could not exist with regular exponents, giving the full proof of Theorem 1.0.1 for regular primes. He then went on to classify all the primes less than 100, showing that the only irregular primes less than 100 are $37, 59$ and 67 [13]. Since $37^2 > 1000$, this proves Fermat's Last Theorem for all integers $3 \leq n \leq 1000$ except for these three! This is remarkable progress compared to the prior state of affairs, when Fermat's Last Theorem was only known for multiples of $3, 4, 5$ and 7 [2].

Our goal will be to fill out the gaps in this proof. We need to show two things:

Property I: the ideals of $\mathbb{Z}[\omega]$ factorise uniquely into prime ideals.

Property II: the ideals of $\mathbb{Z}[\omega]$ under $\sim$ form a finite abelian group.

We will start in Chapter 2 by getting comfortable with the algebra of ideals and modules. We will also define what it means for a ring to be Noetherian, and show that non-units in Noetherian rings factorise (not necessarily uniquely) into a finite product of irreducibles. In Chapter 3 we will define number fields and number rings, and show that $\mathbb{Z}[\omega]$ is the number ring $\mathbb{A} \cap \mathbb{Q}[\omega]$. In Chapter 4 we define a Dedekind domain, show that all number rings are examples, and show that Dedekind domains have Property I. Finally, in Chapter 5 we show all number rings have Property II, finishing the proof of Fermat's Last Theorem for Type I solutions and regular exponents.

Chapter 2

Rings and ideals

Kummer's proof predated the very concept of an ideal: he worked with what he called "ideal numbers". These were later put on a solid footing by Dedekind when he invented the notion of ideals. Ideals are such a key part of modern algebra, it can be difficult to imagine a time before their invention. In fact, Kummer's story tells so well in the language of Dedekind that we will exclusively tell this side of the story. To this end, we spend this chapter establishing preliminary results about ideals, ring modules, and Noetherian rings, inspired by the account in [13]. Some of these results will be revision from undergraduate level algebra. All rings will be assumed to be commutative with multiplicative identity, which ring homomorphisms are assumed to preserve.

2.1 Ideals

Recall the following definitions.

Definition 2.1.1. An **ideal** I of R is a non-empty subset satisfying the following properties:

(i) I is closed under subtraction.

(ii) When $i \in I$, for any $r \in R$, $ri \in I$.

Definition 2.1.2. Given any subset $S \subset R$, the **ideal generated by** S, denoted $\langle S \rangle$, is the smallest ideal of R containing S. It is exactly the set $\{r_1 s_1 + \ldots r_n s_n : r_i \in R, s_j \in S\}$ of finite linear combinations of elements in S. A **principal ideal** is an ideal generated by a single element.

Remark 2.1.3. Since our rings are commutative, we do not need to distinguish between left ideals and right ideals.

Example 2.1.4. For any $n \in \mathbb{Z}$, $\langle n \rangle = n\mathbb{Z}$ is an ideal of the integral domain $\mathbb{Z}$. In fact, every ideal of $\mathbb{Z}$ is of this form. Take any nonzero ideal I of $\mathbb{Z}$ and let n be the smallest positive integer in I. Then given any other $m \in I$, the division and remainder algorithm gives two integers q, r with $m = qn + r$ and $0 \leq r < n$. It follows that $r \in I$. However, n was minimal among positive integers in I, so in fact $r = 0$ and $m \in \langle n \rangle$. Since m was arbitrary, $I = \langle n \rangle$. It follows that every ideal of $\mathbb{Z}$ is principal. An integral domain with this property is called a **principal ideal domains** or **PID**s for short.

Example 2.1.5. Since the divison and remainder algorithm works in any polynomial ring in one variable over a field [5], an almost identical argument to Example 2.1.4 shows that $F[x]$ is a PID for any field F. In particular, given an ideal I of $F[x]$ we can pick a polynomial $f \in I$ of minimal degree. For any $g \in I$ we can find $q, r \in F[x]$ s.t $g = qf + r$ $deg(r) < deg(g)$ by the division and remainder algorithm. Therefore $r \in I$, and since f has minimal degree in I, $deg(r) = 0$ and $g \in \langle f \rangle$, so $I = \langle f \rangle$.

All rings lie on a sliding scale between being close to being a field and being far from being a field. A ring like the polynomial ring $\mathbb{Z}[x]$ is very far from being a field: the only units (multiplicatively invertible elements) are ± 1. If we want to turn $\mathbb{Z}[x]$ into a field, we can try to declare some of the non-units to be zero by factoring out the ideal generated by these elements. Recall that the **quotient** or **factor ring** of a ring R by an ideal I is the ring of cosets $\{r+I : r \in R\}/\sim$ where $r+I \sim s+I \iff r-s \in I$ and addition and multiplication are defined in the canonical way. Factoring $\mathbb{Z}[x]$ by the ideal $\langle x^2 \rangle$ is a bad choice since we miss out on the non-unit x, and $x + \langle x^2 \rangle$ is still a non-unit in $\mathbb{Z}[x]/\langle x^2 \rangle$. The failure is due to the fact $\langle x^2 \rangle \subset \langle x \rangle$, as we now show: if r is a non-unit and an ideal $I \subset \langle r \rangle$ is an ideal, then $r+I$ is a non-unit in R/I. Indeed, for $s \in R$,

$$(r+I)(s+I) = 1+I \iff rs-1 \in I \subset \langle r \rangle \implies 1 \in \langle r \rangle \iff \langle r \rangle = R \iff r \text{ is a unit .}$$

Therefore to form a field by factoring out an ideal we must factor by a **maximal ideal**: a proper ideal I only contained in R and itself. For example, the maximal ideals of $\mathbb{Z}$ are $p\mathbb{Z}$ where p is prime. We already know that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime, so in the ring $\mathbb{Z}$ quotienting by a maximal ideal is not only a sufficient, but also a necessary condition for forming a field. We will show that this is true in general.

Lemma 2.1.6. *A ring R is a field if and only if it contains no non-trivial ideals.*

Proof. If R is a field and I is an ideal containing r, then $1 = rr^{-1} \in I$, so $I = R$. Conversely, if R contains no trivial ideals, then for any $r \in R$, $\langle r \rangle = R$. In particular, $1 \in \langle r \rangle$ so $1 = sr$ for some $s \in R$. □

The correspondence theorem from group theory [3] is easily extended to a correspondence theorem for ideals, as we now show.

Lemma 2.1.7. *[Correspondence Theorem] For any ideal I of R there is a bijection between the set of ideals of R containing I and the set of ideals of R/I.*

Proof. The correspondence theorem for a normal subgroup $I \triangleleft R$ says that the canonical group homomomorphism $can : R \to R/I$ defines a bijection $J \mapsto can(J)$ between subgroups of R containing I and subgroups of R/I. This theorem applies to ideals since ideals are always normal subgroups under $+$. *can* also defines a ring homomorphism, and it is easy to see J is an ideal if and only if $can(J)$ is - we already know *can* takes abelian groups to abelian groups, so additionally if $J = rJ$ then $J + I = rJ + I$ by bijection on abelian groups and vice versa. Therefore, $J \mapsto can(J)$ is an injection between ideals J containing I and ideals in R/I. □

As an immediate consequence of Lemma 2.1.6 and Lemma 2.1.7, we get the following result.

Proposition 2.1.8. *An ideal I of R is maximal if and only if I/R is a field.*

Proof. I is maximal $\iff$ the only ideals containing I are I and R $\iff$ there are no nontrivial ideals in R/I $\iff$ R/I is a field.

□

What if we do not necessarily want to build a field, but are content with an integral domain? Recall that an integral domain is a ring R with no zero divisors. It is exactly the condition that allows us to "cancel out" multiplicatively:

$$ab = ac \implies b = c$$

in an integral domain whenever $a \neq 0$. This is done not by multiplying both sides by a^{-1} (which may not exist), but by noting the ring homomorphism

$$f : R \to R, \quad b \mapsto ab$$

has kernel $\{0\}$ and is therefore injective. To form an integral domain, an idea is to factor out the set S of all zero divisors of a ring R. However, this set does not form an ideal as the difference of two zero divisors need not be a zero divisor. For example, $[2][3] = [0]$ in $\mathbb{Z}_6$ but $[3] - [2] = [1]$ is not a zero divisor. For the same reason, taking the ideal $I = \langle S \rangle$ generated by S is not a good idea either: in the case of $\mathbb{Z}_6$ we would have $I = \mathbb{Z}_6$ whence $\mathbb{Z}_6/I$ is not even a ring. Instead, let us remark that R/I is an integral domain if for $x, y \in R$,

$$(x+I)(y+I) = I \iff x \in I \text{ or } y \in I.$$

Noting $(x+I)(y+I) = I \iff xy \in I$, we can now write down exactly the condition I needs to satisfy for R/I to be an integral domain.

Definition 2.1.9. A **prime ideal** I of R is a proper ideal such that $xy \in I \implies x \in I$ or $y \in I$.

Example 2.1.10. The prime ideals of $\mathbb{Z}$ are exactly $p\mathbb{Z}$ where p is prime. If $xy \in p\mathbb{Z}$ then either x or y is divisible by p, so either x or y is in $p\mathbb{Z}$. Conversely, in $nm\mathbb{Z}$ where $n, m > 1$, $nm \in nm\mathbb{Z}$ but $n, m \notin nm\mathbb{Z}$. Thus in $\mathbb{Z}$, prime ideals and maximal ideals coincide. In general, a maximal ideal I is always prime, since I is maximal $\iff$ R/I is a field $\implies$ R/I is an integral domain $\implies$ I is prime. However, the converse is not always true. For example, $\langle x \rangle$ is a prime ideal of $\mathbb{Z}[x]$, but it is not maximal, since

$$\langle x \rangle \subsetneq \langle x, 2 \rangle \subsetneq \mathbb{Z}[x].$$

It is a fun exercise to take any ring and try to build an integral domain out of it by factoring out a prime ideal. I give two more original examples.

Example 2.1.11. The set $C(\mathbb{R}, \mathbb{R})$ of continuous functions $f : \mathbb{R} \to \mathbb{R}$ can be given a ring structure, with the usual addition and multiplication (not composition) of functions. The additive identity is the constant function $x \mapsto 0$ and the multiplicative identity is $x \mapsto x$. $C(\mathbb{R}, \mathbb{R})$ is not an integral domain: take for example two continuous

functions

$$f(x) = \begin{cases} 0 & x \leq 0 \\ x & x > 0 \end{cases}, \qquad g(x) = \begin{cases} x & x \leq 0 \\ 0 & x > 0 \end{cases}$$

and note $f(x)g(x) = 0$. Let us try to build a prime ideal of $C(\mathbb{R},\mathbb{R})$. Let $a \in \mathbb{R}$ and consider the ideal I_a of all continuous functions $f \in C(\mathbb{R},\mathbb{R}) : f(a) = 0$. This set is clearly closed by subtraction and multiplication by continuous functions. Additionally, if $f(a)g(a) = 0$, then $f(a) = 0$ or $g(a) = 0$, so I_a is prime. It follows that $C(\mathbb{R},\mathbb{R})/I_a$ is an integral domain! The cosets $[f]$ are exactly the sets of functions g that take the same value $f(a) = g(a)$ at a.

Example 2.1.12. Another strange ring[1] is constructed as follows: take any set S and let $P(S)$ be the power set of S. Let multiplication be intersection $AB = A \cap B$ and let $A + B = (A \cup B) \setminus A \cap B$ be the **symmetric difference**: $x \in A + B \iff x \in A$ or $x \in B$ but not both. Clearly $+$ and $\times$ are commutative, and we have additive identity $\emptyset$ and multiplicative identity S. Additive inverses are given by $-A = S \setminus A$. For the distributive law, note $x \in A(B+C) = A \cap (B \cup C/B \cap C) \iff x \in A$ and $x \in B$ or C but not both $\iff x \in A \cap B$ or $x \in A \cap C$ but not both $\iff x \in A \cap B + A \cap C = AB + AC$.

Now clearly $P(S)$ is not an integral domain: $A(S \setminus A) = \emptyset$ for any $A \subset A$, so every element is a zero divisor. Since $0 \in P$ for any prime ideal P, prime ideals contain all zero divisors. Therefore $P(S)$ has no prime ideals, so $P(S)/I$ is not an integral domain for any I. It follows that $P(S)$ has no maximal ideals either. $P(S)$ is, however, a PID! Let I be any ideal of $P(S)$, and note I contains all the singletons $\{x\}$ such that $x \in B$ for some $B \in I$. This holds since $\{x\} = \{x\}B \in I$. Since I is closed under $+$, I also contains the union $U = \{x : x \in B \text{ for some } B \in I\}$. Letting $A \in I$ we have $A = AU$, so $I \subset \langle U \rangle \subset I$. Therefore $I = \langle U \rangle$ is principal. A very strange ring indeed!

Now let us recall this definition given in Chapter 1.

Definition 2.1.13. An invertible element $r \in R$ is called a **unit**. An element $r \in R$ of an integral domain is called **irreducible** if it is non-zero, not a unit and if $r = xy \implies x$ or y is a unit. $r \in R$ is **reducible** if it is neither 0, a unit, or irreducible.

Irreducible and reducible elements generalise the notion of, respectively, prime and composite numbers in $\mathbb{Z}$. The units in $\mathbb{Z}$ are ± 1, and certainly if we allow primes to be negative, p is prime if and only if $p = mn \implies m$ or $n = \pm 1$. In a field F every nonzero element is a unit, so fields do not have (ir)reducibles. The next proposition motivates defining principal ideal domains and irreducible elements.

Proposition 2.1.14. *If R is a PID, then $0 \neq r \in R$ is irreducible $\iff \langle r \rangle$ is maximal $\iff R/\langle r \rangle$ is a field.*

Proof. The second equivalence is just a restatement of Proposition 2.1.8. We may assume r is not a unit, as r is a unit if and only if $\langle r \rangle = R$, and $R/R = \{0\}$ is not a field.

($\implies$) Let r be irreducible and suppose $\langle r \rangle \subset J$ for some proper ideal J. Since R is a PID, $J = \langle s \rangle$ for some non-zero, non-unit $s \in R$. Therefore $r = ts$ for some $t \in R$.

[1] Found on `https://en.wikipedia.org/wiki/Ring_(mathematics)#Commutative_rings`. Accessed 18-03-2022.

Since r is irreducible and s is not a unit, t is a unit. Therefore $s = t^{-1}r$ so $\langle s \rangle \subset \langle r \rangle$. Since J was arbitrary, $\langle r \rangle$ is maximal.

($\Longleftarrow$) Now let $\langle r \rangle$ be maximal. Let $r = xy$ and suppose neither x nor y are units. It follows that $\langle r \rangle \neq \langle x \rangle$. Then

$$\langle r \rangle \subsetneq \langle x \rangle \subsetneq R,$$

a contradiction. Therefore r is irreducible. □

Example 2.1.15. In $\mathbb{Q}[x]$, x^2+1 is irreducible, since its roots are irrational so it cannot be written as a product of two linear polynomials in $\mathbb{Q}$. It follows that $\frac{\mathbb{Q}[x]}{\langle x^2+1 \rangle}$ is a field. In fact, it is isomorphic to $\mathbb{C}$: taking the quotient by x^2+1 is enforcing the rule $x^2+1=0$ i.e. defining $x = \sqrt{-1}$.

Remark 2.1.16. It is essential that R is a PID. For example, 2 is irreducible in $\mathbb{Z}[x]$ but $\frac{\mathbb{Z}[x]}{\langle 2 \rangle}$ is not a field, as $[x]$ is not a unit. This reflects the fact that $\mathbb{Z}[x]$ is not a PID, take for example the non-principal ideal $\langle 2, x \rangle$.

2.2 Noetherian rings and modules

Definition 2.2.1. A ring R is said to be **Noetherian** if every increasing sequence of ideals

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

terminates.

We can extend this definition to $R-$Modules, recalling an $R-$module is an abelian group M equipped with a (distributive, associative, identity-preserving) scalar multiplication function $R \times M \to M$. An $R-$module M is **Noetherian** if every increasing sequence of submodules

$$N_1 \subset N_2 \subset N_3 \subset \dots$$

terminates.

Note that R is trivially an $R-$module, and the submodules are exactly the ideals of R. Therefore R is a Noetherian ring if and only if it is a Noetherian $R-$module. If R is an $S-$module for some other ring S, then the story is more complicated: R may be a Noetherian ring without being a Noetherian $S-$module - see Remark 2.2.8.

Proposition 2.2.2. *The following are equivalent for an R-module M.*

(i) M is Noetherian.

(ii) Every non-empty collection of submodules of M has a maximal element.

(iii) Every submodule N of M is finitely generated as an R−module.

Proof. $(i) \implies (ii)$ easily: a counter-example to (ii) is exactly a collection of submodules containing a non-terminating increasing sequence of ideals. Additionally, $(ii) \implies (i)$ because any increasing sequence of submodules

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \dots$$

gives a collection $\{N_i\}_{i\geq 1}$ of ideals, which then has a maximal element.

$(i) \implies (iii)$ a non-finitely generated submodule N gives rise to a non-terminating sequence of submodules. Let $a_1 \in N$ and $N_1 = \langle a_1 \rangle = \{ra_1 : r \in R\}$. Then let $a_2 \in N \setminus N_1$ and $N_2 = \langle a_1, a_2 \rangle$. Continue this process for all natural numbers to construct the increasing sequence of submodules. It will never terminate as N is not finitely generated.

$(iii) \implies (i)$ Let

$$N_1 \subseteq N_2 \subseteq \dots$$

be an increasing chain of ideals. Then $\bigcup N_i$ is a submodule of M, and therefore finitely generated, say by $\{a_1, \dots a_n\}$. Letting m be the smallest integer such that

$$\{a_1, \dots a_n\} \subset N_m,$$

then N_m is a maximal element of the sequence. [13] □

Example 2.2.3. Any principal ideal domain is Noetherian, as all its ideals are generated by a single element.

Remark 2.2.4. Any ideal I of a Noetherian ring R is always contained in a maximal ideal: simply take the set of all proper ideals containing I. By Proposition 2.2.2, this set has a maximal element, which is then a maximal ideal. If one accepts Zorn's Lemma, then this statement is also true of general rings [13].

We now give some propositions that allow us to generate Noetherian modules from Noetherian rings. First, a result by Hilbert which relies on the axiom of choice.

Theorem 2.2.5 (Hilbert's basis theorem)**.** *If R is a Noetherian, so is $R[x]$.*

Proof. Suppose I is an ideal of $R[x]$ that is not finitely generated. Then we may choose $f_1 \in I$ of minimal degree. Now choose $f_2 \in I \setminus \langle f_1 \rangle$ of minimal degree. By assumption, we never have $I = \langle f_1, \dots, f_n \rangle$, so using the axiom of choice, we may continue this process indefinitely. The sequence $f_1, f_2, \dots$ is of (not necessarily strictly) increasing degree. The sequence of increasing ideals of leading coefficients of the f_i's

$$\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \dots$$

terminates since R is Noetherian, say at a_{n-1}. It follows that $a_n \in \langle a_1, \dots, a_{n-1} \rangle$, so $a_n = \sum_i^{n-1} r_i a_i$ for some $r_i \in R$. By multiplying by appropriate powers of x we may make the degrees of all the f_i's for $i < n$ equal $deg(f_n)$. Then

$$(\sum r_i f_i) - f_n \notin \langle f_1, \dots, f_{n-1} \rangle$$

and has degree less than f_n by construction. This contradicts f_n being of minimal degree. [1] □

Corollary 2.2.6. *If R is Noetherian, so is $R[x_1, x_2, x_3, \dots, x_n]$*

Proof. This follows by induction from Hilbert's basis theorem, by noting

$$R[x_1, x_2, x_3, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n].$$

□

Example 2.2.7. $\mathbb{Z}[x]$ is Noetherian as $\mathbb{Z}$ is. Any field F is clearly Noetherian, therefore $F[x]$ is also Noetherian.

Remark 2.2.8. If a ring R is Noetherian as an $S-module$ for a subring S, then R is also Noetherian as a ring: its ideals are submodules, which are finitely generated over S by assumption, hence also finitely generated over R as ideals.

The converse is **not** true. For example, by Theorem 2.2.5, $\mathbb{Z}[x]$ is Noetherian as a ring. However, it is not Noetherian as a $\mathbb{Z}$-module. Take for example, the non-terminating increasing sequence of submodules

$$R1 \subset \mathbb{Z}1 \oplus \mathbb{Z}x \subset \mathbb{Z}1 \oplus \mathbb{Z}x \oplus \mathbb{Z}x^2 \subset \dots$$

We will also want to show that any finitely generated R-module is Noetherian. (Recall M is finitely generated if there is a finite subset $m_1, \dots, m_n \subset M$ such that every $m \in M$ can be written as $m = r_1 m_1 + dots + r_n m_n$ for some $r_i \in R$.) By the remarks of Remark 2.2.8, this will show that any ring that is a finitely generated module over a Noetherian ring is a Noetherian ring. In particular, $\mathbb{Z}[\omega]$ is a Noetherian ring since $\mathbb{Z}$ is. Note that a submodule of a finitely generated module M need not be finitely generated in general. For example, $R = \mathbb{Z}[x_1, x_2, \dots]$ is a finitely generated $R-module$ with generating set $\{1\}$. However, the submodule $\langle x_1, x_2, \dots \rangle$ is not finitely generated as an $R-$module. We therefore cannot use property (iii) of Proposition 2.2.2 directly. The Noetherian property of R will have to play a key role. We will proceeed as in [13] by first proving a lemma.

Lemma 2.2.9. *Let M be an $R-$module and N be a submodule. Then M is a Noetherian $R-$module if and only if both N and M/N are.*

Proof. ($\Longrightarrow$) N is Noetherian, since its submodules are submodules of M, hence finitely generated. Additionally, a submodule of M/N is of the form A/N for a submodule A of M, so if $\{m_1, \dots m_n\}$ generates A, then $\{m_1 + N, \dots m_n + N\}$ generates A/N.

($\Longleftarrow$) Let

$$M_1 \subset M_2 \subset \dots$$

be an increasing sequence of submodules of M and note

$$M_1 \cap N \subset M_2 \cap N \dots$$

and

$$M_1/N \subset M_2/N \subset \dots$$

are increasing sequences of submodules of respectively N and M/N. By assumption, both terminate, say at $M_n \cap N$ and $M_{n'}/N$. Let m be any integer such that both sequences have terminated by the mth member. Now let $a \in M_{m+1}$. Since $M_m/N = M_{m+1}/N$, there is a $b \in M_m$ with $a - b \in N$. Note $a - b \in M_{m+1}$ since $M_m \subset M_{m+1}$. Since $M_m \cap N = M_{m+1} \cap N$, $a - b \in M_m$ as well, so $a \in M_m$. Since a was arbitrary, $M_m = M_{m+1}$. Since m was an arbitrary integer with $m > n, m > n'$, in fact $M_m = M_{m'}$ for all $m' > m$ so the sequence terminates. [13] □

Corollary 2.2.10. *If R is Noetherian, then any finitely generated module M over R is Noetherian.*

Proof. We prove this by induction on the generating elements of M. If M is generated by a single element m_1, then we have an ideal I of R given by $I = ker(f)$ for

$$f : R \to M, r \mapsto rm.$$

Since f is surjective, the first isomorphism theorem for R-modules gives $M \cong R/I$ and the latter is a Noetherian $R-$module by the lemma, since R is a Noetherian $R-$module.

Now suppose a Noetherian module M is generated by $\{m_1, \dots m_{n-1}\}$ and let M' be generated by $\{m_1, \dots m_{n-1}, m_n\}$. Then M'/M is generated by a single element $\{m_n\}$ and is therefore Noetherian as we have just shown. Since M was Noetherian, M' is Noetherian by the Lemma. [13]. □

We now reach our main motivation for examining Noetherian modules. In $\mathbb{Z}$, we can write any element as a product of primes. In general rings, we want to think about irreducibles instead of primes, so it is natural to ask: in which rings can elements be written as a product of irreducible elements? As it turns out, all Noetherian rings have this property, as proven in [13]. The proof given here is my own.

Lemma 2.2.11. *Any (non-zero, non-unit) element $r \in R$ of a Noetherian ring R can be written as a finite product of irreducible elements*

$$r = r_1 r_2 r_3 \dots r_n.$$

Proof. Let $A = \{$ proper principal ideals I containing $r\}$. $\langle r \rangle \in A$ so A is non-empty. Since R is Noetherian, A has a maximal element $\langle r_1 \rangle$. I claim r_1 is irreducible: it is not a unit since $\langle r_1 \rangle$ is a proper ideal. Furthermore, if $r_1 = ab$ for non-units a, b then $a \notin \langle r \rangle$ since b is not a unit. Then $r \in \langle a \rangle \not\subset \langle r_1 \rangle$ which contradicts r_1 being maximal among proper principal ideals containing r. This is all to show that there exists an irreducible dividing r. Now write $r = r_2' r_1$ and repeat the process on r_2' to find an irreducible r_2 dividing r_2'. This process either stops with r_n' being a unit, giving a finite factorisation $r = u r_1 r_2 r_3 \dots r_n$ for a unit u, or it gives an increasing chain

$$\langle r_1 \rangle \subset \langle r_1 r_2 \rangle \subset \dots$$

which by the Noetherian property terminates: say $\langle r_1 r_2 r_3 \dots r_{m-1} \rangle = \langle r_1 \dots r_m \rangle$. Then $r_1 r_2 \dots r_{m-1} = s r_1 r_2 \dots r_m$ for some $s \in R$, so since R is an integral domain, $1 = s r_m$ so r_m is a unit, a contradiction. □

We are mainly interested in Noetherian rings because of this factorisation property. However, not only Noetherian rings have this property. As an example, let $x \in \mathbb{Z}[x_1, x_2, \dots]$, the ring of polynomials in infinitely many variables, which we have already argued is not Noetherian. Nonetheless, since x is also in the Noetherian ring $\mathbb{Z}[x_1, x_2, \dots, x_n]$ for some n depending on x, x factorises into a product of irreducibles in $\mathbb{Z}[x_1, x_2, \dots, x_n]$, which are easily seen to also be irreducible in $\mathbb{R}[x_1, x_2, \dots]$. $\mathbb{Z}[x_1, x_2, \dots]$ therefore has the factorisation property despite not being Noetherian.

Definition 2.2.12. An integral domain R is a unique factorisation domain (UFD) if every non-zero non-unit $r \in R$ can be written as a product of irreducible elements $r = r_1 r_2 \dots r_n$ **uniquely** up to reordering and multiplication by units.

Definition 2.2.13. A non-zero non-unit $p \in R$ of an integral domain is **prime** if $p|ab \implies p|a$ or $p|b$.

Remark 2.2.14. Note $p \in R$ is prime exactly when $\langle p \rangle$ is a prime ideal, since $p|a \iff a \in \langle p \rangle$.

We argued that the correct notion of "primeness" was irreducibility. We can show that this new notion is strictly stronger: every prime element is irreducible: Let r be prime and $r = xy$. Then $r|xy$, so without loss of generality, $r|x \implies x = cr$ for some $c \in R$. Then

$$r = rcy \implies r(1-cy) = 0 \implies cy = 1 \text{ (integral domain)} \implies y \text{ is a unit.}$$

Additionally, as is easily shown, $\langle p \rangle$ is a prime ideal. As we now show, prime elements give rise to a easier UFD condition.

Proposition 2.2.15. *A Noetherian ring R is a UFD if and only if every irreducible element $r \in R$ is prime.*

Proof. ($\implies$) Let $r \in R$ be irreducible and let $r|xy$. By uniqueness of the factorisation into irreducibles, r appears in the unique factorisation of either x or y, so $r|x$ or $r|y$.

($\impliedby$) By Lemma 2.2.11, any element has a decomposition into irreducibles. We only need to take care of uniqueness. Suppose $r = r_1 r_2 r_3 \dots r_n = s_1 s_2 \dots s_m$ are two decompositions into irreducibles. Since r_1 is prime, $r_1|s_i$ for some i. Since s_i is irreducible, $s_i = ur_1$ for some unit u. Since R is an integral domain,

$$r_2 r_3 \dots r_n = u s_2 s_3 \dots s_m,$$

where we have relabeled the s_i's. We can define $r_2' = r_2 u^{-1}$, which is also irreducible, then continue as before. If $m = n$ we have shown that every $r_i = u_i s_j$ for some j and unit u_i, as required. Otherwise, WLOG, suppose $m > n$. Then at the end, after relabeling the s_i's, we have

$$\bar{u} = s_1 \dots s_k.$$

Then $s_i|\bar{u} \implies \bar{u} = z s_i$ for some z. Then $(\bar{u}^{-1} z) s_i = 1$, so s_i is a unit, a contradiction. [13] □

It is an easy corollary that every PID is a UFD, as we now remark.

Corollary 2.2.16. *Any principal ideal domain R is a UFD.*

Proof. PIDs are integral domains by definition and we have already remarked that they are Noetherian. For an irreducible $r \in R$, $\langle r \rangle$ is maximal by Proposition 2.1.14, in particular it is prime by Example 2.1.10. It follows that r is prime. □

Example 2.2.17. By Example 2.1.5, $\mathbb{Z}_p[x]$ is a PID where p is prime and $\mathbb{Z}_p$ is the finite field of p elements. It follows that $\mathbb{Z}_p[x]$ is a UFD.

Chapter 3

Number fields and number rings

We start this chapter with a brief summary of Galois theory applied to finite dimensional field extensions of $\mathbb{Q}$. Much of this is standard material covered in any undergraduate level Galois course, including one I was enrolled in while writing this dissertation. I have included proofs for results that were new to me at the time of writing and were independently researched from [9].

3.1 Number fields

A **number field** is a subfield of $\mathbb{C}$ that is a finite dimensional vector space over $\mathbb{Q}$. Examples include $\mathbb{Q}$ itself, $\mathbb{Q}[\omega]$ where $\omega = e^{2\pi i/p}, p$ prime - the **p-th cyclotomic field**, and $\mathbb{Q}[\sqrt{n}] = \{a + b\sqrt{n} : a,b \in \mathbb{Q}\}$. Non-examples include $\mathbb{R}$ and $\mathbb{C}$: both are vector spaces over $\mathbb{Q}$, but by virtue of being uncountable, could never have a finite basis over a countable field. The examples $\mathbb{Q}[\sqrt{n}]$ and $\mathbb{Q}[e^{2\pi i/p}]$ have the following in common: both $\sqrt{n}$ and $e^{2\pi i/n}$ satisfy a monic (leading coefficient 1) polynomial over $\mathbb{Q}$. If every element of a ring R satisfies a monic polynomial with coefficients in a subring S we say R is **integral over** S. If a field F is integral over a subfield K we say F is **algebraic over** K. Thus we claim that $\mathbb{Q}[\sqrt{n}]$ and $\mathbb{Q}[e^{2\pi i/p}]$ are algebraic over $\mathbb{Q}$.

Example 3.1.1. $\sqrt{n}$ is algebraic over $\mathbb{Q}$, as it satisfies $f(x) = x^2 - n$. If n is not a square of another integer, then the two roots of f are irrational. It follows that f is irreducible, as it cannot written as a product of linear polynomials in $\mathbb{Q}$. If $n = m^2$ then $x^2 - n$ is not irreducible, but $f(x) = x - m$ is.

Example 3.1.2. $\omega = e^{2\pi i/p}$ is algebraic over $\mathbb{Q}$. It satisfies the monic $f(x) = x^p - 1$. Note f is not irreducible as it is divisible by $(x-1)$. We have already shown (Eq. (1.2)) that $\frac{x^p-1}{x-1} = (x-\omega)\dots(x-\omega^{p-1}) =: g(x)$ when $x \neq 1$. We may additionally note

$$(1+x+x^2+\cdots+x^{p-1})(x-1) = (x+x^2+\cdots+x^p) - (1+x+x^2+\cdots+x^{p-1}) = x^p - 1.$$

Therefore, when $x \neq 1$,

$$g(x) = (1+x+x^2+\cdots+x^{p-1}),$$

and since both functions are analytic on all of $\mathbb{C}$ they also equal on $x = 1$. g is therefore a monic rational polynomial satisfied by ω. In fact, g is irreducible, as shown in [8].

Remark 3.1.3. It was important in Example 3.1.2 that p is prime. $e^{2\pi i/n}$ for $n \in \mathbb{N}$ is certainly algebraic over $\mathbb{Q}$ since it satisfies $x^n - 1$, but $1 + x + x^2 + \cdots + x^{n-1}$ is **not** irreducible over $\mathbb{Q}$ in general. For example, $e^{2\pi i/6}$ satisfies $f(x) = x^2 - x + 1 = 0$: simply check $e^{2\pi i/3} - e^{\pi i/3} = 2\cos(\pi/3) = 1$. As shown in [8], irreducible polynomials are always of minimal degree among polynomials annihilating a, so the existence of f shows $(1 + x + \cdots + x^5)$ is not irreducible.

Example 3.1.1 and Example 3.1.2 have two things in common: in both cases the annihilating monic polynomial $f \in \mathbb{Q}[x]$ can be taken to be irreducible, and in both cases $\mathbb{Q}[a]$ is a number field. It is a standard result of Galois theory that these properties hold in generality: if a is algebraic over $\mathbb{Q}$, its monic annihilating polynomial can be taken to be irreducible, and $\mathbb{Q}[a]$ is a number field. We will also show that any $\alpha \in Q[a]$ is also algebraic over $\mathbb{Q}$. Finally, we will show that any number field is of this form.

Recall the following definition.

Definition 3.1.4. If L and K are fields with an injective field homomorphism $K \to L$ then L is said to be a **field extension** of K, and we write $L : K$. The degree of L as a vector space over K is denoted $[L : K]$.

The following two lemmas are core results of Galois theory, and we refer to [8] for their proofs.

Lemma 3.1.5. *If $f \in \mathbb{Z}[x]$ is monic and $f = gh$ where $g, h \in \mathbb{Q}[x]$ are monics, then in fact $g, h \in \mathbb{Z}[x]$.*

Lemma 3.1.6. *Let M be a field extension of K and let $\alpha \in M$ be algebraic over K. Then there exists an irreducible monic $f \in K[x]$ s.t. $f(\alpha) = 0$.*

Lemma 3.1.7. *Let $K[\alpha] : K$ be a field extension where α is algebraic over K and satisfies monic irreducible f. Then $K[x]/\langle f \rangle \cong K[a]$.*

Remark 3.1.8. Lemma 3.1.6 and Lemma 3.1.7 together prove that the $n-$th cyclotomic fields $\mathbb{Q}[\omega], \omega = e^{2\pi i/n}$ are number fields without explicitly constructing their monic irreducible polynomial over $\mathbb{Q}$.

We will now restrict ourselves to finite-dimensional field extensions between number fields K and L. Note by assumption, $[L : \mathbb{Q}]$ and $[K : \mathbb{Q}]$ are finite - it follows that $[L : K]$ is finite.

The following lemma will show that if L is a field extension of K then any $a \in L$ is algebraic over K. The statement and proof is a generalisation of a theorem from [9].

Lemma 3.1.9. *Let R be a ring and N be a finitely-generated $R-$module. Then any $a \in N$ is integral over R.*

Proof. Let M have generating set $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ and write $a\alpha_j = \sum a_{ij}\alpha_i$ for each j to produce a matrix equation

$$\begin{pmatrix} a\alpha_1 \\ a\alpha_2 \\ \cdots \\ a\alpha_n \end{pmatrix} = \begin{pmatrix} \sum a_{i1}\alpha_i \\ \sum a_{i2}\alpha_i \\ \cdots \\ \sum a_{in}\alpha_i \end{pmatrix} =: M \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \cdots \\ \alpha_n \end{pmatrix}$$

In other words,

$$(aI - M)\begin{pmatrix}\alpha_1\\ \alpha_2\\ \cdots\\ \alpha_n\end{pmatrix} = 0. \tag{3.1}$$

Therefore $\det(aI - M) = 0$. Expanding out the determinant gives a monic degree n polynomial over R satisfied by a, as required. [9] □

Example 3.1.10. The proof of Lemma 3.1.9 gives a recipe for finding monic polynomials over $\mathbb{Q}$ satisfied by any element of a number field. For example,$\mathbb{Q}[\sqrt{2}]$ has basis $\{1, \sqrt{2}\}$ over $\mathbb{Q}$. For $a = 1 + \frac{1}{2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, Eq. (3.1) reads

$$\begin{pmatrix}(1+\frac{1}{2}\sqrt{2}) - 1 & -\frac{1}{2}\\ -1 & (1+\frac{1}{2}\sqrt{2}) - 1\end{pmatrix}\begin{pmatrix}1\\ \sqrt{2}\end{pmatrix} = 0$$

Setting the determinant to zero gives $(a-1)^2 - \frac{1}{2} = 0$ such that $1 + \frac{1}{2}\sqrt{2}$ is algebraic over $\mathbb{Q}$ with monic annihilating polynomial $f(x) = x^2 - 2x + \frac{1}{2}$. In fact f is the unique monic irreducible, as both its roots are irrational. It is important to note, however, that this process may yield a reducible polynomial.

We finish off the section by classifying all number fields. It turns out to be helpful to work not with the vector space structure of a number field L over $\mathbb{Q}$, but rather with embeddings (injective field homomorphisms) $L \to \mathbb{C}$ that restrict to the identity on $\mathbb{Q}$. To explore this link, we need to borrow some results from Galois theory. We will roughly follow Appendix 2 of [9].

Lemma 3.1.11. *Let $\alpha \in \mathbb{C}$ be algebraic over a number field K with monic irreducible f of degree n. Then f has n distinct roots in $\mathbb{C}$.*

Proof. Since $\mathbb{C}$ is algebraically closed, f has n roots counted with multiplicity. We in fact claim these roots are pairwise distinct. Suppose $l(x)$ is linear with $f(x) = l(x)^2 g(x)$. Taking derivates, $f'(x) = 2l(x)g(x) + l(x)^2 g(x)$, so $l | f'$. However, since $I = \langle f \rangle$ is maximal in $K[x]$ and $f'(x) \notin I$, $\langle f, f' \rangle = K[x]$. It follows that

$$1 = f(x)g(x) + f'(x)h(x)$$

for some $g, h \in K[x]$. This is a contradiction since l divides the RHS but not the LHS. [9] □

Definition 3.1.12. Let $a \in \mathbb{C}$ be algebraic over K with irreducible monic f over a number field K. If $b \in \mathbb{C}$ is such that $f(b) = 0$, then a and b are said to be **conjugate over** K.

Let us firstly note that conjugacy over K is an equivalence relation. Additionally, if $\sigma : K \to \mathbb{C}$ is an embedding of a number field, then $\sigma(a)$ must be conjugate to a over $\mathbb{Q}$ by the properties of field homomorphisms: if f is the monic irreducible polynomial over $\mathbb{Q}$ satisfied by a, then

$$\sigma(f(a)) = \sigma(\sum_{i=0}^{n} a_i a^i) = \sum_{i=0}^{n} a_i \sigma(a)^i.$$

Proposition 3.1.13. *Every embedding $K \to \mathbb{C}$ extends to exactly $[L:K]$ embeddings of L in $\mathbb{C}$.*

Proof. Let $\{a_1, a_2, \ldots, a_n\}$ be a basis for L over K. Note

$$L = span(a_1, \ldots, a_n) \subset K[a_1, a_2, \ldots, a_n] \subset L.$$

Therefore $L = K[a_1, a_2, \ldots, a_n]$. Note furthermore that

$$K[a_1, a_2, \ldots, a_n] = K[a_1, \ldots, a_{n-1}][a_n],$$

so we may work inductively on the basis elements. The result is clear if $L = K$, so set $J = K[a_1, a_2, \ldots, a_k]$ and suppose every embedding of K extends to $[J:K]$ embeddings of J. Let $L = J[a]$, $\sigma : J \to \mathbb{C}$ be an embedding and f be the irreducible monic of a over J. By Lemma 3.1.11, f has $n = deg(f)$ distinct roots in $\mathbb{C}$, which are the conjugates of a. $\sigma(a)$ is necessarily one of these conjugates, and each choice of conjugate b defines an embedding of L restricting to σ on J in the following way:

$$\sigma f(a) = \sigma\big(\sum_{i=0}^{n} c_i a^i\big) = \sum_{i=0}^{n} \sigma(c_i) b^i.$$

Since there was no choice involved other than the choice $a \mapsto b$, every embedding of L restricting to σ on J is of this form. There are therefore $n = deg(f)$ such embeddings. Since $L \cong J[x]/\langle f \rangle$, $[L:J] = deg(f)$.

We have shown that every embedding of K extends to $[L:J][J:K]$ embeddings of $J[a]$. To finish the inductive proof, we need to show this equals $[L:K]$, let $\{b_1, b_2, \ldots, b_n\}$ be a basis of J over K and $\{c_1, c_2, \ldots, c_m\}$ be a basis of L over J. This gives a basis $\{b_i c_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ of size nm. It is easy to show this spans L, and

$$\sum_{i \leq n, j \leq m} a_{ij} b_i c_j = 0 \implies \sum_{j \leq m} \big(c_j \sum_{i \leq n} a_{ij} b_i\big) = 0$$

$$\implies \forall j, \sum_{i \leq n} a_{ij} b_i = 0 \text{ (linear independence of the } c_j\text{'s)}$$

$$\implies \forall (i,j), a_{ij} = 0 \text{ (linear independence of the } b_i\text{'s)},$$

giving linear independence. [9] □

Our desired corollary follows directly by considering the canonical inclusion $K \to \mathbb{C}$ as an embedding.

Corollary 3.1.14. *There are $[L:K]$ embeddings of L in $\mathbb{C}$ restricting to the canonical inclusion on K.*

We now justify studying the field extensions of the form $K[a]$ by proving every finite degree number field extension is of this form.

Theorem 3.1.15. *For every number field extension $K \subset L$, $L = K[\alpha]$ for some $\alpha \in L$.*

Proof. We proceed by induction on $n = [L:K]$. The proof is clear in the case $L = K = K[1]$. Now suppose $K[a_1, \ldots, a_n] = K[\alpha]$ for some $\alpha \in L$ and let $L = K[\alpha, \beta]$ for

$\beta \notin K[\alpha]$. Let $0 \neq a \in K$ and consider $\alpha + a\beta$. Suppose for sake of contradiction that $K[\alpha + a\beta] \neq L$. Then $[K[\alpha + a\beta] : K] < n$ where we recall $[K[\alpha + a\beta] : K]$ is the number of conjugates of $\alpha + a\beta$ over K. There are n embeddings of L restricting to the identity on K, and since each one takes $\alpha + a\beta$ to one of its conjugates, of which there are fewer than n, $\sigma(\alpha + a\beta) = \sigma'(\alpha + a\beta)$ for two such embeddings σ, σ'. Since these are field homomorphisms fixing K,

$$\sigma(\alpha) + a\sigma(\beta) = \sigma'(\alpha) + a\sigma'(\beta)$$

so

$$a = \frac{\sigma(\alpha) - \sigma'(\alpha)}{\sigma(\beta) - \sigma'(\beta)}$$

Note the denominator is always nonzero since if $\sigma(\beta) = \sigma'(\beta)$ then $\sigma(\alpha) = \sigma'(\alpha)$ as well, which would imply σ and σ' equal on all of L which we assumed they didn't.

Since there are only finitely many choices for $\sigma(\alpha), \sigma(\alpha'), \sigma(\beta)$ and $\sigma(\beta')$,

$$K[\alpha + a\beta] \neq L$$

for only finitely many $a \in K$. Choosing any other a will give the desired result. [9] $\square$

Example 3.1.16. Consider $L = \mathbb{Q}[i, \sqrt{3}]$ as a field extension of $\mathbb{Q}$. The conjugates of i over $\mathbb{Q}$ are $\pm i$ and the conjugates of $\sqrt{3}$ over $\mathbb{Q}$ are $\pm\sqrt{3}$. Since $\frac{\pm 2i}{\pm 2\sqrt{3}} \notin \mathbb{Q}$, the proof of Theorem 3.1.15 gives that $L \cong \mathbb{Q}[i + a\sqrt{3}]$ for any non-zero $a \in \mathbb{Q}$.

Example 3.1.17. Let us show that

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{4}, \ldots, \sqrt{n}] = \mathbb{Q}[\sqrt{2} + \sqrt{3} + \sqrt{5} + \ldots \sqrt{p}]$$

where p is the largest prime $p \leq n$. It is clear that

$$\mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{4}, \ldots, \sqrt{n}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \ldots, \sqrt{p}]$$

since $\sqrt{nm} \in \mathbb{Q}[\sqrt{n}, \sqrt{m}]$. We may work inductively. $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$ by a similar argument to the previous example. Let $s_q = \sqrt{2} + \sqrt{3} + \cdots + \sqrt{q}$ and consider $\mathbb{Q}[s_q, \gamma]$ where γ is the next prime after q. Let σ, σ' be two embeddings of $\mathbb{Q}[s_q, \gamma]$ fixing $\mathbb{Q}$. Since these are field homomorphisms sending conjugates to conjugates, $\sigma(s_q) - \sigma'(s_q) = \pm 2\sqrt{2}\delta_2 + \pm 2\sqrt{3}\delta_3 + \cdots + \pm 2\sqrt{q}\delta_q$, where $\delta_i = 0$ or 1 and not all δ_i are 0. Since

$$1 \neq \frac{\pm 2\sqrt{2}\delta_2 + \pm 2\sqrt{3}\delta_3 + \cdots + \pm 2\sqrt{q}\delta_q}{\pm 2\sqrt{\gamma}},$$

the proof of Theorem 3.1.15 gives $\mathbb{Q}[s_q, \gamma] \cong \mathbb{Q}[s_q + \gamma]$.

3.2 Normal field extensions

We give a brief remark that any field extension can always be extended to a normal extension, defined below. We again follow [9]

Definition 3.2.1. A field extension L of K is said to be **normal** if each of the $[L:K]$ embeddings of L restricting to the inclusion on K are automorphisms.

Note this equivalent to L containing all its conjugates over K: if $a \in L$ and $a \sim b$ then there is an embedding of L fixing K such that $a \mapsto b$ – take any extension, guaranteed by Proposition 3.1.13, of the embedding $K[a] \to \mathbb{C} : \sum a_i a^i \mapsto \sum a_i b^i$. Since this embedding is an automorphism, $b \in L$. Since a, b were arbitrary, L contains all its conjugates over K.

Conversely, by Theorem 3.1.15 we can set $L = K[\alpha]$. Every embedding fixing K is entirely determined by a choice of conjugate $\alpha \mapsto \beta$. If $\beta \in L$, then

$$\sigma(\sum a_i \alpha^i) = \sum a_i \beta^i \in L$$

so this embedding is an automorphism.

Theorem 3.2.2. *Every finite field extension $K \subset L$ can be extended to a finite normal field extension $K \subset L \subset M$ (normal over both K and L).*

Proof. By Theorem 3.1.15 we may write $L = K[\alpha_1]$ for some $\alpha_1 \in L$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the $n = [L:K]$ conjugates of α_1 over K. Let $M = K[\alpha_1, \alpha_2, \ldots, \alpha_n]$ be a field extension of L (and by extension K) via the inclusion $L \to M$. We need to show M contains all its conjugates over K, and we will then get the second part for free. Indeed, any embedding of M restricting to the inclusion on L also restricts to the inclusion on K and would therefore be an automorphism.

By construction, M contains all the conjugates of α_1. Let σ be an embedding of M fixing K, and let $x = \sum_i \sum_j a_{ij} \alpha_j^i$ be an element of M. σ maps x to one of its conjugates, and as σ is a field homomorphism, $\sigma(x) = \sum_i \sum_j a_{ij} \sigma(\alpha_j)^i \in M$. Therefore M contains all its conjugates over K. [9] □

3.3 Number rings

Inside a number field sit the **algebraic integers**: the elements integral over $\mathbb{Z}$. Letting $\mathbb{A}$ be the algebraic integers in $\mathbb{C}$, we define a **number ring** as the ring $\mathbb{A} \cap K$ of algebraic integers in a number field K. For Fermat's Last Theorem, we are particularly interested in the number ring $\mathbb{A} \cap \mathbb{Q}[\omega]$, where $\mathbb{Q}[\omega]$ is the p-th cyclotomic field for p prime. Of course, we would like to prove that number rings are indeed rings. As shown in [9], this follows from the fact that $a \in \mathbb{C}$ is an algebraic integer iff $\mathbb{Z}[a]$ is a finitely generated $\mathbb{Z}-$module. In fact we prove this more generally for an element a of a field integral over a subring R.

Proposition 3.3.1. *The following are equivalent for an element a of a field L with subring R.*

(1) a is integral over R.

(2) $R[a]$ is a finitely generated R-module

(3) There is a nonzero finitely generated $R-$module M with $aM \subset M$.

Proof. $(1 \implies 2)$ $R[a]$ is clearly a $R-$module for any a. Let $f \in R[x]$ be a monic annihilating polynomial of a of degree n. Then I claim $\{1, a, a^2, \ldots, a^{n-1}\}$ is a generating set for $R[a]$. For an arbitrary element $\alpha = \sum_i^m a_i a^i \in R[a]$ where $m \geq n$ we can let $g(x) = a_m x^{m-n} f(x)$ s.t. $g(a) = 0$. It follows that

$$\alpha = \sum_i^m a_i a^i = \sum_i^m a_i a^i - g(a),$$

and by construction the RHS can be rewritten in the form $\sum_i^{m-1} a_i' a^i$. We may repeat this process $m-(n-1)$ times until α is written in the form $\alpha = \sum_i^{n-1} a_i^* a^i$.

$(2 \implies 3)$ trivially, taking $M = R[a]$.

$(3 \implies 2)$ follows directly from Lemma 3.1.9. □

Corollary 3.3.2. *Number rings are rings.*

Proof. We show the algebraic integers $\mathbb{A} \in \mathbb{C}$ form a ring. By the subring test, it is enough to show that number rings are closed under multiplication and subtraction, and contain 1. 1 is clearly an algebraic integer. If $\mathbb{Z}[a]$ and $\mathbb{Z}[b]$ are finitely generated, then so is $Z[a,b]$ with generating set $\{a_i b_j\}$ where $\{a_i\}$ and $\{b_j\}$ are the finite generating sets of $\mathbb{Z}[a]$ and $\mathbb{Z}[b]$ respectively. Since $a+b, ab \in \mathbb{Z}[a,b]$ they are both algebraic by Lemma 3.1.9.

Finally, we note that the intersection of two rings is always a ring, therefore $\mathbb{A} \cap R$ is a ring for any ring $R \subset \mathbb{C}$. □

Example 3.3.3. As in Example 3.1.10, we can use Lemma 3.1.9 as a recipe for finding monic polynomials over $\mathbb{Z}$ satisfied by an algebraic integer a, given a generating set for $\mathbb{Z}[a]$. For example, take $a = i + \sqrt{2}$. $\mathbb{Z}[i]$ has generating set $\{1, i\}$ and $\mathbb{Z}[\sqrt{2}]$ has generating set $\{1, \sqrt{2}\}$. By the proof of *Corollary* 3.3.2, $i + \sqrt{2} \in \mathbb{Z}[i, \sqrt{2}]$ which has generating set $\{1, i, \sqrt{2}, \sqrt{2}i\}$. Then Eq. (3.1) reads

$$\begin{pmatrix} (i+\sqrt{2}) & -1 & -1 & 0 \\ 1 & i+\sqrt{2} & 0 & -1 \\ -2 & 0 & i+\sqrt{2} & -1 \\ 0 & -2 & 1 & i+\sqrt{2} \end{pmatrix} \begin{pmatrix} 1 \\ i \\ \sqrt{2} \\ i\sqrt{2} \end{pmatrix} = 0$$

The determinant of this matrix expands to

$$a^4 - 2a^2 + 9$$

so $i + \sqrt{2}$ is an algebraic integer satisfying monic $f(x) = x^4 - 2x^2 + 9$ over $\mathbb{Z}$.

Remark 3.3.4. Note Lemma 3.1.5 shows that if $a \in K$ is an algebraic integer, then its monic irreducible polynomial over $\mathbb{Q}$ has integer coefficients. If a satisfies $f \in \mathbb{Z}[x]$ and has monic irreducible $g \in \mathbb{Q}[x]$ then $f = gh$ for some $h \in \mathbb{Q}[x]$ since $f \in \langle g \rangle$, and so $g \in \mathbb{Z}[x]$ by the lemma.

Lemma 3.3.5. *If $A \subset B \subset C$ are rings such that C is integral over B and B is integral over A, then C is integral over A.*

Proof. Let $c \in C$ and write $c = b_0 + b_1 c + \cdots + b_{n-1}c^{n-1} + c^n = 0$. Let $B' = A[b_0, b_1, \ldots, b_{n-1}] \subset B$ so B' is integral over A hence finitely generated as an A-module by Proposition 3.3.1. Additionally, $B'[c]$ is a finitely generated $B'-$module, also by Proposition 3.3.1. It follows that $B'[c]$ is a finitely generated A-module with $cB'[c] \subset B'[c]$ so c is integral over A by Proposition 3.3.1. □

Lemma 3.1.9 and Lemma 3.3.5 show that a complex number α is algebraic over any number field K if and only if it is algebraic over $\mathbb{Q}$. One direction is clear, and the lemma gives the other direction. Thus we may simply call such elements algebraic.

3.4 The p-th cyclotomic fields

We are now ready to prove a remarkable and impactful result which is core to Kummer's proof of Fermat's Last Thereom.

Theorem 3.4.1. *For the $p-$th cyclotomic fields $\mathbb{Q}[\omega]$,*

$$\mathbb{A} \cap \mathbb{Q}[\omega] = \mathbb{Z}[\omega].$$

In fact this statement is true for all n-th cyclotomic fields [9], but the proof of this is more involved and not needed for our purposes. Let us first note that every element in $\mathbb{Z}[\omega]$ is an algebraic integer. This follows directly from Proposition 3.3.1 since $\mathbb{Z}[\omega]$ is a finitely generated $\mathbb{Z}$-module with generating set $\{1, \omega, \omega^2, \ldots, \omega^{p-1}\}$.We proceed as in [9], using the $[K : \mathbb{Q}]$ embeddings of a number field K in $\mathbb{C}$ fixing $\mathbb{Q}$ to define the **norm** and **discriminant** of K.

Definition 3.4.2. Let $n = [K : \mathbb{Q}]$ and let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be the n embeddings of K in $\mathbb{C}$ fixing $\mathbb{Q}$. Let $\alpha \in K$. The **norm** N of K is the function

$$\alpha \mapsto \sigma_1(\alpha)\sigma_2(\alpha)\ldots\sigma_n(\alpha).$$

We will sometimes write N^K to emphasize which number field we are considering the embeddings of.

The first goal is to show that the codomain of N s in fact $\mathbb{Q}$. Furthermore, we wish to show that $N(\alpha) \in \mathbb{Z}$ if α is an algebraic integer. Firstly note since the σ_i's are field homomorphisms that fix $\mathbb{Q}$,

$$N(r\alpha\beta) = r^n N(\alpha)N(\beta).$$

Lemma 3.4.3. *For any $\alpha \in K$, $N(\alpha) \in \mathbb{Q}$. If α is an algebraic integer, then $N(\alpha) \in \mathbb{Z}$.*

Proof. Let α be integral over R where $R = \mathbb{Q}$ or $\mathbb{Z}$. By Remark 3.3.4, the monic irreducible polynomial of α over $\mathbb{Q}$ has coefficients in R. First suppose $K = \mathbb{Q}[\alpha]$. Then each embedding σ_i of K fixing $\mathbb{Q}$ is uniquely defined by a choice of conjugate of α aka root of f. Therefore $N(\alpha)$ is the product of the roots of f, which is $\pm\frac{a_0}{a_n} = \pm a_0 \in R$ where $a_n = 1$ since f is monic.

For general K, each embedding fixing $\mathbb{Q}$ restricts to one of these on $\mathbb{Q}[\alpha]$. Furthermore, each σ_i extends to $n := [K : \mathbb{Q}[\alpha]]$ embeddings of K. Therefore

$$N(\alpha) = \sigma_1(\alpha)^n \sigma_2(\alpha)^n \dots \sigma_k(\alpha)^n = (\sigma_1(\alpha) \dots \sigma_k(\alpha))^n \in R.$$

□

We will return to the norm later. Our next goal is to show that number rings are free abelian as additive groups. Our goal will be to sandwich number rings between two free abelian groups of the same rank. Recall an abelian group G is said to be free abelian of rank n if $G \cong \mathbb{Z}^n$. Recall the following fundamental theorem of group theory which we state without proof - see [3].

Theorem 3.4.4 (Fundamental theorem of finitely generated abelian groups.)**.** *If A is a finitely generated abelian group then*

$$A \cong \mathbb{Z}^n \times \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_m}$$

for some $k_1 | k_2 | \dots | k_m$.

Corollary 3.4.5. *Every subgroup G of a finitely generated free abelian group A is free.*

Proof. This follows from the fundamental theorem by noting G cannot have any elements of order n, since A does not. □

It should be clear that G cannot have a greater rank than A. As argued in [9], it follows that if the number ring contains and is contained by free abelian groups of rank n, then it must itself be free abelian of rank n.

Next, we would like to show that any number field has a basis consisting entirely of algebraic integers. Such a basis is called an **integral basis**. We fill in the details of the following proof from [9].

Proposition 3.4.6. *Any number field K has an integral basis.*

Proof. Take any basis $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$. Let $f \in \mathbb{Q}[x]$ be the monic irreducible satisfied by α_1 and of degree n. Let

$$f = \sum_{i=0}^{n} \frac{a_i}{b_i} x^i$$

where the $\frac{a_i}{b_i}$ are written in lowest terms and $a_n = b_n = 1$. Let $d_1 = lcm(b_0, b_1, \dots, b_n)$. Then α_1 satisfies

$$d_1^n \cdot f(a) = \sum_{i=0}^{n} a_i \frac{d_1^{n-i}}{b_i} (d_1 \alpha_1)^i = 0.$$

By construction, the $\frac{d_1^{n-1}}{b^i}$ are integers, and the $n-$th coefficient is 1. This defines a monic polynomial in integer coefficients satisfied by $d_1\alpha_1$. Repeating this process for each α_i gives a set of algebraic integers $\{d_1\alpha_1, \dots, d_n\alpha_n\}$ which is also a basis for R. □

As argued in [9], this shows that R contains the free abelian group of rank n

$$d_1\alpha_1\mathbb{Z} \times d_2\alpha_2\mathbb{Z} \times \cdots \times d_n\alpha_n\mathbb{Z}.$$

Definition 3.4.7. For any $n-$tuple of elements $(\alpha_1, \alpha_2, \ldots \alpha_n)$ of K, the **discriminant** is

$$disc(\alpha_1, \alpha_2, \ldots, \alpha_n) = |[\sigma_i(\alpha_j)]|^2$$

i.e. the square of the discriminant of the matrix with (i,j)th element $\sigma_i(\alpha_j)$. We also introduce the shorthand $disc(\omega)$=$disc(1, \omega, \omega^2, \ldots, \omega^{p-1})$ for $p = e^{2\pi i/p}$.

Proposition 3.4.8. *Fix an integral basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ of $B = \mathbb{A} \cap K$ over $\mathbb{Q}$. Let $d = disc(\alpha_1, \ldots, \alpha_n)$. Then any $r \in R$ can be written as*

$$r = \frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d}$$

for integers m_i s.t. $d|m_i^2$.

Proof. Write $r = q_1\alpha_1 + \cdots + q_n\alpha_n, q_i \in \mathbb{Q}$. Let $\sigma_1, \ldots \sigma_n$ be the embeddings of K in $\mathbb{C}$. Applying each σ_i to the above equation gives a matrix equation

$$\begin{pmatrix} \sigma_1(r) \\ \sigma_2(r) \\ \ldots \\ \sigma_n(r) \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \ldots & \sigma_2(\alpha_n) \\ & \ldots & & \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} q_1 \\ q_2 \\ \ldots \\ q_n \end{pmatrix}$$

We know there is a solution $(q_1, q_2, \ldots, q_n)$ to this matrix equation, so Cramer's rule gives us a formula

$$q_i = \frac{det(A_i)}{|\sigma_i(\alpha_j)|} =: \frac{\gamma_i}{\zeta}$$

where A_i is the above matrix with the ith column replaced by $\begin{pmatrix} \sigma_1(r) \\ \sigma_2(r) \\ \ldots \\ \sigma_n(r) \end{pmatrix}$. We note γ_i and ζ are both algebraic integers: both determinants expand to a complicated product and sum of algebraic integers, but $\mathbb{A}$ is a ring so $\gamma_i, \zeta \in \mathbb{A}$. By definition, $d = \zeta^2$. Therefore,

$$dq_i = \zeta^2 \frac{\gamma_i}{\zeta} = \zeta\gamma_i \in \mathbb{A}.$$

Since $dq_i \in \mathbb{Q}$, necessarily $dq_i \in \mathbb{Z}$: clearly the integers are algebraic integers and the rational non-integers are not, as a rational $\rho \notin \mathbb{Z}$ has monic irreducible $x - \rho \notin \mathbb{Z}[x]$, so Lemma 3.1.5 shows ρ cannot satisfy a monic in integer coefficients. Therefore we can define $m_i = dq_i \in \mathbb{Z}$ as required. Note

$$\gamma_i^2 = q_i\zeta\gamma_i = dq_i^2 = \frac{m_i^2}{d}$$

Therefore the rational number $\frac{m_i^2}{d} \in \mathbb{A}$, so it is in fact an integer, that is, $d|m_i^2$ as required. [9] □

This shows that $\mathbb{A} \cap K \subset \frac{\alpha_1}{d}\mathbb{Z} \times \frac{\alpha_2}{d}\mathbb{Z} \times \cdots \times \frac{\alpha_n}{d}\mathbb{Z}$. Let us summarise what we have shown in the following corollary.

Corollary 3.4.9. *Any number ring $\mathbb{A} \cap K$ is a free abelian group of rank $n = [\mathbb{Q}[\alpha] : \mathbb{Q}]$. In particular, number rings are Noetherian by Corollary 2.2.10.*

Next, we give a proof of the following exercise from [9]

We are now ready to give the proof of Theorem 3.4.1. We follow the approach of [9], first proving two lemmas.

Lemma 3.4.10. *Let $\omega = e^{2\pi i/p}$ for some prime p. Then*

$$\mathbb{Z}[\omega] = \mathbb{Z}[1-\omega]$$

$$disc(\omega) = disc(1-\omega)$$

Proof. It is clear that $\mathbb{Z}[1-\omega] \subset \mathbb{Z}[\omega]$ by expanding an arbitrary polynomial in $1-\omega$ to give a polynomial in ω. Additionally, since $\omega = 1-(1-\omega)$, an arbitrary polynomial in ω can be expanded to a polynomial in $(1-\omega)$. Therefore $\mathbb{Z}[\omega] \subset \mathbb{Z}[1-\omega]$.

Ordering the embeddings $\sigma_1, \dots \sigma_n$ such that $\sigma_i(\omega) = \omega^i$, we have that

$$disc(\omega) = |\sigma_i(\omega^j)|^2 = |\omega^{ij}|^2 = \prod_{1 \le r < s \le n} (\omega^s - \omega^r)$$

where the last equality is the equation for a Vandermonde determinant [9]. It is a fact that the conjugates of $(1-\omega)$ over $\mathbb{Q}$ are the $(1-\omega^j)'s, 1 \le j < p$ (see [9]), so

$$disc(\omega) = \prod_{1 \le r < s \le n} (\omega^s - \omega^r) = \prod_{1 \le r < s \le n} ((1-\omega^s) - (1-\omega^r)) = disc(1-\omega).$$

[9] □

Lemma 3.4.11.

$$\prod_{k=1}^{p-1} (1-\omega^k) = p$$

Proof. We have already shown in Example 3.1.2

$$\prod_{k=1}^{p-1} (x-\omega^k) = 1 + x^2 + \cdots + x^{p-1}$$

so the result follows by setting $x = 1$. □

Proof of Theorem 3.4.1. Let $\alpha \in B = \mathbb{A} \cap \mathbb{Q}[\omega]$. By Proposition 3.4.8,

$$\alpha = \frac{m_0 + m_1(1-\omega) + \cdots + m_{p-1}(1-\omega)^{p-1}}{d}$$

where $m_i \in \mathbb{Z}$, $d = disc(1-\omega) = disc(\omega)$ and $d | m_i^2$. It is shown in [9] that

$$disc(\omega) = p^m \text{ for some } m \ge 1,$$

we will accept this without proof. If $\mathbb{A} \cap \mathbb{Q}[\omega] \neq \mathbb{Z}[\omega] = \mathbb{Z}[1-\omega]$ then there must exist such an α where $d \not| m_i$ for some i. We may let i be the smallest i where this holds, and,

by subtracting $\frac{m_0}{d} + \frac{m_1}{d}(1-\omega) + \cdots + \frac{m_{i-1}}{d}(1-\omega)^{i-1} \in \mathbb{Z}[1-\omega] \subset B$, and multiplying by p^{m-1}, assume

$$\alpha = \frac{m_i(1-\omega)^i + \cdots + m_{p-1}(1-\omega)^{p-1}}{p}$$

with $p \not| m_i$. By Lemma 3.4.11,

$$\frac{p}{(1-\omega)^{i+1}} = \frac{\prod_{k=1}^{p-1}(1-\omega^k)}{(1-\omega)^{i+1}} = (\prod_{k=1}^{i+1}\frac{1-\omega^k}{1-\omega})\prod_{k=i+1}^{p-1}(1-\omega^k).$$

This product lies in $\mathbb{Z}[1-\omega]$ since the k roots of $(x^k-\omega^k)$ are $\omega, \omega^2, \ldots, \omega^k$ giving the identity $(x-\omega^k) = (x-\omega)(x-\omega^2)\ldots(x-\omega^k)$ which for $x=1$ gives $\frac{1-\omega^k}{1-\omega} = (x-\omega^2)\ldots(x-\omega^k) \in \mathbb{Z}[1-\omega] \subset B$.

It follows that $\alpha\frac{p}{(1-\omega)^{i+1}} \in R$. Note

$$\alpha\frac{p}{(1-\omega)^{i+1}} = \frac{m_i}{1-\omega} + m_{i+1} + m_{i+2}(1-\omega) + \cdots + m_{p-1}(1-\omega)^{p-i-2} \in R$$

By subtracting everything else, which is in $\mathbb{Z}[1-\omega] \subset B$, we find $\frac{m_i}{1-\omega} \in B$.

Since $\frac{m_i}{1-\omega}$ is an algebraic integer, taking the norm over $\mathbb{Q}[\omega]$, $N(\frac{m_i}{1-\omega}) = \frac{N(m_i)}{N(1-\omega)} \in \mathbb{Z}$. $N(1-\omega) = \prod(1-\omega^k) = p$ by Lemma 3.4.11. Additionally, $N(m_i) = m_i^p$ since there are p embeddings of $\mathbb{Q}[\omega]$ fixing $\mathbb{Q}$ and each fixes m_i. It follows that $p|m_i^p$. However, $p \not| m_i | m_i^p$ by assumption, a contradiction. [9] □

Chapter 4

Dedekind Domains

After our tour of ideals, Noetherian rings, number fields and number rings, we are now ready to bring everything back to Kummer's partial proof of Fermat's Last Theorem. Recall that we need to show the ideals in $\mathbb{Z}[\omega]$ factorise uniquely into a product of prime ideals. We will show that this property is always held for a certain type of integral domains, called **Dedekind domains**. Furthermore, we will show all number rings are Dedekind, so that in particular, $\mathbb{Z}[\omega] = \mathbb{A} \cap \mathbb{Q}[\omega]$ is a Dedekind domain. Our approach is inspired by [13]. We start by briefly discussing the field of fractions of a ring R.

4.1 The field of fractions

For any integral domain R sitting inside a field L, what is the smallest subfield containing R? There is always a subfield $F = \{ab^{-1} : a \in R, 0 \neq b \in R\}$ which contains R. Additionally, any subfield of L containing R necessarily contains F. It follows that F is the intersection of all subfields of R, that is, the smallest subfield containing R. F is called the field of fractions of R and can be defined (up to isomorphism) even when a field containing R is not given, in the following way: Define an equivalence relation $\sim$ on $R \times (R \setminus \{0\})$ by $(a,b) \sim (c,d) \iff ad = bc$. The reader should compare this with the equivalence relation on fractions in $\mathbb{Q}$: $\frac{a}{b} = \frac{c}{d} \iff ad = bc$. $\sim$ is clearly reflexive, and is symmetric because R is commutative. It is transitive because if $(a,b) \sim (c,d)$ and $(c,d) \sim (e,f)$ then

$$ad = bc \implies fad = bcf \implies fad = bed \implies af = be$$

where the last equality follows from R being an integral domain. Clearly when $R = \mathbb{Z}$, the equivalence classes under $\sim$ give $\mathbb{Q}$ as a set. Inspired by the field structure on $\mathbb{Q}$, we can show that these equivalence classes for any R define a field, called the field of fractions.

Definition 4.1.1. The **field of fractions** of an integral domain R is the field given by the set $R \times (R \setminus \{0\})/\sim$ and with addition/subtraction defined by

$$[a,b] \pm [c,d] = [ad \pm cb, bd]$$

and multiplication by

$$[a,b] \times [c,d] = [ac,bd].$$

Multiplicative inverses when $[a,b] \neq [0,b]$ are

$$[a,b]^{-1} = [b,a].$$

The 0 element is $[0,1]$ and the 1 element is $[1,1]$.

It is easy to see that $^{-1}$ is well-defined. Let us confirm that $\pm$, $\times$ are well-defined, letting $[a,b] \sim [a',b']$ and $[c,d] \sim [c',d']$. Trivially, $[a,b] \sim [ka,kb]$ for any $0 \neq k$. Then

$$[a,b] \pm [c,d] = [ad \pm cb, bd] = [(ad \pm cb)b'd', (bd)b'd'] = [ab',bb'] + [cd',dd']$$

$$= [a'b,bb'] + [c'd,dd'] = [a',b'] + [c',d'].$$

Similarly,

$$(ac,bd) \sim (a'c',b'd') \iff acb'd' = a'c'bd$$

Which is true since $ab' = a'b$ and $cd' = c'd$ by assumption.

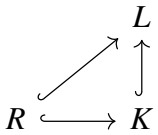
It is tedious (and not hard) to show that $+$ and $\times$ satisfy all properties of a field, in particular closure, commutativity, associativity, and satisfying identities. We will finish by showing the distributive property:

$$[a,b] \times ([c,d] + [e,f]) = [a,b] \times [cf + de, df] = [acf + ade, bdf]$$

$$= [(ac)(bf) + (ae)(bd), (bd)(bf)] = [ac,bd] + [ae,bf] = [a,b] \times [c,d] + [a,b] \times [e,f].$$

Clearly the field of fractions of R defined in Definition 4.1.1 and the field of fractions defined at the start of the section are isomorphic. It follows that the field of fractions satisfies a universal property.

Proposition 4.1.2 (Universal property of the field of fractions)**.** *For every embedding $R \to L$ of an integral domain into a field, there is a unique injection from the field of fractions K of R making the following triangle commute*



Proof. We have already shown existence, simply map K into the field of fractions of R in L. Since $\phi : K \to L$ is a field homomorphism, $\phi(\frac{a}{b}) = \frac{i(a)}{i(b)}$ where $i : R \to L$ is the given injection, so in fact ϕ is uniquely defined. □

This is the formal sense in which K is the smallest field containing an isomorphic image of R.

Given any ring R we may always pass to its field of fractions K. We may then look at the ring of elements in K integral over A: this is called the **integral closure** of A in K. We have shown this forms a ring in the case of the integral closure of $\mathbb{Z}$ in $\mathbb{C}$ in Corollary 3.3.2, and it is easy to see the proof can be extended in generality. If the integral closure of A in its field of fractions is A, we say A is **integrally closed**. We will

want to show that number rings $\mathbb{A} \cap K$ are integrally closed. Inspired by [13], we start by showing the field of fractions of $\mathbb{A} \cap K$ is K itself. We show this in more generality.

Lemma 4.1.3. *If A is a ring with field of fractions K and L is a field extension of K with L algebraic over K, then the field of fractions of the integral closure B of A in L is L.*

Proof. Let $x \in L$. Since L is algebraic over K, we can find $k_i \in K$ such that

$$k_0 + k_1 x + \ldots k_{n-1} x^{n-1} + x^n = 0.$$

Writing the k_i as fractions $\frac{a_i}{b_i}, a_i, b_i \in A$, then multiplying the equation by $b := b_1 b_2 \ldots b_n$ we get a monic in bx with coefficients in A, so bx is integral over A. Writing $bx = \beta \in B$, we see $x = \frac{\beta}{b}$ is in the field of fractions of B. Since x was arbitrary, L is a subset of the field of fractions of B. Since $B \subset L$, the field of fractions of B is a subset of the field of fractions of L, so these are equal.
[13] □

In the case of $\mathbb{A} \cap K$, $A = \mathbb{Z}$ with field of fractions $K = \mathbb{Q}$. $L = K$ is a field extension and the integral closure of L over $\mathbb{Z}$ is $\mathbb{A} \cap K$. It easily follows that number rings are integrally closed.

Proposition 4.1.4. *Number rings are integrally closed.*

Proof. Considering $\mathbb{Z} \subset \mathbb{A} \cap K \subset X$ where X is the integral closure of $\mathbb{A} \cap K$ in K, and note $\mathbb{A} \cap K$ is integral over $\mathbb{Z}$ and X is integral over $\mathbb{A} \cap K$, both by definition. By **??**, X is integral over $\mathbb{Z}$. Since $X \subset K$ by Lemma 4.1.3, in fact $X \subset \mathbb{A} \cap K$ as required.
[13] □

4.2 Number rings are Dedekind domains

Definition 4.2.1. An integral domain R is a **Dedekind domain** if

(1) R is Noetherian.

(2) Every nonzero prime ideal of R is maximal.

(3) R is integrally closed.

We would like to show that number rings $R = \mathbb{A} \cap K$ are Dedekind domains. We have already verified that number rings are Noetherian (Corollary 3.4.9) and integrally closed Proposition 4.1.4. It remains to show that a nonzero prime ideal of R is maximal. This is true in much more generality, for any ring integral over a ring with this property. In particular, $\mathbb{A} \cap K$ is integral over $\mathbb{Z}$ by definition, and the nonzero prime ideals of $\mathbb{Z}$ are exactly $p\mathbb{Z}$ for p prime, which are also the maximal ideals.

Lemma 4.2.2. *If an integral domain R is integral over a subring S with property (2) of a Dedekind domain, then R also has property (2).*

Proof. Let P be a prime ideal of R. $Q := P \cap S$ is also an ideal of S (closed by multiplication by $s \in S$ and subtraction since elements of both P and S are) and in fact it is a prime ideal of S: $xy \in Q \cap S \implies x$ or y is in P (P is prime) and since both were assumed to be in S, x or y is in Q. Furthermore, Q is nonzero: let $0 \neq p \in P$ and write

$$p^n + s_{n-1}p^{n-1} + \cdots + s_0 = 0, s_i \in S, n > 0,$$

since R is integral over S. We may assume $s_0 \neq 0$ by cancelling out the smallest common power p if necessary (R is an integral domain). Now $s_0 \in S$ and also $s_0 = -(p^n + s_{n-1}p^{n-1} + \cdots + ps_1) \in P$, so $0 \neq s_0 \in Q$.

By assumption, Q is maximal in S. Now consider the following diagram, where $p : S \to R/P$ is the composition of the inclusion and the projection map.

$$\begin{array}{ccc} S & \xrightarrow{p} & R/P \\ {\scriptstyle\pi}\downarrow & \nearrow_{\exists! h} & \\ S/Q & & \end{array}$$

Since $Q \subset P$, $p(Q) = 0$, so the universal property of factor rings gives a unique map $h : S/Q \to R/P$ commuting with the diagram. h is the map $a + Q \mapsto a + P$, which is injective since $a - b \in P \implies a - b \in Q \subset P$. Since S/Q is a field by maximality, $im(h)$ is a subfield of the integral domain R/P. It follows that R/P is integral over S/Q: let $r \in R$ satisfy $r^n + s_{n-1}r^{n-1} + \ldots s_0$. Applying the canonical ring homomorphism $\rho : R \to R/P$ to this equation, and noting that commutativity in the diagram gives $\rho(s) = h\pi(s)$ for $s \in S$, gives a monic

$$(r+P)^n + (s_{n-1} + Q)(r+p)^{n-1} + \cdots + (s_0 + Q)$$

where we have written $s + Q$ instead of $h(s + Q)$. Therefore R/P is integral over S/Q. In fact, this forces R/P to be a field itself by the next lemma. It follows that P is maximal as required.

[13]. □

Lemma 4.2.3. *An integral domain R integral (aka algebraic) over a field F is a field.*

Proof. Let $r \in R$ with monic irreducible f. Then $F[r]$ is a $F-$vector space of degree $deg(f)$ by Lemma 3.1.7. The F-linear map $f : F[r] \mapsto F[r]x \mapsto rx$ has kernel 0 since R is an integral domain, and is therefore injective. By the rank-nullity theorem, f is surjective, in particular there is an r' with $f(r') = rr' = 1$. This gives an inverse to r. [13] □

4.3 Dedekind domains have Property I

We have shown that $\mathbb{Z}[\omega]$ is a number ring, and that this implies it is a Dedekind domain. We now show that all Dedekind domains have the desired **Property I**: ideals factorise uniquely into a product of prime ideals. Recall we define a multiplication of two ideals I, J of an integral domain R as $IJ = \langle ij : i \in I, j \in J \rangle$, the smallest ideal

containing all the products of elements from I and J. We can also define a sum on ideals: $I+J = \langle I \cup J \rangle = \{i+j : i \in I, j \in J\}$: the smallest ideal containing both I and J. It is trivial to see that this set is an ideal. Additionally, it contains $I \cup J$ and any set containing $I \cup J$ must contain this set by closure under addition.

We start by proving a weaker version of Property I:

Lemma 4.3.1. *Every ideal of a Noetherian ring A contains a finite product of nonzero prime ideals.*

Proof. Suppose there is an ideal I of A without this property. Since A is Noetherian, the collection of all such ideals has a maximal element J. Let $0 \neq xy \in J$ be such that $x, y \notin J$. It follows that $J \subset J + \langle x \rangle$ and $J \subset J + \langle y \rangle$ where these inclusions are proper. By maximality of J among ideals missing the sought property, both $J + \langle x \rangle$ and $J + \langle y \rangle$ contain finite products of prime ideals, say $P_1 P_2 \dots P_n$ and $Q_1 Q_2 \dots Q_m$ respectively. Then $\prod_{i,j} P_i Q_j$ is a finite product of prime ideals of $(J + \langle x \rangle)(J + \langle y \rangle)$, which is the smallest ideal containing

$$\{(j+rx)(j'+sy) : j, j' \in J, r, s \in R\} = \{jj' + jsy + j'rx + rsxy : j, j' \in J, r, s \in R\} \subset J$$

since J is closed under addition, multiplication by an element of R and contains xy. This contradicts J not containing a finite product of prime ideals. [13] □

We now show that under ideal multiplication, the **fractional ideals** of a Dedekind domain form a group.

Definition 4.3.2. Let a ring R have field of fractions K. A **fractional ideal** of R is an $A-$submodule M of K with the property that there exists a $0 \neq c \in A$ such that $cM \subset A$.

We will call ideals of A **integral ideals** to distinguish from fractional ideals. Recall an ideal of A is exactly an $A-$submodule of A. The definition is motivated by considering the $\mathbb{Z}-$submodules of $\mathbb{Q}$ of the form $M = \{m\frac{a}{c} : m \in \mathbb{Z}\}$ for some fixed a and c. Of course, $cM = a\mathbb{Z} \subset \mathbb{Z}$. For this reason, c is called a **common denominator** of M.

Let us build a group structure on fractional ideals. A will play the role of the identity since $AM = M$ for any $A-$module. We need to find the multiplicative inverse of every fractional ideal. Inspired by the approach in [13], we first prove this property for maximal ideals, then integral ideals, then fractional ideals. The Noetherian property of A will play a key role here.

Lemma 4.3.3. *Let R be a Dedekind domain and M,N be two (integral) ideals of R, where M is prime, such that*

$$N \subset NM^{-1} \subset R.$$

Then the first inclusion is proper.

Proof. We will show that $M^{-1} \supsetneq R$. Then if $N = NM^{-1}$, M^{-1} is integral over R by Lemma 3.1.9, so $M^{-1} \subset R$ by the algebraic closure of R, a contradiction. It suffices to find a single element $m \in M^{-1}$ with $m \notin R$.

Let $0 \neq a \in M$ and let $P_1 \dots P_r$ be a product of primes contained in $\langle a \rangle$ by crefnoetherian-ideals-contain-finite-product-of-primes. Assume r is minimal. Then $P_1 \dots P_n \subset M$, so since M is prime, $P_i \subset M$ for some i. By relabeling, let $i = 1$. Since P_1 is maximal, $P_1 =$

M. Now by assumption, $P_2 \dots P_n \not\subset \langle a \rangle$, so we may choose some $b \in P_2 \dots P_n \setminus \langle a \rangle$. Letting $d = ba^{-1}$, we notice $b \notin aR \implies d \notin R$. However, $dM = ba^{-1}P_1 \in a^{-1}P_1 \dots P_n \subset a^{-1}\langle a \rangle = A$, so $d \in M^{-1}$ as required. [13] □

Lemma 4.3.4. *Any fractional ideal M of a Dedekind domain R has a multiplicative inverse.*

Proof. We do the proof in three stages.

M **is maximal:** We will show that the fractional ideal $M^{-1} = \{k \in K : kM \subset R\}$ is the multiplicative inverse to M. M^{-1} is certainly an $R-$submodule: if $kM \subset R$ the same is true for $akM, a \in R$ and $(k+c)M$ where $cM \subset R$. The remaining properties of being an abelian group are similarly easily checked. The common denominator of M^{-1} is any nonzero $m \in M$. We also have $M^{-1}M \subset R$. In fact $M \subset M^{-1}M$ as well, since $1 \in M^{-1}$. By Lemma 4.3.3, $M \neq M^{-1}M$, so by the maximality of M, $M^{-1}M = R$.

M **is integral.** Suppose M is integral and does not have a multiplicative inverse. Let N be maximal among all such ideals, and let J be a maximal ideal containing N. Both exist since R is Noetherian. Since J is maximal, it has multiplicative inverse J^{-1}. Since $1 \in J^{-1}$, s

$$N \subset NJ^{-1} \subset JJ^{-1} = A.$$

The first inclusion is proper by Lemma 4.3.3. Since N was maximal among integral ideals without multiplicative inverse, NJ^{-1} has inverse C, so N has inverse $J^{-1}C$.

M **is a fractional ideal**. We have (by definition) a $c \in R$ s.t. cM is integral, and therefore has an inverse N. It follows that cN is an inverse to M. [13] □

Thus, the definition of a Dedekind domain, which at first seemed arbitrary, has now been shown to have the very useful property of Lemma 4.3.4. In fact, more is true: Dedekind domains are equivalent to this property, as shown in [13]. We now show that Dedekind domains have the sought-after Property I of unique factorisation of ideals into prime ideals. We will adopt the convention that $I^0 = A$ for any ideal, and give the ideal $I = R$ of R the unique factorisation into prime ideals $R = P^0$ for some prime ideal P. This is similar to allowing 1 to have the unique prime decomposition $1 = 2^0$. The factorisation will be unique up to reordering and multiplication by $A = P^0$, i.e., zero powers of prime ideals, just like the unique factorisation of positive integers into a product of primes.

Theorem 4.3.5 (Dedekind domains have Property I)**.** *Any ideal I of a Dedekind domain R has a unique factorisation into prime ideals $I = P_1^{a_1}P_2^{a_2}\dots P_n^{a_n}$.*

Proof. Let us first prove existence. We have already adopted a convention when $I = R$, so suppose I is a proper ideal that does not factorise into a product of prime ideals. Let J be maximal among all such ideals and let M be a maximal ideal containing J. Note $J \neq M$ since maximal ideals are always prime by Example 2.1.10 so in particular, maximal ideals always factorise into a product of primes. By maximality of J, M factorises into a product of prime ideals $M = P_1P_2\dots P_n$. Now let $N = JM^{-1}$ so $J = NM$. From the proper containment

$$J \subset M$$

we get the proper containment

$$N = JM^{-1} \subset MM^{-1} = R.$$

Additionally, multiplying by $N = JM^{-1}$ on the proper containment

$$M \subset R$$

gives the proper containment

$$J \subset N \subset R$$

By maximality of J, N factorises into a product of prime ideals. Since both M and N have this property, so does their product J - a contradiction.

For uniqueness, suppose an ideal I has two factorisations

$$I = P_1 P_2 \dots P_n = Q_1 Q_2 \dots Q_m.$$

Recall $IJ \subset P \implies I \subset P$ or $J \subset P$ (CITE) for prime P. By induction, $Q_1 \dots Q_m \subset P_1 \implies Q_i \subset P_1$ for some i. By relabeling, let $i = 1$. Since prime ideals are maximal, $Q_1 = P_1$. By taking inverses, we may write $P_2 ... P_n = Q_2 \dots Q_m$. We continue until we have $P_i \dots P_n = A$ (WLOG $n \geq m$) which implies $A \subset P_j$ for each $i \leq j \leq n$, a contradiction. Therefore $n = m$ and the P_i's can be reordered to give the Q_j's.

[13] □

The factorisation can be extended to general fractional ideals M of R. We know there exists a $c \in R$ with $cM \subset R$. Therefore cM has a unique factorisation into prime ideals $cM = P_1^{a_1} \dots P_n^{a_n}$. Additionally, $M = \langle \frac{1}{c} \rangle cM$ where $\langle \frac{1}{c} \rangle = \{ \frac{r}{c} : r \in R \}$ is the fractional ideal generated by $\frac{1}{c}$. If the prime decomposition of $\langle c \rangle$ is $\langle c \rangle = Q_1^{b_1} \dots Q_m^{b_m}$ then

$$\langle \frac{1}{c} \rangle = \{ \frac{r}{q_1, \dots q_m} : q_i \in Q_i^{b_i}, r \in R \} = Q_1^{-b_1} \dots Q_m^{-b_m}$$

where $Q_i^{-b_i} = \{ \frac{r}{q_i} : q_i \in Q_i^{b_i}, r \in R \}$. Therefore

$$M = \frac{P_1^{a_1} \dots P_n^{a_n}}{Q_1^{b_1} \dots Q_m^{b_m}}.$$

After cancelling out any common prime ideals in the numerators and denominators we get a factorisation

$$M = \prod p^{f_p}$$

where the product goes over all prime ideals of R, $f_p \in \mathbb{Z}$ and f_p is nonzero for only finitely many p. This factorisation is also unique, as the cancellation trick from the proof of Theorem 4.3.5 also works for fractional ideals.

As remarked in [13], a prime ideal P appears in the prime decomposition of an ideal I if and only if $I \subset P$. ($\implies$) is clear, and for ($\impliedby$) we have $I = PP_1 \dots P_n \subset P$, therefore $P_i \subset P$ for some i since P is prime and so by the maximality of $P_i, P = P_i$. This remark will allow us to show the prime decompositions of $\langle x + \omega y \rangle$ and $\langle x + \omega^j y \rangle$ in the proof of Fermat's Last Theorem have no prime ideals in common, which we record as the following remark.

Remark 4.3.6. Suppose P appears in both the unique prime decompositions of $\langle x + \omega y \rangle$ and $\langle x + \omega^j y \rangle$ for some $1 < j \leq p$. Both ideals are then subsets of P, so $(x + \omega y) - (x + \omega^j y) \subset P$. We can then follow Lamé's argument almost word-for-word to find that

$py \in P$, and find integers m,n with $mpy+nz=1$. Note that $z \in P$ since P also appears in the prime decomposition of z. It follows $mpy+nz \in P$, however $1 \notin P$ as $P \neq \mathbb{Z}[\omega]$. This gives the desired contradiction. [13]

We finish by showing that multiplication of fractional ideals satisfies a distributive law. This is a basic fact for integral ideals which is easily extended to fractional ideals. Note that the definition of a sum of ideals $I+J=\{i+j : i \in I, j \in J\}$ can easily be extended to fractional ideals. The proof given here is my own.

Lemma 4.3.7. *Let I,J,K be fractional ideals of a Dedekind domain R. Then*

$$I(J+K) = IJ+IK$$

Proof. Since $J \subset J+K$, $IJ \subset I(J+K)$. Similarly, $IK \subset I(J+K)$. It follows that

$$IJ+IK \subset I(J+K).$$

Now let $i \in I$, $j \in J, k \in K$ and note

$$i(j+k) = ij+ik \in \{a+b : a \in \langle\{ij : i \in I, j \in J\}\rangle, b \in \langle\{ik : i \in I, k \in K\}\rangle\} = IJ+IK$$

Since $I(J+K) = \{i(j+k) : i \in I, j \in J, k \in K\}$,

$$I(J+K) \subset IJ_IK.$$

We therefore have equality. □

Chapter 5

Ideal classes

In this section, we prove that number rings have Property II, finishing the proof of Fermat's Last Theorem for regular primes. This exposition will be inspired by Chapter 5 of [9]. We will end with a few notes on proving primes are regular.

5.1 The ideal class group

In this section we will prove that all number rings have **Property II**. We have already shown that the fractional ideals of a number ring form an abelian group. Recall we defined an equivalence relation on ideals of R as

$$I \sim J \iff aI = bJ \text{ for some } a, b \in R.$$

Equivalently, the relation is

$$I \sim J \iff I = kJ \text{ for some } k \in K$$

where K is the field of fractions of R. In fact, we will define this equivalence relation on fractional ideals. Note that since $cM \subset R$ for each fractional ideal M and some $c \in R$, each equivalence class has an integral representation, so the set of equivalence classes is the same whether the relation is defined on integral ideals or fractional ideals.

The standard multiplication is well-defined on the equivalence classes: if $I \sim I'$ with $aI = a'I'$ and $J \sim J'$ with $bJ = b'J'$ then $abIJ = a'b'I'J'$ so $IJ \sim I'J'$. Note since $I \sim aI = \langle a \rangle I$ for any $0 \neq a \in R$, $[\langle a \rangle][I] = [I]$, so $[\langle a \rangle$ must serve as the identity in this group structure. Clearly, any two principal ideals, integral or not, are equivalent. Additionally, if I is such that $I \sim \langle a \rangle$, then $I = k\langle a \rangle$ is itself principal. $[\langle a \rangle]$ is therefore the equivalence class $[R]$ of principal ideals.

We can now very easily prove that the equivalence classes form an abelian group when R is a Dedekind domain. I give an original proof.

Proposition 5.1.1. *The set of equivalence classes of ideals $Cl(R) = \{[I] : I \in R\}$ of a Dedekind domain R with field of fractions K is an abelian group.*

Proof. We have shown the fractional ideals form an abelian group G under this multiplication. The subset H of principal fractional ideals forms a (normal) subgroup by the subgroup test: it is closed under multiplication since $\langle a \rangle \langle b \rangle = \langle ab \rangle$ for any $a, b \in K$,

and closed under inverses since $\langle a\rangle^{-1} = \langle a^{-1}\rangle$. Therefore the quotient group G/H is abelian. The coset of a fractional ideal I is

$$IH = \{I\langle a\rangle : a \in K\} = [I].$$

□

Remark 5.1.2. $Cl(R)$ is called the **ideal class group** of R. It is the trivial group if and only if every ideal of R is principal, i.e., R is a PID. The size of this group is therefore a measure of how far R is from being a PID. Recall PIDs are UFDs. This is an if and only if statement when R is a Dedekind domain [13]. $Cl(R)$ is therefore also a measure of how close R is to being a UFD.

Remark 5.1.3. We noted in the introduction that Kummer's proof of Fermat's Last Thoerem was strictly stronger than Lamé's, even when restricting his proof to only the case when $\mathbb{Z}[\omega]$ is a UFD. By the previous remark, if $\mathbb{Z}[e^{2\pi i/p}]$ is a UFD, its ideal class group is trivial, so p is regular. Kummer's proof is therefore stronger than Lamé's. In fact it is *strictly* stronger; Kummer himself proved that $p = 23$ is regular and that $\mathbb{Z}[e2\pi i/23]$ is not a UFD.

It remains to show that $Cl(R)$ is finite. We will show this for any number ring $\mathbb{A} \cap K$. Our first goal will be the define a norm on ideals I of number rings.

Lemma 5.1.4. *Suppose $B = \mathbb{A} \cap K$ is a number ring and I is a nonzero integral ideal. Then B/I is finite.*

Proof. Let $\alpha \in I$ be non-zero, and let $m = N^K(\alpha)$. m is an integer by Lemma 3.4.3. We can write $m = \beta\alpha$ where β is a product of conjugates of α over $\mathbb{Q}$. Since $\beta = \frac{m}{\alpha}$, we have $\beta \in K$. Additionally, since $\mathbb{A}$ is a ring, $\beta \in \mathbb{A}$ - each conjugate is an algebraic integer and $\mathbb{A}$ is closed under multiplication. Therefore $\beta \in B$ so $m \in I$. It follows that $\langle m\rangle \subset I$, and therefore $|B/I| \leq |B/\langle m\rangle|$, which is finite by the next lemma (recall B is a finitely generated free abelian group under $+$). [9] □

The following lemma is an exercise in [9]; I give an original proof.

Lemma 5.1.5. *If G is a free abelian group of rank n and $m > 1$ an integer, then G/mG is a direct sum of n groups of order m. In particular, $|G/mG| = m^n$.*

Proof. By the fundamental theorem of finitely generated abelian groups, $G \cong \mathbb{Z}^n$ [3]. We have an isomorphism

$$\mathbb{Z}^n/m\mathbb{Z}^n \cong (\mathbb{Z}/m\mathbb{Z})^n, \qquad [(a_1, a_2, \ldots, a_n)] \mapsto ([a_1], [a_2], \ldots, [a_n])$$

This is well-defined since if $(a_1, \ldots a_n) - (a'_1, \ldots a'_n) \in m\mathbb{Z}^n$, then $a_i - a'_i \in m\mathbb{Z}$ for each i. It is clearly surjective, and is injective as its kernel is $\{[a_1, \ldots, a_n] : a_i \in m\mathbb{Z}^n \text{ for each } i\} = [0, 0, \ldots, 0]$. Note $|(\mathbb{Z}/m\mathbb{Z})^n| = |\mathbb{Z}/m\mathbb{Z}|^n = m^n$ as required. □

This justifies defining the **norm** of an ideal I of a number ring B (or more generally a Dedekind domain satisfying the conclusion of Lemma 5.1.4) as the cardinality $|B/I|$.

We regrettably do not have time to explore the background knowledge necessary to fully prove these next two non-trivial results.

Lemma 5.1.6. *Given a number ring B and a positive integer n, there are only finitely many prime ideals P of B such that $||P|| = n$.*

Proof. Omitted. See [9]. □

Lemma 5.1.7. *The norm of ideals I, J of a number ring $B = \mathbb{A} \cap K$ satifies the following properties:*

(1) $||IJ|| = ||I||||J||$

(2) For any $0 \neq \alpha \in B$, $|N^K(\alpha)| = ||\langle \alpha \rangle||$

Proof. (1) We may assume that I and J are prime: the general result will then follow from unique factorisation of general ideals:

$$||I|| = ||P_1^{a_1} \dots P_n^{a_n}|| = ||P_1||^{a_1} \dots ||P_n||^{a_n}$$

Note $\frac{J}{IJ} \leq \frac{B}{IJ}$ as groups. By Lagrange's theorem and the third isomorphism theorem (see [3]),

$$||IJ|| = \left|\frac{B}{IJ}\right| = \left|\frac{B/IJ}{J/IJ}\right| |J/IJ| = |B/J||J/IJ| = ||J|| \cdot |J/IJ|.$$

We therefore need to show $|J/IJ| = |B/I|$. Since I is prime hence maximal, B/I is a (finite) field. J/IJ is a (finite) vector space over B/I, in particular

$$(b+I)(j+IJ) = bj+IJ$$

is well-defined for $b \in B$ and $j \in J$. Fix nonzero $j \in J/IJ$ and consider the linear map

$$f : B/I \to J/IJ, \quad [x] \mapsto [jx].$$

This map is injective since

$$[jx] = [jy] \iff j(x-y) \in IJ \iff (x-y) \in I \iff [x] = [y].$$

Letting $J' = jJ^{-1}$, we note $jB = JJ'$. It follows that

$$I \subset I + J'$$

is a proper inclusion, so by the maximality of I, $I + J' = B$. Since prime ideals of Dedekind domains are maximal, and $I \subset I + J'$ is a proper inclusion, $J' + I = B$. Multiplying by J gives

$$J(J' + I) = (JJ' + IJ) = J$$

where we have used the distributive property of ideal multiplication (Lemma 4.3.7). From this it in fact follows that $im(f) = (jB + IJ)/\sim = J/\sim = J/IJ$ so f is surjective. We have therefore found an isomorphism $B/I \cong J/IJ$, so in particular, $|B/I| = |J/IJ|$ as required. [11]

(2) Proof omitted. See [9].

□

We are now ready to tie the story back to the ideal class group. The next two lemmas will connect the ideal norm to the ideal class group by showing that we can always uniformly choose "small" (in norm) representatives for every ideal class. Armed with Lemma 5.1.6, we can then show that only finitely many ideals are small enough to represent an ideal class.

Lemma 5.1.8. *Let $B = \mathbb{A} \cap K$ be a number ring. There is a positive real number λ such that every nonzero ideal I of B contains a nonzero element α with*

$$|N^K(\alpha)| \leq \lambda ||I||.$$

Proof. Let $\alpha_1, \ldots, \alpha_n$ be an integral basis of B and let $\sigma_1, \ldots, \sigma_n$ be the n embeddings of B in $\mathbb{C}$ fixing $\mathbb{Q}$. Let

$$\lambda = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|$$

Now let m be the unique integer such that

$$m^n \leq ||I|| < (m+1)^n.$$

Since B is a free $\mathbb{Z}-$module with basis $\alpha_1, \ldots \alpha_n$, there are $(m+1)^n$ unique elements

$$\sum_{i=1}^{n} m_i \alpha_i \in B : 0 \leq m_i \leq m$$

Since $||I|| = |B/I| < (m+1)^n$, two of these elements are congruent $\mod I$, so their difference α lies in I. Note α can be written $\alpha = \sum_{j=1}^{n} m_j \alpha_j$ for some $0 \leq |m_j| \leq m$. Now

$$|N(\alpha)| = \prod_{i=1}^{n} |\sigma_i(\alpha)| = \prod_{i=1}^{n} |\sum_{j=1}^{n} m_i \sigma_i(\alpha_j)| \leq \prod_{i=1}^{n} \sum_{j=1}^{n} |m_i||\sigma_i(\alpha_j)| \text{ (triangle inequality)}$$

$$\leq m^n \lambda (\text{since } |m_i| \leq m) \leq \lambda ||I||.$$

[9] □

Lemma 5.1.9. *Every ideal class of a number ring B contains an ideal J with*

$$||J|| \leq \lambda$$

Proof. Let $[I]$ be an ideal class and $[I^{-1}]$ be its inverse. By the previous lemma, find an $\alpha \in I^{-1}$ s.t.

$$|N(\alpha)| \leq \lambda ||I^{-1}||.$$

$II^-1 = \langle a \rangle$, a principal ideal. Since every two principal ideals are equivalent, write $\langle \alpha \rangle = b\langle a \rangle$ and let $J = bI$ so $JI^{-1} = \langle \alpha \rangle$. By Lemma 5.1.7,

$$|N(\alpha)| = ||\langle \alpha \rangle|| = ||I^{-1}||||J|| \leq \lambda ||I^{-1}|| \implies ||J|| \leq \lambda.$$

[9] □

Theorem 5.1.10 (Property II for number rings)**.** *The ideal class group of a number ring is finite.*

Proof. Every equivalence class is represented by an ideal J with $||J|| \leq \lambda$ for a fixed λ. There are only finitely many such J's: in particular, in the prime decomposition of such J we have by Lemma 5.1.7

$$||J|| = \prod_{i=1}^{n} ||P_i||^{a_i}.$$

Therefore no prime ideal P in the decomposition of such J can have a power a greater than $\frac{\ln ||J||}{\ln ||P||}$. There are only finitely many prime ideals of a given norm by Lemma 5.1.6, therefore only finitely many prime ideals of norm less than or equal to J. There are therefore only finitely many possible prime decompositions of such J, hence only finitely many such J, hence only finitely many classes. [9] □

5.2 Regular primes

We have now completed Kummer's proof of Fermat's Last Theorem for Type I solutions. Kummer also found a proof for Type II solutions, completing the proof [13]. Of course, this proof is not of much use without knowing which primes are regular. This turns out to be doable; Kummer himself managed to classify the primes below 100. He also showed that a prime p is regular if and only if it does not divide the numerators of the **Bernoulli numbers** $B_0, B_2, \ldots, B_{p-1}$ (CITE: `https://mathworld.wolfram.com/RegularPrime.html`). The Bernoulli numbers can be defined, among other ways, from the generating function

$$\frac{x}{e^x - 1} = \sum_{i=0}^{n} \frac{B_n x^n}{n!}.$$

This thus turns the problem of classifying primes into an analytic one, so we can use the full arsenal of analytic number theory to calculate Bernoulli numbers, and hence classify primes. In 1978, Wagstaff classified all the primes less than 125000, finding that just over 39% of primes were irregular [12]. Kummer's proof is therefore applicable to a large class of primes. Despite this, it is only known that there are infinitely many irregular primes, and not known whether there are infinitely many regular primes [12].

Chapter 6

Conclusion

Kummer's contributions around this proof have been described as the "first peak" [7] of the theory of algebraic number fields, while Dedekind is credited with formulating and proving the most fundamental theorems of the field of algebraic number theory [7]. Indeed, as we have hopefully shown, their contributions go far beyond a proof of Fermat's Last Theorem for a subset of exponents. Just motivated by Theorem 1.0.1, we have managed to find a condition, being Noetherian, guaranteeing that the elements of a ring factorise into a finite product of irreducibles, and shown how these can be built from each other. We have classified all the finite dimensional number fields, showing they can always be written in the form $\mathbb{Q}[\alpha]$, and then determined the group structure under $+$ of all number rings. We have then classified exactly the type of integral domains, namely Dedekind domains, whose ideals factorise uniquely into a finite product of prime ideals, and shown that every number ring is of this form. We have then finished by giving some preliminary results in the study of the ideal class group of a number ring.

These were the main players of our story; $\mathbb{Z}[\omega]$ just came along for the ride. In fact, it seemed to be almost by chance that $\mathbb{Z}[\omega]$ was a number ring and a Dedekind domain. Indeed, $\mathbb{Z}[\alpha], \alpha \in \mathbb{C}$ is not a number ring in general, and it is an interesting problem to classify when it is. A logical first follow-up to our story, however, would be to work towards proofs of Lemma 5.1.6 and Lemma 5.1.7 part (2). Both results follow from the theory of split primes, namely, for every prime ideal P of a number ring B there is a unique prime ideal $\langle p \rangle$ of $\mathbb{Z}$ with $P \cap B = \langle p \rangle$, for which we say P lies over $\langle p \rangle$ [9]. Conversely, every prime ideal $\langle p \rangle$ of $\mathbb{Z}$ lies under finitely many, and at least one, prime ideal P of B [9]. Of course, there is nothing special about $\mathbb{Z}$ here, and the story can be made more general by replacing $\mathbb{Z}$ with another subring S. These facts, together with further restrictions on the norm $||P||$ arising from this relation, lead us to proofs of our missing theorems, and to more interesting results still.

Suffice it to say, despite a complete proof of Fermat's Last Theorem now being available due to Wiles, Kummer's theory of regular primes is still full of interesting problems, including unsolved ones such as the open question of whether there are infinitely many regular primes. Perhaps this is Kummer's greatest achievement: the ability to mystify and intrigue mathematicians, centuries after his time.

Bibliography

[1] *Hilbert's basis theorem*, https://en.wikipedia.org/wiki/Hilbert%27s_basis_theorem, Accessed: 16-03-2022.

[2] Amanda Brown, *History of fermat's last theorem*, (1996), Undergraduate Honors Capstone Projects.

[3] Tudor Dimofte, *Group theory.*, 2021.

[4] Larry Freeman, *Fermat's one proof*, http://fermatslasttheorem.blogspot.com/2005/05/fermats-one-proof.html, Accessed: 17-03-2022.

[5] Iain Gordon, *Honours algebra.*, 2019.

[6] Thomas L. Heath, *Diophantus of alexandria second edition*, Cambridge University Press, 1910.

[7] H. Koch, *The history of algebraic number theory and its reflection at the international congresses of mathematicians*, **241** (2003), 110–121.

[8] Tom Leinster, *Galois theory.*, 2021.

[9] Daniel A. Marcus, *Number fields*, Universitext, Springer-Verlag, New York, 1977 (eng).

[10] Simon Singh, *Fermat's last theorem*, Harper Perennial, 2007.

[11] George D. Torres, *Algebraic number theory.*, 2017.

[12] Samuel S. Wagstaff, *The irregular primes to 125000*, Mathematics of Computation **32** (1978), no. 142, 583–591.

[13] James Wright, *Unpublished notes on algebraic number theory.*, 2021.