University of BRISTOL

School of Mathematics

On Kummer's Special Case and the Finiteness of Cyclotomic Fields with Unique Factorisation

Oscar J. Martin Dickie

A thesis submitted to the University of Bristol
in accordance with the requirements for the degree of
Master of Engineering in the Faculty of Engineering.

Supervised by
Alice Pozzi
Level 7
40 Credit Points

Wednesday 16th April, 2025

Acknowledgment of Sources

For all ideas taken from other sources (books, articles, the Internet), the source of the ideas is mentioned in the main text and fully referenced at the end of the report.

All material which is quoted essentially word-for-word from other sources is given in quotation marks and referenced.

Pictures and diagrams copied from the Internet or other sources are labelled with a reference to the webpage or book, article, etc.

Oscar J. Martin Dickie
Wednesday 16th April, 2025

Contents

1. Introduction

Some History

Fermat's Last Theorem (FLT) stands among the most famous mathematical problems. It asserts that for $n > 2$, the Diophantine equation

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

has no non-trivial solutions (x, y, z). While the statement is simple, the proof eluded mathematicians for centuries. It has many failed attempts and, as a result, has provided fertile ground for the advancement of mathematics.

One failed attempt was made in 1847; Gabriel Lamé outlined a proof of FLT which depended on uniquely factoring the Diophantine equation into linear terms

$$x^n + y^n = (x + y)(x + \zeta y) \cdots (x + \zeta^{n-1} y),$$

where $\zeta = e^{2\pi i/n}$. Shortly after, it was discovered that Kummer had shown the failure of unique factorisation 3 years prior. Then Kummer discovered a technical alternative using "ideal numbers". He published this technical alternative in 1850, which tackled FLT for "regular primes". As opposed to dealing with individual cases of FLT, Kummer's proof marked one of the first real advancements in tackling FLT for general cases.

Aim

This thesis first explores Kummer's approach of FLT using regular primes, also known as Kummer's special case of FLT. Then, we follow a proceeding advancement in the study of cyclotomic fields. In particular, we will prove that only a finite number of cyclotomic fields exhibit the unique factorisation needed for Lamé's original proof to hold. Equivalently, the class number of the field is one. We begin by reminding the reader of the necessary background. Kummer's special case is the focus of chapter §3, and the finiteness of fields with class number one is the focus of chapter §4.

2. Background Knowledge

As part of pre-requisite knowledge, we assume the reader has the following knowledge:

- Group Theory - We assume the reader has a solid grasp of group theory, involving the Isomorphism Theorems and basic properties about the order of elements in the group.
- Ring Theory - We assume the reader has a solid grasp of ring theory, ideals and associated properties.
- Field Theory - We assume the reader has a solid grasp of fields, algebraic extensions and vector spaces.
- Algebraic Number Theory - We assume the reader is very familiar with number fields, their rings of integers, the discriminant of a field, Dedekind domains, Dirichlet's unit theorem, as well as associated properties like the norm and trace.
- Galois Theory - We assume the reader is familiar with Galois theory, their groups and properties associated with the fundamental theorem of Galois theory.
- Analytical Number Theory - Some familiarity is advised with some common results for Dirichlet characters, big O notation and other techniques.
- Cyclotomic Fields - We also assume the reader is aware of certain properties about the cyclotomic fields, such as their discriminant, some cyclotomic units, and some properties about the intersection between two cyclotomic fields.

In particular, we will remind the reader and explicitly state some of this pre-requisite knowledge. Due to its relevance in this thesis, we will derive some background results of cyclotomic fields.

2.1. Number Fields

We will recall a collection of useful results and basic definitions of the arithmetic of number fields. A **number field** is a finite-degree field extension of the field of rational numbers $\mathbb{Q}$. In other words, it is a field K that contains $\mathbb{Q}$ and is a finite-dimensional vector space over $\mathbb{Q}$. The dimension of K as a $\mathbb{Q}$-vector space is called the **degree** of the number field, denoted $[K : \mathbb{Q}]$.

Unless otherwise stated, we assume K is a number field. These standard definitions and results follow from and are seen in chapters 1 and 2 of [13], but those familiar with the University of Bristol's Algebraic Number Theory course will see a similar layout and explanation. This course was my introduction to the topic.

Definition 2.1. Let K be a subfield of $\mathbb{C}$.

- Let $f(x) \in K[x]$ be a non-zero polynomial. If there is some complex number α subject to $f(\alpha) = 0$, then α is **algebraic** over K.
- Let $m(x) \in K[x]$ be a polynomial which has an algebraic number α over K as a root. If $m(x)$ is the unique non-zero monic polynomial of minimal degree subject to $m(\alpha) = 0$, then $m(x)$ is called the **minimal polynomial**. Often denoted $m_{\alpha,K}(x)$.
- We say the **degree** of α over K is the degree of its minimal polynomial over K.

Furthermore, if $f(x)$ is a polynomial that has some algebraic number over K as a root, then $f(x)$ is the minimal polynomial if and only if $f(x)$ is monic and irreducible over $K[x]$.

Definition 2.2. Let K be a number field and let α be an algebraic element over K. The roots of the minimal polynomial $m_{\alpha,K}(x)$ over K are said to be the **conjugates** of α.

Definition 2.3. Suppose $K \subset \mathbb{C}$ is a number field, and let L be a finite field extension of K. A K**-embedding** of L into $\mathbb{C}$ is a field homomorphism

$$\sigma : L \to \mathbb{C}$$

that fixes every element of K, meaning $\sigma(x) = x$ for all $x \in K$.

Although these embeddings are first described as monomorphisms in [13].

Naturally we define real and complex embeddings as follows:

Definition 2.4. Let $\sigma : L \to \mathbb{C}$ be a field embedding.

- If $\sigma(L) \subseteq \mathbb{R}$, then σ is a **real embedding**.
- If $\sigma(L) \not\subseteq \mathbb{R}$, then σ is a **complex embedding**.

Note that complex embeddings come in complex conjugate pairs.

Example 2.5. $\mathbb{Q}(\sqrt[3]{2})$ has 1 real $\mathbb{Q}$-embedding and 2 complex $\mathbb{Q}$-embeddings. $\lhd$

Theorem 2.6. *Let L be a finite extension of number the number field K with degree $[L : K] = n$.*

1. *The number of distinct K-embeddings of L is equal to the degree $[L : K]$*
2. *Suppose L is a field described by extending K by some $\alpha \in \mathbb{C}$, $L = K(\alpha)$. Now let $\sigma_1, \sigma_2, \ldots, \sigma_n$ denote the set of distinct K-embeddings into L. Then the embeddings permute the conjugates of α with*

$$m_{\alpha,K}(x) = \prod_{i=1}^{n} (x - \sigma_i(\alpha)).$$

Definition 2.7.
- Let $\alpha \in \mathbb{C}$, if α solves a monic polynomial $p(x)$ with only integer coefficients ($p(x) \in \mathbb{Z}[x]$), then α is an **algebraic integer**.
- The set of all such algebraic integers is denoted by $\overline{\mathcal{O}}$.

Definition 2.8. Let K be a number field. We define the **ring of integers** of K to be the intersection of K and $\overline{\mathcal{O}}$.

$$\mathcal{O}_K := K \cap \overline{\mathcal{O}}.$$

In [13], this ring is denoted by a gothic capital "O", $\mathfrak{O}$. This is in reference to the "maximal order" or "principle order" of the field.

Definition 2.9. Let L be a finite field extension of the number field K with degree $n = [L : K]$. For any $\alpha \in L$, the **relative algebraic norm** $N_{L/K}(\alpha)$ is defined multiplicatively through all $K-$embeddings $\sigma_i \colon L \to \mathbb{C}$. Specifically:

$$N_{L/K}(\alpha) := \prod_{i=1}^{n} \sigma_i(\alpha)$$

Theorem 2.10. Let L be an extension of the number field K of degree n.

1. For any $\alpha, \beta \in L$, it follows

   $$N_{L/K} \colon L^\times \to K^\times \qquad\qquad N_{L/K} \colon L^\times \to K^\times$$

   $$N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta) \qquad\qquad \mathrm{Tr}_{L/K}(\alpha + \beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta).$$

   Respectively, they are multiplicative and additive homomorphisms.

2. $N_{L/K}$ and $\mathrm{Tr}_{L/K}$ take $\mathcal{O}_L$ to $\mathcal{O}_K$. Formally, suppose $\alpha \in \mathcal{O}_L$ then $N_{L/K}(\alpha), \mathrm{Tr}_{L/K}(\alpha) \in \mathcal{O}_K$.

3. Let $\alpha, \beta \in \mathcal{O}_L$. Then $N_{L/K}(\alpha)$ divides $N_{L/K}(\beta)$ in $\mathcal{O}_K$ if α divides β in $\mathcal{O}_L$.

4. Let $\alpha \in \mathcal{O}_K$. Then α is a unit in $\mathcal{O}_K$ if and only if its norm satisfies $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

5. If a is an element of K, then its norm from L to K is a^n, and its trace from L to K is na. $N_{L/K}(a) = a^n$ and $\mathrm{Tr}_{L/K}(a) = na$.

Moreover, if $\alpha \in \mathcal{O}_L^\times$, then $\alpha^{-1} \in \mathcal{O}_L^\times$ with $N_{L/K}(\alpha)N_{L/K}(\alpha^{-1}) = 1$ and $N_{L/K}(\alpha) \in \mathcal{O}_K^\times$

See the exercises at the end of chapter 2 [14].

Definition 2.11. Suppose K is a number field of degree n. Then r is the number of real embeddings and c is half the number of complex embeddings. We denote the **signature** as the pair (r, c).

As a personal preference I associate r with real embeddings and c with complex ones, other sources call this pair (r_1, r_2) or (r, s).

Theorem 2.12 (Dirichlet's Unit Theorem)**.** Let (r, c) be the signature of a number field K. Then

$$\mathcal{O}_K^\times \cong W \times \mathbb{Z}^{r+c-1}$$

where W is the group of roots of unity in K, other sources may call it $\mu(K)$.

Equivalently, Dirichlet's theorem tells us there exist units $\varepsilon_1, \ldots, \varepsilon_{r+c-1}$ such that each unit $\varepsilon \in \mathcal{O}_K^\times$ can be uniquely expressed as

$$\varepsilon = \mu \varepsilon_1^{a_1} \cdots \varepsilon_{r+c-1}^{a_{r+c-1}},$$

where $a_i \in \mathbb{Z}$ and $\mu \in W$.

Proof. See appendix B [14]. □

Theorem 2.13. $\mathbb{Z}[\zeta_n]$ is the ring of algebraic integers of $\mathbb{Q}(\zeta_n)$.

Proof. Although we will prove the case for when $n = p$ is prime, the full proof is not in the scope of this thesis, see Thrm. 2.6 [14]. □

Although the following theorem is not exclusively about number fields, it applies to many different situations.

Theorem 2.14 (Eisenstein's criterion)**.** Suppose $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$, $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_i \in \mathbb{Z}$. If there is a prime p that satisfies:

1. p divides all of the integer coefficients a_i.
2. The final coefficient doesn't have p^2 as a factor, $p^2 \nmid a_0$.

Then $f(x)$ is an irreducible polynomial over $\mathbb{Z}$ (thus irreducible over $\mathbb{Q}$).

Proof. See Thrm. 1.8 [14]. □

2.2. Ideals of $\mathcal{O}_K$

Unless otherwise said, assume K is a number field. We will now recall a collection of useful results and basic definitions about ideals of $\mathcal{O}_K$. It is well known that $\mathcal{O}_K$ is a Dedekind domain. Hence although the algebraic integers of K may not have unique factorisation, unique factorisation is recovered in the form of ideals of $\mathcal{O}_K$. Many useful properties can be derived from the factorisation of ideals, as we will soon see.

Some of the first formalisations of ideals arose from Kummer's work on factorising Fermat's Last Theorem. He had shown that unique factorisation fails for some number fields, and then introduced a technical alternative which could be uniquely factorised. He originally called them "ideal numbers" [13].

Unless otherwise stated, we assume K is a number field. As before, these definitions and results are mainly adapted from chapter 5 [13] and chapter 1 section 3 of [9], but follow a similar style to the Algebraic Number Theory lecture notes.

Definition 2.15. For a non-zero ideal I in the ring of integers $\mathcal{O}_K$ of a number field K, the **ideal norm** of I, denoted $N(I)$, is defined as the cardinality of the quotient ring $\mathcal{O}_K/I$.

$$N(I) = |\mathcal{O}_K/I|.$$

The zero ideal is assigned a norm of zero, i.e., $N((0)) = 0$.

Proposition 2.16. In the ring of integers $\mathcal{O}_K$ of a number field K, the norm of a principal ideal (α) generated by an algebraic integer $\alpha \in \mathcal{O}_K$ satisfies

$$N((\alpha)) = \left|N_{K/\mathbb{Q}}(\alpha)\right|,$$

where $N_{K/\mathbb{Q}}(\alpha)$ denotes the field norm of α.

Proof. See corollary 5.10 [14]. □

Proposition 2.17. Let K be a number field and let A, B and C be non-zero ideals of $\mathcal{O}_K$. Then

1. If $AB = AC$, it then then follows that $B = C$.

2. Division is an equivalent condition to containment. Formally, $A \mid B$ if and only if $B \subset A$.

Clearly, if $a \in A$ then $(a)|A$

Proof. See proposition 5.7 [14]. □

Definition 2.18. Let L be a field extension of the number field K. Suppose Q is a prime ideal of $\mathcal{O}_L$, and P is a prime ideal of $\mathcal{O}_K$, both are non-zero. When $Q \mid P\mathcal{O}_L$, we say that Q **lies above** P.

Now we recall the following formalisation of unique factorisation of ideals.

Definition 2.19. Suppose L is a degree n extension of the number field K, and for some non-zero prime ideal P of $\mathcal{O}_K$. Write

$$P\mathcal{O}_L = Q_1^{e_1} Q_2^{e_2} \dots Q_k^{e_k},$$

where Q_i are all ideals of $\mathcal{O}_L$. They are all distinct prime ideals, and the only ones lying above P.

1. For each Q_i, e_i is called the **ramification index** over P.

2. It follows that $\mathcal{O}_K/P$ and $\mathcal{O}_L/Q_i$ are both finite fields. Moreover, the latter is a field extension of the first with degree $f_i = [\mathcal{O}_L/Q_i : \mathcal{O}_K/P]$. We call f_i the **inertial degree** of Q_i over P.

3. If $e_i > 1$ for some i, then P is **ramified in** L/K.

4. We say that a prime ideal is **totally ramified** if there is only one prime Q that lies above it with ramification index n.

5. Let Q_i be the prime ideals lying above P. Suppose we have equal ramification index and inertial degree, $e_i = f_i = 1$, for such primes. Then we say P is **totally split**.

6. If P is a prime ideal of $\mathcal{O}_K$ with no other primes lying above it, then we say P is **inert**. In other words, P remains a prime in $\mathcal{O}_L$ and $P\mathcal{O}_L$ is the only prime lying above $P\mathcal{O}_K$.

Chapter 1, section 3 [9] calls f_i the residue class degree.

Proposition 2.20. Suppose p is a prime number. Let K be a number field extension of degree $n = [K : \mathbb{Q}]$. Then the ideal generated by p in $\mathcal{O}_K$ factorises as

$$(p) = (p)\mathcal{O}_K = Q_1^{e1} Q_2^{e2} \cdots Q_k^{e_k}.$$

Now let f_i denote the inertial degree of Q_i over (p). Then

$$\sum_{i=1}^{k} e_i f_i = n.$$

Proof. See proposition 25 [9]. □

2.3. Class Group

Some rings $\mathcal{O}_K$ are not principle ideal domains. To measure the failure of unique factorisation of ideals, we form a group under the set of equivalence classes.

Unless otherwise stated, we assume K is a number field. These definitions and results are mainly adapted form [9] or [13], but they are defined by fractional ideals. Again, my results follow a similar style to the Algebraic Number Theory lecture notes.

Definition 2.21 (Ideal Equivalence)**.** Let K be a number field and let I and J be non-zero ideals in the ring of integers $\mathcal{O}_K$. We say that I is **equivalent** to J, denoted $I \sim J$, if there exist non-zero elements $\alpha, \beta \in \mathcal{O}_K$ such that

$$(\alpha)I = (\beta)J.$$

In other words, I and J are equivalent if multiplying them by suitable principal ideals yields the same ideal. This relation captures the idea that I and J belong to the same ideal class in the ideal class group of $\mathcal{O}_K$. $[I] = [J]$.

Definition 2.22 (Ideal Class Multiplication)**.** Let K be a number field, then Cl_K denotes the set of ideal classes of $\mathcal{O}_K$. Given two non-zero ideals I and J in $\mathcal{O}_K$, the **product** of their ideal classes, denoted $[I] \cdot [J]$, is defined by

$$[I] \cdot [J] := [IJ],$$

where $[I]$ and $[J]$ are the equivalence classes of I and J, respectively, and $[IJ]$ is the equivalence class of their product.

Proposition 2.23. Under the operation defined by product of ideal classes, Cl_K forms a group.

Proof. See [9], or chapter 9 [13]. □

Definition 2.24. Let K be a number field. The **class number** of K, denoted h_K, is defined to be the number of distinct ideal classes in $\mathcal{O}_K$; that is,

$$h_K := \#\mathrm{Cl}_K.$$

In summary, clearly all principle ideals are in the same equivalence class. This is the identity element of the group, $\mathcal{I}$. Hence if the class number $h_K = 1$, then all ideals are principle, $\mathcal{O}_K$ is a principle ideal domain and elements of $\mathcal{O}_K$ factorise uniquely.

Moreover, let $[J]$ be an ideal class of order n, $\mathrm{ord}([J]) = n$. It follows that I^n is principle for any ideal I in the same class as $[J]$.

2.4. Cyclotomic Fields

The study of cyclotomic fields as we know them first properly emerged thanks to Kummer's work in the 1840s and 1850s on reciprocity laws and Fermat's Last Theorem. Their study helped develop a lot of modern mathematics and they provide a good sampling ground between various related fields [14].

We say w is a primitive nth root of unity if n is the smallest non-zero natural number such that $w^n = 1$.

Definition 2.25. For any positive integer $n \in \mathbb{N}$, consider $\zeta_n = e^{2\pi i/n}$, which is a primitive nth root of unity. The field extension of $\mathbb{Q}$ obtained by adjoining ζ_n, denoted $\mathbb{Q}(\zeta_n)$, is known as a **cyclotomic number field**.

In this section we begin by proving some foundational results of cyclotomic fields. These results will be vital in setting us up to prove our main results. In particular we will factor the equation in Fermat's Last Theorem (FLT) for prime exponents, explore some useful examples of cyclotomic units, derive the minimal polynomial for ζ_{p^a} and expand on the structure of the roots of unity in a cyclotomic field.

The results and definitions in this section mainly follow from [14].

Theorem 2.26 (Fermat's Last Theorem)**.** Let $n \in \mathbb{Z}$ with $n > 2$. Then the Diophantine equation

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

has no non-trivial integer solutions $x, y, z \in \mathbb{Z}$, that is, there exist no solutions with $xyz \neq 0$.

It is well known that Fermat's Last Theorem was proved by Andrew Wiles.

Proposition 2.27. Let $m \in \mathbb{N}$ be an odd integer. Then

$$\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m}),$$

where $\zeta_k = e^{2\pi i/k}$ denotes a primitive kth root of unity.

Proof. Consider $\zeta_m = e^{2\pi i/m}$, a primitive mth root of unity, and $\zeta_{2m} = e^{2\pi i/(2m)}$, a primitive $2m$th root of unity.

Observe that

$$\zeta_{2m}^2 = \left(e^{2\pi i/(2m)}\right)^2 = e^{2\pi i/m} = \zeta_m.$$

It follows that $\zeta_m \in \mathbb{Q}(\zeta_{2m})$, and hence

$$\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{2m}).$$

To show the reverse inclusion, consider that m is odd. Then

$$-\zeta_m^{(m+1)/2} = -e^{2\pi i(m+1)/(2m)} = e^{\pi i} \cdot e^{2\pi i/(2m)} = \zeta_{2m}.$$

Thus $\zeta_{2m} \in \mathbb{Q}(\zeta_m)$, implying that

$$\mathbb{Q}(\zeta_{2m}) \subseteq \mathbb{Q}(\zeta_m).$$

Combining both inclusions, we conclude that

$$\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{2m}).$$

□

When working with cyclotomic fields, we can clearly ignore the trivial cases for $n = 1$ or 2 as $\mathbb{Q}(\zeta_1) = \mathbb{Q}(\zeta_2) = \mathbb{Q}$. Moreover, by Proposition 2.27, we adopt the following assumption to avoid redundancy arising from overlapping cases.

Convention 2.28. Throughout this work, when considering the cyclotomic field $\mathbb{Q}(\zeta_m)$, we assume that m is either odd or divisible by 4, i.e., $m \not\equiv 2 \pmod 4$.

Lemma 2.29. Let p be an odd prime, then $\prod_{i=0}^{p-1} \left(x + \zeta_p^i y\right) = x^p + y^p$.

Proof. Define f to be a function of X as follows:

$$f(X) = X^p - y^p \in \mathbb{Q}(\zeta_p).$$

Then $f(X)$ has p distinct roots, characterised by $X = y\zeta_p^i$, for all i such that $0 \leq i \leq p-1$. Moreover, as $f(X)$ is a polynomial of degree p, this allows us to factorise the function as a product of its roots,

$$f(X) = \prod_{i=0}^{p-1} \left(X - \zeta_p^i y\right).$$

Let's compare this result to the original definition of f. We let $-x = X$ and obtain the following evaluations:

$$f(-x) = \prod_{i=0}^{p-1}\left(-x - \zeta_p^i y\right) = (-1)^p \prod_{i=0}^{p-1}\left(x + \zeta_p^i y\right) = -\prod_{i=0}^{p-1}\left(x + \zeta_p^i y\right)$$
$$f(-x) = (-x)^p - y^p = -(x^p + y^p)$$

Hence we derive the factorisation $\prod_{i=0}^{p-1}\left(x + \zeta_p^i y\right) = x^p + y^p$ as required. □

We note that this factorisation will prove useful as it provides a factorisation of the equation in FLT for prime exponents.

Remark 2.30. Let n be an integer. Clearly 1 is a root of $x^n - 1$, hence $(x-1)$ divides $x^n - 1$. By expanding the following brackets or otherwise, we see

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

and hence

$$\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1.$$

◁

This relation will allow us to more cleanly find the minimal polynomial for ζ_{p^a}.

Lemma 2.31. Let p be any prime and p^a a prime power for some $a \in \mathbb{N}$, then the minimal polynomial of ζ_{p^a} is given by

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

Moreover,

$$m(x) = \prod_{\substack{1 \leq k \leq p^a \\ (k, p^a) = 1}} (x - \zeta_{p^a}^k).$$

Proof. Applying Remark 2.30 we clearly derive the equation

$$x^{p^a} - 1 = m(x) \cdot (x^{p^{a-1}} - 1).$$

Let $f(x) = x^{p^a} - 1$. Take k to be any such that $p \nmid k$, then $\zeta_{p^a}^k$ is a primitive p^ath root of unity. As $f(\zeta_{p^a}^k) = 0$ but $\zeta_{p^a}^k$ is not a root of $(x^{p^{a-1}} - 1)$, it follows that $m(\zeta_{p^a}^k) = 0$. Hence $(x - \zeta_{p^a}^k)$ factor $m(x)$. Moreover, $m(x)$ is monic so we only need to check that it is irreducible to justify that it is the minimal polynomial. Substitute $x = y + 1$:

$$m(y+1) = (y+1)^{p^{a-1}(p-1)} + (y+1)^{p^{a-1}(p-2)} + \cdots + (y+1)^{p^{a-1}} + 1.$$

By considering the binomial expansion of each power we observe

$$m(y+1) \equiv y^{p^{a-1}(p-1)} \pmod{p}.$$

Moreover, the final term of $m(y+1)$ is p. The polynomial $m(y+1)$ satisfies all the conditions of Eisenstein's criterion, Theorem 2.14. Thus, $m(y+1)$ is irreducible over $\mathbb{Q}$. Since irreducibility is preserved under linear transformations, the original polynomial $m(x)$ is also irreducible over $\mathbb{Q}$.

The final statement comes from observing that $\zeta_{p^a}^j$ is only a primitive p^ath root when $(j, p^a) = 1$. There are $\phi(p^a) = (p-1)p^{a-1}$ such distinct roots, $m(x)$ has degree $\phi(p^a)$, and so $\zeta_{p^a}^k$ can give the only factors where $1 \leq k \leq p^a$ and $(k, p^a) = 1$. □

Hence it follows that the $\mathbb{Q}$-embeddings of $\mathbb{Q}(\zeta_{p^a})$ are defined by

$$\sigma_k(\zeta_{p^a}) = \zeta_{p^a}^k, \qquad \text{for } (k,p) = 1.$$

They are the automorphisms of $\mathbb{Q}(\zeta_{p^a})$ and thus generate the Galois group,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q}) \cong (\mathbb{Z}/p^a\mathbb{Z})^\times.$$

See [12] for more detail.

We now introduce the following relations about cyclotomic units. First we consider units of $\mathbb{Z}[\zeta_{p^a}]$

Lemma 2.32. Let p^a be the power of any prime. Suppose r and s are integers with $(p, rs) = 1$. Then $\left(\zeta_{p^a}^r - 1\right) / \left(\zeta_{p^a}^s - 1\right)$ is a unit in $\mathbb{Z}[\zeta_{p^a}]$.

Proof. Since $p \nmid s$, s is a unit in $\mathbb{Z}/p\mathbb{Z}$, writing $ss^{-1}r \equiv st \equiv r \pmod p$ for some t, we have

$$\frac{\zeta_{p^a}^r - 1}{\zeta_{p^a}^s - 1} = \frac{\zeta_{p^a}^{st} - 1}{\zeta_{p^a}^s - 1} = \frac{(\zeta_{p^a}^s)^t - 1}{\zeta_{p^a}^s - 1}.$$

Thus using Remark 2.30

$$\frac{(\zeta_{p^a}^s)^t - 1}{\zeta_{p^a}^s - 1} = 1 + \zeta_{p^a}^s + \cdots + \zeta_{p^a}^{s(t-1)} \in \mathbb{Z}[\zeta_{p^a}].$$

Similarly, $\left(\zeta_{p^a}^s - 1\right) / \left(\zeta_{p^a}^r - 1\right) \in \mathbb{Z}[\zeta_{p^a}]$, where $\frac{\zeta_{p^a}^r - 1}{\zeta_{p^a}^s - 1} \cdot \frac{\zeta_{p^a}^s - 1}{\zeta_{p^a}^r - 1} = 1$. Hence they are both units. □

Thankfully, we also have a relation for units of $\mathbb{Z}[\zeta_n]$ where n is composite.

Proposition 2.33. Suppose n has at least two distinct prime factors. Then $1 - \zeta_n$ is a unit of $\mathbb{Z}[\zeta_n]$ and

$$\prod_{\substack{(j,n)=1 \\ 1 \leq j \leq n-1}} (1 - \zeta_n^j) = 1.$$

Proof. See proposition 2.8 [14]. □

Where D_K denotes the discriminant of the number field K, we reference the following relation:

Proposition 2.34. If $K = \mathbb{Q}(\zeta_n)$, then

$$D_K = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

Proof. See Prop 2.7 [14]. □

Theorem 2.35.

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^{\times},$$

with $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ maps $\zeta_n \mapsto \zeta_n^a$, for $a \in (\mathbb{Z}/n\mathbb{Z})^{\times}$.

$$\deg(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \phi(n)$$

Proof. See Theorem 2.5 [14] □

Lemma 2.36. Let $K = \mathbb{Q}(\zeta_n)$ and $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ be its maximal real subfield, see Proposition 4.4. Also let $\tau_1 \cdots \tau_{\phi(n)/2}$ be the $\mathbb{Q}$-embeddings of K^+. Then each pair $(\sigma, \bar{\sigma})$ of complex embeddings of K extends a unique τ. With τ being the restriction of σ on K^+.

$$\tau_i = \sigma_{i|K^+}$$

Proof. See [12] □

Proposition 2.37. If $(m, n) = 1$ then $\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}$.

Proof. See Proposition 2.4 [14]. □

Now we can formalise the group of roots of unity in a cyclotomic field.

Lemma 2.38. Let $K = \mathbb{Q}(\zeta_n)$ be the cyclotomic field generated by a primitive n-th root of unity ζ_n. Let W be the set of all roots of unity in K. Then

$$W = \begin{cases} \{\pm\zeta_n^i : 0 \leq i \leq n-1\} & \text{if } n \text{ is odd,} \\ \{\zeta_n^i : 0 \leq i \leq n-1\} & \text{if } n \text{ is divisible by 4.} \end{cases}$$

and W is clearly a group.

Proof. Clearly $\pm\zeta_n^k \in K$, hence $\{\pm\zeta_n^k : 1 \leq k \leq n\} \subseteq W$. Now we show the reverse inclusion. Suppose $w \in W$ of order m with $w^m = 1$ such that w is not of the form $\pm\zeta_n^k$. Then w is a primitive root of unity of the form ζ_m^j. By Proposition 2.37, $\zeta_m \notin W$ for $(m, n) = 1$. Then suppose $(m, n) > 1$. Note that if $m|n$ then $\zeta_m \in <\zeta_n>$. Hence for such a $w \in W$ to exist with $m \nmid n$, there must exist a prime $p|m$ with $p \nmid n$. Notice that when $p = 2$, this must mean that n is odd and m a multiple of 4 with

$$\zeta_4 \in \mathbb{Q}(\zeta_4) \subseteq \mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_n).$$

But this is a contradiction as $(4, n) = 1$. Now we suppose p to be an odd prime. As $\zeta_p \in \langle \zeta_m \rangle$,

$$\zeta_p \in \mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_n).$$

But this also contradicts Proposition 2.37 as $(p, n) = 1$, so no such w can exist. All roots of unity in K must be of the form $\pm\zeta_n^k$.

When n is odd the expression for W naturally follows. Then when n is even,

$$\zeta_n^{\frac{n}{2}} = -1.$$

So

$$\zeta_n^{k+\frac{n}{2}} = -\zeta_n^k$$

and hence the negative roots of unity are generated by powers of the positive ones. It clearly follows that $W = \{\zeta_n^i : 0 \le i \le n-1\}$ when n is even, equivalently when $n \equiv 0 \pmod 4$.

□

Lemma 2.39. Let $K = \mathbb{Q}(\zeta_n)$ be the cyclotomic field generated by a primitive n-th root of unity ζ_n. Let W be the group of all roots of unity contained in K. And Let $W^2 = \{w^2 \mid w \in W\}$. Then $|W/W^2| = 2$.

Proof. To analyse W^2, the subgroup of squares of elements in W, observe that the squaring map $\varphi : W \to W^2$, defined by $\varphi(\omega) = \omega^2$, is a surjective group homomorphism. The kernel of φ consists of elements $\omega \in W$ satisfying $\omega^2 = 1$. The only such elements are 1 and -1. Thus, $\ker\varphi = \{1, -1\}$, a subgroup of order 2. By the fundamental homomorphism theorem, $W/\ker\varphi \cong W^2$, implies $|W^2| = |W|/2$. Consequently, $[W : W^2] = 2$.

□

2.5. Dirichlet Characters

Here we define Dirichlet Character and introduce some properties. They may be used to obtain useful information about algebraic number fields. The following results and definitions are adapted from primarily chapter 3 [14].

Definition 2.40. The arithmetic function $\chi : \mathbb{Z} \to \mathbb{C}$ is a **Dirichlet character** of modulus m if it follows the following properties for all integers a, b:

1. $\chi(ab) = \chi(a)\chi(b)$
2. $\chi(a) \begin{cases} = 0 & \text{if } \gcd(a, m) > 1 \\ \neq 0 & \text{if } \gcd(a, m) = 1. \end{cases}$
3. $\chi(a + m) = \chi(a)$

Remark 2.41. Clearly, χ is a multiplicative homomorphism $\pmod m$. If $m|n$, then χ induces a homomorphism $\pmod n$. The same character χ can be defined over multiple modulus by composition with the natural group homomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times$, see Example 2.43. ◁

The smallest modulus for which we can define χ is called the **conductor** f_χ.

Definition 2.42. The **principal** character $\chi_0 \pmod m$ is the simplest character.

$$\chi_0(a) := \begin{cases} = 0 & \text{if } \gcd(a,m) \neq 1. \\ = 1 & \text{if } \gcd(a,m) = 1. \end{cases}$$

When χ_0 is read $\pmod 1$, we denote it by $\chi = 1$.

Example 2.43. Let $\chi \pmod 6$ be defined by $\chi(1) = 1$, $\chi(5) = -1$. Then the natural map $\phi : (\mathbb{Z}/6\mathbb{Z})^\times \to (\mathbb{Z}/3\mathbb{Z})^\times$ sends $\phi(1) = 1 \pmod 3$ and $\phi(5) = 2 \pmod 3$. Therefore the version of this character with minimal period is defined by $\chi(1) = 1 \pmod 3$ and $\chi(2) = -1 \pmod 3$. ◁

Definition 2.44. Later we will need to classify characters into two types. We define χ as **odd** if $\chi(-1) = -1$ and χ as **even** if $\chi(-1) = 1$

When the isomorphism between $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and $(\mathbb{Z}/n\mathbb{Z})^\times$ is employed, every Dirichlet character of modulus n canonically corresponds to a character of this Galois group. It can be beneficial to think of Dirichlet characters as being characters of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ [14].

Remark 2.45. For a number field $K = \mathbb{Q}(\zeta_n)$, there are $\phi(n)$ Dirichlet characters ◁

2.6. Galois Theory

Definition 2.46 (9.1 [12])**.** If K is a subfield of $\mathbb{C}$, the subfield L is an extension of K, and f is a nonzero polynomial over K, then f *splits* over L if it can be expressed as a product of linear factors

$$f(t) = k(t - \alpha_1) \cdots (t - \alpha_n)$$

where $k \in K$ and $\alpha_1, \ldots, \alpha_n \in L$.

Definition 2.47 (9.3 [12])**.** A subfield Σ of $\mathbb{C}$ is a **splitting field** for the nonzero polynomial f over the subfield K of $\mathbb{C}$ if $K \subseteq \Sigma$ and

1. f splits over Σ;
2. If $K \subseteq \Sigma' \subseteq \Sigma$ and f splits over Σ', then $\Sigma' = \Sigma$.

Definition 2.48 (9.8 [12])**.** An algebraic field extension L/K is said to be **normal** if every irreducible polynomial $f \in K[x]$ that has at least one root in L splits completely over L; that is, all the roots of f lie in L.

Theorem 2.49 (12.2 [12])**.** If L/K is a finite normal field extension inside $\mathbb{C}$, with Galois group $\mathrm{Gal}(L : K)$. Then an intermediary field M is a normal extension of K if and only if $\mathrm{Gal}(M : K)$ is a normal subgroup of $\mathrm{Gal}(L : K)$

2.7. Asymptotics and Notation

Now, we introduce some common notation to ultimately help us in bounding functions for the class number. The following results and definitions are adapted from [5]. We begin by defining big O notation.

Definition 2.50 (Big-O)**.** Assume that $f(x)$ and $g(x)$ are functions that accept arguments over some portion of the real number line. We denote

$$f(x) = O(g(x))$$

as $x \to \infty$ when there are constants C and N such that

$$|f(x)| \leq C\,|g(x)| \quad \text{for every } x > N.$$

This expresses the idea that f does not grow faster than g in the long run.

Besides big O notation, another commonly used analytical symbol in mathematics is the *little o*. In general terms, the expression $f(x) = o(g(x))$ indicates that the function f increases at a significantly slower rate than g, making it negligible in comparison.

Definition 2.51 (Little-o)**.** Suppose f and g are functions that accept arguments over some portion of the real number line. We say

$$f(x) = o(g(x))$$

as $x \to \infty$ if, for every constant $C > 0$, there exists a number N such that for all $x > N$, the inequality

$$|f(x)| < C\,|g(x)|$$

holds. Provided that $g(x) \neq 0$, this is equivalent to the limit condition

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

Definition 2.52. Let $f : \mathbb{N} \to \mathbb{R}$ and $g : \mathbb{N} \to \mathbb{R}$ be functions. We say that $f(n)$ is asymptotic to $g(n)$,

$$f(n) \sim g(n) \quad \text{as } n \to \infty,$$

if

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1.$$

That is, $f(n)$ and $g(n)$ are **asymptotically equivalent** if the ratio $f(n)/g(n)$ tends to 1 as $n \to \infty$. This relation expresses that $f(n)$ and $g(n)$ have the same leading-order behaviour in the limit of large n.

It then follows that

$$f(n) \sim g(n) \iff f(n) = g(n) + o(g(n))\,.$$

3. Kummer's Special Case on FLT

Fermat's Last Theorem (FLT) served as a significant motivation for the development of cyclotomic field theory. Prior to the 19th century, efforts towards proving FLT were largely concentrated on intricate methods tailored to specific small exponents. In this chapter, we examine the breakthrough that redirected the focus of FLT research towards a more general approach applicable to a broader class of exponents. This development also provides a natural foundation for the topics discussed in subsequent chapters.

We study the breakthrough made onto a more general approach for FLT through the work of Ernst Kummer's special case of Fermat's Last Theorem. Kummer was primarily driven by the study of quadratic reciprocity. He encountered FLT in his pursuit of discovering higher reciprocity laws. He regarded his special case as a "curiosity of number theory rather than a major item."[4]. In this chapter, we focus on this so-called curiosity, exploring Kummer's detailed proof that the equation

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

has no integer solutions when p does not divide x, y, or z, and when p is an odd **regular prime**—that is, when p does not divide the class number of $\mathbb{Q}(\zeta_p)$. Our proof closely follows the general structure provided by chapter 1 [14], but certain results have been further abstracted to more general cases. Some of the proofs have also been abstracted from chapter 11 [13].

In the context of FLT, elementary methods allow us to disregard the case for $n = 4$ and thus reduce the equation to only consider when n is an odd prime p, as demonstrated in Chapter 11 of [13].

Theorem 3.1 (Kummer's Special Case)**.** Suppose p is an odd prime and p does not divide the class number of the field $\mathbb{Q}\left(\zeta_p\right)$, where ζ_p is a primitive p th root of unity. Then

$$x^p + y^p = z^p, \quad (xyz, p) = 1$$

has no solutions for x, y and z in the rational integers. Where (xyz, p) denotes the greatest common divisor.

Remark 3.2. Note that if any two of the integer solutions share a common factor, then the third shares the same factor. So we may remove the common factors of any solution and henceforth assume that $(x, y) = (x, z) = (y, z) = 1$. ◁

3.1. Overview of the Proof

We are led to use the Dedekind domain $\mathbb{Z}[\zeta_p]$ in order to factor the equation, using Lemma 2.29,

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

We are motivated to consider this equation as a product of ideals. We will show that the ideals are all coprime to each other.

In summary, Kummer's argument relies on being able to express the principal generator of each ideal mentioned as a unit times an integer (mod p). This relation will allow us to create another expression (mod p) depending on just 4 terms of powers of ζ_p. By considering the only possible cases we will prove Theorem 3.1.

For the remainder of the chapter we will assume that $\zeta_p = \zeta$ and the field $K = \mathbb{Q}(\zeta)$, unless otherwise stated.

In order to make use of this previous factorisation, we will prove that the ring of integers of the field $\mathbb{Q}(\zeta)$ is in fact $\mathbb{Z}[\zeta]$. Let's now prove a preliminary result.

3.2. Preliminaries

Lemma 3.3. Let $K = \mathbb{Q}(\zeta_{p^a})$ for any prime p, and let ϕ denote the Euler totient function, $\phi(p^a) = (p-1)p^{a-1}$. The ideal $(1 - \zeta_{p^a})$ is a prime ideal of $\mathcal{O}_K$ with $(1-\zeta_{p^a})^{\phi(p^a)} = (p)$. Therefore p is totally ramified in $\mathbb{Q}(\zeta_{p^a})$.

Proof. We begin by defining the function f, it's factorisation follows from Lemma 2.31:

$$f(X) = (X^{p^a})^{p-1} + (X^{p^a})^{p-2} + \cdots + (X^{p^a}) + 1 = \prod_{\substack{1 \le k \le p^a \\ (k,p^a)=1}} (x - \zeta_{p^a}^k).$$

By considering $X = 1$, we obtain $p = f(1)$. From Lemma 2.32, we have that $(1 - \zeta_{p^a})$ and the other factors of $f(X)$ are associates in $\mathbb{Z}[\zeta_{p^a}]$. Hence the ideals $(1 - \zeta_{p^a})$ and $\left(1 - \zeta_{p^a}^i\right)$ are equivalent when $(k, p^a) = 1$, or equivalently $p \nmid k$. Therefore

$$(p) = \prod_{\substack{1 \le k \le p^a \\ gcd(k,p^a)=1}} (1 - \zeta_{p^a}^k) = (1 - \zeta_{p^a})^{\phi(p^a)}$$

as ideals. Now we show that $(1 - \zeta_{p^a})$ is prime by calculating the norms of (p) and $(1 - \zeta_{p^a})$.

$$N((p)) = N_{K/\mathbb{Q}}(p) = p^{\deg(\mathbb{Q}(\zeta_{p^a})/\mathbb{Q})} = p^{\phi(p^a)}.$$

$$N((1 - \zeta_{p^a})) = N_{K/\mathbb{Q}}(1 - \zeta_{p^a}) = \prod_{\substack{1 \le k \le p^a \\ (k,p^a)=1}} (x - \zeta_{p^a}^k) = p.$$

Hence we confirm that the norm behaves multiplicatively as expected and that the ideal $(1 - \zeta_{p^a})$ divides (p) exactly $\phi(p^a)$ times. Now suppose $(1 - \zeta_{p^a})$ were not a prime ideal. Then it could be expressed factor of two non-trivial proper ideals $(1 - \zeta_{p^a}) = \mathcal{A} \cdot \mathcal{B}$. In which case, $N((1 - \zeta_{p^a})) = N(\mathcal{A}) \cdot N(\mathcal{B})$ contradicts the primality of $N((1 - \zeta_{p^a}))$. Hence $(1 - \zeta_{p^a})$ must be a prime ideal of $\mathcal{O}_k$. □

Definition 3.4. Let $\mathcal{Q}$ be a prime ideal in a Dedekind domain. We define $v_{\mathcal{Q}}(\mathcal{J})$ to be the largest exponent $e \in \mathbb{N}$ of the ideal $\mathcal{Q}$ such that $\mathcal{Q}^e \mid \mathcal{J}$. Also known as the valuation of the ideal $\mathcal{Q}$ on $\mathcal{J}$. Alternatively

$$v_{\mathcal{Q}}(\mathcal{J}) := \max\{e \in \mathbb{N} : \mathcal{Q}^e \mid \mathcal{J}\}.$$

Note that this definition makes sense in Dedekind domains as we have unique factorisation of prime ideals. And when considering the valuation on an algebraic integer $\alpha \in \mathcal{O}_k$, we use $v_{\mathcal{Q}}(\alpha)$ to denote the valuation of the ideal $\mathcal{Q}$ on the ideal generated by α, i.e. (α).

Example 3.5. Let $K = \mathbb{Q}(\zeta)$ and $\mathfrak{p} = (1-\zeta)$, a prime ideal in $\mathcal{O}_K$.

- $v_{\mathfrak{p}}(-2) = 0$ because $p \nmid 2$,
- $v_{\mathfrak{p}}(p) = p-1$ because $(p) = \mathfrak{p}^{p-1}$,
- $v_{\mathfrak{p}}((1-\zeta)^i) = i$.

◁

Definition 3.6. Now let us extend the ideal valuation to include fractional algebraic integers $\frac{\alpha}{\beta} \in \mathbb{Q}(\zeta)$, where $\alpha, \beta \in \mathcal{O}_K$.

$$v_{\mathcal{Q}}(\frac{\alpha}{\beta}) := v_{\mathcal{Q}}(\alpha) - v_{\mathcal{Q}}(\beta).$$

Remark 3.7. Let $\alpha, \beta, \gamma, \delta \in \mathcal{O}_K$ be algebraic integers.

- $v_{\mathcal{Q}}(\alpha \cdot \beta) = v_{\mathcal{Q}}(\alpha) + v_{\mathcal{Q}}(\beta)$.
- $v_{\mathcal{Q}}(\alpha + \beta) \geq \min\{v_{\mathcal{Q}}(\alpha), v_{\mathcal{Q}}(\beta)\}$, with equality when $v_{\mathcal{Q}}(\alpha) \neq v_{\mathcal{Q}}(\beta)$.

These properties can easily be extended to obtain similar relations about the valuation on fractional algebraic integers.

- $v_{\mathcal{Q}}(\frac{\alpha}{\beta} \cdot \frac{\gamma}{\delta}) = v_{\mathcal{Q}}(\alpha \cdot \gamma) - v_{\mathcal{Q}}(\beta \cdot \delta) = v_{\mathcal{Q}}(\frac{\alpha}{\beta}) + v_{\mathcal{Q}}(\frac{\gamma}{\delta})$.

The next point can be seen by noticing $v_{\mathcal{Q}}(\frac{\alpha\delta+\gamma\beta}{\beta\delta}) = v_{\mathcal{Q}}(\alpha\delta + \gamma\beta) - v_{\mathcal{Q}}(\beta\delta)$:

- $v_{\mathcal{Q}}(\frac{\alpha}{\beta} + \frac{\gamma}{\delta}) = \begin{cases} v_{\mathcal{Q}}(\frac{\alpha}{\beta}) & \text{if } v_{\mathcal{Q}}(\alpha \cdot \delta) < v_{\mathcal{Q}}(\beta \cdot \gamma) \\ v_{\mathcal{Q}}(\frac{\gamma}{\delta}) & \text{if } v_{\mathcal{Q}}(\beta \cdot \gamma) < v_{\mathcal{Q}}(\alpha \cdot \delta) \end{cases}$

Alternatively, we could interpret the second bullet point to mean that the valuation on the sum of two fractional algebraic integers is equal to the valuation on the minimum of the two if $v_{\mathcal{Q}}(\frac{\alpha}{\beta}) \neq v_{\mathcal{Q}}(\frac{\gamma}{\delta})$.

$$v_{\mathcal{Q}}\left(\frac{\alpha}{\beta} + \frac{\gamma}{\delta}\right) \geq \min\left\{v_{\mathcal{Q}}\left(\frac{\alpha}{\beta}\right), v_{\mathcal{Q}}\left(\frac{\gamma}{\delta}\right)\right\}, \text{ with equality when } v_{\mathcal{Q}}\left(\frac{\alpha}{\beta}\right) \neq v_{\mathcal{Q}}\left(\frac{\gamma}{\delta}\right).$$

◁

Proposition 3.8. $\mathbb{Z}[\zeta]$ is the ring of algebraic integers in the field $K = \mathbb{Q}(\zeta)$. Therefore $\mathcal{O}_K$ is a Dedekind domain (so we have unique factorization into prime ideals, etc.).

Proof. Let $\mathcal{O}_k$ denote the algebraic integers of $\mathbb{Q}(\zeta)$. Clearly $\mathbb{Z}[\zeta] \subseteq \mathcal{O}_k$. We must show the reverse inclusion.

Let v denote the valuation of the ideal $(1-\zeta)$. So $v(1-\zeta) = 1$ and for $b \in \mathbb{Z}, v(b) \equiv 0 \pmod{p-1}$ because b is either coprime to p or not (both arise to the desired result). Clearly $\mathbb{Q}(\zeta) = \mathbb{Q}(1-\zeta)$, hence we choose $\{1, 1-\zeta, (1-\zeta)^2, \ldots, (1-\zeta)^{p-2}\}$ to be a valid basis for $\mathbb{Q}(\zeta)$ as a vector space over $\mathbb{Q}$. Let $\alpha \in \mathcal{O}_k$. Then

$$\alpha = a_0 + a_1(1-\zeta) + \cdots + a_{p-2}(1-\zeta)^{p-2}$$

with $a_i \in \mathbb{Q}$. First we will use the valuation to show that p doesn't divide the denominator of each a_i. Let $\frac{m}{n} \in \mathbb{Q}$ for $m, n \in \mathbb{Z}$, then it holds that $v(\frac{m}{n}) = v(m) - v(n) \equiv 0 \pmod{p-1}$.

In order to take the valuation of α, we observe that the numbers

$$v(a_i(1-\zeta)^i) \equiv v(a_i) + i \equiv i \pmod{p-1}, \text{ for } 0 \leq i \leq p-2.$$

They are distinct $\pmod{p-1}$ and hence distinct in general. Then there is a minimal element $a_c(1-\zeta)^c$ for some $c \in \mathbb{Z}$, with the property that $v(a_c(1-\zeta)^c + a_k(1-\zeta)^k) = v(a_c(1-\zeta)^c)$ for all $k \neq c$. Therefore we can repeatedly use the result at the end of remark Remark 3.7 to obtain

$$v(\alpha) = \min_{0 \leq i \leq p-2} \{v\left(a_i(1-\zeta)^i\right)\}.$$

Due to the unique factorisation of ideals into prime ideals $v(\alpha) \geq 0$. Moreover, for each i, we must have $v(a_i) \geq 0$, since $v((1-\zeta)^i) > 0$. Therefore a_i is a rational with p not dividing its denominator. Hence we can now rearrange the expression for α in terms of the natural basis for $\mathbb{Q}(\zeta)$ whilst maintaining that p divides no denominator of each coefficient. Formally,

$$a_0 + a_1(1-\zeta) + \cdots + a_{p-2}(1-\zeta)^{p-2} = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2} = \alpha.$$

Since each $b_i \in \mathbb{Q}$ is a linear combination of the a_i, we preserve that p divides no denominator of b_i. Now we will use this property to show that $b_i \in O_K$. We will use a change of basis matrix to show this.

Let σ be a $\mathbb{Q}$-embedding of $\mathbb{Q}(\zeta)$, since they permute the $p-1$ conjugates, they are defined by $\sigma_i(\zeta) = \zeta^i$ for $1 \leq i \leq p-1$. Then we have

$$\begin{bmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_{p-1}(\alpha) \end{bmatrix} = \begin{bmatrix} 1 & \zeta & \zeta^2 & \cdots & \zeta^{p-2} \\ 1 & \zeta^2 & \zeta^4 & \cdots & \zeta^{2(p-2)} \\ 1 & \zeta^3 & \zeta^6 & \cdots & \zeta^{3(p-2)} \\ \vdots & \vdots & \vdots & \ddots & \\ 1 & \zeta^{p-1} & \zeta^{2(p-1)} & & \zeta^{(p-1)(p-2)} \end{bmatrix} \begin{bmatrix} b_0 \\ \vdots \\ b_{p-2} \end{bmatrix}$$

This is a square Vandermonde matrix, hence its determinant is calculated by

$$\det(V) = \prod_{1 \le j < k \le p-1} (\zeta^k - \zeta^j),$$

see Thrm 9.67 [1] for a full proof.

We have $\zeta^k - \zeta^j = \zeta^j(\zeta^{k-j} - 1)$. Since ζ^j is a unit, the critical term is $\zeta^{k-j} - 1$, which factors as $(1-\zeta)(1+\zeta+\cdots+\zeta^{k-j-1})$. Recall that by Lemma 2.32, $(1+\cdots+\zeta^{k-j-1})$ is a unit. Thus :

$$\det(V) = (\text{unit}) \cdot (1-\zeta)^N, \quad \text{for some } N \in \mathbb{N}.$$

To acquire an expression for each b_i, we recall that the Vandermonde matrix is invertible and then the inverse matrix must be made up of algebraic elements. Then the final expression for b_i is obtained:

$$b_i = \frac{\beta_i}{(\text{unit}) \cdot (1-\zeta)^N}, \quad \text{for some } \beta_i \in \mathcal{O}_K.$$

This implies $b_i \cdot (1-\zeta)^N$ is an algebraic integer. To show that $b_i \in \mathbb{Z}$, we suppose that there is some prime q with $q \neq p$ which divides the dominator of b_i. But then $b_i \cdot (1-\zeta)^N$ would not have a minimal polynomial of integer coefficients. Clearly this cannot be the case, and since there is no p in the denominator of b_i, we guarantee that $(1-\zeta)^N$ cancels out no power of p. Therefore, $b_i \in \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$. □

Our proof of Theorem 3.1 will rely on division properties when factoring $x^p + y^p$, this is now possible as $\mathcal{O}_K$ is a Dedekind domain.

3.3. Proof

Now we will begin the proof by considering the case of $p = 3$ separately. It will play a special role in our proof.
Reminder:

$$x^p + y^p = z^p, \quad (xyz, p) = 1$$

has no solutions in rational integers.

Proof of Theorem 3.1. If $p = 3$, and since $p \nmid x$, then $x^3 \equiv \pm 1 \pmod 9$. The same is true for y^3 and z^3. Therefore $x^3 + y^3 \equiv -2, 0$ or $2 \pmod 9$, but then $x^3 + y^3 \neq z^3$. A similar proof shows $p \neq 5$, but for $p = 7$ we have that $1^7 + 2^7 \equiv 3^7 \pmod{49}$. We need a new method. For the remainder of this proof we will assume $p \geq 5$. But before we continue, the following lemma will be very useful for later factorisation.

Lemma 3.9. Assume $p \geq 5$ and suppose $x^p + y^p + (-z)^p = 0$ and $p \nmid xyz$. Then given a solution (x, y, z) there exists a pair that is not equivalent $\pmod p$.

Proof. Suppose we have a solution (x, y, z) with $x \equiv y \equiv -z \pmod{p}$. Then $3(-z)^p \equiv 0$, which is impossible since $p \nmid 3z$. Therefore $x \not\equiv y$, $x \not\equiv -z$ or $y \not\equiv -z$. □

Remark 3.10. Suppose we have an integer solution (a, b, c) for $a^p + b^p + c^p = 0$. Then due to the symmetric nature of the equation, this is equivalent to saying that (a, c, b) or (c, b, a) is a solution. By the previous lemma, we can safely assume that one of the pairs is not equivalent $\pmod{p}$. Without loss of generality, say that $b \not\equiv c$. We can then rearrange the equation as necessary to obtain $b^p + c^p + a^p = 0$. Now relabelling as desired we can obtain $(a')^p + (b')^p + (c')^p = 0$ with $a' \not\equiv b'$. ◁

This is important as we are able to use the previous lemma to relabel the equation where necessary to have $(x')^p + (y')^p = (z')^p$ with $x' \not\equiv y' \pmod{p}$. For the remainder of the proof of Theorem 3.1, we omit the notation for the transformed variables and assume that $x \not\equiv y \pmod{p}$

Lemma 3.11. When considering the factorised form of the equation in Theorem 3.1, the ideals $(x + \zeta^i y)$ are pairwise coprime, $i = 0, 1, \ldots, p-1$.

Proof. Suppose $\mathfrak{P}$ is a prime ideal with $\mathfrak{P} \mid (x + \zeta^i y)$ and $\mathfrak{P} \mid (x + \zeta^j y)$ for some $i \neq j$, without loss of generality assume $i > j$. Then

$$\mathfrak{P} \mid y(\zeta^i - \zeta^j),$$

similarly $\mathfrak{P}$ divides both $\zeta^j(x + \zeta^i y)$ and $\zeta^i(x + \zeta^j y)$, in particular

$$\mathfrak{P} \mid x(\zeta^i - \zeta^j).$$

By factoring out units, we have

$$(\zeta^i - \zeta^j) = \zeta^j(\zeta^{i-j} - 1) = \frac{\zeta^j(\zeta^{i-j} - 1)}{(\zeta - 1)}(\zeta - 1) = (unit)(\zeta - 1).$$

Recall that $(\zeta - 1)$ is prime and $(x, y) = 1$. Therefore, either $\mathfrak{P} = (\zeta - 1)$ or $\mathfrak{P}$ divides both x and y. The latter cannot be the case because then there would be integers a and b such that $xa + yb = 1 \in \mathfrak{P}$, contradicting the primality of $\mathfrak{P}$. Hence $\mathfrak{P} = (\zeta - 1)$, with $x + \zeta^i y \equiv x + y \equiv 0 \pmod{\mathfrak{P}}$. In fact, because $x + y \in \mathbb{Z}$, then $\mathfrak{P}^{p-1} \mid (x + y)$ or equivalently $x + y \equiv 0 \pmod{p}$. But by considering the implications this has on the original equation,

$$z \equiv z^p = x^p + y^p \equiv x + y \equiv 0 \pmod{p}.$$

So $p \mid z$, but this contradicts our original assumption. The ideals must be coprime. □

Returning to the Proof of Theorem 3.1. Now we will encounter the main argument where we use the fact that p is regular.

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

Since the ideals $(x + \zeta^i y)$ are co-prime, each one must be the p^{th} power of an ideal:

$$(x + \zeta^i y) = A_i^p.$$

Consider the congruence class of that ideal as an element of the class group, $[A_i] \in CL_{\mathbb{Q}(\zeta)}$. As A_i^p is principle, $[A_i]^p = \mathcal{I}$, its order must be 1 or p. By standard properties of a group, the order of $[A_i]$ must divide the order of the group. But because p is regular, it does not divide the order of the class group. Consequently, since the class group has order coprime to p, the ideal A_i is also **principal** for some generator α_i, i.e. $(x + \zeta^i y) = (\alpha_i^p)$. The generators are equivalent up to units, so for some $\varepsilon \in \mathcal{O}_K^\times$,

$$x + \zeta^i y = \varepsilon \cdot \alpha_i^p.$$

The rest of the proof involves taking this equation $\pmod p$ and showing there can be no such integer solutions. We may now omit the subscripts as we show there can be no solution for any arbitrary power, $x + \zeta y = \varepsilon \cdot \alpha^p$.

By expressing α in terms of its integral basis $\alpha = b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2}$. Now we consider its powers $\pmod p$. By repeatedly using the binomial expansion or the multinomial theorem expansion,

$$\begin{aligned}\alpha^p = (b_0 + b_1\zeta + \cdots + b_{p-2}\zeta^{p-2})^p &\equiv b_0^p + (b_1\zeta)^p + \cdots + (b_{p-2}\zeta^{p-2})^p \pmod p\\ &\equiv b_0^p + b_1^p + \cdots + b_{p-2}^p \pmod p\end{aligned}$$

So for some $a \in \mathbb{Z}$, $\alpha^p \equiv a \pmod p$. Hence we are left with the more digestible expression

$$x + \zeta y \equiv \varepsilon \cdot a \pmod p.$$

To make further progress on the proof, we would like to take the complex conjugate of this whole expression. As it turns out, we can factor out the real component of the unit ε. But to do this, we need another lemma to determine when an algebraic integer is a root of unity.

The following lemma adapted from Lemma 11.6 [13].

Lemma 3.12. If $P(t) \in \mathbb{Z}[t]$ is a monic polynomial, all of whose roots have absolute value 1. Then every root is a root of unity. Moreover, if α is an algebraic integer all of whose conjugates have absolute value 1, then α is a root of unity.

Proof. We will denote $P(t) = (t - \alpha_1)\ldots(t - \alpha_n)$ to be the factorisation of the minimal polynomial of α with conjugates $\alpha_1, \cdots \alpha_n$. First note that any power of each conjugate also has absolute value 1. This property is crucial as we label the polynomial appropriately,

$$P_l(t) = (t - \alpha_1^l)\ldots(t - \alpha_n^l) = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in \mathbb{Z}[t].$$

Notice that the integer coefficients a_i are all obtained by expanding the linear factors of the conjugates. Hence, by considering the binomial coefficients derived from expanding the roots of P_l each integer a_i is bounded by $|a_i| \leq \binom{n}{j}$. This means there can only be a finite number of these irreducible polynomials which have a power of α as a root, hence by taking further powers of the conjugates, eventually $P_l(t) = P_m(t)$ for some $l \neq m$. Meaning that the functions are equal up to some permutation of the conjugates. Hence there exists a permutation π of $\{1, \ldots, k\}$ such that

$$\alpha_j^l = \alpha_{\pi(j)}^m$$

for $j = 1, \ldots, k$. Now we will show by induction that each α_j is a root of unity. Suppose that

$$\alpha_j^{l^r} = \alpha_{\pi^r(j)}^{m^r}$$

for all $r \in \mathbb{N}$. We will show it then true for $r+1$.

$$\alpha_j^{l^{r+1}} = (\alpha_j^{l^r})^l = (\alpha_{\pi^r(j)}^{m^r})^l = (\alpha_{\pi^r(j)}^l)^{m^r} = \alpha_{\pi^{r+1}(j)}^{m^{r+1}}$$

Hence by induction $\alpha_j^{l^r} = \alpha_{\pi^r(j)}^{m^r}$ for all $r \in \mathbb{N}$. Additionally, since π is a permutation of k elements, after applying it $k!$ times. We have $\pi^{k!}(j) = j$, so $\alpha_j^{l^{k!}} = \alpha_j^{m^{k!}}$ and hence we can find some non-zero power of α such that

$$\alpha_j^{(l^{k!} - m^{k!})} = 1.$$

Since $l^{k!} \neq m^{k!}$, it follows that α_j is a root of unity. □

Now we can begin the lemma which factors the real component out of the unit ε.

Lemma 3.13. Let p^n be the power of an odd prime p. Also let ε be a unit of $\mathbb{Z}[\zeta_{p^n}]$. Then there exists a real $q \in \mathbb{Q}(\zeta_{p^n} + \zeta_{p^n}^{-1})$ and $r \in \mathbb{Z}$ such that $\varepsilon = \zeta_{p^n}^r q$.

Proof. Let $\alpha = \varepsilon/\bar{\varepsilon}$, then α is an algebraic integer since $\bar{\varepsilon}$ is a unit. Since the $\mathbb{Q}$-embeddings σ of $\mathbb{Q}(\zeta_{p^n})$ are field homomorphisms, they commute with complex conjugation. Hence,

$$\overline{\sigma(\alpha)} = \sigma(\overline{\alpha}) = \sigma(\alpha^{-1}),$$

and $|\sigma(\alpha)| = \sqrt{\sigma(\alpha)\sigma(\alpha^{-1})} = 1$. Since all of the conjugates of α have absolute value 1, it follows that α is a root of unity, so $\varepsilon/\bar{\varepsilon} = \pm\zeta_{p^n}^a$ for some a.

Writing $\varepsilon = b_0 + b_1\zeta_{p^n} + b_1\zeta_{p^n}^2 + \cdots$ in terms of the $\mathbb{Z}$ basis and evaluating $\varepsilon \mod (1-\zeta_{p^n})$, we observe that $\varepsilon \equiv \bar{\varepsilon} \pmod{1-\zeta_{p^n}}$. However we now have positive and negative cases to consider,

$$\varepsilon = \pm\varepsilon\zeta_{p^n}^a \equiv \pm\bar{\varepsilon} \pmod{1-\zeta_{p^n}}.$$

Note that $2 \notin (1-\zeta_{p^n})$ because $p \in (1-\zeta_{p^n})$, see Proposition 2.17. Clearly, $\bar{\varepsilon} \notin (1-\zeta_{p^n})$. It follows that $2\bar{\varepsilon} \not\equiv 0 \pmod{1-\zeta_{p^n}}$. Hence, $\varepsilon \not\equiv -\bar{\varepsilon}\zeta_{p^n}^a$, so we need only consider the positive case $\varepsilon/\bar{\varepsilon} = \zeta_{p^n}^a$.

To find the rational factor, take r such that $2r \equiv a \pmod{p}$, and define $q = \bar{\varepsilon}\zeta_{p^n}^r$. To prove that q is real, observe that

$$\bar{q} = \varepsilon\zeta_{p^n}^{-r} = \bar{\varepsilon}\zeta_{p^n}^{a-r} = q.$$

Finally, $\varepsilon = \zeta_{p^n}^r q$, as required. In Proposition 4.4 we show $\mathbb{Q}(\zeta_{p^n} + \zeta_{p^n}^{-1})$ is the largest real subfield of $\mathbb{Q}(\zeta_{p^n})$, and hence q is an element of it. □

In fact, q is also a unit, though this is not necessary for the proof.

Returning to the Proof of Theorem 3.1. Recall that our previous task was to take the complex conjugate on

$$x + \zeta y \equiv \varepsilon \cdot a \pmod{p}$$

By the previous lemma, we have

$$x + \zeta y \equiv \varepsilon a \equiv \zeta^r qa \pmod{p}$$

and

$$x + \zeta^{-1} y \equiv \bar{\varepsilon} a \equiv \zeta^{-r} qa \pmod{p}.$$

Then, rearranging in terms of qa,

$$\zeta^r(x + \zeta^{-1}y) \equiv qa \equiv \zeta^{-r}(x + \zeta y) \pmod{p}.$$

and

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

We are close now, as it turns out, $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$ are not all distinct. We will prove this in the following lemma. This will allow us to consider the cases of which roots of unity are equal to each other.

Lemma 3.14. Suppose $\alpha = a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}$ with $a_j \in \mathbb{Z}$ and at least one $a_i = 0$. If $n \in \mathbb{Z}$ and n divides α then n divides each a_j. Similarly, suppose all $a_i \in \mathbb{Z}_p$ and at least one $a_i = 0$. If p divides α, then p divides each a_j.

Proof. The relation $1 + \zeta + \cdots + \zeta^{p-1} = 0$ implies $\mathbb{Z}[\zeta]$ is a free $\mathbb{Z}$-module with basis $\{1, \zeta, \ldots, \zeta^{p-1}\} \setminus \{\zeta^k\}$ for any k. Suppose $a_k = 0$. Expressing α in terms of this basis, uniqueness of coefficients gives

$$\alpha = \sum_{i \neq k} a_i \zeta^i.$$

If $n \mid \alpha$, then $\alpha = n\beta$ for some $\beta \in \mathbb{Z}[\zeta]$. Writing β in the same basis

$$\beta = \sum_{i \neq k} b_i \zeta^i,$$

we equate the coefficients $a_i = nb_i$. Thus, $n \mid a_i$ for all i. For $\mathbb{Z}_p[\zeta]$, the same basis applies. And so the argument is similar. □

Finale of the Proof of Theorem 3.1
Recall the congruence:

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

Our goal is to derive a contradiction primarily under the assumptions that $p \nmid x$, $p \nmid y$, $x \not\equiv y \pmod{p}$, and $p \geq 5$.

Observe that if the roots of unity $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$ are pairwise distinct, the expression above forces $x \equiv y \equiv 0 \pmod{p}$. Thus, at least two of these powers of ζ must coincide.

Noting that $1 \neq \zeta$ and $\zeta^{2r} \neq \zeta^{2r-1}$, the potential identifications reduce to three distinct cases, which we now analyse separately:

- **Case 1:** $\zeta^{2r} = 1$

  Substituting into the congruence, we obtain:

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

  By Lemma 3.14 $y \equiv 0 \pmod{p}$, contradicting our assumption.

- **Case 2:** $\zeta^{2r-1} = 1$, which is equivalent to $\zeta = \zeta^{2r}$

  Under this condition, the original expression simplifies to:

  $$(x - y) - \zeta(x - y) \equiv 0 \pmod{p},$$

  By Lemma 3.14, we must have $x \equiv y \pmod{p}$, again contradicting our choice of x and y (see Remark 3.10).

- **Case 3:** $\zeta = \zeta^{2r-1}$

  In this scenario, the congruence becomes:

  $$x - \zeta^2 x \equiv 0 \pmod{p},$$

  Finally, by Lemma 3.14, we deduce $x \equiv 0 \pmod{p}$. This is in contradiction with our standing hypothesis that $p \nmid x$.

Since each of the three possible identifications leads to a contradiction, we conclude that no such coincidence among the powers of ζ can occur. Therefore, the original congruence cannot hold under the assumptions made, and the result in Theorem 3.1 follows.

3.4. Regular Primes

As it turns out, there is quite a nice method to figure out if a prime p divides the class number of the field $\mathbb{Q}(\zeta_p)$. Although some of the machinery needed to prove this method is beyond the scope of the thesis, we will outline the claim and further justify some of the process in the next chapter. The information from this section is primarily sourced from [13] and [14]

Let K be a number field and $\mathcal{O}_K$ its ring of integers. The Dedekind zeta function

$$\zeta_K(s) = \sum_{\mathfrak{I} \subseteq \mathcal{O}_K} \frac{1}{\left(\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{I})\right)^s}$$

is defined for complex numbers $s \in \mathbb{C}$ with real part $\mathbb{R}(s) > 1$ by the series where $\mathfrak{I}$ runs over all ideals of $\mathcal{O}_K$. Naturally, when $K = \mathbb{Q}$, this is the Riemann zeta function.

Theorem 3.15 (Class number formula)**.** Let K be a number field with degree $[K : \mathbb{Q}] = m$. Have r denote the number of real embeddings and c denote half the number of complex embeddings, $m = r + 2c$. For K, we let R_K denote its regulator, h_K its class number, D_K its discriminant, and w_K the number of roots in K. Then for $s \in \mathbb{C}$ with real component greater than 1 we have

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^r \cdot (2\pi)^c \cdot R_K \cdot h_K}{w_K \cdot \sqrt{|D_K|}}.$$

Proof. The proof is out of the scope, but we refer the reader to [2]. □

We will define the regulator in the following chapter. But the point of this formula is that everything on the right hand side except for the regulator and class number are easy to compute.

Powerful gadgets and techniques from complex function theory are employed to evaluate the limit. We will briefly mention them in the next chapter.

Relevant to this thesis, when $K = \mathbb{Q}(\zeta_p)$, the following formula can be derived,

$$h_K = h^+ h^-.$$

This formula relies on the fact that h^+, the class number of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, divides h. The quotient class number h^- is just their ratio. In contrast to the class number formula containing transcendental quantities, there exists a formula for h^- which contains no such quantities. Thus divisor properties can be obtained. In the following chapter, we will prove some of the main arguments for the derivation of this formula, such as removing the hard-to-calculate regulator.

The study of regular primes is closely related to Bernoulli numbers.

Definition 3.16 (Bernoulli numbers)**.** Bernoulli numbers B_n are defined by

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$

They return a sequence of fairly irregular fractions, some small examples are:

$$\begin{array}{cccc} B_0 = 1, & B_1 = -\frac{1}{2}, & B_2 = \frac{1}{6}, & B_4 = -\frac{1}{30}, \\ B_6 = \frac{1}{42}, & B_8 = -\frac{1}{30}, & B_{10} = \frac{5}{66}, & B_{12} = -\frac{691}{2730}, \\ B_{14} = \frac{7}{6}, & B_{16} = -\frac{3617}{510}, & \dots & \end{array}$$

In fact for odd $k > 1$, $B_K = 0$. Analysis can show that h^- is divisible by p if p divides the numerator of any of the first $p - 3$ Bernoulli numbers [14].

For example, 691 divides h^- if $K = \mathbb{Q}(\zeta_{691})$.

Returning back to regular primes, one can also show that h^+ and p are coprime if h^- and p are coprime. Hence p is regular ($p \nmid h_K$) if and only if p and h^- are coprime [14].

The first few irregular primes are $37, 59, 67, 101$. It has been proven that there are infinitely many irregular primes [3], but only conjectured that there are infinitely many regular primes [6]. It is conjectured that $\approx 61\%$ of the primes are regular. Thanks to Hart [7], in 2016 the irregular primes up to two billion (2^{31}) have been calculated. See [14] for more details on regular primes and Bernoulli numbers.

4. Cyclotomic Fields with Class Number One

As seen in the last chapter, the study of cyclotomic fields in the context of FLT has led to deeper questions about their arithmetic structure.

In this chapter we use the class number formula to show that there are a finite number of cyclotomic fields with class number 1. The class number formula is of little use to us if we cannot evaluate its limit. Its limit is evaluated by a product of L-series functions. Although the proofs are beyond the scope for this thesis, we will first outline the general case of the arguments and then later explain how this relates to our cyclotomic fields. In order to explore the class number formula in more detail, we will guide the reader to the relevant resources. The general structure of the proofs have been primarily adapted from chapter 4 [14]

The **Dirichlet L-series** is formed for a Dirichlet character χ,

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

where $s \in \mathbb{C}$ is a complex number with real component greater than 1. Notice that when $\chi = 1$ (the principal character), this results in $\zeta(s)$ the Riemann zeta function.

Corollary 4.1. Let X be a group of Dirichlet characters, then we can associate a number field K to it. Meaning that $X \cong \mathrm{Gal}(K/\mathbb{Q})$ for some abelian field extension K (i.e. the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is abelian). Then $\chi : \mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{C}^{\times}$.

Proof. See chapter 3 of [14]. □

Theorem 4.2. Let X be a group of Dirichlet characters with the associated number field K. The Dedekind zeta function of K is denoted $\zeta_K(s)$. Then

$$\zeta_K(s) = \prod_{\chi \in X} L(s,\chi).$$

Proof. See Thrm. 4.3 [14]. □

The use of complex analysis on the Dedekind zeta function allows us to evaluate the residue of the simple pole at $s = 1$ and obtain:

$$\prod_{\chi \in X} L(1,\chi) = \frac{2^r \cdot (2\pi)^c \cdot R_K \cdot h_K}{w_K \cdot \sqrt{|D_K|}}.$$

As before: X is a group of Dirichlet characters with associated field K; K signature (r,c); R_K is the regulator of the field; h_K the class number; w_K the number of distinct roots of unity in K; and D_K the discriminant. The residue is not explicitly derived in [14]; for a more complete proof, see [2].

In order to relate the class number formula to cyclotomic fields, we define the maximal real subfield

Definition 4.3. Let K be a number field, we define the **maximal real subfield** to be the largest real subfield of K. Often denoted as K^+.

Proposition 4.4. Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic field and K^+ its maximal real subfield. Then

$$K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$$

Proof. First, observe that ζ_n is not real for $n > 2$, but the sum $\zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$ is real. Thus, $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subset \mathbb{R}$ is a real subfield of K.

Now consider an arbitrary element $x \in \mathbb{Q}(\zeta_n) \cap \mathbb{R}$. Then x can be written as a rational linear combination of powers of ζ_n:

$$x = \sum_{\substack{0<k<n \\ \gcd(n,k)=1}} a_k\zeta_n^k, \quad a_k \in \mathbb{Q},$$

where at least one a_k is non-zero. Since x is real, we have $\overline{x} = x$, and since complex conjugation sends $\zeta_n^k \mapsto \zeta_n^{-k}$, it follows that

$$\sum a_k\zeta_n^k = \sum a_k\zeta_n^{-k}.$$

Therefore,

$$\sum a_k(\zeta_n^k - \zeta_n^{-k}) = 0.$$

Each term $\zeta_n^k - \zeta_n^{-k}$ is purely imaginary (or zero), because:

$$\zeta_n^k - \zeta_n^{-k} = 2i\sin\left(\frac{2\pi k}{n}\right).$$

Therefore the coefficients of each imaginary part must cancel each other out. Moreover,

$$x = \frac{1}{2}\left(\sum a_k\zeta_n^k + \sum a_k\zeta_n^{-k}\right) = \sum a_k \cdot \frac{\zeta_n^k + \zeta_n^{-k}}{2}.$$

This implies that x is a linear combination of symmetric sums $\zeta_n^k + \zeta_n^{-k} = 2\cos(2\pi k/n)$, which all lie in $\mathbb{Q}(\zeta_n+\zeta_n^{-1})$. Consequently, any real element of $\mathbb{Q}(\zeta_n)$ lies in $\mathbb{Q}(\zeta_n+\zeta_n^{-1})$. □

Corollary 4.5. Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic field and K^+ its maximal real subfield. Then K is a quadratic field extension of K^+, $[K : K^+] = 2$.

Proof. Clearly K is a totally imaginary field and K^+ a totally real subfield with $K^+(\zeta_n) = K$. Observe that

$$x^2 - (\zeta_n + \zeta_n^{-1})x + 1$$

is a polynomial in $K^+[x]$ with a roots ζ_n and ζ_n^{-1}. The polynomial is then irreducible over K^+ and hence the minimal polynomial of ζ_n of degree 2. Hence $[K : K^+] = 2$. □

Moreover, as K is totally complex and K^+ is totally real, it follows that the K^+-embeddings of K are defined by complex conjugation.

4.1. Overview

Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic field and let h be its class number, let h^+ denote the class number of $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. As we will soon see, h^+ divides h. We can write $h = h^+h^-$, for some quotient class number h^-. By bounding and approximating h^-, we will ultimately show that h^- grows increasingly quickly. Hence, there are a bounded number of fields K with $h^- = 1$, and thus only finitely many fields with $h = 1$. Equivalently, there are a finite number of cyclotomic fields K whose ring of integers has unique factorisation (i.e., is a PID). To obtain a formula for h^-, we apply the class number formula on h and $h+$. To properly describe these formulas, we will elaborate on the group of Dirichlet characters associated with K and K^+, respectively.

Let X be the group of Dirichlet characters associated to the cyclotomic field $K = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity. Then we have

$$X = (\mathbb{Z}/n\mathbb{Z})^\times \cong \mathrm{Gal}(K/\mathbb{Q}).$$

The isomorphism associates each $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ to the automorphism $\sigma_a \in \mathrm{Gal}(K/\mathbb{Q})$ defined by

$$\sigma_a(\zeta_n) = \zeta_n^a.$$

Let $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ denote the maximal real subfield of K. This is the fixed field of the complex conjugation automorphism $\tau \in \mathrm{Gal}(K/\mathbb{Q})$, which acts by

$$\tau(\zeta_n) = \overline{\zeta_n} = \zeta_n^{-1}.$$

Hence, complex conjugation corresponds to the element $-1 \in (\mathbb{Z}/n\mathbb{Z})^\times$. Therefore,

$$\mathrm{Gal}(K/K^+) = \langle \sigma_{-1} \rangle \cong C_2.$$

Moreover, let $X^+ := \{\chi \in X : \chi(-1) = 1\}$. Then for each χ, we have

$$\ker(\chi) = \{a \in X : \chi(a) = 1\}.$$

Hence, by the association between the isomorphic groups, complex conjugation is in the kernel of each $\chi \in X^+$.

Thus the field associated to X^+ is K^+,

$$X^+ \cong \mathrm{Gal}(K^+/\mathbb{Q}) \cong \mathrm{Gal}(K/\mathbb{Q})/\,\mathrm{Gal}(K/K^+).$$

Equipped with the characters associated to each field, we can explicitly write out the class number formula for K and K^+.

Formula 4.6 (Class number formulas for h and h^+). If $K = \mathbb{Q}(\zeta_n)$ of signature (r, c), then $r = 0, c = \phi(n)/2$, and

$$\frac{(2\pi)^{\phi(n)/2}hR_K}{w_K\sqrt{|D_K|}} = \prod_{\substack{\chi\in X \\ \chi\neq 1}} L(1,\chi).$$

As K^+ is a totally real field extension, it follows that the signature of K^+ is $(\phi(n)/2, 0)$ and that ± 1 are its only roots of unity ($w_{K^+} = 2$).

$$\frac{2^{\phi(n)/2}h^+R_{K^+}}{2\sqrt{|D_{K^+}|}} = \prod_{\substack{\chi\in X \\ \chi \text{ even} \\ \chi\neq 1}} L(1,\chi),$$

These formulas are still in terms of their regulators. A nice formula in terms of h^- is then generated by evaluating the quotient of the regulators.

4.2. The Regulator

Intuitively, the regulator will measure the "volume" of the lattice formed by the units in a logarithmic space. A smaller regulator means that the "volume" created by the basis of units is small, and hence, the units are closer together, tightly packed or denser.

Let K be a number field with signature (r, c), then let $s = r + c - 1$. Recall from Dirichlet's Unit Theorem, there exist units $\varepsilon_1, \ldots, \varepsilon_s$ such that any unit ε can be uniquely expressed by $\varepsilon = \mu\varepsilon_1^{a_1}\cdots\varepsilon_s^{a_s}$ with μ being a root of unity of K and $a_i \in \mathbb{Z}$. We say that $\{\varepsilon_1, \ldots, \varepsilon_s\}$ is a basis for $\mathcal{O}_K^\times/W$, or the **unit-basis** of K. The regulator is calculated from the unit-basis.

Particularly in this section, the sake of notation, we let $\varepsilon^{\sigma_j} := \sigma_j(\varepsilon)$.

Lemma 4.7. Let L be a number field. We write the embeddings $\sigma : L \to \mathbb{C}$ as $\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \ldots, \sigma_{r+c}, \overline{\sigma}_{r+1}, \ldots, \overline{\sigma}_{r+c}$. Where σ_j $(1 \leq j \leq r)$ are real embeddings and $\sigma_j, \overline{\sigma}_j$ $(r + 1 \leq j \leq r + c)$ are pairs of complex conjugate embeddings. Finally we define the **embedding factor** $\delta_j = 1$ if σ_j is real and $\delta_j = 2$ if σ_j is complex. Each unit ε satisfies

$$\prod_{j=1}^{s+1} |\varepsilon^{\sigma_j}|^{\delta_j} = 1.$$

And hence under logarithms

$$\sum_{i=1}^{s+1} \delta_j \log|\varepsilon^{\sigma_j}| = 0.$$

Proof. The norm $N_{L/\mathbb{Q}}(\varepsilon)$ of a unit ε is ± 1. By definition, the norm is the product of all embeddings of ε:

$$N_{L/\mathbb{Q}}(\varepsilon) = \underbrace{\varepsilon^{\sigma_1}\cdots\varepsilon^{\sigma_r}}_{\text{real embeddings}} \underbrace{\varepsilon^{\sigma_{r+1}}\cdots\varepsilon^{\sigma_{r+c}}\,\varepsilon^{\overline{\sigma}_{r+1}}\cdots\varepsilon^{\overline{\sigma}_{r+c}}}_{\text{complex embeddings}}$$

$$= \prod_{1\le i\le r} \varepsilon^{\sigma_j} \cdot \prod_{r+1\le i\le r+c} \varepsilon^{\sigma_j} \cdot \varepsilon^{\bar{\sigma}_j}.$$

Taking absolute values, we get:

$$|N_{L/\mathbb{Q}}(\varepsilon)| = \prod_{1\le i\le r} |\varepsilon^{\sigma_j}| \cdot \prod_{r+1\le i\le r+c} |\varepsilon^{\sigma_j}|^2 = 1.$$

As required, there is an exponent of 1 whenever the embedding is real, and 2 when the embedding is complex. □

Definition 4.8. Suppose L is a number field with signature (r, c) and $s = r + c - 1$. Let $\{\varepsilon_1, \dots, \varepsilon_s\}$ be any set of independent units of L. We define the $s \times (s + 1)$ matrix

$$M := \left(\delta_j \log|\varepsilon_i^{\sigma_j}|\right)_{\substack{1\le i\le s\\ 1\le j\le s+1}} = \begin{pmatrix} \delta_1 \log|\varepsilon_1^{\sigma_1}| & \delta_2 \log|\varepsilon_1^{\sigma_2}| & \cdots & \delta_{s+1} \log|\varepsilon_1^{\sigma_{s+1}}| \\ \delta_1 \log|\varepsilon_2^{\sigma_1}| & \delta_2 \log|\varepsilon_2^{\sigma_2}| & \cdots & \delta_{s+1} \log|\varepsilon_2^{\sigma_{s+1}}| \\ \vdots & \vdots & \ddots & \vdots \\ \delta_1 \log|\varepsilon_s^{\sigma_1}| & \delta_2 \log|\varepsilon_s^{\sigma_2}| & \cdots & \delta_{s+1} \log|\varepsilon_s^{\sigma_{s+1}}| \end{pmatrix}.$$

Lemma 4.9. Let $M^{(k)}$ denote the $s \times s$ submatrix obtained by removing the k-th column of M, formally,

$$M^{(k)} := \left(\delta_j \log|\varepsilon_i^{\sigma_j}|\right)_{\substack{1\le i\le s\\ 1\le j\le s+1\\ k\neq j}}.$$

Then the determinant of $M^{(k)} = (-1)^m M^{(l)}$ for $l \neq k$ for some integer m. Moreover, the absolute value of the determinant of the submatrix formed by removing one column does not depend on the choice of column deleted.

Proof. M has the property that the sum of the elements in any row is 0, $\sum_{i=1}^{s+1} \delta_i \log|\varepsilon_j^{\sigma_i}| = 0$, as shown in Lemma 4.7. Hence the columns of this matrix are linearly dependent by,

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \delta_1 \log|\varepsilon_1^{\sigma_1}| \\ \delta_1 \log|\varepsilon_2^{\sigma_1}| \\ \vdots \\ \delta_1 \log|\varepsilon_s^{\sigma_1}| \end{pmatrix} + \begin{pmatrix} \delta_2 \log|\varepsilon_1^{\sigma_2}| \\ \delta_2 \log|\varepsilon_2^{\sigma_2}| \\ \vdots \\ \delta_2 \log|\varepsilon_s^{\sigma_2}| \end{pmatrix} + \cdots + \begin{pmatrix} \delta_{s+1} \log|\varepsilon_1^{\sigma_{s+1}}| \\ \delta_{s+1} \log|\varepsilon_2^{\sigma_{s+1}}| \\ \vdots \\ \delta_{s+1} \log|\varepsilon_s^{\sigma_{s+1}}| \end{pmatrix}.$$

We label the k^{th} column as Col_k with

$$\mathrm{Col}_k = -\sum_{\substack{j=1\\ i\neq k}}^{s+1} \mathrm{Col}_j.$$

Without loss of generality, we assume $k < l$. Now consider the matrices $M^{(k)}$ and $M^{(l)}$, each with a respective set of ordered columns

$$C_k = \{\mathrm{Col}_1, \cdots, \mathrm{Col}_{k-1}, \mathrm{Col}_{k+1}, \cdots, \mathrm{Col}_l \cdots, \mathrm{Col}_{s+1}\}$$

and

$$C_l = \{\mathrm{Col}_1, \cdots, \mathrm{Col}_k \cdots, \mathrm{Col}_{l-1}, \mathrm{Col}_{l+1}, \cdots, \mathrm{Col}_{s+1}\}.$$

But clearly we can now represent the elements both sets in terms of the same column vectors,

$$C_l = \{\mathrm{Col}_1, \cdots, -\sum_{\substack{j=1\\ i\neq k}}^{s+1} \mathrm{Col}_j \cdots, \mathrm{Col}_{l-1}, \mathrm{Col}_{l+1}, \cdots, \mathrm{Col}_{s+1}\}$$

We will now apply elementary column operations to justify the sign change in the determinant associated to the matrices. In particular, by adding multiples of one column to another, it is clear that the determinant of matrix associated to C_l would have the same determinant as the matrix associated to the ordered set

$$\{\mathrm{Col}_1, \cdots, \mathrm{Col}_{k-1}, -\mathrm{Col}_l, \mathrm{Col}_{k+1} \cdots, \mathrm{Col}_{l-1}, \mathrm{Col}_{l+1}, \cdots, \mathrm{Col}_{s+1}\}$$

Recall that this ordered set has only s elements and that $-\mathrm{Col}_l$ is now in position k. Hence, $l-1-k$ column swaps must be made to this ordered set to slot $-\mathrm{Col}_l$ in between Col_{l-1} and Col_{l+1}. Finally, we multiply $-\mathrm{Col}_l$ by -1. Thus, we have applied elementary column operations to convert the ordered set C_l into C_k. Altogether, the effect this has on their associated matrices is just a factor of $(-1)^{l-k}$. Hence,

$$\det(M^{(k)}) = (-1)^{l-k} \det(M^{(l)}).$$

And clearly,

$$|\det(M^{(k)})| = |\det(M^{(l)})|.$$

□

Definition 4.10. Let L be a number field and $\{\varepsilon_1, \dots, \varepsilon_s\}$ is any set of multiplicatively independent units of L.

$$\begin{aligned} R_L(\varepsilon_1, \dots, \varepsilon_s) &:= \left| \det \begin{pmatrix} \delta_1 \log|\varepsilon_1^{\sigma_1}| & \delta_2 \log|\varepsilon_1^{\sigma_2}| & \cdots & \delta_s \log|\varepsilon_1^{\sigma_s}| \\ \delta_1 \log|\varepsilon_2^{\sigma_1}| & \delta_2 \log|\varepsilon_2^{\sigma_2}| & \cdots & \delta_s \log|\varepsilon_2^{\sigma_s}| \\ \vdots & \vdots & \ddots & \vdots \\ \delta_1 \log|\varepsilon_s^{\sigma_1}| & \delta_2 \log|\varepsilon_s^{\sigma_2}| & \cdots & \delta_s \log|\varepsilon_s^{\sigma_s}| \end{pmatrix} \right| \\ &= \left| \det \left(\delta_j \log|\varepsilon_i^{\sigma_j}| \right)_{1\leq i,j\leq s} \right|. \end{aligned}$$

If $\{\varepsilon_1, \dots, \varepsilon_s\}$ is a basis for $\mathcal{O}_L^\times/W$, the group of units of L modulo roots of unity, then $R_L(\varepsilon_1, \dots, \varepsilon_s) = R_L$ is called the **regulator** of L.

The fact that we took the absolute value of the determinant makes R_L independent of the choice and ordering of the embeddings σ. We prove that the regulator is also independent on the choice of basis in Lemma 4.16 (and more).

Remark 4.11. Note that not all sets of s independent units form a basis. As for a set of basis elements B, the elements in the set $\{b^2 : b \in B\}$ are clearly linearly independent but may not span the unit group spanned by B. See the example below. $\triangleleft$

Example 4.12. Let $L = \mathbb{Q}(\sqrt{5})$. L has 2 real embeddings, hence the set of units is spanned by just one unit. The ring of integers

$$\mathcal{O}_L = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] = \left\{\frac{a+b\sqrt{5}}{2} \;:\; a \equiv b \pmod 2,\ a, b \in \mathbb{Z}\right\}.$$

Let $\varepsilon = \frac{1+\sqrt{5}}{2} \approx 1.618$, and by taking the norm, $N(\varepsilon) = \frac{1+\sqrt{5}}{2} \cdot \frac{1-\sqrt{5}}{2} = -1$, we showed that ε is in fact a unit. Additionally, we can express an arbitrary unit u as an element of $\mathcal{O}_L$, $u = \frac{x+y\sqrt{5}}{2}$. Where $N(u) = x^2 - 5y^2 = \pm 4$. Giving a form of Pell's equation with fundamental solution (1,1) [10]. Thus every unit $u = \pm\varepsilon^k$ for some integer $k \in \mathbb{Z}$. Moreover, $\{\varepsilon^2\}$ is clearly a set of independent units of size 1 which doesn't span $\mathcal{O}_L^\times/\{\pm 1\}$.

One shows by calculation that $R_L = |\log(\varepsilon)| \approx 0.481$, for the natural logarithm. $\triangleleft$

4.3. Removing the Regulator

As per Formula 4.6, by dividing the formula for h by the formula for h^+ we encounter R_K/R_{K^+}. In this section we will provide a nice relation for this fraction.

We do this in 2 main steps:

1. First we will express the $R_K(\varepsilon_1^+, \dots, \varepsilon_s^+)$ as a power of 2 times R_{K^+}, for some the set $\{\varepsilon_1^+, \dots, \varepsilon_s^+\}$ of K^+'s unit-basis.
2. Then we show that R_K is a multiple of $R_K(\varepsilon_1^+, \dots, \varepsilon_s^+)$ by one or 2.

Refer to Proposition 4.19 for motivation of the end result. Intuitively, we can see that the power of 2 in Proposition 4.19 comes from factoring $2 = \delta_j$ out for each complex embedding. But we will formally calculate this.

The next few results in this section hold for a class of number fields called CM-fields.

Definition 4.13 (CM-field)**.** A number field is called **totally real** if all of its field embeddings are real. Similarly, a number field is called **totally imaginary** if all of its field embeddings are complex, see Definition 2.4. Then a **CM-field** is a totally imaginary field, which is a quadratic extension of a totally real subfield.

One of the motivating reasons for defining a CM-field K of degree n, is that the signature $(r, c) = (0, n/2)$. Then the signature for K^+ is $(n/2, 0)$.

We previously showed that cyclotomic fields are CM-fields, but clearly there are other kinds.

Example 4.14. $K = \mathbb{Q}(\sqrt{2}, i)$ is a CM-field extending the totally real subfield $K^+ = \mathbb{Q}(\sqrt{2})$. Hence K has signature $(0, 1)$ and K^+ has signature $(2, 0)$. ◁

See Example 2.5 for an example of something that isn't a CM-field.

Step 1

Now we begin step 1 of removing the regulator.

Lemma 4.15. Now let K be a CM-field and K^+ its maximal real subfield as before. Let $\varepsilon_1^+, \ldots, \varepsilon_s^+ \in \mathcal{O}_{K^+}$ be multiplicatively independent units whose image modulo W generate $\mathcal{O}_{K^+}^\times$. Then

$$R_K(\varepsilon_1^+, \ldots, \varepsilon_s^+) = 2^s R_{K^+}(\varepsilon_1^+, \ldots, \varepsilon_s^+) = 2^s R_{K^+}.$$

Proof. Suppose K has degree $d = [K : \mathbb{Q}]$ and hence signature $(0, d/2)$, let $s = d/2 - 1$. With only complex embeddings to consider, let $\sigma_i, \bar{\sigma}_i : K \to \mathbb{C}$ be the pairs of complex embeddings for $1 \leq i \leq s + 1$. Furthermore, we have embedding factor $\delta_i = 2$ for all complex embeddings $\sigma_1, \cdots \sigma_{s+1}$. Hence,

$$R_K(\varepsilon_1^+, \ldots, \varepsilon_s^+) = \left| \det \begin{pmatrix} \delta_1 \log |(\varepsilon_1^+)^{\sigma_1}| & \delta_2 \log |(\varepsilon_1^+)^{\sigma_2}| & \cdots & \delta_s \log |(\varepsilon_1^+)^{\sigma_s}| \\ \delta_1 \log |(\varepsilon_2^+)^{\sigma_1}| & \delta_2 \log |(\varepsilon_2^+)^{\sigma_2}| & \cdots & \delta_s \log |(\varepsilon_2^+)^{\sigma_s}| \\ \vdots & \vdots & \ddots & \vdots \\ \delta_1 \log |(\varepsilon_s^+)^{\sigma_1}| & \delta_2 \log |(\varepsilon_s^+)^{\sigma_2}| & \cdots & \delta_s \log |(\varepsilon_s^+)^{\sigma_s}| \end{pmatrix} \right|$$

$$= \left| \det \left(2 \cdot \begin{pmatrix} \log |(\varepsilon_1^+)^{\sigma_1}| & \log |(\varepsilon_1^+)^{\sigma_2}| & \cdots & \log |(\varepsilon_1^+)^{\sigma_s}| \\ \log |(\varepsilon_2^+)^{\sigma_1}| & \log |(\varepsilon_2^+)^{\sigma_2}| & \cdots & \log |(\varepsilon_2^+)^{\sigma_s}| \\ \vdots & \vdots & \ddots & \vdots \\ \log |(\varepsilon_s^+)^{\sigma_1}| & \log |(\varepsilon_s^+)^{\sigma_2}| & \cdots & \log |(\varepsilon_s^+)^{\sigma_s}| \end{pmatrix} \right) \right|$$

Observing that all of K^+'s field embeddings $\tau_i = \sigma_i|_{K^+}$ by Lemma 2.36,

$$\begin{aligned} R_K(\varepsilon_1^+, \ldots, \varepsilon_s^+) &= 2^s \left| \det \begin{pmatrix} \log |(\varepsilon_1^+)^{\tau_1}| & \log |(\varepsilon_1^+)^{\tau_2}| & \cdots & \log |(\varepsilon_1^+)^{\tau_s}| \\ \log |(\varepsilon_2^+)^{\tau_1}| & \log |(\varepsilon_2^+)^{\tau_2}| & \cdots & \log |(\varepsilon_2^+)^{\tau_s}| \\ \vdots & \vdots & \ddots & \vdots \\ \log |(\varepsilon_s^+)^{\tau_1}| & \log |(\varepsilon_s^+)^{\tau_2}| & \cdots & \log |(\varepsilon_s^+)^{\tau_s}| \end{pmatrix} \right| \\ &= 2^s R_{K^+}. \end{aligned}$$

Because $\delta_i = 1$ for each embedding of K^+. □

We note that if K is a CM-field of degree d, with signature $(0, d/2)$, and group of roots of unity W, then K^+ has signature $(d/2, 0)$. By Dirichlet's unit theorem we know that $\mathcal{O}_K^\times / W$ and $\mathcal{O}_{K^+}^\times / \{\pm 1\}$ share the same rank.

Step 2

In fact, we will be proving a more general case for step 2. Intuitively, we will prove that for subgroups $A \subseteq B$ of the units of a field, the difference in "density" for the units in each group is equal to their index $[B : A]$.

Lemma 4.16. Let K be a number field and let $\varepsilon_1, \dots, \varepsilon_r \in \mathcal{O}_K^\times$ be multiplicatively independent units which generate a subgroup A of $\mathcal{O}_K^\times/W$ the units of K modulo the roots of unity. Let $\eta_1, \dots, \eta_r \in \mathcal{O}_K^\times$ generate a subgroup B of $\mathcal{O}_K^\times$. If $A \subseteq B$ of finite index. then

$$[B : A] = \frac{R_K(\varepsilon_1, \dots, \varepsilon_r)}{R_K(\eta_1, \dots, \eta_r)}.$$

Proof. Since $A \subseteq B$, any element of $\varepsilon_i \in A$ can be multiplicatively spanned by B's basis modulo some root of unity. Hence

$$\varepsilon_i = \left(\prod_{l=1}^{r} \eta_l^{c_{i,l}}\right) \zeta_i, \quad c_{i,l} \in \mathbb{Z},\ \zeta_i \in W.$$

Applying logarithmic embeddings, the roots of unity vanish:

$$\log|\sigma_j(\varepsilon_i)| = \sum_{l=1}^{r} c_{i,l} \log|\sigma_j(\eta_l)|,$$

and so including the embedding factors $\delta_j = 1$ (real embeddings) or 2 (complex embeddings), we obtain:

$$\delta_j \log|\sigma_j(\varepsilon_i)| = \sum_{l=1}^{r} c_{i,l}\delta_j \log|\sigma_j(\eta_l)|.$$

This suggests a matrix formulation. Define the injective group homomorphism:

$$\lambda : \mathcal{O}_K^\times/W \to \mathbb{R}^r, \quad \alpha \mapsto \left(\delta_1 \log|\sigma_1(\alpha)|, \dots, \delta_r \log|\sigma_r(\alpha)|\right).$$

Then for each i,

$$\lambda(\varepsilon_i) = \sum_{l=1}^{r} c_{i,l}\lambda(\eta_l).$$

Let $C = (c_{i,l}) \in \mathrm{Mat}_{r\times r}(\mathbb{Z})$, and define:

$$\Lambda_A = \begin{pmatrix} \lambda(\varepsilon_1) \\ \lambda(\varepsilon_2) \\ \vdots \\ \lambda(\varepsilon_r) \end{pmatrix}, \qquad \Lambda_B = \begin{pmatrix} \lambda(\eta_1) \\ \lambda(\eta_2) \\ \vdots \\ \lambda(\eta_r) \end{pmatrix}.$$

Then the relation becomes:

$$\Lambda_A = C \cdot \Lambda_B.$$

Writing this out explicitly:

$$C \cdot \begin{pmatrix} \lambda(\eta_1) \\ \lambda(\eta_2) \\ \vdots \\ \lambda(\eta_r) \end{pmatrix} = \begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,r} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,r} \\ \vdots & \vdots & \ddots & \vdots \\ c_{r,1} & c_{r,2} & \cdots & c_{r,r} \end{pmatrix} \cdot \begin{pmatrix} \delta_1 \log|\sigma_1(\eta_1)| & \delta_2 \log|\sigma_2(\eta_1)| & \cdots & \delta_r \log|\sigma_r(\eta_1)| \\ \delta_1 \log|\sigma_1(\eta_2)| & \delta_2 \log|\sigma_2(\eta_2)| & \cdots & \delta_r \log|\sigma_r(\eta_2)| \\ \vdots & \vdots & \ddots & \vdots \\ \delta_1 \log|\sigma_1(\eta_r)| & \delta_2 \log|\sigma_2(\eta_r)| & \cdots & \delta_r \log|\sigma_r(\eta_r)| \end{pmatrix}$$

$$= \begin{pmatrix} \delta_1 \log|\sigma_1(\varepsilon_1)| & \delta_2 \log|\sigma_2(\varepsilon_1)| & \cdots & \delta_r \log|\sigma_r(\varepsilon_1)| \\ \delta_1 \log|\sigma_1(\varepsilon_2)| & \delta_2 \log|\sigma_2(\varepsilon_2)| & \cdots & \delta_r \log|\sigma_r(\varepsilon_2)| \\ \vdots & \vdots & \ddots & \vdots \\ \delta_1 \log|\sigma_1(\varepsilon_r)| & \delta_2 \log|\sigma_2(\varepsilon_r)| & \cdots & \delta_r \log|\sigma_r(\varepsilon_r)| \end{pmatrix} = \Lambda_A.$$

Now, taking absolute values of determinants gives:

$$R_K(\varepsilon_1, \dots, \varepsilon_r) = |\det(C)| \cdot R_K(\eta_1, \dots, \eta_r).$$

To interpret $\det(C)$, observe that the rows of Λ_A and Λ_B form $\mathbb{Z}$-bases of the lattices $\lambda(A)$ and $\lambda(B)$ in $\mathbb{R}^r$, respectively. Since C is the change-of-basis matrix from $\lambda(B)$ to $\lambda(A)$, we have:

$$[\lambda(B) : \lambda(A)] = |\det(C)|.$$

Because λ is an injective group homomorphism, it preserves finite indices of subgroups:

$$[B : A] = [\lambda(B) : \lambda(A)] = |\det(C)|.$$

Putting this together,

$$[B : A] = \frac{R_K(\varepsilon_1, \dots, \varepsilon_r)}{R_K(\eta_1, \dots, \eta_r)}.$$

□

We briefly motivate our findings by the following remark. For the sake of notation:

- $E = \mathcal{O}_K^\times$
- $E^+ = \mathcal{O}_{K^+}^\times$

Remark 4.17. Let K be a CM-field. By Lemma 4.16 and Lemma 4.15,

$$R_K \cdot [E : WE^+] = R_K(\varepsilon_1^+, \dots, \varepsilon_s^+) = 2^s R_{K^+}.$$

◁

Clearly, all we need to do is evaluate the index $[E : WE^+]$.

Theorem 4.18. Let E be the group of units of the CM-field K, then let E^+ be the group of units for K^+. Finally, we have W denote the group of roots of unity in K. Then

$$Q := [E : WE^+] = 1 \text{ or } 2.$$

Proof. We will analyse the structure of the unit group E of a CM-field K using a homomorphism into the roots of unity. Define the map

$$\phi : E \to W$$

by

$$\phi(\varepsilon) = \varepsilon/\bar{\varepsilon},$$

where $\bar{\varepsilon}$ is the complex conjugate of ε. Since K is a CM-field, complex conjugation is an automorphism, so $\bar{\varepsilon} \in E$. It follows that for any embedding $\sigma : K \to \mathbb{C}$, $|\sigma(\frac{\varepsilon}{\bar{\varepsilon}})| = |\sigma(\phi(\varepsilon))| = 1$. Hence by Lemma 3.12, $\varepsilon/\bar{\varepsilon}$ is a root of unity for all units. Clearly

$$\phi(E) \subseteq W.$$

Now we induce the map

$$\psi : E \to W/W^2.$$

by

$$\psi(\varepsilon) = \phi(\varepsilon) \mod W^2.$$

Where $W^2 = \{w^2 | w \in W\}$. Note that ϕ is a group homomorphism and then so is ψ.

Now we will now show that the kernel of ψ is WE^+.

$$\ker(\psi) = \{\varepsilon | \phi(\varepsilon) \in W^2\}.$$

For arbitrary $\zeta \in W$ and $\varepsilon_1 \in E^+$, let $\varepsilon = \zeta\varepsilon_1$, then $\phi(\varepsilon) = \zeta^2 \in W^2$. So $WE^+ \subseteq \ker(\psi)$.

Now take an arbitrary element ε of the kernel, with

$$\phi(\varepsilon) = \frac{\varepsilon}{\bar{\varepsilon}} = \zeta^2 \in W\cdot$$

Then $\bar{\varepsilon}\zeta = \zeta^{-1}\varepsilon$. In fact this unit is invariant under complex conjugation, $\overline{(\bar{\varepsilon}\zeta)} = \bar{\varepsilon}\zeta$. Hence we may consider it as an element of E^+ for some $\varepsilon_1 = \zeta^{-1}\varepsilon \in E^+$. It follows that

$$\varepsilon = \zeta\varepsilon_1 \in WE^+$$

Implying $\ker(\psi) \subseteq WE^+$. Thus, $\ker(\psi) = WE^+$.

By the fundamental theorem on homomorphisms,

$$E/ker(\psi) = E/WE^+ \cong im(\psi) \subseteq W/W^2.$$

With $|E/WE^+| \leq |W/W^2|$, but by *Lemma* 2.39, the order of W/W^2 is 2. Consequently. $|E/WE^+| = [E : WE^+] \in \{1, 2\}$. □

Proposition 4.19. Let K be a CM-field and K^+ its maximal real subfield. Then

$$\frac{R_K}{R_{K^+}} = \frac{1}{Q}2^s, \quad \text{where } s = \frac{1}{2}\deg(K/\mathbb{Q}) - 1.$$

Proof. By Theorem 4.18 and Remark 4.17. □

4.4. Formula for h^-

In order to derive our formula for h^-, we will apply what we have learnt in the previous section to cyclotomic fields and categorise Q accordingly.

Remark 4.20. Refer back to the map $\phi(\varepsilon) = \varepsilon/\bar{\varepsilon}$ defined in Theorem 4.18. Let $K = \mathbb{Q}(\zeta_n)$ where E is the unit group of K and let W be the roots of unity in K. ϕ is a group homomorphism with $\phi(\zeta_n) = \zeta_n^2 \in W^2$. Hence

$$W^2 \subseteq \phi(E) \subseteq W.$$

Moreover, when $\phi(E) = W$, then $\psi(E) = W/W^2$ and $Q = 2$. But if $\phi(E) = W^2$, then Q = 1. ◁

Corollary 4.21. Let $K = \mathbb{Q}(\zeta_n)$. Then $Q = 1$ if $n = p^m$ is a prime power and $Q = 2$ if n is not a prime power.

Proof. Recall $\phi(\varepsilon) = \varepsilon/\bar{\varepsilon}$ as defined in Theorem 4.18. And let E be the unit group of K. By Remark 4.20,

$$W^2 \subseteq \phi(E) \subseteq W.$$

So to conclude the value of Q, we only need to show which of the reverse inclusions hold.

We will be considering the different cases of n.

1. When p is an odd prime and $n = p^m$:

We recall Lemma 3.13. Any unit $\varepsilon \in E$ can be expressed as $\varepsilon = \zeta_{p^m}^r q$, for some real q. Hence

$$\phi(\varepsilon) = \frac{\zeta_{p^m}^r q}{\zeta_{p^m}^{-r} q} = \zeta_{p^m}^{2r}.$$

It is now clear that $\phi(E) \subseteq W^2$. Hence $W^2 = \phi(E)$ as required, and Q = 1.

2. When $p = 2$ and $n = 2^m$:

Our argument must now be different because $(1 - \zeta_2)$ is not prime. Lemma 3.13 doesn't hold.

Suppose ε is a unit of $\mathbb{Q}(\zeta_{2^m})$ such that $\varepsilon/\bar{\varepsilon} \notin W^2$. By Lemma 3.12, $\varepsilon/\bar{\varepsilon}$ is a root of unity and denote $\zeta' = \varepsilon/\bar{\varepsilon}$. Since ζ' is not a square, its order doesn't divide 2^{m-1} and so ζ' must be primitive of order 2^m.

First we recall that $\mathrm{Gal}(K/\mathbb{Q}(i)) \subseteq \mathrm{Gal}(K/\mathbb{Q})$ since $\mathbb{Q}(i)$ is an intermediary field between $\mathbb{Q}$ and K. Also recall that the automorphisms are described by $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q}), \sigma_i(\zeta) = \zeta^i$. Hence, the automorphisms $\sigma_b \in \mathrm{Gal}(K/\mathbb{Q}(i))$ must fix $\mathbb{Q}(i)$ and are defined by

$\sigma_b(\zeta) = \zeta^b$ where $b \equiv 1 \pmod 4$. Now, let N denote the relative algebraic norm from $\mathbb{Q}(\zeta_{2^m})$ to $\mathbb{Q}(\zeta_{2^4})$, $N = N_{\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}(i)}$. Then for any root of unity ζ,

$$N(\zeta) = \prod_{\sigma_b \in \mathrm{Gal}(K/\mathbb{Q}(i))} \sigma_b(\zeta) = \prod_{\substack{0<b<2^m \\ b\equiv 1 \pmod 4}} (\zeta)^b.$$

Hence $N(\zeta) = \zeta^a$ for some a. We derive a below

$$\begin{aligned} a = \sum_{\substack{0<b<2^m \\ b\equiv 1 \pmod 4}} b = \sum_{j=0}^{2^{m-2}-1} (1+4j) &= 2^{m-2} \cdot 1 + 4 \cdot \frac{2^{m-2}(2^{m-2}-1)}{2} \\ &= 2^{m-2} + 2^{m-1}(2^{m-2}-1) \\ &\equiv 2^{m-2} \pmod{2^{m-1}} \end{aligned}$$

Now, with our guarantee that ζ' is a primitive 2^mth root of unity,

$$\begin{aligned} N(\zeta') = (\zeta')^a &= (\zeta')^{2^{m-2}} \cdot ((\zeta')^{2^{m-1}})^k \\ &= (\zeta')^{2^{m-2}} \cdot (-1)^k \\ &= \pm i \end{aligned}$$

By Theorem 2.10, the norm preserves units and we have

$$N(\zeta') = \frac{N(\varepsilon)}{N(\bar{\varepsilon})} = \frac{N(\varepsilon)}{\overline{N(\varepsilon)}} = \pm i.$$

But as ε is itself a unit, $N(\varepsilon) \in \mathcal{O}^\times_{\mathbb{Q}(i)}$. But $\mathcal{O}^\times_{\mathbb{Q}(i)} = \{\pm 1, \pm i\}$, in either case $N(\varepsilon)/\overline{N(\varepsilon)} = \pm 1$. Hence we contradict our assumption and have $\varepsilon/\bar{\varepsilon} \in W^2$ Hence $W^2 = \phi(E)$. $Q = 1$.

3. When n is not a prime power:

By Proposition 2.33, $1 - \zeta_n$ is a unit. Hence

$$\frac{(1-\zeta_n)}{\overline{(1-\zeta_n)}} = \frac{(1-\zeta_n)\zeta_n}{(1-\bar{\zeta}_n)\zeta_n} = \frac{(1-\zeta_n)\zeta_n}{-(1-\zeta_n)} = -\zeta_n.$$

To conclude, we now show that $\zeta_n^2, -\zeta_n \in \phi(E)$ generate W:
If n is odd, then

$$\begin{aligned} (-\zeta_n)^n &= (-1)^n \cdot \zeta_n^n = -1, \\ (-\zeta_n)^{n+1} &= \zeta_n. \end{aligned}$$

It follows that any element of W can be expressed by just powers of $-\zeta_n$,

$$W = <\zeta_n, -1> .$$

If n is even then n is a multiple of 4 (by Convention 2.28). Say $n = 4 \cdot m$, then

$$(\zeta_n^2)^m = \zeta_{4m}^{2m} = -1.$$

And again we have

$$W = \langle \zeta_n, -1 \rangle \subseteq \langle -\zeta_n, \zeta_n^2 \rangle.$$

In all cases for n not a prime power, we have $W \subseteq \phi(E)$, and so $Q = 2$. □

Theorem 4.22. *Let C be the ideal class group of $K = \mathbb{Q}(\zeta_n)$ and C^+ the ideal class group of the maximal real subfield $K^+ = \mathbb{Q}(\zeta_n)^+$. Then the natural map $C^+ \to C$ is an injection. Hence $h^+|h$.*

Proof. The natural map φ is defined as follows,

$$\begin{aligned} \varphi : \mathrm{Cl}(K^+) &\longrightarrow \mathrm{Cl}(K) \\ [\mathfrak{J}] &\longrightarrow [\mathfrak{J}\mathcal{O}_K], \end{aligned}$$

for $\mathfrak{J}$ an ideal of $\mathcal{O}_{K^+}$. Now suppose I is an ideal of $\mathcal{O}_{K^+}$ and that this ideal is principal when lifted to $\mathcal{O}_K$. We aim to show I was principle to begin with, as then the kernel of this map is trivial.

Now suppose $I = (\alpha)$ as a principal ideal of $\mathcal{O}_K$, so $\alpha \in \mathcal{O}_K$ may be complex. But I was already invariant under complex conjugation as an ideal of $\mathcal{O}_{K^+}$. It follows that

$$\frac{\bar{I}}{I} = (1) = \frac{(\bar{\alpha})}{(\alpha)},$$

where

$$\bar{I} := \{\,\bar{x} \mid x \in I\,\}.$$

Hence, $\bar{\alpha}/\alpha$ is a unit with all of its conjugates having absolute value 1. By Lemma 3.12 $\bar{\alpha}/\alpha$ is a root of unity.

First, we consider when n is not a prime power, hence by Corollary 4.21 and Remark 4.20, $Q = 2$ with $\phi(E) = W$, where ϕ is pulled from before. We now use that any root of unity is the image of some unit $\varepsilon \in E$. Clearly, $\phi(\varepsilon) = \varepsilon/\bar{\varepsilon} = \bar{\alpha}/\alpha$. Moreover, $\varepsilon\alpha = \overline{\alpha\varepsilon} \in \mathbb{Q}(\zeta_n)^+$ is real. Hence

$$(\alpha\varepsilon) = (\alpha) = I \quad \text{, as ideals of } \mathcal{O}_K.$$

But as $\varepsilon\alpha$ is invariant under complex conjugation, it must exist as an ideal of the maximal real subfield

$$(\varepsilon\alpha) = (\overline{\varepsilon\alpha}) \quad \text{, as ideals of } \mathcal{O}_{K^+}.$$

By the unique factorisation of ideals, $I = (\varepsilon\alpha)$ as an ideal of $\mathcal{O}_{K^+}$. Hence I was originally principal.

Secondly, we now consider when $n = p^m$ is a prime power. Let $\pi = \zeta_{p^m} - 1$, by Lemma 3.3, π is totally ramified and the prime ideal that lies above (p). We take the product of π and its conjugate to see that

$$\pi\bar{\pi} = (\zeta_{p^m} - 1)(\zeta_{p^m}^{-1} - 1) = -\zeta_{p^m}^{-1}(\zeta_{p^m} - 1)^2 = -\zeta_{p^m}^{-1}\pi^2,$$

where $-\zeta_{p^m}^{-1}$ is a unit in $\mathcal{O}_{K^+}^{\times}$. But also label

$$\mathfrak{P} := N_{K/K^+}(\pi) = \pi\bar{\pi} = (\zeta_{p^m} - 1)(\zeta_{p^m}^{-1} - 1) = 2 - \zeta_{p^m}^{-1} - \zeta_{p^m} \in \mathbb{Q}(\zeta_{p^m})^+.$$

Recall that $[K : K^+] = 2$ and $[K^+ : \mathbb{Q}] = \phi(n)/2$. We also have

$$\mathfrak{P}^{\frac{\phi(n)}{2}} = \pi^{\phi(n)} = (p)$$

as ideals in $\mathcal{O}_K$. Hence $\mathfrak{P}^{\frac{\phi(n)}{2}} = (p)$ as ideals of O_{K^+}, so it is totally ramified, and $\mathfrak{P}$ must be prime by Proposition 2.20. In other words, if $\mathfrak{P}$ were not prime, then (p) would factor into over $\phi(n)/2$ prime ideals in O_{K^+}. This is clearly not the case and one notes the prime ideal $\mathfrak{P}$ lies above π.

Let v_π denote the valuation of the ideal π on ideals from $\mathcal{O}_K$, as in Definition 3.4. Then

$$v_\pi(\mathfrak{P}) = v_\pi(\pi^2) = 2.$$

It follows that taking the π-adic valuation on elements of $\mathbb{Q}(\zeta_{p^m})^+$ gives an even valuation. Now observe that

$$\frac{\pi}{\bar{\pi}} = \frac{(\zeta_{p^m} - 1)}{(\zeta_{p^m}^{-1} - 1)} = \frac{(\zeta_{p^m} - 1)}{-\zeta_{p^m}^{-1}(\zeta_{p^m} - 1)} = -\zeta_{p^m}.$$

All roots of unity in K are of the form $\pm\zeta_{p^m}^k$, see Lemma 2.38.

If $p = 2$ then

$$-\zeta_{2^m} = \zeta_{2^m}^{2^{m-1}+1}$$

clearly generates the roots of unity in K, $(2^m, 2^{m-1} + 1) = 1$.

If p is odd then $\mathbb{Q}(\zeta_{p^m}) = \mathbb{Q}(\zeta_{2p^m})$ with

$$-\zeta_{p^m} = (-1)(\zeta_{p^m}) = \zeta_{2p^m}^{p^m}\zeta_{2p^m}^2 = \zeta_{2p^m}^{p^m+2}$$

Since $(p^m + 2, 2p^m) = 1$, $-\zeta_{p^m}$ is a primitive $2p^m$th root of unity and generates the roots of unity in $\mathbb{Q}(\zeta_{p^m})$.

It follows that for some exponent d,

$$\overline{\alpha}/\alpha = (\pi/\overline{\pi})^d.$$

Much like before, $\alpha\pi^d = \overline{\alpha\pi}^d \in \mathbb{Q}(\zeta_{p^m})^+$. Then we take the following even valuation,

$$v_\pi(\alpha\pi^d) = v_\pi(\alpha) + d = v_\pi(I) + d.$$

Since I and $\alpha\pi^d$ are real, then $v_\pi(\alpha)$ and d are also even. Meaning, $\overline{\alpha}/\alpha = (-\zeta_{p^m})^d \in W^2$. In particular, for some root of unity ζ',

$$\frac{\overline{\alpha}}{\alpha} = (\zeta')^2 = \frac{\zeta'}{\overline{\zeta'}}.$$

It easily follows that $\alpha\zeta' = \overline{\alpha\zeta'}$ is real with $I = (\alpha\zeta')$ as an ideal of $\mathcal{O}_K$. But the invariance under complex conjugation allows us to consider this as a principle ideal of $\mathcal{O}_{K^+}$.

In all cases, we have shown that the kernel is contained in the subgroup of just the identity of the class group. Hence φ is injective. □

In summary, we have proved that $h^+|h$ and computed Q for various cases. We let $h^- = h/h^+$. Hence we divide their respective formulas in Formula 4.6 to obtain:

$$\frac{h^-(2\pi)^{\phi(n)/2}}{Qw\sqrt{|D_K/D_{K^+}|}} = \prod_{\chi \text{ odd}} L(1,\chi)$$

We justify the division because there is no 0 in the denominator,

Corollary 4.23. $L(1,\chi) \neq 0$.

Proof. See Thrm. 4.4 [14]. □

Now, to obtain our final formula for h^-, we list some results taken from [14] which we will not prove.

Corollary 4.24. Let $\tau(\chi) = \sum_{a=1}^{f} \chi(a)e^{2\pi i a/f}$ be a Gaussian sum, then

$$\prod_{\chi \text{ odd}} \tau(\chi) = i^{\phi(n)/2}\sqrt{|D_K/D_{K^+}|}.$$

Proof. See Corollary 4.6 [14]. □

Lemma 4.25. For odd Dirichlet characters χ, where $\chi(a)\overline{\chi}(a) = 1$ if $(a, f_\chi) = 1$, and is 0 otherwise.

$$L(1,\chi) = \frac{\pi i \tau(\chi)}{f_\chi} B_{1,\overline{\chi}}$$

Proof. See the discussion proceeding Corollary 4.6 [14] □

Theorem 4.26 (Conductor-Discriminant Formula)**.** Let L be the number field associated to the group X of Dirichlet characters. Let c be the number of complex embeddings and f_χ denote the conductor of the character χ. Then the discriminant of L is given by

$$D_L = (-1)^c \prod_{\chi \in X} f_\chi,$$

Proof. See the discussion proceeding Thrm. 4.5 [14]. □

However, when we apply this formula to the fields $K = \mathbb{Q}(\zeta_n)$ and K^+ we derive

$$\sqrt{|D_K/D_{K^+}|} = \left(\prod_{\chi \text{ odd}} f_\chi\right)^{1/2}.$$

Putting these together:

$$\begin{aligned}
\prod_{\chi \text{ odd}} L(1,\chi) &= (\pi i)^{\phi(n)/2} \prod_{\chi \text{ odd}} \frac{\tau(\chi)}{f_\chi} B_{1,\bar{\chi}} \\
&= (\pi i)^{\phi(n)/2} \cdot \left(i^{\phi(n)/2}\sqrt{|D_K/D_{K^+}|}\right) \prod_{\chi \text{ odd}} \frac{1}{f_\chi} B_{1,\bar{\chi}} \\
&= \pi^{\phi(n)/2} i^{\phi(n)} \left(\prod_{\chi \text{ odd}} f_\chi\right)^{1/2} \prod_{\chi \text{ odd}} \frac{1}{f_\chi} B_{1,\bar{\chi}} \\
\frac{h^- 2^{\phi(n)/2} \cancel{(\pi)^{\phi(n)/2}}}{Qw \cancel{\sqrt{|D_K/D_{K^+}|}}} &= \cancel{\pi^{\phi(n)/2}} \cdot i^{\phi(n)} \left(\prod_{\chi \text{ odd}} B_{1,\bar{\chi}}\right) \cancel{\left(\prod_{\chi \text{ odd}} f_\chi\right)^{-1/2}}.
\end{aligned}$$

Recall that there are $\phi(n)/2$ odd characters, $\phi(n)/2$ is even and a product indexing over $\bar{\chi}$ is the same as one over χ, hence

Formula 4.27. The h^- Formula

$$h^- = Qw \prod_{\chi \text{ odd}} \left(-\frac{1}{2} B_{1,\chi}\right).$$

Notice that all of the quantities in the formula lie in the rational numbers, as opposed to the previous class number formula which had transcendental elements. Therefore, we can use this formula to determine properties about the factors of h^-. We will end this chapter by showing that there are a finite number of cyclotomic fields with class number 1.

4.5. The Finiteness of Cyclotomic Fields with $h = 1$

In this section, we show that h^- grows increasingly fast with n, we will use analytical number theory to find a bound for h^-.

It is well-known that the nth prime number, denoted p_n, grows asymptotically with $n \log n$. That is,

$$p_n \sim n \log n \quad \text{as } n \to \infty.$$

Another common formulation is:

$$\pi(x) \sim \frac{x}{\log x},$$

where $\pi(x)$ denotes the number of primes less than x. For more on these classical results, see [8]. We use these relations in the following lemma.

Lemma 4.28. Let $K = \mathbb{Q}(\zeta_n)$ be a cyclotomic field with discriminant D_K, then

$$\log D_K = \phi(n) \log n + o(\phi(n) \log n).$$

Proof. From Proposition 2.34, we have the identity

$$\log D_K = \phi(n) \log n - \phi(n) \sum_{p|n} \frac{\log p}{p-1}.$$

To establish the lemma, it suffices to show that

$$\sum_{p|n} \frac{\log p}{p-1} = o(\log n).$$

Let $\omega(n)$ denote the number of distinct prime divisors of n. Since $\prod_{p|n} p \leq n$, taking logarithms gives

$$\sum_{p|n} \log p \leq \log n,$$

and because $\log p \geq \log 2$ for all $p \mid n$, it follows that

$$\omega(n) \leq \frac{\log n}{\log 2}.$$

To estimate the sum, observe that for all primes $p \geq 2$, we have the inequality

$$\frac{1}{p-1} \leq \frac{2}{p},$$

which yields

$$\sum_{p|n} \frac{\log p}{p-1} \leq 2 \sum_{p|n} \frac{\log p}{p}.$$

Now let $m = \omega(n)$, and let $p_1, \ldots, p_m$ be the distinct primes dividing n. Each p_i is among the first m primes, and the largest of them is at most the m-th prime number, which satisfies $p_m = O(m \log m)$.

Define $x := Cm \log m$ for a sufficiently large constant C, so that all $p_i \leq x$. We split the sum into small and large primes relative to $\sqrt{x}$:

$$\sum_{p|n} \frac{\log p}{p} \leq \sum_{p_i \leq \sqrt{x}} \frac{\log p_i}{p_i} + \sum_{\sqrt{x} < p_i \leq x} \frac{\log p_i}{p_i}.$$

For the small primes $p_i \leq \sqrt{x}$, we crudely approximate that $\frac{\log p_i}{p_i} < 1$, and there are clearly less than $O(\sqrt{x})$. Thus,

$$\sum_{p_i \leq \sqrt{x}} \frac{\log p_i}{p_i} = O(\sqrt{x}) \cdot 1.$$

For the large primes $\sqrt{x} < p_i \leq x$, we have $\frac{\log p_i}{p_i} \leq \frac{\log x}{\sqrt{x}}$, and at most $\pi(x) = O(x/\log x)$ primes in this range, so

$$\sum_{\sqrt{x} < p_i \leq x} \frac{\log p_i}{p_i} \leq \pi(x) \cdot \frac{\log x}{\sqrt{x}} = O\left(\frac{x}{\log x} \cdot \frac{\log x}{\sqrt{x}}\right) = O(\sqrt{x}).$$

Combining both ranges, we obtain

$$\sum_{p|n} \frac{\log p}{p-1} \leq 2 \sum_{p|n} \frac{\log p}{p} = O(\sqrt{x}) = O\left(\sqrt{m \log m}\right).$$

Since $m = O(\log n)$, we conclude that

$$\sum_{p|n} \frac{\log p}{p-1} = O\left(\sqrt{(\log n)(\log \log n)}\right).$$

To finish, we verify that this error term is $o(\log n)$. Indeed,

$$\frac{\sqrt{(\log n)(\log \log n)}}{\log n} = \sqrt{\frac{\log \log n}{\log n}} \to 0 \quad \text{as } n \to \infty.$$

Therefore,

$$O\left(\sqrt{(\log n)(\log \log n)}\right) = o(\log n),$$

and

$$\sum_{p|n} \frac{\log p}{p-1} = o(\log n),$$

We substitute the expression for D_K as required. □

We have just derived a nice relation for how the discriminant grows, we are now motivated to relate the discriminant to the class number.

Theorem 4.29 (Brauer-Siegel Theorem)**.** If K runs over a sequence of abelian number fields of degree $[K:\mathbb{Q}]$. Let D_K denote the discriminant, h_K the class number, R_K the regulator, and suppose

$$\frac{[K:\mathbb{Q}]}{\log |D_K|} \to 0,$$

then we have

$$\log(h_K R_K) \sim \log(|D_K|)^{1/2}.$$

Or equivalently,

$$\frac{\log(h_K R_K)}{\sqrt{\log(|D_K|)}} \to 1.$$

Proof. See [9] for a full proof. □

In fact, we could just use the Brauer-Siegel theorem on K and K^+, but we can apply our nice relation for the discriminant to prove the theorem for K. We will not prove K^+.

For a primitive, non-quadratic Dirichlet character χ with conductor q, and let $L(s,\chi)$ be the corresponding Dirichlet L-function. It is well known, as established in Thm. 11.4 [11], the value of $L(1,\chi)$ satisfies the bound

$$L(1,\chi) = O\left(\log q\right).$$

This bound can be used to prove the Brauer-Siegel theorem specifically for when K is a cyclotomic field.

Lemma 4.30. Suppose $K_i = \mathbb{Q}(\zeta_i)$ is a sequence of number fields such that

$$\lim_{i\to\infty} \frac{[K_i:\mathbb{Q}]}{\log|D_{K_i}|} \to 0.$$

Then

$$\lim_{i\to\infty} \frac{\log(h_{K_i}R_{K_i})}{\log\sqrt{|D_{K_i}|}} \to 1.$$

Proof. Let $K_i = \mathbb{Q}(\zeta_i)$. Then $[K_i:\mathbb{Q}] = \phi(i)$, and the analytic class number formula gives

$$h_{K_i}R_{K_i} = \frac{w_i\sqrt{|D_{K_i}|}}{(2\pi)^{\phi(i)/2}} \prod_{\chi\neq 1} L(1,\chi),$$

where the product runs over all nontrivial Dirichlet characters modulo i, and w_i is the number of roots of unity in K_i.

Taking logarithms, we obtain:

$$\log(h_{K_i}R_{K_i}) = \frac{1}{2}\log|D_{K_i}| - \frac{\phi(i)}{2}\log(2\pi) + \log w_i + \sum_{\chi\neq 1}\log L(1,\chi).$$

Divide both sides by $\frac{1}{2}\log|D_{K_i}|$, yielding:

$$\frac{\log(h_{K_i}R_{K_i})}{\frac{1}{2}\log|D_{K_i}|} = 1 - \frac{\phi(i)\log(2\pi)}{\log|D_{K_i}|} + \frac{2\log w_i}{\log|D_{K_i}|} + \frac{2}{\log|D_{K_i}|}\sum_{\chi\neq 1}\log L(1,\chi).$$

We will show that each of the fractional terms tends to zero.

(i) First term: By assumption,

$$\frac{\phi(i)}{\log|D_{K_i}|} \to 0,$$

so the term $\frac{\phi(i)\log(2\pi)}{\log|D_{K_i}|} = o(1)$.

(ii) Second term: The number of roots of unity in $K_i = \mathbb{Q}(\zeta_i)$ satisfies $w_i \leq 2i$, so

$$\log w_i \leq \log(2i) = \log 2 + \log i.$$

From Lemma 4.28, we have

$$\log|D_{K_i}| = \phi(i)\log i + o(\phi(i)\log i),$$

and hence

$$\frac{\log w_i}{\log|D_{K_i}|} \leq \frac{\log i + \log 2}{\phi(i)\log i + o(\phi(i)\log i)} = o(1).$$

(iii) Third term: To estimate the sum $\sum_{\chi\neq 1}\log L(1,\chi)$, we use the known bound $L(1,\chi) = O(\log q)$ for non-trivial Dirichlet characters modulo q. Taking logarithms, we obtain $\log L(1,\chi) = O(\log\log i)$. There are $\phi(i)-1$ such characters, so:

$$\sum_{\chi\neq 1}\log L(1,\chi) = O(\phi(i)\log\log i).$$

Therefore,

$$\frac{1}{\log|D_{K_i}|}\sum_{\chi\neq 1}\log L(1,\chi) = \frac{O(\phi(i)\log\log i)}{\phi(i)\log i + o(\phi(i)\log i)} = \frac{O(\log\log i)}{\log i + o(\log i)} = o(1).$$

Combining all terms, we conclude:

$$\frac{\log(h_{K_i}R_{K_i})}{\frac{1}{2}\log|D_{K_i}|} = 1 + o(1),$$

so

$$\frac{\log(h_{K_i}R_{K_i})}{\log\sqrt{|D_{K_i}|}} \to 1.$$

□

For a proof on the maximal real subfield K_i^+, we direct the reader back to Theorem 4.29.

Again, this outcome is in terms of the regulator. But we may recycle our evaluation of R_K/R_{K^+} to further analyse.

Unless otherwise stated, let $K = \mathbb{Q}(\zeta_n)$, then we let $d_n = |D_K|$ denote the absolute value of the discriminant, h_K the class number of K, R_K the regulator. Similarly, we let d_n^+, h_{K^+}, and R_{K^+} denote the same corresponding to K^+.

For a relationship between D_K and D_{K^+} we use the following:

As established in the proof of lemma 4.19 [14], which follows from [9] (pg.60-66). Let M/L be a number field extension, then

$$|D_M| = (N(\mathfrak{D}_{M/L}))|D_L|^{\deg(M/L)},$$

where D_M and D_L are the respective discriminants,
where L/K is any extension of number fields, $d(L)$ and $d(K)$ are the respective discriminants, $\mathfrak{D}_{M/L}$, and N is the norm from L to $\mathbb{Q}$.

If there is an algebraic integer that extends the rings by $\mathcal{O}_M = \mathcal{O}_L[\alpha]$ for some $\alpha \in \mathcal{O}_M$, then the difference ideal $\mathfrak{D}_{M/L}$ is determined by the minimal polynomial $f(x)$ of α over L, $\mathfrak{D}_{M/L} = (f'(\alpha))$

Lemma 4.31. For any positive integer n. It follows that:

- If $n = p^a$ is a prime power:
  - $d_n = p(d_n^+)^2$, if p is odd.
  - $d_n = 4(d_n^+)^2$, if p is even.
- If n is not a prime power, then $d_n = (d_n^+)^2$.

Thus, for all cases, we arrive at our nice formula for the discriminant

$$\log d_n^+ = \frac{1}{2}\phi(n)\log n + o(\phi(n)\log n).$$

Proof. The following proof follows Lemma 4.19 [14].
Recall that in our case $K = \mathbb{Q}(\zeta_n)$ extends K^+. Thus:

$$\mathbb{Z}[\zeta_n] = \mathbb{Z}[\zeta_n + \zeta_n^{-1}][\zeta_n]$$

with minimal polynomial:

$$f(X) = X^2 - (\zeta_n + \zeta_n^{-1})X + 1 \in K[X],$$

it follows that $\mathfrak{D}_{K/K^+}$ is generated by

$$f'(\zeta_n) = 2(\zeta_n) - (\zeta_n + \zeta_n^{-1}) = \zeta_n - \zeta_n^{-1} = \zeta_n^{-1}(\zeta_n^2 - 1).$$

Thus,

$$\mathfrak{D}_{K/K^+} = (\zeta_n - \zeta_n^{-1}) = (\zeta_n^2 - 1),$$

since ζ_n^{-1} is a unit in $\mathcal{O}_K$. We now analyse $N(\zeta_n^2 - 1)$ based on cases of n:

Case 1: n is not a prime power. In this case, $\zeta_n^2 - 1$ is a unit in $\mathcal{O}_K$, so its norm is a unit in $\mathbb{Z}$. Thus, $\mathfrak{D}_{K/K^+} = (1)$ and the discriminant satisfies

$$|D_K| = (|D_{K^+}|)^2 \quad \Rightarrow \quad d_n = (d_n^+)^2.$$

Case 2: $n = p^a$, where p is an odd prime. Then ζ_n^2 is a primitive root of unity, and $\zeta_n^2 - 1$ is a prime lying above p.

$$N_{K/\mathbb{Q}}(\zeta_n^2 - 1) = p,$$

so that

$$d_n = |D_K| = N_{K/\mathbb{Q}}(\mathfrak{D}_{K/K^+}) \cdot (|D_{K^+}|)^2 = p(d_n^+)^2.$$

Case 3: $n = 2^a$. In this case, ζ_n^2 is a primitive 2^{a-1}th root of unity. Since $\zeta_n - 1$ has norm 2, it follows that element $\zeta_n^2 - 1$ has norm 4. Therefore,

$$d_n = 4(d_n^+)^2.$$

Finally, we recall the previous asymptotic formula for the discriminant of a cyclotomic field:

$$\log d_n = \phi(n) \log n + o(\phi(n) \log n),$$

where $\phi(n)$ is Euler's totient function. Since $d_n = C_n(d_n^+)^2$ for some constant $C_n \in \{1, p, 4\}$, we have

$$\log d_n^+ = \frac{1}{2} \log d_n + O(1) = \frac{1}{2}\phi(n) \log n + o(\phi(n) \log n),$$

since $o(\phi(n) \log n)$ dominates $O(1)$. □

Finally, we label $h_n = h_K$ for $K = \mathbb{Q}(\zeta_n)$ to exaggerate it's dependency on n. We do the same for h_n^- and h_n^+.

Theorem 4.32. Let h_n^- denote the relative class number for the cyclotomic field $\mathbb{Q}(\zeta_n)$. Then

$$\log h_n^- \sim \frac{1}{4}\phi(n) \log n \quad \text{as } n \to \infty.$$

Proof. This proof follows from Lemma 4.20 [14].

From Lemma 4.28 and Lemma 4.31 , we have

$$\log d_n = \phi(n) \log n \cdot (1 + o(1))$$

and

$$\log d_n^+ = \tfrac{1}{2}\phi(n) \log n \cdot (1 + o(1)).$$

Therefore,

$$\frac{\frac{1}{2}\phi(n)}{\log d_n^+} = \frac{1}{\log n(1 + o(1))} \to 0,$$

and

$$\frac{\phi(n)}{\log d_n} = \frac{1}{\log n(1 + o(1))} \to 0.$$

so Lemma 4.30 applies for d_n. Therefore

$$\log h_n R_n = \frac{1}{2}\log d_n + o(\log d_n)$$

and

$$\log h_n^+ R_n^+ = \frac{1}{2}\log d_n^+ + o(\log d_n).$$

By Proposition 4.19,

$$\frac{R_n}{R_n^+} = \frac{2^s}{Q}, \text{ where } s = \frac{\phi(n)}{2} - 1.$$

Hence,

$$\log\left(\frac{R_n}{R_n^+}\right) = \left(\frac{\phi(n)}{2} - 1\right)\log 2 - \log Q = O(\phi(n)).$$

Finally,

$$\begin{aligned}\log h_n^- &= \log(h_n R_n) - \log(h_n^+ R_n^+) - \log\left(\frac{R_n}{R_n^+}\right)\\ &= \frac{1}{2}\log d_n - \frac{1}{2}\log d_n^+ + o(\log d_n) + O(\phi(n))\\ &= \frac{1}{4}\phi(n)\log n + o(\phi(n)\log n).\end{aligned}$$

The last jump was made through the following observations on the error terms

$$o(\log d_n) = o(\phi(n)\log n) \quad (\text{since } \log d_n \sim \phi(n)\log n)$$

$$O(\phi(n)) = o(\phi(n)\log n) \quad (\text{because } \phi(n) = o(\phi(n)\log n))$$

Hence we have the result as required. Equivalently:

$$h_n^- \sim n^{\frac{\phi(n)}{4}}$$

□

Therefore, if $h_n = 1 = h_n^+ h_n^-$, then $h^- = 1$. Hence as $n \to \infty$, $h_n \to \infty$. So for any fixed c, we can find a sufficiently large N such that for all $n > N$, $h_n^- > c$. That means the set:

$$\{n \in \mathbb{N} : h_n^- \leq c\}$$

is finite. It follows then that for any fixed C, the set

$$\{n \in \mathbb{N} : h_n \leq C\}$$

is also finite. In particular, for $C = 1$, we showed that there are a finite number of cyclotomic fields with $h_n = 1$.

However, this method doesn't help us find a sufficiently large N such that $h_n^- > n$ for $n > N$. These ideas are then explored in chapter 11 [14]. As it turns out, $n = 84$ is the largest such that $h_n = 1$.

References

[1] Sheldon Axler. *Linear algebra done right.* en. Cham, Switzerland: Springer Nature, Oct. 2023 (cit. on p. 23).

[2] Z I Borevich and I R Shafarevich, eds. *Number Theory.* Pure & Applied Mathematics S. San Diego, CA: Academic Press, July 1966 (cit. on pp. 29, 31).

[3] L Carlitz. “Note on irregular primes”. en. In: *Proc. Am. Math. Soc.* 5.2 (1954), pp. 329–331 (cit. on p. 30).

[4] Harold M Edwards. *Fermat’s last theorem.* en. 1st ed. Graduate Texts in Mathematics. New York, NY: Springer, Feb. 1996 (cit. on p. 19).

[5] Ronald L Graham, Donald E Knuth, and Oren Patashnik. *Concrete mathematics.* 2nd ed. Boston, MA: Addison Wesley, Feb. 1994 (cit. on p. 18).

[6] Richard Guy. *Unsolved problems in number theory.* en. 3rd ed. Unsolved Problems in Intuitive Mathematics. New York, NY: Springer, July 2004 (cit. on p. 30).

[7] William Hart, David Harvey, and Wilson Ong. “Irregular primes to two billion”. In: (2016). eprint: 1605.02398 (math.NT) (cit. on p. 30).

[8] G J O Jameson. *London mathematical society student texts: The prime number theorem series number 53.* Cambridge, England: Cambridge University Press, June 2012 (cit. on p. 48).

[9] Serge Lang. *Algebraic number theory.* en. Proceedings in Life Sciences. New York, NY: Springer, Dec. 1986 (cit. on pp. 8, 10, 11, 50, 52).

[10] H. W. Lenstra Jr. “Solving the Pell equation”. In: *Notices Amer. Math. Soc.* 49.2 (2002), pp. 182–192. ISSN: 0002-9920,1088-9477 (cit. on p. 37).

[11] Hugh L Montgomery and Robert C Vaughan. *Cambridge studies in advanced mathematics: Multiplicative number theory I: Classical theory series number 97.* Cambridge, England: Cambridge University Press, Feb. 2010 (cit. on p. 50).

[12] Ian Stewart. *Galois theory.* en. 5th ed. Philadelphia, PA: Chapman & Hall/CRC, Sept. 2022 (cit. on pp. 14, 15, 17).

[13] Ian Stewart and David Tall. *Algebraic number theory and Fermat’s last theorem.* 3rd ed. Natick, MA: A K Peters, Dec. 2001 (cit. on pp. 5–8, 10, 11, 19, 25, 29).

[14] Lawrence C Washington. *Introduction to Cyclotomic Fields.* en. Graduate Texts in Mathematics. New York, NY: Springer, Apr. 1982 (cit. on pp. 7–9, 11, 14–17, 19, 29–31, 46, 47, 52–54).