Computing non-square elements of square norm in a number field.

Joe Kent

December 13, 2023

Abstract

In this thesis we explore the unit group of the ring of integers of number fields. In our exploration we look at Dirichlet's unit theorem which shows that the unit group is a finitely generated abelian group. This will allow us to explore computing the generating set of the unit group. From this basis we then extend the computation of unit groups to describe and implement an algorithm in `PARI` for finding elements in the kernel of the norm mapping $K^\times/K^{\times 2} \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Elements in this mapping are of particular interest for finding Brauer Manin obstructions with current implementations using a set of fundamental units.

Contents

1 Introduction

Let $K = \mathbb{Q}[x]/\langle f(x)\rangle$ for some monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$, $\mathbb{Z}_K$ be the ring of integers of K and $\mathbb{Z}_K^\times$ the unit group. From understanding the unit group we can solve numerous mathematical problems including Pell's equation. The most useful theorem on the unit group is Dirichlet's unit theorem (see Theorem 2.6.1) which tells us the structure of the unit group. From this theorem we can develop a way of generating a set of fundamental units for these applications. In this thesis we will explore the computation of the unit group, subsets of the unit group and finding non-square elements with square norm (with useful application in finding Brauer Manin obstructions). Finally, we will develop and implement an algorithm for generating elements of square norm that are not squares [Ken23].

A famous example of the use of units in number rings is Pell's equation which was posed by Fermat in 1657 and solution attributed to John Pell. Pell's equation is the following

$$x^2 - dy^2 = 1 \tag{1}$$

where we are looking for solutions $x, y \in \mathbb{Z}$ with fixed $d \in \mathbb{Z}$. Now, consider the number field $K = \mathbb{Q}(\sqrt{d})$ with θ the root of the minimal polynomial of K. For this equation the norm is defined as $(x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2 = 1$ which means that we are looking for solutions of norm 1. These solutions will be equivalent to elements $x + y\theta \in \mathbb{Z}_K$ where θ is a root of the polynomial $x^2 - d$. Thus, if we can find units in $\mathbb{Z}_K$ then we can find the solution to our Pell's Equation as units are elements with norm ± 1 (See Lemma 2.2.4). Now it remains to be seen that there are non-trivial units in $\mathbb{Z}_K$, we will check this using Dirichlet's Unit Theorem. If d is not a square then $f(x)$ is irreducible otherwise we can define the minimal polynomial $x^2 - d = (x + \sqrt{d})(x - \sqrt{d})$. Since $f(x)$ is irreducible for d not square from Dirichlet's Unit theorem (see Theorem 2.6.1) we know that only one unit that is not a root of unity is required to generate the unit group. Thus, we know that we have a solution assuming d is not a square. Furthermore, if $d = d'^2$ is a square then Pell's equation becomes $x^2 = 1 + (d'y)^2$ which is impossible to solve as there are no integer squares that are adjacent to each other (except the trivial $x = 1$ and $y = 0 \Rightarrow d'y = 0$ which is always a solution to Pell's Equation). Consider the example where $d = 6$ which will have a unit since d is not a square. Thus, the unit of $\mathbb{Z}_K$ where $K = \mathbb{Q}(\sqrt{d})$ is $2\theta + 5$ (the roots of unity are ± 1). This means that we have the solution $x = 5, y = 2$ to Pell's equation when $d = 6$. This solution is fairly easy to compute, however, it quickly becomes impractical. Consider the case when $d = 1153$. The fundamental unit for this is $30178902568750 73\theta - 1024754004023072656$ which is of order 10^{17} making it impractical to brute force. Thus, we must use more advanced techniques to compute the fundamental units.

A naive way to compute the set of fundamental units is to run through each number in a brute force manner. From our example above we see that this is impractical and would take trillions of computations. Instead, we construct the set of fundamental units using methods that are based on constructive proofs of Dirichlet's Unit theorem. These methods start by generating elements until we obtain elements α, β, such that their norm is equivalent. Then we can take α/β which will have a norm of 1 as the norm mapping is a homomorphism. Practically, we take the valuations of our elements over a prime ideal factorbase $p_1, \ldots, p_k$, that is if $\langle\alpha\rangle = \mathfrak{p}_1^{v_1} \ldots \mathfrak{p}_k^{v_k}$ we store the vector $(v_1, \ldots, v_k)$. We do this as it converts the problem to finding the kernel of a matrix formed by the valuation vectors. If an element does not factor over our chosen factor base then we ignore it for computational efficiency. This leads to a balancing act of including sufficient primes to generate the unit group but having the smallest possible factor base to increase computational efficiency. A sufficient bound on the primes is Minkowski's constant (see Subsection 2.4) as all the primes below it are a sufficient representation of the rest of the number ring for our application. However, practically we can use a smaller bound (for exam-

ple $12\log|D|$) which is sufficient if one assumes the General Riemann Hypothesis (GRH) is true.

Units are used in numerous algorithms, however, an algorithm of interest is finding Brauer Manin obstructions on hyperelliptic curves using the algorithm seen in [CS23]. This algorithm uses the subgroup of $(K^\times/K^{\times 2})_S$ that lies in the kernel of the norm map $K^\times/K^{\times 2} \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. $(K^\times/K^{\times 2})_S$ is a subgroup of $K^\times/K^{\times 2}$ where every element is not ramified over the prime ideals above the primes not in S where S is a set of prime numbers. For this thesis we will assume that S is all the prime numbers. Elements in $\mathbb{Z}_K^\times$ are always going to map to ± 1 with the norm map, so it is natural to use this set for finding elements. Thus, we can simply try to find units in $\mathbb{Z}_K^\times$ which we can use the fundamental unit algorithm to do. However, experiments show that one does not need a full set of fundamental units to still have success when finding obstructions [Ken22]. Indeed, one only needs about a quarter of the full set of fundamental units to find obstructions with sufficient reliability. Thus, it is reasonable to assume that an algorithm could be developed to terminate when a small number of units are found. For this project in particular, we will modify the algorithm to find elements of square norm in $\mathbb{Z}_K$ that are not squares as they will be in the kernel of the norm mapping. This could be done by storing the factorisations of the norm of the elements generated using current methods and then finding the kernel of this matrix modulo 2.

In section 2 we explore the relevant background in algebraic number theory. In section 3 we will go through the history and a detailed implementation of a unit group algorithm. In section 4 we will explain the generation of square norm elements and then provide a tangible example and algorithm for generating these elements. Finally, in section 5 we will briefly summarise the results of this thesis.

2 Background in Algebraic Number Theory

2.1 Algebraic Structures

To start we will define the basic algebraic structures that are used.

Definition 2.1.1 (Group)**.** A group G is a set X and a binary operator $*$ on X such that:

- There is an identity element 1 such that $a * 1 = 1 * a = a$ for all $a \in X$.
- X is closed under $*$.
- For all $a \in X$ there exists $b \in X$ such that $ab = 1$

One can extend the definition of a group to obtain a ring.

Definition 2.1.2 (Ring)**.** A ring is a set R with two binary operators $\times, +$ such that the following axioms are satisfied

- $(R, +)$ for a commutative group.
- The operator $\times$ is associative.
- $\forall a, b, c \in R$ the distributive laws $a \times (b + c) = a \times b + a \times c$ and $(a + b) \times c = a \times c + b \times c$ hold.

An example of a ring is the integers $\mathbb{Z}$ with the operators of addition and multiplication. $\mathbb{Z}$ forms a commutative group with addition as $\forall a \in \mathbb{Z}$ there is an additive inverse $(a + (-a) = 0)$ with identity element 0 and $\mathbb{Z}$ is closed (you can never add two integers and not get an integer). $\mathbb{Z}$ is associative under multiplication as $a \times b = b \times a$ for all $a, b \in \mathbb{Z}$. Finally one can see that the

distributive laws hold. Thus, $\mathbb{Z}$ forms a ring with the operators of addition and multiplication. There are also a number of unique properties that elements in rings can have with the following an important definition.

Definition 2.1.3 (Unit)**.** A *unit* a is an element in a ring R with a corresponding element a^{-1} such that $a \times a^{-1} = 1$, that is, a has a multiplicative inverse.

For example, $\mathbb{Z}$ only has the units ± 1 which has itself as its inverse, but in the ring of rational numbers $\mathbb{Q}$, all non-zero elements are units (consider 2 and 1/2). This definition of a unit naturally leads to a *field* F which is a commutative ring where every nonzero element is a unit. From the definition of a field it is easy to see that $\mathbb{Q}$ is a field. We can also define *subrings* as a subset of a ring R that is a ring under the induced properties of R. Note that a *subfield* is the same as a subring except it is a subset of a field and is itself a field.

Another type of subset is the subset of ideal

Definition 2.1.4 (Ideal)**.** An *ideal* I is a subring of a ring R with the property that with $a \in I$ and $b \in R$ that $ab \in I$.

For example, the subring $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$ as with $a, b' \in Z$ and $b \in 2\mathbb{Z}$ with $2b' = b$ and then $ab = 2ab' \in 2\mathbb{Z}$. There are many properties that an ideal can have, the following are the more useful properties for this thesis. A *prime ideal* $\mathfrak{p}$ of a ring R is an ideal with the property that if $a, b \in R$ and $ab \in \mathfrak{p}$ then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Consider the ideal $3\mathbb{Z}$, as 3 is a prime it has no non-trivial divisors in $\mathbb{Z}$, thus if $a \times b \in 3\mathbb{Z}$ it implies either a or b is a multiple of 3 and thus, is in $3\mathbb{Z}$. Thus, $3\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. However, consider the ideal $6\mathbb{Z}$, now $6 = 2 \times 3$ and $2, 3 \notin 6\mathbb{Z}$ thus, $6\mathbb{Z}$ is not a prime ideal. A principal ideal is an ideal that is generated by a single element in the ring. For example the ideal $\langle 2 \rangle$ in $\mathbb{Z}_K$ where $K = \mathbb{Q}[x]/\langle x^2 - 5 \rangle$ is a principal ideal but the ideal $\langle 2, x - 1 \rangle$ in $\mathbb{Z}_K$ is not a principal ideal. A proper ideal is an ideal I that is neither the complete ring R or the trivial ideal $\{0\}$. For example the ideal $6\mathbb{Z}$ is a proper ideal. A *maximal ideal* is an ideal that is not a subset of any proper ideal. For example $3\mathbb{Z}$ is a maximal ideal but $6\mathbb{Z} \subset 3\mathbb{Z}$ is not a maximal ideal. Now we come to the following observation

Lemma 2.1.1. *A ideal is prime if it is maximal.*

Proof: Let R be a ring and $\mathfrak{a}$ be an ideal of R. The ideals of $R/\mathfrak{a}$ is correspond to ideals of R lying between $\mathfrak{a}$ and R. Suppose $\mathfrak{a}$ is maximal. Then there are no proper ideals in $R/\mathfrak{a}$. This implies that $R/\mathfrak{a}$ is a field as otherwise there would exist a non-unit $1 \neq a \in R/\mathfrak{a}$ and the ideal $\mathfrak{a}$ would not be the $R/\mathfrak{a}$ or $\{0\}$. Since $\mathfrak{a}$ is maximal we know that $\mathfrak{a} \neq R$. Now let us assume that there exists $\mathfrak{bc} \subseteq \mathfrak{a}$ but $\mathfrak{b} \nsubseteq \mathfrak{a}$, $\mathfrak{b} \nsubseteq \mathfrak{a}$. Then we can find elements $b \in \mathfrak{b}, c \in \mathfrak{c}$ with $b, c \notin \mathfrak{a}$ but with $bc \in \mathfrak{a}$. However, this implies that $\mathfrak{a} + b$ and $\mathfrak{a} + c$ are non-zero in $R/\mathfrak{a}$ but $(\mathfrak{a} + b)(\mathfrak{a} + c) = \mathfrak{a} + bc = \mathfrak{a}$ implying $(\mathfrak{a} + b)$ and $(\mathfrak{a} + c)$ are zero-divisors, however, $R/\mathfrak{a}$ is a field so there are no zero divisors a contradiction. Thus, $\mathfrak{a}$ is prime. □
A natural question from this lemma would be whether every prime ideal is maximal. However, this is not the case generally and in Lemma 2.2.9we will show that there is a case where this is true. Finally, we will define a property that some rings have relating to ideals, a number ring is *noetherian* when all the ideals of the number ring are finitely generated. This property will allow us to write out our ideals as a set of elements.

Another area in algebraic number theory that we will consider is that of polynomials. For our case in particular we are mostly interested in the following type of polynomial

Definition 2.1.5 (Irreducible Polynomial)**.** An irreducible polynomial $f(x)$ is a polynomial with coefficients in a ring R such that $f(x) \neq g(x)h(x)$ for all $g(x), h(x) \in R[x]$.

For example, the polynomial $f(x) = x^2 + 1$ is irreducible over $\mathbb{R}$ (the roots of the polynomial are $\pm i \notin \mathbb{R}$). We define the *degree* of a polynomial as highest exponent, that is n in the polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. A polynomial is called a *monic polynomial* when $a_n = 1$. Naturally one can ask if there is a field where all the roots of a polynomial are contained, that is, a field where there are no irreducible polynomials. This leads to the following theorem.

Theorem 2.1.2 (Number of complex roots of a polynomial)**.** *Every polynomial $f(x) \in \mathbb{C}$ of degree n has exactly n roots in $\mathbb{C}$ counting multiplicity.*

Proof: Suppose $n = 1$, then $f(x) = x - \theta$ and $f(\theta) = 0$ proving the statement. Thus, suppose that the theorem holds for $n - 1$. Now from the Fundamental Theorem of Algebra we know that $f(x) \in \mathbb{C}[x]$ has a root in $\mathbb{C}$. Let $\theta' \in \mathbb{C}$ be this root of $f(x)$, then we can write $f(x) = g(x)(x - \theta') \in C$ and $g(x)$ is of degree $n - 1$ which by our assumption has $n - 1$ roots. Thus, $f(x)$ has n roots in $\mathbb{C}$. □

We have considered polynomials as you can create extension fields from monic irreducible polynomials. We define an *extension field* E of a field F as a field which has F as a subfield. We can build these by taking quotients of $F[x]$, that is, we can let $E = F[x]/\langle f(x)\rangle$. For example, we can build the complex numbers as an extension of $\mathbb{R}$ with $\mathbb{C} = \mathbb{R}[x]/\langle f(x)\rangle = \mathbb{R}(i)$ which is a ring containing the roots of $f(x)$ (that is, $\pm i$) and $\mathbb{R}$. This can be seen in the following theorem.

Theorem 2.1.3 (Extension of F)**.** *Let F be a field and $p(x) \in F[x]$ be irreducible over F. If θ is a zero of $p(x)$ in some extension E of F then $F(\theta) \cong F[x]/\langle p(x)\rangle$.*

Proof based on Theorem 20.1 in [Gal21]: Define $\phi : F[x] \to E$ taking $f(x) \mapsto f(\theta)$. This is a ring homomorphism and the image is contained in $F(\theta)$. It can be seen that $\langle p(x)\rangle \subseteq \ker\phi$ as $p(\theta) = 0$. We also have that $\ker\phi \neq F[x]$ as $\phi(1) = 1 \neq 0$. This implies that $\langle p(x)\rangle = \ker\phi$ because $p(x)$ is irreducible so $\langle p(x)\rangle$ is maximal and $\ker\phi \neq F[x]$. This shows us that $F[x]/\langle p(x)\rangle = F[x]/\ker\phi$. Which is isomorphic to $\text{img}(\phi)$ by the first isomorphism theorem (See Theorem 15.3 in [Gal21]). Thus, we see that $\text{img}(\phi) \subseteq F(\theta) \subseteq E$. Now $F[x]/\langle p(x)\rangle$ is a field as $\langle p(x)\rangle$ is maximal which implies that the image of ϕ is a field containing $\phi(x) = \theta$ and that $F(\theta)$ is the smallest field containing F and θ implying $\text{img}(\phi) = F(\theta)$. This proves that $F(\theta) \cong F[x]/\langle p(x)\rangle$. □

Now we need to have a way to select elements in a field that is easy to understand and read. To do this we need to have a basis.

Definition 2.1.6 (basis)**.** Let F be a ring. An *F-basis* of a group or ring E is a set of elements $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ from E such that the following two conditions are true

- For all $\beta \in E$ there are values $a_1, a_2, \ldots, a_n \in F$ such that $\beta = a_1\alpha_1 + a_2\alpha_2 + \ldots a_n\alpha_n$
- There are no values $a_1, a_2, \ldots, a_n \in F$ with at least one non-zero such that $a_1\alpha_1 + a_2\alpha_2 + \ldots a_n\alpha_n = 0$

The first condition is that the basis spans E and the second condition is that all the elements are linearly independent. This allows us to consider E as a vector space over F and also describe each element in E uniquely as a combination of elements. However, this concept is useless if there does not exist an F-basis over E

Theorem 2.1.4 (Basis of $F(\theta)$ over F)**.** *Let F be a field and $p(x) \in F[x]$ be irreducible over F and $F(\theta) = F[x]/\langle p(x)\rangle$. If $\deg(p(x)) = n$, then every member of $F(\theta)$ can be expressed uniquely in the form*

$$c_{n-1}\theta^{n-1} + c_{n-2}\theta^{n-2} + \cdots + c_1\theta + c_0 \tag{2}$$

where $c_0, c_1, \ldots, c_{n-1} \in F$. In other words $\{1, \theta, \ldots, \theta^{n-1}\}$ is a F-basis for $F(\theta)$.

Proof based on Theorem 19.3 in [Gal21]: Suppose $1, \theta, \ldots, \theta^{n-1}$ is a F-basis for $F(\theta)$. Let $\phi : F[x] \to E$ taking $f(x) \mapsto f(\theta)$. Let $\beta \in F(\alpha) = \text{img}(\phi)$ by Theorem 2.1.3. So $\beta = \phi(g(x))$ for some $g(x) \in F[x]$. Now writing $g(x) = p(x)q(x) + r(x)$ with $\deg(r(x)) < n$ we obtain

$$\phi(g) = \phi(p)\phi(q) + \phi(r) = r(\theta) \tag{3}$$

Now from this we see that $r(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ thus,

$$\beta = r(\theta) = c_{n-1}\theta^{n-1} + c_{n-2}\theta^{n-2} + \cdots + c_1\theta + c_0 \tag{4}$$

Implying that this vector space spans. Suppose $c_{n-1}\theta^{n-1} + c_{n-2}\theta^{n-2} + \cdots + c_1\theta + c_0 = 0$ with $c_i \in F$. Then $h(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \ker \phi = \langle p(x) \rangle$. So $h(x) = p(x)g(x)$ with $\deg(h(x)) < n$ and $\deg(p(x)g(x)) \geq n$. Thus, $h(x) = g(x) = 0$, which implies all the coefficients are zero implying that they are linearly independent. Thus, our basis $1, \theta, \ldots, \theta^{n-1}$ spans and is linearly dependent. □

We will now generalise our notation and define some critical definitions. An *algebraic integer* is an element in K such that it is the solution of some monic polynomial with integer coefficients, that is, it is a root of some polynomial in $\mathbb{Z}[x]$. For this project we define K to be the extension field $\mathbb{Q}(\theta)$ where θ is an algebraic integer. Similarly to how we can consider integers in $\mathbb{Q}$ we can consider the following.

Definition 2.1.7 (Ring of Integers)**.** The ring of integers $\mathbb{Z}_K$ of an extension field K is the ring of all algebraic integers contained in K.

For example we can consider the ring of integers $\mathbb{Z}_K$ where $K = \frac{\mathbb{Q}[x]}{\langle x^2-5 \rangle}$. K has the roots θ which map to $\pm\sqrt{5}$ in $\mathbb{C}$ however, this does not mean that $\mathbb{Z}_K$ is equivalent to $\mathbb{Z}[\sqrt{5}]$. Consider the element $\alpha = \frac{1+\sqrt{5}}{2}$, now this element is clearly in K, but it is also in $\mathbb{Z}_K$. This is because α is a root of the polynomial $(x - \frac{1-\sqrt{5}}{2})(x - \frac{1+\sqrt{5}}{2}) = x^2 - x - 1 \in \mathbb{Z}[x]$, thus, it is an algebraic integer and is in $\mathbb{Z}_K$. An *integral basis* for $\mathbb{Z}_K$ is a $\mathbb{Z}$-basis for $\mathbb{Z}_K$. We will define $\omega_1, \ldots, \omega_n$ to be an integral basis for K and we will now show that every ring of integer has a basis. To do this we need to consider the following definition

Definition 2.1.8. The discriminant of a set of element $\alpha_1, \ldots, \alpha_n$ is defined as follows.

$$\delta(\alpha_1, \ldots, \alpha_n) = \det\left(\begin{bmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \ldots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n) \end{bmatrix}\right)^2 \tag{5}$$

This definition will also be useful later for the norm of an ideal.

Lemma 2.1.5. *The ring of integers $\mathbb{Z}_K$ has a $\mathbb{Z}$-basis $\{\omega_1, \ldots, \omega_n\}$.*

Proof from Theorem 1.9 in Chapter 5 of [Ros94]: From Theorem 2.1.4 we know there is at least one set of elements $\{\omega_1, \ldots, \omega_n\}$ that forms a $\mathbb{Q}$-basis for K. We can assume that this $\mathbb{Q}$-basis is a set of algebraic integers as we can multiply by the greatest common denominator. Since $\{1, \theta, \ldots, \theta^{n-1}\}$ is a $\mathbb{Q}$-basis for K we can have $\omega_i = c_{i,0} + c_{i,1}\theta + \cdots + c_{i,n-1}\theta^{n-1}$ and the conjugates as $\sigma_j(\omega_i) = c_{i,0} + c_{i,1}\sigma_j(\theta) + \cdots + c_{i,n-1}\sigma_j(\theta^{n-1})$. This means that $\Delta(\omega_1, \ldots, \omega_n) = (\det(M))^2\Delta(1, \theta, \ldots, \theta^{n-1})$ with M being a matrix with coefficients $c_{i,j}$. Now since $\{\omega_1, \ldots, \omega_n\}$ form a $\mathbb{Q}$-basis in of K that $\det(M) \in \mathbb{Q}$ and will be non-zero. As well as this we know that $\Delta(1, \theta, \ldots, \theta^{n-1})$ will be non-zero and rational as all the conjugates are distinct and form a $\mathbb{Q}$-basis. Thus, we have that there is a minimum set of algebraic integers that is a $\mathbb{Q}$-basis over K as the discriminant is always positive (solution is rational and non-zero). Now suppose

$\omega_1, \ldots, \omega_n$ is a Q-basis over K with minimum discriminant but is not a $\mathbb{Z}$-basis of $\mathbb{Z}_K$. Then there is an element $\beta \in \mathbb{Z}_K$ such that $\beta = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega$ with at least one $a_i \notin \mathbb{Z}$. We will choose a_1 to be one of those elements. Now $a_1 = a_1' + t$ with $0 < t < 1$. From this let use choose a new $\mathbb{Q}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ with $\alpha_1 = \beta - a_1'\omega_1$ and $\alpha_i = \omega_i$ for integer $2 \leq i \leq n$. From this we can form the transformation matrix as

$$T = \begin{bmatrix} t & a_2 & \ldots & a_n \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{6}$$

Taking the discriminant of this new $\mathbb{Q}$-basis we obtain

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det(T)^2\Delta(\omega_1, \ldots, \omega_n) = t^2\Delta(\omega_1, \ldots, \omega_n) \tag{7}$$

as the determinant mapping is a homomorphism. The determinant of this $\mathbb{Q}$-basis is smaller than that of $\{\omega_1, \ldots, \omega_n\}$ which we choose to be minimal. Thus, we have a contradiction and so there is no β that is not an integral linear combination of $\{\omega_1, \ldots, \omega_n\}$ meaning there is a $\mathbb{Z}$-basis for $\mathbb{Z}_K$. □

Another feature of the ring of integers is the following

Lemma 2.1.6. *$\mathbb{Z}_K$ is noetherian.*

The proof of this can be seen in Theorem 5.3b in [ST79]. The *unit group* $\mathbb{Z}_K^\times$ is a group that contains all the units in $\mathbb{Z}_K$ with multiplication the binary operator. A *root of unity* is an unit a such that for some non-zero $n \in \mathbb{Z}$, $a^n = 1$. For example consider $-1 \in \mathbb{Z}^\times$, $(-1)^2 = 1$. The set of roots of unity form a subset of the unit group. Another group that is closely related to the unit group is the class group. Let J_K be the group of fractional ideals of K, that is ideals $I \subseteq K$ that satisfy the property $cI \subseteq \mathbb{Z}_K$ where $c \in \mathbb{Z}_K$ is non-zero. Let P_K be the group of principal fractional ideals of $\mathbb{Z}_K$, which is a subgroup of J_K.

Definition 2.1.9 (Class group)**.** The *class-group* is the quotient group J_K/P_K [ST79].

The order of the class group is called the *class-number* which we will show is finite in Theorem 2.5.1. We say that two ideals $\mathfrak{a}, \mathfrak{b}$ are equivalent, that is $\mathfrak{a} \sim \mathfrak{b}$ if they map to the same element in J_K/P_K. We notate $[\mathfrak{a}]$ as the set of ideals equivalent to $\mathfrak{a}$ and the class group can be seen as the set of these equivalency classes.

2.2 Embeddings and Field Norms

The two fundamental tools used to find units are embeddings and norms. We first define an embedding.

Definition 2.2.1 (Embeddings)**.** An *embedding* is an injective homomorphism from a field E to another field F.

From this one can observe the following.

Lemma 2.2.1. *Let σ be an embedding from $K \to \mathbb{C}$, $\sigma(\alpha) = \alpha$ if $\alpha \in \mathbb{Z}$.*

Proof: We can write $a = \sum_{i=1}^{a} 1$ as $a \in \mathbb{Z}$. Thus, $\sigma(a) = \sigma(\sum_{i=1}^{a} 1) = \sum_{i=1}^{a} \sigma(1) = \sum_{i=1}^{a} 1 = a$ as $\sigma(1) = 1$ and $\sigma(ab) = \sigma(a)\sigma(b)$ from homomorphism properties. □

For a number field K we define an embedding as real if $\sigma(K) \subseteq \mathbb{R}$ and complex if $\sigma(K) \subseteq \mathbb{C}$ but $\sigma(K) \not\subseteq \mathbb{R}$. We define the number or real embeddings as r_1 and the number of pairs of complex embeddings as r_2. Note that they vary from number field to number field. A non-obvious property of embeddings in rational extensions to complex numbers is that there is a finite number of them. Consider the following lemma.

Lemma 2.2.2. *Let σ be an embedding from $K \to \mathbb{C}$ where $K = \mathbb{Q}[x]/\langle f(x)\rangle$ and $f(x)$ is a polynomial of degree n with $f(\theta) = 0$. Then there are exactly $r_1 + 2r_2 = n$ linearly independent embeddings.*

Proof: Consider the embedding $\sigma : \theta \mapsto \theta'$ where $\theta' \in \mathbb{C}$ is a root of $f(x)$ (There are n of these from Theorem 2.1.2). By Theorem 2.1.4 we know that every element in K can be uniquely represented as a combination of roots θ. Thus, if we are only mapping the roots to distinct elements in $\mathbb{C}$ thus, if we are mapping to distinct roots in $\mathbb{C}$ we know that they will be uniquely represented and the map will be injective, thus, an embedding. Suppose that there is another embedding from $K \to \mathbb{C}$, that takes $\sigma(\theta) \to \alpha$ where $f(\alpha) \neq 0$. Now consider $0 = \sigma(0) = \sigma(f(\theta)) = f(\sigma(\theta)) = f(\alpha) \neq 0$ which gives a contradiction, thus, θ must map to a root of $f(x)$. Thus, since every embedding must be of the form $\sigma : \theta \mapsto \theta'$ and all these are embeddings then there are an equal number of embeddings to number of roots. □

Now to define the norm. Let E be an extension of F of finite degree which forms a vector space over F. From Theorem 2.1.4 we know there exists an F-basis for E. From this we can build a linear map for an element $\alpha \in E$ that takes $M_\alpha : b \mapsto b\alpha$. This linear map M_α can be seen as a matrix over the F-basis for E. From this linear map we can define the following

Definition 2.2.2 (Norm of an Element)**.** The norm of an element α is the determinant of the matrix M_α.

From this we can obtain the following lemmas

Lemma 2.2.3. *Let $\alpha, \beta \in E$. Then $\mathcal{N}_{E|F}(\alpha\beta) = \mathcal{N}_{E|F}(\alpha)\mathcal{N}_{E|F}(\beta)$.*

Proof: The statement in the lemma can be restated as follows

$$\det(M_{\alpha\beta}) = \det(M_\alpha)\det(M_\beta) \tag{8}$$

Since the determinant is a homomorphism from $GL_n(F) \to F^\times$ all we need to show is that $M_{\alpha\beta} = M_\alpha M_\beta$. This can be seen as $M_{\alpha\beta} : b \mapsto b\alpha\beta$ and $M_\alpha M_\beta b = M_\alpha b\beta = b\beta\alpha = b\alpha\beta$. Thus, $M_\alpha M_\beta : b \mapsto b\alpha\beta$ which is equivalent to $M_{\alpha\beta}$ thus, the theorem holds. □

Lemma 2.2.4. *Every unit in $\mathbb{Z}_K$ has the norm $\mathcal{N}_{K|\mathbb{Q}}(\alpha) = \pm 1$.*

Proof: Suppose $\alpha \in \mathbb{Z}_K$ is a unit and α^{-1} is the corresponding inverse. From Lemma 2.2.3 we know that $\mathcal{N}_{K|\mathbb{Q}}(\alpha\alpha^{-1}) = \mathcal{N}_{K|\mathbb{Q}}(\alpha)\mathcal{N}_{K|\mathbb{Q}}(\alpha^{-1})$. However, $\mathcal{N}_{K|\mathbb{Q}}(\alpha\alpha^{-1}) = \mathcal{N}_{K|\mathbb{Q}}(\pm 1) = \pm 1$ and so $\mathcal{N}_{K|\mathbb{Q}}(\alpha) = 1/\mathcal{N}_{K|\mathbb{Q}}(\alpha^{-1})$. However, since $\alpha, \alpha^{-1} \in \mathbb{Z}_K$ we see that the determinant of either of the elements must be in $\mathbb{Z}$ (as the M_α depends on the coefficients of the minimal polynomial which is integral). This results in $\mathcal{N}_{K|\mathbb{Q}}(\alpha), \mathcal{N}_{K|\mathbb{Q}}(\alpha^{-1}) \in \mathbb{Z}^\times$ which means that they have the possible values of ± 1. □

Lemma 2.2.5. *The following statement is true*

$$\mathcal{N}_{K|\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \tag{9}$$

where σ_i is an embedding of $K \to \mathbb{C}$.

Proof based on proof in Lemma 4.2 in [Ste20]: Suppose we have that $K = \mathbb{Q}(\alpha)$ then the embeddings map α to the roots of the irreducible polynomial of α. Thus, $h(x) = f(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha))$ is the minimal irreducible polynomial of α. Consider the general case, then $\mathbb{Q}(\alpha)$ has $[K : \mathbb{Q}(\alpha)]$ extensions, and so we obtain that $\prod_{i=1}^{n}(x - \sigma_i(\alpha)) = f(x) = h(x)^{[K:\mathbb{Q}(\alpha)]}$ where $h(x)$ is the minimal polynomial of α. Thus, we have that the minimal polynomial of α at least divides $f(x)$. Let $g(x) = \det(\lambda I - M_\alpha)$ be the characteristic polynomial of M_α. M_α

is a root of $g(x)$ from Cayley-Hamilton Theorem. Similarly M_α is a root of $f(x)$ as M_α is the matrix representation of α. Thus, since $g(x)$ and $f(x)$ both have M_α as roots the minimal polynomial must divide $g(x)$ and $f(x)$. In fact these two polynomials are the same as M_α is also a solution to the minimal polynomial of the conjugates of α (each column represents a conjugate of α). From this we obtain that the constant element in $f(x)$ is $(-1)^k \prod_{i=1}^n \sigma(\alpha)$ and the constant element of $g(x) = (-1)^k \det(M_\alpha)$ which means that if $g(x) = f(x)$ we have that $\mathcal{N}_{K|\mathbb{Q}}(\alpha) = \det(M_\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$ proving our theorem. □
The elements $\sigma_i(\alpha)$ are called conjugates of α. So far we have only considered the norm of an element, however, we can extend this idea to norms of ideals. We define $\delta(I)$ as the discriminant of basis elements of the ideal I and $\delta(K)$ as the discriminant of the $\mathbb{Q}$-basis elements of the field K. And now to consider the norm of an ideal

Definition 2.2.3 (Norm of an ideal)**.** The norm of an ideal I is $\mathcal{N}_{K|\mathbb{Q}}(I) = \sqrt{\frac{\delta(I)}{\delta(K)}}$.

A useful property of the norm of an ideal is

Theorem 2.2.6. *Let I be a non-zero ideal of $\mathbb{Z}_K$. Then $\mathcal{N}_{K|\mathbb{Q}}(I) = card(\mathbb{Z}_K/I)$.*

That is, the number of elements in the quotient ring of $\mathbb{Z}_K$ and I is equal to the norm. The proof of this can be found in Theorem 9.1.3 from [AW03].
So far we have two definitions of the norm, the norm of elements and the norm of ideals. These two definitions are not unrelated, in fact we have the following connection.

Theorem 2.2.7. *Let $\alpha \in \mathbb{Z}_K$, then $\mathcal{N}_{K|\mathbb{Q}}(\langle\alpha\rangle) = |\mathcal{N}_{K|\mathbb{Q}}(\alpha)|$.*

Proof from Theorem 9.2.5 in [AW03]: The ideal $\langle\alpha\rangle$ has the basis $\{\omega_1\alpha, \ldots, \omega_n\alpha\}$. Now from this we can consider the discriminant of this basis

$$\delta(\alpha_1, \ldots, \alpha_n) = \det\left(\begin{bmatrix} \sigma_1(\alpha\omega_1) & \sigma_1(\alpha\omega_2) & \ldots & \sigma_1(\alpha\omega_n) \\ \sigma_2(\alpha\omega_1) & \sigma_2(\alpha\omega_2) & \ldots & \sigma_2(\alpha\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha\omega_1) & \sigma_n(\alpha\omega_2) & \ldots & \sigma_n(\alpha\omega_n) \end{bmatrix}\right)^2 \tag{10}$$

From this we can extra the embedding of α to get the following

$$\begin{aligned} \delta(\alpha_1, \ldots, \alpha_n) &= \det\left(\begin{bmatrix} \sigma_1(\alpha) & 0 & \ldots & 0 \\ 0 & \sigma_2(\alpha) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \sigma_1(\alpha) \end{bmatrix} \begin{bmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \ldots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \ldots & \sigma_2(\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \sigma_n(\omega_2) & \ldots & \sigma_n(\omega_n) \end{bmatrix}\right)^2 \\ &= (\sigma_1(\alpha)\sigma_2(\alpha)\ldots\sigma_n(\alpha))^2\delta(K) \end{aligned} \tag{11}$$

From Lemma 2.2.5 we obtain that $\delta(\langle\alpha\rangle) = \mathcal{N}_{K|\mathbb{Q}}(\alpha)^2\delta(K)$. Thus, from the definition we obtain that $\mathcal{N}_{K|\mathbb{Q}}(\langle\alpha\rangle) = |\mathcal{N}_{K|\mathbb{Q}}(\alpha)|$. □
From this connection we will now prove the following useful theorem.

Theorem 2.2.8. *There are only a finite number of ideals in $\mathbb{Z}_K$ with a given norm and every ideal in $\mathbb{Z}_K$ has integer norm.*

Proof based on proof of Theorem 5.12 in [ST79]: Let I be an ideal of $\mathbb{Z}_K$ From Theorem 2.2.6 we know that $\mathcal{N}_{K|\mathbb{Q}}(I) = \text{card}(\mathbb{Z}_K/I)$. Now since every element $x \in \mathbb{Z}_K$ has order dividing $\mathcal{N}_{K|\mathbb{Q}}(I)$ we know that $\mathcal{N}_{K|\mathbb{Q}}(I)x \in I$. Thus, we know that $\mathcal{N}_{K|\mathbb{Q}}(I) \in I$ as $x = 1 \in \mathbb{Z}_K$. From Theorem 2.3.1 we know that every ideal has a unique factorisation into prime ideals. This implies that there are a finite number of divisors of I (as there is only a finite number of elements in the factorisation). If $a \in I$ then $\langle a\rangle$ is contained in I implying I divides $\langle a\rangle$. Since there are

a finite number of divisors that means there are a finite number of I that contain $\langle a \rangle$ or $a \in I$. Thus, there is a finite number of ideals in $\mathbb{Z}_K$ with a given norm proving the first half. The norm of an element must be in the image of the map and in $\mathbb{Z}_K$ from the statement earlier. However, there is no $a \notin \mathbb{Q} \backslash \mathbb{Z}$ with $a \in \mathbb{Z}_K$ as the generating polynomial of a would not be integral. Thus, ever ideal in $\mathbb{Z}_K$ has integer norm. □

Finally, we will give a case where the other direction of Lemma 2.1.1 holds.

Lemma 2.2.9. *Every prime ideal in $\mathbb{Z}_K$ is maximal.*

Proof as seen in Theorem 5.3d in [ST79]: Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}_K$ with $0 \neq \alpha \in \mathfrak{p}$. Then $\mathcal{N}_{K|\mathbb{Q}}(\alpha) = \alpha\alpha_2 \dots \alpha_n \in \mathfrak{p}$ from Lemma 2.2.5 where α_i is the conjugate $\sigma_i(\alpha)$ and since $\mathfrak{p}$ is a prime ideal. Thus, $\langle \mathcal{N}_{K|\mathbb{Q}}(\alpha) \rangle \subseteq \mathfrak{p}$ so we see that $\mathbb{Z}_K/\mathfrak{p}$ is a quotient ring of $\mathbb{Z}_K/\langle \mathcal{N}_{K|\mathbb{Q}}(\alpha) \rangle \mathbb{Z}_K$. This group will be of size $[\mathbb{Z}_K : \mathfrak{p}]$ which is finite so every element will have finite order. $\mathbb{Z}_K/\mathfrak{p}$ is finite, and it will have no zero divisors. This is because otherwise there are elements $a, b \in \mathbb{Z}_K/\mathfrak{p}$ such that $ab \in \mathfrak{p}$ which would mean that $\mathfrak{p}$ is not a prime ideal. Since $\mathfrak{p} \subset \mathbb{Z}_K$ we have that there are at least two elements with one nonzero. Forall $0 \neq x \in \mathbb{Z}_K/\mathfrak{p}$ with $y \in \mathbb{Z}_K/\mathfrak{p}$ we know that xy are distinct as otherwise $xy = xz$ and we have that $x(y - z) = 0$ with $y \neq z$ implying we have zero divisors. Thus, the set of elements xy must be $\mathbb{Z}_K/\mathfrak{p}$ so there must be at least one y such that $xy = 1$. So every element in $\mathbb{Z}_K/\mathfrak{p}$ is a unit, so it is a field. Now suppose $\mathfrak{p} \subset I \subset \mathbb{Z}_K$ with I an ideal then $\{1\} \subset Z_K/I \subset \mathbb{Z}_K/\mathfrak{p}$ with $\mathbb{Z}_K/I$ an ideal. However, $\mathbb{Z}_K/\mathfrak{p}$ is a field, so it has no proper ideals, a contradiction. Thus, there is no I such that $\mathfrak{p} \subset I \subset \mathbb{Z}_K$ so $\mathfrak{p}$ is maximal. □

2.3 Unique Factorisation of Ideals

In the integers $\mathbb{Z}$ there is the well known concept of factorisation where any two numbers can be factored uniquely into prime numbers. For example, it is known that 6 factors uniquely into 2×3. It is therefore natural to ask if we can factor elements in the ring of integers $\mathbb{Z}_K$. In the general case this is not true as if we consider the number ring $K = \mathbb{Q}[x]/\langle x^2 - 5 \rangle$ where there is the unit $(1 + \sqrt{5})/2$ any element $\alpha \in \mathbb{Z}_K$ can factor into $\alpha \times (1 + \sqrt{5})/2 \times (1 - \sqrt{5})/2$. Thus, we see that if we have non-trivial units that there is no longer unique factorisation. However, the following can be said about factorisation in $\mathbb{Z}_K$.

Theorem 2.3.1 (Unique Factorisation of ideals in $\mathbb{Z}_K$)**.** *Every proper ideal of $\mathbb{Z}_K$ can be written as a product of prime ideals, uniquely up to the order of the factors.*

It gets around the problem of divisibility by a unit as the ideal of a unit is the ring of integers and so is not included in the ideal factorisation. So we can factor elements by factoring the ideal generated by the element.

To prove Theorem 2.3.1 we need a few preliminaries. Since we are considering factorisation it is useful to consider what an inverse of an ideal actually is.

Definition 2.3.1. The inverse of an ideal I is defined to be $I^{-1} = \{x \in K | xI \subseteq \mathbb{Z}_K\}$.

From this definition we can observe the following.

Lemma 2.3.2. *If $I \subseteq \mathfrak{p} \subset \mathbb{Z}_K$ with I an ideal and $\mathfrak{p}$ a prime ideal then $\mathbb{Z}_K \subseteq \mathfrak{p}^{-1} \subseteq I^{-1}$*

Proof: Suppose $\mathfrak{p}^{-1} \nsubseteq I^{-1}$ then there exists $x \in \mathfrak{p}^{-1}$ such that $x\mathfrak{p} \subseteq \mathbb{Z}_K$ with $xI \nsubseteq \mathbb{Z}_K$. This implies there exists $a \in I$ with $xa \notin \mathbb{Z}_K$ but since $a \in \mathfrak{p}$ we see that $x\mathfrak{p} \nsubseteq \mathbb{Z}_K$ a contradiction. Thus, $\mathfrak{p}^{-1} \subseteq I^{-1}$. □
Another property of inverses of ideals is

Lemma 2.3.3. *For every ideal $I \neq 0$, $II^{-1} = \mathbb{Z}_K$.*

This property is similar to the property that an element times its inverse is the same as the multiplicative identity element (the ideal generated by the identity element is $\langle 1 \rangle = \mathbb{Z}_K$). Before we prove this lemma we need the following observation about ideals

Lemma 2.3.4. *If I is a non-zero ideal and $IS \subseteq I$ for any subset $S \subseteq K$ then $S \subset \mathbb{Z}_K$.*

Proof from Theorem 5.5 part (iv) in [ST79]: Let $\alpha \in S$. From Lemma 2.1.6 we know that $\mathbb{Z}_K$ is noetherian so we can write $I = \langle a_1, \ldots, a_m \rangle$, where we can write not all a_i as zero. This implies that $I\alpha \subseteq I$ gives

$$a_1\alpha = b_{11}a_1 + \cdots + b_{1m}a_m \tag{12}$$

$$\vdots \tag{13}$$

$$a_m\alpha = b_{m1}a_1 + \cdots + b_{mm}a_m \tag{14}$$

with $b_{ij} \in \mathbb{Z}_K$. From this we can construct the set of equations

$$(b_{11} - \alpha)x_1 + \cdots + b_{1m}x_m = 0 \tag{15}$$

$$\vdots \tag{16}$$

$$b_{m1}x_1 + \cdots + (b_{mm} - \alpha)x_m = 0 \tag{17}$$

which can give use a non-zero solution $x_1 = a_1, \ldots, x_m = a_m$. Taking the determinant the matrix formed by this system of equations we obtain a polynomial equation with coefficients in $\mathbb{Z}_K$ for every α. Thus, we obtain that $\alpha \in \mathbb{Z}_K$ implying $S \subseteq \mathbb{Z}_K$. □

Now to prove Lemma 2.3.3 based on Theorem 5.5 part (vi) in [ST79]: Consider the case when I is a maximal ideal. Then from definition $I \subseteq II^{-1} \subseteq \mathbb{Z}_K$. However, since I is maximal we have that II^{-1} must either be $\mathbb{Z}_K$ or I. $II^{-1} \neq I$ as the contrary implies from Lemma 2.3.4 that $I^{-1} \subseteq \mathbb{Z}_K$ which is a contradiction to Lemma 2.3.2. Thus, $II^{-1} = \mathbb{Z}_K$ if I is a maximal ideal. Now consider the case that I is not a maximal ideal and select I such that $II^{-1} \neq \mathbb{Z}_K$ where there is no $\mathfrak{b} \subset \mathbb{Z}_K$ where $I \subset \mathfrak{b}$ and $\mathfrak{b}\mathfrak{b}^{-1} \neq \mathbb{Z}_K$. That is, consider I maximal to the condition that it is not contained in any ideal which when multiplied by together is the ring of integers. Then $I \subseteq \mathfrak{p}$ where $\mathfrak{p}$ is maximal. From Lemma 2.3.2 we have that $\mathbb{Z}_K \subseteq \mathfrak{p}^{-1} \subseteq I$. Thus, $I \subseteq I\mathfrak{p}^{-1} \subseteq II^{-1} \subseteq \mathbb{Z}_K$ as $\mathfrak{p}\mathfrak{p}^{-1}$ must be contained within $\mathbb{Z}_K$ by definition and $I \subset \mathfrak{p}$. From this we can observe that $I\mathfrak{p}^{-1} \subseteq \mathbb{Z}_K$ implies that it is an ideal. Suppose that $I = I\mathfrak{p}^{-1}$ then by Lemma 2.3.4 we have that $\mathfrak{p}^{-1} \subseteq \mathbb{Z}_K$ a contradiction to Lemma 2.3.2 so $I \subset I\mathfrak{p}^{-1}$. Now by our maximality condition on I we have that $I\mathfrak{p}^{-1}(I\mathfrak{p}^{-1})^{-1} = \mathbb{Z}_K$. This means that $\mathfrak{p}^{-1}(I\mathfrak{p}^{-1}) \subseteq I^{-1}$. Then, $\mathbb{Z}_K = I\mathfrak{p}^{-1}(I\mathfrak{p}^{-1})^{-1} \subseteq II^{-1} \subseteq \mathbb{Z}_K$ a contradiction and proving the statement. □

Note that we say that an ideal I divides the ideal A when there exists B such that $A = IB$. This condition is equivalent to $A \subseteq I$.

We will now finally prove Theorem 2.3.1 which is based on the proof to Theorem 5.5 in [ST79]: Suppose that an ideal $\mathfrak{a}$ is not a product of prime ideals and choose $\mathfrak{a}$ such that it is maximal subject to this condition. That is there is no $\mathfrak{b}$ with $\mathfrak{a} \subset \mathfrak{b} \subset \mathbb{Z}_K$ that is also not a product of prime ideals. Then it is not prime but it will be contained in some maximal prime ideal $\mathfrak{p}$. Now $\mathfrak{a}\mathfrak{p}^{-1} \nsubseteq \mathfrak{a}$ as from Lemma 2.3.4 we see that this implies $\mathfrak{p}^{-1} \subseteq \mathbb{Z}_K$ a contradiction to Lemma 2.3.2. We also have that $\mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathbb{Z}_K$ as $\mathfrak{p}\mathfrak{p}^{-1}$ must be contained within $\mathbb{Z}_K$ by definition and $\mathfrak{a} \subset \mathfrak{p}$. Thus, $\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathbb{Z}_K$. Now by maximality condition of $\mathfrak{a}$ we obtain that $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_2 \ldots \mathfrak{p}_r$. Hence, we obtain that $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_2 \ldots \mathfrak{p}_r$ proving every ideal of $\mathbb{Z}_K$ can be written as a product of prime ideals. Thus, now it suffices to show that this factorisation is unique. From the definition $\mathfrak{p}$ dividing $\mathfrak{a}\mathfrak{b}$ where $\mathfrak{a}$ and $\mathfrak{b}$ are ideals implies that $\mathfrak{p}$ divides $\mathfrak{a}$ or $\mathfrak{b}$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s$ be prime ideals. Suppose there is the factorisation $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_r = \mathfrak{q}_1 \ldots \mathfrak{q}_s$.

The norm of a prime ideal will be a prime number as from Theorem 2.2.6 we know that $\mathcal{N}_{N|\mathbb{Q}}(\mathfrak{p}) = \text{card}(\mathbb{Z}_K/\mathfrak{p})$ and if the cardinality is not prime then there is a subgroup in $\mathbb{Z}_K/\mathfrak{p}$ implying that there is another proper ideal containing $\mathfrak{p}$ which is a contradiction to Lemma 2.2.9. The norm of $\mathfrak{p}_1 \dots \mathfrak{p}_r$ and $\mathfrak{q}_1 \dots \mathfrak{q}_s$ will be the same and thus, we can expect to have the same prime numbers in the norm however, this requires that $r = s$ as otherwise there is an unaccounted for prime number in the norm. Let k be the number of factors. Now let $k = 1$ then $\mathfrak{a} = \mathfrak{p}_1 = \mathfrak{q}_1$ and clearly there is only one factorisation. Now suppose that factorisation is unique for $k-1$ factors. Then $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_k = \mathfrak{q}_1 \dots \mathfrak{q}_k$. For each $\mathfrak{p}_k$ they must divide at least one of $\mathfrak{q}_j$ so multiplying each side by $\mathfrak{p}_k^{-1}$ we can cancel each out (as by Lemma 2.3.3). This relabeling this obtains $\mathfrak{p}_1 \dots \mathfrak{p}_{k-1} = \mathfrak{q}_1 \dots \mathfrak{p}_{k-1}$ which is unique from the assumption. Thus, by induction, ideal factorisation into prime ideals is unique. □

Now that we have proven there is unique factorisation of ideals we can consider practical uses of this and data structures which will be useful later on. We define a set of primes $\mathfrak{p}_1, \dots, \mathfrak{p}_k \subseteq \mathbb{Z}_K$ a factor base and say that α factors over the factor base if all prime ideal factors of $\langle \alpha \rangle$ are contained in the factor base. For practicality, we define the following valuation:

Definition 2.3.2 (Valuations)**.** A *valuation* of $\langle \alpha \rangle = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k}$ in some field F where $\mathfrak{p}$ is a prime ideal in F is defined as $\text{val}_{\mathfrak{p}_i}(\alpha) = e_i$ for some $i \in \{1, \dots, k\}$.

This leads to a very useful way to store ideals as valuations over a factorbase as a vector. For example the element $14 \in \mathbb{Z}$ factors over the factor base $2, 3, 5, 7$ as $14 = 2^1 \times 3^0 \times 5^0 \times 7^1$ so we would store this as $(1, 0, 0, 1)$ over this factor base. As we see in the example above this definition of valuations also works for prime numbers in $\mathbb{Z}$.

Lemma 2.3.5. *If $\alpha \in K$ has a valuation of at least zero over all primes ideals then it lies in $\mathbb{Z}_K$. Moreover, if the valuation is exactly zero over all prime ideals then it is a unit.*

Proof: If α has a non-negative valuation over all the prime ideals then for the factorisation $\langle \alpha \rangle = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_k^{e_k}$ the set $e_1, \dots, e_k$ is all positive. If e_i is non-negative then $\mathfrak{p}_i^{e_i} \subseteq \mathbb{Z}_K$ as $\mathfrak{p}_i \in \mathbb{Z}_K$, thus, every prime ideal that $\langle \alpha \rangle$ factors into is in $\mathbb{Z}_K$ so $\langle a \rangle \subseteq \mathbb{Z}_K$. Since $a \in \langle \alpha \rangle$ this implies that $a \in \mathbb{Z}_K$. If α has a valuation of zero over all prime ideals then then α is contained in no prime ideals. By Lemma 2.1.1 all maximal ideals are prime. This implies that $\langle \alpha \rangle$ is not contained in any ideal and is not maximal. This implies $\langle a \rangle = \mathbb{Z}_K$ which requires α to be a unit. □

Now there are an infinite number of prime ideals for the ring $\mathbb{Z}_K$ (consider the prime ideals above the ideals $\langle p \rangle$ where p is a prime number). Thus, it is practical to only consider elements who have valuations over specific prime ideals (consider bounding the norm of prime ideals). This definition of valuation provides the following useful definition.

Definition 2.3.3 (Unramified)**.** A prime p is *ramified* over a factor base if $\text{val}_{\mathfrak{p}}(\langle p \rangle) > 1$ for some prime ideal $\mathfrak{p}$, otherwise it is considered unramified.

For example, consider the prime 2 in $\mathbb{Z}$ and let $L = \mathbb{Q}/\langle x^3 + x^2 + 5x - 16 \rangle$ which factors into $2\mathbb{Z}_K = \mathfrak{p}_2\mathfrak{p}_4 = (2, \theta) \cdot (2, \theta^2 + \theta + 1)$ so 2 would be unramified. Now consider 3 which factors into $3\mathbb{Z}_K = \mathfrak{p}_3^2\mathfrak{q}_3 = (2, \theta + 1)^2 \cdot (3, \theta - 1)$ so it would be ramified.

2.4 Minkowski's Theorem

Minkowski's Theorem was proved by Hermann Minkowski in 1889 and is used in many algebraic number theory results. The nature of the proof is geometric in nature. In particular, it can be used in the proof of Dirichlet's Unit Theorem and for proving that the class group is finite. From these it also provides the Minkowski constant which provides a useful bound. Before we get into the theorem we need to cover a number of geometric concepts. A *lattice* L is a subgroup

of F^n generated by the $\mathbb{Z}$-basis $e_1, \ldots, e_m$. A lattice has a *fundamental-domain* defined to be all the elements $\sum a_i e_i$ with $a_i \in \mathbb{R}$ with $0 \leq a_i < 1$. A subset X of F^n is convex if any point on a straight line from x to y with $x, y \in X$ also are in X. Our subset X is symmetric if $x \in X$ implies $-x \in X$. We define the volume of $X \subseteq \mathbb{R}^n$ as $\int_X dx_1 \ldots dx_n$. The circle group $\mathbf{S}$ is the set $\{z \in \mathbb{C} | \ |z| = 1\}$ which is a group under multiplication. A n dimensional torus is a product of n circle groups. For example a 2 dimensional torus can be considered a mapping from points in a square to points on the surface of a donut. The following lemma connects some of these concepts.

Lemma 2.4.1. *If L is an n-dimensional lattice in the vector space $\mathbb{R}^n$ then $\mathbb{R}^n/L$ is isomorphic to the n-dimensional torus $\boldsymbol{T}^n$.*

Proof based on Theorem 6.4 in [ST79]: Let $\{e_1, \ldots, e_n\}$ be a generating set for L. As the set of vectors $\{e_1, \ldots, e_n\}$ are linearly independent, they form a $\mathbb{R}$-basis for $\mathbb{R}^n$. Consider the mapping $\phi : \mathbb{R}^n/L \to T^n, a_1 e_1 + \cdots + a_n e_n \mapsto (e^{2\pi i a_1}, \ldots, e^{2\pi i a_n})$ where $0 \leq a_1, \ldots, a_n < 1$. Now since we are going from an additive group to a multiplicative group we need to show that $\phi(a+b) = \phi(a)\phi(b)$ for all $a, b \in \mathbb{R}^n$.

$$\begin{aligned}
\phi(a+b) &= \phi((a_1+b_1)e_1 + \cdots + (a_n+b_n)e_n) \\
&= (e^{2\pi i(a_1+b_1)}, \ldots, e^{2\pi i(a_n+b_n)}) \\
&= (e^{2\pi i a_1} e^{2\pi i b_1}, \ldots, e^{2\pi i a_n} e^{2\pi i b_n}) \\
&= (e^{2\pi i a_1}, \ldots, e^{2\pi i a_n})(e^{2\pi i b_1}, \ldots, e^{2\pi i b_n}) \\
&= \phi(a_1 e_1 + \cdots + a_n e_n)\phi(b_1 e_1 + \cdots + b_n e_n) \\
&= \phi(a)\phi(b)
\end{aligned}$$

Thus, we see that ϕ is a homomorphism. Each element in $\mathbb{R}^n/L$ will map uniquely to an element in T^n as $0 \leq a_i < 1$ and ϕ maps onto T^n. Thus, ϕ is an isomorphism from $\mathbb{R}^n/L$ to T^n and thus, R^n/L is isomorphic to T^n. □

Using the mapping ϕ as defined in Lemma 2.4.1 we can see that we can define the volume of a subset X of a torus as $\text{vol}(X) = \text{vol}(\phi^{-1}(X))$ as $\phi^{-1}(X) \subseteq T$. Now consider Minkowski's Theorem.

Theorem 2.4.2 (Minkowski's Theorem)**.** *Let L be an n-dimensional lattice in $\mathbb{R}^n$ with fundamental domain T, and let X be a bounded symmetric convex subset of $\mathbb{R}^n$. If vol$(X) > 2^n$vol(T) then X contains a non-zero point in L.*

Proof is based on Theorem 7.1 in [ST79]: Double the size of L to obtain a lattice $2L$ with fundamental domain $2T$. The volume of this will be $2^n\text{vol}(T)$ as there are n elements in T and we are doubling the size of the generating vectors. Consider the torus $\mathbf{T}^n \cong \mathbb{R}^n/2L$, then we see that $\text{vol}(\mathbf{T}^n) = \text{vol}(2T) = 2^n\text{vol}(T)$. Now the mapping $\psi : \mathbb{R}^n \to \mathbf{T}^n$ where ψ is the extension of the mapping ϕ in Lemma 2.4.1 by letting $a_1 \in \mathbb{R}$. This mapping cannot preserve the volume of X as $\text{vol}(X) > 2^n\text{vol}(T) = \text{vol}(\mathbf{T}^n)$, thus, $\text{vol}(\psi(X)) \neq \text{vol}(X)$. Let us assume the mapping $\psi : X \to \mathbf{T}^n$ is injective. Since X is bounded we see that it shares elements with a finite number of sets $T + l$ with $l \in L$. Let $X_l = X \cap (T + l)$. From this one can observe that $X = X_{l_1} \cup \cdots \cup x_{l_n}$ where $\{l_1, \ldots, l_n\}$ is the finite set of l such that X_l is non-empty. Now for each element $l_i \in \{l_1, \ldots, l_n\}$ define $Y_{l_i} = X_{l_i} - l_i$ with $Y_{l_i} \subset T$. From our assumption these Y_{l_i} must be disjoint which implies that $\text{vol}(\cup Y_{l_i}) = \sum \text{vol}(Y_{l_i})$. Now $\text{vol}(X_{l_i}) = \text{vol}(Y_{l_i})$ for all i

and $\psi(X_{l_i}) = \phi(Y_{l_i})$. Now let us compute the following

$$\begin{aligned}\text{vol}(\psi(X)) &= \text{vol}(\psi(\cup X_{l_i})) \\ &= \text{vol}(\cup Y_{l_i}) \\ &= \sum \text{vol}(Y_{l_i}) \\ &= \sum \text{vol}(X_{l_i}) \\ &= \text{vol}(X)\end{aligned}$$

However, we have already seen that $\text{vol}(\psi(X)) \neq \text{vol}(X)$ thus, ψ is not injective. Hence, there exists $x_1, x_2 \in X$ with $x_1 \neq x_2$ such that $\psi(x_1) = \psi(x_2)$. Thus, we can write $x_1 = al + \phi(x_1)$ and $x_2 = bl + \phi(x_2)$ with $a, b \in \mathbb{Z}$ which results in $x_1 - x_2 = (a-b)l \in 2L$. Since X is symmetric and $x_2 \in X$ we also have that $-x_2 \in X$ and from of X concavity we have that $\frac{1}{2}x_1 + \frac{1}{2}(-x_2) \in X$. It follows from $x_1 - x_2 \in 2L$ that $\frac{1}{2}(x_1 - x_2) \in L$ hence $\frac{1}{2}(x_1 - x_2) \in L \cap X$ which gives us our required observation. □

Now to apply Minkowski's Theorem to number fields we need to define a lattice for our number field. To do this let us consider $\mathbb{Z}_K$ which has a $\mathbb{Z}$-basis $\{\omega_1, \ldots, \omega_n\}$ from Lemma 2.1.5 and let $\Phi : Z_K \to \mathbb{C}^n$ where $\Phi : x \to (\sigma_1(x), \ldots, \sigma_n(x))$. It can be seen that $\Phi(\mathbb{Z}_K)$ forms a lattice in $\mathbb{C}^n$ with $\mathbb{C}$-basis vectors $\Phi(\omega_1), \ldots, \Phi(\omega_n)$. This leads to the following theorem

Lemma 2.4.3. *The volume of the fundamental domain of an ideal I over the lattice $\Phi(I)$ is $\mathcal{N}_{K|\mathbb{Q}}(I)\sqrt{|\Delta|}$ where Δ is the determinant of $\mathbb{Z}_K$.*

Proof: Let $\{\omega_1, \ldots, \omega_n\}$ be a $\mathbb{Z}$-basis for I and let M be the $n \times n$ matrix where $M_{ij} = \sigma_i(\omega_j)$. Now the volume of the fundamental domain of this is equivalent to taking the square of the determinant of M. However, from our definition of a norm of an ideal we see that $\det(M)^2 = \mathcal{N}_{K|\mathbb{Q}}(I)\sqrt{|\Delta|}$ proving our statement. □

Another useful mapping is the complex logarithmic embedding which can be used to create a map from multiplicative group of a number field to a lattice allowing us to use Minkowski's Theorem. The complex logarithmic embedding is defined as follows

$$L_C(\alpha) = \left(n_i \left(\ln(\sigma_i(\alpha)) - \frac{\ln(\mathcal{N}_{K/\mathbb{Q}}(\alpha))}{n} \right) \right)_{1 \leq i \leq r_1 + r_2} \tag{18}$$

where $n_i = 1$ for $1 \leq i \leq r_1$ and $n_i = 2$ for $r_1 + 1 \leq i \leq r_1 + r_2$. One can observe from this is the following

Lemma 2.4.4. *The complex embedding of 1 is zero.*

Proof: For all embeddings we have that $\sigma_i(1) = 1$ and the norm of 1 is 1. Thus, clearly from this $L_C(1) = 0$. □

An application of Theorem 2.4.2 is in showing that every ideal is equivalent to an ideal with bounded norm where the bound is called Minkowski's Constant.

Theorem 2.4.5 (Minkowski's Constant)**.** *Every ideal class of the class group H of K contains an integral ideal of norm not exceeding Minkowski's constant given by*

$$M_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|\Delta|} \tag{19}$$

where Δ is the discriminant of K.

Proof as seen in Theorem 5.8 in [Ste20]: Let $I \subset K$ be an ideal of K and X_t be a box consisting of elements $\mathbf{x} = (\sigma_1(x), \ldots, \sigma_n(x))$ where

$$\sum_{n}^{i=1} \sigma_i(x) \leq t \tag{20}$$

This box has volume $\text{vol}(X_t) = 2^{r_1}\pi^{r_2}\frac{t^n}{n!}$ to which we are going to prove with induction. We can simplify our system by only considering pairs of complex embeddings and instead show that $\text{vol}(X_t) = 2^{r_1}(\frac{\pi}{2})^{r_2}\frac{t^n}{n!}$. The reason there is a difference is that we are not counting the conjugates but the conjugate. Let $V_{r_1,r_2}(t)$ be the volume of the box X_t with r_1 and r_2 being the number of real embeddings and number of pairs of complex embeddings respectively. Now $V_{1,0}(t) = 2t$ as $X_t = [-t, t]$ and $V_{0,1}(t) = \pi t^2/4$ as $X_t = \{|\sigma(x)| \leq t/2\}$. Now assume that the $V_{r_1,r_2} = 2^{r_1}(\frac{\pi}{2})^{r_2}\frac{t^n}{n!}$. Then

$$\begin{aligned}
V_{r_1+1,r_2} &= \int_{x=-t}^{t} V_{r_1,r_2}(t - |x|)dx \\
&= \int_{x=-t}^{t} 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{(t-|x|)^n}{n!}dx \\
&= 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} 2\int_{x=0}^{t}\frac{(t-x)^n}{n!}dx \\
&= 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} 2\left[-\frac{(t-x)^{n+1}}{n!(n+1)}\right]_{x=0}^{t} \\
&= 2^{(r_1+1)}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^{n+1}}{(n+1)!}
\end{aligned}$$

Let $z = \rho e^{i\theta}$, then

$$\begin{aligned}
V_{r_1,r_2+1} &= \int_{\theta=0}^{2\pi}\int_{\rho=0}^{t} V_{r_1,r_2}(t-2\rho)\rho d\theta d\rho \\
&= 2\pi\int_{\rho=0}^{t} 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{(t-2\rho)^n}{n!}\rho d\rho \\
&= 2^{r_1}2\pi\left(\frac{\pi}{2}\right)^{r_2}\int_{\rho=0}^{t}\frac{(t-2\rho)^n}{n!}\rho d\rho \\
&= 2^{r_1}2\pi\left(\frac{\pi}{2}\right)^{r_2}\left[\frac{(t+2x)^{n+1}(-t+2(1+n)x)}{(4(n+2)!}\right]_{\rho=0}^{t/2} \\
&= 2^{r_1}2\pi\left(\frac{\pi}{2}\right)^{r_2}\frac{t^{n+1}t}{4(n+2)!} \\
&= 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2+1}\frac{t^{n+2}}{(n+2)!}
\end{aligned}$$

Thus, by induction $\text{vol}(X_t) = 2^{r_1}(\frac{\pi}{2})^{r_2}\frac{t^n}{n!}$. And from our earlier assumption we see $\text{vol}(X_t) = 2^{r_1}\pi^s\frac{t^n}{n!}$. From Lemma 2.4.3 we know that the fundamental domain of the lattice $\Phi(I)$ can be given by $\mathcal{N}_{K|\mathbb{Q}}(I)\sqrt{|\Delta|}$. Now from Theorem 2.4.2 we have that this set X_t will contain an x such that $\psi(x) \in \phi(I) \cap X_t$ if $\text{vol}(X) \geq 2^n\mathcal{N}_{K|\mathbb{Q}}(I)\sqrt{|\Delta|}$ Now let us choose t such that $\text{vol}(X_t) = 2^n\mathcal{N}_{K|\mathbb{Q}}(I)\sqrt{|\Delta|}$, thus

$$\begin{aligned}
2^{r_1}(\frac{\pi}{2})^{r_2}\frac{t^n}{n!} = 2^{r_1+2r_2}\mathcal{N}_{K|\mathbb{Q}}(I)\sqrt{|\Delta|} \\
\Rightarrow \quad t^n \geq n!\left(\frac{4}{\pi}\right)^{r_2}\mathcal{N}_{K|\mathbb{Q}}(I)\sqrt{|\Delta|}
\end{aligned} \tag{21}$$

Now the norm of the element x will be $|\mathcal{N}_{K|\mathbb{Q}}(x)| = \prod_{i=1}^{n}|\sigma(x)|$. Now $(\prod_{i=1}^{n}|\sigma(x)|)^{1/n}$ will not exceed $\frac{1}{n}\sum_{i=1}^{n}|\sigma(x)|$ from Equation 20. Thus, there is an element $x \in I \cap \mathbb{Z}_K$ with norm

$$|\mathcal{N}_{K|\mathbb{Q}}(x)| = \prod_{i=1}^{n}|\sigma(x)| \leq (\frac{1}{n}\sum_{i=1}^{n}|\sigma(x)|)^n \leq t^n/n^n = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\mathcal{N}_{K|\mathbb{Q}}(I)\sqrt{|\Delta|}. \tag{22}$$

If I is invertible then we can create the ideal xI^{-1} which will be contained in the equivalence class $[I^{-1}]$ with norm $\mathcal{N}_{K|\mathbb{Q}}(xI^{-1}) = |\mathcal{N}_{K|\mathbb{Q}}(x)|\mathcal{N}_{K|\mathbb{Q}}(I^{-1}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\mathcal{N}_{K|\mathbb{Q}}(I)\sqrt{|\Delta|}$. Thus, since I was an arbitrary ideal in J_K and every ideal in J_K except the zero ideal is invertible we see that every equivalence class has an ideal as described above. □
One result for this theorem is that it gives us a bound for the prime ideals required to generate the class group as every equivalence class contains an ideal with norm smaller than Minkowski's constant. This does not imply that the bound is necessarily small, in particular consider the field $K = \mathbb{Q}[x]/\langle f(x)\rangle$ where $f(x) = x^8 - 4x^7 + 3x^6 - 2x^5 + 4x^4 - 9x^3 + x^2 + 5x + 2$. This has the discriminant of -77837869969751 which means that $M_K \geq 21202.94071$ and there are 2384 prime numbers below 21202.94. And for larger degree and larger coefficients the discriminant can get even larger. Later we will se that we can consider a smaller bound with the GRH.

2.5 Finitely Generated Abelian Groups

Now we come across the concept of Finitely Generated Abelian groups

Definition 2.5.1 (Finitely Generated Abelian Group (FGAG))**.** A *finitely generated abelian group* is an abelian group G that is generated by a finite number of elements where $\forall a, b \in G$ $ab = ba$.

A trivial example of this is the group $\mathbb{Z} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$ which can be generated by the elements $(1, 0)$ and $(0, 1)$. We will see later that all FGAG are of the same form as the previous example (See Theorem 2.5.4). The unit group and class group are less clear examples of finitely generated abelian groups (which the unit case will be seen in Dirichlet's unit theorem in Theorem 2.6.1). To show the class group is a FGAG consider the following.

Theorem 2.5.1. *The class group is a FGAG.*

Proof (for more see Theorems 5.4 and 5.8 in [Ste20] and Theorem 9.7 in [ST79]): The class group $H = J/P$ is abelian as K is a number field. From Theorem 2.2.8 we know that there is only a finite number of ideals for a given norm and that the norm of these ideals must be integers. From Theorem 2.4.5 we know that every equivalence class contains an integral ideal below a bound. Thus, there is only a finite number of ideals below a given norm and as extension there are only a finite number of equivalence classes. Thus, the group is finite (implying it can be finitely generated) and abelian. □
Earlier we saw that for a number field that we can uniquely describe every element in a number ring as a linear combination of elements. It is the same for a Finitely Generated Abelian Group.

Theorem 2.5.2. *Every FGAG has a $\mathbb{Z}$-basis.*

Before proving this we need to consider the following

Lemma 2.5.3. *If $x_1, \ldots, x_k$ is a generating set for G and integers $c_1, \ldots, c_k \geq 0$ with $\gcd(c_i) = 1$ then there exists a generating set $y_1, \ldots, y_k$ with $y_1 = \sum c_i x_i$.*

Proof as based on Lemma 1.53 in [Mil21]: Let $s = \sum c_i$. Suppose $s = 1$ then that implies that there is one $c_i = 1$ and all others are zero which can be seen as reordering of $x_1, \ldots, x_n$ and is sufficient for the case where $s = 1$. Now suppose $s \geq 2$ implying, without loss of generality, that $c_1 \geq c_2 \geq 0$ and that the theorem is true when $\sum d_i < s$. Consider the generating set $x_1, x_1 + x_2, x_3, \ldots, x_k$ and integers $d_1 = c_1 - c_2, d_2 = c_2, \ldots, d_k = c_k$. From this $\gcd(d_i) = \gcd(c_i) = 1$ and $\sum d_i = (\sum c_i) - c_2 < s$. Thus, from the induction hypothesis we obtain $y_1 = d_1x_1 + d_2(x_1 + x_2) + \cdots + d_kx_k = (c_1x_1 - c_2x_2) + c_2x_1 + c_2x_2 + \cdots + c_kx_k = \sum c_ix_i$. □

Proof of Theorem 2.5.2 based on Theorem 1.54 in [Mil21]: Let k be the size of a generating set of G. Suppose $k = 1$ then we have that $G = \langle x_1\rangle$ so it has a basis. Now suppose that $k > 1$

and that every FGAG generated by fewer than k elements has a $\mathbb{Z}$-basis. Among all elements $x_1, x_2, \ldots, x_k$ in the generating set of size k, choose one element x whose order is minimal and relabel elements so that this element is x_1. If the order of x_1 is one then $x_2, \ldots, x_k$ generate G so G has a $\mathbb{Z}$-basis. Thus, assume the order of x_1 is greater than 1 and suppose that $x_1, x_2, \ldots x_k$ is not a basis. Then there are $a_i \in \mathbb{Z}$ such that $\sum a_i x_i = 0$ where not all $a_i x_i = 0$. We can assume that $0 \leq a_1 \leq \text{ord}(x_1)$ and let $d = \gcd(a_i)$ so that $c_i = a_i/d$. By Lemma 2.5.3 this results in a generating set $y_1, \ldots, y_k$ with $y_i = \sum \frac{a_i}{d} x_i$. However, note that $1 \leq d \leq a_1 \leq \text{ord}(x_1)$ so $dy_1 = d \sum \frac{a_i}{d} x_i = \sum a_i x_i = 0$ so $\text{ord}(y_1) < \text{ord}(x_1)$ a contradiction. Thus, $x_1, \ldots, x_k$ must be a $\mathbb{Z}$-basis. □

This leads us to the following theorem.

Theorem 2.5.4 (Structure theorem for FGAGs)**.** *Let G be a finitely generated abelian group. There exists unique integers $r > 0, m_1, \ldots, m_k \geq 0$ such that $m_1 | m_2 | \ldots | m_k$ and*

$$G \cong \mathbb{Z}^r \times \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{m_k\mathbb{Z}} \tag{23}$$

This tells us that every FGAG is a product of cyclic groups.

Proof as based on Theorem 1.57 in [Mil21]: From Theorem 2.5.2 we know that a FGAG G has a basis $x_1, \ldots, x_k, x_{k+1}, \ldots, x_{k+r}$ where $\text{ord}(x_i) = m_i < \infty$ for $i \in \{1, \ldots, k\}$ and $\text{ord}(x_i) = \infty$ for $i \in \{k+1, \ldots, k+r\}$. Thus, there are r infinite order elements and k finite order elements which gives

$$G \cong \mathbb{Z}^r \times \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{m_k\mathbb{Z}} \tag{24}$$

□

2.6 Dirichlet's Unit Theorem

Now we come to the crucial theorem required to compute units, Dirichlet's unit theorem developed by Peter Dirichlet (who was born in 1805 and died in 1859). This theorem shows that the unit group is a FGAG, and it gives the structure of this into a set of units and a set of roots of unity.

Theorem 2.6.1 (Dirichlet's Unit Theorem)**.** *Let K be an algebraic number field of degree n. Let r_1 be the number of real conjugate fields of K and $2r_2$ the number of complex conjugate fields of K. Then $\mathbb{Z}_K$ contains $r_1 + r_2 - 1$ units $\epsilon_1, \ldots, \epsilon_{r_1+r_2-1}$ such that each unit of $\mathbb{Z}_K$ can be expressed uniquely in the form in the form $\eta\epsilon_1^{\tau_1} \ldots \epsilon_{r_1+r_2-1}^{\tau_{r_1+r_2-1}}$ where η is a root of unity in $\mathbb{Z}_K$ and $\tau_1, dots, \tau_{r_1+r_2-1} \in \mathbb{Z}$.*

These units described in Dirichlet's Unit Theorem are called fundamental units and the theorem tells us how big this set of fundamental units is. For example, by Dirichlet's Unit theorem there is one fundamental unit of $\mathbb{Z}(\sqrt{2})$ being $\{1 + \sqrt{2}\}$ $((1+\sqrt{2})(-1+\sqrt{2}) = -1 + 2 = 1)$. Adding on the roots of unity we obtain that the unit group is $\mathbb{Z}_K^\times =< \pm 1, 1 + \sqrt{2} >$, note that the unit $(1+\sqrt{2})^2 = 3 + 2\sqrt{2}$ would not be a fundamental unit as one cannot generate $1 + \sqrt{2}$ using this unit. There are a number of proofs of Theorem 2.6.1, the proof we will be closely following can be found in Chapter 13 of [AW03]. The basic idea is to generate a set of units where each unit is unique using bounds on the embeddings of elements and by extension on the norm for all but one embedding. Then we show that these units are linearly independent and using bounds on the last embedding we show that every element is generated using these fundamental units and roots of unity. To start let us define some notation that will be useful for the theorem. Let $\alpha = c_1\omega_1 + c_2\omega_2 + \cdots + c_n\omega_n$ with $\alpha \in \mathbb{Z}_K$, $c_1, \ldots, c_n \in \mathbb{Z}$, $\{\omega_1, \ldots, \omega_2\}$ is a basis for $\mathbb{Z}_K$ and $\beta_i(x) = |\sigma_i(x)|$ where $\sigma_i(x)$ is an embedding in K over $\mathbb{Q}$. First we will have to prove a number of lemmas

Lemma 2.6.2. *Let $0 \leq p_i < q_i$ and $p_i, q_i \in \mathbb{Q}$ where $i \in \{1, 2, \ldots, r+s\}$. There exists $a \in K$ such that $p_i < \beta_i(a) < q_i$.*

Let $h_i = \frac{1}{2}(p_i + q_i) \in \mathbb{Q}$ such that $p_i < h_i < q_i$. Now let $h_j = h_{j-r_2}$ where $j \in \{r_1 + r_2 + 1, \ldots, r_1 + 2r_2\}$ and consider a system of n equations where

$$h_i = b_1\sigma_1(\omega_1) + \cdots + b_n\sigma_n(\omega_n). \tag{25}$$

Now let $D = \det(\sigma_j(\omega_j)) \neq 0$ as $D^2 = d(K)$ and the determinant of K is non-zero. Thus, since D is the determinant of the matrix of the system of n equations, there is a unique solution for $b_1, \ldots, b_n \in \mathbb{C}^n$. $h_i \in \mathbb{Q}$ thus, Equation 25 must have a real rational solution. In fact b_i can be considered real coefficients as for the complex embeddings we can simply let $b_j = -b_{j+r_2}$ for $j \in \{r_1 + 1, \ldots, r_1 + r_2\}$ which cancels the imaginary part, thus, $b_1, \ldots, b_n \in \mathbb{R}$. From this let $\delta = \min_{1 \leq i \leq r_1+r_2}(\frac{q_i - p_i}{2Mn})$ where $M = \max_{1 \leq i,j \leq r_1+r_2} |\sigma_i(\omega_j)|$ so that $0 < \delta \leq \frac{q_i - p_i}{2Mn}$ for any $i \in \{1, \ldots, r_1 + r_2\}$. Now choose $c_i \in \mathbb{Q}$ such that $|b_i - c_i| < \delta$ and form $a = c_1\omega_1 + \cdots + c_n\omega_n$. Thus, we obtain

$$\sigma_i(a) - h_i = (c_1 - b_1)\sigma_i(\omega_1) + \cdots + (c_n - b_n)\sigma_i(\omega_n), \quad i = 1, 2, \ldots, n \tag{26}$$

Taking absolute value of Equation 26 we find

$$\begin{aligned} |\sigma_i(a) - h_i| &\leq M(|c_1 - b_1| + \cdots + |c_n - b_n|), \quad i = 1, 2, \ldots, n \\ &< Mn\delta, \quad i = 1, 2, \ldots, n \\ &\leq q_i - p_i, \quad i = 1, 2, \ldots, n \end{aligned}$$

Thus, we see that $h_i - (q_i - p_i)/2 \leq \sigma_i(a) \leq h_i + (q_i - p_i)/2$ which since $h_i = (q_i + p_i)/2$ we obtain that $p_i \leq \beta_i(a) \leq q_i$. □

Lemma 2.6.3. *Let $k \in \mathbb{Z}$ with $k > 0$ and let I be an integral or fractional ideal of $\mathbb{Z}_K$ with $\mathcal{N}_{K|\mathbb{Q}}(I) \leq k^n$. Then there is a non-zero $a \in I$ such that $\beta_i(a) \leq nMk$ $\forall i \in \{1, 2, \ldots, r_1 + r_2\}$ with $M = \max_{1 \leq i,j \leq r_1+r_2} \beta_i(\omega_j)$.*

Proof: Suppose I is integral and let $S = \{b \in \mathbb{Z}_K | b = b_1\omega_1 + \cdots + b_n\omega_n, \quad b_1, \ldots b_n \in \{0, 1, 2, \ldots, k\}\}$. The cardinality of this set will be $(k+1)^n > k^n \geq \mathcal{N}_{K|\mathbb{Q}}(I)$. This means that from Theorem 2.2.6 there are more elements in S than in the quotient group $\mathbb{Z}_K/A$ so we see that there must be two elements in S that map to the same element in $\mathbb{Z}_K/I$ or that there exists $b', b'' \in S$ with $b' \neq b''$ such that $b' + (-b'') \in I$. Let $a = b' - b'' = a_1\omega_1 + \cdots + a_n\omega_n \neq 0$ with $a \in \mathbb{Z}_K$ and $a \in I$. Thus, we have that each a_i satisfies $|a_i| = |b'_i - b''_i| \leq k$ where $i \in \{1, 2, \ldots, r_1 + r_2\}$. From this we obtain the following

$$\begin{aligned} \beta_i(a) &= |\sigma_i(a_1\omega_1 + \cdots + a_n\omega_n)| \\ &= |a_1||\sigma_i(\omega_1)| + \cdots + |a_n||\sigma_i(\omega_n)| \\ &\leq k(M + \cdots + M) \\ &\leq nMk \end{aligned}$$

proving the lemma for the integral case. Now consider when I is fractional and let γ be the common denominator of I. Let $\gamma_1 = \gamma$ and let $\gamma_2, \ldots, \gamma_n$ be the conjugates of γ, that is elements in K such that $m = \mathcal{N}_{K|Q}(\gamma) = \gamma_1\gamma_2 \ldots \gamma_n$ (from Lemma 2.2.5). These elements will be integral as $\gamma \in \mathbb{Z}_K$ from Theorem 2.2.8. From this we obtain $\mathcal{N}_{K|\mathbb{Q}}(\gamma)I = \gamma_2 \ldots \gamma_n(\gamma I) = mA = B$ which is an integral ideal. We know that there will be an element in $b \in B$ such that $\beta_i(b) \leq mkMn$, and since $b \in B$ we have that there exists $a \in I$ such that $am = b$ thus, there exists a $a \in I$ such that $\beta_i(a) = kMn$ for $i \in \{1, 2, \ldots, r_1 + r_2\}$. This proves the lemma for the fractional case. □

Lemma 2.6.4. *For each $j \in \{1, 2, \ldots, r_1 + r_2 - 1\}$ with $r_1 + r_2 \geq 2$ there exists an unit $\epsilon_j \in \mathbb{Z}_K$ such that*

$$\begin{aligned} &\beta_i(\epsilon_j) < 1, \quad i = 1, 2, \ldots, r_1 + r_2, i \neq j \\ &\beta_j(\epsilon_j) > 1. \end{aligned}$$

Proof: Let $a \in L$ be an element unique for each ϵ_j such that if $j \in \{1, 2, \ldots, r_1\}$ with Lemma 2.6.2 we have

$$\begin{aligned} B < \beta_i(a) < 2^{1/n}B, \quad i = 1, 2, \ldots, r_1 + r_2, i \neq j \\ \frac{1}{2B^{n-1}} < \beta_i(a) < \frac{1}{2^{1-1/n}B^{n-1}}, \quad i = j \end{aligned} \tag{27}$$

and if $j \in \{r + 1, \ldots, r_1 + r_2 - 1\}$ then

$$\begin{aligned} B < \beta_i(a) < 2^{1/n}B, \quad i = 1, 2, \ldots, r_1 + r_2, i \neq j \\ \frac{1}{2^{1/2}B^{(n-2)/2}} < \beta_i(a) < \frac{1}{2^{1/2-1/n}B^{(n-2)/2}}, \quad i = j \end{aligned} \tag{28}$$

Either of these cases has $\beta_i(a) > B$ where $i = 1, 2, \ldots, r_1 + r_2, i \neq j$. From Lemma 2.2.5 we know that $\mathcal{N}_{K|\mathbb{Q}}(a) = \prod_{i=1}^{n} \sigma_i(a)$ and it can be clearly seen that

$$|\mathcal{N}_{K|\mathbb{Q}}(a)| = \prod_{i=1}^{r_1+r_2} \beta_i(a)^{d_i} \tag{29}$$

where $d_i = 1$ if σ_i is real and $d_i = 2$ if σ_i is complex. From this we can compute the norm of a using Equation 27 to be

$$\begin{aligned} \frac{1}{2B^{n-1}} B^r (B^{2s}) < &|\mathcal{N}_{K|\mathbb{Q}}(a)| < \frac{1}{2^{1-1/n}B^{n-1}} (2^{1/n}B)^{r-1} (2^{1/n}B)^{2s} \\ \Rightarrow \quad \frac{1}{2} < &|\mathcal{N}_{K|\mathbb{Q}}(a)| < 1 \end{aligned} \tag{30}$$

when $j \in \{1, 2, \ldots, r_1\}$ and using Equation 28

$$\begin{aligned} \frac{1}{2^{1/2}B^{(n-2)/2}} B^{r-1} (B^{2(s-1)}) < &|\mathcal{N}_{K|\mathbb{Q}}(a)| < \frac{1}{2^{1/2-1/n}B^{(n-2)/2}} (2^{1/n}B)^{r} (2^{1/n}B)^{2(s-1)} \\ \Rightarrow \quad \frac{1}{2} < &|\mathcal{N}_{K|\mathbb{Q}}(a)| < 1 \end{aligned} \tag{31}$$

when $j \in \{r_1 + 1, \ldots, r_1 + r_2 - 1\}$. Let $\epsilon \in \mathbb{Z}_K^{\times}$ be a unit and let $I = \langle a \rangle$. Now from Lemma 2.6.3 we know that there exists $b = qa \in I$ such that $\beta_i(b) \leq nM, i = 1, 2, \ldots, r + s$. From this we can obtain the following

$$\begin{aligned} \frac{\mathcal{N}_{K|\mathbb{Q}}(\langle q \rangle)}{2} &< \mathcal{N}_{K|\mathbb{Q}}(\langle q \rangle) \mathcal{N}_{K|\mathbb{Q}}(\langle a \rangle) \\ &= \mathcal{N}_{K|\mathbb{Q}}(\langle b \rangle) \\ &\leq \prod_{i=1}^{r+s} \beta_i(b)_i^d \\ &\leq (nM)^n \end{aligned} \tag{32}$$

Which shows that $\mathcal{N}_{K|\mathbb{Q}}(\langle q \rangle) = \mathcal{N}_{K|\mathbb{Q}}(q) < 2(nM)^n$ hence there are only finitely many principal ideals $\langle q \rangle$ below a bounded norm as there are only finitely many $q \in \mathbb{Z}_K$ with norm smaller than $2(nM)^n$. We will call these principle ideals $\langle q_1 \rangle, \ldots, \langle q_t \rangle$. Now we can write $q = \epsilon q_i$ with

$\epsilon \in \mathbb{Z}_K^\times$ (consider letting $q_i = \epsilon^{-1} q \in \mathbb{Z}_K$). Now let $l = \max_{i=1,\dots,r_1+r_2; j=1,\dots,t} \beta_i(q_j^{-1})$. Then we obtain that

$$1 = \beta_i(1) = \beta_i(q_j q_j^{-1}) \leq l\beta_i(q_j) \tag{33}$$

Which results in

$$\beta_i(\epsilon a) \leq l\beta_i(q_j)\beta_i(\epsilon a) = l\beta_i(qa) = l\beta_i(b) \leq lnM = B \tag{34}$$

Thus, $\beta_i(\epsilon a) \leq B = lnM$. Earlier we found that $\beta_i(a) > B$ for $i = 1, 2, \dots, r_1 + r_2, i \neq j$, thus we have the following

$$\beta_i(\epsilon_j) = \frac{\beta_i(\epsilon_j a)}{\beta_i(a)} < \frac{B}{B} = 1, \quad i = 1, 2, \dots, r+s, i \neq j \tag{35}$$

From this we have

$$\begin{aligned} \mathcal{N}_{K|\mathbb{Q}}(\epsilon_j) &= \prod_{i=1}^{r_1+r_2} \beta_i(\epsilon_j)^{d_i} \\ &< \beta_j(\epsilon_j)^{d_i} \end{aligned}$$

And it follows that $\beta_j(\epsilon_j) > 1$ as the norm of ϵ_j is 1. □
We say that a set of $\{\alpha_1, \dots, \alpha_k\}$ elements are independent if $\alpha_1^{\rho_1}\alpha_2^{\rho_2}\dots\alpha_k^{\rho_k} = 1$ implies that $\rho_1 = \rho_2 = \dots = \rho_k = 0$.

Lemma 2.6.5. *There exists a set $\epsilon_1, \epsilon_2, \dots, \epsilon_{r_1+r_2-1}$ of independent units when $r_1 + r_2 \geq 2$.*

Proof: From Lemma 2.6.4 we know that there exists at least $r_1 + r_2 - 1$ unique units. Suppose these units are not linearly independent, then $\exists \rho_i \in \mathbb{Z}$ with $i \in \{1, \dots, r_1 + r_2 - 1\}$ and at least one $\rho_i > 0$ such that $\prod_{j=1}^{r_1+r_2-1} \epsilon_j^{\rho_j} = 1$. Now we ensure that at least one of these ρ_i is positive as we can take $\rho_i \leftarrow -\rho_i$ which is simply the inverse of ϵ_i. Relabel these such $\rho_i > 0$ with $i \in \{1, \dots, k\}$, $k \geq 1$ and $\rho_i \leq 0$ for $i \in \{k+1, \dots, r_1 + r_2\}$. Now let $\beta'(x) = \beta_1(x)^{d_1} \dots \beta_k(x)^{d_k}$ and $\beta'(x) = \beta_{k+1}(x)^{d_{k+1}} \dots \beta_{r_1+r_2}(x)^{d_{r_1+r_2}}$ where $d_i = 1$ if σ_i is a real embedding and $d_i = 2$ if σ_i is complex. Now we define it this way as we obtain

$$\beta(x)\beta'(x) = \prod_{i=1}^{r+s} |\sigma_i(x)^{d_i}| \tag{36}$$

Which since $|\sigma_j(x)| = |\overline{\sigma_j}(x)|$ where σ_j is a complex embedding we obtain that

$$\beta(x)\beta'(x) = \prod_{i=1}^{n} |\sigma_i(x)| \tag{37}$$

Which by Lemma 2.2.5 tells us that $\beta(x)\beta'(x) = |\mathcal{N}_{K|\mathbb{Q}}(x)|$. Thus, $\beta(\epsilon)\beta'(\epsilon) = 1$ and $\beta(\epsilon) = \beta'(\epsilon)^{-1}$ for every unit $\epsilon \in \mathbb{Z}_K^\times$. From Lemma 2.6.4 have that we can choose ϵ_j such that $\beta_j(\epsilon_j) > 1$ and $\beta_i(\epsilon_j) < 1$ for $i \neq j$. Since $\beta'(\epsilon_j) = \beta_{k+1}(\epsilon_j)^{d_{k+1}} \dots \beta_{r+s}(\epsilon_j)^{d_{r+s}}$ we obtain that $\beta'(\epsilon_j) < 1$ for $j \in \{1, \dots, k\}$. Similarly, we can show that $\beta(\epsilon_j) = \beta_1(\epsilon_j)^{d_1} \dots \beta_k(\epsilon_j)^{d_k}$ and obtain that $\beta(\epsilon_j) < 1$ for $j \in \{k+1, \dots, r_1 + r_2\}$. Now from our assumption we see that $\prod_{j=1}^{r_1+r_2-1} \epsilon_j^{\rho_j} = 1$ now applying β' to this we obtain

$$1 = \beta'(1) = \beta'\left(\prod_{j=1}^{r_1+r_2-1} \epsilon_j^{\rho_j}\right) = \left(\prod_{j=1}^{k} \beta'(\epsilon_j)^{\rho_j}\right)\left(\prod_{j=k+1}^{r_1+r_2} \beta(\epsilon_j)^{\rho_j}\right) \tag{38}$$

However, we see that this is smaller than 1 a contradiction proving our statement. □
Thus, we have a set of units who are all linearly independent, now we need to show that these units and the roots of unity span $\mathbb{Z}_K^\times$ and that they are unique.

Lemma 2.6.6. *For each unit $\epsilon \in \mathbb{Z}_K^\times$ with $\beta_v(\epsilon) \leq 1$, $v = 1, 2, \ldots, r_1 + r_2 - 1$ there exists an unit $\eta \in \mathbb{Z}_K^\times$*

$$\eta = \epsilon \epsilon_1^{\rho_1} \ldots \epsilon_{r_1+r_2-1}^{\rho_{r_1+r_2-1}} \tag{39}$$

that satisfies $1 < \beta_v(\eta) \leq a_v$ and $\beta_{r_1+r_2}(\eta) \geq 1$.

Proof: Let ϵ be a fixed unit satisfying $\beta_v(\epsilon) \leq 1$ with $v = 1, 2, \ldots, r_1+r_2-1$. From Lemma 2.6.3 we can obtain the following

$$\begin{aligned} \beta_{r_1+r_2}(\eta) &= \beta_{r_1+r_2}(\epsilon) \prod_{i=1}^{r_1+r_2-1} \beta_{r_1+r_2}(\epsilon_i)^{\rho_i} \\ &< \beta_{r_1+r_2}(\epsilon) \end{aligned}$$

Now we can also write $\eta = c_1\omega_1 + \cdots + c_n\omega_n$ with $c_i \in \mathbb{Z}$ (from Theorem 2.1.5) which leads to $\sigma_i(\eta) = c_1\sigma_i(\omega_1) + \cdots + c_n\sigma_i(\omega_n)$. Now by Cramer's rule we have that $c_1 = N_i/D$ where N_i is the determinant of the matrix formed by $\sigma_i(\omega_j)$ with the ith column replaced with $\sigma_i(\eta)$. Expanding N_i we obtain

$$N_i = \sum_{k=1}^{n} \sigma_k(a)(-1)^{k+i}\Delta_k \tag{40}$$

with Δ_k the determinant of the $(n-1) \times (n-1)$ matrix with entries in $\sigma_p(\omega_q)|p, q \in 1, 2, \ldots, n$. This can be seen as the matrix whose ith row and column are removed. Importantly all the values in that matrix are bounded, specifically $|\sigma_p(\omega_q)| \leq M$ and thus, $|\Delta_k| \leq (n-1)!M^{n-1}$. This brings Equation 40 to be

$$|N_i| = \sum_{k=1}^{n} \beta_k(a)|\Delta_k| \leq Ln!M^{n-1} \tag{41}$$

This results in each element c_i being bounded and as a result, we see that there are a finite number of η. Thus, we see that there exists $\beta_v(\eta) < a_v$ Now among these η we choose one which has the least valuation $\beta_{r_1+r_2}(\eta)$. Let us assume that for some $v_0 \in \{1, 2, \ldots, r_1 + r_2 - 1\}$ we have $\beta_{v_0}(\eta) \leq 1$. Now let ϵ_{v_0} be a unit such that $\beta_v(v_0) < 1$ for $v = 1, 2, \ldots, r_1 + r_2, v \neq v_0$ and $\beta_{v_0}(v_0) = a_{v_0} > 1$ (exists from Lemma 2.6.4). Now from this we have for $v \neq v_0$ that

$$\beta_v(\epsilon_{v_0}\eta) = \beta_v(\epsilon_{v_0})\beta_v(\eta) < \beta_v(\eta) \leq a_v \tag{42}$$

for $v = v_0$ we obtain

$$\beta_{v_0}(\epsilon_{v_0}\eta) = a_{v_0}\beta_{v_0}(\eta) \leq a_{v_0} \tag{43}$$

for $v = r_1 + r_2$ we obtain

$$\beta_{r+s}(\epsilon_{v_0}\eta) = \beta_{r+s}(\epsilon_{v_0})\beta_{r+s}(\eta) < \beta_{r+s}(\eta) \tag{44}$$

Thus, we see that $\epsilon_{v_0}\eta$ is smaller over β_{r+s}, a contradiction of the minimality of η, thus, $\beta_v(\eta) \geq 1$ for all $v \in \{1, 2, \ldots, r + s - 1\}$. □

Proof of Dirichlet's Unit Theorem: Suppose $r_1 + r_2 = 1$ then $\beta_{r_1+r_2}(\epsilon) = 1$. Now suppose $r_1 + r_2 \geq 2$. Let $\epsilon \in \mathbb{Z}_K^\times$ be a unit with $X = \max_{1 \leq v \leq r_1+r_2-1} \beta_v(\epsilon)$. By Lemma 2.6.6 we know that there exists a $\epsilon_0 = \epsilon_1^{\sigma_1} \ldots \epsilon_{r_1+r_2-1}^{\sigma_{r_1+r_2-1}}$ with integers $\sigma_1, \ldots, \sigma_{r_1+r_2-1}$ such that satisfies $1 < \beta_v(\eta) \leq a_v$ and $\beta_{r_1+r_2}(\eta) \geq 1$ for $v \in \{1, 2, \ldots, r_1 + r_2 - 1\}$ as $\beta_v(1) = 1$. Now set $Y = \min_{1 \leq v \leq r_1+r_2-1} \beta_v(\epsilon_0)$ which has the property $Y > 1$. Now there exists $k \in \mathbb{N}$ such that $Y^k \geq X$ and this implies that $\beta_v(\epsilon_0)^k \geq \beta_v(\epsilon)$ for all $v \in \{1, \ldots, r_1 + r_2 - 1\}$. This leads to the statement $\beta_v(\epsilon\epsilon_0^{-k}) \leq 1$ for $v \in \{1, 2, \ldots, r_1 + r_2 - 1\}$. Thus, if we let $\lambda = \epsilon_0\epsilon$ we obtain from Lemma 2.6.6 that there exists $\eta = \lambda\epsilon_1^{\rho_1} \ldots \epsilon_{r_1+r_2-1}^{\rho_{r_1+r_2-1}}$ with $\rho_1, \ldots, \rho_{r_1+r_2-1}$ integers such that

$1 < \beta_v(\eta) \leq a_v$, $v \in \{1, 2, \ldots, r_1 + r_2 - 1\}$. Expanding η out we obtain $\eta = \epsilon\epsilon_0^{-k}\epsilon_1^{\rho_1} \ldots \epsilon_{r_1+r_2-1}^{\rho_{r_1+r_2-1}}$ which can be simplified to $\eta = \epsilon\epsilon_1^{\rho_1 - k\sigma_1} \ldots \epsilon_{r+s-1}^{\rho_{r_1+r_2-1} - k\sigma_{r_1+r_2-1}}$. Since η is a unit we obtain that $\beta_{r+s}(\eta) \leq 1$ (as otherwise $\mathcal{N}_{K|\mathbb{Q}}(\eta) \neq 1$). Rearranging this we obtain that $\epsilon = \eta\epsilon_1^{\tau_1} \ldots \epsilon_{r_1+r_2-1}^{\tau_{r_1+r_2-1}}$ with $\tau_i = k\sigma_i - \rho_i$. This η has the property that $\beta_i(\eta) \leq B$ for all $i \in \{1, 2, \ldots, r_1+r_2\}$ and we can write it as $\eta = c_1\omega_1 + \cdots + c_n\omega_n$ with $c_i \in \mathbb{Z}$. From this we obtain that $\beta_i(\eta) = M\sum_{i=1}^{n} |c_i| \leq B$ which implies that there are only finitely many η as $|c_i| \leq B/M$ where c_i is an integer. Let h be the number of η and $H = \langle \epsilon_1, \ldots, \epsilon_{r_1+r_2-1} \rangle$ be a subgroup of $\mathbb{Z}_K^\times$. Now $\eta \notin H$ as $\beta_{r_1+r_2}(\eta) \geq 1$ while $\beta_{r_1+r_2}(\epsilon_i) < 1$ for $i \in \{1, 2, \ldots, r_1 + r_2 - 1\}$. Thus, the quotient group $\mathbb{Z}_K^\times / H$ has order h and any $\eta \in \mathbb{Z}_K^\times / H$ are units of finite order which divides h, implying they are roots of unity. This also implies that any unit $\epsilon^h \in H$, thus, we can write it as $\epsilon^h = \epsilon_1^{\xi_1} \ldots \epsilon_{r_1+r_2-1}^{\xi_{r_1+r_2-1}}$ with $\xi_1, \ldots, \xi_{r_1+r_2-1} \in \mathbb{Z}$. Now suppose there are $m \geq r_1 + r_2$ independent units. Then there cannot exist $\lambda_1\lambda_2 \ldots \lambda_m \neq 1$ however this becomes a system of equations with m unknowns and $r_1 + r_2 - 1$ equations which will have a solution. This implies that there are at most $r_1 + r_2 - 1$ independent units and from Lemma 2.6.5 we see that there is such a set of units. Now suppose there is an element that can be represented as $\eta\epsilon_1^{x_1} \ldots \epsilon_{r+s-1}^{x_{r_1+r_2-1}}$ and $\theta\epsilon_1^{y_1} \ldots \epsilon_{r_1+r_2-1}^{y_{r_1+r_2-1}}$ with η, θ roots of unity and $x_i \neq y_i$ from some $i \in \{1, 2, \ldots, r_1 + r_2 - 1\}$. Equating and rearranging we obtain

$$\eta\theta^{-1} = \epsilon_1^{y_1 - x_1} \ldots \epsilon_{r_1+r_2-1}^{y_{r_1+r_2-1} - x_{r_1+r_2-1}} \tag{45}$$

Taking this to the power of k such that $(\eta\theta^{-1})^k = 1$ as η, θ are roots of unity and by group laws so are $\eta\theta^{-1}$.

$$1 = \epsilon_1^{k(y_1 - x_1)} \ldots \epsilon_{r_1+r_2-1}^{k(y_{r_1+r_2-1} - x_{r_1+r_2-1})} \tag{46}$$

However, since $\epsilon_1, \ldots, \epsilon_{r_1+r_2-1}$ are independent we must have that $k(y_i - x_i) = 0$ which implies that $y_i = x_i$ a contradiction. Thus, every unit in $\mathbb{Z}_K^\times$ can be represented uniquely as $\eta\epsilon_1^{\tau_1} \ldots \epsilon_{r_1+r_2-1}^{\tau_{r_1+r_2-1}}$. □

2.7 Regulator and Zeta functions

The concepts in this section are useful in computing the full set of fundamental units but are not vital in generating units. Thus, we will briefly discuss them. The first such concept is the regulator

Definition 2.7.1 (Regulator)**.** Let $\sigma_1, \ldots, \sigma_{r_1+r_2}$ be a set of pairwise non-conjugate embeddings. The *regulator* of a set of $\{\epsilon_1, \ldots, \epsilon_{r_1+r_2-1}\}$ is defined as

$$\operatorname{reg}(\epsilon_1, \ldots, \epsilon_{r_1+r_2-1}) = |\det(d_i \log|\sigma_i\epsilon_j|)_{i,j=1}^{r_1+r_2-1}| \tag{47}$$

with d_i being the usual 1 if σ_i is a real embedding and 2 if σ_i is a complex embedding.

We say that the regulator of $\mathbb{Z}_K$ is the regulator over a set of fundamental units and the regulator of K is the regulator of the ring of integers.

Theorem 2.7.1. *The regulator of K is independent on the set of fundamental units.*

The proof of this can be found in 13.7 in [AW03]. Now the regulator is vital for computing the class group and is useful for checking the set of fundamental units. To understand how we need to consider zeta functions.

Definition 2.7.2 (Dedekind zeta function)**.** The Dedekind zeta function is defined as

$$\zeta_K(t) = \sum_{I \neq 0} (\mathcal{N}_{K|\mathbb{Q}}(I))^{-t} \tag{48}$$

where I is a non-zero ideal in the ring of integers.

We can see this by considering the following connection

Theorem 2.7.2. *Let $R(K)$ be the regulator of K, $h(K)$ be the class number of K and $\omega(K)$ the number of fundamental units of K. Then the following it true*

$$\frac{2^{r_1}(2\pi)^{r_2}h(K)R(K)}{\omega(K)\sqrt{\Delta(K)}} = \prod_p \frac{1-1/p}{\prod_{p|\mathfrak{p}} 1-1/\mathcal{N}_{K|\mathbb{Q}}(\mathfrak{p})} = \zeta_K^*(1) \tag{49}$$

where $\mathfrak{p}$ is the prime ideals over the primes p and $\zeta_K^*(1)$ is the residue at 1.

For more details on this see Theorem 6.3 in [Ste20] and chapter 5 section 1 in [BS66]. We call the sum $\prod_p \frac{1-1/p}{\prod_{p|\mathfrak{p}} 1-1/\mathcal{N}_{K|\mathbb{Q}}(\mathfrak{p})}$ the Euler product. An immediate application of Theorem 2.7.2 is we can compute an estimate for the regulator and class number. However, this is not the only application of the Dedekind zeta function. Indeed, the results of the famous Riemann hypothesis can be applied to the Dedekind zeta function in the following way

Conjecture 2.7.3 (General Riemann hypothesis)**.** *For the zeta function*

$$\zeta_K(t) = \sum_{I\neq 0} (\mathcal{N}_{K|\mathbb{Q}}(I))^{-t} \tag{50}$$

the only values of t with $0 < Re(t) < 1$ such that $\zeta_K(t) = 0$ is only when $Re(t) = \frac{1}{2}$.

This is useful in our case as it provides a much better bound on the prime ideals that generate the class group than Minkowski's constant [CDO97]. Details of this bound can be seen in [Bac90] and is based on the proof seen in [LO77].

2.8 Linear Algebra

The LLL algorithm, also known as Lenstra-Lenstra-Lovász algorithm, is a lattice basis reduction algorithm. The algorithm computes a basis for a lattice that is LLL reduced given by the following definition

Definition 2.8.1 (LLL reduction, Definition 2.6.1 [CCC93])**.** Let $\mathbf{b}_1, \ldots, \mathbf{b}_k$ be a basis for a lattice L and $\mathbf{b}_1^*, \ldots, \mathbf{b}_k^*$ denote an orthogonal basis. We call a basis reduced if for $|\mu_{i,j}| \leq \frac{1}{2}$ where $1 \leq j < i \leq k$ we have

$$|\mathbf{b}_i^*|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) |\mathbf{b}_{i-1}^*|^2. \tag{51}$$

A more general definition is that a $\mathbb{Z}$ basis for a lattice is LLL reduced if over a particular metric if our vectors are short. Now a metric of particular note is the following.

Definition 2.8.2 (v-norm)**.** Let $v = (v_i)_{1\leq i\leq n}$ be a vector of real numbers such that $v_{r_2+i} = v_i$ for $r_1 < i \leq r_1 + r_2$. The v-norm $\|\alpha\|_v$ of α is defined by

$$\|\alpha\|_v^2 = \sum_{i=1}^{n} e^{v_i} |\sigma_i(\alpha)|^2 \tag{52}$$

where σ_i is an embedding.

Which allows use to define an ideal being LLL reduced in a random direction [CDO97].

Definition 2.8.3 (LLL reduced in a random direction)**.** A $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_n$ of an ideal I is LLL-reduced in the direction v if it is LLL-reduced for the quadratic form $\|\alpha\|_v^2$.

Basically here we are changing the metric for LLL reduction so that it is suitable for an ideal. Another linear algebra method that will be of use is finding the Hermite Normal Form (HNF). Hermite Normal Form is a method for row reducing (or in our case column reduce) an integral matrix without dividing. More formally we have the following

Definition 2.8.4 (Hermite normal form, Definition 2.4.2 [CCC93])**.** We will say that an $m \times n$ matrix $M = (m_{i,j})$ with integer coefficients is in *Hermite normal form* if there exists $r \leq n$ and a strictly increasing map f from $[r+1, n]$ to $[1, m]$ satisfying the following properties.

- For $r+1 \leq j \leq n, m_{f(i),j} \geq 1, m_{i,j} = 0$ if $i > f(j)$ and $0 \leq m_{f(k),j} < m_{f(k),k}$ if $k < j$.
- The first r columns of M are equal to zero.

3 Computing Fundamental Units

The initial method for finding a set of fundamental units revolved around generating elements until we find elements $\alpha, \beta \in \mathbb{Z}_K$ such that $\mathcal{N}_{K|\mathbb{Q}}(\beta/\alpha) = 1$. This finds units due to Lemma 2.2.4 which tells us that all units have norm ± 1 and Lemma 2.2.3 telling us that if two elements have the same norm then we can divide one from the other to get a unit. Note that this method is not as effective for any number fields of degree greater than 3. This method was developed by Minkowski and expanded in 1975 by Zassenhaus. Zassenhaus also modified the method to use a linear combination of elements to obtain units decreasing the number of elements required. The main problem with these methods was finding units which where linearly independent of units already found. This was solved with the development of the LLL reduction [Zim96]. In 1989 James Hafner and Kevin McCurley developed the first algorithm with subexponential expected performance [HM89]. This algorithm and the following classical algorithms assume the General Riemann Hypothesis as a bound on the prime numbers that generate the class group. In 1997 H. Cohen, F. Daiz Y Daiz and M. Olivier [CDO97] generalised and improved a method by James Hafner and Kevin McCurley using a technique described by Buchmann [Buc90] and . This algorithm is subexponential in performance and is currently implemented in `PARI/GP`. More recently computing the unit group and class group has become useful in being able to break certain cryptographic methods. With quantum computers being capable of breaking modern encryption, a search has begun for cryptographic methods that are not quickly broken using quantum computers or any classical algorithm. One type of encryption method is lattice-based cryptography which is promising in their resistance to classical and quantum attacks [NDR$^+$19]. Some of these methods make the well based assumption that it is hard to find short vectors in an ideal lattice which the unit group and class group provide significant insight into. As such two algorithms were developed in 2014 for computing the unit group faster, one classical, one quantum. The classical algorithm was developed by Jean-François Biasse and Claus Fieker in [BF14] which was still subexponential time but performed better in large degree number fields. The key difference in the algorithm is that it utilises another lattice reduction algorithm (BKZ) instead of LLL reduction which allows for relations between ideals being found faster. The quantum algorithm was developed by Kirsten Eisenträger, Sean Hallgren, Alexei Kitaev and Fang Song in 2014 [EHKS14]. This algorithm is polynomial time with degree and log of the discriminant and does not assume the General Riemann Hypothesis. This result was improved by Jean-François Biasse and Fang Song in 2016 [BS16] which does assume the General Riemann Hypothesis.

The algorithm that we will be looking at is the 1997 version (See [CDO97]) as it is implemented in `PARI/GP` [PAR22], an open source computational algebra package. The full algorithm for computing a set of fundamental units can be found in [CCC93]. However, we will outline some key details.

Our first step is to select a factor base. Our factor base FB_p over the integers will contain all prime numbers bellow the bound $12\ln^2|D|$ where D is the determinant of the number ring, and it will contain a number of prime numbers bellow the Minkowski's constant as seen in Theorem 2.4.5. We use Minkowski's constant as it gives a sufficient representation of the ring of integers. Since we are assuming the GRH we do not use all the prime numbers below the Minkowski bound. This reduces the size of our factor base and reduces the computational time to find units. After selecting our prime number factor base we factor the prime number ideals into prime ideals in $\mathbb{Z}_K$ and store these to obtain our prime ideal factor base $FB_\mathfrak{p}$. We also store the prime number valuations over the factor base $FB_\mathfrak{p}$ in a relation matrix M and we do this in the following way. The relations matrix M is a $l \times m$ matrix with l the number of elements in the prime ideal factor base and m the number of relations. Each column is the valuation of an element α over the prime ideal factor base. From this construction of a matrix we can store relations by adding another column onto the matrix. As well as this we store our element α in a $n \times m$ matrix M_C as a logarithmic embedding using Equation 18. We do this as it allows for us to do the same operations on M_C as M and the logarithmic embedding is significantly smaller than containing the elements themselves. The only downside is that we have to reverse the complex embedding to get units.

After generating the factor bases we generate and store relations in M and M_C. In the previous section we have already outlined a method for generating the trivial relations. This method is factoring the elements in FB_p over $FB_\mathfrak{p}$ and is done as it increases the number of columns in M to require fewer relations computed using more involved methods. Another method is that we generate elements of small norm and then factor that over the factor base $FB_\mathfrak{p}$. We only store the element if it completely factors over the factor base. We look at small norm elements as they are likely to split over the factor base $FB_\mathfrak{p}$. The most important method for generating relations is generating random ideals and then LLL reducing them in a random direction. We start by selecting random numbers $v_i \leq 20$, where each v_i corresponds to an element in $FB_\mathfrak{p}$, before we select an ideal $\mathfrak{q}$ in the factor base. Finally, we compute a random ideal as $I = \mathfrak{q}\prod_{1\leq i\leq s}\mathfrak{p}^{e_i}$. Note that we can speed up this computation by computing $\mathfrak{p}^{e_i}$ earlier. Then we LLL reduce this ideal in a random direction to get $J = I/\alpha$ (See subsection 2.8). We then try to factor this α over the factor base and, if it does factor, store this relation in the relation matrix M and store the complex embedding of α in M_C.

We use the methods described above to generate relations until we think we have enough to generate a set of fundamental units. We then compute the roots of unity so that we can compute the Euler number z so that we can compute the regulator of the number field from Theorem 2.7.2. We need the Euler number as we see from the definition of the regulator that a set of fundamental units can compute the regulator and since the regulator is independent on the set of fundamental units from Theorem 2.7.1 this means we have a way of checking that we have a set of fundamental units. Now we are going to compute the kernel of M with each element in the kernel corresponding to a combination of elements which by Lemma 2.3.5 are a unit. To do this we get the matrix $MA = W$ where W is the Hermite Normal form of M and similarly compute $M_CA = M'_C$. Thus, any zero column in W will correspond to a unit in M'_C. From this matrix M'_C we LLL-reduce the matrix to get C.

From this we now compute an approximation of the regulator. To start we assume the regulator is $R = 0$ and let $j = r_1 + r_2 - 2$. Let A be a $(r_1 + r_2 - 1) \times (r_1 + r_2 - 1)$ matrix from taking a sufficient number of rows C and the rows $j - r_1 + r_2 + 2$ to j. Now we compute the determinant of A as R_1 before we compute the greatest common divisor of R_1 and R which becomes our new regulator approximation. In finding the greatest common divisor we compute the values u, v and d in $uR_1 + vR = d$. Using these values we set the column C_j to be $vC_j + (-1)^{r_1+r_2}uC_{j-r_u+1}$.

We repeat this until $j > r$ where r is the number of columns in C corresponding to units and the final R becomes our approximation of the regulator. From C we define F to be the last $r_1 + r_2 - 1$ columns which we will use to compute units, the coefficients will be labelled $f_{i,j}$. This step also minimises the first r_1+r_2-1 units so will be where the fundamental units are.

To finally obtain the set of fundamental units we need to reverse the complex embedding. We start this by forming a $n \times r_1 + r_2 - 1$ matrix B with coefficients $b_{i,j} = f_{i,j}$ if $i \leq r_1$, $b_{i,j} = f_{i,j}/2$ if $r_1 < i \leq r_1 + r_2$ and $b_{i,j} = f_{i-r_2,j}$ if $r_1 + r_2 < i \leq n$. This step in terms of the logarithmic embedding seen in Equation 18 can be seen as

$$b_{i,j} = (L_C(\alpha_j)/n_i)_{1 \leq i \leq r_1+r_2} = \ln(\sigma_i(\alpha_j)) \tag{53}$$

We can ignore the second half from Equation 18 as the norm of α is 1. Before we take the exponent of this, we will first LLL reduce the real part of the matrix B to get BU. Now we take the exponents of the elements in BU to get E with coefficients $e_{i,j}$. Looking at the form of this we see that

$$e_{i,j} = \exp((L_C(\alpha_j)/n_i)_{1 \leq i \leq r_1+r_2}) = \sigma_i(\alpha_j) \tag{54}$$

Finally we need to solve for α_j. To do this we take a $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_n$ for $\mathbb{Z}_K$ and form the matrix Ω with each coefficient as $w_{i,j} = \sigma_j(\omega_i)$. Then we solve $F_u = \Omega^{-1}E$ where each column of F_u corresponds to a unit with components over the basis $\omega_1, \ldots, \omega_n$. The components of these units will be near integer but will not be exactly, so we will need to round. Note that from this method we can easily tell if a unit is the trivial unit 1 as from Lemma 2.4.4 we know that this is the zero vector.

Then we can compute the regulator using this set of fundamental units to check that they actually are a full set of fundamental units. That is, we check that $Rh = z\sqrt{2}$ where h is the class number and R is the regulator from the set of units. If this is not true then we compute some more relations and go back to the Hermite reduction stage. This algorithm also computes the class group as the overhead is marginal in the computation process, however, this is not particularly relevant to computing the unit group, so we will not go over the details here.

If we only need a small number of units we can attempt to prematurely halt the fundamental unit algorithm. To prematurely halt we can generate the relations, reduce our matrix and extract any units we find. We would generate relations the same way and would reduce the relation matrix in the same way. The only difference would be that for every column in our matrix corresponding to a unit we would check to see if the element is non-trivial. This would skip having to wait for $r_1 + r_2 - 1$ relations, computing the regulator to check we have a fundamental set and computing things like the class group.

In theory this should be possible and reasonable to do, however the current implementation stores them as the complex logarithmic embedding meaning we have to extract elements which is not a simple task. We also cannot just consider the elements in non-logarithmic form as they result in elements that contain large exponents. We could bypass this by storing the factorisation of an element, however, this makes it harder to check whether we have a non-trivial unit. To check if we have a unit we could look for units whose complex embedding is not the zero vector. However, in the process of trying to implement such an algorithm we struggled to compute non-trivial units and even when we did it was rarely faster than the original algorithm. This is also before we attempted to check if the units were square or linearly independent. Thus, instead we have pivoted to directly computing elements in the kernel of the norm mapping from $K^\times/K^{\times 2} \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$.

4 Square Norm Elements

We have explored finding random units in our algorithm with limited success. However, we can consider finding elements that are not in $K^{\times 2}$ but have norm in $\mathbb{Q}^{\times 2}$. To do this we will generate elements $\{\alpha_1, \ldots, \alpha_m\}$ in the same way as the complete fundamental unit algorithm as seen in Section 3. Then we will factor the norm of these elements over a factor base of primes below a bound (consider the Minkowski's constant) modulo 2, let us call this relation matrix W_p which is a matrix over $\mathbb{Z}_2$. From each vector $v = (v_1, \ldots, v_m)^T \in \ker(W_p)$ we can construct $\beta = \alpha_1^{v_1} \ldots \alpha_m^{v_m}$. Each element β will correspond to an element with square norm. Now we need to find β that are not in $K^{\times}$. To do this one can consider factoring α_i over the prime ideal factor base of L modulo 2 to get the relation matrix $W_{\mathfrak{p}}$. Now each element $v \in \ker(W_{\mathfrak{p}})$ corresponds to an element $\beta \in K^{\times 2}$ using the construction described earlier. Thus, if we want to find elements that are not in $K^{\times 2}$ but have norm in $\mathbb{Q}^{\times 2}$ then we need to find $v \in \ker W_p \backslash \ker W_{\mathfrak{p}}$. We can still look for units as from Lemma 2.2.4 we know that a unit will always map to one the multiplicative identity of the multiplicative group $\mathbb{Q}^{\times}/\mathbb{Q}^{\times 2}$ so it will always be in the kernel of ϕ if the unit is not a square. However, that does not mean that it will be in $K^{\times}/K^{\times 2}$ as it may be a square.

Consider the following two lemmas

Lemma 4.0.1 (Element not in $K^{\times 2}$)**.** *An element α is not a square in K if $val_{\mathfrak{p}}(\alpha) \neq 0 \mod 2$ for at least one prime ideal $\mathfrak{p}$ in $\mathbb{Z}_K$.*

Proof: Suppose $\alpha \in K^{\times 2}$, then there exists $\beta \in K^{\times}$ such that $\beta^2 = \alpha$. Clearly $\langle \alpha \rangle \subseteq \langle \beta \rangle$. Now by Theorem 2.3.1 we know that $\langle \beta \rangle = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_k^{e_k}$ for some $e_1, \ldots, e_k \in \mathbb{Z}$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ prime ideals of $\mathbb{Z}_K$. We also can see that $a \in \mathfrak{p}_1^{2e_1} \ldots \mathfrak{p}_k^{2e_k}$ and by extension $\langle a \rangle \subset \mathfrak{p}_1^{2e_1} \ldots \mathfrak{p}_k^{2e_k}$. Thus, if $\langle a \rangle = \mathfrak{p}_1^{d_1} \ldots \mathfrak{p}_k^{d_k}$ with $d_1, \ldots, d_k \in \mathbb{Z}$ then $e_i \leq d_i$ but $\langle a \rangle$ is the smallest ideal containing a, thus, $e_i = d_i$. This implies that d_i is even or zero which is a contradiction as there is at least one d_i that is odd. □

Lemma 4.0.2 (Square Norm Element)**.** *An element $\alpha \in K$ has square norm if $val_p(\mathcal{N}_{K|\mathbb{Q}}(\alpha)) = 0 \mod 2$ for all primes $p \in \mathbb{Z}$ and $\mathcal{N}_{K|\mathbb{Q}}(\alpha) > 0$.*

Proof: The norm of $\mathcal{N}_{K|\mathbb{Q}}(\alpha) \in \mathbb{Z}$, now if $\mathcal{N}_{K|\mathbb{Q}}(\alpha)$ is a square then there is $\beta \in \mathbb{Z}$ such that $\beta^2 = \mathcal{N}_{K|\mathbb{Q}}(\alpha)$. For this to be true $\mathrm{val}_p(\mathcal{N}_{K|\mathbb{Q}}(\alpha)) = 2 \times \mathrm{val}_p(\beta)$ and since $\mathrm{val}_p(\beta) \in \mathbb{Z}$ for all primes p we know that $\mathrm{val}_p(\mathcal{N}_{K|\mathbb{Q}}(\alpha)) = 0 \mod 2$ for all primes p. □
Lemma 4.0.2 is a sufficient condition but not a necessary condition, to obtain a necessary condition consider the following Lemma.

Lemma 4.0.3. *An element $\alpha \in K$ where K is a number field is a square in K if and only if the polynomial $x^2 - \alpha \in K[x]$ is not irreducible.*

Proof: If α is a square then $\beta^2 = \alpha$ and we can factorise the polynomial $x^2 - \alpha = x^2 - \beta^2 = (x - \beta)(x + \beta)$. If α is not a square then there is no β such that this is true and $x^2 - \alpha$ is irreducible. □
This leads to what we will be using for our algorithm.

Theorem 4.0.4. *An element $\alpha \in K^{\times}$ is a non trivial element of the kernel of the norm map $K^{\times}/K^{\times 2} \to \mathbb{Q}^{\times}/\mathbb{Q}^{\times 2}$ if one of the following is true*

- *$val_{\mathfrak{p}}(\alpha) \neq 0 \mod 2$ for some prime ideal $\mathfrak{p}$ in K, $val_p(\mathcal{N}_{K|\mathbb{Q}}(\alpha)) = 0 \mod 2$ for all primes $p \in \mathbb{Z}$ and $\mathcal{N}_{K|\mathbb{Q}}(\alpha)$ is positive.*
- *$val_{\mathfrak{p}}(\alpha) = 0$ for all prime ideals $\mathfrak{p}$ in K and on the polynomial $x^2 - \alpha \in K[x]$ is irreducible and the norm is positive.*

Proof: From Lemma 4.0.2 we know that α has square norm and from Lemma 4.0.1 we know that it is not square, thus, it will be in the kernel proving the first part. From Lemma 2.3.5 we know that α is a unit and from Lemma 2.2.4 we know that a unit has norm ± 1. If $\text{val}_{-1}(\mathcal{N}_{K|\mathbb{Q}}(\alpha)) = 1 \mod 2$ then we know that the norm will be -1 and will not be in the kernel. Now we need to check if $\alpha \in K^{\times 2}$ which by Lemma 4.0.3 we see that if $x^2 - \alpha$ is irreducible that it is not a square. □

There are a number of things to note with this. Firstly, we are not interested in elements $k \in \mathbb{Z}$ whose norms are k^n with n the degree. These elements will always have square norms in even degree. To see this consider the element 2 factored over the number ring $\mathbb{Z}_K$ where $K = \mathbb{Q}[x]/\langle x^4 + 9x^3 - x^2 - 6x - 9\rangle$. This element factors into the prime ideals $\mathfrak{p}_2\mathfrak{q}_2\mathfrak{v}_2$ yet the norm of the element is 2^4 which is clearly a square. This satisfies our conditions, yet this will always be true for any element $k \in \mathbb{Z}$ in an even degree field. Secondly, we are not interested in elements of the form al^2 where $l \in K^\times$ and $a \in \mathbb{Z}$ for even degree as the norm of a is a^n. To check for this we can factor our norm of α into prime numbers and if a prime number p appears more than n times, it is likely that it was a factor. Thus, we can check if a linear combination of p and α results in them becoming a square. Thirdly, if an element has negative norm then it cannot be in $\mathbb{Q}^{\times 2}$, however we can bypass this by multiplying by -1. This works as from Lemma 2.2.3 we have that $\mathcal{N}_{K|\mathbb{Q}}(-1 \times \alpha) = \mathcal{N}_{K|\mathbb{Q}}(-1)\mathcal{N}_{K|\mathbb{Q}}(\alpha) = -\mathcal{N}_{K|\mathbb{Q}}(\alpha)$. Finally, this is a sufficient check but not a necessary check. This can be seen in Subsection 4.1. A necessary condition is if $y^2 + \beta \in K[x]$ (See Lemma 4.0.3) is irreducible over K.

For our case we will not be directly looking for linear independence as that is impractical to compute without computing the unit group, which we are trying to avoid. Thus, we are going to say that two elements are linearly independent if you can make a square from a linear combination of the two. To do this we form a matrix with each column being the element over the prime ideal factor base and check that the kernel is empty. To form the element we do not need to factor the element over the prime ideal factor base but can instead take $W_\mathfrak{p} v$ where $v \in \ker(W_p)$ to get the factorisation of β over the prime ideal factor base.

4.1 Example

Consider the number field $K = \mathbb{Q}[x]/\langle f(x)\rangle$ where $f(x) = x^3 + x^2 + 5x - 16$ and let $f(\theta) = 0$. We are going to consider elements over the prime number factor base $2, 3, 5, 7$. The factor base of ideals in $\mathbb{Z}_K$ as $\mathfrak{p}_2 = \langle 2, \theta\rangle, \mathfrak{q}_2 = \langle 2, \theta^2 + \theta + 1\rangle, \mathfrak{p}_3 = \langle 3, \theta + 1\rangle, \mathfrak{q}_3 = \langle 3, \theta + 2\rangle, \mathfrak{p}_5 = \langle 5, \theta + 2\rangle, \mathfrak{q}_5 = \langle 5, \theta^2 - \theta + 2\rangle, \mathfrak{p}_7 = \langle 7, \theta - 3\rangle, \mathfrak{q}_7 = \langle 7, \theta + 1\rangle, \mathfrak{v}_7 = \langle 7, \theta + 10\rangle$. Now consider Table 1. The kernel of W_p modulo 2 is given as

$$\ker(W_p) = \text{span}\left\{ \begin{bmatrix}0\\0\\0\\0\\0\\0\\1\\0\\0\\0\\0\end{bmatrix} \begin{bmatrix}0\\0\\0\\0\\0\\0\\0\\0\\0\\1\\0\end{bmatrix} \begin{bmatrix}0\\0\\0\\0\\1\\0\\0\\1\\0\\0\\0\end{bmatrix} \begin{bmatrix}1\\1\\1\\0\\0\\1\\0\\0\\0\\0\\0\end{bmatrix} \begin{bmatrix}0\\0\\0\\0\\0\\0\\0\\1\\1\\0\\1\end{bmatrix} \begin{bmatrix}0\\1\\0\\1\\1\\0\\0\\0\\0\\0\\0\end{bmatrix} \right\} \tag{55}$$

Now clearly elements 1 and 2 are not going to produce square norm elements as if we have a look at their factorisation $\theta + 3$ factors into $\mathfrak{p}_7^2$ and $\theta - 1$ factors into $\mathfrak{p}_3^2$. This can also be seen

Table 1: Ideals of K factored over the two factor bases

Ideals	2	3	5	7	$\theta+1$	$\theta+2$	$\theta+3$	$\theta+4$	$\theta+8$	$\theta-1$	$\theta-2$
W_p											
2	1	0	0	0	0	1	0	0	1	0	1
3	0	1	0	0	1	1	0	1	0	0	1
5	0	0	1	0	0	1	0	0	0	0	0
7	0	0	0	1	1	0	0	1	1	0	0
$W_{\mathfrak{p}}$											
$\mathfrak{p}_2$	1	0	0	0	0	1	0	0	1	0	1
$\mathfrak{q}_2$	1	0	0	0	0	0	0	0	0	0	0
$\mathfrak{p}_3$	0	0	0	0	1	0	0	1	0	0	1
$\mathfrak{q}_3$	0	1	0	0	0	1	0	0	0	0	0
$\mathfrak{p}_5$	0	0	1	0	0	1	0	0	0	0	0
$\mathfrak{q}_5$	0	0	1	0	0	0	0	0	0	0	0
$\mathfrak{p}_7$	0	0	0	1	0	0	0	1	0	0	0
$\mathfrak{q}_7$	0	0	0	1	1	0	0	0	1	0	0
$\mathfrak{v}_7$	0	0	0	1	0	0	0	0	0	0	0

as they sit in the kernel of $W_{\mathfrak{p}}$

$$\ker(W_{\mathfrak{p}}) = \operatorname{span}\left\{ \begin{bmatrix} 0\\0\\0\\0\\0\\0\\0\\0\\0\\1\\0 \end{bmatrix} \begin{bmatrix} 0\\0\\0\\0\\0\\0\\1\\0\\0\\0\\0 \end{bmatrix} \right\} \tag{56}$$

However, using Magma [BCP97] to check if they are squares we find that they are not squares. This shows that our tests are not conclusive if elements are squares or not.

From element 3 we can make $\beta_3 = (\theta+1)(\theta+4) = \theta^2+5\theta+4$ which will not be in $K^{\times 2}$ but its norm will be in $\mathbb{Q}^{\times 2}$. Checking this we see that $\mathcal{N}_{K|\mathbb{Q}}(\beta_3) = 1764 = 2^2 3^2 7^2 = 42^2 \in \mathbb{Q}^{\times 2}$ and that

$$\langle \beta_3 \rangle = \langle 2, x+2 \rangle^2 \langle 3, x+1 \rangle^2 \langle 7, x-3 \rangle \langle 7, x+1 \rangle \tag{57}$$

which is not in $K^{\times 2}$. Similarly, for element 4 we have $\beta_4 = 2\times 3\times 5\times (x+2) = 30\times(\theta+2)$ with norm $\mathcal{N}_{K|\mathbb{Q}}(\beta_4) = 2^4\times 3^4\times 5^4$ and prime ideal factorisation

$$\langle \beta_4 \rangle = \langle 2, \theta+2 \rangle^2 \langle 2, \theta^2+\theta+3 \rangle \langle 3, \theta+1 \rangle^2 \langle 3, \theta+2 \rangle^2 \langle 5, \theta+2 \rangle^2 \langle 5, \theta^2-\theta+2 \rangle \tag{58}$$

which is not in $K^{\times 2}$. For element 5 we have $\beta_5 = (\theta-2)(\theta+8)(\theta+4) = 9\theta^2+3\theta-48$ with norm $\mathcal{N}_{K|\mathbb{Q}}(\beta_5) = -1\times 2^6\times 3^4\times 7^2 = -254016$ and prime ideal factorisation

$$\langle \beta_5 \rangle = \langle 2, \theta+2 \rangle^6 \langle 3, \theta+1 \rangle^2 \langle 3, \theta+2 \rangle^2 \langle 7, \theta-3 \rangle \langle 7, \theta+1 \rangle \tag{59}$$

which is not in $K^{\times 2}$. Thus, $-\beta_5$ would be in the kernel. For element 6 we have $\beta_6 = 3\times 7\times(\theta+1) = 21(\theta+1)$ with norm $\mathcal{N}_{K|\mathbb{Q}}(\beta_6) = 3^4\times 7^4 = 194481$ and prime ideal factorisation

$$\langle \beta_6 \rangle = \langle 3, \theta+1 \rangle^3 \langle 3, \theta+2 \rangle \langle 7, \theta+1 \rangle^2 \langle 7, \theta+10 \rangle \tag{60}$$

which is not in $K^{\times 2}$. This provides a way for odd degree number fields to quickly generate elements in the kernel.

From the above example we can see that we do not actually need to compute $W_{\mathfrak{p}}$ as this is only needed to check that we are finding a square norm element that is not a square in L. Thus, we could instead compute $\ker(W_p)$ and then check that the element is indeed an element of square norm not in $K^{\times 2}$. To do this we need to factor the ideal generated by the element into prime ideals and take the valuation of each of the prime ideals. If the valuations are non-zero modulo 2 then we know that the element is not in $K^{\times 2}$. If the valuations are zero then we have found a unit in $\mathbb{Z}_K$.

4.2 Algorithm

An implementation of this algorithm was made in `PARI` by modifying the fundamental unit algorithm described by Cohen in [CDO97]. The general structure of the algorithm is as follows

Algorithm 4.2.1 (Finding elements of square norm)**.** *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial and λ the number of elements needed.*

1. *Do Steps 1 through 5 in Algorithm 6.5.6 in [CCC93].*
2. *Apply Step 6 in Algorithm 6.5.6 in [CCC93] for δ relations.*
3. *Apply Algorithm 4.2.2.*
4. *If previous step computed at least λ elements then return the elements otherwise go to Step 2.*

The part that we have modified the most is the following

Algorithm 4.2.2 (Computing and checking elements)**.** *Let $A = \{\alpha_1, \ldots, \alpha_m\}$ be m elements that factor over the prime ideal factor base of size l, let $W_{\mathfrak{p}}$ be the $m \times l$ matrix with each column being the valuation of each α_i over the prime ideal factor base and let λ be the number of desired elements.*

1. *Let $i \leftarrow 1$, FB the prime number factor base of size k and W_p be a $m \times k$ matrix.*
2. *Find the valuation of the norm $\mathcal{N}_{K|\mathbb{Q}}(\alpha_i)$ over the prime number factor base and store it as the ith column of W_p.*
3. *If $i \leq m$ then $i \leftarrow i + 1$ and go Step 2.*
4. *Compute the right kernel modulo 2 $\ker(W_p)$ and store each element in the kernel as a column in the matrix $W_{\ker}$, if there are no elements in the kernel then find more elements and return to Step 1.*
5. *Compute $M = W_{\mathfrak{p}} W_{\ker}$ modulo 2.*
6. *Let $j \leftarrow 1$.*
7. *Let β correspond to the jth element of $\ker(W_p)$. If the jth column of M is zero modulo 2 or the jth column of $W_p W_{\ker}$ is non-zero then go to Step 10.*
8. *Set $C = B \cup \{p_1, \ldots, p_l\}$ where $p_1, \ldots, p_l$ are the primes where $val_p(\mathcal{N}_{K|\mathbb{Q}}(\beta)) > n$.*
9. *If the element is independent to C using Algorithm 4.2.3 then set $B \leftarrow B \cup \{\beta\}$*

10. *If $j \leq m$ then $j \leftarrow j+1$ and go Step 7.*

11. *If the number of elements in B is greater than λ then return B otherwise find more elements and return to Step 1.*

Algorithm 4.2.1 can be outlined as follows. We start by computing the factor base and generating elements as described in [CDO97]. Then we factor the norm of the elements over the prime number factor base and store it in the matrix W_p, we do not store each vector modulo 2 as this means we cannot check whether this element is a unit. Then we compute the kernel $\ker(W_p)$ modulo 2 with each column corresponding to a square norm element. Due to how the algorithm is set up, we still generate $W_{\mathfrak{p}}$ and can compute $M = W_{\mathfrak{p}} \ker(W_p)$ modulo 2 to get the prime ideal factorisation of the elements in the kernel. From this we can check each column in M using the checks described above to see if what we have is not in $K^{\times 2}$. A benefit of this method is that at no point do we have to deal with the actual element, it is sufficient to simply store the factors and their valuations of the element. This means that we can store and check elements that would otherwise be impossible to store.

For our algorithm it is important that we check for uniqueness of elements and so to do this we have the following checking algorithm.

Algorithm 4.2.3 (Independence of elements)**.** *Let B be a set of valid elements and α an element we want to test.*

1. *For each element in B add the valuations of the elements over the prime ideal factor base to a matrix M.*

2. *Add the valuation α over the prime ideal factor base to M.*

3. *Compute the kernel of M modulo 2.*

4. *If the kernel is empty then α is independent to all elements in B.*

The implementation of the algorithm can be found on GitHub [Ken23].

4.3 Limitations and Improvements

There are a number of other ways that this algorithm could be improved. For example if the relation between the ideals of the primes and the prime ideals is linear then we could compute $W_{\mathfrak{p}} B = W_p$. This would likely speed up the computation as we are no longer having to factor the norm over the primes (as factoring large elements quickly becomes computationally expensive compared to matrix multiplication). However, this speed is probably marginal as factoring the norm of an element is likely not all that expensive as the prime factors are guaranteed to be over a small factor base. Another potential improvement is to store the relation matrix in as reduced of a form as possible. This would likely reduce the time that it would take to find the kernel and would easily prevent repeated checking of elements. If we were to build the algorithm from scratch it would be better to store the norm of the element and not compute $W_{\mathfrak{p}}$ at all and instead factor each element over the prime ideals as needed. However, that would be beyond the scope of this project.

Another limitation of this approach is that the check in Theorem 4.0.4 is a sufficient condition but not a necessary condition. For example, consider the number ring $K = \mathbb{Q}[x]/\langle f(x) \rangle$ where $f(x) = x^8 - 4x^7 + 3x^6 - 2x^5 + 4x^4 - 9x^3 + x^2 + 5x + 2$ and the element

$$\begin{aligned}\beta = {} & 160103386684687502 3\theta^7 - 700388383382544562 5\theta^6 + 724183508451831607 3\theta^5 \\ & - 528336292240696316 4\theta^4 + 772397219982904368 7\theta^3 - 148738946632108371 28\theta^2 \\ & + 78988455335273102 51\theta + 3766359828176068618.\end{aligned} \tag{61}$$

This element has square norm but is itself not a square and was not found with the algorithm. Alternatively, consider the examples $\theta - 1$ and $\theta + 3$ in Subsection 4.1, here we saw that it was in the kernel of both matrices but it is not a square. To get past this limitation we could directly test whether or not each element is a square as for each element β we can make the polynomial $x^2 - \beta \in K[x]$ and check if it is irreducible over K (see Theorem 4.0.3). If it is then β is not a square if it is reducible then it is a square. This has not been implemented for the algorithm. Also from computing elements in thousands of number rings there have been less than ten unsuccessful number rings and they were all in degree less than 7 and, as we will see, the difference in speed is trivial compared to computing a full set of fundamental units which provides sufficient insight for our application.

4.4 Optimisation

For this algorithm we have to choose the number of relations δ we find before running Algorithm 4.2.1. To work this out we are going to use a bracketing technique to find the optimal number of relations for each degree. To do this we assume that there is a single minimum point over the entire domain. For each value of δ we are going to compute the average time for approximately 1000 polynomials (2000 polynomials for degree less than 15) that have maximum coefficients of 10. We will start by computing $a = 1, b = 100$ where a and b are the boundaries of our bracket before selecting two points $c = (b - a)/3$ and $d = 2 \times (b - a)/3$. If $c < d$ then $a \leftarrow a, b \leftarrow d$ and repeat until the difference of a and b are sufficiently small. Applying this algorithm for our problem we find optimisation seen in Figure 1.

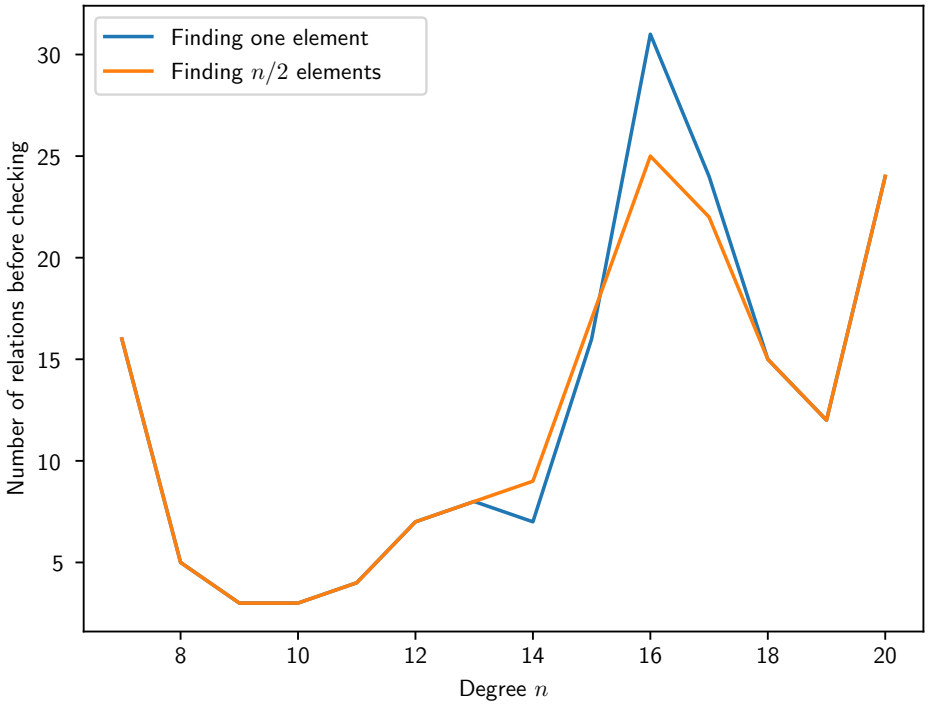


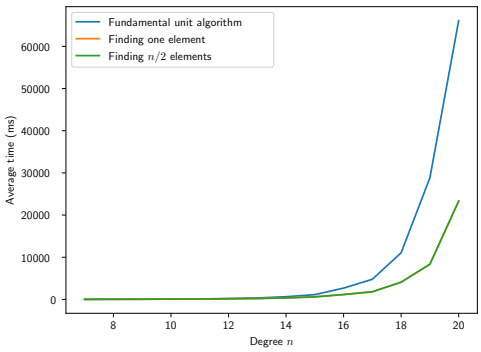
Figure 1: Optimal l value for our algorithm.

From this data it is hard to tell if there is a correlation between the number of elements selected and degree. This could be because a small number of number fields skewed the data. Interestingly, the two different lines match very closely showing that there is very little difference

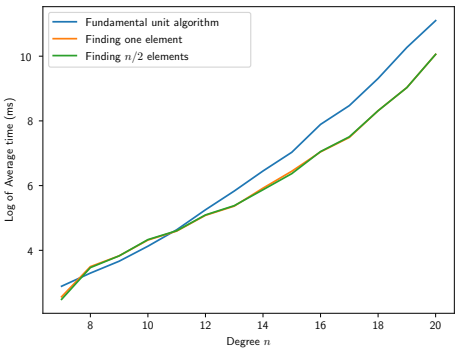
between finding one element and many elements.

4.5 Algorithm Testing

Using the algorithm implementation described in Algorithm 4.2.1 we can compare the performance of our algorithm verses computing the fundamental set of units. From Figure 2 we



(a) Average time comparison between the fundamental unit algorithm and Algorithm 4.2.1



(b) Log of the average time comparison between the fundamental algorithm and Algorithm 4.2.1

Figure 2

see that Algorithm 4.2.1 is faster than the fundamental unit algorithm. Interestingly the difference between computing a single element and $n/2$ elements is fairly similar. When fitting a exponential function to each of the performances we obtained that the average time was $e^{(0.6306\pm0.0005)x-2.07\pm0.10}$ for the original algorithm, $e^{(0.5224\pm0.0004)x-1.08\pm0.09}$ for the single element and $e^{(0.4984\pm0.0003)x-0.83\pm0.06}$ for $n/2$. This new algorithm performs better than the original by a reasonable margin.

4.6 Result for degree 20 number field

Consider the following polynomial $f(x) = x^{20} + 6x^{19} + 6x^{18} + 5x^{17} - 7x^{16} - 3x^{15} + 10x^{14} - 6x^{13} + 10x^{12} + 9x^{11} - 8x^{10} + 5x^8 - x^7 - 2x^4 + 9x^3 - x^2 - 6x - 9$ with $f(\theta) = 0$ and $\mathfrak{p}_{i,j}$ as the jth relevant prime ideal above the prime i. Running Algorithm 4.2.1 on the number field $K = \mathbb{Q}[x]/\langle f(x)\rangle$ we find that we obtain the element $\beta = \alpha_1\alpha_2\alpha_3\alpha_4$ which is an element in the

kernel of the norm mapping from $K^\times/K^{\times 2} \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. The four elements are the following

$$\begin{aligned}
\alpha_1 &= \frac{-1}{3}\theta^{19} - 2\theta^{18} - 2\theta^{17} - \frac{5}{3}\theta^{16} + \frac{7}{3}\theta^{15} + \theta^{14} - \frac{10}{3}\theta^{13} + 2\theta^{12} - \frac{10}{3}\theta^{11} - 3\theta^{10} + \frac{8}{3}\theta^9 \\
&\quad - \frac{5}{3}\theta^7 + \frac{1}{3}\theta^6 + \frac{5}{3}\theta^3 - \frac{14}{3}\theta + 1 \\
\alpha_2 &= \frac{-2}{9}\theta^{19} - \frac{5}{3}\theta^{18} - \frac{10}{3}\theta^{17} - \frac{28}{9}\theta^{16} - \frac{1}{9}\theta^{15} + 3\theta^{14} - \frac{11}{9}\theta^{13} - 2\theta^{12} - \frac{2}{9}\theta^{11} - \frac{16}{3}\theta^{10} \\
&\quad - \frac{11}{9}\theta^9 + \frac{8}{3}\theta^8 - \frac{10}{9}\theta^7 - \frac{13}{9}\theta^6 + \frac{1}{3}\theta^5 + \frac{13}{9}\theta^3 + \frac{8}{3}\theta^2 - \frac{43}{9}\theta - \frac{13}{3} \\
\alpha_3 &= \frac{-1}{9}\theta^{19} - \frac{1}{3}\theta^{18} + \frac{4}{3}\theta^{17} + \frac{13}{9}\theta^{16} + \frac{31}{9}\theta^{15} + 4\theta^{14} + \frac{35}{9}\theta^{13} + 9\theta^{12} - \frac{91}{9}\theta^{11} - \frac{2}{3}\theta^{10} \\
&\quad + \frac{125}{9}\theta^9 - \frac{26}{3}\theta^8 + \frac{85}{9}\theta^7 + \frac{97}{9}\theta^6 - \frac{25}{3}\theta^5 + \frac{38}{9}\theta^3 - \frac{26}{3}\theta^2 - \frac{17}{9}\theta - \frac{11}{3} \\
\alpha_4 &= \frac{4}{9}\theta^{19} + \frac{7}{3}\theta^{18} + \frac{2}{3}\theta^{17} + \frac{11}{9}\theta^{16} + \frac{2}{9}\theta^{15} + \theta^{14} + \frac{40}{9}\theta^{13} - 18\theta^{12} + \frac{94}{9}\theta^{11} + \frac{41}{3}\theta^{10} \\
&\quad - \frac{203}{9}\theta^9 + \frac{56}{3}\theta^8 + \frac{11}{9}\theta^7 - \frac{172}{9}\theta^6 + \frac{25}{3}\theta^5 + \frac{4}{\theta}^4 - \frac{107}{9}\theta^3 + \frac{20}{3}\theta^2 - \frac{22}{9}\theta + \frac{8}{3}
\end{aligned} \tag{62}$$

with the following prime ideal decomposition

$$\begin{aligned}
\langle \alpha_1 \rangle &= \mathfrak{p}_{3,1}^2 \mathfrak{p}_{3,2} \mathfrak{p}_{29,1} \mathfrak{p}_{2273,1} \mathfrak{p}_{3079,1} \mathfrak{p}_{5021,1} \mathfrak{p}_{5387,1} \\
\langle \alpha_2 \rangle &= \mathfrak{p}_{2,1}^3 \mathfrak{p}_{3,1} \mathfrak{p}_{29,1} \mathfrak{p}_{2273,1} \mathfrak{p}_{3079,1} \mathfrak{p}_{5021,1} \mathfrak{p}_{5387,1} \\
\langle \alpha_3 \rangle &= \mathfrak{p}_{3,1}^3 \mathfrak{p}_{3,3} \mathfrak{p}_{79,1} \mathfrak{p}_{139,1} \mathfrak{p}_{193,1} \mathfrak{p}_{523,1} \mathfrak{p}_{1657,1} \mathfrak{p}_{2467,1} \mathfrak{p}_{5417,1} \\
\langle \alpha_4 \rangle &= \mathfrak{p}_{2,1} \mathfrak{p}_{3,1}^3 \mathfrak{p}_{3,3}^3 \mathfrak{p}_{79,1} \mathfrak{p}_{139,1} \mathfrak{p}_{193,1} \mathfrak{p}_{523,1} \mathfrak{p}_{1657,1} \mathfrak{p}_{2467,1} \mathfrak{p}_{5417,1}
\end{aligned} \tag{63}$$

Multiplying these together we obtain

$$\begin{aligned}
\alpha_1\alpha_2\alpha_3\alpha_4 &= \beta \\
&= \frac{-481}{3}\theta^{19} - 1682\theta^{18} - 5505\theta^{17} - \frac{19124}{3}\theta^{16} - \frac{10130}{3}\theta^{15} + 4605\theta^{14} + \frac{9284}{3}\theta^{13} \\
&\quad - 3637\theta^{12} + \frac{18179}{3}\theta^{11} - 1367\theta^{10} - \frac{23152}{3}\theta^9 + 434\theta^8 - \frac{9926}{3}\theta^7 - \frac{11480}{3}\theta^6 \\
&\quad + 6909\theta^5 + 7633\theta^4 + \frac{7736}{3}\theta^3 + 1944\theta^2 - \frac{6281}{3}\theta - 2243
\end{aligned} \tag{64}$$

This has the norm

$$\begin{aligned}
\mathcal{N}_{K|\mathbb{Q}}(\beta) &= 2^4 \times 3^{14} \times 29^2 \times 79^2 \times 139^2 \times 193^2 \times 523^2 \times 1657^2 \times 2273^2 \times 2467^2 \times 3079^2 \\
&\quad \times 5021^2 \times 5387^2 \times 5417^2
\end{aligned} \tag{65}$$

and the prime ideal factorisation

$$\langle \beta \rangle = \mathfrak{p}_{2,1}^4 \mathfrak{p}_{3,1}^9 \mathfrak{p}_{3,2} \mathfrak{p}_{3,3}^4 \mathfrak{p}_{29,1}^2 \mathfrak{p}_{79,1}^2 \mathfrak{p}_{139,1}^2 \mathfrak{p}_{193,1}^2 \mathfrak{p}_{523,1}^2 \mathfrak{p}_{1657,1}^2 \mathfrak{p}_{2273,1}^2 \mathfrak{p}_{2467,1}^2 \mathfrak{p}_{3079,1}^2 \mathfrak{p}_{5021,1}^2 \mathfrak{p}_{5387,1}^2 \mathfrak{p}_{5417,1}^2. \tag{66}$$

Thus, by Theorem 4.0.4 we obtain that this is an element in the kernel. This took 115 relations to find this element and took 5098ms compared to the fundamental unit algorithm which took 29728ms.

5 Summary

We have explored the background for computing units and the unit group of the ring of integers of a number field which has led us to attempt to develop a random unit algorithm. With the limited success of the random unit algorithm we then explored finding elements of square norm

in a number field. This led to the development of an algorithm in PARI to compute elements of square norm. This algorithm performed better than finding a full set of fundamental units and is able to compute a large quantity of elements with minimal additional cost. These results are good but could be improved if one checked whether the elements were square directly (using Theorem 4.0.3). One could also expect improvements if the algorithm was built from the ground up as this algorithm is based of an algorithm for computing a full set of fundamental units. Additionally, modifying the method for finding the kernel in the matrix W_p as described in Section 4 would likely improve the efficiency of the algorithm. We also did not explore any different bounds on the primes which could reduce the time or reduce the spread of the elements.

Acknowledgements

This thesis would not be possible without the resources and support of the University of Canterbury. Brendan Creutz has also provided numerous insights and has been vital in the crafting of this Thesis.

References

[AW03] Saban Alaca and Kenneth S. Williams. *Introductory Algebraic Number Theory*. Cambridge University Press, United Kingdom, 2003.

[Bac90] Eric Bach. Explicit bounds for primality testing and related problems. *Mathematics of Computation*, 55(191):355–380, 1990.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BF14] Jean-François Biasse and Claus Fieker. Subexponential class group and unit group computation in large degree number fields. *LMS Journal of Computation and Mathematics*, 17(A):385–403, 2014.

[BS66] Z. I. Borevich and I. R. Shafarevich. *Number theory*. Academic Press, New York, 1966.

[BS16] Jean-François Biasse and Fang Song. *Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields*, pages 893–902. 2016.

[Buc90] J Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number elds. s eminaire de th eorie des nombres, paris 1988-1989, 27-41, 1990.

[CCC93] Henri Cohen, Henry Cohen, and Henri Cohen. *A course in computational algebraic number theory*, volume 8. Springer-Verlag Berlin, 1993.

[CDO97] Henri Cohen, F Diaz Y Diaz, and Michel Olivier. Subexponential algorithms for class group and unit computations. *Journal of Symbolic Computation*, 24(3-4):433–441, 1997.

[CS23] Brendan Creutz and Duttatrey N. Srivastava. Brauer-manin obstructions on hyperelliptic curves. *Advances in Mathematics*, 431, 2023.

[EHKS14] Kirsten Eisenträger, Sean Hallgren, Alexei Kitaev, and Fang Song. A quantum algorithm for computing the unit group of an arbitrary degree number field. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 293–302, 2014.

[Gal21] Joseph Gallian. *Contemporary abstract algebra*. Chapman and Hall/CRC, 10 edition, 2021.

[HM89] James L Hafner and Kevin S McCurley. A rigorous subexponential algorithm for computation of class groups. *Journal of the American mathematical society*, 2(4):837–850, 1989.

[Ken22] Joseph Kent. Random Brauer Manin obstructions on hyperelliptic curves, summer project at the University of Canterbury. 2022.

[Ken23] Joseph Kent. Jedijoe100/SquareNormElements: Square Norm Elements Algorithm, December 2023.

[LO77] Jeffrey C Lagarias and Andrew M Odlyzko. Effective versions of the chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, volume 7, pages 409–464, 1977.

[Mil21] James S. Milne. Group theory (v4.00), 2021. Available at www.jmilne.org/math/.

[NDR+19] Hamid Nejatollahi, Nikil Dutt, Sandip Ray, Francesco Regazzoni, Indranil Banerjee, and Rosario Cammarota. Post-quantum lattice-based cryptography implementations: A survey. *ACM computing surveys*, 51(6):1–41, 2019.

[PAR22] The PARI Group, Univ. Bordeaux. *PARI/GP version* `2.10.0`, 2022. available from http://pari.math.u-bordeaux.fr/.

[Ros94] H. E. Rose. *A course in number theory.* Clarendon Press, New York;Oxford;, 2nd edition, 1994.

[ST79] Ian Stewart and David O. Tall. *Algebraic number theory.* Chapman and Hall, London;New York;, 1979.

[Ste20] P. Stevenhagen. Number rings. 2020. Available at https://websites.math.leidenuniv.nl/algebra/ant.pdf.

[Zim96] Horst G. Zimmer. *Unit group and class group.* Group Theory, Algebra, and Number Theory. De Gruyter, Inc, Germany, 1996.