university of groningen / faculty of science and engineering / mathematics and applied mathematics

Finding units in $\mathbb{Z}[X]/(f)$ for f a cubic, monic irreducible polynomial with one real root.

Bachelor's Project Mathematics

July 2022

Student: J. Pruim

First supervisor: Prof.dr. J. Top

Second assessor: Dr. P. Kilicer

Contents

1 Introduction

Let $f \in \mathbb{Z}[X]$ be an irreducible monic polynomial, with either of these following criteria:

1. f is quadratic and has two real roots.
2. f is cubic and has exactly one real root.

Consider $R = \mathbb{Z}[\alpha]$, with α a real root of f. According to a special case of Dirichlet's unit theorem, we have that its unit group is of the form

$$R^\times = \{\pm v^k : k \in \mathbb{Z}\}$$

for some unique $v \in R^\times$ satisfying $v > 1$. In this project, we give and implement an algorithm to find units of R and specifically the generator v. Additionally, we give a proof for the fact that the unit group is in this specific form.

First, we look at the norm function, which helps us with determining whether an element in R is a unit. After that, we look at finding units in the quadratic case, which makes use of Dirichlet's theorem. Subsequently, we find an algorithm for finding units in the cubic case. The small vector algorithm gives us a method for finding these units and Minkowski's theorem shows we will find infinitely many units in this way.

2 The Norm and its Relation to Units

In this section, we take a look at the norm function. Specifically important is that we see how the norm precisely determines whether an element in the ring $\mathbb{Z}[X]/(f)$ is a unit. Here we let f be any monic and irreducible polynomial with $\deg(f) \geq 2$. The first subsection defines the norm and discusses some of its properties. The second subsection discusses embeddings and how they can be used to give an alternative but equivalent definition of the norm.

2.1 Defining the Norm

Let us look at $R = \mathbb{Z}[X]/(f)$ as a $\mathbb{Z}$-module. There, we can see that multiplying by an element $r \in R$ is a $\mathbb{Z}$-module homomorphism $\varphi_r : R \to R$, in other words, a linear map. One verifies that the map $r \to \varphi_r$ is a ring homomorphism from R to $\mathrm{End}_{\mathbb{Z}}(R)$. In this way one defines a norm on r by taking the determinant of φ_r.

Definition 2.1.1. Let $f \in \mathbb{Z}[X]$ be monic and irreducible of degree $n \geq 2$, and consider the ring $R = \mathbb{Z}[X]/(f)$. Also, let $L : R \to \mathbb{Z}^n$ be a $\mathbb{Z}$-module isomorphism. Then the norm $N : R \to \mathbb{Z}$ with respect to L is defined as

$$N(r) = \det(L \circ \varphi_r \circ L^{-1}),$$

where $\varphi_r : R \to R$ is the $\mathbb{Z}$-module homomorphism defined by $\varphi_r(s) = rs$ [4].

In other words, the norm of an element r is the determinant of a matrix representation of φ_r. Notice that since this matrix representation is in the integers, we have that $N(r)$ is an integer.

Example. Consider $f = X^2 - d$, with L defined by $L(1 + (f)) = e_1, L(X + (f)) = e_2$ and extended linearly. The ring $R = \mathbb{Z}[X]/(X^2 - d)$ here is isomorphic to $\mathbb{Z}[\sqrt{d}]$. Then we have

$$N(a + bX) = \det \begin{bmatrix} L(a + bX) & L(aX + bX^2) \end{bmatrix} = \det \begin{bmatrix} a & bd \\ b & a \end{bmatrix} = a^2 - db^2.$$

Some students might recognize this norm from the course 'Algebraic Structures'.

It turns out that this norm function has some nice properties, which are summarised in the following proposition.

Proposition 2.1.2. *Consider the ring $R = \mathbb{Z}[X]/(f)$ with $f \in \mathbb{Z}[X]$ monic and irreducible of degree n. Then the following statements hold:*

1. *The norm $N : R \to \mathbb{Z}$ is independent of $\mathbb{Z}$-module isomorphism L.*
2. *The norm $N : R \to \mathbb{Z}$ is multiplicative, meaning that for all $r, s \in R$:*

$$N(rs) = N(r)N(s).$$

3. *$N(r) = 0$ if and only if $r = 0$.*
4. *$N(1) = 1$.*
5. *An element $r \in R$ is a unit if and only if $N(r) = \pm 1$.*

Proof. 1. Let $L, K : R \to \mathbb{Z}^n$ be two $\mathbb{Z}$-module isomorphisms, with corresponding norms N_L, N_K. Then we have

$$\begin{aligned} N_K(r) = \det(K \circ \varphi_r \circ K^{-1}) &= \det(K \circ L^{-1} \circ L \circ \varphi_r \circ L^{-1} \circ L \circ K^{-1}) \\ &= \det(K \circ L^{-1}) N_L(r) \det(L \circ K^{-1}) \\ &= \det(K \circ L^{-1} \circ L \circ K^{-1}) N_L(r) = \det(I) N_L(r) = N_L(r). \end{aligned}$$

2. Let $r, s \in R$ be arbitrary. We obtain

$$\begin{aligned} N(rs) = \det(L \circ \varphi_{rs} \circ L^{-1}) &= \det(L \circ \varphi_r \circ \varphi_s \circ L^{-1}) \\ &= \det(L \circ \varphi_r \circ L^{-1}) \det(L \circ \varphi_s \circ L^{-1}) = N(r)N(s). \end{aligned}$$

3. If $r = 0$, then we have

$$N(0) = \det(L \circ \varphi_0 \circ L^{-1}) = \det(O) = 0.$$

If $N(r) = 0$ however, then we obtain

$$\begin{aligned} 0 &= \det(L \circ \varphi_r \circ L^{-1}). \\ O &= L \circ \varphi_r \circ L^{-1}. \\ \varphi_r &= L^{-1} O L = 0. \end{aligned}$$

Therefore, $r = \varphi_r(1) = 0$.

4. We calculate

$$N(1) = \det(L \circ \varphi_1 \circ L^{-1}) = \det(L \circ \mathrm{id}_R \circ L^{-1}) = \det(\mathrm{id}_{\mathbb{Z}^n}) = 1.$$

5. **'If':** We are given that $K := L \circ \varphi_r \circ L^{-1}$ has determinant ± 1. Therefore it is invertible in $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}^n)$, let us call the inverse $M : \mathbb{Z}^n \to \mathbb{Z}^n$. We are given an injective ring homomorphism

$$R \longrightarrow \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}^n) \ : \ r \mapsto L \circ \varphi_r \circ L^{-1} = K.$$

To see that M is in the image, observe that by Cayley-Hamilton K satisfies an equation

$$K^n + a_{n-1}K^{n-1} + \ldots + a_1 K \pm 1 = 0.$$

Since K is in the image of R under $R \to \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}^n)$, this shows that the same holds for M. As a result, $r \in R^\times$.

'Only if': If r is a unit, then

$$1 = N(1) = N(rr^{-1}) = N(r)N(r^{-1}).$$

However, since $N(r)$ is an integer, the only option is that $N(r) = \pm 1$.

□

2.2 Embeddings

As it turns out, there is also another equivalent way to define the norm. Before we give this definition, we need to discuss embeddings.

Proposition 2.2.1. *Let $f \in \mathbb{Z}[X]$ be monic, irreducible and of degree $n \geq 2$, and let the ring R be $\mathbb{Z}[X]/(f)$. Denote its roots as $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. Then the function $\sigma_i : R \to \mathbb{Z}[\alpha_i] \subset \mathbb{C}$, which is given by*

$$\sigma_i(g + (f)) = g(\alpha_i),$$

is an isomorphism for $i = 1, \ldots, n$. These σ_i's are called the embeddings of R.

Proof. Consider $\mathrm{ev}_{\alpha_i} : \mathbb{Z}[X] \to \mathbb{C}$ to be the evaluation homomorphism. Note that its kernel is precisely all polynomials g s.t. $\mathrm{ev}_{\alpha_i}(g) = g(\alpha_i) = 0$. Since f is irreducible and monic, we have that it is the minimal polynomial for α_i. If we do division with remainder, we see that there is some $r \in \mathbb{Z}[X]$ with $\deg(r) < n$ and $q \in \mathbb{Z}[X]$ such that $g = qf + r$. When we apply ev_{α_i} on both sides, we see that

$$0 = g(\alpha_i) = q(\alpha_i)f(\alpha_i) + r(\alpha_i) = r(\alpha_i),$$

so we see that α_i is a root of r. Since $\deg(r) < n$ and f is the minimal polynomial for α_i, we have that $r = 0$. Therefore, since g was arbitrary in the kernel, we see that $\ker(\mathrm{ev}_{\alpha_i}) = (f)$. Hence by the first homomorphism theorem, we have that

$$R = \mathbb{Z}[X]/(f) \cong \mathrm{ev}_{\alpha_i}(\mathbb{Z}[X]) = \mathbb{Z}[\alpha_i],$$

with corresponding isomorphism σ_i. □

First of all, this proposition immediately tells us that $\mathbb{Z}[X]/(f)$ is isomorphic to $\mathbb{Z}[\alpha]$, with α a root of f. Furthermore, the ring structure of $\mathbb{Z}[\alpha]$ is the same for all roots α of a monic irreducible $f \in \mathbb{Z}[X]$. The embeddings σ_i can be used to translate between these different rings. With these embeddings, we can give our equivalent definition of a norm, which is more straightforward for calculation.

Proposition 2.2.2. *Let $f \in \mathbb{Z}[X]$ be monic and irreducible, of degree $n \geq 2$. Then the norm $N : \mathbb{Z}[X]/(f) \to \mathbb{Z}$ satisfies*

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

for all $r \in \mathbb{Z}[X]/(f)$ [5].

Proof. Consider an arbitrary $r \in \mathbb{Z}[X]/(f)$, and let $g = X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0$ be some polynomial with r as root. In the definition of the norm, let L be the $\mathbb{Z}$-module isomorphism induced by $L(r^{k-1} + (f)) = e_k$ for $k = 1, \ldots, n$. Then $L \circ \varphi_r \circ L^{-1}$ has the following matrix (with respect to the standard basis):

$$\begin{bmatrix} L(r + (f)) & L(r^2 + (f)) & \ldots & L(r^n + (f)) \end{bmatrix} = \begin{bmatrix} & & & \\ e_2 & e_3 & \ldots & \begin{bmatrix} -b_0 \\ -b_1 \\ \vdots \\ -b_{n-1} \end{bmatrix} \end{bmatrix}$$

One can easily see that this matrix has determinant $(-1)^n b_0$. Let us now compute b_0.

We can show that $\sigma_i(r)$ is a root of g for $i = 1, 2, \ldots, n$, using the fact that σ_i is an isomorphism.

$$\begin{aligned} g(\sigma_i(r)) &= (\sigma_i(r))^n + b_{n-1}(\sigma_i(r))^{n-1} + \cdots + b_1\sigma_i(r) + b_0 \\ &= \sigma_i(r^n + b_{n-1}r^{n-1} + \cdots + b_1 r + b_0) = \sigma_i(0) = 0. \end{aligned}$$

Therefore we can expand g over $\mathbb{C}$ as

$$g(X) = (X - \sigma_1(r)) \cdots (X - \sigma_n(r)),$$

and so

$$N(r) = (-1)^n b_0 = (-1)^n g(0) = (-1)^{2n} \prod_{i=1}^{n} \sigma_i(r) = \prod_{i=1}^{n} \sigma_i(r).$$

□

3 Quadratic Extensions

In this section, we focus on quadratic extensions $\mathbb{Z}[X]/(f)$ with $f = X^2 + c_1X + c_0 \in \mathbb{Z}[X]$. Let $\alpha_\pm = \frac{-c_1 \pm \sqrt{c_1^2 - 4c_0}}{2c_0}$ be its roots, then we notice that $c_1 = -\alpha_+ - \alpha_-$ and $c_0 = \alpha_+\alpha_-$. Using this, we see that the norm is given by

$$\begin{aligned} N(a + bX + (f)) = (a + b\alpha_+)(a + b\alpha_-) &= a^2 + ab(\alpha_+ + \alpha_-) + b^2\alpha_+\alpha_- \\ &= a^2 - c_1ab + c_0b^2 \\ &= b^2 f(\frac{-a}{b}). \end{aligned}$$

The latter of course only holds for $b \neq 0$. Therefore, finding units is an equivalent notion to finding integer solutions (a, b) of the equation

$$a^2 - c_1ab + c_0b^2 = \pm 1$$

or equivalently whenever $b \neq 0$;

$$f(\frac{-a}{b}) = \frac{\pm 1}{b^2}.$$

Since f has a positive coefficient for X^2, it has a minimum. If f has a positive minimum , then we cannot make $f(\frac{-a}{b})$ as close to 0 as we like, and therefore, there are only finitely many units in that scenario. In fact, since this implies the order of units to be finite, one can show that no other units are possible than $\pm 1, \pm i, \pm\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$. Hence we wish to look at the more interesting case, where f has a negative minimum. In this case, f has two real irrational roots and the discriminant of f is positive.

In the first subsection, we discuss a principal idea behind finding units that is helpful for $\mathbb{Z}[X]/(f)$ with $f \in \mathbb{Z}[X]$ any monic and irreducible polynomial, it does not have to be quadratic. Subsequently in the second subsection, we find an algorithm specifically for quadratic extensions. In the final subsection, we prove that the unit group in this case is of the form

$$\mathbb{Z}[\alpha_+]^\times = \{\pm\beta^k : k \in \mathbb{Z}\}$$

for some generator $\beta > 1$, and discuss how one can find the generator using found units. The ideas in this section are mostly based on [1] and [8].

3.1 A General Idea for Finding Units

The first idea that one can have when wanting to find units, is to divide elements that generate the same ideal, since they are a unit multiple of each other. A necessary but insufficient condition for two elements to generate the same ideal, is that their norms are equal up to sign, as is proven in the following proposition.

Proposition 3.1.1. *Let $f \in \mathbb{Z}[X]$ be monic, irreducible and of degree $n \geq 2$. Furthermore, let $r, s \in \mathbb{Z}[X]/(f)$ be non-zero and satisfy $(r) = (s)$. Then $|N(r)| = |N(s)|$.*

Proof. Since $(r) = (s)$, we have that there is some unit u such that $r = us$. Since u is a unit, we have that

$N(u) = \pm 1$. We can use the multiplicative property of the norm and obtain

$$|N(r)| = |N(us)| = |N(u)||N(s)| = |N(s)|.$$

□

What we plan to show, is that there is some integer k for which we have finitely many principal ideals (r) with $|N(r)| = k$, but we can find infinitely many elements r with norm $\pm k$. In this way, by the pigeonhole principle, we can find infinitely many elements that generate the same ideal. Then we have a sequence of elements $r_1, r_2, r_3, \ldots$ such that

$$(r_1) = (r_2) = (r_3) = \ldots,$$

and so we can find infinitely many distinct units

$$\frac{r_1}{r_2}, \frac{r_1}{r_3}, \frac{r_1}{r_4}, \ldots$$

Lemma 3.1.2. *Let $f \in \mathbb{Z}[X]$ be monic, irreducible and of degree $n \geq 2$. Also, let $R = \mathbb{Z}[X]/(f)$. Then we have that the set*

$$S = \{(r) \text{ principal ideal of } R : |N(r)| = k\}$$

is finite for all $k \in \mathbb{N}$.

Proof. Throughout this whole proof, $k \in \mathbb{N}$ is arbitrary. Let $L : R \to \mathbb{Z}^n$ be a $\mathbb{Z}$-module isomorphism. Consider $\pi_r \circ L^{-1} : \mathbb{Z}^n \to R/(r)$, where π_r is the canonical map from R to $R/(r)$. It is a composition of surjective $\mathbb{Z}$-module homomorphisms, and therefore a surjective $\mathbb{Z}$-module homomorphism itself. We have:

$$\begin{aligned}\ker(\pi_r \circ L^{-1}) &= \{v \in \mathbb{Z}^n : L^{-1}v \in \varphi_r(R)\} \\ &= (L \circ \varphi_r)(R) = (L \circ \varphi_r \circ L^{-1})\mathbb{Z}^n.\end{aligned}$$

Thus the first homomorphism theorem tells us that (as $\mathbb{Z}$-modules) we have

$$R/(r) \cong \mathbb{Z}^n/(L \circ \varphi_r \circ L^{-1})\mathbb{Z}^n.$$

Isomorphic $\mathbb{Z}$-modules have the same number of elements, and so

$$\#(R/(r)) = \#(\mathbb{Z}^n/(L \circ \varphi_r \circ L^{-1})\mathbb{Z}^n) = |\det(L \circ \varphi_r \circ L^{-1})| = |N(r)|.$$

Therefore we can deduce that

$$S = \{(r) \text{ principal ideal of } R : \#R/(r) = k\}$$

Let (r) be a principal ideal of R such that $\#R/(r) = k$. We can also view $R/(r)$ as an additive group, and so the additive order of any element in $R/(r)$ divides k. This is why for any $s + (r) \in R/(r)$ we deduce that

$$ks + (r) = k \cdot (s + (r)) = 0 + (r).$$

This shows that for any $s \in R$, $ks \in I$ and so $(k) \subset (r)$. Therefore, we currently have

$$S = \{(r) \text{ principal ideal of } R : \#R/(r) = k\} \subset \{(r) \text{ principal ideal of } R : (k) \subset (r)\} = T.$$

Assume for a contradiction that the latter set T has more than k^n elements. Let $b_1, \ldots, b_n$ be a basis for R, and denote any $r \in R$ as

$$r = r_1 b_1 + \cdots + r_n b_n$$

where $r_1, \ldots, r_n \in \mathbb{Z}$. Then there must be distinct $(r), (s) \in T$ such that $r_i \equiv s_i \mod k$ for $i = 1, \ldots, n$, by the pigeonhole principle. In this case, we see that

$$r - s = k(\frac{r_1 - s_1}{k} b_1 + \cdots + \frac{r_n - s_n}{k} b_n) \in (k).$$

Notice that (r) and (s) are in T, and so $(k) \subseteq (r)$ and $(k) \subseteq (s)$. This shows that $r - s \in (r)$ and $r - s \in (s)$. Therefore, $s \in (r)$ and $r \in (s)$, and so $(r) = (s)$. This is a contradiction, so the assumption that T has more than k^n elements is false. Therefore T is finite, and hence S is also finite. □

3.2 Finding Elements of Equal Absolute Norm

In order to find as many elements of small norm as we wish, we like to make use of Dirichlet's theorem, which gives infinitely many good approximations of any irrational number.

Theorem 3.2.1 (Dirichlet)**.** *For any $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ there are infinitely many co-prime pairs $(a, b) \in \mathbb{Z}^2$ with $b \geq 1$ such that*

$$|\frac{a}{b} - \alpha| < \frac{1}{b^2}$$

Proof. Notice that $(a, b) = (\lfloor \alpha \rfloor, 1)$ is already such a pair, so existence is guaranteed. Now assume for a contradiction that there are only t many such pairs. (where t is a natural number.) Let us denote these pairs (a_i, b_i) for $i = 1, \ldots, t$. Now let ϵ be defined as

$$\epsilon = \min\{|\frac{a_i}{b_i} - \alpha| : i = 1, \ldots, t\}.$$

Note that by the irrationality of α, we have that $\epsilon > 0$. Choose $n \in \mathbb{N}$ such that $\frac{1}{n} < \epsilon$. Divide up the half-open interval $(0, 1]$ into subintervals $(0, \frac{1}{n}], \ldots (\frac{n-1}{n}, 1]$. Also consider the numbers $i\alpha - \lfloor i\alpha \rfloor$ for $i = 1, \ldots, n + 1$. These numbers all lay in $(0, 1]$, and by the pigeonhole principle there must be two of them within the same subinterval $(\frac{k}{n}, \frac{k+1}{n}]$. Call these numbers $i\alpha - \lfloor i\alpha \rfloor$ and $j\alpha - \lfloor j\alpha \rfloor$. The difference between these numbers is smaller than $\frac{1}{n}$, and so we see that

$$|(\lfloor i\alpha \rfloor - \lfloor j\alpha \rfloor) - (i - j)\alpha| < \frac{1}{n}.$$

Denote g to be $\gcd(i - j, \lfloor i\alpha \rfloor - \lfloor j\alpha \rfloor)$. Furthermore, let $(a, b) = (\frac{\lfloor i\alpha \rfloor - \lfloor j\alpha \rfloor}{g}, \frac{i-j}{g})$. We then get

$$|a - b\alpha| < \frac{1}{ng}.$$
$$|\frac{a}{b} - \alpha| < \frac{1}{nbg} \leq \frac{1}{b^2 g^2} \leq \frac{1}{b^2}.$$

Here we have used that $n > i - j = bg$. The first inequality of the last line also gives us $|\frac{a}{b} - \alpha| < \frac{1}{n} < \epsilon$, which shows that (a, b) is not one of the pairs $(a_1, b_1), \ldots, (a_t, b_t)$. Therefore the assumption of there only being t such pairs is false, and hence there are infinitely many such pairs. □

From here, we can look at elements $r = a + bX$ with (a, b) as in Dirichlet's theorem, and bound the norm.

Lemma 3.2.2. *Let $f = X^2 + c_1X + c_0 \in \mathbb{Z}[X]$ be irreducible with discriminant $D > 0$ and consider $R = \mathbb{Z}[X]/(f)$. Then we can find infinitely many $r \in R$ such that $|N(r)| < 1 + \sqrt{D}$.*

Proof. Denote $\alpha_\pm = \frac{-c_1 \pm \sqrt{D}}{2}$. Suppose (a, b) is a co-prime pair with $b \geq 1$ such that $|\frac{a}{b} + \alpha_+| < \frac{1}{b^2} \leq 1$. Then we get:

$$\begin{aligned} |N(a + bX)| &= |\sigma_1(a + bX)||\sigma_2(a + bX)| \\ &= b^2|\frac{a}{b} + \alpha_+||\frac{a}{b} + \alpha_-| \\ &< |\frac{a}{b} + \alpha_-| \leq |\frac{a}{b} + \alpha_+| + |\alpha_- - \alpha_+| \leq 1 + \sqrt{D}. \end{aligned}$$

Since there are infinitely many such pairs, we can find infinitely many $r = a + bX \in R$ with $|N(r)| < 1 + \sqrt{D}$. □

Now we can even find infinitely many elements with a specific norm, up to sign.

Corollary 3.2.3. *Given $f = X^2 + c_1X + c_0 \in \mathbb{Z}[X]$ irreducible and with discriminant $D > 0$, and $R = \mathbb{Z}[X]/(f)$, we can find infinitely many $r \in \mathbb{Z}[X]/(f)$ with $|N(r)| = k$ for some integer $1 \leq k < 1 + \sqrt{D}$.*

Proof. We know we can find infinitely many elements in the set

$$\{r \in R : |N(r)| < 1 + \sqrt{D}\} = \cup_{l=1}^{\lfloor 1+\sqrt{D} \rfloor} \{r \in R : |N(r)| = l\}.$$

If we could only find finitely many elements of $\{r \in R : |N(r)| = l\}$ for each $l = 1, \ldots, \lfloor 1 + \sqrt{D} \rfloor$, then we would only be able to find finitely elements of $\{r \in R : |N(r)| < 1 + \sqrt{D}\}$. This is a contradiction, so there is some $k \in \{1, \ldots, 1 + \lfloor \sqrt{D} \rfloor\}$ such that we can obtain infinitely many elements of $\{r \in R : |N(r)| < k\}$. □

Corollary 3.2.4. *Let $f = X^2 + c_1X + c_0 \in \mathbb{Z}[X]$ be irreducible with discriminant $D > 0$. Then there exists a non-trivial unit $u \in \mathbb{Z}[X]/(f)$. (So $u \neq \pm 1$.)*

Proof. From corollary 3.2.3, we know that there is some $1 \leq k < 1 + \sqrt{D}$ for which there are infinitely many $r \in \mathbb{Z}[X]/(f)$ with $|N(r)| = k$. Since by Lemma 3.1.2 there are only finitely many principal ideals (r) with $|N(r)| = k$, we know by the pigeonhole principle that there must be $r \neq \pm s$ with $|N(r)| = |N(s)|$ and $(r) = (s)$. Therefore, there is some unit $u \neq \pm 1$ such that $r = us$. □

3.3 The Generator

Now we wish to prove a special case of Dirichlet's unit theorem for quadratic extensions. The following lemma is general for all extensions $\mathbb{Z}[X]/(f)$ with f monic and irreducible.

Lemma 3.3.1. *Let $f \in \mathbb{Z}[X]$ be irreducible with r_1 real roots and $2r_2$ non-real roots, with roots $\alpha_1, \ldots, \alpha_{r_1+r_2}, \overline{\alpha_{r_1+1}}, \ldots, \overline{\alpha_{r_1+r_2}}$ (In this order specifically). Let σ_i be the corresponding embeddings for*

$i = 1, \ldots, r_1 + 2r_2$. *Then the range of the function* $h : (\mathbb{Z}[X]/(f))\backslash\{0\} \to \mathbb{R}^{r_1+r_2}$ *given by*

$$h(r) = (\log|\sigma_1(r)|, \ldots, \log|\sigma_{r_1+r_2}(r)|)$$

is discrete. Meaning; in all bounded subsets of $\mathbb{R}^{r_1+r_2}$ *there are only finitely many elements in the image of* h.

Proof. It is enough to show there are finitely many elements in closed intervals $(-\infty, C]^{r_1+r_2}$, since any bounded set is contained within such a bounded interval. A non-zero element $r \in \mathbb{Z}[X]/(f)$ with $h(r) \in (-\infty, C]^{r_1+r_2}$ satisfies $\log|\sigma_i(r)| \leq C$ and hence $|\sigma_i(r)| \leq e^C$ for all $i = 1, \ldots, r_1 + r_2$. (Even for the other embeddings as well, as they're just the conjugate.) Consider g given by

$$g = (X - \sigma_1(r)) \cdots (X - \sigma_{r_1+2r_2}(r)),$$

as in the proof of proposition 2.2.2. The absolute value of the k'th coefficient of g is given by

$$\begin{aligned}\left|\sum_{S\subset\{1,\ldots,r_1+2r_2\}:\#S=k}\left(\prod_{j\in S}\sigma_j(r)\right)\right| &\leq \sum_{S\subset\{1,\ldots,r_1+2r_2\}:\#S=k}\left(\prod_{j\in S}|\sigma_j(r)|\right)\\ &\leq \sum_{S\subset\{1,\ldots,r_1+2r_2\}:\#S=k} e^{kC} = \binom{r_1+2r_2}{k}e^{kC}.\end{aligned}$$

Therefore, we see for non-zero r with $h(r)$ in $(-\infty, C]^{r_1+r_2}$, the coefficients of the corresponding g are bounded by a constant (independent of r). So the set

$$\{(X - \sigma_1(r)) \ldots (X - \sigma_{r_1+2r_2}(r)) : r \in h^{-1}((-\infty, C]^{r_1+r_2})\}$$

is finite. Since there are only finitely many r that can correspond to the same g, we can see that the pre-image $h^{-1}((-\infty, C]^{r_1+r_2})$ is finite as well. □

Below is a visualisation of the range of h along with the line $x + y = 0$, for f quadratic with two real roots.

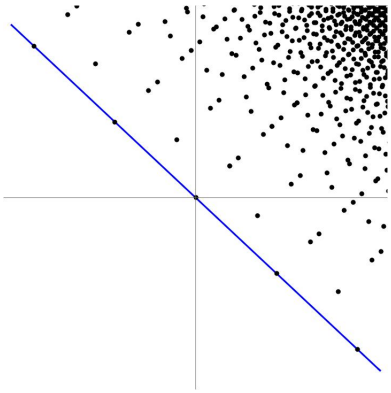

Figure 1: Range of h.

Notice how there are points on this line. As we shall see, these points are precisely the image of units. This

insight helps up in proving a special case of Dirichlet's unit theorem.

Proposition 3.3.2 (Special case of Dirichlet's unit theorem)**.** *Let $f = X^2 + c_1X + c_0 \in \mathbb{Z}[X]$ be irreducible with discriminant $D > 0$, and let $\alpha_\pm$ be its roots. Then $\mathbb{Z}[\alpha_+]^\times$ is of the form*

$$\mathbb{Z}[\alpha_+]^\times = \{\pm\beta^k : k \in \mathbb{Z}\},$$

for some unique $\beta > 1$ in $\mathbb{Z}[\alpha_+]$.

Proof. Consider h as in lemma 3.3.1. Then notice $r \in \mathbb{Z}[X]/(f)$ is a unit precisely when $h(r)$ lies on the line $\{(x, y) \in \mathbb{R}^2 : x + y = 0\}$, since

$$\log|\sigma_1(r)| + \log|\sigma_2(r)| = \log|\sigma_1(r)\sigma_2(r)| = \log|N(r)|.$$

By corollary 3.2.4, there exists some unit $u \neq \pm 1$ in $(\mathbb{Z}[X]/(f))^\times$. Since σ_i is an isomorphism for $i = 1, 2$, we have that $\sigma_i(u) \neq \pm 1$. Therefore, also $h(u) \neq 0$. Consider $(0, h(u)]$; meaning the line-piece from 0 to $h(u)$, excluding 0, but including $h(u)$. This is a bounded region, so by lemma 3.3.1 this line-piece only contains finitely many points in the image of h. It also contains at least one point, namely $h(u)$. Therefore, we find a $h(v)$ on this line-piece for which $||h(v)||$ is minimal.

Now consider $\beta = \max(|\sigma_1(v)|, |\sigma_1(v)|^{-1})$. Suppose for a contradiction that there was a unit $u \in \mathbb{Z}[\alpha_+]^\times$ such that $u > 0$ is not of the form β^n, with $n \in \mathbb{Z}$. Then there would be an integer n such that $\beta^n < u < \beta^{n+1}$. Then we have that $1 < u\beta^{-n} < \beta$. Since $h(\sigma_1^{-1}(u\beta^{-n}))$ and $h(\sigma_1^{-1}(\beta))$ lie on the same line $\{(x, y) \in \mathbb{R}^2 : x + y = 0\}$, this implies that

$$1 < ||h(\sigma_1^{-1}(u\beta^{-n}))|| < ||h(\sigma_1^{-1}(\beta))|| = || \pm h(v)||.$$

The latter comes from the fact that h satisfies $h(\pm v^{-1}) = -h(v)$. This is a contradiction of how we chose v.

If we suppose for a contradiction that there was a $u < 0$ that is not of the form $-\beta^n$, then multiplying by -1 gives us a unit $-u > 0$ not of the form β^n, which is again a contradiction. Therefore, our assumption that there exists such a unit is false and hence the unit group can indeed be written as

$$\mathbb{Z}[\alpha_+]^\times = \{\pm\beta^k : k \in \mathbb{Z}\},$$

where we notice that $\beta > 1$. If there were two such generators $\beta, \gamma > 1$, then we would have

$$\beta = \gamma^k = (\beta^l)^k$$

for some positive integers l, k. This would mean that $1 = lk$, and hence $l = k = 1$. This shows that $\beta = \gamma$ and hence the generator is unique. □

Now that we have the unit group generated by some element $\beta > 1$, let us see if we can out how the units we find relate to the generator. In this way, we can find the generator once we have some units.

Proposition 3.3.3. *Let $f = X^2 + c_1X + c_0 \in \mathbb{Z}[X]$ be irreducible with discriminant $D > 0$, and let α_+, α_- be its roots. Then every unit $u > 1$ (except potentially $\pm\alpha_+$) in $\mathbb{Z}[\alpha_+]$ satisfies $u \geq \sqrt{D-3}$.*

Proof. Let $u = a + b\alpha_+ > 1$ be a unit. As we have seen in the proof of proposition 2.2.2, it is root of the polynomial

$$g(X) = (X - a - b\alpha_+)(X - a - b\alpha_-).$$

Since we see that $\sqrt{D} = \alpha_+ - \alpha_-$, similarly we see here that the discriminant of g is

$$(a + b\alpha_+ - (a + b\alpha_-))^2 = (b\sqrt{D})^2 = b^2 D \geq D.$$

Notice that in the last inequality, we make use of the fact that $b \neq 0$. But also notice that the inverse of $a + b\alpha_+$ is given as $\pm(a + b\alpha_-)$. Therefore, we obtain

$$D \leq (u \mp u^{-1})^2 = u^2 \mp 2 + u^{-2} \leq u^2 + 3.$$

From here, we get $u \geq \sqrt{D-3}$ □

Corollary 3.3.4. *Let $f = X^2 + c_1 X + c_0 \in \mathbb{Z}[X]$ be irreducible with discriminant $D > 0$ and let $\alpha_\pm$ be its roots. Let $u > 1$ be a unit and $n > 1$. Then if $1 < u < (\sqrt{D-3})^n$, we have that $u \in \{v, \ldots, v^{n-1}\}$, where $v > 1$ is the generator.*

Now let us see how any unit we find relates to the generator.

Proof. Let us do a proof by contra-position. Suppose $u \geq v^n$. Then we see that when we apply proposition 3.3.3 on v, we get

$$u \geq v^n \geq (\sqrt{D-3})^n.$$

□

4 Cubic Extensions

In this section, we take a look at cubic extensions $\mathbb{Z}[X]/(f)$, with f monic, irreducible and exactly one real root. The case of f having three real roots will not be discussed here, as there the unit group takes on a more complex form, where it is not generated by one, but two elements.

We start off with some basic algebraic number theory in the first subsection. Additionally, we use Minkowski's theorem to show that there exists an element of a lattice representation of $\mathbb{Z}[X]/(f)$, in any big enough set with appropriate properties. In the second subsection, we take a look at a method to find all points of the lattice within any ellipsoid, called the short vector algorithm. Using the result from the first subsection, we know that such elements exist. It also turns out that such elements are of small norm, and therefore we can use this to find units. In the last subsection, we prove the special case of Dirichlet's unit theorem for cubic extensions with one real root. Furthermore we give a relation between found units and the generator.

4.1 Minkowski's Theorem

Let us first dive into some basic notions of algebraic number theory that are necessary to draw the conclusions we wish to make.

Definition 4.1.1. A field K is called an algebraic number field if it is a field extension of $\mathbb{Q}$ with finite degree. Its ring of integers $\mathcal{O}_K$ is given as

$$\mathcal{O}_K = \{\alpha \in K : p(\alpha) = 0 \text{ for some monic } p \in \mathbb{Z}[X]\}.$$

An order $\mathcal{O} \subset \mathcal{O}_K$ is a subring with finite index.

For any algebraic $\alpha \in \mathbb{C}$ with minimal polynomial f, we have that $\mathbb{Z}[\alpha] \subset \mathcal{O}_{\mathbb{Q}[\alpha]}$ is an order and equivalently $\mathbb{Z}[X]/(f) \subset \mathcal{O}_{\mathbb{Q}[X]/(f)}$ is an order. It may be tempting to say that $\mathcal{O}_{\mathbb{Q}[\alpha]} = \mathbb{Z}[\alpha]$, but this is often not the case.

Example. Consider the algebraic number field $\mathbb{Q}(\sqrt{5})$. Let $\alpha \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$ be arbitrary. Then we know it is the root of some monic quadratic polynomial $X^2 + c_1X + c_0$, so it is of the form $\alpha = \frac{-c_1 \pm \sqrt{c_1^2 - 4c_0}}{2}$. Also, since α is in $\mathbb{Q}(\sqrt{5})$, we have that $c_1^2 - 4c_0$ is of the form $5k^2$, with $k \in \mathbb{Z}$. So we have $\alpha = \frac{-c_1 \pm k\sqrt{5}}{2}$. If we take it modulo 2, we see that $c_1^2 = k^2$ modulo 2. So c_1 and k are of the same parity. If they are both even, then it is easy to see that $\alpha \in \mathbb{Z}[\sqrt{5}]$. If they are both odd, then we can write

$$\alpha = \frac{1+\sqrt{5}}{2} + \frac{(-c_1 - 1) + (-1 \pm k)\sqrt{5}}{2} \in \frac{1+\sqrt{5}}{2} + \mathbb{Z}[\sqrt{5}].$$

Therefore, $\alpha \in \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. Since α was arbitrary, we conclude that $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} \subset \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. The golden ratio $\frac{1+\sqrt{5}}{2}$ has minimal polynomial $X^2 - X - 1$ which is monic, and hence $\frac{1+\sqrt{5}}{2}$ is in $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. We conclude that $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}[\frac{1+\sqrt{5}}{2}] \neq \mathbb{Z}[\sqrt{5}]$.

Definition 4.1.2. The *discriminant* of an order $\mathcal{O} \subset \mathcal{O}_K$ with integral basis $b_1, \ldots, b_n$ (as $\mathbb{Z}$-module) is

defined as

$$\operatorname{disc}(\mathcal{O}) = \det \begin{bmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \cdots & \sigma_1(b_n) \\ \sigma_2(b_1) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \sigma_n(b_1) & \cdots & \cdots & \sigma_n(b_n) \end{bmatrix}^2$$

where $\sigma_1, \ldots, \sigma_n$ are the embeddings.

Example. Let $f = X^3 + c_2X^2 + c_1X + c_0$ be irreducible with exactly one root α_1. Denote the other two complex roots $\alpha_2 = x + iy, \alpha_3 = x - iy$, where $x, y \in \mathbb{R}$. One can do this, because complex roots of real polynomials come in conjugate pairs. We calculate the discriminant of order $\mathbb{Z}[X]/(f) \subset \mathcal{O}_{\mathbb{Q}[X]/(f)}$, which has basis $1, X, X^2$. Then we get

$$\operatorname{disc}(\mathbb{Z}[X]/(f)) = \det \begin{bmatrix} \sigma_1(1) & \sigma_1(X) & \sigma_1(X^2) \\ \sigma_2(1) & \sigma_2(X) & \sigma_2(X^2) \\ \sigma_3(1) & \sigma_3(X) & \sigma_3(X^2) \end{bmatrix}^2 = \det \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & x+iy & (x+iy)^2 \\ 1 & x-iy & (x-iy)^2 \end{bmatrix}^2.$$

In the matrix presented here, every row is a geometric progression. A matrix with this property is called a Vandermonde matrix and has a Vandermonde determinant. Hence, we can calculate this further as

$$\begin{aligned} \operatorname{disc}(\mathbb{Z}[X]/(f)) &= ((\alpha_1 - (x+iy))(\alpha_1 - (x-iy))(2iy))^2 \\ &= -4(y((\alpha_1 - x)^2 + y^2))^2 \\ &= -4y^2((\alpha_1 - x)^2 + y^2)^2 \end{aligned}$$

By setting the imaginary part of $f(\alpha_2)$ equal to 0, we obtain

$$\begin{aligned} 0 &= -y^3 + x^2y + c_2(2xy) + c_1y \\ &= -y(y^2 - (x^2 + 2c_2x + c_1)) \end{aligned}$$

This implies that $y^2 = x^2 + 2c_2x + c_1$, which we can use to calculate this further. Using an algebraic calculator such as Magma, we calculate this to be equal to

$$\operatorname{disc}(\mathbb{Z}[X]/(f)) = -27c_0^2 + 18c_0c_1c_2 - 4c_0c_2^3 - 4c_1^3 + c_1^2c_2^2$$

The following proposition is not as important, but necessary for a proposition about the generator in the last subsection.

Proposition 4.1.3. *Let K be an algebraic number field, and $\mathcal{O}, \mathcal{O}' \subset \mathcal{O}_K$ be two orders with $\mathcal{O} \subset \mathcal{O}'$. Then we have*

$$|\mathit{disc}(\mathcal{O})| \geq |\mathit{disc}(\mathcal{O}')|.$$

[6]

Proof. Let $b_1, \ldots, b_n$ be a basis for $\mathcal{O}'$, and $c_1, \ldots, c_n$ a basis for $\mathcal{O}$, as $\mathbb{Z}$-modules. Then since $\mathcal{O} \subseteq \mathcal{O}'$, every a basis of $\mathcal{O}$ has every basis vector to be an integer linear combination of $b_1, \ldots, b_n$. This shows that there

is some integer matrix M such that

$$\begin{bmatrix} \sigma_1(c_1) & \sigma_1(c_2) & \cdots & \sigma_1(c_n) \\ \sigma_2(b_1) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \sigma_n(c_1) & \cdots & \cdots & \sigma_n(c_n) \end{bmatrix} = M \begin{bmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \cdots & \sigma_1(b_n) \\ \sigma_2(b_1) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \sigma_n(b_1) & \cdots & \cdots & \sigma_n(b_n) \end{bmatrix}.$$

Taking the determinant on both sides and squaring both sides gives us

$$|\mathrm{disc}(\mathcal{O})| = |\det(M)|^2 |\mathrm{disc}(\mathcal{O}')|.$$

Because M is an integer matrix, we know its determinant to be integer. And because of finite index, we know that M is non-singular and therefore $|\det(M)| \geq 1$. This shows the result. □

Minkowski's theorem turns out to be useful for knowing where to find units. This theorem first requires a definition of a lattice.

Definition 4.1.4. An additive subgroup $L \subset \mathbb{R}^n$ is a *lattice* if there exists a basis $b_1, \ldots, b_n$ of $\mathbb{R}^n$ that generates L. In this case, the *determinant* of L, denoted $d(L)$, is defined by

$$d(L) = |\det \begin{bmatrix} b_1 & \ldots & b_n \end{bmatrix}|.$$

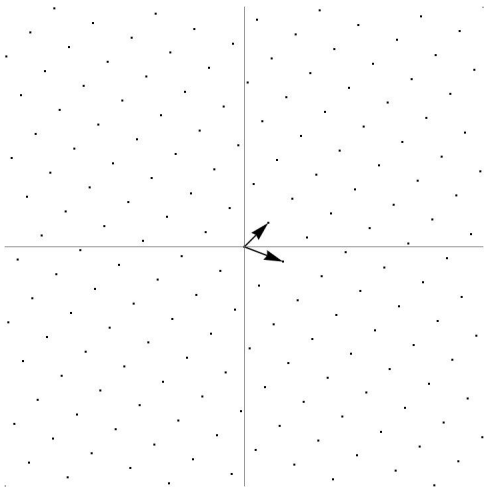

Figure 2: Lattice in $\mathbb{R}^2$ generated by the two depicted vectors.

Theorem 4.1.5 (Minkowski's Theorem)**.** *Let $L \subset \mathbb{R}^n$ be a lattice and let $S \subset \mathbb{R}^n$ be closed, convex and symmetric. If we have that*

$$vol(S) \geq 2^n d(L),$$

then S contains a non-zero lattice point [7].

We can now look at a lattice representation of the ring $\mathbb{Z}[X]/(f)$ and find an element of the ring by finding a lattice point in a nice enough set. Minkowski's theorem helps us with the existence of such a point.

Corollary 4.1.6. *Let $f = X^3 + c_2X^2 + c_1X + c_0$ be irreducible, with exactly one real root, denoted α_1. Furthermore let $\sigma : \mathbb{Z}[X]/(f) \to \mathbb{R}^3$ be defined by*

$$\sigma(r) = (\sigma_1(r), Re(\sigma_2(r)), Im(\sigma_2(r))),$$

where σ_1, σ_2 are the embeddings corresponding to α_1, α_2 respectively. Lastly, let $S \subset \mathbb{R}^3$ be closed, convex and symmetric, with $vol(S) \geq 4\sqrt{|disc(\mathbb{Z}[X]/(f))|}$. Then S contains a non-zero point in the image of σ.

Proof. One can check that σ is an injective $\mathbb{Z}$-module homomorphism. The image of σ therefore forms a lattice in $\mathbb{R}^3$, with basis $\sigma(1), \sigma(X), \sigma(X^2)$, let us call this lattice L. Let $\alpha_2, \overline{\alpha_2}$ be the complex roots of f. Then we obtain

$$\begin{aligned} d(L) = \left| \det \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \mathrm{Re}(\alpha_2) & \mathrm{Re}(\alpha_2^2) \\ 0 & \mathrm{Im}(\alpha_2) & \mathrm{Im}(\alpha_2^2) \end{bmatrix} \right| &= \frac{1}{2} \left| \det \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \mathrm{Re}(\alpha_2) + i\mathrm{Im}(\alpha_2) & \mathrm{Re}(\alpha_2^2) + i\mathrm{Im}(\alpha_2^2) \\ 1 & \mathrm{Re}(\alpha_2) - i\mathrm{Im}(\alpha_2) & \mathrm{Re}(\alpha_2^2) - i\mathrm{Im}(\alpha_2^2) \end{bmatrix} \right| \\ &= \frac{1}{2} \left| \det \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 \\ 1 & \alpha_2 & \alpha_2^2 \\ 1 & \overline{\alpha_2} & \overline{\alpha_2^2} \end{bmatrix} \right| = \frac{1}{2}\sqrt{|\mathrm{disc}(\mathbb{Z}[X]/(f))|}. \end{aligned}$$

Here we have taken complex linear combinations of rows. Therefore, we see that

$$\mathrm{vol}(S) \geq 4\sqrt{|\mathrm{disc}(\mathbb{Z}[X]/(f))|} = 2^3 \frac{1}{2}\sqrt{|\mathrm{disc}(\mathbb{Z}[X]/(f))|} = 2^3 d(L).$$

By Minkowski's theorem, S therefore contains a non-zero lattice point of L, which is indeed in the image of σ. □

4.2 The Short Vector Algorithm

In the first subsection, we have looked at sufficient requirements for a set to contain lattice points in a lattice representation of $\mathbb{Z}[X]/(f)$. In this subsection, we find an actual method to compute all of these lattice points within a big enough ellipsoid. One can check that ellipsoids are closed, convex and symmetric. Therefore we are indeed guaranteed of existence of a lattice point if we take the ellipsoid big enough.

Before we discuss this method, called the Short Vector Algorithm, let us first give some the definition of a quadratic form.

Definition 4.2.1. A *quadratic form* $Q : \mathbb{R}^n \to \mathbb{R}$ is a n-variate polynomial where all terms are of degree 2. This means a quadratic form can always be written as

$$Q(x) = x^T M x$$

for some symmetric matrix $M \in \mathbb{R}^{n \times n}$.

A quadratic form is called *positive definite* if $Q(x) > 0$ for all $x \neq 0$.

Given a positive definite quadratic form $Q : \mathbb{R}^n \to \mathbb{R}$ and a constant C, the Short Vector algorithm computes all the integer vectors $x \in \mathbb{Z}^n$ with $Q(x) \leq C$. Let us illustrate the basic principle for the case

where Q is of the form $Q(x) = q_{1,1}x_1^2 + \cdots + q_{n,n}x_n^2$. We firstly know that any $x \in \mathbb{Z}^n$ with $Q(x) \leq C$ certainly has $|x_1| \leq \sqrt{\frac{C}{q_{1,1}}}$. This creates finitely many possibilities for x_1. With all these possibilities, one can compute that $|x_2| \leq \sqrt{\frac{C-q_{1,1}x_1^2}{q_{2,2}}}$. Then this creates finitely many possibilities for x_2, et cetera. For other quadratic forms, one can do something similar.

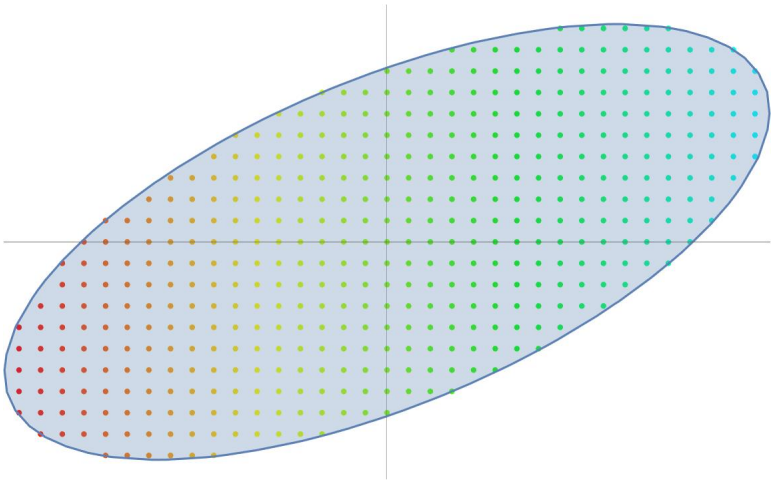

Figure 3: Solutions to $Q(x) \leq C$, with Q a quadratic form in two variables.

This gives rise to the Short Vector algorithm.

Algorithm (Short Vectors)**.** *Let $Q : \mathbb{R}^n \to \mathbb{R}$ be a positive definite quadratic form given by*

$$Q(x) = \sum_{i=1}^{n} q_{i,i}(x_i + \sum_{j=i+1}^{n} q_{i,j}x_j)^2.$$

Then given a constant $C > 0$, the following algorithm computes all $x \in \mathbb{Z}^n$ such that $Q(x) \leq C$:

1. *Set $i = n$, $T_i = C$ and $U_i = 0$.*
2. *Set $Z_i = \sqrt{\frac{T_i}{q_{i,i}}}$, $L_i = \lfloor Z_i - U_i \rfloor$, $x_i = \lceil -Z_i - U_i \rceil - 1$.*
3. *Increase x_i by 1.*
   - *If $x_i > L_i$, increase i by 1. Then repeat step 3.*
   - *If $x_i \leq L_i$ and $i > 1$, then set $T_{i-1} = T_i - q_{i,i}(x_i + U_i)^2$. After that, decrease i by 1, and set $U_i = \sum_{j=i+1}^{n} q_{i,j}x_j$. Then go to step 2.*
   - *If $x_i \leq L_i$ and $i = 1$, then x is a solution, and $Q(x)$ is given by*

$$Q(x) = C - T_1 + q_{1,1}(x_1 + U_1)^2.$$

   Also $-x$ is a solution, with $Q(-x) = Q(x)$. If $x \neq 0$, repeat step 3 for more solutions.

The following quadratic form turns out to be essential to finding the desired lattice points.

Definition 4.2.2. Let $f \in \mathbb{Z}[X]$ be monic and irreducible of degree n. Furthermore let $v \in \mathbb{R}^n$ be with all positive entries. The v-norm $||\cdot||_v^2 : \mathbb{Z}[X]/(f) \to \mathbb{R}$ is defined by

$$||r||_v^2 = \sum_{i=1}^{n} v_i |\sigma_i(r)|^2.$$

If $L : \mathbb{Z}[X]/(f) \to \mathbb{Z}^n$ is a $\mathbb{Z}$-module isomorphism, then $x \to ||L^{-1}x||_v^2$ can be naturally extended to a positive definite quadratic form [2].

Lemma 4.2.3. *Let $f = X^3 + c_2X^2 + c_1X + c_0 \in \mathbb{Z}[X]$ be irreducible and have exactly one real root. Then we can find infinitely many $r \in \mathbb{Z}[X]/(f)$ with $|N(r)| < \frac{3}{\pi}\sqrt{|disc(\mathbb{Z}[X]/(f))|}$.*

Proof. Consider the ellipsoid $S_{h,w}$ given by

$$\begin{aligned} S_{h,w} &= \{(x,y,z) \in \mathbb{R}^3 : \frac{x^2}{h^2} + \frac{y^2+z^2}{w^2} \leq 1\} \\ &= \{(x,y,z) \in \mathbb{R}^3 : \frac{x^2}{h^2} + \frac{|y+iz|^2}{w^2} \leq 1\}. \end{aligned}$$

This ellipsoid has volume $\text{vol}(S_{h,w}) = \frac{4\pi}{3}hw^2$. Choose $h, w > 0$ such that $\text{vol}(S_{h,w}) = 4\sqrt{|\text{disc}(\mathbb{Z}[X]/(f))|}$. Then by Corollary 4.1.6, $S_{h,w}$ contains a non-zero element in the image of σ, let us call it $\sigma(r)$. By applying the Short Vectors Algorithm on the quadratic form defined as in proposition 4.2.2 with the appropriate v, we know we can actually find this element. Since this element is in $S_{h,w}$, we see that

$$\frac{(\sigma_1(r))^2}{h^2} + \frac{|\sigma_2(r)|^2}{w^2} \leq 1,$$

from which we deduce that $|\sigma_1(r)| < h$ and $|\sigma_2(r)|^2 < w^2$. Then we get that

$$|N(r)| = |\sigma_1(r)||\sigma_2(r)|^2 < hw^2 = \frac{3}{4\pi}\text{vol}(S_{h,w}) = \frac{3}{\pi}\sqrt{|\text{disc}(\mathbb{Z}[X]/(f))|}.$$

If you already have t elements $r_1, \ldots, r_t$, with $|N(r_i)| < \frac{3}{\pi}\sqrt{|\text{disc}(\mathbb{Z}[X]/(f))|}$ for $i = 1, \ldots, t$, then one can apply this procedure with $h < \min\{|\sigma_1(r_i)| : i = 1, \ldots, t\}$, and the corresponding appropriate w, given by

$$w = \sqrt{\frac{3}{\pi h}\sqrt{|\text{disc}(\mathbb{Z}[X]/(f))|}}.$$

This way, you will obtain an element $r \in \mathbb{Z}[X]/(f)$ with $|N(r)| < \frac{3}{\pi}\sqrt{|\text{disc}(\mathbb{Z}[X]/(f))|}$, but is not among the $r_1, \ldots, r_n$, since

$$|\sigma_1(r)| < h < \min\{|\sigma_1(r_i)| : i = 1, \ldots, t\}.$$

Therefore, one can find infinitely many $r \in \mathbb{Z}[X]/(f)$ with $|N(r)| < \frac{3}{\pi}\sqrt{|\text{disc}(\mathbb{Z}[X]/(f))|}$ in this fashion. □

Corollary 4.2.4. *Let $f = X^3+c_2X^2+c_1X+c_0 \in \mathbb{Z}[X]$ be irreducible and have exactly one real root α_1. Then we can find infinitely many $r \in \mathbb{Z}[X]/(f)$ with $|N(r)| = k$ for some integer $1 \leq k < \frac{3}{\pi}\sqrt{|disc(\mathbb{Z}[X]/(f))|}$.*

Proof. The proof is completely analogous to the one for corollary 3.2.3. □

Corollary 4.2.5. *Let $f = X^3 + c_2X^2 + c_1X + c_0 \in \mathbb{Z}[X]$ be irreducible with exactly one real root. Then there exists a non-trivial unit $u \neq \pm 1$ of $\mathbb{Z}[X]/(f)$.*

Proof. The proof is completely analogous to the one for corollary 3.2.4. □

4.3 The Generator

Let us prove a special of Dirichlet's unit theorem.

Proposition 4.3.1 (Special case of Dirichlet's unit theorem)**.** *Let $f = X^3 + c_2X^2 + c_1X + c_0 \in \mathbb{Z}[X]$ be irreducible with exactly one root, α_1. Then $\mathbb{Z}[\alpha_1]^\times$ is of the form*

$$\mathbb{Z}[\alpha_1]^\times = \{\pm\beta^k : k \in \mathbb{Z}\}$$

for some unique $\beta > 1$ in $\mathbb{Z}[\alpha_1]^\times$.

Proof. The proof is analogous to the one for proposition 3.3.2, where instead of the line $\{(x, y) \in \mathbb{R}^2 : x+y = 0\}$, the image of h under units lies on the line $\{(x, y) \in \mathbb{R}^2 : x + 2y = 0\}$. □

Proposition 4.3.2. *Let $f = X^3 + c_2X^2 + c_1X + c_0 \in \mathbb{Z}[X]$ be irreducible with exactly one real root α_1. Let u, v be units in $\mathbb{Z}[X]/(f)$ with $1 \leq \sigma_1(v) \leq \sigma_1(u)$. Then we have that*

$$|\sigma_1(v)|^2 + 2|\sigma_2(v)|^2 \leq |\sigma_1(u)|^2 + 2|\sigma_2(u)|^2.$$

Proof. Consider the function $g : \mathbb{R} \to \mathbb{R}$ given by $g(x) = x^2 + \frac{2}{x}$. Its derivative is given by

$$g'(x) = 2(x - \frac{1}{x^2}) = 2\frac{x^3 - 1}{x^2}$$

We see that g' is non-negative in the interval $[1, \infty)$, and so g is non-decreasing there. From that fact and the fact that the norm of units is ± 1, we can derive our result. □

The idea behind this proposition can be seen in the following figure.

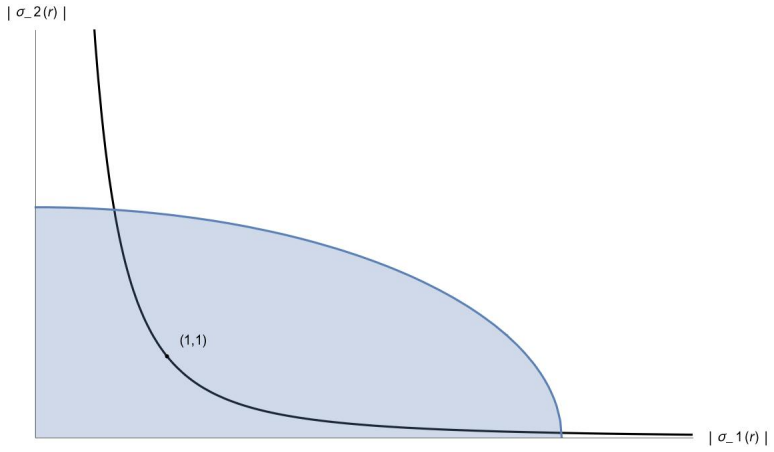

Figure 4: Region $Q(x) \leq C$ along with the curve of units.

Once we have found a unit u using the short vector algorithm, chances are that we have already found the generator, using this proposition as intuition. To be sure, we can apply the short vector algorithm on the quadratic form $Q = ||\cdot||^2_{(1,2)}$ and constant $C = |\sigma_1(u)|^2 + 2|\sigma_2(u)|^2$. Then the proposition tells us that among the elements we find, the unit is there. In practise, this is not a very efficient method. Instead, let us consider the following proposition.

Proposition 4.3.3. *Let $f = X^3 + c_2X^2 + c_1x + c_0 \in \mathbb{Z}[X]$ be irreducible with exactly one real root α_1. Then for every unit $u \in \mathbb{Z}[\alpha_1]$ with $u > 1$, we have that $|disc(\mathbb{Z}[X]/(f))| < 4u^3 + 24$. [3]*

Proof. Denote $u = \sigma_1(r)$ and let us estimate $\sqrt{|\mathrm{disc}(1, r, r^2)|}$. Let us denote $u = x^2$ and $\sigma_2(u) = xe^{iy}, \sigma_3(u) = xe^{-iy}$, for some $x > 1$ and $y \in \mathbb{R}$. Then, thanks to Vandermonde, we compute

$$\begin{aligned}\sqrt{|\mathrm{disc}(1, r, r^2)|} &= |(x^2 - x^{-1}e^{iy})(x^2 - x^{-1}e^{-iy})x^{-1}(e^{iy} - e^{-iy})| \\ &= 2|\sin(y)|(x^3 - 2\cos(y) + x^{-3})\end{aligned}$$

where we used the exponential identities for $\cos(y)$ and $\sin(y)$. We can substitute $\eta = \frac{x^3+x^{-3}}{2}$ and obtain

$$\sqrt{|\mathrm{disc}(1, r, r^2)|} = 4|\sin(y)|(\eta - \cos(y)).$$

Then, we take the partial derivative with respect to y, in attempt to find where the expression is maximal. We get

$$\begin{aligned}g(\cos(y)) = \frac{\partial}{\partial y}[\sin(y)(\eta - \cos(y))] &= \cos(y)(\eta - \cos(y)) + \sin^2(y) \\ &= -2\cos^2(y) + \cos(y)\eta + 1.\end{aligned}$$

Here, $g(X) = -2X^2 + X\eta + 1$ is just a handy notation. Notice that

$$g(\frac{-1}{2x^3}) = -\frac{1}{2x^6} - \frac{\eta}{2x^3} + 1 = \frac{-2 - x^6 - 1 + 4x^6}{4x^6} = \frac{4}{3}(1 - x^{-6}) > 0$$

and also

$$g(1) = -1 + \eta = \frac{-2 + x^3 + x^{-3}}{2} > \frac{-2 + 1^3 + 1^{-3}}{2} = 0.$$

The latter we obtain from the fact that $x^3 + x^{-3}$ is increasing on $[1, \infty)$. To see this, notice that the derivative of $x^3 + x^{-3}$ is $3x^{-4}(x^6 - 1)$, which is non-negative on this interval. Since the leading coefficient of g is negative, we know that any root of g must lay outside the interval $[\frac{-1}{2x^3}, 1]$. Since $\cos(y)$ is always in the interval $[-1, 1]$, this shows that the root we wish lays in interval $[-1, \frac{-1}{2x^3})$. Denote this root $w < \frac{-1}{2x^3}$.

Using that $w\eta = 2w^2 - 1$, we see that

$$\begin{aligned}
|\mathrm{disc}(1, r, r^2)| &\leq 16(1-w^2)(\eta - w)^2 \\
&= 16(1-w^2)(\eta^2 - 2\eta w + w^2) \\
&= 16(1-w^2)(\eta^2 - 2(2w^2-1) + w^2) \\
&= 16(1-w^2)(\eta^2 - 3w^2 + 2) \\
&= 16(\eta^2 - 5w^2 + 2 - w^2\eta^2 + 3w^4) \\
&= 16(\eta^2 - 5w^2 + 2 - (4w^4 - 4w^2 + 1) + 3w^4) \\
&= 16(\eta^2 - w^2 - w^4 + 1) \\
&= 4x^6 + 24 + 4(x^{-6} - 4w^2 - 4w^4).
\end{aligned}$$

Since $w < \frac{-1}{2x^3}$, we have that $\frac{1}{x^6} - 4w^2 < 0$. Therefore, we see that

$$|\mathrm{disc}(1, r, r^2)| \leq 4x^6 + 24 + 4(x^{-6} - 4w^2 - 4w^4) < 4u^3 + 24.$$

However notice that $(1, r, r^2) \subset \mathbb{Z}[X]/(f)$ are orders in $\mathcal{O}_{\mathbb{Q}[X]/(f)}$, so by proposition 4.1.3 we have that

$$|\mathrm{disc}(\mathbb{Z}[X]/(f))| \leq |\mathrm{disc}(1, r, r^2)| < 4u^3 + 24.$$

□

Corollary 4.3.4. *Let $f = X^3 + c_2X^2 + c_1x + c_0 \in \mathbb{Z}[X]$ be irreducible with exactly one root α_1. Also let v be the generator for $\mathbb{Z}[\alpha_1]^\times$. If for $u \in \mathbb{Z}[\alpha_1]$ with $u > 1$, $4u^{3/n} + 24 \leq |disc(\mathbb{Z}[X]/(f))|$, then $u \in \{v, \ldots, v^{n-1}\}$.*

Proof. A proof by contraposition. Suppose that $u \geq v^n$. Then apply proposition 4.3.3 on v to see that

$$4u^{3/n} + 24 \geq 4v^3 + 24 > |\mathrm{disc}(\mathbb{Z}[X]/(f))|.$$

□

5 Units for reducible f

A natural question to ask is how to find units in $\mathbb{Z}[X]/(f)$ when $f \in \mathbb{Z}[X]$ is not of the type discussed. One could for example look at the case where we let go of the criterion that f is irreducible. This is what we look at in this short section. Let us write a reducible $f \in \mathbb{Z}[X]$ as a product of monic polynomials.

Proposition 5.0.1. *Let $f, f_1, \ldots, f_k \in \mathbb{Z}[X]$ be monic such that $f = f_1 \cdots f_k$. Then $r + (f)$ is a unit in $\mathbb{Z}[X]/(f)$ if and only if $r + (f_i)$ is a unit in $\mathbb{Z}[X]/(f_i)$ for all $i = 1, \ldots, k$.*

Proof. If: Given is that $r + (f_i)$ is a unit in $\mathbb{Z}[X]/(f_i)$ for all $i = 1, \ldots, k$. Then we obtain that there exist polynomials $s_1, \ldots, s_k$ such that $rs_i - 1 \in (f_i)$ for all i. If we take the product of these $rs_i - 1$, and think about how multiplying it out works, then we get that there is some polynomial $t \in \mathbb{Z}[X]$ such that

$$(-1)^{n+1} \prod_{i=1}^{n} (rs_i - 1) = rt - 1.$$

Because each $rs_i - 1$ is a multiple of f_i, we know that $rt - 1$ is a multiple of $f_1 \cdots f_k = f$, and therefore $rt - 1 \in (f)$. This shows that $r + (f)$ is a unit in $\mathbb{Z}[X]/(f)$.

Only if: Since $r + (f)$ is a unit in $\mathbb{Z}[X]/(f)$, we have that there is some $s \in \mathbb{Z}[X]$ such that $rs - 1 \in (f)$. Since $f = f_1 \cdots f_k$, we have that $(f) \subset (f_i)$ for all i. Therefore, $rs - 1 \in (f_i)$ for all i, and hence $r + (f_i)$ is a unit in $\mathbb{Z}[X]/(f_i)$ for all i. □

From this proposition, we have a way of determining units in $\mathbb{Z}[X]/(f)$, but to determine the group structure of the unit group is not always as obvious.

6 Implementations

6.1 Quadratic case

Example 6.1.1. We shall take $f = X^2 + 3X - 3$. It has roots $\alpha_\pm = \frac{-3\pm\sqrt{21}}{2}$, which are irrational and real. So f is of the type of polynomial we'd like to study. In order to do this, we approximate $-\alpha_+ = -\frac{-3+\sqrt{21}}{2}$. We shall do this with the method used in the proof of Dirichlet's Theorem. First off, we can approximate $-\alpha_+$ with $\lfloor -\alpha_+ \rfloor = \frac{-1}{1}$. This gives us element $-1-X$, which has norm $(-1-\alpha_+)(-1-\alpha_-) = f(-1) = -5$. Then we take $\epsilon = |-1+\alpha_+| \approx 0.21 > \frac{1}{5} = \frac{1}{n}$. Let us take a look at the intervals $[0,\frac{1}{5}),\ldots,[\frac{4}{5},1)$. We have $-\alpha_+ \approx -1 + 0.21$ and $-6\alpha_+ \approx -5 + 0.25$. The numbers 0.21 and 0.25 are both in $[\frac{1}{5},\frac{2}{5})$. From this we see that $|5\alpha_+ - 4| \approx 0.04 < \frac{1}{5}$. So let us look at the element $-4+5X$. It has norm

$$N(-4+5X) = (-4+5\alpha_+)(-4+5\alpha_-) = 16 + 20(-\alpha_+ - \alpha_-) + 25\alpha_+\alpha_- = 16 + 60 - 75 = 1.$$

So in $\mathbb{Z}[\alpha_+]$, $-4+5\alpha_+$ has inverse $-4+5\alpha_- = -4+5(-3-\alpha_+) = -19-5\alpha_+$. So we have a unit $u = 19+5\alpha_+ > 1$. Magma tells us that the polynomial X^2-u is factorable as $(X-\alpha_+-4)(X+\alpha_++4)$, so we know that $u = (4+\alpha_+)^2$ and so $4+\alpha_+$ is also a unit. Notice that $4+\alpha_+ = \frac{5+\sqrt{21}}{2} \approx 4.79 < 18 = (\sqrt{D-3})^2$. Therefore $4+\alpha_+$ is the generator and we have

$$\mathbb{Z}[\frac{-3+\sqrt{21}}{2}]^\times = \{\pm(\frac{5+\sqrt{21}}{2})^k : k \in \mathbb{Z}\}.$$

Example 6.1.2. Let us take $f = X^2 - 29$. The roots are $\pm\sqrt{29}$. Let us approximate $\sqrt{29}$ with the method of Dirichlet's theorem. Our first approximation is $\lfloor\sqrt{29}\rfloor = \frac{5}{1}$. This gives rise to element $5-X$, with norm

$$N(5-X) = (5-\sqrt{29})(5+\sqrt{29}) = 25 - 29 = -4.$$

Let us therefore search further. Set $\epsilon = |\sqrt{29}-5| \approx 0.39 > \frac{1}{3} = \frac{1}{n}$. Consider the intervals $[0,\frac{1}{3}),[\frac{1}{3},\frac{2}{3})$ and $[\frac{2}{3},1)$. We calculate that $\sqrt{29} \approx 5.39$ and $4\sqrt{29} \approx 21.54$. Notice that 0.39 and 0.54 are both in $[\frac{1}{3},\frac{2}{3})$. We see that $|3\sqrt{29}-16| \approx 0.16 < \frac{1}{3}$. So let us consider the element $3X-16$. Its norm is given as

$$N(3X-16) = (3\sqrt{29}-16)(-3\sqrt{29}-16) = -9\cdot 29 + 16^2 = -5.$$

We have not found a unit yet, so let us continue searching. Let $\epsilon = \min(|\sqrt{29}-5|, |\sqrt{29}-\frac{16}{3}|) \approx 0.052 > \frac{1}{20} = \frac{1}{n}$. We consider the intervals $[0,\frac{1}{20}),\ldots,[\frac{19}{20},1)$. We calculate $\sqrt{29} \approx 5.3852$ and $14\sqrt{29} \approx 75.3923$. So then we get $13\sqrt{29} - 70 \approx 0.007 < \frac{1}{13}$. The element $13X-70$ has norm

$$N(13X-70) = (13\sqrt{29}-70)(-13\sqrt{29}-70) = -169\cdot 29 + 4900 = -1.$$

Therefore, $13\sqrt{29}-70$ is a unit. However, we must take its inverse to get a unit bigger than 1. The inverse is given by $u = 13\sqrt{29}+70 \approx 140.007$. The discriminant is $D = 4\cdot 29 = 116$, so we see that $u < (\sqrt{D-3})^3$. Therefore $u = v$ or $u = v^2$, where v is the generator. Since Magma tells us that the polynomial X^2-u is irreducible in $\mathbb{Q}(\sqrt{29})[X]$, we know that u is indeed the generator. Therefore we get

$$\mathbb{Z}[\sqrt{29}]^\times = \{\pm(13\sqrt{29}+70)^k : k \in \mathbb{Z}\}.$$

6.2 Cubic case

Example 6.2.1. Let us look at an unlucky polynomial and see if the algorithm even works without luck. The polynomial $f = X^3 + X + 13$ has derivative $3X^2 + 1$, which is always positive. Therefore, f is monotonic and hence we know for sure that f has only one real root. Also, it doesn't have any rational roots, because any rational root has to be an integer dividing 13. Therefore, since it's a cubic polynomial, it is irreducible. We can calculate the discriminant to be -4567 (Remember that we calculated the general formula for the discriminant in subsection 4.1).

MATLAB finds a unit in $\mathbb{Z}[\alpha_1]^\times$ which is $u = 1206 - 453\alpha_1 + 205\alpha_1^2 \approx 3208.04$. (where $\alpha_1 \approx -2.2098$ is the real root of f) We calculate that $4u^{3/4} + 24 < |\mathrm{disc}(\mathbb{Z}[X]/(f))|$. Therefore, corollary 4.3.4 gives us that either $u = v$, $u = v^2$ or $u = v^3$, where v is the generator. Magma tells us that the polynomials $X^2 - u, X^3 - u$ are irreducible in $\mathbb{Z}[\alpha_1]$, and therefore $u = v$ must be the case. Hence we obtain

$$\mathbb{Z}[\alpha_1]^\times = \{\pm(1206 - 453\alpha_1 + 205\alpha_1^2)^k : k \in \mathbb{Z}\}.$$

Example 6.2.2. Let us take a look at $f = X^3 - 23$. MATLAB finds two elements of norm -2 which differ by a multiple of 2, namely r, s given by

$$r = -10619 - 3734\sqrt[3]{23} - 1313\sqrt[3]{23}^2$$
$$s = -39 + 136\sqrt[3]{23} - 43\sqrt[3]{23}^2.$$

Dividing these two elements gives a unit $u = 2166673601 + 761875860\sqrt[3]{23} + 267901370\sqrt[3]{23}^2 \approx 6.5 \cdot 10^9$. Since we see that $4u^{3/9} + 24 < |\mathrm{disc}(\mathbb{Z}[\sqrt[3]{23}])| = 14283$, we have that $u \in \{v, \ldots, v^8\}$, where v is the generator. Magma gives that the polynomials $X^k - u$ are irreducible for $k = 2, \ldots, 8$. Therefore, u is the generator, and we see that

$$\mathbb{Z}[\sqrt[3]{23}]^\times = \{\pm(2166673601 + 761875860\sqrt[3]{23} + 267901370\sqrt[3]{23}^2)^k : k \in \mathbb{Z}\}.$$

Example 6.2.3. Take $f = X^3 + 4X^2 - 13X + 27$, just to take something random. One can calculate the local minimum to be positive, so this has exactly one real root. We find two elements of norm -3 differing by a multiple of 3, given by

$$r = -19428 + 12301\alpha_1 - 4744\alpha_1^2$$
$$s = 21 - 10\alpha_1 - 2\alpha_1^2.$$

Dividing r by $-s$ gives a unit $u = 4190542 - 2653277\alpha_1 + 1023262\alpha_1^2 \approx 6.6 \cdot 10^7$. Since $4u^{3/6} + 24 < |\mathrm{disc}(\mathbb{Z}[\sqrt[3]{23}])|$, we know $u \in \{v, v^2, v^3, v^4, v^5\}$, where v is the generator. We factorise $X^k - u$ in $\mathbb{Q}(\alpha_1)[X]$ using Magma for $k = 2, 3, 4, 5$. There, the only linear factors we find are not in $(\mathbb{Z}[\alpha_1])[X]$, and hence we deduce that u is the generator. Hence we see

$$\mathbb{Z}[\alpha_1]^\times = \{\pm(4190542 - 2653277\alpha_1 + 1023262\alpha_1^2)^k : k \in \mathbb{Z}\}.$$

7 Conclusion

In this project, we studied the unit group of $\mathbb{Z}[X]/(f)$ for the following two cases:

1. The polynomial $f = X^2 + c_1X + c_0 \in \mathbb{Z}[X]$ is irreducible with two real roots.
2. The polynomial $f = X^3 + c_2X^2 + c_1X + c_0 \in \mathbb{Z}[X]$ is irreducible with exactly one real root.

In both cases, we have proven that the unit group is of the form

$$(\mathbb{Z}[X]/(f))^\times = \{\pm\beta^k : k \in \mathbb{Z}\}$$

for some unit $\beta \neq \pm 1$. We have developed methods for finding units and successfully implemented them. For the quadratic case, this was done using Dirichlet's theorem. For the cubic case, this was done using the Short Vector Algorithm. The Short Vector Algorithm can also be applied to the quadratic case, but there is no need for that, since applying Dirichlet's theorem is already effective enough.

Implementing the Short Vector Algorithm within Matlab had one downside however. When the ratio between the height and width of the ellipsoid becomes too small, Matlab does not recognize the quadratic form as positive definite anymore and the algorithm stops working. In most cases, we found enough units before this happened. Still there are some cubic extensions for which this is a problem.

What we have not done in this project, is look at the case where f is of fourth degree with no real roots. Dirichlet's unit theorem claims that in this case we also have the unit group to be of the form $\{\pm\beta^k : k \in \mathbb{Z}\}$. Proving this and finding units in this case can be done similarly to the cubic case.

Even more so, for any monic and irreducible f, we can find units similarly to the cubic case. When the degree of f is large, it may be good to replace the ordinary Short Vector Algorithm with the Fincke-Pohst Algorithm. This is just an improved version, improving on the speed. In general, Dirichlet's unit theorem says that if $f \in \mathbb{Z}[X]$ is monic and irreducible and has r_1 real roots and r_2 conjugate pairs of non-real roots, then the unit group is given in the form

$$(\mathbb{Z}[X]/(f))^\times = \{\zeta^l\beta_1^{k_1}\dots\beta_{r_1+r_2-1}^{k_{r_1+r_2-1}} : l, k_1, \dots, k_{r_1+r_2-1} \in \mathbb{Z}\}.$$

Here, ζ is some root of unity and $\beta_1, \dots, \beta_{r_1+r_2-1}$ are some multiplicatively independent units not being ± 1. Therefore, for other f, the difficulty lies in finding these multiple generators $\beta_1, \dots, \beta_{r_1+r_2-1}$. Namely, it can be tough to actually show that elements are multiplicatively independent. We see that even though we can still find units, finding the unit group becomes tougher.

Proving Dirichlet's unit theorem in general could perhaps be done as follows. First, one shows that the function h as in Lemma 3.3.1 maps the unit group into a subspace of $\mathbb{R}^n$ with dimension $r_1 + r_2 - 1$, where r_1 is the number of real roots of f and r_2 is the number of conjugate pairs of non-real roots of f. Then, one proves that specifically, the unit group gets mapped onto an additive subgroup of this subspace, generated by a basis for the subspace. (Similarly to how a lattice is defined) In this latter step, there might be some difficulty, as it could be hard to show that this image of units under h doesn't form a group generated by less than $r_1 + r_2 - 1$ elements.

MATLAB Codes

The following is an implementation of the Short Vector Algorithm in MATLAB.

```
function [arr,outp]=shortvecalg(Q,const)
    % [arr,outp]=shortvecalg(Q,const).
    % Calculates an array arr of row vectors arr(i) s.t. outp(i)=arr(i,:)*Q*arr(i,:)^T≤const.
    count=1;
    [n,¬]=size(Q);
    i=n;
    T=const*ones(1,n);
    U=zeros(1,n);
    x=ones(1,n);
    Z=sqrt(T./diag(Q)');
    L=floor(Z-U);
    x=ceil(-Z-U)-1;
    step=2;
    while (1)
        if (step==2)
            Z(i)=sqrt(T(i)/Q(i,i));
            L(i)=floor(Z(i)-U(i));
            x(i)=ceil(-Z(i)-U(i))-1;
            step=3;
        end
        if (step==3)
            x(i)=x(i)+1;
            if (x(i)>L(i))
                i=i+1;
                step=3;
                continue;
            elseif (i>1)
                T(i-1)=T(i)-Q(i,i)*(x(i)+U(i))^2;
                i=i-1;
                U(i)=0;
                for j=i+1:n
                   U(i)=U(i)+Q(i,j)*x(j);
                end
                step=2;
                continue;
            else
                arr(count,:)=x;
                outp(count)=const-T(1)+Q(1,1)*(x(1)+U(1))^2;
                if (x==0)
                    return;
                end
                count=count+1;
                step=3;
                continue;
            end
        end
    end
end
```

The matrix corresponding to the v-norm is calculated in the following function.

```
function M=vnorm2matrix(v,alpha1,alpha2)
    % M=vnorm2matrix(v,alpha1,alpha2)
    % Turns the vnorm^2 into the matrix M corresponding to it, s.t.
    % [a b c]*M*[a b c]' is ||a+bX+cX^2||_(log.(v))^2.
    % Warning: this computes it without raising e to v(i)'s, it
    % just takes the v(i)'s.
    if (v(1)≤0 || v(2)≤0)
        error('vnorm2matrix needs positive entries for v');
    end
    x=real(alpha2);
    y=imag(alpha2);
    sigma1mat=[1,alpha1,alpha1^2;
        alpha1,alpha1^2,alpha1^3;
        alpha1^2,alpha1^3,alpha1^4];
    sigma2mat=[1,x,x^2-y^2;
        x,x^2+y^2,x*(x^2+y^2);
        x^2-y^2,x*(x^2+y^2),(x^2+y^2)^2];
    M=v(1)*sigma1mat+v(2)*sigma2mat;
end
```

The following function `sigma` calculates the output of an embedding corresponding to `alpha` with element represented by `arr` with respect to basis $1, X, X^2$.

```
function y=sigma(arr,alpha)
    [¬,k]=size(arr);
    if (k≠3)
        error('Wrong input type, array has incorrect size.');
    end
    y=arr(:,1)+arr(:,2)*alpha+arr(:,3)*alpha^2;
end
```

Using the function `sigma`, the function `algnorm` calculates the norm of an element represented by `arr` with respect to basis $1, X, X^2$.

```
function y=algnorm(arr,alpha1,alpha2)
    y=round(sigma(arr,alpha1).*abs(sigma(arr,alpha2)).^2);
end
```

Now in our main file, we use the Short Vector Algorithm to calculate elements of small norms, and display a table with their coordinates (with respect to basis $1, X, X^2$), their norm, and the coordinates modulo the absolute norm. The latter is done to detect when two elements have the same absolute norm N and differ by a multiple of N. This table is sorted with respect to the absolute norm. A factor `fact` is used to increase the volume of the ellipsoid. This increases both the number of elements as well the variance in norm. In practise, this factor is set high to find more elements.

```
clear all;
c2=4;
```

```
c1=-13;
c0=27;
f=@(x) x.^3+c2*x.^2+c1*x+c0;
df=@(x) 3*x.^2+2*c2*x+c1;
tol=10^-10;
x0=-c2;
maxIt=10^7;
% Calculating alpha1, the real root of f.
[alpha1,success,¬,¬]=newton(f,df,x0,tol,maxIt);
if success≠1
    error('Approximation of alpha1 not close enough. Try increasing the maximal number of
    iterations.');
end
% Here we write the complex roots as x+iy and x-iy, and use relations we derived earlier.
x=(-c2-alpha1)/2;
if 3*x^2+2*c2*x+c1≤0
    error('Polynomial has three real roots. Change the coefficients please.');
end
y=sqrt(3*x^2+2*c2*x+c1);
alpha2=x+1i*y;
alpha3=x-1i*y;
disc=-27*c0^2+18*c0*c1*c2-4*c0*c2^3-4*c1^3+c1^2*c2^2;
fact=10^4;
% A is the maximal norm.
A=3/pi*sqrt(abs(disc))*fact;
k1=10^6;
k2=sqrt(A/k1);
totalelms=[];
while (k1≥10^-8)
    M=vnorm2matrix([1/(k1^2),1/(k2^2)],alpha1,alpha2);
    % Here we transform the quadratic form to the desired form, in order to apply the ...
        short vector algorithm. The loop breaks if the Cholesky Factorisation does not work.
    try C=chol(M);
    catch ME
        break;
    end
    Q=zeros(3);
    for i=1:3
        for j=i:3
            if (i==j)
                Q(i,j)=C(i,j)^2;
            else
                Q(i,j)=C(i,j)/C(i,i);
            end
        end
    end
    [elms,outp]=shortvecalg(Q,1);
    [s,¬]=size(elms);
    % We omit the final row vector, as it is always the zero vector.
    totalelms=[totalelms;elms(1:s-1,:)];
    % If for some reason, MATLAB does not detect the non-zero vector with bounded ...
        quadratic form, we just lower the height and try again.
    if (s==1)
       k1=0.99*k1;
```

```
        k2=sqrt(A/k1);
        continue;
    end
    % The 0.99 is to make sure the height is strictly smaller than the sigma_1 of any element.
    k1=0.99*min(abs(sigma(elms(1:s-1,:),alpha1)));
    k2=sqrt(A/k1);
end
% Filtering out duplicate elements, that can still occur due to rounding errors.
totalelms=unique(totalelms,'rows');
norms=algnorm(totalelms,alpha1,alpha2);
array=[totalelms norms];
sortedarray=[];
modulosortedarray=[];
nicearraytemp=[];
% Sorting the elements based on norm, and also calculating the coordinates modulo the ...
    absolute norm.
for N=1:floor(A/fact)
    nicearray=array(abs(norms)==N,:);
    tempmoduloarray=rem(nicearray(:,1:3),N)+N;
    tempmoduloarray=rem(tempmoduloarray,N);
    sortedarray=[sortedarray;nicearray];
    modulosortedarray=[modulosortedarray;tempmoduloarray];
end
% Outputting the table
table=array2table([sortedarray modulosortedarray ...
    sigma(sortedarray(:,1:3),alpha1)],'VariableNames',{'a','b','c','N(orm)','a mod |N|','b ...
    mod |N|', 'c mod |N|','Sigma1'})
```

This makes use of the function `newton`, which calculates roots using the newton method. I won't add the MATLAB code for that function, as it is nothing special.

References

[1] Wieb Bosma, Jaap Top, and Jan Brinkhuis. Algebra & getaltheorie, 2019.

[2] Henri Cohen. *A course in computational number theory*. Springler, 1996.

[3] James S. Milne. Algebraic number theory (v3.08), 2020. Available at `www.jmilne.org/math/`.

[4] Joseph Jonah Rotman. *Advanced modern algebra*, page 940. Prentice Hall, 2002.

[5] Joseph Jonah Rotman. *Advanced modern algebra*, page 943. Prentice Hall, 2002.

[6] William Stein. *A brief Introduction to classical and adelic Algebraic Number Theory*. online, 2004.

[7] Peter Stevenhagen. The arithmetic of number rings. 01 2008.

[8] L. van Timmeren. Eenheden van de polynoomring van gehele getallen geëvalueerd in derdemachtswortel m.