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

Finding units in the quotient ring $\mathbb{Z}[X]/(f)$

Bachelor's Project Mathematics

July 2025

Student: Jelmer Bouma

First supervisor: Jaap Top

Second assessor: Ekin Ozman

Contents

This thesis discusses a proof that $\mathbb{Z}[X]/(f)$ always contains a nontrivial unit for monic, irreducible f of degree 4 with no real roots. We also discuss the structure of the unit group of this ring.

1 Introduction

Consider f a polynomial with integer coefficients that is monic, irreducible and of degree 4 with no real roots. We can show that

$$\mathbb{Z}[X]/(f) \cong \mathbb{Z}[\alpha],$$

with α a root of f. We show that the unit group of $\mathbb{Z}[\alpha]$ is an abelian group of rank 1, and moreover that

$$\mathbb{Z}[\alpha]^\times \cong \mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

for some specific values of n.
To prove this, we consider a specific norm function, with the norm being multiplicative and the property that the norm of an element is ± 1 if and only if that element is a unit. We rewrite the norm as a product of embeddings. First we show that $\mathbb{Z}[X]/(f)$ has a nontrivial unit. From this, we show that all the units land on a line under the image of a certain function with even spacing, and hence we have a single generator.

2 The Norm Function and Embeddings

2.1 The Norm

One of the goals of this paper is to find units in $\mathbb{Z}[X]/(f)$, with f monic, irreducible and of degree 4 with no real roots. To start finding these units, we introduce a handy function, namely the norm function. This section is largely based on [3].
Notice that, in general for such f with degree n, we have that $\mathbb{Z}[X]$ is isomorphic as a $\mathbb{Z}$-module to $\mathbb{Z}^{\deg(f)}$, under the following isomorphism: $L : \mathbb{Z}[X]/(f) \to \mathbb{Z}^n$, with

$$c_{n-1}X^{n-1} + \ldots + c_1X + c_0 \mapsto (c_{n-1}, \ldots, c_1, c_0).$$

We can now define the norm, we write $R := \mathbb{Z}[X]/(f)$ to avoid a notational mess.

Definition 2.1 (norm)**.** *Consider $\mathbb{Z}[X]/(f)$ with f monic, irreducible, and of degree n. Let $L : \mathbb{Z}[X]/(f) \to \mathbb{Z}^n$ be a $\mathbb{Z}$ module isomorphism. Then the norm is defined as*

$$N_L(r) = det(L \circ \phi_r \circ L^{-1}),$$

where $\phi_r : \mathbb{Z}[X]/(f) \to \mathbb{Z}[X]/(f)$ is the linear map multiplying by $r \in \mathbb{Z}[X]/(f)$ from the left.

Note that since $L^{-1} \circ \phi_r \circ L$ is a linear map from $\mathbb{Z}^n$ to $\mathbb{Z}^n$, we get that $N_L(r)$ is an integer. We show some properties of this norm, where property 4 is a main ingredient for later results.

Theorem 2.1. *Consider the norm $N : \mathbb{Z}[X]/(f) \to \mathbb{Z}$, with f monic, irreducible, and of degree n. Then the following statements hold:*

1. *N is independent of the chosen $\mathbb{Z}$-module isomorphism L.*
2. *N is multiplicative, so $N(rs) = N(r)N(s)$ for all $r, s \in \mathbb{Z}[X]/(f)$.*
3. *$N(1) = 1$.*
4. *$N(r) = \pm 1$ if and only if $r \in (\mathbb{Z}[X]/(f))^\times$, i.e. r is a unit.*
5. *[5] $N(r) \neq 0$ if and only if R/rR is finite, and in that case, $\#R/rR = |N(r)|$.*

Proof. 1. Take K, L to be two $\mathbb{Z}$-module isomorphisms as above. Then we have

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

2. Let $r, s \in \mathbb{Z}[X]/(f)$. Then we have

$$\begin{aligned} N(r)N(s) &= \det(L \circ \phi_r \circ L^{-1})\det(L \circ \phi_s \circ L^{-1}) \\ &= \det(L \circ \phi_r \circ L^{-1} \circ L\phi_s \circ L^{-1}) \\ &= \det(L \circ \phi_r \circ \phi_s \circ L^{-1}) \\ &= \det(L \circ \phi_{rs} \circ L^{-1}) = N(rs). \end{aligned}$$

3. We calculate that

$$N(1) = \det(L \circ \phi_1 \circ L^{-1}) = \det(L \circ \mathrm{id}_{\mathbb{Z}[X]/(f)} \circ L^{-1}) = \det(\mathrm{id}_{\mathbb{Z}^n}) = 1.$$

4. First, suppose that r is unit, then

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

We showed earlier that $N(r) \in \mathbb{Z}$, hence the only option is that $N(r) \in \{-1, 1\}$.

Second, suppose that $N(r) \in \{-1, 1\}$, then by definition $\det(L \circ \phi_r \circ L^{-1}) \in \{-1, 1\}$, hence this matrix is invertible. Let us call this matrix K, and the inverse M. We define a $\mathbb{Z}$-module isomorphism $\psi : \mathbb{Z}[X]/(f) \to \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}^n)$ with $r \to L \circ \phi_r \circ L^{-1}$. By the theorem of Cayley-Hamilton, we know that there exist integer coefficients $c_0, c_1, \ldots, c_{n-1}$ such that

$$K^n + c_{n-1}K^{n-1} + \ldots + c_1 K \pm 1 = 0.$$

By rewriting, we obtain

$$M = \pm(K^{n-1} + c_{n-1}K^{n-2} + \ldots + c_1 I),$$

which is a linear combination of powers of K. Since K is in the image of ψ, then so is M in the image of ψ. Hence $M = L \circ \phi_s \circ L^{-1}$, with $s \in \mathbb{Z}[X]/(f)$. This implies that $s = r^{-1}$, therefore $r \in R^\times$.

5. This statement follows from the following observation:

$$R/rR = R/\phi_r(R) \cong \mathbb{Z}^n/(L \circ \phi_r \circ L^{-1})\mathbb{Z}^n.$$

We know that $\mathbb{Z}^n/(L \circ \phi_r \circ L^{-1})\mathbb{Z}^n$ is finite if and only if $\det(L \circ \phi_r \circ L^{-1}) \neq 0$, and in that case this $\mathbb{Z}$-module has $|\det(L \circ \phi_r \circ L^{-1})| = |N(r)|$ elements. □

2.2 Embeddings

We now show an equivalent way of writing the norm, which will prove to be very useful to find units of $\mathbb{Z}[X]/(f)$. In our case, f has no real roots, so we denote the set of roots of f as follows: $\{\alpha_1, \overline{\alpha_1}, \alpha_2, \overline{\alpha_2}\}$, with the bar being the complex conjugate. A simple calculation shows that if α is a root of f, then so is $\overline{\alpha}$. Since f is irreducible, we know that we have four distinct roots.

Lemma 2.2. *Let f be monic, irreducible, of degree n, denote the roots of f as $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Then*

$$\mathbb{Z}[X]/(f) \cong \mathbb{Z}[\alpha_i].$$

Proof. Consider the evaluation ring homomorphism $\mathrm{Ev}_{\alpha_i} : \mathbb{Z}[X] \to \mathbb{Z}[\alpha_i]$, with $\mathrm{Ev}_{\alpha_i}(g) = g(\alpha_i)$. Note that since $\mathrm{Ev}_{\alpha_i}(f) = f(\alpha_i) = 0$, $(f) \in \ker(\mathrm{Ev}_{\alpha_i})$. Let $h \in \ker(\mathrm{Ev}_{\alpha_i})$, then $\mathrm{Ev}_{\alpha_i}(h) = h(\alpha_i) = 0$. Applying division with remainder on h, we get that $h = qf + r$, with $q, r \in \mathbb{Z}[X]$ and $\deg r < \deg f$. We have that

$$0 = h(\alpha_i) = q(\alpha_i)f(\alpha_i) + r(\alpha_i) = r(\alpha_i).$$

Since f is monic and irreducible and has α_i as a root, f is the minimal polynomial for α_i, so $r = 0$, hence $h \in (f)$, implying that $(f) = \ker(\mathrm{Ev}_{\alpha_i})$. Then by the first isomorphism theorem, we get that

$$\mathbb{Z}[X]/(f) \cong \mathbb{Z}[\alpha_i].$$

□

This proof also shows us that the structure of $\mathbb{Z}[\alpha_i]$ is the same for all i, so we simply denote it by $\mathbb{Z}[\alpha]$, because it does not matter which root of f we choose, since they are the same up to isomorphism. We can now define embeddings.

Definition 2.2 (embedding)**.** *Let $f \in \mathbb{Z}[X]$ be monic, irreducible of degree n. Denote the roots of f as $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$. Then the embedding $\sigma_i : \mathbb{Z}[X]/(f) \to \mathbb{Z}[\alpha_i]$ for $1 \leq i \leq n$, is defined as*

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

Note that the embedding is well-defined, we take two different representatives of the same equivalence class in $\mathbb{Z}[X]/(f)$. Let $g = q * f + r, h = p * f + r$ be two such elements. Then we have

$$\sigma_i(g+(f)) = g(\alpha_i) = q(\alpha_i)f(\alpha_i)+r(alpha_i) = r(alpha_i) = p(\alpha_i)f(\alpha_i)+r(alpha_i) = h(\alpha_i) = \sigma_i(h+(f)).$$

Also note that σ_i is precisely the ring isomorphism between the two isomorphic rings we found in Lemma 2.2. The norm can be rewritten as a product of these embeddings.

Theorem 2.3 (equivalent expression for the norm)**.** *Let $f \in \mathbb{Z}[X]$ be monic, irreducible of degree n. The norm function $N : \mathbb{Z}[X]/(f) \to \mathbb{Z}$ satisfies the following equality:*

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

Proof. Since f is irreducible, we can rewrite it in $\mathbb{C}[X]$ as

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

where α_i denote the roots of f. Since f is irreducible, and by applying the Chinese remainder theorem, we obtain

$$\mathbb{C}[X]/(f) \cong \mathbb{C}[X]/(X-\alpha_1) \times \mathbb{C}[X]/(X-\alpha_2) \times \ldots \times \mathbb{C}[X]/(X-\alpha_n).$$

For each of these rings, consider the evaluation homomorphism $\mathrm{Ev}_{\alpha_i} : \mathbb{C}[X]/(X-\alpha_1) \to \mathbb{C}$ for $1 \leq i \leq n$. This homomorphism is surjective and has as image $\mathbb{C}$, because every element in $\mathbb{C}[X]/(X-\alpha_1)$ can be written as a constant complex number, and each complex number is in the ring. Ev_{α_i} is also injective, take $g \in \ker(\mathrm{Ev}_{\alpha_i})$, then $0 = g(\alpha_i) = g(X)$, but g is a constant, so the kernel is trivial. Hence, by the first isomorphism theorem and by the transitive property of isomorphisms, we obtain that

$$\mathbb{C}[X]/(f) \cong \mathbb{C}^n.$$

The corresponding isomorphism maps

$$r \mapsto r(\alpha_1), r(\alpha_2), \ldots, r(\alpha_n)) = (\sigma_1(r), \sigma_2(r), \ldots, \sigma_n(r)).$$

The corresponding multiplication matrix ϕ_r after applying this isomorphism would look like

$$\begin{bmatrix} \sigma_1(r) & 0 & \ldots & 0 \\ 0 & \sigma_2(r) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \sigma_n(r) \end{bmatrix}$$

This follows from the fact that multiplication is component wise in $\mathbb{C}^n$. This matrix has determinant $\prod_{i=1}^{n} \sigma_i(r)$, and hence the proof is done. $\square$

3 A Method to Find Units

We want to use the results from the previous section to find units. Since we have shown that the norm function is multiplicative, we can try to find elements of $\mathbb{Z}[X]/(f)$ of the same norm and dividing them to hopefully again obtain an element of $\mathbb{Z}[X]/(f)$. There is a problem, because in general the fraction is in $\mathbb{Q}[X]/(f)$, and not in $\mathbb{Z}[X]/(f)$. We show that if we find two elements that generate the same ideal, their fraction is an element of $\mathbb{Z}[X]/(f)$. This section is based on [3].

Theorem 3.1. *Let $r, s \in \mathbb{Z}[X]/(f)$ be nonzero such that $(r) = (s)$. Consider $f \in \mathbb{Z}[X]$ monic, irreducible, and of degree $n \geq 2$. Then $|N(r)| = |N(s)|$.*

Proof. Assume that $(r) = (s)$. Then $r = xs$ and $s = yr$ for some $x, y \in \mathbb{Z}[X]/(f)$, implying that $r = xyr$. Since r is nonzero, this means that x and y are units. We showed before that the norm of a unit is ± 1. Hence we get

$$|N(r)| = |N(x)|\,|N(s)| = |N(s)|\,.$$

□

Note that if we can find such elements r, s, then $\frac{r}{s}$ is indeed a unit in $\mathbb{Z}[X]/(f)$. The problem is that finding such elements is hard.
We now plan to show that there exist finitely many principal ideals (r) such that $|N(r)| = k$ for any natural number k, but at the same time, that there only exist infinitely many elements r with norm k. This means that we have a guarantee to eventually find two elements that generate the same ideal if we keep finding elements with norm k, hence we can find a unit in this way. This takes up a big part of the rest of the paper.

Theorem 3.2. *Consider $\mathbb{Z}[X]/(f)$, with f monic, irreducible and of degree $n \geq 2$. Then the set*

$$S = \{(r) \textit{is a principal ideal of } \mathbb{Z}[X]/(f) : |N(r)| = k\}$$

is finite for all natural numbers k.

Proof. Let $L : \mathbb{Z}^n \to \mathbb{Z}[X]/(f)$ be a $\mathbb{Z}$-module isomorphism, take $r \in \mathbb{Z}[X]/(f)$ and ϕ_r as the map that multiplies elements by r. Let $\pi_r : \mathbb{Z}[X]/(f) \to (\mathbb{Z}[X]/(f))/(r)$ be the canonical map. Then we have that

$$\begin{aligned}\ker(\pi_r \circ L^{-1}) &= \{v \in \mathbb{Z}^n : (\pi_r \circ L^{-1})(v) = 0 + (r)\} = \{v \in \mathbb{Z}^n : L^{-1}(v) = \phi_r(\mathbb{Z}[X]/(f))\} \\ &= (L \circ \phi_r)(\mathbb{Z}[X]/(f)) = (L \circ \phi_r \circ L^{-1})(\mathbb{Z}^n).\end{aligned}$$

The function $\pi_r \circ L^{-1} : \mathbb{Z}^n \to (\mathbb{Z}[X]/(f))/(r)$ is surjective, since it is a composition of two surjective $\mathbb{Z}$-module homomorphisms. Then by the first isomorphism theorem, we have that

$$\mathbb{Z}^n/(L \circ \phi_r \circ L^{-1})(\mathbb{Z}^n) \cong (\mathbb{Z}[X]/(f))/(r).$$

By using the fact that the index of a subgroup is precisely the determinant of the generator of that subgroup, we obtain

$$|N(r)| = \left|\det(L \circ \phi_r \circ L^{-1})\right| = \#(\mathbb{Z}^n/(L \circ \phi_r \circ L^{-1})(\mathbb{Z}^n)) = \#((\mathbb{Z}[X]/(f))/(r)).$$

We can conclude from this that

$$S = \{(r) \text{ is a principal ideal of } \mathbb{Z}[X]/(f) : \#((\mathbb{Z}[X]/(f))/(r)) = k\}.$$

Let (r) be a principal ideal such that $\#((\mathbb{Z}[X]/(f))/(r)) = k$. Take $s + (r) \in (\mathbb{Z}[X]/(f))/(r))$, we deduce

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

This follows from the fact that the order of $s + (r)$ divides k. From this we can conclude that $ks \in (r)$ for any s, hence $(k) \subset (r)$. We get that

$$\begin{aligned} S &= \{(r)\text{is a principal ideal of } \mathbb{Z}[X]/(f) : \#((\mathbb{Z}[X]/(f))/(r)) = k\} \\ &\subset \{(r)\text{is a principal ideal of } \mathbb{Z}[X]/(f) : (k) \subset (r)\} =: T. \end{aligned}$$

Aiming for a contradiction, assume that T has more than k^n elements. Let $\{b_1, b_2, \ldots, b_n\}$ be a basis of $\mathbb{Z}[X]/(f)$, write $r \in \mathbb{Z}[X]/(f)$ as $r = r_1b_1 + r_2b_2 + \ldots + r_nb_n$, with r_i integers for all $1 \leq i \leq n$. By the pigeonhole principle, there exists distinct $(r), (s) \in T$ such that $r_i \equiv s_i \bmod k$ for all $1 \leq i \leq n$. Then

$$r - s = k(\frac{r_1 - s_1}{k} + \frac{r_2 - s_2}{k} + \ldots + \frac{r_n - s_n}{k}) \in (k).$$

This holds because we showed that $\frac{r_i - s_i}{k}$ is an integer. Since $(k) \subset (r)$ and $(k) \subset (s)$, $r - s \in (r)$ and $r - s \in (s)$, hence $r \in (s)$ and $s \in (r)$. This means that $(r) = (s)$, which is a contradiction, thus $\#T \leq k^n$, so S is finite. □

Now we have a way to find units, but in practice this is not that helpful yet. We show a simple example how we can apply this theorem in practice, where f is of degree 4.

Example: Let $f(X) = X^4+1$, which is indeed monic and irreducible without real roots. Notice that $r = X^2 + 1$ and $s = X^2 + 2X + 1$ generate the same ideal, since $r = (-X^3 + X - 1)s$ and $s = (-X^3 + X + 1)r$ Hence r and s have the same norm, and thus

$$\frac{r}{s} = -X^3 + X - 1$$

is a unit. We check that. Take L to be the $\mathbb{Z}$-module isomorphism defined by $L(e_i) = X^i$ for $0 \leq i \leq 3$, with e_i the standard basis vectors of $\mathbb{Z}^4$. Then

$$N(\frac{r}{s}) = \det \begin{bmatrix} -1 & 1 & 0 & -1 \\ 1 & -1 & 1 & 0 \\ 0 & 1 & -1 & 1 \\ -1 & 0 & 1 & -1 \end{bmatrix} = 1,$$

and hence we found an example using the theorem we discovered.

4 The Discriminant and Minkowski's Theorem

4.1 The Discriminant

The discriminant of a polynomial can give a lot of information about some properties of the polynomial. The discriminant of $f = X^4 + c_3X^3 + c_2X^2 + c_1X + c_0$ is given by

$$\begin{aligned}\operatorname{disc}(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2 &= 256c_0^3 - 192c_3c_1c_0^2 - 128c_2^2c_0^2 + 144c_2c_1^2c_0 - 27c_1^4 \\ &+ 144c_3^2c_2c_0^2 - 6c_3^2c_1^2c_0 - 80c_3c_2^2c_1c_0 + 18c_3c_2c_1^3 + 16c_2^4c_0 - 4c_2^3c_1^2 - 27c_3^4c_0^2 \\ &+ 18c_3^3c_2c_1c_0 - 4c_3^3c_1^3 - 4c_3^2c_2^3c_0 + c_3^2c_2^2c_1^2.\end{aligned}$$

There also exists such a notion for algebraic number fields, which we do not cover here, but we look at the specific case of the discriminant of $\mathbb{Z}[X]/(f)$, and prove that it is actually equal to the discriminant of f.

Definition 4.1 (discriminant)**.** *The discriminant of* $\mathbb{Z}[X]/(f)$*, denoted disc(*$\mathbb{Z}[X]/(f)$*),*

$$= det\begin{bmatrix}1 & \alpha_1 & \alpha_1^2 & \alpha_1^3 \\ 1 & \alpha_2 & \alpha_2^2 & \alpha_2^3 \\ 1 & \alpha_3 & \alpha_3^2 & \alpha_3^3 \\ 1 & \alpha_4 & \alpha_4^2 & \alpha_4^3\end{bmatrix}^2$$

We want to give an explicit formula for the discriminant of $\mathbb{Z}[X]/(f)$, so we need to find the determinant of the matrix above. Such a matrix, where each row is a geometric progression, is called a VanderMonde matrix, we will show the general formula for the determinant of such a matrix in the following lemma.

Lemma 4.1. *Let* M_{n+1} *be an* $(n+1)\times(n+1)$ *Vandermonde matrix, with*

$$M_{n+1} = \begin{bmatrix}1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n\end{bmatrix}, \text{ then } det(M_{n+1}) = \prod_{0\le i<j\le n}(x_j - x_i)$$

Proof. This is a proof by induction, for the base case $n = 2$, a simple calculation shows that $\det(M) = x_1 - x_0$.
For the induction step, suppose that the lemma already holds for $(n+1)\times(n+1)$ matrices. Let $M_{n+2} = \begin{bmatrix}1 & x_0 & x_0^2 & \dots & x_0^{n+1} \\ 1 & x_1 & x_1^2 & \dots & x_1^{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n+1} & x_{n+1}^2 & \dots & x_{n+1}^{n+1}\end{bmatrix}$
and V is equal to M_{n+1} with shifted indices, where $V := \begin{bmatrix}1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n+1} & x_{n+1}^2 & \dots & x_{n+1}^n\end{bmatrix}$.

Then

$$\begin{aligned}
\det(M_{n+2}) &= \det \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & x_1 - x_0 & x_1(x_1 - x_0) & \dots & x_1^n(x_1 - x_0) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n+1} - x_0 & x_{n+1}(x_{n+1} - x_0) & \dots & x_{n=1}^n(x_{n+1} - x_0) \end{bmatrix} \\
&= \det \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & x_1 - x_0 & x_1(x_1 - x_0) & \dots & x_1^n(x_1 - x_0) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{n+1} - x_0 & x_{n+1}(x_{n+1} - x_0) & \dots & x_{n=1}^n(x_{n+1} - x_0) \end{bmatrix} \\
&= \prod_{1 \le i \le n+1} (x_i - x_0) \det(V)
\end{aligned}$$

Here, we have used basic properties of determinants while performing row operations. □

We have proven here that the discriminant of $\mathbb{Z}[X]/(f)$ is the discriminant of f, for which we already found a formula earlier. This will be useful for later theorems in this section.

4.2 Minkowski's Theorem

[4] Minkowski's theorem can help us finally find some units, for which we need to define a lattice first.

Definition 4.2 (Lattice)**.** *[2] An additive subgroup $L \subset \mathbb{R}^n$ is a lattice, if there exists a basis $b_1, \dots, b_n$ of $\mathbb{R}^n$ that generates L. Then, the determinant of L, denoted $d(L)$ is defined by $d(L) = |det[b_1 \dots b_n]|$.*

Theorem 4.2 (Minkowski)**.** *Let $L \subset \mathbb{R}^n$ be a lattice and let $S \subset \mathbb{R}^n$ be a closed, convex and symmetric set. If $vol(S) \ge 2^n d(L)$, then S contains a non-zero lattice point.*

This means that, if we represent $\mathbb{Z}[X]/(f)$ as a lattice, we can find at least one element in such a set S, which will help finding units later.

Theorem 4.3. *Let $f = X^4 + c_3X^3 + c_2X^2 + c_1X + c_0$ be irreducible, with no real roots. Let $\sigma : \mathbb{Z}[X]/(f) \to \mathbb{R}^4$, where*

$$\sigma(r) = (Re(\sigma_1(r)), im(\sigma_1(r)), Re(\sigma_2(r)), im(\sigma_2(r))).$$

Let $S \subset \mathbb{R}^4$ be closed, convex and symmetric, with $vol(S) \ge 4\sqrt{disc(\mathbb{Z}[X]/(f))}$. Then S contains a non-zero lattice point of the image of σ.

Proof. Denote the roots of f as $\{\alpha_1, \overline{\alpha_1}, \alpha_2, \overline{\alpha_2}\}$.Let us calculate the determinant of the matrix $D$with columns $\{\sigma(1), \sigma(X), \sigma(X^2), \sigma(X^3)\}$. Then

$$\begin{aligned}
|\det(D)| &= \det \left| \begin{bmatrix} 1 & \mathrm{Re}(\alpha_1) & \mathrm{Re}(\alpha_1^2) & \mathrm{Re}(\alpha_1^3) \\ 0 & \mathrm{Im}(\alpha_1) & \mathrm{Im}(\alpha_1^2) & \mathrm{Im}(\alpha_1^3) \\ 1 & \mathrm{Re}(\alpha_2) & \mathrm{Re}(\alpha_2^2) & \mathrm{Re}(\alpha_2^3) \\ 0 & \mathrm{Im}(\alpha_2) & \mathrm{Im}(\alpha_2^2) & \mathrm{Im}(\alpha_2^3) \end{bmatrix} \right| \\
&= \frac{1}{4} \det \left| \begin{bmatrix} 1 & \mathrm{Re}(\alpha_1) + i\mathrm{Im}(\alpha_1) & \mathrm{Re}(\alpha_1^2) + i\mathrm{Im}(\alpha_1^2) & \mathrm{Re}(\alpha_1^3) + i\mathrm{Im}(\alpha_1^3) \\ 0 & -2i\mathrm{Im}(\alpha_1) & -2i\mathrm{Im}(\alpha_1^2) & -2i\mathrm{Im}(\alpha_1^3) \\ 1 & \mathrm{Re}(\alpha_2) + i\mathrm{Im}(\alpha_2) & \mathrm{Re}(\alpha_2^2) + i\mathrm{Im}(\alpha_2^2) & \mathrm{Re}(\alpha_2^3) + i\mathrm{Im}(\alpha_2^3) \\ 0 & -2i\mathrm{Im}(\alpha_2) & -2i\mathrm{Im}(\alpha_2^2) & -2i\mathrm{Im}(\alpha_2^3) \end{bmatrix} \right| \\
&= \frac{1}{4} \det \left| \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \alpha_1^3 \\ 1 & \overline{\alpha_1} & \overline{\alpha_1}^2 & \overline{\alpha_1}^3 \\ 1 & \alpha_2 & \alpha_2^2 & \alpha_2^3 \\ 1 & \overline{\alpha_2} & \overline{\alpha_2}^2 & \overline{\alpha_2}^3 \end{bmatrix} \right| = \frac{1}{4}\sqrt{|\mathrm{disc}[\mathbb{Z}[X]/(f)]|}.
\end{aligned}$$

We have applied elementary row operations here to transform the matrix. Note that the discriminant of f is nonzero, since the roots of f are distinct. This means that this determinant is also nonzero, which means that $\{\sigma(1), \sigma(X), \sigma(X^2), \sigma(X^3)\}$ are linearly independent, implying that this set is a basis of $\mathbb{R}^4$. We conclude that $\sigma(\mathbb{Z}[X]/(f))$ is a lattice L, with $d(L) = |\det(D)|$. Using this result, we can see that

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

The previous equation shows that we fulfill the requirements of Minkowski's theorem, hence we have a non-zero lattice point of L in S. □

The previous theorem will prove to be quite helpful in the following section. We want to develop a more systematic approach to finding units, since we do not have a structured way to find elements that generate the same ideal yet, which is not desirable if we want to use theorem 3.1. The following section describes a way to guarantee finding such elements.

5 The Generator

5.1 Infinitely Many Elements with Small Norm

The aim of the following section is to show that we always have a nontrivial unit for any monic irreducible f of degree 4 with no real roots. This takes some time and needs a few proofs before we can get that result. The first three paragraphs of this section are based on [3].
We have shown a naive and simple way to find units, and we give a way to search for units in a more systematic way later. First we want to talk about the structure of the group of units of $\mathbb{Z}[X]/(f)$ using Dirichlet's unit theorem. But first we show that the units of the ring do not accumulate in a point under a certain map, which means that the image of this map is discrete.

Theorem 5.1. *Let $f \in \mathbb{Z}[X]$ with r_1 real roots and $2r_2$ non-real roots, writing in the following order: $\alpha_1, \dots, \alpha_{r_1+r_2}, \overline{\alpha_{r_1+1}}, \dots, \overline{\alpha_{r_1+r_2}}$. Let $h(r) : \mathbb{Z}[X]/(f) \to \mathbb{R}^{r_1+r_2}$, be defined as*

$$h(r) = (\log|\sigma_1(r)|, \log|\sigma_2(r)|, \dots, \log|\sigma_{r_1+r_2}(r)|).$$

Then the image of h is discrete, meaning that in all bounded subsets of $\mathbb{R}^{r_1+r_2}$, there exist only finitely many points which are in the image of h.

Proof. Without loss of generality, we show that the image of h has a finite number of points in intervals of the form $(-\infty, C]^{r_1+r_2}$ for some real constant C, since all bounded sets are contained within such intervals. Let $r \in \mathbb{Z}[X]/(f)$ be nonzero with $h(r) \in (-\infty, C]^{r_1+r_2}$, then $\log|\sigma_i(r)| < C$ for all $1 \le i \le r_1+r_2$. Consider g given by

$$g(X) = (X - \sigma_1(r))(X - \sigma_2(r)) \dots (X - \sigma_{r_1+r_2}(r)),$$

where we take g as the polynomial with the embeddings of r as roots. Then the absolute value of the k-th coefficient of g is given by

$$\left| \sum_{S \subset \{1,2,\dots,r_1+2r_2\} : \#S = k} \left(\sum_{j \in S} |\sigma_j(r)| \right) \right| \le \sum_{S \subset \{1,2,\dots,r_1+2r_2\} : \#S = k} \left(\sum_{j \in S} |\sigma_j(r)| \right)$$
$$\le$$
$$\sum_{S \subset \{1,2,\dots,r_1+2r_2\} : \#S = k} e^{kC} = \binom{r_1 + 2r_2}{k} e^{kC}.$$

Thus the coefficients for g are bounded by a constant, this means we have finitely many options, since all coefficients of g are in $\mathbb{Z}[\alpha]$, hence the pre-image of $h(r)$ under h is finite, as there are only finitely many r that correspond to the same g, we have that $h^{-1}((-\infty, C]^{r_1+r_2})$ is finite as well. □

Note: let us look at the situation where f is monic, irreducible, of degree 4 with no real roots. We see that $r_1 + 2r_2 = 4$, because $r_1 = 0$ and $2r_2 = 4$. Then

note that

$$\binom{r_1 + 2r_2}{k} \leq 6.$$

We continue with our proof, and we show that we can find infinitely many elements r which have a norm smaller than a certain value.

Theorem 5.2. *Let $f \in \mathbb{Z}[X]$ be monic, irreducible, and with no real roots, with f of degree 4. Then we can find infinitely many $r \in \mathbb{Z}[X]/(f)$ with $|N(r)| < \frac{8}{\pi^2}\sqrt{|disc(\mathbb{Z}[X]/(f))|}$.*

Proof. Consider the hyper-ellipsoid $S_{k,l}$ given by

$$\begin{aligned} S_{k,l} &= \{(x,y,z,w) \in \mathbb{R}^4 : \frac{x^2+y^2}{k^2} + \frac{z^2+w^2}{l^2} \leq 1\} \\ &= \{(x,y,z,w) \in \mathbb{R}^4 : \frac{|x+iy|^2}{k^2} + \frac{|z+iw|^2}{l^2} \leq 1\}, \end{aligned}$$

where k, l are real numbers. The volume of this hyper-ellipsoid is given by $\text{vol}(S_{k,l}) = \frac{\pi^2}{2}k^2l^2$. Now, choose $k, l > 0$ such that $\text{vol}(S_{k,l}) = 4\sqrt{|disc(\mathbb{Z}[X]/(f))|}$. Then by theorem 4.3, we know that $S_{k,l}$ contains a non-zero element under the image of σ, call this element $\sigma(r)$. For practical purposes, we can actually find this element by using the short vectors algorithm on $S_{k,l}$, since a hyper-ellipsoid is a quadratic form of the form $M = A^TA$, and possibly we find more non-zero lattice points, but we know we can find at least one this way.
Since $\sigma(r) \in S_{k,l}$, we get that

$$\frac{|\sigma_1(r)|^2}{k^2} + \frac{|\sigma_2(r)|^2}{l^2} \leq 1.$$

Note that each $\sigma_i(r) \neq 0$ for $i \in \{1, 2\}$, by the following reasoning: we have chosen $\sigma_r \neq 0$, this means that at least one $\sigma_i(r) \neq 0$, which means that $r \neq 0$, since σ_i is an isomorphism, but that means all $\sigma_i(r) \neq 0$. From here we can deduce that $|\sigma_1(r)| < k$ and $|\sigma_2(r)| < l$. From this we obtain that

$$|N(r)| = |\sigma_1(r)|^2|\sigma_2(r)|^2 < k^2l^2 = \frac{2}{\pi^2}\text{vol}(S_{k,l}) = \frac{8}{\pi^2}\sqrt{|disc(\mathbb{Z}[X]/(f))|}.$$

We have shown that we can find one element with the required norm, but we claim that are infinitely many. This can be done by induction. Suppose that we have already found n such elements $r_1, r_2, \ldots, r_n$, with $|N(r_i)| < \frac{8}{\pi^2}\sqrt{|disc(\mathbb{Z}[X]/(f))|}$ for $1 \leq i \leq n$. Then we can choose $k < \min\{|\sigma_1(r_i)| : 1 \leq i \leq n\}$, and the corresponding l, given by

$$l = \sqrt{\frac{8}{\pi^2k^2}\sqrt{|disc(\mathbb{Z}[X]/(f)|}}.$$

Applying the above reasoning again, we can find an element r with $|N(r)| < \frac{8}{\pi^2}\sqrt{|disc(\mathbb{Z}[X]/(f))|}$, but this r is not equal to any of the $r_1, r_2, \ldots, r_n$, since

$$|\sigma_1(r)| < k < \min\{|\sigma_1(r_i)| : 1 \leq i \leq n\}.$$

By repeatedly doing this, we can find infinitely many such r. □

5.2 The Short Vector Algorithm

In the previous proof, we mention the short vector algorithm , which calculates all vectors in a lattice with length less than a certain constant. The short vector algorithm takes as input a positive definite quadratic form, so we need to define what that means first.

Definition 5.1 (quadratic form)**.** *A quadratic form $Q : \mathbb{R}^n \to \mathbb{R}$ is a polynomial in n variables, where all terms are of degree 2. This means that any quadratic form can be rewritten as*

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

for a symmetric $n \times n$ real matrix M.

We can rewrite every quadratic form Q in a certain way if $M = A^T A$: Since

$$Q(x) = x^T M x = \sum_{i,j=1}^{n} m_{i,j} x_i x_j.$$

We can apply Cholesky's method to rewrite the quadratic form Q into a sum of squares, by repeatedly completing the square. This can be done by using the following algorithm. [1]

1) Set $q_{i,j} = m_{i,j}$.
2) Then for $i \in \{1, 2, \ldots, n-1\}$, set $q_{j,i} = q_{i,j}$ and $q_{i,j} = \frac{q_{i,j}}{q_{i,i}}$, with $i + 1 \leq j \leq n$.
3) for each i and $k \in \{i+1, \ldots, n\}$, set $q_{k,l} = q_{k,l} - q_{k,i} q_{i,k}$ for $k \leq l \leq n$.
4) Then
$$Q(x) = \sum_{i=1}^{n} q_{i,i} (x_i + \sum_{j=i+1}^{n} q_{i,j} x_j)^2.$$

This then leads to the short vector algorithm, which calculates all vectors of length less than a given constant C.

Definition 5.2 (short vector algorithm)**.** *Let $Q : \mathbb{R}^n \to \mathbb{R}$ be a positive definite quadratic form given by*

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

Let $C > 0$ be a constant, then this 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 $Z_i = \sqrt{\frac{T_i}{q_{i,i}}}$, $L_i = \lfloor Z_i - U_i \rfloor$ and $x_i = \lceil -Z_i - U_i \rceil - 1$.

3) increase x_i by 1. Then, if

- *$x_i > L_i$, increase i by 1, repeat step 3.*
- *$x_i \leq L_i$ and $i > 1$, then set $T_{i-1} = T_i - q_{i,i}(x_i + U_i)^2$. Then, decrease i by 1 and set $U_i = \sum_{j=i+1}^{n} q_{i,j}x_j$, then repeat step 2.*
- *$x_i \leq L_i$ and $i = 1$, then x is a solution. If $x \neq 0$, repeat step 3 for more solutions.*

Example: Consider $n = 4$, then a hyper-ellipsoid of the form

$$Q(x)\sum_{i=1}^{4}\frac{x_i^2}{c_i}$$

is of the form as in the definition of the short vector algorithm, and hence we can apply it in the proof.
The theorem above gives us some nice corollaries.

5.3 A Nontrivial Unit

Corollary 5.3. *Let $f \in \mathbb{Z}[X]$ be monic, irreducible, and with no real roots, with f of degree 4. Then we can find infinitely many $r \in \mathbb{Z}[X]/(f)$ such that $|N(r)| = k$ for some integer $1 \leq k \leq \frac{8}{\pi^2}\sqrt{|disc(\mathbb{Z}[X]/(f))|}$.*

Proof. Aiming for a contradiction, suppose that for all such k, that there only exist finitely many r such that $|N(r)| = k$. This would mean that there are also only finitely many r with $N(r) < \frac{8}{\pi^2}\sqrt{|disc(\mathbb{Z}[X]/(f))|}$, since the finite unit of finite sets is a finite set. This would contradict theorem 5.2, and hence we are done. □

Corollary 5.4. *Let $f \in \mathbb{Z}[X]$ be monic, irreducible, and with no real roots, with f of degree 4. Then there exists a non-trivial unit u in $\mathbb{Z}[X]/(f)$.*

Proof. We showed in theorem 5.3 that there exists an integer k such that there are infinitely many r with $|N(r)| = k$, and in theorem 3.2 that for all integers k, there are only finitely many different prime ideals where the generator has norm k. By the pigeonhole principle, there is now a guarantee that using the above method, we find two different elements generating the same prime ideal which do not differ by a root of unity ζ, and hence by theorem 3.1, we can divide them to obtain a non-trivial unit u. This is because we can specifically find r, s such that $r \neq \zeta s$, since we have infinite options to choose from, so if we have at least thirteen elements that generate the same ideal, we can do this. This means that $u \neq \zeta$. □

5.4 The Generator

We showed that for any f that is monic, irreducible and of degree 4 with no real roots, we have a way to construct a non-trivial unit. We can use this result to really show something about the structure of the unit group of $\mathbb{Z}[\alpha]$, namely that the unit group of $\mathbb{Z}[\alpha]$ has rank 1.

Theorem 5.5 (Special case of Dirichlet's unit theorem)**.** *[4] Let $f \in \mathbb{Z}[X]$ be monic, irreducible, and with no real roots, with f of degree 4. Let α be a root of f, then*

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

for some unique β in $\mathbb{Z}[\alpha]$ up to sign.

Proof. Consider h as in 5.1. Note that $r \in \mathbb{Z}[X]/(f)$ is a unit if and only if $h(r)$ lies on the line $\{(x, y) \in \mathbb{R}^2 : x + y = 0\}$, since

$$0 = 2\log|\sigma_1(r)| + 2\log|\sigma_1(r)| = \log|\sigma_1(r)||\overline{\sigma_1(r)}||\sigma_2(r)||\overline{\sigma_2(r)}| = \log|N(r)|.$$

By corollary 5.4, there exists a non-trivial unit $u \in \mathbb{Z}[X]/(f)$, and since σ_i is an isomorphism, we get that $\sigma_i \neq \pm 1$. This means that $h(u) \neq 0$. Consider the line piece $(0, h(u)]$. This line piece is a bounded region, and since we proved that h is discrete in 5.1, we know that there are only finitely many points on this line that are in the image of h. Choose the smallest such number, i.e. we choose v such that $||h(v)||_2$ is minimal among all points on this line that are in the image of h. We know this minimum exists, since a finite set of real numbers always has a minimum, and we know this set is not empty, since $h(u)$ is there. We take $||.||_2$ as the usual Euclidean 2-norm.
Consider $\beta = \max(|\sigma_1(v)|, |\sigma_1(v)|^{-1})$. Aiming for a contradiction, assume there exists a unit $u \in \mathbb{Z}[\alpha]$ such that u is not a power of β. This means there exists an integer k such that $|\beta^k| < |u| < |\beta^{k+1}|$. This follows from the fact that if $|\beta^k| = |u|$, then $||h(\sigma_1^{-1}(u))||_2 = ||\pm h(\sigma_1^{-1}(\beta))||_2$, which contradicts our assumption. Then this means that $1 < |u\beta^{-k}| < |\beta|$, which implies that

$$1 < ||h(\sigma_1^{-1}(u\beta^{-k}))||_2 < ||h(\sigma_1^{-1}(\beta)||_2 = ||\pm h(v)||_2.$$

This contradicts the minimality of the norm of v, and hence we have that

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

We also claim that β is unique up to sign. Suppose there were two such generators β, γ, then

$$\beta = \gamma^k = (\beta^l)^k = \beta^{kl}.$$

This means that kl=1, hence $\gamma = \beta$, or $\gamma = \beta^{-1} = -\beta$, since we consider $\mathbb{Z}[\alpha]$ as an additive group. □

5.5 The Structure of the Unit Group of $\mathbb{Z}[X]/(f)$

We have one final result about the structure of the unit group of $\mathbb{Z}[X]/(f)$ for the case where f is of degree 4, we use a special case of Dirichlet's unit theorem.

Theorem 5.6 (Dirichlet's unit theorem)**.** *[4] Consider $\mathbb{Z}[X]/(f)$, with f monic, irreducible and of degree n. Let α be a root of f, then*

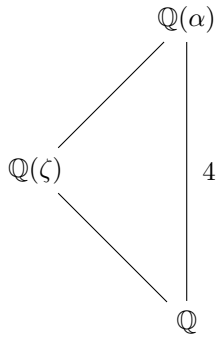
$$\mathbb{Z}[\alpha]^\times \cong \mathbb{Z}^d \times \mathbb{Z}/n\mathbb{Z},$$

where f has r_1 real roots, $2r_2$ non-real roots, $d = r_1 + r_2 - 1$ and n is the number of roots of unity in $\mathbb{Q}(\alpha)$.

We now discuss how this applies to the case where f has degree 4. Consider ζ a primary n-th rooth of unity in $\mathbb{Z}[\alpha]^\times$, i.e. n is the smallest positive integer such that ζ^n=1. We know that the degree $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. By the multiplicative property of degrees of field extensions, we have that

$$[\mathbb{Q}(\alpha) : \mathbb{Q}(\zeta)] \cdot [\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4.$$

This means that $[\mathbb{Q}(\zeta) : \mathbb{Q}] \in \{1, 2, 4\}$. Consider the following diagram of field extensions:



Since $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ is equal to the degree of the minimal polynomial of ζ, we get that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \Phi(n)$, where Φ is the Euler totient function. We now want to find all possibilities for n such that $\Phi(n) \in \{1, 2, 4\}$.
Solving $\Phi(n) = 1$ gives us that $n \in \{1, 2\}$. The other two cases are a bit harder. For $\Phi(n) = x$, we need to have that $n = x + 1$ if and only if $x + 1$ is a prime, or if $x = p^k - p^{k-1}$ with p a prime, we have that $n = p^k$, or if we can find two coprime n_1, n_2 such that

$$x = \Phi(n_1)\Phi(n_2) = \Phi(n_1 n_2).$$

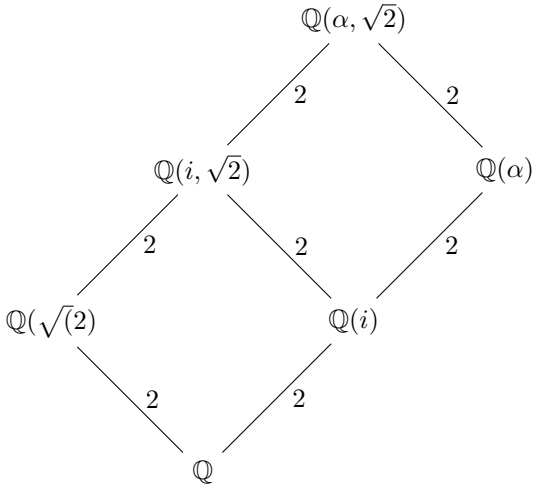
This all follows from properties of the Euler totient function. Hence we can perform an exhaustive search, and obtain the following: If $\Phi(n) = 2$, then $n \in \{3, 6, 4\}$ and if $\Phi(n) = 4$, then $n \in \{5, 10, 8, 12\}$. We conclude that

$n \in \{1, 2, 3, 6, 4, 5, 10, 8, 12\}$, depending on which root of unity is primary in $\mathbb{Z}[\alpha]$. Note that it can be quite hard to know that the found root of unity is truly primary, and that there does not exist another one with a higher degree. We show an example where this is not so hard.

Example: Let us continue looking at the specific example where $f(X) = X^4 + 1$. Notice that all roots of f are roots of unity, since $\alpha^4 = -1$, and hence $\alpha^8 = 1$. f is the minimal polynomial of α, so we know for sure that α is a primary 8-th root of unity. We have that $\Phi(8) = 4$, which implies that

$$\mathbb{Z}[\alpha]^\times \cong \mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}.$$

Example: We can ask ourselves if the splitting field of f always behaves nicely. In general, it does not. Take $f(X) = X^4 - 2X^2 + 2$, which is irreducible over $\mathbb{Q}$, since f is an Eisenstein polynomial for the prime 2. Note that $\alpha = \sqrt{1+i}$ is a root of f, and since f is a polynomial with only even terms, the complete set of roots of f is given by $\{\alpha, -\alpha, \overline{\alpha}, -\overline{\alpha}\}$. We want to know if $\mathbb{Q}(\alpha)$ is the splitting field of f. We can rewrite $f(X)$ as $f(X) = (X^2 - \alpha^2)(X^2 - \frac{2}{\alpha})$. This means that $\overline{\alpha} = \pm\frac{\sqrt{2}}{\alpha}$. We conclude from this that $\mathbb{Q}(\alpha)$ is the splitting field of f if and only if $\sqrt{2} \in \mathbb{Q}(\alpha)$, which holds if and only if $\mathbb{Q}(\alpha) = \mathbb{Q}(i, \sqrt{2})$. Using Magma calculator, we obtain that the Galois group is the dihedral group D_4, and hence it cannot be the case that $\mathbb{Q}(\alpha)$ is the splitting field, since D_4 is not a subset of S_4. This also means that $\mathbb{Q}(\alpha) \neq \mathbb{Q}(i, \sqrt{2})$. This leads to the following diagram of field extensions:



This implies that we do not have a primary 8-th root of unity in $\mathbb{Q}(\alpha)$. This follows from the fact that if there would be a primary 8-th root, then $\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \in \mathbb{Q}(\alpha)$, which implies that

$$(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i)(1 - i) = \sqrt{2} \in \mathbb{Q}(\alpha).$$

This is a contradiction. We have to ask ourselves if we have a primary third root of unity in $\mathbb{Q}(\alpha)$. This is not possible, since $\sqrt{3} \notin \mathbb{Q}(\alpha)$. This means that $\mathbb{Q}(\alpha)$ has exactly four roots of unity, and we can conclude from Dirichlet's unit theorem that

$$\mathbb{Z}[\alpha]^\times \cong \mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

6 Conclusion

In this thesis, we proved that We did this by first considering a norm function, with the important property that the norm of an element r is ± 1 if and only if r is a unit. We rewrite the norm as a product of embeddings, so we can later show that all the units end up on a line under a certain map, which we use to prove that the group of units has rank 1. We also showed what the precise structure of the group of units is, and showed some examples where we have different amounts of roots of unity in $\mathbb{Q}(\alpha)$.
A recommendation for further research could be finding a way to explicitly find the generator of $\mathbb{Z}[X]/(f)$, or by considering cases where f is of higher degree than 4. We can already conclude from Dirichlet's unit theorem that the rank of $\mathbb{Z}[\alpha]^\times$ is higher than 1.

References

[1] U. Fincke and M. Pohst. "Improved Methods for Calculating Vectors of Short Length in a Lattice, Including a Complexity Analysis". In: *Mathematics of Computation* Vol. 44, No. 170, p. 463-471 (1985).

[2] James S. Milne. *Algebraic Number Theory (v3.08)*. p.73-75 Available at www.jmilne.org/math/. 2020.

[3] J. Pruim. *Finding units in $\mathbb{Z}[X]/(f)$ for f a cubic, monic irreducible polynomial with one real root.* 2022.

[4] P. Stevenhagen. *Number Rings*. p.49-59 Available at https://websites.math.leidenuniv.nl/algebra/ant.pdf. 2020.

[5] J Top and J.S. Muller. *Group Theory*. p.93. 2018.