T. Tilly

Units in Monogenic Orders

Bachelor's thesis, August 14th, 2012

Supervisor: prof.dr. H.W. Lenstra

Mathematisch Instituut, Universiteit Leiden

Contents

1. Introduction

This paper is concerned with monogenic orders of which the group of units is finite. The main result is that the group of units of a monogenic order is finite if and only if it is isomorphic to a subgroup of $C_2^3 \times C_3 \times C_4$, but not to C_3 or $C_3 \times C_4$, where C_n is a cyclic group of n elements.

Definition 1.0.1. An *order* is a commutative ring $(A, +, \cdot)$ for which there exists a nonnegative integer n such that $(A, +) \cong (\mathbb{Z}^n, +)$.

Equivalently, an order is a commutative ring of which the additive group is finitely generated and torsion-free.

Example 1.0.2. For any finite abelian group G the group ring $\mathbb{Z}[G]$ is an order, and later we will see that the ring of integers of an algebraic number field is an order as well. Also, for any monic $f \in \mathbb{Z}[X]$ the quotient ring $\mathbb{Z}[X]/(f)$ is an order. The product of two orders with componentwise ring operations is an order, and any subring of an order is again an order.

Definition 1.0.3. An order A is called *monogenic* if there exists a monic $f \in \mathbb{Z}[X]$ such that $A \cong \mathbb{Z}[X]/(f)$.

Example 1.0.4. Some familiar examples are the ring of integers, the ring of Gaussian integers and the ring of Eisenstein integers. These rings are isomorphic to $\mathbb{Z}[X]/(f)$ for $f = X$, $f = X^2 + 1$ and $f = X^2 + X + 1$, respectively. More generally, for ζ_n a primitive n-th root of unity we have $\mathbb{Z}[\zeta_n] \cong \mathbb{Z}[X]/(\Phi_n(X))$, where $\Phi_n(X)$ is the n-th cyclotomic polynomial.

The main result presented in this paper is the following theorem.

Theorem 1.0.5. *A finite group is isomorphic to the group of units of a monogenic order if and only if it is isomorphic to a subgroup of $C_2^3 \times C_3 \times C_4$, but not isomorphic to either C_3 or $C_3 \times C_4$.*

Throughout this paper we assume the reader to be familiar with basic group theory, ring theory and linear algebra, and this will suffice for all but the second chapter. In this chapter we present a natural setting for orders, for which we require a few results from

commutative algebra and number theory. For a thorough introduction to commutative algebra we refer to [1], of which chapters 1, 2, 3 and 8 are of particular importance, and for the results in number theory we refer to [4] and [5].

In chapter three we present a criterion for determining whether $(\mathbb{Z}[X]/(f))^\times$ is finite for any monic $f \in \mathbb{Z}[X]$, and we show that for such f we have $(\mathbb{Z}[X]/(f))^\times \cong C_2^a \times C_3^b \times C_4^c$ for some $a, b, c \in \mathbb{Z}_{\geq 0}$. We construct a very restricted but important class $\mathcal{S}$ of monic polynomials in $\mathbb{Z}[X]$ such that whenever $(\mathbb{Z}[X]/(f))^\times$ is finite for some monic $f \in \mathbb{Z}[X]$, there exists $g \in \mathcal{S}$ dividing f such that $(\mathbb{Z}[X]/(f))^\times$ embeds naturally into $(\mathbb{Z}[X]/(g))^\times$. For $g \in \mathcal{S}$ we will show that $(\mathbb{Z}[X]/(g))^\times \cong C_2^a \times C_3^b \times C_4^c$, where $a+c \leq 4$, $b \leq 1$ and $c \leq 1$ and conclude that if $(\mathbb{Z}[X]/(f))^\times$ is finite, it is isomorphic to a subgroup of $C_2^3 \times C_3 \times C_4$, and we give some examples of monic $g \in \mathbb{Z}[X]$ such that $(\mathbb{Z}[X]/(g))^\times \cong C_2^3 \times C_3 \times C_4$.

For most subgroups $H \subseteq C_2^3 \times C_3 \times C_4$ there exists $f \in \mathcal{S}$ such that $(\mathbb{Z}[X]/(f))^\times \cong H$, the only exceptions being the subgroups isomorphic to either C_3, $C_3 \times C_4$, C_2^4 or $C_2^3 \times C_4$. A direct consequence of Theorem 1.0.5 is that there exists no monic $f \in \mathbb{Z}[X]$ such that $(\mathbb{Z}[X]/(f))^\times$ is isomorphic to either C_3 or $C_3 \times C_4$. Another consequence is that there are monic $f_1, f_2 \in \mathbb{Z}[X]$ such that $(\mathbb{Z}[X]/(f_1))^\times \cong C_2^4$ and $(\mathbb{Z}[X]/(f_2))^\times \cong C_2^3 \times C_4$, which is the subject of the final section.

2. Preliminaries

2.1 The rank

Definition 2.1.1. Let A be an abelian group.

i. An element $x \in A$ is called a *torsion element* if it has finite order.

ii. The set of all torsion elements of A is denoted by A_{tor}.

It is easily verified that A_{tor} is a subgroup of A, which we call the *torsion subgroup* of A. If $A_{\text{tor}} = 0$, then A is called *torsion free*.

For an abelian group A and a field K, we denote the K-vector space $A \otimes_{\mathbb{Z}} K$ by A_K.

Definition 2.1.2. Let A be an abelian group. The *free rank* of A is

$$\operatorname{rank}(A) := \dim_{\mathbb{Q}}(A_{\mathbb{Q}}).$$

We will often refer to $\operatorname{rank}(A)$ as simply the *rank* of A, and by the rank of a ring we will always mean the rank of its additive group. A few properties of the rank are immediate from the definition.

Proposition 2.1.3. i. *If*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

is a short exact sequence of abelian groups, then $\operatorname{rank}(B) = \operatorname{rank}(A) + \operatorname{rank}(C)$.

ii. *If A is a finitely generated abelian group with* $\operatorname{rank}(A) = n$, *then* $A/A_{\text{tor}} \cong \mathbb{Z}^n$.

Proof. i. This is immediate from the fact that tensoring with $\mathbb{Q}$ (over $\mathbb{Z}$) is exact, and that dimension of vector spaces is additive over short exact sequences.

ii. See [2], Theorem I.1.8.4.

□

Clearly the additive group of any order is a torsion free finitely generated abelian group. Most groups we encounter in this paper will be finitely generated abelian groups, though this is not always immediate. Proposition 2.1.3.ii shows that the rank is a strong invariant for such groups; a torsion free finitely generated abelian group is determined up to isomorphism by its rank. There is a similar invariant for the torsion of a finitely generated abelian group, which is a finite abelian group. For the sake of legibility we denote the set $\{p^k \big| \ p \text{ prime and } k \in \mathbb{Z}_{>0}\}$ of all prime powers by $\mathcal{Q}$.

Definition 2.1.4. For any finite abelian group A and any $p^k \in \mathcal{Q}$ the *p^k-rank* of A is

$$\mathrm{r}_{p^k}(A) := \dim_{\mathbb{F}_p}(p^{k-1}A/p^kA).$$

Proposition 2.1.5. *Let A be a finite abelian group and $B \subseteq A$ a subgroup. Then for any $p^k \in \mathcal{Q}$ we have $\mathrm{r}_{p^k}(B) \leq \mathrm{r}_{p^k}(A)$.*

Proof. If $B \subseteq A$ then $p^{k-1}B \subseteq p^{k-1}A$, so without loss of generality we assume $k = 1$. For any finite abelian group G we have a short exact sequence

$$0 \longrightarrow [G]_p \longrightarrow G \longrightarrow pG \longrightarrow 0,$$

where the map $G \to pG$ is multiplication by p and $[G]_p = \{g \in G \big| \ pg = 0\}$ is its kernel. By exactness we have $\#G = \#[G]_p \cdot \#pG$, and it is clear that $[B]_p \subseteq [A]_q$, so

$$\#(B/pB) = \frac{\#B}{\#pB} = \#[B]_p \leq \#[A]_p = \frac{\#A}{\#pA} = \#(A/pA),$$

from which it is immediate that $\mathrm{r}_p(B) \leq \mathrm{r}_p(A)$. □

The following observation is known as the fundamental theorem on finite abelian groups.

Proposition 2.1.6. *For any finite abelian group A there is an isomorphism*

$$A \cong \bigoplus_{q \in \mathcal{Q}} C_q^{n_q},$$

where $n_{p^k} = r_{p^k}(A) - r_{p^{k+1}}(A) \geq 0$ for all $p^k \in \mathcal{Q}$.

Proof. See [2], Theorems I.1.8.1 and I.1.8.2. □

A finite abelian group is thus isomorphic to a finite direct sum of cyclic groups of prime power order, and the number of these cyclic groups is determined by the q-ranks of the finite abelian group. This easily extends to the fundamental theorem on finitely generated abelian groups, as such a group is the direct sum of its torsion subgroup and a finitely generated free abelian group. We conclude that a finitely generated abelian group is determined up to isomorphism by its free rank and the q-ranks of its torsion subgroup.

2.2 Reduced orders in rings of integers

We recall a few definitions concerning rings. Let A be a commutative ring.

Definition 2.2.1. The *nilradical* $\sqrt{0_A}$ of A is the set of all nilpotent elements of A.

Proposition 2.2.2. *The nilradical of A is the intersection of all prime ideals of A.*

Proof. See [1], Proposition 1.8. □

In particular the nilradical $\sqrt{0_A}$ is itself an ideal of A.

Definition 2.2.3. i. A ring A is called *reduced* if $\sqrt{0_A} = 0$.

ii. The ring $A_{\text{red}} := A/\sqrt{0_A}$ is called the *reduced ring* of A.

Lemma 2.2.4. *For any order A there natural map $A^\times_{\text{tor}} \to (A_{\text{red}})^\times_{\text{tor}}$ is injective.*

Proof. The projection $A \twoheadrightarrow A_{\text{red}}$ induces a surjection of the groups of units with kernel $1 + \sqrt{0_A}$. Consider its restriction $p : A^\times_{\text{tor}} \to (A_{\text{red}})^\times_{\text{tor}}$ to the groups of torsion units. Let $a \in \ker p$. Note that $\ker p \subseteq 1 + \sqrt{0_A}$ so there exists $x \in \sqrt{0_A}$ such that $a = 1 + x$. Let $n \in \mathbb{Z}_{>0}$ be such that $a^n = 1$, so that

$$a^n = (1 + x)^n = 1 + nx + \ldots + nx^{n-1} + x^n = 1,$$

from which it is immediate that $x(n + \ldots + nx^{n-2} + x^{n-1}) = 0$. If the parenthesised part of this product is a zero divisor, then so is n because the sum of a zero divisor and a nilpotent is again a zero divisor. But A has no additive torsion element other than zero because it is an order, so n is not a zero divisor. Then $x = 0$ and $a = 1$, so $\ker p$ is trivial. We see that the map $p : A^\times_{\text{tor}} \to (A_{\text{red}})^\times_{\text{tor}}$ is an injection. □

Henceforth we concern ourselves mostly with reduced orders, as the group of units of any order is isomorphic to a subgroup of the group of units of its reduced order. The natural setting of reduced orders is within the framework of number fields, or more precisely, their rings of integers.

Definition 2.2.5. A *number field* is a field extension of $\mathbb{Q}$ of finite degree.

Example 2.2.6. Of course $\mathbb{Q}$ is itself a number field. Other familiar examples are $\mathbb{Q}(\text{i})$, and more generally the quadratic fields $\mathbb{Q}(\sqrt{d})$ for d an integer, as well as the cyclotomic fields $\mathbb{Q}(\zeta_n)$ where ζ_n is a primitive n-th root of unity. Note that any number field K is of the form $K = \mathbb{Q}(x)$ for some $x \in K$.

Definition 2.2.7. Let K be a number field. The *ring of integers* of K is the set

$$\mathcal{O}_K := \{\alpha \in K \,\big|\, (\exists f \in \mathbb{Z}[X])(f \text{ is monic and } f(\alpha) = 0)\}.$$

As the name suggests, the ring of integers of a number field is indeed a ring. It is easily verified that $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, and that $\mathcal{O}_{\mathbb{Q}(\mathrm{i})} = \mathbb{Z}[\mathrm{i}]$, and similarly we have $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. The ring of integers of any number field K is an order; clearly $\mathcal{O}_K^+$ is torsion-free, and to for a proof of the fact that it is finitely generated see [5], Corollary 2.30.

Definition 2.2.8. A commutative ring is called *Artinian* if every descending chain of ideals stabilises.

Definition 2.2.9. The *spectrum* $\mathrm{Spec}(A)$ of A is the set of all prime ideals of A.

Proposition 2.2.10. i. *In an Artinian ring every prime ideal is maximal.*

ii. *The spectrum of an Artinian ring is finite.*

iii. *In an Artinian ring the nilradical is nilpotent.*

iv. *Let k be a field and V a ring, and $f : k \longrightarrow V$ a ring homomorphism. If V is finitely generated as a ring over the image of k in V, then V is Artinian.*

*Proof.*i.−iii. See [1], Propositions 8.1, 8.3 and 8.4.

iv. Let K be the image of k in V. If V is finitely generated as a ring over K then it is a finite dimensional K-vector space. Its ideals are then K-vector subspaces, and dimension is decreasing in a descending chain of K-vector subspaces, so any descending chain of ideals in V stabilises.

□

Theorem 2.2.11. *A ring A is a reduced order if and only if it is isomorphic to a subring of finite index of a finite product of rings of integers.*

Proof. By Example 1.0.2 a subring of finite index of a finite product of rings of integers is an order. Rings of integers are reduced because they are contained in number fields, and it is immediate that any subring of a finite product of rings of integers is also reduced.

To see that the converse holds, note that the map $A \longrightarrow A_{\mathbb{Q}} : a \longmapsto a \otimes 1$ is injective, and that $A_{\mathbb{Q}}$ is reduced because A is. Of course $A_{\mathbb{Q}}$ is a finite dimensional $\mathbb{Q}$-vector space, so $A_{\mathbb{Q}}$ is Artinian by Proposition 2.2.10.iv. Consider the map

$$A_{\mathbb{Q}} \longrightarrow \prod_{\mathfrak{p} \in \mathrm{Spec}(A_{\mathbb{Q}})} A_{\mathbb{Q}}/\mathfrak{p} : a \longmapsto (a + \mathfrak{p})_{\mathfrak{p} \in \mathrm{Spec}(A_{\mathbb{Q}})}.$$

By Proposition 2.2.10.i all prime ideals of $A_{\mathbb{Q}}$ are maximal, so by the Chinese remainder theorem this map is surjective. Its kernel is the intersection of all prime ideals of $A_{\mathbb{Q}}$, i.e. the nilradical of $A_{\mathbb{Q}}$, which is zero because $A_{\mathbb{Q}}$ is reduced, so this map is an isomorphism.

The residue fields $A_{\mathbb{Q}}/\mathfrak{p}$ are finite dimensional $\mathbb{Q}$-vector spaces, and hence number fields. Denote the product of the rings of integers of these number fields by $\mathcal{O}$, which is a finite product by Proposition 2.2.10.ii. The image of an element $a \in A$ is contained $\mathcal{O}$ if and only if for all $\mathfrak{p} \in \mathrm{Spec}(A_{\mathbb{Q}})$ there exists a monic $f_{\mathfrak{p}} \in \mathbb{Z}[X]$ with $f_{\mathfrak{p}}(a \otimes 1) \in \mathfrak{p}$. This is satisfied if there exists a monic $f \in \mathbb{Z}[X]$ with $f(a) = 0$. Of course the powers of a generate a subgroup of the additive group A^+ which is finitely generated because A^+ is, from which it follows that indeed there exists a monic $f \in \mathbb{Z}[X]$ such that $f(a) = 0$. It follows that A is isomorphic to a subring of $\mathcal{O}$. Both rings are finitely generated, and we have

$$\mathrm{rank}(\mathcal{O}) = \mathrm{rank}\left(\prod_{\mathfrak{p}\in\mathrm{Spec}(A_{\mathbb{Q}})} A_{\mathbb{Q}}/\mathfrak{p}\right) = \mathrm{rank}(A_{\mathbb{Q}}) = \mathrm{rank}(A),$$

so A is isomorphic to a subring of finite index in $\mathcal{O}$, a finite product of rings of integers. □

For a group G and a subgroup $H \subseteq G$ we denote the index of H in G by $(G : H)$.

Lemma 2.2.12. *Let A be a commutative ring and $B \subseteq A$ a subring. If $(A^+ : B^+)$ is finite, then $(A^\times : B^\times)$ is also finite.*

Proof. First note that $\#(A^+/B^+) = (A^+ : B^+) < \infty$ and $\#(A^\times/B^\times) = (A^\times : B^\times)$. Consider the natural action of B on A^+/B^+ by multiplication

$$\varphi : B \longmapsto \mathrm{End}(A^+/B^+) : b \longmapsto (\overline{a} \longmapsto \overline{ba}).$$

Given that A^+/B^+ is finite so is $\mathrm{End}(A^+/B^+)$, and it follows that $B/\ker\varphi$ is finite. Note that $\ker\varphi = \{b \in B : (\forall a \in A)(ba \in B)\}$ is also an ideal of A, and it is clear that

$$\#(A/\ker\varphi) = ((A/\ker\varphi)^+ : (B/\ker\varphi)^+) \cdot \#(B/\ker\varphi) = (A^+ : B^+) \cdot \#(B/\ker\varphi),$$

so $A/\ker\varphi$ is also finite. Next consider the canonical projection $\pi : A^\times \twoheadrightarrow (A/\ker\varphi)^\times$. Of course $\ker\pi = 1 + \ker\varphi$, from which we find that $\ker\pi \subseteq B^\times$. This yields maps

$$A^\times/B^\times \twoheadleftarrow A^\times/\ker\pi \hookrightarrow (A/\ker\varphi)^\times,$$

where $A/\ker\varphi$ is finite. It follows that $A^\times/B^\times$ is finite, so $B^\times \subseteq A^\times$ is of finite index. □

Consequently if A is a reduced order isomorphic to a subring of finite index of a product $\prod_{i=1}^m \mathcal{O}_{K_i}$ of rings of integers, then the group of units $A^\times$ is of finite index in $\prod_{i=1}^m \mathcal{O}_{K_i}^\times$. In particular their ranks are equal, and we find

$$\mathrm{rank}(A^\times) = \mathrm{rank}\left(\prod_{i=1}^m \mathcal{O}_{K_i}^\times\right) = \sum_{i=1}^m \mathrm{rank}(\mathcal{O}_{K_i}^\times).$$

2.3 The Dirichlet unit theorem

There is a rather convenient result from number theory, the Dirichlet unit theorem, which we state without proof.

Theorem 2.3.1. *(Dirichlet unit theorem) Let K be a number field. Let r be the number of embeddings $K \hookrightarrow \mathbb{R}$, and s the number of conjugate pairs of embeddings $K \hookrightarrow \mathbb{C}$ whose image is not contained in $\mathbb{R}$. Then $\mathcal{O}_K^\times$ is finitely generated, and*

$$\operatorname{rank}(\mathcal{O}_K^\times) = r + s - 1.$$

Proof. See [5], Theorem 5.1. □

This enables us to determine the rank of the group of units of the ring of integers of any number field, and by extension the rank the group of units of any reduced order. From Lemma 2.2.11 it is immediate that the group of units of any reduced order is finitely generated.

Theorem 2.3.2. *Let A be an order. Then*

$$\operatorname{rank}(A^\times) = \#\operatorname{Spec}(A_{\mathbb{R}}) - \#\operatorname{Spec}(A_{\mathbb{Q}}) + \operatorname{rank}(\sqrt{0_A}).$$

Proof. We first show that $\operatorname{rank}(A^\times) = \operatorname{rank}(A_{\mathrm{red}}^\times) + \operatorname{rank}(\sqrt{0_A})$. The sequence

$$1 \longrightarrow 1 + \sqrt{0_A} \longrightarrow A^\times \longrightarrow (A_{\mathrm{red}})^\times \longrightarrow 1$$

is short exact, from which it is immediate that $\operatorname{rank}(A^\times) = \operatorname{rank}(A_{\mathrm{red}}^\times) + \operatorname{rank}(1 + \sqrt{0_A})$. Note that $\sqrt{0_{A_{\mathbb{Q}}}}$ is nilpotent by Proposition 2.2.10.iii because $A_{\mathbb{Q}}$ is Artinian, as before. This is also immediate from the fact that $\sqrt{0_{A_{\mathbb{Q}}}}$ is finitely generated because $A_{\mathbb{Q}}$ is. Then there exists $k \in \mathbb{Z}_{>0}$ such that $x^k = 0$ holds for all $x \in \sqrt{0_{A_{\mathbb{Q}}}}$, hence the maps

$$\begin{aligned} \exp: \quad & \sqrt{0_{A_{\mathbb{Q}}}} \longrightarrow 1 + \sqrt{0_{A_{\mathbb{Q}}}} : \; x \longmapsto \sum_{i=0}^{\infty} \frac{x^i}{i!}, \\ \log: \quad & 1 + \sqrt{0_{A_{\mathbb{Q}}}} \longrightarrow \sqrt{0_{A_{\mathbb{Q}}}} : \; 1 - x \longmapsto -\sum_{i=1}^{\infty} \frac{x^i}{i}. \end{aligned}$$

are well-defined because the sums are finite. Moreover, these are homomorphisms and they are each others inverses, hence they are isomorphisms, see also section 17.2 of [3]. Clearly $\sqrt{0_A} \subseteq \sqrt{0_{A_{\mathbb{Q}}}}$ and $1 + \sqrt{0_A} \subseteq 1 + \sqrt{0_{A_{\mathbb{Q}}}}$ are subgroups. The restriction of exp to the subgroup $k!\sqrt{0_A}$ is injective, and its image is contained in $1 + \sqrt{0_A}$ because the factor $k!$ cancels out all denominators. Analogously the restriction of log to the subgroup $1 + \sqrt{0_A}$ is injective, and its image is contained in the subgroup $\frac{1}{k!}\sqrt{0_A}$ because the lcm of the denominators divides $k!$. These injections yield inequalities

$$\operatorname{rank}(k!\sqrt{0_A}) \leq \operatorname{rank}(1 + \sqrt{0_A}) \leq \operatorname{rank}\left(\frac{1}{k!}\sqrt{0_A}\right).$$

Of course multiplication by $k!$ yields isomorphisms $\frac{1}{k!}\sqrt{0_A} \cong \sqrt{0_A} \cong k!\sqrt{0_A}$. It is then immediate that $\operatorname{rank}(1+\sqrt{0_A}) = \operatorname{rank}(\sqrt{0_A})$, hence $\operatorname{rank}(A^\times) = \operatorname{rank}(A^\times_{\mathrm{red}}) + \operatorname{rank}(\sqrt{0_A})$.

It remains to show that $\operatorname{rank}(A^\times) = \#\operatorname{Spec}(A_\mathbb{R}) - \#\operatorname{Spec}(A_\mathbb{Q})$ holds if A is reduced. In this case Theorem 2.2.11 yields an embedding $A \hookrightarrow \prod_{i=1}^m \mathcal{O}_{K_i}$, where the K_i are number fields, and the image of A is a subring of finite index. By Lemma 2.2.12 we have

$$\operatorname{rank}(A^\times) = \operatorname{rank}\left(\prod_{i=1}^m \mathcal{O}_{K_i}^\times\right) = \sum_{i=1}^m \operatorname{rank}\left(\mathcal{O}_{K_i}^\times\right).$$

Let r_i and $2s_i$ denote the number of real and imaginary non-real embeddings of K_i, respectively. Then the Dirichlet unit theorem yields

$$\operatorname{rank}(A^\times) = \sum_{i=1}^m \operatorname{rank}\left(\mathcal{O}_{K_i}^\times\right) = \sum_{i=1}^m (r_i + s_i - 1).$$

Note that $A_\mathbb{Q} \cong \prod_{i=1}^m (\mathcal{O}_{K_i} \otimes \mathbb{Q}) \cong \prod_{i=1}^m K_i$, and from $A_\mathbb{R} = A_\mathbb{Q} \otimes \mathbb{R}$ we find

$$A_\mathbb{R} \cong \prod_{i=1}^m (K_i \otimes \mathbb{R}) \cong \prod_{i=1}^m (\mathbb{R}^{r_i} \times \mathbb{C}^{s_i}),$$

where the latter isomorphism is a direct consequence of the Chinese remainder theorem; the embeddings of K_i into $\mathbb{R}$ and $\mathbb{C}$ correspond to the real roots and pairs of imaginary roots of f_i, where $K_i \cong \mathbb{Q}[X]/(f_i)$. Having expressed both $A_\mathbb{Q}$ and $A_\mathbb{R}$ as products of fields, we readily calculate

$$\#\operatorname{Spec}(A_\mathbb{R}) = \sum_{i=1}^m (r_i + s_i), \qquad \text{and} \qquad \#\operatorname{Spec}(A_\mathbb{Q}) = m.$$

It is now immediate that $\operatorname{rank}(A^\times) = \sum_{i=1}^m (r_i + s_i - 1) = \#\operatorname{Spec}(A_\mathbb{R}) - \#\operatorname{Spec}(A_\mathbb{Q})$. □

Proposition 2.3.3. *For a reduced order A we have $\#\operatorname{Spec}(A_\mathbb{R}) \geq \#\operatorname{Spec}(A_\mathbb{Q})$.*

Proof. We continue using the notation used in the proof of Theorem 2.3.2. We have $\#\operatorname{Spec}(A_\mathbb{R}) = \sum_{i=1}^m (r_i + s_i)$ where $m = \#\operatorname{Spec}(A_\mathbb{Q})$. Also $K_i \otimes \mathbb{R} \cong \mathbb{R}^{r_i} \times \mathbb{C}^{s_i}$ holds for all i, so either $r_i \geq 1$ or $s_i \geq 1$. It follows that $\#\operatorname{Spec}(A_\mathbb{R}) \geq \sum_{i=1}^m 1 = \#\operatorname{Spec}(A_\mathbb{Q})$. □

Corollary 2.3.4. *The group of units of an order A is finite if and only if A is reduced and $\#\operatorname{Spec}(A_\mathbb{R}) = \#\operatorname{Spec}(A_\mathbb{Q})$.*

Proof. The group of units of A is finite if and only if $\operatorname{rank}(A^\times) = 0$, or equivalently $\#\operatorname{Spec}(A_\mathbb{R}) - \#\operatorname{Spec}(A_\mathbb{Q}) + \operatorname{rank}(\sqrt{0_A}) = 0$ by Theorem 2.3.2. From Corollary 2.3.3 we find that $\#\operatorname{Spec}(A_\mathbb{R}) - \#\operatorname{Spec}(A_\mathbb{Q}) \geq 0$, so $A^\times$ is finite if and only if $\#\operatorname{Spec}(A_\mathbb{R}) = \#\operatorname{Spec}(A_\mathbb{Q})$ and $\operatorname{rank}(\sqrt{0_A}) = 0$. □

3. Finite groups of units in monogenic orders

3.1 Monogenic orders

We recall that a monogenic order is a ring A for which there exists a monic $f \in \mathbb{Z}[X]$ such that $A \cong \mathbb{Z}[X]/(f)$. For a monogenic order $A \cong \mathbb{Z}[X]/(f)$ the result of Theorem 2.3.2 translates directly to the irreducible factors of f; we have $A_{\mathbb{Q}} \cong \mathbb{Q}[X]/(f)$ and $A_{\mathbb{R}} \cong \mathbb{R}[X]/(f)$ and the prime ideals of these rings are the principal ideals generated by the irreducible factors of f. The rank of $\sqrt{0_A}$ is simply the degree of $f/\operatorname{rad}(f)$, where the *radical* of f is the product of the distinct monic irreducible factors of f over $\mathbb{Q}$.

Corollary 3.1.1. *For monic $f \in \mathbb{Z}[X]$ the following are equivalent:*

i. *All monic irreducible factors of f over $\mathbb{Q}$ are distinct and irreducible over $\mathbb{R}$.*

ii. *$(\mathbb{Z}[X]/(f))^\times$ is finite.*

Proof. 'i. $\Rightarrow$ ii.': The ring $\mathbb{Z}[X]/(f)$ is a subring of the ring of integers of $\mathbb{Q}[X]/(f)$, so $(\mathbb{Z}[X]/(f))^\times$ is finitely generated by Theorem 2.3.1. All irreducible factors of f over $\mathbb{Q}$ are distinct so $\operatorname{rad}(f) = f$, from which it is immediate that $\operatorname{rank}(\sqrt{0_A}) = \deg(f/\operatorname{rad}(f)) = 0$. Then $\#\operatorname{Spec}(A_{\mathbb{Q}})$ is the number of irreducible factors of f over $\mathbb{Q}$, and each of these factors is irreducible over $\mathbb{R}$ so $\#\operatorname{Spec}(A_{\mathbb{Q}}) \geq \#\operatorname{Spec}(A_{\mathbb{R}})$. Equality holds by Corollary 2.3.3, so $\operatorname{rank}(\mathbb{Z}[X]/(f))^\times = 0$ by Corollary 2.3.4 which means $(\mathbb{Z}[X]/(f))^\times$ is finite.

'ii. $\Rightarrow$ i.': If $A = (\mathbb{Z}[X]/(f))^\times$ is finite for a given monic $f \in \mathbb{Z}[X]$, then by Corollary 2.3.4 we have $\#\operatorname{Spec}(A_{\mathbb{Q}}) = \#\operatorname{Spec}(A_{\mathbb{R}})$ and $\operatorname{rank}(\sqrt{0_A}) = 0$. The latter tells us that $f = \operatorname{rad}(f)$, i.e. that all irreducible factors of f over $\mathbb{Q}$ are distinct. The numbers of irreducible factors of f over $\mathbb{Q}$ and over $\mathbb{R}$ are equal because $\#\operatorname{Spec}(A_{\mathbb{Q}}) = \#\operatorname{Spec}(A_{\mathbb{R}})$, so all irreducible factors of f over $\mathbb{Q}$ are irreducible over $\mathbb{R}$. □

The polynomials $f \in \mathbb{Z}[X]$ having the two equivalent properties described in Corollary 3.1.1 can be characterised more explicitly. To this end we let

$$\mathcal{D} := \{g \in \mathbb{Z}[X] \big| \ g \text{ monic and irreducible over } \mathbb{R}\}.$$

We can describe $\mathcal{D}$ very explicitly; a polynomial $g \in \mathbb{Z}[X]$ is irreducible over $\mathbb{R}$ if and only if it is either linear, or quadratic with negative discriminant. Note that $\operatorname{Aut}\mathbb{Z}[X]$ acts naturally on $\mathcal{D}$.

Proposition 3.1.2. *A homomorphism $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[X]$ is an automorphism of $\mathbb{Z}[X]$ if and only if $\varphi(X) = aX + b$ for some $a \in \mathbb{Z}^\times$ and some $b \in \mathbb{Z}$.*

Proof. First note that any homomorphism $\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[X]$ is fully determined by the value of $\varphi(X)$. It is clear that if $\varphi(X) = aX + b$ with $a \in \mathbb{Z}^\times$ and $b \in Z$, then φ is an automorphism; its inverse is given by $\varphi^{-1}(X) = aX - ab$.

Conversely, if φ is a ring automorphism and $d := \deg(\varphi(X))$, then for any non-constant polynomial $f \in \mathbb{Z}[X]$ we have $\deg(\varphi(f)) \geq d$ because f is a linear combination of powers of X. However φ is surjective, so there exists a non-constant $f \in \mathbb{Z}[X]$ such that $\varphi(f) = X$. It follows that $d = 1$, so $\varphi(X) = aX + b$ for some $a, b \in \mathbb{Z}$. Of course φ^{-1} is also an automorphism, hence $\varphi^{-1}(X) = a'X + b'$ for some $a', b' \in \mathbb{Z}$, and so $X = (\varphi^{-1} \circ \varphi)(X) = a'aX + a'b + b'$, from which it is immediate that $a \in \mathbb{Z}^\times$. □

We see that two polynomials $f, g \in \mathcal{D}$ are in the same orbit under the action of $\operatorname{Aut}\mathbb{Z}[X]$ if and only if $\Delta(f) = \Delta(g)$, where $\Delta(f)$ denotes the discriminant of f.

For finite subsets $S \subset \mathcal{D}$ we introduce the notations

$$f_S := \prod_{g \in S} g \qquad \text{and} \qquad S^\times := (\mathbb{Z}[X]/(f_S))^\times.$$

Proposition 3.1.3. *The map from the set of finite subsets of $\mathcal{D}$ to the set of monic $f \in \mathbb{Z}[X]$ for which $(\mathbb{Z}[X]/(f))^\times$ is finite, given by $S \mapsto f_S$, is a bijection.*

Proof. Let S be a finite subset of $\mathcal{D}$, so that f_S is monic and has no repeated irreducible factors over $\mathbb{Q}$. Of course the irreducible factors of f_S over $\mathbb{Q}$ are precisely the $g \in S$, which are irreducible over $\mathbb{R}$. It follows from Corollary 3.1.1 that $(\mathbb{Z}[X]/(f))^\times$ is finite.

Conversely, let $f \in \mathbb{Z}[X]$ be monic and such that $(\mathbb{Z}[X]/(f))^\times$ is finite. Consider the set

$$S = \{g \in \mathbb{Z}[X] \big| \ g \text{ irreducible over } \mathbb{Q} \text{ and } g \mid f\}.$$

Of course S is finite and all $g \in S$ are monic. By Corollary 3.1.1 all $g \in S$ are irreducible over $\mathbb{R}$, so S is a finite subset of $\mathcal{D}$. Also, by Corollary 3.1.1 all irreducible factors of f are distinct so $f = f_S$. We see that the map $S \mapsto f_S$ is a bijection between the finite subsets of $\mathcal{D}$ and the monic $f \in \mathbb{Z}[X]$ for which $(\mathbb{Z}[X]/(f))^\times$ is finite. □

Next we classify the isomorphism types of the groups of units of $\mathbb{Z}[X]/(g)$ for all $g \in \mathcal{D}$.

Lemma 3.1.4. *For all $g \in \mathcal{D}$ the group of units of $\mathbb{Z}[X]/(g)$ is cyclic. More precisely,*

$$\{g\}^\times \cong \begin{cases} C_6 & \text{if } \Delta(g) = -3 \\ C_4 & \text{if } \Delta(g) = -4 \\ C_2 & \text{otherwise} \end{cases}.$$

Proof. Note that $\mathbb{Z}[X]/(g) \cong \mathbb{Z}[\alpha]$ for any complex root α of g. It is immediate from Proposition 3.1.3 that $\{g\}^\times$ is finite. Then the units of $\mathbb{Z}[\alpha]$ are torsion elements of $\mathbb{C}^\times$, so for a unit $u \in \mathbb{Z}[\alpha]$ we have $|u| = 1$, and in particular $|\operatorname{im}(u)| \leq 1$. Letting $z = x + y\alpha \in \mathbb{Z}[\alpha]$ with $x, y \in \mathbb{Z}$ we see that $\operatorname{im}(z) = y \operatorname{im}(\alpha) = \frac{y}{2}\sqrt{-\Delta(g)}$. For $\Delta(g) < -4$ it is immediate that if $|\operatorname{im}(z)| \leq 1$, then $y = 0$, so the units of $\mathbb{Z}[\alpha]$ are ± 1. It follows that $(\mathbb{Z}[X]/(g))^\times \cong \mathbb{Z}[\alpha]^\times \cong C_2$.

For $\Delta(g) = -4$ we have $|\operatorname{im}(x + y\alpha)| = |y|$, so there are at most four units in $\mathbb{Z}[\alpha]$. For $g = X^2 + bX + c$ we see that b is even, and letting $x := \frac{b}{2}$ we find that $x + \alpha$ is a primitive fourth root of unity, so $(\mathbb{Z}[X]/(g))^\times \cong \mathbb{Z}[\alpha]^\times \cong C_4$.

For $\Delta(g) = -3$ we have $|\operatorname{im}(x + y\alpha)| = \frac{1}{2}\sqrt{3}|y|$, so there are at most six units in $\mathbb{Z}[\alpha]$. For $g = X^2 + bX + c$ we see that b is odd, and letting $x := \frac{b+1}{2}$ we find that $x + \alpha$ is a primitive sixth root of unity, so $(\mathbb{Z}[X]/(g))^\times \cong \mathbb{Z}[\alpha]^\times \cong C_6$. □

Corollary 3.1.5. *Let A be a monogenic order with a finite group of units. Then the exponent of $A^\times$ divides 12.*

Proof. As $A^\times$ is finite there exists a finite subset $S \subset \mathcal{D}$ such that $A \cong \mathbb{Z}[X]/(f_S)$. We have an embedding $A \hookrightarrow \prod_{g \in S} \mathbb{Z}[X]/(g)$, which induces an embedding of the groups of units

$$A^\times \hookrightarrow \prod_{g \in S} \{g\}^\times \cong C_2^a \times C_4^b \times C_6^c,$$

for some $a, b, c \in \mathbb{Z}_{\geq 0}$, as a direct consequence of Lemma 3.1.4. Hence $A^\times$ is isomorphic to a subgroup of $C_2^a \times C_4^b \times C_6^c$, from which it is immediate that the exponent of $A^\times$ divides $\operatorname{lcm}(2, 4, 6) = 12$. □

Proposition 3.1.6. *For any finite $S \subset \mathcal{D}$ we have $\mathrm{r}_2(S^\times) \leq \#S$.*

Proof. Let $S \subset \mathcal{D}$ be finite. From Lemma 3.1.4 it is immediate that $\mathrm{r}_2(\{g\}^\times) \leq 1$ for any $g \in \mathcal{D}$, and we have seen that $S^\times$ is isomorphic to a subgroup of $\prod_{g \in S} \{g\}^\times$. Then by Proposition 2.1.5 we find that for any finite $S \subset \mathcal{D}$

$$\mathrm{r}_2(S^\times) \leq \mathrm{r}_2\left(\prod_{g \in S} \{g\}^\times\right) = \sum_{g \in S} \mathrm{r}_2(\{g\}^\times) \leq \#S.$$

□

3.2 $\mathcal{S}$-polynomials

For a finite subset $S \subset \mathcal{D}$ with $g \in S$ we introduce the notation

$$\ker_{S,g} := \ker(S^\times \longrightarrow (S - \{g\})^\times),$$

in which the map is induced by the canonical projection $\mathbb{Z}[X]/(f_S) \twoheadrightarrow \mathbb{Z}[X]/(f_S/g)$. We focus on the subsets $S \subset \mathcal{D}$ for which $\ker_{S,g}$ is non-trivial for all $g \in S$. Let

$$\mathcal{S} := \{S \subset \mathcal{D} \big| \ S \text{ is finite and } (\forall g \in S)(\#\ker_{S,g} > 1)\}.$$

Note that $\varnothing \in \mathcal{S}$, and also $\{g\} \in \mathcal{S}$ for any $g \in \mathcal{D}$. If T is in $\mathcal{S}$ then any subset S of T is also in $\mathcal{S}$. The following proposition clarifies why it makes sense to focus on these subsets.

Proposition 3.2.1. *Let $T \subset \mathcal{D}$ be finite. Then there exists a subset $S \subseteq T$ with $S \in \mathcal{S}$ such that the natural map $T^\times \longrightarrow S^\times$ is injective.*

Proof. Suppose there exists a finite subset $T \subset \mathcal{D}$ for which there is no subset $S \subseteq T$ with $S \in \mathcal{S}$ and a natural injection $T^\times \hookrightarrow S^\times$. Let T_0 be such a subset of minimal order, so that in particular $T_0 \notin \mathcal{S}$. Then T_0 is nonempty and there exists $g \in T_0$ such that $\#\ker_{T_0,g} = 1$. Let $R := T_0 - \{g\}$, so we have a subset $R \subset T$ with a natural injection $T_0^\times \hookrightarrow R^\times$ because $\#\ker_{T_0,g} = 1$. By the minimality of the order of T_0 there exists a subset $S \subseteq R$ with $S \in \mathcal{S}$ together with a natural injection $R^\times \hookrightarrow S^\times$, and hence by composition we have a natural injection $T_0^\times \hookrightarrow S^\times$, where $S \subset T_0$ and $S \in \mathcal{S}$, a contradiction. □

So for any group of units $T^\times$ corresponding to a finite subset $T \subset \mathcal{D}$, there exists a subset $S \subseteq T$ such that $S \in \mathcal{S}$, and $T^\times$ is isomorphic to a subgroup of $S^\times$. Hence the maximal groups of units are found in $\mathcal{S}$.

Proposition 3.2.2. *Let $S \subset \mathcal{D}$ be finite and let $g \in S$. Then there is a canonical injection* $\ker_{S,g} \hookrightarrow \{g\}^\times$.

Proof. As before the canonical projection $\mathbb{Z}[X]/(f_S) \twoheadrightarrow \mathbb{Z}[X]/(g)$ induces a group homomorphism on the groups of units. Consider its restriction $\pi : \ker_{S,g} \to \{g\}^\times$ to $\ker_{S,g}$. Let $h \in \ker\pi$, so that in particular $h \in \ker_{S,g}$, i.e. $h \equiv 1 \bmod(f_S/g)$. Of course $h \in \ker\pi$ means that $h \equiv 1 \bmod(g)$, and as f_S/g and g have no common divisor it follows immediately that $h \equiv 1 \bmod(f_S)$. We see that $\ker\pi$ is trivial, so π is an injection. □

In view of Lemma 3.1.4 it is clear that $\#\ker_{S,g} = 2$, 3, 4 or 6 for any $S \in \mathcal{S}$ and any $g \in S$. So either $2 \mid \#\ker_{S,g}$ or $3 \mid \#\ker_{S,g}$, or both. We explore these three cases further. In order to make a clear classification it is convenient to introduce the resultant.

Definition 3.2.3. For nonzero $f, g \in \mathbb{Z}[X]$ factoring over $\mathbb{C}$ as $f = a\prod_{i=1}^{m}(X-\alpha_i)$ and $g = b\prod_{j=1}^{n}(X-\beta_j)$, the *resultant* of f and g is

$$R(f,g) := a^n b^m \prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i - \beta_j).$$

The following facts concerning the resultant are immediate from the definition.

Proposition 3.2.4. *Let $f, g \in \mathbb{Z}[X]$ factor over $\mathbb{C}$ as before. Then we have*

i $R(f,g) = (-1)^{mn}R(g,f)$.

ii $R(f,g) = a^n \prod_{i=1}^{m} g(\alpha_i)$,

iii *If $g \equiv g_1 \bmod(f)$ with $\deg(g_1) = m_1$, then $R(f,g) = a^{m-m_1}R(f,g_1)$.*

iv *For any nonzero $h \in \mathbb{Z}[X]$ we have $R(fg,h) = R(f,h)R(g,h)$.*

These four properties allow us to calculate $R(f,g)$ for any pair of polynomials $f, g \in \mathbb{Z}[X]$ without the need for explicit knowledge of the complex roots of f and g. Given nonzero $f, g \in \mathbb{Z}[X]$ we may repeatedly apply i and iii, reducing the degrees of the polynomials until either one is constant, which is then the value of their resultant. In particular we see that the resultant of any two nonzero $f, g \in \mathbb{Z}[X]$ is an integer, and that $R(f,g) \in (f,g)$.

Lemma 3.2.5. *For any two distinct $f, g \in \mathcal{D}$ we have $\#\mathbb{Z}[X]/(f,g) = |R(f,g)|$.*

Proof. If $\deg(f) = 1$ then $f = X - n$ for some $n \in \mathbb{Z}$, so by Proposition 3.2.4.ii we have $R(f,g) = g(n)$. We also have isomorphisms $\mathbb{Z}[X]/(f,g) \cong (\mathbb{Z}[X]/(f))/(\overline{g}) \cong \mathbb{Z}/(g(n))$, and it is immediate that $\#\mathbb{Z}[X]/(f,g) = \#\mathbb{Z}/(g(n)) = |g(n)| = |R(f,g)|$.

Suppose $\deg(f) = \deg(g) = 2$. Let $\alpha_1, \alpha_2 \in \mathbb{C}$ be the roots of f, so we have a s.e.s.

$$0 \longrightarrow \mathbb{Z}[\alpha_1]/(g(\alpha_1)) \xrightarrow{\iota} \mathbb{Z}[\alpha_1]/(g(\alpha_1)g(\alpha_2)) \xrightarrow{\pi} \mathbb{Z}[\alpha_2]/(g(\alpha_2)) \longrightarrow 0.$$

The map ι is given by multiplication by $g(\alpha_2)$, and π is the canonical projection. By Proposition 3.2.4.ii we have $g(\alpha_1)g(\alpha_2) = R(f,g)$, from which it is immediate that $\#\mathbb{Z}[\alpha_1]/(g(\alpha_1)g(\alpha_2)) = |R(f,g)|^2$. Then all three groups are finite, and in particular

$$|R(f,g)|^2 = \#\mathbb{Z}[X]/(g(\alpha_1)g(\alpha_2)) = \#\mathbb{Z}[\alpha_1]/(g(\alpha_1)) \cdot \#\mathbb{Z}[\alpha_2]/(g(\alpha_2)).$$

For $i = 1, 2$ we have isomorphisms $\mathbb{Z}[X]/(f,g) \cong (\mathbb{Z}[X]/(f))/(\overline{g}) \cong \mathbb{Z}[\alpha_i]/(g(\alpha_i))$, from which it follows that $\#\mathbb{Z}[X]/(f,g) = |R(f,g)|$. □

Remark 3.2.6. This lemma allows us to compute $\#\mathbb{Z}[X]/(f_S, f_T)$ for any two finite subsets $S, T \subset \mathcal{D}$, using Proposition 3.2.4.iv. Lemma 3.2.5 in fact holds for any two monic $f, g \in \mathbb{Z}[X]$ that have no common divisor, see [6] for a proof.

Lemma 3.2.7. *Let $S \subset \mathcal{D}$ be finite and let $g \in S$. Then $2 \mid \#\ker_{S,g}$ if and only if 2 is contained in the $\mathbb{Z}[X]$-ideal generated by g and f_S/g.*

Proof. Let $K \subseteq \{g\}^\times$ be the image of $\ker_{S,g}$ under the injection of Proposition 3.2.2. Then $2 \mid \#\ker_{S,g}$ if and only if $-1 \in K$, i.e. if and only if there exist $h_1, h_2 \in \mathbb{Z}[X]$ such that $1 + h_1 \cdot f_S/g = -1 + h_2 \cdot g$. Of course $2 \in (g, f_S/g)$ if and only if there exist $h_1, h_2 \in \mathbb{Z}[X]$ such that $h_1 \cdot f_S/g - h_2 \cdot g = 2$, or equivalently $1 + h_1 \cdot f_S/g = -1 + h_2 \cdot g$, thus proving the lemma. □

An analogous statement holds in case the order of the kernel is divisible by three.

Lemma 3.2.8. *Let $S \subset \mathcal{D}$ be finite and let $g \in S$. Then $3 \mid \#\ker_{S,g}$ if and only if $\Delta(g) = -3$ and $|R(g, f_S/g)| \mid 3$.*

Proof. If $3 \mid \#\ker_{S,g}$ then also $3 \mid \#\{g\}^\times$, hence $\Delta(g) = -3$ by Lemma 3.1.4. Without loss of generality $g = X^2 + X + 1$. Let $K \subseteq \{g\}^\times$ be the image of $\ker_{S,g}$ under the injection of Proposition 3.2.2. As in the proof of the previous lemma we find that $3 \mid \#\ker_{S,g}$ if and only if $X \in K$, which is equivalent to $X - 1 \in (g, f_S/g)$. Then it remains to prove that $X - 1 \in (g, f_S/g)$ if and only if $|R(g, f_S/g)| \mid 3$.

'$\Rightarrow$' From $X - 1 \in (g, f_S/g)$ we get an inclusion $(g, X - 1) \subseteq (g, f_S/g)$, hence a surjection $\mathbb{Z}[X]/(X^2 + X + 1, X - 1) \twoheadrightarrow \mathbb{Z}[X]/(g, f_S/g)$. As $\mathbb{Z}[X]/(X^2 + X + 1, X - 1) \cong \mathbb{Z}/3\mathbb{Z}$, it follows immediately that $\#\mathbb{Z}[X]/(g, f_S/g) \mid 3$, and so $|R(g, f_S/g)| \mid 3$ by Lemma 3.2.5.

'$\Leftarrow$' If $|R(g, f_S/g)| = 1$ then $(g, f_S/g) = \mathbb{Z}[X]$ and then of course $X - 1 \in (g, f_S/g)$. Suppose $|R(g, f_S/g)| = 3$, so that $\#\mathbb{Z}[X]/(g, f_S/g) = 3$ and hence $3 \in (g, f_S/g)$. Then $\#\mathbb{Z}[X]/(g, f_S/g) = \#(\mathbb{Z}[X]/(g, 3))/(f_S/g)$, where $\#\mathbb{Z}[X]/(g, 3) = 3^2$. Then $f_S/g + (g, 3)$ is not a unit and not zero in $\mathbb{Z}[X]/(g, 3)$. Then by elimination we conclude that $f_S/g \equiv \pm(X - 1) \bmod (g, 3)$, from which it follows immediately that $X - 1 \in (g, f_S/g)$. □

Lemma 3.2.9. *Let $S \in \mathcal{S}$ and $g \in S$. Then $\#\ker_{S,g} \neq 3$.*

Proof. Suppose towards a contradiction that $\#\ker_{S,g} = 3$. Then by Lemma 3.2.8 we have $\Delta(g) = -3$ and $|R(g, f_S/g)| \mid 3$. If $|R(g, f_S/g)| = 1$ then $2 \in (g, f_S/g) = \mathbb{Z}[X]$ and so $2 \mid \#\ker_{S,g}$ by Lemma 3.2.7, which contradicts our assumption that $\#\ker_{S,g} = 3$.

Then $|R(g, f_S/g)| = 3$, so there exists a unique $h \in S$ such that $|R(g, h)| = 3$ by Proposition 3.2.4.iv. Then $3 \in (g, f_S/g)$ but $1 \notin (g, f_S/g)$, so in particular $2 \notin (g, f_S/g)$. It follows from Lemma 3.2.7 that $\#\ker_{S,g}$ is not divisible by 2, hence $3 \mid \#\ker_{S,h}$. From Lemma 3.2.8 we find that $\Delta(h) = -3$. Then $g \equiv h \equiv X^2 + X + 1 \bmod (2)$, hence taking the quotient of $\mathbb{Z}[X]/(g, h)$ by the ideal generated by 2 yields a surjection

$$\mathbb{Z}[X]/(g, h) \twoheadrightarrow \mathbb{F}_2[X]/(X^2 + X + 1),$$

where $\mathbb{F}_2[X]/(X^2 + X + 1) \cong \mathbb{F}_4$. It follows that $4 \mid |R(g, h)|$, a contradiction. □

This allows for a more explicit characterization of $\mathcal{S}$.

Theorem 3.2.10. *For any finite subset $S \subset \mathcal{D}$ the following are equivalent:*

i. $S \in \mathcal{S}$,

ii. $(\forall g \in S)(2 \in (g, f_S/g))$,

iii. $\mathrm{r}_2(S^\times) = \#S$.

Proof. 'i. $\Rightarrow$ ii.': Let $S \in \mathcal{S}$ and $g \in S$. From Proposition 3.2.2 we find that $\#\ker_{S,g} \mid 12$, and from $S \in \mathcal{S}$ it follows that $\#\ker_{S,g} \neq 1$ as well as $\#\ker_{S,g} \neq 3$ by Lemma 3.2.9. Then $2 \mid \#\ker_{S,g}$ and so from Lemma 3.2.7 we find that $2 \in (g, f_S/g)$.

'ii. $\Rightarrow$ iii.': Suppose that $2 \in (g, f_S/g)$ holds for all $g \in S$. Then for every $g \in S$ there exists $h_g \in \mathbb{Z}[X]/(f_S)$ such that $h_g \equiv -1 \bmod (g)$ and $h_g \equiv 1 \bmod (f_S/g)$. Each of the h_g has order 2 in $S^\times$, and the h_g are multiplicatively independent, meaning

$$\prod_{g \in S} h_g^{n_g} = 1 \qquad \Rightarrow \qquad n_g \equiv 0 \bmod 2 \ \text{ for all } g \in S.$$

It follows immediately that $\mathrm{r}_2(S^\times) \geq \#S$, and equality follows from Proposition 3.1.6.

'iii. $\Rightarrow$ i.': Suppose that $\mathrm{r}_2(S^\times) = \#S$ and $S \notin \mathcal{S}$, so there exists $g \in S$ with $\#\ker_{S,g} = 1$, yielding an injection $S^\times \hookrightarrow (S - \{g\})^\times$. Then it follows from Proposition 2.1.5 that $\mathrm{r}_2((S-\{g\})^\times) \geq \mathrm{r}_2(S^\times) = \#S$. But from Proposition 3.1.6 we find that $\mathrm{r}_2((S-\{g\})^\times) \leq \#(S - \{g\}) < \#S$, a contradiction. $\square$

3.3 A visual approach

The purpose of this section is to give a visual representation of $\mathcal{D}$ and $\mathcal{S}$. To this end we embed $\mathcal{D}$ into $\mathbb{C}$, by mapping $f \in \mathcal{D}$ to its unique root $\alpha_f \in \mathbb{C}$ with nonnegative imaginary part. We easily see that the map $\mathcal{D} \longrightarrow \mathbb{C} : f \longmapsto \alpha_f$ is injective; for α in the image the corresponding original is the minimal polynomial f_α of α over $\mathbb{Q}$. The image of this embedding is the discrete subset of $\mathbb{C}$ given by

$$\mathbb{D} := \left\{ \frac{a + \mathrm{i}\sqrt{b}}{2} \;\middle|\; a \in \mathbb{Z},\ b \in \mathbb{Z}_{\geq 0},\ b \equiv -a^2 \bmod 4 \right\}.$$

Figure 3.3 shows a part of $\mathbb{D}$ in the upper half-plane.

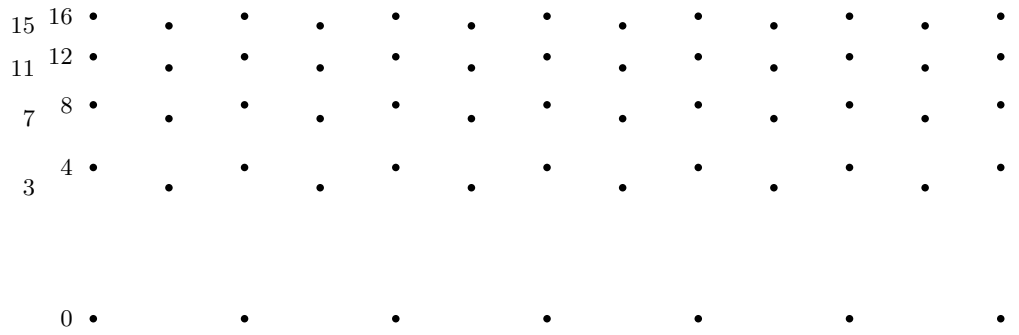


Figure 3.1: Part of $\mathbb{D}$, with $\mathrm{im}(\alpha)^2 = -\Delta(f_\alpha)$ to the left of each row.

The action of $\mathrm{Aut}\,\mathbb{Z}[X]$ on $\mathcal{D}$ extends to an action on $\mathbb{D}$. The automorphisms of the form $X \mapsto X + n$ correspond to horizontal translations of the upper half-plane, and the automorphisms of the form $X \mapsto -X + n$ correspond to reflections in the vertical lines with real part equal to $\frac{n}{2}$. It is then easy to see that two points $\alpha, \beta \in \mathbb{D}$ are in the same orbit if and only if $\mathrm{im}(\alpha) = \mathrm{im}(\beta)$, which is equivalent to $\Delta(f_\alpha) = \Delta(f_\beta)$.

Next we draw a graph, with $\mathbb{D}$ as the set of vertices. Two distinct vertices α and β are connected by an edge if and only if $\{f_\alpha, f_\beta\} \in \mathcal{S}$. It follows from Theorem 3.2.10 that this is the case if and only if $2 \in (f_\alpha, f_\beta)$. Both f_α and f_β are of degree at most two, so the ring $\mathbb{Z}[X]/(f_\alpha, f_\beta)$ is an $\mathbb{F}_2$-vector space of dimension at most two. We assign a weight to every edge; the weight of the edge connecting α and β is $\dim_{\mathbb{F}_2}(\mathbb{Z}[X]/(f_\alpha, f_\beta))$.

By Theorem 3.2.10 for any $S \in \mathcal{S}$ and any two distinct $f, g \in S$ the corresponding vertices α_f and α_g are connected by an edge, so any $S \in \mathcal{S}$ corresponds to a complete subgraph, which we will call a clique from here on. Not every clique in this graph corresponds to an $S \in \mathcal{S}$, however. After having constructed the graph we will establish a criterion for determining whether a clique corresponds to an $S \in \mathcal{S}$.

We draw four graphs; first one graph for each weight of edges, and finally the entire graph showing edges of all weights.

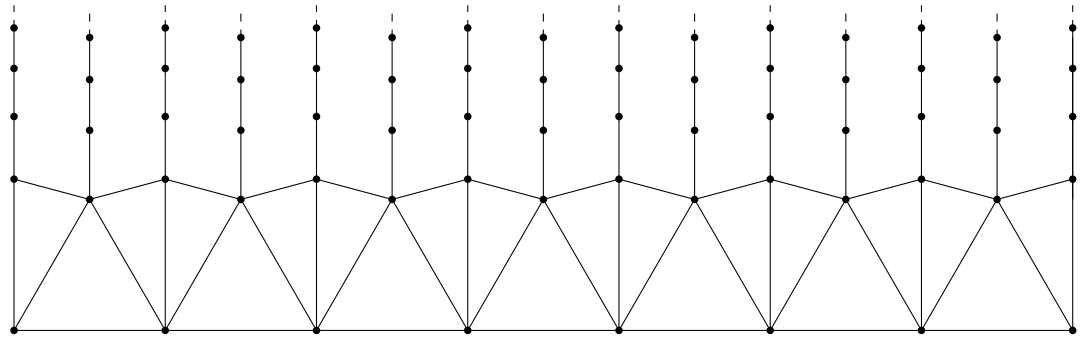


Figure 3.2: Two vertices are connected by an edge of weight 0 if and only if the $\mathbb{Z}[X]$-ideal generated by the two corresponding polynomials has index 1 in $\mathbb{Z}[X]$.

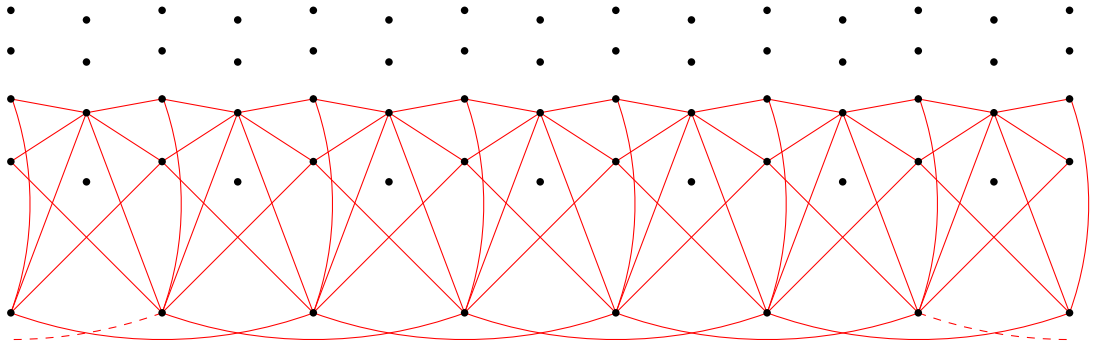


Figure 3.3: Two vertices are connected by an edge of weight 1 if and only if the $\mathbb{Z}[X]$-ideal generated by the two corresponding polynomials has index 2 in $\mathbb{Z}[X]$.

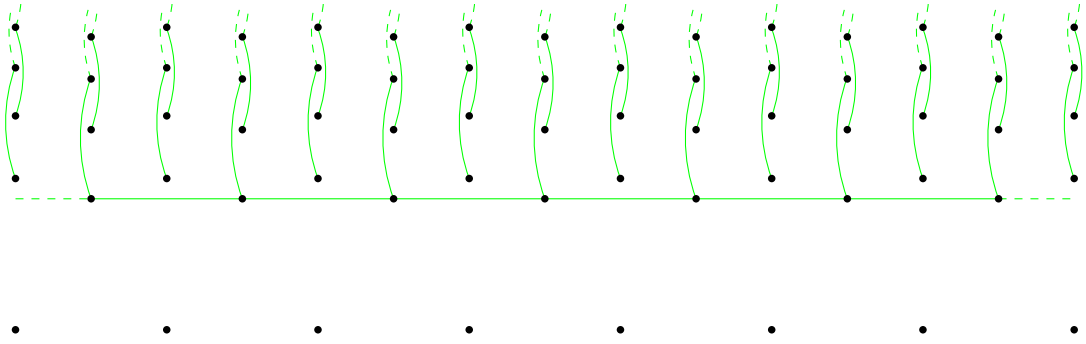


Figure 3.4: Two vertices are connected by an edge of weight 2 if and only if the $\mathbb{Z}[X]$-ideal generated by the corresponding polynomials has index 4 in $\mathbb{Z}[X]$ and contains 2.

As $\operatorname{Aut}\mathbb{Z}[X]$ acts on $\mathbb{D}$ and hence on the graph, to construct the entire graph we may simply choose a representative from each orbit under the action of $\operatorname{Aut}\mathbb{Z}[X]$, and determine all edges that connect to these representatives. We take $\{X, X^2+n, X^2+X+n \mid n \in \mathbb{Z}_{>0}\}$ as our set of representatives.

We first determine all edges of weight 0. For linear $f \in \mathcal{D}$ we have the representative $f = X$, in which case $\mathbb{Z}[X]/(f,g) \cong \mathbb{Z}/(g(0))$. So $\dim_{\mathbb{F}_2}(\mathbb{Z}[X]/(f,g)) = 0$ if and only if the constant term of g is ± 1. There are precisely 5 such polynomials in $\mathcal{D}$, these are $X \pm 1$, $X^2 \pm X + 1$ and $X^2 + 1$, yielding the 5 edges of weight 0 connecting to the vertex α_f with $f = X$, shown in Figure 3.2.

All remaining edges of weight 0 are between pairs of quadratic polynomials in $\mathcal{D}$. The $\mathbb{Z}[X]$-ideal (f,g) generated by distinct quadratic $f, g \in \mathcal{D}$ has index 1 if and only if the ring $\mathbb{Z}[X]/(f,g) \cong (\mathbb{Z}[X]/(f))/(\overline{g})$ is the zero ring, where $\overline{g} = g + (f)$. This is the case if and only if $(\overline{g}) = \mathbb{Z}[X]/(f)$, i.e. if and only if $\overline{g}$ is a unit in $\mathbb{Z}[X]/(f)$, and Lemma 3.1.4 describes $(\mathbb{Z}[X]/(f))^\times$ entirely for any $f \in \mathcal{D}$. We distinguish three cases:

i. For $\Delta(f) = -3$ we have the representative $f = X^2 + X + 1$ with $\{f\}^\times = \{\overline{\pm 1}, \overline{\pm X}, \overline{\pm(X+1)}\}$. The monic quadratic $g \in \mathbb{Z}[X]$ with $\overline{g} \in \{f\}^\times$ are thus

$$\begin{array}{ccc} f+1 = X^2+X+2 & f+X = X^2+2X+1 & f+(X+1) = X^2+2X+2 \\ f-1 = X^2+X & f-X = X^2+1 & f-(X+1) = X^2 \end{array}$$

Of these, X^2+X+2, X^2+2X+2 and X^2+1 are in $\mathcal{D}$, yielding a total of 5 edges of weight 0 connecting to vertex α_f with $f = X^2+X+1$, shown in Figure 3.2.

ii. For $\Delta(f) = -4$ we have the representative $f = X^2 + 1$ with $\{f\}^\times = \{\overline{\pm 1}, \overline{\pm X}\}$. The monic quadratic $g \in \mathbb{Z}[X]$ with $\overline{g} \in \{f\}^\times$ are thus

$$\begin{array}{cc} f+1 = X^2+2 & f+X = X^2+X+1 \\ f-1 = X^2 & f-X = X^2-X+1 \end{array}$$

Of these, X^2+2, X^2+X+1 and X^2-X+1 are in $\mathcal{D}$, yielding a total of 4 edges of weight 0 connecting to the vertex α_f with $f = X^2+1$, shown in Figure 3.2.

iii. For $\Delta(f) < -4$ there is a representative either of the form $f = X^2 + n$ or of the form $f = X^2 + X + n$ for some $n \in \mathbb{Z}_{>0}$, and in all cases $\{f\}^\times = \{\overline{\pm 1}\}$. The monic quadratic $g \in \mathbb{Z}[X]$ with $\overline{g} \in \{f\}^\times$ are thus $f \pm 1$, which are both in $\mathcal{D}$, yielding two edges of weight 0 connecting to these vertices, shown in Figure 3.2.

Hence we have determined all edges of weight 0 connecting to our representatives, which by symmetry determines all edges of weight 0 in the graph. A complete overview is shown in Figure 3.2.

Next we determine all edges of weight 1. For linear $f \in \mathcal{D}$ we have the representative $f = X$, in which case $\mathbb{Z}[X]/(f,g) \cong \mathbb{Z}/(g(0))$. So $\dim_{\mathbb{F}_2}(\mathbb{Z}[X]/(f,g)) = 1$ if and only if the constant term of g is ± 2. There are precisely 7 such polynomials in $\mathcal{D}$, these are $X \pm 2$, $X^2 \pm 2X + 2$, $X^2 \pm X + 2$ and $X^2 + 2$, yielding the 7 edges of weight 1 connecting to this vertex, shown in Figure 3.3.

For the quadratic $f, g \in \mathcal{D}$ we have $\#\mathbb{Z}[X]/(f,g) = 2$ if and only if either $(f,g) = (2, X)$ or $(f,g) = (2, X+1)$, and so $\Delta(f) \not\equiv \Delta(g) \bmod 4$. This means that any edge of weight 1 connects to a polynomial f with $4 \mid \Delta(f)$. We determine the edges of weight 1 connecting to these polynomials, and in doing so we distinguish three cases:

i. For $\Delta(f) = -4$ we have the representative $f = X^2 + 1$. Then

$$|R(X^2+1, X^2+aX+b)| = |R(X^2+1, aX+(b-1))| = a^2 + (b-1)^2,$$

and we find that $|R(f, X^2+aX+b)| = 2$ has the four solutions

$$X^2 + X, \qquad X^2 - X, \qquad X^2 + X + 2, \qquad X^2 - X + 2,$$

where $X^2 + X$ and $X^2 - X$ are not in $\mathcal{D}$, and $X^2 + X + 2$ and $X^2 - X + 2$ are in $\mathcal{D}$. This adds up to a total of four edges connecting to the vertex α_f with $f = X^2 + 1$.

ii. For $\Delta(f) = -8$ we have the representative $f = X^2 + 2$. Then

$$|R(X^2+2, X^2+aX+b)| = |R(X^2+2, aX+(b-2))| = 2a^2 + (b-2)^2,$$

and we find that $|R(f, X^2+aX+b)| = 2$ has the two solutions

$$X^2 + X + 2 \qquad \text{and} \qquad X^2 - X + 2,$$

which are both in $\mathcal{D}$. This adds up to a total of three edges connecting to the vertex α_f with $f = X^2 + 2$.

iii. For $\Delta(f) = -4n$ with $n > 2$ we have the representatives $f = X^2 + n$. Then

$$|R(X^2+n, X^2+aX+b)| = |R(X^2+n, aX+(b-n))| = na^2 + (b-n)^2,$$

and we find that $|R(f, X^2+aX+b)| = 2$ has no solutions, hence there are no edges connecting to the vertices α_f with $f = X^2 + n$ for $n > 2$.

Now we have determined all edges of weight 1 connecting to our representatives, which by symmetry and by the argument above determines all edges of weight 1 in the graph. A complete overview is shown in Figure 3.3.

Finally we determine all edges of weight 2. For linear $f \in \mathcal{D}$ we have the representative $f = X$, in which case $\mathbb{Z}[X]/(f,g) \cong \mathbb{Z}/(g(0))$ is cyclic, hence it is not a 2-dimensional $\mathbb{F}_2$-vector space, so there are no edges of weight 2 connected to this vertex.

For the quadratic $f \in \mathcal{D}$ the quotient ring $\mathbb{Z}[X]/(f,g)$ is a 2-dimensional $\mathbb{F}_2$ vector space if and only if $2 \in (f,g)$ and $\#\mathbb{Z}[X]/(f,g) = 4$. This is the case if and only if $\overline{g} = 2\overline{u}$ for some $\overline{u} \in \{f\}^\times$, and this condition is easily checked. We distinguish three cases:

i. For $\Delta(f) = -3$ we have the representative $f = X^2+X+1$, and the monic quadratic $g \in \mathbb{Z}[X]$ with $\overline{g} \in 2\{f\}^\times$ are

$$\begin{array}{lll} f+2 = X^2+X+3 & f+2X = X^2+3X+1 & f+2(X+1) = X^2+3X+3 \\ f-2 = X^2+X-1 & f-2X = X^2-X+1 & f-2(X+1) = X^2-X-1 \end{array}$$

Of these, X^2+X+3, X^2+3X+3 and X^2-X+1 are in $\mathcal{D}$, yielding the 3 edges of weight 2 connecting to this vertex, shown in Figure 3.4.

ii. For $\Delta(f) = -4$ we have the representative $f = X^2+1$, and the monic quadratic $g \in \mathbb{Z}[X]$ with $\overline{g} \in 2\{f\}^\times$ are

$$\begin{array}{ll} f+2 = X^2+3 & f+2X = X^2+2X+1 \\ f-2 = X^2-1 & f-2X = X^2-2X+1 \end{array}$$

Of these, only X^2+3 is in $\mathcal{D}$, yielding the single edge of weight 2 connecting to this vertex, shown in Figure 3.4.

iii. For $\Delta(f) < -4$ we have a representative $f = X^2+n$ or $f = X^2+X+n$ for some $n \in \mathbb{Z}_{>1}$, and in all cases the monic quadratic $g \in \mathbb{Z}[X]$ with $\overline{g} \in 2\{f\}^\times$ are $f \pm 2$. For $n = 2$ only $f+2$ is in $\mathcal{D}$, and for $n > 2$ both $f+2$ and $f-2$ are in $\mathcal{D}$, yielding the 1 or 2 edges of weight 2 connecting to these vertices, shown in Figure 3.4.

Hence we have determined all edges of weight 2 connecting to our representatives, which by symmetry determines all edges of weight 2 in the graph. A complete overview is shown in Figure 3.4.

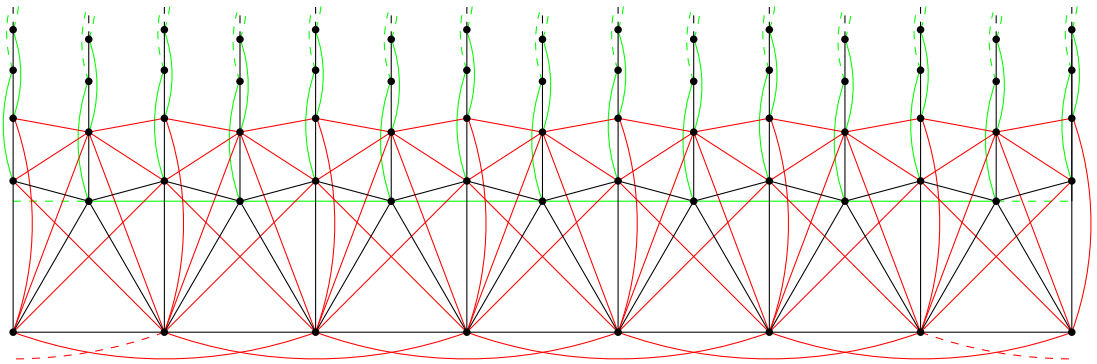


Figure 3.5: The full graph, showing edges of weights 0, 1 and 2 in black, red and green respectively.

3.4 A classification

The graph of Figure 3.5 shows whether $\{f, g\} \in \mathcal{S}$ for any two distinct $f, g \in \mathcal{D}$. It also shows whether $S \in \mathcal{S}$ for any $S \subset \mathcal{D}$, the following lemma explains how.

Lemma 3.4.1. *For any finite subset $S \subset \mathcal{D}$ the following are equivalent:*

i. $S \in \mathcal{S}$,

ii. *For any two distinct $f, g \in S$ we have $2 \in (f, g)$ and for any $g \in S$ we have*

$$\sum_{f \in S - \{g\}} \dim_{\mathbb{F}_2}(\mathbb{Z}[X]/(f, g)) \leq \deg g.$$

Proof. It follows from Lemma 3.2.5 and Proposition 3.2.4 that

$$\prod_{f \in S - \{g\}} \#\mathbb{Z}[X]/(f, g) = \prod_{f \in S - \{g\}} |R(f, g)| = |R(g, f_S/g)| = \#\mathbb{Z}[X]/(g, f_S/g),$$

so the inequality above is equivalent to $\#\mathbb{Z}[X]/(g, f_S/g) \mid 2^{\deg(g)}$.

'i. $\Rightarrow$ ii.': If $\#\mathbb{Z}[X]/(g, f_S/g) \mid 2$ then clearly $2 \in (g, f_S/g)$. If $\#\mathbb{Z}[X]/(g, f_S/g) = 4$ then either $|R(f, g)| = 4$ for some $f \in S - \{g\}$, or $|R(f_1, g)| = |R(f_2, g)| = 2$ for two distinct $f_1, f_2 \in S - \{g\}$. In the former case we have $(g, f_S/g) = (f, g)$ and hence $2 \in (g, f_S/g)$. In the latter case, note that $\deg(g) = 2$ so Figure 3.3 shows that $-4 \leq \Delta(g) \leq -8$. If either $\Delta(g) = -4$ or $\Delta(g) = -8$ then $\Delta(f_1) = \Delta(f_2) = -7$, and Figure 3.5 shows that $\{f_1, f_2\} \notin \mathcal{S}$, a contradiction. Hence $\Delta(g) = -7$ so without loss of generality we may assume that $g = X^2 + X + 2$ and $\{f_1, f_2\} = \{X^2 + 1, X^2 + 2\}$. It is then easily verified that $f_1 f_2 \equiv -2 \bmod (g)$, so indeed $2 \in (g, f_1 f_2)$ and hence $2 \in (g, f_S/g)$.

'ii. $\Rightarrow$ i.': For any $S \in \mathcal{S}$ and any $g \in S$ we have $2 \in (g, f_S/g)$ by to Theorem 3.2.10, so in particular $2 \in (f, g)$ holds for any $f \in S - \{g\}$. Moreover, it follows that $\mathbb{Z}[X]/(g, f_S/g)$ is an $\mathbb{F}_2$-vector space of dimension at most $\deg(g)$, from which it is immediate that $\#\mathbb{Z}[X]/(g, f_S/g) \mid 2^{\deg(g)}$. □

According to Lemma 3.4.1 the $S \in \mathcal{S}$ correspond bijectively to those cliques in the graph in Figure 3.5 for which the sum of the weights of the edges at each vertex is no greater than the degree of the polynomial corresponding to that vertex. We call a clique with this property a *suitable clique*. Theorem 3.2.10 allows us to determine the 2-rank of the group of units corresponding to a suitable clique; it is the number of vertices of the clique. The following lemmas allow us to easily determine the 3-rank and the 4-rank of $S^\times$ for any $S \in \mathcal{S}$ by inspecting the corresponding clique.

Lemma 3.4.2. *For $S \in \mathcal{S}$ we have*

$$\mathrm{r}_3(S^\times) = \begin{cases} 0 & \text{if } (\forall g \in S)(\Delta(g) = -3 \;\Rightarrow\; g+2 \in S), \\ 1 & \text{otherwise.} \end{cases}$$

Proof. First note that for any $S \in \mathcal{S}$ the 3-rank of $S^\times$ is no greater than the number of $g \in S$ with $\Delta(g) = -3$. So if there are no $g \in S$ with $\Delta(g) = -3$ then $\mathrm{r}_3(S^\times) = 0$, and indeed the condition is trivially met. From Figure 3.5 it is clear that any $S \in \mathcal{S}$ contains no more than two polynomials with discriminant -3; all edges connecting two such polynomials are of weight 2, hence no three such vertices form a suitable clique.

Suppose there exists a unique $g \in S$ with $\Delta(g) = -3$, and that $g+2 \in S$. Then for all $f \in S - \{g, g+2\}$ we have $|R(f,g)| = |R(f,g+2)| = 1$ because $|R(g,g+2)| = 4 = 2^{\deg(g)}$, so by the Chinese remainder theorem we have $S^\times \cong \{g, g+2\}^\times \times (S - \{g, g+2\})^\times$, from which it is immediate that $\mathrm{r}_3(S^\times) = \mathrm{r}_3(\{g, g+2\}^\times)$. From the canonical embedding

$$\{g, g+2\}^\times \;\longrightarrow\; \{g\}^\times \times \{g+2\}^\times : \; f \;\longmapsto\; (f \bmod (g), f \bmod (g+2)),$$

we see that $\mathrm{r}_3(\{g, g+2\}^\times) = 1$ if and only if there exists an $f \in \{g, g+2\}^\times$ that satisfies the congruences $f \equiv X \bmod (g)$ and $f \equiv 1 \bmod (g+2)$. But it is clear that this impossible, so $\mathrm{r}_3(S^\times) = \mathrm{r}_3(\{g, g+2\}^\times) = 0$.

Suppose there exists a unique $g \in S$ with $\Delta(g) = -3$, and that $g+2 \notin S$. In Figure 3.4 we see that this excludes all edges of weight 2 connecting to g, and in Figure 3.3 we see that there are no vertices of weight 1 connecting to g. Then $|R(g, f_S/g)| = 1$, so the Chinese remainder theorem yields $S^\times \cong \{g\}^\times \times (S - \{g\})^\times$, hence $\mathrm{r}_3(S^\times) = \mathrm{r}_3(\{g\}^\times) = 1$.

Suppose there are distinct $g_1, g_2 \in S$ with $\Delta(g_1) = \Delta(g_2) = -3$. Then from Figure 3.4 it is clear that g_1 and g_2 are adjacent, so we may assume without loss of generality that $g_1 = X^2 + X + 1$ and $g_2 = X^2 - X + 1$. We see that $|R(g_1, g_2)| = 4$, so for any $f \in S - \{g_1, g_2\}$ we have $|R(f, g_1)| = |R(f, g_2)| = 1$, and therefore $g_1 + 2, g_2 + 2 \notin S$. Then the Chinese remainder theorem yields $S^\times \cong \{g_1, g_2\}^\times \times (S - \{g_1, g_2\})^\times$, from which it is immediate that $\mathrm{r}_3(S^\times) = \mathrm{r}_3(\{g_1, g_2\})^\times$. From the canonical embedding

$$\{g_1, g_2\}^\times \;\longrightarrow\; \{g_1\}^\times \times \{g_2\}^\times : \; f \;\longmapsto\; (f \bmod (g_1), f \bmod (g_2)),$$

we see that $\mathrm{r}_3(S^\times) = 2$ if and only if there exist $f_1, f_2 \in \mathbb{Z}[X]$ satisfying the congruences

$$f_1 \equiv X \bmod (g_1), \qquad f_1 \equiv 1 \bmod (g_2), \qquad f_2 \equiv 1 \bmod (g_1), \qquad f_2 \equiv X \bmod (g_2).$$

Of course such f_1 and f_2 exist if and only if $X - 1 \in (g_1, g_2)$, and in the proof of Lemma 3.2.8 we saw that this is equivalent to $|R(g_1, g_2)| \mid 3$. But it is easily verified that $|R(g_1, g_2)| = 4$, see also the proof of 3.2.9, a contradiction. It follows that $\mathrm{r}_3(S^\times) < 2$. Note that $g_1 g_2 = X^4 + X^2 + 1 = g_1(X^2)$, from which it is immediate that X^2 has order 3 in $\{g_1, g_2\}^\times$, which shows that $\mathrm{r}_3(S^\times) = 1$. □

Lemma 3.4.3. *For $S \in \mathcal{S}$ we have*

$$\mathrm{r}_4(S^\times) = \begin{cases} 0 & \text{if } (\forall g \in S)(\Delta(g) = -4 \;\Rightarrow\; g+2 \in S), \\ 1 & \text{otherwise.} \end{cases}$$

Proof. For any $S \in \mathcal{S}$ the 4-rank is no greater than the number of $g \in S$ with $\Delta(g) = -4$, so if there are no such $g \in S$ then $\mathrm{r}_4(S^\times) = 0$. If there exists $g \in S$ with $\Delta(g) = -4$, then Figure 3.5 shows that no two distinct $g_1, g_2 \in \mathcal{D}$ with $\Delta(g_1) = \Delta(g_2) = -4$ are connected by an edge, so g is unique and without loss of generality we assume $g = X^2 + 1$. Then $\mathrm{r}_4(S^\times) \leq 1$, and $\mathrm{r}_4(S^\times) = 1$ if and only if there exists $f \in S^\times$ satisfying

$$f \equiv \pm X \bmod(g) \qquad \text{and} \qquad f \equiv \pm 1 \bmod(h) \;\text{ for all }\; h \in S - \{g\}.$$

Because $S \in \mathcal{S}$ we have $\mathrm{r}_2(S^\times) = \#S$ by Theorem 3.2.10, so for any $h \in S$ there exists $f_h \in \mathbb{Z}[X]$ such that $f_h \equiv -1 \bmod(h)$ and $f_h \equiv 1 \bmod(k)$ for all $k \in S - \{h\}$. So the congruences above are satisfied if and only if there exists $f \in S^\times$ satisfying

$$f \equiv X \bmod(g) \qquad \text{and} \qquad f \equiv 1 \bmod(f_S/g).$$

This is the case if and only if $X - 1 \in (g, f_S/g)$, and entirely analogous to the proof of Lemma 3.2.8 we see that $X - 1 \in (g, f_S/g)$ if and only if $|R(g, f_S/g)| \mid 2$. We conclude that $\mathrm{r}_4(S^\times) = 1$ if and only if for all $g \in S$ with $\Delta(g) = -4$ we have $|R(g, f_S/g)| \mid 2$.

Suppose $g + 2 \in S$. Then Figure 3.4 shows that $|R(g, g+2)| = 4$, and so $\mathrm{r}_4(S^\times) = 0$. Suppose $g + 2 \notin S$. Then Figure 3.4 shows there is no $h \in S$ such that $|R(g, h)| = 4$. Moreover, if there exists $h \in S$ with $|R(g, h)| = 2$ then this h is unique. To see this, suppose there are distinct $h_1, h_2 \in S$ such that $|R(g, h_1)| = |R(g, h_2)| = 2$. If $\deg(h_1) = 1$ then without loss of generality we may assume that $h_1 = X + 1$. From Figure 3.3 it is immediate that either $h_2 = X - 1$ or $h_2 = X^2 + X + 2$. In either case

$$|R(h_1, f_S/h_1)| \geq |R(h_1, g)R(h_1, h_2)| = 4 > 2^{\deg(h_1)},$$

a contradiction. By symmetry it follows that both $\deg(h_1) \neq 1$ and $\deg(h_2) \neq 2$. Then $\Delta(h_1) = \Delta(h_2) = -7$, but Figure 3.5 shows that $\{h_1, h_2\} \notin \mathcal{S}$, a contradiction. So if $\Delta(g) = -4$, then $|R(g, f_S/g)| \mid 2$ if and only if $g + 2 \notin S$. □

The group of units $S^\times$ of any finite subset $S \subset \mathcal{D}$ is determined up to isomorphism by its 2-, 3- and 4-ranks. Theorem 3.2.10 allows us to determine the 2-rank of the group of units corresponding to any given suitable clique, and Lemmas 3.4.2 and 3.4.3 allow us to determine the 3-rank and the 4-rank, respectively. Hence we are able to determine the isomorphism type of the group of units of any $S \in \mathcal{S}$, simply by looking at the corresponding clique in the graph. It is evident from inspecting the graph that there exists $n \in \mathbb{Z}_{>0}$ for which there exists no suitable n-clique, and it follows that $S^\times$ is isomorphic to a subgroup of $C_2^{n-2} \times C_3 \times C_4$ for any $S \in \mathcal{S}$.

We therefore determine the least n for which no suitable n-clique exists. Every vertex is a suitable 1-clique, every edge yields a suitable 2-clique, and suitable 3-cliques are plentiful. It is however not evident whether suitable 4-cliques or even 5-cliques exist, but with some patience one may discover suitable 4-cliques like those in Figure 3.6.

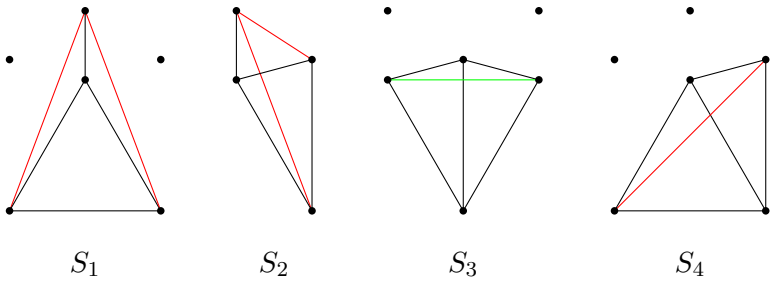


Figure 3.6: Four distinct 4-cliques, corresponding to sets $S_1, S_2, S_3, S_4 \in \mathcal{S}$

It is instructive to verify that these graphs are indeed in the graph of Figure 3.5, and that the corresponding sets $S_i \subset \mathcal{D}$ satisfy Lemma 3.4.1.ii and hence $S_i \in \mathcal{S}$. Then Lemmas 3.4.2 and 3.4.3 allow us to read off $\mathrm{r}_3(S_i^\times)$ and $\mathrm{r}_4(S_i^\times)$ directly from the graph, and Theorem 3.2.10 tells us that for each i we have $\mathrm{r}_2(S_i^\times) = \#S_i = 4$.

S_1: There is precisely one $f \in S_1$ with $\Delta(f) = -3$, and $f + 2 \notin S_1$ so $\mathrm{r}_3(S_1^\times) = 1$. There is no $g \in S_1$ with $\Delta(g) = -4$, so $\mathrm{r}_4(S_1^\times) = 0$.

S_2: There is precisely one $f \in S_2$ with $\Delta(f) = -3$, and $f + 2 \notin S_2$ so $\mathrm{r}_3(S_2^\times) = 1$. There exists $g \in S_2$ with $\Delta(g) = -4$, and $g + 2 \notin S_2$ so $\mathrm{r}_4(S_2^\times) = 1$.

S_3: There are distinct $f_1, f_2 \in S_3$ with $\Delta(f_1) = \Delta(f_2) = -3$, and $f_1 + 2, f_2 + 2 \notin S$ so $\mathrm{r}_3(S_3^\times) = 1$. There exists $g \in S_3$ with $\Delta(g) = -4$, and $g + 2 \notin S_3$ so $\mathrm{r}_4(S_3^\times) = 1$.

S_4: There is precisely one $f \in S_4$ with $\Delta(f) = -3$, and $f + 2 \notin S_4$, so $\mathrm{r}_3(S_4^\times) = 1$. There exists $g \in S_4$ with $\Delta(g) = -4$, and $g + 2 \notin S_4$ so $\mathrm{r}_4(S_4^\times) = 1$.

These results are summarised in the table below.

i	f_{S_i}	r_2	r_3	r_4	$\cong$
1	$X(X+1)(X^2+X+1)(X^2+X+2)$	4	1	0	$C_2^4 \times C_3$
2	$X(X^2+1)(X^2+X+1)(X^2+X+2)$	4	1	1	$C_2^3 \times C_3 \times C_4$
3	$X(X^2+1)(X^2+X+1)(X^2-X+1)$	4	1	1	$C_2^3 \times C_3 \times C_4$
4	$X(X+1)(X^2+1)(X^2+X+1)$	4	1	1	$C_2^3 \times C_3 \times C_4$

Table 3.1: The structure of $S_i^\times$ for $i \in \{1, 2, 3, 4\}$

Table 3.2 shows various isomorphism types of $S^\times$ for a selection of $S \in \mathcal{S}$. The verifications are left as an exercise for the reader. They require nothing more than the application of Lemmas 3.4.2 and 3.4.3 and Theorem 3.2.10 as before.

f_S	r_2	r_3	r_4	$S^\times$
1	0	0	0	C_1
X	1	0	0	C_2
$X(X+1)$	2	0	0	C_2^2
$X(X+1)(X-1)$	3	0	0	C_2^3
	4	0	0	C_2^4
	0	1	0	C_3
X^2+X+1	1	1	0	$C_2 \times C_3$
$X(X^2+X+1)$	2	1	0	$C_2^2 \times C_3$
$X(X+1)(X^2+X+1)$	3	1	0	$C_2^3 \times C_3$
$X(X+1)(X^2+X+1)(X^2+X+2)$	4	1	0	$C_2^4 \times C_3$
X^2+1	1	0	1	C_4
$X(X^2+1)$	2	0	1	$C_2 \times C_4$
$X(X+1)(X^2+1)$	3	0	1	$C_2^2 \times C_4$
	4	0	1	$C_2^3 \times C_4$
	1	1	1	$C_3 \times C_4$
$(X^2+1)(X^2+X+1)$	2	1	1	$C_2 \times C_3 \times C_4$
$X(X^2+1)(X^2+X+1)$	3	1	1	$C_2^2 \times C_3 \times C_4$
$X(X+1)(X^2+1)(X^2+X+1)$	4	1	1	$C_2^3 \times C_3 \times C_4$

Table 3.2: An overview of the isomorphism type of $S^\times$ for a selection of $S \in \mathcal{S}$.

One might ask whether there exist $S \in \mathcal{S}$ to fill up the four suggestive gaps in this table, and whether there are $S \in \mathcal{S}$ such that $\#S > 4$, i.e. if there exist any 5-cliques in the graph. The next lemma helps to answer the first question partially, and the second question entirely.

Lemma 3.4.4. *Every $S \in \mathcal{S}$ with $\#S = 4$ is in the orbit of one of the S_i.*

Proof. Let $S \in \mathcal{S}$ with $\#S = 4$, and suppose towards a contradiction that S is not in the orbit of any of the S_i under the action of $\operatorname{Aut}\mathbb{Z}[X]$. First note that there is no $g \in S$ with $\Delta(g) < -8$, as it is clear from Figure 3.5 that none of these vertices are part of a 4-clique.

Next suppose that there exists $g \in S$ such that $\Delta(g) = -3$. Without loss of generality we may assume that $g = X^2 + X + 1$. Figure 3.5 shows eight vertices connected to g, of which we just excluded the vertex $X^2 + X + 3$. If $X^2 - X + 1 \in S$ then X and $X^2 + 1$ are the only vertices connected to both $X^2 + X + 1$ and $X^2 - X + 1$, and we see that S is then in the orbit of S_3, a contradiction. By symmetry we have excluded the remaining edges of weight 2, so only the five edges of weight 0 remain.

Suppose $X^2 + X + 2 \in S$. We distinguish three cases:

i Both $X \in S$ and $X + 1 \in S$. Then S is in the orbit of S_1, a contradiction.

ii Both $X \in S$ and $X^2 + 1 \in S$. Then S is in the orbit of S_2, a contradiction.

iii Both $X \in S$ and $X^2 + 2X + 2 \in S$. Then $|R(X, f_S/X)| > 2^{\deg(X)}$, a contradiction.

This covers all cases with $X^2 + X + 2 \in S$ up to symmetry because $2 \notin (X^2 + 1, X^2 + 2X + 2)$. Then there remain two symmetric cases with $X^2 + X + 2 \notin S$, and we see that S is in the orbit of S_4, a contradiction. We conclude that there is no $g \in S$ with $\Delta(g) = -3$.

Now suppose that there exists $g \in S$ with $\deg(g) = 1$. Without loss of generality we may assume that $g = X$. There is at most one edge of weight 1 connecting to g, hence there are at least two edges of weight 0 connecting to g. We distinguish two cases:

i Both $X - 1 \in S$ and $X + 1 \in S$. The only vertex connecting to $X - 1$, X and $X + 1$ is $X^2 + 1$, but then $|R(X - 1, f_S/(X - 1))| = 4 > 2^{\deg(X-1)}$, a contradiction.

ii Both $X - 1 \in S$ and $X^2 + 1 \in S$. The only remaining vertex connecting to $X - 1$, X and $X^2 + 1$ is $X^2 + X + 2$, but then $|R(X - 1, f_S/(X - 1))| = 4 > 2^{\deg(X-1)}$, a contradiction.

We conclude that there is no $g \in S$ with $\deg(g) = 1$, and so for all $g \in S$ we have $-4 \leq \Delta(g) \leq -8$. Then $g \not\equiv X^2 + X + 1 \bmod(2)$ holds for all $g \in S$, and because there are only four polynomials of degree 2 in $\mathbb{F}_2[X]$ and $\#S = 4$, there are at least two distinct $g_1, g_2 \in S$ such that $g_1 \equiv g_2 \bmod(2)$. Then $|R(g_1, g_2)| = 4$, a contradiction. We conclude that every suitable 4-clique is in the orbit of one of the S_i. □

Corollary 3.4.5. *There exists no $S \in \mathcal{S}$ such that $S^\times \cong C_2^4$ or $S^\times \cong C_2^3 \times C_4$.*

Proof. Suppose towards a contradiction that there exists $S \in \mathcal{S}$ such that either $S^\times \cong C_2^4$ or $S^\times \cong C_2^3 \times C_4$. Then $\mathrm{r}_2(S^\times) = 4$ and so $\#S = 4$. It follows from the previous lemma that S is in the orbit of one of the S_i, hence we find from Table 3.4 that either $S^\times \cong C_2^4 \times C_3$ or $S^\times \cong C_2^3 \times C_3 \times C_4$, a contradiction. □

Corollary 3.4.6. *For $S \in \mathcal{S}$ we have $\#S < 5$.*

Proof. Suppose towards a contradiction that there exists $S \in \mathcal{S}$ such that $\#S \geq 5$. Then in particular there exists $S \in \mathcal{S}$ with $\#S = 5$, and for every $g \in S$ there exists i such that $S - \{g\}$ is in the orbit of S_i by the previous lemma. Note that for every i there exists $g \in S_i$ with $\Delta(g) = -3$, so there must be some $g \in S$ with $\Delta(g) = -3$. Moreover, there must be some $h \in S - \{g\}$ with $\Delta(h) = -3$. It is clear from the graph that g and h must be adjacent, and from Figure 3.2 we find that there are only two vertices connecting to both g and h. Hence there is no 5-clique S such that $g, h \in S$, a contradiction. □

Then the question remains; do there exist $S \in \mathcal{S}$ such that $S^\times \cong C_3$ or $S^\times \cong C_3 \times C_4$?

Proposition 3.4.7. *There is no monic $f \in \mathbb{Z}[X]$ such that $(\mathbb{Z}[X]/(f))^\times \cong C_3$.*

Proof. Suppose that there exists $f \in \mathbb{Z}[X]$ with $(\mathbb{Z}[X]/(f))^\times \cong C_3$. Then $\mathbb{Z}[X]/(f)$ is not the trivial ring so $-1 \neq 1$, and $(-1)^2 = 1$. But C_3 contains no element of order 2, a contradiction. □

Proposition 3.4.8. *There is no monic $f \in \mathbb{Z}[X]$ such that $(\mathbb{Z}[X]/(f))^\times \cong C_3 \times C_4$.*

Proof. Suppose that there exists a monic $f \in \mathbb{Z}[X]$ such that $(\mathbb{Z}[X]/(f))^\times \cong C_3 \times C_4$. By Proposition 3.1.3 there exists a finite $S \subset \mathcal{D}$ such that $f = f_S$, and from the embedding $S^\times \hookrightarrow \prod_{g \in S} \{g\}^\times$ it is clear that there exists $g \in S$ with $\Delta(g) = -3$, by Lemma 3.1.4. Because $S^\times$ is cyclic there exists $h \in S^\times$ that generates $S^\times$, hence h satisfies $h^6 = -1$. But $h^6 \equiv 1 \bmod(g)$ as $\{g\}^\times \cong C_6$ so $h \neq -1$, a contradiction. □

Summing up these results, for a monic $f \in \mathbb{Z}[X]$ we know that if $(\mathbb{Z}[X]/(f))^\times$ is finite, then it is isomorphic to a subgroup of $C_2^3 \times C_3 \times C_4$, but not isomorphic to C_3 or $C_3 \times C_4$. Moreover, if $f = f_S$ for some $S \in \mathcal{S}$, then $(\mathbb{Z}[X]/(f))^\times$ is not isomorphic to either C_2^4 or $C_2^3 \times C_4$. One might ask whether there exists a finite subset $S \subset \mathcal{D}$ such that $S^\times \cong C_2^4$ or $S^\times \cong C_2^3 \times C_4$. This is the subject of the final section.

3.5 The subgroups C_2^4 and $C_2^3 \times C_4$

The purpose of this section is to show the existence of monogenic orders A and B such that $A^\times \cong C_2^3 \times C_4$ and $B^\times \cong C_2^4$. By Proposition 3.1.3 there are finite $S, T \subset \mathcal{D}$ such that $A \cong \mathbb{Z}[X]/(f_S)$ and $B \cong \mathbb{Z}[X]/(f_T)$, but Corollary 3.4.5 yields $S, T \notin \mathcal{S}$. The methods developed in the previous sections therefore do not apply to such monogenic orders, so a new approach to determining the isomorphism type of $S^\times$ for finite subsets $S \subset \mathcal{D}$ is required.

Definition 3.5.1. For sets X, Y and Z with maps $f : X \longrightarrow Z$ and $g : Y \longrightarrow Z$, the *fibered product of X and Y over Z (with respect to f and g)* is the set

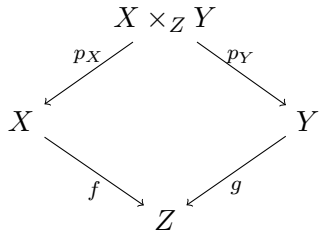
$$X \times_Z Y := \{(x, y) \in X \times Y \,\big|\, f(x) = g(y)\}.$$

The maps f and g are usually understood, and so they do not appear in the notation. A few properties of the fibered product are immediate from the definition.

Proposition 3.5.2. *Let X, Y and Z be sets with maps $f : X \longrightarrow Z$ and $g : \longrightarrow Z$. If $\#Z = 1$ then $X \times_Z Y = X \times Y$.*

Proof. As Z is a singleton set, we have $f(x) = g(y)$ for all $(x, y) \in X \times Y$. □

Proposition 3.5.3. *Let X, Y and Z be sets with maps $f : X \longrightarrow Z$ and $g : Y \longrightarrow Z$, and let p_X and p_Y be the projections from $X \times_Z Y$ onto X and Y respectively. Then the following diagram commutes.*



Proof. It is immediate from the definition of the fibered product that $f \circ p_X = g \circ p_Y$. □

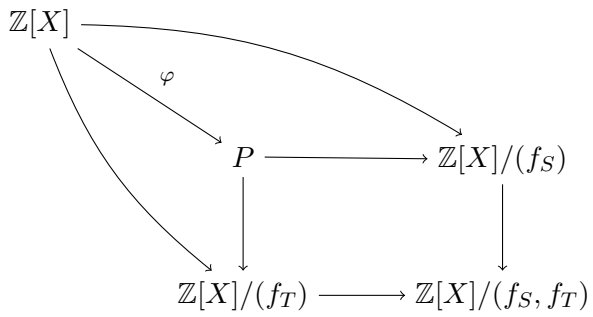
Proposition 3.5.4. *For groups (rings) A, B and C with group (ring) homomorphisms $f : A \longrightarrow C$ and $g : B \longrightarrow C$, the fibered product $A \times_C B$ is again a group (ring).*

Proof. The product $A \times B$ is a group (ring) with pointwise group (ring) operations. Given that f and g are group (ring) homomorphisms it is easily verified that $A \times_C B$ is a subgroup (subring) of $A \times B$. □

Theorem 3.5.5. *For finite subsets $S, T \subset \mathcal{D}$, letting $Z = \mathbb{Z}[X]/(f_S, f_T)$ we have*

$$(S \cup T)^\times \cong S^\times \times_{Z^\times} T^\times.$$

Proof. Consider the following diagram



In this diagram P is the fibered product of $\mathbb{Z}[X]/(f_S)$ and $\mathbb{Z}[X]/(f_T)$ over $\mathbb{Z}[X]/(f_S, f_T)$, so the square diagram commutes by Proposition 3.5.3. The map φ is given by the canonical map $\mathbb{Z}[X] \longrightarrow \mathbb{Z}[X]/(f_S) \times \mathbb{Z}[X]/(f_T)$, which maps into the fibered product because the outer square also commutes. It is clear that $\ker \varphi = (f_S) \cap (f_T) = (f_{S \cup T})$, yielding an isomorphism $\mathbb{Z}[X]/(f_{S\cup T}) \cong P$. The units of P are the pairs $(u, v) \in S^\times \times T^\times$ for which u and v have the same image in $(\mathbb{Z}[X]/(f_S, f_T))^\times$. We see that

$$\begin{aligned}(S \cup T)^\times &= P^\times = \big(\mathbb{Z}[X]/(f_S) \times_{\mathbb{Z}[X]/(f_S,f_T)} \mathbb{Z}[X]/(f_T)\big)^\times \\ &= (\mathbb{Z}[X]/(f_S))^\times \times_{(\mathbb{Z}[X]/(f_S,f_T))^\times} (\mathbb{Z}[X]/(f_T))^\times = S^\times \times_{Z^\times} T^\times.\end{aligned}$$

□

Corollary 3.5.6. *For finite subsets $S, T \subset \mathcal{D}$, if $|R(f_S, f_T)| \mid 2$ then $(S \cup T)^\times = S^\times \times T^\times$.*

Proof. If $|R(f_S, f_T)| = 2$ then $\mathbb{Z}[X]/(f_S, f_T) = \{0, 1\}$ and so $(\mathbb{Z}[X]/(f_S, f_T))^\times$ is trivial. From Proposition 3.5.2 and Theorem 3.5.5 it follows that $(S \cup T)^\times = S^\times \times T^\times$. □

Lemma 3.5.7. *For $S = \{X, X^2 + 1, X^2 - X + 1, X^2 + X + 1, X^2 + X + 2\}$ we have $S^\times \cong C_2^3 \times C_4$.*

Note that $S \subset \mathcal{D}$, but $S \notin \mathcal{S}$ because $\{X^2 - X + 1, X^2 + X + 2\} \notin \mathcal{S}$. The graphs corresponding to S, $S - \{X\}$ and $S' := S - \{X, X^2 + 1\}$ are shown in Figure 3.7.

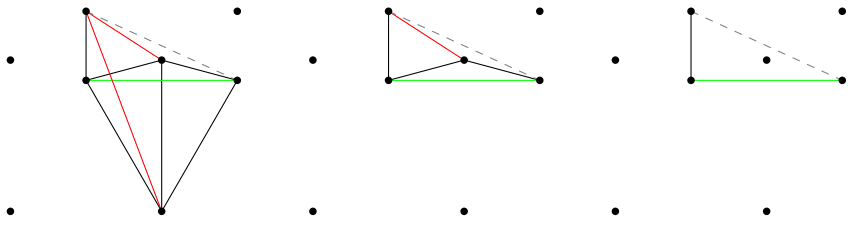


Figure 3.7: From left to right are the graphs corresponding to S, $S - \{X\}$ and S', respectively. Note that the gray dashed edge is not in the graph of Figure 3.5.

Proof. Counting the the weights of the edges connecting to X yields $|R(X, f_S/X)| = 2$, hence it follows from Corollary 3.5.6 that $S^\times \cong \{X\}^\times \times (S - \{X\})^\times \cong C_2 \times (S - \{X\})^\times$. Similarly for X^2+1 we find that $|R(X^2+1, f_{S-\{X\}}/(X^2+1))| = 2$, and Corollary 3.5.6 tells us that $(S-\{X\})^\times \cong \{X^2+1\}^\times \times S'^\times \cong C_4 \times S'^\times$, and we have $S^\times \cong C_2 \times C_4 \times S'^\times$.

Let $g = X^2 + X + 2$. Theorem 3.5.5 yields an isomorphism $S'^\times \cong \{g\}^\times \times_{Z^\times} (S' - \{g\})^\times$, where $Z = \mathbb{Z}[X]/(g, f_{S'}/g)$. From Lemma 3.2.5 and Proposition 3.2.4 we find that

$$\#Z = |R(g, f_{S'}/g)| = |R(g, X^2 - X + 1)| = 7,$$

hence $Z \cong \mathbb{F}_7$. The only common root of $X^2 + X + 2$ and $X^2 - X + 1$ in $\mathbb{F}_7$ is 3, hence the isomorphism $\psi : Z \longrightarrow \mathbb{F}_7$ given by $\psi(X) = 3$ is the only isomorphism.

Let φ_1 and φ_2 be the maps from $\{g\}^\times$ and $(S' - \{g\})^\times$ to $Z^\times$ as in the fibered product. By Lemma 3.1.4 we have $\{g\}^\times \cong C_2$ so $\{g\}^\times = \{\pm 1\}$, and it follows that $\mathrm{im}(\pi_1) = \{\pm 1\}$ and $-1 \neq 1$ because $2 \notin (g, f_{S'}/g)$. Then it remains to determine $\varphi_2^{-1}(1)$ and $\varphi_2^{-1}(-1)$.

Note that $S' - \{g\} \in \mathcal{S}$, so by our earlier methods we find that $(S' - \{g\})^\times \cong C_2^2 \times C_3$. It is easily verified that X has order 6 in $(S' - \{g\})^\times = (\mathbb{Z}[X]/(X^4 + X^2 + 1))^\times$ and $X^3 \not\equiv -1 \bmod (X^4 + X^2 + 1)$, so $(S' - \{g\})^\times$ is generated by $\{-1, X\}$. Then for any $u \in (S - \{g\})^\times$ there exists $m \in \{0, 1\}$ and $n \in \{0, 1, 2, 3, 4, 5\}$ such that $u = (-1)^m X^n$, and so $(\psi \circ \pi_2)(u) = (-1)^m 3^n$. As 3 has order 6 in $\mathbb{F}_7^\times$, for any $u \in (S - \{g\})^\times$ we have

$$\pi_2(u) = 1 \quad \Leftrightarrow \quad u = 1 \vee u = -X^3 \qquad \text{and} \qquad \pi_2(u) = -1 \quad \Leftrightarrow \quad u = -1 \vee u = X^3.$$

It follows that $\{g\}^\times \times_{Z^\times} (S' - \{g\})^\times = \{(1, 1), (1, -X^3), (-1, -1), (-1, X^3)\}$, and in particular that $S'^\times \cong C_2^2$. We conclude that $S \cong C_2^3 \times C_4$. □

Lemma 3.5.8. *For $T = S \cup \{X + 1\}$ we have $T^\times \cong C_2^4$.*

Again $T \subset \mathcal{D}$ is finite but $T \notin \mathcal{S}$ because $S \notin \mathcal{S}$. The graphs corresponding to T, $T - \{X\}$ and $T' := T - \{X, X + 1\} = S - \{X\}$ are shown in Figure 3.8.

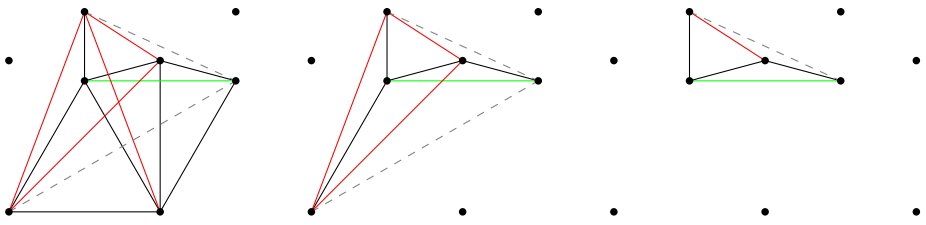


Figure 3.8: From left to right are the graphs corresponding to T, $T - \{X\}$ and T', respectively. Note that the gray dashed edges are not in the graph of Figure 3.5.

Proof. Figure 3.8 shows that $|R(X, f_T/X)| = 2$, so we have $T^\times \cong \{X\}^\times \times (T - \{X\})^\times$ by Corollary 3.5.6, where of course $\{X\}^\times \cong C_2$. For $T - \{X\}$ Theorem 3.5.5 yields

$$(T - \{X\})^\times \cong \{X + 1\}^\times \times_{Y^\times} (T - \{X, X + 1\})^\times,$$

where $T - \{X, X+1\} = S - \{X\}$ and $Y = \mathbb{Z}[X]/(X+1, f_S/X)$. Then Y is cyclic of order $|R(X+1, f_S/X)| = 4 \cdot |R(X+1, X^2 - X + 1)| = 12$. The map $\pi : (S - \{X\})^\times \longrightarrow Y^\times$ as in the fibered product therefore sends any $g \in (S - \{X\})^\times$ to $g(-1) \bmod 12$. We claim that the polynomials g_1, g_2 and g_3 given by

$$\begin{aligned} g_1 &= 1 - (X^4 + X^2 + 1)(X^2 + X + 2), \\ g_2 &= 1 - X(X^2 - X + 1)(X^2 + 1)(X^2 + X + 2), \\ g_3 &= 1 + X(X^2 + X + 1)(X^2 + 1), \end{aligned}$$

generate $(S - \{X\})^\times$. To see this, recall from the proof of the previous lemma that

$$(S - \{X\})^\times \cong \{X^2 + 1\}^\times \times (\{X^2 + X + 1, X^2 - X + 1\}^\times \times_{Z^\times} \{X^2 + X + 2\}^\times),$$

with Z as in Lemma 3.5.7. Denote the right-hand side by R and let $\varphi : (S - \{X\})^\times \longrightarrow R$ be the isomorphism induced by the canonical projections of the corresponding rings. We determine $\varphi(g_i)$ for $i = 1, 2, 3$.

For g_1 only the image in $\{X^2 + 1\}^\times$ is nontrivial. As $X^4 + X^2 + 1 \equiv 1 \bmod (X^2 + 1)$ and $X^2 + X + 2 \equiv X + 1 \bmod (X^2 + 1)$, we see that $g_1 \equiv -X \bmod (X^2 + 1)$, so g_1 has order 4. Similarly for g_2 only the image in $\{X^2 + X + 1, X^2 - X + 1\}^\times$ is nontrivial. We have

$$\begin{aligned} (X^2 + X + 2)(X^2 - X + 1) &\equiv X^2 - X + 1 \bmod (X^4 + X^2 + 1), \\ (X^2 + 1)(X^2 - X + 1) &\equiv (-X)(X^2 - X + 1) \bmod (X^4 + X^2 + 1), \end{aligned}$$

hence $g_2 \equiv 1 + X^2(X^2 - X + 1) \equiv -X^3 \bmod (X^4 + X^2 + 1)$.
For g_3 we clearly have $g_3 \equiv 1 \bmod (X^2 + 1)$, and from the congruences

$$\begin{aligned} (X^2 + X + 1)(X^2 + 1) &\equiv (X^2 + X + 1)X \bmod (X^4 + X^2 + 1), \\ X^2 + X + 1 &\equiv -1 \bmod (X^2 + X + 2), \\ X^2 + 1 &\equiv -(X + 1) \bmod (X^2 + X + 2), \end{aligned}$$

it follows immediately that $g_3 \equiv 1 + X^2(X^2 + X + 1) \equiv X^3 \bmod (X^4 + X^2 + 1)$ and $g_3 \equiv 1 + X(X + 1) \equiv -1 \bmod (X^2 + X + 2)$, so the images of the g_i are

$$\varphi(g_1) = (-X, 1, 1), \qquad \varphi(g_2) = (1, -X^3, 1), \qquad \varphi(g_3) = (1, X^3, -1).$$

We see that $\{\varphi(g_1), \varphi(g_2), \varphi(g_3)\}$ generate R, hence $(S - \{X\})^\times$ is generated by $\{g_1, g_2, g_3\}$.

The images of the g_i in Y are

$$g_1(-1) = -5, \qquad g_2(-1) = 13 \equiv 1 \bmod 12, \qquad g_3(-1) = -1,$$

and note that $g_1(-1)^2 \equiv 1 \bmod 12$. Because $\{X + 1\}^\times$ maps to $\{\pm 1\} \subset Y$ we have $\mathrm{r}_4(T - \{X\})^\times = 0$, and we count $\#(T - \{X\})^\times = 8$. It follows that $(T - \{X\})^\times \cong C_2^3$, and we conclude that $T^\times \cong C_2^4$. □

This shows that for any finite group A that is isomorphic to a subgroup of $C_2^3 \times C_3 \times C_4$, but not isomorphic to either C_3 or $C_3 \times C_4$, there exists an $f \in \mathbb{Z}[X]$ such that $(\mathbb{Z}[X]/(f))^\times \cong A$. Conversely we have already shown that for any monogenic order A the group of units, if it is finite, is isomorphic to a subgroup of $C_2^3 \times C_3 \times C_4$, but not isomorphic to either C_3 or $C_3 \times C_4$, thus proving Theorem 1.0.5.

To conclude we would like to propose the problem of finding a method for determining $S^\times$ for any finite $S \subset \mathcal{D}$ less cumbersome than the methods presented in the final section, perhaps as simple as the methods we developed for the $S \in \mathcal{S}$. More modestly we would like to propose the problem of finding $S \subset \mathcal{D}$ with $\#S = 5$ such that $S^\times \cong C_2^4$.

Acknowledgements

I would like to thank my thesis advisor Hendrik Lenstra. His ideas form the foundations of this thesis, and his enthusiasm and guidance were invaluable in developing the presented theory. Without his help I could not have written this thesis.

Furthermore I would like to thank Johan Commelin, Jasmin Blackshaw, Nick Towner and Alexander Tonkelaar for the conversations that clarified my thinking on the subject and other matters, and the many helpful suggestions they made. I also owe credit to the user 'Matt E' of math.stackexchange.com for the elegance of the proof of Lemma 2.2.4.

Finally I would like to thank all other people not mentioned here, who have in some way contributed to this thesis.

Tristan Tilly

Bibliography

[1] M.F. Atiyah and I.G. MacDonald, *Introduction to Commutative Algebra*. Reading, MA: Addison-Wesley, 1969.

[2] S. Lang, *Algebra*. Reading, MA: Addison-Wesley, 1993.

[3] P. Ribenboim, *Classical Theory of Algebraic Numbers*. New York: Springer-Verlag, 2001.

[4] P. Stevenhagen, *Number Rings*. Leiden, 2008.
Available at http://websites.math.leidenuniv.nl/algebra/.

[5] J.S. Milne, *Algebraic Number Theory*. Ann Arbor, 2012.
Available at http://www.jmilne.org/math/CourseNotes/ant.html.

[6] G. Myerson, "Norms in Polynomial Rings", *Bulletin of the Australian Mathematical Society* 41, June 1990: 381-386.