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

Explicit Realization of Dihedral Galois Groups over $\mathbb{Q}$

Bachelor's Project Mathematics
July 2022
Student: M. Devetak
First supervisor: Dr J. Top
Second assessor: Dr P. Kilicer

Contents

1 Introduction

This thesis aims to find explicit polynomials such that their Galois group over $\mathbb{Q}$ is dihedral. The question we ask is remarkably simple. Nevertheless, to answer it, we will draw from the rich theory of elliptic curves and class fields.

The structure of the thesis is as follows. The first section provides a recap of Galois's theory, which is necessary for us in order to pose the research question exactly. In the next section, we present some ways one can think about dihedral groups, which will later inform the choice of methods to realise dihedral groups we will use. After that, we present two results from Galois theory, which will be relevant to realising dihedral groups. The next three sections offer some background regarding the theory we will employ to realise dihedral Galois groups. In doing so, we will mention and use a lot of theorems and important results, usually reserved for the final chapters of textbooks. For this reason, we will often use results without proving them.

After that, we present three methods to realise dihedral Galois groups. The first one by Mestre uses function fields of elliptic curves equipped cwith a rational n-torsion point. The second one we present uses the n-torsion subgroup of an elliptic curve with complex multiplication. We will show that this method does not realise dihedral groups. The third and last uses the Hilbert class field of an imaginary quadratic extension with a cyclic ideal class group. We will see what each of these statements means in the dedicated sections.

In the appendix we present the code used for the computations as well as multiple polynomials that realize dihedral Galois groups. The largest dihedral group we realized is D_{31}.

2 Galois Theory

This section aims to give a brief overview of Galois Theory. A much deeper discussion of the subject matter is provided in the lecture notes of "Advanced Algebraic Structures" [21] from which most of the material discussed is drawn as well as from the preceding course "Algebraic Structures" [22]. The last part provides some background about the inverse Galois problem, which is the starting point of this thesis. Readers who are already familiar with Galois theory can safely skip this section.

2.1 Splitting Field

In this part, we will look at a type of field extension called splitting field. The underlying idea is relatively simple. Given a field K and a polynomial f with coefficients in K, so $f \in K[X]$, we want to find a field that contains all the zeros of f.

In general, it is not the case that for $f \in K[X]$, we have that all the zeros of f are contained in K. For example, think where the coefficients of $f(X) = X^2 + 1$ are from and where the zeros lie. Therefore, if we want to find such field L, we will have to look for something larger than K itself. So that $K \subset L$. We say that L is a field extension of K.

This allows for too much freedom. Given $f \in K[X]$, there are countless field extensions L such that all zeros of f are contained in L. For example, consider $f(X) = X^2 + 1 \in \mathbb{Q}[X]$ as before then f splits in $\mathbb{Q}(i)$, recall that simply $\mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}$, but also in $\mathbb{C}$. Therefore, our starting point needs to be narrowed a bit. We consider not just any field extension, but minimal ones which we call splitting fields. From [21] we therefore get the following definition:

Definition 1. *A* ***splitting field*** *of $f \in K[X]$ is a field extension L of K such that:*

1. *f splits into a product of linear factors in $L[X]$*
2. *Let $a_1, a_2, a_3, \ldots, a_s$ denote the zeros of f in L, then $L = K(a_1, a_2, a_3, \ldots, a_s)$.*

Remark 1. *Notice that from the first condition of Definition 1 we get that all the zeros of f are contained in L(and also the name splitting), and the second condition implies that L is the smallest of all possible such fields, namely we have added only what was strictly necessary to the field K. In this respect, recall that for $k \in K$, we have that $K(k) = K$.*

So far, we have only defined such a splitting field but have said nothing about its existence and uniqueness. It turns out that both properties hold, namely, the splitting field of a polynomial always exists, and it is unique up to isomorphism. We now take a closer look at this second condition.

2.2 The Galois Group

In the last part, we have left with saying that given polynomial $f \in K[X]$ the splitting field is unique up to isomorphism. Furthermore, we have also given a positive characterization of the splitting field. Namely if $a_1, a_2, \ldots, a_s$ are the zeros of f then the splitting field L is simply $K(a_1, a_2, \ldots, a_s)$.

Imagine now we are given two splitting fields of a single polynomial. Let our polynomial yet again be $f(X) = X^2 + 1$ in $\mathbb{Q}[X]$. Since it is of degree two it has two zeros, a_1, a_2 such that $f(X) = (X - a_1)(X - a_2)$. One such choice of zeros can be $a_1 = i$ and $a_2 = -i$. We let the first splitting field be $L_1 = \mathbb{Q}(i, -i)$. Of course, not necessarily we need to draw from $\mathbb{C}$ in order to get the zeros of $f(X)$, we could also define a j such that $j^2 = -1$ and then let our splitting field be $L_2 = \mathbb{Q}(j, -j)$. Clearly, the two fields are isomorphic by the map $i \mapsto j$. This is boring since the isomorphism does not uncover any deep mathematics but just allows us to showcase how many letters we know. However, there is another interesting thing to consider.

Let's restrict ourselves only to the case $a_1 = i$ and $a_2 = -i$ with the splitting field being $L = \mathbb{Q}(i, -i)$. There is no good reason, except for convention, on why we choose $a_1 = i$ rather than the opposite. Let now $b_1 = -i$ and $b_2 = i$, then those are also zeros of our polynomial $f(X)$. Then the isomorphism between field extension is given by $a_1 \mapsto b_2$ or rather $i \mapsto -i$. Notice that this is also an automorphism of L.

Notice that we have found two types of isomorphisms between the splitting field of a polynomial. One is a simple renaming, which we will not be concerned with. The other is a permutation of the zeros of the original polynomial. This second type of isomorphism is precisely the concern of Galois's theory.

Before proceeding with the formal definition of a Galois group, we need to put some restrictions on our polynomial $f \in K[X]$. These restrictions are not strictly necessary, and Galois Theory can be developed without them. See, for example, Chapter 5 in Hungerford's Algebra for a different treatment [7]. The benefit is that they make the theory more intuitive since, in this case, we can think of the Galois group as permutations of zeros rather than abstract K-automorphisms of L. We require that $f \in K[X]$ is separable. That is, all its zeros are distinct. From [21] we, therefore, get the following two important definitions:

Definition 2. *A field extension L is called a* ***Galois extension*** *of K if L is the splitting field of a separable polynomial $f \in K[X]$.*

Definition 3. *The* ***Galois group*** *of a Galois extension L of K denoted by $Gal(L/K)$ is the group of all field automorphisms of L that fix K.*

Remark 2. *The Galois Group is indeed a group with the identity element being the identity automorphism, and the operation is the composition of functions. Recall that the composition of isomorphisms is an isomorphism.*

Remark 3. *Any $\sigma \in Gal(L/K)$ permutes the zeros of f, and σ is determined by this permutation. If f were not separable and had a multiple zero, then elements in $L \setminus K$ may exist that are fixed by every σ. In general, it is the case that $Gal(L/K) \subseteq S_n$, but not necessarily equal, with n being the degree of f. More details are provided in remark 2.1.6 in [21].*

Remark 4. *It follows that the Galois group can be interpreted as the isomorphisms mentioned earlier that show the uniqueness of the splitting field of a polynomial. That is, it contains all the isomorphisms that are not mere renaming.*

2.3 The Inverse Galois Problem

From the previous part, it follows that a separable polynomial $f \in K[X]$ gives rise to Galois extension L, such that the K-automorphisms of L form a group. The inverse Galois problem asks whether any group can appear as a Galois group of a Galois extension. This only requires showing that such an extension is possible and not computing it. Therefore the explicit inverse Galois problem asks:

Problem 1. *Given a group G, find field K and separable polynomial $f \in K[X]$ such that the Galois group of the field extension generated by f is isomorphic to G.*

Notice that we can pick the field within which to work, but what if we fixed the base field K? Let's say $K = \mathbb{Q}$. Then the explicit inverse Galois problem over $\mathbb{Q}$ asks:

Problem 2. *Given a group G, find a separable polynomial $f \in \mathbb{Q}[X]$ such that the Galois group of the field extension generated by f is isomorphic to G.*

A group G for which we find appropriate f we call realizable over $\mathbb{Q}$. It is not known whether the solutions to this problem is positive, and there are many groups for which we do not know whether they are realizable over $\mathbb{Q}$, some of which are relatively small, like the sporadic group M_{23}[10].

In this bachelor thesis, we will be concerned with whether dihedral groups are realizable, which are the groups of symmetries of regular n-gons. That is, we ask:

Problem 3. *Given a dihedral group D, find a separable polynomial $f \in \mathbb{Q}[X]$ such that the Galois group of the field extension generated by f is isomorphic to D.*

It is known that this is the case that every dihedral group is realizable over $\mathbb{Q}$. Therefore, we "only" have to find the appropriate polynomial f, and we are done.

3 Thinking About Dihedral Groups

This short section presents what a dihedral group is and how we can think about them. This will be relevant as it will inform the methods we will use to try to realize dihedral groups as Galois groups of extensions over $\mathbb{Q}$. The general and abstract definition of a dihedral group is:

Definition 4. *A (nth-)**dihedral group** of order $2n$ denoted by D_n is the group generated by ρ of order n and σ of order 2 such that $\sigma\rho\sigma = \rho^{-1}$, which we call the dihedral property.*

This section aims to provide different ways of thinking about dihedral groups.

3.1 Geometric View of Dihedral Groups

It is customary to introduce dihedral groups as the groups of symmetries of a regular n-gon. This is done, for example, in Top's lecture notes for "Group Theory"[20]. This is a natural setting in which dihedral groups arise. Given a regular n-gon, what symmetries do there exist (i.e., isometries of the plane that preserve the n-gon)? It turns out that the group of symmetries needs to be generated by two elements. In particular, there is a rotation in which each vertex gets transposed to the one on its left. Such an operation is of order n since after n rotations, each vertex will be back at its starting point. We also have reflections through an axis, which is of order 2. It turns out, see Theorem 5.3.4 from [20], that these two operations generate all the possible symmetries and satisfy the dihedral property.

3.2 Exact Sequence and Semi-direct Product View of Dihedral Groups

We now provide a way of thinking about dihedral groups, which, although less intuitive than the geometric representation of dihedral groups, will offer the background by which we will motivate the three methods we will use in this thesis. We start by defining exact sequences.

Definition 5. *Given groups $A_1, A_2, A_3, \dots$ and homomorphisms $a_{12}, a_{23}, \dots$ such that a_{ij} is a homomorphism from A_i to A_j an exact sequence is such that the image of a_{ij} is the same as the kernel of a_{jk}. Graphically we represent this relationship by:*

$$\cdots \longrightarrow A_i \longrightarrow A_j \longrightarrow \dots$$

For a given D_n we can construct the following exact sequence:

$$1 \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow D_n \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1.$$

In this case the map from $\mathbb{Z}/n\mathbb{Z}$ to D_n is $\overline{1} \mapsto \rho$. Furthermore the map from D_n to $\mathbb{Z}/2\mathbb{Z}$ is determined by $\sigma \mapsto 1$ and $\rho \mapsto 0$. It is easy to verify that the given sequence is exact. Note that every $\phi \in D_n$, we can think of it as σ appearing at most once, since otherwise, we could use the dihedral property to remove two σ's.

If D_n were to be abelian, we could say from the above that either $D_n = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ or $D_n = \mathbb{Z}/2n\mathbb{Z}$. This is not the case for $n > 2$. We now define a split exact sequence:

Definition 6. *Given an exact sequence:*

$$A \overset{b}{\twoheadrightarrow} B \longrightarrow 1.$$

We say that $a : B \to A$ splits the sequence if $b \circ a = id_B$.

We ask what possibilities there are to make the sequence $D_n \overset{b}{\twoheadrightarrow} \mathbb{Z}/2\mathbb{Z}$ split. In particular we are looking for a map $a : \mathbb{Z}/2\mathbb{Z} \to D_n$ such that $b \circ a = id_{\mathbb{Z}/2\mathbb{Z}}$. The problem we face is that the choice of a is not unique. We can summarize the above discussion in the definition of the semi-direct product as presented in Mac Lane's and Birkoff's "Algebra"[14].

Definition 7. *Given a non-abelian group D and a normal subgroup N of D such that we have the split exact sequence:*

$$1 \longrightarrow N \longrightarrow D \overset{a}{\curvearrowleft}\!\!\longrightarrow D/N \longrightarrow 1,$$

then we say that D is the ***semi-direct product*** *of D/N acting on N. We write it as $D = D/N \ltimes N = N \rtimes D/N$. In this case we let $\theta : D/N \to Aut(N)$ be the conjugation by elements of $a(D/N) \subset D$, which is well defined since N is normal. As a set then $D = N \times D/N$ with the operation being:*

$$(a, b)(c, d) = (a\theta(b)(c), bd).$$

Remark 5. *In the definition, we assumed that we know what the group D is, but what would happen if we were only given groups isomorphic to N and G and told that they give rise to an exact sequence with D? In that case, it is not always possible to see the structure of D since we are missing θ, as we have already seen above in the case of D_n.*

Remark 6. *Using the above definition we say that $D_n = \mathbb{Z}/2\mathbb{Z} \ltimes \mathbb{Z}/n\mathbb{Z}$ with $\mathbb{Z}/2\mathbb{Z} \simeq D_n/\langle\rho\rangle$ acting on $\mathbb{Z}/n\mathbb{Z} \simeq \langle\rho\rangle$ by $n-1$, or equivalently by -1 or by the inverse. That is $\theta : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ has $\theta(\overline{1}) = \rho^{-1}$*

We can now use semi-direct products to show a simple result about the Galois extension, which will be relevant later.

Lemma 1. *Let $K \subset L$ be a field extension, of characteristic greater than two, such that $Gal(L/K) = D_n$. Then we have an intermediate field $K \subset K(\sqrt{d}) \subset L$, such that:*

$$Gal(L/K) = Gal(K(\sqrt{d})/K) \ltimes Gal(L/K(\sqrt{d})).$$

Proof. Consider the normal subgroup $\langle \rho \rangle$ of D_n which is generated by the rotation. This is a subgroup of order n and hence the element of L which are invariant under this subgroup are a field extension $K(\sqrt{d})$ of K of order 2. Such that $Gal(L/K(\sqrt{d}))$ corresponds to rotations and $Gal(K(\sqrt{d})/K) = D_n/\langle \rho \rangle$ which proves the theorem.

■

4 Two Tools in Dihedral Galois Extension Hunting

In this section, we present two results that can be helpful when looking to solve the inverse Galois problem over $\mathbb{Q}$ for some group. The first is an extension of a theorem by Hilbert, and the second is a result by Williamson.

4.1 Hilbert's Irreducibility Theorem

We present a theorem, which is helpful when looking for Galois groups. Sometimes, it is easier to find an extension of $\mathbb{Q}(t)$ with a given Galois group than directly an extension of $\mathbb{Q}$. The theorem states that for almost any $q \in \mathbb{Q}$, setting $t = q$ will give us the same Galois extension.

Theorem 1. *Given a Galois extension of $\mathbb{Q}(t)$ to $\mathbb{Q}(t, \alpha)$ generated by an irreducible polynomial $f(t, x)$ then there exists infinitely many $q \in \mathbb{Q}$ such that $f(q, x) \in \mathbb{Q}[x]$ is irreducible and $Gal(\mathbb{Q}(\alpha_q), \mathbb{Q}) \simeq Gal(\mathbb{Q}(t, \alpha), \mathbb{Q}(t))$. Here α_q is α with all the occurrences of t replaced by q.*

Remark 7. *A proof of this theorem is slightly beyond the scope of this thesis, a good understandable reference Chariker's paper 'The inverse Galois problem, Hilbertian fields and Hilbert's irreducibility theorem' [4].*

4.2 A Theorem By Williamson

This part elaborates and generalizes Williamson's proof of proposition four from [24]. In particular, we extend their method to cover even field extension. Furthermore, we provide conditions such that the resulting extension is dihedral.

Let L_1 and L_2 be Galois Extensions of a quadratic extension K of $\mathbb{Q}$ of degree n_1 and n_2 respectively. Let f_1 be the minimal polynomial of the extension L_1 with roots α_i, similarly define f_2 with roots β_i. Finally, let L_1L_2 be the extension of K generated by the polynomial f_1f_2. The notation L_1L_2 comes from noticing that L_1L_2 is generated over K by the products e_if_j with $\{e_i\}$ a basis of L_1 and $\{f_j\}$ a basis of L_2.

$$\begin{tikzcd}
& L_1L_2 \arrow[dl, no head] \arrow[dr, no head] & \\
L_1 & & L_2 \\
& K \arrow[ul, no head, "n_1"'] \arrow[ur, no head, "n_2"'] & \\
& \mathbb{Q} \arrow[u, no head, "2"] &
\end{tikzcd}$$

We can now state the following lemmas:

Lemma 2. *If L_1 and L_2 are Galois over $\mathbb{Q}$ then so is L_1L_2.*

Proof. If τ denotes the nontrivial automorphism of $K = \mathbb{Q}(\sqrt{d})$ then the assumption implies that $\tau(f_1)$ and $\tau(f_2)$ split in L_1L_2. Hence L_1L_2 is the splitting field of the polynomial $(X^2-d)f_1f_2\tau(f_1f_2)$, which is a polynomial over $\mathbb{Q}$. ■

Lemma 3. *With the assumptions of Lemma 2 and moreover the condition that L_1 and L_2 are linearly independent over K (meaning that $L_1 \cap L_2 = K$), we have that $Gal(L_1L_2/K) = Gal(L_1/K) \times Gal(L_2/K)$.*

Proof. Any $(\sigma_1, \sigma_2) = \sigma \in Gal(L_1/K) \times Gal(L_2/K)$ determines an automorphism of L_1L_2 which fixes K by construction. Therefore $Gal(L_1/K) \times Gal(L_2/K) \subseteq Gal(L_1L_2/K)$. Equally by Galois theory we have that $|Gal(L_1L_2/K)| = [L_1L_2 : K]$, hence $Gal(L_1/K) \times Gal(L_2/K)$ is the whole group $Gal(L_1L_2/K)$ completing the proof.

■

Note that the condition of linear Independence over K implies $[L_1L_2 : \mathbb{Q}] = [L_1L_2 : K][K : \mathbb{Q}] = n_1n_2 \cdot 2$.

Theorem 2. *With the same assumptions as in Lemma 2 if $Gal(L_1/\mathbb{Q}) = D_{n_1}$ and $Gal(L_2/\mathbb{Q}) = D_{n_2}$ and n_1 and n_2 are co-prime then $Gal(L_1L_2/\mathbb{Q}) = D_{n_1n_2}$.*

Proof. Since $Gal(K/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$, from this it follows that $Gal(L_1/K) = \mathbb{Z}/n_1\mathbb{Z}$ and $Gal(L_2/K) = \mathbb{Z}/n_2\mathbb{Z}$. By our choices of n_1 and n_2 and the Chinese Remainder Theorem we have that $Gal(L_1L_2/K) = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} = \mathbb{Z}/n_1n_2\mathbb{Z}$. Therefore $Gal(L_1L_2/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \ltimes \mathbb{Z}/n_1n_2\mathbb{Z}$ from Lemma 1.
We now show that $\tau \in \mathbb{Z}/n_2\mathbb{Z}$ acts on elements of $\mathbb{Z}/n_1n_2\mathbb{Z}$ by -1, or put simply it acts in the dihedral way. For $\sigma = (\sigma_1, \sigma_2) \in Gal(L_1L_2/K)$ we have:

$$\tau\sigma\tau = \tau(\sigma_1, \sigma_2)\tau = (\tau\sigma_1\tau, \tau\sigma_2\tau) = (\sigma_1^{-1}, \sigma_2^{-1}) = \sigma^{-1}.$$

This completes the proof.

■

A natural question is what would happen if, in Lemma 3, n_1 and n_2 were not co-prime. In that case, we would not be able to use the Chinese Remainder Theorem, and therefore we would have that $C_2 \ltimes (\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z})$. Nevertheless, the rest of the proof is still valid. Williamson refers to such groups as a generalization of dihedral groups. This is warranted because the element of order two still acts by -1, as in the standard dihedral groups. We will not be concerned with those groups.

5 Elliptic Curves

In this section, we provide the definition of an elliptic curve. Since we are concerned with the inverse Galois problem over $\mathbb{Q}$ for dihedral groups, we omit most of the rich theory of elliptic curves and provide only the parts which will be relevant in the following sections. A general overview of elliptic curves can be found in Silverman's "The Arithmetic of Elliptic Curves"[3] from which most of the material we cover is taken.

5.1 The Group of an Elliptic Curve

In the following, we will use the Weierstrass notation for elliptic curves over a field K. A small note is that this notation is valid only for fields K for which the algebraic closure has characteristics different than 2 or 3. Since $\overline{\mathbb{Q}} = \mathbb{C}$ has characteristic 0, this will always be the case.

Definition 8. *An* ***elliptic curve*** *in Weierstrass form defined over a field K, such that the characteristic of $\overline{K}$ is not 2 or 3, is an equation of the form:*

$$y^2 = x^3 + a_4 x + a_6, \tag{1}$$

together with "a point at infinity" denoted by O. In this case, we can write:

$$E : y^2 = x^3 + a_4 x + a_6. \tag{2}$$

Remark 8. *Two questions arise immediately from the definition. Why the point at infinity and the odd numbering of the coefficients of x. The point at infinity will be relevant later in order to construct the group of an elliptic curve. The numbering of the coefficients arises from the Riemann-Roch theorem, which unfortunately falls beyond the scope of this thesis. For the interested reader, Chapter 2 Section 5 of Silverman's book[3] provides an excellent introduction to the subject.*

Since we are dealing with only two coefficients, we let $E : y^2 = x^3 + ax + b$ for simplicity. This is sometimes referred to as the short Weierstrass form. For $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ such that $x_P, y_P, x_Q, y_Q \in K$ and chosen in a way that they satisfy the equation of an elliptic curve E, we can define the composition law. This is a standard definition. See Silverman's book for more details[3].

Definition 9. *Let P and Q be points on an elliptic curve. Then we define $P + Q$ as follows.*

If $P = Q$ we take the tangent line of E at P, otherwise we take the line passing through P and Q. If this line crosses E at another point R we say that $P + Q = -R$ else we say that $P + Q = O$. Furthermore $P + O = P$.

Remark 9. *In our case, $-R$ is simply R projected through the x axis. We can see that a line from R to $-R$ passes only through these two points because our equation has only two solutions for each x, and hence it will go to infinity. Therefore $R + (-R) = O$.*

We can now define the group of an elliptic curve.

Definition 10. *Given an elliptic curve E over K, we define the group of E as $E(K)$, where the group is composed of all pairs $x, y \in K$ such that they satisfy the equation of E, and O which is also the identity element of the group. The composition law gives the operation of the group.*

Remark 10. *This defines a group, the proof of which is beyond these short remarks.*

Since we will be working over $\mathbb{Q}$, then the group of an elliptic curve E will be denoted by $E(\mathbb{Q})$. Despite being complicated to compute, it is reasonably easy to grasp what object we are dealing with intuitively. Simply put, it is all the solutions to the equation of E

plus an extra point at infinity.

It will be helpful to consider mappings between elliptic curves, which preserve the structure. Since E is an algebraic curve and $E(\mathbb{Q})$ is simply a group, they are the group homomorphisms that can be described by rational functions in the variables x, y. For elliptic curves, these mappings are called isogenies. The formal definition is given below.

Definition 11. *Given elliptic curves E and E', an isogeny from E to E' is a group homomorphism from $E(\mathbb{Q})$ to $E'(\mathbb{Q})$ that also preserves the structure of the elliptic curve over $\mathbb{Q}$.*

Remark 11. *It is noticeable that no definition of preserving the structure of the elliptic curve is given, a complete account of which would be beyond the scope of this thesis. A more detailed account is given on pages 12, and 13 of Silverman's book [3].*

Remark 12. *Since we are dealing with elliptic curves, which are in some sense stricter objects than groups, Silverman notes in 3.6.1 that for an isogeny $\phi : E \to E'$, we have that $\phi(E)$ is either E' or $\{O\}$ [3].*

5.2 Elliptic Curves with Complex Multiplication

We will now consider a special type of isogenies, that is, isogenies from an elliptic curve E to E itself. Such isogenies are called endomorphisms. All the endomorphisms of an elliptic curve also form a ring under functional addition and multiplication. We denote this ring as $End(E)$. Note that these are defined to be the isogenies which can be represented by rational functions and that in order to get a ring, we also need to consider the zero isogeny $\phi(E) = O$.

We will now state a few properties regarding the structure of $End(E)$ when E is an elliptic curve over $\mathbb{Q}$. We will not provide proofs as they are beyond this thesis's scope since this section's primary goal is to provide an introduction to the theory we will use. Again Silverman's book offers a more detailed introduction to the subject matter [3].

In general, it is the case that $End(E) \simeq \mathbb{Z}$, but that is not necessarily always true. For some elliptic curves, the endomorphism ring is bigger than simply $\mathbb{Z}$. In particular, the following definition will be helpful, but first a short remark.

Remark 13. *In the definition of complex multiplication, we will consider the group of an elliptic curve $E(\mathbb{C})$, which is defined in the same way as the above-mentioned $E(\mathbb{Q})$ except for the fact that we are now considering all complex coordinates. Naturally $E(\mathbb{Q}) \subset E(\mathbb{C})$.*

Definition 12. *An elliptic curve E with coefficients in $\mathbb{Q}$ **allows for complex multiplication** if the endomorphism ring is isomorphic to $\mathbb{Z}[\iota]$ for some $\iota \in \mathbb{C} \setminus \mathbb{R}$. (In this case, ι necessarily is a zero of a monic quadratic polynomial over $\mathbb{Z}$).*

Remark 14. *The definition is a bit abstract so we provide an example. Consider $E : y^2 = x^3 - x$ then the map $\iota : (x, y) \mapsto (-x, iy)$ is a complex isogeny. Since $(iy)^2 = -y^2 = -(x^3 - x) = -x^3 + x = (-x)^3 - (-x)$. We also note that $\iota^2 = -1$, therefore in this case $\iota = i$.*

6 Some Facts About Torsion Point of Elliptic Curves

In this section, we will cover some important results regarding torsion points of elliptic curves. Torsion points are points P of $E(K)$ such that $nP = O$, that is points of finite order. In this case, we say that P is a point of torsion n. The results we present are deep, and the proofs are very involved, some even beyond the level of a "Graduate Text in Mathematics". Therefore we provide no proof of the theorem we state. The first part gives a characterization of the coordinates of points with torsion, which is useful if we want to find a point with specific torsion. We will see that such coordinates need to be zeros of a specific polynomial. For our specific application, that is, torsion points of elliptic curves over $\mathbb{Q}$ said polynomials do not need to have zeros in $\mathbb{Q}$ therefore, the second part provides a method of finding elliptic curves such that they have a point of torsion n for some specific n. The final part will explain why this is the case, since only for a few selected n does an elliptic curve with a point of torsion n exist, namely $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ and 12. Finally, we will consider the n torsion group of an elliptic curve defined over $\overline{K}$, that is the collection of all the points of torsion n, in that case, we will show that said group has a very specific structure, namely $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

6.1 Division Polynomial

Consider an elliptic curve $E : y^2 = x^3 + ax + b$ with coefficients in $\mathbb{Q}$. Under what conditions does $P \in E(\overline{\mathbb{Q}})$ satisfy $nP = O$? It turns out that there exists a recursive formula. The proof is computationally involved, but the details can be found in Sutherland's lecture notes [2].

Definition 13. *We define the zeroth, first, second and third division polynomial as follows:*

$$\psi_0 = 0,$$

$$\psi_1 = 1,$$

$$\psi_2 = 2y,$$

$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$

and we define the other ***nth division polynomials*** *recursively as follows, depending whether n is odd or even:*

$$\psi_{n=2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3,$$

$$\psi_{n=2m} = \left(\frac{\psi_m}{2y}\right)\left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right).$$

Theorem 3. *For a given elliptic curve $E : y^2 = x^3 + ax + b$ if we pick $A = a$ and $B = b$ in the definition of division polynomial then for $(x, y) = P \in E(\mathbb{C})$ we have that:*

$$nP = \left(x - \frac{\psi_{n-1}(x)\psi_{n+1}(x)}{\psi_n^2(x)}, \frac{\psi_{2n}(x)}{2\psi_n^4(x)}\right).$$

For odd n follows that $nP = O$, the point at infinity if x is a zero of ψ_n. For even n we need to consider also possible linear combinations with the points of order 2.

Remark 15. *We note that since x being a zero of ψ_n only implies that $nP = O$, there is a possibility that only points of order dividing n will be found. For example, taking the zeros of the sixth division polynomial could correspond to the x-coordinates of points of order 3, since $6P = 3P + 3P = O + O = O$. This is not something to worry about since $deg(\Psi_3) < deg(\Psi_6)$ we have that a point of order 6, and not just torsion 6, will be found.*

Remark 16. *The limitation on even n is easily calculated since for a point P of order 2 we have that $P = -P$. But following the composition law that implies that the y coordinate needs to be zero, that is $0 = x^3 + ax + b$.*

6.2 Tate's Normal Form

From the above, it follows that we need to find the roots of Ψ_n if we want to find a point of order n. In the first method we will use, it will be important not only to find the root but also that the root is rational. Therefore, we ask under what conditions does the root of Ψ_n corresponding to a point of order n lie in $\mathbb{Q}$?

With some manipulations of a general elliptic curve of the form $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and starting from a point $P \in E(\mathbb{Q})$ of order > 3 we can put the equation in the so-called Tate's normal form: $y^2 + uxy + vy = x^3 + vx^2$, and here P is simply $(0, 0)$. Then with some computations, we can show the following theorem. The proof of which is remarkably shallow, involving mostly computations. For this reason, we decided to omit it. For details on how the proof plays out, chapter 4 of Husemoller's book [8] for $n = 4, 5, 6, 8$ and 9 is very informative. A complete table can be found in a paper by Kubert [12].

Lemma 4. *For an elliptic curve $E : y^2 + uxy + vy = x^3 + vx^2$ then the point $(0, 0)$ is a rational point of torsion n if:*

- *For $n = 4$ we have that $v = -\alpha$ and $u = 1$.*
- *For $n = 5$ we have that $v = -\alpha$ and $u = 1 - \alpha$.*
- *For $n = 6$ we have that $v = -\alpha - \alpha^2$ and $u = 1 - \alpha$.*
- *For $n = 7$ we have that $v = -\alpha^3 + \alpha^2$ and $u = 1 - \alpha^2 + \alpha$.*
- *For $n = 8$ we have that $v = -(2\alpha - 1)(\alpha - 1)$ and $u = 1 - \frac{-v}{\alpha}$.*
- *For $n = 9$ we have that $u = 1 - \alpha^2(\alpha - 1)$ and $v = -(1 - u)(\alpha(\alpha - 1) + 1)$.*
- *For $n = 10$ we have that $u = 1 - \frac{(2\alpha^3 - 3\alpha^2 + \alpha)}{\alpha - (\alpha - 1)^2}$ and $v = -\frac{(1-u)\alpha^2}{\alpha - (\alpha - 1)^2}$.*
- *For $n = 12$ we have that $u = 1 - \frac{(3\alpha^2 - 3\alpha + 1)(\alpha - 2\alpha^2)}{(\alpha - 1)^3}$ and $v = -\frac{(1-u)(2\alpha - 2\alpha^2 - 1)}{\alpha - 1}$.*

  For almost any $\alpha \in \mathbb{Q}$.

Remark 17. *Note the switching of u and v from the cases $n = 8$ and $n = 9$. This is done in order to simplify and clarify the writing.*

Remark 18. *The definition we gave of the elliptic curve above is different from the one in the previous section. We can quickly transform from the Tate form to the reduced Weierstrass form.*

Lemma 5. *A curve in the form* $E : y^2 + uxy + vy = x^3 + vx^2$ *is equivalent to a curve in the form* $E : y^2 = x^3 + 27(24uv - u^4)x + 216(u^6 - 36u^3v + 216uv)$.

Proof. This is a simple direct computation from the maps Silverman provides in Chapter 3 Section 1 of his book[3].
We first consider the transformation $y \mapsto \frac{1}{2}(y - ux - v)$, this transformation allows us to move to the simpler:

$$y^2 = 4x^3 + u^2x^2 + 2uvx + v^2.$$

Then we transform $x \mapsto \frac{x-3u^2}{36}$ and $y \mapsto \frac{y}{108}$ to get the reduced Weierstrass equation:

$$y^2 = x^3 + 27(24uv - u^4)x + 216(u^6 - 36u^3v + 216uv).$$

■

Remark 19. *The transformation in Lemma 5 has the side effect that the point of order* n *is no longer* $(0, 0)$ *but* $(-\frac{1}{12}u^2, -\frac{1}{216}v)$.

6.3 Mazur's Theorem

In the previous two parts, we first provided a way of finding arbitrary n-torsion points of an elliptic curve. After that, we provided a family of elliptic curves such that they have a rational point of order n. Then there is a natural question: why did we only provide the families for elliptic curves for certain n and not others? The answer lies in Mazur's theorem.

Theorem 4. *Given an elliptic curve* E *over* $\mathbb{Q}$ *then* $E(\mathbb{Q})$ *can only contain a point of order* $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$ *or infinite order.*

Remark 20. *The proof of Mazur's theorem is beyond the scope of this thesis. For what is worth, some details can be found in Mazur's original paper [15], but beware, Silverman's book, which we often reference for proofs beyond the scope of this short notes, refers to the proof as "far beyond the scope of this book"[3].*

Remark 21. *Another fact that jumps to the eye are that in Lemma 4 we did not consider points of order* 2 *and* 3*. This is because Tate's normal form does not allow such points. Furthermore, as we will see later, those points could only give rise to extensions for* D_2 *and* D_3*. In this case, those two groups are not particularly interesting. By being small, they are straightforward to realize explicitly. Therefore, we decided to skip those rather than introducing separate conditions.*

6.4 Velu's Formula

Another piece of theory we will use is Velu's formula. Given an elliptic curve E with a point P of order n it provides an explicit isogeny α to another elliptic curve E' such that $\ker \alpha = \langle P \rangle$. The proof that this is an isogeny and will have the desired kernel is beyond the scope of this thesis. For those, the original paper, translated from French, is a good reference [23].

Theorem 5. *Let E be an elliptic curve, let P be a point of order n. Then for any $(x, y) \in E(\mathbb{Q})$ we set:*

$$X = x + \sum_{i=1}^{n-1}(((x, y) + iP)_1 - iP_1),$$
$$Y = y + \sum_{i=1}^{n-1}(((x, y) + iP)_2 - iP_2),$$

where the subscript indicates the first or the second coordinate. Then the isogeny $\alpha : (x, y) \mapsto (X, Y)$ will have kernel $\langle P \rangle$.

Remark 22. *We note that if we pick $(x, y) = P$ then the equations simplify to:*

$$X = x + \sum_{i=1}^{n-1} P_1 = x + (n-1)P_1 = O,$$
$$Y = y + \sum_{i=1}^{n-1} P_2 = y + (n-1)P_2 = O.$$

As claimed $\alpha(P) = O$.

Remark 23. *It is immediately noticeable that Velu's formula does not provide a simple formula for the isogeny in question. In particular, adding and subtracting points to get the correct X and Y is particularly difficult and prone to mistakes when done by hand, given the complexity of operations on elliptic curves. This task is better left for a machine.*

6.5 The Structure of $E[n]$

In this section, we take an elliptic curve E with coefficients in $\mathbb{Q}$ and consider the group $E(\mathbb{C})$. An important result which we use is that in this case the n-torsion subgroup $E[n]$ that is all the points $P \in E(\mathbb{C})$ such that $nP = O$ is isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. We state the theorem formally, a proof of which can be found in Chapter 3, Section 6 of Silverman's book[3].

Theorem 6. *For an elliptic curve E we have that:*

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Remark 24. *This implies that $E[n]$ is generated by two points of order n which we can identify with $(\overline{0}, \overline{1})$ and $(\overline{1}, \overline{0})$.*

7 Ideal Class Groups

This section aims at introducing some elementary notions from class field theory. Namely, we show what an ideal class group is and prove some of its properties. After that, we present the j-invariant and the Hilbert class field. We only present the results we will be using to realize dihedral groups since a complete treatment of them would be beyond the scope of this thesis.

In particular, in order to present the theory in the clearest possible way, these short notes are not taken from any book but rather are a re-elaboration of Cox's presentation on the matter from "Primes of the Form x^2+ny^2 [5], Dogger's thesis on the subject[6], the paper by Kaltofen and Yui which informed the method we will later use this theory for[11], as well as many fruitful discussions with my first supervisor.

7.1 The Definition of an Ideal Class Group

Consider now an imaginary quadratic extension of $\mathbb{Q}$ given by $\mathbb{Q}(\sqrt{-d})$ for $d > 0$ square free. We first define the notion of an algebraic integer.

Definition 14. *For any $\alpha \in \mathbb{Q}(\sqrt{-d})$ we say that it is an **algebraic integer** if the minimal polynomial of α is monic and had integer coefficients.*

We now find all the algebraic integers of $\mathbb{Q}(\sqrt{-d})$.

Lemma 6. *The integer ring of $\mathbb{Q}(\sqrt{-d})$ is $\mathbb{Z}[\omega]$ for:*

$$\omega = \begin{cases} \sqrt{-d} & \text{if } -d \equiv 2,3 \mod 4, \\ \frac{1+\sqrt{-d}}{2} & \text{if } -d \equiv 1 \mod 4. \end{cases}$$

Proof. Clearly we have that any element of $\mathbb{Z}$ is also an integer of $\mathbb{Q}(\sqrt{-d})$. Now consider any $\alpha = a + b\sqrt{-d} \in \mathbb{Q}(\sqrt{-d})$ its minimal polynomial in $\mathbb{Q}[X]$ is given by:

$$(X-a)^2 + b^2 d = X^2 - 2aX + a^2 + a^2 + b^2 d.$$

Therefore for this polynomial to have integer coefficients, we require that $2a$ is an integer and that $a^2 + b^2 d$ is an integer. We, therefore, distinguish two cases.
First consider $a \in \mathbb{Z}$. Then $2a \in \mathbb{Z}$. Then $a^2 + b^2 d \in \mathbb{Z}$ requires that $b^2 d \in \mathbb{Z}$. Since d is square free then it will not be able to cancel out any of the possible denominators of b^2, because they are all squares it follows that $b \in \mathbb{Z}$. Hence any element of $\mathbb{Z}[\sqrt{-d}]$ is an algebraic integer.
Consider now that $a = \frac{c}{2}$ for an odd integer c. Then $\frac{c^2}{4} + 4b^2 d = \frac{c^2+4b^2d}{4}$ is an integer. Hence we have that $c^2 + 4b^2 d$ is not only an integer, but also divisible by 4. We write $c^2 + 4b^2 d \cong 0 \mod 4$. Of course $c^2 \not\cong 0 \mod 4$ since it is odd. Then we note that $c^2 \cong 1 \mod 4$ since it is a square. Let now $b \in \mathbb{Q}$ be $\frac{g}{h}$ such that $gcd(g,h) = 1$. Then $c^2 + 4b^2 d = c^2 + 4\frac{g^2}{h^2} d$.
In the case, $-d \cong 2 \mod 4$ then $d \cong 2 \mod 4$ cancelling out one of the numerators. Hence the h^2 will cancel out. This means that for $-d \cong 2 \mod 4$ we found all the integers with $\mathbb{Z}[\sqrt{-d}]$. In the other cases where d is odd, we have that $h^2 = 4$ in order for the whole expression to be an integer.
It the case $-d \cong 3 \mod 4$ then $d \cong 1 \mod 4$ then no solutions exist. Since g^2 is a square then $g^2 \cong 1 \mod 4$ and hence the whole expression is congruent to 2. We found all the integers with $\mathbb{Z}[\sqrt{-d}]$.
In the case $-d \cong 1 \mod 4$ then $d \cong 3 \mod 4$. Since g^2 is a square then $g^2 \cong 1 \mod 4$ and hence the whole expression mdulus 4 simplifies to $1 + 1 \cdot 3 = 4$. Therefore it is an integer. Since we took $a = \frac{c}{2}$ and $b = \frac{g}{2}$ then this algebraic integers can be written as $\frac{1}{2}\mathbb{Z}[\sqrt{-d}]$ hence we found that all the algebraic integers in the case $-d \cong 1 \mod 4$ are in $\mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$ as claimed.

■

Remark 25. *We also claimed that all the integers of* $\mathbb{Q}(\sqrt{-d})$ *form a ring. This is since* $\mathbb{Z}[\omega]$ *is a ring. It is closed under addition and multiplication.*

We can now introduce the notion of a discriminant of $\mathbb{Q}(\sqrt{-d})$.

Definition 15. *The **discriminant**, denoted by* D*, of the imaginary quadratic field* $\mathbb{Q}(\sqrt{-d})$ *with integer ring* $\mathbb{Z}[\omega]$ *is:*

$$D = det\left(\begin{bmatrix} 1 & \omega \\ 1 & \overline{\omega} \end{bmatrix}\right)^2 = -4\mathrm{Im}(\omega)^2 = \begin{cases} -4d & if\ -d \equiv 2,3 \mod 4, \\ -d & if\ -d \equiv 1 \mod 4. \end{cases}$$

We now prove a lemma regarding non-principal ideals of $\mathbb{Z}[\omega]$.

Lemma 7. *Every ideal* $I \subset \mathbb{Z}[\omega]$ *is generated (as a* $\mathbb{Z}$*-module) by at most two elements.*

Proof. From definition we know that $\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$ is a rank 2 $\mathbb{Z}$ module. Consider now an ideal $I \subseteq \mathbb{Z}[\omega]$. Clearly as a $\mathbb{Z}$ module I can be of at most rank 2. We conclude that $I = \{a\omega_1 + b\omega_2 | a, b \in \mathbb{Z}\}$ for some ω_1 and ω_2 in $\mathbb{Z}[\omega]$. ■

We now define an equivalence relation on the ideals of $\mathbb{Z}[\omega]$.

Definition 16. *For two ideals* $I, J \subseteq \mathbb{Z}[\omega]$ *such that:*

$$(a)I = (b)J,$$

for principal ideals $(a), (b)$ *generated by* $a, b \in \mathbb{Z}[\omega]$ *we say that they are equivalent and we denote that by* $I \sim J$.

Remark 26. *It is easy to see that the relationship is reflexive and symmetric. It is transitive since for equivalent* I, J, K *ideals of* $\mathbb{Z}[\omega]$ *we have that if* $(a)I = (b)J$ *and* $(c)J = (d)K$ *then:*

$$(ca)I = (c)(a)I = (c)J = (d)K.$$

Which is the case since $\mathbb{Z}[\omega]$ *is commutative.*

Therefore, we can now consider the ideal class group $\mathbb{Z}[\omega]/\sim$. We need to show that, indeed, it is a group.

Lemma 8. *The ideal class group* $\mathbb{Z}[\omega]/\sim$ *is an abelian group. We have that the operation on two representatives* $[I]$ *and* $[J]$ *is* $[I] \cdot [J] = [IJ]$*, the inverses of this operation exist, and the unit is* $[\mathbb{Z}[\omega]]$ *which is the class of all principal ideals, where we used the square brackets to represent the classes of specific ideals.*

Proof. Of course any principal ideal $P \subseteq \mathbb{Z}[\omega]$ is equivalent to the whole ring. Since P is principal then it is generated by a single element p. Then:

$$(1)P = (p)\mathbb{Z}[\omega].$$

It also follows that for any ideal equivalent to the integer ring, such an ideal must be principal. We show that $[\mathbb{Z}[\omega]]$ is the identity. Indeed this is the case since for any ideal I, we have that $\mathbb{Z}[\omega]I = I$.

Thirdly we show that the operation is well defined. Consider ideals $I \sim J$ such that $(a)I = (b)J$ then for any other ideal class represented by $[K]$ we have that:

$$[IK] = [I][K] = [(a)][I][K] = [(a)I][K] = [(b)J][K] = [(b)][J][K] = [JK].$$

Finally we show that inverses exits. Consider a non-principal ideal $I \subset \mathbb{Z}[\omega]$ then from Lemma 7 we know that I is generated by two elements, say α and β. Furthermore without loss of generality we can pick α to be an integer. Since if not we compute $I \sim (\overline{\alpha})(\alpha, \beta) = (\overline{\alpha}\alpha, \overline{\alpha}\beta)$. Then consider the ideal $J = (\alpha, \overline{\beta})$ then:

$$IJ = (\alpha, \beta)(\alpha, \overline{\beta}) = (\alpha^2) + (\beta\alpha) + (\overline{\beta}\alpha) + (\beta\overline{\beta}).$$

Notice that the first and last ideals are generated by integers. Furthermore:

$$(\beta\alpha) + (\overline{\beta}\alpha) = (\beta\alpha, \overline{\beta}\alpha) = (a)(\beta, \overline{\beta}) = (a)(\beta\overline{\beta}).$$

Hence all three ideals are generated by integers, and their sum is a principal ideal generated by the greatest common divisor. So we found an inverse.

■

Remark 27. *In the last part of the previous proof, in which we found the inverse of an ideal I, we also showed that the inverse of this ideal is the complex conjugate. That is $[I]^{-1} = [\overline{I}]$.*

Another important result in the theory of ideal class groups is the following lemma which states that the ideal class group is finite. A detailed proof of this statement can be found in Chapter four of Milne's textbook on algebraic number theory[18].

Lemma 9. *The abelian group $\mathbb{Z}[\omega]/\sim$ is finite.*

Remark 28. *It is customary to denote $\mathbb{Z}[\omega]$ as $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$ as for example in Cox's book[5].*

7.2 Integral Binary Quadratic Forms

We will now look for a way to find representatives of $\mathbb{Z}[\omega]/\sim$. It turns out that there is a classical algorithm by Gauss to find them. First, we introduce the notion of a positive definite reduced primitive quadratic form. Most of the section is taken from Kaltofen's and Yui's[11].

Definition 17. *A* ***positive definite reduced primitive quadratic form*** *is an expression of the form:*

$$ax^2 + bxy + cy^2,$$

for a, b, c integers. We also let $a > 0$, hence positive. We also let $gcd(a, b, c) > 1$, hence primitive. Welet the discriminant of this form be $D = b^2 - 4ac$. We denote the form by simply $[a, b, c]$.

We define an equivalence relation between forms as follows:

Definition 18. *In the form $f(x,y) = ax^2 + bxy + cy^2$, we replace x with $\alpha x + \beta y$ and y with $\gamma x + \delta y$ in such way that:*

$$\det\left(\begin{bmatrix}\alpha & \beta \\ \gamma & \delta\end{bmatrix}\right) = 1 \;\; \textit{and} \;\; \alpha, \beta, \gamma, \delta \in \mathbb{Z}.$$

Then the resulting form $g(x,y)$ is said to be ***equivalent*** *to the form $f(x,y)$.*

For each equivalence class of forms with a given discriminant we can find representatives satisfying either $-a < b \leq a < c$ or $0 \leq b \leq a = c$.

Remark 29. *Similarly, as with the ideal class group, we can think of all the possible binary quadratic forms of a given discriminant under this equivalence relation as an abelian group. What will be relevant for realizing dihedral groups are the following two lemmas. A proof of which can be found in Dogger's bachelor thesis[6].*

Lemma 10. *There is an isomorphism between binary quadratic forms in an equivalence class of discriminant $-d$ and the ideal class group of the integers $\mathbb{Q}(\sqrt{-d})$. It is given by the map α:*

$$\alpha : [a,b,c] \mapsto \left[\left(2a^2, -b + \sqrt{-d}\right)\right].$$

Lemma 11. *An algorithm to compute all reduced binary quadratic forms of discriminant $d < 0$ is as follows:*

$a \leftarrow 1$
$b \leftarrow -a$
$c \leftarrow \frac{b^2-d}{4a}$
while $a \leq \sqrt{-\frac{d}{3}}$ ***do***
  if *c is integer and $c \geq a$ and $\gcd(a,b,c) = 1$* ***then***
    if *$|b| = a$ or $a = c$* ***then***
      if $b \geq 0$ ***then***
        print(a,b,c)
      end if
    end if
  else *print(a,b,c)*
  end if
  $b \leftarrow b + 1$
  if $b > a$ ***then***
    $a \leftarrow a + 1$
    $b \leftarrow -a$
  end if
  $c \leftarrow \frac{b^2-d}{4a}$
end while

Remark 30. *Despite being quite long, the algorithm is simple. It iterates through all the possible values of a and b and sets c such that the discriminant will be correct. After that, check whether the triple satisfies any of the two conditions mentioned above.*

7.3 j-Invariants

In this part, we introduce the notion of the j-invariant and generalize it to ideals of $\mathbb{Z}[\omega]$. After that, we provide some remarks to glimpse the importance of the j-invariant.

Definition 19. *The **j-invariant** is the unique complex differentiable function on:*

$$\{z \in \mathbb{C} | im(z) > 0\} \to \mathbb{C},$$

satisfying $j(\frac{a\tau+b}{c\tau+d}) = j(\tau)$ for all integers such that $ad - bc = 1$. The Laurent q-series expansion is

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

with $q = e^{2\pi i \tau}$.

Remark 31. *In the definition, we make two claims. First, the j-invariant is complex and differentiable; second, it is unique. Proof of both claims can be found in Chapter 10 of Cox's book[5] another slightly more accessible text is Milne's Chapter three of Milne's "Elliptic Curves"[17].*

We can now ready to extend the j-invariant to ideals of $\mathbb{Z}[\omega]$ and show that it is invariant under $\sim$, so it yields a function on the ideal class group $\mathbb{Z}[\omega]/\sim$. Recall that in Lemma 7 we showed that one or two elements generate every ideal of $\mathbb{Z}[\omega]$.

Definition 20. *For an ideal I in $\mathbb{Z}[\omega]$ we define $j(I)$ as $j(\omega)$ if I is a principal ideal. Otherwise, for a non-principal ideal I generated by a and b we define it as $j(\frac{a}{b})$ or $j(\frac{b}{a})$ depending on which fraction will have positive imaginary part.*

Lemma 12. *For two ideals I and J in $\mathbb{Z}[\omega]$ $I \sim J$ implies that $j(I) = j(J)$.*

Proof. In the case the ideals are principal then the proof is trivial. Consider now $I = (a, b)$ and $J = (c, d)$ and $\alpha, \beta \in \mathbb{Z}[\omega]$ such that $(\alpha)I = (\beta)J$.

We start by noticing that:

$$(\alpha)I = (\alpha)(a, b) = (\alpha)((a) + (b)) = (\alpha)(a) + (\alpha)(b) = (\alpha a) + (\alpha b) = (\alpha a, \alpha b).$$

Similarly then:

$$(\beta)J = (\beta c, \beta d).$$

Without loss of generality we assume $im(\frac{a}{b}) > 0$ and $im(\frac{c}{d}) > 0$. We have then:

$$j((\alpha)I) = j((\alpha a, \alpha b)) = j(\frac{\alpha a}{\alpha b}) = j(\frac{a}{b}) = j(I).$$

Furthermore:

$$j((\beta)J) = j((\beta c, \beta d)) = j(\frac{\alpha c}{\alpha d}) = j(\frac{c}{d}) = j(J).$$

And since $j((\alpha)I) = j((\beta)J)$ we conclude:

$$j(I) = j(J).$$

Assume now that $j(I) = j(J)$.

$\blacksquare$

Remark 32. *Showing that $j(I) = j(J)$ implies $I \sim J$ is slightly more involved, a proof of this statement can be found in Chapter 11 of Cox's book[5]. The above two statements show that the j-invariant yields an injective map $j\colon (\mathbb{Z}[\omega]/\sim) \to \mathbb{C}$.*

Remark 33. *As it appears, the j-invariant is uncorrelated to any of the theories we mentioned so far. This is not the case. It can be shown that the j-invariant is invariant on the lattices of $\mathbb{C}$. An ideal generated by two elements can be tough as a lattice. Furthermore, an elliptic curve E over $\mathbb{C}$ is also connected to a lattice, it can be shown $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$. All the different sections are connected. A full description of this theory would be beyond the scope of these remarks. For a more detailed discussion, Cox's book is a good starting point [5].*

7.4 Hilbert Class Field

In this part we present how to construct a field extension H of $\mathbb{Q}(\sqrt{-d})$ in the way that $Gal(H/\mathbb{Q}(\sqrt{-d})) \simeq \mathbb{Z}[\omega]/\sim$. The proof of the statements we will use are somewhat involved and therefore are omitted. In case Cox's book "Primes of the Form $x^2 + ny^2$" is a good reference [5].

First, we define the Hilbert class field, for which we will see that it has all the desired properties.

Definition 21. *Fix $\mathbb{Q}(\sqrt{-d})$. Let $I_1, I_2, \ldots, I_n$ be representatives for all the classes of $\mathbb{Z}[\omega]/\sim$. The* ***Hilbert class field*** *of $\mathbb{Q}(\sqrt{-d})$ is:*

$$\mathbb{Q}(\sqrt{-d})(j(I_1), j(I_2), \ldots, j(I_n)).$$

We will denote the Hilbert class field as H.

We want to show that H over $\mathbb{Q}(\sqrt{-d})$ is a Galois extension. Of course, a necessary condition is that H is an extension of $\mathbb{Q}$ of finite degree. This is guaranteed by the fact that $\mathbb{Z}[\omega]/\sim$ is finite by Lemma 9. In this case, we will need the following lemma.

Lemma 13. *For any $J \in \mathbb{Z}[\omega]/\sim$ then $j(J)$ is an algebraic integer over H. The minimal polynomial of which is:*

$$p(X) = \prod_{I \in \mathbb{Z}[\omega]/\sim} (X - j(I)).$$

Remark 34. *It follows from Lemma 13 that all the j-invariants of ideals in $\mathbb{Z}[\omega]$ have the same minimal polynomial. In particular then $H = \mathbb{Q}(\sqrt{-d}, j(I))$ for only one $j(I)$.*

Remark 35. *A fact that will be used later is that the minimal polynomial of an algebraic integer is monic and has integer coefficients.*

Finally, we state that H has the property which we wanted it to have.

Theorem 7. *We have that $Gal(H/\mathbb{Q}(\sqrt{-d})) \simeq \mathbb{Z}[\omega]/\sim$.*

Remark 36. *We note that any $\sigma \in Gal(H/\mathbb{Q}(\sqrt{-d}))$ acts by taking one $j(I)$ to a $j(J)$, since it needs to permute the roots of the polynomial from Lemma 13.*

The isomorphism is given explicitly by the Artin map.

Definition 22. *The **Artin map**, denoted by A, is an isomorphism from $\mathbb{Z}[\omega]/\sim$ to $Gal(H/\mathbb{Q}(\sqrt{-d}))$ given by:*

$$A : [I] \mapsto \tau_I,$$

Where for any $j(J) \in H$ then:

$$\tau_I(j(J)) = j(I^{-1}J).$$

8 Method by Torsion

This section presents the first of the three methods we tried in our search for polynomials with dihedral Galois group over $\mathbb{Q}$. Mestre in [16] and Williamson in [24] already use this method to realize some dihedral groups over $\mathbb{Q}$. In this section, we discuss the theory behind this construction, as well as its limitations. The appendix provides the polynomials for all the realizable dihedral Galois groups with this method.

8.1 Motivation

Consider an elliptic curve E and a point $P \in E(\mathbb{Q})$ of order n. Clearly the isogeny "translation by P" is of order n. How can we make it dihedral? We need an isogeny of order 2, the simplest of which is "taking the inverse", that is, multiplication by -1. It is simple to check that this gives rise to a dihedral structure. This follows from the fact that for $Q \in E(\mathbb{Q})$ we have that:

$$-(-Q + P) = Q - P = Q + (n-1)P.$$

In the language of semi-direct products, we see that "taking the inverse" acts on "translation by P" by -1. A useful thing to remember is that for an E in Weierstrass form and a point $(a, b) \in E(\mathbb{Q})$ we have that $-(a, b) = (a, -b)$. How can we get a Galois extension from this, and what is its polynomial?

8.2 Theory

To find a field extension, we first must deal with fields, not groups. Therefore we begin by introducing the notion of a function field of an Elliptic curve. For an elliptic curve E, we have that its function field $\mathbb{Q}_E(x, y)$ is all the rational functions in two variables such that x and y satisfy the equation of E. Formally we say:

Definition 23. *Let E be an elliptic curve over $\mathbb{Q}$. Then the **function field** $\mathbb{Q}_E(x, y)$ is all the rational functions contained in $\mathbb{Q}(x, y)$ but restricted to the points of $E(\mathbb{Q})$.*

In practice we drop the E in the notation and simply write that the function field of E is $\mathbb{Q}(x, y)$. As an example, consider $E : y^2 = x^3 + 1$ then the polynomial $g(x, y) = y^2 - x^3 - 1$ is identical to the polynomial $h(x, y) = 0$ in $\mathbb{Q}(x, y)$. In fact, as it is shown in this webpage[1] any rational function can be expressed as $a(x) + yb(x)$ with $a(x), b(x) \in \mathbb{Q}(x)$ by simply substituting the equation defined by the elliptic curve E enough times.

Of course, by its very construction, the field $\mathbb{Q}(x, y)$ is closely related to E. For an elliptic curve, E with a point P of order n, $\mathbb{Q}(x, y)$ will be precisely the field we will be extending into. What is the base field? It is helpful to go in steps.

First, we need to find a field where "translation by P" leaves the field intact. In this case, we can remove P from our elliptic curve. Of course, just doing $E(\mathbb{Q}) \cap \langle P \rangle$ will not work. The resulting intersection is not even a group. In this case we can use Velu's formula from [23] in order to get an isogeny ϕ from E to another E' such that $\ker \phi = \langle P \rangle$, to the new E' we associate a function field $\mathbb{Q}(X, Y)$. It follows that in this case, E' is invariant under "translation by P" since for $Q \in E'(\mathbb{Q})$ we have that:

$$\phi(Q + P) = \phi(Q) + \phi(P) = \phi(Q) + O = \phi(Q).$$

Since ϕ is already given in the form of $(x, y) \mapsto (r(x), yh(x))$ it can naturally be extended to the function fields. In particular it takes $a(x)+yb(x) \in \mathbb{Q}(x, y)$ to $a(r(x))+yh(x)b(h(x))$ which is by construction an element of $\mathbb{Q}(X, Y)$, the function field of E'.

We focus now on E' and it's function field $\mathbb{Q}(X, Y)$. Since E' is also in Weierstrass form, we have that "taking the inverse" takes $a(X) + yb(X)$ to $a(X) - yb(X)$. It follows that if we only consider $\mathbb{Q}(X) \subset \mathbb{Q}(X, Y)$ such field is invariant under "taking the inverse".

Remark 37. *From the above, it follows that the isogeny ϕ determines an isomorphism between the function field of the new elliptic curve into which we are mapping and the subfield of the original function field invariant under translation by P. Therefore we say that $\mathbb{Q}(X, Y) \simeq \mathbb{Q}(r(x), yh(x))$. For the continuation of the section we will only consider $\mathbb{Q}(r(x), yh(x))$.*

Now we need to find the polynomial that determines the extension $\mathbb{Q}(r(x))$ to $\mathbb{Q}(x)$. For this, we state a simple lemma.

Lemma 14. *Given a field extension from $K(k)$ to $K(t)$ such that $k = \frac{a(t)}{b(t)}$ for a field K and $a(t), b(t)$ polynomials in $K[t]$ such that they are coprime. We have that the minimal polynomial of t in $K(k)[x]$ is:*

$$p(x) = a(x) - kb(x).$$

Proof. Since $k = \frac{a(t)}{b(t)}$ then $a(t) - kb(t) = 0$ and hence t is a zero of $p(x)$. We note that $p(x)$ is also a polynomial in $K[k][x] = K[x][k]$. The polynomial has degree 1 in $K[x][k]$ and hence it is irreducible. Furthermore since $a(x)$ and $b(x)$ are coprime, we cannot reduce the polynomial anymore. Therefore the polynomial is irreducible and since t is a zero of it, it is the minimal polynomial of t in $K[k][x]$.

■

Remark 38. *This implies that the minimal polynomial of x in $\mathbb{Q}(r(x))[X]$ is simply:*

$$p(X) = numerator(r(X)) - r(x) \cdot denominator(r(X)).$$

We know to show how this polynomial can be used to find a dihedral Galois extension.

Lemma 15. *The extension $\mathbb{Q}(x)$ of $\mathbb{Q}(r(x))$ is not Galois for $n > 2$.*

Proof. We know that $Gal(\mathbb{Q}(x,y)/\mathbb{Q}(r(x))) \simeq D_n$. Then $\mathbb{Q}(x)$ is the intermediate field invariant under σ, that is taking the inverse. Since $\langle\sigma\rangle$ is not normal for $n > 2$ then by the inverse Galois theorem it is not Galois over the base field. That is $\mathbb{Q}(x)$ is not Galois over $\mathbb{Q}(r(x))$.

■

Remark 39. *This implies that the minimal polynomial we found for x in $\mathbb{Q}(r(x))$ does not have all its roots in $\mathbb{Q}(x)$. We now ask for the Galois closure for such field extension, that is, the field extension of $\mathbb{Q}(r(x))$ generated by the minimal polynomial we found.*

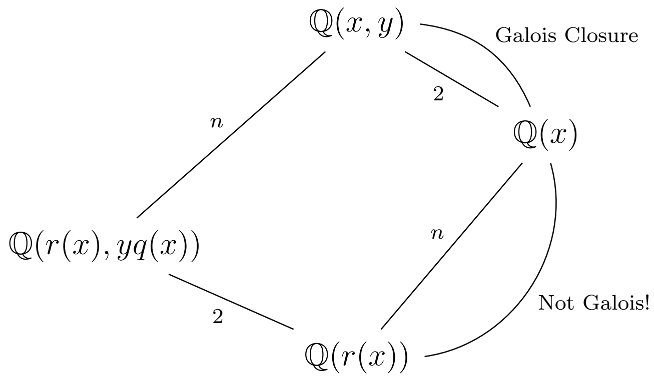
Lemma 16. *The field $\mathbb{Q}(x,y)$ is the Galois closure of the extension of $\mathbb{Q}(x)$ over $\mathbb{Q}(r(x))$.*

Proof. We know that $\mathbb{Q}(x,y)$ is Galois over $\mathbb{Q}(r(x))$ and we know that $\mathbb{Q}(x,y)$ is an extension of degree two over $\mathbb{Q}(x)$, namely for y satisfying the equation of the elliptic curve. Since all extensions are of degree 2 or higher, $\mathbb{Q}(x,y)$ is the smallest extension of $\mathbb{Q}(x)$ possible since it is already Galois, that is, the Galois closure.

■

Remark 40. *To illustrate this last lemma consider $\mathbb{Q}$ and the polynomial $X^3 - 2$. Then $\mathbb{Q}(\sqrt[3]{2})$ is an extension of $\mathbb{Q}$, but it is not Galois, since it is not generated by a polynomial. Namely, there is no polynomial in $\mathbb{Q}[x]$ such that $\sqrt[3]{2}$ is a zero and all the other zeros lie in $\mathbb{Q}(\sqrt[3]{2})$, hence the Galois closure is $\mathbb{Q}(\sqrt[3]{2}, -\frac{1}{2} - i\frac{\sqrt{3}}{2})$. In fact $Gal(\mathbb{Q}(\sqrt[3]{2}, -\frac{1}{2} - i\frac{\sqrt{3}}{2})/\mathbb{Q}) \simeq D_3$.*

Therefore for an elliptic curve E with a point of order n, we can create an extension $\mathbb{Q}(x,y)$ of $\mathbb{Q}(r(x))$ with dihedral Galois group and find the polynomial that generates this extension. We can now apply Theorem 1 and pick almost any specialization $r(x) \in \mathbb{Q}$ to find an explicit Galois extension of $\mathbb{Q}$ with a dihedral Galois group. Graphically we can represent the whole story as:



8.3 Examples

We will now use all the above to find a polynomial f that realizes D_{12} over $\mathbb{Q}$.

Using Lemma 5 we find that $E : y^2 = x^3 - 33339627 * x + 73697852646$ has a point of order 12. That is $P = (-4533, -362880)$.

Using Theorem 5 we find that the isogeny α with kernel $\langle P\rangle$ such that $x \mapsto \frac{a(x)}{b(x)}$. And hence using Lemma 14 we find the following polynomial which we can specialize for almost any $k \in \mathbb{Q}$ to realize D_{12} over $\mathbb{Q}$:

$$
\begin{aligned}
p(x,k) = {} & x^{12} - 32937x^{11} + 1011647295x^{10} - 11733790286799x^{9} + 27782194869630090x^{8} \\
& + 5008596999778497121 02x^{7} - 518540832707432765877145 8x^{6} + 2463361190597513295234489760 2x^{5} \\
& - 760150132057270732694692680763 47x^{4} + 18180189018199766976984066051746 4915x^{3} \\
& - 34840609977040099427743545081067177 1373x^{2} + 44624950005495789760425060656997621871 7949x \\
& - 2614811654910355043459550820560096058 91719584 \\
& - k(x^{11} - 32937x^{10} + 375230943x^{9} - 1259120668815x^{8} - 7692611128393302x^{7} \\
& + 7627572599713690339 8x^{6} - 1767425581733408352442 26x^{5} - 403331918837306576020931646x^{4} \\
& + 30952470014897013612867313177 65x^{3} - 6981291834207905731725051152397741x^{2} \\
& + 72083264343024182320000385228323223 55x - 28847919344152269461940872495965296654 75)
\end{aligned}
$$

Similarly, we can find a polynomial for D_9.

$$
\begin{aligned}
p(x,k) = {} & x^{9} - 648x^{8} + 685260x^{7} - 82528632x^{6} - 16669414602x^{5} + 3739189115304x^{4} \\
& - 190196095139028x^{3} + 7845192239384952x^{2} - 108446199923644 1775x \\
& + 522053019456935048 64 - k(x^{8} - 648x^{7} + 86508x^{6} + 14212584x^{5} - 2777940522x^{4} \\
& - 12149449848x^{3} + 18748258502796x^{2} - 810662163391080x + 9704892934962225)
\end{aligned}
$$

8.4 Using a Theorem by Williamson

It follows from Theorem 4 that using this method we can only realize some dihedral groups, that is $D_4, D_5, \dots D_{10}$ and D_{12}. Nevertheless, we could potentially find other realizations of dihedral groups using Theorem 2.

For example after we have specialized $r(x)$ with a suitable element in $\mathbb{Q}$ then the following extension:

$$
\begin{array}{c}
\mathbb{Q}(r(x), yh(x)) \\
{\scriptstyle 2}\Big| \\
\mathbb{Q}(r(x))
\end{array}
$$

Becomes $\mathbb{Q}(\xi)$ over $\mathbb{Q}$, where the minimal polynomial of ξ is simply the equation of the elliptic curve we mapped into with our isogeny that had a kernel of order n.

For example we could consider D_{12} and D_7 and in this way realize D_{84}. Unfortunately, it turns out that finding a common quadratic extension is harder than expected. Consider for example an elliptic curve $E : y^2 = x^3 + ax + b$. In the case above when we specialize $r(x)$ we specialize the x of this variable. It follows that the minimal polynomial of y in $\mathbb{Q}$ become $t^2 - (x^3 + ax + b)$ and hence we have dealing with the quadratic extension $\mathbb{Q}(\xi)$ for $\xi = \sqrt{x^3 + ax + b}$. Similarly for another extension we could have another $\Xi = \sqrt{X^3 + AX + B}$. We now require as per Theorem 2 that $\xi\Xi \in \mathbb{Q}$. Hence $(x^3 + ax + b)(X^3 + AX + B)$ is a square. In the case for D_{12} as presented above and in the case for D_7 as presented in the appendix we find that the equation is:

$$(x^3 - 3215421377x - 73335132522234)(X^3 - 275643X - 61114986).$$

It should now be clear that this is hard to do in general. Despite our best effort, we did not find any pair $x, X \in \mathbb{Q}$ such that the above expression is a square.

9 Method by Complex Multiplication

This section presents a possible method for realizing dihedral Galois groups over $\mathbb{Q}$. Using a very recent result by Lozano [13] we will show that this method will not give any dihedral Galois group.

9.1 Motivation

In the previous section, we had luck with torsion points, but we were stopped by the fact that on $E(\mathbb{Q})$, we can only find n-torsion points for only certain n. In Theorem 6 we stated that $E[n] = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and therefore it is generated by two elements.
What looks even more promising is that Tiesinga in his bachelor thesis[19] showed that in the case E has the endomorphism ring isomorphic to $\mathbb{Z}[i]$, we have that:

$$Gal(\mathbb{Q}(E[p])/\mathbb{Q}) \simeq C_2 \ltimes C_{p^2-1}.$$

9.2 Some Prerequisites

In order to state a result we need in the following part, we, unfortunately, need to provide a few definitions. A full explanation of which and their motivation would be beyond the scope of this short thesis. Except for a simple connection between inert primes and discriminant, all three definitions will not be particularly relevant and will not be used in the following proof. We nevertheless present them for completeness's sake.

Definition 24. *Let $\mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic extension with integer ring $\mathbb{Z}[\omega]$. Let f be an integer. Then the order of $\mathbb{Q}(\sqrt{-d})$ of* ***conductor*** *f is $\mathbb{Z}[f\omega]$.*

Definition 25. *Given an imaginary quadratic extension $\mathbb{Q}(\sqrt{-d})$ with $d > 0$ square-free with discriminant Δ, we say that a prime p is* ***inert*** *if and only if Δ is not a square of p. Using the Legendre symbol we have $(\frac{\Delta}{p}) = -1$.*

9.3 Theory

We will now see that although $Gal(\mathbb{Q}(E[n])\mathbb{Q})$ looks promising, it is not the case that it is a dihedral group. Let E be an elliptic curve with complex multiplication. Let Δ be the discriminant of the field such that the ring of endomorphisms of E is isomorphic to the order of conductor f, that is, to $\mathbb{Z}[f\omega]$. Define now $\delta = \frac{\Delta f^2}{4}$. From Lozano, we have the following theorem[13].

Theorem 8. *With the above notation. The Galois group of the extension $\mathbb{Q}(E[p])$, for p odd and inert in the endomorphism ring of E which allows for complex multiplication, over $\mathbb{Q}$ is contained in:*

$$N = \left\langle C, \sigma = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \right\rangle.$$

with $C = \left\{ \begin{bmatrix} a & b \\ \delta b & a \end{bmatrix} : a, b \in \mathbb{F}_p, a^2 - \delta b^2 \in (\mathbb{Z}/p\mathbb{Z})^\times \right\}$.

We state now our theorem.

Theorem 9. *With the notation above, we have that σ acts on the elements of C through the Frobenius map.*

Before we state the proof, we make a few observations.

Remark 41. *The constraints we have put on our choice of a, b are equivalent to requiring that the matrix has a non-zero determinant. Therefore since p is prime, we have that C has order $p^2 - 1$. Furthermore, each matrix is uniquely determined by our choice of a and b.*

Notice that $F_{p^2}^\times$ has also order $p^2 - 1$. We claim that there is an isomorphism between $\mathbb{F}_{p^2}^\times$ and C. We have already determined that C is uniquely determined by our choice of $a, b \in \mathbb{F}_p$. To make the isomorphism more explicit we need a basis of $\mathbb{F}_{p^2}$. We pick basis $1, \sqrt{\delta}$. Indeed $\delta^2 \in \mathbb{F}_p$. Furthermore $\delta \notin \mathbb{F}_p$ since by our choice of p we have that Δ is not a square. This means $1, \sqrt{\delta}$ span $\mathbb{F}_{p^2}$.

Lemma 17. *With the notation as above $\mathbb{F}_{p^2}^\times \cong C$. The explicit isomorphism is given by:*

$$\Phi : a + b\sqrt{\delta} \mapsto \begin{bmatrix} a & b \\ \delta b & a \end{bmatrix}.$$

Remark 42. *We also note that taking the norm of an element of $\mathbb{F}_{p^2}$ is the same as taking the discriminant on the elements of C. This is the case since $|a+b\delta| = (a+b\delta)(a+b\delta)^p = (a+b\delta)(a-b\delta) = a^2 - b^2\delta$. The equality $(a+b\delta)^p = a - b\delta$ follows by noting that $\mathbb{F}_{p^2}$ is of characteristic p and that the Frobenius map fixes the elements of $\mathbb{F}_p$ but does not fix all elements of $\mathbb{F}_{p^2}$.*

We are now ready to prove Theorem 9.

Proof. With the notation as defined above. We begin by noting that:

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ \delta b & a \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ -\delta b & a \end{bmatrix}.$$

Therefore by Lemma 17 we are sending $a + \delta b$ to $a - \delta b$, which we saw in Remark 42 to be the Frobenius map. This concludes the proof. ∎

Remark 43. *This implies that for $\tau \in C$ we have that $\sigma\tau\sigma = \tau^p$ if p is an inert prime. We also noted that C is or order $p^2 - 1$. Therefore if we want to have that σ acts by the dihedral property we have that $\tau^p = \tau^{-1}$ which implies that $p = p^2 - 2$, but that is not the case for any odd prime p. We conclude that in the case $Gal(\mathbb{Q}(E[p])/\mathbb{Q}) \simeq N$ it is not a dihedral Galois extension.*

10 Method by Class Group

This section presents the third and last method we used to realize dihedral Galois groups. The fact that one can use the Hilbert class field to realize dihedral Galois groups is a direct consequence of the ideal class theory, as we will see in this section. Nevertheless, computing the polynomials associated with these extensions is not that simple. The method we present is from "Explicit Construction of the Hilbert Class Fields of Imaginary Quadratic Fields by Integer Lattice Reduction" by Kaltofen and Yui[11].

10.1 Theory

Given an imaginary quadratic extension $\mathbb{Q}(\sqrt{-d})$ with $d > 0$ square-free, we have seen that we can construct an extension H, called the Hilbert class field, such that the Galois group is isomorphic to the ideal class group of the ring of integers of $\mathbb{Q}(\sqrt{-d})$. Let now, $\mathbb{Z}[\omega]$ be the ring of integers and $\mathbb{Z}[\omega]/\sim$ the ideal class group. Now consider a special case, let $\mathbb{Z}[\omega]/\sim$ be cyclic of order n. Then we have the following tower of extensions:

$$\begin{array}{c} H \\ {\scriptstyle n}\big| \\ \mathbb{Q}(\sqrt{(-d)}) \\ {\scriptstyle 2}\big| \\ \mathbb{Q} \end{array}$$

We now show that the overall field extension is Galois with a dihedral Galois group.

Theorem 10. *With the above notation we have that $Gal(H/\mathbb{Q}) \simeq D_n$.*

Before we can prove this theorem, we need a technical lemma about the complex conjugation on j invariants.

Lemma 18. *Let I be an ideal of an integer ring $\mathbb{Z}[\omega]$ then $\overline{j(I)} = j(I^{-1})$.*

Proof. Let $I = (a, b)$ with $a \in \mathbb{Z}$, then without loss of generality let $j(I) = j(\frac{a}{b}) = j(\tau)$. Then using the q-expansion of the j-invariant for $q = e^{2\pi i\tau}$ we have that:

$$j(\tau) = q^{-1} + 744 + 19688q + \dots$$

We note that for $\tau = a + bi$ we have that $q = e^{2\pi ia}e^{-2\pi b}$.
So that $\overline{q} = e^{-2\pi ia}e^{-2\pi b} = e^{2\pi i(-a+bi)} = e^{2\pi(-\overline{\tau})}$.
We have already noticed in the proof of Lemma 8 that for $I = (a, b)$ with $a \in \mathbb{Z}$ we have that $I^{-1} = (a, \overline{b})$ and hence since -1 is a unit we have that $I^{-1} = (a, -\overline{b})$ which indeed has j-invariant $j(-\overline{\tau})$ as desired. ∎

Proof. First, we show that the extension H over $\mathbb{Q}$ is Galois. This follows from Lemma 13 where we stated that there exists a minimal polynomial of the j-invariants of the ideal class groups. Therefore, since all j-invariants share the same minimal polynomial, we can think of H as the extension of $\mathbb{Q}$ by the minimal polynomial of one class group.

Now we show that the Galois group is as desired. By Lemma 1 we have that:

$$Gal(H/\mathbb{Q}) \simeq Gal(\mathbb{Q}(\sqrt{-d})/\mathbb{Q}) \ltimes Gal(H/\mathbb{Q}(\sqrt{-d})).$$

Since $\mathbb{Z}[\omega]/\sim$ is cyclic we let it be generated by an element I, which means that $Gal(H/\mathbb{Q}(\sqrt{-d}))$ is generated by θ_I. Then we verify that for any $j(J) \in H$ we have:

$$\sigma \circ \tau_I \circ \sigma(j(J)) = \sigma \circ \tau_I(j(J^-1)) = \sigma(j(I^-1J^-1)) = j(IJ) = \tau_{I^-1}(J) = \tau^{-1}(J).$$

Where we used Lemma 18 and Definition 22 of the Artin map. We conclude that the semi-direct product is the same as the semi-direct product of a dihedral group of order $2n$, namely $Gal(\mathbb{Q}(\sqrt{-d})/\mathbb{Q})$ or order 2 acts by -1 on $Gal(H/\mathbb{Q}(\sqrt{-d}))$ of order n.

■

Remark 44. *From Lemma 13 we know that the polynomial determining the field extension from $\mathbb{Q}$ to H has integer coefficients and is $\prod_{I\in\mathbb{Z}[\omega]/\sim}(x - j(I))$. Therefore following Kaltofel and Yui, we find a way of computing it[11]. We can compute $j(I)$'s to a good enough precision and from there estimate the coefficients of $\prod_{I\in\mathbb{Z}[\omega]/\sim}(x - j(I))$, knowing that they must be integers we can round them to the nearest integer. Given that we computed the $j(I)$'s precisely, the rounding will give the correct integer.*

10.2 Example

We want to find a polynomial to realize D_{11}, as it is the smallest dihedral group we did not realize so far. We let $d = 167$. We know from theory that it has a class group of order 11. Therefore it must be $\mathbb{Z}/11\mathbb{Z}$ since it is abelian. We can now compute the reduced binary quadratic forms using Lemma 11.

a	b	c	I
1	1	42	$(2, -1 + \sqrt{-167})$
2	± 1	21	$(8, \mp 1 + \sqrt{-167})$
3	± 1	14	$(18, \mp 1 + \sqrt{-167})$
6	± 1	7	$(72, \mp 1 + \sqrt{-167})$
4	± 3	11	$(32, \mp 3 + \sqrt{-167})$
6	± 5	8	$(72, \mp 5 + \sqrt{-167})$

Then we can compute the polynomial $\prod_{I\in\mathbb{Z}[\sqrt{-167}]/\sim}(x - j(I))$ to be:

$$\begin{gathered}
x^{11} + 428181809075068500x^{10} - 31044384829443550596875 0x^9+ \\
18333989555607357095852154557812500 0x^8- \\
1326537753099406348444543069796193847656 25x^7+ \\
99968421621214354876138160879405119659423828125x^6+ \\
3228424186003694107655062744056610278450012207031250x^5+ \\
549483427443181673778849396297643559590511322021484375 00x^4- \\
191958603447999118217843290597001892823611319065093994140625x^3+ \\
1237516544134781800061438580917239295417235270142555236816406 25x^2+ \\
41726839319627438364938202440270256635260256938636302947998046875x+ \\
303375885640623735763330301476291089935190830146893858909606933 59375
\end{gathered}$$

Remark 45. *Despite being very large, computing such polynomial does not take a long time on modern machines. In this case, the computational time was 10ms.*

Remark 46. *Although this polynomial realizes D_{11}, we immediately see that the coefficients of the polynomial are large and hence tricky to deal with. Kaltofen and Yui present a method in order to reduce the coefficients of the polynomial while maintaining the same Galois group [11].*

Remark 47. *It is still an open problem which abelian groups can occur as the ideal class group of imaginary quadratic fields, although it seems that one would sooner run out of computing power rather than find a cyclic group which is not an ideal class group. Furthermore, Ishibashi provided a sufficient condition for it to be the case when the order of the ideal class group is not prime[9]. Both final remarks could form a basis for another bachelor thesis on the matter.*

11 Conclusion

In these short notes, we explored the explicit realization of dihedral Galois groups over $\mathbb{Q}$. Although it is already known that such groups are realizable over $\mathbb{Q}$, realising them is still a non-trivial task. We attempted to find such dihedral groups using three distinct methods, for which we proved why or why not they would not be successful. We also provided a theorem that given two dihedral groups D_n and D_m realized over $\mathbb{Q}$ with m and n co-prime gives us a way of realizing D_{mn}, for which we were not able to provide examples.

11.1 Acknowledgments

I want to thank my supervisor Jaap Top, without whom this thesis would not be possible. And Roy Rodenburg, Elia Chimenti, Viktor Vesely and Hana Glumac for helping me along the way.

A More Polynomials With Dihedral Galois Group over $\mathbb{Q}$

We provide a list of polynomials such that their splitting field has a Galois group isomorphic to D_n.

A.1 Method by Torsion

In this case, the polynomials $p \in \mathbb{Q}[x, k]$ have a dihedral Galois group over $\mathbb{Q}(k)$.

A.1.1 n = 4

$$p(x,k) \;=\; x^4 - 9x^3 + 891x^2 + 459621x - 4455648 - k(x^3 - 9x^2 - 1701x - 22491)$$

A.1.2 n = 5

$$\begin{aligned} p(x,k) = x^5 - 60x^4 + 16902x^3 + 647460x^2 - 11799999x + 606411360 \\ - k(x^4 - 60x^3 - 1242x^2 + 64260x + 1147041) \end{aligned}$$

A.1.3 n = 6

$$\begin{aligned} p(x,k) = x^6 - 159x^5 + 92538x^4 + 8561106x^3 - 1018111275x^2 - 9289268163x - 1077720357600 \\ - k(x^5 - 159x^4 - 13734x^3 + 1624914x^2 + 98133525x - 308641347) \end{aligned}$$

A.1.4 n = 7

$$\begin{aligned} p(x,k) = x^7 - 162x^6 + 54999x^5 + 656100x^4 - 346007457x^3 \\ + 16047038142x^2 - 366043274775x + 8925096681504 \\ - k(x^6 - 162x^5 + 567x^4 + 726084x^3 - 10504161x^2 - 720988290x + 14468481225) \end{aligned}$$

A.1.5 n = 8

$$\begin{aligned} p(x,k) = x^8 - 597x^7 + 474525x^6 - 22473585x^5 \\ - 38171689101x^4 + 9351097332561x^3 - 1006441961594481x^2 \\ + 67204402984571445x - 2403712209857218272 \\ - k(x^7 - 597x^6 + 57213x^5 + 20869839x^4 \\ - 3372634989x^3 - 110102053167x^2 + 36413799008175x - 1392079585876875) \end{aligned}$$

A.1.6 n = 9

$$\begin{aligned} p(x,k) = x^9 - 648x^8 + 685260x^7 - 82528632x^6 - 16669414602x^5 + 3739189115304x^4 \\ - 190196095139028x^3 + 7845192239384952x^2 - 108446199236441775x \\ + 522053019456935048 64 - k(x^8 - 648x^7 + 86508x^6 + 14212584x^5 - 2777940522x^4 \\ - 12149449848x^3 + 18748258502796x^2 - 810662163391080x + 9704892934962225) \end{aligned}$$

A.1.7 n = 10

$$
\begin{gathered}
p(x,k) = x^{10} - 1395x^{9} + 3047652x^{8} - 934757820x^{7} - 199488386466x^{6} \\
+ 109417350553110x^{5} - 6274406969713548x^{4} - 801258575698323180x^{3} \\
-11113611645444414767 1x^{2} + 252528531556264337344 05x - 10695688573945458164656 32 \\
- k(x^{9} - 1395x^{8} + 453060x^{7} + 88252740x^{6} \\
- 47384507682x^{5} + 541704904470x^{4} + 1114874748207540x^{3} - 75861292413416940x^{2} \\
+ 425026691914714281x - 6224624912048460 75)
\end{gathered}
$$

A.1.8 n = 12

$$
\begin{gathered}
p(x,k) = x^{12} - 32937x^{11} + 1011647295x^{10} - 11733790286799x^{9} + 27782194869630090x^{8} \\
+50085969997784971210 2x^{7} - 518540832707432765877145 8x^{6} + 24633611905975132952344897602x^{5} \\
- 76015013205727073269469268076347x^{4} + 1818018901819976697698406605174649 15x^{3} \\
-34840609977040099427743545081067177137 3x^{2} + 44624950005495789760425060656997621871794 9x \\
- 26148116549103550434595508205600960589171958 4 \\
- k(x^{11} - 32937x^{10} + 375230943x^{9} - 1259120668815x^{8} - 7692611128393302x^{7} \\
+76275725997136903398x^{6} - 176742558173340835244226x^{5} - 4033319188373065760209316 46x^{4} \\
+ 30952470014897013612867313177 65x^{3} - 69812918342079057317250511523977 41x^{2} \\
+72083264343024182320000385228323223 55x - 28847919344152269461940872495965296654 75)
\end{gathered}
$$

A.2 Method by Class Group

Given the size of the coefficient of polynomials that we find with this method, we present them in a slightly unusual way. In particular, they are presented as a list, in which the first element is the constant coefficient, the second one is the coefficient of degree 1, and so on.

A.2.1 n = 3

$$
\begin{array}{l}
12771880859375 \\
-5151296875 \\
3491750 \\
1
\end{array}
$$

A.2.2 n = 4

$$
\begin{array}{l}
-208929750630400000000000 \\
-31850703872000000000 \\
-75843692160000000 \\
-178211040000 \\
1
\end{array}
$$

A.2.3 n = 5

$$
\begin{array}{l}
16042929600623870849609375 \\
-14982472850828613281250 \\
5115161850595703125 \\
-9987963828125 \\
2257834125 \\
1
\end{array}
$$

A.2.4 n = 6

$$
\begin{array}{l}
549806430204864490157810211109208064 \\
432181202257616392838287353464320 \\
497577733884372638735595703120 \\
28321090578679361484375000 \\
85585228375218750 \\
5321761711875 \\
1
\end{array}
$$

A.2.5 n = 7

$$
\begin{array}{l}
737707086760731113357714240894402560 \\
-425319473946139603274605151263232 \\
5138800366453976780323726329184 \\
-823534263439730779968091389 \\
98394038810047812049302 \\
-3091990138604570 \\
313645809715 \\
1
\end{array}
$$

A.2.6 n = 8

$$
\begin{array}{l}
107789694576540010002976772007214029511589888 \\
2110631639116675267953915424895605508407296 \\
-1437415939871573574572839011043808116736 \\
352163322858664726762725228310167552 \\
-13089776536501963407329479984464 \\
395013575867144519258203125 \\
-688170786018119250 \\
19874477919500 \\
1
\end{array}
$$

A.2.7 n = 9

607371299984970035446600042273714235270815762662178845150412 8

$-2626485656349386308710549909704194559303008333786595616358 4$

81311504213341585710631261057125322964037498479549874176

$-15361831050875895680622837467354104376002875070873600$

9346828488034341558973586625189893912638877859 84

23969299805117437326359388515618137342738432

311741055246397228842310784101128339456

13313031001892568168374 34

17656190279770938660

1

A.2.8 n = 10

$-11669920442373800031513478208250726083599525972874887168$

346485626218561739292181172701303261671192813805502464

$-29222392883084871101102263776408995466489556579123 2$

29494022920507896313766601310443791747655925760

124806112558095456896271445409846622253219 84

4794937071328670764609540039305206956032

$-528557124686794965810654876920709 12$

585035810262130969538043606625

-70241355662808988599

764872171216961

1

A.2.9 n = 11

30337588564062373576333030149520883764735773966310862366567603109888

41726839319627438364938202443143299216465026155700915835378860032

1237516544134781800061438581086822693407348310594687322942341 12

$-19195860344799911821784329061668874609291766881316946889932 8$

549483427443181673778849396348028588349336145080583454 72

3228424186003694107655062744250732327523958701162496

99968421621214354876138160881646311586287058944

$-132653775309940634844454306980010032889856$

183339895556073570958521545575890944

$-310443848294435505968750$

428181809075068500

1

A.2.10 n = 12

16954979143612226905161985598903623567772157572066530152382043382674324831726062628188979200
−111911641881180244275001821733054793970279480270202377121098750429934009326621095488389 12
20058565362820886465850364874298186526812569410126144491424470447492986345819356528640
−48170352187674846943319058413567236391223868212468492779569384911113940902084608 00
1499739139222507371812925435620730633956537034169808612954297067541185890877440
−378814746857953498319330657232485655846471797909509880302313058547489832 96
79847153885444868834050330056045880279907537107532227522971797521694 72
77340437008401154333774866162435332708919329197337708457340436 48
374833189994697125435526419953847852531919718867847557939 2
22101453729906995739871545203239112190925270417408
7973037576426163375730622291087 36
4701218323824481581438750
1

A.2.11 n = 13

58256749348304523248144969890943054324034804984298325800424301591359973694111744
42312753036411362230230450306128701068251802370182332065037512623919143583744
14061234326903814621176226215386334162749379582571874782367817427213877248
−4937591170791174343291724220703527700323324673039671557510052250753433 6
15253788701960481284921391492838584837268492866659324375332512858112
−832818220571586800392164743938246660084961402238840236427706368
541808230910284083390456000822488450309777105998875761573888
−1476863840583089413497242762110173295631883721625514803 2
199518440359885837424153227308464475949688588075008
−103386239396269087020741974277059248094445568
51536266750679803854633551768454168576
−14412129900790076822258611
7178874489555770070
1

A.2.12 n = 17

21993600315997864678504669495637412212841409746517019162958019599571371812082411024819781593317408046584226434695986937856 0
54285333609308942748141803126320839249632609812487671782679057108040306585649781982044273145844047152362908846361935872
76560383006298213692539215495857172958731737718361632590501351351506755207758915370005451884724540380918288011283660 8
−62577470793580318723162040554059395531990543135926077584577896472842169302190331160284425033531885939379800742297 6
17118993554590300678468628159890655170969716905703902159985718279191754291492920316222317770417890861481616998 4
−21240446733558728423120402042063718756449226063275747996444885888409931584306867070206585657974683642888192
20177680095555311718569209800916156065242891273171412525713088454310142838575148299053071322895446179 84
29783683905531251952444306144294689251371977508279611181718581471045279665236932810243304249622528
−24714457406921470525240049321805332397466248164239679440282961678336085188708934185138603950 08
−45196937703500115295789585554822747831745471068596170127028274552576147768943291555381248
35982633518681366681328465631217224231715922621711523226645693182215021818220327731 20
−107713688824621483558057951997885828020118064733593262814227306541261682376704 0
161118450982562226625664238786114536405174149699261290453626531329605632 0
−202698793039733837552369176832131233378298180004936994131017728
25278029570823933439072444650838137554800714715234304 0
−403162713488260150493480012932448256
502772608032346430357516125
1

A.2.13 n = 19

167619627859809778456593134715651393507100238156365133719421275161141918666134069674129459872444170988518791349840904192

−14033327386253215663069650054262500988384417689643707568143334071152766728059872935731614977225450960483339107670425600

8653188131073657534659971312549882617050407818503423935724804571325112134231141551922006057496931901966153727082496

−6380671474022520186865342133399519414700289684069488171926882119826050576858267442157004178272115113335753539584

1636564533180350518985887758814189528639026132885562477749516100713376242319934341682331784942841722329628672

−280368723199023212452013447871230515128123133713295470088912543354008545703058505959553368370546848301056

691825491788183943812892962288979011993297668947791062695625913393627438514486677150095744051856801792

19869266968011330937247944616592966728366368875037696365175830053522523235189731257271712433045504

−6083156081341802828244370192556880642079959027491959644711230635582493052703549300508144435200

−293215182819796337555040025662804511382504833216930229979476194304545727854452599395713024

61158678932313320213787561385896460717956355784833296103381080721224001882081242120192

630554072611458034329952205100113951977619670177139694058375349955666702770372608

16388999625036382476760258838966329102859048350201036756651049374392537579520

21641001503579573253005919226352040295410207903820766639164805408096256

14340511511438590716588234840217155333526878499641655082442817536

−136828412090023608299771971693157439294307039113725870080

1324579917469218106400780032947227488047016706048

−118889488223763098576321565332864

1150903951252590564004008

1

A.2.14 n = 23

13789510352849843721059134371512089616572064913526314473359852283128999115406732371763602999805647157467869001987253927411407695775277166274094028390781070042530605907845316608
−366143212646540606431943435916184184777272025883922620145705792797076494861769717144038081661828603289550834598807399990595026134850411962248328318384341533100499585833369 60
−13209954437351304503271159367376830071730141106282973569585235785345160189737301194098631229573922858035834636560298741614304809745275992435014189837023896149773528124 6208
36357745705095988090771192583555017117755961882269504927468783992359592857960319962283032917174227049743876054696103994068748301973212095263438464137801039472427112857 6
27377023143026966392312937439045805048934464093671204363521225593987603464222374474124461617334505809237878791692593708486056862158517246079636835035794883925036236 80
−54685061104962891196094756154393780928887652516050448650035993196965580418445471685105794524298984708642922110192734882268153176934035827928513949747511044006215 68
35229065297629763633510985415161686668973472570215483298125561240483631485339095398814354877936662459727662837604213489815082998143846499510251246195755020451840
−53076875978062108305206049837211369821219439340680074846194762800219458530526201031315611923178101875818238210035448314028779707829207739576315775446679552 0
18687960354865385660880811166545849329885475112649483677031542705681081020000900725507638725840601814642907007985290029383160497291265716232968002443673 6
13265237054731200416875200336628708191326144249236933068053338113625345747323164678795985239865076111632739335032891932010202270042835635247933030 4
89167284712669400204970807271522472162897425827108957089177637883146093445820827819956325244038049773117987353283341388050186349448551209107456
11888179623966802877342168359568621222395992162779108905418219493055693948828859527192382909916086312774987314349310952437261399499116380 16
10583615922709183362724608419587507845834204028226110874521361179529651148685860403993257651750705648339546302142042360287933931454464
−31384006302417743337935538640695368293524152296808997817756131270731400564382095298767972803345522176375116884646119977600942 08
−28617933688863464374778474034201109229687376184278042551313824802428468464141111855279689125900294569013691260127883663769 6
83623636551363032600292985512758618141532546758141946928310932609370892631113715254287573465469393129176143778283 52
79041415394369981751769861986467241959664215479601621169252777352290288488302616761844441869880156695063166976
23538116358169603720577254557518886790331812201949657469173213426724347184921183449013422232996256153 6
350476734577200489933329091166215456144443530104225919976655045516376499390257376510934515712
−9472783821022183892463187715026134393140867679001734480294184422197449106936299 52
25649866968386987963279655798224205011367464380349940056711047225016 32
−187040247976303685075235591084439507929483182 08
5064569771295266328390701589299200 0
1

A.2.15 n = 31

In this case the arrows indicate an entire number. For example: $12 = 1 \rightarrow\leftarrow 2$.

1906892014817153746528474988912794545625599362647944049554554432029057470482685477191677277864939081456331283704→
← 516936357322617403754521558033172516963075746213873060081351591832171876678677408784458262792696108369628364 8
− 32793693512381646129547561835581514636568041220143215307980584625894586934317884752848129339796336195339459 9 →
← 173560877614778199316029915394242457878220900194615988489197969552952836900438297747738929467548540120843943936
257834638524243794028480660222981543040027147239794088845662468630764192399626391466811975172979805854670810114254098213 2 →
← 0118750031235950471956448667761173457936184516371365904723750360876256020881728854975488353894 40
−6494383215780670658021188361241370100013575164948259722138511891486328714223251102004265392728795141006704051104482650949500948171649901045479630074130348217177486567773454724533191071491348151696268827590872006656
9065649375833062118367716296402997736276119052727778770791900948889963656918901150953183643276693634993086958689267385720032082503676472471868504621237389525046421189734881389175859686096530057205278116589600768
−7878042909650477143342839936539879465285226727687382755957915646258423735237469947509021143215997981224202096754838290335316094911243445651015356512819831566936521288783056856417727514273207249916394060382208
3902729365738510741198182304936225919248660816647371171188807794139868905158985186667752689439908957402044661300964556326019402905973671974954585589310295732828642154543781068408163665043573761216402685952
−7009820531404658441410807463915539346977997426841151901999015037668179173116041789896347094486860474582438869425349186111430873858748165669217947632588885914483491234230396391007099710597313247649464 32
−2153229950800051507583813588957583157966717121930701171640960922316505701300619543543427366070097153730228239198451016895246774081733485302437529476918735686066736978160858458337348357195519806668 80
1025873163889254322319541222759201286742544721070516563786441756297554551682590555398665070590500413443425548936657306960597963934685023793880280279237790977912300629419137511705762707742098718 72
− 4254832950510867825343984896408427135500421295216953571347650824113809230808694040663669089424261677844932685543538202220361762975185000110307174654398062143128099072118135186981938580684 8
− 5661058386247733694440666541177041588319586803067533344079349656967174717809117361628760769622902013767484441075156322830006341200693429814103663846498975282703492663553122424978014837145 6
9564504471091320675730791455462220532104962146297520030221836903479998105761028874257268461466523620294963316979807385558483510337044532239489714920774172122122901981566505510869401 60
− 4411828462504858083624666683670866555260209742237590646794487800829425825818150815061702076925866130246589306137376450183782766623412749099624075279105650956647968129633403849932 8
− 1007452829929848696398960618769054497739339375081733423776081827918500756487690149864307073900609219395707891195722915074429135979121039501297146714311201010484246977735294976
7301293564024177570709403367844113737277623374524388560658274766787031966985918427919981157252138514284789830399940083823780967762826740271076117278847751265434238084710 4
1893515672890770843691749020587977760112596010328199894555496825793972401461102085621933762566965607926386191674763758067089637714765069723943170629482298247298940928
− 3418757395269791628423060534060342795146785646358174814304254341298716913821087697386907172653268180864037225311221933742046955245917640265031613794465601290240
7402715513336853555948366311128326825951225304662286485661194805912153699519258631464883755257295365736138948337651607623212834712591708243779161647847833 6
− 3678453328653878434542600060724247586048074876003689602389417022952941942137811496890577441158103417444850394712474488594440438668282328606985682944
− 4708603371097040534491446854959836915044546175704595608039126050784731978009628674412728013375349590825350543150850164316171360811613600664780 8
2320372166012477658368331614912678366704122100029755658062466710221090300519560997764960860943411098263247473946013308327903225079398400
3056074820489458270369010988690786939561490454541967715595104754669612170386142203716361098126456838094903485194863679943643391590 4
− 241784997195427513731698695807982933573330554818187887428285756531429800673489239819329453406779385627084574426935050685644 8
7343801016088987135604920159812465051242586739025075883767635000376401937066543162223687993381151021473945228830310 4
− 729905979583602516034174107317758423428345992461945692880980811891743989447166217859884919587867248946053 12
3627130145718047218959111656968272336197868082666560369367166126192895919893409313425554235038105 6
− 231572604225450479010405623408518633820947000479585935359476408991253280447401704816 64
1476568522374217900500091780910843950112562397982079469489116123977954099 2
− 602643361872681135028308402999559974368146830131 2
384261437353954889149029270958374912 0
1

B Overview of the Used Code

This appendix aims to go over the code used for the computations from the thesis. Instead of simply listing the code, we use this opportunity to provide some context for those who are unfamiliar with the MAGMA computing language.

B.1 Finding Galois Groups

We let K be a field and $f \in K[X]$ be a polynomial with zeros α_i. We want to know what is $Gal(K(\alpha_i)/K)$. Note that in this case, any polynomial will work. In this case, the code would look like this:

```
G:=GaloisGroup(f);
GroupName(G);
```

For example, for $X^2 + 1 \in \mathbb{Q}[X]$ we have:

```
P<x> := PolynomialRing(Rationals());
f := x^2 + 1;
G :=GaloisGroup(f);
GroupName(G);
```

Note that the function GaloisGroup() is not necessarily correct. In case one can check with GaloisProof(), one does so in the following way:

```
P<x> := PolynomialRing(Rationals());
f := x^2 + 1;
G,R,S:=GaloisGroup(f);
GroupName(G);
GaloisProof(f,S);
```

If we know that $f \in K[X]$ is irreducible, then another method used by Tiesinga in his bachelor thesis[19], is:

```
Q := Rationals();
Z<X> := PolynomialRing(Q);
A<a> := ext<Q|f>;
N := AutomorphismGroup(A,Q);
GroupName(N);
```

This method is slower than the previous one, but it has the benefit of working also for a tower of field extensions. In particular, we could have extended the field A further into a field B, the splitting field of another irreducible polynomial $g \in A[X]$ and then computed AutomorphismGroup(B, Q). Without knowing the minimal polynomial explicitly.

B.2 Elliptic Curves

Let $E : y^2 = x^3 + ax + b$ then one writes:

```
E := EllipticCurve([a, b]);
```

equivalently for a general $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ one writes:

```
E := EllipticCurve([a1, a2, a3, a4, a6]);
```

If we have a point $P \in E(K)$ with coordinates (x, y) we can represent it as:

```
P := E ! [x,y];
```

Note that the coordinates (x, y) need to be correct, or an error will follow. To compute all the points in $E(K)$ with torsion n, one asks:

```
G := TorsionSubgroupScheme(E, n);
Points(G);
```

Note that, for $Q \in E(K)$ if $2Q = O$, Q is also a point of torsion 4. In order to get the order of Q, one writes:

```
Order(Q);
```

In order to get the n-th division polynomial, one writes:

```
DivisionPolynomial(E,n)
```

If a polynomial ring were not declared beforehand, the polynomial would be in the variable \$.1.

B.3 Velu's Formula

Given an elliptic curve E and a point on it of order n, we can compute Velu's formula as follows:

```
Eprime, phi := IsogenyFromKernel(E, &*{(x-(n*P)[1]) : n in [1..Order(P)-1]});
```

Where phi will represent the isogeny and Eprime, the new elliptic curve we are mapping to. Note that since the kernel is in the form of a polynomial, we need to have declared a polynomial ring in x before invoking the IsogenyFromKernel() function.

B.4 Binary Quadratic Forms

In order to compute the reduced binary quadratic forms of the class group of $\mathbb{Q}(\sqrt{d})$ for $d < 0$ we can use:

```
Q := BinaryQuadraticForms(-167);
ReducedForms(Q);
```

We can then compute the minimal polynomial of $\mathbb{Q}(j(\Lambda), \sqrt{d})$ in the following way:

```
for a in Q do
    f := f*(x - jInvariant(a));
end for;
f;
```

Note that this will give a polynomial with coefficients in $\mathbb{Q}(i)$, which we need to be rounded to get the correct polynomial we are looking for. Recall that it has coefficients in $\mathbb{Z}$. Kaltofel and Yui propose a series of tests to check whether the resulting polynomial is likely the correct ones[11]. In particular, the discriminant should be a cube. We compute it as:

```
Discriminant(f);
```

MAGMA generally has enough precision for the resulting calculations to be correct. However, packages are available to increase the accuracy, although they cannot be installed in the online evaluator. In case PARI/GP is a valid alternative. Putting it all together, we get:

```
B := BinaryQuadraticForms(-167);
Q := ReducedForms(B);
P<x> := PolynomialRing(Rationals());
f := 1;
for a in Q do
    f := f*(x - jInvariant(a));
end for;
f;
A := Eltseq(f);
for a in A do
    r := Real(a);
    Round(r);
end for;
```

References

[1] Field of Rational Functions . `https://crypto.stanford.edu/pbc/notes/elliptic/funcfield.html`. Accessed: 2022-16-03.

[2] Andrew Sutherland. 18.783 Elliptic Curves: Lecture Notes 6, 2015. [Online; accessed 08-July-2022].

[3] J. H. S. (auth.). *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics 106. Springer New York, 1986.

[4] L. Chariker. The Inverse Galois Problem, Hilbertian Fields, and Hilbert's Irreducibility Theorem.

[5] D. A. Cox. *Primes of the Form $x^2 + ny^2$*. Pure and Applied Mathematics: A Wiley-Interscience Series of Texts, Monographs and Tracts. Wiley-Interscience, wiley edition, 1997.

[6] F. Dogger. Computing Class Numbers of Orders in Imaginary Quadratic Fields, 2019.

[7] T. W. Hungerford. *Algebra*, volume 73. Springer Science & Business Media, 2012.

[8] D. Husemoller. *Elliptic Curves*. Springer Verlag, 1987.

[9] M. Ishibashi. A Sufficient Arithmetical Condition for the Ideal Class Group of an Imaginary Quadratic Field to be Cyclic. *Proceedings of the American Mathematical Society*, 117(3):613–618, 1993.

[10] Jürgen Klüners, Gunter Malle. Missing Polynomials, Unknown Year. [Online; accessed 09-July-2022].

[11] E. Kaltofen and N. Yui. Explicit Construction of the Hilbert Class Fields of Imaginary Quadratic Fields by Integer Lattice Reduction. In *Number theory*, pages 149–202. Springer, 1991.

[12] D. S. Kubert. Universal Bounds on the Torsion of Elliptic Curves. *Proceedings of the London Mathematical Society*, 3(2):193–237, 1976.

[13] Á. Lozano-Robledo. Galois Representations Attached to Elliptic Curves With Complex Multiplication. *arXiv preprint arXiv:1809.02584*, 2018.

[14] S. Mac Lane and G. Birkhoff. *Algebra*, volume 330. American Mathematical Soc., 1999.

[15] B. Mazur and D. Goldfeld. Rational Isogenies of Prime Degree. *Inventiones mathematicae*, 44(2):129–162, 1978.

[16] J.-F. Mestre. Courbes Elliptiques et Groupes de Classes d'idéaux de Certains Corps Quadratiques. *Séminaire de Théorie des Nombres de Bordeaux*, pages 1–18, 1979.

[17] J. S. Milne. *Elliptic curves*. World Scientific, 2006.

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

[19] H. Tiesinga. The Inverse Galois Problem, 2016.

[20] J. Top. Group Theory.

[21] L. N. M. van Geemen, H. W. Lenstra, F. Oort, and J. Top. Advanced Algebraic Structures.

[22] L. N. M. van Geemen, H. W. Lenstra, F. Oort, and J. Top. Algebraic Structures.

[23] J. Vélu. Isogenies Between Elliptic Curves. Accessed: 2022-13-04.

[24] C. J. Williamson. Odd Degree Polynomials with Dihedral Galois Groups. *Journal of Number Theory*, 34:153–173, 1990.