university of groningen

faculty of science and engineering

mathematics and applied mathematics

Computation of polynomials generating abelian and $\mathrm{GL}_2(\mathbb{F}_p)$ extensions of $\mathbb{Q}$

Bachelor's Project Mathematics

June 2024

Student: K. Letiņa

Supervisor: Dr. T. Keller

First examiner: Prof. Dr. J. Top

Second examiner: Prof. J.S. Müller

Abstract

The Inverse Galois problem asks whether any finite group G appears as the Galois group of some Galois extension $L/\mathbb{Q}$. In this paper, we begin by proving that any finite abelian group appears as the Galois group of some intermediate field of a cyclotomic extension of $\mathbb{Q}$. Additionally, using elliptic curves and their p-torsion points, we prove this result for the groups $\mathrm{GL}_2(\mathbb{F}_p)$ as well. Lastly, we provide the necessary methods to compute polynomials in $\mathbb{Q}[X]$ generating these extensions.

Contents

1 Introduction

The field of Galois Theory arose in the 19th century to answer a question that was still open at the time - given a field K of characteristic 0 and $a_i \in K$, how to determine whether the equation

$$p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0 \tag{1}$$

can be solved by radicals?

Around 1700 B.C., Babylonians showed that all quadratic equations can be solved by radicals. The same was shown for cubic and quartic equations around the year 1500 in Italy. However, it was not until the 1820s that Abel and later Galois showed that it is impossible to solve a general quintic equation in a similar manner, by only using radicals. [Edw84, § 1-7]

With this motivation, Évariste Galois (1811 – 1832) established the field of Galois Theory to determine whether (1) can be solved by radicals by considering the splitting field L of $p(x)$ over K. As it turns out, the answer to the question lies in the properties of the field automorphisms of L that stabilize K. These automorphisms form a group, called the Galois group of L/K. More details of this will be covered in Section 2. Therefore, Galois theory provides a translation of problems in field theory to group-theoretical problems.

The Inverse Galois problem is concerned with the question of which finite groups occur as the Galois group of a Galois extension $K/\mathbb{Q}$. Therefore, while Galois theory investigates the Galois group of certain field extensions, the Inverse Galois problem works the other way. More insights about Inverse Galois Theory are covered in [MM18].

In this paper, we solve the Inverse Galois problem for two types of finite groups. The first of these is finite abelian groups, and to prove this result we work with cyclotomic extensions. We prove the result that any abelian group A appears as the Galois group of some intermediate field of a cyclotomic extension of $\mathbb{Q}$. Moreover, we also show that the extension can always chosen to be totally real.

The second type of group we consider are $\mathrm{GL}_2(\mathbb{F}_p)$ groups, which consist of invertible matrices of size 2×2 over the finite field $\mathbb{F}_p$. To show that these groups appear as Galois groups of some extension of $\mathbb{Q}$, we introduce elliptic curves and the concept of points of finite order on an elliptic curve. With this approach, we can establish what we will call the mod p Galois representation of an elliptic curve.

We conclude the sections regarding abelian and $\mathrm{GL}_2(\mathbb{F}_p)$ groups by computing the polynomials generating these extensions. This means that we will show how to find a polynomial $f \in \mathbb{Q}[X]$ such that the splitting field of f will have a Galois group isomorphic to our desired group.

2 Galois theory

In this section, we provide a brief introduction to Galois theory and the field theory prerequisites needed in this paper. Further details can be found in [Lan02].

2.1 Preliminaries

In this section we present the most fundamental background on Galois theory. We begin by stating the definition of Galois extensions.

Definition 1. *A finite field extension L/K is called a Galois extension if it is normal and separable.*

Note that in some sources, an alternative definition is that L/K is Galois if L occurs as a splitting field of a separable polynomial over K.

Definition 2. *The group of all K-linear automorphisms of the Galois extension L/K is called the Galois group* $\mathrm{Gal}(L/K)$ *of the field extension L/K.*

Now that we have established the definition of Galois extension and its corresponding Galois group, we lay out some crucial properties of Galois extensions. First, we describe the cardinality of a Galois group using [Lan02, § VI.1, Thm. 1.8].

Theorem 3. *Let L/K be a finite Galois extension. Then we have that*

$$\#\,\mathrm{Gal}(L/K) = [L : K].$$

Second, we can characterize the intermediate fields of a Galois extension with the following theorem from [Lan02, § VI.1, Thm. 1.10].

Theorem 4. *Let L/K be a Galois extension and let F be a subfield $K \subset F \subset L$. Then F is normal over K if and only if* $\mathrm{Gal}(L/F)$ *is a normal subgroup of* $\mathrm{Gal}(L/K)$*. If F is normal over K, then F/K is Galois and we have*

$$\mathrm{Gal}\,(F/K) \cong \mathrm{Gal}\,(L/K)\,/\,\mathrm{Gal}\,(L/F)\,.$$

Next we have to establish some integral properties of field extensions. First of these is the so-called Primitive element theorem from [Lan02, § V.4, Thm. 4.6].

Theorem 5 (Primitive element theorem)**.** *Let L be a finite extension of a field K. If L/K is separable, then there exists an element $\alpha \in L$ such that $L = K(\alpha)$.*

Second, we restate the well-known tower law from [Lan02, § V.1, Prop. 1.2].

Theorem 6 (Tower law)**.** *Let $K \subset F \subset L$ be a tower of field extensions. Then*

$$[L : K] = [L : F] \cdot [F : K].$$

Third, we need to define the concept of splitting fields from [Lan02, p. 235-236].

Definition 7 (Splitting field)**.** *Let K be a field and let f be a polynomial in $K[X]$ of degree ≥ 1. The splitting field of f over K is defined as the field extension L/K such that*

i. f splits into linear factors in L. In other words,

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

for $\alpha_i \in L$.

ii. $L = K(\alpha_1, \ldots, \alpha_n)$ is generated by all the roots of f.

Therefore, when we talk of a polynomial generating a field extension, we mean that this extension is the splitting field of this polynomial.

Next up we define the concept of an algebraic element and extension using [Lan02, p. 223-224].

Definition 8 (Algebraic element)**.** *Let L/K be a field extension. An element $\alpha \in L$ is said to be algebraic over K if α is a root of some non-zero polynomial $f \in K[X]$.*

Definition 9 (Algebraic extension)**.** *A field extension L/K is said to be algebraic if every element of L is algebraic over K.*

With a similar motivation, we can define an algebraically closed field from [Lan02, p. 178].

Definition 10. *A field K is said to be algebraically closed if every non-constant polynomial of $K[X]$ has a root in K.*

Now that we have established the concept of an algebraically closed field, we can define the algebraic closure of a field from [LMF24, Algebraic closure of a field].

Definition 11 (Algebraic closure)**.** *Let K be a field. An algebraic closure of K is a minimal (in a well-defined sense) algebraically closed field extension of K, denoted by $\bar{K}$. The algebraic closure of a field is unique up to isomorphism.*

Using [LMF24, Galois closure of an extension], we can introduce a similar concept to an algebraic closure - the Galois closure of a field.

Definition 12 (Galois closure)**.** *If L is a separable algebraic extension of a field K, then its Galois closure over K is the smallest field containing L that is Galois over K.*

2.2 Cyclotomic extensions

Following the description of cylotomic extensions over general fields in [Lan02, § VI.3], we introduce the concept of cylotomic extensions over $\mathbb{Q}$.

Let $n \geq 1$ be an integer. Any root $\zeta \in \mathbb{C}$ of the polynomial $x^n - 1$ is called a *n-th root of unity*. Over $\mathbb{Q}$ the polynomial $x^n - 1$ is separable since its derivative nx^{n-1} is coprime to $x^n - 1$. Therefore, the polynomial $x^n - 1$ has n distinct roots in $\overline{\mathbb{Q}}$. All of these n-th roots of unity form a cyclic group, whose (non-unique) generator is called a *primitive n-th root of unity*. We denote the primitive n-th root of unity by ζ_n, and usually set $\zeta_n = e^{2\pi i/n}$, since all the n-th roots of unity can be written as $\zeta_n^k = e^{2\pi ik/n}$, where $1 \leq k \leq n$.

The field extension $\mathbb{Q}(\zeta_n)$ is called the *n-th cyclotomic extension*. This extension is Galois since it is the splitting field of the separable polynomial $x^n - 1$ over $\mathbb{Q}$. To further characterize the Galois group of these extensions, we introduce a theorem from [Lan02, § VI.3, Thm. 3.1].

Theorem 13. *Let ζ_n be a primitive n-th root of unity. Then*

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n),$$

where φ is the Euler's totient function. Moreover, we have that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*.$$

The proof of the second part of this theorem is derived using the fact that any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ acts on the n-th roots of unity by $\sigma(\zeta) = \zeta^a$, where a is an integer coprime to n. This concludes the brief introduction of cyclotomic extensions over $\mathbb{Q}$.

2.3 Inverse Galois Problem

Galois theory consists of investigating field extensions and computing the corresponding group of automorphisms. The Inverse Galois problem works backwards - it asks whether, for every finite group G, there exists a Galois field extension $L/\mathbb{Q}$ such that the Galois group of this extension is isomorphic to G. In general, the Inverse Galois problem is unsolved, however, it has been solved for some finite groups.

The simplest result to derive is the case of finite abelian groups, for which we present the proof in Section 3. We can classify some other known results about the Inverse Galois problem using the preface of [MM18].

In 1892 using his irreducibility theorem Hilbert proved that there exist infinitely many Galois extensions of $\mathbb{Q}$ with the Galois group isomorphic to S_n and A_n, the symmetric and alternating groups. The next result regarding the Inverse Galois Problem was proven by Scholz and Reichardt in 1937. They proved that all finite p-groups for an odd prime p can be realised as Galois groups over $\mathbb{Q}$ by solving number theoretic embedding problems. Continuing with this approach, Šafarevič proved the case for all solvable groups over arbitrary number fields.

The Inverse Galois problem has also been solved for 25 out of the 26 sporadic groups, which are finite simple groups that do not fit into any of the infinite families of finite simple groups. [Asc94] The only sporadic group for which the problem is still unsolved is the Mathieu group M_{23}. Further elaboration on this result can be found in [MM18, § II.9].

Another type of group for which the Inverse Galois problem is still unsolved is general Lie-type groups. However, it has been solved for some Lie-type groups, one of which is $\mathrm{GL}_2(\mathbb{F}_p)$. We present the proof of this result in Section 5.

3 Abelian groups

It is a well-known result that for any abelian group A, we can find a Galois field extension L of $\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to A. In this chapter, we begin by proving this result using cyclotomic extensions. Additionally, we provide the methods needed to construct a polynomial such that L is the splitting field of it. Lastly, we show that we can always construct L in a way that this field extension is totally real.

3.1 Preliminaries

Before presenting the proof of the Inverse Galois Problem for abelian groups, we restate some prerequisites from group theory that will prove to be essential in this chapter.

Theorem 14. *For any integer $a \in \mathbb{Z}_{\geq 1}$, there exist infinitely many prime numbers q such that $q \equiv 1 \mod a$.*

Proof. To prove this result, we employ Dirichlet's theorem on arithmetic progressions from [Ros11, Thm. 3.3], which states that for two relatively prime positive integers a and b, the arithmetic progression $am + b$, $m = 1, 2, 3, \ldots$, contains infinitely many primes. Let $b = 1$ in this case. Therefore, for any positive integer a the progression $am + 1$ contains infinitely many primes. This equivalently means that there exist infinitely many primes q and positive integers m such that $q = am + 1$, or $q \equiv 1 \mod a$. □

Afterwards, we restate the theorem commonly known as the first isomorphism theorem from [Lan02, p. 16].

Theorem 15 (The First Isomorphism theorem)**.** *If $\psi : G \to G'$ is a group homomorphism, then $H := \ker(\psi)$ is a normal subgroup of G and we have that*

$$G/H \cong \psi(G) \leq G'.$$

Additionally, if ψ is surjective, then $G/H \cong G'$.

Following [Lan02, § I.8], we introduce the following theorem which will be essential for solving the Inverse Galois problem for finite abelian groups.

Theorem 16 (Structure theorem of finitely generated abelian groups)**.** *If A is a finitely generated abelian group, there exists a unique integer $r \geq 0$ and a unique finite sequence $(d_1, \ldots, d_m)$ of integers $d_i > 1$ satisfying $d_m \mid d_{m-1} \mid \ldots \mid d_1$, such that*

$$A \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_m\mathbb{Z}.$$

An integral result from group theory is the Chinese Remainder Theorem, which we restate from [Lan02, § II.2, Thm. 2.1 and Cor. 2.2].

Theorem 17 (Chinese Remainder Theorem)**.** *Let $a_1, \ldots, a_n$ be pairwise coprime integers. Then there is a well-defined group isomorphism*

$$\begin{aligned} \mathbb{Z}/a_1 \cdot \ldots \cdot a_n\mathbb{Z} &\to \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z} \\ x \mod a_1 \cdot \ldots \cdot a_n &\mapsto (x \mod a_1, \ldots, x \mod a_n). \end{aligned}$$

Moreover, this map induces a group isomorphism

$$(\mathbb{Z}/a_1 \cdot \ldots \cdot a_n\mathbb{Z})^* \cong (\mathbb{Z}/a_1\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/a_n\mathbb{Z})^*.$$

Lemma 18. *Let $G_1, \ldots, G_n$ be a family of cyclic groups and $B_1 \subseteq G_1, \ldots, B_n \subseteq G_n$ a family of subgroups. Then*

$$G_1/B_1 \times \ldots \times G_n/B_n \cong (G_1 \times \ldots \times G_n) \,/\, (B_1 \times \ldots \times B_n)\,.$$

Proof. To prove the claim, first prove that $G_1/B_1 \times G_2/B_2 \cong (G_1 \times G_2) \,/\, (B_1 \times B_2)$. Define the group homomorphism

$$\begin{aligned} \varphi : G_1 \times G_2 &\to G_1/B_1 \times G_2/B_2 \\ (x, y) &\mapsto (xB_1, yB_2). \end{aligned}$$

This map is surjective, since for any $(xB_1, yB_2) \in G_1/B_1 \times G_2/B_2$, we can find $(x, y) \in G_1 \times G_2$ such that $\varphi(x, y) = (xB_1, yB_2)$. Now we would like to find the kernel of φ. By definition,

$$\ker(\varphi) = \{(c, d) \in G_1 \times G_2 \;\mid\; \varphi(c, d) = (B_1, B_2)\} = B_1 \times B_2 \subset G_1 \times G_2.$$

Therefore, by the First Isomorphism Theorem 15,

$$\begin{aligned} &(G_1 \times G_2) \,/\, \ker(\varphi) \cong G_1/B_1 \times G_2/B_2 \\ \implies \quad &(G_1 \times G_2) \,/\, (B_1 \times B_2) \cong G_1/B_1 \times G_2/B_2. \end{aligned}$$

The general case follows inductively. □

Lastly, we prove an elementary result regarding field homomorphisms that will prove useful later on.

Proposition 19. *If L, K are field extensions of $\mathbb{Q}$ and $\sigma : L \to K$ is a field homomorphism, then $\sigma \mid_{\mathbb{Q}} \equiv \mathrm{id} \mid_{\mathbb{Q}}$.*

Proof. Let $\frac{a}{b} \in \mathbb{Q}$. Then, we can see that

$$\sigma\left(\frac{a}{b}\right) = a \cdot \sigma\left(\frac{1}{b}\right) = a \cdot \frac{1}{b} \cdot b \cdot \sigma\left(\frac{1}{b}\right) = \frac{a}{b} \cdot \sigma(b) \cdot \sigma\left(\frac{1}{b}\right) = \frac{a}{b} \cdot \sigma\left(\frac{b}{b}\right) = \frac{a}{b} \cdot \sigma(1) = \frac{a}{b},$$

where we used the properties of a field homomorphism that $\sigma(1) = 1$ and $\sigma(b) = \sigma(1 + \ldots + 1) = \sigma(1) + \ldots \sigma(1) = 1 + \ldots + 1 = b$ for $b \in \mathbb{Z}$. Therefore, we have found that $\sigma \mid_{\mathbb{Q}} \equiv \mathrm{id} \mid_{\mathbb{Q}}$. □

3.2 Inverse Galois Problem for finite abelian groups

Now that we have laid out all the necessary tools, we are ready to solve the Inverse Galois problem for finite abelian groups. In the proof of the following theorem, we not only show the existence of the desired field extension but also the procedure to construct it.

Theorem 20. *For any finite abelian group A, there exists a Galois extension $L/\mathbb{Q}$ with $\mathrm{Gal}\,(L/\mathbb{Q}) \cong A$.*

Proof. First, since A is a finite group, we know it is finitely generated (since we can choose all elements of A to be the generators). Using the structure theorem of abelian groups 5, we know that for any finitely generated abelian group A, there exists a unique integer $r \geq 0$ and integers $a_1, \ldots, a_n > 0$ such that

$$A \cong \mathbb{Z}^r \times \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z}. \tag{2}$$

Since we know that A is finite, this implies that $r = 0$. Therefore,

$$A \cong \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z}.$$

Using Theorem 14, we know that for each of these integers a_i we can find primes p_i such that $p_i \equiv 1 \mod a_i$. Additionally, we know that even though all a_i's are not necessarily distinct, we can find the corresponding p_i's such that all of the primes are.

Now we consider the group $(\mathbb{Z}/p_i\mathbb{Z})^*$, which is cyclic because p_i is prime. We know that this group has order $\varphi(p_i) = p_i - 1$. Since we chose the primes p_i in a way that $p_1 \equiv 1 \mod a_i$, we have that $a_i \mid p_i - 1$. Thus, $\frac{p_i-1}{a} \mid (p_i - 1)$, which means that $(\mathbb{Z}/p_i\mathbb{Z})^*$ contains a unique cyclic subgroup B_i of order $(p_i - 1)/a_i$. Therefore, $(\mathbb{Z}/p_i\mathbb{Z})^* / B_i$ is also cyclic and of order a_i.

Thus, since $\mathbb{Z}/a_i\mathbb{Z}$ and $(\mathbb{Z}/p_i\mathbb{Z})^* / B_i$ are both cyclic and have the same order, we have found that

$$\mathbb{Z}/a_i\mathbb{Z} \cong (\mathbb{Z}/p_i\mathbb{Z})^* / B_i$$

for all a_i. Therefore,

$$A \cong \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z} \cong (\mathbb{Z}/p_1\mathbb{Z})^* / B_1 \times \ldots \times (\mathbb{Z}/p_n\mathbb{Z})^* / B_n.$$

Using Lemma 18 we know that

$$A \cong (\mathbb{Z}/p_1\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p_n\mathbb{Z})^* / B_1 \times \ldots \times B_n.$$

Since we chose all the primes p_i to be pairwise distinct, we can employ the Chinese Remainder Theorem to see that

$$(\mathbb{Z}/p_1\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p_n\mathbb{Z})^* \cong (\mathbb{Z}/p_1 \cdot \ldots \cdot p_n\mathbb{Z})^*.$$

Next, we can denote $N := p_1 \cdot \ldots \cdot p_n$. Since $B_1 \times \ldots \times B_n$ is a subgroup of $(\mathbb{Z}/p_1\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p_n\mathbb{Z})^* \cong (\mathbb{Z}/N\mathbb{Z})^*$, we can see that

$$B_1 \times \ldots \times B_n \cong B$$

for B a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$. Therefore, we have found that

$$A \cong (\mathbb{Z}/N\mathbb{Z})^* / B.$$

For the next step, we have to employ cyclotomic extensions. By Proposition 13 we know that

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_N)/\mathbb{Q}\right) \cong (\mathbb{Z}/N\mathbb{Z})^*,$$

where ζ_N is the N-th root of unity. As we know that B is a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$, it corresponds to a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. We can also easily see that B is abelian due to it being a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$. Therefore, B is a normal subgroup of $\mathrm{Gal}\left(\mathbb{Q}(\zeta_N)/\mathbb{Q}\right)$, so by Theorem 4, $\mathbb{Q}(\zeta_N)^B/\mathbb{Q}$ is a Galois extension with Galois group

$$\mathrm{Gal}\left(\mathbb{Q}(\zeta_N)^B/\mathbb{Q}\right) \cong \mathrm{Gal}\left(\mathbb{Q}(\zeta_N)/\mathbb{Q}\right) / \mathrm{Gal}\left(\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_N)^B\right) \cong (\mathbb{Z}/N\mathbb{Z})^* / B \cong A.$$

□

Now that we have shown that indeed any abelian group appears as the Galois group of some (non-unique) extension of $\mathbb{Q}$, we need to show how the polynomial generating this extension is computed. Since this extension is finite and separable, we can apply the Primitive element theorem 5 to deduce that there exists an element $\alpha \in \mathbb{Q}(\zeta_N)^B$ such that

$$\mathbb{Q}(\zeta_N)^B = \mathbb{Q}(\alpha).$$

Therefore, the polynomial generating this extension will simply be the minimal polynomial of α over $\mathbb{Q}$.

Proposition 21. *A primitive element α of the fixed field $\mathbb{Q}(\zeta_N)^B$ for $B \subseteq (\mathbb{Z}/N\mathbb{Z})^* \cong \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ can be computed as*

$$\alpha = \sum_{k \in B} \zeta_N^k.$$

Proof. To prove this result we first have to show that $\alpha \in \mathbb{Q}(\zeta_N)^B$. We can already see that $\alpha \in \mathbb{Q}(\zeta_N)$, so we only have to show that α is invariant under the action of any element of B. Let $b \in B$. Then we know that b corresponds to the element $\sigma_b \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ such that $\sigma_b(\zeta_N) = \zeta_N^b$. Therefore,

$$\sigma_b(\alpha) = \sigma_b\left(\sum_{k \in B} \zeta_N^k\right) = \left(\sum_{k \in B} \zeta_N^k\right)^b = \sum_{k \in B} \zeta_N^{bk}.$$

To show that $\sum_{k \in B} \zeta_N^k = \sum_{k \in B} \zeta_N^{bk}$, we have to consider the left cosets of B. Since $b \in B$, we know that $bB = B$, which means that bB spans the elements of B. Therefore, $\sigma_b(\alpha) = \alpha$.

Second, we have to prove that the element α is not fixed by any non-trivial element σ_a of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)^B/\mathbb{Q})$. σ_a corresponds to the element $a \in (\mathbb{Z}/N\mathbb{Z})^*/B$. In other words, we have to show that the cosets aB and B are distinct. This can be easily shown by noting that $a \in aB$, since $a = a \cdot 1$ and $1 \in B$ due to B being a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$. But, on the other hand, $a \notin B$, since we chose a to be a non-trivial element of $a \in (\mathbb{Z}/N\mathbb{Z})^*/B$. Therefore, $aB \neq B$, and we know that α is not stabilized by any non-trivial element of $(\mathbb{Z}/N\mathbb{Z})^*/B$.

Lastly, we would like to show that the Galois conjugates of α by two distinct non-trivial elements $\sigma_a, \sigma_{a'} \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)^B/\mathbb{Q})$ are distinct. The elements $\sigma_a, \sigma_{a'}$ correspond to the non-trivial elements a, a' of $(\mathbb{Z}/N\mathbb{Z})^*/B$ such that $a \neq a'$. So we only have to show that $aB \neq a'B$. Assume that there exists an element $c \in aB \cap a'B$. This means that $c = ab = a'b'$ for some $b, b' \in B$. Then we have that $a = a'b'b^{-1}$. Since $b'b^{-1} \in B$, this implies that a and a' are not distinct in $(\mathbb{Z}/N\mathbb{Z})^*/B$, which is a contradiction. Therefore, $aB \cap a'B = \varnothing$, and $aB \neq a'B$. This shows that $\sigma_a(\alpha) \neq \sigma_{a'}(\alpha)$.

As a result, we have shown that all the Galois conjugates of the element α under $\mathrm{Gal}(\mathbb{Q}(\zeta_N)^B/\mathbb{Q})$ are distinct, which, according to the last part of the proof of the Primitive element theorem from [Lan02, § V.4, Thm. 4.6], implies that α is indeed a primitive element of the extension $\mathbb{Q}(\zeta_N)^B$. □

Now that we have found the primitive element α of the extension $\mathbb{Q}(\zeta_N)^B$, we can find the polynomial generating this extension by simply computing the minimal polynomial f of α over $\mathbb{Q}$. The splitting field of f will be the field $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta_N)^B$ with the Galois group isomorphic to A.

3.3 Totally real extensions

After proving the Inverse Galois problem for finite abelian groups, we can further show that we can choose the corresponding extension to be totally real. Before proving this result, we first define what a totally real field is.

Definition 22. *A finite field extension $L/\mathbb{Q}$ is called totally real if the image of all embeddings of L into the complex number field $\mathbb{C}$ is contained in $\mathbb{R}$.*

Now we will see that by making some slight alterations to the algorithm of computing the field extension we can construct the field extension in a way that it is totally real.

Theorem 23. *Every finite abelian group can be realised as a totally real extension of $\mathbb{Q}$.*

Proof. To prove this theorem, we first need to prove an intermediate result concerning the group B constructed in the proof of Theorem 20.

Claim: For any abelian group A, the group B can always be constructed in a way that $-1 \in B$.

To prove the claim, we first need to prove that we can always construct the subgroups B_i in a way that $-1 \in B_i$. Recall from the proof of the abelian case that each B_i is a subgroup of the cyclic group $(\mathbb{Z}/p_i\mathbb{Z})^*$ for p_i prime, which is a cyclic group. Therefore, each B_i is also cyclic, and as shown before, it has order $\#B_i = (p_i - 1)/a_i$.

We want to construct the subgroups B_i such that they all have even order. This can be done by choosing the distinct primes p_i in a way that $p_i \equiv 1 \mod 2a_i$ (instead of just $p_i \equiv 1 \mod a_i$ like before). The existence of distinct primes like these is guaranteed by Dirichlet's theorem on arithmetic progressions again. Therefore, we have the property that $2a_i \mid p_i - 1$, which implies that $2 \mid \frac{p_i - 1}{a_i}$, and $\#B_i$ is even.

We have just shown that we can always choose the subgroups B_i to be of even order. Since B_i is a cyclic group, this means that it will contain an element of order 2. Let $a \in B_i$ such that $\text{ord}(a) = 2$. This implies that

$$a^2 \equiv 1 \mod p_i \quad \Longrightarrow \quad a^2 - 1 \equiv 0 \mod p_i \quad \equiv \quad p_i \mid a^2 - 1 = (a-1)(a+1).$$

Since p_i is an odd prime, we must have that either $p_i \mid a - 1$ or $p_i \mid a + 1$. This means that $a \equiv \pm 1 \mod p_i$, but since $\text{ord}(a) = 2$, we know that $a \not\equiv 1 \mod p_i$. Therefore, $a_i \equiv -1 \mod p_i$ and $-1 \in B_i$.

As proven before, $B = B_1 \times \ldots \times B_n$ and each B_i is a subgroup of $(\mathbb{Z}/p_i\mathbb{Z})^*$ where all p_i are distinct primes. Therefore, by the Chinese Remainder Theorem 17, if $-1 \in B_i$ for all subgroups B_i, then $-1 \in B$, which proves the claim.

As we have just proved that $-1 \in B$, this corresponds to an element $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ such that $\sigma(\zeta) = \zeta^{-1}$ for ζ every N-th root of unity. Since $\zeta \cdot \zeta^{-1} = 1 = \zeta \cdot \bar{\zeta}$, and $a = \bar{a}$ for all $a \in \mathbb{Q}$, σ acts on $\mathbb{Q}(\zeta_N)$ by complex conjugation. Therefore, complex conjugation acts trivially on the fixed field $\mathbb{Q}(\zeta_N)^B$.

Next, since the field extension $\mathbb{Q}(\zeta_N)^B/\mathbb{Q}$ is finite and separable due to being Galois, we can apply Primitive Element Theorem to deduce that there exists an element $\alpha \in \mathbb{Q}(\zeta_N)^B$ such that $\mathbb{Q}(\zeta_N)^B = \mathbb{Q}(\alpha)$. We also know that $\mathbb{Q}(\zeta_N)^B = \mathbb{Q}(\alpha)$ is invariant under complex conjugation, which means that all elements of this field are real. More specifically, $\alpha \in \mathbb{R}$.

Lastly, to prove that $\mathbb{Q}(\alpha)$ is indeed a totally real extension, we have to show that the image of every embedding of this field into the complex numbers $\mathbb{C}$ is contained in $\mathbb{R}$. Let $\iota : \mathbb{Q}(\alpha) \to \mathbb{C}$ be an embedding of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$. By the definition of embedding, ι is injective and structure-preserving, in this case, a field homomorphism.

Using Proposition 19, we know that $\iota \mid_{\mathbb{Q}} \equiv \text{id} \mid_{\mathbb{Q}}$. Therefore, we only need to consider the image of α under ι. Recall that we already established that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is separable. This means that the minimal polynomial f of α over $\mathbb{Q}$ splits completely in $\mathbb{Q}(\alpha)$. Therefore, all roots of the minimal polynomial f are real, since we already showed that all the elements of $\mathbb{Q}(\alpha)$ are real. Since α is a root of f, so is $\iota(\alpha)$, since $\iota(f(\alpha)) = f(\iota(\alpha)) = 0$ due to ι being a field homomorphism and f a polynomial. This shows that $\iota(\alpha)$ is real. Thus, we can conclude that the image of $\mathbb{Q}(\alpha)$ under the embedding ι is real, which proves that $\mathbb{Q}(\alpha)$ is totally real. This concludes the proof that any abelian group A can be realised as a totally real extension $\mathbb{Q}(\alpha)/\mathbb{Q}$. □

As we saw in the proof of Theorem 23, by adding the additional condition that $p_i \equiv 1 \mod 2a_i$ instead of just $p_i \equiv 1 \mod a_i$, we can ensure that the constructed field extension will be totally real.

3.4 Construction of polynomials generating abelian extensions of $\mathbb{Q}$

Following the structure of the proof of the inverse Galois problem for finite abelian groups, we can construct a systematic algorithm to compute a polynomial f whose splitting field will have a Galois group isomorphic to the desired abelian group A. Additionally, we can indicate if we

wish the extension to be totally real or not. Below we present the algorithm corresponding to the Magma code in the appendix.

Important to note is the fact that the input of integers corresponding to the abelian group A does not necessarily have to be in the form as in Theorem 16. Due to the Chinese Remainder Theorem, the representation need not be unique, and this goes both for the algorithm and the proof of Theorem 20.

Algorithm 1.
INPUT: A list $a\_list = [a_1, a_2, \ldots, a_n]$ of integers > 1 corresponding to the elementary divisors of the abelian group A.
A boolean flag *totally_real = true/false* indicating if the desired extension of $\mathbb{Q}$ should be totally real or not.

OUTPUT: Polynomial $f \in \mathbb{Q}[x]$ whose splitting field corresponds to the Galois extension of $\mathbb{Q}$ with a Galois group isomorphic to A.

1. [Initialize] Set *primes_list* := [ ] and *subgroups* := [ ] to store the primes and corresponding subgroups.
2. [Loop over elementary divisors] For each $a_i \in primes\_list$:
   a. If $totally\_real = false$, find a prime p_i such that $p_i \equiv 1 \mod a_i$, and all p_i's are distinct.
   b. If $totally\_real = true$, find a prime p_i such that $p_i \equiv 1 \mod 2a_i$, and all p_i's are distinct.
   c. Append the prime p_i to *primes_list*.
3. [Loop over the primes] For each $p_i \in primes\_list$:
   a. Compute a generator g of the cyclic group $(\mathbb{Z}/p_i\mathbb{Z})^*$.
   b. Compute the cardinality of the subgroup $B_i \subset (\mathbb{Z}/p_i\mathbb{Z})^*$ as $\#B_i = (p_i - 1)/a_i$.
   c. Compute a generator $h = g^{a_i}$ of the subgroup B_i.
   d. Construct the subgroup $B_i = \left[h^j \mod p_i \text{ for } j \in [1, \ldots, \#B_i]\right]$.
   e. Append the subgroup B_i to *subgroups*.
4. Compute the product of the primes in *primes_list* as $N := p_1 \cdot p_2 \cdot \ldots \cdot p_n$.
5. [Initialize] Set B := [ ] to store the elements of the subgroup $B \subset (\mathbb{Z}/N\mathbb{Z})^*$.
6. [Construct the subgroup B] Loop over all the combinations of elements in $B_1 \times B_2 \times \ldots \times B_n$.
   a. Apply Chinese Remainder Theorem to find the corresponding element in $(\mathbb{Z}/N\mathbb{Z})^*$.
   b. Append the found element to the list B.
7. [Compute the polynomial f] Using the subgroup $B \subset (\mathbb{Z}/N\mathbb{Z})^*$:
   a. Define $\mathbb{Q}(\zeta_N)$ to be the cyclotomic field extension, where ζ_p is a primitive N-th root of unity.
   b. Compute the primitive element α generating the intermediate field $\mathbb{Q}(\zeta_N)^B$ as $\alpha = \sum_{k \in B} \zeta_N^k$.
   c. Compute the minimal polynomial f of the primitive element α; then $\mathbb{Q}(\zeta_N)^B$ is the splitting field of f.
8. Return f.

4 Elliptic curves

In this section, we introduce the concept of elliptic curves and some associated properties that will prove to be useful when constructing the extensions with Galois group isomorphic to $\mathrm{GL}_2(\mathbb{F}_p)$.

4.1 Introduction

Before defining elliptic curves, we need to define the notion of an affine space from [Sil09, p. 1] and a projective space from [Sil09, p. 6].

Definition 24 (Affine space)**.** *The affine n-space over a field K is defined as the set of n-tuples*

$$\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \{P = (x_1, \ldots, x_n) : x_i \in \overline{K}\}.$$

Equivalently, we can define the set of K-rational points of $\mathbb{A}^n$ as the set

$$\mathbb{A}^n(K) = \{P = (x_1, \ldots, x_n) \in \mathbb{A}^n : x_i \in K\}.$$

When $n = 2$, we call $\mathbb{A}^2$ the affine plane over K.

Definition 25 (Projective space)**.** *The projective n-space $\mathbb{P}^n$ over a field K is the set of all $(n+1)$-tuples $(x_0, \ldots, x_n) \in \mathbb{A}^{n+1}$ such that at least one x_i is nonzero, together with the equivalence relation*

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \quad \iff \quad \text{there exists } \lambda \in \overline{K}^* \text{ such that } x_i = \lambda y_i \text{ for all } i.$$

An equivalence class of a point in the projective plane is denoted by $[x_0 : \ldots : x_n]$, and $x_0, \ldots, x_n$ are called homogeneous coordinates for the corresponding point in $\mathbb{P}^n$.

When $n = 2$, we call $\mathbb{P}^2$ the projective plane over K.

With the concept of projective spaces, we can define a projective elliptic curve, meaning that the points on the curve are in either $\mathbb{P}^2(\mathbb{R})$ or $\mathbb{P}^2(\mathbb{C})$. We follow [Sil09, § III.1] for the definitions below.

Definition 26 (Elliptic curve)**.** *An elliptic curve E over a field K is a smooth projective curve given by the homogeneous equation*

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{3}$$

with $a_1, \ldots, a_6 \in K$. If $K = \mathbb{Q}$, then we call E a rational elliptic curve.

We can view E as an affine curve by using non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$ to transform the curve into the form called Weierstrass equation given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{4}$$

Each point in affine coordinates (x, y) on the elliptic curve then corresponds to the point $[x : y : 1]$ in the projective plane. Equivalently, each point $[X : Y : Z]$ in the projective plane corresponds to a point $(X/Z, Y/Z)$ in affine coordinates, unless $Z = 0$. When $Z = 0$, this is called the *line at infinity* of the projective plane. Setting $Z = 0$ in Equation (3) gives $X^3 = 0$, therefore, the elliptic curve E intersects the line at infinity three times at exactly one projective point $\mathcal{O} = [0 : 1 : 0]$, which we call the *point at infinity*. This is considered to be the point in the affine plane where all vertical lines meet. By convention, when we talk of an elliptic curve in affine coordinates as defined in Equation (4), we consider all the points in the affine xy-plane satisfying E together with the point at infinity $\mathcal{O}$.

Lastly, we need to define a specific form of an elliptic curve that will prove to be essential later on.

Definition 27 (Weierstrass form)**.** *An equation for an elliptic curve is said to be in Weierstrass form if it is given by*

$$y^2 = 4x^3 - g_2x - g_3.$$

Equivalently, the more general equation

$$y^2 = x^3 + ax^2 + bx + c$$

is also called the Weierstrass form.

Every rational elliptic curve can be transformed into Weierstrass form, with the necessary procedure laid out explicitly in [ST15, § 1.3].

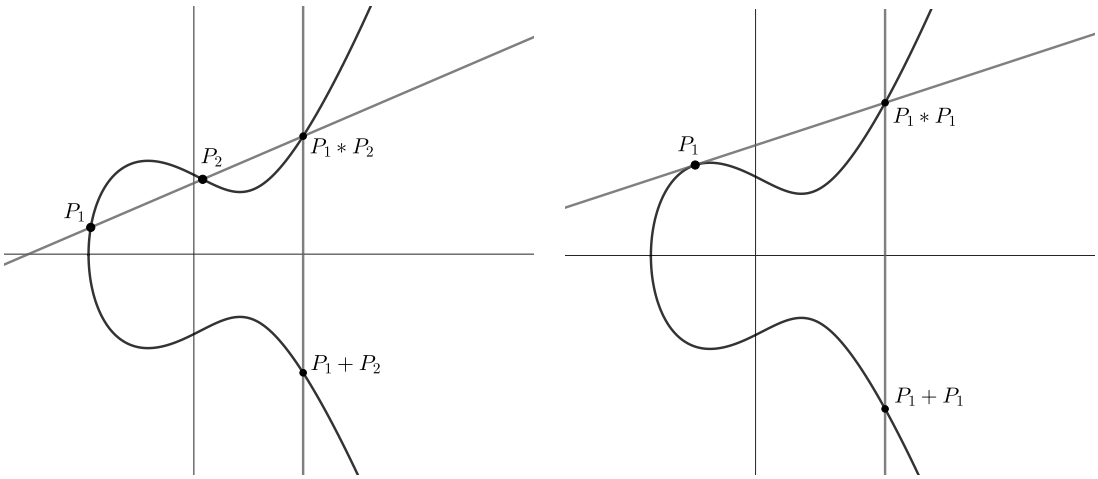
Group law

Let E be an elliptic curve in Weierstrass form. It turns out that the points on E in the xy-plane together with the point at infinity $\mathcal{O}$ can be equipped with a group structure. To illustrate this, we lay out a procedure to equip E with a group operation below, following [Sil09, § III.2].

Let P_1 and P_2 be two points on the elliptic curve E. Let L be the line through P_1 and P_2. Denote the third point of intersection of L and E by $P_1 * P_2$. The existence of a third point of intersection is guaranteed by Bezout's theorem, and more details can be found in [ST15, § A.3]. Let L' be the line through $P_1 * P_2$ and $\mathcal{O}$. This line will intersect E at a third point, which we denote by $P_1 + P_2$. This procedure defines a group law on the points of the elliptic curve, together with the identity element - the point at infinity $\mathcal{O}$. In other words, we define the addition of points on E as

$$P_1 + P_2 := \mathcal{O} * (P_1 * P_2).$$

In the case that we want to add a point to itself, we can consider the elements P_1 and P_2 to overlap. This means that the line through P_1 and P_2 will simply be the tangent line of E at that point. Both cases of addition of points when P_1 and P_2 are distinct or overlap are illustrated in Figure 4.1 below.



With the procedure laid out above, we can equip the points on E with a group structure. Moreover, this group will be abelian, since there is only one way to draw a line through two points, no matter which one we consider first.

An important property of the group law on an elliptic curve in Weierstrass form is that the inverse of each point is the same point mirrored around the x-axis.

To prove that $-P$ is the inverse of P with respect to the group law defined before, we must show that $P + (-P) = \mathcal{O}$. Therefore, we must first connect the points P and $-P$ by a straight line L. Since these two points are symmetrical around the x-axis, the line L connecting them will simply be vertical. Therefore, the third point of intersection of L and E will be the point at infinity $\mathcal{O}$. In other words, $P * (-P) = \mathcal{O}$. Thus, we have that $P + (-P) = \mathcal{O} * (P * (-P)) = \mathcal{O} * \mathcal{O}$. The line tangent to the point at infinity intersects E at exactly three points, which are all $\mathcal{O}$. From this, we can see that indeed $P + (-P) = \mathcal{O}$, hence P and $-P$ are inverses of each other.

4.2 Points of finite order

Now that we have equipped the points on an elliptic curve with a group structure, we can consider the concept of points of finite order. Below we present the definition from [ST15, § 2.1].

Definition 28. *A point P of an elliptic curve E is defined to have order n if*

$$[n]P = \underbrace{P + P + \ldots + P}_{n \text{ times}} = \mathcal{O},$$

but $n'P \neq \mathcal{O}$ for all integers $1 \leq n' < n$. If such an n exists, then P is said to have finite order, otherwise, it has infinite order.

Therefore, points of order n are the points that equal the identity element if summed together exactly n times, and no less. Similarly, we can introduce the concept of torsion points with the less strict condition that adding the element to itself n times will yield the identity element, even if the order is possibly smaller. We present the definition from [Sil09, § III.4].

Definition 29. *For an elliptic curve E and an integer $n \in \mathbb{Z}_{\geq 1}$, the n-torsion subgroup of E is the set of points of E that have order dividing n. In other words, we define the n-torsion group $E[n]$ as*

$$E[n] := \{P \in E : [n]P = \mathcal{O}\}.$$

As we saw before that the addition of points on an elliptic curve is quite involved, we spend the rest of this section laying out an approach to construct the n-torsion subgroup of E. We follow the procedure laid out in [ST15, § 2.2].

First, transform the rational elliptic curve into Weierstrass form such that E is given by

$$E : y^2 = 4x^3 - g_2 x - g_3.$$

When E is nonsingular, meaning that $g_2^3 - 27g_3^2 \neq 0$, we can find $\mathbb{R}$-linearly independent complex numbers ω_1 and ω_2, called *periods*. They will be used to define a function from Λ to complex points on E. Using these periods, we can form a group Λ called a *lattice* by taking all the $\mathbb{Z}$-linear combinations of the periods as follows

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{n_1\omega_1 + n_2\omega_2 \mid n_1, n_2 \in \mathbb{Z}\}.$$

There are many different choices for the periods, but the coefficients g_2, g_3 of the elliptic curve uniquely determine the period lattice Λ. Similarly, the lattice Λ uniquely determines g_2 and g_3 via the correspondence

$$g_2 = 60 \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^4} \qquad \& \qquad g_3 = 140 \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^6}.$$

Using the periods ω_1 and ω_2, we can define a meromorphic function $\wp$, called the *Weierstrass $\wp$-function* as follows

$$\wp(u) = \frac{1}{u^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} \right).$$

This function has the property that it has a double pole at each point of the lattice Λ and no other poles. Additionally, $\wp$ is doubly periodic with respect to the periods of the lattice, meaning that

$$\wp(u + \omega_1) = \wp(u) \qquad \& \qquad \wp(u + \omega_2) = \wp(u) \quad \text{for all } u \in \mathbb{C}.$$

This property implies that

$$\wp(u + \omega) = \wp(u) \quad \text{for all } u \in \mathbb{C} \text{ and all } \omega \in \Lambda.$$

Moreover, the Weierstrass $\wp$-function satisfies the differential equation

$$\wp'(u)^2 = 4\wp(u) - g_2\wp(u) - g_3.$$

Therefore, for every complex number u, we get a complex-valued point $(\wp(u), \wp'(u))$ on the elliptic curve E. Thus, using the function $\wp$, we can construct a map from the complex plane to $E(\mathbb{C})$. This map is surjective, but cannot be injective, since $\wp$ is doubly periodic in the complex number plane. However, if we take the quotient of the complex plane by the lattice Λ, we can define an isomorphism of $\mathbb{C}/\Lambda$ and the complex points on the elliptic curve E using the Weierstrass $\wp$-function and its derivative.

Thus, we can construct a map

$$\phi : \mathbb{C}/\Lambda \to E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}), \quad z \mapsto [\wp(z) : \wp'(z) : 1],$$

where $E(\mathbb{C})$ denotes the points on E with complex coordinates. According to [Sil09, § VI.3, Prop. 3.6b], ϕ is a complex analytic isomorphism of complex Lie groups. Therefore, ϕ is an isomorphism from the additive group of complex numbers onto the complex points of E with respect to the addition of points defined on elliptic curves. Using this map, we can describe the points of order dividing n on the elliptic curve. Since the points on the lattice Λ are poles of $\wp$ and $\wp'$, under ϕ they are mapped to the point at infinity $\mathcal{O}$ of E. Therefore, we would first like to find the set of all points v of $\mathbb{C}/\Lambda$ such that $nv \in \Lambda$.

In the figure below, we can see an illustration of the construction of n-torsion points of $\mathbb{C}/\Lambda$ for $n = 5$.

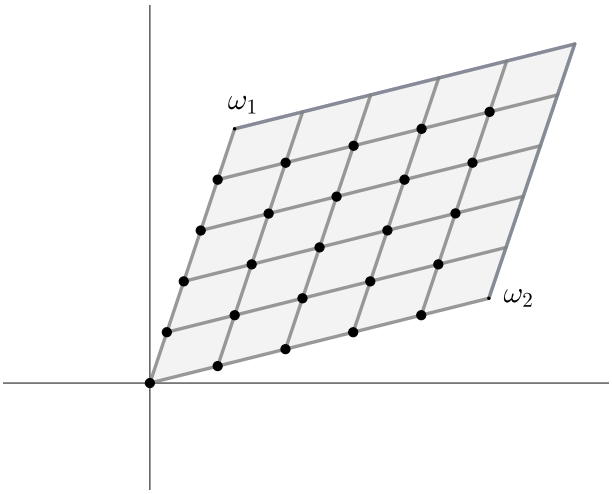


Figure 1: The set of all 5-torsion points of $\mathbb{C}/\Lambda$.

Therefore, we can denote the set of these points in $\mathbb{C}/\Lambda$ by

$$(\mathbb{C}/\Lambda)[n] := \left\{ \frac{a\omega_1 + b\omega_2}{n} \in \mathbb{C}/\Lambda \;\middle|\; a, b \in \mathbb{Z}/n\mathbb{Z} \right\} \subset \mathbb{C}/\Lambda.$$

We can see that any element $v \in (\mathbb{C}/\Lambda)[n]$ will land in the lattice Λ when multiplied by n. Thus, since ϕ is a group isomorphism, the image of any $v \in (\mathbb{C}/\Lambda)[p]$ under ϕ will correspond to a point $\phi(v) \in E(\mathbb{C})$ such that $n \cdot \phi(v) = \mathcal{O}$. In other words,

$$\phi\left((\mathbb{C}/\Lambda)[n]\right) = E[n] \quad \Longrightarrow \quad (\mathbb{C}/\Lambda)[n] \cong E[n].$$

Employing this approach, we can find the points of finite order on an elliptic curve simply and systematically by avoiding rigorous computations of the addition of points on an elliptic curve. In other words, we translate the hard problem of finding $E[n]$ to the easy problem of finding $(\mathbb{C}/\Lambda)[n]$.

Using the isomorphism ϕ, we can even describe the structure of $E[n]$.

Proposition 30. $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Proof. Since we already know that $E[n] \cong (\mathbb{C}/\Lambda)[n]$, we only have to show that $(\mathbb{C}/\Lambda)[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. This can be done by constructing a map

$$\begin{aligned} \psi : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\to (\mathbb{C}/\Lambda)[n] \\ (a_1, a_2) &\mapsto \frac{a_1\omega_1 + a_2\omega_2}{n} \end{aligned}$$

and showing that ψ is a group isomorphism. First, prove that ψ is a group homomorphism. Let $(a_1, a_2), (b_1, b_2) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Then we can see that

$$\psi\left((a_1, a_2) + (b_1, b_2)\right) = \psi\left((a_1 + b_1, a_2 + b_2)\right) = \frac{(a_1 + b_1)\omega_1 + (a_2 + b_2)\omega_2}{n}$$

$$= \frac{a_1\omega_1 + a_2\omega_2}{n} + \frac{b_1\omega_1 + b_2\omega_2}{n} = \psi\left((a_1, a_2)\right) + \psi\left((b_1, b_2)\right),$$

which shows that ψ is indeed a group homomorphism.

To prove that ψ is an isomorphism, we first need to show that it is injective. Let $(c_1, c_2) \in \ker(\psi)$. This means that

$$\psi\left((c_1, c_2)\right) = \frac{c_1\omega_1 + c_2\omega_2}{n} = 0.$$

Since the image of ψ is in $\mathbb{C}/\Lambda$, this implies that

$$c_1\omega_1 + c_2\omega_2 = n(n_1\omega_1 + n_2\omega_2)$$

for $n_1, n_2 \in \mathbb{Z}$. Previously we established that ω_1 and ω_2 are $\mathbb{R}$-linearly independent, therefore, we have that

$$\begin{cases} c_1\omega_1 = nn_1\omega_1 \\ c_2\omega_2 = nn_2\omega_2 \end{cases} \implies \begin{cases} c_1 = nn_1 \\ c_2 = nn_2 \end{cases} \implies \begin{cases} c_1 \equiv 0 \mod n \\ c_2 \equiv 0 \mod n \end{cases}$$

This shows that $\ker(\psi) = \{(0, 0)\}$, which proves that ψ is injective.

To prove surjectivity, we only need to recall that any point in $(\mathbb{C}/\Lambda)[n]$ can be written in the form $(a_1\omega_1 + a_2\omega_2)/n$ by the definition of $(\mathbb{C}/\Lambda)[n]$. Then we can clearly see that for any point $(a_1\omega_1 + a_2\omega_2)/n \in (\mathbb{C}/\Lambda)[n]$, we can choose $(a_1, a_2) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ to construct the point of $(\mathbb{C}/\Lambda)[n]$ as $\psi(a_1, a_2) = (a_1\omega_1 + a_2\omega_2)/n$. This proves that ψ is surjective.

Since we have just shown that ψ is a bijective group homomorphism, therefore, a group isomorphism, this proves that

$$E[n] \cong (\mathbb{C}/\Lambda)[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

□

We have just provided the proof that $E[n]$ is isomorphic to a direct product of two cyclic groups of order n. Because of this result, we know that it is finitely generated. For convenience, we can choose the generators of $(\mathbb{C}/\Lambda)[n]$ to be $\frac{\omega_1}{n}$ and $\frac{\omega_2}{n}$. Therefore, we can set the points corresponding to the image of these generators under ϕ to be the generators of $E[n]$. In other words, set

$$P_1 := \phi\left(\frac{\omega_1}{n}\right) \quad \& \quad P_2 := \phi\left(\frac{\omega_2}{n}\right) \tag{5}$$

to be the points in $E[n]$ that generate $E[n]$.

Therefore, we can write the n-torsion group as follows:

$$E[n] = \{a_1P_1 + a_2P_2 \mid a_1, a_2 \in \mathbb{Z}/n\mathbb{Z}\}. \tag{6}$$

The choice that $a_1, a_2 \in \mathbb{Z}/n\mathbb{Z}$ comes from the fact that $nP = \mathcal{O}$ for any $P \in E[n]$. From this we can see that any $P \in E[n]$ can be written as $P = a_1P_1 + a_2P_2$ for unique $a_1, a_2 \in \mathbb{Z}/n\mathbb{Z}$.

4.3 Adjoining $E[n]$ to $\mathbb{Q}$

Now that we have laid out an approach to compute the n-torsion points of an elliptic curve, we can work further with the coordinates of these points in the affine plane.

Let E be an elliptic curve with rational coefficients given by the Weierstrass equation

$$E : y^2 = x^3 + ax^2 + bx + c.$$

We know that $E(\mathbb{C})$ forms a group under the addition of points on an elliptic curve. If K is a subfield of $\mathbb{C}$, we can consider the K-rational points on E, which is the set

$$E(K) = \{(x, y) \mid (x, y) \in E \text{ and } x, y \in K\} \cup \{\mathcal{O}\}.$$

Using [ST15, § VI.3, Prop. 6.3a] we can even show that the K-rational points form a subgroup of $E(\mathbb{C})$.

Proposition 31. *If E is an elliptic curve with coefficients in $\mathbb{Q}$ and K is a field extension of $\mathbb{Q}$, then $E(K)$ is a subgroup of $E(\mathbb{C})$.*

Proof. Since the identity element - the point at infinity $\mathcal{O}$ - is contained in $E(K)$ by convention, we must only show that $E(K)$ is closed under addition. Let $P, Q \in E(K)$. This means that their x and y coordinates are in the field K, therefore, the x and y coordinates of $P + Q$ will also be in K due to the group law on E being defined via rational functions with coefficients in $\mathbb{Q}$. This shows that $P + Q \in E(K)$, so $E(K)$ is closed under addition, which proves that indeed $E(K)$ is a subgroup of $E(\mathbb{C})$. □

To investigate how the Galois elements act on points on an elliptic curve, we use [ST15, § VI.3, Prop. 6.3b].

Proposition 32. *Let E be an elliptic curve with rational coefficients and let K be a Galois extension of $\mathbb{Q}$. For $P \in E(K)$ and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, we can define*

$$\sigma(P) = \begin{cases} (\sigma(x), \sigma(y)) & \text{if } P = (x, y), \\ \mathcal{O} & \text{if } P = \mathcal{O}. \end{cases}$$

Then $\sigma(P) \in E(K)$.

Proof. Let $P = (x, y)$ be a point in $E(K)$. Since σ is an automorphism of the field K, we know that $\sigma(x), \sigma(y) \in K$. Therefore, we only have to show that $\sigma(P) = (\sigma(x), \sigma(y))$ is on the elliptic curve E. Since $P \in E(K)$, we can see that

$$y^2 = x^3 + ax^2 + bx + c \quad \Longrightarrow \quad \sigma\left(y^2\right) = \sigma\left(x^3 + ax^2 + bx + c\right).$$

Due to the properties of a field homomorphism, we can see that

$$\sigma\left(y^2\right) = \sigma\left(x^3\right) + \sigma\left(ax^2\right) + \sigma(bx) + \sigma(c) \quad \Longrightarrow \quad \sigma(y)^2 = \sigma(x)^3 + \sigma(a)\sigma(x)^2 + \sigma(b)\sigma(x) + \sigma(c).$$

Since σ reduces to the identity map on $\mathbb{Q}$, we then have that

$$\sigma(y)^2 = \sigma(x)^3 + a\sigma(x)^2 + b\sigma(x) + c,$$

which shows that $(\sigma(x), \sigma(y))$ satisfies the equation of the elliptic curve E, so indeed $\sigma(P) \in E(K)$. □

We further introduce the following propositions from [ST15, § VI.3, Prop. 6.3d,e].

Proposition 33. *Let E be an elliptic curve with rational coefficients, $P, Q \in E(K)$ and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Then we have that*

$$\sigma(P + Q) = \sigma(P) + \sigma(Q) \quad \& \quad \sigma(-P) = -\sigma(P).$$

Moreover, $\sigma(nP) = n(\sigma(P))$ for all integers n.

Proof. The proof of this proposition using the properties of the addition law is given in [ST15, p. 215]. □

Proposition 34. *Let $P \in E(K)$ be a point of order n and let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Then $\sigma(P)$ has order n as well.*

Proof. Since $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, we know that σ is a group automorphism, therefore, it preserves the order of elements. □

As we already showed before, the set of n-torsion points forms a group of the form

$$E[n] = \{\mathcal{O}, (x_1, y_1), \ldots, (x_m, y_m)\}.$$

Since the coordinates of the points of $E[n]$ are in the field $\mathbb{C}$, we can extend the subfield $\mathbb{Q} \subset \mathbb{C}$ using the n-torsion points as follows

$$\mathbb{Q}(E[n]) := \mathbb{Q}(x_1, y_1, \ldots, x_m, y_m).$$

Now that we have constructed this field extension, we can show that it is both algebraic and Galois.

Proposition 35. *Let E be an elliptic curve with rational coefficients. Then $\mathbb{Q}(E[n])$ is algebraic over $\mathbb{Q}$.*

Proof. A computational proof of this result can be found in [ST15, Prop. 6.5a], so we only outline it here. The result is proven using the fact that for any point on E, we can always derive a multiplication-by-n formula of the x-coordinate that will be a rational function. Using this, we can prove that the x-coordinate of an n-torsion point is algebraic. Therefore, the y-coordinate will also be algebraic, since it satisfies $y^2 = x^3 + ax^2 + bx + c$. □

Proposition 36. *$\mathbb{Q}(E[n])/\mathbb{Q}$ is a Galois extension.*

Proof. To prove that $\mathbb{Q}(E[n])$ is Galois over $\mathbb{Q}$, we will show that every field homomorphism $\sigma : \mathbb{Q}(E[n]) \to \mathbb{C}$ is a field automorphism. Since we already know that $\mathbb{Q}(E[n])$ is a finite algebraic field extension of $\mathbb{Q}$ from the previous proposition, we can consider its Galois closure over $\mathbb{Q}$, which we denote by L. All field homomorphisms from $\mathbb{Q}(E[n])$ to $\mathbb{C}$ are obtained by restricting each $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ to $\mathbb{Q}(E[n])$. The image of $\sigma\,|_{\mathbb{Q}(E[n])}$ is fully determined by the image of each $P \in E[n]$, since σ reduces to the identity on $\mathbb{Q}$. For every $P \in E[n]$, we know that $\sigma(P) \in E[n]$ as well, according to Proposition 34. Thus, σ induces a permutation of the n-torsion points. This shows that $\sigma(\mathbb{Q}(E[n])) \subseteq \mathbb{Q}(E[n])$. Since σ is a field homomorphism, this indeed shows that σ is an automorphism. As a result, $\mathbb{Q}(E[n])$ is Galois over $\mathbb{Q}$. □

Going back to Equation (6), recall that we established that the elements of the n-torsion group can be written as

$$E[n] = \{a_1 P_1 + a_2 P_2 \mid a_1, a_2 \in \mathbb{Z}/n\mathbb{Z}\}.$$

Using this representation of the n-torsion points, we can investigate further how the elements of $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ act on the group $E[n]$.

Let $P \in E[n]$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$. Then, using Proposition 33 we can see that

$$\sigma(P) = \sigma(a_1 P_1 + a_2 P_2) = a_1 \sigma(P_1) + a_2 \sigma(P_2).$$

Since $\sigma(P_1), \sigma(P_2) \in E[n]$ according to Proposition 34, we can also write them in the form of Equation 6. Therefore,

$$\sigma(P_1) = a(\sigma) P_1 + c(\sigma) P_2$$
$$\sigma(P_2) = b(\sigma) P_1 + d(\sigma) P_2$$

for $a(\sigma), b(\sigma), c(\sigma), d(\sigma) \in \mathbb{Z}/n\mathbb{Z}$. This shows that any element of $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is fully determined by how it acts on P_1 and P_2. We can see that σ acts as a change of basis on the points of $E[n]$.

Following this, we can construct a map

$$\begin{aligned} \rho_n : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) &\to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \\ \sigma &\mapsto \begin{bmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{bmatrix}. \end{aligned} \tag{7}$$

Proposition 37. *ρ_n is an injective group homomorphism.*

Proof. First, we would like to prove that ρ_n is a group homomorphism. Let $\sigma, \delta \in \mathrm{Gal}(\mathbb{Q}(E[n]/\mathbb{Q})$ such that

$$\rho_n(\sigma) = \begin{bmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{bmatrix}, \quad \rho_n(\delta) = \begin{bmatrix} a(\delta) & b(\delta) \\ c(\delta) & d(\delta) \end{bmatrix}.$$

To prove that ρ_n is a homomorphism, we have to show that

$$\rho_n(\sigma\delta) = \rho_n(\sigma)\rho_n(\delta).$$

To compute the left-hand side, we first note that

$$\begin{aligned} & & \delta(P_1) &= a(\delta)P_1 + c(\delta)P_2 \\ \implies \quad & \sigma(\delta(P_1)) &= \sigma(a(\delta)P_1 + c(\delta)P_2) = a(\delta)(a(\sigma)P_1 + c(\sigma)P_2) + c(\delta)(b(\sigma)P_1 + d(\sigma)P_2) \\ & &= (a(\delta)a(\sigma) + c(\delta)b(\sigma))P_1 + (a(\delta)c(\sigma) + c(\delta)d(\sigma))P_2. \end{aligned}$$

Similarly,

$$\begin{aligned} & & \delta(P_2) &= b(\delta)P_1 + d(\delta)P_2 \\ \implies \quad & \sigma(\delta(P_2)) &= \sigma(b(\delta)P_1 + d(\delta)P_2) = b(\delta)(a(\sigma)P_1 + c(\sigma)P_2) + d(\sigma)(b(\sigma)P_1 + d(\sigma)P_2) \\ & &= (b(\delta)a(\sigma) + d(\delta)b(\sigma))P_1 + (b(\delta)c(\sigma) + d(\delta)d(\sigma))P_2. \end{aligned}$$

Therefore, by the construction of the map ρ_n, we have that

$$\rho_n(\sigma\delta) = \begin{bmatrix} a(\delta)a(\sigma) + c(\delta)b(\sigma) & b(\delta)a(\sigma) + d(\delta)b(\sigma) \\ a(\delta)c(\sigma) + c(\delta)d(\sigma) & b(\delta)c(\sigma) + d(\delta)d(\sigma) \end{bmatrix}.$$

To compute the right-hand side, we simply have to perform matrix multiplication to get that

$$\rho_n(\sigma)\rho_n(\delta) = \begin{bmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{bmatrix} \cdot \begin{bmatrix} a(\delta) & b(\delta) \\ c(\delta) & d(\delta) \end{bmatrix} = \begin{bmatrix} a(\delta)a(\sigma) + c(\delta)b(\sigma) & b(\delta)a(\sigma) + d(\delta)b(\sigma) \\ a(\delta)c(\sigma) + c(\delta)d(\sigma) & b(\delta)c(\sigma) + d(\delta)d(\sigma) \end{bmatrix}.$$

Therefore, we have shown that for any $\sigma, \delta \in \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$, $\rho_n(\sigma\delta) = \rho_n(\sigma)\rho_n(\delta)$, which proves that ρ_n is a group homomorphism.

Second, to prove that ρ_n is injective, we would like to show that the kernel of this homomorphism is trivial. Let $\tau \in \ker(\rho_n)$. This means that

$$\rho_n(\tau) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

which in turn implies that

$$\tau(P_1) = P_1, \quad \tau(P_2) = P_2.$$

Therefore, since we can write any $P \in E[n]$ in the form $P = a_1P_1 + a_2P_2$ according to 6, we can see that

$$\tau(P) = \tau(a_1P_1 + a_2P_2) = a_1\tau(P_1) + a_2\tau(P_2) = a_1P_1 + a_2P_2 = P.$$

This shows that τ is the identity map on $\mathbb{Q}(E[n])$. In other words,

$$\ker(\rho_n) = \left\{ \mathrm{id} \mid_{\mathbb{Q}(E[n])} \right\},$$

so the kernel is trivial, which proves that ρ_n is an injective group homomorphism. □

5 Galois representations of elliptic curves

Now that we have defined the map ρ_n, we have established a link between the Galois group of some finite extension of $\mathbb{Q}$ and the group $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. We dedicate this section to investigating when this connection is an isomorphism.

5.1 Maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$

In the case that we choose the value of n to be a prime number p, the ring $\mathbb{Z}/p\mathbb{Z}$ can be denoted by $\mathbb{F}_p$, since it inherits a finite field structure of characteristic p. In this case, the map ρ_p defined in (7) is called the *mod p Galois representation of the elliptic curve*. We would like to examine the map more closely in this case and find out when ρ_p is an isomorphism, not only an injective homomorphism. According to [Ser72, § 4.2, Thm. 2], the mod p Galois representation of a non-CM elliptic curve is surjective for all but finitely many prime numbers p.

In other words, we want to find when $\mathrm{im}(\rho_p) = \mathrm{GL}_2(\mathbb{F}_p)$ for a prime p. This can be done by considering all the possible maximal subgroups Γ of $\mathrm{GL}_2(\mathbb{F}_p)$ and showing that $\mathrm{im}(\rho_p) \nsubseteq \Gamma$, which would prove the necessary equality.

Before going into the details, we need to define a few prerequisites. First of these is introducing first of the subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ from [Lan02, p. 536].

Definition 38. *The special linear group of size* 2 *over* $\mathbb{F}_p$*, denoted by* $\mathrm{SL}_2(\mathbb{F}_p)$*, is the subgroup of* $\mathrm{GL}_2(\mathbb{F}_p)$ *consisting of matrices that have determinant* 1*.*

Using [Lan02, p. 14] again, we can also define the center of a group.

Definition 39. *The center of a group G is defined as the abelian subgroup*

$$\mathcal{Z}(G) := \{x \in G \mid xy = yx \text{ for all } y \in G\} \subseteq G.$$

Proposition 40. *The center of* $\mathrm{GL}_2(\mathbb{F}_p)$ *is the subgroup of scalar matrices, or, equivalently,*

$$\mathcal{Z}\left(\mathrm{GL}_2(\mathbb{F}_p)\right) = \{a \cdot I_2 \mid a \in \mathbb{F}_p^\times\},$$

where I_2 denotes the identity matrix of size 2×2. From now on, we denote this subgroup simply by $\mathcal{Z}$, since we are only concerned with the group $\mathrm{GL}_2(\mathbb{F}_p)$*.*

Using the concept of the center of a group, we can introduce the projective group using the definition from [Lan02, p. 536].

Definition 41. *The projective linear group is defined to be the quotient group*

$$\mathrm{PGL}_2(\mathbb{F}_p) := \mathrm{GL}_2(\mathbb{F}_p)/\mathcal{Z}.$$

Definition 42. *The projective special linear group is defined to be the quotient group*

$$\mathrm{PSL}_2(\mathbb{F}_p) := \mathrm{SL}_2(\mathbb{F}_p)/\mathcal{Z}.$$

In accordance with [KS23, Def. 2.3.1] we denote the image of the homomorphism ρ_p defined in (7) with $n = p$ prime by

$$G_p := \rho_p\left(\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}\right) \subseteq \mathrm{GL}_2\left(\mathbb{F}_p\right).$$

Analogously with the projective linear group defined in Definition 41, we can also define the projective image as

$$\mathbb{P}G_p := G_p/\mathcal{Z},$$

where $\mathcal{Z}$ is the center of $\mathrm{GL}_2(\mathbb{F}_p)$ as defined in Proposition 40.

The projective images are introduced to simplify the process of excluding each maximal subgroup from containing the image of ρ_p. Below we present the proposition from [KS23, Prop. 2.3.4].

Proposition 43. *Let $G \leq \mathrm{GL}_2(\mathbb{F}_p)$ be a subgroup such that $\det(G) = \mathbb{F}_p^\times$ and $\mathbb{P}G = \mathrm{PGL}_2(\mathbb{F}_p)$. Then $G = \mathrm{GL}_2(\mathbb{F}_p)$.*

One can show that $\det \circ \rho_p$ is surjective, so $\det(G_p) = \mathbb{F}_p^\times$. Therefore, we only have to show that the projective image $\mathbb{P}G_p$ is not contained in any of the maximal subgroups of $\mathrm{PGL}_2(\mathbb{F}_p)$. Since $\det(G_p) = \mathbb{F}_p^\times$, we already know that $\mathbb{P}G_p$ is not contained in $\mathrm{PSL}_2(\mathbb{F}_p)$ for $p > 2$. For $p = 2$, $\mathrm{PGL}_2(\mathbb{F}_p) = \mathrm{PSL}_2(\mathbb{F}_p)$. To classify the rest of the maximal subgroups of $\mathrm{PGL}_2(\mathbb{F}_p)$, we use [KS23, Thm. 2.4.2].

Theorem 44. *Let $p \neq 2$ be a prime and let $q = p^{2e+1}$ be an odd power of p. The maximal subgroups of $\mathrm{PGL}_2(\mathbb{F}_q)$ different from $\mathrm{PSL}_2(\mathbb{F}_q)$ are as follows.*

(i) *(Borel) The stabilizer of a point of $\mathbb{P}^1(\mathbb{F}_q)$. It has order $q(q-1)$.*

(ii) *(Sub-line) The stabilizer $\mathrm{PGL}_2(\mathbb{F}_{q'})$ of a subline $\mathbb{P}^1(\mathbb{F}_{q'})$ by matrix multiplication, where $q = q'^\ell$ with a prime ℓ (in particular, $\ell \mid 2e+1$).*

(iii) *(Dihedral) Stabilizers of a pair of points in $\mathbb{P}^1(\mathbb{F}_q)$ (normalizer of a split Cartan subgroup, order $2(q-1)$, when $q > 5$) or of a pair of $\mathbb{F}_q$-conjugate points in $\mathbb{P}^1(\mathbb{F}_{q^2})$ (normalizer of a nonsplit Cartan subgroup, order $2(q+1)$).*

(iv) *(Exceptional) Subgroups isomorphic to S_4 (when $e = 0$ and $3 < p \equiv \pm 3 \mod 8$), and if $q = 3$, A_4.*

Although we are only concerned with $q = p$ in this thesis, we state the more general result for potential future extensions. Therefore, in this case, in Theorem 44, $q = p$, or, equivalently, $e = 0$. From now on we use the p instead of q for computations following the definition above.

Now we would like to derive criteria to show that $\mathbb{P}G_p \nsubseteq \Gamma$ for Γ being each of the maximal subgroups of $\mathrm{PGL}_2(\mathbb{F}_p)$ classified above. This can be done by using characteristic polynomials of $\rho_p(\mathrm{Frob}_\ell)$ for prime numbers $\ell \nmid Np$. From [KS23, Thm. 2.1.6] we know that these characteristic polynomials are of the form

$$T^2 - \bar{a}_\ell T + \bar{\ell},$$

where $\bar{x}$ denotes the image of x in the field $\mathbb{F}_p$.

Definition 45. *If $\mathbb{F}$ is a finite field of odd characteristic, the Legendre symbol of $a \in \mathbb{F}$ is defined as*

$$\left(\frac{a}{\mathbb{F}}\right) = \begin{cases} 0 & \text{if } a = 0, \\ 1 & \text{if } a = b^2 \text{ for some } b \in \mathbb{F}^\times, \\ -1 & \text{otherwise.} \end{cases}$$

Next, using [Ser72, § 2] we define some invariants associated to the elements of $\mathrm{PGL}_2(\mathbb{F}_p)$. Below we present the lemma describing these invariants from [KS23, Lem. 2.5.1].

Lemma 46. *Let $\mathbb{F}$ be a finite field.*

i. *The function*

$$\mathrm{GL}_2(\mathbb{F}) \to \mathbb{F}, \quad M \mapsto \frac{\mathrm{Tr}(M)^2}{\det(M)}$$

descends to a function $u : \mathrm{PGL}_2(\mathbb{F}) \to \mathbb{F}$.

ii. *Assume that $\mathbb{F}$ has characteristic $p \neq 2$. The function*

$$\mathrm{GL}_2(\mathbb{F}) \to \{0, 1, -1\}, \quad M \mapsto \left(\frac{\mathrm{Tr}(M)^2 - 4\det(M)}{\mathbb{F}}\right)$$

descends to a function $\Delta : \mathrm{PGL}_2(\mathbb{F}) \to \{0, 1, -1\}$.

Using the invariants presented above and the Fourier coefficients a_ℓ, we can compute

$$u(\ell) := u(\mathbb{P}\rho_p(\mathrm{Frob}_\ell)) = \frac{\bar{a}_\ell^2}{\bar{\ell}}, \quad \Delta(\ell) := \Delta(\mathbb{P}\rho_p(\mathrm{Frob}_\ell)) = \left(\frac{a_\ell^2 - 4\ell}{\mathbb{F}_p}\right)$$

for primes $\ell \nmid Np$.

To make conclusion about the order of elements in $\mathbb{P}G_p$, we need to employ the proposition below from [KS23, Prop. 2.5.3]

Proposition 47. *Let $\mathbb{F}$ be a finite field of characteristic p and let $g \in \mathrm{PGL}_2(\mathbb{F})$.*

1. *g is unipotent $\iff$ $u(g) = 4$ $\iff$ $\Delta(g) = 0$.*
2. *If $p \neq 2$: $\mathrm{ord}(g) = 2$ $\iff$ $u(g) = 0$.*
3. *If $p \neq 3$: $\mathrm{ord}(g) = 3$ $\iff$ $u(g) = 1$.*
4. *If $p \neq 2$: $\mathrm{ord}(g) = 4$ $\iff$ $u(g) = 2$.*
5. *If $p \neq 5$: $\mathrm{ord}(g) = 5$ $\iff$ $u(g)^2 - 3u(g) + 1 = 0$.*

Borel subgroup

Before deriving conditions of the image being contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ or not, we need to define what a Borel subgroup is explicitly. We present the definition below from [Lan02, p. 537].

Definition 48. *The standard Borel subgroup B of $\mathrm{GL}_2(\mathbb{F}_p)$ is the subgroup of all upper-triangular matrices, or, equivalently*

$$B := \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mid a, b, d \in \mathbb{F}_p, ab \neq 0 \right\} \subset \mathrm{GL}_2(\mathbb{F}_p).$$

The Borel subgroup is the subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ which is conjugate to the standard Borel subgroup. We can equally define the Borel subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$ by replacing $\mathrm{GL}_2(\mathbb{F}_p)$ with this group in the definition.

Any matrix in the Borel subgroup will have a reducible characteristic polynomial due to the structure of elements in the subgroup. Therefore, if we find a prime $\ell \nmid Np$ such that the characteristic polynomial of $\rho_p(\mathrm{Frob}_\ell)$ is irreducible, we can conclude that $\mathbb{P}G_p \not\subseteq B$. We know that $T^2 - \bar{a}_\ell + \bar{\ell}$ is irreducible if $a_\ell^2 - 4\ell$ is not a square in $\mathbb{F}_p$, which is equivalent to $\Delta(\ell) = -1$. This provides the criteria to conclude that $\mathbb{P}G_p \not\subseteq B$.

Sub-line stabilizer subgroups

Since we already know that in our case $e = 0$ in Theorem 44, we immediately find that $\ell = 1$. Therefore, $p = p'$ and the sub-line subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$ is simply the entire group $\mathrm{PGL}_2(\mathbb{F}_p)$. This means that in this case, the sub-line subgroup does not need to be considered.

Dihedral subgroups

From Theorem 44, we know that the dihedral subgroups of $\mathrm{PGL}_2(\mathbb{F}_q)$ correspond to the normalizer of a split Cartan subgroup and the normalizer of a nonsplit Cartan subgroup. Before deriving the conditions to show that $\mathbb{P}G_p$ is not contained in any of these maximal subgroups, we must first define what these subgroups are. Below we present the definitions from [LMF24, Split Cartan subgroup] and [LMF24, Non-split Cartan subgroup].

Definition 49. *A split Cartan subgroup $C_s \subset \mathrm{GL}_2(\mathbb{F}_p)$ is defined to be the subgroup conjugate to the subgroup of diagonal matrices. Therefore, up to conjugation, C_s is of the form*

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} : a, d \in \mathbb{F}_p, ad \neq 0 \right\}.$$

Definition 50. *A non-split Cartan subgroup $C_{ns} \subset \mathrm{GL}_2(\mathbb{F}_p)$ is defined to be the subgroup conjugate to*

$$\left\{ \begin{bmatrix} a & \epsilon b \\ b & a \end{bmatrix} : a, b \in \mathbb{F}_p, a^2 - \epsilon b^2 \neq 0 \right\},$$

where ϵ is the smallest positive integer generating $\mathbb{F}_p^\times$.

Now that we know what the Cartan subgroups are, we define the normalizer using [Lan02, p. 14].

Definition 51. *The normalizer $N_G(S)$ of a subset S of a group G is defined to be the subgroup of G of elements that normalize S. Equivalently, we can define*

$$N_G(S) := \{g \in G \mid gS = Sg\} = \{g \in G \mid gSg^{-1} = S\}.$$

From [KS23, p. 19] we know that the elements of $N(C) \setminus C$ have order 2, so $u = 0$ according to Proposition 47. The nontrivial elements of a split Cartan subgroup have $\Delta = 1$, while the nontrivial elements of a non-split Cartan subgroup have $\Delta = -1$. Therefore, if $p \neq 2$ and we find an element with $u \neq 0$ and $\Delta = -1$, we can exclude the normalizer of a split Cartan subgroup from containing the projective image $\mathbb{P}G_p$. Similarly, if $p \neq 2$ and we find an element with $u \neq 0$ and $\Delta = 1$, we can exclude the normalizer of a non-split Cartan subgroup from containing the image.

Exceptional subgroups

When $p \neq 3$, the only possible exceptional subgroup that can contain the projective image $\mathbb{P}G_p$ is S_4. To exclude this case, we need to consider the order of elements in S_4. We know that elements of this subgroup have order at most 4. Therefore, to show that $\mathbb{P}G_p \not\subseteq S_4$, we only have to find an element $g \in \mathbb{P}G_p$ such that $\mathrm{ord}(g) \geq 5$. According to Proposition 47, this happens when $u \notin \{0, 1, 2, 4\}$. Hence, if we find a prime $\ell \nmid Np$ such that $u(\ell) \notin \{0, 1, 2, 4\}$, we can exclude S_4 from containing the projective image $\mathbb{P}G_p$.

In this subsection we have derived all the necessary conditions to individually exclude all the maximal subgroups of $\mathrm{PGL}_2(\mathbb{F}_p)$ from containing $\mathbb{P}G_p$. Following this, we can implement an algorithm that can determine for which primes a fixed elliptic curve does not have a maximal mod p Galois representation.

5.2 Determining if the mod p image is maximal

Below we present an algorithm that loops over the primes ℓ for each prime p and computes the invariants to exclude the possible maximal subgroups from containing the projective image $\mathbb{P}G$. The symbol R is used to denote the Borel subgroup, N_s and N_{ns} for the normalizer of split and non-split Cartan subgroup and S_4 for the corresponding subgroup isomorphic to the symmetric group. This algorithm will return a list of all primes below the bound that do not have a surjective mod p Galois representation.

Algorithm 2.
Input: An elliptic curve E.
A bound B.

Output: A list of primes for which the image of the mod p Galois representation of E is not maximal.

1. [Initialize] Set *non_max_primes* := [ ] to store the primes for which the image is not maximal.
2. Compute the modular form f of E to find the Fourier coefficients a_ℓ of f.
3. Compute the conductor N of E.
4. [Loop over primes] For all primes $p \leq B$:
   a. If $p = 3$, compute the three-torsion subgroup using $ThreeTorsionType(E)$, and if it is not *Generic* (= maximal image), then add 3 to *non_max_primes*.
   b. Set $S = \{R, N_s, N_{ns}, S_4\}$.
   c. If $p = 2$, remove N_s, N_{ns} and S_4 from S.
   d. If $p \not\equiv \pm 3 \mod 8$, then remove S_4 from S.
   e. For each prime $\ell \leq B$ such that $\ell \nmid Np$:
      i. Compute the image $u(\ell)$ of a_ℓ^2/ℓ in $\mathbb{F}_p$.
      ii. If $p \neq 2$, compute $\Delta(\ell) := \left(\frac{a_\ell^2 - 4\ell}{\mathbb{F}_p}\right)$
      iii. If $u \notin \{0, 1, 2, 4\}$, remove S_4 from S.
      iv. If $p = 2$ and $u = 1$, remove R from S.
      v. If $p \neq 2$ and $\Delta = -1$, remove R from S.
      If in addition $u \neq 0$, remove N_s from S.
      vi. If $p \neq 2$, $\Delta = 1$ and $u \neq 0$, then remove N_{ns} from S.
   f. If $S \neq \varnothing$, add p to *non_max_primes*.
5. Return *non_max_primes*.

Using the algorithm presented above, we can check for which primes the mod p image of an elliptic curve is not maximal. This is essential in our process of construction of $\mathrm{GL}_2(\mathbb{F}_p)$ extensions.

5.3 Computation of elements generating $\mathbb{Q}(E[p])$

Now that we have derived a method to verify whether an elliptic curve has a maximal mod p Galois representation, we can start laying out an approach to compute the polynomials generating the extensions with Galois group isomorphic to $\mathrm{GL}_2(\mathbb{F}_p)$. We begin by computing the degree of the extension, and thus, the generating polynomial.

Proposition 52. *The order of the group* $\mathrm{GL}_2(\mathbb{F}_p)$ *is* $(p^2 - 1)(p^2 - p)$.

Proof. To compute the number of elements in $\mathrm{GL}_2(\mathbb{F}_p)$, we must recall the properties of the group. The first row of each element in $\mathrm{GL}_2(\mathbb{F}_p)$ can be any vector in $\mathbb{F}_p^2$ except the zero vector since the determinant must be non-zero. Then we can deduce that the second row of any element can be any vector in $\mathbb{F}_p^2$ except the scalar multiples of the first row, again due to the fact that the determinant must be non-zero. There are exactly p possibilities of a scalar multiple of the first row of the matrix. This means that there are $p^2 - p$ choices for the second row of the matrix. Combining this, we can see that there are $(p^2-1)(p^2-p)$ ways to construct an element of $\mathrm{GL}_2(\mathbb{F}_p)$, which proves the proposition. □

Using this proposition, we can already compute the degree of the desired polynomial. According to Theorem 3,

$$[\mathbb{Q}(E[p]) : \mathbb{Q}] = \#\operatorname{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) = \#\,\mathrm{GL}_2(\mathbb{F}_p) = (p^2 - 1)(p^2 - p).$$

Therefore, the degree of the polynomial that has a splitting field $\mathbb{Q}(E[p])$ will be $(p^2 - 1)(p^2 - p)$.

Using Algorithm 2, we can determine for which primes the Galois representation is maximal for a specific elliptic curve. Thus, if we find an elliptic curve E that has a maximal image for a

desired prime p (or more), we can use the p-torsion group $E[p]$ to construct the field extension $\mathbb{Q}(E[n])$ which will have a maximal Galois group, which is isomorphic to $\mathrm{GL}_2(\mathbb{F}_p)$. To find a specific polynomial generating the extension for a fixed value of p, we must first investigate the intermediate fields and the degrees of extensions.

Since we already established that the field extension $\mathbb{Q}(E[p])$ is constructed by adjoining the x and y coordinates of all the p-torsion points of E, a natural question one might ask is what is the degree of extension when adjoining only one non-trivial p-torsion point to $\mathbb{Q}$. To answer this question, we must look at the tower of extensions.

$$\begin{array}{c} \mathbb{Q}(E[p]) \\ | \\ \mathbb{Q}(P) \\ | \\ \mathbb{Q} \end{array}$$

The degree of the field extension $\mathbb{Q}(E[p])/\mathbb{Q}(P)$ is exactly the number of elements of its Galois group. As we already know that the Galois group of the extension $\mathbb{Q}(E[p])/\mathbb{Q}$ is the group of invertible 2×2 matrices over the field $\mathbb{F}_p$, we can deduce that the Galois group of the extension $\mathbb{Q}(E[p])/\mathbb{Q}(P)$ will be the subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ consisting of matrices that preserve the point P.

Definition 53 (Stabilizer)**.** *Let G be a group acting on a set B and let x be an element of B. Then the stabilizer of x is defined as*

$$\mathrm{Stab}_G(x) = \{g \in G \mid g(x) = x\},$$

and it consists of all elements of G that fix the point x.

Combining what we saw before, we now know that $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}(P) \cong \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{F}_p)}(P)$. Now we would like to compute the order of the stabilizer of the point P.

Proposition 54. $\#\,\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{F}_p)}(P) = p^2 - p$.

Proof. Let $P = a_1P_1 + a_2P_2$, where $a_1, a_2 \in \mathbb{F}_p$ and P_1, P_2 are the generators of the group $E[p]$ as defined in Equation (6). We would like to find how many matrices $A \in \mathrm{GL}_2(\mathbb{F}_p)$ exist such that

$$A \cdot \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}.$$

Any nonzero vector in $\mathbb{F}_p^2$ can be linearly transformed to a basis vector $(1, 0)$. Therefore, we only have to compute how many matrices in $\mathrm{GL}_2(\mathbb{F}_p)$ stabilize the vector $(1, 0)$. Let

$$D = \begin{bmatrix} d_1 & d_2 \\ d_3 & d_4 \end{bmatrix} \in \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{F}_p)}((1, 0)).$$

Therefore, we have that

$$D \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \Longrightarrow \quad \begin{bmatrix} d_1 & d_2 \\ d_3 & d_4 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \Longrightarrow \quad \begin{bmatrix} d_1 \\ d_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

This shows that $d_1 = 1$ and $d_3 = 0$. Hence, we can see that the stabilizer of $(1, 0)$ consists of matrices of the form

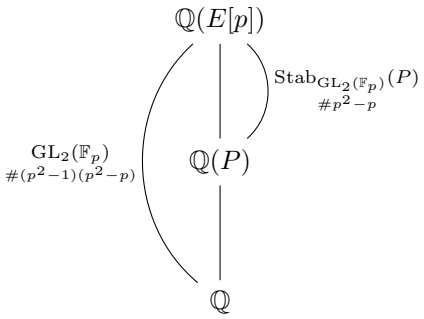
$$\begin{bmatrix} 1 & d_2 \\ 0 & d_4 \end{bmatrix}, \quad \text{where } d_2 \in \mathbb{F}_p,\ d_4 \in \mathbb{F}_p^{\times}.$$

The choice that $d_4 \in \mathbb{F}_p^\times$ instead of the whole field $\mathbb{F}_p$ comes from the fact that we require the determinant of the matrix to be nonzero to be in the group $\mathrm{GL}_2(\mathbb{F}_p)$. Consequently,

$$\#\operatorname{Stab}_{\mathrm{GL}_2(\mathbb{F}_p)}(P) = \#\operatorname{Stab}_{\mathrm{GL}_2(\mathbb{F}_p)}((1,0)) = \#\mathbb{F}_p \cdot \#\mathbb{F}_p^\times = p(p-1) = p^2 - p,$$

which proves the proposition. □

Now that we know the Galois groups of $\mathbb{Q}(E[p])/\mathbb{Q}$ and $\mathbb{Q}(E[p])/\mathbb{Q}(P)$ and their respective cardinalities, we can add this information to our illustration of the tower of extensions.



From this, we can compute the degree of the extension $\mathbb{Q}(P)/\mathbb{Q}$ using the tower law. According to Theorem 6,

$$[\mathbb{Q}(P):\mathbb{Q}] = \frac{[\mathbb{Q}(E[p]):\mathbb{Q}]}{[\mathbb{Q}(E[p]):\mathbb{Q}(P)]} = \frac{(p^2-1)(p^2-p)}{p^2-p} = p^2 - 1.$$

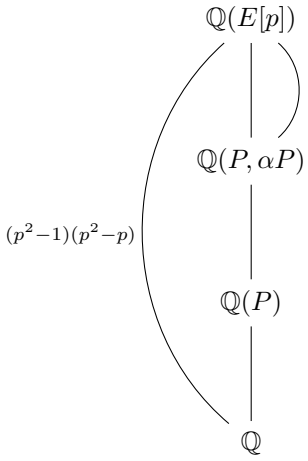
So far we know that the degree of the field extension when adjoining all p-torsion points of E to $\mathbb{Q}$ is $(p^2-1)(p^2-p)$ and the degree when adjoining just one of these points to $\mathbb{Q}$ is p^2-1. We can easily see that we do not even have to consider all the p-torsion points of E to construct the polynomial generating the full extension. To elaborate on this, recall the representation of the p-torsion group using two generators, repeated from Equation (6):

$$E[p] = \{a_1P_1 + a_2P_2 \mid a_1, a_2 \in \mathbb{F}_p\}.$$

Looking closer at this representation, we can already see there is some redundancy - some of the points are multiples of others. If this were multiplication in the usual sense over $\mathbb{Q}$, we could already claim that adjoining one point to $\mathbb{Q}$ will yield the same extension as adjoining all the multiples of this point to $\mathbb{Q}$. Since in this case, multiplication by a scalar corresponds to the addition of points on an elliptic curve, we cannot make this claim without further elaboration. This is because the coordinates of a multiple of a point on the elliptic curve will not be multiples of the original point. Turns out this issue can be resolved by considering a tower of extensions again, this time by considering the extensions $\mathbb{Q}(P)$ and $\mathbb{Q}(P, \alpha P)$, where $\alpha \in \mathbb{F}_p^\times$.

Proposition 55. *If $P \in E[p]$, then $\mathbb{Q}(P) = \mathbb{Q}(P, \alpha P)$ for $\alpha \in \mathbb{F}_p^\times$.*

Proof. To begin the proof, we once again lay out a tower of extensions.



Using this tower of extensions, we would now like to compute the degree of the extension $\mathbb{Q}(E[p])/\mathbb{Q}(P, \alpha P)$. This can be done by once again considering its Galois group - this will be the subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ consisting of matrices that preserve both P and αP. If $P = a_1P_1 + a_2P_2$, then $\alpha P = \alpha a_1 P_1 + \alpha a_2 P_2$. Therefore, we need to find which matrices preserve the vectors (a_1, a_2) and $(\alpha a_1, \alpha a_2)$. Coming back to the definition of stabilizer, we know that if A stabilizes a vector (a_1, a_2), this means that

$$A \cdot \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \quad \Longrightarrow \quad A \cdot \alpha \cdot \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} = \alpha \cdot \begin{bmatrix} a_1 \\ a_2 \end{bmatrix},$$

therefore, A also stabilizes the scalar multiple of the vector. This means that $\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{F}_p)}(P) = \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{F}_p)}(P, \alpha P)$. From this, we know that

$$[\mathbb{Q}(E[p]) : \mathbb{Q}(P)] = [\mathbb{Q}(E[p]) : \mathbb{Q}(P, \alpha P)].$$

Since $\mathbb{Q}(P) \subset \mathbb{Q}(P, \alpha P)$, this indeed proves that $\mathbb{Q}(P) = \mathbb{Q}(P, \alpha P)$. □

Now we have to consider points in $E[p]$ that are not scalar multiples of each other. As it turns out, this is where projective spaces come in handy again, more specifically, the projective line, which identifies two vectors if they are scalar multiples of each other. Following the more general Definition 25, we can define the projective line as follows.

Definition 56 (Projective line)**.** *The projective line $\mathbb{P}^1(\mathbb{F}_p)$ over the finite field $\mathbb{F}_p$ is defined as the the set of all 2-tuples $(x_0, x_1) \in \mathbb{F}_p^2$ such that at least one of x_0 and x_1 is nonzero, together with the equivalence relation*

$$(x_0, x_1) \sim (y_0, y_1) \quad \Longleftrightarrow \quad \text{there exists } \lambda \in \mathbb{F}_p^\times \text{ such that } x_0 = \lambda y_0 \text{ and } x_1 = \lambda y_1.$$

Proposition 57. *The set of all points on the projective line $\mathbb{P}^1(\mathbb{F}_p)$ can be written explicitly as*

$$\mathbb{P}^1(\mathbb{F}_p) = \{(1, 0), (0, 1), (1, 1), (2, 1), \ldots, (p-1, 1)\}. \tag{8}$$

Moreover, the cardinality of this set is $\#\mathbb{P}^1(\mathbb{F}_p) = p + 1$.

Proof. We begin by working out the number of elements on the projective line. We know that $\mathbb{F}_p^2$ contains exactly $p^2 - 1$ nonzero vectors. In the projective line, two vectors are identified if they are scalar multiples of one another. Therefore, each nonzero vector in $\mathbb{F}_p^2$ is identified with $\#\mathbb{F}_p^\times = p - 1$ others. As a result, there are exactly $\frac{p^2-1}{p-1} = p + 1$ distinct points in $\mathbb{P}^1(\mathbb{F}_p)$.

Secondly, to show that any point in $\mathbb{P}^1(\mathbb{F}_p)$ can be written in the form 8, we consider two cases. Let $(a, b) \in \mathbb{P}^1(\mathbb{F}_p)$.

- If $b = 0$, we can see that $(a, b) \equiv (a, 0) \equiv a^{-1}(a, 0) \equiv (1, 0)$.

- If $b \neq 0$, we have that $(a, b) \equiv b^{-1}(a, b) \equiv (ab^{-1}, 1)$.

This shows that any point on the projective line is in the form as in 8. □

Now that we have established that the p-torsion points of E that correspond to the same point in $\mathbb{P}^1(\mathbb{F}_p)$ generate the same extension of $\mathbb{Q}$, a natural question that might arise is what happens if we adjoin two points with different representatives of $\mathbb{P}^1(\mathbb{F}_p)$ to $\mathbb{Q}$.

Let $P = a_1P_1 + a_2P_2$ and $Q = b_1P_1 + b_2P_2$ be two p-torsion points of E such that they have different representatives in $\mathbb{P}^1(\mathbb{F}_p)$, meaning that $(a_1, a_2) \neq (b_1, b_2)$ in $\mathbb{P}^1(\mathbb{F}_p)$, or that the two vectors are linearly independent. Now consider the field extension $\mathbb{Q}(P)(Q)$ generated by the x and y coordinates of these points. We would like to compute $[\mathbb{Q}(E[p]) : \mathbb{Q}(P)(Q)]$. This can be done by considering what the elements of $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}(P)(Q))$ are. These are the matrices of $\mathrm{GL}_2(\mathbb{F}_p)$ that stabilize both of the vectors (a_1, a_2) and (b_1, b_2).

Proposition 58. *If $v, w \in \mathbb{F}_p^2$ are two linearly independent vectors, then*

$$\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{F}_p)}(v) \cap \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{F}_p)}(w) = \{I\}.$$

Proof. Let $A \in \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{F}_p)}(v) \cap \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{F}_p)}(w)$. This means that

$$Av = v \quad \& \quad Aw = w.$$

Let $a, b \in \mathbb{F}_p$. Then we have that

$$A(av + bw) = aAv + bAw = av + bw \quad \Longrightarrow \quad (A - I)(av + bw) = 0.$$

Since $v, w \in \mathbb{F}_p^2$ are linearly independent, they form a basis of $\mathbb{F}_p^2$. Therefore, we have found that $(A - I)u = 0$ for all $u \in \mathbb{F}_p^2$. This implies that $A - I = 0$, hence, $A = I$. We have just shown that if $A \in \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{F}_p)}(v) \cap \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{F}_p)}(w)$, then $A = I$, which concludes the proof. □

As a consequence of Proposition 58, the Galois group of $\mathbb{Q}(E[p])/\mathbb{Q}(P)(Q)$ consists only of one element - the identity matrix. This implies that $[\mathbb{Q}(E[p]) : \mathbb{Q}(P)(Q)] = 1$, which means that $\mathbb{Q}(E[p]) = \mathbb{Q}(P)(Q)$ for P and Q being two points in the p-torsion group with different representatives in $\mathbb{P}^1(\mathbb{F}_p)$.

5.4 Construction of polynomials generating $\mathrm{GL}_2(\mathbb{F}_p)$ extensions of $\mathbb{Q}$

Below we present the algorithm to construct the polynomial generating the extension with Galois group isomorphic to $\mathrm{GL}_2(\mathbb{F}_p)$, given that we have already found an elliptic curve that has a maximal image modulo p using Algorithm 2. In the implementation, we choose P_1 and P_2 to be the generators of $E[p]$ as defined in (5). Therefore, the field extension will be constructed using the fact that $\mathbb{Q}(E[p]) = \mathbb{Q}(P_1)(P_2)$.

The elliptic curve in the input of the Magma function has to be in Weierstrass form $y^2 = x^3 + ax^2 + bx + c$.

Algorithm 3.
INPUT: A prime p.
An elliptic curve E in Weierstrass form with maximal image modulo p.

OUTPUT: Polynomial $g \in \mathbb{Q}[x]$ that generates the extension $\mathbb{Q}(E[p])$ with Galois group isomorphic to $\mathrm{GL}_2(\mathbb{F}_p)$.

1. Using Algorithm 2, verify that E has a maximal mod p Galois representation. If not, output an error label.

2. Compute the analytic Jacobian J of the function f defining the elliptic curve $E : y^2 = f(x)$.

3. Compute the full period matrix of J. This will be a 1×2 matrix $[\omega_1\ \omega_2]$, where ω_1 and ω_2 are the periods of the lattice Λ.
4. Compute the generators of the lattice Λ as $\frac{\omega_1}{p}$ and $\frac{\omega_2}{p}$.
5. Using the analytic Jacobian J, map the generators of the lattice to the generators P_1 and P_2 of $E[p]$.
6. For the point $P_1 = (x, y) \in E[p]$:
   a. Compute the minimal polynomials f_1 and f_2 of the x and y coordinates of the point over $\mathbb{Q}$.
   b. Create the number field $K = \mathbb{Q}(\alpha)$ obtained by adjoining a root α of f_1 to $\mathbb{Q}$.
   c. Extend the field K by adjoining a root β of f_2 to K to find the field $L = K(\beta)$. This will be the field extension $\mathbb{Q}(P_1)$ of degree $p^2 - 1$.
   d. Verify that P_1 is not the point at infinity, and that $[p]P_1 = \mathcal{O}$. If this is satisfied, P_1 is indeed a p-torsion point of E.
   e. Repeat the same procedure for P_2 to construct the field extension $\mathbb{Q}(P_2)$.
7. Compute the composite field $\mathbb{Q}(P_1)(P_2)$ of degree $(p^2-1)(p^2-p)$ of the fields $\mathbb{Q}(P_1)$ and $\mathbb{Q}(P_2)$. This will be the field extension $\mathbb{Q}(E[p])$.
8. Compute the minimal polynomial $g \in \mathbb{Q}[x]$ of a primitive element of $\mathbb{Q}(E[p])$. This will be an irreducible polynomial of degree $(p^2 - 1)(p^2 - p)$.
9. Return g.

The algorithm above provides a method to compute a polynomial generating a $\mathrm{GL}_2(\mathbb{F}_p)$ extension of $\mathbb{Q}$. It is important to note that this polynomial is accurate up to the chosen precision. Therefore, even though we work with algebraic numbers of complex approximations, step 6.d in Algorithm 3 verifies that the found point is indeed a p-torsion point of E up to the chosen precision. This is done by verifying that the point does not overlap with the point at infinity and that adding this point to itself p times will yield the point at infinity. If these conditions are satisfied, then the point found will be an algebraic approximation to the (possibly non-algebraic) generator of the p-torsion group.

6 Conclusion

In this paper, we proved some sub-results concerning the open Inverse Galois problem for two classes of groups.

First, using cyclotomic extensions of $\mathbb{Q}$, we proved the well-known result that any finite abelian group A appears as the Galois group of some intermediate field of a cyclotomic extension. Furthermore, we showed that this extension is not unique. Because of this, we also saw that we can always construct the field extension in a way that it is totally real. Additionally, by computing the primitive element of the extension, we can find a polynomial $f \in \mathbb{Q}[X]$ such that the splitting field of this polynomial will be the field extension with Galois group isomorphic to A.

Second, we provided a brief introduction to projective geometry and elliptic curves. Using the concept of p-torsion points, we established a connection between elliptic curves and Galois representations. To investigate whether an elliptic curve has a maximal mod p Galois representation, we classified the maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$. We provided the necessary criteria to show that the image of the Galois representation is not contained in any of the maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$. This was used to find when the Galois representation of an elliptic curve is indeed isomorphic to the general linear group.

After finding a suitable elliptic curve whose p-torsion points generate the desired field extension of $\mathbb{Q}$, we outlined the procedure to compute the polynomial generating this extension.

In conclusion, this paper provides a systematic approach to find the field extensions with Galois group isomorphic to any finite abelian group or $\mathrm{GL}_2(\mathbb{F}_p)$, as well as a procedure to compute the polynomials generating these extensions.

References

[Asc94] Michael Aschbacher. *Sporadic groups*. Number 104. Cambridge University Press, 1994.

[Edw84] Harold M. Edwards. *Galois theory*. Springer New York, 1984.

[KS23] Timo Keller and Michael Stoll. Complete verification of strong BSD for many modular abelian surfaces over $\mathbf{Q}$, 2023.

[Lan02] S. Lang. *Algebra*. Springer, 3 edition, 2002.

[LMF24] The LMFDB Collaboration. The L-functions and modular forms database. https://www.lmfdb.org, 2024.

[MM18] Gunter Malle and B. Heinrich Matzat. *Inverse Galois Theory*. Springer Berlin, Heidelberg, 2 edition, 2018.

[Ros11] Kenneth H. Rosen. *Elementary number theory and its applications*. Addison-Wesley, 6 edition, 2011.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. math*, 15:259–331, 1972.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer New York, NY, 2 edition, 2009.

[ST15] Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves*. Springer Cham, 2 edition, 2015.

Appendix

Magma code corresponding to Algorithm 1

```
Qx<x> := PolynomialRing(Rationals());

function abelian_polynomial(a_list: totally_real:=true)

primes_list := []; // list to store primes p_i
subgroups := []; // list to store subgroups B_i

// finding the necessary primes and subgroups of (Z/p_iZ)^*
for a in a_list do
    prime := 0; // initialize prime for each a

    for p in PrimesUpTo(1000) do // iterate through primes < 1000
        if (p mod (totally_real select 2*a else a)) eq 1 then // check
            if p is congruent 1 mod a or 2a (for a totally real
           extension)
            if p notin primes_list then // check if p_i is distinct
               from the other primes
                Append(~primes_list, p); // append p_i to primes_list

                generator := PrimitiveRoot(p); // generator of (Z/p_iZ
                   )^*
                gen := generator^a; // generator of the subgroup B_i
                bsize := (p - 1) div a; // cardinality of B_i
                subgroup := [gen^i mod p : i in [1..bsize]]; //
                   constructing the subgroup B_i
                Append(~subgroups, subgroup); // append B_i to list of
                    subgroups
                break;
            end if;
        end if;
    end for;
end for;

N := &*[prime : prime in primes_list]; // computing N = p_1 * p_2 *
    ... p_n

B := []; // initializing the subgroup B

iterators := [1 : _ in a_list]; // initializing a list of the same
   size as a_list containing only 1's

all_done := false;
while not all_done do // loop over all combinations of elements in B_1
    x B_2 x ... B_n

    current_elements := []; // initializing a list to store the
       current elements from subgroups

    for i in [1..#a_list] do
        current_elements[i] := subgroups[i][iterators[i]]; //
```

```
            combination of elements corresponding to iterators
        end for;

        combined_element := CRT(current_elements, primes_list); //
            computing the element of B corresponding to current_elements of
             B_1 x B_2 x ... x B_n
        Append(~B, combined_element); // appending the element to subgroup
             B

        for i in Reverse([1..#a_list]) do // updating iterators
            iterators[i] +:= 1;
            if iterators[i] le #subgroups[i] then
                break;
            elif i eq 1 then
                all_done := true;
            else
                iterators[i] := 1;
            end if;
        end for;
    end while;

    K<w> := CyclotomicField(N);
    alpha := &+[K| w^x : x in B]; // primitive element generating the
        extension
    f := MinimalPolynomial(alpha); // polynomial generating the extension;
         minimal polynomial of c

    return f;
    end function;

    a_list := [5, 2, 2]; // an example input of numbers corresponding to
        abelian group A
    f := abelian_polynomial(a_list); // the corresponding minimal
        polynomial generating the extension
    Qalpha := NumberField(f); // the corresponding extension Q(c)
        generated by f

    f;
    IsTotallyReal(Qalpha); // this will return true or false depending on
        whether Q(alpha) is totally real or not.
```

Magma code corresponding to Algorithm 2 and 3

```
C<I> := ComplexField(200);
Cx<x> := PolynomialRing(C);

function non_maximal_primes(E, B)
    // E: an elliptic curve
    // B: the bound

    non_max_primes := [];
    primes := PrimesUpTo(B);
```

```
f := ModularForm(E);
qexp := qExpansion(f, B);
l_list := PrimesUpTo(B);
OK := Integers(CoefficientField(f));
al_list := [OK | Coefficient(qexp, l) : l in l_list];

N := Conductor(E);

for p in primes do
    if p eq 3 then
        if ThreeTorsionType(E) ne "Generic" then
            Append(~non_max_primes, p);
        end if;
    else
        S := {"R", "Ns", "Nns", "S4"};
        if p eq 2 then S diff:= {"Ns", "S4", "Nns"}; end if;
        if p mod 8 notin {3, 5} then Exclude(~S, "S4"); end if;

        F, toFp := ResidueClassField(p);

        for i -> l in l_list do
            if l ne p and not IsDivisibleBy(N, l) then
                u := toFp(al_list[i])^2 / toFp(l);
                if p ne 2 then
                    D := toFp(al_list[i])^2 - toFp(4 * l);
                    D := (D eq 0) select 0 else (IsSquare(D)
                        select 1 else -1);
                // else
                  //  D := 0; // Initialize D for p == 2
                end if;

                if u notin {F | 0, 1, 2, 4} then Exclude(~S, "S4")
                    ; end if;
                if p eq 2 and u eq 1 then Exclude(~S, "R"); end if
                    ;

                if p ne 2 and D eq -1 then
                    Exclude(~S, "R");
                    if u ne 0 then Exclude(~S, "Ns"); end if; end
                        if;
                if p ne 2 and D eq 1 and u ne 0 then
                    Exclude(~S, "Nns");
                end if;

                if IsEmpty(S) then break; end if;
            end if;
        end for;

        if not IsEmpty(S) then
            Append(~non_max_primes, p);
        end if;
    end if;
end for;
```

```
    return non_max_primes;
end function;

function gen_pol(E,p)
    // E: an elliptic curve in Weierstrass form
    // p: a prime

    nonMaxPrimes := non_maximal_primes(E, p+1);
    if p in nonMaxPrimes then
        printf "The %o does not have a maximal mod %o Galois
            representation\n", E, p;
    else

    a2 := Coefficients(E)[2];
    a4 := Coefficients(E)[4];
    a6 := Coefficients(E)[5];
    f := x^3 + a2 * x^2 + a4 * x + a6;

    J := AnalyticJacobian(f);
    W := BigPeriodMatrix(J);

    w_1 := Matrix([[W[1][1]]]); // quantities associated to the
        lattice Lambda
    w_2 := Matrix([[W[1][2]]]);

    P1 := FromAnalyticJacobian(w_1/p, J);
    f1 := MinimalPolynomial(P1[1][1],p^2);
    f2 := MinimalPolynomial(P1[1][2],p^2);

    P2 := FromAnalyticJacobian(w_2/p, J);
    g1 := MinimalPolynomial(P2[1][1],p^2);
    g2 := MinimalPolynomial(P2[1][2],p^2);

    K<a> := NumberField(f1);
    L<b> := ext<K | Factorization(ChangeRing(f2, K))[1,1] >;
    EL := BaseExtend(E,L);
    pt := EL![a,b];
    assert (pt ne EL!0) and (p*pt eq EL!0);

    K1<a1> := NumberField(g1);
    L1<b1> := ext<K1 | Factorization(ChangeRing(g2, K1))[1,1] >;
    EL1 := BaseExtend(E,L1);
    pt1 := EL1![a1,b1];
    assert (pt1 ne EL1!0) and (p*pt1 eq EL1!0);

    B := CompositeFields(L, L1);

    i := 0;
    while i lt # B do
        i +:= 1;
        if Degree(B[i]) eq (p^2-1)*(p^2-p) then
            QE := B[i];
        end if;
    end while;
```

```
    F := MinimalPolynomial(PrimitiveElement(QE));

return F;
end if;
end function;

E := EllipticCurve([0, 0, 0, -1, 1]);
p := 3;

F := gen_pol(E,p);
F;
IsIrreducible(F);
```