Entanglement of Galois representations of elliptic curves over $\mathbb{Q}$

Master's Thesis

Joost Mein, under the supervision of Valentijn Karemaker,
with Gunther Cornelissen as second reader

August 24, 2022

ABSTRACT. When studying elliptic curves over a field K one can define their n-torsion fields to be K adjoined with the x, y-coordinates of the n-torsion points. Then we can look at the Galois representations associated to these n-torsion fields and ask when these representations are surjective. It turns out that there are multiple ways in which the image can fail to be surjective, corresponding to different kinds of entanglement. We focus mainly on so-called horizontal entanglements and different ways in which these can occur. Of particular interest will be Weil entanglement and Serre entanglement. The latter occurs because of the fact that the discriminant of an elliptic curve is always contained in a cyclotomic field, as implied by the Kronecker-Weber theorem. One of the main contributions will be on how Serre entanglement induces horizontal entanglement. Furthermore we will study Weil entanglement by looking at the conductor of corresponding quadratic and cubic number fields.

Table of contents

1 Introduction

For an elliptic curve $E/\mathbb{Q}$ it is a fact that the torsion subgroup of E, given by $E[n]$, is a $\mathbb{Z}/n\mathbb{Z}$-module for $n \in \mathbb{N}$ isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. The automorphisms of $E[n]$ form a group, denoted by $\mathrm{Aut}(E[n])$, which is isomorphic to $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$. A Galois representation is defined as a continuous group homomorphism from the absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ to a general linear group $\mathrm{GL}(n, R)$ with R a topological ring. We have that $\sigma \in G_{\mathbb{Q}}$ permutes n-torsion points of E, and therefore this gives rise to a Galois representation

$$\rho_{E,n} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z}).$$

We also have the following Galois representations, induced by the ℓ-adic Tate module $T_\ell(E)$ and adelic Tate module $T(E)$:

$$\rho_{E,\ell^\infty} : G_{\mathbb{Q}} \to \mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}(2, \mathbb{Z}_\ell),$$

$$\rho_E : G_{\mathbb{Q}} \to \mathrm{Aut}(T(E)) \cong \mathrm{GL}(2, \hat{\mathbb{Z}}).$$

The different reasons for which the images of these Galois representations can be non-surjective are defined as entanglement, which is mainly divided in vertical entanglement and horizontal entanglement. Vertical entanglement happens when ρ_{E,ℓ^∞} is non-surjective for some prime ℓ, while horizontal entanglement happens when $\rho_{E,n}$ is non-surjective but ρ_{E,p^e} is surjective for all p primes such that $p^e \mid n$. This occurs when $\mathbb{Q} \subsetneq \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b])$ for a, b coprime divisors of n, as we will show in Chapter 3.

There has been a lot of research already aimed at understanding when the full representation ρ_E is non-surjective, see for instance [5],[8],[9],[11],[27],[28]. If E has no CM then it has been shown by Serre [33] that the image of ρ_E is always an open subgroup of $\mathrm{GL}(2, \hat{\mathbb{Z}})$ and therefore it has finite index i_E. This is refered to as Serre's open image theorem. Serre also showed that i_E is always ≥ 2 for an elliptic curve over $\mathbb{Q}$, so the full representation is never surjective. For $E/\mathbb{Q}$ an elliptic curve with CM we have that the image of the full representation is very small [4].

In Chapter 2 we will start by listing necessary properties of elliptic curves and results of Galois theory. Then we will be able to define the notion of Galois representations and in particular Galois representations of elliptic curves.

Then in Chapter 3 we will define different kinds of entanglement, starting with vertical and horizontal entanglement, mainly following [11]. We will then focus in more detail on Serre entanglement, which is entanglement induced by $\mathbb{Q}(\Delta_E) \subseteq \mathbb{Q}(E[2]) \cap \mathbb{Q}(\zeta_n)$ for some $n \geq 3$ with Δ_E being the discriminant of E. Some new contributions done by myself are for instance showing in what ways Serre entanglement is responsible for a smaller image of ρ_E and providing infinite non-isomorphic families of elliptic curves over $\mathbb{Q}$ which have Serre entanglement for specific $n \geq 3$.

In Chapter 4 we will introduce modular curves. By studying non-cuspidal rational points on the modular quotient curve X_H with $H \subseteq \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\}$, one can try to classify all elliptic curves $E/\mathbb{Q}$ for which $\mathrm{Im}(\rho_{E,N})$ is conjugate to a subgroup of H. This is called Mazur's Program B [24] and has been extensively studied, see for example [27], [28]. For instance in [27] all elliptic curves over $\mathbb{Q}$ are classified which have a certain form of vertical ℓ-entanglement by studying rational points on the modular quotient curve X_H with $H \subseteq \mathrm{GL}(2, \mathbb{Z}_\ell)/\{-I\}$.

Finally in Chapter 5 we will focus in more detail on Weil entanglement, which for instance occurs for elliptic curves with a rational point of order p with p prime and is induced by $\mathbb{Q}(P) \subseteq \mathbb{Q}(E[p]) \cap \mathbb{Q}(\zeta_n)$ for some $n \in \mathbb{N}$. Here n is equal to the conductor of $\mathbb{Q}(P)$, which is an abelian cyclic field. We will mainly focus on the cases where $p = 2, 3$. I contributed to this topic by studying the conductor of $\mathbb{Q}(P)$, which is the smallest integer $n \geq 1$ for which $\mathbb{Q}(P) \subseteq \mathbb{Q}(\zeta_n)$, and using this to pinpoint where the Weil entanglement occurs. We will also list infinite families of non-isomorphic elliptic curves over $\mathbb{Q}$ which have certain forms of Weil entanglement, following [11].

2 Galois representations of elliptic curves

2.1 Elliptic curves

We start this chapter by stating a few important properties of elliptic curves. For this subsection we refer to [35].

Definition 2.1. Let K be a field. An **elliptic curve E defined over** K is a projective curve described by the homogenisation of a *Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_i \in K$ and $\Delta_E \neq 0$. Δ_E is called the **discriminant of** E and is a polynomial expression in the coefficients a_i. Another important variable is the **j-invariant of** E, usually referred to as $j(E)$. E also has the point at infinity $\mathcal{O} := (0 : 1 : 0) \in \mathbb{P}^2(K)$.

An important property of the aforementioned j-invariant is that for elliptic curves $E, E'/K$ we have that $E \cong E'$ over $\bar{K}$ if and only if $j(E) = j(E')$ [35,III.1.4].

We have that if $\mathrm{char}(K) \neq 2, 3$, then every elliptic curve $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, over K is isomorphic to an elliptic curve E' over K given by a so-called *short Weierstrass equation*

$$E' : y^2 = x^3 + Ax + B \tag{1}$$

with $A, B \in K$ [35, III.1.3]. In this case we have

$$\Delta_E = -16 \cdot (4A^3 + 27B^2) \quad \text{and} \quad j(E) = 1728 \cdot \frac{4A^3}{4A^3 + 27B^2}.$$

In this case the isomorphism between E and E' is given by

$$(x, y) \to \left(\frac{x - 3(a_1^2 + 4a_2)}{36}, \frac{1}{216}(y - a_1x - a_3)\right).$$

Note that this isomorphism is defined over K. For such an elliptic curve E/K we say that E can be written in short Weierstrass form.

We have that rational maps between elliptic curves $E, E'/K$ are called isogenies, which are given by rational maps of algebraic curves for which $\mathcal{O}_E$ is sent to $\mathcal{O}_{E'}$. If these maps are not the zero map, then they always have a finite kernel [35, III.4.9]. If K is separable we say that E has a n-isogeny if it has an isogeny with kernel of order n. This is also known as the degree of the isogeny. If an isogeny has an inverse map which is also an isogeny, we call it an isomorphism. We furthermore have that the set of endomorphisms End(E) of isogenies from $E(\bar{K}) \to E(\bar{K})$ forms a group and for most elliptic curves we have that End(E) is isomorphic to $\mathbb{Z}$. If End(E) is strictly larger then we say that E has **complex multiplication**, or in short that E has CM.

Later on we shall mainly focus on elliptic curves defined over $\mathbb{Q}$, and as $\operatorname{char}(\mathbb{Q}) = 0$ every elliptic curve over $\mathbb{Q}$ is isomorphic over $\mathbb{Q}$ to an elliptic curve which can be written in short Weierstrass form. We also denote the following lemma, which we shall use a couple of times in later chapters.

Lemma 2.2. *Let $E, E'/\mathbb{Q}$ be elliptic curves such that $E \cong E'$ over $\bar{\mathbb{Q}}$. Then $\Delta_E \equiv \Delta_{E'} \pmod{(\mathbb{Q}^*)^2}$.*

Proof: First of all we have that every elliptic curve over $\mathbb{Q}$ is isomorphic over $\mathbb{Q}$ to an elliptic curve of the form $E : y^2 = x^3 + Ax + B$ by the isomorphism given in Definition 2.1. So we get that E, E' are isomorphic respectively to $\bar{E} : x^3 + Ax + B$ and $\bar{E}' : x^3 + A'x + B'$ with $A, A', B, B' \in \mathbb{Q}$. Therefore $\bar{E} \cong \bar{E}'$ over $\bar{\mathbb{Q}}$ as well. We have by [35, III.1.3] that an isomorphism between these two curves corresponds to an element $u \in (\bar{\mathbb{Q}})^*$ such that $u^4 A = A'$, $u^6 B = B'$. If $A, B \neq 0$ this implies that $u^4 \in \mathbb{Q}^*$ and that $u^6 \in \mathbb{Q}^*$, but then $u^2 = \frac{u^6}{u^4} \in \mathbb{Q}^*$ as well. If $A = 0 = A'$ we only get that $u^6 \in \mathbb{Q}^*$ and If $B = 0 = B'$ we only get that $u^4 \in \mathbb{Q}^*$. In all cases we get that u^{12} is a square. As [35, III.1.3] also gives that $u^{12}\Delta_{\bar{E}} = \Delta_{\bar{E}'}$ we get that $\Delta_{\bar{E}}$ and $\Delta_{\bar{E}'}$ differ a square. Furthermore when looking at the explicit isomorphism given in Definition 2.1 between E and $\bar{E}$, we find in [35, Table 3.1] with $u = \frac{1}{6}$ that Δ_E and $\Delta_{\bar{E}}$ differ by $(\frac{1}{6})^{12}$ which is a square. The same argument holds true for E' and $\bar{E}'$ and so

$$\Delta_E \equiv \Delta_{\bar{E}} \equiv \Delta_{\bar{E}'} \equiv \Delta_{E'} \pmod{(\mathbb{Q}^*)^2}.$$

□

We continue with elliptic curves over general fields K. We write $E(\bar{K})$ (sometimes denoted as just E) for the set of points with coordinates in $\bar{K}$ that satisfy the Weierstrass equation defining E. We write $E(K)$ for the points on E with coordinates in K, often called the rational points on E. An important property of elliptic curves is that while the curve itself is defined in geometric terms, we have that its points $E(\bar{K})$ form an abelian group. The addition formulas which explicitly give the operation of this group can be found in [35, III.2.3]), and are given by rational functions over $\mathbb{Q}$. The identity element of $E(\bar{K})$ is the point $\mathcal{O}$, and $E(K)$ is a subgroup of $E(\bar{K})$. It turns out that isogenies of elliptic curves preserve this group structure.

For every $n \geq 1$ we therefore define the n-torsion group

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

where $[n] : E \to E$ is the multiplication by n map sending a point P to the sum of itself n times. Note that the map $[n]$ is a group homomorphism. An element of $E[n]$ we call an n-torsion point. We similarly have that $E[n](K)$ consists of all n-torsion points which lie in $E(K)$ (rational n-torsion points) and that this forms a subgroup of $E[n]$.

We have for every elliptic curve E/K and $n \geq 2$ coprime to $\mathrm{char}(K)$ that

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

as can be seen in [35, III.6.4]. This implies in particular for elliptic curves $E/\mathbb{Q}$ that we have for $n \geq 2$ that $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

2.1.1 Tate module

Before we define the Tate module of an elliptic curve we first quickly recall the notion of inverse limits, as seen in Definition 1.2 in [23]. Let $\{A_i\}_{i\in I}$ be a collection of groups (or sets, rings, topological spaces) with I a partially ordered set and let $\phi_{ij} : A_i \to A_j$ for $j \leq i$ be morphisms (maps, homomorphisms, continuous maps) for which $\phi_{ii} : A_i \to A_i = \mathrm{id}_{A_i}$ and $\phi_{ij} \circ \phi_{jk} = \phi_{ik}$ for $k \leq j \leq i$. These maps we call projection maps. Then we define the inverse limit of $(\{A_i\}, \{\phi_{ij}\})$ as follows:

Definition 2.3. The **inverse limit of** $(\{A_i\}, \{\phi_{ij}\})$ is given by

$$\varprojlim_i A_i := \{(a_i)_{i\in I} \in \prod_{i\in I} A_i \mid \phi_{ij}(a_i) = a_j \text{ for all } j \leq i\}.$$

In the case of topological spaces we endow $\varprojlim_i A_i$ with the subspace topology obtained by the inclusion $\varprojlim_i A_i \subseteq \prod_{i\in I} A_i$.

Example 2.4. An example of an inverse limit is the ℓ-adic integers $\mathbb{Z}_\ell$ given by $\varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z}$. We take the standard ordening on $\mathbb{N}$ and the projection maps are given by the standard maps

$$\mathbb{Z}/\ell^n\mathbb{Z} \xrightarrow{(\mathrm{mod}\ \ell^m)} \mathbb{Z}/\ell^m\mathbb{Z}$$

for $m \leq n$. Another example is the so-called profinite integers $\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$ where we take $m \leq n$ if and only if $m \mid n$ as ordening on $\mathbb{N}$ with projection maps

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{(\mathrm{mod}\ m)} \mathbb{Z}/m\mathbb{Z}.$$

Similar to the inverse limit construction of ℓ-adic numbers we have the following inverse limit obtained by taking the limit of the ℓ^n-torsion groups of an elliptic curve:

Definition 2.5. Let E/K be an elliptic curve and ℓ prime. Then we have the **ℓ-adic Tate module of E** given by

$$T_\ell(E) := \varprojlim_n E[\ell^n],$$

where the limit is defined by the multiplication by ℓ maps $[\ell] : E[\ell^{n+1}] \to E[\ell^n]$.

By [35, III.6.4] we also have for every $n \geq 1$ that $E[n]$ is a finite $\mathbb{Z}/\ell^n\mathbb{Z}$-module, so this implies that $T_\ell(E)$ has the structure of a $\mathbb{Z}_\ell$-module. We therefore get the following proposition for the structure of the ℓ-adic Tate module:

Theorem 2.6. [35, III.7.1]
We have for the ℓ-adic Tate module that:
(a) $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ if $\ell \neq \mathrm{Char}(K)$,
(b) $T_\ell(E) \cong \{0\}$ or $\mathbb{Z}_\ell$ if $\ell = \mathrm{Char}(K)$.

Proof: Let ℓ be a prime such that $\ell \neq \mathrm{Char}(K)$. Then we have for all $n \geq 1$ that $E[\ell^n] \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$ as $\mathbb{Z}/\ell^n\mathbb{Z}$-modules. We also have the following commutative diagram:

$$\begin{tikzcd}
E[\ell^{n+1}] \arrow[r, "{[\ell]}"] \arrow[d, "\cong"'] & E[\ell^n] \arrow[d, "\cong"] \\
(\mathbb{Z}/\ell^{n+1}\mathbb{Z}) \times (\mathbb{Z}/\ell^{n+1}\mathbb{Z}) \arrow[r, "\bmod \ell^n"] & (\mathbb{Z}/\ell^n\mathbb{Z}) \times (\mathbb{Z}/\ell^n\mathbb{Z})
\end{tikzcd}$$

To show that this diagram commutes we note that $[\ell]$ is a surjective map by [35, II.2.3] combined with the fact that $[\ell]$ is non-constant [35, III.4.2]. If P, Q is a basis for $E[\ell^{n+1}]$, we get that $[\ell]P, [\ell]Q$ is a basis for $E[\ell^n]$ by surjectivity of $[\ell]$ combined with the fact that $[\ell]$ is a group homomorphism. But this equivalent to commutativity of the diagram above, which tells us that the isomorphisms $E[\ell^n] \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$ for $n \geq 1$ can be extended to an isomorphism between the inverse limits of both these objects. Therefore we get $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ as $\mathbb{Z}_\ell$-modules. If $\ell = \mathrm{Char}(K)$ then for all $n \geq 1$ we have that $E[\ell^n] \cong \{0\}$ or for all $n \geq 1$ we have that $E[\ell^n] \cong \mathbb{Z}/\ell^n\mathbb{Z}$ and this also clearly induces an isomorphism on the level of inverse limits. So in these cases $T_\ell(E) \cong \{0\}$ or $T_\ell(E) \cong \mathbb{Z}_\ell$.

□

Furthermore we can also copy the construction of the profinite integers $\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$ to get the adelic variant of the Tate module:

Definition 2.7. Let E/K be an elliptic curve. Then we have the **adelic Tate module of E** given by

$$T(E) := \varprojlim_n E[n],$$

where the projection maps are given for $n \mid m$. If $m = kn$ then this is the map $[k] : E[kn] \xrightarrow{[k]} E[n]$.

Remark 2.8. We get that $T(E)$ has the structure of a $\hat{\mathbb{Z}}$ module. If Char(K) = 0 (for instance if $K = \mathbb{Q}$) then we get by the same argument as for the ℓ-adic Tate module that

$$T(E) \cong \hat{\mathbb{Z}} \times \hat{\mathbb{Z}}.$$

Also note that for the profinite integers $\hat{\mathbb{Z}}$ we have that $\hat{\mathbb{Z}} \cong \prod_{\ell} \mathbb{Z}_\ell$, and similar to this we get for Tate modules that

$$T(E) \cong \prod_{\ell} T_\ell(E).$$

2.1.2 Weil pairing

We end this subsection by introducing the Weil pairing. We will not give the explicit definition, which can be found in [35, III.8], but we state the following proposition:

Theorem 2.9. [35,III.8.1] *Let $\boldsymbol{\mu}_n \subseteq (\bar{K})^*$ be the group of n-th roots of unity. Then the **Weil e_n-pairing** is given by a map*

$$e_n : E[n] \times E[n] \to \boldsymbol{\mu}_n$$

with the following properties:
(a) It is bilinear:

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T),$$
$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2).$$

(b) It is alternating:

$$e_n(T, T) = 1.$$

In particular this implies that $e_n(S, T) = e_n(T, S)^{-1}$.

(c) It is non-degenerate:

$$\textit{If } e_n(S, T) = 1 \text{ for all } S \in E[n], \text{ then } T = \mathcal{O}.$$

(d) It is Galois invariant:

$$\sigma(e_n(S, T)) = e_n(\sigma(S), \sigma(T)) \text{ for all } \sigma \in \mathrm{Gal}(\bar{K}, K).$$

Here $\sigma(P)$ with $P = (x, y)$ is defined as $\sigma(P) := (\sigma(x), \sigma(y))$ and $\sigma(\mathcal{O}) = \mathcal{O}$ as $\mathcal{O}$ is defined over K.

(e) It is compatible with projections:

$$e_{nn'}(S, T) = e_n([n']S, T) \text{ for all } S \in E[nn'] \text{ and } T \in E[n].$$

2.2 Galois theory and Galois representations

This subsection we introduce the notion of general Galois representations, after which we will focus our attention on Galois representations of elliptic curves.

2.2.1 Galois Theory

We start by listing a few important facts from Galois theory. We will mainly use [3] and [23] as a reference.

Let K be a field and let L/K be a finite field extension of K. Then we have the following definition of its Galois group:

Definition 2.10. Let K be a field and let L/K be a finite field extension of K. Then we define the **Galois group of** L/K as

$$\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_K = \mathrm{id}_K\}.$$

Recall that an algebraic extension L/K is normal if every irreducible polynomial over $K[X]$ with a root in L has all roots in L, and L/K is separable if every irreducible polynomial over $K[X]$ with roots in L has no roots with multiplicity bigger than 1. For L/K both normal and separable we have that $|\mathrm{Gal}(L/K)| = [L : K]$ and we call L a **Galois extension of** K. For these extensions we have that K is precisely the subfield of L on which all $\sigma \in \mathrm{Gal}(L/K)$ restrict to the identity.

Example 2.11. An easy example of a Galois extension is a quadratic extension. For instance $\mathbb{Q}(\sqrt{2})$ is a Galois extension with Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z}$. It is generated by the element σ of order 2 sending $\sqrt{2} \to -\sqrt{2}$. We also have for every integer n the cyclotomic field $\mathbb{Q}(\zeta_n)$ given by adjoining $\mathbb{Q}$ with a primitive n-th root of unity (i.e. an element ζ_n for which $\zeta_n^n = 1$). These cyclotomic fields are also Galois extensions with Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ by the homomorphism $\sigma \to \alpha$ where α is given by $\sigma(\zeta_n) = \zeta_n^\alpha$ for $\zeta_n \in \boldsymbol{\mu}_n$.

We have even more, which is called the fundamental theorem of Galois theory. This states that there is a one-to-one connection between intermediate fields $K \subseteq M \subseteq L$ and subgroups H of $\mathrm{Gal}(L/K)$. Note that for an intermediate field M with $K \subseteq M \subseteq L$ we have that L/M is again a Galois extension [3, Theorem 8.3.6]. We also define for a subgroup H of $\mathrm{Gal}(L/K)$ its **fixed field**

$$L^H := \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in H\}.$$

Now we state the theorem:

Theorem 2.12. [3,Theorem 9.2.1, Theorem 9.2.2] *Let L/K be a Galois extension. Then there is a one-to-one correspondence between intermediate fields $K \subseteq M \subseteq L$ and subgroups*

H of $\mathrm{Gal}(L/K)$ *given by the map:*

$$M \to \mathrm{Gal}(L/M),$$

its inverse being

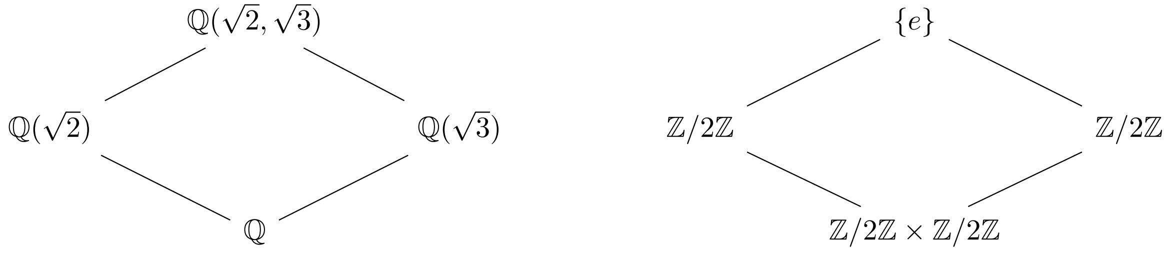
$$H \to L^H.$$

The intermediate fields $K \subseteq M \subseteq L$ with M/K a Galois extension correspond to normal subgroups of $\mathrm{Gal}(L/K)$*. In this case we have that*

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

Remark 2.13. Note that this correspondence is inclusion-reversing: If we have $K \subseteq M \subseteq M' \subseteq L$ with L/K Galois, then we have that $\mathrm{Gal}(L/M') \subseteq \mathrm{Gal}(L/M)$. For instance if we have an element $\sigma \in \mathrm{Gal}(L/M')$, then σ is the identity on M' and therefore also on M. So $\sigma \in \mathrm{Gal}(L/M)$. Conversely if we have that $H \subseteq H' \subseteq \mathrm{Gal}(L/K)$, then $L^{H'} \subseteq L^H$ as every element which is fixed by H' is also fixed by H.

Example 2.14. As an example we look at the Galois extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. We have that an element σ of its Galois group is determined by what it does on $\sqrt{2}$ and $\sqrt{3}$. It must send zeroes of polynomials to zeroes of the same polynomials, so σ can only send $\sqrt{2}$ to $\pm\sqrt{2}$ and $\sqrt{3}$ to $\pm\sqrt{3}$. We get that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Its normal proper non trivial normal subgroups are $\{0\} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \{0\}$ and we summarize the correspondence between these normal subgroups and their fixed fields in the following diagram:



Definition 2.15. We define the compositum L_1L_2 of two fields $L_1, L_2/K$ as the smallest field extension of K containing both L_1, L_2 as subfields.

We have the following two lemmas concerning the intersection and compositum of two Galois extensions.

Lemma 2.16. *Let L/K be a Galois extension of K and let $L_1, L_2 \subseteq L$ be two intermediate subfields of L. Then*

$$\mathrm{Gal}(L/L_1 \cap L_2) \cong \langle \mathrm{Gal}(L/L_1), \mathrm{Gal}(L/L_2) \rangle,$$

which is the subgroup of $\mathrm{Gal}(L/K)$ *generated by elements of* $\mathrm{Gal}(L/L_1)$ *and* $\mathrm{Gal}(L/L_2$.

Proof: Let $H_1 := \mathrm{Gal}(L/L_1)$ and let $H_2 := \mathrm{Gal}(L/L_2)$. Then we claim that

$$\mathrm{Gal}(L/L_1 \cap L_2) \cong \langle H_1, H_2 \rangle.$$

Let $x \in L_1 \cap L_2$ and let $\sigma \in H := \langle H_1, H_2 \rangle$, then σ is the finite composition of $\sigma_i \in H_1$ and $\tau_j \in H_2$, write $\sigma = \sigma_1 \cdot ... \cdot \tau_1 \cdot ... \sigma_n \cdot ... \cdot \tau_m$. We get that $\sigma(x) = \sigma_1(x) \cdot ... \cdot \tau_1(x) \cdot ... \sigma_n(x) \cdot ... \cdot \tau_m(x)$. As $x \in L_1 \cap L_2$ we get that σ_i and τ_j leave x fixed and so σ leaves x fixed. This implies that $x \in L^H = \{x \in L \mid \sigma(x) = x \text{ for all } x \in H\}$ and so $L_1 \cap L_2 \subseteq L^H$. As $H_1 \subseteq H$ and $H_2 \subseteq H$ we get by Remark 2.13 that $L^H \subseteq L^{H_1} = L_1$ and $L^H \subseteq L^{H_2} = L_2$, so $L^H \subseteq L_1 \cap L_2$. This now gives that $L_1 \cap L_2 = L^H$ and so $H = \mathrm{Gal}(L/L_1 \cap L_2)$.

□

Lemma 2.17. *Let $L_1, L_2/K$ be Galois extensions of K. Then the compositum $L := L_1L_2$ is also a Galois extension of K. We have that the group homomorphism*

$$\phi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$$

defined by

$$\phi(\sigma) = (\sigma|_{L_1}, \sigma|_{L_2})$$

is an isomorphism if and only if $L_1 \cap L_2 = K$.

Proof: We first show that L is finite. We have that L_1 is a finite extension, so $[L_1 : K] = n$ for some $n \in \mathbb{N}$. Let $\alpha_1, ..., \alpha_n$ be a generating set for L_1. We have that L_2 is also finitely generated, so $L_2(\alpha_1)$ is finitely generated as well. We inductively see that

$$L_2 \subseteq L_2(\alpha_1) \subseteq ... \subseteq L_2(\alpha_1, ..., \alpha_n)$$

and so that $L_2(\alpha_1, ..., \alpha_n)$ is finitely generated. As $L_1 \subseteq L_2(\alpha_1, ..., \alpha_n) \subseteq L$ we must have that $L_2(\alpha_1, ..., \alpha_n) = L$ as L was the smallest field containing both L_1 and L_2. So L is finitely generated and $[L : K] = d$ for some $d \in \mathbb{N}$. If we have $\alpha \in L$, then $1, \alpha, ..., \alpha^d$ must form a linearly dependent set of vectors over K, so there exist $c_0, ..., c_d \in K$ such that $0 = c_0 + c_1\alpha + ... + c_d\alpha^d$. But this gives an element in $K[x]$ defined by $c_0 + c_1x + ... + c_dx^d$ for which α is a root and so α is algebraic. Therefore L/K is an algebraic extension.

Note that if $\bar{K}$ is an algebraic closure of K then we define its Galois group by $\mathrm{Gal}(\bar{K}/K) \cong \varprojlim_{M} \mathrm{Gal}(M/K)$ with M/K finite Galois. By Lemma 9.3.2 in [3] we get that L is normal if and only if for $\sigma \in \mathrm{Gal}(\bar{K}/K)$ we have that $\sigma(L) \subseteq L$. As L_1, L_2 are normal we get for $\sigma \in \mathrm{Gal}(\bar{K}/K)$ that $\sigma(L_1) \subseteq L_1$ and so all α_i get mapped into L_1. We also get that $\sigma(L_2) \subseteq L_2$ and so $\sigma(L) \subseteq L$ as $L = L_2(\alpha_1, ..., \alpha_n)$. Therefore L is normal.

For separability we take $\alpha \in L$. Then $\alpha \in L_2(\alpha_1, ..., \alpha_n)$. If $[L_2 : K] = m$ for some $m \in \mathbb{N}$ and we take $\beta_1, ..., \beta_m$ as a generating set for L_2, then $L = K(\alpha_1, ..., \alpha_n, \beta_1, ..., \beta_m)$ with $\alpha_1, ..., \alpha_n, \beta_1, ..., \beta_m$ separable as L_1, L_2 are separable. So $\alpha = k_1\alpha_1 + ... + k_n\alpha_n + l_1\beta_1 + ... + l_m\beta_m$ with $k_1, ..., k_n, l_1, ..., l_m \in K$. As sums and products of separable elements are separable we get that α is separable. Therefore L is separable and we conclude that L is a Galois extension.

Let the map

$$\phi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$$

be given by

$$\phi(\sigma) = (\sigma|_{L_1}, \sigma|_{L_2}).$$

Note that $\sigma|_{L_1}$ is well defined as L_1 is normal and so $\sigma(L_1) \subseteq L_1$, similarly for L_2. This is a group homomorphism as $(\sigma + \tau)_{L_1} = \sigma|_{L_1} + \tau|_{L_1}$ for $\sigma, \tau \in \mathrm{Gal}(L/K)$ and similarly for L_2. If $\sigma|_{L_1} = \mathrm{id}_{L_1}$ and $\sigma|_{L_2} = \mathrm{id}_{L_2}$ then $\sigma = \mathrm{id}_L$ as every element of L is a linear combination of elements in L_1 and L_2. So ϕ is an injective group homomorphism.

Assume $L_1 \cap L_2 = K$. Let $(\sigma_1, \sigma_2) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$ and write $L_1 = K(\alpha_1, ..., \alpha_n)$ and $L_2 = K(\beta_1, ..., \beta_m)$. We have that σ_1 as a map is completely determined by its image of $\alpha_1, ..., \alpha_n$ and σ_2 by its image of $\beta_1, ..., \beta_m$. As $L_1 \cap L_2 = K$ we get that $\alpha_i \neq \beta_j$ for $1 \leq i \leq n$ and $1 \leq j \leq m$. As an element of $\mathrm{Gal}(L/K)$ is completely determined by its image of $\alpha_1, ..., \alpha_n, \beta_1, ..., \beta_m$ we get that σ_1, σ_2 together give rise to an element $\sigma \in \mathrm{Gal}(L/K)$ for which $\sigma|_{L_1} = \sigma_1$ and $\sigma|_{L_2} = \sigma_2$. So in the case where $L_1 \cap L_2 = K$ we get that ϕ is also surjective. If $L_1 \cap L_2 \neq K$, then there exists a α_i that is a K-rational combination of $\beta_j, ..., \beta_l$. This implies that σ_1, σ_2 do not necessarily give rise to an element $\sigma \in \mathrm{Gal}(L/K)$ as then $\sigma_1(\alpha_i)$ is dependent on $\sigma|_{L_2}(\beta_j), ..., \sigma|_{L_2}(\beta_l)$. So ϕ is surjective if and only if $L_1 \cap L_2 = K$.

□

Galois theory provides us with the ability to prove the following theorem, which states that every prime cyclotomic field has a unique quadratic subfield.

Theorem 2.18. *Let p be an odd prime number and let ζ_p be a primitive p-th root of unity. Then the prime cyclotomic field $\mathbb{Q}(\zeta_p)$ has a unique quadratic subfield given by $\mathbb{Q}(\sqrt{\epsilon p})$ where $\epsilon = (-1)^{\frac{p-1}{2}}$.*

Proof: We want to show $\mathbb{Q}(\zeta_p)$ has a unique quadratic subfield. To show the existence of this quadratic subfield we will make use of the so called Gaussian sum

$$\tau = \sum_{0 \leq i < p} \zeta_p^{i^2}.$$

Note that $\tau \in \mathbb{Q}(\zeta_p)$. We have the following important fact for the p-th root of unity ζ_p, namely that $\sum_{0 \leq n < p} \zeta_p^i = 0$. This can be seen by studying the minimal polynomial of ζ_p, which is given by

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + ... + x + 1.$$

If we evaluate this polynomial at ζ_p we get

$$0 = \frac{\zeta_p^p - 1}{\zeta_p - 1} = \zeta_p^{p-1} + \zeta_p^{p-2} + ... + \zeta_p + 1 = \sum_{0 \leq i < p} \zeta_p^i.$$

We now claim that $\tau\bar{\tau} = p$. Note that for roots of unity we have that $\overline{\zeta_p^i} = \zeta_p^{-i}$ for all $0 \leq i < p$, as $\zeta_p^i \cdot \overline{\zeta_p^i} = |\zeta_p^i|^2 = 1$. So we get that

$$\tau\overline{\tau} = \sum_{0 \leq i < p} \zeta_p^{i^2} \cdot \sum_{0 \leq j < p} \zeta_p^{-j^2} = \sum_{0 \leq i,j < p} \zeta_p^{i^2} \cdot \zeta_p^{-j^2} = \sum_{0 \leq i,j < p} \zeta_p^{(i-j)(i+j)}.$$

We see that the values of $i - j$ modulo p cover every value in $\mathbb{Z}/p\mathbb{Z}$ if we vary i and j, and so we can substitute $i - j$ with $r \in \mathbb{Z}$ such that $0 \leq r < p$. We get that $i + j = r + 2j$ which for fixed r also covers every value in $\mathbb{Z}/p\mathbb{Z}$ if we vary j, so we can substitute this as well with the variable s such that $0 \leq s < p$. We can therefore rewrite the sum as the following:

$$\tau\overline{\tau} = \sum_{0 \leq r,s < p} \zeta_p^{rs}.$$

If $r = 0$ then we get that $\zeta_p^{rs} = 1$ for all $0 \leq j < p$ and therefore we get that

$$\tau\overline{\tau} = p + \sum_{1 \leq r < p, 0 \leq s < p} \zeta_p^{rs}.$$

Now note that for each fixed $1 \leq r < p$ we have that

$$\sum_{0 \leq s < p} \zeta_p^{rs} = \sum_{0 \leq s < p} \zeta_p^s = 0$$

as rs covers the same values as s if we vary s because $r \not\equiv 0 \pmod{p}$. We conclude that $\tau\overline{\tau} = p$.

Now we show that either τ is a real number, or it is totally imaginary. Recall that p is an odd prime, so $p \equiv 1, 3 \pmod{4}$. We claim that if $p \equiv 1 \pmod{4}$, then $\tau \in \mathbb{R}$ and if $p \equiv 3$

(mod 4) then $\tau/i \in \mathbb{R}$. First assume $p \equiv 1 \pmod 4$, then we have that -1 is a square modulo p. If $-1 \equiv a^2 \equiv \pmod p$ for some $a \in \mathbb{Z}/p\mathbb{Z}$ with $a \not\equiv 0 \pmod p$, then we get that

$$\overline{\tau} = \sum_{0 \le i < p} \zeta_p^{-i^2} = \sum_{0 \le i < p} \zeta_p^{(ai)^2}.$$

As ai covers every value in $\mathbb{Z}/p\mathbb{Z}$ if we vary i (because $a \not\equiv 0 \pmod p$) we get that

$$\overline{\tau} = \sum_{0 \le i < p} \zeta_p^{(ai)^2} = \sum_{0 \le i < p} \zeta_p^{i^2} = \tau$$

and therefore τ is real.

Now conversely assume that $p \equiv 3 \pmod 4$. In this case -1 is not a square modulo p. As half of the elements of $(\mathbb{Z}/p\mathbb{Z})^*$ are quadratic residues, we claim that multiplying those elements with -1 gives the other half of the elements of $(\mathbb{Z}/p\mathbb{Z})^*$ which are not quadratic residues. If this was not the case, then $i \equiv a^2 \pmod p$ and $-i \equiv b^2 \pmod p$ for some $i, a, b \in (\mathbb{Z}/p\mathbb{Z})^*$. But then $-1 \equiv (\frac{a}{b})^2 \pmod p$ with $\frac{a}{b} \in (\mathbb{Z}/p\mathbb{Z})^*$ which cannot be. So we get that

$$\tau + \overline{\tau} = \sum_{0 \le i < p} \zeta_p^{i^2} + \sum_{0 \le j < p} \zeta_p^{-j^2} = 2 \cdot \sum_{0 \le i < p} \zeta_p^{i} = 0$$

which implies that $\tau = -\overline{\tau}$ and therefore τ must be fully imaginary.

We have now shown that if $p \equiv 1 \pmod 4$ we have that $\tau^2 = \tau\overline{\tau} = p$, as τ is real and so $\overline{\tau} = \tau$. In this case we have that $\sqrt{p} = \tau \in \mathbb{Q}(\zeta_p)$ and therefore $\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\zeta_p)$.

In the other case where $p \equiv 3 \pmod 4$ we get that $\overline{\tau} = -\tau$ and so $\tau^2 = -\tau\overline{\tau} = -p$. We now have that $\tau = \sqrt{-p}$ and so $\mathbb{Q}(\sqrt{-p}) \subseteq \mathbb{Q}(\zeta_p)$.

We conclude that $\mathbb{Q}(\sqrt{\epsilon p}) \subseteq \mathbb{Q}(\zeta_p)$ where $\epsilon = (-1)^{\frac{p-1}{2}}$. To show that this is the unique quadratic subfield we need some Galois theory. We have that $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$, which is a cyclic group of order $p-1$. Because p is odd, this number is even, and as every cyclic group with order n has a unique subgroup of order d for every $d \mid n$, we get that $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ has a unique subgroup of order 2, which fixed field must be $\mathbb{Q}(\sqrt{\epsilon p})$.

□

We now get the following corollary, which is a simple case of the Kronecker-Weber Theorem (this theorem in general states that every Galois extension over $\mathbb{Q}$ with abelian Galois group lies in some cyclotomic field).

Corollary 2.19. *Let $n \in \mathbb{Z}$ with $n \neq 0$ and squarefree. Then*

$$\begin{cases} \mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta_{|n|}) & \text{if } n \equiv 1 \pmod 4 \\ \mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta_{4|n|}) & \text{if } n \equiv 2, 3 \pmod 4. \end{cases}$$

Note that the absolute value of the discriminant of $\mathbb{Q}(\sqrt{n})$ is in both cases the same as the number corresponding to the cyclotomic field in which it lies. This value is defined as the conductor of $\mathbb{Q}(\sqrt{n})$.

Proof: First of all let $n \equiv 1 \pmod 4$. As n is squarefree we can write $n = \pm p_1 \cdot p_2 \cdot ... \cdot p_n$ with $p_1, ..., p_n$ distinct primes. By Theorem 2.18 we have for all primes p_i with $p_i \equiv 1 \pmod 4$= that $\sqrt{p_i} \in \mathbb{Q}(\zeta_{p_i})$, while for all primes p_i with $p_i \equiv 3 \pmod 4$ we have that $\sqrt{-p_i} \in \mathbb{Q}(\zeta_{p_i})$. As $\mathbb{Q}(\zeta_{p_i}) \subseteq \mathbb{Q}(\zeta_{|n|})$ we get that $\sqrt{n} = \prod\limits_{1 \leq i \leq n} \sqrt{\epsilon_i p_i} \in \mathbb{Q}(\zeta_{|n|})$ with $\epsilon_i = (-1)^{\frac{p_i - 1}{2}}$. This works out because $n \equiv 1 \pmod 4$: If n is positive, then an even number of primes is equivalent to $3 \pmod 4$ which gives an even amount of minus signs in the product. If conversely n is negative, then an odd number of primes is equivalent to $3 \pmod 4$, which gives an odd number of minus signs.

If $n \equiv 3 \pmod 4$ then $-n \equiv 1 \pmod 4$ and by the previous statement we get that $\sqrt{-n} \in \mathbb{Q}(\zeta_{|n|})$. As $\sqrt{-1} \in \mathbb{Q}(\zeta_4)$ we get that $\sqrt{n} = \sqrt{-1}\sqrt{-n} \in \mathbb{Q}(\zeta_{4|n|})$.

Finally if $n \equiv 2 \pmod 4$, then $n = 2 \cdot m$ with $m \equiv 1, 3 \pmod 4$. In either case we have that $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\zeta_{4|m|}) \subseteq \mathbb{Q}(\zeta_{4|n|})$ as $m \mid n$. Now note that

$$(\zeta_8 + \zeta_8^7)^2 = \zeta_8^2 + 2\zeta_8\zeta_8^7 + \zeta_8^6 = \sqrt{-1} + 2 - \sqrt{-1} = 2$$

as $\zeta_8^2 = \sqrt{-1}$ and $\zeta_8^6 = -\sqrt{-1}$. This implies that $\sqrt{2} = \zeta_8 + \zeta_8^7 \in \mathbb{Q}(\zeta_8) \subseteq \mathbb{Q}(\zeta_{4|n|})$. We therefore get that $\sqrt{n} = \sqrt{2}\sqrt{m} \in \mathbb{Q}(\zeta_{4|n|})$, which concludes the proof.

□

2.2.2 Infinite Galois theory

So far we have only been able to define the Galois group for finite extensions L/K, but this definition can be extended to infinite extensions as well.

First note that for an algebraic extension L/K we define its Galois group to be $\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K)$. If we have L/K an algebraic extension which is not necessarily finite, then we take the set of intermediate fields $K \subseteq M \subseteq L$ such that M is a finite normal separable extension (Galois extension). We can order this by $M \leq M'$ if and only if $M \subseteq M'$ and take as projection maps the maps $\mathrm{Gal}(M/K) \to \mathrm{Gal}(M'/K)$ given by sending σ to $\sigma|_{M'}$ (these maps are well defined group homomorphisms by [3, Lemma 9.2.3]). This defines the inverse limit

$$\varprojlim_{M} \mathrm{Gal}(M/K) = \{(\sigma_M) \in \prod_{M} \mathrm{Gal}(M/K) \mid \sigma_M|_{M'} = \sigma_{M'}\}.$$

We have the following theorem in [23], which shows for L/K a normal separable extension which is not necessarily finite that the Galois group of L/K is isomorphic to the aforementioned inverse limit:

Theorem 2.20. [23, Theorem 1.7] *Let L/K be a normal separable extension. Then we have the following isomorphism of groups:*

$$\mathrm{Gal}(L/K) \cong \varprojlim_M \mathrm{Gal}(M/K),$$

the limit ranging over all $K \subseteq M \subseteq L$ with M a finite Galois extension of K.

Example 2.21. We have the following important example of a Galois group of an infinite extension: Take $\bar{\mathbb{Q}}$ to be an algebraic closure of $\mathbb{Q}$, then $\bar{\mathbb{Q}}$ is an infinite algebraic extension of $\mathbb{Q}$. This extension is by construction normal and it is separable as extensions over $\mathbb{Q}$ are always separable. Therefore we get that $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \cong \varprojlim_M \mathrm{Gal}(M/\mathbb{Q})$ with $M/\mathbb{Q}$ a finite Galois extension. We call this Galois group the **absolute Galois group of** $\mathbb{Q}$.

We also endow these Galois groups with a topology as follows: For each finite Galois extension M/K we give $\mathrm{Gal}(M/K)$ the discrete topology. Then $\varprojlim_M \mathrm{Gal}(M/K)$ (seen as an inverse limit of topological spaces) has the subspace topology obtained from the topological space $\prod_M \mathrm{Gal}(M/K)$. This is called the Krull topology (note that we can endow the rings $\mathbb{Z}_\ell$ and $\hat{\mathbb{Z}}$ with a topology in the same fashion). Using this topology we have the following analogue of the fundamental theorem of Galois theory for infinite normal separable extensions L/K:

Theorem 2.22. [23,Theorem 1.12] *Let L/K be a normal separable extension. Then we have a one-to-one correspondence between closed subgroups H of $\mathrm{Gal}(L/K)$ and intermediate fields $K \subseteq M \subseteq L$ given by the map*

$$M \to \mathrm{Gal}(L/M)$$

with inverse

$$H \to L^H.$$

This bijection restricts to a one-to-one correspondence between normal closed subgroups H of $\mathrm{Gal}(L/K)$ and intermediate Galois extensions $K \subseteq M \subseteq L$ and to a one-to-one correspondence between open and closed subgroups H of $\mathrm{Gal}(L/K)$ and intermediate finite extensions $K \subseteq M \subseteq L$.

2.2.3 Galois representations

Now we focus on Galois representations, which are representations of the absolute Galois group of $\mathbb{Q}$ to some matrix group over a given topological field. For this part we follow again [23]. Write $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ for the absolute Galois group over $\mathbb{Q}$. We have the following definition:

Definition 2.23. A **Galois representation** (of dimension n) over a (topological) ring R is a continuous group homomorphism

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}(n, R).$$

If R is a subring of a field extension of $\mathbb{Q}_\ell$ we call this representation an **ℓ-adic Galois representation**

Note that $G_{\mathbb{Q}}$ has the Krull topology and that $\mathrm{GL}(n, R)$ has the subspace topology given by $\mathrm{GL}(n, R)^n$ with R^n having the product topology.

Example 2.24. An example of an ℓ-adic Galois representation is the so-called **ℓ-adic cyclotomic character**, which is given by the following: We have that $\boldsymbol{\mu}_n \subseteq (\bar{\mathbb{Q}})^*$ is the group of n-th roots of unity in $\bar{\mathbb{Q}}$. We have for every $n \geq 1$ that $\mathbb{Q}(\boldsymbol{\mu}_n)/\mathbb{Q}$ is Galois and that $\mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Now let ℓ be a prime number, then we define $\boldsymbol{\mu}_{\ell^\infty} := \bigcup_n \boldsymbol{\mu}_{\ell^n}$. By Theorem 2.20 we get that

$$\mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_{\ell^\infty})/\mathbb{Q}) \cong \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_n)/\mathbb{Q}).$$

For all $n \geq 1$ we have $\mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_{\ell^n})/\mathbb{Q}) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^*$ and we have the following commutative diagram for $m \leq n$:

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_{\ell^n})/\mathbb{Q}) \arrow[r, "r"] \arrow[d, "\cong"'] & \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_{\ell^m})/\mathbb{Q}) \arrow[d, "\cong"] \\
(\mathbb{Z}/\ell^n\mathbb{Z})^* \arrow[r, "\text{mod } \ell^m"] & (\mathbb{Z}/\ell^m\mathbb{Z})^*
\end{tikzcd}$$

Here we write r for the restriction map. Note that this commutes as ζ_{ℓ^m} is also an ℓ^n root of unity if $m \leq n$ and so if $\sigma(\zeta_{\ell^m}) = (\zeta_{\ell^m})^\alpha$ with $\alpha \in (\mathbb{Z}/\ell^n\mathbb{Z})^*$, then σ gets sent to the element α. For $\beta = \alpha \pmod{\ell^m}$ we have that $(\zeta_{\ell^m})^\alpha = (\zeta_{\ell^m})^\beta$ as $(\zeta_{\ell^m})^{km} = 1$ and so $\sigma|_{\mathbb{Q}(\boldsymbol{\mu}_{\ell^m})}$ gets sent to the element β.

This implies that

$$\varprojlim_n \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_n)/\mathbb{Q}) \cong \varprojlim_n (\mathbb{Z}/\ell^n\mathbb{Z})^* \cong (\mathbb{Z}_\ell)^*.$$

As we also have the restriction map $G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_{\ell^\infty})/\mathbb{Q})$ we now define the ℓ-adic cyclotomic character of an element $\sigma \in G_{\mathbb{Q}}$ as the image of σ under the following maps:

$$G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_{\ell^\infty})/\mathbb{Q}) \cong (\mathbb{Z}_\ell)^* \cong \mathrm{GL}(1, \mathbb{Z}_\ell)^*.$$

Note that this is now an ℓ-adic Galois representation of dimension 1.

2.2.4 Galois representations of elliptic curves

Before we define Galois representations of elliptic curves we first introduce the notion of n-division fields of E with E an elliptic curve over $\mathbb{Q}$:

Definition 2.25. Let $E/\mathbb{Q}$ be an elliptic curve and let $n \geq 1$, then we define the **n-division field of E** as

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

where $x_i, y_i \in \bar{\mathbb{Q}}$ are the x, y-coordinates of the affine n-torsion points of E for $1 \leq i \leq m$. Note that $\mathbb{Q}(E[1])$ is just $\mathbb{Q}$.

Remark 2.26. We recall that the compositum of two fields K, L is defined as the smallest field containing both L, K as subfields. We have by [6, Lemma 2.1.1] that for $n_1, n_2 \geq 1$ the compositum of the division fields $\mathbb{Q}(E[n_1])$ and $\mathbb{Q}(E[n_2])$ is the division field $\mathbb{Q}(E[n])$ with $n = \operatorname{lcm}(n_1, n_2)$.

We note that the Weil pairing implies for $E/\mathbb{Q}$ that the n-cyclotomic field is always a subfield of its n-division field:

Lemma 2.27. *Let $E/\mathbb{Q}$ be an elliptic curve and let $n \geq 1$. Then $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$.*

Proof: We first of all note that there exist points $S, T \in E[n]$ such that $e_n(S, T)$ is a primitive n-th root of unity [35, III.8.1.1]. We also have that $\bar{\mathbb{Q}}/\mathbb{Q}(E[n])$ is Galois as $\bar{\mathbb{Q}}/\mathbb{Q}$ is Galois, and as we have for $\sigma \in \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(E[n]))$ that

$$\sigma(e_n(S, T)) = e_n(\sigma(S), \sigma(T)) = e_n(S, T)$$

(recall that for $S = (x, y)$ we have that $\sigma(S) := (\sigma(x), \sigma(y)))$ we get by the fundamental theorem of Galois theory that $e_n(S, T) \in \mathbb{Q}(E[n])$. So $\mathbb{Q}(E[n])$ contains a primitive n-th root of unity and therefore $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$.

□

Example 2.28. Take the elliptic curve $E : y^2 = x^3 + x + 1$. Then we can compute using Sage that $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 6$ and that $\mathbb{Q}(E[2]) \cong \mathbb{Q}[x]/(x^6 - 3x^5 + 7x^4 - 9x^3 + 7x^2 - 3x + 1)$. For $n = 3$ we compute that $[\mathbb{Q}(E[3]) : \mathbb{Q}] = 48$ (note that the degree quickly grows very large if we increase n) and we can also compute that $\mathbb{Q}(E[3])$ has a unique quadratic subfield given by $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$, which is consistent with the previous lemma.

Definition 2.29. We will now define Galois representation of elliptic curves. First of all let $\sigma(P)$ for $P \in E(\bar{\mathbb{Q}})$ be defined by $\sigma(P) = (\sigma(x), \sigma(y))$ for $\sigma \in G_{\mathbb{Q}}$. As the Weierstrass equation of E is a polynomial with coefficients in $\mathbb{Q}$, we have that $(\sigma(x), \sigma(y))$ is also a solution to this equation and therefore $\sigma(P) \in E(\bar{\mathbb{Q}})$. Therefore σ induces a map $\sigma : E(\bar{\mathbb{Q}}) \to E(\bar{\mathbb{Q}})$ given by sending $P \to \sigma(P)$. We also have that the addition formulas for points on elliptic curves over $\mathbb{Q}$ are rational functions with coefficients in $\mathbb{Q}$. So if we have $P, Q \in E(\bar{\mathbb{Q}})$ then $P + Q = (r(P, Q), s(P, Q))$ with $r, s \in \mathbb{Q}(x)$. This implies that

$$\sigma(P+Q) = (\sigma(r(P,Q), \sigma(s(P,Q)) = (r(\sigma(P), \sigma(Q), s(\sigma(P), \sigma(Q)) = \sigma(P) + \sigma(Q).$$

So $\sigma : E(\bar{\mathbb{Q}}) \to E(\bar{\mathbb{Q}})$ is a group homomorphism. In particular this means that σ sends n-torsion points to n-torsion points and therefore we get an action of $G_{\mathbb{Q}}$ on $E[n]$ for all $n \geq 1$. We can formalise this as the homomorphism: $G_{\mathbb{Q}} \to \operatorname{Aut}(E[n])$. As $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for $n \geq 1$ we get that this induces a **Galois representation of elliptic curves** given by

$$\rho_{E,n} : G_{\mathbb{Q}} \to \operatorname{Aut}(E[n]) \cong \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$$

(here we endow $\mathbb{Z}/n\mathbb{Z}$ with the discrete topology to make it into a topological ring.)

Note that $\rho_{E,N}(G_{\mathbb{Q}})$ depends on the choice of isomorphism between $E[n]$ and $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and is therefore only defined up to conjugation. This means that different isomorphisms $\phi, \phi' : E[N] : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ induce different Galois representations $\rho_{E,N}(G_{\mathbb{Q}})$, $\rho'_{E,N}(G_{\mathbb{Q}})$ with $\rho_{E,N}(G_{\mathbb{Q}}) = g(\rho'_{E,N}(G_{\mathbb{Q}}))g^{-1}$ for some $g \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

We now prove the following lemma:

Lemma 2.30. *Let $E/\mathbb{Q}$ be an elliptic curve and let $n \geq 1$. Then $\mathbb{Q}(E[n])$ is a Galois extension.*

Proof: The n-division field is a finite extension which is algebraic by the Weierstrass equation for E. It is also separable as it is an extension of $\mathbb{Q}$. For normality we recall that an element $\sigma \in G_{\mathbb{Q}}$ sends n-torsion points to n-torsion points. So x, y-coordinates of n-torsion points get sent to x, y-coordinates of n-torsion points and therefore $\sigma(\mathbb{Q}(E[n])) \subseteq \mathbb{Q}(E[n])$. As we have the following tower of field extensions $\mathbb{Q} \subseteq \mathbb{Q}(E[n]) \subseteq \bar{\mathbb{Q}}$ we get by [3, Lemma 9.2.3] that $\mathbb{Q}(E[n])$ is normal.

□

Remark 2.31. The kernel of the Galois representation $\rho_{E,n}$ consists of all $\sigma \in G_{\mathbb{Q}}$ with $\sigma(P) = P$ for $P \in E[n]$, or in other words all $\sigma \in G_{\mathbb{Q}}$ such that $\sigma(x) = x$ for all $x \in \mathbb{Q}(E[n])$. By the fundamental theorem of Galois theory this is precisely the subgroup of $G_{\mathbb{Q}}$ given by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(E[n]))$. So we get that $\rho_{E,n}$ induces an injective Galois representation

$$\widetilde{\rho_{E,n}} : G_{\mathbb{Q}}/\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(E[n])) \to \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z}).$$

By [3, Theorem 9.2.2] combined with the fact that $\mathbb{Q}(E[n])/\mathbb{Q}$ is a Galois extension we get that $G_{\mathbb{Q}}/\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(E[n])) \cong \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ and therefore we get the injective Galois representation

$$\widetilde{\rho_{E,n}} : \mathrm{Gal}(\mathbb{Q}(E[n]/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z}).$$

Note that the first isomorphism theorem of groups now implies that

$$\rho_{E,n}(G_{\mathbb{Q}}) \cong \mathrm{Gal}(\mathbb{Q}(E[n]/\mathbb{Q}).$$

We now focus on the Galois group of $\mathbb{Q}(E[n])/\mathbb{Q}$ in the case where $n = 2$:

Lemma 2.32. [1, Proposition 5.4.2] *Let $E/\mathbb{Q}$ be an elliptic curve. Then we have that the Galois group of $\mathbb{Q}(E[2])$ over $\mathbb{Q}$ is isomorphic to the following:*

$$\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) = \begin{cases} \mathrm{GL}(2,\mathbb{Z}/2\mathbb{Z}) \cong S_3 \textit{ if } \ \Delta_E \notin (\mathbb{Q}^*)^2 \textit{ and } E[2] \textit{ contains no rational points,} \\ \mathbb{Z}/3\mathbb{Z} \textit{ if } \ \Delta_E \in (\mathbb{Q}^*)^2 \textit{ and } E[2] \textit{ contains no rational points,} \\ \mathbb{Z}/2\mathbb{Z} \textit{ if } \ \Delta_E \notin (\mathbb{Q}^*)^2 \textit{ and } E[2] \textit{ contains a rational point,} \\ \{0\} \textit{ if } \ \Delta_E \in (\mathbb{Q}^*)^2 \textit{ and } E[2] \textit{ contains a rational point.} \end{cases}$$

In particular we have that $\mathbb{Q}(\sqrt{\Delta_E})$ is the unique quadratic subfield of $\mathbb{Q}(E[2])$.

Proof: We first assume $E/\mathbb{Q}$ is of the form $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Q}$. We have that $\mathbb{Q}(E[2])$ consists of the coordinates of 2-torsion points of E. The 2-torsion points are then precisely the points of E with y-coordinate 0 and x-coordinate a root of $x^3 + Ax + B$. Note that the discriminant Δ_E of E is given by $\Delta_E = 16(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2$ with $\alpha_1, \alpha_2, \alpha_3$ the roots of $x^3 + Ax + B$. We see that

$$\sqrt{\Delta_E} = 4(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) \in \mathbb{Q}(E[2]).$$

We claim that $\mathbb{Q}(E[2]) = \mathbb{Q}(\alpha_1, \sqrt{\Delta_E})$. The inclusion from right to left is obvious. For the other inclusion note that first of all we have that

$$x^3 + Ax + B = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3).$$

Note that $-\alpha_1 \cdot \alpha_2 \cdot \alpha_3 = B$. We have that not both A, B are zero, as then $\Delta_E = 0$. So there is at least one root which is non-zero. Without loss of generality we can assume $\alpha_1 \neq 0$. Also we have that the coefficient of x^2 is zero, so $\alpha_1 + \alpha_2 + \alpha_3 = 0$. We therefore get that

$$\begin{aligned} &\sqrt{\Delta_E} = 4(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3) = \\ &4(\alpha_1^2 - \alpha_1\alpha_2 - \alpha_1\alpha_3 + \alpha_2\alpha_3)(\alpha_2 - \alpha_3) = \\ &4(2\alpha_1^2 + \alpha_2\alpha_3)(\alpha_2 - \alpha_3) = \\ &4(2\alpha_1^2 + \frac{B}{\alpha_1})(\alpha_2 - \alpha_3). \end{aligned}$$

This implies that $\alpha_2 - \alpha_3 \in \mathbb{Q}(\alpha_1, \sqrt{\Delta_E})$. As also $\alpha_2 + \alpha_3 = -\alpha_1$ we get that

$$\mathbb{Q}(E[2]) = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \subseteq \mathbb{Q}(\alpha_1, \sqrt{\Delta_E}).$$

So we have that $\mathbb{Q}(E[2]) = \mathbb{Q}(\alpha_1, \sqrt{\Delta_E})$. Its Galois group must therefore have order dividing 6. We consider multiple cases.

If $x^3 + Ax + B$ is irreducible over $\mathbb{Q}[X]$, then there is no rational root, so $\mathbb{Q}(\alpha_1) \neq \mathbb{Q}$ and $[\mathbb{Q}(E[2]) : \mathbb{Q}] \geq 3$. If $\sqrt{\Delta_E} \in \mathbb{Q}$ then $\mathbb{Q}(E[2]) = \mathbb{Q}(\alpha_1)$, $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 3$ and $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$. If this is not the case then $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 6$ and so $|\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})| = 6$. In order to see what group structure its Galois group has we note the following: We have that $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ is generated by σ, τ with first of all σ defined by $\sigma(\alpha_1) = \alpha_2$, $\sigma(\alpha_2) = \alpha_3$ and $\sigma(\alpha_3) = \alpha_1$ and $\sigma(\sqrt{\Delta_E}) = \sqrt{\Delta_E}$ (note that this is well defined as permuting the roots in this way does not change the sign of the discriminant), while τ is defined by $\tau(\alpha_1) = \alpha_3$, $\tau(\alpha_3) = \alpha_1$, $\tau(\alpha_2) = \alpha_2$ and $\tau(\sqrt{\Delta_E}) = -\sqrt{\Delta_E}$ (Interchanging only two roots does change the sign of the discriminant). We get that $\sigma^3 = \mathrm{id}$ and that $\tau^2 = \mathrm{id}$. We also see that $\sigma\tau(\alpha_1) = \alpha_1$, $\sigma\tau(\alpha_2) = \alpha_3$, $\sigma\tau(\alpha_3) = \alpha_2$ and $\sigma\tau(\sqrt{\Delta_E}) = -\sqrt{\Delta_E}$. On the other hand we have that $\tau\sigma^2(\alpha_1) = \alpha_1$, $\tau\sigma^2(\alpha_2) = \alpha_3$, $\tau\sigma^2(\alpha_3) = \alpha_2$ and $\tau\sigma^2(\sqrt{\Delta_E}) = -\sqrt{\Delta_E}$, which implies that $\sigma\tau = \tau\sigma^2$ and therefore that $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) = S_3$.

Now we assume $x^3 + Ax + B$ is reducible. Then either $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 2$ or $\mathbb{Q}(E[2]) = \mathbb{Q}$. As $\sqrt{\Delta_E} \in \mathbb{Q}(E[2])$ we get that $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{\Delta_E})$ and so either $\sqrt{\Delta_E} \notin \mathbb{Q}$ which implies that $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 2$ and $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$, or we have that $\sqrt{\Delta_E} \in \mathbb{Q}$ and $\mathbb{Q}(E[2]) = \mathbb{Q}$.

We have the following diagram which gives the Galois correspondence of the (normal) subgroups of S_3 and the corresponding fixed fields of $\mathbb{Q}(E[2])$:

$$\begin{tikzcd}
& \mathbb{Q}(E[2]) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\alpha) \arrow[dr, dash] & & \mathbb{Q}(\sqrt{\Delta_E}) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
& \{e\} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Z}/2\mathbb{Z} \arrow[dr, dash] & & \mathbb{Z}/3\mathbb{Z} \arrow[dl, dash] \\
& \mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z}) &
\end{tikzcd}$$

Now for the general case we note that every $E/\mathbb{Q}$ is isomorphic over $\mathbb{Q}$ to an elliptic curve $E'/\mathbb{Q}$ in short Weierstrass form, and we have just seen for elliptic curves E' in short Weierstrass form that $\mathbb{Q}(E'[2]) = \mathbb{Q}(\alpha, \sqrt{\Delta_{E'}})$ for some $\alpha \in \bar{\mathbb{Q}}$. Because $E \cong E'$ over $\mathbb{Q}$ we get that $\Delta_E \equiv \Delta_{E'} \pmod{(\mathbb{Q}^*)^2}$ and so $\Delta_E \notin (\mathbb{Q}^*)^2$ if and only if $\Delta_{E'} \notin (\mathbb{Q}^*)^2$. We also get that E has a rational point if and only if E' has a rational point. Now we also get that $\Delta_E \equiv \Delta_{E'} \pmod{(\mathbb{Q}^*)^2}$ implies that

$$\mathbb{Q}(E'[2]) = \mathbb{Q}(\alpha, \sqrt{\Delta_{E'}}) = \mathbb{Q}(\alpha, \sqrt{\Delta_E}).$$

The isomorphism between E' and E induces a group isomorphism between $E'[2]$ and $E[2]$, and as the isomorphism between E and E' was given over $\mathbb{Q}$ we get that the coordinates of $E[2]$ are rational combinations of the coordinates of $E'[2]$. We have that $\mathbb{Q}(E'[2]) = \mathbb{Q}(\alpha, \sqrt{\Delta_E})$ and so the coordinates of the points of $E'[2]$ are given by rational combinations of α and $\sqrt{\Delta_E}$. This now also holds for the coordinates of the points of $E[2]$ as they where given by rational combinations of the coordinates of $E'[2]$ in turn. Therefore $\mathbb{Q}(E[2]) = \mathbb{Q}(\alpha, \sqrt{\Delta_E})$ as well. In particular we have that $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(E[2])$. Now finally recall that E has a rational point if and only if E' has a rational point and that $\Delta_E \notin (\mathbb{Q}^*)^2$ if and only if $\Delta_{E'} \notin (\mathbb{Q}^*)^2$. This then concludes the proof.

□

2.2.5 ℓ-adic- and full Galois representations of elliptic curves

We have constructed a Galois representation on $E/\mathbb{Q}$ for all $n \geq 1$ by using the fact that $G_{\mathbb{Q}}$ acts on E_n. But we can also extend this and show that $G_{\mathbb{Q}}$ acts on the ℓ-adic Tate module $T_\ell(E)$ and the adelic Tate module $T(E)$ as well.

Definition 2.33. First of all note that for $\sigma \in G_{\mathbb{Q}}$ the following diagram commutes:

$$\begin{tikzcd}
E[\ell^{n+1}] \arrow[r, "\sigma"] \arrow[d, "{[\ell]}"'] & E[\ell^{n+1}] \arrow[d, "{[\ell]}"] \\
E[\ell^n] \arrow[r, "\sigma"] & E[\ell^n]
\end{tikzcd}$$

This follows because for $P \in E[\ell^{n+1}]$ we have that $[\ell](\sigma(P)) = \sigma([\ell](P))$. Therefore we get that the actions of $G_{\mathbb{Q}}$ on all $E[\ell^{n+1}]$ by sending $P \mapsto \sigma(P)$ for $n \geq 1$ induce an action of $G_{\mathbb{Q}}$ on $T_\ell(E)$. We get the **ℓ-adic Galois representation**

$$\rho_{E,\ell^\infty} : G_{\mathbb{Q}} \to \mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}(2, \mathbb{Z}_\ell)$$

where the last isomorphism follows from the fact that for elliptic curves $E/\mathbb{Q}$ we have that $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ (Theorem 2.6).

We can repeat this argument for the adelic Tate module.

Definition 2.34. The following diagram also commutes:

$$\begin{tikzcd}
E[kn] \arrow[r, "\sigma"] \arrow[d, "{[k]}"'] & E[kn] \arrow[d, "{[k]}"] \\
E[n] \arrow[r, "\sigma"] & E[n]
\end{tikzcd}$$

So we also get an induced action $G_{\mathbb{Q}}$ on $T(E)$ which gives rise to the Galois representation

$$\rho_E : G_{\mathbb{Q}} \to \mathrm{Aut}(T(E)) \cong \mathrm{GL}(2, \hat{\mathbb{Z}})$$

where the last isomorphism follows from the fact that for elliptic curves $E/\mathbb{Q}$ we have that $T(E) \cong \hat{\mathbb{Z}} \times \hat{\mathbb{Z}}$ (Remark 2.8) We call this representation the **full Galois representation** of E.

We close this chapter by showing, using the properties of the Weil pairing, that the determinant of the image of $\sigma \in G_{\mathbb{Q}}$ under $\rho_{E,n}$ is equal to the n-th cyclotomic character of σ:

Lemma 2.35. [6, Proposition 1.3.14 *Let $E/\mathbb{Q}$ be an elliptic curve, let ℓ be a prime and let $\sigma \in G_{\mathbb{Q}}$. Then*

$$\sigma(\zeta_n) = \zeta_n^{\det(\rho_{E,n}(\sigma))}$$

for all n-th roots of unity ζ_n. If we define $\det(\rho_{E,n}(G_{\mathbb{Q}}))$ *as the group given by*

$$\{\det(\rho_{E,n}(\sigma) \mid \sigma \in G_{\mathbb{Q}}\},$$

then we get that $\det(\rho_{E,n}(G_{\mathbb{Q}})) \cong (\mathbb{Z}/N\mathbb{Z})^*$.

Proof: For this proof we refer to [6]. The Weil pairing is surjective [35, III.8.1.1], so there exist S, T in $E[n]$ such that for ζ_n a primitive n-th root of unity we have that $\zeta_n = e_n(S,T)$. We now show that S, T generate $E[n]$. To do this we show that S, T are linearly independent over $\mathbb{Z}/n\mathbb{Z}$. Assume that there are $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$ such that $\alpha S + \beta T = \mathcal{O}$. Then by properties of the Weil pairing we get that

$$1 = e_n(\mathcal{O}, T) = e_n(\alpha S + \beta T, T) \overset{(a)}{=} e_n(S,T)^{\alpha} \cdot e_n(T,T)^{\beta} \overset{(b)}{=} \zeta_n^{\alpha}$$

which implies that $\alpha = 0$. We can repeat this argument to show that $\beta = 0$ and therefore S, T are linearly independent. Now we have that

$$\sigma(\zeta_n) = \sigma(e_n(S,T)) = e_n(\sigma(S), \sigma(T)).$$

This implies that there are $p, q \in \mathbb{Z}/n\mathbb{Z}$ such that $\sigma(S) = pS + qT$ and $v, w \in \mathbb{Z}/n\mathbb{Z}$ such that $\sigma(T) = vS + wT$. We get

$$e_n(\sigma(S), \sigma(T)) = e_n(pS + qT, vS + wT) \overset{(a)}{=}$$
$$e_n(S,S)^{pv} e_n(S,T)^{pw} e_n(T,S)^{qv} e_n(T,T)^{qw} \overset{(b)}{=} e_n(S,T)^{pw-qv} = \zeta_n^{\det(\rho_{E,n}(\sigma))}.$$

Here the last equality follows from the fact that σ sends S, T to respectively $pS + qT$ and $vS + wT$ and therefore σ gets sent to the matrix $\begin{pmatrix} p & v \\ q & w \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ which has determinant $pw - qv$. Now because $\sigma(\zeta_n) = \zeta_n^{\det(\rho_{E,n}(\sigma))}$ for a primitive n-th root of unity, and every n-th root of unity is a power of a primitive n-th root of unity, we get that $\sigma(\zeta_n) = \zeta_n^{\det(\rho_{E,n}(\sigma))}$ holds for all n-th roots of unity as σ is a homomorphism. Note that this does not depend on the choice of Galois representation, as the determinant of $\rho_{E,n}(\sigma)$ is always the same for every choice of $\rho_{E,n}$.

$\square$

3 Entanglement of Galois representations of elliptic curves

In this chapter we shall study different reasons why the images of the Galois representations attached to elliptic curves are not as big as they could be. We give definitions of different kinds of obstructions for surjectivity of these representations, of which the most important ones are called vertical entanglement and horizontal entanglement. We list multiple known results for these kinds of obstructions and provide a few examples. We shall mainly follow [11].

Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$ and let $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$ with $\bar{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$. We have for $n \geq 1$ the n-torsion group $E[n]$ of $E(\bar{\mathbb{Q}})$ and the associated Galois representation

$$\rho_{E,n} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z}).$$

We also have for ℓ prime the ℓ-adic Tate module $T_\ell(E)$ and we get an ℓ-adic Galois representation

$$\rho_{E,\ell^\infty} : G_{\mathbb{Q}} \to \mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}(2, \mathbb{Z}_\ell).$$

Finally we have the adelic Tate module $T(E)$ and its associated full Galois representation

$$\rho_E : G_{\mathbb{Q}} \to \mathrm{Aut}(T(E)) \cong \mathrm{GL}(2, \hat{\mathbb{Z}}).$$

Definition 3.1. Recall that elliptic curves E can have N-isogenies $\phi : E \to E'$, where we have that $\ker(\phi) \subset E[N]$ is a cyclic group of order N. We call ϕ a **cyclic N-isogeny** if $\ker(\phi)$ is cyclic and we call ϕ a **rational N-isogeny** if $\ker(\phi)$ is stable under the action of $G_{\mathbb{Q}}$, meaning that for $\sigma \in G_{\mathbb{Q}}$ and $P \in \ker(\phi) \subset E[N]$ we have that $\sigma(P) \in \ker(\phi)$.

Remark 3.2. We note that every subgroup of $E(\mathbb{C})$ of order N gives rise to an N-isogeny [35, III.4.12] and the kernel of every N-isogeny is a subgroup of $E(\mathbb{C})$ of order N. Also a subgroup of $E(\mathbb{C})$ is $G_{\mathbb{Q}}$ stable and/or cyclic if and only if the corresponding N-isogeny is rational and/or cyclic. This implies that $E/\mathbb{Q}$ having a (rational/cyclic) N-isogeny is equivalent to $E(\mathbb{C})$ having a ($G_{\mathbb{Q}}$ stable/cyclic) subgroup.

For elliptic curves $E/\mathbb{Q}$ which have rational points of given order or have a rational n-isogeny we can show that the image of $\rho_{E,n}$ is of the following particular forms:

Proposition 3.3. *Let $E/\mathbb{Q}$ be an elliptic curve. Then we have the following:*

1. *E contains a point $P \in E(\mathbb{Q})$ of order N if and only if $\rho_{E,N}(G_{\mathbb{Q}}) \subseteq gHg^{-1}$ with*

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}(\mathbb{Z}/N\mathbb{Z}) \mid b, d \in \mathbb{Z}/N\mathbb{Z} \right\}$$

for some $g \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

2. E has a rational cyclic N-isogeny (or equivalently $E(\mathbb{C})$ has a rational cyclic subgroup) if and only if $\rho_{E,N}(G_{\mathbb{Q}}) \subseteq gHg^{-1}$ with

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}(\mathbb{Z}/N\mathbb{Z}) \mid a, b, d \in \mathbb{Z}/N\mathbb{Z} \right\}$$

for some $g \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

Proof: We first prove 1. Take $\sigma \in G_{\mathbb{Q}}$ and let $P \in E(\mathbb{Q})$ be the point of order N, then we can choose a isomorphism $\phi : E[N] \cong \mathbb{Z}/N\mathbb{Z}/ \times \mathbb{Z}/N\mathbb{Z}$ in such a way that P gets sent to $(1, 0)$. This induces the Galois representation $\rho_{E,N}(G_{\mathbb{Q}})$. Note that P is rational and therefore we get that $\sigma(P) = P$. Let $Q \in E[N]$ be the point for which $\phi(Q) = (0, 1)$, then we must have that $\sigma(Q) = bP + dQ$ for some $b, d \in \mathbb{Z}/N\mathbb{Z}$. This means that

$$\rho_{E,N}(\sigma) = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$$

for some $b, d \in \mathbb{Z}/N\mathbb{Z}$ and so we get that $\rho_{E,N}(G_{\mathbb{Q}}) \subseteq H$ with

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}(\mathbb{Z}/N\mathbb{Z}) \mid b, d \in \mathbb{Z}/N\mathbb{Z} \right\}.$$

Note that Lemma 2.35 implies that d corresponds to the N-th cyclotomic character of σ. As $\rho_{E,N}(G_{\mathbb{Q}})$ is defined up to conjugation in $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$, we get that in general $\rho_{E,N}(G_{\mathbb{Q}}) \subseteq gHg^{-1}$ for some $g \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$. Conversely if $\rho_{E,N}(G_{\mathbb{Q}}) \subseteq gHg^{-1}$ for some $g \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$, then there exists a Galois representation $\rho'_{E,N}$ such that $\rho_{E,N}(G_{\mathbb{Q}}) \subseteq H$. But then $\sigma(P) = P$ for some point $P \in E[N]$ of order N, which implies that $P \in E(\mathbb{Q})$.

Now we prove 2. Again take $\sigma \in G_{\mathbb{Q}}$ and let ϕ be the rational cyclic N-isogeny of E. Then there exists a $P \in E(\mathbb{Q})$ of order N which generates the kernel of ϕ. We can choose a isomorphism $\phi : E[N] \cong \mathbb{Z}/N\mathbb{Z}/ \times \mathbb{Z}/N\mathbb{Z}$ in such a way that P gets sent to $(1, 0)$. This induces the Galois representation $\rho_{E,N}(G_{\mathbb{Q}})$. As ϕ is rational we get that $\sigma(P) \in \ker(\phi)$ and therefore $\sigma(P) = aP$ for some $a \in \mathbb{Z}/N\mathbb{Z}$. Let Q be the point for which $\phi(Q) = (0, 1)$, then we must have that $\sigma(Q) = bP + dQ$ for some $b, d \in \mathbb{Z}/N\mathbb{Z}$. This means that in general $\rho_{E,N}(G_{\mathbb{Q}}) \subseteq gHg^{-1}$ with

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}(\mathbb{Z}/N\mathbb{Z}) \mid b, d \in \mathbb{Z}/N\mathbb{Z} \right\}$$

for some $g \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$. Conversely if $\rho_{E,N}(G_{\mathbb{Q}}) \subseteq gHg^{-1}$ for some $g \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$, then there exists a Galois representation $\rho'_{E,N}$ such that $\rho_{E,N}(G_{\mathbb{Q}}) \subseteq H$. But then $E[N]$ contains a cyclic subgroup stable under $G_{\mathbb{Q}}$, or in other words E has a rational cyclic N-isogeny.

□

Remark 3.4. Note that the isomorphism $\phi : \hat{\mathbb{Z}} \cong \prod_{\ell} \mathbb{Z}_\ell$ induces an isomorphism $\mathrm{GL}(2, \hat{\mathbb{Z}}) \cong \prod_{\ell} \mathrm{GL}(2, \mathbb{Z}_\ell)$ which restricts to an injective map

$$\rho_E(G_{\mathbb{Q}}) \xrightarrow{\psi} \prod_{\ell} \rho_{E,\ell^\infty}(G_{\mathbb{Q}}) \subseteq \prod_{\ell} \mathrm{GL}(2, \mathbb{Z}_\ell) \cong \mathrm{GL}(2, \hat{\mathbb{Z}})$$

where ψ sends the matrix $X = (x_i) \in \rho_E(G_{\mathbb{Q}}) \subseteq \mathrm{GL}(2, \hat{\mathbb{Z}})$ to the tuple of matrices $(X_\ell)_\ell$, which is given by sending each coordinate $x_i \in X$ to $\phi(x_i) \in \prod_{\ell} \mathbb{Z}_\ell$. Thi sshows that we have two main ways in which the image of the full representation is smaller than it could be. We either have for at least one prime ℓ that ρ_{E,ℓ^∞} is non-surjective, so-called vertical entanglement. Or we have that the map ψ is not surjective which we call horizontal entanglement. We first define vertical entanglement.

3.1 Vertical entanglement

Definition 3.5. Let $E/\mathbb{Q}$ be an elliptic curve and let ℓ be a prime number. Then we have **vertical ℓ-entanglement** if $\rho_{E,\ell^\infty} : G_{\mathbb{Q}} \to \mathrm{GL}(2, \mathbb{Z}_\ell)$ is not surjective.

Example 3.6. We have shown in Lemma 2.32 for $E/\mathbb{Q}$ that the Galois group of $\mathbb{Q}(E[2])/\mathbb{Q}$ is isomorphic to the following:

$$\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) = \begin{cases} \mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z}) \cong S_3 \text{ if } \Delta_E \notin (\mathbb{Q}^*)^2 \text{ and } E[2] \text{ contains no rational points,} \\ \mathbb{Z}/3\mathbb{Z} \text{ if } \Delta_E \in (\mathbb{Q}^*)^2 \text{ and } E[2] \text{ contains no rational points,} \\ \mathbb{Z}/2\mathbb{Z} \text{ if } \Delta_E \notin (\mathbb{Q}^*)^2 \text{ and } E[2] \text{ contains a rational point,} \\ \{0\} \text{ if } \Delta_E \in (\mathbb{Q}^*)^2 \text{ and } E[2] \text{ contains a rational point.} \end{cases}$$

We have that $\rho_{E,2^\infty}$ is only surjective if $\rho_{E,2}$ is surjective. Furthermore as $\rho_{E,2}(G_{\mathbb{Q}}) \cong \mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ we have that $\rho_{E,2^\infty}$ is only surjective if $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong S_3$.

We have the following known results for vertical entanglement: First of all for $\ell \neq 2, 3$ we have that ρ_{E,ℓ^∞} is surjective if and only if $\rho_{E,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}(2, \mathbb{Z}/\ell\mathbb{Z})$ is surjective as shown by Serre [32].

For $\ell = 2$ we have that $\rho_{E,2^\infty}$ is surjective if and only if $\rho_{E,8} : G_{\mathbb{Q}} \to \mathrm{GL}(2, \mathbb{Z}/8\mathbb{Z})$ is surjective [14] and for $\ell = 3$ we have that $\rho_{E,3^\infty}$ is surjective if and only if $\rho_{E,9} : G_{\mathbb{Q}} \to \mathrm{GL}(2, \mathbb{Z}/9\mathbb{Z})$ is surjective [15].

It also follows from Serre's open image theorem [33] that if K is an algebraic number field and E/K an elliptic curve with no CM, then for only finitely many ℓ prime the ℓ-adic representation can have vertical entanglement. For $\mathbb{Q}$ it is generally believed that the ℓ-adic representation can only have vertical entanglement for $\ell \leq 37$ [33].

In [27] all elliptic curves over $\mathbb{Q}$ are classified which have a certain form of vertical ℓ-entanglement by studying rational points on the modular quotient curve X_H with $H \subseteq \mathrm{GL}(2, \mathbb{Z}_\ell)/\{-I\}$.

3.2 Horizontal entanglement

Before we define horizontal entanglement we first note the following. Assume we have that $\rho_{E,n}$ is not surjective with $n = p_1^{e_1} \cdot \ldots \cdot p_m^{e_m}$ but for all $1 \leq i \leq m$ we have that $\rho_{E,p_i^{e_i}}$ is surjective. We showed earlier that the image of the full representation factors through the images of the ℓ-adic representations, so we must have that the injective map

$$\rho_{E,n}(G_\mathbb{Q}) \xrightarrow{\psi} \prod_i \rho_{E,p_i^{e_i}}(G_\mathbb{Q})$$

is not surjective. We recall that $\rho_{E,n}(G_\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ and that $\rho_{E,p_i^{e_i}}(G_\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(E[p_i^{e_i}])/\mathbb{Q})$. So we get an injective map

$$\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \xrightarrow{\hat{\psi}} \prod_i \mathrm{Gal}(\mathbb{Q}(E[p_i^{e_i}])/\mathbb{Q}).$$

Note that $\mathbb{Q}(E[n])$ is the compositum of $\mathbb{Q}(E[p_j^{e_j}])$ for all $1 \leq j \leq m$ and that $\hat{\psi}$ is the restriction map, so Lemma 2.17 now gives us that $\hat{\psi}$ is surjective if and only if $\mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]) = \mathbb{Q}$ for all a, b coprime divisors of n. This indicates that the second way in which the image of the full representation can be non-surjective is when $\mathbb{Q}(E[m]) \cap \mathbb{Q}(E[n]) \neq \mathbb{Q}$ for m, n coprime integers. This brings us to the definition of horizontal entanglement.

Definition 3.7. Let $E/\mathbb{Q}$ be an elliptic curve and let $a < b$ be integers with $d = \gcd(a, b)$. Then we have **horizontal** (a, b)**-entanglement** if

$$\mathbb{Q}(E[d]) \subsetneq \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]).$$

We define the **type** of this entanglement to be the isomorphism class of the Galois group corresponding to $\mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b])/\mathbb{Q}(E[d])$.

Corresponding to this definition we have the following diagram:

$$\begin{tikzcd}
\mathbb{Q}(E[a]) \arrow[dr, dash] & & \mathbb{Q}(E[b]) \arrow[dl, dash] \\
& \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]) \arrow[d, dash] & \\
& \mathbb{Q}(E[d]) &
\end{tikzcd}$$

We have from Lemma 3.4 in [9] that horizontal (fa, fb)-entanglement induces horizontal (a, b)-entanglement if $\gcd(a, f) = \gcd(b, f) = 1$. For a proof of this lemma we refer to the proof of Lemma 3.26. If furthermore a, b are coprime we have shown that the full representation ρ_E is non-surjective. This is the reason why we do not immediately restrict our definition of horizontal entanglement to coprime integers.

Example 3.8. Take the elliptic curve $E : y^2 = x^3 + 3$. Its discriminant is given by $\Delta_E = -3888 = -1 \cdot 2^4 \cdot 3^5$. Lemma 2.32 shows us that $\mathbb{Q}(\sqrt{\Delta_E}) = \mathbb{Q}(\sqrt{-3}) \subseteq \mathbb{Q}(E[2])$. We also have by Theorem 2.18 that $\mathbb{Q}(\sqrt{-3})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_3)$ and by Lemma 2.27 that $\mathbb{Q}(\zeta_3) \subseteq \mathbb{Q}(E[3])$. Combining all this we get that

$$\mathbb{Q}(\sqrt{-3}) \subseteq \mathbb{Q}(E[2]) \cap \mathbb{Q}(E[3])$$

and so we get horizontal $(2, 3)$-entanglement. As 2,3 are coprime we get that $\mathrm{Gal}(\mathbb{Q}(E[6])/\mathbb{Q})$ is not of maximal rank and therefore that $\rho_{E,6}$ is non-surjective. This entanglement is induced by the Weil pairing (and the Kronecker-Weber Theorem) and is called Weil entanglement. This kind of entanglement we will discuss in more detail in the next subsection.

Note that our two definitions of vertical and horizontal entanglement coincide with the definitions given in [11].

Horizontal entanglement is less well understood than vertical entanglement, but there have been recent results ([9],[10],[11]).

3.3 Abelian and Weil entanglement

Following [11] we now define another type of entanglement, called abelian entanglement. We denote by $\mathbb{Q}^{\mathrm{ab}}$ the largest Galois extension of $\mathbb{Q}$ such that the Galois group of the extension is abelian. This implies that the intersections of other Galois extensions with $\mathbb{Q}^{\mathrm{ab}}$ are abelian as well, as these intersections are subfields of $\mathbb{Q}^{\mathrm{ab}}$ and quotients of abelian groups are abelian.

Definition 3.9. Let $E/\mathbb{Q}$ be an elliptic curve and let $a < b$ be integers with $d = \gcd(a, b)$. Then E has **abelian (a, b)-entanglement** if

$$\mathbb{Q}(\zeta_d) \subsetneq \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]) \cap \mathbb{Q}^{\mathrm{ab}}.$$

We have the following diagram corresponding to this definition:

$$\begin{tikzcd}
\mathbb{Q}(E[a]) \arrow[dr, dash] & & \mathbb{Q}(E[b]) \arrow[dl, dash] \\
& \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]) \arrow[d, dash] & \\
& \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]) \cap \mathbb{Q}^{\mathrm{ab}} \arrow[d, dash] & \\
& \mathbb{Q}(\zeta_d) &
\end{tikzcd}$$

Note that $\mathbb{Q}(\zeta_d) \subseteq \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]) \cap \mathbb{Q}^{\mathrm{ab}}$ as $\mathbb{Q}(\zeta_d) \subseteq \mathbb{Q}(E[d]) \subseteq \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b])$ and $\mathbb{Q}(\zeta_d) \subseteq \mathbb{Q}^{\mathrm{ab}}$. The name abelian entanglement comes from the fact that the intersection field $\mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]) \cap \mathbb{Q}^{\mathrm{ab}}$ is an abelian extension of $\mathbb{Q}$. Note that if E has abelian (m, n)-entanglement with m, n coprime, then we get horizontal (m, n)-entanglement of coprime integers which leads to a smaller image of the full representation.

We also have a subclass of abelian entanglement, which is called Weil entanglement.

Definition 3.10. Let $E/\mathbb{Q}$ be an elliptic curve and let $a < b$ be integers with $d = \gcd(a, b)$. Let $K_a = \mathbb{Q}(E[a]) \cap \mathbb{Q}^{\mathrm{ab}}$ and $K_b = \mathbb{Q}(E[b]) \cap \mathbb{Q}^{\mathrm{ab}}$. Then E has **Weil** (a, b)**-entanglement** if

$$\mathbb{Q}(\zeta_d) \subsetneq K_a \cap \mathbb{Q}(\zeta_b) \quad \text{or} \quad \mathbb{Q}(\zeta_d) \subsetneq \mathbb{Q}(\zeta_a) \cap K_b.$$

We have the following diagram corresponding to this definition:

$$\begin{tikzcd}
\mathbb{Q}(E[a]) \arrow[d, dash] & & & \mathbb{Q}(E[b]) \arrow[d, dash] \\
K_a = \mathbb{Q}(E[a]) \cap \mathbb{Q}^{\mathrm{ab}} \arrow[d, dash] \arrow[ddrr, dash] & & & K_b = \mathbb{Q}(E[b]) \cap \mathbb{Q}^{\mathrm{ab}} \arrow[d, dash] \arrow[ddll, dash] \\
\mathbb{Q}(\zeta_a) \arrow[dr, dash] & & & \mathbb{Q}(\zeta_b) \arrow[dl, dash] \\
& K_b \cap \mathbb{Q}(\zeta_a) \arrow[d, dash] & K_a \cap \mathbb{Q}(\zeta_b) \arrow[d, dash] & \\
& \mathbb{Q}(\zeta_d) & \mathbb{Q}(\zeta_d) &
\end{tikzcd}$$

To see that Weil entanglement is a form of abelian entanglement, we note that if $\mathbb{Q}(\zeta_d) \subsetneq K_a \cap \mathbb{Q}(\zeta_b)$, then $\mathbb{Q}(\zeta_d) \subsetneq K_a \cap \mathbb{Q}(\zeta_b) \subseteq \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]) \cap \mathbb{Q}^{\text{ab}}$ as $\mathbb{Q}(\zeta_b) \subseteq \mathbb{Q}(E[b])$ by the Weil pairing. Similarly $\mathbb{Q}(\zeta_d) \subsetneq \mathbb{Q}(\zeta_a) \cap K_b$ also implies that $\mathbb{Q}(\zeta_d) \subsetneq \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]) \cap \mathbb{Q}^{\text{ab}}$.

Remark 3.11. The name Weil entanglement comes from the fact that it gives rise to (abelian) entanglement by properties of the Weil pairing. We also note that by the Kronecker-Weber Theorem an abelian extension is always contained in some n-cyclotomic field, so Weil entanglement for elliptic curves over $\mathbb{Q}$ can be seen as a consequence of the Weil pairing combined with the Kronecker-Weber Theorem.

Example 3.12. We have in [11] the following example of abelian entanglement which is not Weil. Let $E/\mathbb{Q}$ be the elliptic curve over $\mathbb{Q}$ given by LMFDB label 448.g3. Then $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(E[3]) = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$, so $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$ and therefore

$$\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[3]) = \mathbb{Q}(\sqrt{2}).$$

The Galois extension $\mathbb{Q}(\sqrt{2})$ has Galois group $\mathbb{Z}/2\mathbb{Z}$, which is abelian and therefore we have abelian entanglement. On the other hand $\mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\zeta_2)$ and $\mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\zeta_3)$, so this is not Weil entanglement.

3.4 Serre entanglement

We have a very important example of Weil entanglement in the form of Serre entanglement, which is given by Weil $(2, n)$-entanglement of type $\mathbb{Z}/2\mathbb{Z}$ (meaning that its corresponding Galois group is isomorphic to $\mathbb{Z}/2\mathbb{Z}$). The following theorem [11, Theorem 3.7] states that for an elliptic curve there is always Serre entanglement, except when the discriminant is a square which leads to vertical 2-entanglement:

Theorem 3.13. [11, Theorem 3.7]
Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$. Then we have the following two cases:

(1) Δ_E is a square and E has vertical 2-entanglement.
(2) Δ_E is a not a square and E has Serre $(2, 4|\Delta_E|)$-entanglement.

Proof: The first case follows from the fact that if Δ_E is a square, then $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$ or $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ is trivial by Lemma 2.32 and therefore $\rho_{E,2^\infty}$ cannot be surjective.

Now assume Δ_E is a not a square. Then Lemma 2.32 shows that $\mathbb{Q}(\sqrt{\Delta_E})$ is a non-trivial subfield of $\mathbb{Q}(E[2])$. By Corollary 2.19 we have that $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(\zeta_m)$ with $m = 4|\Delta_E|$ (here $\sqrt{\Delta_E}$ should be read as the square root of the squarefree part of Δ_E). This implies that $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(E[2]) \cap \mathbb{Q}(\zeta_m)$ and as $\mathbb{Q}^{\text{ab}} \cap \mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{\Delta_E})$ we get

$$\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{\Delta_E}) = \mathbb{Q}(E[2]) \cap \mathbb{Q}(\zeta_m) \cap \mathbb{Q}^{\text{ab}}.$$

This gives a $(2, 4|\Delta_E|)$ Weil-entanglement with Galois group $\mathbb{Z}/2\mathbb{Z}$, or in other words Serre entanglement.

□

To expand on the work done in [11] we now highlight the connection between Serre entanglement and horizontal entanglement in the following two examples:

Example 3.14. Take the elliptic curve $E : y^2 = x^3 + x + 3$. Its discriminant Δ_E is given by $-3952 = -1 \cdot 2^4 \cdot 13 \cdot 19$. This is not a square and therefore E has Serre $(2, 4 \cdot \Delta_E)$-entanglement. As the squarefree part of -3952 is given by $-13 \cdot 19 = -247$ we get that $\mathbb{Q}(\sqrt{\Delta_E}) = \mathbb{Q}(\sqrt{-247})$ and as $-247 \equiv 1 \pmod 4$ we get by Corollary 2.19 that $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(\zeta_{|247|})$. Note that $\mathbb{Q}(\zeta_{|247|}) \subseteq \mathbb{Q}(E[247])$ by Lemma 2.27 and so because 247 is odd E also has horizontal $(2, 247)$-entanglement.

Example 3.15. Take the elliptic curve $E' : y^2 = x^3 - x + 2$. Its discriminant $\Delta_{E'}$ is $-1664 = -1 \cdot 2^7 \cdot 13$. Here we get that E' has Serre $(2, 4 \cdot \Delta_{E'})$-Serre entanglement. We have that $\mathbb{Q}(\sqrt{\Delta_{E'}}) = \mathbb{Q}(\sqrt{-26})$, and as $-26 \equiv 2 \pmod 4$, Corollary 2.19 gives that $\mathbb{Q}(\sqrt{\Delta_{E'}}) \subseteq \mathbb{Q}(\zeta_{|104|})$. But 104 is even and so this does not induce horizontal entanglement. This shows that abelian (in this case Weil) entanglement does not always directly lead to horizontal entanglement. Now note that $13 = \frac{-26}{-2} \equiv 1 \pmod 4$ and therefore that $\mathbb{Q}(\sqrt{13}) \subseteq \mathbb{Q}(\zeta_{13}) \subseteq \mathbb{Q}(E[13])$. We have that $\sqrt{-26} \in \mathbb{Q}(E[2])$, and as the Weil pairing implies that

$$\sqrt{-1} \in \mathbb{Q}(E[4]) \subseteq \mathbb{Q}(E[8])$$

and that $\sqrt{2} \in \mathbb{Q}(E[8])$ we get that $\sqrt{13} = \frac{\sqrt{-26}}{\sqrt{-2}} \in \mathbb{Q}(E[8])$ and so E' does have horizontal $(8, 13)$-entanglement.

The previous two examples shows that Serre entanglement is very closely related to horizontal entanglement between coprime integers, and therefore to the fact that for every elliptic curve $E/\mathbb{Q}$ the index of the full representation ρ_E is bigger than 1, which is what Serre showed in [33]. Like we have stated in Remark 3.4 that the image of the full representation ρ_E can only get smaller by either vertical or horizontal entanglement, we expand the previous theorem in terms of these kinds of entanglement:

Proposition 3.16. *Let $E/\mathbb{Q}$ be an elliptic curve and let $\overline{\Delta_E}$ be the squarefree part of its discriminant Δ_E with $\overline{\Delta_E} \in \mathbb{Z}$. Then we have four cases:*

(1) E has vertical 2-entanglement,
(2a) $\overline{\Delta_E} \equiv 1 \pmod 4$ and E has horizontal $(2, |\overline{\Delta_E}|)$-entanglement,
(2b) $\overline{\Delta_E} \equiv 3 \pmod 4$ and E has horizontal $(4, |\overline{\Delta_E}|)$-entanglement,
(2c) $\overline{\Delta_E} \equiv 2 \pmod 4$ and E has horizontal $(8, |\frac{\overline{\Delta_E}}{2}|)$-entanglement.
In particular we have that the full representation ρ_E is non-surjective.

Proof: Serre has shown in [32] that vertical 2-entanglement occurs if and only if $\rho_{E,8}$ is non-surjective. In [14] Dokchitser and Dokchitser in turn have shown that if $\rho_{E,8}$ is surjective, then $\Delta_E \notin \pm 1 \cdot (\mathbb{Q}^*)^2$ and $\Delta_E \notin \pm 2 \cdot (\mathbb{Q}^*)^2$. So we can assume that either E has vertical 2-entanglement or we have that $\Delta_E \notin \pm 1 \cdot (\mathbb{Q}^*)^2$ and $\Delta_E \notin \pm 2 \cdot (\mathbb{Q}^*)^2$.

Let $m := \overline{\Delta_E}$ be the squarefree part of Δ_E and assume $m \equiv 1 \pmod 4$. The following part of the proof is very similar to the proof of the previous theorem. As Δ_E is not a square we get that $\mathbb{Q}(\sqrt{m})$ is non-trivial. By Corollary 2.19, which was the simple case of the Kronecker Weber Theorem, we get that $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\zeta_{|m|})$ as $m \equiv 1 \pmod 4$. Furthermore by Lemma 2.27 we get that $\mathbb{Q}(\zeta_{|m|}) \subseteq \mathbb{Q}(E[|m|])$ and so

$$\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\zeta_{|m|}) \subseteq \mathbb{Q}(E[|m|]).$$

We also have by Lemma 2.32 that $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(E[2])$ as $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{\Delta_E})$. Therefore we have that

$$\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(E[2]) \cap \mathbb{Q}(E[|m|]).$$

As $\mathbb{Q}(\sqrt{m})$ is non-trivial and $2, |m|$ are coprime, we get that $\mathbb{Q} \subsetneq \mathbb{Q}(E[2]) \cap \mathbb{Q}(E[|m|])$ and so E has horizontal $(2, |\overline{\Delta_E}|)$-entanglement. Note that this entanglement is induced by the Serre entanglement from Theorem 3.13.

Now assume $m \equiv 3 \pmod 4$. In this case we have that $-m \equiv 1 \pmod 4$ and therefore $\sqrt{-m} \in \mathbb{Q}(\zeta_{|m|})$ by Corollary 2.19. By Lemma 2.27 we get that $\mathbb{Q}(\sqrt{-m}) \subseteq \mathbb{Q}(\zeta_{|m|}) \subseteq \mathbb{Q}(E[|m|])$. Recall that $\sqrt{m} \in \mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[4])$. Lemma 2.27 also implies that $\mathbb{Q}(\zeta_4) \subseteq \mathbb{Q}(E[4])$, so $\sqrt{-1} \in \mathbb{Q}(E[4])$ and therefore $\sqrt{-m} = \sqrt{-1}\sqrt{m} \in \mathbb{Q}(E[4])$. We get that

$$\mathbb{Q}(\sqrt{-m}) \subseteq \mathbb{Q}(E[4]) \cap \mathbb{Q}(E[|m|]).$$

As $\Delta_E \notin -1 \cdot (\mathbb{Q}^*)^2$ we have that $\mathbb{Q}(\sqrt{-m})$ is non-trivial. Also $4, |m|$ are coprime and so E has horizontal $(4, |\overline{\Delta_E}|)$-entanglement. Also here the entanglement is induced by Weil entanglement, but this time it is not Serre entanglement.

Now finally if we have that $m \equiv 2 \pmod 4$, then $\frac{m}{2} \equiv 1, 3 \pmod 4$. If $\frac{m}{2} \equiv 1 \pmod 4$ then again by combining Corollary 2.19 and Lemma 2.27 we get that $\sqrt{\frac{m}{2}} \in \mathbb{Q}(E[|\frac{m}{2}|])$. By Corollary 2.19 combined with Lemma 2.27 we get that $\sqrt{2} \in \mathbb{Q}(\zeta_8) \subseteq \mathbb{Q}(E[8])$, and as by Lemma 2.32 we have that $\sqrt{m} \in \mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[8])$ we get that $\sqrt{\frac{m}{2}} = \frac{\sqrt{m}}{\sqrt{2}} \in \mathbb{Q}(E[8])$. Therefore we get that

$$\mathbb{Q}\left(\sqrt{\frac{m}{2}}\right) \subseteq \mathbb{Q}(E[8]) \cap \mathbb{Q}(E[|\frac{m}{2}|]).$$

As $\Delta_E \notin 2 \cdot (\mathbb{Q}^*)^2$ we have that $\mathbb{Q}\left(\sqrt{\frac{m}{2}}\right)$ is non-trivial, and because $8, |\frac{m}{2}|$ are coprime E has horizontal $(8, |\frac{\overline{\Delta_E}}{2}|)$-entanglement (induced by Weil entanglement).

If $\frac{m}{2} \equiv 3 \pmod 4$ then we have that $\sqrt{\frac{-m}{2}} \in \mathbb{Q}(E[|\frac{m}{2}|])$. By Lemma 2.27 we had that $\sqrt{-m} \in \mathbb{Q}(E[4]) \subseteq \mathbb{Q}(E[8])$, so we get that $\sqrt{\frac{-m}{2}} = \frac{\sqrt{-m}}{\sqrt{2}} \in \mathbb{Q}(E[8])$. Now we get that

$$\mathbb{Q}\left(\sqrt{\frac{-m}{2}}\right) \subseteq \mathbb{Q}(E[8]) \cap \mathbb{Q}(E[|\frac{m}{2}|]).$$

As $\Delta_E \notin -2 \cdot (\mathbb{Q}^*)^2$ we have that $\mathbb{Q}\left(\sqrt{\frac{-m}{2}}\right)$ is non-trivial, and so like before E has horizontal $(8, |\frac{\Delta_E}{2}|)$-entanglement (induced by Weil entanglement).

Note that in all cases E either has vertical 2-entanglement leading to smaller image of ρ_E or E has horizontal entanglement between coprime division fields also leading to a smaller image of ρ_E. This explains why the index of the image of ρ_E is always bigger than 1.

□

Remark 3.17. Theorem 1 in [14] proven by Dokchitser and Dokchitser actually states the following:
Let $E : y^2 = x^3 + Ax + B$ an elliptic curve over $\mathbb{Q}$, then
(1) $\rho_{E,2}$ is surjective if and only if $x^3 + Ax + B$ is irreducible over $\mathbb{Q}[X]$ and $\Delta_E \notin (\mathbb{Q}^*)^2$.
(2) $\rho_{E,4}$ is surjective if and only if $\rho_{E,2}$ is surjective, $\Delta_E \notin -1 \cdot (\mathbb{Q}^*)^2$ and $j(E) \neq -4t^3(t+8)$ for some $t \in \mathbb{Q}^*$.
(3) $\rho_{E,2}$ is surjective if and only if $\rho_{E,4}$ is surjective and $\Delta_E \notin \pm 2 \cdot (\mathbb{Q}^*)^2$.

We now continue with Serre entanglement, first of all showing that for all quadratic number fields $K/\mathbb{Q}$ we can find an elliptic curve E which has Serre entanglement given by $\mathbb{Q}(\sqrt{\Delta_E}) = K$. We then continue by giving for any odd prime number an infinite family of elliptic curves with Serre $(2, p)$-entanglement. Every elliptic curve which has Serre $(2, p)$-entanglement is isomorphic to a curve of this family. We then generalise this from odd primes to integers. We first need the following lemma.

Lemma 3.18. [11, Remark 3.8]
Let $E/\mathbb{Q}$ be an elliptic curve with j-invariant $j(E) \neq 1728$ and let $d \in \mathbb{Q}^*$ be squarefree. Then we have that $\Delta_E \equiv d \pmod{(\mathbb{Q}^*)^2}$ if and only if $j(E) = dt^2 + 1728$ for some $t \in \mathbb{Q}^*$.

Proof: We provide two proofs for this lemma, the first proof done by myself. For the first proof we start by assuming E is of the form $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Q}$. We have that

$$\Delta_E = -16(4A^3 + 27B^2) \quad \text{and} \quad j(E) = 1728 \cdot \frac{4A^3}{4A^3 + 27B^2}.$$

So we get that

$$j(E) - 1728 = 1728 \cdot \frac{4A^3}{4A^3 + 27B^2} - 1728 =$$
$$1728 \cdot (\frac{4A^3}{4A^3 + 27B^2} - 1) = 1728 \cdot (\frac{-27B^2}{4A^3 + 27B^2}) =$$
$$-2^6 3^6 \frac{B^2}{4A^3 + 27B^2} = -16(4A^3 + 27B^2) \cdot \frac{2^2 3^6 B^2}{(4A^3 + 27B^2)^2}.$$

And therefore $\Delta_E \equiv j(E) - 1728 \pmod{(\mathbb{Q}^*)^2}$ (note that here we need that $j(E) \neq 1728$)). If now $\Delta_E \equiv d \pmod{(\mathbb{Q}^*)^2}$ then $d \equiv j(E) - 1728 \pmod{(\mathbb{Q}^*)^2}$ and so $j(E) = dt^2 + 1728$ for some $t \in \mathbb{Q}^*$. If conversely $j(E) = dt^2 + 1728$ for some $t \in \mathbb{Q}^*$ then $\Delta_E \equiv j(E) - 1728 \equiv d \pmod{(\mathbb{Q}^*)^2}$.

Now by Lemma 2.2 we have for isomorphic elliptic curves over $\bar{\mathbb{Q}}$ that their discriminants differ by a square and by [35, III.1.4] that their j-invariants are the same. As every elliptic curve $E/\mathbb{Q}$ is isomorphic over $\mathbb{Q}$ to an elliptic curve in short Weierstrass form we get that for general $E/\mathbb{Q}$ with $j(E) \neq 1728$ that $E \cong E'$ with E' in short Weierstrass form and $\Delta_{E'} \equiv \Delta_E \pmod{(\mathbb{Q}^*)^2}$. If now $\Delta_E \equiv d \pmod{(\mathbb{Q}^*)^2}$ then $\Delta_{E'} \equiv d \pmod{(\mathbb{Q}^*)^2}$ and so $j(E') = dt^2 + 1728$ for some $t \in \mathbb{Q}^*$. If conversely $j(E) = dt^2 + 1728$ for some $t \in \mathbb{Q}^*$, then $j(E') = j(E)$ and so $\Delta_E \equiv \Delta_{E'} \equiv d \pmod{(\mathbb{Q}^*)^2}$. This concludes the first proof.

For the second proof we refer to the proof of [11, 3.8]. Here the universal elliptic curve provided by Silverman in the proof of [35, III.1.4] is used. This universal elliptic curve is given for $j_0 \in \mathbb{Q} \setminus \{0, 1728\}$ by

$$E_{j_0} : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

and this curve has j-invariant $j(E_{j_0}) = j_0$ and discriminant $\Delta_{E_{j_0}} = \frac{j_0^2}{(j_0 - 1728)^3}$. For these elliptic curves we then get that $\Delta_E \equiv j(E) - 1728 \pmod{(\mathbb{Q}^*)^2}$. We also have for $j_0 = 0$ the elliptic curve $y^2 + y = x^3$ with $\Delta = -27$ and also for this curve $\Delta \equiv -1728 \pmod{(\mathbb{Q}^*)^2}$. So we have found for every $j_0 \in \mathbb{Q} \setminus \{1728\}$ an elliptic curve E such that $\Delta_E \equiv j(E) - 1728 \pmod{(\mathbb{Q}^*)^2}$. For these curves a similar argument to the first proof then gives that $\Delta_E \equiv d \pmod{(\mathbb{Q}^*)^2}$ if and only if $j(E) = dt^2 + 1728$ for some $t \in \mathbb{Q}^*$.

Now for general elliptic curves $E/\mathbb{Q}$ with $j(E) \neq 1728$ we note that there is always an elliptic curve E_{j_0} with $j_0 = j(E)$. We get that $E \cong E_{j_0}$ over $\bar{\mathbb{Q}}$ and therefore that their discriminants differ a square. Again a similar argument to the first proof then gives that also for E we have that $\Delta_E \equiv d \pmod{(\mathbb{Q}^*)^2}$ if and only if $j(E) = dt^2 + 1728$ for some $t \in \mathbb{Q}^*$.

□

This lemma will prove useful in the following theorem:

Theorem 3.19. [11, Proposition 3.9]
For a quadratic number field $K/\mathbb{Q}$ there are infinitely many $\bar{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$ with Serre entanglement given by K.

Proof: First note that elliptic curves $E/\mathbb{Q}$ are isomorphic over $\bar{\mathbb{Q}}$ if and only if their j-invariant is equal [35, III.1.4]. Now if we have $K = \mathbb{Q}(\sqrt{d})$ for $d \in \mathbb{Z}^*$ squarefree, then for all elliptic curves $E/\mathbb{Q}$ such that $j_E = dt^2 + 1728$ for $t \in \mathbb{Q}^*$ (such an elliptic curve always exists by [35, III.1.4]) we get that $\Delta_E \equiv d \pmod{(\mathbb{Q}^*)^2}$ by the previous lemma. Therefore we get that $\mathbb{Q}(\sqrt{\Delta_E}) = \mathbb{Q}(\sqrt{d})$. As d is squarefree we have that E has Serre $(2, 4d)$-entanglement given by $\mathbb{Q}(\sqrt{d})$. As for every $t \in \mathbb{Q}^*$ there exist such an elliptic curve and for different t they have different j-invariants (so they are not isomorphic over $\bar{\mathbb{Q}}$) we get infinitely many $\bar{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$ with Serre entanglement given by K.

□

We also give an infinite family of non-isomorphic elliptic curves which have Serre $(2, p)$-entanglement:

Theorem 3.20. [11, Example 3.10]
Let p be an odd prime and let $\epsilon = (-1)^{\frac{p-1}{2}}$. For $t \in \mathbb{Q}^*$ we take the elliptic curve

$$E_{t,p} : y^2 + \epsilon ptxy = x^3 - 36(\epsilon p)^3 t^2 x - (\epsilon p)^5 t^4.$$

We get that $E_{t,p}$ has Serre $(2, p)$-entanglement. Furthermore we have that every elliptic curve $E/\mathbb{Q}$ with Serre $(2, p)$-entanglement is isomorphic over $\bar{\mathbb{Q}}$ to $E_{t,p}$ for some $t \in \mathbb{Q}^*$.

Proof: Using Sage we find that $j_{E_{t,p}} = \epsilon pt^2 + 1728$. This implies that $\Delta_{E_{t,p}} \equiv \epsilon p \pmod{(\mathbb{Q}^*)^2}$ and so $\mathbb{Q}(\sqrt{\epsilon p}) \subseteq \mathbb{Q}(E_{t,p}[2])$. As also $\mathbb{Q}(\sqrt{\epsilon p}) \subseteq \mathbb{Q}(\zeta_p)$ by Theorem 2.18 we get that

$$\mathbb{Q}(\sqrt{\epsilon p}) \subseteq \mathbb{Q}(E_{t,p}[2]) \cap \mathbb{Q}(\zeta_p)$$

and therefore $E_{t,p}$ has Serre $(2, p)$-entanglement.

Now if we have another elliptic curve $E/\mathbb{Q}$ with Serre $(2, p)$-entanglement, then this must be given by the quadratic subfield $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(\zeta_p)$. By Theorem 2.18 this can only be $\mathbb{Q}(\sqrt{\epsilon p})$ and therefore $\Delta_E \equiv \epsilon p$ (mod $(\mathbb{Q}^*)^2$.) This then implies by Lemma 3.18 that $j(E) = \epsilon pt^2 + 1728$ for some $t \in \mathbb{Q}^*$ and so E is isomorphic over $\bar{\mathbb{Q}}$ to $E_{t,p}$ as they have the same j-invariant.

□

Instead of only looking at primes, I improved on this by for integers $m > 2$. We can say the following:

Proposition 3.21. *Let $m > 2$ be an integer. Then there exist infinitely many non-isomorphic elliptic curves which have Serre $(2, m)$-entanglement.*

Proof: Let $\bar{m}$ be the squarefree part of m. Then it is enough to show there are infinitely many non-isomorphic elliptic curves which have Serre $(2, \bar{m})$-entanglement as $\mathbb{Q}(\zeta_{\bar{m}}) \subseteq \mathbb{Q}(\zeta_m)$ and so these elliptic curves also have Serre $(2, m)$-entanglement. First of all let $\bar{m}$ be odd. If $\bar{m} \equiv 1 \pmod 4$ we get that

$$E_{t,\bar{m}} : y^2 + \bar{m}txy = x^3 - 36\bar{m}^3t^2x - \bar{m}^5t^4$$

for $t \in \mathbb{Q}^*$ is an elliptic curve with $j_{E_{t,\bar{m}}} = \bar{m}t^2 + 1728$ (computed using Sage). We have that $\Delta_{Et,\bar{m}} \equiv \bar{m} \pmod{(\mathbb{Q}^*)^2}$ and therefore $\mathbb{Q}(\sqrt{\bar{m}}) \subseteq \mathbb{Q}(E_{t,\bar{m}}[2])$. By Corollary 2.19 we get that $\mathbb{Q}(\sqrt{\bar{m}}) \subseteq \mathbb{Q}(\zeta_{\bar{m}})$ as well and therefore $E_{t,\bar{m}}$ has Serre $(2, \bar{m})$-entanglement. If on the other hand $\bar{m} \equiv 3 \pmod 4$, then

$$E_{t,-\bar{m}} : y^2 - \bar{m}txy = x^3 + 36\bar{m}^3t^2x + \bar{m}^5t^4$$

for $t \in \mathbb{Q}^*$ is an elliptic curve with $j_{E_{t,-\bar{m}}} = -\bar{m}t^2+1728$ and so $\Delta_{Et,-\bar{m}} \equiv -\bar{m} \pmod{(\mathbb{Q}^*)^2}$. So $\mathbb{Q}(\sqrt{-\bar{m}}) \subseteq \mathbb{Q}(E_{t,\bar{m}}[2])$ and again by Corollary 2.19 we get that $\mathbb{Q}(\sqrt{-\bar{m}}) \subseteq \mathbb{Q}(\zeta_{\bar{m}})$. Therefore $E_{t,-\bar{m}}$ has Serre $(2, \bar{m})$-entanglement.

Now let $\bar{m}$ be even. As $\bar{m}$ is squarefree and bigger than 2 we get that $\frac{\bar{m}}{2}$ is odd and bigger than 1. Depending on whether $\frac{\bar{m}}{2} \equiv 1, 3 \pmod 4$ we then get that $E_{t,\frac{\bar{m}}{2}}$ or $E_{t,\frac{-\bar{m}}{2}}$ has Serre $(2, \frac{\bar{m}}{2})$-entanglement. As $\mathbb{Q}(\zeta_{\frac{\bar{m}}{2}}) \subseteq \mathbb{Q}(\zeta_{\bar{m}})$ this also leads to Serre $(2, \bar{m})$-entanglement.

□

We also list for every elliptic curve $E/\mathbb{Q}$ with Serre $(2, m)$-entanglement for $m > 2$ another elliptic curve such that E is isomorphic to that curve over $\bar{\mathbb{Q}}$.

Proposition 3.22. *Let $m > 2$ and let $E/\mathbb{Q}$ be an elliptic curve with Serre $(2, m)$-entanglement. Then for some squarefree $d \mid m$ we have that $\Delta_E \equiv d \pmod{(\mathbb{Q}^*)^2}$ and that E is isomorphic over $\bar{\mathbb{Q}}$ to $E_{t,d} : y^2 + dtxy = x^3 - 36d^3t^2x - d^5t^4$ for some $t \in \mathbb{Q}^*$.*

Proof: If E has Serre $(2, m)$-entanglement this must mean that $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(\zeta_m)$. We will therefore establish the different quadratic subfields of $\mathbb{Q}(\zeta_m)$. We write $m = 2^k \cdot p_2^{e_2} \cdot \ldots \cdot p_n^{e_n}$ with p_i prime, $k \geq 0$ and $e_i \geq 1$ for $2 \leq i \leq n$. We have that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^* \cong (\mathbb{Z}/2^{e_1}\mathbb{Z})^* \times (\mathbb{Z}/p_2^{e_2}\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p_n^{e_n}\mathbb{Z})^*$$

by the Chinese remainder theorem.

We have for $p_i \neq 2$ that $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$ is cyclic [7, Theorem 4], and as it is of even order it has a unique subgroup of order 2 which by the Galois correspondence is linked to the quadratic subfield

$$\mathbb{Q}(\sqrt{\epsilon p}) \subseteq \mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_{p^{e_i}})$$

where $\epsilon = (-1)^{\frac{p-1}{2}}$.

For $p = 2$ we have that $(\mathbb{Z}/2^k\mathbb{Z})^*$ is cyclic if $k = 1, 2$ and is the product of two cyclic groups if $k \geq 3$ [7, Theorem 5]. If $k = 1$ then $(\mathbb{Z}/2^k\mathbb{Z})^*$ is trivial and so has no subgroup of order 2. If $k = 2$ then $(\mathbb{Z}/2^k\mathbb{Z})^*$ has order 2 and therefore has a unique subgroup of order 2 corresponding to the quadratic subfield

$$\mathbb{Q}(\sqrt{-1}) \subseteq \mathbb{Q}(\zeta_4).$$

Finally if $k \geq 3$ then $(\mathbb{Z}/2^k\mathbb{Z})^*$ is the product of two cyclic groups and so it has three subgroups of order 2, corresponding to

$$\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}) \subseteq \mathbb{Q}(\zeta_8) \subseteq \mathbb{Q}(\zeta_{2^k}).$$

We see that that $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*$ has one subgroup of order 2 for $2 \leq i \leq n$ and that $(\mathbb{Z}/2^k\mathbb{Z})^*$ has zero subgroups if $k = 1$, one if $k = 2$ and two if $k \geq 3$. So we get that the amount of subgroups of $(\mathbb{Z}/m\mathbb{Z})^*$ of order 2 is given by $\begin{cases} 2^{n-1} - 1 & \text{if} \quad k = 1 \\ 2^n - 1 & \text{if} \quad k = 2 \\ 2^{n+1} - 1 & \text{if} \quad k \geq 3. \end{cases}$

These subgroups correspond to the quadratic subfields

$$\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_{|d|}) \subseteq \mathbb{Q}(\zeta_m)$$

with $d \mid 2p_2 \cdot ... \cdot p_n$ (note that d can be negative). We conclude that $\mathbb{Q}(\sqrt{\Delta_E}) = \mathbb{Q}(\sqrt{d})$ for some $d \mid 2^k p_2 \cdot ... \cdot p_n$ and so $\Delta_E \equiv d \pmod{(\mathbb{Q}^*)^2}$. By Lemma 3.18 we get that $j(E) = dt^2 + 1728$ for some $t \in \mathbb{Q}^*$. It is then isomorphic over $\bar{\mathbb{Q}}$ to

$$E_{t,d} : y^2 + dtxy = x^3 - 36d^3t^2x - d^5t^4$$

as $j(E_{t,d}) = dt^2 + 1728$ as well (Computed by Sage).

□

3.5 Serre curves

Definition 3.23. If we take an elliptic curve $E/\mathbb{Q}$, then we have shown in Proposition 3.16 that for the index i_E of the full representation ρ_E we have that $i_E \geq 2$. If for an elliptic curve $E/\mathbb{Q}$ we have that i_E is precisely 2, then we call E a **Serre curve**.

There has been a lot of research about these kinds of elliptic curves ([5],[8],[20]). First of all it was also shown in [5] by Brau and Jones using modular curves that for an elliptic curve $E/\mathbb{Q}$ being a Serre curve is equivalent to having no exceptional primes (meaning $\rho_{E,\ell}$ is surjective for all ℓ prime), $\rho_{E,8}$ and $\rho_{E,9}$ being surjective, and $\mathbb{Q}(E[2]) \not\subseteq \mathbb{Q}(E[3])$. This implies that if an elliptic curve has no vertical entanglement but is not a Serre curve, we must have that $\mathbb{Q}(E[2]) \not\subseteq \mathbb{Q}(E[3])$. The authors also showed a necessary property of the j-invariant of elliptic curves for which $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$, which are therefore non-Serre curves. It was shown later on in [20] by Jones that almost all elliptic curves over $\mathbb{Q}$ are Serre curves. Daniels in [8] also gave an infinite family of Serre curves dependent on a parameter t.

3.6 CM entanglement

We will mainly focus on entanglements on elliptic curves without CM, but we note the following important result about elliptic curves with CM:

Lemma 3.24. [4, Lemma 3.15]
Let $E/\mathbb{Q}$ be an elliptic curve with CM given by an order $\mathcal{O}_K$ of an imaginary quadratic field K. Then $K \subseteq \mathbb{Q}(E[n])$ for all $n \geq 3$.

This lemma implies that for all $a, b \geq 3$ we have horizontal (a,b)-entanglement induced by $K \subseteq \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b])$. This shows that the image of the full representation ρ_E is very small for an elliptic curve $E/\mathbb{Q}$ with CM.

3.7 Horizontal entanglement in terms of group theory

In the final part of this chapter we will introduce another definition of horizontal entanglement. In [9] the first and last author of [11], Daniels and Morrow, have found a method to describe horizontal entanglement in group theoretic terms. This is done as follows: Let $E/\mathbb{Q}$ be an elliptic curve, n be an integer and $a < b$ divisors of n, and let $d = \gcd(a,b)$ and $c = \operatorname{lcm}(a,b)$. Then we have

$$G_n := \rho_{E,n}(G_{\mathbb{Q}}) \subseteq \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z}).$$

Recall that $G_n \cong \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$. There is the reduction map $\pi_c : \mathrm{GL}(2,\mathbb{Z}/n\mathbb{Z}) \to \mathrm{GL}(2,\mathbb{Z}/c\mathbb{Z})$, which just sends every coordinate in $\mathbb{Z}/n\mathbb{Z}$ to its image in $\mathbb{Z}/c\mathbb{Z}$, and we set $G_c := \pi_c(G_n)$. Note that if a, b are coprime, then $n = c$ and $G_n = G_c$. For $e \in \{a, b, d\}$ we also have reduction maps $\pi_e : \mathrm{GL}(2,\mathbb{Z}/c\mathbb{Z}) \to \mathrm{GL}(2,\mathbb{Z}/e\mathbb{Z})$. We take $N_e := \ker(\pi_e) \cap \pi_c(G)$ and we define the following:

Definition 3.25. [9, Definition 3.1]
We say that the group G_n has (a,b)-**entanglement** if we have

$$\langle N_a, N_b \rangle \subsetneq N_d.$$

By properties of Galois theory we have that G_n has (a, b)-entanglement if and only if E has horizontal (a, b)-entanglement. To see this we note that first of all $G_c := \pi_c(G_n) \cong \mathrm{Gal}(\mathbb{Q}(E[c])/\mathbb{Q})$ as $\pi_m \circ \rho_{E,n} = \rho_{E,m}$ for all $m \mid n$. Then for $e \in \{a, b, d\}$ we also get $\pi_e(G_c) \cong \mathrm{Gal}(\mathbb{Q}(E[e])/\mathbb{Q})$. Now by Theorem 2.12 we have that

$$\mathrm{Gal}(\mathbb{Q}(E[e])/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(E[c])/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(E[c])/\mathbb{Q}(E[e]))$$

as $\mathbb{Q}(E[e])/\mathbb{Q}$ is a Galois extension and so $\mathrm{Gal}(\mathbb{Q}(E[c])/\mathbb{Q}(E[e]))$ is normal. On the other hand we have that

$$G_c/(\ker(\pi_e) \cap G_c) \cong \pi_e(G_c)$$

by the first isomorphism theorem for groups. As $N_e = \ker(\pi_e) \cap G_c$ and as $\mathrm{Gal}(\mathbb{Q}(E[e])/\mathbb{Q}) \cong \pi_e(G_c)$ and $\mathrm{Gal}(\mathbb{Q}(E[c])/\mathbb{Q}) \cong G_c$ we get that $N_e \cong \mathrm{Gal}(\mathbb{Q}(E[c])/\mathbb{Q}(E[e]))$. This implies by the Galois correspondence that N_e is the subgroup of G_c corresponding to the subfield $\mathbb{Q}(E[e])$ of $\mathbb{Q}(E[c])$. We also know from Lemma 2.16 that the subgroup corresponding to $\mathbb{Q}(E[a] \cap \mathbb{Q}(E[b])$ must then be $\langle N_a, N_b \rangle$ and we get that

$$\langle N_a, N_b \rangle \subsetneq N_d$$

if and only if

$$\mathbb{Q}(E[d]) \subsetneq \mathbb{Q}(E[a] \cap \mathbb{Q}(E[b]).$$

We summarize this Galois correspondence in the following picture:

$$\begin{tikzcd}
 & \mathbb{Q}(E[c]) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(E[a]) \arrow[dr, dash] & & \mathbb{Q}(E[b]) \arrow[dl, dash] \\
 & \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]) \arrow[d, dash] & \\
 & \mathbb{Q}(E[d]) \arrow[d, dash] & \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \{e\} \arrow[dl, dash] \arrow[dr, dash] & \\
N_a \arrow[dr, dash] & & N_b \arrow[dl, dash] \\
 & \langle N_a, N_b \rangle \arrow[d, dash] & \\
 & N_d \arrow[d, dash] & \\
 & G_c &
\end{tikzcd}$$

Note that using this group theoretic definition of horizontal entanglement we can prove [9, Lemma 3.4], which implies that (a, b)-entanglement for integers a, b can lead to entanglement of smaller integers dividing a, b:

Lemma 3.26. [9, Lemma 3.4]
Let $n \geq 1$, let $a < b < f$ be divisors of n, and let $d = \gcd(a, b)$. If $\gcd(a, f) = \gcd(b, f) = 1$ and G_n has $(f \cdot a, f \cdot b)$-entanglement then G_n has (a, b)-entanglement as well.

Proof: Suppose G_n does not have (a, b)-entanglement. Then $\langle N_a, N_b \rangle = N_d$ which implies that for all 2 by 2-matrices $X = (x_{ij})_{1 \leq i,j \leq 2} \in G_c$ with $c = \operatorname{lcm}(a, b)$ we have that $d \mid x_{ij}$ for all x_{ij} if and only if $a \mid x_{ij}$ for all x_{ij} or $b \mid x_{ij}$ for all x_{ij}. We claim that for $Y \in G_{f \cdot c}$ (note that $f \cdot c = \operatorname{lcm}(f \cdot a, f \cdot b)$) we have that $f \cdot d \mid y_{ij}$ if and only if $f \cdot a \mid y_{ij}$ for all y_{ij} coordinates of Y or $f \cdot b \mid x_{ij}$ for all y_{ij} coordinates of Y. This implies that

$$\langle N_{f \cdot a}, N_{f \cdot b} \rangle = N_{f \cdot d}$$

which means that G_n does not have $(f \cdot a, f \cdot b)$-entanglement, but this contradicts our assumption.

Now we prove our claim: If $f \cdot a \mid y_{ij}$ for all y_{ij} or $f \cdot b \mid y_{ij}$ for all y_{ij}, then also $f \cdot d \mid y_{ij}$ for all y_{ij} as $d \mid a, b$. If conversely $f \cdot d \mid y_{ij}$ for all x_{ij}, then we can look at the image of Y under the map

$$\pi : \mathrm{GL}(2, \mathbb{Z}/f \cdot c\mathbb{Z}) \to \mathrm{GL}(2, \mathbb{Z}/c\mathbb{Z}).$$

If we write $\overline{Y} := \pi(Y)$ with coordinates $\overline{y_{ij}}$, then for all y_{ij} we have that

$$y_{ij} = \overline{y_{ij}} + k_{ij} \cdot c.$$

As $f \cdot d \mid y_{ij}$ for all y_{ij}, we get that

$$d \mid f \cdot d \mid y_{ij}$$

for all y_{ij}. Also $d \mid c$ and so

$$d \mid \overline{y_{ij}} = y_{ij} - k_{ij} \cdot c$$

for $1 \leq i \leq 2$. Therefore either a divides all $\overline{y_{ij}}$ or b divides all $\overline{y_{ij}}$. Assume that $a \mid \overline{y_{ij}}$ for all $\overline{y_{ij}}$, then $a \mid y_{ij}$ for all y_{ij} as $y_{ij} = \overline{y_{ij}} + k_{ij} \cdot c$ and $a \mid c$. As also $\gcd(a, f) = 1$ and $f \mid y_{ij}$ for all y_{ij} we must have that $f \cdot a \mid y_{ij}$ for all y_{ij}. This works similarly in the case that $b \mid y_{ij}$ and therefore $f \cdot d \mid y_{ij}$ for all y_{ij} if and only if $f \cdot a \mid y_{ij}$ for all y_{ij} or $f \cdot b \mid y_{ij}$ for all y_{ij}. So we have proven our claim and the contradiction follows. We therefore conclude that G_n has (a, b)-entanglement as well.

□

Daniels and Morrow also define the following type of group theoretic entanglement:

Definition 3.27. [9, Definition 3.7]
The group G_n has **explained** (a, b)**-entanglement** if G_n has (a, b)-entanglement and

$$[(\mathbb{Z}/c\mathbb{Z})^* : \det(\langle N_a, N_b \rangle)] = [\pi_c(G_n) : \langle N_a, N_b \rangle].$$

They then claim that G_n having explained (a, b)-entanglement means that the entanglement is entirely explained by E having Weil (a, b)-entanglement. Note that by Lemma 2.35 $\det(\langle N_a, N_b \rangle)$ is the c-th cyclotomic character.

4 Modular curves

This section we will give an introduction to the theory of modular curves, which are complex algebraic curves with points corresponding to isomorphism classes of elliptic curves with specific level structure. This will be useful in listing elliptic curves with specific images of their corresponding Galois representations. These modular curves are given by quotients of the complex upper half plane by subgroups of the quotient group $\mathrm{SL}(2,\mathbb{Z})/\{-I\}$, which are called congruence subgroups. We will start this section by recalling the connection between elliptic curves over $\mathbb{C}$ and complex lattices.

4.1 Elliptic curves over $\mathbb{C}$ and complex lattices

Definition 4.1. A complex **lattice** $\Lambda \subset \mathbb{C}$ is given by a discrete subgroup of the complex plane. If we have such a lattice Λ then $\{\omega_1, \omega_2\}$ is a basis for Λ if for all $x \in \Lambda$ we have that $x = \alpha\omega_1 + \beta\omega_2$ for some $\alpha, \beta \in \mathbb{Z}$. We call Λ_1, Λ_2 **homothetic** if $\Lambda_1 = \alpha\Lambda_2$ for some $\alpha \in \mathbb{C}^*$.

The quotient $\mathbb{C}/\Lambda$ for some lattice Λ is a complex Riemann surface of genus one with the structure of an abelian group, so in particular it is a complex Lie group. This is called a complex torus. Every complex torus is of the form $\mathbb{C}/\Lambda$ and is isomorphic as a complex Lie group to an elliptic curve E_Λ over $\mathbb{C}$ [35, Proposition VI.3.6]. The Uniformization Theorem [35. Theorem VI.5.1] also states that every elliptic curve over $\mathbb{C}$ is isomorphic (as a complex Lie group) to $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$. As by [35. Corollary VI.4.1] we get that $E_{\Lambda_1} \cong E_{\Lambda_2}$ if and only if Λ_1 and Λ_2 are homothetic, we get a bijection between isomorphism classes of elliptic curves over $\mathbb{C}$ and homothety classes of complex lattices:

$$\frac{\text{Complex lattices}}{\mathbb{C}^*} \cong \frac{\text{Elliptic curves over } \mathbb{C}}{\text{isomorphic over } \mathbb{C}}.$$

For the following subsection we refer to [34, Chapter 1, §1,2]. We will show that the complex upper half plane is closely related to the set of complex lattices which we shall denote by $\mathcal{L}$. To see this we note that if we have a complex lattice $\Lambda \in \mathcal{L}$ with basis $\{\omega_1, \omega_2\}$, then we can always swap ω_1 and ω_2 such that the angle from ω_2 to ω_1 is always positive, or in other words that $\mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0$. This implies that Λ is homothetic to another complex lattice Λ' with basis $\{\frac{\omega_1}{\omega_2}, 1\}$ for which $\mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0$. As $\frac{\omega_1}{\omega_2}$ then lies in the complex upper half plane $\mathbb{H} \subset \mathbb{C}$ this precisely means that the map $\mathbb{H} \to \mathcal{L}/\mathbb{C}^*$ given by sending $\tau \in \mathbb{H}$ to the lattice $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$ is surjective. To make this map injective as well we need to see for which $\tau_1, \tau_2 \in \mathbb{H}$ we get that Λ_{τ_1} is homothetic to Λ_{τ_2}. For this we have the following lemma:

Lemma 4.2. 34, Lemma 1.2]
Let $\tau_1, \tau_2 \in \mathbb{H}$. Then we have that Λ_{τ_1} is homothetic to Λ_{τ_2} if and only if

$$\tau_1 = \frac{a\tau_2 + b}{c\tau_2 + d}$$

for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$. *Recall that* $\mathrm{SL}(n, \mathbb{Z}) \subseteq \mathrm{GL}(n, \mathbb{Z})$ *is the subgroup of matrices with determinant equal to 1.*

Proof: First assume Λ_{τ_1} is homothetic to Λ_{τ_2}. We get that $\mathbb{Z}\tau_1 + \mathbb{Z} = \mathbb{Z}\alpha\tau_2 + \mathbb{Z}\alpha$ for some $\alpha \in \mathbb{C}^*$. Therefore there are integers $a, b, c, d, a', b', c', d' \in \mathbb{Z}$ such that

$$\begin{aligned} \tau_1 &= a\alpha\tau_2 + b\alpha, \quad & \alpha\tau_2 &= a'\tau_1 + b' \\ 1 &= c\alpha\tau_2 + d\alpha, \quad & \alpha &= c'\tau_1 + d'. \end{aligned}$$

Substituting the left expressions into the right ones gives us

$$\alpha\tau_2 = a'(a\alpha\tau_2 + b\alpha) + b'(c\alpha\tau_2 + d\alpha).$$

As we have that τ_1 and τ_2 are linearly independent from 1, we must have that $a'a + b'c = 1$ and that $a'b + b'd = 0$. Similarly we get that $c'a + d'd = 1$ and that $c'b + d'c = 0$. This implies that

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

One can similarly show that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Note that

$$\tau_1 = \frac{\tau_1}{1} = \frac{a\alpha\tau_2 + b\alpha}{c\alpha\tau_2 + d\alpha} = \frac{a\tau_2 + b}{c\tau_2 + d}.$$

We also have, as stated in [34, Lemma 1.1], if we write $\tau_2 = e + fi$ with $e, f \in \mathbb{R}$, that

$$\begin{aligned} &\frac{a\tau_2 + b}{c\tau_2 + d} = \frac{(c\bar{\tau_2} + d)}{(c\bar{\tau_2} + d)} \frac{(a\tau_2 + b)}{(c\tau_2 + d)} = \\ &\frac{(ce - cfi + d)(ae + afi + b)}{\overline{(c\tau_2 + d)}(c\tau_2 + d)} = \\ &\frac{ac(e^2 + f^2) + (ad + bc)e + bd + (ad - bc)fi}{|c\tau_2 + d|^2}. \end{aligned}$$

This implies that

$$\mathrm{Im}(\frac{a\tau_2+b}{c\tau_2+d}) = \frac{(ad-bc)f}{|c\tau_2+d|^2}$$

and because $\mathrm{Im}(\frac{a\tau_2+b}{c\tau_2+d}) = \mathrm{Im}(\tau_1) > 0$ and $f = \mathrm{Im}(\tau_2) > 0$ we must have that $ad - bc > 0$. But this means that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$.

Conversely assume $\tau_1 = \frac{a\tau_2+b}{c\tau_2+d}$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$. Then we have that $\mathbb{Z}(a\tau_2 + b) + \mathbb{Z}(c\tau_2+d) = \mathbb{Z}\tau_2 + \mathbb{Z}$ as the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible and so $\{a\tau_2+b, c\tau_2+d\}$ and $\{\tau_2, 1\}$ both form a basis for the same lattice. Note that

$$\mathbb{Z}(a\tau_2+b) + \mathbb{Z}(c\tau_2+d) = \mathbb{Z}(c\tau_2+d)\tau_1 + \mathbb{Z}(c\tau_2+d) = (c\tau_2+d)\Lambda_{\tau_1}.$$

This implies that

$$(c\tau_2+d)\Lambda_{\tau_1} = \mathbb{Z}(a\tau_2+b) + \mathbb{Z}(c\tau_2+d) = \mathbb{Z}\tau_2 + \mathbb{Z} = \Lambda_{\tau_2}.$$

As c, d cannot both be equal to 0 and τ_2 and 1 are linearly independent we must have that $c\tau_2 + d \in \mathbb{C}^*$ and therefore that Λ_{τ_1} is homothetic to Λ_{τ_2}. This concludes the proof.

□

If we define the action of $\mathrm{SL}(2,\mathbb{Z})$ on $\mathbb{H}$ by sending τ to $\frac{a\tau_2+b}{c\tau_2+d}$ then the previous lemma implies that we have a bijection

$$\mathbb{H}/\mathrm{SL}(2,\mathbb{Z}) \to \mathcal{L}/\mathbb{C}^*$$

given by sending τ to $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$. Note that the matrix $-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ acts trivially on $\mathbb{H}$. We denote the quotient group $\mathrm{SL}(2,\mathbb{Z})/\{-I\}$ by $\Gamma(1)$ (this notation will become clear later) and get that

$$\mathbb{H}/\Gamma(1) \cong \mathcal{L}/\mathbb{C}^*.$$

We stated at the beginning of Subsection 4.1 that we also have a bijection between $\mathcal{L}/\mathbb{C}^*$ and elliptic curves over $\mathbb{C}$ up to isomorphism. Therefore we get that points $\tau \in \mathbb{H}/\Gamma(1)$ are in one-to-one connection with isomorphism classes of elliptic curves over $\mathbb{C}$.

Definition 4.3. We let $Y(1) := \mathbb{H}/\Gamma(1)$ be the **modular curve corresponding to the group $\mathbf{\Gamma(1)}$**. We have by [34, Section 1.2] that $Y(1)$ can be turned into a topological space, which looks like a sphere with a point missing. We can extend this sphere into a compact Riemann surface [34, Theorem 2.5] by instead of $\mathbb{H}$ taking the space $\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ and taking $X(1) := \mathbb{H}^*/\Gamma(1)$ (this is possible as $\Gamma(1)$ also acts on $\mathbb{P}^1(\mathbb{Q})$ by sending $(x, y) \in \mathbb{P}^1(\mathbb{Q})$ to $(ax + b, cy + d)$). We call $X(1)$ a **compactified modular curve**. We call the point in $X(1) \setminus Y(1)$ the **cusp** of $X(1)$.

Because $X(1)$ is a compact Riemann surface of dimension 1 it is equivalent to a projective algebraic curve, which is the reason it is called a modular curve. We have that $X(1)$ is isomorphic to the Riemann sphere $\mathbb{P}^1(\mathbb{C})$ as its genus is zero [34, Theorem 2.5].

4.2 Congruence subgroups Γ

We have that non-cuspidal points of $X(1)$, or in other words points of $Y(1)$, correspond to isomorphism classes of elliptic curves over $\mathbb{C}$. But we can also look at modular curves which parametrize elliptic curves over $\mathbb{C}$ with more structure. In order to define these we will need more theory on groups similar to $\Gamma(1)$. For this we shall closely follow [13]. We first define the following subgroups of $\Gamma(1)$:

Definition 4.4. We define for $N \in \mathbb{N}$ the subgroup

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid a, d \equiv 1 \pmod{N},\ b, c \equiv 0 \pmod{N} \right\}$$

as the **principal congruence subgroup of level N**.

Note that this subgroup fits in the following exact sequence:

$$0 \to \Gamma(N) \to \Gamma(1) \to \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\} \to 0$$

where the first non-trivial map is the inclusion map and the second non-trivial map is the map sending each coordinate of a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) = \mathrm{SL}(2, \mathbb{Z})/\{-I\}$ to its corresponding residue class in $\mathbb{Z}/N\mathbb{Z}$. The first isomorphism theorem of groups then gives us that

$$\Gamma(1)/\Gamma(N) \cong \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\}.$$

We also have the following class of subgroups of $\Gamma(1)$:

Definition 4.5. We call a subgroup $\Gamma \subseteq \Gamma(1)$ a **congruence subgroup** if $\Gamma(N) \subseteq \Gamma$ for some $N \in \mathbb{Z}$.

Example 4.6. The two most important examples of congruence subgroups are

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid c \equiv 0 \pmod{N} \right\}$$

and

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid a, d \equiv 1 \pmod{N},\ c \equiv 0 \pmod{N} \right\}.$$

Note that we have the following chain of inclusions of subgroups:

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \Gamma(1).$$

These congruence subgroups also act on the complex upper half plane $\mathbb{H}$ in the same way as $\Gamma(1)$ acts on $\mathbb{H}$. If we quotient $\mathbb{H}$ with these subgroups, we then end up with different modular curves.

Definition 4.7. We define

$$Y(N) := \mathbb{H}/\Gamma(N)$$

as the **modular curve corresponding to the group $\boldsymbol{\Gamma(N)}$** and $X(N) := \mathbb{H}^*/\Gamma(N)$ as its compactified modular curve.
We similarly define

$$Y_0(N) := \mathbb{H}/\Gamma_0(N)$$

as the **modular curve corresponding to the group $\boldsymbol{\Gamma_0(N)}$** and

$$Y_1(N) := \mathbb{H}/\Gamma_1(N)$$

as the **modular curve corresponding to the group $\boldsymbol{\Gamma_1(N)}$**. Their corresponding compactified modular curves we have as $X_0(N) := \mathbb{H}^*/\Gamma_0(N)$ and $X_1(N) := \mathbb{H}^*/\Gamma_1(N)$.

Like $X(1)$ and $Y(1)$ these modular curves are topological spaces and their compactified forms are compact Riemann surfaces which are therefore equivalent to complex projective curves [13, Chapter 2]. We will show in Subsection 4.4 that the modular curves $X(N)$ can be defined over the cyclotomic field $\mathbb{Q}(\zeta_n)$ and furthermore that $X_0(N)$ and $X_1(N)$ can be defined over $\mathbb{Q}$.

4.3 Elliptic curves with level structure

We have seen that the modular curve $Y(1)$ parametrizes elliptic curves over $\mathbb{C}$. We have that $Y(N), Y_0(N), Y_1(N)$ also parametrize elliptic curves but with more structure. What we mean by this we shall define in more detail. We first recall the fact that for elliptic curves $E/\mathbb{C}$ we have for $N \in \mathbb{N}$ that

$$E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

If we take a complex lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ then for E_Λ we have that its N-torsion points correspond to the points in

$$(\mathbb{Z}\frac{\omega_1}{N} + \mathbb{Z}\frac{\omega_2}{N})/\Lambda \subset \mathbb{C}/\Lambda$$

(see [35, VI,5,4]). The isomorphism between $E[N]$ and $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ is dependent on a choice of basis. We therefore have the following definition:

Definition 4.8. Let $E/\mathbb{C}$ be an elliptic curve. We call an isomorphism $\alpha : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \to E[N]$ a **level $\boldsymbol{N}$ structure**.

Recall that for $E/\mathbb{C}$ we have the Weil pairing $e_N : E[N] \times E[N] \to \boldsymbol{\mu}_N \subset \mathbb{C}^*$ sending two N-torsion points to a complex N-th root of unity $e^{\frac{2\pi k i}{N}}$ with $k \in \mathbb{Z}$. This brings us to the next definition:

Definition 4.9. Let $E/\mathbb{C}$ be an elliptic curve and let $\alpha : \mathbb{Z}/NZ \times \mathbb{Z}/N\mathbb{Z} \to E[N]$ be a level N structure. We say that α is a **canonical level $\boldsymbol{N}$ structure** if

$$e_N(\alpha(1,0), \alpha(0,1)) = e^{\frac{2\pi i}{N}}.$$

Note that an elliptic curve $E/\mathbb{C}$ with a canonical level N structure is equivalent to a tuple (E, P, Q) with $\{P, Q\}$ the N-torsion points forming an $E[N]$ basis given respectively by the images of $\alpha(1,0)$ and $\alpha(0,1)$ such that $e_N(P,Q) = e^{\frac{2\pi i}{N}}$.

Before we prove our main theorem of this subsection, Theorem 4.10, we look at the following three sets: We first have the set

$$S(N)_1 := \{(E, P) \mid E/\mathbb{C} \text{ an elliptic curve and } P \text{ a point of } E \text{ of order } N\}$$

where $(E, P) \cong (E', P')$ if there exists an isomorphism $E \cong E'$ sending P to P'. We also have the set

$$S(N)_0 := \{(E, G) \mid E/\mathbb{C} \text{ an elliptic curve and } G \text{ a cyclic subgroup of } E(\mathbb{C}) \text{ of order } N\}$$

where $(E, G) \cong (E', G')$ if there exists an isomorphism $E \cong E'$ sending G to G'. Finally we have the set

$$S(N) := \{(E, P, Q) \mid E/\mathbb{C} \text{ an elliptic curve and } \{P, Q\} \text{ defining a canonical level } N \text{ structure}\}$$

where $(E, P, Q) \cong (E', P', Q')$ if there exists an isomorphism $E \cong E'$ sending P to P' and Q to Q'. This leads to the following theorem linking these sets to points on the modular curves $Y_0(N), Y_1(N), Y(N)$:

Theorem 4.10. [13, Theorem 1.5.1]
We have a bijection between the following sets:

1. $Y_1(N) \cong S(N)_1/\sim$
2. $Y_0(N) \cong S(N)_0/\sim$
3. $Y(N) \cong S(N)/\sim$.

Proof: For this proof we refer to the proof of [13, Theorem 1.5.1]. We start by proving 1. First of all we take the map

$$\phi : \mathbb{H} \to S(N)_1/\sim$$

defined by sending $\tau \in \mathbb{H}$ to the isomorphism class of $(E_{\Lambda_\tau}, \frac{1}{N})$ with $\frac{1}{N}$ the point of E_{Λ_τ} of order N corresponding to $\frac{1}{N} \in C/\Lambda_\tau$. We will first show that this map is surjective and then that $\phi(\tau_1) = \phi(\tau_2)$ if and only if $\tau_1 = \frac{a\tau_2+b}{c\tau_2+d}$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$.

Let E be an elliptic curve over $\mathbb{C}$ and let P be a point of E of order N. Then there exists a $\tau \in \mathbb{H}$ such that $E \cong E_{\Lambda_\tau}$ by what we have have seen in Subsection 4.1. We have that the basis of $E_{\Lambda_\tau}[N]$ is given by the points corresponding to $\frac{\tau}{N}, \frac{1}{N} \in \mathbb{C}/\Lambda_\tau$. This implies that P corresponds to a point $\frac{k\tau}{N} + \frac{l}{N} \in \mathbb{C}/\Lambda_\tau$ with $k, l \in \mathbb{Z}$. Because the order of P is exactly N we get that $\gcd(k, l, N) = 1$ and therefore there exist $a, b, c \in \mathbb{Z}$ such that $al - bk - cN = 1$. But now we can take the residue class of the matrix $\begin{pmatrix} a & b \\ k & l \end{pmatrix} \in \mathrm{Mat}(2, \mathbb{Z})$ and get a matrix in $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$. Because the reduction map $\mathrm{SL}(2, \mathbb{Z}) \to \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ is surjective we can lift this into a matrix $\begin{pmatrix} a' & b' \\ k' & l' \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$. Note that the point $\frac{k'\tau}{N} + \frac{l'}{N} \in \mathbb{C}/\Lambda_\tau$ still corresponds to P as k', l' are equivalent to respectively k, l modulo N. we take $\tau' := \frac{a'\tau+b'}{k'\tau+l'}$. Then similarly to the proof of Lemma 4.2 we get that $k'\tau + l'\Lambda_{\tau'} = \Lambda_\tau$ and so $\Lambda_{\tau'}$ and Λ_τ are homothetic. This implies that $E \cong E_{\Lambda_\tau} \cong E_{\Lambda_{\tau'}}$. We also have that

$$k'\tau + l'\left(\frac{1}{N}\right) = \frac{k'\tau}{N} + \frac{l'}{N}$$

which is the point corresponding to P. So we get that the isomorphism between $E_{\Lambda_{\tau'}}$ and E sends the point corresponding to $\frac{1}{N} \in \mathbb{C}/\Lambda_{\tau'}$ to P and therefore

$$(E, P) \cong \left(E_{\Lambda_{\tau'}}, \frac{1}{N}\right)$$

and ϕ is surjective.

Now assume for $\tau_1, \tau_2 \in \mathbb{H}$ we have that $\tau_1 = \frac{a\tau_2+b}{c\tau_2+d}$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$. This implies that $a, d \equiv 1 \pmod N$ and that $c \equiv 0 \pmod N$ Then $E_{\Lambda_{\tau_1}} \cong E_{\Lambda_{\tau_2}}$ as $\Gamma_1(N) \subset \Gamma(1)$. We have for $\frac{1}{N} \in \mathbb{C}/\Lambda_{\tau_1}$ that

$$(c\tau_2 + d)\frac{1}{N} = \frac{c\tau_2}{N} + \frac{d}{N} \equiv \frac{0}{N} + \frac{1}{N} \pmod N$$

and so $(c\tau_2 + d)\frac{1}{N}$ is is equivalent to $\frac{1}{N} \in \mathbb{C}/\Lambda_{\tau_2}$ modulo Λ_{τ_2}. This implies that the point of $E_{\Lambda_{\tau_1}}$ corresponding to $\frac{1}{N} \in \mathbb{C}/\Lambda_{\tau_1}$ gets sent to the point of $E_{\Lambda_{\tau_2}}$ corresponding to $\frac{1}{N} \in \mathbb{C}/\Lambda_{\tau_2}$ and so

$$\left(E_{\Lambda_{\tau_1}}, \frac{1}{N}\right) \cong \left(E_{\Lambda_{\tau_2}}, \frac{1}{N}\right).$$

If conversely we have that $(E_{\Lambda_{\tau_1}}, \frac{1}{N}) \cong (E_{\Lambda_{\tau_2}}, \frac{1}{N})$ for some $\tau_1, \tau_2 \in \mathbb{H}$, then we must have that there exists some $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_{\tau_1} = \Lambda_{\tau_2}$ and $\frac{\alpha}{N} \equiv \frac{1}{N} \pmod{\Lambda_{\tau_2}}$. The proof of Lemma 4.2 tells us that $\alpha\tau_1 = a\tau_2 + b$ and that $\alpha = c\tau_2 + d$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$. We can take its residue class in $\Gamma(1)$. We also get that $\frac{c\tau_2+d}{N} \equiv \frac{1}{N} \pmod{\Lambda_{\tau_2}}$ and so $a \equiv 1 \pmod{N}$ and $c \equiv 0 \pmod{N}$. We must have then that $d \equiv 1 \pmod{N}$ as well as $ad - bc \equiv 1 \pmod{N}$ and so we get that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N).$$

This concludes the proof of 1. We will now prove 2. We take the map

$$\phi : \mathbb{H} \to S(N)_0/\sim$$

defined by sending $\tau \in \mathbb{H}$ to the isomorphism class of $(E_{\Lambda_\tau}, \langle\frac{1}{N}\rangle)$ with $\langle\frac{1}{N}\rangle$ the subgroup of $E_{\Lambda_\tau}(\mathbb{C})$ of order N generated by the point corresponding to $\frac{1}{N} \in C/\Lambda_\tau$. This map is surjective by the same reasoning as in the proof of 1. We have for G a subgroup of E that G is generated by a point P of order N. So by the same argument as before we have that $(E, P) \cong (E_{\Lambda_{\tau'}}, \frac{1}{N})$ for some $\tau' \in \mathbb{H}$. But then $(E, G) \cong (E_{\Lambda_{\tau'}}, \langle\frac{1}{N}\rangle)$. Now assume that for $\tau_1, \tau_2 \in \mathbb{H}$ we have that $\tau_1 = \frac{a\tau_2+b}{c\tau_2+d}$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, so $c \equiv 0 \pmod{N}$ and $a, d \in (\mathbb{Z}/N\mathbb{Z})^*$. Then for $\frac{1}{N} \in \mathbb{C}/\Lambda_{\tau_1}$ we have that

$$c\tau_2 + d(\frac{1}{N}) \equiv \frac{d}{N} \pmod{N}.$$

Because d is invertible modulo N we get that $\frac{d}{N}$ generates the same subgroup as $\frac{1}{N}$ and so we get that

$$(E_{\Lambda_{\tau_1}}, \langle\frac{1}{N}\rangle) \cong (E_{\Lambda_{\tau_2}}, \langle\frac{1}{N}\rangle).$$

If conversely we have that $(E_{\Lambda_{\tau_1}}, \langle\frac{1}{N}\rangle) \cong (E_{\Lambda_{\tau_2}}, \langle\frac{1}{N}\rangle)$ for some $\tau_1, \tau_2 \in \mathbb{H}$, then we must have that there exists some $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_{\tau_1} = \Lambda_{\tau_2}$ and $\frac{\alpha}{N} \equiv \frac{k}{N} \pmod{\Lambda_{\tau_2}}$ with $k \in (\mathbb{Z}/N\mathbb{Z})^*$. We get, similarly to before, that $\alpha\tau_1 = a\tau_2 + b$ and that $\alpha = c\tau_2 + d$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$. We again take its residue class in $\Gamma(1)$. We now have that $\frac{c\tau_2+d}{N} \equiv \frac{k}{N} \pmod{\Lambda_{\tau_2}}$ and so $c \equiv 0 \pmod{N}$ and we get that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

Finally we prove 3. We take the map

$$\phi : \mathbb{H} \to S(N)/\sim$$

defined by sending $\tau \in \mathbb{H}$ to the isomorphism class of $(E_{\Lambda_\tau}, \frac{\tau}{N}, \frac{1}{N})$ with $\frac{\tau}{N}, \frac{1}{N}$ the points of E_{Λ_τ} corresponding to $\frac{\tau}{N}, \frac{1}{N} \in \mathbb{C}/\Lambda_\tau$. We have that

$$e_N(\frac{\tau}{N}, \frac{1}{N}) = e^{\frac{2\pi i}{N}}$$

by [17], so this map is well-defined as $(\frac{\tau}{N}, \frac{1}{N})$ defines a canonical level N structure. We now show this map is surjective. Assume we have an elliptic curve $E/\mathbb{C}$ and two points $P, Q \in E[N]$ which define a canonical level N structure. Then $E \cong E_{\Lambda_\tau}$ for some $\tau \in \mathbb{H}$. E_{Λ_τ} has the canonical level N structure given by the points corresponding to $\frac{\tau}{N}, \frac{1}{N} \in \mathbb{C}/\Lambda_\tau$. We get that P, Q correspond respectively to points

$$\frac{a\tau}{N} + \frac{b}{N}, \frac{c\tau}{N} + \frac{d}{N} \in \mathbb{C}/\Lambda_\tau.$$

We get by properties of the Weil pairing that

$$e_N(P, Q) = e_N(\frac{a\tau}{N} + \frac{b}{N}, \frac{c\tau}{N} + \frac{d}{N}) = e_N(\frac{\tau}{N}, \frac{1}{N})^{ad-bc} = (e^{\frac{2\pi i}{N}})^{ad-bc}.$$

Because $e_N(P, Q) = e^{\frac{2\pi i}{N}}$ as well we must have that $ad - bc \equiv 1 \pmod N$ and so we get that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$. We can lift this matrix to a matrix $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$. Again we have that P, Q correspond to the points $\frac{a'\tau}{N} + \frac{b'}{N}, \frac{c'\tau}{N} + \frac{d'}{N} \in \mathbb{C}/\Lambda_\tau$ as well because a, b, c, d are equivalent to a', b', c', d' modulo N. We similarly to the proof of 1 take $\tau' := \frac{a'\tau + b'}{c'\tau + d'}$. Then $(c'\tau + d')\Lambda_{\tau'} = \Lambda_\tau$ and so these lattices are homothetic. We also have that

$$(c'\tau + d')\frac{1}{N} = \frac{c'\tau}{N} + \frac{d'}{N}$$

and that

$$(c'\tau + d')\frac{\tau'}{N} = \frac{a'\tau}{N} + \frac{b'}{N}$$

and so the isomorphism between $E_{\Lambda_{\tau'}}$ and E_{Λ_τ} induced by $c'\tau + d'$ sends $(\frac{\tau'}{N}, \frac{1}{N})$ to the points $\frac{a'\tau}{N} + \frac{b'}{N}, \frac{c'\tau}{N} + \frac{d'}{N} \in \mathbb{C}/\Lambda_\tau$ corresponding to the points $(P, Q) \in E(\mathbb{C})$. We conclude that

$$(E, P, Q) \cong (E_{\Lambda_{\tau'}}, \frac{\tau'}{N}, \frac{1}{N}).$$

Now assume that for $\tau_1, \tau_2 \in \mathbb{H}$ we have that $\tau_1 = \frac{a\tau_2 + b}{c\tau_2 + d}$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N)$, so $a, d \equiv 1 \pmod N$ and $b, c \equiv 0 \pmod N$. Then for $\frac{1}{N} \in \mathbb{C}/\Lambda_{\tau_1}$ we have that

$$c\tau_2 + d(\frac{1}{N}) \equiv \frac{1}{N} \pmod N$$

and for $\frac{\tau_1}{N} \in \mathbb{C}/\Lambda_{\tau_1}$ that

$$c\tau_2 + d(\frac{\tau_1}{N}) \equiv \frac{\tau_2}{N} \pmod{N}.$$

So we get that

$$(E_{\Lambda_{\tau_1}}, \frac{\tau_1}{N}, \frac{1}{N}) \cong (E_{\Lambda_{\tau_2}}, \frac{\tau_2}{N}, \frac{1}{N}).$$

If conversely we have that $(E_{\Lambda_{\tau_1}}, \frac{\tau_1}{N}, \frac{1}{N}) \cong (E_{\Lambda_{\tau_2}}, \frac{\tau_2}{N}, \frac{1}{N})$ for some $\tau_1, \tau_2 \in \mathbb{H}$, then we must have that there exists some $\alpha \in \mathbb{C}$ such that $\alpha\Lambda_{\tau_1} = \Lambda_{\tau_2}$ and that $\frac{\alpha}{N} \equiv \frac{1}{N} \pmod{\Lambda_{\tau_2}}$ and $\frac{\alpha\tau_1}{N} \equiv \frac{\tau_2}{N} \pmod{\Lambda_{\tau_2}}$. We have that $\alpha\tau_1 = a\tau_2 + b$ and that $\alpha = c\tau_2 + d$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in$ $\mathrm{SL}(2,\mathbb{Z})$. Also here we take its residue class in $\Gamma(1)$. The facts that $\frac{\alpha}{N} \equiv \frac{1}{N} \pmod{\Lambda_{\tau_2}}$ and $\frac{\alpha\tau_1}{N} \equiv \frac{\tau_2}{N} \pmod{\Lambda_{\tau_2}}$ imply that $a, d \equiv 1 \pmod{N}$ and that $b, c \equiv 0 \pmod{N}$ and so we get that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N).$$

This concludes the proof.

□

Remark 4.11. Note that the set

$$\{(E, G) \mid E/\mathbb{C} \text{ an elliptic curve and } G \text{ a cyclic subgroup of } E(\mathbb{C}) \text{ of order } N\}$$

is in bijection with the set of $\{(E, \phi) \mid E/\mathbb{C}$ an elliptic curve and ϕ an N-isogeny$\}$ as stated in remark 3.1. So we get that $Y_0(N)$ also parametrizes elliptic curves with an N-isogeny.

4.4 The quotient curve X_H

We have seen multiple different modular curves $X(N), X_0(N), X_1(N)$ parametrizing elliptic curves over $\mathbb{C}$ with varying structure. As these modular curves are compact Riemann surfaces of dimension 1 they are given by algebraic curves. We can even define $X(N)$ over $\mathbb{Q}(\zeta_N)$. To do this we need to know what the function field of $X(N)$ is. We have for $X_0(1) = X_1(1) = X(1) \cong \mathbb{P}^1(\mathbb{C})$ that $\mathbb{C}(X(1)) = \mathbb{C}(j)$ where j is the so called modular invariant which corresponds to the j-invariant of an elliptic curve given by a point $P \in X(1)$ [13, Section 3.2]. We also have the following proposition:

Theorem 4.12. [13, Proposition 7.5.2]
We have that the function field of the modular curve $X(N)$ is given by

$$\mathbb{C}(X(N)) = \mathbb{C}(x(E_{j_0}[N]), j)$$

where E_{j_0} is the universal elliptic curve given by

$$E_{j_0} : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}.$$

Furthermore the field extension $\mathbb{C}(x(E_{j_0}[N]), j)/\mathbb{C}(j)$ is Galois with Galois group given by

$$\mathrm{Gal}(\mathbb{C}(x(E_{j_0}[N]), j)/\mathbb{C}(j)) = \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\}.$$

We can also take the field extension $\mathbb{Q}(x(E_{j_0}[N]), j)/\mathbb{Q}(j)$. This is Galois as well with Galois group given by $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ and we have that

$$\mathbb{Q}(x(E_{j_0}[N]), j) \cap \bar{\mathbb{Q}} = \mathbb{Q}(\zeta_N)$$

[13, Section 7.6]. We have from [35, II.2.5] that function fields $\mathbb{K}/\mathbb{Q}$ for which $\mathbb{K} \cap \bar{\mathbb{Q}} = K$ correspond to algebraic curves defined over K, so we get that the field $\mathbb{Q}(x(E_{j_0}[N]), j)$ corresponds to an algebraic curve, which we denote as $X(N)_{\mathrm{alg}}/\mathbb{Q}(\zeta_N)$ defined over $\mathbb{Q}(\zeta_N)$, which has a function field given by $\mathbb{Q}(x(E_{j_0}[N]), j)$. The points of $X(N)_{\mathrm{alg}}$ with coordinates in $\mathbb{C}$ form a curve which is isomorphic to $X(N)$ [13, Theorem 7.7.1].

We have the map $X(N) \to X(1)$ induced by sending a point $[\tau] \in \mathbb{H}/\Gamma(N)$ to $[\tau] \in \mathbb{H}/\Gamma(1)$. This map gives rise to the map of function fields $\mathbb{C}(X(1)) \to \mathbb{C}(X(N))$. We have that $\mathbb{C}(X(N))/\mathbb{C}(X(1)$ is Galois given by $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\}$. This is an example of a Galois covering, for which we give the definition:

Definition 4.13. Let X, Y be curves and let $\phi : X \to Y$ be a covering of topological spaces. We call ϕ a **Galois covering** if $K(X)/K(Y)$ is a Galois extension.

We have by the fundamental theorem of Galois coverings [16, Theorem 2.1] that normal subgroups $G \subseteq \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\}$ correspond to intermediate Galois coverings given by $X(N)/G := \{[P] \mid P \in X(N)\}$ where $[P]$ is given by the orbit of P under the action of G. Note that as $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\} \cong \Gamma(1)/\Gamma(N)$ we get for $G = \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\}$ that

$$X(N)/G \cong \frac{\mathbb{H}/\Gamma(N)}{\Gamma(1)/\Gamma(N)} \cong \mathbb{H}/\Gamma(1) = X(1),$$

while on the other hand we have for $G = \{[I]\} \subset \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\}$ that

$$X(N)/\{[I]\} \cong X(N).$$

Definition 4.14. Now take $H \subseteq \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\}$, then for $H_0 := H \cap \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\}$ we define the **quotient curve** $X_H := X(N)/H_0$.

Remark 4.15. Note that because non-cuspidal points of $X(N)$ correspond to isomorphism classes of elliptic curves over $\mathbb{C}$ and canonical level N structures, we have that non-cuspidal points of X_H correspond to isomorphism classes of elliptic curves $E/\mathbb{C}$ and H_0-orbits of canonical level N structures of E. Note that H_0-orbits of canonical level N structures correspond to unique H-orbits of level N structures of E as every H-orbit of level N structures contains a unique H_0-orbit of canonical level N structures. So we also have that non-cuspidal points of X_H correspond to isomorphism classes of elliptic curves $E/\mathbb{C}$ and H-orbits of level N structures of E.

We have seen that $X(N)$ admits a natural structure over $\mathbb{Q}(\zeta_N)$, meaning there exists a algebraic curve $X(N)_{\text{alg}}/\mathbb{Q}(\zeta_N)$ such that $\mathbb{C}$-points of $X(N)_{\text{alg}}$ correspond to points of $X(N)$. Let

$$\det(\mathrm{H}) := \mathrm{Im}(\det(\mathrm{H})) \subseteq (\mathbb{Z}/N\mathbb{Z})^*$$

with $\det : \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \to (\mathbb{Z}/N\mathbb{Z})^*$ the determinant map, then for X_H we similarly have that X_H admits natural structure over $\mathbb{Q}(\zeta_N)^{\det(\mathrm{H})}$ which is the subfield of $\mathbb{Q}(\zeta_N)$ fixed by $\det(H)$ seen as a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ [12, IV.3.20.4]. We have the following theorem which states that for quotient curves X_H we have that under certain conditions X_H admits a natural structure over $\mathbb{Q}$.

Theorem 4.16. [13, Theorem 7.6.3]
Let $H \subseteq \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\}$ and let X_H be its corresponding quotient curve. Then X_H admits a natural structure over $\mathbb{Q}$ if and only if $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$*. Here natural structure over $\mathbb{Q}$ means that there exists an algebraic curve $(X_H)_{\text{alg}}/\mathbb{Q}$ such that $\mathbb{C}$-points of $(X_H)_{\text{alg}}$ bijectively correspond to points of X_H.*

Example 4.17. We have that the modular curves $X_0(N), X_1(N)$ are isomorphic to quotient curves X_H for specific H. We can also show that these curves admit natural structure over $\mathbb{Q}$. If we first of all take

$$H = \left\{ \pm \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\} \right\}$$

then

$$H_0 = H \cap \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\} = \left\{ \pm \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in H \mid ac \equiv 1 \pmod{N} \right\} / \{-I\} \cong \Gamma_0(N)/\Gamma(N).$$

Therefore we have that

$$X_H = X(N)/H_0 = \frac{\mathbb{H}/\Gamma(N)}{\Gamma_0(N)/\Gamma(N)} \cong \mathbb{H}/\Gamma_0(N) = X_0(N).$$

We also have for

$$H = \left\{ \pm \begin{pmatrix} 1 & b \\ 0 & c \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\} \right\}$$

that

$$H_0 = \left\{ \pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in H \right\} / \{-I\} \cong \Gamma_1(N)/\Gamma(N).$$

We now get that

$$X_H = X(N)/H_0 = \frac{\mathbb{H}/\Gamma(N)}{\Gamma_1(N)/\Gamma(N)} \cong \mathbb{H}/\Gamma_1(N) = X_1(N).$$

Note that in both cases we have that $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$ and therefore both $X_0(N)$ and $X_1(N)$ admit a natural structure over $\mathbb{Q}$.

4.5 Rational points on modular curves

We finally return to our main topic of Galois representations of elliptic curves. How this topic is related to modular curves we will now explain. From here on we assume that $H \subseteq \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\}$ has the property that $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$. As the quotient curve X_H has a natural structure over $\mathbb{Q}$, it makes sense to define $X_H(\mathbb{Q}) := (X_H)_{\mathrm{alg}}(\mathbb{Q})$. We will show that non-cuspidal rational points of $X_H(\mathbb{Q})$ are represented by elliptic curves over $\mathbb{Q}$ with Galois representations

$$\rho_{E,N}(G_{\mathbb{Q}}) = \mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \subseteq gHg^{-1}$$

for some $g \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

Remark 4.18. Recall that for $E/\mathbb{Q}$ an elliptic curve and $\sigma \in G_{\mathbb{Q}}$ we have that σ induces an action on $E[N] \cong \mathbb{Z}/N\mathbb{Z}/\times\mathbb{Z}/N\mathbb{Z}$. We can extend this to elliptic curves $E/\mathbb{C}$ as follows: Let

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

be the Weierstrass equation for E with $a_1, ..., a_6 \in \mathbb{C}$. Then we define E^σ as the curve

$$E^\sigma : y^2 + \sigma(a_1)xy + \sigma(a_3)y = x^3 + \sigma(a_2)x^2 + \sigma(a_4)x + \sigma(a_6).$$

Now σ induces a group homomorphism $\sigma : E(\mathbb{C}) \to E^\sigma(\mathbb{C})$ defined by $\sigma(P) = (\sigma(x), \sigma(y))$ for $P = (x, y)$: If $P = (x, y)$ is a point of E, then $y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$, so then $\sigma(P)$ is a solution of E^σ as σ is a group homomorphism and so

$$\sigma(y)^2 + \sigma(a_1)\sigma(x)\sigma(y) + \sigma(a_3)\sigma(y) - \sigma(x)^3 - \sigma(a_2)\sigma(x)^2 - \sigma(a_4)\sigma(x) - \sigma(a_6) = \\ \sigma(y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6) = 0.$$

We also have, similar to elliptic curves over $\mathbb{Q}$, that σ induces an group isomorphism $\sigma : E[N] \to E^\sigma[N]$. If we take a level N structure for E given by $\alpha : \mathbb{Z}/N\mathbb{Z}/\times\mathbb{Z}/N\mathbb{Z} \to E[N]$ then $\sigma \circ \alpha$ defines a level N-structure of E^σ. If we now take a point $P \in X_H$ then P corresponds to a pair $([E], [\alpha])$ with $[E]$ the isomorphism class of $E/\mathbb{C}$ an elliptic curve and $[\alpha]$ an H-orbit of the level N-structure α of E. Note that $([E], [\alpha])$ and $([E'], [\alpha'])$ represent the same point of X_H if there exists an isomorphism $\phi : E \to E'$ over $\mathbb{C}$ such that $\alpha' = \phi \circ \alpha \circ h$ for some $h \in H$. We have that $\sigma(P)$ is the point of X_H represented by $[E^\sigma]$ and the H-orbit of $\sigma \circ \alpha$. Note that $X_H(\mathbb{Q})$ consists of precisely the points in X_H stable under the action of $\sigma \in G_{\mathbb{Q}}$. [38, Section 3.1].

Note that if E is defined over $\mathbb{Q}$ then $E^\sigma = E$ and $\sigma \in \mathrm{Aut}(E[N])$ and $\rho_{E,N}(\sigma) \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ as we have established before.

We state the following theorem:

Theorem 4.19. [38, Lemma 3,1 and Proposition 3.2]
Let $H \subseteq \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\}$ have the property that $\det(H) = (\mathbb{Z}/N\mathbb{Z})^*$ and let X_H be its corresponding quotient curve.
Let $P \in X_H(\mathbb{Q})$ with P non-cuspidal. Then P is represented by an elliptic curve $E/\mathbb{Q}$.
We furthermore have for $P \in X_H$ represented by an elliptic curve $E/\mathbb{Q}$ with $j(E) \neq 0, 1728$ that $P \in X_H(\mathbb{Q})$ if and only if

$$\rho_{E,N}(G_{\mathbb{Q}}) = \mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \subseteq gHg^{-1}$$

for some $g \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

Proof: Let $P \in X_H(\mathbb{Q})$ be represented by the elliptic curve $E/\mathbb{C}$ and the H-orbit of the level N structure $\alpha : \mathbb{Z}/N\mathbb{Z}/ \times \mathbb{Z}/N\mathbb{Z} \to E[N]$. We have for all $\sigma \in G_{\mathbb{Q}}$ that $\sigma(P)$ is represented by $\sigma(E)$ and the H-orbit of $\sigma \circ \alpha$. As $P \in X_H(\mathbb{Q})$ we get that $\sigma(P) = P$ and therefore $E \cong E^\sigma$ over $\mathbb{C}$. In particular we get that

$$j(E) = j(E^\sigma) = \sigma(j(E))$$

and therefore $j(E) \in \mathbb{Q}$ as well. We get that

$$E_{j(E)} : y^2 + xy = x^3 - \frac{36}{j(E) - 1728}x - \frac{1}{j(E) - 1728}$$

is an elliptic curve over $\mathbb{Q}$ such that there exists an isomorphism $\phi : E_{j(E)} \to E$ over $\mathbb{C}$. Then P is also represented by $E_{j(E)}/\mathbb{Q}$ and the H-orbit of $\phi \circ \alpha$.

Now assume $P \in X_H$ is represented by an elliptic curve $E/\mathbb{Q}$ and the H-orbit of the level N structure α. We get that $E^\sigma = E$ and so $\sigma(P)$ is represented by E and the H-orbit of the level N structure $\sigma \circ \alpha$. We have that $P \in X_H(\mathbb{Q})$ if and only if $\sigma(P) = P$, which is now equivalent to stating that

$$\sigma \circ \alpha = \phi \circ \alpha \circ h$$

for some isomorphism $\phi \in \mathrm{Aut}(E)$ and $h \in H$. Assume that $\sigma \circ \alpha = \phi \circ \alpha \circ h$ for some $h \in H$, then

$$\alpha^{-1} \circ \phi^{-1} \circ \sigma \circ \alpha = h.$$

Because $j(E) \neq 0, 1728$ we have that $\mathrm{Aut}(E) = \{\pm 1\}$ [35, Theorem III.10.1]. So

$$\alpha^{-1} \circ \sigma \circ \alpha = \pm I \circ h$$

and as $I = -I$ in $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\}$ as well we get that $\sigma = \alpha \circ h \circ \alpha^{-1}$ and so

$$\rho_{E,N}(G_{\mathbb{Q}}) \subseteq gHg^{-1}$$

for $g =\in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$. Conversely assume $\rho_{E,N}(G_{\mathbb{Q}}) \subseteq gHg^{-1}$ for $g \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$, then for all $\sigma \in G_{\mathbb{Q}}$ we have that $\alpha^{-1} \circ \sigma \circ \alpha \in H$. If we take $\phi = 1$ then

$$\alpha^{-1} \circ \phi^{-1} \circ \sigma \circ \alpha \in H$$

and so $\sigma(P) = P$ and $P \in X_H(\mathbb{Q})$.

□

Example 4.20. We can use this theorem to get a better understanding of the non-cuspidal rational points of $X_0(N), X_1(N)$.

First of all we get that points $P \in X_0(N)(\mathbb{Q})$ are represented by elliptic curves $E/\mathbb{Q}$ with $\rho_{E,N}(G_{\mathbb{Q}}) \subseteq gHg^{-1}$ for some $g \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ with

$$H = \left\{ \pm \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\} \right\} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \right\}.$$

Note that this corresponds by Proposition 3.3 to elliptic curves $E/\mathbb{Q}$ with a cyclic subgroup of $E(\mathbb{Q})$ over order N stable under $G_{\mathbb{Q}}$ (or in other words a rational cyclic N-isogeny).

We furthermore get that points $P \in X_1(N)(\mathbb{Q})$ are represented by elliptic curves $E/\mathbb{Q}$ with $\rho_{E,N}(G_{\mathbb{Q}}) \subseteq gHg^{-1}$ for some $g \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ with

$$H = \left\{ \pm \begin{pmatrix} 1 & b \\ 0 & c \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\} \right\} = \left\{ \begin{pmatrix} 1 & b \\ 0 & c \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \right\}.$$

Note that this corresponds by Proposition 3.3 to elliptic curves $E/\mathbb{Q}$ with a rational point of order N.

Example 4.21. We have that $X(N)$ admits a natural structure over $\mathbb{Q}(\zeta_N)$. Similarly to the case of natural structure over $\mathbb{Q}$, we get that a non-cuspidal point $P \in X(N)(\mathbb{Q}(\zeta_N))$ is represented by an elliptic curve E over $\mathbb{Q}(\zeta_N)$. Note that $X(N)$ can be seen as the quotient curve X_H with

$$H = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})/\{-I\} \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \right\}.$$

We can also extend our definition of Galois representations of elliptic curves to elliptic curves over $\mathbb{Q}(\zeta_N)$ by only taking the image of elements in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\zeta_N))$. We then furthermore get that $\mathrm{Im}(\rho_{E,N}) \subseteq gHg^{-1}$ for some $g \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$. Note that this implies that $\mathbb{Q}(E[N]) = \mathbb{Q}(\zeta_N)$ as the torsion points are left fixed by elements of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\zeta_N))$.

Example 4.22. As we briefly mentioned in Subsection 3.5, the authors of [5] have shown that the elliptic curves over $\mathbb{Q}$ which have $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$ are parametrized by the non-cuspidal rational points of the modular quotient curve X_H with $H \subseteq \mathrm{GL}(2, \mathbb{Z}/6\mathbb{Z})/\{-I\}$ given by

$$H = \left\{ \pm \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \mid x^2 + y^2 \equiv 1 \pmod 3 \right\} \sqcup \left\{ \pm \begin{pmatrix} x & y \\ y & -x \end{pmatrix} \mid x^2 + y^2 \equiv -1 \pmod 3 \right\}.$$

The authors have furthermore shown that isomorphism classes of elliptic curves $E/\mathbb{Q}$ correspond to points of the modular curve X_H if and only if its j-invariant j_E has the property that

$$j_E = 2^{10} 3^3 t^3 (1 - 4t^3)$$

for some $t \in \mathbb{Q}$. This implies for $E/\mathbb{Q}$ that $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$ if and only if $j_E = 2^{10} 3^3 t^3 (1 - 4t^3)$.

5 Weil entanglement

This chapter we will focus more on Weil entanglement. We will mostly focus on cases where we have Weil $(2, n)$ and Weil $(3, n)$-entanglement. For Weil $(3, n)$-entanglement in particular we will use our obtained knowledge of modular curves to find elliptic curves with particular torsion structure, which we can modify further to find elliptic curves with specific Weil entanglement. For both Weil $(2, n)$- and $(3, n)$-entanglement we will also, similarly to how we handled Serre entanglement, study the conductor of certain quadratic and cubic abelian field extensions in order to precisely pinpoint for which $n \in \mathbb{N}$ the Weil entanglement occurs. We refer back to Definition 3.10 for the definition of Weil entanglement.

5.1 Weil $(2, n)$-entanglement of type $\mathbb{Z}/3\mathbb{Z}$

We begin by studying Weil $(2, n)$-entanglement in more detail. Because $\mathbb{Q}(\zeta_2) = \mathbb{Q}$ we get that this kind of entanglement can only be of the form

$$\mathbb{Q} \subsetneq (\mathbb{Q}(E[2]) \cap \mathbb{Q}^{\mathrm{ab}}) \cap \mathbb{Q}(\zeta_n).$$

Note that if $\rho_{E,2}$ is surjective, then Lemma 2.32 implies that $\mathrm{Gal}(\mathbb{Q}(E[2]/\mathbb{Q}) \cong S_3$ and that $(\mathbb{Q}(E[2]) \cap \mathbb{Q}^{\mathrm{ab}}) = \mathbb{Q}(\sqrt{\Delta_E})$. If furthermore $\mathrm{Gal}(\mathbb{Q}(E[2]/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ then also $(\mathbb{Q}(E[2]) \cap \mathbb{Q}^{\mathrm{ab}}) = \mathbb{Q}(\sqrt{\Delta_E})$. In these cases we get Weil $(2, n)$-entanglement of type $\mathbb{Z}/2\mathbb{Z}$ which we called Serre entanglement and already studied in more detail. We will now focus on the remaining case, which occurs when $\mathrm{Gal}(\mathbb{Q}(E[2]/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. By Lemma 2.32 this case corresponds to elliptic curves $E/\mathbb{Q}$ which have no rational 2-torsion points and for which $\Delta_E \in (\mathbb{Q}^*)^2$.

Remark 5.1. Let

$$H := \left\{ I, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\} \subset \mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z})$$

be the unique subgroup of order 3. We have that $I = -I$ in $\mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z})$ and that $\det(H) = (\mathbb{Z}/2\mathbb{Z})^* \cong \{1\}$, so we get by Theorem 4.19 that the non-cuspidal rational points of the modular quotient curve X_H parametrize elliptic curves $E/\mathbb{Q}$ such that $\mathrm{Im}(\rho_{E,2})$ is conjugate to a subgroup of H. In this case $\mathrm{Gal}(\mathbb{Q}(E[2]/\mathbb{Q})$ is either isomorphic to $\mathbb{Z}/3\mathbb{Z}$ or it is trivial. In [37, Theorem 1.1] the authors show that these elliptic curves $E/\mathbb{Q}$ parametrized by non-cuspidal rational points of X_H have the property that $j_E = t^2 + 1728$ for some $t \in \mathbb{Q}$. Note that by Lemma 3.18 this is equivalent to saying that $\Delta_E \in (\mathbb{Q}^*)^2$, which is in line with the statements given in Lemma 2.32.

Remark 5.2. Recall that in the proof of Lemma 2.32 we have shown for an elliptic curve $E/\mathbb{Q}$ without rational 2-torsion points and for which $\Delta_E \in (\mathbb{Q}^*)^2$, that E is isomorphic over $\mathbb{Q}$ to $E'/\mathbb{Q}$ with $E' : y^2 = x^3 + Ax + B$ and $A, B \in \mathbb{Q}$ for which we also have that E' has no rational 2-torsion points and $\Delta_E' \in (\mathbb{Q}^*)^2$. Furthermore we can clear the denominators of A, B by finding a $u \in \mathbb{Q}$ such that E' is isomorphic over $\mathbb{Q}$ to $E'' : y^2 = x^3 + A''x + B''$ with $A'' = u^4 A \in \mathbb{Z}$ and $B'' = u^6 B \in \mathbb{Z}$. We have that $\mathbb{Q}(E[2]) = \mathbb{Q}(E'[2])$ and also that $\mathbb{Q}(E''[2]) = \mathbb{Q}(E'[2])$ as the isomorphisms between E, E' and E', E'' were over $\mathbb{Q}$. Therefore we get that the Weil $(2, n)$-entanglement of E is the same as the Weil $(2, n)$-entanglement of E''. This implies that the Weil $(2, n)$-entanglement of general elliptic curves over $\mathbb{Q}$ is dependent on the Weil $(2, n)$-entanglement of isomorphic elliptic curves of the form $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. We will therefore focus on elliptic curves of this form.

If we now take such an elliptic curve $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$ and with $\text{Gal}(\mathbb{Q}(E[2]/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$, then Lemma 2.32 gives us that $\Delta_E \in (\mathbb{Q}^*)^2$ and so $\Delta_E = 16(-4A^3 - 27B^2) = 16C^2$ for some $C \in \mathbb{Q}$. Also the fact that E has no rational 2-torsion points implies that $x^3 + Ax + B$ is irreducible over $\mathbb{Z}[X]$. In other words we have that $\mathbb{Q}(E[2]) = \mathbb{Q}(\alpha)$ with $\alpha \in \mathbb{C}$ a root of $x^3 + Ax + B$, where $\mathbb{Q}(\alpha)$ is a cubic abelian field extension of $\mathbb{Q}$.

Definition 5.3. The **conductor** of an abelian field extension is defined by the smallest $N \in \mathbb{N}$ such that $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta_N)$.

Studying the conductor N of $\mathbb{Q}(\alpha)$ will be key in determining where the entanglement occurs as E will then have Weil $(2, N)$-entanglement of type $\mathbb{Z}/3\mathbb{Z}$. We summarize this in the following proposition:

Proposition 5.4. *Let $E/\mathbb{Q}$ be an elliptic curve. Then* $\text{Gal}(\mathbb{Q}(E[2]/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$ *if and only if $\Delta_E \in (\mathbb{Q}^*)^2$ and E has no rational points. Furthermore if this is the case then $\mathbb{Q}(E[2]) = \mathbb{Q}(\alpha)$ for some $\alpha \in \mathbb{C}$ with $\mathbb{Q}(\alpha)$ an cubic abelian field extension of $\mathbb{Q}$. Let N be the conductor of $\mathbb{Q}(\alpha)$. Then we have that E has Weil $(2, N)$-entanglement of type $\mathbb{Z}/3\mathbb{Z}$.*

We now provide two methods for computing the conductor of a cubic abelian field extension of $\mathbb{Q}$. The first method uses the so called conductor-discriminant formula [31]. This formula tells us that for the discriminant Δ_K and the conductor N_K of abelian cubic field extensions $K/\mathbb{Q}$ we have that

$$\Delta_K = (N_K)^2.$$

Let $K := \mathbb{Q}(\alpha)$ be a field extension of $\mathbb{Q}$ with $\alpha \in \mathbb{C}$ the root of the irreducible polynomial $f(x) := x^3 + Ax + B \in \mathbb{Z}[X]$. The discriminant of this polynomial we call Δ_{f_α} and is given by $\Delta_{f_\alpha} = -4A^3 - 27B^2$. Let $-4A^3 - 27B^2 = C^2$ for some $C \in \mathbb{Q}$, then we have seen that $\mathbb{Q}(\alpha)$ is a cubic abelian field extension of $\mathbb{Q}$. Note that by [36, Theorem 4.10] we have that

$$\Delta_{f_\alpha} = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2 \cdot \Delta_K$$

with $\mathcal{O}_K$ the ring of integers of K. Let $i_\alpha := [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Then the conductor of K is given by

$$\sqrt{\frac{\Delta_{f_\alpha}}{i_\alpha^2}} = \frac{\sqrt{-4A^3 - 27B^2}}{i_\alpha}.$$

This implies for elliptic curves $E : y^2 = x^3+Ax+B$ with $A, B \in \mathbb{Q}$ and with $\mathrm{Gal}(\mathbb{Q}(E[2]/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$, that we get for the conductor of $\mathbb{Q}(\alpha) = \mathbb{Q}(E[2])$ with $\alpha \in \mathbb{C}$ a root of $x^3 + Ax + B$ that

$$N_{\mathbb{Q}(\alpha)} = \frac{\sqrt{-4A^3 - 27B^2}}{i_\alpha} = \frac{\sqrt{\Delta_E}}{4i_\alpha}.$$

We summarize this in the following proposition:

Proposition 5.5. *Let $E/\mathbb{Q}$ be an elliptic curve of the form $E : y^2 = x^3 + Ax + B$ with $A.B \in \mathbb{Z}$ and with* $\mathrm{Gal}(\mathbb{Q}(E[2]/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. *Then $\mathbb{Q}(E[2]) = \mathbb{Q}(\alpha)$ with $\alpha \in \mathbb{C}$ a root of $x^3 + Ax + B$ and E has Weil* $(2, \frac{\sqrt{\Delta_E}}{4i_\alpha})$*-entanglement.*

Using this method we still have to determine the value of the index $i_\alpha := [\mathcal{O}_K : \mathbb{Z}[\alpha]]$, which we can compute by using Sage. We provide a few examples of elliptic curves with $\mathrm{Gal}(\mathbb{Q}(E[2]/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$ where we explicitly determine the index i_α.

Example 5.6. Let $E : y^2 = x^3 - 3x - 1$ be an elliptic curve over $\mathbb{Q}$. We have that the discriminant of E equals $\Delta_E = -16(4(-3)^3 + 27(-1)^2) = 1296 = 36^2$. We also have that $x^3 - 3x - 1$ is irreducible over $\mathbb{Z}[X]$ and so $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. By Lemma 2.32 we get that $\mathbb{Q}(E[2]) = \mathbb{Q}(\alpha)$ with $\alpha \in \mathbb{C}$ a root of $x^3 - 3x - 1$. Using Sage we find that $i_\alpha = 1$, and therefore the conductor of $\mathbb{Q}(\alpha)$ equals

$$N_{\mathbb{Q}(\alpha)} = \frac{\sqrt{1296}}{4} = \frac{36}{4} = 9.$$

So we get that $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\zeta_9)$ is the unique cubic subfield of $\mathbb{Q}(\zeta_9)$. We conclude that E has Weil $(2, 9)$-entanglement. Note that this is horizontal $(2, 9)$-entanglement.

Example 5.7. Take the elliptic curve $E : y^2 = x^3 - 21x - 28$. Its discriminant equals $\Delta_E = -16(4(-21)^3 + 27(-28)^2) = 254016 = 504^2$ and $x^3 - 21x - 28$ is irreducible over $\mathbb{Z}[X]$. So $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. Let $\alpha \in \mathbb{C}$ be a root of $x^3 - 21x - 28$. Using Sage we find that the index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}_{\mathbb{Q}(\alpha)}$ equals $i_\alpha = 2$. So the conductor of $\mathbb{Q}(\alpha)$ equals

$$N_{\mathbb{Q}(\alpha)} = \frac{\sqrt{254016}}{4 \cdot 2} = 63.$$

Therefore we conclude that E has Weil $(2, 63)$-entanglement. Also here we get that this induces horizontal $(2, 63)$-entanglement as well.

The second way of finding the conductor of a cubic abelian field extension involves the paper [19]. Again we note that if we have $\alpha \in \mathbb{C}$ a root of the polynomial $x^3 + Ax + B$ with $A, B \in \mathbb{Z}$ and $-4A^3 - 27B^2 = C^2$ for some $C \in \mathbb{Q}$, then $\mathbb{Q}(\alpha)$ is a cubic abelian field extension of $\mathbb{Q}$. Hasse showed in [18] that if $p_1, ..., p_n$ are the primes which ramify in $\mathbb{Q}(\alpha)$, then the conductor of this field is given by

$$N_{\mathbb{Q}(\alpha)} = \begin{cases} p_1 \cdot ... \cdot p_n, & \text{if 3 ramifies in } \mathbb{Q}(\alpha), \\ 9 \cdot p_1 \cdot ... \cdot p_n, & \text{if 3 does not ramify in } \mathbb{Q}(\alpha). \end{cases}$$

The authors of [19] furthermore give the following explicit formula for the conductor of $\mathbb{Q}(\alpha)$:

Theorem 5.8. [19, Theorem 1]
Let $\alpha \in \mathbb{C}$ be a root of the polynomial $x^3 + Ax + B$ with $A, B \in \mathbb{Z}$ and $-4A^3 - 27B^2 = C^2$ for some $C \in \mathbb{Q}$. Also let A, B be minimal in the sense that there does not exist an $R \in \mathbb{Z}$ with $R^2 \mid A$ and $R^3 \mid B$. Then $\mathbb{Q}(\alpha)$ is a cubic abelian field extension of $\mathbb{Q}$ with conductor given by

$$N_{\mathbb{Q}(\alpha)} = 3^k \prod_{\substack{p \text{ (prime)} \equiv 1 \pmod 3 \\ p|A, p|B}} p.$$

Let $a, b \in \mathbb{Z}$ and $e \geq 1$, then we write $a^e \mid\mid b$ if $a^e \mid b$ but $a^{e+1} \nmid b$. Then $k = \begin{cases} 1 & \text{if } 3 \nmid A \text{ or } 3 \mid\mid A, 3 \nmid B, 3^3 \mid C, \\ 2 & \text{if } 3^2 \mid\mid A \text{ or } 3 \mid\mid A, 3 \nmid B, 3^2 \mid\mid C. \end{cases}$

We provide a few examples where we explicitly establish the conductor of a cubic abelian field using this formula.

Example 5.9. We again take the elliptic curve $E : y^2 = x^3 - 21x - 28$. We have already seen that $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$ and that $\mathbb{Q}(E[2]) = \mathbb{Q}(\alpha)$ with $\alpha \in \mathbb{C}$ a root of $x^3 - 21x - 28$ with $4(-21)^3 + 27(-28)^2 = 126^2$. The only prime which divides both -21 and -28, and is equivalent to 1 modulo 3, is the number 7. We also have that $3 \mid\mid -21$, $3 \nmid -28$ and $3^2 \mid\mid 126$. Therefore Theorem 5.8 gives us that the conductor of $\mathbb{Q}(\alpha)$ is equal to

$$N_{\mathbb{Q}(\alpha)} = 3^2 \cdot 7 = 63,$$

which is similar to what we found in Example 5.7.

Example 5.10. Take the elliptic curve $E : y^2 = x^3 - 57x - 133$. We have that $4(-57)^3 + 27(-133)^2 = 263169 = 513^2$ and $x^3 - 57x - 133$ is irreducible over $\mathbb{Z}[X]$. This implies that $\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. We have that the only prime which divides both -57 and -133, and is equivalent to 1 modulo 3, is the number 19. We also have that $3 \mid\mid -57$, $3 \nmid -133$ and $3^3 \mid 513$. We therefore get by Theorem 5.8 that the conductor of $\mathbb{Q}(\alpha)$ is equal to

$$N_{\mathbb{Q}(\alpha)} = 19.$$

Using Sage we also find the index of α to be 27. So the first method would imply that

$$N_{\mathbb{Q}(\alpha)} = \frac{2052}{4 \cdot 27} = 19$$

which indeed gives the same answer. This implies that E has Weil $(2, 19)$-entanglement, which is horizontal $(2, 19)$-entanglement.

To conclude our subsection on Weil $(2, n)$-entanglement of type $\mathbb{Z}/3\mathbb{Z}$, we now give an infinite family of non-isomorphic elliptic curves over $\mathbb{Q}$ which have Weil $(2, p^e)$-entanglement of type $\mathbb{Z}/3\mathbb{Z}$ with p an odd prime and $e \geq 1$. For this we follow [11, 4.1]. We first note that if $3 \mid p^{e-1}(p-1)$, then $\mathbb{Q}(\zeta_{p^e})$ contains a unique cubic abelian subfield $L/\mathbb{Q}$. This is because $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^e})/\mathbb{Q}) \cong (\mathbb{Z}/p^e\mathbb{Z})^*$ and $(\mathbb{Z}/p^e\mathbb{Z})^*$ is a cyclic group of order $p^{e-1}(p-1)$ which is divisible by 3, so it has a unique subgroup of order 3 corresponding to a cubic abelian subfield of $\mathbb{Q}(\zeta_p^e)$. If $p \neq 3$ then $3 \mid p-1$ and we get that $\mathbb{Q}(\zeta_p)$ also has a unique cubic abelian subfield. Because $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_{p^e})$ we get that this unique subfield must be $L \subseteq \mathbb{Q}(\zeta_p) \subseteq (\mathbb{Q}(\zeta_{p^e})$. If on the other hand $p = 3$ then we must have that $3 \mid 3^{e-1}$ and so $e \geq 2$. We also have that $\mathbb{Q})\zeta_9)$ has the unique cubic abelian subfield given by $\mathbb{Q}[X]/(x^3 - 3x - 1)$. In this case we therefore get that $L = \mathbb{Q}[X]/(x^3 - 3x - 1)$ as $\mathbb{Q}(\zeta_9) \subseteq \mathbb{Q}(\zeta_{3^e})$. This implies that when studying elliptic curves over $\mathbb{Q}$ with Weil $(2, p^e)$-entanglement of type $\mathbb{Z}/3\mathbb{Z}$, it suffices to focus on elliptic curves which have Weil $(2, p)$-entanglement of type $\mathbb{Z}/3\mathbb{Z}$ for $p \neq 3$ and Weil $(2, 9)$-entanglement of type $\mathbb{Z}/3\mathbb{Z}$. This leads us to the following two propositions:

Proposition 5.11. [25, Proposition 8.7]
Let p be a prime with $p > 3$ and $3 \mid p-1$. Then there exists an infinite family of non-isomorphic elliptic curves over $\mathbb{Q}$ which have Weil $(2, p)$-entanglement of type $\mathbb{Z}/3\mathbb{Z}$.

Proof: We first of all note that if $3 \mid p-1$, then $p \geq 7$. In [25, Proposition 8.7] the authors state that Gauss showed that $\mathbb{Q}(\zeta_p)$ has the unique cubic abelian subfield L induced by the irreducible polynomial

$$x^3 + x^2 + \frac{(p-1)}{3}X - \frac{p-1+3kp}{27}$$

where k is the integer uniquely determined by the integral representation $4p = (3k-2)^2 + 27N^2$ for some $N \in \mathbb{Z}$. If we now take

$$E : y^2 = x^3 + x^2 + \frac{(p-1)}{3}X - \frac{p-1+3kp}{27}$$

then $\mathbb{Q}(E[2]) = L$. The authors then use a construction from [30] which for an elliptic curve $E/\mathbb{Q}$ provides an infinity family of elliptic curves $\mathcal{E}$, which have $\mathbb{Q}(E'[2]) = \mathbb{Q}(E[2])$

if $E' \in \mathcal{E}$. The authors obtain the following family of elliptic curves over $\mathbb{Q}$:

$$\begin{aligned} E_t : y^2 = x^3 + &\frac{(1727pt^2 + p + 9/4k^2t^2 - 9/4k^2 - 3kt^2 + 3k + t^2 - 1)}{(p - 9/4k^2 + 3k - 1)}x + \\ &\frac{(-1727pt^3 - 5181pt^2 + 3pt + p - 9/4k^2t^3 - 27/4k^2t^2)}{(p - 9/4k^2 + 3k - 1)} + \\ &\frac{(-27/4k^2t - 9/4k^2 + 3kt^3 + 9kt^2 + 9kt + 3k - t^3 - 3t^2 - 3t - 1)}{(p - 9/4k^2 + 3k - 1)}. \end{aligned}$$

The j-invariant of this family of E_t with $t \in \mathbb{Q}$ is a non-constant function dependent on t and so this family contains infinitely many non-isomorphic elliptic curves $E_t/\mathbb{Q}$ for which $\mathbb{Q}(E_t[2]) = \mathbb{Q}(E[2])$. As $\mathbb{Q}(E[2]) = L$ we get that E_t has Weil $(2, p)$-entanglement for all $t \in \mathbb{Q}$, which concludes the proof.

□

Proposition 5.12. [11, Proposition 4.2]
There exists an infinite family of non-isomorphic elliptic curves over $\mathbb{Q}$ which have Weil $(2, 9)$-entanglement of type $\mathbb{Z}/3\mathbb{Z}$.

Proof: The proof of this proposition follows very similarly to the previous proof. The authors of [11] state that the unique cubic abelian subfield $L \subseteq \mathbb{Q}(\zeta_9)$ is induced by the irreducible polynomial $x^3 - 6x^2 + 9x - 3$. The elliptic curve $E : y^2 = x^3 = 6x^2 + 9x - 3$ therefore has the property that $\mathbb{Q}(E[2]) = L$. With the same method from [30] as in the previous proof, the authors in [11] find the family

$$E_t : y^2 = x^3 - 3888(2303t^2 + 1)x - 46656(-2303t^3 - 6909t^2 + 3t + 1).$$

The j-invariant of this family of E_t with $t \in \mathbb{Q}$ is again a non-constant function dependent on t and so we get infinitely many non-isomorphic elliptic curves $E_t/\mathbb{Q}$ for which $\mathbb{Q}(E_t[2]) = \mathbb{Q}(E[2])$. We conclude that E_t has Weil $(2, 9)$-entanglement for all $t \in \mathbb{Q}$.

□

These two propositions together with our observations that Weil $(2, p^e)$-entanglement is induced by Weil $(2, p)$-entanglement for $p \geq 7$ or Weil $(2, 9)$-entanglement if $p = 3$ now imply the following corollary:

Corollary 5.13. *Let p be a prime and $e \geq 1$ with $3 \mid p^{e-1}(p-1)$. Then there exists an infinite family of non-isomorphic elliptic curves over $\mathbb{Q}$ which have Weil $(2, p^e)$-entanglement of type $\mathbb{Z}/3\mathbb{Z}$.*

5.2 Weil $(3, n)$-entanglement of type $\mathbb{Z}/2\mathbb{Z}$

Now we move on to elliptic curves which have Weil $(3, n)$-entanglement. Specifically we will focus on entanglement of the form $\mathbb{Q} \subsetneq \mathbb{Q}(E[3]) \cap \mathbb{Q}(\zeta_n)$ with $n \geq 1$ such that $3 \nmid n$ and $\mathbb{Q}(E[3]) \cap \mathbb{Q}(\zeta_n)$ is a quadratic extension of $\mathbb{Q}$ (so of type $\mathbb{Z}/2\mathbb{Z}$).

We first state the following theorem from [11]:

Theorem 5.14. [11, Theorem 3.18]
Let $E/\mathbb{Q}$ be an elliptic curve and let p be an odd prime. Let $K_p(E) = \mathbb{Q}(E[p]) \cap \mathbb{Q}^{\text{ab}}$. Then:

1. *$\text{Gal}(K_p(E)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^* \times C$, with C a cyclic group of order dividing $p - 1$.*
2. *If $E/\mathbb{Q}$ does not have a rational p-isogeny, then C is trivial or of order 2 and $K_p(E) = F(\zeta_p)$ with $F/\mathbb{Q}$ a trivial or quadratic extension of $\mathbb{Q}$.*
3. *If the image of $\rho_{E,p}$ is surjective, then $K_p(E) = \mathbb{Q}(\zeta_p)$.*

Finally, if $p = 2$, then $K_p(E)$ is a trivial, quadratic, or cubic extension of $\mathbb{Q}$.

If for an elliptic curve $E/\mathbb{Q}$ we have that $\rho_{E,3}$ is surjective, then Theorem 5.14.3 shows that $\mathbb{Q}(E[3]) \cap \mathbb{Q}^{\text{ab}} = \mathbb{Q}(\zeta_3)$. If we take $3 \nmid n$ this implies that $\mathbb{Q}(E[3]) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$. In order to get Weil $(3, n)$-entanglement we will therefore study elliptic curves $E/\mathbb{Q}$ such that that $\rho_{E,3}$ is non-surjective. This is the case for instance when $\text{Im}(\rho_{E,3})$ is conjugate to a subgroup of the Borel subgroup of $\text{GL}(2, \mathbb{Z}/3\mathbb{Z})$, given by

$$B(3) := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{Z}/3\mathbb{Z},\ ac \equiv 1, 2 \pmod 3 \right\} \subset \text{GL}(2, \mathbb{Z}/3\mathbb{Z}).$$

Remark 5.15. We have seen in Proposition 3.3 that elliptic curves $E/\mathbb{Q}$ for which $\text{Im}(\rho_{E,3})$ is conjugate to a subgroup of $B(3)$ are precisely the elliptic curves over $\mathbb{Q}$ having a rational 3-isogeny (or equivalently a $G_{\mathbb{Q}}$ stable subgroup of order 3). In Example 4.20 we saw that these elliptic curves are parametrized by the non-cuspidal rational points of the modular curve $X_0(3)$. In [37, Theorem 1.2] the authors show that such an elliptic curve $E/\mathbb{Q}$ has the property that

$$j_E = 27 \frac{(t+1)(t+9)^3}{t^3}.$$

For $\mathbb{Q}(E[3]) \cap \mathbb{Q}(\zeta_n)$ to be non-trivial for $3 \nmid n$ we need that $\mathbb{Q}(E[3]) \cap \mathbb{Q}^{\text{ab}} \neq \mathbb{Q}(\zeta_n)$. If $\text{Im}(\rho_{E,3})$ is conjugate to a subgroup of $B(3)$ then the possible size of $\mathbb{Q}(E[3]) \cap \mathbb{Q}^{\text{ab}}$ depends on the abelianization of $B(3)$. We have the following lemma:

Lemma 5.16. *The abelianization of the Borel subgroup $B(3) \subset \text{GL}(2, \mathbb{Z}/3\mathbb{Z})$ is given by*

$$B(3)/[B(3), B(3)] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Proof: The borel group $B(3)$ has order 12 and consists of 4 conjugacy classes of the form $G_{i,j} := \left\{ \begin{pmatrix} i & 0 \\ 0 & j \end{pmatrix}, \begin{pmatrix} i & 1 \\ 0 & j \end{pmatrix}, \begin{pmatrix} i & -1 \\ 0 & j \end{pmatrix} \right\}$ with $i, j \in \{1, -1\}$. The abelianization of $B(3)$ is defined as the quotient of $B(3)$ by the smallest normal subgroup $H \subseteq B(3)$ such that the quotient $B(3)/H$ is abelian. The subgroup $G_{1,1}$ is a normal subgroup of $B(3)$ with $B(3)/G_{1,1}$ consisting of the four conjugacy classes. The elements of this quotient are then represented by the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

which shows that $B(3)/G_{1,1} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Also we have that conjugacy classes will always become equivalent in the abelianization, and so we must have that $G_{1,1}$ is contained in H. As H was the smallest normal subgroup such that the quotient of $B(3)$ with H is abelian, we get that

$$B(3)/[B(3), B(3)] \cong B(3)/G_{1,1} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

□

We see that as $B(3) \cong \mathbb{Z}/2\mathbb{Z}/ \times \mathbb{Z}/2\mathbb{Z}$ it has three subgroups of order 2 and by Galois theory $\mathbb{Q}(E[3])$ contains up to 3 different quadratic subfields, depending on the image of $\rho_{E,3}$. We know by properties of the Weil pairing that $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$ is a quadratic subfield of $\mathbb{Q}(E[3])$, and so

$$\mathbb{Q}(E[3]) \cap \mathbb{Q}^{\text{ab}} = \mathbb{Q}(\sqrt{-3}, \sqrt{d})$$

for some $d \in \mathbb{Z}$. We have the following proposition which claims that $\mathbb{Q}(P) \subseteq \mathbb{Q}(E[3])$ is either equal to $\mathbb{Q}$ or a quadratic extension of $\mathbb{Q}$ with $P \in E[3]$ the generator of the kernel of the 3-isogeny of E:

Proposition 5.17. *Let $E/\mathbb{Q}$ be an elliptic curve such that $\operatorname{Im}(\rho_{E,3})$ is conjugate to a subgroup of $B(3)$. Then E has a rational 3-isogeny and we have for the generator of the kernel of this isogeny, $P \in E[3]$, that $\mathbb{Q}(P) \subseteq \mathbb{Q}(E[3])$ is a trivial or quadratic extension.*

Proof: We first assume $E/\mathbb{Q}$ is of the form $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Q}$. We have that $\operatorname{Im}(\rho_{E,3})$ is conjugate to a subgroup of $B(3)$ which means that E has a rational 3-isogeny. The kernel of this isogeny is then a subgroup of order 3 which is stable under the action of $G_{\mathbb{Q}}$. The kernel is generated by a point $P = (x, y) \in E[3]$ with $x, y \in \mathbb{C}$. Because P has order 3 we get that $\mathbb{Q}(P) \subseteq \mathbb{Q}(E[3])$. We furthermore have that $2P = -P$ and so the kernel is given by $\{\mathcal{O}, P, -P\}$, and as E is in short Weierstrass form we have that $-P = (x, -y)$ [35, III.2.3]. The fact that the kernel is stable under the action of $G_{\mathbb{Q}}$ means that $\sigma(P) = \pm P$ for $\sigma \in G_{\mathbb{Q}}$. Therefore $\sigma(x) = x$, which implies that $x \in \mathbb{Q}$, and $\sigma(y) = \pm y$. If $P \notin E(\mathbb{Q})$ then we must have that $\mathrm{Gal}(\mathbb{Q}(y)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ and that $\mathbb{Q}(P) = \mathbb{Q}(y)$ is a quadratic extension. If $P \in E(\mathbb{Q})$ then $\mathbb{Q}(P)$ is trivial.

In general let $E/\mathbb{Q}$ be an elliptic curve with $\mathrm{Im}(\rho_{E,3})$ conjugate to a subgroup of $B(3)$ and let $P \in E[3]$ be the generator of the kernel of the 3-isogeny belonging to E. We have that $E \cong E'$ over $\mathbb{Q}$ with E' of the form $E' : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Q}$. As this isomorphism is defined over $\mathbb{Q}$, we have that it commutes with the action of $G_{\mathbb{Q}}$. This implies that E' has a rational 3-isogeny as well, generated by $P' \in E'[3]$ with P' the image of P under the given isomorphism. Again because the isomorphism was defined over $\mathbb{Q}$ we get that $\mathbb{Q}(P) = \mathbb{Q}(P')$. Because E' has a rational 3-isogeny we get that $\mathbb{Q}(P')$ is a trivial or quadratic extension, and therefore $\mathbb{Q}(P)$ is as well.

□

This proposition implies that $\mathbb{Q}(E[3]) \cap \mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\sqrt{-3}, P)$ with $P \in E[3]$ the generator of the kernel of the 3-isogeny of E. If P is not rational then $\mathbb{Q}(P)$ is a quadratic extension with given conductor $N \in \mathbb{N}$. In this case we get that E has Weil $(3, N)$-entanglement of type $\mathbb{Z}/2\mathbb{Z}$. We will now focus on finding the conductor of $\mathbb{Q}(P)$.

Remark 5.18. Every elliptic curve over $\mathbb{Q}$ is isomorphic to an elliptic curve in short Weierstrass form using the explicit isomorphism over $\mathbb{Q}$ given in Definition 2.1. We also have for $E/\mathbb{Q}$ that E has a rational 3-isogeny if an only if its corresponding curve $E'/\mathbb{Q}$ in short Weierstrass form has a rational 3-isogeny. This is because the isomorphism is given over $\mathbb{Q}$ and so it commutes with action of $G_{\mathbb{Q}}$, which then implies that subgroups stable under $G_{\mathbb{Q}}$ get sent to subgroups stable under $G_{\mathbb{Q}}$. It thus suffices to study the conductor of $\mathbb{Q}(P)$ for elliptic curves over $\mathbb{Q}$ in short Weierstrass form, as for general elliptic curves over $\mathbb{Q}$ we can change to short Weierstrass form and get that $\mathbb{Q}(P) = \mathbb{Q}(P')$ with P' the image of P under the isomorphism.

To compute the conductor we need the following theorem:

Theorem 5.19. [2, Theorem 5.2]
Let $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Q}$ be an elliptic curve. Then $\mathrm{Im}(\rho_{E,3})$ is conjugate to a subgroup of $B(3)$ if and only if E belongs to one of the following families of elliptic curves over $\mathbb{Q}$:

1. $$y^2 = x^3 + bx + \frac{16b^2 - 216a_0^2 b - 243a_0^4}{288a_0}$$

   with $b, a_0 \in \mathbb{Q}^*$.

2. $$y^2 = x^3 + c$$

   with $c \in \mathbb{Q}^*$.

3.

$$y^2 = x^3 + (-3m^2 + 6\beta m)x + 2\alpha^3 + 12\alpha\beta^2 - 6\alpha\beta m$$

with $\alpha, \beta, m \in \mathbb{Q}, \beta \neq 0$ *and* $m^2 = \alpha^2 + 3\beta^2$*.*

We now have the following three propositions, which are my own contributions, showing the Weil entanglement for each family of Theorem 5.19:

Proposition 5.20. *Let* E *be of the form*

$$E : y^2 = x^3 + bx + \frac{16b^2 - 216a_0^2 b - 243a_0^4}{288a_0}$$

with $b, a_0 \in \mathbb{Q}^*$ *and let* $\overline{2a_0}$ *be the squarefree part of* $2a_0$ *such that* $\overline{2a_0} \in \mathbb{Z}$*. Then if* $3 \nmid 2a_0$ *we have that*

E *has* $\begin{cases} \text{Weil } (3, \overline{2a_0})\text{-entanglement if } \overline{2a_0} \equiv 1 \pmod 4, \\ \text{Weil } (3, 4 \cdot \overline{2a_0})\text{-entanglement if } \overline{2a_0} \equiv 2, 3 \pmod 4. \end{cases}$

Proof: If $E/\mathbb{Q}$ is of this form, then the authors show in the proof of [2, Lemma 4.5] that E has a point of order three given by $P = \left(\frac{3a_0}{2}, \frac{4b+27a_0^2}{12\sqrt{2a_0}}\right) \in E[3]$. We have that $-P = \left(\frac{3a_0}{2}, -\frac{4b+27a_0^2}{12\sqrt{2a_0}}\right)$ and so $\sigma(P) = \pm P$ for $\sigma \in G_{\mathbb{Q}}$. This implies that the subgroup of $E[3]$ given by $\{\mathcal{O}, P, -P\}$ is stable under action of $G_{\mathbb{Q}}$ and so P is the generator of the kernel of the 3-isogeny of E. We have then that $\mathbb{Q}(E[3]) \cap \mathbb{Q}^{\text{ab}} = \mathbb{Q}(\sqrt{-3}, P)$ with

$$\mathbb{Q}(P) = \mathbb{Q}(\sqrt{2a_0}).$$

Let $\overline{2a_0}$ be the squarefree part of $2a_0$ such that $\overline{2a_0} \in \mathbb{Z}$, then $\mathbb{Q}(\sqrt{2a_0}) = \mathbb{Q}(\sqrt{\overline{2a_0}})$. We get by Corollary 2.19 for the conductor N of $\mathbb{Q}(\sqrt{2a_0})$ that

$$N = \begin{cases} \overline{2a_0} & \text{if } \overline{2a_0} \equiv 1 \pmod 4, \\ 4 \cdot \overline{2a_0} & \text{if } \overline{2a_0} \equiv 2, 3 \pmod 4. \end{cases}$$

In the first case we get that E has Weil $(3, \overline{2a_0})$-entanglement, in the second case E has Weil $(3, 4 \cdot \overline{2a_0})$-entanglement.

□

Proposition 5.21. *Let* E *be of the form*

$$E : y^2 = x^3 + c$$

with $c \in \mathbb{Q}^*$ *and let* $\overline{c}$ *be the squarefree part of* c *such that* $\overline{c} \in \mathbb{Z}$*. Then if* $3 \nmid c$ *we have that*

E *has* $\begin{cases} \text{Weil } (3, \overline{c})\text{-entanglement if } \overline{c} \equiv 1 \pmod 4, \\ \text{Weil } (3, 4\overline{c})\text{-entanglement if } \overline{c} \equiv 2, 3 \pmod 4. \end{cases}$

Proof: If $E/\mathbb{Q}$ is of this form, then the authors show in [2, Theorem 3.2] that $P = (0, \sqrt{c}) \in E(\mathbb{C})$ is a point of order 3. We have that $-P = (0, -\sqrt{c})$ and so $\{\mathcal{O}, P, -P\}$ is a subgroup of $E[3]$ stable under action of $G_{\mathbb{Q}}$. P is therefore the generator of the kernel of the 3-isogeny of E. We get that

$$\mathbb{Q}(P) = \mathbb{Q}(\sqrt{c})$$

and if we take $\bar{c}$ to be the squarefree part of c such that $\bar{c} \in \mathbb{Z}$ we have that $\mathbb{Q}(\sqrt{c}) = \mathbb{Q}(\sqrt{\bar{c}})$. By Corollary 2.19 we get for the conductor of $\mathbb{Q}(\sqrt{\bar{c}})$ that

$$N = \begin{cases} \bar{c} \;\text{ if } \bar{c} \equiv 1 \pmod 4, \\ 4\bar{c} \;\text{ if } \bar{c} \equiv 2, 3 \pmod 4. \end{cases}$$

In the first case E has Weil $(3, \bar{c})$-entanglement, in the second case E has Weil $(3, 4\bar{c})$-entanglement.

□

Proposition 5.22. *Let E be of the form*

$$y^2 = x^3 + (-3m^2 + 6\beta m)x + 2\alpha^3 + 12\alpha\beta^2 - 6\alpha\beta m$$

with $\alpha, \beta, m \in \mathbb{Q}, \beta \neq 0$ and $m^2 = \alpha^2 + 3\beta^2$ and let $\overline{-2(\alpha + m)}$ be the squarefree part of $-2(\alpha + m)$ such that $\overline{-2(\alpha + m)} \in \mathbb{Z}$. Then if $3 \nmid 2(\alpha + m)$ we have that

$$E \textit{ has } \begin{cases} \text{Weil } (3, \overline{-2(\alpha + m)})\text{-entanglement if } \overline{-2(\alpha + m)} \equiv 1 \pmod 4, \\ \text{Weil } (3, 4 \cdot \overline{-2(\alpha + m)})\text{-entanglement if } \overline{-2(\alpha + m)} \equiv 2, 3 \pmod 4. \end{cases}$$

Proof: If E is of this form, then in [26, 2.3] the author shows that

$$P = \Big(-\alpha + (2m - 3\beta), (2m - 3\beta)\sqrt{-2(\alpha - m)}\Big) \in E(\mathbb{C})$$

is a point of order 3. We have that $-P = \Big(-\alpha + (2m - 3\beta), -(2m - 3\beta)\sqrt{-2(\alpha - m)}\Big)$ and so $\{\mathcal{O}, P, -P\}$ is a subgroup of $E[3]$ stable under action of $G_{\mathbb{Q}}$ with P being its generator. We get that

$$\mathbb{Q}(P) = \mathbb{Q}(\sqrt{-2(\alpha + m)}) = \mathbb{Q}(\sqrt{\overline{-2(\alpha + m)}})$$

with $\overline{-2(\alpha + m)}$ the squarefree part of $-2(\alpha + m)$ such that $\overline{-2(\alpha + m)} \in \mathbb{Z}$. By Corollary 2.19 we get for the conductor of $\mathbb{Q}(\overline{-2(\alpha + m)})$ that

$$N = \begin{cases} \overline{-2(\alpha + m)} \;\text{ if } \overline{-2(\alpha + m)} \equiv 1 \pmod 4, \\ 4 \cdot \overline{-2(\alpha + m)} \;\text{ if } \overline{-2(\alpha + m)} \equiv 2, 3 \pmod 4. \end{cases}$$

In the first case E has Weil $(3, \overline{-2(\alpha+m)})$-entanglement, in the second case Weil $(3, 4\cdot \overline{-2(\alpha+m)})$-entanglement.

□

In [11] the authors also provide for $3 \nmid n$ an infinite family of non-isomorphic elliptic curves over $\mathbb{Q}$ which have Weil $(3, n)$-entanglement, using the modular curve $X(3)$.

Proposition 5.23. [11, Proposition 4.6]
Let $n \geq 1$ such that $3 \nmid n$. Let K be a quadratic subfield of $\mathbb{Q}(\zeta_n)$. Then there are infinitely many non-isomorphic elliptic curves $E/\mathbb{Q}$ such that $\mathbb{Q}(E[3]) \cap \mathbb{Q}(\zeta_n) = K$ and E has Weil $(3, n)$-entanglement of type $\mathbb{Z}/2\mathbb{Z}$.

Proof: We have that $K = \mathbb{Q}(\sqrt{d})$ for some $d \in \mathbb{Z}$ with d squarefree. Recall that we have shown in Example 4.21 that the modular curve $X(3)$ has structure over $\mathbb{Q}(\sqrt{3})$ and that the non-cuspidal points in $X(3)(\mathbb{Q}(\sqrt{3})$ parametrize elliptic curves $E/\mathbb{Q}$ over $\mathbb{Q}(\sqrt{3})$ with $\mathbb{Q}(E[3]) = \mathbb{Q}(\sqrt{3})$.

In [29] the authors provide for a variable t the Hesse cubic given by

$$X^3 + Y^3 + Z^3 = 3tXYZ$$

over $\mathbb{Q}(t)$. This is an elliptic curve over $\mathbb{Q}(t)$ with origin $(0, 1, -1)$. It has a rational point of order 3 given by $(-1, 1, 0)$ and it has a subgroup of order 3 given by $\{(0, 1, -1), (0, \zeta_3, -1), (0, (\zeta_3)^2, -1)\}$. Note that this is stable under action of $G_{\mathbb{Q}}$. The Hesse cubic also has the following Weierstrass form:

$$E_t : y^2 = x^3 - 27t(t^3 + 8)x + 54(t^6 - 20t^3 - 8).$$

The authors show in [29, 1.1] that the set of E_t with $t \in \mathbb{Q}$ is in bijection with the non-cuspidal rational points on $X(3)$ and that for $t \in \mathbb{Q}$ we have that

$$jX(3)(t) = j(E_{X(3)}(t)) = 27t^3 \frac{(t^3 + 8)^3}{(t^3 - 1)^3}.$$

We therefore get that the non-cuspidal rational points on $X(3)$ are parametrized by $E_t : y^2 = x^3 - 27t(t^3 + 8)x + 54(t^6 - 20t^3 - 8)$ for $t \in \mathbb{Q}$ and so for E_t we have that $\mathbb{Q}(E_t[3]) = \mathbb{Q}(\sqrt{3})$. We also have that E_t has a rational point P_t of order 3. This last part will be crucial in the rest of the proof.

We now take the twist of E_t by d. This is an elliptic curve given by

$$E_t^d : y^2 = x^3 - 27d^2t(t^3 + 8)x + 54d^3(t^6 - 20t^3 - 8).$$

The twist of E_t is isomorphic to E_t over $\mathbb{Q}(\sqrt{d})$ by sending $(x, y) \in E_t(\mathbb{C})$ to $(dx, \sqrt{d^3}y) \in E_t^d(\mathbb{C})$. This implies that the rational point P_t of order 3 gets sent to a point $P_t' \in E_t^d[3]$

with $\mathbb{Q}(P_t') = \mathbb{Q}(\sqrt{d})$ and therefore

$$\mathbb{Q}(E_t^d[3]) = \mathbb{Q}(\sqrt{3}, \sqrt{d}).$$

Because $3 \nmid n$ we get that $\mathbb{Q}(E_t^d[3]) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\sqrt{d}) = K$ and so that E_t^d has Weil $(3,n)$-entanglement of type $\mathbb{Z}/2\mathbb{Z}$. Also note that the family of E_t^d has infinitely many non-isomorphic elliptic curves, as $j_{E_t^d} = j_{E_t} = 27t^3\frac{(t^3+8)^3}{(t^3-1)^3}$ is a non-constant function depending on $t \in \mathbb{Q}$.

□

5.3 Weil (p,n)-entanglement for primes $p \geq 5$

We conclude this section by more generally looking at elliptic curves $E/\mathbb{Q}$ which have Weil (p,n)-entanglement for $n \geq 1$ and primes $p \geq 5$. Again we focus on entanglement of the form $\mathbb{Q} \subsetneq \mathbb{Q}(E[p]) \cap \mathbb{Q}(\zeta_n)$. For this to occur we need that $p \nmid n$. By Theorem 5.14 we also need $\rho_{E,P}$ to be non-surjective. If in particular we have that $\operatorname{Im}(\rho_{E,p})$ is conjugate to a subgroup of the Borel subgroup $B(p) \subset \mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$, then E has a rational p-isogeny. For the generator of the kernel of this isogeny, given by $P \in E[p]$, we have the following theorem:

Proposition 5.24. [22, Theorem 9.3]
Let $E/\mathbb{Q}$ be an elliptic curve with $\operatorname{Im}(\rho_{E,p})$ conjugate to a subgroup of the Borel subgroup $B(p)$. Then E has a p-isogeny and we have for the generator $P \in E[p]$ of its kernel, that $\mathbb{Q}(P)/\mathbb{Q}$ is a Galois cyclic extension of degree dividing $p-1$.

Proof: We can assume that P, Q with $Q \in E[p]$ is the fixed basis used for the definition of the Galois representation $\rho_{E,p}$. In this case $\operatorname{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \operatorname{Im}(\rho_{E,p}) \subseteq B(p)$ and $\mathbb{Q}(P)$ is the fixed field by the subgroup

$$H := \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mid a \in \mathbb{Z}/p\mathbb{Z}, b \in (\mathbb{Z}/p\mathbb{Z})^* \right\} \cap \operatorname{Im}(\rho_{E,p}).$$

We have that $H' := \left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mid a \in \mathbb{Z}/p\mathbb{Z}, b \in (\mathbb{Z}/p\mathbb{Z})^* \right\} \subset B(p)$ is a normal subgroup of $B(p)$ and therefore H is a normal subgroup of $\operatorname{Im}(\rho_{E,p})$. By Theorem 2.12 $\mathbb{Q}(P)/\mathbb{Q}$ is then a Galois extension. We also get that

$$\operatorname{Gal}(\mathbb{Q}(P)/\mathbb{Q}) \cong \operatorname{Im}(\rho_{E,p})/H \hookrightarrow B(p)/H' \cong (\mathbb{Z}/p\mathbb{Z})^*.$$

So $\operatorname{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ is isomorphic to a subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ and as $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group with order $p-1$ we get that $\operatorname{Gal}(\mathbb{Q}(P)/\mathbb{Q})$ is cyclic with order dividing $p-1$. We conclude that $\mathbb{Q}(P)/\mathbb{Q}$ is a Galois cyclic extension of degree dividing $p-1$. □

This then implies the following corollary:

Corollary 5.25. *Let $E/\mathbb{Q}$ be an elliptic curve with $\mathrm{Im}(\rho_{E,p})$ conjugate to a subgroup of the Borel subgroup $B(p)$. Then for the generator $P \in E[p]$ of the kernel of the p-isogeny of E we have that $\mathbb{Q}(P)$ is cyclic and therefore abelian. Let N be the conductor of $\mathbb{Q}(P)$. Then if $p \nmid N$ we get that E has Weil (p, N)-entanglement with its Galois group being a group of order dividing $p-1$.*

This, like in the cases where $p = 3$, suggests that in order to understand the level of this entanglement we need to study the conductor of $\mathbb{Q}(P)$. This would therefore seem a good place for further research. We also focused mainly on the cases where $\mathrm{Im}(\rho_{E,p})$ is conjugate to a subgroup of the Borel subgroup $B(p)$ and then in particular on the field of definition of the generator of the kernel of the associated p-isogeny. This could also be expanded upon in further research.

To conclude we note that the authors of [11] also provided for $m \geq 5$ more infinite non-isomorphic families of elliptic curves over $\mathbb{Q}$ with Weil (m, n)-entanglement, as listed in Theorem 3.29. Note that for $m = 5, 7$ a similar strategy to the case where $m = 3$ was used, where a family of elliptic curves was provided which had $\mathbb{Q}(E[p]) = \mathbb{Q}(\zeta_p)$ for $p = 5, 7$ and rational points of respectively order 5 and 7. Then using twisting a new family was given with the corresponding torsion points now having specific quadratic fields as their fields of definition.

6 Appendix

In this appendix we will list some known results on horizontal entanglement.

First of all using the method of describing horizontal entanglement, Daniels, Lozano-Robledo and Morrow have shown in [11] that there are infinitely many non-isomorphic elliptic curves with specific abelian entanglement which is not Weil or CM entanglement. More specifically we have the following theorem:

Theorem 6.1. [11, Theorem A]
Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$, and let $p < q$ be primes such that E has abelian (p, q)-entanglement with Galois group S. Then there is a finite set $J \subseteq \mathbb{Q}$, that does not depend on p, q or S such that if $j(E) \in J$ and the entanglement is not of Weil or CM type, then either $S = \mathbb{Z}/3\mathbb{Z}$ and $(p, q) = (2, 7)$ or $S = \mathbb{Z}/2\mathbb{Z}$ and $(p, q) = (3, 5)$. If $S = \mathbb{Z}/3\mathbb{Z}$ and $(p, q) = (2, 7)$, then we have for the j-invariant $j(E)$ that it belongs to one of the following three families of j-invariants with $t \in \mathbb{Q}$:

$$
\begin{aligned}
j_1(t) &:= \frac{(t^2+t+1)^3(t^6+5t^5+12t^4+9t^3+2t^2+t+1)P_1(t)^3}{t^{14}(t+1)^{14}(t^3+2t^2-t-1)^2},\\
j_2(t) &:= \frac{7^4(t^2+t+1)^3(9t^6+39t^5+64t^4+23t^3+4t^2+15t+9)P_2(t)^3}{(t^3+t^2-2t-1)^{14}(t^3+8t^2+5t-1)^2},\\
j_3(t) &:= \frac{(t^2-t+1)^3(t^6-5t^5+12t^4-9t^3+2t^2-t+1)P_3(t)^3}{(t-1)^2t^2(t^3-2t^2-t+1)^{14}}.
\end{aligned}
$$

where

$$
\begin{aligned}
&P_1(t) = t^{12}+8t^{11}+25t^{10}+34t^9+6t^8-0t^7-17t^6+6t^5-4t^3+3t^2+4t+1,\\
&P_2(t) = t^{12}+18t^{11}+131t^{10}+480t^9+1032t^8+1242t^7+805t^6+306t^5+132t^4+60t^3-t^26t+1,\\
&P_3(t) = t^{12}-8t^{11}+265t^{10}-1474t^9+5046t^8-10050t^7+\\
&\qquad 11263t^6-7206t^5+2880t^4-956t^3+243t^2-4t+1.
\end{aligned}
$$

In the case that $S = \mathbb{Z}/2\mathbb{Z}$ and $(p, q) = (3, 5)$, $j(E)$ belongs to one of the following two families of j-invariants:

$$
\begin{aligned}
j_4(t) &:= \frac{2^{12}P_4(t)^3}{(t1)^{15}(t+1)^{15}(t^2-4t-1)^3},\\
j_5(t) &:= \frac{2^{12}P_5(t)^3}{(t1)^{15}(t+1)^{15}(t^2-4t-1)^3}.
\end{aligned}
$$

where

$$
\begin{aligned}
&P_4(t) = t^{12}-9t^{11}+39t^{10}-75t^9+75t^8-114t^7+26t^6+114t^5+75t^4+75t^3+39t^2+9t+1,\\
&P_5(t) = 211t^{12}-189t^{11}-501t^{10}-135t^9+345t^8+966t^7+\\
&\qquad 146t^6-966t^5+345t^4+135t^3-501t^2+189t+211.
\end{aligned}
$$

Daniels and Morrow also provided more results on Weil entanglement for specific integers. The first two families we have discussed in more detail in Chapter 5.

Theorem 6.2. [11, Theorem B]
There are infinitely many $\bar{\mathbb{Q}}$-isomorphism classes of elliptic curves $E/\mathbb{Q}$ with:

(1) a Weil $(2, p^e)$-entanglement with Galois group $\mathbb{Z}/3\mathbb{Z}$ where $3 \mid p^{e-1}(p-1)$,

(2) a Weil $(3, n)$-entanglement with Galois group $\mathbb{Z}/2\mathbb{Z}$ where $3 \nmid n$,

(3) a Weil $(5, n)$-entanglement with Galois group $\mathbb{Z}/4\mathbb{Z}$ where $5 \nmid n$,

(4) a Weil $(7, n)$-entanglement with Galois group $\mathbb{Z}/6\mathbb{Z}$ where $6 \nmid n$,

(5) a Weil (m, n)-entanglement with Galois group $\mathbb{Z}/2\mathbb{Z}$ where $n > 3$ and $m \in \{3, 4, 5, 6, 7, 9\}$.

We remark that the first case was not included in Theorem B [11] but still proven in Proposition 4.2 of [11].

6.1 Coincidence

Finally we list some results about a specific kind of entanglement, namely coincidence. This is entanglement where $\mathbb{Q}(E[m]) = \mathbb{Q}(E[n])$ for $m \neq n$. Daniels and Lozano-Robledo have in [10] studied first of all for which elliptic curves and integers m, n we have an equality of division fields $\mathbb{Q}(E[m]) = \mathbb{Q}(E[n])$. They also tried to answer for which primes $p < q$ we have that $\mathbb{Q} \subsetneq \mathbb{Q}(E[p]) \cap \mathbb{Q}(\zeta_q)$ (note that this entanglement is similar to the Serre entanglement we have discussed before).

These questions have been studied both in terms of towers (ranging over m, n with m dividing n) and for coprime integers m, n. In terms of towers we have the following:

Theorem 6.3. [10, Theorem 1.4]
Let $E/\mathbb{Q}$ be an elliptic curve, let p be a prime, and let $n \geq 1$.
(1) Suppose that $\mathbb{Q}(E[p^{n+1}]) = \mathbb{Q}(E[p^n])$. Then $p = 2, n = 1$, and there is a rational number $t \in \mathbb{Q}$ such that E is isomorphic over Q to an elliptic curve of the form

$$E_t : y^2 = x^3 + A(t) \cdot x + B(t),$$

where

$$A(t) = -27t^8 + 648t^7 - 4212t^6 - 2376t^5 + 60102t^4 +$$
$$79704t^3 - 105732t^2 - 235224t - 107811,$$
$$B(t) = 54t^{12} - 1944t^{11} + 24300t^{10} - 97848t^9 - 251262t^8 + 1722384t^7 + 48217$$
$$-8697456t^5 - 64323558t^4 - 140447736t^3 - 157012020t^2 - 90561240t -$$

(2) If $\mathbb{Q}(E[p^n]) \cap \mathbb{Q}(\zeta_{p^{n+1}}) = \mathbb{Q}(\zeta_{p^{n+1}})$, then $p = 2$.

For distinct primes we have the following:

Theorem 6.4. [10, Theorem 1.6]
Let $E/\mathbb{Q}$ be an elliptic curve, let $p < q$ be primes, and let $n, m \geq 1$ be integers.
(1) If $\mathbb{Q}(E[p^n]) = \mathbb{Q}(E[q^m])$, then $p^n = 2$ and $q^m = 3$. Further, there is some $t \in \mathbb{Q}$ such that E is $\mathbb{Q}$-isomorphic to

$$\begin{aligned} &E' : y^2 = x^3 - 3t^9)(t^3-2)(t^3+2)^3(t^3+4)x \\ &\quad -2t^{12}(t^3+2)^4(t^4-2t^3+4t-2)(t^8+2t^7+4t^6+8t^5+10t^4+8t^3+16t^2+8t+4) \end{aligned}$$

or its twist by -3.
(2) Let $K_p(E) = \mathbb{Q}(E[p]) \cap \mathbb{Q}^{\mathrm{ab}}$. Then, $\mathrm{Gal}(K_p(E)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^* \times C$, where C is a cyclic group of order dividing $p-1$. Further, if E does not have a rational p-isogeny, then C is trivial or $\mathbb{Z}/2\mathbb{Z}$ and $K_p(E) = F(\zeta_p)$ with $F/\mathbb{Q}$ a trivial or quadratic extension.
(3) In particular, if $\mathbb{Q}(\zeta_{q^n}) \subseteq \mathbb{Q}(E[p])$, then either $\mathbb{Q}(\zeta_{q^n}) \in \{\mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\zeta_3)\}$, or E has a rational p-isogeny with $p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$, and in this case $\phi(p^n)$ divides $p-1$.

Finally we have the following theorem for abelian extensions:

Theorem 6.5. [10, Theorem 1.7]
Let $E/\mathbb{Q}$ be an elliptic curve and let $n > m \geq 2$ be integers with $\mathbb{Q}(E[n])/\mathbb{Q}$ an abelian extension of $\mathbb{Q}$.
(1) If $\mathbb{Q}(E[n]) = \mathbb{Q}(E[m])$, then $m = 2, n = 4$, and for some $t \in \mathbb{Q}$, E is $\mathbb{Q}$-isomorphic to

$$y^2 = x^3 + (-432t^8 + 1512t^4 - 27)x + (3456t^{12} + 28512t^8 - 7128t^4 - 54).$$

In this case, $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4]) = \mathbb{Q}(i)$.
(2) Let p be prime, such that $\mathbb{Q}(E[p])/\mathbb{Q}$ is abelian, and let $q \neq p$ be another prime. Then $Q(E[p]) \cap \mathbb{Q}(\zeta_{q^k})$ can be trivial, quadratic, cubic (for $p = 2$), or cyclic quartic (for $p = 5$).

6.2 Non-abelian entanglement

Brau and Jones in [5] have found an infinite family of non-isomorphic elliptic curves with non-abelian entanglement induced by the inclusion of $\mathbb{Q}(E[2])$ in $\mathbb{Q}(E[3])$. Jones and McMurdy in [21] expanded on this and showed the following theorem for elliptic curves over function fields $K(t)$ with K a number field (We only list the case where $K = \mathbb{Q}$):

Theorem 6.6. [21, Theorem 18]
Let $E/\mathbb{Q}$ be an elliptic curve. Then E has non-abelian entanglement if and only if the j-invariant $j_E \in \mathbb{Q}$ satisfies

$$j_E \in \{j_6(t), j_{10}(t), j_{18}(t) : t \in \mathbb{Q}\},$$

where

$$\begin{aligned}
j_6(t) &:= 2^{10}3^3t^3(1-4t^3),\\
j_{10}(t) &:= s_{10}^3(s_{10}^2+5s_{10}+40), \quad s_{10} = \frac{3t^6+12t^5+80t^4+50t^3-20t^2-8t+8}{(t-1)^2(t^2+3t+1)^2},\\
j_{18}(t) &:= \frac{-3^3t^3(t^3-2)(3t^3-4)^3(3t^3-2)^3}{(t^3-1)^2}.
\end{aligned}$$

Finally, if $j_E = j_m(t)$ for $m \in \{6, 10, 18\}$ and some $t \in \mathbb{Q}$, then E has non-abelian entanglement with Galois group S_3 (note that the case $m = 15$ is excluded because this can only happen if $\sqrt{-15} \in K$).

We remark that the case of $j_6(t)$ corresponds to the family of elliptic curves that was given in [5].

References

[1] Clemens Adelmann. *The decomposition of primes in torsion point fields*, volume 1761 of *Lecture Notes in Mathematics.* Springer-Verlag, Berlin, 2001.

[2] Andrea Bandini and Laura Paladino. *Number fields generated by the 3-torsion points of an elliptic curve. Monatsh. Math.*, 168(2):157–181, 2012.

[3] Frits Beukers. *Rings and Galois theory.* `https://webspace.science.uu.nl/~beuke106/ringengalois/dic.pdf`, 2016.

[4] Abbey Bourdon, Pete L. Clark, and James Stankewicz. *Torsion points on CM elliptic curves over real number fields. arXiv e-prints*, page arXiv:1411.2742, 2015.

[5] Julio Brau and Nathan Jones. *Elliptic curves with* 2*-torsion contained in the* 3*-torsion field. Proc. Amer. Math. Soc.*, 144(3):925–936, 2016.

[6] Francesco Campagna. *Cyclic reduction of elliptic curves.* `https://www.math.u-bordeaux.fr/~ybilu/algant/documents/theses/Campagna.pdf`, 2018.

[7] R. C. Daileda. *The structure of* $(\mathbb{Z}/n\mathbb{Z})^*$. `http://ramanujan.math.trinity.edu/rdaileda/teach/s18/m3341/ZnZ.pdf`, 2018.

[8] Harris B. Daniels. *An infinite family of Serre curves. J. Number Theory*, 155:226–247, 2015.

[9] Harris B. Daniels and Jackson S. Morrow. *A group theoretic perspective on entanglements of division fields. arXiv e-prints*, page arXiv:2008.09886, 2020.

[10] Harris B. Daniels and Álvaro Lozano-Robledo. *Coincidences of division fields. arXiv e-prints*, page arXiv:1912.05618, 2021.

[11] Harris B. Daniels, Álvaro Lozano-Robledo, and Jackson S. Morrow. *Towards a classification of entanglements of Galois representations attached to elliptic curves. arXiv e-prints*, page arXiv:2105.02060, 2021.

[12] P. Deligne and M. Rapoport. *Les schémas de modules de courbes elliptiques.* In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349, 1973.

[13] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2005.

[14] Tim Dokchitser and Vladimir Dokchitser. *Surjectivity of mod* 2^n *representations of elliptic curves. Math. Z.*, 272(3-4):961–964, 2012.

[15] Noam D. Elkies. *Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9. arXiv e-prints*, page arXiv:0612734, 2006.

[16] Dennis Eriksson and Ulf Persson. *Galois theory and coverings.* `http://www.math.chalmers.se/~dener/Galois-theory-of-Covers.pdf`, 2011.

[17] Steven D. Galbraith. *The Weil pairing on elliptic curves over* $\mathbb{C}$. `https://eprint.iacr.org/2005/323.pdf`, 2005.

[18] Helmut Hasse. *Arithmetische theorie der kubischen zahlkörper auf klassenkörpertheoretischer grundlage. Math. Z.*, 31(1):565–582, 1930.

[19] James G. Huard, Blair K. Spearman, and Kenneth S. Williams. *A short proof of the formula for the conductor of an abelian cubic field.* `https://people.math.carleton.ca/~williams/papers/pdf/184.pdf`, 1994.

[20] Nathan Jones. *Almost all elliptic curves are Serre curves. Trans. Amer. Math. Soc.*, 362(3):1547–1570, 2010.

[21] Nathan Jones and Ken McMurdy. *Elliptic curves with non-abelian entanglements. arXiv e-prints*, page arXiv:2008.09087, 2020.

[22] Álvaro Lozano-Robledo. *On the field of definition of p-torsion points on elliptic curves over the rationals. Math. Ann.*, 357(1):279–305, 2013.

[23] Samuel Marks. *Galois representations.* `https://people.math.harvard.edu/~smarks/mod-forms-tutorial/mf-notes/galois-reps.pdf`.

[24] B. Mazur. *Rational points on modular curves.* In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 107–148. Lecture Notes in Math., Vol. 601, 1977.

[25] Jackson S. Morrow. *Composite images of Galois for elliptic curves over* $\mathbb{Q}$ *& Entanglement fields. arXiv e-prints*, page arXiv:1707.04646, 2017.

[26] Laura Paladino. *Elliptic curves with* $\mathbb{Q}(E[3]) = \mathbb{Q}(\zeta_3)$ *and counterexamples to local-global divisibility by 9. J. Théor. Nombres Bordeaux*, 22(1):139–160, 2010.

[27] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. *ℓ-adic images of Galois for elliptic curves over* $\mathbb{Q}$. *arXiv e-prints*, page arXiv:2106.11141, 2021.

[28] Jeremy Rouse and David Zureick-Brown. *Elliptic curves over* $\mathbb{Q}$ *and 2-adic images of Galois. arXiv e-prints*, page arXiv:1402.5997, 2015.

[29] K. Rubin and A. Silverberg. *Families of elliptic curves with constant mod p representations.* In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 148–161. Int. Press, Cambridge, MA, 1995.

[30] K. Rubin and A. Silverberg. *Mod 2 representations of elliptic curves. Proc. Amer. Math. Soc.*, 129(1):53–57, 2001.

[31] Martha Rzedowski–Calderon. *Conductor–Discriminant Formula for Global Function Fields.* `http://www.m-hikari.com/ija/ija-2011/ija-29-32-2011/villasalvadorIJA29-32-2011.pdf`, 2011.

[32] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves.* W. A. Benjamin, Inc., New York-Amsterdam, 1968. (McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute).

[33] Jean-Pierre Serre. *Propriétés Galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math.*, 15(4):259–331, 1972.

[34] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[35] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[36] Peter Stevenhagen. *Number rings.* `https://websites.math.leidenuniv.nl/algebra/ant.pdf`, 2020.

[37] David Zywina. *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$. arXiv e-prints*, page arXiv:1508.07660, 2015.

[38] David Zywina. *Possible indices for the Galois image of elliptic curves over $\mathbb{Q}$. arXiv e-prints*, page arXiv:1508.07663, 2015.