Entanglements of Galois Representations for Elliptic Curves over $\mathbb{Q}$:

Foundations and Future Directions

Alessandro Campanella

A Thesis
in the
Department of Mathematics

Presented in Partial Fulfillment of the Requirements
for the Degree of Master of Arts, Mathematics at

Concordia University
Montreal, Québec, Canada

August 2025

CONCORDIA UNIVERSITY
School of Graduate Studies

This is to certify that the thesis prepared

By: Campanella, Alessandro

Entitled: Entanglements of Galois Representations for Elliptic Curves over • : Foundations and Future Directions

and submitted in partial fulfillment of the requirements for the degree of

Master of Arts

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

_____ Chair
Dr. Chantal David

_____ Examiner

_____ Examiner

_____ Thesis Supervisor(s)
Dr. Giovanni Rosso

_____ Thesis Supervisor(s)
Dr. Carlo Pagano

Approved by _____
Dr. Lea Popovic Chair of Department or Graduate Program Director

_____
Dr. Pascale Sicotte Dean of Faculty of Arts & Science

Abstract

Entanglements of Galois Representations for Elliptic Curves over $\mathbb{Q}$: Foundations and Future Directions
Alessandro Campanella

This thesis investigates the non-surjectivity of adelic Galois representations associated with elliptic curves over $\mathbb{Q}$, a phenomenon explained by two forms of entanglement. We introduce and differentiate between vertical and horizontal entanglements, providing a group-theoretic perspective on the latter. We also develop the concept of 'entanglement networks', diagrams derived from a theorem on field intersections, which offer a framework for analyzing these phenomena and suggest avenues for future combinatorial and cryptographic study. Computationally, we address the classification of potential mod-n Galois images by providing SageMath code to compute all applicable subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ for any n. Further SageMath implementations are presented to compute relevant entanglements for a given elliptic curve, utilizing data from the LMFDB database. Finally, we present a theorem providing conditions for the surjectivity of mod-n Galois representations, linking it to the surjectivity of mod-p representations for prime factors p of n and a constant related to Serre's work.

Acknowledgements

I wish to express my deepest gratitude to my supervisors, Dr. Carlo Pagano and Dr. Giovanni Rosso. Their patience and guidance throughout this research journey have been invaluable. I am immensely thankful for their mentorship, which has been instrumental in shaping this thesis and my development as a researcher.

My heartfelt thanks also go to my family and my girlfriend, Laura. Though the intricacies of my research remained a mystery to them, their unwavering support, encouragement, and consistent inquiries about my progress provided a constant source of strength and motivation.

Perhaps the richest and most transformative part of my time as a Master's student was the opportunity to meet and collaborate with an incredible group of peers from around the world: Alex, Antonio, Devang, Fadia, Francesco, Jalal, Leonardo, Michael, Mohammad, Nikol, Paola, Semwell and Dr. Sébastien Darses. I learned so much about myself, human nature, and indeed mathematics, by being surrounded by such a unique, intelligent, and supportive team. They were always generous with their time, willing to answer my questions (no matter how trivial!), and the camaraderie we shared was truly special. Amidst the hard work, our shared laughter and moments of goofing off created lasting memories and forged friendships that I will always cherish. I eagerly look forward to the day our departmental adventures inspire that long-promised sitcom!

This journey would not have been the same without each of these individuals, and this thesis is as much a testament to their support as it is to my own efforts.

Contents

List of Figures

Introduction

For an elliptic curve E defined over the field of rational numbers $\mathbb{Q}$, the set of its n-torsion points, $E[n]$, forms a $\mathbb{Z}/n\mathbb{Z}$-module isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. The action of the absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on these points gives rise to a family of Galois representations:

$$\rho_{E,n} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

These representations can be collected into the adelic Galois representation $\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$, which encodes the entire Galois action on the torsion subgroup of E. The image of this representation, a subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, holds a wealth of arithmetic information about the curve.

For an elliptic curve without complex multiplication (non-CM), the foundational Open Image Theorem of Serre [1] states that the image of ρ_E is always an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and thus has finite index. Serre also proved that for any elliptic curve over $\mathbb{Q}$, this index is always greater than 1, meaning the representation is never surjective. The reasons for this non-surjectivity are explained by phenomena known as "entanglements", which can be broadly divided into two types. *Vertical entanglement* occurs when the ℓ-adic component of the representation, ρ_{E,ℓ^∞}, is non-surjective for some prime ℓ. *Horizontal entanglement* occurs when the adelic image is not the full direct product of its ℓ-adic images, a situation arising from non-trivial intersections between torsion fields of coprime level.

This thesis investigates these phenomena from both a theoretical and computational standpoint. We present a group-theoretic framework to analyze the structure of Galois images and provide tools to explicitly compute and interpret entanglements. One of the central results presented in this work is a theorem that provides a practical criterion for the surjectivity of mod-n Galois representations, linking it to the surjectivity of the constituent mod-p representations and a constant related to Serre's work. A key theoretical contribution is the concept of "entanglement networks", which are diagrams derived from a theorem on field intersections. These networks provide a visual and structural framework for analyzing entanglement phenomena and suggest new avenues for future combinatorial and cryptographic investigation. Computationally, this thesis addresses the problem of classifying potential Galois images by providing a concrete algorithm, implemented in SageMath, to construct all "applicable subgroups" of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ for any given integer n. We further present SageMath implementations to compute entanglement data for specific elliptic curves, leveraging the extensive resources of the LMFDB database.

The thesis is structured as follows.

- **Chapter 1** provides the necessary foundations in algebra, reviewing key concepts from Galois theory, field theory, and the theory of profinite groups, culminating in an overview of infinite Galois theory.

- **Chapter 2** introduces the main objects of study: elliptic curves and their associated Galois representations. We cover the geometry of elliptic curves, the Weil pairing, the construction of Tate modules, and the formal definitions of the mod-n, ℓ-adic, and adelic representations.

- **Chapter 3** develops the group-theoretic tools that underpin the main results of this thesis. This chapter is dedicated to proving the necessary structural theorems about

subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ that are required for both the surjectivity criterion and the classification of applicable subgroups.

- **Chapter 4** is the heart of the thesis, where we apply these tools to the study of entanglements. We define the adelic level and index, and then systematically investigate vertical and horizontal entanglements. We present a group-theoretic interpretation of horizontal entanglement and use a field-theoretic degree formula to analyze its size. This culminates in the introduction of entanglement networks, which we illustrate with detailed case studies. The chapter concludes by presenting a new criterion for constructing integers whose associated torsion fields are unentangled.

- Finally, the **Appendix** contains the complete SageMath code for the algorithms developed in this thesis, including the construction of applicable subgroups and the computation of entanglement data.

1. Foundations in Algebra: Galois Theory, Fields and Profinite Groups

This chapter lays the algebraic groundwork necessary for understanding the subsequent material on elliptic curves and their Galois representations. We will review key concepts from Galois theory, field theory, and the theory of profinite groups.

1.1. Galois Theory

We briefly recall the essential definitions and results from Galois theory needed for our discussion. For a more comprehensive treatment, see [2]. Throughout, let K be a field and $\overline{K}$ a fixed algebraic closure of K.

Definition 1.1.1 (Automorphism Group)**.** *Let L/K be a field extension. The automorphism group of L over K is the group of field automorphisms of L that fix every element of K:*

$$\mathrm{Aut}(L/K) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma(x) = x \text{ for all } x \in K\}.$$

Definition 1.1.2 (Separability)**.** *An irreducible polynomial $f(X) \in K[X]$ is separable if it has distinct roots in $\overline{K}$. An element $\alpha \in L$, where L/K is an algebraic extension, is separable over K if its minimal polynomial over K is separable. The extension L/K is separable if every element $\alpha \in L$ is separable over K.*

Remark 1.1.1. *In characteristic 0, all irreducible polynomials and all algebraic extensions are separable. In characteristic $p > 0$, issues arise only for inseparable polynomials like $X^p - t$ over $\mathbb{F}_p(t)$.*

Definition 1.1.3 (Normality)**.** *An algebraic extension L/K is called normal if it satisfies the following equivalent conditions:*

(a) Every irreducible polynomial in $K[X]$ that has at least one root in L splits completely into linear factors in $L[X]$.

(b) L is the splitting field over K for some family of polynomials in $K[X]$.

(c) For every K-embedding $\sigma : L \hookrightarrow \overline{K}$, the image $\sigma(L)$ is equal to L.

The key concept connecting field extensions and group theory is that of a Galois extension.

Theorem 1.1.1 (Characterization of Galois Extensions)**.** *For a finite field extension L/K, the following conditions are equivalent:*

(a) L/K is separable and normal.

(b) L is the splitting field over K of a separable polynomial in $K[X]$.

(c) The fixed field of the automorphism group $\mathrm{Aut}(L/K)$ is precisely K, i.e., $L^{\mathrm{Aut}(L/K)} = K$.

(d) The order of the automorphism group equals the degree of the extension, i.e., $|\mathrm{Aut}(L/K)| = [L : K]$.

Definition 1.1.4 (Galois Extension)**.** *A finite field extension L/K satisfying the equivalent conditions of above is called a Galois extension. In this case, the group* $\mathrm{Aut}(L/K)$ *is called the Galois group of L over K, denoted by* $\mathrm{Gal}(L/K)$*. Its order is* $|\mathrm{Gal}(L/K)| = [L : K]$*.*

Definition 1.1.5 (Fixed Field)**.** *Let L be a field and let H be a subgroup of* $\mathrm{Aut}(L)$*. The fixed field of H is the subfield*

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

If L/K is Galois, then $L^{\mathrm{Gal}(L/K)} = K$.

Example 1.1.1 (Quadratic Extensions)**.** *If* $\mathrm{Char}(K) \neq 2$*, any quadratic extension L/K is Galois. Such an extension can be written as $L = K(\sqrt{d})$ for some $d \in K$ which is not a square in K. L is the splitting field of the separable polynomial $X^2 - d \in K[X]$. The Galois group* $\mathrm{Gal}(L/K)$ *has order $[L : K] = 2$. The non-identity element σ is determined by $\sigma(\sqrt{d}) = -\sqrt{d}$.*

Example 1.1.2 (Cyclotomic Extensions)**.** *For $n \geq 1$, the n-th cyclotomic field $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n-th root of unity, is a Galois extension of $\mathbb{Q}$. Its Galois group is isomorphic to the group of units modulo n, $(\mathbb{Z}/n\mathbb{Z})^\times$. An automorphism σ_a corresponding to $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ is defined by $\sigma_a(\zeta_n) = \zeta_n^a$.*

Theorem 1.1.2 (Subextensions)**.** *If L/K is a finite Galois extension and F is an intermediate field ($K \subseteq F \subseteq L$), then the extension L/F is also Galois. (Note: F/K is not necessarily Galois).*

The cornerstone of the theory is the relationship between the structure of the Galois group and the structure of the intermediate fields.

Theorem 1.1.3 (Fundamental Theorem of Galois Theory)**.** *Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Let $\mathcal{F}$ be the set of intermediate fields F such that $K \subseteq F \subseteq L$, and let $\mathcal{G}$ be the set of subgroups H of G. There is an inclusion-reversing bijection between $\mathcal{F}$ and $\mathcal{G}$ given by the maps:*

$$\begin{aligned} \Phi : \mathcal{F} &\to \mathcal{G} & \qquad \Psi : \mathcal{G} &\to \mathcal{F} \\ F &\mapsto \mathrm{Gal}(L/F) & \qquad H &\mapsto L^H \end{aligned}$$

These maps are inverses ($\Psi \circ \Phi = \mathrm{id}_{\mathcal{F}}$, $\Phi \circ \Psi = \mathrm{id}_{\mathcal{G}}$) and satisfy the following properties for corresponding pairs $F \leftrightarrow H$ (i.e., $H = \mathrm{Gal}(L/F)$ and $F = L^H$):

(a) $|H| = [L : F]$ *and* $[G : H] = [F : K]$*.*

(b) Let F and F' be two intermediate fields of the extension, and let H and H' be their corresponding subgroups in G. The intermediate fields F and F' are isomorphic over K if and only if H and H' are conjugate subgroups of G. In particular, for any $\sigma \in G$,

$$\mathrm{Gal}(L/\sigma(F)) = \sigma \,\mathrm{Gal}(L/F)\sigma^{-1}.$$

(c) The extension F/K is Galois if and only if the corresponding subgroup $H = \mathrm{Gal}(L/F)$ is a normal subgroup of G ($H \triangleleft G$). If F/K is Galois, then the restriction map $\sigma \mapsto \sigma|_F$ induces an isomorphism

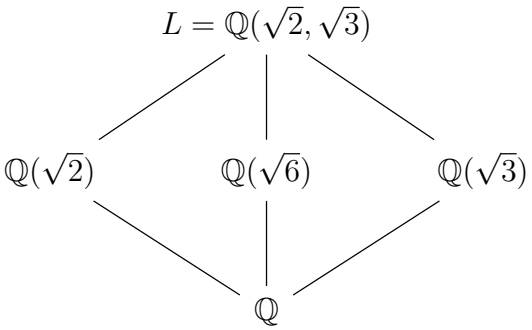
$$G/H \cong \mathrm{Gal}(F/K).$$

Example 1.1.3 (Illustration of FTGT)**.** *Consider the extension $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $K = \mathbb{Q}$. This is the splitting field of $(X^2-2)(X^2-3)$, hence it is Galois. The degree is $[L : \mathbb{Q}] = 4$. The Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to the Klein four-group $V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let σ and τ be the automorphisms defined by:*

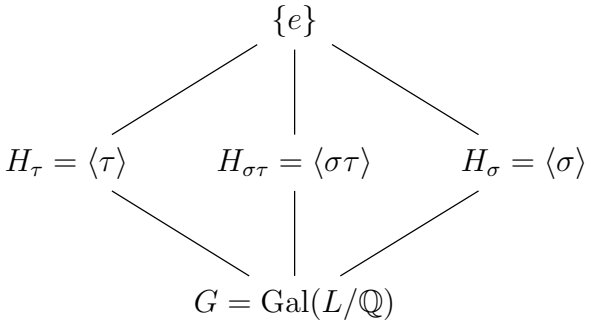
$$\sigma(\sqrt{2}) = -\sqrt{2}, \qquad \sigma(\sqrt{3}) = \sqrt{3}$$
$$\tau(\sqrt{2}) = \sqrt{2}, \qquad \tau(\sqrt{3}) = -\sqrt{3}$$

Then $G = \{e, \sigma, \tau, \sigma\tau\}$. The intermediate fields and corresponding subgroups are shown below.

Lattice of Subfields:



Lattice of Subgroups:



The Galois correspondence ($F \leftrightarrow H = \mathrm{Gal}(L/F)$) is:

- $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \longleftrightarrow \{e\}$
- $\mathbb{Q}(\sqrt{2}) \longleftrightarrow H_\tau = \{e, \tau\}$
- $\mathbb{Q}(\sqrt{3}) \longleftrightarrow H_\sigma = \{e, \sigma\}$
- $\mathbb{Q}(\sqrt{6}) \longleftrightarrow H_{\sigma\tau} = \{e, \sigma\tau\}$ *(since $\sigma\tau$ fixes $\sqrt{6} = \sqrt{2}\sqrt{3}$)*
- $\mathbb{Q} \longleftrightarrow G$

Note that all subgroups of G are normal (since G is abelian), corresponding to the fact that all intermediate fields $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$, and $\mathbb{Q}(\sqrt{6})/\mathbb{Q}$ are Galois extensions.

The following proposition, particularly part (b) concerning the condition for the Galois group of a compositum to be the direct product of individual Galois groups, will be crucial in our later analysis of horizontal entanglements.

Proposition 1.1.1. *Let L_1 and L_2 be finite Galois extensions of K.*

(a) There is an injective homomorphism

$$\phi : \mathrm{Gal}(L_1L_2/K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$$

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

(b) The embedding ϕ *is an isomorphism if and only if* $L_1 \cap L_2 = K$. *In particular,*

$$[L_1L_2 : K] = [L_1 : K][L_2 : K]$$

if and only if $L_1 \cap L_2 = K$.

Proof. (a) First, note that a composite of Galois extensions is Galois [3, Section 14.4, Proposition 21], so L_1L_2/K is Galois.

Any $\sigma \in \mathrm{Gal}(L_1L_2/K)$ restricted to L_1 or L_2 is an automorphism of that subfield. This holds because L_1 and L_2 are both Galois over K and, in particular, normal extensions. As a result, we can define a map

$$\phi : \mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$$

by sending $\sigma \mapsto (\sigma|_{L_1}, \sigma|_{L_2})$. We will now show that ϕ is an injective homomorphism.

To show ϕ is a homomorphism, it suffices to show that the component maps $\phi_i : \mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_i/K)$ given by $\phi_i(\sigma) = \sigma|_{L_i}$ are homomorphisms for $i = 1, 2$. Let $\sigma, \tau \in \mathrm{Gal}(L_1L_2/K)$ and let $\alpha \in L_1$. Then

$$(\sigma\tau)|_{L_1}(\alpha) = (\sigma\tau)(\alpha) = \sigma(\tau(\alpha)).$$

Since L_1/K is Galois, we know $\tau(\alpha) \in L_1$. Therefore,

$$\sigma(\tau(\alpha)) = \sigma|_{L_1}(\tau(\alpha)).$$

Furthermore, since $\alpha \in L_1$, we have $\tau(\alpha) = \tau|_{L_1}(\alpha)$. Thus,

$$\sigma|_{L_1}(\tau(\alpha)) = \sigma|_{L_1}(\tau|_{L_1}(\alpha)) = (\sigma|_{L_1} \circ \tau|_{L_1})(\alpha).$$

Combining these, we have shown $(\sigma\tau)|_{L_1}(\alpha) = (\sigma|_{L_1} \circ \tau|_{L_1})(\alpha)$ for all $\alpha \in L_1$. This means the functions are equal:

$$(\sigma\tau)|_{L_1} = \sigma|_{L_1} \circ \tau|_{L_1}.$$

The proof that $(\sigma\tau)|_{L_2} = \sigma|_{L_2} \circ \tau|_{L_2}$ is identical.

To show injectivity, consider the kernel of ϕ. Suppose $\sigma \in \ker(\phi)$ then $\phi(\sigma) = (\sigma|_{L_1}, \sigma|_{L_2}) = (e_{L_1}, e_{L_2})$. This means that σ fixes every element of L_1 and every element of L_2. Any automorphism fixing all elements in L_1 and L_2 must fix all elements in L_1L_2. Therefore, σ must be the identity automorphism on L_1L_2. The kernel of ϕ is thus trivial, which proves that ϕ is injective.

(b) Because ϕ is injective, ϕ is an isomorphism if and only if $[L_1L_2 : K] = [L_1 : K][L_2 : K]$, or equivalently, by the tower law, $[L_1L_2 : L_2] = [L_1 : K]$. We will show this equality occurs if and only if $L_1 \cap L_2 = K$.

We compare the Galois groups corresponding to these degrees to compare $[L_1L_2 : L_2]$ and $[L_1 : K]$. Consider the restriction homomorphism:

$$\Phi : \mathrm{Gal}(L_1L_2/L_2) \to \mathrm{Gal}(L_1/K)$$

sending $\sigma \mapsto \sigma|_{L_1}$. Any automorphism σ in the kernel of Φ fixes L_1 and fixes L_2. Thus, σ fixes the composite field L_1L_2, meaning σ is the identity automorphism. The kernel is therefore trivial, and Φ is injective.

The fact that the image of a group homomorphism is a subgroup of its codomain and the Fundamental Theorem of Galois Theory tells us that the image of Φ is of the form $\mathrm{Gal}(L_1/E)$ for some intermediate field E with $K \subseteq E \subseteq L_1$. The field E is the fixed field $L_1^{\mathrm{Im}(\Phi)}$, which consists of the elements of L_1 fixed by $\mathrm{Im}(\Phi) = \{\sigma|_{L_1} \mid \sigma \in \mathrm{Gal}(L_1L_2/L_2)\}$. An element $\alpha \in L_1$ is fixed by all such $\sigma|_{L_1}$ if and only if $\sigma(\alpha) = \alpha$ for all $\sigma \in \mathrm{Gal}(L_1L_2/L_2)$. An element of L_1L_2 is fixed by $\mathrm{Gal}(L_1L_2/L_2)$ if and only if it lies in L_2. So, we are looking for elements $\alpha \in L_1$ that also lie in L_2. Thus, the fixed field is $E = L_1 \cap L_2$.

Hence, $\mathrm{Im}(\Phi) = \mathrm{Gal}(L_1/(L_1 \cap L_2))$ and the injectivity of Φ provides an isomorphism:

$$\mathrm{Gal}(L_1L_2/L_2) \cong \mathrm{Gal}(L_1/(L_1 \cap L_2)).$$

Comparing the orders of these groups which equal the degrees of the corresponding field extensions:

$$[L_1L_2 : L_2] = [L_1 : L_1 \cap L_2].$$

This degree $[L_1 : L_1 \cap L_2]$ is equal to $[L_1 : K]$ if and only if $L_1 \cap L_2 = K$. Therefore, the condition $[L_1L_2 : L_2] = [L_1 : K]$ which is equivalent to ϕ being an isomorphism holds if and only if $L_1 \cap L_2 = K$.

□

1.2. Field Theory

This section presents several miscellaneous results, primarily from Field Theory. The opening result, however, is group-theoretic; it is included here because it is instrumental in proving a subsequent field-theoretic statement within this collection. These results are specifically gathered for their application in our later section on horizontal entanglements in terms of group theory.

Lemma 1.2.1 (Dedekind's Modular Law)**.** *Let H, K, L be subgroups of a group and assume that $K \subseteq L$. Then $(HK) \cap L = (H \cap L)K$.*

Proof. The proof was taken from [4, Result 1.3.14]. In the first place $(H \cap L)K \subseteq HK$ and $(H \cap L)K \subseteq LK = L$: hence $(H \cap L)K \subseteq (HK) \cap L$. Conversely let $x \in (HK) \cap L$ and write $x = hk$, $(h \in H, k \in K)$: then $h = xk^{-1} \in LK = L$, so that $h \in H \cap L$. Hence $x \in (H \cap L)K$. □

Proposition 1.2.1 (Modular Law for Galois Extensions)**.** *Let H, K, L be finite Galois extensions for some base field F and assume that $K \subseteq L$. Then $(HK) \cap L = (H \cap L)K$.*

Proof. First note that the compositum HKL is Galois over F by [3, Chapter 14, Proposition 21]. So $(HK) \cap L$ and $(H \cap L)K$ are intermediate fields between F and HKL. By the Galois correspondence, proving $(HK) \cap L = (H \cap L)K$ is equivalent to proving

$$\mathrm{Gal}(HKL/((H \cap L)K)) = \mathrm{Gal}(HKL/((HK) \cap L)).$$

Let $M = HKL$. We define the following corresponding Galois groups:

$$G_H := \mathrm{Gal}(M/H)$$
$$G_K := \mathrm{Gal}(M/K)$$
$$G_L := \mathrm{Gal}(M/L)$$

Staying consistent with this notation and using [2, Theorem 5.13], we obtain the groups corresponding to the relevant field constructions:

- Field: $H \cap L \quad \longleftrightarrow \quad$ Group: $\mathrm{Gal}(M/(H \cap L)) = \langle G_H, G_L \rangle$
- Field: $(H \cap L)K \quad \longleftrightarrow \quad$ Group: $\mathrm{Gal}(M/((H \cap L)K)) = \langle G_H, G_L \rangle \cap G_K$
- Field: $HK \quad \longleftrightarrow \quad$ Group: $\mathrm{Gal}(M/HK) = G_H \cap G_K$
- Field: $(HK) \cap L \quad \longleftrightarrow \quad$ Group: $\mathrm{Gal}(M/((HK) \cap L)) = \langle G_H \cap G_K, G_L \rangle$

Using the above, the statement we are trying to prove (equality of Galois groups) becomes

$$\langle G_H, G_L \rangle \cap G_K = \langle G_H \cap G_K, G_L \rangle.$$

Let $G := \mathrm{Gal}(M/F)$. Since H, K, L are finite Galois extensions of F, their corresponding groups G_H, G_K, G_L are normal subgroups of G (i.e., $G_H \triangleleft G$, $G_K \triangleleft G$, $G_L \triangleleft G$).

We now claim that $\langle G_H, G_L \rangle = G_H G_L$ and $\langle G_H \cap G_K, G_L \rangle = (G_H \cap G_K)G_L$. This claim is true if and only if $G_H G_L$ and $(G_H \cap G_K)G_L$ are subgroups, which in turn is true if and only if $G_H G_L = G_L G_H$ and $(G_H \cap G_K)G_L = G_L(G_H \cap G_K)$ respectively [3, Chapter 3, Proposition 14]. The proof of our claim is as follows:

- Since L/F is Galois, $G_L \triangleleft G$. Therefore, any subgroup of G normalizes G_L. In particular, G_H (being a subgroup of G) normalizes G_L. Thus, $G_H G_L = G_L G_H$, which implies $\langle G_H, G_L \rangle = G_H G_L$.
- Similarly, $G_H \cap G_K$ normalizes G_L. Thus, $(G_H \cap G_K)G_L = G_L(G_H \cap G_K)$, which implies $\langle G_H \cap G_K, G_L \rangle = (G_H \cap G_K)G_L$.

The statement to prove now becomes

$$(G_H G_L) \cap G_K = (G_H \cap G_K)G_L.$$

By the Galois correspondence, the field inclusion $K \subseteq L$ implies the group inclusion $G_L \subseteq G_K$. We can now apply Dedekind's Modular Law for groups to the subgroups G_H, G_L, and G_K of G to obtain

$$(G_H G_L) \cap G_K = (G_H \cap G_K)G_L.$$

This is precisely the group equality we needed to show, which completes the proof. □

Proposition 1.2.2. *Let M, L, K be finite Galois extensions for some base field F and assume that $K \subseteq L$. Then $M \cap L \subseteq K$ if and only if $MK \cap L = ML \cap K$.*

Proof. Since $K \subseteq L$, we have that $K \subseteq ML$ and as a result $K \subseteq ML \cap K$. Conversely $ML \cap K$ is contained in K so we have that $ML \cap K = K$. The statement we wish to prove is show $M \cap L \subseteq K$ if and only if $MK \cap L = K$ given our assumptions.

Suppose that $M \cap L \subseteq K$. Since $K \subseteq MK$ and $K \subseteq L$ we have that $K \subseteq MK \cap L$. On the other hand, $MK \cap L = (M \cap L)K \subseteq KK = K$, where the equality follows from the previous Proposition and the containment follows from our assumption. Thus, $MK \cap L = K$.

Conversely, suppose that $MK \cap L = K$. Let x be an element of $M \cap L$. In particular, x is an element of $M \subseteq MK$ and also $x \in L$. Thus, $x \in MK \cap L = K$. □

Proposition 1.2.3. *Let M, L, K be finite field extensions over the same base field F. Then $LK \cap M = (L \cap M)(K \cap M)$ if and only if $(LK \setminus (L \cup K)) \cap M \subseteq (L \cap M)(K \cap M)$.*

Proof. First note that $LK \cap M = ((LK \setminus (L \cup K)) \cap M) \cup (L \cap M) \cup (K \cap M)$. Suppose first that $LK \cap M = (L \cap M)(K \cap M)$. Then $(L \cap M)(K \cap M) = ((LK \setminus (L \cup K)) \cap M) \cup (L \cap M) \cup (K \cap M)$. Therefore we must have that $(LK \setminus (L \cup K)) \cap M \subseteq (L \cap M)(K \cap M)$.

Conversely, suppose that $(LK \setminus (L \cup K)) \cap M \subseteq (L \cap M)(K \cap M)$. We know that $(L \cap M) \cup (K \cap M) \subseteq (L \cap M)(K \cap M)$ so $((LK \setminus (L \cup K)) \cap M) \cup (L \cap M) \cup (K \cap M) \subseteq (L \cap M)(K \cap M)$ which implies that $LK \cap M \subseteq (L \cap M)(K \cap M)$. We now want to show that $(L \cap M)(K \cap M) \subseteq LK \cap M$. $L \cap M \subseteq LK \cap M$ and $K \cap M \subseteq LK \cap M$ and so $(L \cap M)(K \cap M) \subseteq LK \cap M$ as $LK \cap M$ is a field that contains both those fields so it contains their compositum. Finally, $(L \cap M)(K \cap M) = LK \cap M$. □

Remark 1.2.1. *It is important to note that the proposition establishes an equivalence between an equality of fields and a set-theoretic inclusion.*

Let us recall a few well-known facts from algebraic number theory without proof.

Lemma 1.2.2. *(a) Let p be an odd prime. Then $\sqrt{\epsilon \cdot p} \in \mathbb{Q}(\zeta_p)$ where $\epsilon = (-1)^{(p-1)/2}$. In particular, $\sqrt{p} \in \mathbb{Q}(\zeta_p)$ if $p \equiv 1 \pmod 4$, and $\sqrt{-p} \in \mathbb{Q}(\zeta_p)$ if $p \equiv 3 \pmod 4$.*

(b) $\mathbb{Q}(\zeta_8)$ contains $\sqrt{2}$, $\sqrt{-2}$, and i.

(c) Let $n, m > 1$ be integers. Then the compositum $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{\mathrm{lcm}(n,m)})$.

The following proposition will be instrumental when we later demonstrate that the adelic Galois representation is never surjective for an elliptic curve over $\mathbb{Q}$.

Proposition 1.2.4. *Let $n \in \mathbb{Z}$, $n \neq 0$, be square-free. Then:*

(a) $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta_{|n|})$ if $n \equiv 1 \pmod 4$.

(b) $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta_{4|n|})$ if $n \equiv 2 \pmod 4$ or $n \equiv 3 \pmod 4$.

Proof. First let us suppose that $n \equiv 1 \pmod 4$. As n is square-free, $n = \pm p_1 p_2 \dots p_k$ with p_i distinct odd primes (The latter also hods if $n \equiv 3 \pmod 4$). We claim that $\sqrt{n} = \prod_{1 \leq i \leq k} \sqrt{\varepsilon_i p_i} = \sqrt{\prod_{1 \leq i \leq k} \varepsilon_i} \cdot \sqrt{\prod_{1 \leq i \leq k} p_i}$. If the claim were true, then $\sqrt{n} \in \mathbb{Q}(\zeta_{p_1})\mathbb{Q}(\zeta_{p_2}) \dots \mathbb{Q}(\zeta_{p_k}) = \mathbb{Q}(\zeta_{|n|})$ by Lemma 1.2.2 part (a) and (c). The goal is to prove our claim for $n \equiv 1 \pmod 4$ and $n \equiv 3 \pmod 4$. The case where $n \equiv 2 \pmod 4$ will then be addressed by reducing it to one of these preceding cases.

- Suppose that n is positive. Then $n = p_1 \dots p_k \equiv 1 \pmod 4$, which means that the number of p_i such that $p_i \equiv 3 \pmod 4$ (where $\varepsilon_i = -1$) is even. This further implies that $\prod_{1 \le i \le k} \varepsilon_i = 1$. Thus $\sqrt{n} = \sqrt{\prod p_i} = \sqrt{1 \cdot \prod p_i} = \sqrt{(\prod \varepsilon_i) \prod p_i} = \prod_{1 \le i \le k} \sqrt{\varepsilon_i p_i}$.
- Suppose now that n is negative. Then $n = -|n|$, and $-|n| \equiv 1 \pmod 4$, meaning $|n| \equiv 3 \pmod 4$. And so $|n| = p_1 \dots p_k \equiv 3 \pmod 4$ implies that the number of p_i such that $p_i \equiv 3 \pmod 4$ (where $\varepsilon_i = -1$) is odd. Therefore, $\prod_{1 \le i \le k} \varepsilon_i = -1$. Then $\sqrt{n} = \sqrt{-|n|} = \sqrt{(\prod \varepsilon_i) \prod p_i} = \prod_{1 \le i \le k} \sqrt{\varepsilon_i p_i}$.

Thus, for $n \equiv 1 \pmod 4$, we have that $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta_{|n|})$.

Let us suppose that $n \equiv 3 \pmod 4$. Then we can use a similar argument as above to show that $\sqrt{-n} \in \mathbb{Q}(\zeta_{|n|})$.

- Suppose n is positive. Knowing that $n = p_1 \dots p_k \equiv 3 \pmod 4$, we can infer that there are an odd number of primes p_i such that $p_i \equiv 3 \pmod 4$ (where $\varepsilon_i = -1$). Thus, $\prod_{1 \le i \le k} \varepsilon_i = -1$. Then $\sqrt{-n} = \sqrt{(-1) \prod p_i} = \sqrt{(\prod \varepsilon_i) \prod p_i} = \prod_{1 \le i \le k} \sqrt{\varepsilon_i p_i} \in \mathbb{Q}(\zeta_{|n|})$.
- Suppose that n is negative. Then $n = -|n|$, so $-|n| \equiv 3 \pmod 4$, which implies $|n| \equiv 1 \pmod 4$. This means there are an even number of primes p_i (in the factorization of $|n|$) such that $p_i \equiv 3 \pmod 4$. And, $\prod_{1 \le i \le k} \varepsilon_i = 1$. Then $\sqrt{-n} = \sqrt{|n|} = \sqrt{\prod p_i} = \sqrt{(\prod \varepsilon_i) \prod p_i} = \prod_{1 \le i \le k} \sqrt{\varepsilon_i p_i} \in \mathbb{Q}(\zeta_{|n|})$.

As $\sqrt{-1} \in \mathbb{Q}(\zeta_4)$, we get $\sqrt{n} = \sqrt{-1}\sqrt{-n} \in \mathbb{Q}(\zeta_4)\mathbb{Q}(\zeta_{|n|}) = \mathbb{Q}(\zeta_{4|n|})$ (since $|n|$ is odd when $n \equiv 3 \pmod 4$).

Finally, if $n \equiv 2 \pmod 4$, then $n = 2m$ with m odd and square-free, so $m \equiv 1$ or $3 \pmod 4$. In either case using the results above for m, we get $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(\zeta_{4|m|}) \subseteq \mathbb{Q}(\zeta_{4|n|})$ where the last inclusion comes from $m \mid n$. As $8 \mid 4|n|$ (since $|n|$ is even), we get $\mathbb{Q}(\zeta_8) \subseteq \mathbb{Q}(\zeta_{4|n|})$. Moreover, $\sqrt{2} \in \mathbb{Q}(\zeta_8)$, so $\sqrt{2} \in \mathbb{Q}(\zeta_{4|n|})$. Thus, $\sqrt{n} = \sqrt{2}\sqrt{m} \in \mathbb{Q}(\zeta_{4|n|})$. □

1.3. Profinite Groups

This section is dedicated to presenting several results about profinite groups which are instrumental for understanding Galois representations of elliptic curves. The definitions, theorems, and propositions in this section are taken from the lecture notes [5].

Definition 1.3.1. *A poset $(J, \preceq)$ is an inverse system if for any $i, j \in J$ there is some $k \in J$ such that $i \preceq k$ and $j \preceq k$.*

An inverse system of groups consists of an inverse system $(J, \preceq)$ and a collection of groups indexed by J such that whenever $i \preceq j$, we have some homomorphism $\phi_{ji} : G_j \to G_i$ such that $\phi_{ii} = \mathrm{id}_{G_i}$ and $\phi_{ji} \circ \phi_{kj} = \phi_{ki}$ when $i \preceq j \preceq k$. The abbreviation for the notion of the inverse system of groups is as follows: $(G_j)_{j \in J}$. The maps ϕ_{ji} are called transition maps.

We will state the following proposition to define the inverse limit of an inverse system of groups.

Proposition 1.3.1. *Let $(G_j)_{j \in J}$ be an inverse system of groups. Then the inverse limit of $(G_j)_{j \in J}$ exists, and is given by*

$$\varprojlim G_j = \{(g_j)_{j \in J} \in \prod_{j \in J} G_j \mid \phi_{ji}(g_j) = g_i \text{ for all } i \preceq j\}.$$

The inverse limit of an inverse system of groups comes equipped with the maps $p_i : \varprojlim G_j \to G_i$ such that $p_i = \phi_{ji} \circ p_j$ when $i \preceq j$.

Definition 1.3.2. *A profinite group is the inverse limit of an inverse system of finite groups.*

The explicit description of an inverse limit in the proposition above allows us to define a topology on a profinite group. Let's now recall the basis for the discrete and product topology, as we will invoke both topologies when we define the topology of a profinite group.

In the discrete topology on a set X, every subset of X is open. Therefore, the basis for the discrete topology is simply the set of all singletons: $\mathcal{B} = \{\{x\} \mid x \in X\}$. This is because any subset of X can be written as a union of singletons, and thus is open.

The product topology on $X = \prod_{j \in J} X_j$ has basis

$$\{\prod_{j \in J} U_j \mid U_j \subseteq X_j \text{ is open and } U_i = X_i \text{ for all but finitely many } i\}$$

Notice that the box and product topologies are the same if the indexing set is finite.

Definition 1.3.3. *Let $(G_j)_{j \in J}$ be an inverse system of finite groups. Endow each G_j with the discrete topology, and give $\prod_{j \in J} G_j$ the product topology. The topology on $\varprojlim G_j \subseteq \prod_{j \in J} G_j$ is the subspace topology.*

Remark 1.3.1. *By Tychonoff's Theorem, $\prod_{j \in J} G_j$ is compact and Hausdorff. Each condition $\phi_{ij}(g_i) = g_j$ describes a closed subset of $\prod_{j \in J} G_j$, and the intersection of all these subsets is $\varprojlim G_j$. Thus, the inverse limit, endowed with the subspace topology, is a closed subspace of $\prod_{j \in J} G_j$. Note that $\varprojlim G_j$ is thus a compact Hausdorff space.*

Definition 1.3.4. *A topological group is a group G endowed with a topology such that the multiplication and inversion maps are continuous.*

A profinite group endowed with the topology above is a topological group.

Proposition 1.3.2. *Let $f : H \to G$ be a homomorphism from a topological group to a finite group (equipped with the discrete topology). Then f is continuous if and only if $\ker(f)$ is an open subgroup of H.*

Proof. Since $\{e\}$ is an open subset in the discrete topology on G, if f is continuous, then $\ker(f) = f^{-1}(\{e\})$ is open.

Conversely, suppose $f^{-1}(\{e\})$ is open. Let U be an open set in G, i.e., a subset of G since it has the discrete topology. If U is empty, then $f^{-1}(U)$ is empty, which is open. If U is not empty, then for each $g \in U$, $f^{-1}(\{g\})$ is either empty (open) or $f^{-1}(\{g\}) = h \cdot f^{-1}(\{e\})$ where $h \in H$ such that $f(h) = g$. Moreover, $f^{-1}(\{g\})$ is open because translations of open sets are open since left (or right) multiplication is a homeomorphism. Finally, $f^{-1}(U) = \bigcup_{g \in U} f^{-1}(\{g\})$ is open since each $f^{-1}(\{g\})$ is open and the union of open sets is open. □

Proposition 1.3.3. *Let $\mathcal{G}$ be a compact topological group. A subgroup of $\mathcal{G}$ is open if and only if it has finite index and is closed.*

Proof. Let U be an open subgroup. We have $G = \bigcup_{g\in G} gU$, and each gU is open for similar reasons as stated in the proposition above, so $\bigcup_{g\in G} gU$ is an open cover of G. By compactness, it has a finite subcover, $G = g_1U \cup \cdots \cup g_nU$. The g_i form a finite set of coset representatives for U, which thus has a finite index in G. We also have that $U = G \setminus (g_1^{-1}g_2U \cup \cdots \cup g_1^{-1}g_nU)$ by multiplying both sides of $G = g_1U \cup \cdots \cup g_nU$ by g_1^{-1} and rearranging. The latter implies that U is the complement of an open set and, hence, is closed.

Conversely, suppose U has a finite index and is closed in G. Let $g_1, \ldots, g_n$ be the coset representatives of U in G, then $U = G \setminus (g_1^{-1}g_2U \cup \cdots \cup g_1^{-1}g_nU)$. And so, U is open because it's the complement of a closed set as the finite union of closed sets is closed, and homeomorphisms send closed sets to closed sets.

□

It is immediate from the definition of a profinite group $\mathcal{G} = \varprojlim G_j$ that $\mathcal{G}$ has a good supply of open subgroups: the kernels U_j of the maps $p_j : \mathcal{G} \to G_j$. In fact the topology of a profinite group is entirely governed by its open subgroups.

Proposition 1.3.4. *Let $(G_j)_{j\in J}$ be an inverse system of finite groups with inverse limit $\mathcal{G}$. The open subgroups $U_j = \ker(p_j : \mathcal{G} \to G_j)$ form a basis of open neighbourhoods of the identity in the sense that any open set $V \subseteq \mathcal{G}$ which contains the identity contains some U_j.*

Proof. Let V be an open subset of $\mathcal{G}$ containing the identity, $e_{\mathcal{G}}$. By definition of the product topology, V is a union of basic open sets of the form $p_{j_1}^{-1}(X_{j_1}) \cap \cdots \cap p_{j_n}^{-1}(X_{j_n})$ for some $j_1, \ldots, j_n \in J$ and $X_{j_i} \subseteq G_{j_i}$. Fix one such basic open set that contains the identity, then certainly $e_{j_i} \in X_{j_i}$ for each i as homomorphisms maps identity to identity. So we have

$$e_{\mathcal{G}} \in p_{j_1}^{-1}(\{e_{j_1}\}) \cap \cdots \cap p_{j_n}^{-1}(\{e_{j_n}\}) = U_{j_1} \cap \cdots \cap U_{j_n} \subseteq p_{j_1}^{-1}(X_{j_1}) \cap \cdots \cap p_{j_n}^{-1}(X_{j_n}) \subseteq V$$

The goal now is to turn the first intersection above into a single U_j. We achieve the latter by using the definition of an inverse system to find $k \in J$ such that $j_i \preceq k$ for all i. Since $p_{j_i} = \phi_{kj_i} \circ p_k$ where ϕ_{kj_i} is a transition map, we have $\ker(p_k) \subseteq \ker(p_{j_i})$ hence $U_k \subseteq U_{j_i}$ for all i, and $e_{\mathcal{G}} \in U_k \subseteq V$. □

Example 1.3.1. *Let $J = \mathbb{N}$ with the usual ordering. For each $n \in \mathbb{N}$, let $G_n = \mathbb{Z}/p^n\mathbb{Z}$, which is the cyclic group of order p^n. These are our finite groups.*

Now, for $n \leq m$, define the transition map ϕ_{mn} to be the reduction modulo p^n map. The following conditions: $\phi_{ii} = \mathrm{id}_{G_i}$ and $\phi_{ji} \circ \phi_{kj} = \phi_{ki}$ when $i \leq j \leq k$ are satisfied as the transition maps are surjective.

Thus, $(\mathbb{Z}/p^n\mathbb{Z})_{n\in\mathbb{N}}$ with the transition maps ϕ_{mn} forms an inverse system of finite groups. The inverse limit of this system is precisely the p-adic integers, $\mathbb{Z}_p$:

$$\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}.$$

Since each $\mathbb{Z}/p^n\mathbb{Z}$ is finite (and thus compact with the discrete topology), $\mathbb{Z}_p$ is a compact Hausdorff space by Tychonoff's theorem.

Example 1.3.2. *The profinite completion of $\mathbb{Z}$, denoted $\hat{\mathbb{Z}}$, is another example of profinite group.*

Let $J = \mathbb{N}$ ordered by divisibility (i.e., $i \preceq j$ if i divides j). For each $n \in \mathbb{N}$, let $G_n = \mathbb{Z}/n\mathbb{Z}$, which is the cyclic group of order n.

Now, for $m, n \in \mathbb{N}$ with $n|m$, define the transition map $\phi_{mn} : G_m \to G_n$ by the reduction modulo n map. The conditions for the latter to be an inverse system of groups are satisfied similarly as above.

Thus, $(\mathbb{Z}/n\mathbb{Z})_{n\in\mathbb{N}}$ with the transition maps ϕ_{mn} forms an inverse system of finite groups. The inverse limit of this system is precisely the profinite completion of $\mathbb{Z}$, denoted $\hat{\mathbb{Z}}$:

$$\hat{\mathbb{Z}} \cong \varprojlim \mathbb{Z}/n\mathbb{Z}.$$

The following theorem makes use of the previous two examples to produce a vital isomorphism that will play a crucial role in the section on Entanglements.

Theorem 1.3.1. *There is an isomorphism of topological rings*

$$\hat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p.$$

Example 1.3.3. *Matrix groups over $\mathbb{Z}_p$ and $\hat{\mathbb{Z}}$ provide interesting examples of profinite groups. For instance, consider the general linear group of degree N over the p-adic integers, denoted $GL_N(\mathbb{Z}_p)$. This group can be expressed as the inverse limit of matrix groups over finite rings:*

$$GL_N(\mathbb{Z}_p) = \varprojlim GL_N(\mathbb{Z}/p^n\mathbb{Z}).$$

Similarly, the general linear group over the profinite completion of $\mathbb{Z}$, denoted $GL_N(\hat{\mathbb{Z}})$, can be expressed as

$$GL_N(\hat{\mathbb{Z}}) = \varprojlim GL_N(\mathbb{Z}/n\mathbb{Z}) \cong \prod_p GL_N(\mathbb{Z}_p),$$

where the product is taken over all prime numbers p. These examples highlight how matrix groups with coefficients in profinite rings inherit a profinite structure.

1.4. Infinite Galois Theory

Finite Galois theory establishes a fundamental correspondence between intermediate fields of a finite Galois extension L/K and subgroups of the Galois group $\mathrm{Gal}(L/K)$. Infinite Galois theory seeks to extend this framework to extensions of infinite degree. We primarily follow the exposition in [6] and in [7, Chapter 7].

Definition 1.4.1 (Infinite Galois Extension)**.** *An algebraic field extension L/K is called Galois if it is normal and separable. This is equivalent to saying that L is the splitting field over K of some (possibly infinite) family of separable polynomials in $K[X]$. The Galois group is* $\mathrm{Gal}(L/K) = \mathrm{Aut}(L/K)$.

A naive attempt to directly generalize the Fundamental Theorem fails because the map from subgroups of $\mathrm{Gal}(L/K)$ to intermediate fields $F = L^H$ is generally not injective when $[L : K]$ is infinite. There can be distinct subgroups $H_1 \neq H_2$ such that $L^{H_1} = L^{H_2}$.

Example 1.4.1 (Cardinality Mismatch)**.** *Let $L = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \dots)$, the compositum of $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{p})$ for all primes p. Then $\mathrm{Gal}(L/\mathbb{Q}) \cong \prod_{p \text{ prime}} \{\pm 1\}$ (where the first component corresponds to $\sqrt{-1}$), a countable direct product of the group $\{\pm 1\}$. This is an abelian group where each non-identity element has order 2. The group $\mathrm{Gal}(L/\mathbb{Q})$ is uncountable as $|\mathrm{Gal}(L/\mathbb{Q})| = 2^{\aleph_0}$, so $\mathrm{Gal}(L/\mathbb{Q})$ has uncountably many subgroups of order 2. At the same time, L has only countably many subfields of each finite (2-power) degree over $\mathbb{Q}$, more precisely $\aleph_0$ many. Therefore the subfields of L and the subgroups of $\mathrm{Gal}(L/\mathbb{Q})$ do not have the same cardinality.*

The resolution, proposed by Krull (building on ideas of Dedekind), is to introduce a topology on the Galois group $\mathrm{Gal}(L/K)$. This *Krull topology* restricts the Galois correspondence to a bijection between intermediate fields and *closed* subgroups of $\mathrm{Gal}(L/K)$.

The intuition behind the topology is that two automorphisms $\sigma, \tau \in \mathrm{Gal}(L/K)$ are "close" if they agree on a "large" finite Galois subextension F/K of L/K. The topology is formally defined using subgroups corresponding to finite extensions.

Lemma 1.4.1. *Let L/K be a Galois extension (possibly infinite) with $G = \mathrm{Gal}(L/K)$.*

(a) For $\sigma \in G$ and an intermediate field F between L and K, the coset $\sigma\,\mathrm{Gal}(L/F)$ is all automorphisms of G that look like σ on F:

$$\sigma\,\mathrm{Gal}(L/F) = \{\tau \in G \mid \tau|_F = \sigma|_F\}.$$

(b) If F/K is a finite extension inside L then $\mathrm{Gal}(L/F)$ has index $[F : K]$ in $\mathrm{Gal}(L/K)$.

Definition 1.4.2 (Krull Topology)**.** *Let L/K be a Galois extension. The Krull topology on $G = \mathrm{Gal}(L/K)$ is defined by taking the set of all cosets*

$$\{\sigma\,\mathrm{Gal}(L/F) \mid \sigma \in G,\ K \subseteq F \subseteq L,\ [F : K] < \infty\}$$

as a basis of open sets. Equivalently, the subgroups $\mathrm{Gal}(L/F)$ for finite extensions F/K form a basis of open neighborhoods of the identity element $e \in G$.

Remark 1.4.1 (Properties of Krull Topology)**.** *The Galois group $\mathrm{Gal}(L/K)$ equipped with the Krull topology is a profinite group. This means it is:*

- *Hausdorff: Distinct elements can be separated by open sets.*
- *Compact: Every open cover has a finite subcover.*
- *Totally disconnected: The only connected subsets are single points.*

In fact, $\mathrm{Gal}(L/K)$ can be realized as an inverse limit of finite groups: $\mathrm{Gal}(L/K) \cong \varprojlim \mathrm{Gal}(F/K)$, where the limit is taken over all finite Galois subextensions F/K. The Krull topology coincides with the topology inherited from this inverse limit structure. For a finite Galois extension L/K, the Krull topology is the discrete topology (all subgroups are open and closed).

The main theorem of infinite Galois theory establishes the correspondence using this topology.

Proposition 1.4.1. *Let L/K be a Galois extension (possibly infinite) with Galois group $G = \mathrm{Gal}(L/K)$ equipped with the Krull topology.*

(a) Let F be an intermediate field, i.e., $K \subseteq F \subseteq L$. Then L/F is also a Galois extension, the group $\mathrm{Gal}(L/F)$ is a closed subgroup of G, and the fixed field of $\mathrm{Gal}(L/F)$ is F (i.e., $L^{\mathrm{Gal}(L/F)} = F$).

(b) For every subgroup H of G, the Galois group $\mathrm{Gal}(L/L^H)$ is the closure of H in G. That is, $\mathrm{Gal}(L/L^H) = \overline{H}$.

Theorem 1.4.1 (Fundamental Theorem of (Infinite) Galois Theory)**.** *Let L/K be a Galois extension (possibly infinite) with Galois group $G = \mathrm{Gal}(L/K)$ equipped with the Krull topology. The maps*

$$H \longmapsto L^H \quad \text{and} \quad F \longmapsto \mathrm{Gal}(L/F)$$

are inverse bijections between the set of closed subgroups of G and the set of intermediate fields F such that $K \subseteq F \subseteq L$:

$$\{\text{closed subgroups } H \text{ of } G\} \quad \longleftrightarrow \quad \{\text{intermediate fields } F, K \subseteq F \subseteq L\}.$$

Moreover, this correspondence has the following properties:

(a) $H_1 \supseteq H_2 \iff L^{H_1} \subseteq L^{H_2}$ (the correspondence is inclusion-reversing).

(b) A closed subgroup H of G is open if and only if its fixed field L^H has finite degree over K. In this case, the index $[G : H]$ is equal to the degree $[L^H : K]$.

(c) For any $\sigma \in G$ and any closed subgroup $H \subseteq G$, $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$. For any $\sigma \in G$ and any intermediate field F, $\mathrm{Gal}(L/\sigma(F)) = \sigma \,\mathrm{Gal}(L/F)\sigma^{-1}$.

(d) A closed subgroup H of G is a normal subgroup (i.e., $H \triangleleft G$) if and only if its fixed field L^H is a Galois extension of K. In this case:

$$\mathrm{Gal}(L^H/K) \cong G/H.$$

Example 1.4.2 (Algebraic Closure of $\mathbb{Q}$)**.** *Consider the absolute Galois group of the rational numbers, $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This is a central object in number theory. It is an extremely complex profinite group. The Fundamental Theorem guarantees a correspondence between subfields $K \subseteq \overline{\mathbb{Q}}$ (which are the number fields and their infinite algebraic extensions) and the closed subgroups of $G_{\mathbb{Q}}$. For example, the field $\mathbb{Q}(\zeta_\infty) = \bigcup_n \mathbb{Q}(\zeta_n)$ corresponds to the closed kernel of the cyclotomic character $\chi : G_{\mathbb{Q}} \to \widehat{\mathbb{Z}}^\times \cong \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times$. Finite extensions $K/\mathbb{Q}$ correspond to open (and hence closed) subgroups of finite index in $G_{\mathbb{Q}}$.*

2. Elliptic Curves and Their Galois Representations

This section reviews fundamental results concerning elliptic curves, with the material primarily drawn from Chapter III of J.H. Silverman's "The Arithmetic of Elliptic Curves" [8]. For brevity and focus, most proofs will be omitted; however, proofs will be included if they offer particular insight relevant to the subsequent discussion of entanglements. Results not originating from this source and chapter will have their specific references cited within their respective statements or proofs.

2.1. The Geometry of Elliptic Curves

Let K be a perfect field and $\overline{K}$ an algebraic closure of K.

Definition 2.1.1. *An elliptic curve E over K can be defined equivalently as:*

(a) A nonsingular projective plane curve E/K of degree 3 with a specified K-rational point $O \in E(K)$.

(b) A nonsingular projective plane curve E of genus 1 together with a specified K-rational point $O \in E(K)$.

(c) A nonsingular projective plane curve over K defined by a generalized Weierstrass equation:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

where $a_i \in K$ for $i = 1, 2, 3, 4, 6$. The specified point O is taken to be $[0 : 1 : 0]$.

The set of K-rational points on E is denoted by $E(K)$.

The assumption that K is a *perfect field* is significant for these definitions, particularly concerning the term "nonsingular." A field K is perfect if every algebraic extension of K is separable. This implies that the separable closure K^{sep} (the maximal separable extension of K within $\overline{K}$) is identical to the algebraic closure $\overline{K}$ itself, i.e., $K^{sep} = \overline{K}$. (Recall that all fields of characteristic 0 are perfect; a field of characteristic $p > 0$ is perfect if and only if every element has a p-th root in K). Working over a perfect field K ensures that the notion of nonsingularity (or smoothness) behaves as expected geometrically.

Specifically, if E is defined over a perfect field K and is nonsingular over K, then it remains nonsingular when considered over any algebraic extension of K, including the algebraic closure $\overline{K}$. Since for a perfect field $K^{sep} = \overline{K}$, there are no purely inseparable extensions to cause complications when extending scalars to $\overline{K}$. If K were not perfect, a curve could be nonsingular over K but develop singularities upon base change to $\overline{K}$ due to inseparable phenomena.

For convenience, we often work with the affine form of the Weierstrass equation by setting $x = X/Z$ and $y = Y/Z$ (remembering the additional point O at infinity):

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.1}$$

The set of K-rational points in affine coordinates is

$$E(K) = \{(x, y) \in K^2 \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}.$$

If $\mathrm{Char}(K) \neq 2, 3$, a change of variables simplifies the equation to the short Weierstrass form:

$$E : y^2 = x^3 + Ax + B, \tag{2.2}$$

with $A, B \in K$. Associated with this equation are the quantities:

Definition 2.1.2 (Discriminant and j-invariant)**.** *Let E be an elliptic curve given by the short Weierstrass equation $y^2 = x^3 + Ax + B$, where $A, B \in K$.*

- *The discriminant of E, denoted Δ_E, is defined as:*

$$\Delta_E = -16(4A^3 + 27B^2).$$

- *If $\Delta_E \neq 0$ (i.e., the curve is nonsingular), the j-invariant of E, denoted $j(E)$ or simply j, is defined as:*

$$j = -1728\frac{(4A)^3}{\Delta_E}.$$

More general formulas for Δ_E and the j-invariant also exist for elliptic curves given by the general Weierstrass equation (2.1); these can be found in [8, Appendix A].

Proposition 2.1.1. *A curve given by a Weierstrass equation (2.1) (or (2.2)) is nonsingular if and only if its discriminant $\Delta_E \neq 0$.*

Proposition 2.1.2. *Two elliptic curves E_1, E_2 defined over K are isomorphic over the algebraic closure $\overline{K}$ if and only if they have the same j-invariant, i.e., $j(E_1) = j(E_2)$.*

Remark 2.1.1. *Given an elliptic curve E in short Weierstrass form (2.2) defined over K, and $\lambda \in K^\times$, the change of variables $(x, y) \mapsto (\lambda^{-2}x, \lambda^{-3}y)$ yields an isomorphic curve*

$$y^2 = x^3 + (\lambda^4 A)x + (\lambda^6 B).$$

This allows scaling of the coefficients (A, B). Moreover, any elliptic curver over $\mathbb{Q}$ is isomorphic to (2.2) where $a, b \in \mathbb{Z}$.

The set of points $E(\overline{K})$ on an elliptic curve E forms an abelian group with the specified K-rational point O as the identity element. The group law can be defined geometrically. A crucial ingredient for this geometric definition is Bézout's Theorem, which guarantees the number of intersection points between curves.

Theorem 2.1.1 (Bézout's Theorem)**.** *Let C_1 and C_2 be projective plane curves over a field K of degrees m and n respectively. If C_1 and C_2 have no irreducible component in common, then C_1 and C_2 intersect in $\overline{K}$ in exactly mn points, counted with multiplicity. That is,*

$$\sum_{P \in C_1(\overline{K}) \cap C_2(\overline{K})} I(P, C_1 \cap C_2) = mn,$$

where $I(P, C_1 \cap C_2)$ denotes the intersection multiplicity of C_1 and C_2 at the point P.

Proof. The proof can be found in [9, I.Corollary 7.8]. □

With Bézout's Theorem in mind, the group law is defined as follows:

Definition 2.1.3 (Group Law)**.** *Let $P, Q \in E(\overline{K})$.*

1. *Let L be the line passing through P and Q. If $P = Q$, let L be the tangent line to E at P.*

2. *An elliptic curve E has degree 3, and a line L has degree 1. Since L is not a component of E (because E is not nonsingular cubic curve), by Bézout's Theorem, L and E intersect in 3 points in $E(\overline{K})$, counted with multiplicity. Two of these points are P and Q (if $P = Q$, then P is counted with multiplicity at least 2). Let the third point of intersection be $R \in E(\overline{K})$.*

3. *Let L' be the line passing through R and the identity element O. Again, by Bézout's Theorem, L' intersects E at a third point. This third point is defined as $P+Q \in E(\overline{K})$.*

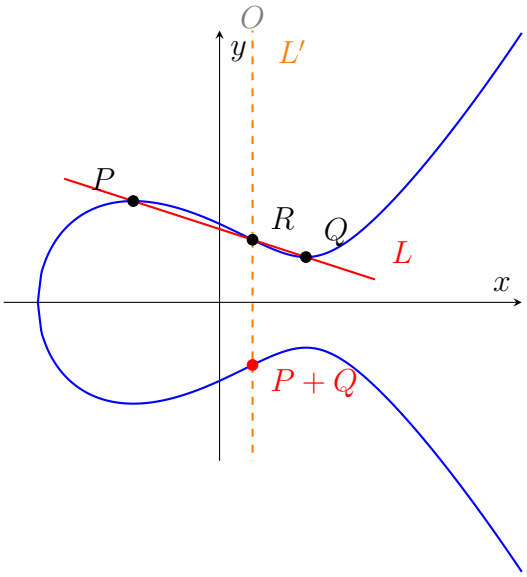


Figure 2.1: Geometric illustration of the addition law $P + Q$ on an elliptic curve.

Remark 2.1.2. *Equivalently, three points $P, Q, R \in E(\overline{K})$ sum to the identity O, i.e., $P + Q + R = O$, if and only if P, Q, R are collinear. The set of K-rational points $E(K)$ forms a subgroup of $E(\overline{K})$.*

Proposition 2.1.3. *The composition law defined above makes $E(\overline{K})$ into an abelian group with identity element O. Specifically:*

(a) (Identity) $P + O = P$ for all $P \in E$.

(b) (Commutativity) $P + Q = Q + P$ for all $P, Q \in E$.

(c) (Inverse) For each $P \in E$, there exists a point $-P \in E$ such that $P + (-P) = O$. If $P = (x, y)$ in affine coordinates for equation (2.1) or (2.2), then $-P = (x, -a_1x - a_3 - y)$ or $-P = (x, -y)$ respectively.

(d) (Associativity) $(P+Q)+R = P+(Q+R)$ *for all* $P, Q, R \in E$.

Definition 2.1.4 (Isogeny)**.** *Let* E_1, E_2 *be elliptic curves over* K *with identity points* O_1, O_2*. An isogeny from* E_1 *to* E_2 *is a morphism of algebraic curves* $\phi : E_1 \to E_2$ *satisfying* $\phi(O_1) = O_2$*. If* ϕ *can be defined by rational functions with coefficients in* K*, we say* ϕ *is defined over* K*. An isogeny* ϕ *is called a non-zero isogeny if it is not the zero map (the constant map sending all points of* E_1 *to* O_2*). It is a known result that any non-zero isogeny is automatically a surjective morphism [9, II.Proposition 6.8]. Two elliptic curves* E_1 *and* E_2 *are isogenous over* K *if there exists a non-zero isogeny* $\phi : E_1 \to E_2$ *defined over* K*.*

Proposition 2.1.4. *Every isogeny* $\phi : E_1 \to E_2$ *is a group homomorphism. Furthermore, the kernel of a non-zero isogeny is a finite subgroup of* $E_1(\overline{K})$*.*

Definition 2.1.5 (Endomorphism Rings)**.** *Let* E_1, E_2 *be elliptic curves defined over a field* K*.*

- *We denote the set of all isogenies from* E_1 *to* E_2 *(defined over the algebraic closure* $\overline{K}$*) by* $\mathrm{Hom}(E_1, E_2)$*. This set forms an abelian group under pointwise addition.*
- *The subgroup of isogenies that are defined over* K *is denoted by* $\mathrm{Hom}_K(E_1, E_2)$*.*
- *The endomorphism ring of* E*, denoted* $\mathrm{End}(E)$*, is the ring* $\mathrm{Hom}(E, E)$ *where multiplication is composition. The subring of endomorphisms defined over* K *is denoted* $\mathrm{End}_K(E)$*.*

Example 2.1.1 (Multiplication-by-m maps)**.** *For any integer* $m \in \mathbb{Z}$*, the multiplication-by-*m *map* $[m] : E \to E$ *is defined by* $[m](P) = P + \cdots + P$ *(*m *times) if* $m > 0$*,* $[0](P) = O$*, and* $[m](P) = [-m](-P)$ *if* $m < 0$*. The map* $[m]$ *is an endomorphism defined over the field of definition of* E*. If* $m \neq 0$*,* $[m]$ *is a non-zero isogeny.*

Definition 2.1.6 (Complex Multiplication)**.** *Let* E *be an elliptic curve defined over a field* K*. The map* $m \mapsto [m]$ *gives an injective ring homomorphism from* $\mathbb{Z}$ *into the full endomorphism ring,* $\mathrm{End}(E)$*.*

- *We say* E *does not have complex multiplication (non-CM) if this map is an isomorphism, i.e.,* $\mathrm{End}(E) \cong \mathbb{Z}$*.*
- *We say* E *has complex multiplication (CM) if the endomorphism ring is strictly larger than the integers, i.e.,* $\mathrm{End}(E) \supsetneq \mathbb{Z}$*.*

Definition 2.1.7 (Torsion Subgroups)**.** *Let* E *be an elliptic curve and let* $m \geq 1$ *be an integer.*

- *The* m*-torsion subgroup of* E *is* $E[m] = \ker[m] = \{P \in E(\overline{K}) \mid [m]P = O\}$*.*
- *The torsion subgroup of* E *is* $E_{tors} = \bigcup_{m=1}^{\infty} E[m]$*.*

If E *is defined over* K*,* $E[m](K) = E[m] \cap E(K)$ *and* $E_{tors}(K) = E_{tors} \cap E(K)$ *denote the* m*-torsion points and torsion points rational over* K*, respectively.*

Theorem 2.1.2 (Structure of Torsion Subgroups)**.** *Let E be an elliptic curve defined over a field K and let $m \in \mathbb{Z}_{\neq 0}$.*

(a) The degree of the multiplication-by-m map is $\deg[m] = m^2$.

(b) If $\mathrm{Char}(K) = 0$ *or if* $\mathrm{Char}(K) = p > 0$ *and* $p \nmid m$*, then*

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

(c) If $\mathrm{Char}(K) = p > 0$*, then either* $E[p^e] = \{O\}$ *for all* $e \geq 1$*, or* $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$ *for all* $e \geq 1$.

Remark 2.1.3.

- *It is important to note that in each of the cases described in Theorem 2.1.2(b) and (c), the torsion subgroup $E[N]$ (where $N = m$ in case (b), or $N = p^e$ in case (c)) is naturally a module over the ring $\mathbb{Z}/N\mathbb{Z}$.*
- *Furthermore, for any integer $m \neq 0$, the m-torsion subgroup $E[m]$ is identical to the $(-m)$-torsion subgroup $E[-m]$.*

Example 2.1.2. *Assume* $\mathrm{Char}(K) \neq 2$*. Let E be given by $y^2 = x^3 + Ax + B$. A point $P = (x, y)$ satisfies $P = -P$ if and only if $y = 0$. Thus, the points of order 2 are O and the points $(x_i, 0)$ where x_1, x_2, x_3 are the roots of $x^3 + Ax + B = 0$. Since $\Delta_E \neq 0$, the roots are distinct. Thus, $E[2] = \{O, (x_1, 0), (x_2, 0), (x_3, 0)\}$. This is a group of order 4 where every non-identity element has order 2, so $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, consistent with Theorem 2.1.2(b).*

Having laid some groundwork, we can now state some crucial properties related to torsion points that will be essential for our upcoming discussion on entanglements. Let E be an elliptic curve defined over $\mathbb{Q}$. The coordinates of points in $E[m]$ are algebraic over $\mathbb{Q}$. The field extension $\mathbb{Q}(E[m])$ obtained by adjoining the coordinates of all points in $E[m]$ to $\mathbb{Q}$ is a finite Galois extension of $\mathbb{Q}$. Further details will be explored later in this chapter.

2.2. The Weil Pairing

Let E/K be an elliptic curve defined over a perfect field K, and let $\overline{K}$ be a fixed algebraic closure of K. The Weil pairing is a crucial tool for the material presented in this paper. An explicit construction often relies on the theory of divisors, which would require extensive background. Therefore, this section will introduce the Weil pairing by its characteristic properties, which are sufficient for our purposes.

Definition 2.2.1 (Weil Pairing)**.** *Let $m \geq 2$ be an integer. Assume that if* $\mathrm{Char}(K) = p > 0$*, then $p \nmid m$. The Weil e_m-pairing is a map*

$$e_m : E[m] \times E[m] \longrightarrow \mu_m,$$

where $E[m] = \{P \in E(\overline{K}) \mid [m]P = O\}$ is the m-torsion subgroup of E, and $\mu_m = \{\zeta \in \overline{K}^\times \mid \zeta^m = 1\}$ is the group of m-th roots of unity in $\overline{K}$.

The Weil pairing possesses several fundamental properties, crucial for studying the arithmetic of elliptic curves:

Proposition 2.2.1 (Properties of the Weil Pairing)**.** *The Weil e_m-pairing has the following properties for all $S, S_1, S_2, T, T_1, T_2 \in E[m]$:*

(a) ***Bilinearity:***

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

(b) ***Alternating:***

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

This implies $e_m(S, T) = e_m(T, S)^{-1}$.

(c) ***Nondegeneracy:*** *If $e_m(S, T) = 1$ for all $S \in E[m]$, then $T = O$.*

(d) ***Galois Invariance:*** *For all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ (the absolute Galois group of K),*

$$\sigma(e_m(S, T)) = e_m(\sigma(S), \sigma(T)).$$

(e) ***Compatibility:*** *For integers $m, m' \geq 2$ (satisfying the characteristic condition),*

$$e_{mm'}(S, T) = e_m([m']S, T) \text{ for all } S \in E[mm'] \text{ and } T \in E[m].$$

A key consequence of nondegeneracy and the structure of $E[m]$ is:

Corollary 2.2.1. *There exist points $S, T \in E[m]$ such that $e_m(S, T)$ is a primitive m-th root of unity. In particular, if $E[m] \subseteq E(K)$, then $\mu_m \subseteq K^\times$.*

Proof. Consider $\{e_m(S, T) \mid S, T \in E[m]\} \subseteq \mu_m$ and note by the first two properties of the Weil pairing that $\{e_m(S, T) \mid S, T \in E[m]\}$ is in fact a subgroup of μ_m and so $\{e_m(S, T) \mid S, T \in E[m]\} = \mu_d$ for some $d|m$. We now want to show that $d = m$. Suppose $d \neq m$. Fix an $S \in E[m]$ and consider

$$1 = e_m(S, T)^d = e_m([d]S, T)$$

the second equality results from the bilinearity of the Weil pairing. The above is true for all $T \in E[m]$ which implies that $[d]S = O$ by the nondegeneracy of the Weil Pairing. Moreover, we can pick $S \in E[m]$ to have exact order m, which forces $d = m$.

Finally, suppose $E[m] \subseteq E(K)$ and let $S, T \in E[m]$ such that $e_m(S, T)$ is a primitive m-th root of unity. For all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ we have

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

where the second equality follows from $E[m] \subseteq E(K)$. The latter implies $e_m(S, T) \in K^\times$ hence $\mu_m \subseteq K^\times$. □

Remark 2.2.1. *As we shall see in Lemma 2.4.2, the existence of a basis $\{S, T\}$ for $E[m]$ such that the Weil pairing $e_m(S, T)$ generates μ_m is fundamental. It connects the arithmetic of the elliptic curve's torsion points to cyclotomic fields and plays a vital role in understanding Galois representations and entanglement phenomena, which will be discussed later.*

2.3. Tate Modules

Building upon the concept of inverse limits, we define important modules associated with the torsion subgroups of an elliptic curve E defined over a perfect field K, namely the ℓ-adic and adelic Tate modules.

First, let ℓ be a prime number. We construct an inverse system of groups indexed by $\mathbb{N}$ with its usual ordering $\leq$. For each $n \in \mathbb{N}$, let $G_n = E[\ell^n]$, the ℓ^n-torsion subgroup of $E(\overline{K})$. For $n \leq m$, the transition map $\phi_{m,n} : G_m \to G_n$ is given by multiplication by ℓ^{m-n}, i.e., $\phi_{m,n} = [\ell^{m-n}] : E[\ell^m] \twoheadrightarrow E[\ell^n]$. This forms an inverse system as checked previously.

Definition 2.3.1 (ℓ-adic Tate Module)**.** *Let E/K be an elliptic curve and ℓ a prime. The ℓ-adic Tate module of E is the inverse limit of the system described above:*

$$T_\ell(E) := \varprojlim_n E[\ell^n] = \left\{ (P_n)_{n\geq 1} \in \prod_{n\geq 1} E[\ell^n] \mid [\ell]P_{n+1} = P_n \text{ for all } n \geq 1 \right\}.$$

Recall that $E[\ell^n]$ is a module over the ring $\mathbb{Z}/\ell^n\mathbb{Z}$. The transition maps $\phi_{m,n} = [\ell^{m-n}]$ are surjective homomorphisms of these modules, compatible with the natural ring homomorphisms $\mathbb{Z}/\ell^m\mathbb{Z} \to \mathbb{Z}/\ell^n\mathbb{Z}$. Consequently, the inverse limit $T_\ell(E)$ naturally inherits the structure of a module over the inverse limit ring $\varprojlim \mathbb{Z}/\ell^n\mathbb{Z} = \mathbb{Z}_\ell$, the ring of ℓ-adic integers. The structure of this $\mathbb{Z}_\ell$-module is well-known:

Theorem 2.3.1 (Structure of $T_\ell(E)$)**.** *Let E/K be an elliptic curve and ℓ a prime.*

(a) If $\ell \neq \mathrm{Char}(K)$, then $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ as a $\mathbb{Z}_\ell$-module.

(b) If $\ell = p = \mathrm{Char}(K) > 0$, then $T_p(E) \cong \{0\}$ or $\mathbb{Z}_p$ as a $\mathbb{Z}_p$-module.

Next, analogous to the construction of the profinite completion $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$ using the divisibility ordering, we define the adelic Tate module. Consider the inverse system indexed by $\mathbb{N}$ where the partial order is divisibility ($n \preceq m$ if $n|m$). For each $n \in \mathbb{N}$, let $G_n = E[n]$. For $n|m$, the transition map $\phi_{m,n} : G_m \to G_n$ is given by multiplication by m/n, i.e., $\phi_{m,n} = [m/n] : E[m] \twoheadrightarrow E[n]$. This forms an inverse system.

Definition 2.3.2 (Adelic Tate Module)**.** *Let E/K be an elliptic curve. The adelic Tate module (or full Tate module) of E is the inverse limit of this system:*

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

Remark 2.3.1. *Similar to the ℓ-adic case, $E[n]$ is a $\mathbb{Z}/n\mathbb{Z}$-module and the transition maps are compatible with the ring maps $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Therefore, the adelic Tate module $T(E)$ inherits the structure of a module over $\varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$, the ring of profinite integers.*

If $\mathrm{Char}(K) = 0$ (e.g., $K = \mathbb{Q}$), then for every n, $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Taking the inverse limit preserves this structure, yielding

$$T(E) \cong \hat{\mathbb{Z}} \times \hat{\mathbb{Z}} \quad (\text{if } \mathrm{Char}(K) = 0).$$

Furthermore, just as the ring of profinite integers decomposes as a product over primes, $\hat{\mathbb{Z}} \cong \prod_\ell \mathbb{Z}_\ell$, the adelic Tate module decomposes accordingly via the Chinese Remainder Theorem applied to torsion subgroups:

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

2.4. Galois Representations of Elliptic Curves

The primary goal of this section is to formally define the mod-n Galois representation, denoted $\rho_{E,n}$, attached to an elliptic curve E. We will then establish several fundamental properties concerning the n-torsion field $\mathbb{Q}(E[n])$, namely:

- The cyclotomic field $\mathbb{Q}(\zeta_n)$ is contained within the n-torsion field, i.e., $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$.
- The n-torsion field $\mathbb{Q}(E[n])$ is a finite Galois extension of $\mathbb{Q}$.
- The image of the mod-n Galois representation is isomorphic to the Galois group of the n-torsion field: $\rho_{E,n}(G_{\mathbb{Q}}) \cong \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$.

From this section onwards, unless otherwise specified, we will restrict our attention to elliptic curves defined over the field of rational numbers. Thus, let $K = \mathbb{Q}$. An elliptic curve E over $\mathbb{Q}$ can then be given by a Weierstrass equation of the form

$$E : y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{Z}$.

Proposition 2.4.1. *Let E be an elliptic curve defined by an equation with coefficients in $\mathbb{Q}$, and let K be a Galois extension of $\mathbb{Q}$.*

(a) The set $E(K)$ of points with coordinates in K is a subgroup of $E(\overline{\mathbb{Q}})$.

(b) For $P \in E(K)$ and $\sigma \in Gal(K/\mathbb{Q})$, define

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

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

(c) For all $P \in E(K)$ and all $\sigma, \tau \in Gal(K/\mathbb{Q})$,

$$(\sigma\tau)_E(P) = \sigma_E(\tau_E(P)).$$

Further, the identity element $e \in Gal(K/\mathbb{Q})$ acts trivially, $e_E(P) = P$.

(d) For all $P, Q \in E(K)$ and all $\sigma \in Gal(K/\mathbb{Q})$,

$$\sigma_E(P + Q) = \sigma_E(P) + \sigma_E(Q) \quad \text{and} \quad \sigma_E(-P) = -\sigma_E(P).$$

In particular, $\sigma_E([n]P) = [n]\sigma_E(P)$ for all integers n.

(e) Let $P \in E(K)$ be a point of order n and let $\sigma \in Gal(K/\mathbb{Q})$. Then $\sigma_E(P)$ also has order n.

Proof. (a) Refer to [10, Proposition 6.3]. Similalry for (b)-(d).

(e) Let $P \in E(K)$ have order n. Using (d), we find that

$$O = \sigma_E([n]P) = [n]\sigma_E(P)$$

So $\sigma_E(P)$ has finite order m and $m|n$. Conversely, using that $O = [m]\sigma_E(P) = \sigma_E([m]P)$ and applying σ_E^{-1} to both sides, we find that

$$O = \sigma_E^{-1}(O) = \sigma_E^{-1}(\sigma_E([m]P)) = (\sigma^{-1}\sigma)_E([m]P) = [m]P$$

Hence $n|m$ and $m = n$.

□

Remark 2.4.1. *Part (b) follows because the coefficients defining the elliptic curve E are in $\mathbb{Q}$ and are thus fixed by $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Part (d) is true because the group law on E is defined by rational functions with coefficients in $\mathbb{Q}$. While a full proof of (d) involves the explicit formulas for elliptic curve addition, we omit it here to avoid overburdening the reader with details not essential for the current development.*

The proposition states that every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ can be extended to act upon the points $P \in E(K)$. Moreover, every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ induces an endomorphism on $E(K)$. Since σ has an inverse in $\mathrm{Gal}(K/\mathbb{Q})$, every induced endomorphism has an inverse as well, so every σ induces an automorphism on $E(K)$.

Corollary 2.4.1. *The map*

$$\rho_{E/\mathbb{Q},K} : Gal(K/\mathbb{Q}) \longrightarrow Aut(E(K))$$

$$\sigma \mapsto \sigma_E$$

is a group homomorphism.

Fortunately for us, $\mathbb{Q}$ is a perfect field and so $\overline{\mathbb{Q}}$ is Galois over $\mathbb{Q}$. We can consider:

$$\rho_{E,\mathbb{Q}/\overline{\mathbb{Q}}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E(\overline{\mathbb{Q}}))$$

As established in Proposition 2.4.1(e), any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ preserves the order of points in $E(\overline{\mathbb{Q}})$. Since $E[n] \subseteq E(\overline{\mathbb{Q}})$ (a fact that will be formally addressed shortly), σ thus maps $E[n]$ to itself, effectively permuting its points. This restricted action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the n-torsion subgroup defines the mod-n Galois representation:

$$\rho_n : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[n])$$

$$\sigma \mapsto \sigma_E|_{E[n]}$$

Given that $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, selecting a basis for $E[n]$ leads to the conclusion that $\mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. To illustrate this more precisely, consider P_1 and P_2 as a basis for $E[n]$. Consequently, any $P \in E[n]$ can be expressed as

$$P = [a]P_1 + [b]P_2$$

where $a, b \in \mathbb{Z}/n\mathbb{Z}$. Therefore, with $\sigma \in \mathrm{Aut}(E[n])$ (omitting the subscript), it follows that

$$\sigma(P) = [a]\sigma(P_1) + [b]\sigma(P_2).$$

This implies that to fully determine the automorphism σ, it suffices to know the images of the basis elements, $\sigma(P_1)$ and $\sigma(P_2)$. For conciseness in the following, we will often denote the induced automorphism on $E[n]$ simply as σ.

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

Since σ has an inverse, the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible and we can now define the following map:

$$\Phi : \mathrm{Aut}(E[n]) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$
$$\sigma \mapsto M_\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

One can show that Φ is a group isomorphism. We are now ready to show that there exists a homomorphism from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

Corollary 2.4.2. *Let $E/\mathbb{Q}$ be an elliptic curve and $n \in \mathbb{Z}_{\geq 2}$. Fix generators P_1 and P_2 for $E[n]$. Then the map*

$$\rho_{E,n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$
$$\rho_{E,n} = \Phi \circ \rho_n$$

is a group homomorphism.

Remark 2.4.2.

- *We denote the absolute Galois group of $\mathbb{Q}$ by $G_\mathbb{Q} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.*
- *The group homomorphism $\rho_{E,n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is commonly known as the mod-n Galois representation attached to the elliptic curve E.*

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 $\phi, \phi' : E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ 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 have now defined the mod-n Galois representation attached to an elliptic curve. Our focus will next shift to defining division fields and stating some important results associated with them.

$E[n]$ is a finite subgroup of $E(\overline{\mathbb{Q}})$ of order n^2. Therefore, we can write $E[n]$ as

$$E[n] = \{O, (x_1, y_1), \ldots, (x_{n^2-1}, y_{n^2-1})\}.$$

We construct the n-division field by adjoining the coordinates from every element in $E[n]$ to $\mathbb{Q}$.

Definition 2.4.1. *Let $E/\mathbb{Q}$ be an elliptic curve and let $n \geq 1$, then we define the n-division field of E as*

$$\mathbb{Q}(E[n]) := \mathbb{Q}(x_1, y_1, \ldots, x_{n^2-1}, y_{n^2-1}).$$

Note that $\mathbb{Q}(E[1])$ is just $\mathbb{Q}$.

Every $x \in \overline{\mathbb{Q}}$ is algebraic over $\mathbb{Q}$, that is, $[\mathbb{Q}(x) : \mathbb{Q}] < \infty$. The degree of the extension of $\mathbb{Q}(E[n])$ is finite because we are adjoining only a finite number of algebraic elements to $\mathbb{Q}$.

Proposition 2.4.2. *Let E be an elliptic curve defined by an equation with coefficients in $\mathbb{Q}$.*

(a) Let $P = (x_1, y_1) \in E[n]$ be a point of order dividing n. Then x_1 and y_1 are algebraic over $\mathbb{Q}$, i.e., x_1 and y_1 are roots of polynomials with rational coefficients.

(b) $\mathbb{Q}(E[n])$ is a Galois extension of $\mathbb{Q}$.

Proof. Refer to [10, Proposition 6.5]. □

Remark 2.4.3. *The proof uses the fact that the x coordinates of the torsion points on an elliptic curve are roots to division polynomials, which are polynomials with rational coefficients. Part (b) follows quite easily from Proposition 2.4.2(a) and Proposition 2.4.1(e).*

Lemma 2.4.1. *Let $E/\mathbb{Q}$ be an elliptic curve and let $n \in \mathbb{Z}_{\geq 1}$. Then $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$.*

Proof. As we have seen, there exists $S, T \in E[n]$ such that $e_n(S, T)$ is a primitive n-th root of unity. Moreover, we have that $\overline{\mathbb{Q}}/\mathbb{Q}(E[n])$ is a Galois extension as $\overline{\mathbb{Q}}/\mathbb{Q}$ is a Galois extension. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[n]))$ then consider,

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

Where the first equality comes from the Galois invariance of the Weil pairing. Thus, Galois theory tells us that $e_n(S, T) \in \mathbb{Q}(E[n])$ i.e. $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$. □

Lemma 2.4.2. *Let $E/\mathbb{Q}$ be an elliptic curve and let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then $\sigma(\zeta_n) = \zeta_n^{\det(\rho_{E,n}(\sigma))}$ for all n-th roots of unity ζ_n. Consequently, the determinant map is full ,i.e., $\det(\rho_{E,n}(G_{\mathbb{Q}})) = (\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof. Note that the result doesn't depend on the choice of basis used to define the Galois representation $\rho_{E,n}$, as the determinant $\det(\rho_{E,n}(\sigma))$ is invariant under conjugation and thus the same for any choice of basis for $E[n]$.

By Corollary 2.2.1, there exist $S, T \in E[n]$ such that $e_n(S, T) = \zeta_n$, where ζ_n is a primitive n-th root of unity. We now show that S, T form a basis for $E[n]$ (as a $\mathbb{Z}/n\mathbb{Z}$-module). Suppose they are linearly dependent, so there exist $u, v \in \mathbb{Z}/n\mathbb{Z}$, not both zero, such that $[u]S + [v]T = O$. Then by properties of the Weil pairing we obtain:

$$\begin{aligned}
1 &= e_n(O, T) \\
&= e_n([u]S + [v]T, T) \\
&= e_n([u]S, T) \cdot e_n([v]T, T) \quad \text{(by bilinearity)} \\
&= e_n(S, T)^u \cdot e_n(T, T)^v \\
&= \zeta_n^u \cdot 1^v = \zeta_n^u.
\end{aligned}$$

Since ζ_n is a primitive n-th root of unity, $\zeta_n^u = 1$ implies $u \equiv 0 \pmod{n}$. The linear dependence assumption thus simplifies to $[v]T = O$. Applying a similar argument:

$$\begin{aligned} 1 &= e_n(S, O) \\ &= e_n(S, [v]T) \\ &= e_n(S, T)^v \\ &= \zeta_n^v. \end{aligned}$$

This implies $v \equiv 0 \pmod{n}$. Therefore, $u = v = 0$ in $\mathbb{Z}/n\mathbb{Z}$, which contradicts our assumption that S, T were linearly dependent with not both coefficients zero. Thus, S, T are linearly independent and, since $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$, they form a basis for $E[n]$.

Let $\sigma \in G_{\mathbb{Q}}$. By the Galois invariance of the Weil pairing, we have $\sigma(\zeta_n) = \sigma(e_n(S, T)) = e_n(\sigma(S), \sigma(T))$. Recall that σ maps n-torsion points to n-torsion points, so $\sigma(S), \sigma(T) \in E[n]$. Since S, T form a basis for $E[n]$, we can write $\sigma(S) = [a]S + [c]T$ and $\sigma(T) = [b]S + [d]T$ for unique $a, b, c, d \in \mathbb{Z}/n\mathbb{Z}$. The matrix for the action of σ with respect to the basis $\{S, T\}$ is therefore

$$\rho_{E,n}(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

and its determinant is $\det(\rho_{E,n}(\sigma)) = ad - bc$.

Using the properties of the Weil pairing:

$$\begin{aligned} \sigma(\zeta_n) &= e_n(\sigma(S), \sigma(T)) \\ &= e_n([a]S + [c]T, [b]S + [d]T) \\ &= e_n([a]S, [b]S) \cdot e_n([a]S, [d]T) \cdot e_n([c]T, [b]S) \cdot e_n([c]T, [d]T) \quad \text{(by bilinearity)} \\ &= e_n(S, S)^{ab} \cdot e_n(S, T)^{ad} \cdot e_n(T, S)^{cb} \cdot e_n(T, T)^{cd} \\ &= 1^{ab} \cdot \zeta_n^{ad} \cdot (\zeta_n^{-1})^{cb} \cdot 1^{cd} \quad \text{(using } e_n(X, X) = 1 \text{ and } e_n(Y, X) = e_n(X, Y)^{-1}\text{)} \\ &= \zeta_n^{ad-cb} \\ &= \zeta_n^{\det(\rho_{E,n}(\sigma))}. \end{aligned}$$

This establishes the identity for a primitive n-th root of unity ζ_n. Now, let $\xi = \zeta_n^k$ be any n-th root of unity for some integer k. Since σ is a field automorphism, it acts as a homomorphism on the group of n-th roots of unity:

$$\sigma(\xi) = \sigma(\zeta_n^k) = (\sigma(\zeta_n))^k = \left(\zeta_n^{\det(\rho_{E,n}(\sigma))}\right)^k = (\zeta_n^k)^{\det(\rho_{E,n}(\sigma))} = \xi^{\det(\rho_{E,n}(\sigma))}.$$

Thus, the identity holds for all n-th roots of unity.

From $\sigma(\zeta_n) = \zeta_n^{\det(\rho_{E,n}(\sigma))}$, we identify $\det(\rho_{E,n}(\cdot))$ with the n-th cyclotomic character χ_n. The surjectivity of $\chi_n : G_{\mathbb{Q}} \to (\mathbb{Z}/n\mathbb{Z})^\times$ follows because χ_n factors as the surjective restriction $G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ composed with the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Thus, $\det(\rho_{E,n}(G_{\mathbb{Q}})) = (\mathbb{Z}/n\mathbb{Z})^\times$. □

Remark 2.4.4 (Kernel and Image of $\rho_{E,n}$)**.** *Let $E/\mathbb{Q}$ be an elliptic curve and consider its mod-n Galois representation*

$$\rho_{E,n} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

The kernel of this representation, $\ker(\rho_{E,n})$*, consists of the automorphisms in* $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *that act trivially on the* n*-torsion subgroup* $E[n]$*. An automorphism* σ *fixes every point in* $E[n]$ *if and only if it fixes the field extension generated by their coordinates,* $\mathbb{Q}(E[n])$*. By the Galois correspondence, this subgroup is precisely* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[n]))$*. Thus,*

$$\ker(\rho_{E,n}) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[n])).$$

The First Isomorphism Theorem for groups then gives an isomorphism between the image of the representation and the quotient of the domain by the kernel:

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

Furthermore, since $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[n]))$ *is a normal subgroup of* $G_{\mathbb{Q}}$*, the Fundamental Theorem of Infinite Galois Theory (Theorem 1.4.1) provides the canonical isomorphism for the quotient group:*

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

We conclude this section by combining these isomorphisms to show that the image of the Galois representation is precisely the Galois group of the n*-torsion field:*

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

2.5. ℓ-adic and Adelic Galois Representations of Elliptic Curves

We have previously established that for an elliptic curve $E/\mathbb{Q}$, the absolute Galois group $G_{\mathbb{Q}}$ acts on each finite n-torsion subgroup $E[n]$. This action can be extended naturally to define actions on the ℓ-adic Tate module $T_\ell(E)$ and the adelic Tate module $T(E)$.

Consider the ℓ-adic Tate module $T_\ell(E) = \varprojlim_n E[\ell^n]$. Recall that an element of $T_\ell(E)$ is a sequence $(P_n)_{n\geq 1}$ with $P_n \in E[\ell^n]$ such that the transition map $[\ell] : E[\ell^{n+1}] \to E[\ell^n]$ relates consecutive terms: $[\ell]P_{n+1} = P_n$ for all $n \geq 1$.

Let $\sigma \in G_{\mathbb{Q}}$. We know that the action of σ commutes with the multiplication-by-m maps for any integer m. In particular, for any $P \in E[\ell^{n+1}]$, we have:

$$[\ell](\sigma(P)) = \sigma([\ell]P). \tag{2.3}$$

We define the action of σ on an element $(P_n)_{n\geq 1} \in T_\ell(E)$ component-wise:

$$\sigma((P_n)_{n\geq 1}) := (\sigma(P_n))_{n\geq 1}.$$

We must verify that this resulting sequence is indeed an element of $T_\ell(E)$. Let $P'_{n+1} = \sigma(P_{n+1})$ and $P'_n = \sigma(P_n)$. We need to check if $[\ell]P'_{n+1} = P'_n$. Using the compatibility condition (2.3) and the fact that $(P_n)_{n\geq 1} \in T_\ell(E)$ (so $[\ell]P_{n+1} = P_n$), we have:

$$[\ell]P'_{n+1} = [\ell](\sigma(P_{n+1})) = \sigma([\ell]P_{n+1}) = \sigma(P_n) = P'_n.$$

Thus, the compatibility condition $[\ell]P'_{n+1} = P'_n$ holds for the sequence $\sigma((P_n)_{n\geq 1})$, confirming that $\sigma((P_n)_{n\geq 1}) \in T_\ell(E)$.

Since σ acts as a group automorphism on each $E[\ell^n]$ and respects the inverse limit structure, the induced map $\sigma|_{T_\ell(E)}$ is an automorphism of the $\mathbb{Z}_\ell$-module $T_\ell(E)$. The map sending $\sigma \in G_{\mathbb{Q}}$ to $\sigma|_{T_\ell(E)} \in \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E))$ is a group homomorphism.

Definition 2.5.1 (ℓ-adic Galois Representation)**.** *The ℓ-adic Galois representation attached to $E/\mathbb{Q}$ is the continuous group homomorphism*

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

induced by the action of $G_{\mathbb{Q}}$ on $T_\ell(E)$. As $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$, choosing a basis yields the matrix representation

$$\rho_{E,\ell^\infty} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Remark 2.5.1. *The homomorphism ρ_{E,ℓ^∞} is continuous with respect to the Krull topology on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and the ℓ-adic topology on $\mathrm{GL}_2(\mathbb{Z}_\ell)$ (induced by the topology on $\mathbb{Z}_\ell$). A similar remark can be made for the following defintion.*

An analogous argument applies to the adelic Tate module $T(E) = \varprojlim_n E[n]$. The transition maps are $\phi_{m,n} = [m/n]$ for $n|m$. Since the action of $\sigma \in G_{\mathbb{Q}}$ commutes with $[m/n]$ for the same reason as above ($\sigma([k]P) = [k]\sigma(P)$), the action extends component-wise to an action on $T(E)$.

Definition 2.5.2 (Adelic Galois Representation)**.** *The adelic Galois representation (or full Galois representation) attached to $E/\mathbb{Q}$ is the continuous group homomorphism*

$$\rho_E : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}_{\hat{\mathbb{Z}}}(T(E))$$

induced by the action of $G_{\mathbb{Q}}$ on $T(E)$. As $T(E) \cong \hat{\mathbb{Z}} \times \hat{\mathbb{Z}}$, choosing a basis yields the matrix representation

$$\rho_E : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\hat{\mathbb{Z}}) \cong \prod_{\ell \text{ prime}} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Remark 2.5.2. *The isomorphism $T(E) \cong \hat{\mathbb{Z}} \times \hat{\mathbb{Z}}$ relies on the fact that E is defined over $\mathbb{Q}$, a field of characteristic 0. If E were defined over a field K with positive characteristic $p = \mathrm{Char}(K)$, the structure of the p-primary part of the Tate module $T(E)$, namely $T_p(E)$, could differ (it might be $\{0\}$ or $\mathbb{Z}_p$ instead of $\mathbb{Z}_p \times \mathbb{Z}_p$). This would alter the overall structure of $T(E)$ and consequently the target group of the adelic representation.*

We end this section and chapter by stating the most important result related to the Adelic Galois representation attached to an elliptic curve.

Theorem 2.5.1 (Serre's open image theorem)**.** *Let E be a non-CM elliptic curve defined over a number field K. Then $\rho_E(\mathrm{Gal}(\overline{K}/K))$ is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$. Equivalently, $\rho_E(\mathrm{Gal}(\overline{K}/K))$ is a finite index subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$.*

Proof. Refer to [1]. □

Remark 2.5.3. *Serre's open image theorem implies that there exists only a finite number of primes ℓ for which the representation $\rho_{E,\ell}$ is not surjective. The details of this implication can be found in [1].*

3. Group-Theoretic Tools for Entanglements

This chapter develops the group-theoretic machinery required to prove two main results related to entanglements. The proof of the first main result is deferred to a later chapter. The first section establishes the necessary background to prove the following result on the surjectivity of mod-n Galois representations:

Theorem. *If E is an elliptic curve defined over $\mathbb{Q}$ and n is any integer with $\gcd(n, 30) = 1$, then the Galois representation*

$$\rho_{E,n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

is surjective if and only if the Galois representations $\rho_{E,p}$ are surjective for every prime $p \mid n$. In particular, if E is a non-CM elliptic then $\rho_{E,n}$ is surjective for every integer n with $\gcd(n, A_{30}(E)) = 1$ (See Definition 4.9.1 for $A_{30}(E)$).

In the second section, we present the results required for our second main result and prove the second main result. This result is of practical importance for this thesis, as it provides the theoretical justification for the algorithm we developed to construct all applicable subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

Proposition. *Let $E/\mathbb{Q}$ be an elliptic curve for which the mod-n Galois representation $\rho_{E,n}$ is not surjective. Then the subgroup $\{\pm I\}\rho_{E,n}(G_{\mathbb{Q}})$ is an applicable subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.*

Definition (Applicable Subgroup)**.** *We say that a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is applicable if it satisfies the following conditions:*

- *$G \neq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$,*
- *$-I \in G$ and $\det(G) = (\mathbb{Z}/n\mathbb{Z})^\times$,*
- *G contains an element with trace 0 and determinant -1 that fixes a point in $(\mathbb{Z}/n\mathbb{Z})^2$ of order n.*

3.1. Group Theory for Surjectivity Criterion

This section presents a sequence of technical results, the exposition of which is adapted from Kani [11, Appendix].

Definition 3.1.1. *Let G be a group. The commutator subgroup (or derived subgroup) of G, denoted G' or $[G, G]$, is the subgroup generated by the set of all its commutators:*

$$G' := \langle \{[x, y] \mid x, y \in G\} \rangle,$$

where the commutator of two elements $x, y \in G$ is defined as $[x, y] = xyx^{-1}y^{-1}$.

Remark 3.1.1. *The normality of the commutator subgroup G' follows from the identity $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$.*

Definition 3.1.2. *A group G is said to be simple if it possesses exactly two normal subgroups: $\{e\}$ and G itself.*

Remark 3.1.2. *The trivial group is not a simple group as it only has one normal subgroup.*

Definition 3.1.3. *Let G be a group. A composition series of G is a finite sequence of subgroups*

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

where G_{i+1}/G_i is simple for all $0 \leq i < n$. We refer to G_{i+1}/G_i as a composition factor of G.

Remark 3.1.3. *If we relax the condition that the factor groups G_{i+1}/G_i must be simple, the sequence is called a subnormal series.*

Theorem 3.1.1 (Jordan-Hölder)**.** *Let G be a group. Suppose G has two composition series*

$$\{e\} = G_0 \triangleleft \cdots \triangleleft G_n = G,$$

and

$$\{e\} = H_0 \triangleleft \cdots \triangleleft H_m = H.$$

Then there is a bijection $\pi : \{1, ..., n\} \to \{1, ..., m\}$ such that

$$G_{\pi(i)}/G_{\pi(i)-1} = H_i/H_{i-1},$$

for all $0 \leq i < n$. The existence of a bijection implies $n = m$.

Remark 3.1.4. *It should be noted that while all finite groups admit a composition series, not all infinite groups do. Nevertheless, if an infinite group does possess a composition series, the conclusion of the Jordan-Hölder theorem still holds.*

The following well-known facts can be found in [12, Theorems II.6.13 and II.8.14]:

Lemma 3.1.1. *Let p and q be prime numbers. Define $PSL_2(p) := SL_2(\mathbb{Z}/p\mathbb{Z})/\{\pm I\}$. Then:*

(a) $PSL_2(p)$ is a simple group for any $p \geq 5$;

(b) $PSL_2(p) \cong PSL_2(q)$ if and only if $p = q$;

(c) If H is a proper subgroup of $PSL_2(p)$, then H is solvable or $H \cong A_5$;

(d) $PSL_2(p) \cong A_5$ if and only if $p = 5$.

Lemma 3.1.2. *No proper subgroup of $SL_2(\mathbb{Z}/p\mathbb{Z})$ maps onto $PSL_2(p)$.*

Proof. The case $p = 2$ is special. The center $K = \{\pm I\}$ of $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ is trivial, since $-I = I$ in characteristic 2. Thus, the natural projection $\pi : \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \to \mathrm{PSL}_2(2)$ is an isomorphism. Consequently, the only subgroup of $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ that maps onto $\mathrm{PSL}_2(2)$ is $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ itself, so no *proper* subgroup with this property.

Now, let p be an odd prime. Let $K = \{\pm I\}$ be the center of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Assume for contradiction that there exists a proper subgroup $H \subset \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ that maps surjectively onto $\mathrm{PSL}_2(p)$. For any $g \in \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, surjectivity provides an $h \in H$ such that $gK = hK$,

which implies $gh^{-1} \in K$. We can then write $g = (gh^{-1})h$; since $gh^{-1} \in K$ and $h \in H$, we have $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) = KH$.

The intersection $H \cap K$ must be a subgroup of K, so it is either $\{I\}$ or K. If $H \cap K = K$, then $K \subseteq H$, which together with $KH = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ implies $H = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. This contradicts our assumption that H is a proper subgroup. Therefore, we must have $H \cap K = \{I\}$.

The conditions $KH = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, $H \cap K = \{I\}$, and $HK = KH$ (since K is the center) imply that $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is the direct product of H and K by [13, Theorem 2.1]. Thus, we have a group isomorphism:

$$\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \cong H \times K = H \times \{\pm I\}.$$

It is a standard result that $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is generated by the matrices $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, both of which have order p. Let's consider the generator T. Under the isomorphism, T corresponds to a pair (h, k) for some $h \in H$ and $k \in K$. The order of T must be $\mathrm{lcm}(\mathrm{ord}(h), \mathrm{ord}(k))$. Since $\mathrm{ord}(T) = p$ (an odd prime) and $\mathrm{ord}(k)$ is either 1 or 2, we must have $\mathrm{ord}(k) = 1$. This means $k = I$. Therefore, T corresponds to the pair (h, I), which implies that T is an element of H. By the same logic, the generator S must also be in H. Since H contains a generating set for $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, it follows that $H = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. This contradicts our initial assumption that H was a proper subgroup. Thus, no such proper subgroup H can exist. □

Remark 3.1.5. *The proof of the fact that* $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *and* $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ *generate* $SL_2(\mathbb{Z}/p\mathbb{Z})$ *can be found in [14, Corollary 3.5].*

Corollary 3.1.1. *If* $p \geq 5$ *is a prime, then the commutator subgroup* $SL_2(\mathbb{Z}/p\mathbb{Z})'$ *of* $SL_2(\mathbb{Z}/p\mathbb{Z})$ *is* $SL_2(\mathbb{Z}/p\mathbb{Z})$.

Proof. Let $G = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. For $p \geq 5$, we know from Lemma 3.1.1(a) that the group $\mathrm{PSL}_2(p)$ is simple. A simple group is abelian if and only if it is cyclic of prime order. The order of $\mathrm{PSL}_2(p)$ is $\frac{p(p^2-1)}{2}$, which is not prime for $p \geq 5$. Thus, $\mathrm{PSL}_2(p)$ is a non-abelian simple group.

The commutator subgroup of any group is always a normal subgroup. Since $\mathrm{PSL}_2(p)$ is simple, its commutator subgroup, $\mathrm{PSL}_2(p)'$, must be either the trivial group or $\mathrm{PSL}_2(p)$ itself. If $\mathrm{PSL}_2(p)'$ were trivial, the group would be abelian, which is a contradiction. Therefore, $\mathrm{PSL}_2(p)' = \mathrm{PSL}_2(p)$.

Now, consider the natural surjective projection map $\pi : G \to \mathrm{PSL}_2(p)$. A standard theorem of group theory states that the image of the commutator subgroup is the commutator subgroup of the image. That is, $\pi(G') = (\mathrm{PSL}_2(p))'$. Combining these results, we have:

$$\pi(G') = \mathrm{PSL}_2(p).$$

This shows that the commutator subgroup $G' = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})'$ is a subgroup of G that maps surjectively onto $\mathrm{PSL}_2(p)$. By Lemma 3.1.2, the only subgroup of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ with this property is $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ itself. Therefore, we must conclude that $G' = G$. □

To generalize the previous result to $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ for an arbitrary integer m, let $d \mid m$ be a divisor of m and consider the surjective group homomorphism

$$\mathrm{pr}_d = \mathrm{pr}_d^{(m)} : \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}),$$

induced by reduction modulo d.

Lemma 3.1.3. *Let $\ell \geq 5$ be a prime and let X be a closed subgroup of $SL_2(\mathbb{Z}_\ell)$ whose image in $SL_2(\mathbb{Z}/\ell\mathbb{Z})$ is $SL_2(\mathbb{Z}/\ell\mathbb{Z})$. Then $X = SL_2(\mathbb{Z}_\ell)$.*

Remark 3.1.6. *The proof in [15] uses an inductive argument to show that*

$$X \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$$

for every $n \in \mathbb{N}$ using properties of the Lie algebra $\mathfrak{sl}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Corollary 3.1.2. *Let H be a subgroup of $SL_2(\mathbb{Z}/p^r\mathbb{Z})$, where $p \geq 5$ is a prime and r is a positive integer. If $pr_p(H) = SL_2(\mathbb{Z}/p\mathbb{Z})$, then $H = SL_2(\mathbb{Z}/p^r\mathbb{Z})$.*

Proof. Let $\pi_r : \mathrm{SL}_2(\mathbb{Z}_p) \to \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$ be the natural projection and consider the preimage $X = \pi_r^{-1}(H)$. The target group $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$ is finite and is thus endowed with the discrete topology, in which every subset is closed. Therefore, the subgroup H is a closed set. Since the projection π_r is continuous, the preimage X is a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_p)$.

The image of X under the mod-p projection $\pi_1 : \mathrm{SL}_2(\mathbb{Z}_p) \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is given by $\pi_1(X) = \mathrm{pr}_p(H)$. By hypothesis, this is $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

Thus, X satisfies the hypotheses of the Lemma 3.1.3, and we conclude that $X = \mathrm{SL}_2(\mathbb{Z}_p)$. Applying the surjective projection π_r to this equality immediately yields

$$H = \pi_r(X) = \pi_r(\mathrm{SL}_2(\mathbb{Z}_p)) = \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z}),$$

which completes the proof. □

Corollary 3.1.3. *For any positive integer m with $(m, 6) = 1$, we have that the commutator subgroup $SL_2(\mathbb{Z}/m\mathbb{Z})'$ is $SL_2(\mathbb{Z}/m\mathbb{Z})$.*

Proof. Since $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \cong \prod_{p^r \| m} \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$ by the Chinese Remainder Theorem, it is enough to show $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})' = \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$ for $p \geq 5$ as the commutator subgroup of a direct product is isomorphic to the direct product of the individual commutator subgroups [16, Result 1.6.2(b)]. Consider the following:

$$\mathrm{pr}_p(\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})') = \mathrm{pr}_p(\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z}))' = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})' = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}).$$

The first equality comes from the fact that the image of the commutator subgroup is the commutator subgroup of the image, and the third equality comes from Corollary 3.1.1. Finally, Corollary 3.1.2 applied to $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})'$ yields the result. □

Corollary 3.1.4. *Let m be a positive integer with $(m, 6) = 1$. If*

$$SL_2(\mathbb{Z}/m\mathbb{Z}) \leq H \leq GL_2(\mathbb{Z}/m\mathbb{Z})$$

then $H' = SL_2(\mathbb{Z}/m\mathbb{Z})$. In particular, $GL_2(\mathbb{Z}/m\mathbb{Z})' = SL_2(\mathbb{Z}/m\mathbb{Z})$.

Proof. Let $G = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ and let $N = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. It is a standard result that N is a normal subgroup of G, with the quotient G/N being isomorphic to the abelian group $(\mathbb{Z}/m\mathbb{Z})^\times$ via the determinant map.

We are given an intermediate subgroup H such that $N \leq H \leq G$. Since $N \triangleleft G$, it follows that N is also a normal subgroup of H. Consider the quotient group H/N. We have the inclusion of groups:

$$H/N \leq G/N \cong (\mathbb{Z}/m\mathbb{Z})^\times.$$

Since any subgroup of an abelian group is abelian, H/N is abelian.

We now use the standard group-theoretic result that if H/N is abelian, then the commutator subgroup H' must be contained in N [3, Section 5.4, Proposition 7(4)]. This gives us our first inclusion:

$$H' \leq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}).$$

From our assumption $N \leq H$, it follows that $N' \leq H'$. Combining the latter and Corollary 3.1.3 gives:

$$\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})' \leq H'.$$

We have shown both $H' \leq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \leq H'$, which together imply the desired equality $H' = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. The particular case for $H = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ follows directly. □

The following definitions are crucial for formulating and proving the subsequent results. We begin by defining two sets associated with the composition factors of a finite group G.

Definition 3.1.4. *Given a finite group G, we define $\mathcal{N}(G)$ to be the set of isomorphism classes of non-abelian composition factors of G itself.*

Definition 3.1.5. *Given a finite group G, we define $Occ(G)$ (for "occurs") to be the set of all non-abelian simple groups that appear as a composition factor of at least one subgroup of G. This can be expressed as the union of the sets $\mathcal{N}(H)$ over all subgroups $H \leq G$:*

$$Occ(G) = \bigcup_{H \leq G} \mathcal{N}(H).$$

The following example illustrates the crucial distinction between these two sets.

Example 3.1.1. *Consider the symmetric group S_n for $n \geq 5$. Its only non-abelian composition factor is the alternating group A_n, so $\mathcal{N}(S_n) = \{A_n\}$.*

Now, let's specialize to the case $G = S_{10}$. We have $\mathcal{N}(S_{10}) = \{A_{10}\}$. However, to compute $Occ(S_{10})$, we must consider all of its subgroups. The group A_5 can be embedded as a subgroup of S_{10} by letting it act on the first 5 elements of a set of 10 and fixing the remaining 5. Since A_5 is simple, its only non-abelian composition factor is itself, so $\mathcal{N}(A_5) = \{A_5\}$.

Because A_5 is a subgroup of S_{10}, the set $Occ(S_{10})$ must contain $\mathcal{N}(A_5)$. It must also contain $\mathcal{N}(S_{10})$. Therefore,

$$\{A_5, A_{10}\} \subseteq Occ(S_{10}).$$

This example clearly shows that the set of non-abelian composition factors found among the subgroups of a group can be strictly larger than the set of non-abelian composition factors of the group itself.

Lemma 3.1.4. *Let G be a finite group. Then $\mathcal{N}(G) = \mathcal{N}(H) \cup \mathcal{N}(G/H)$ where $H \triangleleft G$.*

Proof. Let us first recall that any finite group admits a composition series. Let $\{e\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_n = H$ be a composition series for H. And let $\{H\} = K_0 \triangleleft K_1 \triangleleft \cdots \triangleleft K_m = G$ be a series of subgroups of G such that K_i/H form a composition series for G/H via the correspondence theorem [3, Section 3.3, Theorem 19 and 20] where also $K_i/K_{i-1} \cong (K_i/H)/(K_{i-1}/H)$. Now combine the composition series of H and G/H to form a composition series for G:

$$\{e\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_n = H = K_0 \triangleleft K_1 \triangleleft \cdots \triangleleft K_m = G.$$

The set of composition factors of this series is the union of the composition factors of H and G/H. By the Jordan-Hölder theorem, this set is uniquely determined up to isomorphism. Therefore, the set of non-abelian composition factors $\mathcal{N}(G)$ is the union of $\mathcal{N}(H)$ and $\mathcal{N}(G/H)$. □

Definition 3.1.6. *A finite group G is said to be solvable if it has a subnormal series whose factor groups are all abelian, equivalently if $\mathcal{N}(G) = \emptyset$.*

Lemma 3.1.5. *Let G be a finite group. Then:*

(a) $Occ(G) = \emptyset$ if and only if G is solvable.

(b) If H is a normal subgroup of G, then $Occ(G) = Occ(H) \cup Occ(G/H)$.

Proof. (a) If $\mathrm{Occ}(G) = \emptyset$, then $\mathcal{N}(G) = \emptyset$, which implies that G is solvable. Conversely, if G is solvable, then so are any of its subgroups $H \leq G$. Therefore, $\mathcal{N}(H) = \emptyset$ for all $H \leq G$ and $\mathrm{Occ}(G) = \emptyset$.

(b) We prove the equality by showing two set inclusions.

($\supseteq$) We first show that $\mathrm{Occ}(G) \supseteq \mathrm{Occ}(H) \cup \mathrm{Occ}(G/H)$.

- Let $S \in \mathrm{Occ}(H)$. By definition, $S \in \mathcal{N}(B)$ for some subgroup $B \leq H$. Since B is also a subgroup of G, $\mathcal{N}(B) \subseteq \mathrm{Occ}(G)$, so $S \in \mathrm{Occ}(G)$. Thus, $\mathrm{Occ}(H) \subseteq \mathrm{Occ}(G)$.
- Let $S \in \mathrm{Occ}(G/H)$. Then $S \in \mathcal{N}(L)$ for some $L \leq G/H$. By the Correspondence Theorem, $L = A/H$ for some subgroup A with $H \leq A \leq G$. By Lemma 3.1.4, we know that $\mathcal{N}(L) = \mathcal{N}(A/H) \subseteq \mathcal{N}(A)$. Since $A \leq G$, $\mathcal{N}(A) \subseteq \mathrm{Occ}(G)$. Thus, $\mathrm{Occ}(G/H) \subseteq \mathrm{Occ}(G)$.

Combining these two results gives the first inclusion.

($\subseteq$) For the reverse inclusion, we must show that $\mathrm{Occ}(G) \subseteq \mathrm{Occ}(H) \cup \mathrm{Occ}(G/H)$. This is equivalent to showing that for any arbitrary subgroup $K \leq G$, we have $\mathcal{N}(K) \subseteq \mathrm{Occ}(H) \cup \mathrm{Occ}(G/H)$.

By the Second Isomorphism Theorem [3, Section 3.3, Theorem 18], $H \cap K$ is a normal subgroup of K, and $K/(H \cap K) \cong (KH)/H$. Applying Lemma 3.1.4 to the group K and its normal subgroup $H \cap K$, we have:

$$\begin{aligned} \mathcal{N}(K) &= \mathcal{N}(H \cap K) \cup \mathcal{N}(K/(H \cap K)) \\ &= \mathcal{N}(H \cap K) \cup \mathcal{N}((KH)/H) \end{aligned}$$

Now we analyze each term in the union.

- Since $H \cap K$ is a subgroup of H, by definition $\mathcal{N}(H \cap K) \subseteq \mathrm{Occ}(H)$.
- Since $(KH)/H$ is a subgroup of G/H, by definition $\mathcal{N}((KH)/H) \subseteq \mathrm{Occ}(G/H)$.

Therefore, $\mathcal{N}(K) \subseteq \mathrm{Occ}(H) \cup \mathrm{Occ}(G/H)$. As this holds for any subgroup $K \leq G$, the union over all $\mathcal{N}(K)$ (which is $\mathrm{Occ}(G)$) must also be contained in this set. This proves the inclusion and completes the proof.

□

Lemma 3.1.6. *If m is a positive integer, then*

$$Occ(GL_2(\mathbb{Z}/m\mathbb{Z})) = Occ(SL_2(\mathbb{Z}/m\mathbb{Z})) = \bigcup_{p|m} Occ(PSL_2(p)).$$

Moreover, if $p \geq 5$ is a prime, then

$$\{PSL_2(p)\} \subseteq Occ(PSL_2(p)) \subseteq \{PSL_2(p), A_5\}.$$

Proof. First note that $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \triangleleft \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, thus

$$\mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})) = \mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})) \cup \mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})) = \mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}))$$

as $\mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})) = \emptyset$ since $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ is abelian and hence solvable.

Now consider the subnormal series of the direct product $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) = \prod_{p^r||m} \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$:

$$\{e_1\} \times \cdots \times \{e_k\} \triangleleft \mathrm{SL}_2(\mathbb{Z}/p_1^{r_1}\mathbb{Z}) \times \{e_2\} \times \cdots \times \{e_k\}$$
$$\triangleleft \mathrm{SL}_2(\mathbb{Z}/p_1^{r_1}\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/p_2^{r_2}\mathbb{Z}) \times \{e_3\} \times \cdots \times \{e_k\} \triangleleft \cdots \triangleleft \prod_{i=1}^{k} \mathrm{SL}_2(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$$

whose factors are isomorphic to $\mathrm{SL}_2(\mathbb{Z}/p_1^{r_1}\mathbb{Z}), \ldots, \mathrm{SL}_2(\mathbb{Z}/p_k^{r_k}\mathbb{Z})$. We repeatedly use Lemma 3.1.5(b) to obtain

$$\mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})) = \bigcup_{p^r||m} \mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})).$$

We would now like to show that $\mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})) = \mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}))$. We can show the latter by considering $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})/\ker(\mathrm{pr}_p) \cong \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, which allows us to write

$$\mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})) = \mathrm{Occ}(\ker(\mathrm{pr}_p)) \cup \mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}))$$

where $\mathrm{Occ}(\ker(\mathrm{pr}_p)) = \emptyset$ as $\ker(\mathrm{pr}_p)$ is a p-group and hence is solvable. An easy way to see that $\ker(\mathrm{pr}_p)$ is a p-group is to compute

$$\frac{|\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})|}{|\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})|} = p^{3r-3}.$$

Finally, what's left to show is $\mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})) = \mathrm{Occ}(\mathrm{PSL}_2(p))$, which is clear because $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})/\{\pm I\} = \mathrm{PSL}_2(p)$ and $\{\pm I\}$ is abelian. Therefore,

$$\mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})) = \bigcup_{p^r||m} \mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})) = \bigcup_{p|m} \mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})) = \bigcup_{p|m} \mathrm{Occ}(\mathrm{PSL}_2(p)).$$

The second statement of the Lemma follows from Lemma 3.1.1(a) and (c). □

Remark 3.1.7. *One may wonder if a direct product $G = G_1 \times \cdots \times G_m$ can have a composition factor that is not a composition factor of any of the individual groups G_i. This is not possible. The set of composition factors of G is precisely the union of the sets of composition factors of the G_i. This can be proven by applying Lemma 3.1.4 inductively to the subnormal series:*

$$\{(e_1, \ldots, e_m)\} \lhd G_1 \times \{e_2\} \times \cdots \times \{e_m\} \lhd G_1 \times G_2 \times \{e_3\} \times \cdots \times \{e_m\} \lhd \cdots \lhd G$$

whose factors are isomorphic to $G_1, G_2, \ldots, G_m$. A full proof can be found in the work of Keith Conrad [14, Lemma 4.1].

Corollary 3.1.5. *If $p > 5$ is a prime and m is an integer such that $p \nmid m$, then $\mathrm{PSL}_2(p) \notin \mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}))$.*

Proof. Since $p > 5$, we have by Lemma 3.1.1 that $\mathrm{PSL}_2(p)$ is not isomorphic to A_5 and that $\mathrm{PSL}_2(p)$ is not isomorphic to $\mathrm{PSL}_2(q)$ for any prime $q \mid m$. Thus, $\mathrm{PSL}_2(p) \notin \mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}))$ by Lemma 3.1.6. □

Dickson, in [17], provides a classification of the subgroups of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ up to conjugacy by analyzing their images in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$. This classification is fundamental to the results that follow.

Theorem 3.1.2. *Let $H \leq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ with image $H' \leq \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$. Up to conjugacy, one of the following holds:*

1. *H contains an element of order p.*
   - *(a) $H \leq B(p)$*
   - *(b) $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \leq H$*
2. *H does not contain an element of order p.*
   - *(a) H' is cyclic and $H \leq C_s(p)$ or $C_{ns}(p)$.*
   - *(b) H' is dihedral and $H \leq N(C_s(p))$ or $N(C_{ns})(p)$ but $H \not\leq C_s(p)$, $C_{ns}(p)$*
   - *(c) $H' \simeq A_4, S_4$ or A_5 and $H \not\leq N(C_s(p))$, $N(C_{ns})(p)$.*

Remark 3.1.8. *The Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, $B(p)$, (i.e. group of upper-triangular matrices) is solvable and can be seen by constructing a subnormal series with abelian composition factors. Consider the unipotent subgroup $U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z}/p\mathbb{Z} \right\} \cong (\mathbb{Z}/p\mathbb{Z}, +)$. Notice that U is the kernel of the surjective homomorphism $\phi : B(p) \to (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$ defined by $\phi\left(\begin{pmatrix} a & c \\ 0 & d \end{pmatrix}\right) = (a, d)$, which proves that U is a normal subgroup of $B(p)$. By the First Isomorphism Theorem, the quotient group $B(p)/U \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$ is also abelian. The series $\{I\} \lhd U \lhd B(p)$ thus demonstrates that $B(p)$ is solvable.*

Lemma 3.1.7. *Let $G \leq \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z})$, where $p \geq 5$ is a prime and r is a positive integer. Then the following statements are equivalent:*

(i) $\mathrm{PSL}_2(p) \in \mathrm{Occ}(G)$.

(ii) $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z}) \leq G$.

(iii) $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \leq \mathrm{pr}_p(G)$.

Proof. (ii) $\implies$ (i): $\mathrm{PSL}_2(p)$ is a composition factor of $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$ as $\mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})) = \mathrm{Occ}(\mathrm{PSL}_2(p))$ and $\{\mathrm{PSL}_2(p)\} \subseteq \mathrm{Occ}(\mathrm{PSL}_2(p))$ by Lemma 3.1.6.

(iii) $\implies$ (ii): Consider $H := G' \leq \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z})' = \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z})$ where the last equality follows from Corollary 3.1.4. Since $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \leq \mathrm{pr}_p(G)$ by hypothesis, we have $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})' \leq \mathrm{pr}_p(G)' = \mathrm{pr}_p(G') = \mathrm{pr}_p(H) \leq \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ where the first equality comes from the fact that the image of the commutator subgroup is the commutator subgroup of the image. But $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})' = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ by Corollary 3.1.1, and so $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) = \mathrm{pr}_p(H)$. Therefore, (ii) follows from Corollary 3.1.2 as $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z}) = H = G' \leq G$.

(i) $\implies$ (iii): Let $H := G \cap \ker(\mathrm{pr}_p)$ then by the first isomorphism theorem, $\mathrm{pr}_p(G) \cong G/H$ where $H \leq \ker(\mathrm{pr}_p)$ is a p-group as $\ker(\mathrm{pr}_p)$ is. By Lemma 3.1.5, we have $\mathrm{Occ}(G) = \mathrm{Occ}(H) \cup \mathrm{Occ}(G/H) = \mathrm{Occ}(G/H) = \mathrm{Occ}(\mathrm{pr}_p(G))$ as $\mathrm{Occ}(H) = \emptyset$ since H is a p-group, hence solvable. Now, for any subgroup $K \leq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, we know by Theorem 3.1.2 that $K \geq \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ if and only if $p \mid |K|$ and K is not contained in a Borel subgroup. Now, we apply Theorem 3.1.2 setting $K := \mathrm{pr}_p(G)$. By our assumption, $\mathrm{PSL}_2(p) \in \mathrm{Occ}(G) = \mathrm{Occ}(K)$, which means K is not solvable and hence cannot be contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ as they are solvable Remark 3.1.8. All that is left to show is $p \mid |K|$. $\mathrm{PSL}_2(p) \in \mathrm{Occ}(K)$ so $\mathrm{PSL}_2(p) \cong L/N$ for some $L \leq K$ and $N \lhd L$, which implies $|\mathrm{PSL}_2(p)| \mid |L|$ and $|L| \mid |K|$ by Lagrange's theorem. Furthermore we know $p \mid |\mathrm{PSL}_2(p)|$, so the result follows. □

Theorem 3.1.3. *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ where $(m, 30) = 1$. Then:*

(a) $G = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ if and only if $G \geq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ and $\varphi(m) \mid [G : G']$.

(b) $G \geq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ if and only if $\mathrm{PSL}_2(p) \in \mathrm{Occ}(G)$ for all primes $p \mid m$.

Proof. (a) If $G = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, then clearly $G \geq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. Moreover, $\varphi(m) = [\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})] = [\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})'] = [G : G']$, where the second equality follows from Corollary 3.1.4, so in particular $\varphi(m) \mid [G : G']$.

Conversely, if $G \geq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ then $G' = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ by Corollary 3.1.4 so $[G : G'] \cdot |\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})| = |G|$. Using the fact that $|\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})| = \varphi(m) \cdot |\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})|$ and the second part of the hypothesis, $\varphi(m) \mid [G : G']$ (i.e., $k \cdot \varphi(m) = [G : G']$), we obtain:

$$\begin{aligned} [G : G'] \cdot |\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})| &= |G| \\ k \cdot \varphi(m) \cdot |\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})| &= |G| \\ k \cdot |\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})| &= |G| \end{aligned}$$

Thus, $|\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})|$ divides $|G|$ and hence $G = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

(b) If $G \geq \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$, then $G/\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ is abelian as it is a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$ and hence solvable. Now, $\mathrm{Occ}(G) = \mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})) \cup \mathrm{Occ}(G/\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})) = \mathrm{Occ}(\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})) \supseteq \{\mathrm{PSL}_2(p) : p \mid m\}$ where the first and second equality follow from Lemma 3.1.5, and the containment follows from Lemma 3.1.6.

Conversely, suppose that $\mathrm{Occ}(G) \supseteq \{\mathrm{PSL}_2(p) : p \mid m\}$. For any $p^r \,||\, m$, consider the following:

$$\begin{array}{ccc} \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) & \xrightarrow{\mathrm{pr}_{m/p^r}} & \mathrm{GL}_2(\mathbb{Z}/(m/p^r)\mathbb{Z}) \\ \cong \downarrow & & \downarrow \cong \\ \prod_{q|m} \mathrm{GL}_2(\mathbb{Z}/q^{r_q}\mathbb{Z}) & \xrightarrow{\pi} & \{e\} \times \prod_{\substack{q|m \\ q\neq p}} \mathrm{GL}_2(\mathbb{Z}/q^{r_q}\mathbb{Z}) \end{array}$$

Thus, $\ker(\mathrm{pr}_{m/p^r}) \cong \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z})$. Now, for any subgroup $H \leq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, let $H^{(p)} := H \cap \ker(\mathrm{pr}_{m/p^r})$. Note that $H^{(p)} \lhd H$ is a normal subgroup of H [18, Proposition 7.8] and that $H^{(p)} \leq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})^{(p)} \cong \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z})$.

We claim that $\mathrm{PSL}_2(p) \in \mathrm{Occ}(H^{(p)})$. First note that $\mathrm{PSL}_2(p) \notin \mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}/(m/p^r)\mathbb{Z}))$ by Corollary 3.1.5 as $p \nmid (m/p^r)$. Since $H/H^{(p)} \cong \mathrm{pr}_{m/p^r}(H)$, we can consider the following $\mathrm{Occ}(H) = \mathrm{Occ}(H^{(p)}) \cup \mathrm{Occ}(\mathrm{pr}_{m/p^r}(H))$ by Lemma 3.1.5. Because $\mathrm{Occ}(\mathrm{pr}_{m/p^r}(H)) \subseteq \mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}/(m/p^r)\mathbb{Z}))$ and we know that $\mathrm{PSL}_2(p) \notin \mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}/(m/p^r)\mathbb{Z}))$ but $\mathrm{PSL}_2(p) \in \mathrm{Occ}(H)$ by our hypothesis then we have that $\mathrm{PSL}_2(p) \in \mathrm{Occ}(H^{(p)})$. With the latter, we can apply the (i) $\implies$ (ii) direction of Lemma 3.1.7 to $H^{(p)}$, which is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z})$, and so $\mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z}) \leq H^{(p)}$. Since this is true for all $p \mid m$, we obtain

$$\prod_{p|m} \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z}) \leq \prod_{p|m} H^{(p)} \leq H.$$

But by the Chinese Remainder Theorem, we have

$$\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \cong \prod_{p|m} \mathrm{SL}_2(\mathbb{Z}/p^r\mathbb{Z}),$$

and so we obtain $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \leq H$ as desired. □

3.2. Group Theory for Applicable Subgroups

The exposition in this section follows the appendix of Zywina's work in [19, Appendix] and the second section of his subsequent paper [20, Section 2].

Definition 3.2.1. *The abelianization of a group G, often denoted G^{ab}, is the quotient of G by its commutator subgroup, $G' = [G, G]$. It is defined as:*

$$G^{ab} := G/G'.$$

The abelianization is the largest abelian quotient of G.

Remark 3.2.1 (Universal Property of the Abelianization)**.** *Let $\pi : G \to G^{ab}$ be the canonical projection. For any abelian group H and any group homomorphism $\varphi : G \to H$, there exists a unique homomorphism $\psi : G^{ab} \to H$ such that $\varphi = \psi \circ \pi$.*

Lemma 3.2.1. *(Goursat's Lemma) Let G_1 and G_2 be groups and let $G \leq G_1 \times G_2$ be a subgroup such that the projections $\pi_1 : G \to G_1$ and $\pi_2 : G \to G_2$ are surjective. Then, there exists a group Q and surjective homomorphisms $\psi_1 : G_1 \to Q$, $\psi_2 : G_2 \to Q$ such that*

$$G = \{(a, b) \in G_1 \times G_2 \mid \psi_1(a) = \psi_2(b)\}.$$

Proof. Let $N_1 = (G_1 \times \{e_2\}) \cap G$ and $N_2 = (\{e_1\} \times G_2) \cap G$, then $N_1 = \ker(\pi_2)$ and $N_2 = \ker(\pi_1)$. Note that $N_1 \triangleleft G$ as it is the kernel of π_2, hence $\pi_1(N_1) \leq \pi_1(G)$ as homomorphisms are structure-preserving maps. So it follows $\pi_1(N_1) \leq G_1$ as $\pi_1(G) = G_1$. Similarly we have $\pi_2(N_2) \leq G_2$. Note that $\pi_i(N_i) \cong N_i$, thus $(G_1 \times \{e_2\})/N_1 \cong G_1/\pi_1(N_1)$ and $(\{e_1\} \times G_2)/N_2 \cong G_2/\pi_2(N_2)$.

Define $\psi_1 : G_1 \to G_2/\pi_2(N_2)$ where $a \mapsto b\pi_2(N_2)$ where $(a, b) \in G$. If $(a, b), (a, c) \in G$, then $(e_1, b^{-1}c) = (a, b)^{-1}(a, c) \in G$ implies $b^{-1}c \in \pi_2(N_2)$ and hence $b\pi_2(N_2) = c\pi_2(N_2)$. So, ψ_1 is well-defined. It is easily checked that ψ_1 is a surjective homomorphism. We will now show that $\ker(\psi_1) = \pi_1(N_1)$.

Indeed, if $a \in \ker(\psi_1)$, then for $(a, b) \in G$, $b \in \pi_2(N_2)$. But then $(e_1, b) \in G$ from the definition of N_2 and $(a, e_2) = (a, b)(e_1, b)^{-1} \in G$ which gives $a \in \pi_1(N_1)$. So by the first isomorphism theorem, $G_1/\pi_1(N_1) \cong G_2/\pi_2(N_2)$.

Similarly, we define $\psi_2 : G_2 \to G_1/\pi_1(N_1)$ where $b \mapsto a\pi_1(N_1)$ where $(a, b) \in G$ and obtain $\ker(\psi_2) = \pi_2(N_2)$. The result now follows. □

Remark 3.2.2.

- *Notice that if $G = G_1 \times G_2$, then $\pi_1(N_1) = G_1$ and $\pi_2(N_2) = G_2$. Moreover, $Q = \{e\}$ where $Q := G_1/\pi_1(N_1) \cong G_2/\pi_2(N_2)$ and $G/(\pi_1(N_1) \times \pi_2(N_2)) \cong \{e\}$. In a sense, when $G \leq G_1 \times G_2$, $G/(\pi_1(N_1) \times \pi_2(N_2))$ measures how far G is from being the direct product $G_1 \times G_2$.*

- *Let K be an arbitrary subgroup of $G_1 \times G_2$, not necessarily with surjective projection maps. We can then apply Goursat's Lemma to $\pi_1(K) \times \pi_2(K)$. Thus, Goursat's Lemma is the general result describing a direct product's subgroups.*

The following definition and two subsequent results are not strictly required for the group-theoretic tools this section aims to develop. They are included, however, as they represent an interesting and relevant extension of the ideas discussed.

Definition 3.2.2. *Given a finite group G, we define $In(G)$ to be the set of isomorphism classes of all simple groups that appear as a composition factor of some subgroup $H \leq G$.*

The set $\mathrm{In}(G)$ contains both the abelian and non-abelian simple composition factors. Our previously defined set, $\mathrm{Occ}(G)$, consists of only the non-abelian ones. Therefore, we have the subset relation $\mathrm{Occ}(G) \subseteq \mathrm{In}(G)$.

Lemma 3.2.2. *Let G be a finite group.*

(a) $In(G) = \emptyset$ if and only if $G = \{e\}$.

(b) If H is a normal subgroup of G, then $In(G) = In(H) \cup In(G/H)$.

Proof. (a) The first direction follows from the fact that every nontrivial finite group has a composition series. The other direction is trivial.

(b) The proof is the same as Lemma 3.1.5(b).

□

Lemma 3.2.3. *Let G_1, G_2 be two finite groups. The following statements are equivalent:*

(i) $In(G_1) \cap In(G_2) = \emptyset$.

(ii) Every subgroup of $G_1 \times G_2$ is of the form $H_1 \times H_2$ with $H_1 \leq G_1$ and $H_2 \leq G_2$.

Proof. (i) $\implies$ (ii) Let H be a subgroup of $G_1 \times G_2$ and set $H_1 = \pi_1(H)$ and $H_2 = \pi_2(H)$, where π_1 and π_2 are the projection homomorphisms. We apply Goursat's Lemma to $H \leq H_1 \times H_2$ and obtain $H_1/\pi_1(N_1) \cong H_2/\pi_2(N_2)$ where $N_1 = (H_1 \times \{e_2\}) \cap H$ and $N_2 = (\{e_1\} \times H_2) \cap H$. Let us consider $\phi : H \to H_1/\pi_1(N_1)$ where $(a, b) \mapsto a\pi_1(N_1)$. It is easily checked that ϕ is a surjective homomorphism. We will now show that $\ker(\phi) = \pi_1(N_1) \times \pi_2(N_2)$.

$$\begin{aligned}\ker(\phi) &= \{(a, b) \in H \mid a \in \pi_1(N_1)\} \\ &= \{(a, b) \in H \mid (a, e_2) \in H\} \\ &= \{(a, b) \in H \mid (a, e_2) \in H, (e_1, b) \in H\} \\ &= \pi_1(N_1) \times \pi_2(N_2)\end{aligned}$$

The third equality follows from $(e_1, b) = (a, b)(a, e_2)^{-1} \in H$. As a consequence,

$$H_1/\pi_1(N_1) \cong H/(\pi_1(N_1) \times \pi_2(N_2)) \cong H_2/\pi_2(N_2).$$

Suppose H is not a direct product, i.e., $H \neq H_1 \times H_2$, then $H/(\pi_1(N_1) \times \pi_2(N_2)) \neq \{e\}$ and so we have a non-empty set

$$\mathrm{In}(H_1/\pi_1(N_1)) = \mathrm{In}(H/(\pi_1(N_1) \times \pi_2(N_2))) = \mathrm{In}(H_2/\pi_2(N_2))$$

contained in $\mathrm{In}(G_1) \cap \mathrm{In}(G_2)$ where we implicitly used the second statement of the previous Lemma.

(ii) $\implies$ (i) Suppose there exists $S \in \mathrm{In}(G_1) \cap \mathrm{In}(G_2)$, then there exist subgroups $N_1 \triangleleft H_1$ of G_1 and $N_2 \triangleleft H_2$ of G_2 such that $S \cong H_1/N_1 \cong H_2/N_2$. Let $\phi_i : H_i \to H_i/N_i \cong S$ for $i = 1, 2$. Then $(\phi_1, \phi_2) : H_1 \times H_2 \to S \times S$. Consider the subgroup $D = \{(s, s) \mid s \in S\}$ (the diagonal subgroup) and its inverse image $H = (\phi_1 \times \phi_2)^{-1}(D)$. Then H is a subgroup of $H_1 \times H_2$ as the inverse image of a subgroup is a subgroup. We claim that H is not a direct product of a subgroup of G_1 with a subgroup of G_2.

Note that $\pi_1(H) = H_1$ and $\pi_2(H) = H_2$ which follows from ϕ_i being surjective. So, it suffices to show that $H \neq H_1 \times H_2$. Let $h_1 \in H_1 \setminus N_1$ and $h_2 \in N_2$ (We can always find an $h_1 \in H_1 \setminus N_1$ because N_1 is strictly contained in H_1, and the latter follows from the definition of a composition series). Then $(\phi_1, \phi_2)(h_1, h_2) = (\phi_1(h_1), e_2)$ where $\phi_1(h_1) \neq e_1$, and so $(h_1, h_2) \in (H_1 \times H_2) \setminus H$. □

Lemma 3.2.4. *Let $G_1, \ldots, G_n$ be finite groups, and assume that for each $i \neq j$, $\mathcal{N}(G_i) \cap \mathcal{N}(G_j) = \emptyset$ and $\gcd(|G_i^{ab}|, |G_j^{ab}|) = 1$. Let H be a subgroup of $G_1 \times \cdots \times G_n$ such that $\pi_i(H) = G_i$ for every projection $\pi_i : G_1 \times \cdots \times G_n \to G_i$. Then $H = G_1 \times \cdots \times G_n$.*

Proof. By induction, we may reduce to the case $n = 2$. We apply Goursat's Lemma to $H \leq G_1 \times G_2$ and obtain $G_1/\pi_1(N_1) \cong G_2/\pi_2(N_2)$ where $N_1 = (G_1 \times \{e_2\}) \cap H$ and $N_2 = (\{e_1\} \times G_2) \cap H$. The latter isomorphism and Lemma 3.1.4 gives $\mathcal{N}(G_1/\pi_1(N_1)) = \mathcal{N}(G_2/\pi_2(N_2)) \subseteq \mathcal{N}(G_1) \cap \mathcal{N}(G_2) = \emptyset$, thus $G_1/\pi_1(N_1)$ and $G_2/\pi_2(N_2)$ are solvable.

Recall that G/N is abelian if and only if $G' \leq N$. Moreover, if we have $G' \lhd N \lhd G$, then the Third Isomorphism Theorem yields $(G/G')/(N/G') \cong G/N$, which implies that the order of every abelian quotient of G divides the order of $G^{ab} = G/G'$. Thus G_1 and G_2 have no common abelian quotients besides $\{e\}$ because $\gcd(|G_1^{ab}|, |G_2^{ab}|) = 1$.

We have the following composition series for $G_1/\pi_1(N_1)$:

$$\{e\} \lhd K_1/\pi_1(N_1) \lhd \cdots \lhd K_n/\pi_1(N_1) \lhd G_1/\pi_1(N_1)$$

Then the composition factor $(G_1/\pi_1(N_1))/(K_n/\pi_1(N_1)) \cong G_1/K_n$ is a quotient of G_1 and abelian as $G_1/\pi_1(N_1)$ is solvable. However, $G_1/\pi_1(N_1) \cong G_2/\pi_2(N_2)$ so G_1/K_n is also an abelian composition factor for $G_2/\pi_2(N_2)$ (also solvable) but G_1 and G_2 have no common abelian quotients besides $\{e\}$ and so $G_1/K_n = \{e\}$ which implies $G_1/\pi_1(N_1) = G_2/\pi_2(N_2) = \{e\}$. Furthermore, we obtain $N_1 = G_1 \times \{e_2\}$ and $N_2 = \{e_1\} \times G_2$ meaning that H contains $G_1 \times \{e_2\}$ and $\{e_1\} \times G_2$ hence $H = G_1 \times G_2$. □

In the next examples, our aim is to give explicit descriptions of $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})^{\mathrm{ab}}$, $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})^{\mathrm{ab}}$ and $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})^{\mathrm{ab}}$ for the sake of the Lemmas that come next.

Example 3.2.1. *It is known that* $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$*, so we'll now find the abelianization of* S_3*. The only normal subgroups of* S_3 *are* $\{e\}$, $\langle(123)\rangle$ *and itself. We quotient* S_3 *by all three of them and find that the largest abelian quotient is* $S_3/\langle(123)\rangle \cong \mathbb{Z}/2\mathbb{Z}$*. Therefore,* $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})^{\mathrm{ab}} \cong \mathbb{Z}/2\mathbb{Z}$*.*

Example 3.2.2. *The order of* $SL_2(\mathbb{Z}/3\mathbb{Z})^{ab}$ *can be computed in Sage as follows:*

```
SL2Z3Z = SL(2,Integers(3))
commutators = list(set([A*B*A^(-1)*B^(-1) for A in SL2Z3Z for B in SL2Z3Z]))
SL2Z3Z_prime = SL2Z3Z.subgroup(commutators)
elements_SL2Z3Z_prime = [A for A in SL2Z3Z_prime]
order_SL2Z3Z_ab = len(SL2Z3Z)/len(SL2Z3Z_prime)
```

From the code above we obtain $|\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})^{\mathrm{ab}}| = 3$ *which means* $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})^{\mathrm{ab}} \cong \mathbb{Z}/3\mathbb{Z}$*. We are then able to find explicit representatives for the cosets of* $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})^{\mathrm{ab}}$ *by selecting any element of* $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}) \setminus \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})'$ *and using it as the generator of* $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})^{\mathrm{ab}}$*. The fourth line of code allows us to view the elements of* $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})'$ *explicitly. We see that* $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \notin \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})'$ *and so we use it as the generator. The set of coset representatives for* $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})^{\mathrm{ab}}$ *is:* $\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} \right\}$*. Also note that* $-I = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})'$*. The latter will become useful in the discussion following the next example.*

Example 3.2.3. *Similarly, the order of* $SL_2(\mathbb{Z}/4\mathbb{Z})^{ab}$ *can be computed in Sage as follows:*

```
SL2Z4Z = SL(2,Integers(4))
commutators = list(set([A*B*A^(-1)*B^(-1) for A in SL2Z4Z for B in SL2Z4Z]))
SL2Z4Z_prime = SL2Z4Z.subgroup(commutators)
elements_SL2Z4Z_prime = [A for A in SL2Z4Z_prime]
order_SL2Z4Z_ab = len(SL2Z4Z)/len(SL2Z4Z_prime)
```

We obtain $|\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})^{\mathrm{ab}}| = 4$*, which means* $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})^{\mathrm{ab}} \cong \mathbb{Z}/4\mathbb{Z}$ *or* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*. We notice that* $-I = \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix} \notin \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})'$*, thus, we use it as one of our coset representatives. However, the order of* $-I$ *in* $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})^{\mathrm{ab}}$ *is 2, so it is still not clear whether* $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})^{\mathrm{ab}}$ *is isomorphic to* $\mathbb{Z}/4\mathbb{Z}$ *or* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *yet. We need to search for one more representative. We compute the coset of* $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})^{\mathrm{ab}}$ *with* $-I$ *as representative with the code below.*

```
minusI = Matrix(Integers(4),[[3, 0], [0, 3]])
coset_minusI = [minusI*B for B in SL2Z4Z_prime]
```

We notice that $\begin{bmatrix} 1 & 3 \\ 2 & 3 \end{bmatrix}$ *is not in* $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})'$ *nor in the coset of* $-I$*. The order of* $\begin{bmatrix} 1 & 3 \\ 2 & 3 \end{bmatrix}$ *in* $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})^{\mathrm{ab}}$ *is 4, so we have found its generator and namely that* $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})^{\mathrm{ab}} \cong \mathbb{Z}/4\mathbb{Z}$*. The set of coset representatives for* $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})^{\mathrm{ab}}$ *is* $\left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 3 \\ 2 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix} \right\}$.

The universal property of the abelianization of a group gives us the following diagram:

$$\begin{array}{ccc} \mathrm{SL}_2(\mathbb{Z}) & \xrightarrow{f} & \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})^{\mathrm{ab}} \\ {\scriptstyle g}\downarrow & \nearrow_{h} & \\ \mathrm{SL}_2(\mathbb{Z})^{\mathrm{ab}} & & \end{array}$$

Where f is the composition of the reduction map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ with the natural surjection map $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})' = \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})^{\mathrm{ab}}$. Moreover, g is the natural surjection map, and h is the unique homomorphism we obtain from the universal property. As seen by the example above, f takes $-I$ to one of the non-identity cosets represented in our example by $-I$. In other words, $-I \notin \ker(f)$. Consequently, $-I \notin \ker(g)$ since $f = h \circ g$, which tells us that $-I \notin \mathrm{SL}_2(\mathbb{Z})'$.

It is well known that $-I$ is in the center of $\mathrm{SL}_2(\mathbb{Z})$, so it commutes with everything, and in particular, it doesn't contribute to the commutator structure. Using this and $-I \notin \mathrm{SL}_2(\mathbb{Z})'$, we obtain $\mathrm{SL}_2(\mathbb{Z})' \cong \mathrm{PSL}_2(\mathbb{Z})'$ where $\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$.

Lemma 3.2.5. *Let* $m > 1$ *be an integer, and define* $b := \gcd(m, 12)$*. Reduction modulo* b *induces an isomorphism*

$$SL_2(\mathbb{Z}/m\mathbb{Z})^{ab} \xrightarrow{\sim} SL_2(\mathbb{Z}/b\mathbb{Z})^{ab}.$$

The group $SL_2(\mathbb{Z}/m\mathbb{Z})^{ab}$ *is cyclic of order* b*.*

Proof. It is well-known that the group $PSL_2(\mathbb{Z})$ has a presentation $\langle A, B : A^2 = 1, B^3 = 1\rangle$ [14, Theorem C.1], thus $PSL_2(\mathbb{Z})^{ab}$ is a cyclic group of order 6.

From our discussion above, we learned that $\mathrm{SL}_2(\mathbb{Z})' \cong \mathrm{PSL}_2(\mathbb{Z})'$ which yields the following:

$$\mathrm{PSL}_2(\mathbb{Z})/\,\mathrm{PSL}_2(\mathbb{Z})' \cong (\mathrm{SL}_2(\mathbb{Z})/\{\pm I\})/\,\mathrm{SL}_2(\mathbb{Z})' \cong (\mathrm{SL}_2(\mathbb{Z})/\,\mathrm{SL}_2(\mathbb{Z})')/\{\pm I\}$$

More succinctly, $\mathrm{SL}_2(\mathbb{Z})^{\mathrm{ab}}/\{\pm I\} \cong \mathrm{PSL}_2(\mathbb{Z})^{\mathrm{ab}}$ which means $|\,\mathrm{SL}_2(\mathbb{Z})^{\mathrm{ab}}|$ is either 6 or 12. Suppose it is 6, then $-I$ lies in the coset represented by the identity in $\mathrm{SL}_2(\mathbb{Z})^{\mathrm{ab}}$, but that's impossible if $-I \notin \mathrm{SL}_2(\mathbb{Z})'$ thus $|\,\mathrm{SL}_2(\mathbb{Z})^{\mathrm{ab}}| = 12$.

We have seen in an earlier proof that the commutator subgroup of a direct product is isomorphic to the direct product of the commutator subgroups of each component [16, Result 1.6.2(b)]. The latter and [3, Section 5.1, Exercise 14] give us that the abelianization of a direct product is isomorphic to the direct product of the abelianizations of each component. We now apply this result to $\mathrm{SL}_2(\mathbb{Z}/12\mathbb{Z}) \cong \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ and obtain

$$\mathrm{SL}_2(\mathbb{Z}/12\mathbb{Z})^{\mathrm{ab}} \cong \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})^{\mathrm{ab}} \times \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})^{\mathrm{ab}} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$$

where the before last isomorphism follows from the two previous examples.

For each integer $m > 1$, the natural reduction map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ is onto [14, Theorem 3.2]. The previous surjection induces:

$$\begin{array}{ccc} \mathrm{SL}_2(\mathbb{Z}) & \twoheadrightarrow & \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{\mathrm{ab}} \\ \downarrow & \nearrow & \\ \mathrm{SL}_2(\mathbb{Z})^{\mathrm{ab}} & & \end{array}$$

In particular, $\mathrm{SL}_2(\mathbb{Z})^{\mathrm{ab}} \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/12\mathbb{Z})^{\mathrm{ab}}$ where both groups are of order 12, therefore $\mathrm{SL}_2(\mathbb{Z})^{\mathrm{ab}} \cong \mathrm{SL}_2(\mathbb{Z}/12\mathbb{Z})^{\mathrm{ab}}$. Finally, $\mathrm{SL}_2(\mathbb{Z}/12\mathbb{Z})^{\mathrm{ab}} \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{\mathrm{ab}}$ meaning:

$$\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{\mathrm{ab}} \cong \mathrm{SL}_2(\mathbb{Z}/2^e\mathbb{Z})^{\mathrm{ab}} \times \mathrm{SL}_2(\mathbb{Z}/3^f\mathbb{Z})^{\mathrm{ab}},$$

where $\gcd(m, 12) = 2^e 3^f$. Moreover, $\mathrm{SL}_2(\mathbb{Z}/2^e\mathbb{Z})^{\mathrm{ab}} \cong \{e\}$ or $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$ when $2^e = 1$ or $2^e = 2$ or $2^e \geq 4$ respectively, and $\mathrm{SL}_2(\mathbb{Z}/3^f\mathbb{Z})^{\mathrm{ab}} \cong \{e\}$ or $\mathbb{Z}/3\mathbb{Z}$ when $3^f = 1$ or $3^f \geq 3$ respectively. □

Remark 3.2.3. *Our last step in the proof implies Corollary 3.1.3.*

We have seen in Lemma 3.1.1 that for $p \geq 5$, $\mathrm{PSL}_2(p)$ is a non-abelian simple group. It has been hinted, but never explicitly said, until now that the groups $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ are solvable. Lemma 3.1.4 of the group-theoretic section allows us to write $\mathcal{N}(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})) = \mathcal{N}(\{\pm I\}) \cup \mathcal{N}(\mathrm{PSL}_2(p)) = \mathcal{N}(\mathrm{PSL}_2(p)) = \{\mathrm{PSL}_2(p)\}$. Similarly to the proof of Lemma 3.1.6, with the previous information, we obtain:

$$\mathcal{N}(\mathrm{SL}_2(\mathbb{Z}/d\mathbb{Z})) = \bigcup_{p|d} \mathcal{N}(\mathrm{PSL}_2(p)) = \{\mathrm{PSL}_2(p) \mid p|d, p \geq 5\}$$

where $d \in \mathbb{Z}_{>1}$.

Lemma 3.2.6. *Let $m, n \in \mathbb{Z}_{>1}$ be relatively prime and let H be a subgroup of $\mathrm{SL}_2(\mathbb{Z}/mn\mathbb{Z})$. Then $H = \mathrm{SL}_2(\mathbb{Z}/mn\mathbb{Z})$ if and only if H surjects onto $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ by reduction modulo m and n, respectively.*

Proof. The first direction is immediate.

Suppose H surjects onto $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. Since $\gcd(m, n) = 1$, we have $\mathcal{N}(\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})) \cap \mathcal{N}(\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})) = \emptyset$ by the discussion above and Lemma 3.2.5 tells us that $\gcd(|\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})^{\mathrm{ab}}|, |\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})^{\mathrm{ab}}|) = \gcd(m, n, 12) = 1$. The result is now a direct consequence of Lemma 3.2.4. □

Lemma 3.2.7. *Let $f : G \to H$ be a surjective group homomorphism and let $K \leq H$ be a subgroup of finite index. Then $f^{-1}(K)$ is a subgroup of G and*

$$[G : f^{-1}(K)] = [H : K].$$

Proof. The fact that $f^{-1}(K)$ is a subgroup of G is a well-known result from group theory [3, Section 3.1, Exercise 1].

For each coset $hK \in H/K$, its preimage under f is the set $f^{-1}(hK) := \{g \in G \mid f(g) \in hK\}$. Note that $f^{-1}(hK) = gf^{-1}(K)$ where $f(g) = h$. This shows that each coset of K in H corresponds to a coset of $f^{-1}(K)$ in G. Consider the map:

$$\phi : G/f^{-1}(K) \to H/K \quad \text{defined by} \quad \phi(gf^{-1}(K)) = f(g)K.$$

We show that ϕ is a well-defined bijection.

Well-defined: We need to show that if $g_1 f^{-1}(K) = g_2 f^{-1}(K)$, then $f(g_1)K = f(g_2)K$.

$$\begin{aligned} g_1 f^{-1}(K) = g_2 f^{-1}(K) &\implies g_1^{-1} g_2 \in f^{-1}(K) \\ &\implies f(g_1^{-1} g_2) \in K \\ &\implies f(g_1)^{-1} f(g_2) \in K \\ &\implies f(g_1)K = f(g_2)K. \end{aligned}$$

Thus, ϕ is well-defined.

Surjective: It is induced by the surjectivity of f.

Injective: We need to show that if $\phi(g_1 f^{-1}(K)) = \phi(g_2 f^{-1}(K))$, then $g_1 f^{-1}(K) = g_2 f^{-1}(K)$.

$$\begin{aligned} \phi(g_1 f^{-1}(K)) = \phi(g_2 f^{-1}(K)) &\implies f(g_1)K = f(g_2)K \\ &\implies f(g_1)^{-1} f(g_2) \in K \\ &\implies f(g_1^{-1} g_2) \in K \\ &\implies g_1^{-1} g_2 \in f^{-1}(K) \\ &\implies g_1 f^{-1}(K) = g_2 f^{-1}(K). \end{aligned}$$

Thus, ϕ is injective.

Since ϕ is a well-defined bijection between the sets of cosets $G/f^{-1}(K)$ and H/K. We obtain,

$$[G : f^{-1}(K)] = [H : K].$$

□

Lemma 3.2.8. *There is no proper subgroup S of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ such that $\{\pm I\}S = \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.*

Proof. Suppose there is a proper subgroup, call it S, such that $\{\pm I\}S = \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. Let S_i be the image of S in $\mathrm{SL}_2(\mathbb{Z}/\ell_i^{e_i}\mathbb{Z})$ (where $n = \prod \ell_i^{e_i}$). If for every i, $S_i = \mathrm{SL}_2(\mathbb{Z}/\ell_i^{e_i}\mathbb{Z})$ then by Lemma 3.2.6 $S = \prod_i S_i = \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$, contradicting that S is proper. So there is a prime, ℓ_j, such that $S_j \subsetneq \mathrm{SL}_2(\mathbb{Z}/\ell_j^{e_j}\mathbb{Z})$. Moreover, $\{\pm I\}S_j = \mathrm{SL}_2(\mathbb{Z}/\ell_j^{e_j}\mathbb{Z})$ since the reduction of $\{\pm I\}S$ is equal to $\{\pm I\}S_j$. So without loss of generality, we may assume that $n = \ell^e$ and now set $S := S_j$.

The group S has index 2 in $\mathrm{SL}_2(\mathbb{Z}/\ell^e\mathbb{Z})$; therefore, S is normal and $\mathrm{SL}_2(\mathbb{Z}/\ell^e\mathbb{Z})/S \cong \mathbb{Z}/2\mathbb{Z}$. Recall that if G is a group, then every abelian quotient is a quotient of G^{ab}. So, $2 = |\mathbb{Z}/2\mathbb{Z}|$ must divide $|\mathrm{SL}_2(\mathbb{Z}/\ell^e\mathbb{Z})^{ab}| = \gcd(\ell^e, 12)$, by Lemma 3.2.5, which forces ℓ to be 2. Moreover, from Lemma 3.2.5, we have that $\mathrm{SL}_2(\mathbb{Z}/2^e\mathbb{Z})^{ab} \cong \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$, depending on e.

We claim that S is the unique group of index 2 in $\mathrm{SL}_2(\mathbb{Z}/2^e\mathbb{Z})$. The number of index 2 subgroups for a group G is equal to the number of nontrivial homomorphisms from G to $\mathbb{Z}/2\mathbb{Z}$. The homomorphisms correspond to elements of $\mathrm{Hom}(G^{ab}, \mathbb{Z}/2\mathbb{Z})$ since every homomorphism from G to $\mathbb{Z}/2\mathbb{Z}$ factors through its abelianization. In either case when $\mathrm{SL}_2(\mathbb{Z}/2^e\mathbb{Z})^{ab} \cong \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$, there exists exactly one such nontrivial homomorphism. So we conclude that S is the unique subgroup of index 2 in $\mathrm{SL}_2(\mathbb{Z}/2^e\mathbb{Z})$.

The uniqueness of S and Lemma 3.2.7 tells us that S maps to $A_3 \cong \mathbb{Z}/3\mathbb{Z}$, the unique index 2 subgroup in $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$, under the reduction homomorphism $\mathrm{SL}_2(\mathbb{Z}/2^e\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$. Therefore, $\{\pm I\}S$ maps to A_3 also, as $I \equiv -I \pmod 2$. But we assumed $\{\pm I\}S = \mathrm{SL}_2(\mathbb{Z}/2^e\mathbb{Z})$, and the image of $\mathrm{SL}_2(\mathbb{Z}/2^e\mathbb{Z})$ under the reduction map is $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) = S_3$. This implies $S_3 = A_3$, which is false. This contradiction ensures no such S exists. □

Fix an integer $n \geq 2$. For an elliptic curve $E/\mathbb{Q}$, let $E[n]$ be the n-torsion subgroup. After choosing a basis for $E[n]$ as a $\mathbb{Z}/n\mathbb{Z}$-module, the natural $G_{\mathbb{Q}}$-action on $E[n]$ can be expressed in terms of a Galois representation,

$$\rho_{E,n} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

We now describe some restrictions on the possible images of $\rho_{E,n}$.

Definition 3.2.3 (Applicable Subgroup)**.** *We say that a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is applicable if it satisfies the following conditions:*

- $G \neq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$,
- $-I \in G$ *and* $\det(n) = (\mathbb{Z}/N\mathbb{Z})^\times$,
- G *contains an element with trace 0 and determinant* -1 *that fixes a point in* $(\mathbb{Z}/n\mathbb{Z})^2$ *of order* n.

Remark 3.2.4. *The property of being an applicable subgroup is invariant under conjugation. We now show that each condition from the above condition is invariant under conjugation:*

1. *The property of being a proper subgroup is preserved, as conjugation is an automorphism of the ambient group.*

2. *The determinant of a subgroup is invariant under conjugation. Furthermore, since $-I$ is a central element, it is fixed by conjugation.*

3. *If $M \in G$ has trace 0 and determinant -1, its conjugate gMg^{-1} has the same trace and determinant, as both are invariant under conjugation. Moreover, if M fixes a point v of order n, then gMg^{-1} fixes the point gv. This new point gv also has order n since g is an automorphism of the module $(\mathbb{Z}/n\mathbb{Z})^2$*

This definition is justified by the following.

Proposition 3.2.1. *Let $E/\mathbb{Q}$ be an elliptic curve for which the mod-n Galois representation $\rho_{E,n}$ is not surjective. Then the subgroup $\{\pm I\}\rho_{E,n}(G_{\mathbb{Q}})$ is an applicable subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.*

Proof. Set $G := \{\pm I\}\rho_{E,n}(G_{\mathbb{Q}})$. Clearly G contains $-I$. By Lemma 2.4.2, we have that $\det(\rho_{E,n}(G_{\mathbb{Q}})) = (\mathbb{Z}/n\mathbb{Z})^\times$, so $\det(G) = (\mathbb{Z}/n\mathbb{Z})^\times$.

Let $c \in G_{\mathbb{Q}}$ be an automorphism corresponding to complex conjugation under some embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and set $g := \rho_{E,n}(c)$. As a topological group, the connected component of $E(\mathbb{R})$ containing the identity is isomorphic to S^1 [21, Chapter 2.2, p.17]. Therefore $E(\mathbb{R})$ contains a point P_1 of order n and we know $P_1 \in E(\mathbb{Q})$ as $E(\overline{\mathbb{Q}})$ contains all points of finite order on an elliptic curve. We may assume that $\rho_{E,n}$ is chosen with respect to a basis whose first term is P_1, and hence g is upper triangular whose first diagonal term is 1. We know from Lemma 2.4.2 that $\sigma(\zeta_n) = \zeta_n^{\det(\rho_{E,n}(\sigma))}$ and because c acts by inversion on n-th roots of unity, $c(\zeta_n) = \zeta_n^{-1}$. Thus $\det(g) = -1$. Therefore g is upper triangular with diagonal entries 1 and -1 and hence $\mathrm{tr}(g) = 0$.

Now suppose that $G = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Define $S := \rho_{E,n}(G_{\mathbb{Q}}) \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. Since $G = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, $\rho_{E,n}(G_{\mathbb{Q}}) \neq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ (by hypothesis), and $\det(\rho_{E,n}(G_{\mathbb{Q}})) = (\mathbb{Z}/n\mathbb{Z})^\times$, we deduce that $S \neq \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. If $S = \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$, then $\rho_{E,n}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ by a similar decomposition argument as in Example 4.2.1 which would then contradict the hypothesis. Moreover, it follows from $G = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) = \{\pm I\}\rho_{E,n}(G_{\mathbb{Q}})$ that $\{\pm I\}S = \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$. However, the existence of such a proper subgroup S is impossible by Lemma 3.2.8. So we must have $G \neq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. □

Remark 3.2.5. *If we relax Definition 3.2.3 by removing the condition that $-I \in G$, then for any elliptic curve E, the image of its Galois representation, $\rho_{E,n}(G_{\mathbb{Q}})$, is a subgroup satisfying this less restrictive definition. The condition $-I \in G$ was included in the definition by experts in the field because its presence allows one to associate a modular curve X_G to the subgroup G. In the Appendix A.1 where we present the code to compute applicable subgroups, we will, in fact, compute all subgroups satisfying this more slack definition.*

4. Entanglements in Adelic Galois Representations

Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$ and let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$, where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. We have for $n \geq 2$ the n-torsion group $E[n]$ of $E(\overline{\mathbb{Q}})$ 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 $T_\ell(E) = \varprojlim_k E[\ell^k]$ 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 $T(E) \cong \prod_\ell T_\ell(E) \cong \widehat{\mathbb{Z}}^2$ and its associated full Galois representation

$$\rho_E : G_{\mathbb{Q}} \to \mathrm{Aut}(T(E)) \cong \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

Let's recall the following isomorphism $\phi : \hat{\mathbb{Z}} \cong \prod_\ell \mathbb{Z}_\ell$. Note that ϕ induces an isomorphism $\mathrm{GL}_2(\hat{\mathbb{Z}}) \cong \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$. Let's call this induced isomorphism Φ. If $X \in \mathrm{GL}_2(\hat{\mathbb{Z}})$ has entries $x_{ij} \in \hat{\mathbb{Z}}$, then $x_{ij} = (x_{ij,\ell})_\ell$ where $x_{ij,\ell} \in \mathbb{Z}_\ell$. Then $\Phi(X) = (X_\ell)_\ell$, where X_ℓ is the matrix $(x_{ij,\ell})$ with entries in $\mathbb{Z}_\ell$.

The image of the full adelic representation is $\rho_E(G_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$. The map ψ takes an element $X \in \rho_E(G_{\mathbb{Q}})$ and maps it to its "tuple of components" under the isomorphism Φ.

$$\psi : \rho_E(G_{\mathbb{Q}}) \to \prod_\ell \rho_{E,\ell^\infty}(G_{\mathbb{Q}}) \subseteq \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell),$$

Essentially, if $\sigma \in G_{\mathbb{Q}}$, then $\rho_E(\sigma)$ is a matrix in $\mathrm{GL}_2(\hat{\mathbb{Z}})$. $\psi(\rho_E(\sigma))$ is the tuple $(\rho_{E,\ell^\infty}(\sigma))_\ell$.

Crucially, ψ is always injective. If $\rho_E(\sigma)$ acts as the identity on all torsion, it certainly acts as the identity on $T_\ell(E)$ for every ℓ. Conversely, if $(\rho_{E,\ell^\infty}(\sigma))_\ell$ is the identity tuple (i.e., $\rho_{E,\ell^\infty}(\sigma)$ is identity for all ℓ), then $\rho_E(\sigma)$ must be the identity. In other words, the kernel is trivial.

The "maximum possible size" for the image $\rho_E(G_{\mathbb{Q}})$ would be the full $\mathrm{GL}_2(\hat{\mathbb{Z}})$. This never happens for an elliptic curve over $\mathbb{Q}$ as we'll see in Proposition 4.4.2. Moreover, for a non-CM elliptic curve over $\mathbb{Q}$, Serre's Open Image Theorem says $\rho_E(G_{\mathbb{Q}})$ is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, which means it has finite index. This implies $\rho_{E,\ell^\infty}(G_{\mathbb{Q}})$ is $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for all but finitely many primes ℓ. We have two ways in which the image of the full representation is smaller than it could be.

Vertical Entanglement: $\rho_{E,\ell^\infty}(G_{\mathbb{Q}})$ is non-surjective for some ℓ An elliptic curve $E/\mathbb{Q}$ is said to have a vertical entanglement if there is at least one prime ℓ where the image of the ℓ-adic representation, $\rho_{E,\ell^\infty}(G_{\mathbb{Q}})$, is a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. The group $\mathrm{GL}_2(\mathbb{Z}_\ell)$ is the "largest possible" image for the ℓ-adic representation.

Horizontal Entanglement: The map ψ is not surjective Recall $\psi : \rho_E(G_{\mathbb{Q}}) \hookrightarrow \prod_\ell \rho_{E,\ell^\infty}(G_{\mathbb{Q}})$. If ψ is not surjective, it means that the adelic image $\rho_E(G_{\mathbb{Q}})$ is strictly smaller than the Cartesian product of the individual ℓ-adic images. These individual images, $\rho_{E,\ell^\infty}(G_{\mathbb{Q}})$, might themselves already be smaller than $\mathrm{GL}_2(\mathbb{Z}_\ell)$ due to a vertical entanglement. When

ψ is not surjective, indicating that $\rho_E(G_{\mathbb{Q}})$ does not "fill" this product of its actual ℓ-adic components, we call this phenomenon horizontal entanglement.

Before we proceed to our analysis of vertical and horizontal entanglements, we must first define two important quantities associated with an elliptic curve: the adelic level and the adelic index.

4.1. Adelic Level and Index

Let $E/\mathbb{Q}$ be an elliptic curve with its adelic Galois representation $\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\hat{\mathbb{Z}})$. For any integer $n \geq 2$, we define the natural projection map onto the components corresponding to primes dividing n:

$$P_n : \mathrm{GL}_2(\hat{\mathbb{Z}}) \cong \prod_{\ell} \mathrm{GL}_2(\mathbb{Z}_\ell) \longrightarrow \prod_{\ell | n} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Consider the following composition map:

$$\phi_n : G_{\mathbb{Q}} \xrightarrow{\rho_E} \mathrm{GL}_2(\hat{\mathbb{Z}}) \cong \prod_{\ell} \mathrm{GL}_2(\mathbb{Z}_\ell) \xrightarrow{P_n} \prod_{\ell | n} \mathrm{GL}_2(\mathbb{Z}_\ell)$$

We denote the image of this map by G_n:

$$G_n := \mathrm{im}(\phi_n) = P_n(\rho_E(G_{\mathbb{Q}})) \leq \prod_{\ell | n} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Remark 4.1.1 (Kernel and Image of ϕ_n)**.** *The kernel* $\ker(\phi_n)$ *consists of all* $\sigma \in G_{\mathbb{Q}}$ *such that* $\rho_E(\sigma)$ *projects trivially onto* $\prod_{\ell|n} \mathrm{GL}_2(\mathbb{Z}_\ell)$*. This means* $\rho_{E,\ell^\infty}(\sigma)$ *must be the identity for all primes* $\ell \mid n$*. This is equivalent to* σ *fixing all points in* $E[\ell^m]$ *for all* $m \geq 1$ *and all* $\ell | n$*. This set of points generates the field extension* $K_n := \mathbb{Q}(\bigcup_{m \geq 1} E[n^m])$*. The field* K_n *can be called the "n-power torsion field" of* E*. By Galois theory,*

$$\ker(\phi_n) = \mathrm{Gal}(\overline{\mathbb{Q}}/K_n).$$

By the First Isomorphism Theorem for groups and the fundamental theorem of Galois theory, we have

$$G_n \cong G_{\mathbb{Q}}/\ker(\phi_n) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\mathrm{Gal}(\overline{\mathbb{Q}}/K_n) \cong \mathrm{Gal}(K_n/\mathbb{Q}).$$

For brevity, let $G(n)$ denote the image of the mod n representation: $G(n) := \rho_{E,n}(G_{\mathbb{Q}}) \leq GL_2(\mathbb{Z}/n\mathbb{Z})$. Recall that $G(n) \cong \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$.

We now define conditions related to how the full adelic image $\rho_E(G_{\mathbb{Q}})$ relates to its projections G_n and reductions $G(n)$.

Definition 4.1.1 (Splitting Integer)**.** *An integer* $n \in \mathbb{Z}_{\geq 2}$ *is said to split* ρ_E *if the image of the adelic representation decomposes as a direct product corresponding to the prime factors of* n*:*

$$\rho_E(G_{\mathbb{Q}}) \cong G_n \times \prod_{\ell \nmid n} \mathrm{GL}_2(\mathbb{Z}_\ell)$$

Remark 4.1.2.

- *The property of n splitting ρ_E depends only on the set of prime factors of n, not on the specific powers of those primes appearing in n. For example, if 6 splits ρ_E, then 12 also splits ρ_E.*
- *The group G_n is a subgroup of the product $\prod_{\ell|n} \mathrm{GL}_2(\mathbb{Z}_\ell)$, but it is not necessarily equal to the product of the individual ℓ-adic images, $\prod_{\ell|n} \rho_{E,\ell^\infty}(G_\mathbb{Q})$. There might be "horizontal" relations or entanglement between the different ℓ-adic components within G_n.*

Now we relate the ℓ-adic information contained in G_n to the mod n information in $G(n)$. Let

$$\pi_n : \prod_{\ell|n} \mathrm{GL}_2(\mathbb{Z}_\ell) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

be the natural reduction map.

Definition 4.1.2 (Stable Integer)**.** *An integer $n \in \mathbb{Z}_{\geq 2}$ is said to be stable (for ρ_E) if the projected adelic image G_n is exactly the pre-image of the mod n image under the reduction map π_n. That is, n is stable if*

$$G_n = \pi_n^{-1}(G(n)).$$

Remark 4.1.3. *In the following lemma and subsequent definitions, we will use π_n to denote the reduction map from the full adelic group $\mathrm{GL}_2(\hat{\mathbb{Z}})$ to $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.*

Lemma 4.1.1. *For every elliptic curve $E/\mathbb{Q}$ without CM, there is a positive integer m which splits ρ_E and is stable for ρ_E.*

Proof. Let $G := \rho_E(G_\mathbb{Q})$. Since G is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}}) \cong \varprojlim_n \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ according to Serre's open image theorem (2.5.1), it contains an open neighborhood of the identity matrix I. By Proposition 1.3.4, this implies that G contains some principal congruence subgroup U_m for an integer $m \geq 1$. Recall that $U_m = \ker(\pi_m : \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}))$.

We claim that this integer m satisfies $G = \pi_m^{-1}(G(m))$, where $G(m) = \pi_m(G)$ is the reduction of G modulo m.

($\subseteq$) Let $g \in G$. By definition of $G(m)$, we have $\pi_m(g) \in G(m)$. This directly implies that $g \in \pi_m^{-1}(G(m))$.

($\supseteq$) Let $h \in \pi_m^{-1}(G(m))$ then $\pi_m(h) \in G(m)$. By the definition of $G(m)$, there exists some element $g \in G$ such that $\pi_m(h) = \pi_m(g)$. We have $\pi_m(hg^{-1}) = \pi_m(h)\pi_m(g)^{-1} = \pi_m(g)\pi_m(g)^{-1} = I$, where I is the identity in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Therefore, $hg^{-1} \in \ker(\pi_m) = U_m$. Since we established that $U_m \subseteq G$, we have $hg^{-1} \in G$. Because G is a group and both $hg^{-1} \in G$ and $g \in G$, their product $h = (hg^{-1})g$ must also be an element of G.

Finally, $G = \pi_m^{-1}(G(m)) = G_m \times \prod_{\ell\nmid m} \mathrm{GL}_2(\mathbb{Z}_\ell)$. □

Given an integer $m \in \mathbb{Z}_{\geq 2}$ which is *stable* and *splits* ρ_E, we see that the adelic image $G := \rho_E(G_\mathbb{Q})$ is completely determined by its reduction modulo m, denoted by $G(m)$. The structure of G can therefore be described by finitely many conditions related to the finite group $G(m)$. Note also that if an integer m is stable and splits ρ_E, then so is any integer m' such $m \mid m'$. The group G has the following invariants:

Definition 4.1.3 (Adelic Level)**.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve. The Adelic Level of G is the smallest positive integer m_E such that G is the full inverse image of its projection modulo m_E meaning*

$$G = \pi_{m_E}^{-1}(G(m_E)).$$

Definition 4.1.4 (Adelic Index)**.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve. The Adelic Index of G is the index of the reduction $G(m_E)$ within the group $\mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z})$, where m_E is the level defined above. It is the positive integer*

$$[\mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z}) : G(m_E)].$$

Remark 4.1.4.

- *The equality of indices $[\mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z}) : G(m_E)] = [\mathrm{GL}_2(\hat{\mathbb{Z}}) : G]$ follows directly from the index preservation property of the Lattice Isomorphism Theorem [3, Section 3.3, Theorem 20]. This application of this theorem leverages the fact that $U_{m_E} \subseteq G$.*
- *The minimal integer m_E necessarily divides any other integer m' that is stable and splits ρ_E.*

Nathan Jones, in his work [22], proves an interesting result that provides an upper bound for the adelic level of an elliptic curve using the adelic index.

Theorem 4.1.1. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve, and let m_E be the adelic level associated to this elliptic curve. Then one has*

$$m_E \leq 2 \cdot [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})] \cdot \mathrm{rad}(|\Delta_E|),$$

where Δ_E denotes the minimal discriminant of E, and $\mathrm{rad}(n) := \prod_{\ell | n, \ell \text{ prime}} \ell$.

Remark 4.1.5. *The author makes reference to results indicating that there are infinitely many elliptic curves $E/\mathbb{Q}$ satisfying*

$$m_E = 2 \cdot [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})] \cdot \mathrm{rad}(|\Delta_E|).$$

Thus, the bound for m_E given in the theorem is sharp.

Furthermore, Zywina [23] formulates a conjecture identifying the complete set of possible values for the adelic index.

Conjecture 4.1.1. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve, then the index $[GL_2(\widehat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})]$ lies in the set:*

$$\{2, 4, 6, 8, 10, 12, 16, 20, 24, 30, 32, 36, 40, 48, 54, 60, 72, 80, 84, 96, 108,$$
$$112, 120, 128, 144, 160, 182, 192, 200, 216, 220, 224, 240, 288, 300, 336,$$
$$360, 384, 480, 504, 576, 768, 864, 1152, 1200, 1296, 1536, 2736\}.$$

We conclude this section by providing references for the practical computation of the adelic image.

Determining the adelic image $G = \rho_E(G_{\mathbb{Q}})$ often involves finding an integer m (a level) such that $G = \pi_m^{-1}(G(m))$. While finding the adelic level m_E can be complex, practical algorithms provide a suitable level. Brau Avila, in his doctoral thesis [24], details such an algorithm.

His approach begins by defining a set of critical primes $T := \{2, 3\} \cup S_E \cup \{\ell \text{ prime} \mid \ell \mid \Delta_E\}$, where S_E consists of primes of non-surjective mod ℓ representation and Δ_E is the minimal discriminant of E (Zywina in [20] gives a simple and practical algorithm to compute the finite set S_E consisting of these exceptional primes ℓ). Let $m_0 := \prod_{\ell \in T} \ell$. A key result [24, Lemma 1.5.1] is that this m_0 splits ρ_E:

$$G = G_{m_0} \times \prod_{\ell \nmid m_0} \mathrm{GL}_2(\mathbb{Z}_\ell),$$

where G_{m_0} is the projection of G onto $\prod_{\ell \mid m_0} \mathrm{GL}_2(\mathbb{Z}_\ell)$. It follows that all prime factors of the adelic level m_E must be in T.

Furthermore, a method described in [24, Proposition 1.5.3] determines an integer $\tilde{m}$, divisible only by primes in T, such that $\tilde{m}$ serves as a level for G:

$$G = \pi_{\tilde{m}}^{-1}(G(\tilde{m})).$$

This implies $m_E \mid \tilde{m}$. Although $\tilde{m}$ may not be the adelic level m_E, it and the corresponding mod-$\tilde{m}$ image $G(\tilde{m})$ are sufficient to completely determine the full adelic image G. This computational description is crucial for analyzing G and its properties such as horizontal entanglements.

4.2. Prelude to Vertical Entanglement

The purpose of this section is to prove a key result that will be mentioned repeatedly in the following subsection on Vertical Entanglements.

Lemma 4.2.1. *Let $\ell \geq 5$ be a prime and let X be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ whose projection modulo ℓ contains $SL_2(\mathbb{Z}/\ell\mathbb{Z})$. Then X contains $SL_2(\mathbb{Z}_\ell)$.*

Proof. This follows from Lemma 3.1.3. □

Example 4.2.1. *Let R be a commutative ring with identity. Let $G := \mathrm{GL}_2(R)$, $H := SL_2(R)$, and $K := \left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \mid x \in R^\times \right\}$ ($K \cong R^\times$). For each $g \in G$, let $d := \det(g) \in R^\times$. The matrix $k_d = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}$ is in K and has $\det(k_d) = d$. We can write*

$$g = \left(g \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}^{-1} \right) \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}.$$

The first factor $gk_d^{-1} \in H$ and the second factor $k_d \in K$. Thus, $\mathrm{GL}_2(R) = HK$.

Remark 4.2.1. *The logic of this example can be generalized: Any subgroup of* $\mathrm{GL}_2(R)$ *that contains* $\mathrm{SL}_2(R)$ *and has a surjective determinant map must be* $\mathrm{GL}_2(R)$ *itself. This is because any element* $g \in \mathrm{GL}_2(R)$ *can be written as the product of an element from* $\mathrm{SL}_2(R)$ *and an element with the same determinant as* g*.*

Before we can prove the main result of this section, one final point must be addressed. This is best illustrated by the following commutative diagram:

$$\begin{array}{ccc} G(\ell^{n+1}) & \xrightarrow{\det} & (\mathbb{Z}/\ell^{n+1}\mathbb{Z})^\times \\ {\scriptstyle (\mathrm{mod}\ \ell^n)}\downarrow & & \downarrow{\scriptstyle (\mathrm{mod}\ \ell^n)} \\ G(\ell^n) & \xrightarrow{\det} & (\mathbb{Z}/\ell^n\mathbb{Z})^\times \end{array}$$

We saw in Lemma 2.4.2 that $\det(G(\ell^n)) = (\mathbb{Z}/\ell^n\mathbb{Z})^\times$ for all $n \geq 1$. Although it was not explicitly written in this form, in Section 2.5 we identified the ℓ-adic image of the Galois representation as the inverse limit of the reductions, i.e. $\varprojlim_n G(\ell^n) = \rho_{E,\ell^\infty}(G_\mathbb{Q})$. Let $G_\ell = \rho_{E,\ell^\infty}(G_\mathbb{Q})$. Combining this identification with the commutativity shown in the preceding diagram, we obtain:

$$\det(G_\ell) = \det\left(\varprojlim_n G(\ell^n)\right) = \varprojlim_n \det(G(\ell^n)) = \varprojlim_n (\mathbb{Z}/\ell^n\mathbb{Z})^\times = \mathbb{Z}_\ell^\times.$$

In other words, the determinant of the ℓ-adic image is the full group of ℓ-adic units:

$$\det(\rho_{E,\ell^\infty}(G_\mathbb{Q})) = \det(G_\ell) = \mathbb{Z}_\ell^\times.$$

Corollary 4.2.1. *Let* $E/\mathbb{Q}$ *be an elliptic curve. Let* $\ell \geq 5$ *be a prime and let* $G(\ell) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$*. Then* $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$*.*

Proof. G_ℓ is a profinite group, so it is closed (details are in Remark 1.3.1). Its projection modulo ℓ is $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, which therefore contains $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. By Lemma 4.2.1, $G_\ell \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$. Since $\det(G_\ell) = \mathbb{Z}_\ell^\times$, for every $d \in \mathbb{Z}_\ell^\times$, G_ℓ contains an element g_d such that $\det(g_d) = d$. Combining $G_\ell \supseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$ with $\det(G_\ell) = \mathbb{Z}_\ell^\times$, the decomposition argument shown in Example 4.2.1 implies that $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$. □

4.3. Vertical Entangelement

We will now dive a little deeper into *vertical entanglements* and in the following subsection we will do the same for *horizontal entanglements*.

Definition 4.3.1. *Let* $E/\mathbb{Q}$ *be a non-CM elliptic curve and* ℓ *a prime. We say that* ℓ *is exceptional for* E *if the mod-*ℓ *Galois representation* $\rho_{E,\ell}$ *is not surjective.*

Definition 4.3.2. *Let* $E/\mathbb{Q}$ *be a non-CM elliptic curve and* ℓ *a prime. We say that* ℓ *is adically-exceptional for* E *if the* ℓ*-adic Galois representation* ρ_{E,ℓ^∞} *is not surjective.*

Remark 4.3.1. *The definition of* ℓ *being adically-exceptional for* E *means that the* ℓ*-adic Galois representation* ρ_{E,ℓ^∞} *is not surjective. This is precisely the condition for* E *to exhibit vertical entanglement at the prime* ℓ*.*

As seen in Corollary 4.2.1, a prime ℓ is *exceptional* if and only if it is *adically-exceptional*, provided $\ell \geq 5$. This equivalence may fail only for $\ell = 2$ or $\ell = 3$. The reason is that there are proper subgroups of $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z}/8\mathbb{Z})$ that surject onto $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ under the standard reduction map, as well as a proper subgroup of $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ that surjects onto $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$.

For the primes $\ell = 2$ and $\ell = 3$, the surjectivity of the full ℓ-adic representation is determined by surjectivity at a specific finite level:

- For $\ell = 2$, the 2-adic representation $\rho_{E,2^\infty}$ is surjective if and only if the mod-8 representation $\rho_{E,8}$ is surjective [15].
- For $\ell = 3$, the 3-adic representation $\rho_{E,3^\infty}$ is surjective if and only if the mod-9 representation $\rho_{E,9}$ is surjective [25].

Definition 4.3.3. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve. For each prime ℓ, let $k_\ell \geq 1$ be the smallest integer such that the mod-ℓ^{k_ℓ} Galois representation $\rho_{E,\ell^{k_\ell}}$ is non-surjective. If ρ_{E,ℓ^n} is surjective for all $n \geq 1$, set $k_\ell = 0$. Then, Serre's constant associated to E is defined as*

$$A(E) = \prod_{\ell \text{ prime}} \ell^{k_\ell}.$$

In other words, $A(E)$ is a product over the *adically-exceptional primes* ℓ. As a consequence of the preceding discussion, which establishes that a prime $\ell \geq 5$ is exceptional if and only if it is adically-exceptional, we deduce that $k_\ell = 1$ for all adically-exceptional primes $\ell \geq 5$. This implies that $A(E)$ is square-free, except possibly at the primes $\ell = 2$ and $\ell = 3$. For these primes, the maximum possible exponents k_ℓ are bounded: $k_2 \leq 3$ and $k_3 \leq 2$. In the case where there are no *adically-exceptional primes* for E, we have $A(E) = 1$. Furthermore, Jones in [26] proved that almost all non-CM elliptic curves over $\mathbb{Q}$ have $A(E) = 1$.

In his influential paper [1], Serre established that for any non-CM elliptic curve $E/\mathbb{Q}$, the ℓ-adic Galois representation ρ_{E,ℓ^∞} is surjective onto $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for all sufficiently large primes ℓ. Building upon this, Serre inquired whether an absolute constant C (not depending on E) exists such that ρ_{E,ℓ^∞} achieves surjectivity for all primes $\ell > C$. Moreover, he asked wheter that surjectivity might occur for all $\ell > 37$. Zywina and Sutherland independently conjectured a slightly stronger version of Serre's question in [20] and [27], respectively. We denote the j-invariant of E by j_E.

Conjecture 4.3.1 (Zywina, Sutherland)**.** *If E is a non-CM elliptic curve over $\mathbb{Q}$ and $\ell > 13$ is a prime, then either $\rho_{E,\ell}(G_\mathbb{Q}) = GL_2(\mathbb{Z}/\ell\mathbb{Z})$ or*

$$(\ell, j_E) \in \{(17, -17^2 \cdot 101^3/2), (17, -17 \cdot 373^3/2^{17}), (37, -7 \cdot 11^3), (37, -7 \cdot 137^3 \cdot 2083^3)\}.$$

Consequently, assuming the conjecture to be true, for non-CM elliptic curves and primes $\ell > 13$, vertical entanglement that stems from the non-surjectivity of the mod ℓ representation is confined to these few, explicitly identified, exceptional cases. For the remaining small primes $\ell \leq 13$, Zywina's work [20] already provides a complete classification of all possible mod-ℓ images.

The problem of classifying the possible images of ℓ-adic Galois representations attached to elliptic curves over $\mathbb{Q}$ is completely resolved for the prime $\ell = 2$. This classification was given by Rouse and Zureick-Brown [28]. For primes $\ell > 2$, the analogous problem remains open.

In essence, Nathan Jones's theorem 4.1.1 provides a relationship between the adelic level, m_E, and the adelic index. Building upon this, we now seek to establish a connection between the adelic level m_E and Serre's constant $A(E)$. Let's recall that:

$$m_E = \min\{m \in \mathbb{N} \mid \ker(\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})) \subseteq \rho_E(G_{\mathbb{Q}})\},$$

where the condition is equivalent to $\ker\left(\prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell) \to \prod_{\ell|m} \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})\right) \subseteq \rho_E(G_{\mathbb{Q}}) \hookrightarrow \prod_\ell \rho_{E,\ell^\infty}(G_{\mathbb{Q}})$. The main differences between m_E and $A(E)$ are the following:

1. A prime power ℓ^e divides m_E whenever $\ker(\mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell^{e-1}\mathbb{Z})) \not\subseteq \rho_{E,\ell^\infty}(G_{\mathbb{Q}})$ and the prime power ℓ^n that appears as a factor of m_E respects the latter and $\ker(\mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})) \subseteq \rho_{E,\ell^\infty}(G_{\mathbb{Q}})$. Thus, $\rho_{E,\ell^\infty}(G_{\mathbb{Q}}) = \pi_{\ell^n}^{-1}(G(\ell^n))$ using a similar argument in Lemma 4.1.1. It is evident now that $A(E)$ divides m_E because $A(E)$ collects the minimal exponents of non-surjectivity for each prime and a prime power dividing $A(E)$ is at most ℓ^n. In other words, for each prime ℓ, m_E encodes the action of $G_{\mathbb{Q}}$ on the entire ℓ-adic Tate module, whereas, for $\ell \geq 5$, $A(E)$ only encodes the action of $G_{\mathbb{Q}}$ on the ℓ-torsion of E.

2. It may happen that there is a non-trivial intersection $\mathbb{Q} \neq \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b])$ for some $a, b \in \mathbb{Z}_{\geq 2}$ with $\gcd(a, b) = 1$. The constant m_E encodes such horizontal entanglements whereas $A(E)$ does not. Because m_E captures these horizontal entanglements, it often has more distinct prime factors in its factorization than $A(E)$.

In some sense, $A(E)$ sees things on a local level while m_E sees things on a global level. We are now ready to dive deeper into the second point above.

4.4. Horizontal Entanglement

We begin with the key lemma upon which the rest of this subsection is built.

Lemma 4.4.1. *Let $E/\mathbb{Q}$ be an elliptic curve, let $\tilde{a}, d, a$ be positive integers such that $\tilde{a} = da$ and $\gcd(d, a) = 1$. Then the field $\mathbb{Q}(E[\tilde{a}])$ is the compositum of $\mathbb{Q}(E[d])$ and $\mathbb{Q}(E[a])$, i.e., $\mathbb{Q}(E[\tilde{a}]) = \mathbb{Q}(E[d])\mathbb{Q}(E[a])$.*

Proof. We aim to prove the equality $\mathbb{Q}(E[\tilde{a}]) = \mathbb{Q}(E[d])\mathbb{Q}(E[a])$ by establishing containment in both directions. Recall that $E[\tilde{a}] \cong (\mathbb{Z}/\tilde{a}\mathbb{Z})^2$. Since $\gcd(d, a) = 1$, the Chinese Remainder Theorem and properties of direct products yield the following group isomorphism:

$$E[\tilde{a}] \cong (\mathbb{Z}/\tilde{a}\mathbb{Z})^2 \cong (\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z})^2 \cong (\mathbb{Z}/d\mathbb{Z})^2 \times (\mathbb{Z}/a\mathbb{Z})^2 \cong E[d] \times E[a].$$

This isomorphism means that, more concretely, using Bézout's identity $xd + ya = 1$, any point $P \in E[\tilde{a}]$ can be uniquely decomposed as $P = P_d + P_a$, where $P_d = [ya]P \in E[d]$ and $P_a = [xd]P \in E[a]$ via the elliptic curve group law.

First, we establish that $\mathbb{Q}(E[d])\mathbb{Q}(E[a]) \subseteq \mathbb{Q}(E[\tilde{a}])$. Since d and a both divide $\tilde{a}$, any point $P \in E[d]$ or $P' \in E[a]$ must satisfy $[\tilde{a}]P = \mathcal{O}$ and $[\tilde{a}]P' = \mathcal{O}$, respectively. Thus, $E[d] \subseteq$

$E[\tilde{a}]$ and $E[a] \subseteq E[\tilde{a}]$. It follows directly that the fields generated by their coordinates, $\mathbb{Q}(E[d])$ and $\mathbb{Q}(E[a])$, are both subfields of $\mathbb{Q}(E[\tilde{a}])$. The compositum $\mathbb{Q}(E[d])\mathbb{Q}(E[a])$, being the smallest field containing both, must therefore also be contained within $\mathbb{Q}(E[\tilde{a}])$.

Next, we show the reverse containment $\mathbb{Q}(E[\tilde{a}]) \subseteq \mathbb{Q}(E[d])\mathbb{Q}(E[a])$. The field $\mathbb{Q}(E[\tilde{a}])$ is generated over $\mathbb{Q}$ by the coordinates of all points $P \in E[\tilde{a}]$. As established earlier, any such P can be expressed as $P = P_d + P_a$ where $P_d \in E[d]$ and $P_a \in E[a]$. The coordinates of P are computed using the elliptic curve addition law, which involves rational functions (with coefficients in $\mathbb{Q}$) of the coordinates of P_d and P_a. Since the coordinates of P_d lie in $\mathbb{Q}(E[d])$ and the coordinates of P_a lie in $\mathbb{Q}(E[a])$, the coordinates of P must necessarily reside in the compositum field $\mathbb{Q}(E[d])\mathbb{Q}(E[a])$. Thus, $\mathbb{Q}(E[\tilde{a}]) = \mathbb{Q}(E[d])\mathbb{Q}(E[a])$. □

Consider an integer $n \geq 2$ with prime factorization $n = p_1^{e_1} \cdot \ldots \cdot p_m^{e_m}$. The n-torsion $E[n]$ decomposes as a direct product:

$$E[n] \cong \prod_{i=1}^{m} E[p_i^{e_i}].$$

This isomorphism induces an isomorphism of automorphism groups:

$$\mathrm{Aut}(E[n]) \cong \prod_{i=1}^{m} \mathrm{Aut}(E[p_i^{e_i}]),$$

which, upon choosing bases, translates to an isomorphism for the general linear groups:

$$\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \cong \prod_{i=1}^{m} \mathrm{GL}_2(\mathbb{Z}/p_i^{e_i}\mathbb{Z}).$$

The Galois representation $\rho_{E,n} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[n])$ can thus be viewed as a map whose image lands in this product. Let $G_n := \rho_{E,n}(G_{\mathbb{Q}})$ and for each i, let $G_{p_i^{e_i}} := \rho_{E,p_i^{e_i}}(G_{\mathbb{Q}})$. The projection of G_n onto the i-th factor $\mathrm{Aut}(E[p_i^{e_i}])$ is precisely $G_{p_i^{e_i}}$. This gives us a natural injective homomorphism:

$$\psi_n : G_n \hookrightarrow \prod_{i=1}^{m} G_{p_i^{e_i}}.$$

Now, let's suppose that G_n is *not* the full product $\prod_{i=1}^{m} G_{p_i^{e_i}}$ (i.e., ψ_n is not surjective). The non-surjectivity of ψ_n signifies a dependency or correlation between the action of Galois on the different $E[p_i^{e_i}]$ components.

We can translate this into the language of Galois field extensions. Recall that $G_n \cong \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ and $G_{p_i^{e_i}} \cong \mathrm{Gal}(\mathbb{Q}(E[p_i^{e_i}])/\mathbb{Q})$. The field $\mathbb{Q}(E[n])$ is the compositum of the fields $\mathbb{Q}(E[p_i^{e_i}])$ for $i = 1, \ldots, m$. Let $L = \mathbb{Q}(E[n])$ and $L_i = \mathbb{Q}(E[p_i^{e_i}])$. Then $L = L_1 L_2 \ldots L_m$. The map ψ_n corresponds to the natural restriction map:

$$\Psi_n : \mathrm{Gal}(L/\mathbb{Q}) \to \prod_{i=1}^{m} \mathrm{Gal}(L_i/\mathbb{Q}), \quad \text{defined by } \sigma \mapsto (\sigma|_{L_1}, \ldots, \sigma|_{L_m}).$$

We can analyze the condition for Ψ_n being an isomorphism by recursively applying Proposition 1.1.1. Let $n = ab$ be any factorization of n into coprime positive integers a and b.

Let $K_a = \mathbb{Q}(E[a])$ and $K_b = \mathbb{Q}(E[b])$. By Lemma 4.4.1, $L = \mathbb{Q}(E[n])$ is equal to K_aK_b. Proposition 1.1.1 states that the natural map $\mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{Gal}(K_a/\mathbb{Q}) \times \mathrm{Gal}(K_b/\mathbb{Q})$ is an isomorphism if and only if $K_a \cap K_b = \mathbb{Q}$.

The target group of Ψ_n can be decomposed according to the factorization $n = ab$. Let $I_a = \{i \mid p_i^{e_i} | a\}$ and $I_b = \{j \mid p_j^{e_j} | b\}$. Then

$$\prod_{k=1}^{m} \mathrm{Gal}(L_k/\mathbb{Q}) \cong \left(\prod_{i \in I_a} \mathrm{Gal}(L_i/\mathbb{Q}) \right) \times \left(\prod_{j \in I_b} \mathrm{Gal}(L_j/\mathbb{Q}) \right).$$

Assuming $K_a \cap K_b = \mathbb{Q}$, for Ψ_n to be an isomorphism, we then require that the maps $\Psi_a : \mathrm{Gal}(K_a/\mathbb{Q}) \to \prod_{p_i^{e_i}|a} \mathrm{Gal}(\mathbb{Q}(E[p_i^{e_i}])/\mathbb{Q})$ and $\Psi_b : \mathrm{Gal}(K_b/\mathbb{Q}) \to \prod_{p_j^{e_j}|b} \mathrm{Gal}(\mathbb{Q}(E[p_j^{e_j}])/\mathbb{Q})$ are themselves isomorphisms. To check if Ψ_a is an isomorphism, we repeat the process: if $a = a_1a_2$ with $\gcd(a_1, a_2) = 1$, let $K_{a_1} = \mathbb{Q}(E[a_1])$ and $K_{a_2} = \mathbb{Q}(E[a_2])$. Then $\mathrm{Gal}(K_a/\mathbb{Q}) \cong \mathrm{Gal}(K_{a_1}/\mathbb{Q}) \times \mathrm{Gal}(K_{a_2}/\mathbb{Q})$ if and only if $K_{a_1} \cap K_{a_2} = \mathbb{Q}$. If this holds, we then require Ψ_{a_1} and Ψ_{a_2} to be isomorphisms. This recursive argument continues until the factors are prime powers $p_k^{e_k}$. And then we repeat this argument for Ψ_b.

Therefore, Ψ_n is an isomorphism if and only if $\mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]) = \mathbb{Q}$ for all coprime divisors a, b of n. Furthermore, the existence of such coprime a, b implies that the full adelic Galois representation ρ_E is non-surjective by the commutative diagram below,

$$\begin{array}{ccc} \rho_E(G_{\mathbb{Q}}) & \xhookrightarrow{\psi} & \prod_\ell \rho_{E,\ell^\infty}(G_{\mathbb{Q}}) \\ \downarrow & & \downarrow \\ G_n = \rho_{E,n}(G_{\mathbb{Q}}) & \xhookrightarrow{\psi_n} & \prod_{i=1}^{m} \rho_{E,p_i^{e_i}}(G_{\mathbb{Q}}). \end{array}$$

Motivated by the significance of the intersection $\mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b])$ when a and b are coprime, we now present the general definition of horizontal entanglement for arbitrary integers a, b, as given by Daniels, Lozano-Robledo, and Morrow in [29].

Definition 4.4.1. *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 the field extension $\big(\mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b])\big)/\mathbb{Q}(E[d])$.*

Remark 4.4.1. *If $a|b$, then $d = \gcd(a, b) = a$. Therefore, $\mathbb{Q}(E[d]) = \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b])$. Thus, there is no horizontal (a, b)-entanglement when $a|b$.*

We dedicate the remainder of this section to proving the fundamental result that the adelic Galois representation attached to an elliptic curve over $\mathbb{Q}$ is never surjective. Our proof will rely on two key results, which we now state without proof before proceeding to the main argument.

Proposition 4.4.1. *Let $E/\mathbb{Q}$ be an elliptic curve. Then $Gal(\mathbb{Q}(E[2])/\mathbb{Q})$ is isomorphic to the following:*

(a) $GL_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$ *if* $\Delta_E \notin (\mathbb{Q}^\times)^2$ *and* $E[2]$ *contains no rational points,*

(b) $\mathbb{Z}/3\mathbb{Z}$ *if* $\Delta_E \in (\mathbb{Q}^\times)^2$ *and* $E[2]$ *contains no rational points,*

(c) $\mathbb{Z}/2\mathbb{Z}$ *if* $\Delta_E \notin (\mathbb{Q}^\times)^2$ *and* $E[2]$ *contains a rational point,*

(d) $\{e\}$ *if* $\Delta_E \in (\mathbb{Q}^\times)^2$ *and* $E[2]$ *contains a rational point.*

In particular, we have that $\mathbb{Q}(\sqrt{\Delta_E})$ *is the unique quadratic subfield of* $\mathbb{Q}(E[2])$ *when* $\Delta_E \notin (\mathbb{Q}^\times)^2$*. (Note:* Δ_E *is the minimal discriminant.)*

Proof. The proof can be found in [30, Proposition 5.4.2]. □

Theorem 4.4.1. *Let* $E : y^2 = x^3 + ax + b$ *be an elliptic curve over* $\mathbb{Q}$ *with minimal discriminant* $\Delta_E = -16(4a^3 + 26b^2)$ *and* j*-invariant* $j = -1728(4a)^3/\Delta_E$*. Then*

(a) $\rho_{E,2}$ *is surjective if and only if* $x^3 + ax + b$ *is irreducible and* $\Delta_E \notin (\mathbb{Q}^\times)^2$*.*

(b) $\rho_{E,4}$ *is surjective if and only if* $\rho_{E,2}$ *is surjective,* $\Delta_E \notin -1 \cdot (\mathbb{Q}^\times)^2$ *and* $j \neq -4t^3(t+8)$ *for any* $t \in \mathbb{Q}$*.*

(c) $\rho_{E,8}$ *is surjective if and only if* $\rho_{E,4}$ *is surjective and* $\Delta_E \notin \pm 2 \cdot (\mathbb{Q}^\times)^2$*.*

Proof. The proof can be found in [31]. □

Proposition 4.4.2. *Let* $E/\mathbb{Q}$ *be an elliptic curve and let* $\overline{\Delta_E}$ *be the squarefree part of its minimal discriminant* Δ_E*. Then* E *exhibits* (1) *or* $(2i)$ *or* (1) *and* $(2i)$*.*

(1) E *has a 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 adelic Galois representation ρ_E *is non-surjective.*

Proof. The proof presented here follows the strategy of Mein [32, Proposition 3.16].

We begin by recalling a key result from Serre in [15] that says vertical 2-entanglement in an elliptic curve E occurs if and only if the Galois representation $\rho_{E,8}$ is non-surjective. Consequently, assuming $\rho_{E,8}$ is non-surjective directly implies that E exhibits vertical 2-entanglement.

For our analysis, we will consider a set of conditions, which we term 'Condition (B)', that are related to, but weaker than, the full surjectivity of $\rho_{E,8}$. Drawing from the previously stated theorem, Condition (B) consists of the following three assumptions:

(1) $\rho_{E,2}$ is surjective.

(2) $\Delta_E \notin -1 \cdot (\mathbb{Q}^\times)^2$.

(3) $\Delta_E \notin \pm 2 \cdot (\mathbb{Q}^\times)^2$.

It is important to understand how Condition (B) relates to the surjectivity of $\rho_{E,8}$. According to the previous theorem if Condition (B) holds and the additional criterion $j \neq -4t^3(t+8)$ for any $t \in \mathbb{Q}$ is met, then $\rho_{E,8}$ is surjective. Conversely, if Condition (B) holds but $j = -4t^3(t+8)$ for some $t \in \mathbb{Q}$, then $\rho_{E,4}$ would be non-surjective, which in turn implies $\rho_{E,8}$ is non-surjective (and thus E would have vertical 2-entanglement).

Therefore, our proof strategy involves two main perspectives:

1. The direct implication from Serre: non-surjective $\rho_{E,8} \implies$ vertical 2-entanglement.
2. A detailed analysis under Condition (B). Within this framework, $\rho_{E,8}$ may be either surjective or non-surjective, depending on the j-invariant as outlined above.

For the remainder of this proof, our arguments will proceed under the assumption that Condition (B) holds. Let $n := \overline{\Delta_E}$ be the squarefree part of Δ_E. Note that $\mathbb{Q}(\sqrt{n})$ is non-trivial (i.e., $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{n})$) as $\Delta_E \notin (\mathbb{Q}^\times)^2$, since $\rho_{E,2}$ is surjective by the previous theorem.

Let us assume that $n \equiv 1 \pmod 4$. By Proposition 1.2.4, $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta_{|n|})$ as $n \equiv 1 \pmod 4$. Furthermore, by Lemma 2.4.1, $\mathbb{Q}(\zeta_{|n|}) \subseteq \mathbb{Q}(E[|n|])$ and so $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(E[|n|])$. Also by Proposition 4.4.1 we have that $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(E[2])$, therefore $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(E[2]) \cap \mathbb{Q}(E[|n|])$. As $\mathbb{Q}(\sqrt{n})$ is non-trivial and $\gcd(2,|n|) = 1$, we get that $\mathbb{Q} \subsetneq \mathbb{Q}(E[2]) \cap \mathbb{Q}(E[|n|])$ and so E has horizontal $(2, |\overline{\Delta_E}|)$-entanglement.

Let us assume that $n \equiv 3 \pmod 4$. So, $-n \equiv 1 \pmod 4$ and we obtain $\mathbb{Q}(\sqrt{-n}) \subseteq \mathbb{Q}(\zeta_{|n|})$ by Proposition 1.2.4. Similarly, as in the last argument, by Lemma 2.4.1, $\mathbb{Q}(\sqrt{-n}) \subseteq \mathbb{Q}(\zeta_{|n|}) \subseteq \mathbb{Q}(E[|n|])$. We also know that $\sqrt{n} \in \mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[4])$. Lemma 2.4.1 also implies that $\mathbb{Q}(\zeta_4) \subseteq \mathbb{Q}(E[4])$ and in particular $\sqrt{-1} \in \mathbb{Q}(E[4])$. So, $\sqrt{-n} = \sqrt{-1}\sqrt{n} \in \mathbb{Q}(E[4])$, therefore $\mathbb{Q}(\sqrt{-n}) \subseteq \mathbb{Q}(E[4]) \cap \mathbb{Q}(E[|n|])$. $\mathbb{Q}(\sqrt{-n})$ is non-trivial because $\Delta_E \notin -1 \cdot (\mathbb{Q}^\times)^2$. Since $\gcd(4,|n|) = 1$, E has horizontal $(4, |\overline{\Delta_E}|)$-entanglement.

Let us assume that $n \equiv 2 \pmod 4$, then $n/2 \equiv 1, 3 \pmod 4$. Let us suppose further that $n/2 \equiv 1 \pmod 4$. By Proposition 1.2.4 and Lemma 2.4.1 we get $\mathbb{Q}(\sqrt{n/2}) \subseteq \mathbb{Q}(E[|n/2|])$. We know $\sqrt{2} \in \mathbb{Q}(\zeta_8) \subseteq \mathbb{Q}(E[8])$ by Lemma 1.2.2 and Lemma 2.4.1. Moreover, $\sqrt{n} \in \mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[8])$ by Proposition 4.4.1. We obtain $\sqrt{n/2} = \sqrt{n}/\sqrt{2} \in \mathbb{Q}(E[8])$. Thus, $\mathbb{Q}(\sqrt{n/2}) \subseteq \mathbb{Q}(E[8]) \cap \mathbb{Q}(E[|n/2|])$ and $\mathbb{Q}(\sqrt{n/2})$ is non-trivial since $\Delta_E \notin \pm 2 \cdot (\mathbb{Q}^\times)^2$. We have $\gcd(8,|n/2|) = 1$ so E has horizontal $(8, |\overline{\Delta_E}/2|)$-entanglement.

Now let's consider the case when $n/2 \equiv 3 \pmod 4$, equivalently $-n/2 \equiv 1 \pmod 4$. By Proposition 1.2.4 and Lemma 2.4.1 we get $\mathbb{Q}(\sqrt{-n/2}) \subseteq \mathbb{Q}(E[|n/2|])$. Note that $\sqrt{-n} = \sqrt{n}\sqrt{-1} \in \mathbb{Q}(E[4]) \subseteq \mathbb{Q}(E[8])$, so we get that $\sqrt{-n/2} = \sqrt{-n}/\sqrt{2} \in \mathbb{Q}(E[8])$. Thus, $\mathbb{Q}(\sqrt{-n/2}) \subseteq \mathbb{Q}(E[8]) \cap \mathbb{Q}(E[|n/2|])$ and $\mathbb{Q}(\sqrt{-n/2})$ is non-trivial since $\Delta_E \notin \pm 2 \cdot (\mathbb{Q}^\times)^2$. We have $\gcd(8,|n/2|) = 1$ so E has horizontal $(8, |\overline{\Delta_E}/2|)$-entanglement.

In summary, E exhibits case (1) from the statement of the Proposition if $\rho_{E,8}$ is non-surjective and E doesn't satisfy Condition (B). E exhibits case (2i) if $\rho_{E,8}$ is surjective, which implies Condition (B) is satisfied by the previous theorem. E exhibits both cases (1) and (2i) if $\rho_{E,8}$ is non-surjective and E satisfies Condition (B). In particular, we have that the index of the image of ρ_E is always bigger than 1. □

Proposition 4.4.3. *Let $E/\mathbb{Q}$ be an elliptic curve with minimal discriminant Δ_E. Let $\overline{\Delta_E}$ be the squarefree part of Δ_E, and suppose it admits a factorization $\overline{\Delta_E} = ab$ where a and b are coprime, odd integers different than 1, both congruent to 1 (mod 4). Then E exhibits horizontal entanglement for the pairs $(2, |ab|)$, $(2|a|, |b|)$, and $(|a|, 2|b|)$.*

Proof. The proof relies on the known inclusions $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(E[2])$ (Proposition 4.4.1) and, for a squarefree integer $m \equiv 1 \pmod 4$, $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(E[|m|])$ (Proposition 1.2.4 & Lemma 2.4.1).

Since $ab \equiv 1 \pmod 4$, both $\mathbb{Q}(E[2])$ and $\mathbb{Q}(E[|ab|])$ contain $\sqrt{ab}$. Their intersection is therefore larger than $\mathbb{Q}$, which implies $(2, |ab|)$-entanglement.

For the pair $(2|a|, |b|)$, we consider the intersection $\mathbb{Q}(E[2|a|]) \cap \mathbb{Q}(E[|b|])$. The compositum field $\mathbb{Q}(E[2|a|]) = \mathbb{Q}(E[2])\mathbb{Q}(E[|a|])$ contains both $\sqrt{ab}$ and $\sqrt{a}$, and thus contains their product $\sqrt{b}$. Since $\mathbb{Q}(E[|b|])$ also contains $\sqrt{b}$, their intersection is a non-trivial extension of $\mathbb{Q}$, proving $(2|a|, |b|)$-entanglement.

The argument for $(|a|, 2|b|)$-entanglement is identical by symmetry, with $\sqrt{a}$ being in the intersection $\mathbb{Q}(E[|a|]) \cap \mathbb{Q}(E[2|b|])$. □

Example 4.4.1. *The elliptic curve with LMFDB label* `65.a1` *is a curve satisfying the hypotheses of the above proposition.*

Example 4.4.2. *The elliptic curve with LMFDB label* `216.a1` *exhibits both case (1) and case (2a) from Proposition 4.4.2. This scenario is possible because Condition (B) from the proof is satisfied, while the full 2-adic representation remains non-surjective. The existence of vertical 2-entanglement is confirmed by data from the LMFDB showing that its mod-4 Galois representation is not surjective, even though its mod-2 representation is. Simultaneously, $\overline{\Delta_E} = -3$, the condition $-3 \equiv 1 \pmod 4$ implies the existence of horizontal $(2, 3)$-entanglement, satisfying case (2a).*

Example 4.4.3. *Consider the elliptic curve with LMFDB label* `7098.v1`*. The adelic level for this elliptic curve is $m_E = 4$. Recall that the adelic level m_E captures all entanglement phenomena of an elliptic curve. Given $m_E = 4$, this particular elliptic curve serves as an example where there is no horizontal entanglement. The primary entanglement present would be vertical 2-entanglement. Furthermore, examining the data provided on the LMFDB page for this elliptic curve reveals that its mod 2 Galois representation is surjective, while its mod 4 representation is not surjective. Note that Condition (B) from the proof of Proposition 4.4.2 is not satisfied.*

Example 4.4.4. *Consider the elliptic curve with LMFDB label* `162.d2`*. The adelic level for this curve is $m_E = 12 = 2^2 \cdot 3$. Although the adelic level has two distinct prime factors, this curve serves as a key example that exhibits no horizontal entanglement. The only entanglements present are vertical. Note that Condition (B) from the proof of Proposition 4.4.2 is not satisfied.*

We conclude this section with a question that stems from the observations in the preceding two examples.

Question 4.4.1. *Can we characterize all elliptic curves $E/\mathbb{Q}$ such that their adelic level m_E has at least two distinct prime factors, yet E exhibits no horizontal entanglements?*

4.5. Horizontal Entanglement in Terms of Group Theory

In their work [33], Daniels and Morrow developed a method to characterize horizontal entanglement using primarily group-theoretic language. Their framework is established as follows.

Let $E/\mathbb{Q}$ be an elliptic curve, $n \in \mathbb{Z}_{\geq 2}$, and $a < b$ be divisors of n. Define $d = \gcd(a, b)$ and $c = \operatorname{lcm}(a, b)$. The image of the mod-$n$ Galois representation is $G_n := \rho_{E,n}(G_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, which is isomorphic to $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$. Since $c = \operatorname{lcm}(a, b)$ divides n, the natural reduction homomorphism $\pi_c : \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/c\mathbb{Z})$ induces a map on the image of the mod-n representation. We define $G_c := \pi_c(G_n)$. Given that $\pi_c \circ \rho_{E,n} = \rho_{E,c}$ as $c \mid n$, G_c is equal to $\rho_{E,c}(G_{\mathbb{Q}}) \cong \mathrm{Gal}(\mathbb{Q}(E[c])/\mathbb{Q})$. For any $e \in \{a, b, d\}$, there are further reduction maps $\pi_e : \mathrm{GL}(2, \mathbb{Z}/c\mathbb{Z}) \to \mathrm{GL}(2, \mathbb{Z}/e\mathbb{Z})$. The relevant subgroups are then defined as $N_e := \ker(\pi_e) \cap G_c$. With this group-theoretic apparatus, Daniels and Morrow provide the following definition:

Definition 4.5.1. *The group G_n (or more precisely, its image G_c) is said to have horizontal (a, b)-entanglement if*

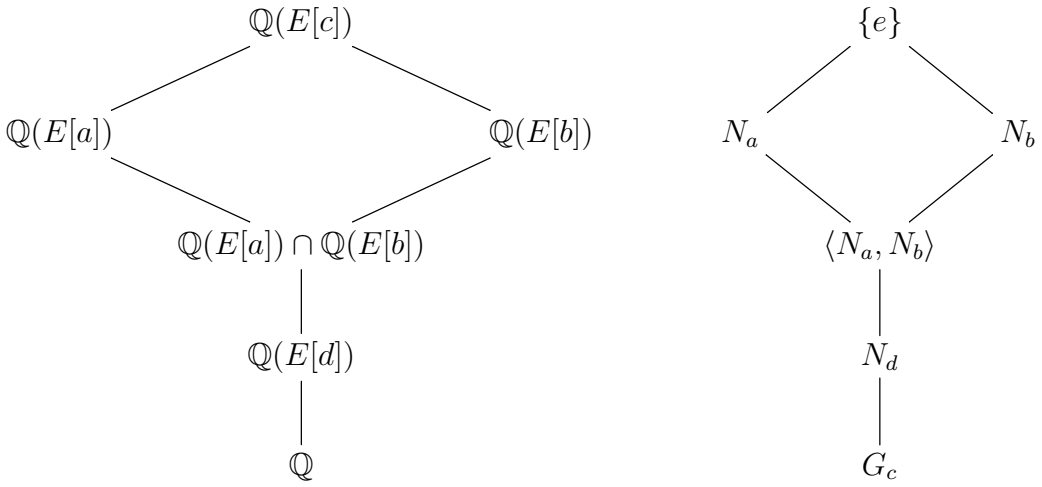
$$\langle N_a, N_b \rangle \subsetneq N_d.$$

The type of this entanglement is the isomorphism class of the quotient group $N_d/\langle N_a, N_b \rangle$.

This group-theoretic condition is equivalent to the field-theoretic definition of horizontal entanglement previously established, and the type defined here corresponds to the Galois group of $(\mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]))/\mathbb{Q}(E[d])$. The equivalence arises from the Galois correspondence as we will now see. We have $G_c \cong \mathrm{Gal}(\mathbb{Q}(E[c])/\mathbb{Q})$. For $e \in \{a, b, d\}$, the image $\pi_e(G_c)$ is $\rho_{E,e}(G_{\mathbb{Q}}) \cong \mathrm{Gal}(\mathbb{Q}(E[e])/\mathbb{Q})$. By the First Isomorphism Theorem for groups, $G_c/(\ker(\pi_e) \cap G_c) \cong \pi_e(G_c)$. Since $N_e = \ker(\pi_e) \cap G_c$, this yields $G_c/N_e \cong \rho_{E,e}(G_{\mathbb{Q}}) \cong \mathrm{Gal}(\mathbb{Q}(E[e])/\mathbb{Q})$. The fundamental theorem of Galois theory states that $\mathrm{Gal}(\mathbb{Q}(E[c])/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(E[c])/\mathbb{Q}(E[e])) \cong \mathrm{Gal}(\mathbb{Q}(E[e])/\mathbb{Q})$, as $\mathbb{Q}(E[e])/\mathbb{Q}$ being a Galois extension ensures that $\mathrm{Gal}(\mathbb{Q}(E[c])/\mathbb{Q}(E[e]))$ is a normal subgroup of $\mathrm{Gal}(\mathbb{Q}(E[c])/\mathbb{Q})$. Comparing the latter isomorphisms and recalling $G_c \cong \mathrm{Gal}(\mathbb{Q}(E[c])/\mathbb{Q})$, we deduce that $N_e \cong \mathrm{Gal}(\mathbb{Q}(E[c])/\mathbb{Q}(E[e]))$. Therefore, N_e is precisely the subgroup of G_c that fixes the intermediate field $\mathbb{Q}(E[e])$.

According to [2, Theorem 5.13], the subgroup corresponding to $\mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b])$ is $\langle N_a, N_b \rangle$. Thus, $\langle N_a, N_b \rangle$ is the subgroup of G_c fixing $\mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b])$. The group-theoretic condition $\langle N_a, N_b \rangle \subsetneq N_d$ is then translated by the inclusion-reversing property of the Galois correspondence directly to the field-theoretic condition $\mathbb{Q}(E[d]) \subsetneq \mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b])$. Furthermore, the quotient group $N_d/\langle N_a, N_b \rangle$ corresponds, by Galois theory, to the Galois group of the field extension $(\mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]))/\mathbb{Q}(E[d])$. This demonstrates the equivalence of the two definitions of entanglement, including their types.

This Galois correspondence is summarized in the following diagram:



Definition 4.5.2. *The* size *of a horizontal* (a, b)*-entanglement is defined as the degree*

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

It is noted that this quantity is also equal to the group index

$$[N_d : \langle N_a, N_b \rangle].$$

The work presented in the remainder of this thesis is original, unless otherwise noted. We will now give a group-theoretic interpretation of the size of a horizontal (a, b)-entanglement, followed by its field-theoretic interpretation in the next section.

Lemma 4.5.1. *Let* $a, b \in \mathbb{Z}_{\geq 2}$ *such that* $\gcd(a, b) = 1$*. Then*

$$[N_d : \langle N_a, N_b \rangle] = [\rho_{E,a}(G_{\mathbb{Q}}) \times \rho_{E,b}(G_{\mathbb{Q}}) : \rho_{E,c}(G_{\mathbb{Q}})].$$

Proof. First note that $d = 1$ and $c = ab$. As a result, $N_d = \ker(\pi_d) \cap G_c = \mathrm{GL}_2(\mathbb{Z}/c\mathbb{Z}) \cap G_c = G_c$. And so what we are really trying to prove is

$$[G_c : \langle N_a, N_b \rangle] = [\rho_{E,a}(G_{\mathbb{Q}}) \times \rho_{E,b}(G_{\mathbb{Q}}) : \rho_{E,c}(G_{\mathbb{Q}})].$$

We first want to show that $\langle N_a, N_b \rangle = N_a N_b$ and the latter is true if and only if $N_a N_b$ is a subgroup and that is true if and only if $N_a N_b = N_b N_a$ [3, Section 3.2, Proposition 14]. We aim to prove $N_a N_b = N_b N_a$ by showing that $N_a \trianglelefteq \langle N_a, N_b \rangle$. Recall that $N_a \trianglelefteq G_c$ by the Galois correspondence because $\mathbb{Q}(E[a])/\mathbb{Q}$ is Galois, which implies that $N_a \trianglelefteq \langle N_a, N_b \rangle$.

Our goal now is to show that $N_a N_b \cong N_a \times N_b$. Consider,

$$\begin{aligned} \{e\} &= \mathrm{Gal}(\mathbb{Q}(E[c])/\mathbb{Q}(E[c])) \\ &= \mathrm{Gal}(\mathbb{Q}(E[c])/\mathbb{Q}(E[a])\mathbb{Q}(E[b])) \\ &= N_a \cap N_b \end{aligned}$$

where the second equality follows from $\mathbb{Q}(E[c]) = \mathbb{Q}(E[a])\mathbb{Q}(E[b])$ since $\gcd(a, b) = 1$, and the third equality follows from [2, Theorem 5.12]. Thus, $N_a \cap N_b = \{e\}$. And so, we have

that $N_aN_b = N_bN_a$ (as $N_a, N_b \trianglelefteq G_c$) and $N_a \cap N_b = \{e\}$, which implies $N_aN_b \cong N_a \times N_b$ by [13, Theorem 4.1]. This gives us

$$|\langle N_a, N_b\rangle| = |N_aN_b| = |N_a \times N_b| = |N_a||N_b|.$$

We're finally ready to prove the statement in the Lemma.

$$\begin{aligned}
[G_c : \langle N_a, N_b\rangle] &= \frac{|\operatorname{Gal}(\mathbb{Q}(E[ab])/\mathbb{Q})|}{|\operatorname{Gal}(\mathbb{Q}(E[ab])/\mathbb{Q}(E[a]))| \cdot |\operatorname{Gal}(\mathbb{Q}(E[ab])/\mathbb{Q}(E[b]))|} \\
&= \frac{|\operatorname{Gal}(\mathbb{Q}(E[ab])/\mathbb{Q})|}{\frac{|\operatorname{Gal}(\mathbb{Q}(E[ab])/\mathbb{Q})|}{|\operatorname{Gal}(\mathbb{Q}(E[a])/\mathbb{Q})|} \cdot \frac{|\operatorname{Gal}(\mathbb{Q}(E[ab])/\mathbb{Q})|}{|\operatorname{Gal}(\mathbb{Q}(E[b])/\mathbb{Q})|}} \\
&= \frac{|\operatorname{Gal}(\mathbb{Q}(E[a])/\mathbb{Q})||\operatorname{Gal}(\mathbb{Q}(E[b])/\mathbb{Q})|}{|\operatorname{Gal}(\mathbb{Q}(E[ab])/\mathbb{Q})|}
\end{aligned}$$

where in the second equality, we used $\operatorname{Gal}(\mathbb{Q}(E[e])/\mathbb{Q}) \cong \frac{\operatorname{Gal}(\mathbb{Q}(E[c])/\mathbb{Q})}{\operatorname{Gal}(\mathbb{Q}(E[c])/\mathbb{Q}(E[e]))}$.

Clearly,

$$[\rho_{E,a}(G_\mathbb{Q}) \times \rho_{E,b}(G_\mathbb{Q}) : \rho_{E,c}(G_\mathbb{Q})] = \frac{|\operatorname{Gal}(\mathbb{Q}(E[a])/\mathbb{Q})||\operatorname{Gal}(\mathbb{Q}(E[b])/\mathbb{Q})|}{|\operatorname{Gal}(\mathbb{Q}(E[ab])/\mathbb{Q})|}.$$

□

The Lemma established above is particularly useful. It provides a framework for calculating the index $[\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : G_n]$, where $n \in \mathbb{Z}_{\geq 2}$. This calculation relies on understanding the indices of the individual mod-ℓ representations, and the sizes of of all nontrivial horizontal entanglements among the divisors of n. Furthermore, if n represents the adelic level of the representation, then this approach can be used to determine the adelic index.

To apply this, consider $a, b \in \mathbb{Z}_{\geq 2}$ with $\gcd(a, b) = 1$. Let $c = ab$. By the Chinese Remainder Theorem, $\mathrm{GL}_2(\mathbb{Z}/c\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/b\mathbb{Z})$. Then the index we are interested in, $[\mathrm{GL}_2(\mathbb{Z}/c\mathbb{Z}) : \rho_{E,c}(G_\mathbb{Q})]$, can be written as:

$$[\mathrm{GL}_2(\mathbb{Z}/c\mathbb{Z}) : \rho_{E,c}(G_\mathbb{Q})] = [\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/b\mathbb{Z}) : \rho_{E,c}(G_\mathbb{Q})].$$

Here, $\rho_{E,c}(G_\mathbb{Q})$ is identified with its image under the natural injection $\psi_c : \rho_{E,c}(G_\mathbb{Q}) \hookrightarrow \rho_{E,a}(G_\mathbb{Q}) \times \rho_{E,b}(G_\mathbb{Q})$. We now proceed depending on whether there is horizontal (a, b)-entanglement:

1. **Suppose there is no horizontal (a, b)-entanglement.** This means $\mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]) = \mathbb{Q}$ (since $d = \gcd(a, b) = 1$). By Proposition 1.1.1, this implies that $\rho_{E,c}(G_\mathbb{Q}) \cong \rho_{E,a}(G_\mathbb{Q}) \times \rho_{E,b}(G_\mathbb{Q})$. Thus,

$$\begin{aligned}
[\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/b\mathbb{Z}) : \rho_{E,c}(G_\mathbb{Q})] &= [\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/b\mathbb{Z}) : \rho_{E,a}(G_\mathbb{Q}) \times \rho_{E,b}(G_\mathbb{Q})] \\
&= [\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z}) : \rho_{E,a}(G_\mathbb{Q})] \cdot [\mathrm{GL}_2(\mathbb{Z}/b\mathbb{Z}) : \rho_{E,b}(G_\mathbb{Q})].
\end{aligned}$$

   The last equality holds because for groups G_1, G_2 and subgroups $H_1 \leq G_1, H_2 \leq G_2$, the index $[G_1 \times G_2 : H_1 \times H_2] = [G_1 : H_1][G_2 : H_2]$.

2. **Suppose there is horizontal (a, b)-entanglement.** This means $\mathbb{Q}(E[a])\cap\mathbb{Q}(E[b]) \supsetneq \mathbb{Q}$. Consequently, $\rho_{E,c}(G_{\mathbb{Q}})$ is a proper subgroup of $\rho_{E,a}(G_{\mathbb{Q}}) \times \rho_{E,b}(G_{\mathbb{Q}})$. Using the tower law for indices,

$$\begin{aligned}[\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/b\mathbb{Z}) : \rho_{E,c}(G_{\mathbb{Q}})] &= [\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/b\mathbb{Z}) : \rho_{E,a}(G_{\mathbb{Q}}) \times \rho_{E,b}(G_{\mathbb{Q}})] \\ &\quad \cdot [\rho_{E,a}(G_{\mathbb{Q}}) \times \rho_{E,b}(G_{\mathbb{Q}}) : \rho_{E,c}(G_{\mathbb{Q}})] \\ &= [\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z}) : \rho_{E,a}(G_{\mathbb{Q}})] \cdot [\mathrm{GL}_2(\mathbb{Z}/b\mathbb{Z}) : \rho_{E,b}(G_{\mathbb{Q}})] \\ &\quad \cdot [\rho_{E,a}(G_{\mathbb{Q}}) \times \rho_{E,b}(G_{\mathbb{Q}}) : \rho_{E,c}(G_{\mathbb{Q}})].\end{aligned}$$

   The term $[\rho_{E,a}(G_{\mathbb{Q}}) \times \rho_{E,b}(G_{\mathbb{Q}}) : \rho_{E,c}(G_{\mathbb{Q}})]$ is precisely the index that measures the entanglement. From the previous lemma, this factor can be written as $[G_c : \langle N_a, N_b\rangle]$. This index is also equal to $[\mathbb{Q}(E[a]) \cap \mathbb{Q}(E[b]) : \mathbb{Q}]$.

To compute the individual indices $[\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z}) : \rho_{E,a}(G_{\mathbb{Q}})]$ and $[\mathrm{GL}_2(\mathbb{Z}/b\mathbb{Z}) : \rho_{E,b}(G_{\mathbb{Q}})]$, we would recursively apply this same logic, breaking down a and b into their coprime factors until we reach prime powers.

We now present an example to illustrate the concepts discussed, calculating the index of a specific mod-n representation in two different ways.

Example 4.5.1. *Consider the elliptic curve with LMFDB label* `84.b2`*. Using SageMath, we have computed the following:*

- *Horizontal* $(2, 3)$*-entanglement with size* 2 *(i.e.,* $[G_6 : \langle N_2, N_3\rangle] = 2$*).*
- *No horizontal* $(3, 7)$*-entanglement.*
- *No horizontal* $(6, 7)$*-entanglement.*
- *Horizontal* $(2, 21)$*-entanglement with size* 2*.*

Furthermore, from the LMFDB database, we know the individual indices:

- $[\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) : \rho_{E,2}(G_{\mathbb{Q}})] = 3$*.*
- $[\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) : \rho_{E,3}(G_{\mathbb{Q}})] = 8$*.*
- $[\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z}) : \rho_{E,7}(G_{\mathbb{Q}})] = 1$*.*

We will now compute $[\mathrm{GL}_2(\mathbb{Z}/42\mathbb{Z}) : \rho_{E,42}(G_{\mathbb{Q}})]$ *in two different ways, using the formula derived from the previous discussion:*

$$\begin{aligned}[\mathrm{GL}_2(\mathbb{Z}/c\mathbb{Z}) : \rho_{E,c}(G_{\mathbb{Q}})] &= [\mathrm{GL}_2(\mathbb{Z}/a\mathbb{Z}) : \rho_{E,a}(G_{\mathbb{Q}})] \cdot [\mathrm{GL}_2(\mathbb{Z}/b\mathbb{Z}) : \rho_{E,b}(G_{\mathbb{Q}})] \\ &\quad \cdot [\rho_{E,a}(G_{\mathbb{Q}}) \times \rho_{E,b}(G_{\mathbb{Q}}) : \rho_{E,c}(G_{\mathbb{Q}})]\end{aligned}$$

for $c = ab$ *with* $\gcd(a, b) = 1$*. The last factor is* 1 *if there is no* (a, b)*-entanglement, and is the size of the horizontal* (a, b)*-entanglement otherwise.*

Way 1: *Decomposing* $42 = 6 \cdot 7$.

$$\begin{aligned}
[\mathrm{GL}_2(\mathbb{Z}/42\mathbb{Z}) : \rho_{E,42}(G_{\mathbb{Q}})] &= [\mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z}) : \rho_{E,6}(G_{\mathbb{Q}})] \cdot [\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z}) : \rho_{E,7}(G_{\mathbb{Q}})] \\
&\quad \cdot \underbrace{[\rho_{E,6}(G_{\mathbb{Q}}) \times \rho_{E,7}(G_{\mathbb{Q}}) : \rho_{E,42}(G_{\mathbb{Q}})]}_{\textit{No (6,7)-entanglement, so } =1} \\
&= [\mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z}) : \rho_{E,6}(G_{\mathbb{Q}})] \cdot 1 \cdot 1 \\
&= [\mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z}) : \rho_{E,6}(G_{\mathbb{Q}})] \\
&= [\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) : \rho_{E,2}(G_{\mathbb{Q}})] \cdot [\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) : \rho_{E,3}(G_{\mathbb{Q}})] \\
&\quad \cdot \underbrace{[\rho_{E,2}(G_{\mathbb{Q}}) \times \rho_{E,3}(G_{\mathbb{Q}}) : \rho_{E,6}(G_{\mathbb{Q}})]}_{\textit{(2,3)-entanglement, type size } =2} \\
&= 3 \cdot 8 \cdot 2 \\
&= 48.
\end{aligned}$$

Way 2: *Decomposing* $42 = 2 \cdot 21$.

$$\begin{aligned}
[\mathrm{GL}_2(\mathbb{Z}/42\mathbb{Z}) : \rho_{E,42}(G_{\mathbb{Q}})] &= [\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) : \rho_{E,2}(G_{\mathbb{Q}})] \cdot [\mathrm{GL}_2(\mathbb{Z}/21\mathbb{Z}) : \rho_{E,21}(G_{\mathbb{Q}})] \\
&\quad \cdot \underbrace{[\rho_{E,2}(G_{\mathbb{Q}}) \times \rho_{E,21}(G_{\mathbb{Q}}) : \rho_{E,42}(G_{\mathbb{Q}})]}_{\textit{(2,21)-entanglement, type size } =2} \\
&= [\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) : \rho_{E,2}(G_{\mathbb{Q}})] \\
&\quad \cdot \Big([\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) : \rho_{E,3}(G_{\mathbb{Q}})] \cdot [\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z}) : \rho_{E,7}(G_{\mathbb{Q}})] \\
&\qquad \cdot \underbrace{[\rho_{E,3}(G_{\mathbb{Q}}) \times \rho_{E,7}(G_{\mathbb{Q}}) : \rho_{E,21}(G_{\mathbb{Q}})]}_{\textit{No (3,7)-entanglement, so } =1} \Big) \\
&\quad \cdot 2 \\
&= 3 \cdot (8 \cdot 1 \cdot 1) \cdot 2 \\
&= 3 \cdot 8 \cdot 2 \\
&= 48.
\end{aligned}$$

Both ways yield the same result, as expected.

Remark 4.5.1. *The SageMath code used to compute the size of the horizontal entanglements is provided in the appendix at the end of this thesis.*

4.6. Miscellaneous Results related to the Division Fields

To enrich the subsequent discussion, we first present some relevant results from [30] before giving our field-theoretic interpretation of the size of a horizontal (a, b)-entanglement.

Given any finite subgroup U of an elliptic curve E defined over some number field, K, there exists an elliptic curve E' defined over $\overline{K}$ and a separable isogeny $\phi : E \to E'$ satisfying $\ker(\phi) = U$. If U is stable under the action of $\mathrm{Gal}(\overline{K}/K)$, then E' and ϕ can be chosen to be defined over K. In this case, the curve E' is uniquely determined up to K-isomorphism, is denoted by E/U, and its j-invariant $j(E/U)$ is an element of K.

Let $E/\mathbb{Q}$ be an elliptic curve. The cyclic subgroups of order n of $E[n]$ can be viewed as kernels of isogenies. Any such subgroup U is stable under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[n]))$. The quotient curve E/U is therefore defined over $\mathbb{Q}(E[n])$. We thus set:

Definition 4.6.1 (j-Invariants Field)**.** *Let $E/\mathbb{Q}$ be an elliptic curve and $n \geq 2$ an integer. The set of isogeny j-invariants is*

$$J_n = J_n(E) := \{j(E/U) \mid U \leq E[n] \text{ is a cyclic subgroup of order } n\}.$$

The field $\mathbb{Q}(J_n)$ is the extension of $\mathbb{Q}$ generated by the elements of this set.

Remark 4.6.1. *The discussion above shows that $J_n \subseteq \mathbb{Q}(E[n])$, which implies the field inclusion $\mathbb{Q}(J_n) \subseteq \mathbb{Q}(E[n])$.*

Proposition 4.6.1. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve and let $n \in \mathbb{Z}_{\geq 2}$ be an integer such that representation $\rho_{E,n}$ is surjective, i.e., $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.*

(a) For any integer $m \geq 2$ with $m \mid n$, we have $\mathbb{Q}(E[m]) \subseteq \mathbb{Q}(E[n])$. The corresponding fixed group is the kernel of the reduction map modulo m:

$$\ker\left(\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})\right) = \left\{A \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \mid A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{m}\right\}.$$

(b) We have $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$, and the corresponding fixed group is $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

(c) We have $\mathbb{Q}(J_n) \subseteq \mathbb{Q}(E[n])$, and the corresponding fixed group is the center, $Z(\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Remark 4.6.2. *The inclusion $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$ was established previously in Lemma 2.4.1.*

Proposition 4.6.2. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Let p be a prime and $m \in \mathbb{N}$ be such that the representation $\rho_{E,p^{m+1}}$ is surjective.*

(a) If $p \neq 2$, then $\mathbb{Q}(E[p^{m+1}])$ is the compositum of three key subfields:

$$\mathbb{Q}(E[p^{m+1}]) = \mathbb{Q}(E[p^m])\mathbb{Q}(\zeta_{p^{m+1}})\mathbb{Q}(J_{p^{m+1}}).$$

(b) If $p = 2$ and $m \in \mathbb{N}$, there exists an additional subfield $M_{2^{m+1}}$ such that:

$$\mathbb{Q}(E[2^{m+1}]) = \mathbb{Q}(E[2^m])\mathbb{Q}(\zeta_{2^{m+1}})\mathbb{Q}(J_{2^{m+1}})M_{2^{m+1}}.$$

Remark 4.6.3. *The field $M_{2^{m+1}}$ appearing in part (b) of the proposition can be described via Galois theory. It is the fixed field of a specific subgroup of $\mathrm{GL}_2(\mathbb{Z}/2^{m+1}\mathbb{Z})$. Let $W_{2^{m+1}}$ be the subgroup defined as:*

$$W_{2^{m+1}} := \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2^m \\ 2^m & 1 \end{pmatrix}, \begin{pmatrix} 1+2^m & 2^m \\ 0 & 1+2^m \end{pmatrix}, \begin{pmatrix} 1+2^m & 0 \\ 2^m & 1+2^m \end{pmatrix}\right\}.$$

The field $M_{2^{m+1}}$ is then the subfield of $\mathbb{Q}(E[2^{m+1}])$ fixed by the group $\pm W_{2^{m+1}}$.

Proof Sketch. By the Fundamental Theorem of Galois Theory, the compositum of fields corresponds to the intersection of their fixed groups. The fixed group of the compositum $\mathbb{Q}(E[p^m])\mathbb{Q}(\zeta_{p^{m+1}})\mathbb{Q}(J_{p^{m+1}})$ is the intersection of the corresponding subgroups inside $\mathrm{GL}_2(\mathbb{Z}/p^{m+1}\mathbb{Z})$:

$$H = \ker(\pi_{p^m}) \cap \mathrm{SL}_2(\mathbb{Z}/p^{m+1}\mathbb{Z}) \cap Z(\mathrm{GL}_2(\mathbb{Z}/p^{m+1}\mathbb{Z})).$$

A direct calculation shows that this intersection is:

$$H = \begin{cases} \{I\} & \text{if } p \neq 2, \\ \{I, (1+2^m)I\} & \text{if } p = 2. \end{cases}$$

For $p \neq 2$, the trivial intersection implies the compositum is the entire field, proving (a). For $p = 2$, the intersection is a non-trivial group of order 2. This shows that an additional field extension is needed to reduce the fixed group to the identity. This extension is precisely $M_{2^{m+1}}$, whose fixed group $\pm W_{2^{m+1}}$ doesn't contain $(1+2^m)I$, thus proving (b). □

Corollary 4.6.1. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve (not necessarily with surjective representation). The compositum formulas from Proposition 4.6.2 still hold.*

Proof Sketch. The proof strategy is identical to that of Proposition 4.6.2, except we work within the actual Galois image $G(p^{m+1}) := \rho_{E,p^{m+1}}(G_{\mathbb{Q}})$. The fixed group of the compositum is now the intersection

$$H = G(p^{m+1}) \cap \ker(\pi_{p^m}) \cap \mathrm{SL}_2(\mathbb{Z}/p^{m+1}\mathbb{Z}) \cap Z(\mathrm{GL}_2(\mathbb{Z}/p^{m+1}\mathbb{Z})).$$

This is simply the intersection of the previous group H with the actual Galois image $G(p^{m+1})$. □

The main purpose of this section was to establish that the torsion field $\mathbb{Q}(E[p^{m+1}])$ can be decomposed as the compositum of the next-lowest torsion field and a field K containing the remaining structural information. That is,

$$\mathbb{Q}(E[p^{m+1}]) = \mathbb{Q}(E[p^m])K,$$

where K is the compositum of the cyclotomic and j-invariants field (and the field $M_{2^{m+1}}$ in the case $p = 2$).

4.7. The Size of Horizontal Entanglement in Terms of Field Theory

We are now ready for our field-theoretic interpretation for the size of a horizontal (a, b)-entanglement. Let M, L, K be finite Galois extensions over the same base field F. First, note that $(L \cap M)(K \cap M)$ is a subfield of $LK \cap M$. Using [3, Section 14.4, Corollary 20], the degree of the compositum $(L \cap M)(K \cap M)$ over F is given by:

$$\begin{aligned}[(L \cap M)(K \cap M) : F] &= \frac{[L \cap M : F][K \cap M : F]}{[(L \cap M) \cap (K \cap M) : F]} \\ &= \frac{[L \cap M : F][K \cap M : F]}{[L \cap M \cap K : F]}.\end{aligned}$$

By the tower law for field extensions, we have

$$\begin{aligned}[LK \cap M : F] &= [LK \cap M : (L \cap M)(K \cap M)] \cdot [(L \cap M)(K \cap M) : F] \\ &= [LK \cap M : (L \cap M)(K \cap M)] \cdot \frac{[L \cap M : F][K \cap M : F]}{[L \cap M \cap K : F]} \\ &= \frac{[L \cap M : F][K \cap M : F] \cdot [LK \cap M : (L \cap M)(K \cap M)]}{[L \cap M \cap K : F]}.\end{aligned}$$

We consider the case where M, L, K are the torsion fields $\mathbb{Q}(E[m]), \mathbb{Q}(E[l]), \mathbb{Q}(E[k])$ respectively, for an elliptic curve $E/\mathbb{Q}$ where $\gcd(lk, m) = 1$ and $\gcd(l, k) = 1$ (i.e. pairwise coprime), which implies $\mathbb{Q}(E[l])\mathbb{Q}(E[k]) = \mathbb{Q}(E[lk])$. Suppose further that l and k are prime. If m is not prime, we can find coprime factors u, v such that $uv = m$. Then $M = \mathbb{Q}(E[m]) = \mathbb{Q}(E[u])\mathbb{Q}(E[v])$. The task of computing degrees such as $[L \cap M : F]$ (i.e., $[\mathbb{Q}(E[l]) \cap \mathbb{Q}(E[m]) : \mathbb{Q}]$) and $[K \cap M : F]$ (i.e., $[\mathbb{Q}(E[k]) \cap \mathbb{Q}(E[m]) : \mathbb{Q}]$) would then involve a recursive approach with the field degree formula above by repeatedly decomposing m.

We now apply this general degree formula to analyze the entanglement between the prime-power torsion field $\mathbb{Q}(E[p^{k+1}])$ and a torsion field $\mathbb{Q}(E[m])$ where $m \geq 2$ is an integer such that $\gcd(p^{k+1}, m) = 1$. From the decomposition in Proposition 4.6.2, we can set:

- $L = \mathbb{Q}(E[p^k])$
- $K = \mathbb{Q}(\zeta_{p^{k+1}})\mathbb{Q}(J_{p^{k+1}})$ (and its extra component if $p = 2$)
- $M = \mathbb{Q}(E[m])$

With these definitions, the compositum is $LK = \mathbb{Q}(E[p^{k+1}])$. We are interested in the size of the entanglement between m and p^{k+1}, which is the degree $[LK \cap M : \mathbb{Q}]$. Our formula applies directly:

$$\begin{aligned}[\mathbb{Q}(E[p^{k+1}]) \cap \mathbb{Q}(E[m]) : \mathbb{Q}] = &\frac{[\mathbb{Q}(E[p^k]) \cap \mathbb{Q}(E[m]) : \mathbb{Q}] \cdot [K \cap \mathbb{Q}(E[m]) : \mathbb{Q}]}{[\mathbb{Q}(E[p^k]) \cap K \cap \mathbb{Q}(E[m]) : \mathbb{Q}]} \\ &\cdot [\mathbb{Q}(E[p^{k+1}]) \cap \mathbb{Q}(E[m]) : (\mathbb{Q}(E[p^k]) \cap \mathbb{Q}(E[m]))(K \cap \mathbb{Q}(E[m]))].\end{aligned}$$

This formula shows that the total entanglement is determined by the entanglement of m with the previous torsion level ($L = \mathbb{Q}(E[p^k])$) and with the non-torsion structural parts (K). Any degree term on the right-hand side being greater than 1 pinpoints a specific source of this interaction.

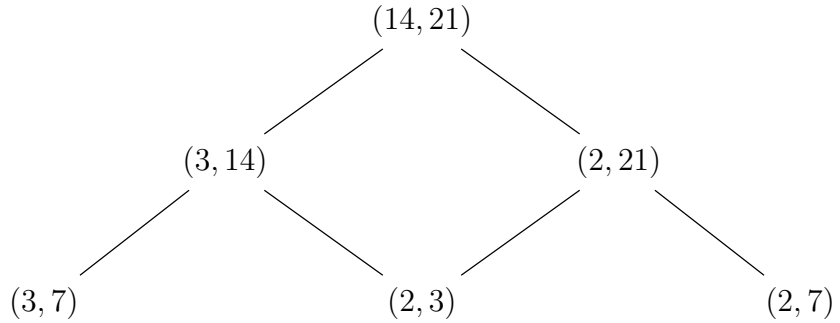
These two applications provide a complete recursive framework by repeatedly using the first strategy to break down composite levels and the second to break down prime-power levels. The following examples will illustrate the use of the previously described formula, in order to clarify each of its terms in the numerator and denominator. Before we turn to these examples, however, we want to introduce a question that remains open to us.

Question 4.7.1. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Let $m, l, k \in \mathbb{Z}_{\geq 2}$ such that $\gcd(lk, m) = 1$ and $\gcd(l, k) = 1$. Then*

$$[\mathbb{Q}(E[m]) \cap \mathbb{Q}(E[l]) \cap \mathbb{Q}(E[k]) : \mathbb{Q}] = 1.$$

Remark 4.7.1. *For elliptic curves with complex multiplication (CM), the answer to this question is known to be "no". A result in [34, Lemma 3.15.] demonstrates the latter.*

Example 4.7.1. *The diagram below represents the first "entanglement network" example discussed in this paper. The theoretical result that formally allows the construction and interpretation of such networks will be presented after the following set of illustrative examples. We focus here on various horizontal entanglements for the elliptic curve with LMFDB label* `700.c1`*. The following diagram visualizes some of these relationships:*



Based on computations using SageMath, we have determined the following entanglement properties for this curve:

- *No horizontal* $(2, 3)$*-entanglement.*
- *No horizontal* $(3, 7)$*-entanglement.*
- *Horizontal* $(2, 7)$*-entanglement with size* 2*.*
- *No horizontal* $(3, 14)$*-entanglement.*
- *Horizontal* $(2, 21)$*-entanglement with size* 2*.*
- *No horizontal* $(14, 21)$*-entanglement.*

Notice that the horizontal $(2, 21)$*-entanglement is actually a horizontal* $(2, 7)$*-entanglement, as their entanglement sizes are both* 2 *(details below). Initially, one might hypothesize that* $(14, 21)$ *would also exhibit entanglement due to the underlying* $(2, 7)$*-entanglement. However, it's not the case. The details of why that is will be worked out in the following example. Consider:*

$$[\mathbb{Q}(E[21]) \cap \mathbb{Q}(E[2]) : \mathbb{Q}] = \frac{[\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[2]) : \mathbb{Q}] \cdot [\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[2]) : \mathbb{Q}]}{[\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[3]) \cap \mathbb{Q}(E[7]) : \mathbb{Q}]} \cdot [\mathbb{Q}(E[21]) \cap \mathbb{Q}(E[2]) : (\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[2]))(\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[2]))]$$

Note the following values from Sage computations:

- $[\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[2]) : \mathbb{Q}] = 1.$
- *As a consequence,* $[\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[3]) \cap \mathbb{Q}(E[7]) : \mathbb{Q}] = [\mathbb{Q} \cap \mathbb{Q}(E[7]) : \mathbb{Q}] = 1.$

- $[\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[2]) : \mathbb{Q}] = 2$.

Since Sage also indicates that $[\mathbb{Q}(E[21]) \cap \mathbb{Q}(E[2]) : \mathbb{Q}] = 2$*, substituting these values into the formula implies that the remaining degree term must be 1:*

$$[\mathbb{Q}(E[21]) \cap \mathbb{Q}(E[2]) : (\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[2]))(\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[2]))] = 1.$$

By Proposition 1.2.3, this degree is 1 if and only if

$$\begin{aligned}(\mathbb{Q}(E[3])\mathbb{Q}(E[7]) \setminus (\mathbb{Q}(E[3]) \cup \mathbb{Q}(E[7]))) \cap \mathbb{Q}(E[2]) \\ \subseteq (\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[2]))(\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[2])).\end{aligned}$$

Given $\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[2]) = \mathbb{Q}$*, the right-hand side simplifies:*

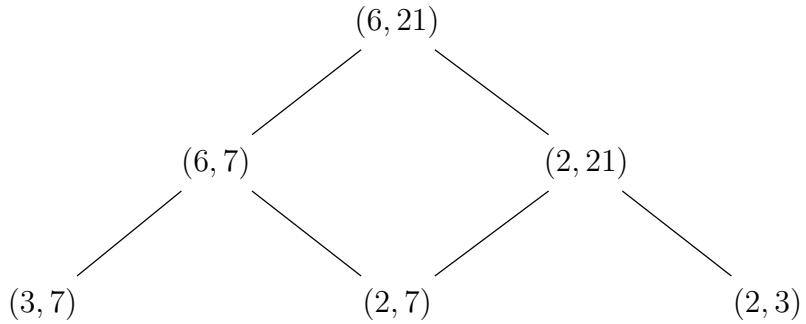
$$(\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[2]))(\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[2])) = \mathbb{Q} \cdot (\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[2])) = \mathbb{Q}(E[7]) \cap \mathbb{Q}(E[2]).$$

Thus, the condition from Proposition 1.2.3, combined with our derived equality, implies

$$(\mathbb{Q}(E[21]) \setminus (\mathbb{Q}(E[3]) \cup \mathbb{Q}(E[7]))) \cap \mathbb{Q}(E[2]) = \emptyset.$$

This is what we were expecting because the size of the $(2, 21)$*-entanglement is the same as the* $(2, 7)$*-entanglement in this context.*

Example 4.7.2. *The following diagram illustrates an entanglement network for the elliptic curve with LMFDB label* `2646.g2`*.*



Based on our computations using SageMath for this curve:

- *No horizontal* $(2, 7)$*-entanglement.*
- *Horizontal* $(3, 7)$*-entanglement with size* 2*.*
- *Horizontal* $(2, 3)$*-entanglement with size* 2*.*
- *Horizontal* $(6, 7)$*-entanglement with size* 2*.*
- *Horizontal* $(2, 21)$*-entanglement with size* 2*.*
- *No horizontal* $(6, 21)$*-entanglement.*

Observing the sizes, we can infer relationships between these entanglements. Since the sizes are the same, the $(6,7)$*-entanglement is really a* $(3,7)$*-entanglement. Similarly, the* $(2,21)$*-entanglement is really a* $(2,3)$*-entanglement. Interestingly, despite having entanglements at lower levels that contribute to the factors of* 6 *and* 21*, the pair* $(6,21)$ *itself does not exhibit horizontal entanglement. For the non-coprime case* $(6,21)$*, the definition of entanglement requires the intersection* $\mathbb{Q}(E[6]) \cap \mathbb{Q}(E[21])$ *to be a proper extension of* $\mathbb{Q}(E[3])$*. Our computational data suggests that the entanglements between the prime factors of 6 and 21 are already accounted for within* $\mathbb{Q}(E[3])$*, leading to the trivial result* $\mathbb{Q}(E[6]) \cap \mathbb{Q}(E[21]) = \mathbb{Q}(E[3])$*.*

In Sage, we have already shown that $[\mathbb{Q}(E[6]) \cap \mathbb{Q}(E[21]) : \mathbb{Q}(E[3])] = 1$*, but we would like to prove this again using our techniques developed in Section 1.2.*

By the tower law, we have:

$$[\mathbb{Q}(E[21]) \cap \mathbb{Q}(E[6]) : \mathbb{Q}] = [\mathbb{Q}(E[21]) \cap \mathbb{Q}(E[6]) : \mathbb{Q}(E[3])] \cdot [\mathbb{Q}(E[3]) : \mathbb{Q}]. \tag{4.1}$$

From our previous discussion, letting $M = \mathbb{Q}(E[6])$*,* $L = \mathbb{Q}(E[7])$*,* $K = \mathbb{Q}(E[3])$ *(so* $LK = \mathbb{Q}(E[21])$ *as* $\gcd(3,7) = 1$*), we have:*

$$\begin{aligned}[\mathbb{Q}(E[21]) \cap \mathbb{Q}(E[6]) : \mathbb{Q}] = \frac{[\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[6]) : \mathbb{Q}] \cdot [\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[6]) : \mathbb{Q}]}{[\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[6]) \cap \mathbb{Q}(E[3]) : \mathbb{Q}]} \\ \cdot [\mathbb{Q}(E[21]) \cap \mathbb{Q}(E[6]) : (\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[6]))(\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[6]))]\end{aligned} \tag{4.2}$$

Since $\mathbb{Q}(E[3]) \subseteq \mathbb{Q}(E[6])$*, we have* $\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[6]) = \mathbb{Q}(E[3])$*. Also,* $\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[6]) \cap \mathbb{Q}(E[3]) = \mathbb{Q}(E[7]) \cap \mathbb{Q}(E[3])$*. Substituting these into (4.2):*

$$\begin{aligned}[\mathbb{Q}(E[21]) \cap \mathbb{Q}(E[6]) : \mathbb{Q}] = \frac{[\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[6]) : \mathbb{Q}] \cdot [\mathbb{Q}(E[3]) : \mathbb{Q}]}{[\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[3]) : \mathbb{Q}]} \\ \cdot [\mathbb{Q}(E[21]) \cap \mathbb{Q}(E[6]) : (\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[6]))\mathbb{Q}(E[3])].\end{aligned}$$

Comparing this with equation (4.1) and dividing both sides by $[\mathbb{Q}(E[3]) : \mathbb{Q}]$*, we obtain:*

$$\begin{aligned}[\mathbb{Q}(E[6]) \cap \mathbb{Q}(E[21]) : \mathbb{Q}(E[3])] = \frac{[\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[6]) : \mathbb{Q}]}{[\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[3]) : \mathbb{Q}]} \\ \cdot [\mathbb{Q}(E[21]) \cap \mathbb{Q}(E[6]) : (\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[6]))\mathbb{Q}(E[3])].\end{aligned}$$

By Proposition 1.2.1, since $\mathbb{Q}(E[3]) \subseteq \mathbb{Q}(E[6])$*, we have*

$$\mathbb{Q}(E[21]) \cap \mathbb{Q}(E[6]) = (\mathbb{Q}(E[7])\mathbb{Q}(E[3])) \cap \mathbb{Q}(E[6]) = (\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[6]))\mathbb{Q}(E[3]).$$

Therefore, the degree term

$$[\mathbb{Q}(E[21]) \cap \mathbb{Q}(E[6]) : (\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[6]))\mathbb{Q}(E[3])] = 1.$$

So,

$$[\mathbb{Q}(E[6]) \cap \mathbb{Q}(E[21]) : \mathbb{Q}(E[3])] = \frac{[\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[6]) : \mathbb{Q}]}{[\mathbb{Q}(E[7]) \cap \mathbb{Q}(E[3]) : \mathbb{Q}]}.$$

The above is equal to 1 by our Sage computations from the beginning of the example. Therefore, there is no horizontal $(6, 21)$*-entanglement. However, while interactions between components like* $\mathbb{Q}(E[2])$ *(from* $\mathbb{Q}(E[6])$*) and* $\mathbb{Q}(E[3])$ *(from* $\mathbb{Q}(E[21])$*) might suggest entanglement, these interactions are contained within* $\mathbb{Q}(E[3])$*. Our field-theoretic definition specifically requires entanglement to manifest outside of* $\mathbb{Q}(E[\gcd(a, b)])$*.*

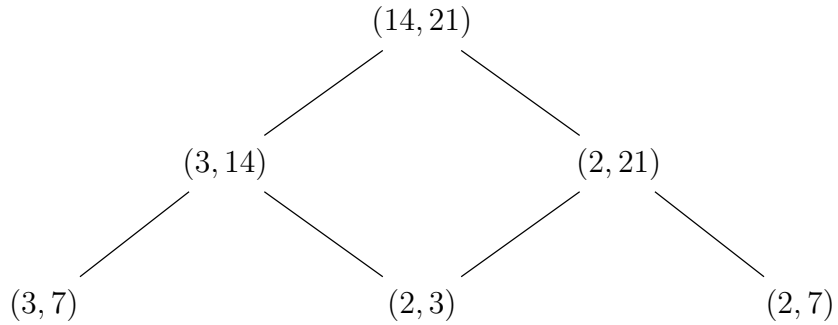
Remark 4.7.2. *This phenomenon, where lower-level entanglements are not visible at a higher composite level, has the potential to be exploited in cryptographic applications, such as a honeytoken.*

We dedicated significant thought to the following statement, and while a proof is offered in [32, Lemma 3.26], we remained unsettled by its conclusions.

Statement 4.7.1. *Let* $n \geq 12$*. Let* $\tilde{a}, \tilde{b}$ *be divisors of* n *such that* $\tilde{a} < \tilde{b}$*. Let* $\tilde{d} = \gcd(\tilde{a}, \tilde{b})$*. Define* $a := \tilde{a}/\tilde{d}$ *and* $b := \tilde{b}/\tilde{d}$*. (Note that* $\gcd(a, b) = 1$*). Suppose* $\gcd(\tilde{d}, a) = 1$ *and* $\gcd(\tilde{d}, b) = 1$*. If* G_n *has* $(\tilde{a}, \tilde{b})$*-entanglement, then* G_n *has* (a, b)*-entanglement.*

My reservations were eventually confirmed when I discovered the following counterexample that disproves the statement as originally formulated.

Example 4.7.3. *The following diagram illustrates an entanglement network for the elliptic curve with LMFDB label* `2541.f1`*.*



Based on computations using SageMath, we have determined the following entanglement properties for this curve:

- *No horizontal* $(2, 3)$*-entanglement.*
- *No horizontal* $(3, 7)$*-entanglement.*
- *No horizontal* $(2, 7)$*-entanglement.*
- *Horizontal* $(14, 3)$*-entanglement with size* 2*.*
- *Horizontal* $(2, 21)$*-entanglement with size* 2*.*
- *Horizontal* $(14, 21)$*-entanglement with size* 2*.*

Since we have no entanglements at lower levels that would contribute to a $(14,3)$*-entanglement, any* $(14,3)$*-entanglement would have to be considered intrinsic to this pair. A similar argument can be made for* $(2,21)$*, suggesting its entanglement status is also not merely inherited from the non-entanglement of its sub-pairs like* $(2,3)$ *and* $(2,7)$*.*

The goal now is to show with precision where the horizontal $(3,14)$*-entanglement is happening. We start with the degree formula:*

$$[\mathbb{Q}(E[14])\cap\mathbb{Q}(E[3]):\mathbb{Q}] = \frac{[\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3]):\mathbb{Q}]\cdot[\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3]):\mathbb{Q}]}{[\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3])\cap\mathbb{Q}(E[7]):\mathbb{Q}]} \cdot [\mathbb{Q}(E[14])\cap\mathbb{Q}(E[3]):(\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3]))(\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3]))] \tag{4.3}$$

Our previous computations from Sage shows that there is no $(3,7)$ *horizontal entanglement. This means* $[\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3]):\mathbb{Q}] = 1$*. As a consequence, the denominator becomes* $[\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3])\cap\mathbb{Q}(E[7]):\mathbb{Q}] = [\mathbb{Q}\cap\mathbb{Q}(E[2]):\mathbb{Q}] = [\mathbb{Q}:\mathbb{Q}] = 1$*. The formula thus simplifies to:*

$$[\mathbb{Q}(E[14])\cap\mathbb{Q}(E[3]):\mathbb{Q}] = [\mathbb{Q}(E[14])\cap\mathbb{Q}(E[3]):(\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3]))(\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3]))].$$

Furthermore, if we know from Sage that $[\mathbb{Q}(E[14])\cap\mathbb{Q}(E[3]):\mathbb{Q}] = 2$*, then it must be that*

$$[\mathbb{Q}(E[14])\cap\mathbb{Q}(E[3]):(\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3]))(\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3]))] = 2.$$

A degree greater than 1 implies that the fields are not equal:

$$\mathbb{Q}(E[14])\cap\mathbb{Q}(E[3]) \neq (\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3]))(\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3])).$$

Using Proposition 1.2.3 (which states $LK\cap M \neq (L\cap M)(K\cap M)$ *if and only if* $(LK\setminus(L\cup K))\cap M \not\subseteq (L\cap M)(K\cap M)$*), which means there exists an element in*

$$(\mathbb{Q}(E[14])\setminus(\mathbb{Q}(E[2])\cup\mathbb{Q}(E[7])))\cap\mathbb{Q}(E[3])$$

that is not in

$$(\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3]))(\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3])).$$

Since $\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3]) = \mathbb{Q}$ *and* $\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3]) = \mathbb{Q}$*, their compositum is* $\mathbb{Q}$*. So, the condition means there exists an element in* $(\mathbb{Q}(E[14])\setminus(\mathbb{Q}(E[2])\cup\mathbb{Q}(E[7])))\cap\mathbb{Q}(E[3])$ *that is not in* $\mathbb{Q}$*. It is a long-winded way to articulate what our intuition might suggest, but developing a precise language for these phenomena is always beneficial.*

More importantly, this example provides a counterexample to the previous statement, as $(14,21)$*-entanglement does not imply* $(2,3)$*-entanglement.*

The endeavor of constructing and seeking this counterexample was, however, fruitful in an unexpected way: it led us to an important theorem that gives precise language to the observations I had been grappling with and which I will now present.

4.8. Entanglement Networks

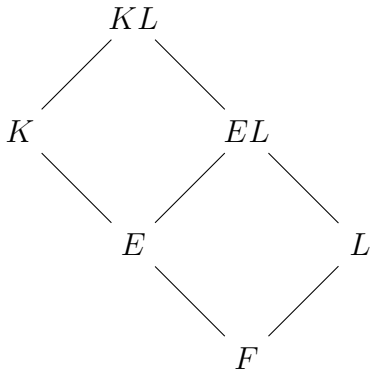
We now present a pivotal result that will serve as our primary guide, our "north star" in navigating the complexities of horizontal entanglements. The discussion and consequences derived from this theorem will form the core of our current study. However, to fully capture the horizontal entanglement phenomenon in its entirety, especially the precise arithmetic origins, the insights gained here should ideally be supplemented by a rigorous analysis of the division polynomials of the elliptic curve. This deeper arithmetic exploration is a natural avenue for future research. For now, the following theorem illuminates the path forward.

Theorem 4.8.1. *Let K and L be finite Galois extensions of F, and let E be a finite Galois extension of F such that $F \subseteq E \subseteq K$. Then*

$$K \cap L = F \iff (E \cap L = F \text{ and } K \cap EL = E).$$

Proof. The proof can be found in [35, Theorem 20.12]. □

A diagram illustrating the theorem:

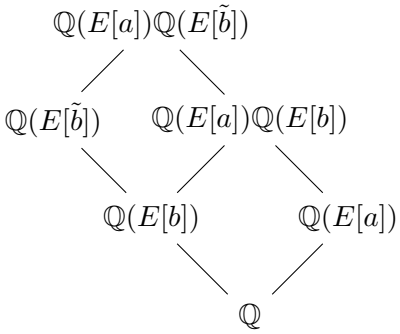


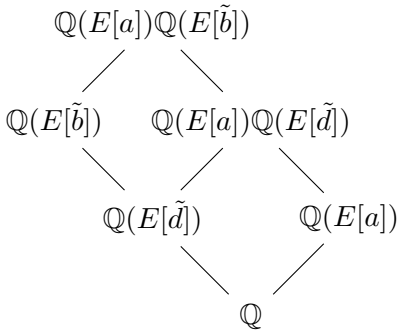
The hypothesis of the theorem can be relaxed. Instead of requiring both E and L to be finite Galois extensions of F, it is enough that at least one of them is, as long as K remains a finite Galois extension of F. For a detailed explanation, see [35, Example 20.6]. However, the version of the theorem where K, E, and L are all assumed to be finite Galois extensions of F is particularly well-suited to our current application. This is because we intend to use this theorem by setting $K = \mathbb{Q}(E[k])$, $E = \mathbb{Q}(E[e])$, $L = \mathbb{Q}(E[l])$, and $F = \mathbb{Q}$ for some elliptic curve $E/\mathbb{Q}$, where $k, e, l \in \mathbb{Z}_{\geq 2}$. As established in Proposition 2.4.2, these division fields are, in fact, finite Galois extensions of $\mathbb{Q}$. To connect this theorem specifically to the analysis of horizontal entanglement, we will also use the property that if $\gcd(a, b) = 1$, then $\mathbb{Q}(E[ab]) = \mathbb{Q}(E[a])\mathbb{Q}(E[b])$. This property allows us to impose conditions such as $\gcd(k, l) = 1$ and $\gcd(e, l) = 1$, which helps structure the fields $\mathbb{Q}(E[k]), \mathbb{Q}(E[e])$, and $\mathbb{Q}(E[l])$ in a manner conducive to applying the theorem within this context.

Let us begin our study of horizontal entanglements from our newfound perspective. Let $\tilde{a}, \tilde{b} \in \mathbb{Z}_{\geq 2}$ such that $\tilde{a} < \tilde{b}$. Define $\tilde{d} = \gcd(\tilde{a}, \tilde{b})$, and let $a = \tilde{a}/\tilde{d}$ and $b = \tilde{b}/\tilde{d}$. Note that this construction ensures $\gcd(a, b) = 1$. We will now examine two cases, imposing further conditions on a, b and $\tilde{d}$. In the first case, we will provide a detailed analysis, whereas the second case will be presented more concisely.

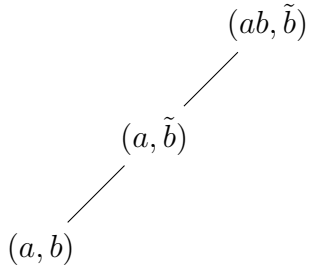
4.8.1. Case 1

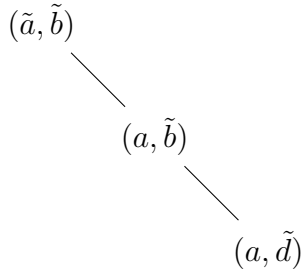
Suppose $\gcd(a, \tilde{d}) = 1$. We can build the following diagrams with the help of Theorem 4.8.1.





Theorem 4.8.1, when applied to the context of horizontal entanglement and interpreted for the diagram shown above on the left, states the following: There is no horizontal $(a, \tilde{b})$-entanglement if and only if there is no horizontal (a, b)-entanglement AND no horizontal $(ab, \tilde{b})$-entanglement. Equivalently (by negating both sides of the biconditional), there IS horizontal $(a, \tilde{b})$-entanglement if and only if there IS horizontal (a, b)-entanglement OR there IS horizontal $(ab, \tilde{b})$-entanglement. A similar reformulation can be made for the diagram shown above on the right. These conceptual relationships can be visualized as depicted below.





We refer to the middle node in our diagrams as the *entanglement key*. Based on the reformulation of Theorem 4.8.1, if the entanglement key itself is "turned off" (meaning there is no horizontal entanglement associated directly with its defining parameters), then we can deduce that both nodes directly connected to it must also be "turned off".

In a more extensive entanglement network, the relationships between various nodes and a specific entanglement key may become less immediately apparent. A notable pattern, however, is that the greatest common divisor of the two integers defining a "higher" node (the node above the entanglement key) often appears as one of the integers defining a "lower" node connected to it or to the key.

We can conclude the theoretical discussion in this subsection by illustrating how an *entanglement network* can be formed by combining the two diagrams presented above.

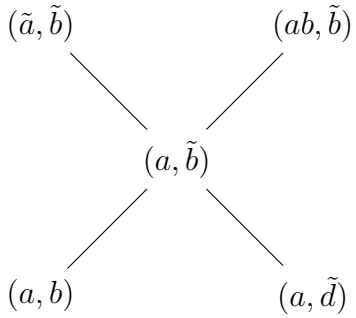
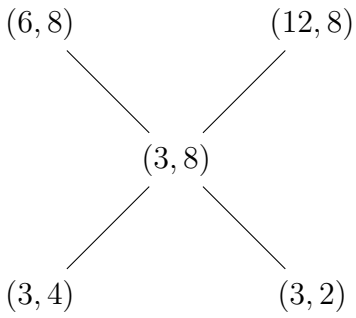


Figure 4.1: Entanglement Network for Case 1

Remark 4.8.1. *If the entanglement key $(a, \tilde{b})$ is "turned off" (i.e., exhibits no horizontal entanglement associated with its parameters), then as a consequence, the four outer nodes connected to it in our combined diagram are also "turned off".*

Definition 4.8.1. *An* entanglement network *is a diagram constructed by meshing together multiple individual* entanglement diagrams*, where each such individual diagram is derived from the application of Theorem 4.8.1.*

Example 4.8.1. *Let us consider the elliptic curve with LMFDB label* `21.a1`*. We will construct an entanglement network related to this curve, analogous to the general structure discussed above, taking $\tilde{a} = 6$ and $\tilde{b} = 8$. The corresponding parameters would be $\tilde{d} = \gcd(6, 8) = 2$, $a = \tilde{a}/\tilde{d} = 6/2 = 3$, and $b = \tilde{b}/\tilde{d} = 8/2 = 4$. The entanglement key in this specific instance would correspond to $(a, \tilde{b})$ from our general diagram, which is $(3, 8)$.*



For the elliptic curve `21.a1`*, the following entanglement properties were computed using Sage:*

- *No horizontal $(3, 2)$-entanglement.*
- *Horizontal $(3, 4)$-entanglement with size 2.*
- *Horizontal $(3, 8)$-entanglement (the key) with size 2.*
- *Horizontal $(6, 8)$-entanglement with size 2.*
- *No horizontal $(12, 8)$-entanglement.*

Remark 4.8.2. *Conventionally, any entanglement pair is denoted as (a, b) where $a < b$. However, in the preceding example, we have not strictly adhered to this convention for all listed pairs. This was done intentionally so that the position and order of the variables in the entanglement pairs correspond to the structure and labeling of the general diagram presented before the example.*

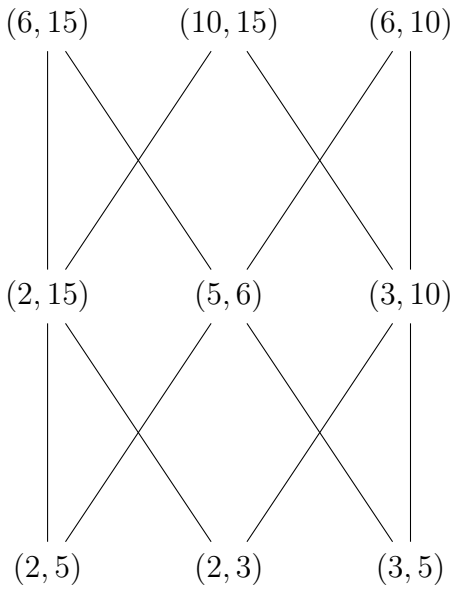
The adelic level, m_E (see Definition 4.1.3), captures all the entanglement behavior, both horizontal and vertical, associated with an elliptic curve. Our prior analysis of horizontal entanglements suggests to investigate horizontal entanglements arising from coprime integers. Therefore, a thorough understanding of the adelic index requires examining all pairs of coprime integers (a, b) such that $a \mid m_E$, $b \mid m_E$, and their product $ab \leq m_E$ (Since $\gcd(a, b) = 1$, it is necessarily true that $ab \leq m_E$). Of course, a complete understanding of the adelic index would also necessitate a thorough analysis of all vertical entanglements. However, in this section, our focus is specifically confined to horizontal entanglements.

Definition 4.8.2. *A full entanglement network for a given elliptic curve $E/\mathbb{Q}$ is an entanglement network that explicitly includes all nodes (a, b) for which the pair of integers (a, b) exhibits a horizontal entanglement relevant to E and $\gcd(a, b) = 1$.*

Remark 4.8.3. *Proposition 4.4.2 states that for an elliptic curve over $\mathbb{Q}$, the adelic Galois image is never surjective onto $\mathrm{GL}_2(\hat{\mathbb{Z}})$. Suppose that an elliptic doesn't exhibit only condition (1) from Proposition 4.4.2, then there is always at least one node in the full entanglement network that is "turned on".*

Example 4.8.2. *Let us consider the elliptic curve with LMFDB label `300.b2`. The LMFDB indicates that its adelic level is $m_E = 30$. We are interested in pairs of coprime integers: $(2, 3)$, $(2, 5)$, $(3, 5)$, $(2, 15)$, $(3, 10)$, and $(5, 6)$.*

Furthermore, we can build three distinct entanglement networks based on Figure 4.1 and then mesh these three networks together to obtain a full entanglement network for the elliptic curve `300.b2`.



In this network, the middle row represents the entanglement keys. The nodes in the above row don't contribute to the computation of the adelic index. Our computations in Sage for the elliptic curve `300.b2` *show the following horizontal entanglement properties:*

- *Has horizontal* $(2,3)$*-entanglement with size 6.*
- *Has no horizontal* $(2,5)$*-entanglement.*
- *Has horizontal* $(2,15)$*-entanglement with size 6.*
- *Has horizontal* $(3,5)$*-entanglement with size 2.*
- *Has horizontal* $(3,10)$*-entanglement with size 12.*
- *Has horizontal* $(5,6)$*-entanglement with size 2.*

Moreover, data from the LMFDB tells us that the mod-2 and mod-5 Galois representations are surjective, while the index $[\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) : \rho_{E,3}(G_{\mathbb{Q}})] = 4$*. We can now compute the adelic index for the given elliptic curve.*

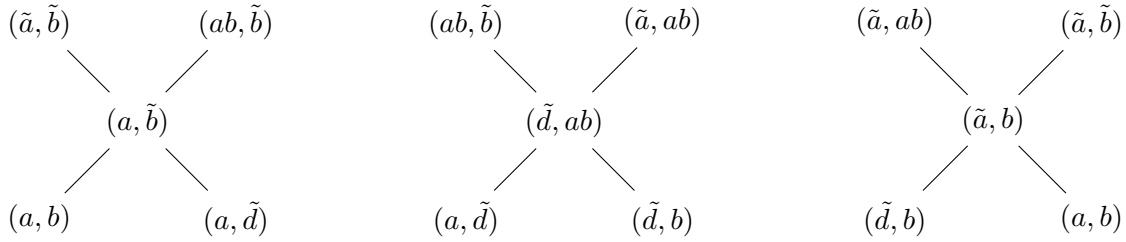
$$\begin{aligned}
[\mathrm{GL}_2(\mathbb{Z}/30\mathbb{Z}) : \rho_{E,30}(G_{\mathbb{Q}})] &= [\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) : \rho_{E,3}(G_{\mathbb{Q}})] \cdot [\mathrm{GL}_2(\mathbb{Z}/10\mathbb{Z}) : \rho_{E,10}(G_{\mathbb{Q}})] \\
&\quad \cdot [\rho_{E,3}(G_{\mathbb{Q}}) \times \rho_{E,10}(G_{\mathbb{Q}}) : \rho_{E,30}(G_{\mathbb{Q}})] \\
&= 4 \cdot [\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) : \rho_{E,2}(G_{\mathbb{Q}})] \cdot [\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z}) : \rho_{E,5}(G_{\mathbb{Q}})] \\
&\quad \cdot [\rho_{E,3}(G_{\mathbb{Q}}) \times \rho_{E,10}(G_{\mathbb{Q}}) : \rho_{E,30}(G_{\mathbb{Q}})] \\
&= 4 \cdot 1 \cdot 1 \cdot 12 = 48
\end{aligned}$$

Remark 4.8.4. *Consider the entanglement network above as an entanglement network and not a full entanglement network associated to an elliptic curve. If two of the entanglement keys (i.e. two of* $(2,15), (5,6), (3,10)$*) were "turned off", then the entire network would also be "turned off".*

Remark 4.8.5. *Several interesting questions arise from this perspective. For instance, what is the minimum number of key entanglement nodes that need to be "turned off" for the entire entanglement network to be off? Exploring the structure of these entanglement networks might benefit from combinatorial approaches. Furthermore, one might speculate whether these entanglement networks could have potential cryptographic applications.*

4.8.2. Case 2

Suppose $\gcd(a, \tilde{d}) = 1$ and $\gcd(b, \tilde{d}) = 1$. We can build the three following diagrams with the help of Theorem 4.8.1.



We now mesh the diagrams presented above to form a comprehensive entanglement network. This network is specifically tailored to the assumptions outlined at the beginning of this subsection.

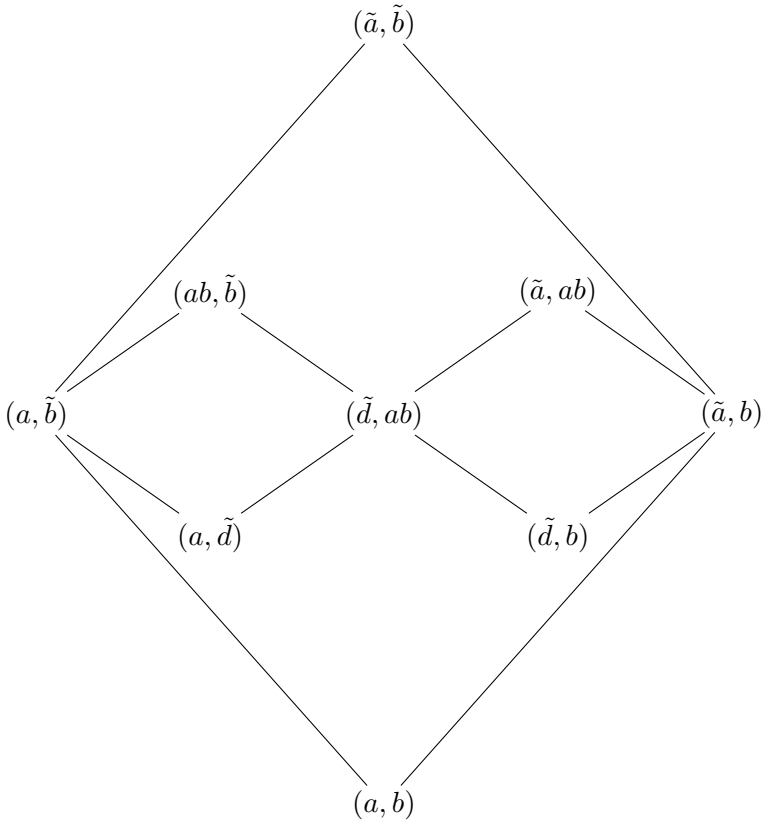
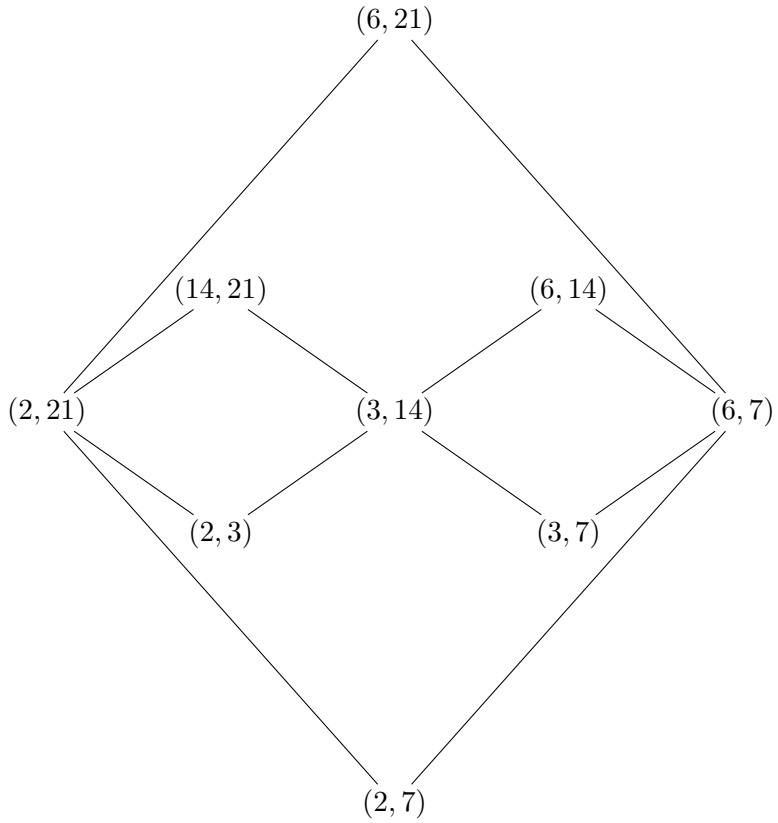


Figure 4.2: Entanglement Network for Case 2

The nodes $(a, \tilde{b})$, $(\tilde{d}, ab)$, and $(\tilde{a}, b)$ serve as the *entanglement keys* for the entanglement network depicted above. If any two of these three keys are "turned off" (i.e., exhibit no horizontal entanglement associated with their parameters), then the entire network would consequently be "turned off".

Each entanglement key is connected to two "higher" nodes and two "lower" nodes in the diagram. A "higher" node is related to a "lower" node if the greatest common divisor of the two integers defining the "higher" node appears as one of the integers defining the "lower" node.

Example 4.8.3. *Below is a numerical example, corresponding to the structure of Figure 4.2, for the elliptic curve with LMFDB label* `2646.g2`.



Based on computations using SageMath, we have determined the following horizontal entanglement properties for this curve:

- *No horizontal* $(6, 21)$*-entanglement.*
- *Horizontal* $(14, 21)$*-entanglement with size 2.*
- *Horizontal* $(6, 14)$*-entanglement with size 2.*
- *Horizontal* $(2, 21)$*-entanglement with size 2.*
- *Horizontal* $(3, 14)$*-entanglement with size 4.*

- *Horizontal* $(6,7)$*-entanglement with size 2.*
- *Horizontal* $(2,3)$*-entanglement with size 2.*
- *Horizontal* $(3,7)$*-entanglement with size 2.*
- *No horizontal* $(2,7)$*-entanglement.*

The only "real" horizontal entanglements in this network are the $(2,3)$ *and* $(3,7)$*. Consider*

$$[\mathbb{Q}(E[14])\cap\mathbb{Q}(E[3]):\mathbb{Q}] = \frac{[\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3]):\mathbb{Q}]\cdot[\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3]):\mathbb{Q}]}{[\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3])\cap\mathbb{Q}(E[7]):\mathbb{Q}]} \cdot [\mathbb{Q}(E[2])\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3]):(\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3]))(\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3]))]$$

We know the LHS of the equation is 4 *and* $[\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3]):\mathbb{Q}] = [\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3]):\mathbb{Q}] = 2$*, which forces*

$$\frac{[\mathbb{Q}(E[2])\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3]):(\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3]))(\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3]))]}{[\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3])\cap\mathbb{Q}(E[7]):\mathbb{Q}]} = 1.$$

Also, we know that $[\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3])\cap\mathbb{Q}(E[7]):\mathbb{Q}] = 1$ *as there is no* $(2,7)$ *entanglement, therefore*

$$[\mathbb{Q}(E[2])\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3]):(\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3]))(\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3]))] = 1,$$

meaning the $(3,14)$ *entanglement is strictly from* $(2,3)$ *and* $(3,7)$ *as*

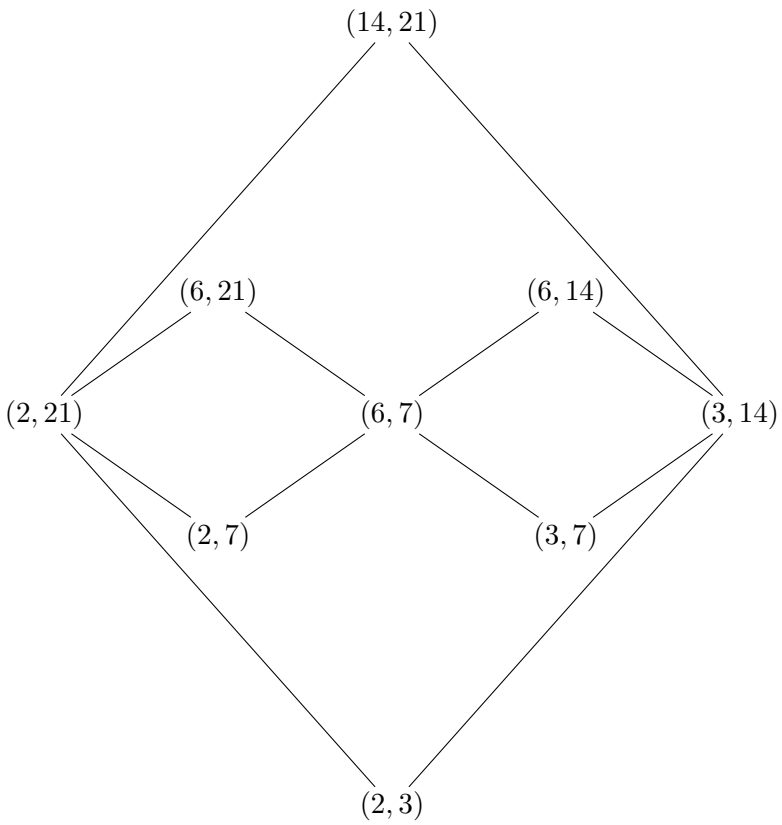
$$(\mathbb{Q}(E[14])\setminus(\mathbb{Q}(E[2])\cup\mathbb{Q}(E[7])))\cap\mathbb{Q}(E[3]) \subseteq (\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3]))(\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3])),$$

this means that $\mathbb{Q}(E[14])\cap\mathbb{Q}(E[3])$ *contains* $\mathbb{Q}(E[2])\cap\mathbb{Q}(E[3])$*,* $\mathbb{Q}(E[7])\cap\mathbb{Q}(E[3])$*, and their aggregate. So there is no inherent or true entanglement happening between* $\mathbb{Q}(E[14])$ *and* $\mathbb{Q}(E[3])$*.*

In a similar way, one can show that all other pairs that exhibit horizontal entanglement in this network are really from $(2,3)$ *or* $(3,7)$*.*

Furthermore, $(6,21)$ *exhibits no entanglement as per the definition because all entanglements happen under the* gcd *threshold.*

Example 4.8.4. *Below is another numerical example, corresponding to the structure of Figure 4.2, for the elliptic curve with LMFDB label* `700.c1`*.*



Based on computations using SageMath, we have determined the following horizontal entanglement properties for this curve:

- *No horizontal* $(14, 21)$*-entanglement.*
- *Horizontal* $(6, 21)$*-entanglement with size 2.*
- *No horizontal* $(6, 14)$*-entanglement.*
- *Horizontal* $(2, 21)$*-entanglement with size 2.*
- *Horizontal* $(6, 7)$*-entanglement with size 2.*
- *No horizontal* $(3, 14)$*-entanglement.*
- *Horizontal* $(2, 7)$*-entanglement with size 2.*
- *No horizontal* $(3, 7)$*-entanglement.*
- *No horizontal* $(2, 3)$*-entanglement.*

We will not go into detail as the tools for navigating such examples have been presented. However, we note that in this network, the only "real" entanglement is the horizontal $(2, 7)$*-entanglement.*

Remark 4.8.6. *The diagrams presented in the previous two examples portray a full entanglement network for their respective elliptic curves. This is because each diagram is constructed to include all nodes* (a, b) *such that* $\gcd(a, b) = 1$, $a \mid m_E$, $b \mid m_E$ *and* $ab \leq m_E$ *for the corresponding elliptic curve.*

We will now conclude this section on entanglements by presenting an interesting example of a phenomenon related to entanglement that, to our knowledge, appears to be new. This phenomenon we term *entangled entanglements*.

Example 4.8.5. *For the elliptic curve with LMFDB label* `2541.f1`*, we have seen that* $[\rho_{E,2}(G_{\mathbb{Q}}) \times \rho_{E,3}(G_{\mathbb{Q}}) : \rho_{E,6}(G_{\mathbb{Q}})] = 1$, $[\rho_{E,2}(G_{\mathbb{Q}}) \times \rho_{E,7}(G_{\mathbb{Q}}) : \rho_{E,14}(G_{\mathbb{Q}})] = 1$, *and* $[\rho_{E,3}(G_{\mathbb{Q}}) \times \rho_{E,7}(G_{\mathbb{Q}}) : \rho_{E,21}(G_{\mathbb{Q}})] = 1$, *as there is no* $(2, 3)$, $(2, 7)$, *or* $(3, 7)$ *horizontal entanglement. We also know that* $[\rho_{E,14}(G_{\mathbb{Q}}) \times \rho_{E,3}(G_{\mathbb{Q}}) : \rho_{E,42}(G_{\mathbb{Q}})] = 2$ *as* E *has horizontal* $(3, 14)$*-entanglement with size 2. Moreover, the LMFDB database tells us that* $m_E = 42$, $[\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) : \rho_{E,2}(G_{\mathbb{Q}})] = 1$, $[\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z}) : \rho_{E,7}(G_{\mathbb{Q}})] = 1$, *and* $[\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) : \rho_{E,3}(G_{\mathbb{Q}})] = 8$. *We calculate the adelic index in three different ways:*

1. $[\mathrm{GL}_2(\mathbb{Z}/42\mathbb{Z}) : \rho_{E,42}(G_{\mathbb{Q}})] = [\mathrm{GL}_2(\mathbb{Z}/14\mathbb{Z}) : \rho_{E,14}(G_{\mathbb{Q}})] \cdot [\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) : \rho_{E,3}(G_{\mathbb{Q}})]$
$\cdot [\rho_{E,14}(G_{\mathbb{Q}}) \times \rho_{E,3}(G_{\mathbb{Q}}) : \rho_{E,42}(G_{\mathbb{Q}})]$
$= [\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) : \rho_{E,2}(G_{\mathbb{Q}})] \cdot [\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z}) : \rho_{E,7}(G_{\mathbb{Q}})]$
$\cdot [\rho_{E,2}(G_{\mathbb{Q}}) \times \rho_{E,7}(G_{\mathbb{Q}}) : \rho_{E,14}(G_{\mathbb{Q}})]$
$\cdot [\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) : \rho_{E,3}(G_{\mathbb{Q}})] \cdot [\rho_{E,14}(G_{\mathbb{Q}}) \times \rho_{E,3}(G_{\mathbb{Q}}) : \rho_{E,42}(G_{\mathbb{Q}})] = (1 \cdot 1 \cdot 1) \cdot 8 \cdot 2 = 16.$

2. $[\mathrm{GL}_2(\mathbb{Z}/42\mathbb{Z}) : \rho_{E,42}(G_{\mathbb{Q}})] = [\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) : \rho_{E,2}(G_{\mathbb{Q}})] \cdot [\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) : \rho_{E,3}(G_{\mathbb{Q}})] \cdot [\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z}) : \rho_{E,7}(G_{\mathbb{Q}})] \cdot [\rho_{E,21}(G_{\mathbb{Q}}) \times \rho_{E,2}(G_{\mathbb{Q}}) : \rho_{E,42}(G_{\mathbb{Q}})]$. *Since the LHS is 16, and the product of the first three terms on the RHS is* 8*, this forces* $[\rho_{E,21}(G_{\mathbb{Q}}) \times \rho_{E,2}(G_{\mathbb{Q}}) : \rho_{E,42}(G_{\mathbb{Q}})] = 2$*, meaning there is horizontal* $(2, 21)$*-entanglement with size 2.*

3. $[\mathrm{GL}_2(\mathbb{Z}/42\mathbb{Z}) : \rho_{E,42}(G_{\mathbb{Q}})] = [\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) : \rho_{E,2}(G_{\mathbb{Q}})] \cdot [\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) : \rho_{E,3}(G_{\mathbb{Q}})] \cdot [\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z}) : \rho_{E,7}(G_{\mathbb{Q}})] \cdot [\rho_{E,6}(G_{\mathbb{Q}}) \times \rho_{E,7}(G_{\mathbb{Q}}) : \rho_{E,42}(G_{\mathbb{Q}})]$. *Similarly, this forces* $[\rho_{E,6}(G_{\mathbb{Q}}) \times \rho_{E,7}(G_{\mathbb{Q}}) : \rho_{E,42}(G_{\mathbb{Q}})] = 2$*, meaning there is horizontal* $(6, 7)$*-entanglement with size 2.*

The entanglements $(3, 14)$, $(2, 21)$, *and* $(6, 7)$ *are all "true" entanglements as they do not arise from entanglements at the lower level (in our case, the lower level would be* $(2, 3)$, $(2, 7)$, *and* $(3, 7)$*, which have no entanglement). In some sense, for this specific example, once we know that there is horizontal* $(3, 14)$*-entanglement, then we know immediately that there is also* $(2, 21)$ *and* $(6, 7)$*-entanglement because of the calculations above. Therefore, these entanglements are entangled.*

Let us define

- $K_2 := (\mathbb{Q}(E[21]) \setminus (\mathbb{Q}(E[3]) \cup \mathbb{Q}(E[7]))) \cap \mathbb{Q}(E[2])$, *and* $K_2 \not\subseteq \mathbb{Q}$.
- $K_3 := (\mathbb{Q}(E[14]) \setminus (\mathbb{Q}(E[2]) \cup \mathbb{Q}(E[7]))) \cap \mathbb{Q}(E[3])$, *and* $K_3 \not\subseteq \mathbb{Q}$.
- $K_7 := (\mathbb{Q}(E[6]) \setminus (\mathbb{Q}(E[2]) \cup \mathbb{Q}(E[3]))) \cap \mathbb{Q}(E[7])$, *and* $K_7 \not\subseteq \mathbb{Q}$.

Furthermore, these distinct entanglement phenomena (represented by K_2, K_3, K_7*) do not originate from a single, common underlying intersection. This is evidenced by the fact that* $K_2 \cap K_3 = \emptyset$, $K_2 \cap K_7 = \emptyset$, *and* $K_3 \cap K_7 = \emptyset$, *because we first mentioned that* $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[3]) = \mathbb{Q}$, $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[7]) = \mathbb{Q}$, *and* $\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[7]) = \mathbb{Q}$.

4.9. Finding Unentangled Integers

We conclude this chapter by presenting a theorem from [11] that provides a condition for constructing integers n such that there is no entanglement among the torsion fields associated with its divisors. The proof of this theorem will draw heavily upon the group-theoretic results established in Section 3.1.

The following result requires a specific constant, which is a variation of Serre's constant.

Definition 4.9.1. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve. We define the constant $A_{30}(E)$ by the formula*

$$A_{30}(E) = 30 \cdot \prod_{p \in S_E} p,$$

where S_E is the set of primes p for which the mod-p Galois representation $\rho_{E,p}$ is not surjective.

Theorem 4.9.1. *If E is an elliptic curve defined over $\mathbb{Q}$ and n is any integer with $\gcd(n, 30) = 1$, then the Galois representation*

$$\rho_{E,n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

is surjective if and only if the Galois representations $\rho_{E,p}$ are surjective for every prime $p \mid n$. In particular, if E is a non-CM elliptic curve then $\rho_{E,n}$ is surjective for every integer n with $\gcd(n, A_{30}(E)) = 1$.

Proof. If $\rho_{E,n}$ is surjective, then so is $\rho_{E,p} = \mathrm{pr}_p^{(n)} \circ \rho_{E,n}$ for every $p \mid n$.

Conversely, suppose $\rho_{E,p}$ is surjective for all $p \mid n$. Then $\rho_{E,n}(G_{\mathbb{Q}}) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, i.e., $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is a quotient of $\rho_{E,n}(G_{\mathbb{Q}}) \leq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ by the First Isomorphism Theorem. As a result, applying Lemma 3.1.5 and Lemma 3.1.6, $\mathrm{Occ}(\rho_{E,n}(G_{\mathbb{Q}})) \supseteq \bigcup_{p|n} \mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})) = \bigcup_{p|n} \mathrm{Occ}(\mathrm{PSL}_2(p))$ and so $\mathrm{PSL}_2(p) \in \mathrm{Occ}(\rho_{E,n}(G_{\mathbb{Q}}))$ for every $p \mid n$ and hence $\rho_{E,n}(G_{\mathbb{Q}}) \geq \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ by Theorem 3.1.3(b).

Recall that $\rho_{E,n}(G_{\mathbb{Q}}) \cong \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ and that $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$ by the existence of the Weil Pairing. Via the Galois correspondence, we have

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

and so $\varphi(n) = [\rho_{E,n}(G_{\mathbb{Q}}) : H]$ where $H := \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}(\zeta_n))$. Finally, because $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is abelian we have that $\rho_{E,n}(G_{\mathbb{Q}})' \leq \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}(\zeta_n))$, which means $|\rho_{E,n}(G_{\mathbb{Q}})'| \cdot k = |H|$ and so

$$\varphi(n) = \frac{|\rho_{E,n}(G_{\mathbb{Q}})|}{|H|} = \frac{|\rho_{E,n}(G_{\mathbb{Q}})|}{|\rho_{E,n}(G_{\mathbb{Q}})'| \cdot k}$$

$$k \cdot \varphi(n) = \frac{|\rho_{E,n}(G_{\mathbb{Q}})|}{|\rho_{E,n}(G_{\mathbb{Q}})'|} = [\rho_{E,n}(G_{\mathbb{Q}}) : \rho_{E,n}(G_{\mathbb{Q}})'].$$

The result now follows from Theorem 3.1.3(a).

The last assertion is clear, for by definition $A_{30}(E) = 30 \prod_{p \in S_E} p$, where S_E is the set of primes p such that $\rho_{E,p}$ is not surjective. □

Bibliography

[1] Jean-Pierre Serre. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques". In: *Inventiones Mathematicae* 15.4 (1972), pp. 259–331. DOI: 10.1007/BF01405086.

[2] Keith Conrad. "The Galois Correspondence". Expository notes available online. No date provided. URL: https://kconrad.math.uconn.edu/blurbs/galoistheory/galoiscorr.pdf (visited on 10/27/2023).

[3] David S. Dummit and Richard M. Foote. *Abstract algebra*. Third. John Wiley & Sons, Inc., Hoboken, NJ, 2004, pp. xii+932. ISBN: 0-471-43334-9.

[4] Derek J. S. Robinson. *A course in the theory of groups*. Second. Vol. 80. Graduate Texts in Mathematics. Springer-Verlag, New York, 1996, pp. xviii+499. ISBN: 0-387-94461-3. DOI: 10.1007/978-1-4419-8594-1. URL: https://doi.org/10.1007/978-1-4419-8594-1.

[5] Gareth Wilkes. "Part III Profinite Groups". Expository notes available online. No date provided. URL: https://www.dpmms.cam.ac.uk/~grw46/LectureNotes.pdf (visited on 10/27/2023).

[6] Keith Conrad. "Infinite Galois Theory". Expository notes available online. No date provided. URL: https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2020/06/CTNT-InfGaloisTheory.pdf (visited on 10/27/2023).

[7] James S. Milne. "Fields and Galois Theory". Version 4.62. 2021. URL: https://www.jmilne.org/math/CourseNotes/FT.pdf (visited on 10/26/2023).

[8] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Second. Vol. 106. Graduate Texts in Mathematics. New York: Springer, 2009. ISBN: 978-0387094939.

[9] Robin Hartshorne. *Algebraic Geometry*. Vol. 52. Graduate Texts in Mathematics. New York: Springer-Verlag, 1977. ISBN: 978-0387902449.

[10] Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves*. Second. Undergraduate Texts in Mathematics. Cham: Springer International Publishing, 2015. ISBN: 978-3319185873.

[11] Ernst Kani. "On the Surjectivity of Galois Representations Associated to Elliptic Curves". Preprint available online. Mar. 2004. URL: https://mast.queensu.ca/~kani/papers/surjective-mar03.pdf (visited on 10/27/2023).

[12] Bertram Huppert. *Endliche Gruppen I*. Vol. 134. Die Grundlehren der mathematischen Wissenschaften. Berlin-New York: Springer-Verlag, 1967.

[13] Keith Conrad. "Semidirect Products". Expository notes available online. No date provided. URL: https://kconrad.math.uconn.edu/blurbs/grouptheory/semidirect-product.pdf (visited on 10/27/2023).

[14] Keith Conrad. "$\mathrm{SL}(2,\mathbb{Z})$". Expository notes available online. No date provided. URL: https://kconrad.math.uconn.edu/blurbs/grouptheory/SL(2,Z).pdf (visited on 10/27/2023).

[15] Jean-Pierre Serre. *Abelian ℓ-adic Representations and Elliptic Curves*. Based on lectures given at McGill University, 1967. New York-Amsterdam: W. A. Benjamin, Inc., 1968.

[16] Hans Kurzweil and Bernd Stellmacher. *The Theory of Finite Groups: An Introduction*. Universitext. New York: Springer-Verlag, 2004. ISBN: 0-387-40510-0.

[17] Leonard Eugene Dickson. *Linear Groups with an Exposition of Galois Field Theory*. Reprint of the 1901 original published by B. G. Teubner. Cosimo Classics, Lightning Source Incorporated, 2007. ISBN: 978-1602062939.

[18] John F. Humphreys. *A Course in Group Theory*. Oxford: Oxford University Press, 1996. ISBN: 978-0198534594.

[19] David Zywina. *Elliptic Curves with Maximal Galois Action on their Torsion Points*. 2008. arXiv: 0809.3482 [math.NT].

[20] David Zywina. "On the Possible Images of the mod ℓ Representations Associated to Elliptic Curves over $\mathbb{Q}$". In: *Transactions of the American Mathematical Society* 367.10 (2015), pp. 6977–7015.

[21] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*. 2nd. Discrete Mathematics and Its Applications. Boca Raton, FL: Chapman and Hall/CRC, 2008. ISBN: 978-1420071467.

[22] Nathan Jones. *A Bound for the Conductor of an Open Subgroup of* GL_2 *Associated to an Elliptic Curve*. 2019. arXiv: 1904.10431 [math.NT].

[23] David Zywina. *Explicit Open Images for Elliptic Curves over* $\mathbb{Q}$. 2022. arXiv: 2206.14959 [math.NT].

[24] Julio Brau Avila. "Galois Representations of Elliptic Curves and Abelian Entanglements". Doctoral Thesis. Leiden University, Dec. 2015. URL: https://scholarlypublications.universiteitleiden.nl/handle/1887/37019.

[25] Noam D. Elkies. *Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9*. 2006. arXiv: math/0612734 [math.NT].

[26] Nathan Jones. *Almost all elliptic curves are Serre curves*. 2006. arXiv: math/0611096 [math.NT].

[27] Andrew V. Sutherland. *Computing images of Galois representations attached to elliptic curves*. 2015. arXiv: 1504.07618 [math.NT].

[28] Jeremy Rouse and David Zureick-Brown. *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*. 2014. arXiv: 1402.5997 [math.NT].

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

[30] Clemens Adelmann. *The decomposition of primes in torsion point fields*. Vol. 1761. Lecture Notes in Mathematics. Springer-Verlag, Berlin, 2001, pp. vi+142. ISBN: 3-540-42035-5. DOI: 10.1007/b80624. URL: https://doi.org/10.1007/b80624.

[31] Tim Dokchitser and Vladimir Dokchitser. *Surjectivity of mod 2^n representations of elliptic curves*. 2011. arXiv: 1104.5031 [math.NT].

[32] Joost Mein. "Entanglements of Galois representations of elliptic curves over $\mathbb{Q}$". Master's Thesis. Utrecht University, Aug. 2022. URL: https://studenttheses.uu.nl/bitstream/handle/20.500.12932/42532/Entanglement.pdf?sequence=1 (visited on 10/27/2023).

[33] Harris B. Daniels and Jackson S. Morrow. "A group theoretic perspective on entanglements of division fields". In: *Trans. Amer. Math. Soc. Ser. B* 9 (2022), pp. 827–858. ISSN: 2330-0000. DOI: 10.1090/btran/95. URL: https://doi.org/10.1090/btran/95.

[34] Abbey Bourdon, Pete L. Clark, and James Stankewicz. *Torsion Points on CM Elliptic Curves Over Real Number Fields*. 2015. arXiv: 1411.2742 [math.NT].

[35] Patrick Morandi. *Field and Galois Theory*. Vol. 167. Graduate Texts in Mathematics. New York: Springer-Verlag, 1996. ISBN: 978-0-387-94753-2. DOI: 10.1007/978-1-4612-4040-3.

[36] Andrew V. Sutherland and David Zywina. "Modular curves of prime-power level with infinitely many rational points". In: *Algebra Number Theory* 11.5 (2017), pp. 1199–1229. DOI: 10.2140/ant.2017.11.1199.

[37] Andrew V. Sutherland and David Zywina. *GL2Invariants.m: MAGMA code for subgroup invariants*. GitHub repository. Accessed: 2025-07-01. 2017. URL: https://github.com/jmorrow4692/Entanglements/blob/master/AuxillaryFiles/%5BSZ17%5D/GL2Invariants.m.

[38] Enrique González-Jiménez and Álvaro Lozano-Robledo. *Elliptic Curves with abelian division fields*. 2015. arXiv: 1511.08578 [math.NT].

Appendix A. CODE

The following appendix is divided into two sections. The first section is dedicated to providing the SageMath code for an algorithm that constructs all applicable subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ for any integer $n \geq 2$. The second section provides the SageMath code used to compute the horizontal entanglement data for a specific elliptic curve.

A.1. CODE for Applicable Subgroups

The SageMath code presented in this section was inspired by the MAGMA implementation written by Sutherland and Zywina, which is designed to compute all applicable subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ for any integer $n \geq 2$. The original code is associated with the work in [36] and is available online [37].

To avoid potential errors caused by copying code from this PDF, please use the original source available on GitHub:

`https://github.com/campanella98/Computing-Applicable-Subgroups-of-GL2-Z-nZ-in-SageMath`

Using the GitHub version is highly recommended for accuracy.

The following definition is essential for understanding the logic of the subsequent code.

Definition A.1.1 (Invariant Factor Decomposition)**.** *Any finite abelian group G is isomorphic to a direct product of cyclic groups of the form:*

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$$

where the integers d_i satisfy the divisibility condition $d_n \mid d_{n-1} \mid \cdots \mid d_2 \mid d_1$. The integers $d_1, d_2, \ldots, d_n$ are called the invariant factors *(or simply* invariants*) of G.*

Remark A.1.1 (Isomorphism Criterion)**.** *Two finite abelian groups are isomorphic if and only if they have the same sequence of invariant factors.*

The function `GL2ModuleInvariants(V)` computes the abelian group invariants of a $\mathbb{Z}/n\mathbb{Z}$-submodule of $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. The function assumes that `V` is generated by at most two elements.

```
def GL2ModuleInvariants(V):
    # Define n earlier to avoid repeating len(V.base_ring())
    n = len(V.base_ring())
    # Check if the module has no generators
    if len(V.gens()) == 0:
        return []

    # Check if the module has one generator. Use set() to avoid duplicates
    in the list.
    if len(V.gens()) == 1:
        # Calculate #V
        V_elements = [tuple(a * V.gens()[0]) for a in range(n)]
```

```
        return [len(set(V_elements))]

    # Assert there are at most 2 generators
    assert len(V.gens()) <= 2

    # The list of elements generated by the first generator
    firstgen_list = set([tuple(a * V.gens()[0]) for a in range(n)])

    # The list of elements generated by the second generator
    secondgen_list = set([tuple(a * V.gens()[1]) for a in range(n)])

    # Compute r1 and r2 upfront
    r1 = len(firstgen_list)
    r2 = len(secondgen_list)

    # Function to check if two vectors are dependent
    def are_dependent(v, list):
        return v in list

    # Check if the generators are dependent (checking both conditions)
    if are_dependent(tuple(V.gens()[1]), firstgen_list) or
    are_dependent(tuple(V.gens()[0]),
    secondgen_list):
    # If dependent, return max(r1, r2)
        rmax = max(r1, r2)
        return [rmax]

    # If not dependent (linearly independent), return gcd and lcm
    return [gcd(r1, r2), lcm(r1, r2)]
```

The function `find_largest_order_element(generator_list)` iterates through the list of generators of a submodule, computes the order of each element, and returns the element from the list that corresponds to the largest computed order.

```
def find_largest_order_element(generator_list):
    largest_order = 0
    largest_order_element = generator_list[0]  # Initialize first element

    for element in generator_list:
        order = element.order()

        if order > largest_order:
            largest_order = order
            largest_order_element = element
```

```
    return largest_order_element
```

The function `SubmoduleRank(V)` reduces the generator list of a submodule `V` of $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ to at most two generators, prioritizing combinations involving the generator of highest order.

```
def SubmoduleRank(V):
    R = V[0][0].base_ring()
    M = R^2
    V_sub = M.submodule(V)
    generators = V_sub.gens()
    n = len(R)

    if len(generators) == 0:
        return M.submodule([])  # Submodule gen. by (0,0)

    if len(generators) == 1:
        return M.submodule([generators[0]])  # Submodule with one generator

    #m is the index of one of the generators with the highest order
    m = generators.index(find_largest_order_element(generators))

    #V_elements is the set with all the elements in V
    V_elements = set(V)

    # Iterate through pairs of generators
    for i in range(len(generators)):
        if set([tuple(a*generators[m]+(b*generators[i])) for a in range(n)
        for b in range(n)])
        == V_elements:
            return M.submodule([generators[m], generators[i]])
```

The function `GL2FixModule(H)` takes a finite subgroup of $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ as input and computes the abelian group invariants of the submodule of $(\mathbb{Z}/n\mathbb{Z})^2$ fixed pointwise by the left matrix multiplication action of every element in `H`.

- It initializes a list `V` containing all elements of $(\mathbb{Z}/n\mathbb{Z})^2$.
- It iterates through the generators `h` of `H`. In each iteration, it filters the list `V`, keeping only those elements `v` such that $h \cdot v = v$. After checking all generators, `V` contains the set of elements fixed by all of `H`.
- It then calls `SubmoduleRank(V)` on this list of fixed elements to obtain a representation of the fixed submodule, aiming for at most two generators.

- Finally, it passes this resulting submodule object to `GL2ModuleInvariants` to calculate and return the list of invariants (typically `[]`, `[a]`, or `[a, b]` where $a \mid b \mid n$).

```
from sage.modules.free_module_element import vector
from sage.matrix.constructor import Matrix

def GL2FixModule(H):
    # Determine the ring Z/nZ
    R = H.base_ring()
    M = R^2

    # Find the submodule fixed by the left action of H.
    # Start with all of (Z/nZ)^2. In Magma this is Eigenspace(Identity(H),1);

    V = [(x, y) for x in R for y in R] # (Z/nZ)^2 represented as a list of tuples

    # In Magma take of transpose h_sage (Magma default is right action!)
    for h in H.gens(): #Iterate over the generators, as that is sufficient.
       new_V = []
       for v in V:
            v = vector(R, list(v))
            h_sage = Matrix(R,h) #Convert h to a standard Sage matrix
            if (h_sage * v == v):
              new_V.append(tuple(v))
       V = [value for value in V if value in new_V]

    """
    SubmoduleRank(V) limits the generating set to two elements. However,
    the two generating elements may not be linearly independent so inside
    the GL2ModuleInvariants(V) function, we have an extra filter to deal with that.
    """

    V_twogen = SubmoduleRank(V)

    return GL2ModuleInvariants(V_twogen)
```

The function `GL2IsSubModule(A, B)` takes two lists of integers, `A` $= [a_1, a_2]$ and `B` $= [b_1, b_2]$, representing the abelian group invariants of two $\mathbb{Z}/n\mathbb{Z}$-modules, M_A and M_B, respectively. It returns `True` if M_A is isomorphic to a submodule of M_B, and `False` otherwise.

```
    def GL2IsSubModule(A, B):
    i = len(B) - len(A)
    if i < 0:
        return False
```

```
    # loop with python 0-based indexing
    for j in range(len(A)):
        if B[i + j] % A[j] != 0: # python indexing starts at 0.  Magma starts at 1.
            return False

    return True
```

The function `GL2ContainsCC(H)` checks if a given subgroup H of $\mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$ contains an element h with trace $\mathrm{tr}(h) = 0$ and determinant $\det(h) = -1$ such that the cyclic subgroup $C = \langle h \rangle$ fixes a submodule of $(\mathbb{Z}/n\mathbb{Z})^2$ isomorphic to $\mathbb{Z}/n\mathbb{Z}$. This latter condition implies that h fixes at least one element of order n in $(\mathbb{Z}/n\mathbb{Z})^2$.

The implementation iterates through elements $h \in H$, testing $\det(h) = -1$ and $\mathrm{tr}(h) = 0$. If these hold, it then verifies the fixed submodule condition using `GL2IsSubModule([n], GL2FixModule(`$\langle h \rangle$`))`. The function returns `True` if such an h is found, and `False` otherwise. (Note: This method of checking the determinant, trace, and the fixed submodule of the cyclic group is stated to be faster than explicitly checking if H contains an element conjugate to $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$).

```
    def GL2ContainsCC(H):
    R = H.base_ring()
    found = False
    for h in H:
        h_sage = Matrix(R, h)
        if h_sage.det() == -1 and h_sage.trace() == 0:

            #Check this element to see if its' GL2SubModule stuff works.
            invariants_base_ring = [R.cardinality()] # size of R = Z/nZ
            cyclic_group = H.subgroup([h])
            invariants_fixed_module = GL2FixModule(cyclic_group)
            if GL2IsSubModule(invariants_base_ring, invariants_fixed_module):
                found = True
                break  # Exit the loop early once a suitable element is found

    return found
```

The final algorithm presented in this section incorporates the following result from [38], which allows us to add an effective computational filter.

Theorem A.1.1. *Let $E/\mathbb{Q}$ be an elliptic curve. If there is an integer $n \geq 2$ such that $\mathbb{Q}(E[n]) = \mathbb{Q}(\zeta_n)$, then $n = 2, 3, 4,$ or 5. More generally, if $\mathbb{Q}(E[n])/\mathbb{Q}$ is abelian, then $n = 2, 3, 4, 5, 6,$ or 8. Moreover, $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is isomorphic to one of the following groups:*

n	2	3	4	5	6	8
$\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$	$\{0\}$ $\mathbb{Z}/2\mathbb{Z}$ $\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$	$\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$ $(\mathbb{Z}/2\mathbb{Z})^3$ $(\mathbb{Z}/2\mathbb{Z})^4$	$\mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ $(\mathbb{Z}/4\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^2$ $(\mathbb{Z}/2\mathbb{Z})^3$	$(\mathbb{Z}/2\mathbb{Z})^4$ $(\mathbb{Z}/2\mathbb{Z})^5$ $(\mathbb{Z}/2\mathbb{Z})^6$

Furthermore, each possible Galois group occurs for infinitely many distinct j-invariants.

Corollary A.1.1. *For any $n \geq 9$, and any elliptic curve $E/\mathbb{Q}$, the image of $\rho_{E,n}$ is non-abelian.*

This result allows us to add the condition that any subgroup must be non-abelian as a filter in our code. This significantly restricts the pool of candidate subgroups, making the computation more efficient, although it should be noted that the algorithm's runtime still grows substantially with n.

The function `GL2Subgroups_with_surjectivedet_CC(n)` computes a list of representatives for conjugacy classes of subgroups of $G = \mathrm{GL}(2, \mathbb{Z}/n\mathbb{Z})$. The returned subgroups satisfy the following conditions:

1. **Surjective Determinant:** The map $\det : H \to (\mathbb{Z}/n\mathbb{Z})^\times$ is surjective. This is checked by verifying that the set $\{\det(h) \mid h \in H\}$ is equal to the set of units modulo n.

2. **Contains Complex Conjugation Element:** The subgroup H must contain an element satisfying the criteria checked by the helper function `GL2ContainsCC(H)`.

3. **Non-Abelian Pre-filter (Conditional):** If $n \geq 9$, the function *first* filters the initial list of all conjugacy class representatives, keeping only the non-abelian ones before applying checks (1) and (2). If $n < 9$, all representatives are considered.

The function iterates through the appropriate set of subgroup representatives, applies these checks, and returns a list containing those subgroups that satisfy all applicable conditions.

```
def GL2Subgroups_with_surjectivedet_CC(n):
    # Define GL(2, Z/nZ)
    GLN = GL(2, IntegerModRing(n))

    # Get the set of numbers coprime to n
    coprime_set = set(x for x in range(1, n) if gcd(x, n) == 1)

    # Generate all possible subgroups (this may be slow for large n)
    subgroups = GLN.conjugacy_classes_subgroups()

    if n >= 9:
        subgroups = [H for H in subgroups if not H.is_abelian()]

    # List to store subgroups with surjective determinant maps and CC
    surjectiveCC_subgroups = []
```

```
    for H in subgroups:
    # Compute the set of determinants for this subgroup
        determinants = {mat.matrix().det() for mat in H}

        # If the set of determinants is equal to the set of numbers coprime to n
        if determinants == coprime_set:
            if GL2ContainsCC(H) == True:
                surjectiveCC_subgroups.append(H)

    return surjectiveCC_subgroups
```

A.2. CODE for Horizontal Entanglements

The function `coprime_divisor_pairs(n)` takes a positive integer `n` as input. It returns a list of all unique pairs (d_1, d_2) where d_1 and d_2 are positive divisors of `n` and are coprime to each other. Each pair is typically represented as a tuple.

```
def coprime_divisor_pairs(n):
    divs = divisors(n) # Get divisors and sort them

    coprime_pairs = []
        for i in range(1, len(divs)): # Start range at first index to avoid 1
            for j in range(i, len(divs)): # Iterate from i onwards avoid duplicates
                if gcd(divs[i], divs[j]) == 1:
                    coprime_pairs.append((divs[i], divs[j]))

    return coprime_pairs
```

The function `reduce_subgroup_mod_c(subgroup, n, c)` reduces a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ modulo c, where c is a divisor of n.

```
def reduce_subgroup_mod_c(subgroup, n, c):
    if n % c != 0:
        raise ValueError("c must be a divisor of n.")

    Zn = IntegerModRing(n)
    Zc = IntegerModRing(c)
    GLc = GL(2, Zc) #Define general linear group GL(2, Z/cZ)

    def reduce_mod_c(matrix_in_Zn):
    """Reduces a 2x2 matrix over Z/nZ to a 2x2 matrix over Z/cZ."""
        matrix_Zn = matrix(Zn, matrix_in_Zn.list())
        return GLc(matrix(Zc, [[matrix_Zn[i, j] % c for j in range(2)]
        for i in range(2)]))
```

```
    reduced_subgroup = [reduce_mod_c(g) for g in subgroup]
    return reduced_subgroup
```

The function `GL_mod_homomorphism(N, M)` computes the kernel of the natural reduction homomorphism $\phi : GL_2(\mathbb{Z}/N\mathbb{Z}) \to GL_2(\mathbb{Z}/M\mathbb{Z})$. The function returns a representation of this kernel as a list of matrices.

```
def GL_mod_homomorphism(N, M):
    if N % M != 0:
        raise ValueError("M must divide N for the reduction to be well-defined.")

    # Define the general linear groups
    GLN = GL(2, IntegerModRing(N))
    GLM = GL(2, IntegerModRing(M))

    # Define the identity matrix in GL(2, Z/MZ)
    I_M = GLM(matrix(IntegerModRing(M), [[1, 0], [0, 1]]))

    # Define the homomorphism that reduces entries modulo M
    def modM_homomorphism(MN):
        MN_sage = matrix(IntegerModRing(N), MN.list())
        return GLM(matrix(IntegerModRing(M), [[MN_sage[i, j] % M for j in
        range(2)] for i in range(2)]))

    # Compute the kernel: elements mapping to the identity matrix mod M
    kernel = [MN for MN in GLN if modM_homomorphism(MN) == I_M]

    return kernel
```

We now present the SageMath implementation for computing all (a, b)-horizontal entanglements of an elliptic curve such that $\gcd(a, b) = 1$. This implementation utilizes the functions previously defined in this section and employs generators of the mod-m_E Galois image, ρ_{E,m_E}, sourced from the LMFDB database. The methodology will be illustrated by presenting the specific code used to compute all horizontal entanglements for the elliptic curve with LMFDB label `300.b2`.

Example A.2.1.

```
n = 30
G = GL(2, Integers(n))
gens = [G([[21,16],[25,21]]), G([[1,0],[6,1]]), G([[25,6],[24,7]]),
G([[5,6],[18,29]]),
G([[2,5],[1,3]]), G([[1,6],[0,1]])]
H = G.subgroup(gens)
coprime_pairs = coprime_divisor_pairs(n)
for pair in coprime_pairs:
```

```
a = pair[0]
b = pair[1]
c = lcm(a,b)
GLc = GL(2, Integers(c))
Gc = reduce_subgroup_mod_c(H, n, c)
ker_a = GL_mod_homomorphism(c, a)
ker_b = GL_mod_homomorphism(c, b)
Na = [x for x in ker_a if x in Gc]
Nb = [x for x in ker_b if x in Gc]
GroupGc = GLc.subgroup(Gc)
Nab = GLc.subgroup(Na+Nb)
if len(Nab) < len(GroupGc):
  print(f"({a},{b})-entanglement with size {len(GroupGc)/len(Nab)}")
```

In the preceding example, the elliptic curve has an adelic level of 30, which determined our choice of $n = 30$. The specific generators for $\rho_{E,m_E}(G_{\mathbb{Q}})$ used were obtained from the LMFDB data for that curve. To apply this code for computing horizontal entanglements of an arbitrary elliptic curve, two modifications are necessary:

1. The variable `n` must be set to the adelic level of the desired elliptic curve.
2. The set of generators must be replaced with those corresponding to $\rho_{E,m_E}(G_{\mathbb{Q}})$ for the target elliptic curve, typically also sourced from a database like LMFDB.

A significant limitation, however, is the computational cost: as `n` (the adelic level) becomes very large, the execution time for these computations can increase substantially, potentially becoming prohibitively long.

For non-coprime pairs (a, b), the implementation requires a modification from the coprime case presented above. The following example checks for $(14, 21)$-entanglement for the elliptic curve with LMFDB label `2541.f1`.

Example A.2.2.

```
a = 14
b = 21
c = lcm(a,b)
d = gcd(a,b)
G = GL(2, Integers(c))
gens = [G([[1,0],[6,1]]), G([[4,3],[9,7]]), G([[38,9],[1,22]]),
G([[3,4],[8,11]]), G([[37,6],[36,7]]), G([[39,40],[32,35]]), G([[1,6],[0,1]]),
Gc = G.subgroup(gens)
ker_a = GL_mod_homomorphism(c, a)
ker_b = GL_mod_homomorphism(c, b)
ker_d = GL_mod_homomorphism(c, d)
Na = [x for x in ker_a if x in Gc]
Nb = [x for x in ker_b if x in Gc]
```

```
Nd = [x for x in ker_d if x in Gc]
Nab = G.subgroup(Na+Nb)
if len(Nab) < len(Nd):
  print(f"({a},{b})-entanglement with size {len(Nd)/len(Nab)}")
```

In the preceding example, the specific generators for $\rho_{E,42}(G_{\mathbb{Q}})$ used were obtained from the LMFDB data for that curve.