NNT/NL : 0000AIXM0000/000ED000

THÈSE DE DOCTORAT

Soutenue à Aix-Marseille Université
le 13 décembre 2024 par

Zoé YVON

Galois representations of elliptic curves and Entanglement of division fields

Discipline

Mathématiques

École doctorale

ED 184 – MATHEMATIQUES ET INFORMATIQUE

Laboratoire/Partenaires de recherche

Institut de Mathématiques de Marseille (I2M)

Composition du jury

Sara ARIAS-DE-REYNA Université de Séville, Rang B	Rapporteuse
Samir SIKSEK Université de Warwick, Rang A	Rapporteur
Cécile ARMANA Université de Franche-Comté, Rang B	Examinatrice
Olivier DUDAS Aix-Marseille Université, Rang A	Examinateur
Jean-Marc COUVEIGNES Université de Bordeaux, Rang A	Président du jury
David KOHEL Aix-Marseille Université, Rang A	Directeur de thèse
Samuele ANNI Aix-Marseille Université, Rang B	Co-directeur de thèse

Affidavit

I, undersigned, Zoé Yvon, hereby declare that the work presented in this manuscript is my own work, carried out under the scientific direction of Samuele Anni and David Kohel, in accordance with the principles of honesty, integrity and responsibility inherent to the research mission. The research work and the writing of this manuscript have been carried out in compliance with both the French national charter for Research Integrity and the Aix-Marseille University charter on the fight against plagiarism.

This work has not been submitted previously either in this country or in another country in the same or in a similar version to any other examination body.

Place Marseille, date October 17th, 2024

Liste de publications

1. Polynomials realizing images of Galois representations of an elliptic curve, *Functiones et Approximatio Commentarii Mathematici*, 69(1), 2023.
2. Coincidences of division fields of an elliptic curve defined over a number field, *preprint*, 2024, `https://arxiv.org/abs/2407.14370`.

Participation aux conférences

- Arizona Winter School, Online, January 2021. Courses: A friendly introduction to the theory of modular forms and An introduction to modular groups.
- Seminari de Teoria de Nombres de Barcelona, Universitat de Barcelona (Barcelone, Espagne), Janvier 2022. Exposé : Valuation of coefficients of polynomials geometrically realizing $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.
- Seminari de Teoria de Nombres de Barcelona, Universitat de Barcelona (Barcelone, Espagne), Janvier 2023. Exposé : Coincidence of division fields of an elliptic curve defined over a number field.
- Conference SAGA (Symposium of Algebraic Geometry and Applications), CIRM (Marseille, France), Février 2023.
- Conference COUNT (Computations and their uses in number theory), CIRM (Marseille, France), Février 2023.
- Workshop Density problems in Arithmetic, CIRM (Marseille, France), April 2023. Exposé : Coincidence of division fields of an elliptic curve defined over a number field.
- Conference Arithmetic Statistics, CIRM (Marseille, France), Mai 2023.
- Workshop An expedition into Arithmetic geometry, Lorentz Center (Leiden, The Netherlands), Mai 2023.
- Conference AGC^{2}T (Arithmetic Geometry Cryptography and Code Theory), CIRM (Marseille, France), Juin 2023.

- Conférence FoCM (Fundations of Computational Mathematics), Workshop Computational Number Theory, Sorbonne Université (Paris, France), Juin 2023.

- Journée de l'équipe AGRL (Arithmétique, Géométrie, Logique et Représentations), I2M (Marseille, France), Décembre 2023. Exposé : Galois representations of elliptic curves.

- European Congress of Mathematics, Workshop Inverse Galois theory and arithmetic, Séville, Espagne, Juillet 2024. Exposé: Coincidence of division fields of an elliptic curve defined over a number field.

- Seminari de Teoria de Nombres de Barcelona, Universitat de Barcelona (Barcelone, Espagne), Février 2024. Exposé : Vertical coincidence of an elliptic curve defined over a number field.

- Séminaire hebdomadaire des doctorants de l'I2M et du CPT, I2M (Marseille, France). Exposés : The inverse Galois problem / Torsion point on elliptic curves (x2) / Ramification in number fields (x2) / Modular curves.

- Séminaire hebdomadaire de l'équipe ATI (Arithmétique de Théorie de l'Information), I2M (Marseille, France). Exposé : Valuation of coefficients of polynomials geometrically realizing $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

Résumé

Soit E/F une courbe elliptique sur un corps de nombres. Le groupe absolu de Galois de F agit sur les points de m-torsion de la courbe, donnant une représentation galoisienne $\rho_{E,m}$ du groupe absolu de Galois dans $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Le groupe de Galois de l'extension $F(E[m])/F$, engendrée par les coordonnées des points d'ordre m de la courbe, est isomorphe à l'image de $\rho_{E,m}$. Un résultat de Serre de 1972 et d'autres plus récents montrent que cette représentation est surjective pour presque toutes les courbes elliptiques définies sur F. Dans cette thèse, on travaille sur l'enchevêtrement des corps de division, autrement dit sur la non-surjectivité des représentations $\rho_{E,m}$, lorsque m n'est pas premier.

D'une part, on questionne la possibilité d'avoir la coïncidence de deux corps de division $F(E[m]) = F(E[n])$ pour des entiers m, n distincts. Cette question a déjà été traitée pour F étant le corps des rationnels. Dans cette thèse, on donne des résultats sur les corps de nombres.

D'autre part, dans le cadre du problème inverse de Galois, on souhaite une méthode pour construire des polynômes avec corps de décomposition $F(E[m])$. Cette question a déjà été traitée pour $m = p$ un premier et $\rho_{E,p}$ surjective. Dans cette thèse, on généralise le résultat à tous les entiers m et à toutes les images de $\rho_{E,m}$ possibles. De plus, on donne un minorant pour les valuations des coefficients des polynômes obtenus.

Mots-clés: Géométrie arithmétique, Problème inverse de Galois, Théorie des représentations, Courbes elliptiques, Enchevêtrement de représentations, Théorie algorithmique des nombres.

Abstract

Let E/F be an elliptic curve over a number field. The absolute Galois group of F acts on the m-torsion points of the curve, giving rise to a Galois representation $\rho_{E,m}$ from the absolute Galois group into $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. The Galois group of the extension $F(E[m])/F$, generated by the coordinates of the points of order m of the curve, is isomorphic to the image of $\rho_{E,m}$. A result by Serre from 1972, along with more recent results, show that this representation is surjective for almost all elliptic curves defined over F. In this thesis, we focus on the entanglement of division fields, i.e. the non-surjectivity of the representations $\rho_{E,m}$, when m is not prime.

On the one hand, we examine the possibility of having the coincidence of two division fields $F(E[m]) = F(E[n])$ for distinct integers m, n. This question has already been studied for F being the field of rationals. In this thesis, we provide results over number fields.

On the other hand, within the framework of the inverse Galois problem, we seek a method to construct polynomials whose splitting fields is $F(E[m])$. This question has already been addressed for $m = p$ a prime and $\rho_{E,p}$ surjective. In this thesis, we generalize the result to all integers m and to all possible images of $\rho_{E,m}$. Moreover, we give a lower bound for the valuations of the coefficients of the polynomials obtained.

Keywords: Arithmetic Geometry, Inverse Galois problem, Representation theory, Elliptic curves, Entanglement of representations, Algorithmic number theory.

Acknowledgments

Contents

Introduction

In this thesis we approach the study of images of Galois representations of elliptic curves from two different contexts. The first involves the entanglement of Galois representations, and ask whether two division fields of an elliptic curves do coincide. The second concerns the inverse Galois problem, and more specifically, the construction of explicit polynomials realizing the images of Galois representations.

Galois theory and the inverse Galois problem: motivation

Galois theory is the study of algebraic numbers, which are roots of polynomials with coefficients in $\mathbb{Q}$. It arose from the question of finding formulas for roots of polynomials. Let $f \in \mathbb{Q}[X]$ be a monic and irreducible polynomial, with roots α_i in $\overline{\mathbb{Q}}$. To the polynomial f we associate a unique field $\mathbb{Q}(f)$ which consists of all the numbers which are arithmetic combinations of the α_i's over $\mathbb{Q}$. The field $\mathbb{Q}(f)$ is called *the splitting field of f*. Such an extension of $\mathbb{Q}$ is said to be Galois. Let us remark that the associate polynomial is not unique: there are infinitely many irreducible and monic polynomial $g \in \mathbb{Q}[X]$ such that $\mathbb{Q}(f) = \mathbb{Q}(g)$.

For a finite extension $L/\mathbb{Q}$, *i.e.* a field generated by finitely many algebraic numbers, we consider the $\mathbb{Q}$-automorphism group of L, that is

$$\mathrm{Aut}(L/\mathbb{Q}) := \{\sigma : L \to L \mid \sigma \text{ is a isomorphism and } \sigma|_{\mathbb{Q}} = \mathrm{id}\}.$$

When $L/\mathbb{Q}$ is Galois, this group is called the *Galois group of L* and is denoted by $\mathrm{Gal}(L/\mathbb{Q})$. Therefore, to a polynomial, we associate a group: its Galois group.

All the structure of the reasoning and the results above are valid replacing the ground field $\mathbb{Q}$ by any number field, *i.e.* any finite extension of $\mathbb{Q}$, and even any field, namely F. We obtain the following diagram:

$$\begin{tikzcd}
\{\text{polynomials with coefficients in F}\} \arrow[rr, two heads] \arrow[dr] & & \{\text{finite Galois extensions of F}\} \arrow[dl] \\
& \{\text{finite groups}\} &
\end{tikzcd}$$

The *finite inverse Galois problem* consists of determining the image of the arrows to {finite groups}, and in particular whether they are surjective. If the ground field is $F = \mathbb{Q}$, it is conjectured that the answer is yes. For other ground fields, almost nothing is known.

We obtain extensions of the ground field F by adding algebraic numbers over F. Above, we considered finite extensions. We can also build extensions generated by infinitely many algebraic numbers. In general, Galois extensions of F are algebraic extensions L/F such that, for all $\alpha \in L$ such that α is the root of an irreducible polynomial f_α with coefficients in F, all the roots of f_α are in L. In this case, the Galois group of L/F is infinite, and has a structure of profinite group: it is a topological group which is the inverse limit of finite discrete groups, see Section 1.4. In particular, a finite group is profinite. Thus, we have an arrow:

$$\{\text{Galois extensions of F}\} \longrightarrow \{\text{profinite groups}\}$$

The *general inverse Galois problem* consists of determining the image of this map. We highlight that if the inverse limit of finite groups G_i, $i \in I$, where I is a countable set, is in the image then all the G_i's are in the image. In this thesis, we study Galois representations $\rho : G_F \to G$ where G is a subgroup of the group $\mathrm{GL}_2(\hat{\mathbb{Z}})$ of invertible matrices with coefficients in the profinite limit $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}$. Let L/F be the fixed field of the kernel of ρ, then the image of ρ is isomorphic to the Galois group of L/F.

Galois representations of elliptic curves

An elliptic curve is a non-singular projective curve of genus 1 with a fixed base point. This base point determines a group law, making the elliptic curve into an abelian variety of dimension 1. For any integer m, the group $E[m]$ of m-torsion points of an elliptic curve E defined over a number field F is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$. Moreover, the absolute Galois group $G_F = \mathrm{Gal}(\overline{F}/F)$ acts on the points of order m, giving rise to a mod m Galois representation

$$\rho_{E,m} : G_F \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

whose kernel is fixed by the division field $F(E[m])$, and furthermore, for any prime p, to a p-adic and an adelic Galois representation

$$\rho_{E,p^\infty} : G_F \to \mathrm{GL}_2(\mathbb{Z}_p) \quad \text{and} \quad \rho_E : G_F \to \mathrm{GL}_2(\hat{\mathbb{Z}}).$$

We denote by $F(E[p^\infty])$ the fixed field of the kernel of ρ_{E,p^∞}.

In 1972, Serre proved that, for non-CM elliptic curves - which is the generic case - the index of the image of the adelic Galois representation in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is finite, and called the *adelic index.* Equivalently, for every non-CM elliptic curve, the p-adic Galois representation is non surjective only for finitely many primes p, called the *exceptional primes.* There is a rich litterature on the topic. In particular, various authors investigated the question of finding upper bounds for exceptional primes. Algorithms by Zywina and Sutherland compute exceptional primes and their corresponding mod p and p-adic Galois images. Jones, for $F = \mathbb{Q}$, and Zywina, for $F \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$ and $F \neq \mathbb{Q}$, show that almost all elliptic curves have surjective p-adic Galois representations for all primes p.

Beyond local constraints, the failure of the adelic representation ρ_E to be surjective is due to the non-surjectivity of the injective morphism

$$\rho_E(G_F) \to \prod_{p \text{ prime}} \rho_{E,p^\infty}(G_F),$$

which corresponds to the non-linear disjointness over F of the family of division fields $(F(E[p^\infty]))$. In this case, we say that the family $(F(E[p^\infty]))$ is *entangled.* Serre first raised the problem of entanglement, in 1972, observing that, for an elliptic curve over $\mathbb{Q}$, the division field $\mathbb{Q}(E[2])$ has a non-trivial intersection with a cyclotomic field. This forces the adelic index to be even for every elliptic curve, even though the p-adic Galois representations can be surjective for all p. In this latter case, the field $\mathbb{Q}(E[2^\infty])$ is entangled with an other division field. It was not until 2010 that this issue was addressed again, by Jones, Greicius and Zywina, and later, from 2016 onwards, also by Brau, Daniels, Lozano-Robledo, Morrow, Campagna, Pengo, Stevenhagen et al. The terminology of *vertical entanglement* for the non-surjectivity of $\rho_{E,p^\infty}(G_F)$ for some p, and of *horizontal entanglement* for the non-surjectivity in the product, has been first introduced by Daniels, Lozano-Robledo and Morrow in 2021.

The case where the ground field F is a general number field is very different from the case $F = \mathbb{Q}$. Indeed, on the one hand, the Kronecker-Weber theorem is only valid over $\mathbb{Q}$. On the other hand, the possible non-trivial intersection $F \cap \mathbb{Q}^{\text{cyc}}$ gives rise to the non surjectivity of the composition of ρ_E with the determinant map $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \hat{\mathbb{Z}}^*$. As a consequence, we distinguish the properties of $\rho_E(G_F)$ resulting from the intersection $F \cap \mathbb{Q}^{\text{cyc}}$.

Contributions to entanglement

Let E/F be an elliptic curve. An extreme case of both vertical and horizontal entanglement is the equality of two division fields $F(E[m]) = F(E[n])$, in which case we say that E/F has an (m,n)-coincidence. Previous results have been proved for elliptic curves defined over the rationals, by Rouse and Zureick-Brown, Jones and Brau, and Daniel and Lozano-Robledo.

In this thesis, we study the question of coincidence for elliptic curves over an arbitrary number field. As for entanglement, we distinguish (p^k, p^{k+1})-coincidences where p is a prime, called *vertical coincidences*, and (m, mp^k)-coincidences where $p \nmid m$, called *horizontal coincidences*.

We prove that if E/F has an (m,n)-coincidence and p is a prime not dividing m and n with the same exponent, then p is either even, or ramified in $F/\mathbb{Q}$, or a prime of bad reduction for E, see Theorem 4.42.

In addition to refining the set of possible prime divisors of m and n, we give constraints on the possible exponents on the prime divisors in case of horizontal coincidence, using the obstructions given by the inclusion $F(\zeta_m) \subseteq F(E[m])$. Combining previous results on the relation between the ramification of $F(E[m])/F$ and the type of reduction of the elliptic curve, we obtain Table 4.21 giving necessary conditions for $F(E[m])$ to contain the p^k-th cyclotomic field $F(\zeta_{p^k})$, where p is a prime, and so to have an (m, mp^k)-coincidence.

Concerning vertical coincidences, we use that the group $\rho_{E,p^k}(G_F)$ is the image of $\rho_{E,p^{k+1}}(G_F)$ in $\mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$. We show that the sequence (i_{k+1}/i_k), where i_k denotes the index of $\rho_{E,p^k}(G_F)$ in $\mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$, is non-increasing from $k \geq 1$ if p is odd and $k \geq 2$ if $p = 2$, then constant. In particular, if a (p^k, p^{k+1})-coincidence occurs, then it occurs from the beginning. Moreover, in this case, the adelic index is divisible by p^{4k} if p is odd and $\max\left\{2^4, 2^{4(k-1)}\right\}$ if $p = 2$.

Furthermore, if m divides n, then an (m,n)-coincidence implies that the reduction map $\rho_{E,n}(G_F) \to \rho_{E,m}(G_F)$ is an isomorphism. This motivates the study of coincidences in chains

$$F(E[m]) = F(E[pm]) = \cdots = F(E[p^k m]),$$

and the associated problem of splittings of the surjections $\rho_{E,pm}(G_F) \to \rho_{E,m}(G_F)$ introduced in Subsection 4.5.4. In the case of (p^k, p^{k+1})-coincidences, with $k \geq 2$ for $p = 2, 3$, then the mod p^k image does not contain a conjugates of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, see Theorem 4.66.

If $F = \mathbb{Q}$, a (p^k, p^{k+1})-coincidence is possible only for $p = 2$, see [DLR23]. We prove that, more generally, this is true if $F \cap \mathbb{Q}(\zeta_{p^k}) = \mathbb{Q}$, this is Corollary 4.39. If E has CM by a quadratic field K and $F \subseteq K(j(E))$, then Proposition 4.69 gives a more precise statement: a (p^k, p^{k+1})-coincidence is not possible for p odd and $k \geq 2$.

In addition, if the mod m image is large, *i.e.* contains $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$, we give further constraints for a coincidence in Section 4.6, resulting from the study of the abelianization of the image of $\rho_{E,m}$.

Up to this point, we have only examined necessary conditions for having a coincidence. We conclude the presentation of the results on coincidences with the statement of sufficient conditions. Over $\mathbb{Q}$, the only possible vertical coincidence is a $(2, 4)$-coincidence. It is even expected that the known $(2, 4)$, $(2, 3)$, $(2, 6)$ and $(3, 6)$-coincidences are the only possible coincidences over $\mathbb{Q}$. For any elliptic curve E/F, we can construct an (m, mp^k)-coincidence with a base change from F to $F(E[mp^k])$, but such a base change provides a trivial construction. We prove the existence of a $(4, 8)$-coincidence with a base change from $\mathbb{Q}$ to an extension linearly disjoint from $\mathbb{Q}(E[4])$, see Theorem 4.27. Together with this theorem, in Subsection 4.5.1 we define the notion of a *minimal base change* and give necessary and sufficient condition to construct an (m, mp^k)-coincidence by a minimal base change of the ground field.

Contributions to the inverse Galois problem

As we previously described, the inverse Galois problem of a group G over a field F consists of determining whether G is isomorphic to the Galois group of an extension of F. In the context of elliptic curves, images of mod m Galois representations are realizable as the Galois group over F of the mod m division field. As we saw, finite Galois groups correspond to splitting fields of polynomials. The explicit inverse Galois problem for G over F consists of determining a (family of) polynomial(s) in $F[X]$ whose splitting field has Galois group G. In the case of surjective image of mod p Galois representations for elliptic curves, with p a prime, Reverter and Vila provide a solution for this problem, considering a short Weierstrass equation for E, and using the function $x + y \in F(E)$. In this thesis, we generalize their result for any equation for E, any image of $\rho_{E,m}$, with m an integer not necessarily prime, and we consider a broader choice of functions in $F(E)$ than $x + y$. Since m is not necessarily prime, in Subsection 5.1.1 we define the m-th primitive division polynomial $\widetilde{\psi}_m$, which is a factor of the m-th division polynomial corresponding to the points of exact order m.

Theorem. *(Theorems 5.11, 5.22 and 5.34) Let E/F be an elliptic curve with Weierstrass equation $w_E(x, y) = 0$. Let $m \geq 3$ and $u \in F(E)$ with degree 1 in x and y satisfying $F(u, [-1]^*u) = F(x, y)$.*

1. *The m-th primitive division polynomial $\widetilde{\psi}_m$ has Galois group isomorphic to the quotient $\rho_{E,m}(G_F)/\{\pm \mathrm{id}\}$. If the action of G_F on the points of order m is transitive, then $\widetilde{\psi}_m$ is irreducible.*

2. *The characteristic polynomial $\chi_{u,m}$ of multiplication by u in the ring $F[X, Y]/(w_E, \widetilde{\psi}_m)$ has Galois group isomorphic to $\rho_{E,m}(G_F)$. Moreover, $\chi_{u,m}$ is irreducible if and only if G_F acts transitively on the points of order m.*

The degree of $\chi_{u,m}$ is $2 \deg \widetilde{\psi}_m$ which is less than or equal to $m^2 - 1$. Hence this theorem gives a way to construct polynomials of high degree with known Galois groups, which are subgroups of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, for an arbitrary integer m.

We conclude with the determination of a lower bound for the valuations of the coefficients of the polynomials arising in our construction.

Structure of the manuscript

The general structure is as follows: we motivate the study of adelic Galois representations of elliptic curves by the inverse Galois problem, then describe their images, starting from local conditions and moving to entanglement. This motivates the study of the extreme case: coincidences. We then return to the inverse Galois problem with an explicit construction.

Chapter 1 is an introduction to the inverse Galois problem, and its relation to the study of Galois representations. We introduce the concepts of linearly disjoint extensions and of profinite groups.

In **Chapter 2**, we give some preliminaries on elliptic curves and their associated Galois representations, with a particular focus on the possible non-surjectivity of the cyclotomic character for a general ground field. Then we describe the current state of knowledge on images of p-adic Galois representations.

In **Chapter 3**, we describe the phenomena of horizontal entanglement, which leads to the presentation of results concerning the adelic index and the adelic level.

Chapter 4 is about coincidence of division fields. We describe the question, then give the known results over $\mathbb{Q}$, and then move our attention to number fields. We analyse horizontal coincidences, vertical coincidences, and the case of large images. This chapter essentially follows [Yvo24].

In **Chapter 5**, we discuss the explicit inverse Galois problem for the image of mod m Galois representations of elliptic curves over F. This chapter follows [Yvo23].

In **Chapter 6**, we briefly gives some ideas for future works: one consists of constructing entanglement using modular curve, and the second concerns coincidences of division fields of abelian varieties.

In **Appendix A**, we treat the derived group of general linear group $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ and the special linear group $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ with detailed proof, which are used in Chapter 4.

In **Appendix B**, we give background on the theory of modular curves, which is referred to occasionally in the manuscript, with examples specific to entanglement.

Notations

Through out this manuscript, we will use the following notation.

- For a finite set S, we denote by $\#S$ its cardinality.
- For a ring R, we denote by R^* its unit group.
- $\mathcal{P}$ denotes the set of prime numbers;
- We denote by $\varphi : \mathbb{Z} \to \mathbb{N}$ the Euler totient function;
- For m, n two integers, $\gcd(n, m)$ denotes their greatest common divisor, and $\operatorname{lcm}(n, m)$ denotes their lowest common multiple, and write $m \mid n$ when m divides n;
- For p a prime, $\mathbb{Z}_p = \varprojlim_k \mathbb{Z}/p^k\mathbb{Z}$ denotes the ring of p-adic integers and $\hat{\mathbb{Z}} = \varprojlim_m \mathbb{Z}/m\mathbb{Z}$ denotes the ring of profinite integers;
- For m a positive integer, we set $\mathrm{GL}_2(m) = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ and $\mathrm{SL}_2(m) = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$.

We fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and let F be a field.

- We fix $(\zeta_m)_{m\geq 1}$ a compatible system of roots of unity in $\overline{\mathbb{Q}}$, that is $\zeta_{km}^k = \zeta_m$ for k, m positive integers. We denote by $\boldsymbol{\mu}_m$ the group of m-th roots of unity for some fixed m and $\boldsymbol{\mu}_{p^\infty}$ the multiplicative group of p^k-th roots of unity for all k;
- For finite extensions of number fields $K \subseteq L \subseteq M$ such that M/L is Galois, and a prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$, we denote by $e_{\mathfrak{p}}(M/K)$ the ramification index of M/K at $\mathfrak{p}$;
- We denote by $\overline{F}$ an algebraic closure of F and by $G_F = \mathrm{Gal}(\overline{F}/F)$ its Galois group;
- For a prime p, $F(\boldsymbol{\mu}_{p^\infty})$ denotes the extension of F generated by elements of $\boldsymbol{\mu}_{p^\infty}$ and F^{cyc} is the extension of F generated by the roots of unity. We note that $\mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}^{\mathrm{ab}}$.
- For $f \in F[X]$, we denote by $F(f) \subseteq \overline{F}$ the splitting field of f in $\overline{F}$ and $\mathrm{Gal}(f)$ the Galois group of $F(f)/F$;
- For $(L_i)_{i\in I}$ a family of (algebraic) extensions of F, we denote by $\prod(L_i)$ the compositum of the L_i;
- For $\alpha \in F$, $\sqrt{\alpha}$ denotes a root of $X^2 - \alpha$.
- If F is a number field, $\mathcal{O}_F$ denotes its ring of integers of F and Δ_F its discriminant.

Given an elliptic curve E defined over F (abbreviated as E/F), a rational function $u \in F(E)$ and a subset $A \subseteq E(\overline{F})$, we use the following notations:

$$u(A) = \{u(P), P \in A\}, \quad F(u(A)) := F(\{u(P), P \in A\}) \quad \text{and} \quad F(A) = F(x(A), y(A))$$

Chapter 1

Galois theory and the inverse Galois problem

1.1 Definition and overview

Now, let us define properly what is the inverse Galois problem and give some basic result in this area.

Definition 1.1. We say that an algebraic extension L/F is *Galois* if it is normal and separable. In this case, we denote by $\mathrm{Gal}(L/F)$ its F-automorphism group.

Definition 1.2. Let G be a group and F be a field. We say that G is *realizable as a Galois group over F* if there exists a Galois extension L/F such that $\mathrm{Gal}(L/F) \simeq G$.

Problem 1.3. The *inverse Galois problem (IGP) for G over F* consists in determining whether G is realizable as a Galois group over F.

If G is finite, the extension L/F must be finite and then corresponds to the splitting field of a polynomial in $F[X]$.

Definition 1.4. We say that a polynomial $f \in F[X]$ *realizes* G if $G \simeq \mathrm{Gal}(f)$.

We define four variations on solving the IGP:

Problem 1.5. Let G be a group and F be a field. Here are a hierarchy of problems for solving the IGP for G over F:

1. *Classical IGP*: existence of a field extension of F with Galois group G,
2. *Effective IGP*: method of construction of such a field extension,
3. *Explicit/Parametric IGP*: method of construction of explicit polynomials matching this extension.

For each of the above IGP's, we also define an *IGP with ramification*: construction of such an extension with some prescribed ramification properties.

Example 1.6. Let d be a squarefree integer. We have $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$. In particular $\mathbb{Z}/2\mathbb{Z}$ is realizable over $\mathbb{Q}$, by the irreducible polynomial $X^2 - d$. The extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is ramified (with ramification index 2) at primes dividing d if $d \equiv 1 \pmod 4$ and $4d$ if $d \equiv 2, 3 \pmod 4$. We analyse further this example in Example 1.26.

Example 1.7. Let n be a positive integer. We have $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$. In particular $(\mathbb{Z}/n\mathbb{Z})^*$ is realizable over $\mathbb{Q}$, by the (reducible) polynomial $X^n - 1$. The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is ramified at primes p dividing n, with ramification index $\varphi(p^{v_p(n)})$. We examine further this example in Example 1.24.

Remark 1.8. Suppose that G is realizable over F by an extension M/F. Let H be a subgroup of G. The fundamental theorem of Galois theory says that there exists a intermediate extension $F \subseteq L \subseteq M$ such that $H \simeq \mathrm{Gal}(M/L)$. Moreover, if H is normal, we have $G/H \simeq \mathrm{Gal}(L/F)$. Then any quotient of a realizable group by a normal subgroup is realizable over the same base field F.

Theorem 1.9. *Every finite abelian groups is realizable over $\mathbb{Q}$, by a subextension of a cyclotomic extension.*

Proof. Let G be a finite abelian group. Then, by the fundamental structure theorem of abelian groups, there exists $a_1, \ldots, a_n$ such that $G \simeq \prod \mathbb{Z}/a_i\mathbb{Z}$. Dirichlet's theorem on arithmetic progression tells us that, for any $a \in \mathbb{Z}$, there exists infinitely many primes congruent to 1 modulo a. Then, let us take $p_1, \ldots, p_n$ distinct such that $a_i \mid p_i - 1$ for each i. It follows that $\mathbb{Z}/a_i\mathbb{Z}$ is a quotient of $(\mathbb{Z}/p_i\mathbb{Z})^*$, and so G a quotient of

$$\prod (\mathbb{Z}/p_i\mathbb{Z})^* \simeq (\mathbb{Z}/n\mathbb{Z})^* \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}),$$

where $n = \prod p_i$. Therefore, by Remark 1.8, the group G is realizable over $\mathbb{Q}$ by a subextension of $\mathbb{Q}(\zeta_n)$. □

Theorem 1.10 ([SD08, Section 4.4, Remark 2 on Example])**.** *For all n, the symmetric group S_n is realizable as a Galois group over $\mathbb{Q}$, by the irreducible polynomial $X^n - X - 1$.*

Remark 1.11. Cayley's Theorem [Jac12, Chapter I.10, Corollary of Theorem 1] specifies that every finite group of order n is a subgroup of the symmetric group S_n and so is isomorphic to $\mathrm{Gal}(\mathbb{Q}(X^n - X - 1)/L)$ for some intermediate extension $\mathbb{Q} \subseteq L \subseteq \mathbb{Q}(X^n - X - 1)$. In particular, every finite group is realizable as a Galois group over a number field.

There is a classic specialization of third point of Problem 1.5 called the *tame inverse Galois problem*.

Definition 1.12. Let L/F be an finite field extension, p be a prime and and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ above p. We say that L/F is

- *tamely ramified at* $\mathfrak{p}$ if $p \nmid e_{\mathfrak{p}}(L/F)$,
- *tamely ramified at* p if L/F is tamely ramified at every prime ideal above p,
- *tamely ramified* if L/F is tamely ramified at every prime.

The *tame IGP over F* ask whether a given group is realizable by a tamely ramified extension of F. This question has an affirmative answer over $\mathbb{Q}$ for solvable groups, together with the groups S_n and A_n for any n, see [KM04], [Pla03], [PV03].

Generically, a random irreducible polynomial of degree n has Galois group S_n. In other words, it has *maximal* Galois group.

Theorem 1.13 ([Coh79, Theorem 1])**.** *The proportion of irreducible polynomials of degree n which have Galois group S_n is* 1.

Nevertheless, the IGP is conjectured to have a solution for every finite group:

Conjecture 1.14 ([SD08, Conjecture 4.1.1])**.** *All finite groups are realizable as a Galois group over $\mathbb{Q}$.*

A generic method to deal with the IGP is through continuous representations. Let G be a group that we want to realize over F. It suffices to find a surjective continuous representation $\rho : G_F \to G$, which is a non-trivial problem. Then, the kernel of the representation ρ is $\mathrm{Gal}(\overline{F}/L)$ for some extension L/F which is Galois since the kernel of a homomorphism is a normal subgroup. The fundamental theorem of Galois theory says that $\mathrm{Gal}(L/F) \simeq G$. In Section 1.3, we explore this approach through representations on torsion subgroups of elliptic curves.

1.2 Linear disjoint extensions: realization of direct products

In order to realize direct products of realizable groups, we are interested in the concept of linear disjoint extensions. This concept is at the heart of the phenomena of *entanglement*, introduced in Section 3. Let I be a countable set. For a family $(L_i)_{i\in I}$ of subfields of $\overline{F}$, the compositum of the extensions L_i is denoted by $\prod(L_i) = \mathrm{im}(\otimes_F L_i \to \overline{F})$.

Definition 1.15. Let $(L_i)_{i\in I}$ be a family of extensions of F. We say that $(L_i)_{i\in I}$ is a family of *linear disjoint*, or *linearly independant*, extensions over F if one of the following equivalent conditions is satisfied:

1. The canonical surjective morphism of F-algebra $\bigotimes_F L_i \to \prod(L_i)$ is an isomorphism.
2. The F-algebra $\bigotimes_F L_i$ is a field.

The equivalence of these two statements is given in [Coh12, Section 11.6].

Proposition 1.16. *Two extensions L/F and M/F, with L/F finite, are linearly disjoint if and only if $[LM : M] = [L : F]$.*

Proof. See [Bou81, A.V.13, Proposition 5]. □

Corollary 1.17. *A family (L_i) of finite extensions is linearly disjoint over F if and only if for any finite subset $J \subseteq I$,*

$$\left[\prod_{i\in J}(L_i) : F\right] = \prod_{i\in J}[L_i : F].$$

In particular, this condition is automatically satisfied if the degrees $[L_i : F]$ are coprime.

Proof. Let L/F and M/F be linearly disjoint extensions. Then we have

$$[LM : F] = [LM : L][L : F] = [M : F][L : F],$$

the second equality coming from Proposition 1.16. The result follows by induction. □

When an extension is Galois, we have a simpler characterization of linear disjointness:

Proposition 1.18. *If L/F is Galois, then L/F and M/F are lineary disjoint over F if and only if $L \cap M = F$.*

Proof. See [Coh12, Theorem 11.6.5]. □

The proposition below is sometimes considered as a definition for linearly disjoint Galois extension (see for example [CP22a]):

Proposition 1.19. *If the extensions L_i/F are Galois, then the family (L_i) is linearly disjoint over F if and only if the following restriction morphism is an isomorphism:*

$$\mathrm{Gal}\left(\prod(L_i)/F\right) \to \prod \mathrm{Gal}(L_i/F).$$

Proof. It follows from Proposition 1.18 and [Bou81, A.V.66, Corollary 6]. □

Proposition 1.20. *Set $A = (L_i)_{i\in I}$ and suppose that the L_i are Galois. There exists a subset $S_A \subseteq I$ such that a subset $S \subseteq I$ satisfies*

$$\mathrm{Gal}\left(\prod_{i\in I} L_i/F\right) \simeq \mathrm{Gal}\left(\prod_{i\in S}(L_i)/F\right) \times \prod_{i\notin S} \mathrm{Gal}(L_i/F)$$

if and only if $S_A \subseteq S$. Moreover, for all $j \in S_A$,

$$L_j \cap \prod_{\substack{i\in S_A\\ i\neq j}} (L_i) \neq F.$$

Proof. We set $S_A = I$ and $M = \prod_{i\in S_A} (L_i)$. While there exists j such that $L_j \cap \prod_{\substack{i\in S_A\\ i\neq j}} (L_i) = F$ *i.e.*

$$\mathrm{Gal}(M/F) \simeq \mathrm{Gal}(L_j/F) \times \mathrm{Gal}\left(\prod_{\substack{i\in S_A\\ i\neq j}} (L_i)/F\right)$$

then remove j from S_A. When the loop stops, then we have the desired set S_A. □

Remark 1.21. Let $(L_i)_{i\in I}$ be a family of linear disjoint extensions of F and K/F be a subfield of $\prod_{i\in I} L_i$. Suppose that $K = \prod_{i\in I}(K_i)$ with $K_i \subseteq L_i$ for all $i \in I$. For all $i \in I$, we have $K_i \subseteq K \cap L_i$ and, since $\prod_{i\in I}(K_i) = \bigotimes_{i\in I} K_i$,

$$\bigotimes_{i\in I} K_i \subseteq \bigotimes_{i\in I}(K \cap L_i) \subseteq K = \bigotimes_{i\in I} K_i.$$

Hence $K_i = K \cap L_i$.

Remark 1.22. If L/F and M/F are finite Galois extensions, then the restriction morphism

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

is an isomorphism. We deduce that

$$[LM : F] = \frac{[L : F][M : F]}{[L \cap M : F]}.$$

This agree with Corollary 1.17 and Proposition 1.18.

From Proposition 1.19, if we find a realization of groups G_i by respectively the extensions L_i/F such that the L_i are linearly disjoint over F, then we obtain a realization of the direct product of the G_i's as the Galois group of $\prod(L_i)/F$.

Example 1.23. Let $f(x) = x^3+x^2-77x-289$. The extension $\mathbb{Q}(f)/\mathbb{Q}$ has Galois group S_3. Let Δ_f be the discriminant of the polynomial f. We know that $\sqrt{\Delta_f} \in \mathbb{Q}(f)$. Here, we have

$$\mathbb{Q}(\Delta_f) = \mathbb{Q}(\sqrt{-11}) \subseteq \mathbb{Q}(\zeta_{11})$$

by [Neu99, Chapter I, Proof of Proposition 10.5]. Then $\mathbb{Q}(\sqrt{-11}) \subseteq \mathbb{Q}(f) \cap \mathbb{Q}(\zeta_{11})$. It follows that $\mathbb{Q}(f)$ and $\mathbb{Q}(\zeta_{11})$ are not linearly disjoint over $\mathbb{Q}$. We say that there is *Serre entanglement*, see Section 3. However, the extensions $\mathbb{Q}(f)$ and $\mathbb{Q}(\zeta_{11})$ are linearly disjoint over $F = \mathbb{Q}(\sqrt{-11})$. Indeed, the degree of $\mathbb{Q}(f)$ over F is $6/2 = 3$ and the degree of $\mathbb{Q}(\zeta_{11})$ over F is $(11-1)/2 = 5$. Then we use Corollary 1.17. The extension $\mathbb{Q}(f)(\zeta_{11})/F$ has Galois group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ by Proposition 1.19. We have obtained a realization of $\mathbb{Z}/15\mathbb{Z}$ over F taking the compositum of a cubic and a quintic extension.

Example 1.24. We continue Example 1.7. We saw that $\mathbb{Q}(\zeta_{p^k})/\mathbb{Q}$ with p prime is Galois and is only ramified at p. Since the only unramified extension of $\mathbb{Q}$ is $\mathbb{Q}$ itself, then the family $(\mathbb{Q}(\zeta_{p^{k_p}}))_{p\in\mathcal{P}}$ is linearly disjoint over $\mathbb{Q}$ for any family $(k_p)_{p\in\mathcal{P}}$. More generally, the family $(\mathbb{Q}(\boldsymbol{\mu}_{p^\infty}))_{p\in\mathcal{P}}$ is linearly disjoint over $\mathbb{Q}$.

The conjecture that every finite group is realizable as a Galois group over $\mathbb{Q}$ has a stronger version:

Conjecture 1.25 ([SD08, Conjecture 4.1.1])**.** *For any finite group G, there are infinitely many linearly disjoint Galois extensions over $\mathbb{Q}$ with Galois group G.*

Example 1.26. We continue Example 1.6. For two squarefree integers $d \neq d'$, we have $\mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}(\sqrt{d'})$. Since two quadratic extension are either equal or with trivial intersection, then two different quadratic extension are linearly disjoint by Proposition 1.18. However, the family of quadratic extensions is not linearly disjoint: we have $\sqrt{2}\cdot\sqrt{-1} = \sqrt{-2}$ and so

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{-2},\sqrt{-1})/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{-1})/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q}).$$

Thus the family $(\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-1}))$ is not linearly disjoint over $\mathbb{Q}$. Nevertheless, the extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is ramified at every prime dividing d, and so the extensions $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ with d squarefree and positive are all differently ramified, and so are linearly dijsoint over $\mathbb{Q}$. This proves the above conjecture for $G = \mathbb{Z}/2\mathbb{Z}$.

1.3 Representations coming from elliptic curves

In the context of elliptic curves, we focus on subgroups of $\mathrm{GL}_2(m)$. Let us take a number field F, an elliptic curve E/F and a positive integer m. The group $E[m]$ of m-torsion points of $E(\overline{F})$ is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ and the absolute Galois group G_F acts on $E[m]$. Then, we obtain a Galois representation

$$\rho_{E,m} : G_F \to \mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(m).$$

It follows that the image of $\rho_{E,m}$ is realizable as a Galois group over F. This is the Galois group of the fixed field of $\ker(\rho_{E,m})$: the extension of F obtained by adjoining the coordinates of the m-torsion points and denoted by $F(E[m])$. We also define, for a prime p, the group $E[p^\infty]$ to be the group of p^k-torsion of for all k and E_{tors} to be the group of all the torsion points of E.

Serre's open image theorem tells that, if E/F does not have CM, then $\rho_{E,m}(G_F)$ is surjective for all m coprime to the adelic level M_E of ρ_E, see Section 2.4. Hence, $\mathrm{GL}_2(m)$ is realizable as a Galois group for all m coprime to M_E. Going further, we obtain the following:

Theorem 1.27. *The group* $\mathrm{GL}_2(m)$ *is realizable as a Galois group over* $\mathbb{Q}$ *for any odd positive integer* m*.*

Proof. The elliptic curve $E/\mathbb{Q}$ with LMFDB label 37.a1 has adelic level $2\cdot 37$ and surjective mod 37 Galois representation. Thus, $E/\mathbb{Q}$ satisfies $\rho_{E,m}(G_{\mathbb{Q}}) = \mathrm{GL}_2(m)$ for all m not divisible by $2\cdot 37$. In particular, it is surjective for all odd m. □

Proposition 1.28. *The group* $\mathrm{GL}_2(2^k)$ *is realizable as a Galois group over* $\mathbb{Q}$ *for all* $k \geq 1$*.*

Proof. The elliptic curve $E/\mathbb{Q}$ with LMFDB label 11.a1 has surjective 2-adic Galois representation *i.e.* surjective 2^k Galois representation for any $k \geq 1$. □

For $\mathrm{GL}_2(m)$ with m even (but not a power of 2), the difficulty comes from the *Serre entanglement*, described in Section 3.

In Chapter 2 and 3, we give more information about the image of $\rho_{E,m}$.

Remark 1.29. We cannot realize all subgroups of $\mathrm{GL}_2(m)$ over $\mathbb{Q}$ in this way. Indeed, if E is defined over a number field F, we have $\det(\mathrm{Im}(\rho_{E,m})) \simeq \mathrm{Gal}(F(\zeta_m)/F)$ by Proposition 2.13. In particular, the subgroups of $\mathrm{GL}_2(m)$ with non-surjective determinant cannot be realized as $\rho_{E,m}(G_{\mathbb{Q}})$ for any elliptic curve $E/\mathbb{Q}$.

In Section 1.1, we recalled that polynomials of degree n generically have Galois group S_n, in other words maximal Galois group. The same was expected for Galois representation of elliptic curves, which was finally proved in 2010: the mod m representation of a random elliptic curve is generically maximal. Maximal image means that it contains $\mathrm{SL}_2(m)$, since the image of the cyclotomic representation in $\mathrm{GL}_2(m)/\mathrm{SL}_2(m)$ only depends on F, as we will see in Section 2.3.

Theorem 1.30 (Theorem 3.41, 3.23 and 3.19)**.** *Let* m *be an integer. Then almost all elliptic curves* E/F *with* $F \neq \mathbb{Q}$ *satisfy* $\mathrm{SL}_2(m) \leq \mathrm{Gal}(F(E[m])/F)$*. If* m *is odd, then almost all elliptic curves* $E/\mathbb{Q}$ *satisfy* $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) = \mathrm{GL}_2(m)$*.*

Proof. For elliptic curves over F with $F \neq \mathbb{Q}$, we use Theorem 3.20. Now, by Theorem 3.41, a Serre curve $E/\mathbb{Q}$ satisfies $\rho_{E,m}(G_F) \simeq \mathrm{GL}_2(m)$ for all m not divisible by $M_{\Delta_{\mathrm{sf}}(E)}$, which is even. In particular, the isomorphism occurs for every odd m. But, by Theorem 3.23 almost all elliptic curves are Serre curves. □

We also have information about the ramification of $F(E[m])/F$. Arias-de-Reyna and Vila provided an affirmative answer to the tame IGP for $\mathrm{GL}_2(p)$ over $\mathbb{Q}$, see [AdRV09, Theorem 1.2]. More generally, for elliptic curves defined over a number field F, Table 4.21 gives upper bounds on the ramification index of $F(E[m])/F$ at primes not dividing m, depending on the reduction of the curve (see Definition 2.8). In particular:

Theorem 1.31. *Suppose that* E/F *is semistable, with good or split multiplicative reduction at* 2 *if* m *is odd. Then* $F(E[m])/F$ *is tamely ramified outside of set of the prime divisors of* m*.*

We say that an elliptic curve defined over a finite field of caracteristic p is *supersingular* if it does not have non-trivial p-torsion point. Serre proved that:

Theorem 1.32 ([Ser72, Proposition 12])**.** *Let* p *be a prime. If* E/F *has good supersingular reduction at* p*, then* $F(E[p])/F$ *is tamely ramified at* p*.*

However, the field $F(E[m])$ contains $\mathbb{Q}(\zeta_{p^{v_p(m)}})$, which has ramification index at p over $\mathbb{Q}$ equal to $p^{v_p(m)-1}(p-1)$. Then, if $v_p(m) \geq 2$ and $F/\mathbb{Q}$ has ramification index at p with valuation smaller than $v_p(m)-1$, then $F(E[m])/F$ will be wildly ramified at p, from Table 4.22.

Finally, about explicit IGP, the construction of explicit polynomial with Galois group $\rho_{E,m}(G_F)$ is the topic of Chapter 5.

Other groups can be realize with methods of arithmetic geometry, for example:

Theorem 1.33. *For all positive integers m, the normalizer of the Cartan subgroup $N_{\delta,\phi}(m)$ (defined in Section 2.4.2) is realizable as a Galois group over $\mathbb{Q}$.*

Proof. We apply [LR22, Theorem 1.2.(1)] to $K = \mathbb{Q}(\sqrt{-3})$ and $f = 1$. With the notation of [LR22] and from [Sil94, Appendix A.3], we have $\mathbb{Q}(j_{K,f}) = \mathbb{Q}$. □

We call such realisations *geometric*, because it uses a geometric object: an elliptic curve. More generally, we talk about *geometric* realization when we use abelian varieties to realize groups as Galois groups. Let A be an abelian variety of dimension g, defined over F. The group G_F acts on the m-torsion points of A, giving rise to a Galois representation $G_F \to \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$ where $\mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$ denoted the general symplectic group over $\mathbb{Z}/m\mathbb{Z}$. We denote by $F(A[m])$ the extension of F generated by the coordinates of m-torsion points of A. For example, we can take for A the jacobian of a curve of genus g.

Theorem 1.34 ([AD20])**.** *Let p be a prime. Suppose that there exists $q_1, q_2, q_3, q_4, q_5 \in \mathcal{P}$ such that $\{q_1, q_2\} \neq \{q_4, q_5\}$, $q_1, q_2, q_4, q_5 < q_3 < 2g+2$ and $2g+2 = q_1+q_2 = q_4+q_5$. Then, there exists explicit hyperelliptic curves of genus g such that their jacobian J satisfies*

$$\mathrm{Gal}(\mathbb{Q}(J[p])/\mathbb{Q}) \simeq \mathrm{GSp}_{2g}(\mathbb{Z}/p\mathbb{Z}).$$

This method makes it possible to tabulate extensions of number fields with fixed Galois group and specified ramification. As already pointed out for the elliptic curves, which are abelian varieties of dimension 1, the ramification of $F(A[m])/F$ is controlled by m and the conductor of A, see [ST68, Theorem 1, and Corollary 2 of Theorem 2].

1.4 The profinite perspective of the inverse Galois problem

The absolute Galois group G_F is a profinite group. Hence every realizable group is profinite.

Example 1.35. The additive group $\mathbb{Z}$ is not realizable as a Galois group.

We recall the definition of a profinite group. Let $\mathcal{C}$ be the category of groups or rings.

Definition 1.36. An *inverse system on $\mathcal{C}$* is the set of the following data:

1. A partially ordered set $(I, \leq)$ such that for all $i, j \in I$ there exists $k \in I$ such that $i \leq k$ and $j \leq k$,
2. For each $i \in I$, an object G_i of $\mathcal{C}$,
3. For each pair $(i, j) \in I^2$ with $i \leq j$, a morphism $\phi_{ij} : G_j \to G_i$ of $\mathcal{C}$ such that
   (a) $\phi_{ii} = \mathrm{id}_{G_i}$,
   (b) For each triple $(i, j, k) \in I^3$ with $i \leq j \leq k$, the equality $\phi_{ik} = \phi_{ij} \circ \phi_{jk}$ holds.

The inverse limit is the unique object $G = \varprojlim_i G_i$ of $\mathcal{C}$ such that

1. G is equipped with morphism $\phi_i : G \to G_i$ such that for all $i \leq j$ we have $\phi_i = \phi_{ij} \circ \phi_j$,

2. G is universal for the property.

When the morphisms ϕ_{ij} are understood, we simply denote by $(G_i)_{i \in I}$ the inverse system.

Remark 1.37. The inverse limit of an inverse system $((G_i), (\phi_{ij}))$ is isomorphic to

$$G = \{(g_i)_{i \in I} \mid \forall i \in I \quad g_i \in G_i \text{ et } \forall i \leq j \quad \phi_{ij}(g_j) = g_i\} \subseteq \prod G_i \in \mathcal{C}.$$

Moreover, if $(R_i)_{i \in I}$ is an inverse system of rings, then $R^* = R \cap \prod R_i^* = \varprojlim R_i^*$.

Definition 1.38. A *profinite group* is a topological group which is the inverse limit of an inverse system of finite groups equipped with the discrete topology.

Remark 1.39. Let (G_i) be an inverse system of finite groups equipped with discrete topology. The topology on $\varprojlim G_i$ is the minimal topology such that the associated morphism ϕ_i are continuous. It is induced by the product topology on $\prod G_i$.

Remark 1.40. Every open subgroups of a profinite group is also closed, see [Ser13, Proposition 2.(iii)]. The open subgroups of a profinite group are exactly the subgroups with finite index, see [NSN07, Theorem 1.1].

Example 1.41. For a prime p, the ring $\mathbb{Z}_p$ of p-adic integers is a profinite group defined as the inverse limit of the inverse system of rings $(\mathbb{Z}/p^k\mathbb{Z})_{k \geq 1}$ where the morphism $\mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^r\mathbb{Z}$ with $r \leq k$ are the morphism of reduction mod p^r. The induced product topology is the same as the topology given by the p-adic valuation. The group $\hat{\mathbb{Z}}$ is profinite by definition: it is the inverse limit of the inverse system $(\mathbb{Z}/m\mathbb{Z})_{m \geq 2}$. From the Chinese remainder theorem we have $\hat{\mathbb{Z}} \simeq \prod_{p \in \mathcal{P}} \mathbb{Z}_p$.

Let M/F be an infinite Galois extensions. Then $\mathrm{Gal}(M/F)$ has a structure of profinite group. The system $(\mathrm{Gal}(L/F))_{L \subseteq M, L/F \text{ Galois}}$ is an inverse system: the set $\{L \subseteq M, L/F \text{ Galois}\}$ is partially order by inclusion and for $L \subseteq M$ the morphism $\mathrm{Gal}(M/F) \to \mathrm{Gal}(L/F)$ is the restriction morphism. Then

$$\mathrm{Gal}(M/F) = \varprojlim_{\substack{L \subseteq M \\ L/F \text{ Galois}}} \mathrm{Gal}(L/F).$$

We equip $\mathrm{Gal}(L/F)$ with the Krull topology, see [DS05, Section 9.3]. In particular, the absolute Galois group G_F is a profinite group obtained as the projective limit of all finite Galois extensions of F.

Proposition 1.42. *Let $(G_i)_{i \in I}$ be an inverse system of finite groups such that all the morphisms $G_j \to G_i$ are surjective. Let $G = \varprojlim G_i$. The two following conditions are equivalent:*

1. *G is realizable as the Galois group of L/F.*

2. *For all $i \in I$, G_i are realizable as the Galois group of L_i/F such that $L_i \subseteq L_j$ for all $i \leq j$.*

In this case, $L = \prod(L_i)$.

Proof. (1) $\implies$ (2): If $\mathrm{Gal}(L/F) \simeq G$, then there are surjective morphism

$$\phi_i : \mathrm{Gal}(L/F) \to G_i$$

such that for all $i \leq j$, $\phi_i = \phi_{ij} \circ \phi_j$. In particular, $\ker\phi_j \subseteq \ker\phi_i$ for all $i \leq j$. For $i \in I$, let L_i be the fixed field of $\ker\phi_i$. Then $G_i \simeq \mathrm{Gal}(L_i/F)$ and $L_i \subseteq L_j$. It follows that $\prod(L_i) \subseteq L$. Since G is universal, then we have $L = \prod(L_i)$. (2) $\implies$ (1): For the other direction, if $G_i \simeq \mathrm{Gal}(L_i/F)$ such that $L_i \subseteq L_j$ for all $i \leq j$, then $(\mathrm{Gal}(L_i/F))_{i\in I}$ form a projective system with the restriction morphisms $\mathrm{Gal}(L_j/F) \to \mathrm{Gal}(L_i/F)$ and its inverse limit is $\mathrm{Gal}(\prod(L_i)/F)$. □

Knowing the structure of G_F provides a solving of the IGP over F for any group.

Cyclotomic character

An automorphism $\sigma \in G_F$ acts on ζ_m as $\sigma(\zeta_m) = \zeta_m^{a(\sigma)}$ for some $a(\sigma)$ unique modulo m. Thus, we obtain a Galois representation of dimension 1, called the *mod m cyclotomic character*:

$$\chi_m : G_F \to (\mathbb{Z}/m\mathbb{Z})^* \quad \sigma \mapsto a(\sigma).$$

This character does not depend on the choice of ζ_m. The kernel of this representation is $\mathrm{Gal}(\overline{F}/F(\zeta_m))$ and so $\chi_m(G_F) \simeq \mathrm{Gal}(F(\zeta_m)/F)$. The families $(\chi_{p^k}(G_F))_{k\geq 1}$ and $(\chi_m(G_F))_{m\geq 2}$ form inverse systems, whose inverse limit are respectively subgroups of $\mathbb{Z}_p^*$ and $\hat{\mathbb{Z}}^*$. They give rise to the p-adic cyclotomic character and the adelic cyclotomic character:

$$\chi_{p^\infty} : G_F \to \mathbb{Z}_p^* \quad \text{and} \quad \chi_{\mathrm{cyc}} : G_F \to \hat{\mathbb{Z}}^*.$$

By Proposition 1.42, we have

$$\chi_{p^\infty}(G_F) \simeq \mathrm{Gal}(F(\boldsymbol{\mu}_{p^\infty})/F) \quad \text{and} \quad \chi_{\mathrm{cyc}}(G_F) \simeq \mathrm{Gal}(F^{\mathrm{cyc}}/F).$$

For $F = \mathbb{Q}$, the representation χ_m is surjective for all m, and so are χ_{p^∞} and χ_{cyc}. It follows that, for $F \neq \mathbb{Q}$, the image of χ_{cyc} only depends on the intersection $F \cap \mathbb{Q}^{\mathrm{cyc}}$. If $F \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$, then χ_{cyc} and χ_{p^∞} are surjective, which gives a realization of $\mathbb{Z}_p^*$ and $\hat{\mathbb{Z}}$ over F. Since $\hat{\mathbb{Z}} = \prod \mathbb{Z}_p$ and $F^{\mathrm{cyc}} = \prod_{p\in\mathcal{P}} F(\boldsymbol{\mu}_{p^\infty})$, it follows from Section 1.2 that the family $(F(\boldsymbol{\mu}_{p^\infty}))_{p\in\mathcal{P}}$ is linearly disjoint over F. For $F = \mathbb{Q}$, this also follows from the ramification of cyclotomic fields, see Example 1.24. However, this is not the case for all number fields F, as the following example shows:

Example 1.43. Since $\varphi(7) = 6$ and $\varphi(13) = 12$, the field $\mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\zeta_{13})$ each have a subfied of degree 3 over $\mathbb{Q}$, say K_7 and K_{13}. Since $\mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\zeta_{13})$ are linearly disjoint over $\mathbb{Q}$, then so are K_7 and K_{13}. Set $K := K_7K_{13}$. Then $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ by Proposition 1.19, and so $K/\mathbb{Q}$ have a subextension F, linearly disjoint from K_7 and K_{13} such that $\mathrm{Gal}(F/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$. Therefore, we have

$$F \neq K = FK_7 = FK_{13} \subseteq F(\zeta_7) \cap F(\zeta_{13}),$$

which shows that the family $(F(\boldsymbol{\mu}_{p^\infty}))_{p\in\mathcal{P}}$ is not linearly disjoint over F.

Definition 1.44. Let a, b positive integers and $d = \gcd(a, b)$. We say that F has a *cyclotomic (a, b)-entanglement* if $F(\zeta_a) \cap F(\zeta_b) \neq F(\zeta_d)$.

If $F \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$, then F does not have any cyclotomic entanglement. On the other hand, the field F in Example 1.43 has a $(7, 13)$-entanglement.

The end of this section follows from Section 2.2. In the context of elliptic curves, the families $(E[p^k])_{k\geq 1}$ with p prime, and $(E[m])_{m\geq 1}$ form inverse systems, giving rise to profinite groups $T_p(E)$ and $T(E)$ called the p-adic Tate module and the Tate module. Then, the Galois representations $\rho_{E,m}$ give rise to (continuous) p-adic and global Galois representation

$$\rho_{E,p^\infty} : G_F \to \mathrm{GL}_2(\mathbb{Z}_p) \simeq \varprojlim_k \mathrm{GL}_2(p^k)$$

and

$$\rho_E : G_F \to \mathrm{GL}_2(\hat{\mathbb{Z}}) \simeq \varprojlim_m \mathrm{GL}_2(m).$$

We have:

$$\rho_{E,p^\infty}(G_F) = \varprojlim_k \rho_{E,p^k}(G_F) \quad \text{and} \quad \rho_E(G_F) = \varprojlim_m \rho_{E,m}(G_F).$$

The study of the representations $\rho_{E,m}$ for each m is equivalent to the study of ρ_E.

Theorem 1.45. *Suppose that $F \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$ and $F \neq \mathbb{Q}$. The profinite group $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is realizable over F as the Galois group of $F(E_{\mathrm{tors}})/F$ for some elliptic curve E/F.*

Proof. See [Zyw10, Theorem 1.2]. □

In fact, the *loc.cit.* theorem says that this is the case for almost all elliptic curves E/F and this is what we use for Theorem 1.30. From the previous theorem and the fundamental theorem of Galois theory, we obtain:

Corollary 1.46. *Every open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ occurs as $\rho_E(G_F)$ for some number field F and some elliptic curve E/F.*

Theorem 1.47. *Suppose that $F \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$. The profinite group $\prod_{p\neq 2} \mathrm{GL}_2(\mathbb{Z}_p)$ is realizable over F, as the Galois group of $\prod_{p\neq 2}(F(E[p^\infty]))/F$, for some elliptic curve E/F. Moreover, $\mathrm{GL}_2(\mathbb{Z}_2)$ is realizable over F, as the Galois group of $F(E[2^\infty])/F$, for some elliptic curve E/F.*

Proof. For $F \neq \mathbb{Q}$, this is previous theorem, since $\mathrm{GL}_2(\hat{\mathbb{Z}}) \simeq \prod_{p\in\mathcal{P}} \mathrm{GL}_2(\mathbb{Z}_p)$. For $F = \mathbb{Q}$, we use the elliptic curve $E/\mathbb{Q}$, with LMFDB label 37.a1, of the proof of Theorem 1.27 for the realization of $\prod_{p\neq 2} \mathrm{GL}_2(\mathbb{Z}_p)$, and the elliptic curve $E/\mathbb{Q}$, with LMFDB label 11.a1, of the proof of Proposition 1.28 for $\mathrm{GL}_2(\mathbb{Z}_2)$. □

Chapter 2

Elliptic curves and Galois representations

Elliptic curves are both geometric and arithmetic objects and are one of the main objects of study of this thesis. They are projective curves of genus 1, provided with a composition law making the points of the curve into an abelian group, in other words an elliptic curve is also an abelian variety of dimension 1. This gives rise to Galois representations. As shown in Section 1.3, the study of these Galois representations brings answers to certain instances of the inverse Galois problem. In this chapter, we present some preliminaries on elliptic curves and a state-of-the-art on the images of the p-adic Galois representations associated to their Tate modules. We will present the theory briefly, focusing mostly on what is relevant in the next chapters. For more details on the theory of elliptic curves, see [Sil09], specifically Chapter III and VII.

2.1 Elliptic curves and associated equations

An *elliptic curve E defined over a field F* is a smooth projective curve of genus 1 defined over F provided with a point $\mathrm{O} \in E(F)$, called the *point at infinity*. Every elliptic curve E/F admits an equation of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, a_2, a_3, a_4, a_6 \in F, \tag{2.1}$$

using the Riemann-Roch theorem. Such an equation is called a *Weierstrass equation for E*. On the projective plane the equation becomes

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \quad a_1, a_2, a_3, a_4, a_6 \in F$$

and $\mathrm{O} = [0 : 1 : 0]$ is the point at infinity. We also define the following quantities, which will be useful to define the discriminant, the j-invariant and latter the division polynomials:

$$\begin{aligned} b_2 &= a_1^2 + a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned}$$

The points of E are the points of the affine curve (2.1), together with the point at infinity. If F does not have characteristic 2 or 3 then, after a change of variables, the elliptic curves

E has an equation of the form

$$E : y^2 = x^3 + Ax + B, \quad A, B \in F,$$

called a *short Weiertrass equation for E.* In this case

$$b_2 = 0, \quad b_4 = 2A, \quad b_6 = 4B, \quad b_8 = A^2.$$

Remark 2.1. A change of variables defined over F between two short Weierstrass equations maps $y^2 = x^3 + Ax + B$ to

$$y^2 = x^3 + u^4Ax + u^6B$$

for some $u \in F^*$. Hence, every elliptic curve $E/\mathbb{Q}$ has a unique short Weierstrass equation $E : y^2 = x^3 + Ax + B$ such that $v_p(\gcd(|A|^3, |B|^2)) < 12$ for all prime p. We define the *naive height of E* as $\max(|A|^3, |B|^2)$.

Remark 2.2. Let $d \in F^* \backslash F^{*2}$ and let E/F be an elliptic curve with Weierstrass equation $y^2 = x^3 + Ax + B$. The elliptic curve $E^{(d)} : dy^2 = x^3 + Ax + B$ is isomorphic to E over $F(\sqrt{d})$, but not over F, and is called the *quadratic twist of E by d.*

Definition 2.3. For an elliptic curve E/F with Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, a_2, a_3, a_4, a_6 \in F,$$

we define the *discriminant $\Delta_E \in F$ of E* and the *j-invariant $j(E) \in F$ of E* as

$$\Delta_E = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \quad \text{and} \quad j(E) = \frac{(b_2^2 - 24b_4)^3}{\Delta_E}.$$

A Weierstrass equation define a non-singular curve if and only if Δ_E is non-zero. Thus, $j(E)$ is well-defined.

If E/F has a short Weiertrass equation $E : y^2 = x^3 + Ax + B$, then

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

Proposition 2.4 ([Sil09, Chapter 3, Proposition 1.4.(b)])**.** *The j-invariant of E does only depend on the isomorphism class of E over $\overline{F}$.*

Bézout theorem says that a projective curve of degree n cut every line in n points counted with multiplicities. In the case of elliptic curves, a line intersects the elliptic curve in exactly three points P, Q, R with multiplicity. Then, we equip the elliptic curve with a composition law $+$ which satisfies $P + Q + R = \mathrm{O}$.

Proposition 2.5 ([Sil09, Proposition III.2.2])**.** *For all $L \subseteq \overline{F}$, the pair $(E(L), +)$ forms an abelian group with identity* O*.*

There are explicit formulas to compute the addition of points, which are rational functions over F. They are given in [Sil09, Group law Algorithm III.2.3]. Let us remark that the structure of $E(L)$ does not depends on the choice of a Weierstrass equation for E.

Proposition 2.6 ([Sil09, Group law Algorithm III.2.3.(a)])**.** *Let E/F be an elliptic curve with Weierstrass equation $y^2 = f(x)$. Let $\alpha_1, \alpha_2, \alpha_3$ be the distinct roots of f. Then the points of order* 2 *of $E(\overline{F})$ have coordinates $(x, y) = (\alpha_i, 0)$, $i = 1, 2, 3$.*

Elliptic curves over number fields

From now on, let F be a number field. Let p be a prime, and $\mathfrak{p}$ be an ideal of $\mathcal{O}_F$ above p. For $a \in F$, we define $v_{\mathfrak{p}}(a)$ the $\mathfrak{p}$-adic valuation of a as the greatest integer k such that $a\mathcal{O}_F \subseteq \mathfrak{p}^k$. For an elliptic curve E/F, we can choose a Weiertrass equation with coefficients in $\mathcal{O}_F$, whose discriminant Δ_E has minimal $\mathfrak{p}$-adic valuation. Such an equation is called a *minimal equation for E at $\mathfrak{p}$* and its discriminant is called the *minimal discriminant of E at $\mathfrak{p}$*. An equation which is minimal at every prime is called a *global minimal Weierstrass equation.*

Proposition 2.7 ([Sil09, Chapter VIII, Corollary 8.3])**.** *If F has class number 1, then every elliptic curve E/F has a global minimal Weierstrass equation.*

Once we have a minimal equation for E at $\mathfrak{p}$, we can take the image of its coefficients in $\mathcal{O}_F/\mathfrak{p}$, say $\widetilde{a}_i$, and we obtain a curve over $\mathcal{O}_F/\mathfrak{p}$ with Weiertrass equation

$$E_{\mathfrak{p}} : y^2 + \widetilde{a}_1 xy + \widetilde{a}_3 y = x^3 + \widetilde{a}_2 x^2 + \widetilde{a}_4 x + \widetilde{a}_6.$$

Definition 2.8. Let E/F be an elliptic curve and $E_{\mathfrak{p}}$ be the reduction modulo $\mathfrak{p}$ of a minimal equation for E at $\mathfrak{p}$.

1. E has *good reduction at* $\mathfrak{p}$ if $E_{\mathfrak{p}}$ is non-singular,

2. E has *split* (respectively *non-split*) *multiplicative reduction at* $\mathfrak{p}$ if $E_{\mathfrak{p}}$ has a node with slopes of the tangent lines in $\mathcal{O}_F/\mathfrak{p}$ (respectively not in $\mathcal{O}_F/\mathfrak{p}$),

3. E has *additive reduction at* $\mathfrak{p}$ if $E_{\mathfrak{p}}$ has a cusp.

In the cases (2) and (3) we say that E has *bad reduction at* $\mathfrak{p}$. If at each prime $\mathfrak{p}$, E has good or multiplicative reduction, we say that E/F is *semistable.*

Definition 2.9. With same notations as in the previous definition, we define the quantity

$$a_p(E) = p + 1 - E_{\mathfrak{p}}(\mathbb{F}_p).$$

Definition 2.10. Let $\mathcal{P}$ be the set of prime ideals of $\mathcal{O}_F$. We define the conductor of E/F as $\mathfrak{f}_E = \prod\limits_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}^{f_{\mathfrak{p}}(E)}$ where

$$f_{\mathfrak{p}}(E) = \begin{cases} 0 & \text{if } E/F \text{ has good reduction at } \mathfrak{p} \\ 1 & \text{if } E/F \text{ has multiplicative reduction at } \mathfrak{p} \\ 2 & \text{if } E/F \text{ has additive reduction at } \mathfrak{p}. \end{cases}$$

If $F = \mathbb{Q}$, we also called *conductor of E* the integer f_E satisfying $\mathfrak{f}_E = f_E\mathbb{Z}$.

In this manuscript, when we talk about an elliptic curve E/F, we refer to the isomorphism class of the elliptic curve E up to a change of variables defined over F. Sometimes, we will talk about Δ_E without fixing a Weierstrass equation: it is when we are interested in $F(\sqrt{\Delta_E})/F$ for example, and this extension does not depends on the choice of the Weiertrass equation.

2.2 Galois representations of elliptic curves

Every definition and assumption in this section is up to a change of variables over F.

As said in the previous section, the points of $E(\overline{F})$ form a group. For $m \in \mathbb{Z}$, we define the endomorphism $[m] : E \to E$ which maps P on $[m]P = \underbrace{P + \cdots + P}_{m \text{ times}}$. For $m \neq n$, we have $[m] \neq [n]$. Therefore, after an identification between m and $[m]$, we have the ring inclusion $\mathbb{Z} \subseteq \operatorname{End}(E)$.

Definition 2.11. We say that E/F has *complex multiplication* (*CM*) if $\operatorname{End}(E) \neq \mathbb{Z}$.

There are only finitely many j-invariant defined over F corresponding to elliptic curves having complex multiplication, see [Sil09, Appendix C, Corollary 11.1.1] and [BFGR06].

We denote by $E[m]$ the group of m-torsion points of E, *i.e.*

$$E[m] := \ker\big([m] : E(\overline{F}) \to E(\overline{F})\big) = \{P \in E(\overline{F}) \mid [m]P = \mathrm{O}\}.$$

The group $E[m]$ is a $\mathbb{Z}/m\mathbb{Z}$-module. More precisely:

Proposition 2.12 ([Sil09, Chapter III, Corollary 6.4])**.** *Over any field of characteristic* 0*, we have the group isomorphism*

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

The *p-adic Tate module of E* is the $\mathbb{Z}_p$-module

$$T_p(E) := \varprojlim_{k} E[p^k],$$

the inverse limit being taken with respect to the natural maps $[p] : E[p^{n+1}] \longrightarrow E[p^n]$. We also define the *Tate module of E* as the $\hat{\mathbb{Z}}$-module

$$T(E) := \varprojlim_{m} E[m],$$

the inverse limit being taken with respect to the natural maps $[n] : E[mn] \longrightarrow E[m]$. For every integer m, let (P_m, Q_m) be a compatible basis of $E[m]$ over $\mathbb{Z}/m\mathbb{Z}$ such that, for $m, n \geq 2$,

$$(nP_{mn}, nQ_{mn}) = (P_m, Q_m).$$

Since $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, we deduce that $T_p(E) \simeq \mathbb{Z}_p^2$ and $T(E) \simeq \hat{\mathbb{Z}}^2$. It follows that

$$\operatorname{Aut}(E[m]) \simeq \mathrm{GL}_2(m), \quad \operatorname{Aut}(T_p(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_p), \quad \operatorname{Aut}(T(E)) \simeq \mathrm{GL}_2(\hat{\mathbb{Z}}).$$

Let E_{tors} be the group of torsion points of E and, for a prime p, $E[p^\infty]$ be the group of p^k-torsion points of E for $k \geq 1$, *i.e.*

$$E_{\text{tors}} = \bigcup_{m \geq 2} E[m] \simeq \varinjlim_{m \geq 2} E[m] \quad \text{and} \quad E[p^\infty] = \bigcup_{k \geq 1} E[p^k] \simeq \varinjlim_{k \geq 1} E[p^k].$$

One can check that

$$\operatorname{Aut}(\varinjlim E[m]) \simeq \operatorname{Aut}(\varprojlim E[m])$$

i.e.

$$\operatorname{Aut}(E_{\text{tors}}) \simeq \operatorname{Aut}(T(E)) \simeq \mathrm{GL}_2(\hat{\mathbb{Z}}).^{1}$$

[1] In [Mor19], E_{tors} is the notation used for $T(E)$ and in [BJ16], Brau and Jones talk about a $\hat{\mathbb{Z}}$-basis for E_{tors}.

We also have
$$\mathrm{Aut}(E[p^\infty]) \simeq \mathrm{Aut}(T_p(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_p).$$
Thus, we will consider indifferently ρ_{E,p^∞} with image in $\mathrm{Aut}(T_p(E))$ or $\mathrm{Aut}(E[p^\infty])$ and ρ_E with image in $\mathrm{Aut}(T(E))$ or $\mathrm{Aut}(E_{\mathrm{tors}})$.

Let $P \in E(\overline{F})$. For $\sigma \in G_F$, we define $\sigma(P)$ to be the point of $E(\overline{F})$ such that, if P has coordinates (x_P, y_P), then $\sigma(P)$ has coordinates $(\sigma(x_P), \sigma(y_P))$. The Galois group G_F acts on $E[m]$ as follows

$$G_F \times E[m] \to E[m] \quad (\sigma, P) \mapsto \sigma(P),$$

giving the representations

$$\rho_{E,m} : G_F \to \mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

called the *mod m Galois representation of E/F*,

$$\rho_{E,p^\infty} : G_F \to \mathrm{Aut}(T_p(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$$

called the *p-adic Galois representation of E/F* and

$$\rho_E : G_F \to \mathrm{Aut}(T(E)) \simeq \mathrm{GL}_2(\hat{\mathbb{Z}})$$

called the *adelic* (or *global*) *Galois representation of E/F*. By definition, the image of $\rho_E(G_F)$ in $\mathrm{GL}_2(m)$ is $\rho_{E,m}(G_F)$, the image of $\rho_E(G_F)$ in $\mathrm{GL}_2(\mathbb{Z}_p)$ is $\rho_{E,p^\infty}(G_F)$ and the image of $\rho_{E,p^\infty}(G_F)$ in $\mathrm{GL}_2(p^k)$ is $\rho_{E,p^k}(G_F)$. The following diagramm is commutative:

$$\begin{tikzcd}
\mathrm{GL}_2(\hat{\mathbb{Z}}) \arrow[r, two heads] \arrow[dr, two heads] & \mathrm{GL}_2(\mathbb{Z}_p) \arrow[d, two heads] \\
 & \mathrm{GL}_2(p^k)
\end{tikzcd}$$

The isomorphism $\mathrm{GL}_2(\hat{\mathbb{Z}}) \simeq \prod_{p \in \mathcal{P}} \mathrm{GL}_2(\mathbb{Z}_p)$ gives an injective morphism:

$$\rho_E(G_F) \to \prod_{p \in \mathcal{P}} \rho_{E,p^\infty}(G_F). \tag{2.2}$$

In particular, for integers a, b, m such that $m = \mathrm{lcm}(a, b)$, there are injective morphisms:

$$\rho_{E,m}(G_F) \to \prod_{p \in \mathcal{P}} \rho_{E,p^{v_p(m)}}(G_F) \quad \text{and} \quad \rho_{E,m}(G_F) \to \rho_{E,a}(G_F) \times \rho_{E,b}(G_F) \tag{2.3}$$

The kernel of the Galois representation $\rho_{E,m}$ is the set of $\sigma \in G_F$ such that σ acts trivially on the m-torsion points. In other words, $\sigma \in \ker \rho_{E,m}$ fixes the extension of F generated by the coordinates of the m-torsion points, denoted by $F(E[m])$, and called *the m-division field of E*. We note that this extension does not depends on the choice of a Weierstrass equation for E. Therefore $\ker\rho_{E,m} = \mathrm{Gal}(\overline{F}/F(E[m]))$ is a normal subgroup of G_F, the extension $F(E[m])/F$ is Galois and

$$\mathrm{Gal}(F(E[m])/F) \simeq \rho_{E,m}(G_F).$$

This provides a solution for the IGP over F for subgroups of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ which are images of such representations, see Chapter 1 for more information about the inverse Galois problem.

Similarly, the kernel of ρ_{E,p^∞} and ρ_E are respectively the subgroups $\mathrm{Gal}(\overline{F}/F(E[p^\infty]))$ and $\mathrm{Gal}(\overline{F}/F(E_{\mathrm{tors}}))$ and so

$$\mathrm{Gal}(F(E[p^\infty])/F) \simeq \rho_{E,p^\infty}(G_F)$$

and

$$\mathrm{Gal}(F(E_{\mathrm{tors}})/F) \simeq \rho_E(G_F).$$

In this manuscript, we consider the image of ρ_E (respectively ρ_{E,p^∞}, $\rho_{E,m}$) in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ (respectively $\mathrm{GL}_2(\mathbb{Z}_p)$, $\mathrm{GL}_2(m)$) without precising the choice of the basis. It is understood that the image is not necessarily equal but conjugate to the given group. This choice is motivated by the fact that this does not change the properties that interest us. In other words, we only consider the equivalence class of the Galois representations of E.

2.3 Weil pairing and maximal image

Let $\det : \mathrm{GL}_2(m) \to (\mathbb{Z}/m\mathbb{Z})^*$ be the determinant map. The Galois representation $\rho_{E,m} : G_F \to \mathrm{GL}_2(m)$ gives rise to a Galois representation of dimension 1:

$$\det \circ \rho_{E,m} : G_F \to (\mathbb{Z}/m\mathbb{Z})^*.$$

The determinant being stable under conjugation, the representation $\det \circ \rho_{E,m}$ does not depends on the choice of the $\mathbb{Z}/m\mathbb{Z}$-basis for $E[m]$.

Proposition 2.13. *We have $\chi_m = \det \circ \rho_{E,m}$. In particular, $F(\zeta_m)$ is contained in $F(E[m])$ and we have the isomorphisms*

$$\mathrm{Gal}(F(\zeta_m)/F) \simeq \det \circ \rho_{E,m}(G_F) \quad \textit{and} \quad \mathrm{Gal}(F(E[m])/F(\zeta_m)) \simeq \mathrm{SL}_2(m) \cap \rho_{E,m}(G_F).$$

This result is due to the existence and the properties of the Weil pairing (definition given in [Sil09, III.8])

$$e_m : E[m] \times E[m] \to \boldsymbol{\mu}_m.$$

where $\boldsymbol{\mu}_m$ is the group of m-th roots of unity.

Proposition 2.14 ([Sil09, III.Proposition 8.1])**.** *The Weil pairing is bilinear, alternating, non-degenerate, Galois invariant and compatible with the projective limit.*

Proof of Proposition 2.13. The Weil pairing being non-degenerate, we can choose $P, Q \in E[m]$ such that $e_m(P,Q) = \zeta_m$ (see [Sil09, III, Corollary 8.1.1]). The pair (P,Q) is a $\mathbb{Z}/m\mathbb{Z}$-basis of $E[m]$, otherwise P and Q would be on the same line and, since the Weil pairing is bilinear and alternating, we would have $e_m(P,Q) = 1$. Let $\sigma \in G_F$ such that $\rho_{E,m}(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in the basis (P,Q). Then

$$\begin{aligned} \sigma(\zeta_m) = \sigma(e_m(P,Q)) &= e_m(\sigma(P), \sigma(Q)) && \text{(Galois invariance)} \\ &= e_m(aP + cQ, bP + dQ) \\ &= e_m(P,Q)^{ad-bc} && \text{(bilinear and alternating)} \\ &= \zeta_m^{ad-bc} = \zeta_m^{\det \circ \rho_{E,m}(\sigma)} \end{aligned}$$

This shows that the action of G_F by $\det \circ \rho_{E,m}$ and χ_m is the same. Then the kernel of $\det \circ \rho_{E,m}$ is $\operatorname{Gal}(\overline{F}/F(\zeta_m))$ and contains the kernel of $\rho_{E,m}$ which is $\operatorname{Gal}(\overline{F}/F(E[m]))$. □

Corollary 2.15. *We have* $\chi_{\mathrm{cyc}} = \det \circ \rho_E$ *and* $\chi_{p^\infty} = \det \circ \rho_{E,p^\infty}$.

As a consequence of Proposition 2.13, if $F \cap \mathbb{Q}(\zeta_m) \neq \mathbb{Q}$, then $\rho_{E,m}$ cannot be surjective, since its composition with the determinant map is not. The possible images have determinant $\chi_m(G_F)$, and the largest possible image is the largest subgroup of $\mathrm{GL}_2(m)$ with determinant $\chi_m(G_F)$, which is equivalent to have $\rho_{E,m}(G_F)$ containing $\mathrm{SL}_2(m)$.

Definition 2.16. Let E/F be a non-CM elliptic curve. We say that the image of $\rho_{E,m}$, respectively ρ_{E,p^∞}, ρ_E, is *maximal* if it contains $\mathrm{SL}_2(m)$, respectively $\mathrm{SL}_2(\mathbb{Z}_p)$, $\mathrm{SL}_2(\hat{\mathbb{Z}})$.

As we will see in Section 2.4, the image of ρ_E has finite index in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ if E does not have CM and infinite index otherwise. Thus, we define differently *maximal image* in the CM case, see Section 2.4.2.

We denote by $\mathcal{G}_{F,m}$, respectively $\mathcal{G}_{F,p^\infty}$, $\mathcal{G}_F$, the largest subgroup of $\mathrm{GL}_2(m)$, respectively $\mathrm{GL}_2(\mathbb{Z}_p)$, $\mathrm{GL}_2(\hat{\mathbb{Z}})$ with determinant $\chi_m(G_F)$, respectively $\chi_{p^\infty}(G_F)$, $\chi_\infty(G_F)$. We have $\mathcal{G}_{\mathbb{Q},p^\infty} = \mathrm{GL}_2(\mathbb{Z}_p)$ and $\mathcal{G}_{\mathbb{Q}} = \mathrm{GL}_2(\hat{\mathbb{Z}})$.

To illustrate the three previous sections, we end it by an example:

Example 2.17. The elliptic curve with LMFDB label 11.a1 and minimal Weierstrass equation

$$E : y^2 + y = x^3 - x^2 - 7820x - 263580$$

has discriminant $\Delta_E = -11$ and j-invariant $j(E) = -2^{12} \cdot 11^{-1} \cdot 29^3 \cdot 809^3$. It has good reduction at every prime but 11, for which it has split multiplicative reduction. In particular, E/F is semistable. The conductor of E is $f_E = 11$. The p-adic Galois representations ρ_{E,p^∞} are surjective for all primes p but 5, and even surjective for all n coprime to 550. More precisely we have $\rho_E(G_{\mathbb{Q}}) = \pi^{-1}(\rho_{E,550}(G_{\mathbb{Q}}))$ where π is the natural projection $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(550)$. We obtain, for n coprime to 550,

$$\operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \simeq \mathrm{GL}_2(n)$$

and for primes $p \neq 5$:

$$\operatorname{Gal}(\mathbb{Q}(E[p^\infty])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{Z}_p).$$

For $p = 5$, the image of $\rho_{E,5}$ has index 24 in $\mathrm{GL}_2(5)$, and

$$\operatorname{Gal}(\mathbb{Q}(E[5])/\mathbb{Q}) \simeq \left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -2 & -1 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(5).$$

The image of $\rho_{E,25}$ has index 120 in $\mathrm{GL}_2(25)$ and

$$\operatorname{Gal}(\mathbb{Q}(E[25])/\mathbb{Q}) \simeq \left\langle \begin{pmatrix} -9 & 12 \\ 0 & 11 \end{pmatrix}, \begin{pmatrix} -2 & 9 \\ 0 & 11 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(25).$$

Moreover, $\rho_{E,5^\infty}(G_F)$ is the full inverse image of $\rho_{E,25}(G_F)$ in $\mathrm{GL}_2(\mathbb{Z}_5)$. In particular, it has index 120. For $n = 22$, the image of $\rho_{E,22}$ has index 2 in $\mathrm{GL}_2(22)$. For $n = 550$, the image of $\rho_{E,550}$ has index $1200 = 120 \cdot 2 \cdot 5$ in $\mathrm{GL}_2(550)$. As we will see later, that corresponds to $(2, 11)$ and $(11, 25)$-entanglement: $\mathbb{Q}(E[11]) \cap \mathbb{Q}(E[2])$ is a quadratic field and $\mathbb{Q}(E[25]) \cap \mathbb{Q}(E[11])$ is a $\mathbb{Z}/5\mathbb{Z}$-extension of $\mathbb{Q}$.

2.4 Image of the p-adic representations

In this section, we summarize the state-of-the-art concerning the images of the mod p and p-adic representations $\rho_{E,p}$ and ρ_{E,p^∞}. We have to distinguish the CM and the non-CM cases (see Definition 2.11), because the behaviour of the curve and its Galois representations are generically really different, as we will see.

2.4.1 Elliptic curves without complex multiplication

Serre's open image theorem

The starting result, which is a major advance forward in the study of non-CM elliptic curves, is the following:

Theorem 2.18 (Serre's open image theorem, global version)**.** *Let E/F be a non-CM elliptic curve. Then $\rho_E(G_F)$ has finite index in* $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

Proof. It follows from [Ser72, Section 4.2, Théorème 2] and [Ser89, IV.19, Proposition]. □

Roughly, the image of ρ_E in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is large: there exists an integer m such that $\rho_E(G_F)$ is the full inverse image in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ of $\rho_{E,m}(G_F)$. We recall that $\rho_E(G_F) \subseteq \mathcal{G}_F$ and $\rho_{E,p^\infty}(G_F) \subseteq \mathcal{G}_{F,p^\infty}$.

Definition 2.19. Let E/F be a non-CM elliptic curve. The *adelic level* of ρ_E, denoted by M_E, is the smallest integer m such that $\rho_E(G_F)$ is the full inverse image of $\rho_{E,m}(G_F)$ in $\mathcal{G}_F$. The *adelic index* of ρ_E is the finite index $[\mathcal{G}_F : \rho_E(G_F)]$.

In particular, the representation $\rho_{E,m}$ is maximal for all m coprime to M_E and the radical of M_E is the smallest integer sastisfying this condition. Therefore, a prime p such that $\rho_{E,p}$ is non maximal is called an *exceptional prime for E/F*. This terminology was introduced by Jones for elliptic curves over $\mathbb{Q}$ in [Jon10, Definition 1].

Remark 2.20. In [RSZB22] the terminology *exceptional images* is used for images $\rho_{E,m}(G_F)$ which occur for only finitely many non-CM j-invariants. On the other hand, we talk about *exceptional subgroups* for subgroups of $\mathrm{GL}_2(p)$ having projective image in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ isomorphic to A_4, A_5 or S_4. But these three notions of exceptional primes, exceptional images and exceptional groups have no link, except for the fact that an exceptional image occurs only at an exceptional prime. However, in [Sut16], the terminology *exceptional images* has been used for images of non-surjective Galois representation.

In the database [LMF24], the adelic level is given for elliptic curves over $\mathbb{Q}$, together with the p-adic level for all p, defined as follow:

Definition 2.21. Let E/F be a non-CM elliptic curve and p be a prime. The *p-adic level* of ρ_E is the smallest prime power p^k such that $\rho_{E,p^\infty}(G_F)$ is the full inverse image of $\rho_{E,p^k}(G_F)$ in $\mathcal{G}_{F,p^\infty}$. The power k is called the *p-adic depth* of ρ_E.

The exceptional primes are those for which the p-adic depth is positive. For every prime p, the p-adic level divides the adelic level. Indeed, since the inverse image of $\rho_{E,M_E}(G_F)$ in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is $\rho_E(G_F)$, then the inverse image of $\rho_{E,p^{v_p(M_E)}}(G_F)$ in $\mathrm{GL}_2(\mathbb{Z}_p)$ is $\rho_{E,p^\infty}(G_F)$. For the other divisors of M_E, these are those which are involved in an horizontal entanglement, which is the topic of Section 3.

Remark 2.22. In the same way, we define the *p-adic depth of χ_∞* as the smallest integer r such that one of the following equivalent conditions holds:

1. $\chi_{p^\infty}(G_F)$ is the full inverse image of $\chi_{p^r}(G_F)$ in $\mathbb{Z}_p^*$.
2. $F \cap \mathbb{Q}(\boldsymbol{\mu}_{p^\infty}) \subseteq \mathbb{Q}(\zeta_{p^r})$.

We observe that, if the p-adic depth k of ρ_E is greater than the p-adic depth of χ_∞, then it comes down to the same to take the inverse image of $\rho_{E,p^k}(G_F)$ in $\mathcal{G}_{F,p^\infty}$ or in $\mathrm{GL}_2(\mathbb{Z}_p)$.

As stated in [Ser89, IV.19, Proposition][2], Serre's open image theorem is equivalent to the following:

Theorem 2.23 (Serre's open image theorem, local version)**.** *Let E/F be a non-CM elliptic curve. Then $\rho_{E,p}$ is surjective for almost all primes p.*

Serre proved the local version in order to prove the global version. He proceeded by contraposition, proving that if E/F has infinitely many exceptional primes, then it must have CM. His method, which is a recurrent method for the results of this section, is based on the classification of subgroups of $\mathrm{GL}_2(\mathbb{Z}_p)$, see [Ser72, Section 2], and a deep study of the link between the reduction type of the curve and the image through $\rho_{E,p}$ of the inertia subgroups of G_F attached to p.

Exceptional primes

By Serre's open image theorem, every non-CM elliptic curve has surjective mod p Galois representation for almost all prime p. Duke proved in 1997 that, in terms of arithmetic statistics, almost all elliptic curves over $\mathbb{Q}$ have surjective mod p Galois representation for any prime p:

Theorem 2.24 ([Duk97])**.** *If we order elliptic curves over $\mathbb{Q}$ by their naive height, then the proportion of elliptic curves over $\mathbb{Q}$ with exceptional primes is* 0.

This shows that an elliptic curve over $\mathbb{Q}$ has generically surjective mod p Galois representation for any prime p. Later, Jones and Zywina proved stronger results, as we will see in Chapter 3, which are summerized in Theorem 1.30.

Now, for which prime p the representation $\rho_{E,p}$ is not surjective, and what is the image in these cases? We can reformulate this question in the following general program, sets by Mazur in [Maz06, Maz-3]:

Mazur's Program B. Given a number field F and a subgroup H of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, classify all elliptic curves defined over F whose adelic Galois representation maps G_F into H.

This program is equivalent to the following:

Problem 2.25. Given a number field F and a subgroup H of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, determine $X_H(F)$ where X_H is the modular curve associated to H.

For information about modular curves, see Appendix B. From the classification of subgroups of $\mathrm{GL}_2(p)$ (see [Sut16, Section 3], or [Ser72, Section 2]), the image of $\rho_{E,p}$ contains $\mathrm{SL}_2(p)$ or is contained in one of the following subgroups:

- a Borel subgroup, in this case $E/\mathbb{Q}$ has a p-rational isogeny *i.e.* there exists $P \in E[p]\backslash\{O\}$ such that G_F acts on the group generated by P,
- the normalizer of a (split or non-split) Cartan subgroup,

[2] The reference [Ser89] was first published in 1968, so before [Ser72], and was reprinted in 1989.

- an exceptional group, *i.e.* with image in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ (the quotient of $\mathrm{GL}_2(p)$ by diagonal matrices) isomorphic to A_4, S_4 or A_5.

Hence, to study mod p images of Galois representation of elliptic curves, one can look for the rational points on the modular curves associated to each of these groups.

Serre's open image theorem says that, for every elliptic curve E/F without CM, there exists an integer c_E such that, for all prime p greater than c_E, the representation $\rho_{E,p}$ is surjective. In 1978, Mazur proved the Mordell-Weil theorem which gives the exact list of possible group structure for $E_{\mathrm{tors}}(\mathbb{Q})$, see [Maz78, Theorem 2]. As a consequence, he showed that, if E is defined over $\mathbb{Q}$ and semistable, then $c_E = 7$ works:

Theorem 2.26 ([Maz78, Theorem 4]). *Let $E/\mathbb{Q}$ be a semistable elliptic curve. Then $\rho_{E,p}$ is surjective for all $p \geq 11$.*

Serre asked whether there exists a constant c_E independent of $E/\mathbb{Q}$. It is known as *Serre's uniformity question.* He formulated an even more precise question:

Question 2.27 ([Ser81b, Questions, p.399]). *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Is $\rho_{E,p}$ surjective for all $p > 37$?*

We expect that this question has an affirmative answer, which is commonly referred as the *Serre's Uniformity Bound*, but for now, we do not even know if the Serre's uniformity question has a positive answer. More recently, Zywina made a more precise conjecture:

Conjecture 2.28 ([Zyw15, Conjecture 1.12]). *Let $E/\mathbb{Q}$ be a non-CM elliptic curve and $p > 13$ be a prime such that $(p, j(E)) \notin S$ where*

$$S = \left\{ \left(17, \frac{-17^2 \cdot 101^3}{2}\right), \left(17, \frac{-17 \cdot 373^3}{2^{17}}\right), \left(37, -7 \cdot 11^3\right), \left(37, -7 \cdot 137^3 \cdot 2083^3\right) \right\}.$$

Then $\rho_{E,p}$ is surjective.

The conjecture is "optimal" in the sense that there exists a CM elliptic curve with j-invariant j and $\rho_{E,p}$ non-surjective for all $(p, j) \in S$ and infinitely many j-invariant such that $\rho_{E,p}$ non-surjective and $p \leq 13$ from [SZ17, Corollary 1.6] and [RSZB22, Theorem 1.6]. In the hypotheses of Conjecture 2.28, the image $\rho_{E,p}(G_{\mathbb{Q}})$ is maximal or contained in the normalizer of a non-split Cartan subgroup, see [Zyw15, Theorem 1.11]. In the same paper, Zywina gives an algorithm to compute all possible images $\rho_{E,p}(G_F)$ assuming Conjecture 2.28. Hence, it gives at least all possible images $\rho_{E,p}(G_F)$ for $p \leq 13$. He determined the list of possible images mod p for each prime p, and for each subgroup H in this list, the (one-parameter) family of elliptic curves E such that $\rho_{E,p}(G_{\mathbb{Q}})$ is conjugate to H. His method is based on the theory of modular curves and modular functions, specifically the j-map corresponding to these modular curves. The same year, he gives an algorithm [Zyw22a, Section 1.1] to compute, for a given non-CM elliptic curve, a finite set containing the exceptional primes, using the reduction of the curve. He proved that:

Proposition 2.29 ([Zyw22a, Proposition 1.6]). *Let $p > 13$ be a prime. The representation $\rho_{E,p}$ is surjective if and only if $(p, j(E)) \notin S$ and there is a prime $q \nmid p \cdot f_E$ such that $a_q(E) \neq 0 \pmod{p}$ and $a_q(E)^2 - 4q$ is a non-zero square mod p.*

He also finds explicit upper bounds for the exceptional primes. In particular, one can take $c_E = \max\{37, \sqrt{\mathrm{N}(\mathfrak{f}_E)}\}$. If $E/\mathbb{Q}$ has multiplicative reduction at p, then $c_E \leq \max\{17, (p+1)/2\}$ works also. This improves bounds given in 2005 by Cojocaru in [CK05].

For elliptic curves defined over number field, Larson and Vaintrob [LV13] give, under the Generalized Riemann Hypothesis, many upper bounds for the exceptional primes, depending on the conductor of the elliptic curve. In particular,

Theorem 2.30 ([LV13, Theorem 23]). *We assume GRH. Let E/F be a non-CM elliptic curve and p be an exceptional prime for E. Then there are effectively computable constant A, B depending only on F such that*

$$p \leq A \cdot \log(\mathrm{N}(\mathfrak{f}_E)) \cdot (\mathrm{loglog}(\mathrm{N}(\mathfrak{f}_E)))^3 + B.$$

Lombardo [Lom16, Theorem 1.4] also gives a bound for exceptional primes, depending on the degree of F and the Falting heights of the non-CM elliptic curve E/F. Moreover, Sutherland [Sut16] gives two probabilistic algorithms to compute images mod p, for p prime[3]. They determine $\rho_{E,p}(G_F)$ up to local conjugacy (defined in *op.cit.*), which is a relatively weaker notion than conjugacy. Both Larson and Vaitrob, and Sutherland, used the image of Frobenius elements of G_F in their method. Coming back to the Serre uniformity question, Zywina gives an analogue over number field:

Conjecture 2.31 ([Zyw24b, Conjecture 2.11]). *For any number field F, the following equivalent conditions hold:*

1. *There is a constant c_F such that for any prime $p > c_F$ and any non-CM elliptic curves E/F, the image $\rho_{E,p}(G_F)$ is maximal.*
2. *There is a finite set $J_F \subseteq F$ such that for any prime $p > 19$ and any non-CM elliptic curve E/F with $j(E) \notin J_F$, the image $\rho_{E,p}(G_F)$ is maximal.*

In *op.cit.*, Zywina gives a preliminary description of the possibility for the indexes and the image $\rho_E(G_F) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ for any number field F.

There are many other works on images of mod p Galois representations of elliptic curves as [RV01], [BP11], [BPR13], [BDM$^+$19], [BDM$^+$23].

p-adic images

Now we have an overview of the current knowledge about images of mod p Galois representations, we turn to images of mod p^k and p-adic representations, in particular the p-adic depth. If $\rho_{E,p^\infty}(G_F)$ is maximal, or when $F = \mathbb{Q}$, we have quite precise answers to this question. In [Ser89, IV, 3.4, Lemme 3], Serre observed that if $p \geq 5$ and G is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ with image in $\mathrm{GL}_2(p)$ containing $\mathrm{SL}_2(p)$, then G contains $\mathrm{SL}_2(\mathbb{Z}_p)$. This is not valid for $p = 2, 3$, but there are similar results in this case. We obtain:

Theorem 2.32 ([KS09, Lemma 1 and following paragraph]). *Let E/F be an non-CM elliptic curve. For $p \geq 5$, the representation ρ_{E,p^∞} has maximal image if and only if $\rho_{E,p}$ has maximal image. Moreover, $\rho_{E,3^\infty}$ has maximal image if and only if $\rho_{E,9}$ has maximal image, and $\rho_{E,2^\infty}$ has maximal image if and only if $\rho_{E,8}$ has maximal image.*

In other words, if $\rho_{E,p}(G_F)$ is maximal, then the p-adic depth is 0 if $p \geq 5$, at most 2 if $p = 3$ and at most 3 if $p = 2$. For elliptic curves over $\mathbb{Q}$, the two following points complete Theorem 2.32 about caracterisation for the surjectivity of p-adic Galois representations:

- [Elk06] shows that there are infinitely many j-invariant in $\mathbb{Q}$ for which the associated elliptic curves have surjective mod 3 Galois representation but not mod 9. They are parameterized by the modular curve $\mathcal{X}_9 = X(9)/G$ where G is a *split lifting* of $\mathrm{SL}_2(3)$ in $\mathrm{SL}_2(9)$: it is a subgroup of $\mathrm{SL}_2(9)$ which maps isomorphically onto $\mathrm{SL}_2(3)$. The existence of such G was observed by [Ser89, IV, 3.4, Exercice 3]. For now, we do not know if the modular curve $\mathcal{X}_9$ parametrized all elliptic curves with this property.

[3] The mod p Galois images data in LMFDB was computed using the algorithm given by [Sut16].

Figure 2.1: Table of possible p-adic depth

Prime p	Possible p-adic depth	Example or comments
2	0	37.a1
	1	69.a1
	2	33.a1
	3	15.a2
	4	15.a1
	5	15.a4
3	0	37.a1
	1	26.a2
	2	14.a1
	3	19.a1
5	0	37.a1
	1	11.a2
	2	11.a1
$7, 11$	0	37.a1
	1	26.b1, 121.a1
	2	In the database [LMF24], there are only elliptic curve over $\mathbb{Q}$ with a p-adic level 0 or 1
$13, 17, 37$	0	37.a1
	1	147.b1, 14450.b1, 1225.b1
$19, 23, 29, 31, p \geq 41$	0	37.a1
	1	Conjecture 2.28 implies that the p-adic depth is always 0

- Dokchitser and Dokchitser [DD11] give necessary and sufficient conditions on Δ_E and $j(E)$ for the surjectivity of $\rho_{E,2}$, $\rho_{E,4}$ and $\rho_{E,8}$ for E defined over $\mathbb{Q}$.

Few years later, Rouse and Zureick-Brown classify all possible images $\rho_{E,2^\infty}(G_\mathbb{Q})$[4] and their index in $\mathrm{GL}_2(\mathbb{Z}_2)$. In particular, they showed that the 2-adic depth is at most 5:

Theorem 2.33 ([RZB15, Corollary 1.3])**.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve. The image of $\rho_{E,2^\infty}$ is the full inverse image of $\rho_{E,32}(G_\mathbb{Q})$ in $\mathrm{GL}_2(\mathbb{Z}_2)$.*

Recently, Sutherland and Zywina classified all possible images $\rho_{E,p^\infty}(G_\mathbb{Q})$ except for a finite set of j-invariant:

Theorem 2.34 ([SZ17, Corollary 1.6])**.** *For $p = 2, 3, 5, 7, 11, 13$ there are respectively $1201, 47, 23, 15, 2, 11$ subgroups of $\mathrm{GL}_2(\mathbb{Z}_p)$ arising as $\rho_{E,p^\infty}(G_\mathbb{Q})$ for infinitely many elliptic curves $E/\mathbb{Q}$ with distinct j-invariant; for $p > 13$ the only such subgroup is $\mathrm{GL}_2(\mathbb{Z}_p)$.*

Following this work, Rouse, Sutherland and Zureick-Brown dealt with exceptional images, that are subgroups which arise as $\rho_{E,p^\infty}(G_\mathbb{Q})$ for finitely many elliptic curves $E/\mathbb{Q}$ with distinct j-invariant. Their main result [RSZB22, Theorem 1.6] gives us information about the p-adic depth for non-CM elliptic curve over $\mathbb{Q}$, summerized in Table 2.1. An algorithm given in [RSZB22, Section 11] return, for a given non-CM elliptic curve $E/\mathbb{Q}$, the list of non-maximal images $\rho_{E,p^\infty}(G_\mathbb{Q})$[5].

Finally, there are elliptic curves such that ρ_{E,p^∞} is surjective for all p, as the following example shows:

[4] The 2-adic Galois images data in LMFDB was computed using the algorithm given by [RZB15].

[5] The p-adic Galois images data in LMFDB was computed using the algorithm given by [RSZB22].

Example 2.35. The elliptic curve $E : y^2+y = x^3-x$ with LMFDB label 37.a1 has surjective p-adic representation for all p.

Example 2.36 ([Gre10, Theorem 1.5]). Let α be a roots of $x^3 + x + 1$ and $F = \mathbb{Q}(\alpha)$. The elliptic curve $E : y^2 + 2xy + \alpha y = x^3 - x^2$ has surjective p-adic representation for all p. It has even surjective adelic representation.

In fact, this is the case for almost all elliptic curves:

Theorem 2.37. *Almost all elliptic curves over F have maximal p-adic Galois representation for any p.*

Proof. For $F \neq \mathbb{Q}$, it follows from Theorem 3.20. Suppose that $F = \mathbb{Q}$. From Theorem 3.41 and Theorem 2.32, if $E/\mathbb{Q}$ is an elliptic curve with adelic index 2, then $\rho_{E,p^k}(G_\mathbb{Q})$ is surjective except eventually when $8 \mid p^k$. In this case $[\mathrm{GL}_2(8) : \rho_{E,8}(G_\mathbb{Q})] = 2$ and, by [Jon10, Lemma 28], this is the case only for a proportion of elliptic curves equal to 0. Otherwise, if $\rho_{E,8}$ is surjective then so is $\rho_{E,2^\infty}$, by Theorem 2.32. Moreover, the proportion of elliptic curve with adelic index 2 is equal to 1, see Theorem 3.23. □

However, for E defined over $\mathbb{Q}$, the Galois representation ρ_E is never surjective in $\mathrm{GL}_2(\hat{\mathbb{Z}})$. There are other obstructions to the surjectivity of $\rho_{E,m}$ when m is not a prime power, due to entanglement of division fields. This topic is covered in Section 3.

2.4.2 Elliptic curves with complex multiplication.

Let E/F be an elliptic curve, $\mathcal{O} := \mathrm{End}(E)$ and K be the field of fraction of $\mathcal{O}$. Then E_{tors} is an $\mathcal{O}$-module. We have $\mathcal{O} = \mathbb{Z}$ and $K = \mathbb{Q}$ if E/F does not have CM and $\mathcal{O}$ is an order in the imaginary quadratic field K otherwise. Suppose that E/F has CM *i.e.* that $\mathcal{O}$ is not $\mathbb{Z}$. In this case $\mathcal{O}$ is an order in a imaginary quadratic field, *i.e.* $\mathcal{O} \simeq \mathbb{Z} + f\mathcal{O}_K$ for some positive integer f, called the *conductor* of $\mathcal{O}$, and some imaginary quadratic field K, called the *CM field of E*. By [ST68, Corollary 1], we have

$$\mathrm{Aut}_\mathcal{O}(E_{\mathrm{tors}}) \simeq (\mathcal{O} \otimes_\mathbb{Z} \hat{\mathbb{Z}})^*.$$

In the CM case, we have $K(x(E_{\mathrm{tors}})) \subseteq K^{\mathrm{ab}}$, by [Sil94, Corollary 5.7]. But the extension $K(E[m])$ has index 2 over $K(x(E[m]))$, see Theorem 5.11 and $\mathrm{GL}_2(m)$ does not have any abelian subgroups of index 2. Thus $\rho_E(G_F)$ has infinite index in $\mathrm{GL}_2(\hat{\mathbb{Z}})$. Nevertherless, Campagna and Pengo [CP22b] give a generalisation of Serre's open image theorem to CM elliptic curves. If $K \not\subseteq F$, let $\tau \in G_F$ such that its restriction to FK generates $\mathrm{Gal}(FK/F)$. We recall that $\mathrm{Aut}(E_{\mathrm{tors}}) \simeq \mathrm{GL}_2(\hat{\mathbb{Z}})$ and $\mathrm{Aut}_\mathcal{O}(E_{\mathrm{tors}}) \leq \mathrm{Aut}(E_{\mathrm{tors}})$. We define by $\mathcal{G}(E/F)$ the largest subgroup of

$$\begin{cases} \mathrm{Aut}_\mathcal{O}(E_{\mathrm{tors}}) & \text{if } K \subseteq F \\ \langle \mathrm{Aut}_\mathcal{O}(E_{\mathrm{tors}}), \rho_E(\tau)\rangle & \text{otherwise.} \end{cases}$$

whose image in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ has determinant $\chi_{\mathrm{cyc}}(G_F)$. We also define, for a prime p, the group $\mathcal{G}(E/F, p^\infty)$ as the image of $\mathcal{G}(E/F)$ in $\mathrm{GL}_2(\mathbb{Z}_p)$ and, for an integer m, the group $\mathcal{G}(E/F, m)$ as its image in $\mathrm{GL}_2(m)$. If E/F does not have CM, then $\mathcal{G}(E/F, m) = \mathcal{G}_{F,m}$ for any integer m, $\mathcal{G}(E/F, p^\infty) = \mathcal{G}_{F,p^\infty}$ for any prime p and $\mathcal{G}(E/F) = \mathcal{G}_F$.

Theorem 2.38 ([CP22b, Lemma 2.2])**.** *Let E/F be an elliptic curve. Then $\rho_E(G_F)$ has finite index in $\mathcal{G}(E/F)$.*

Definition 2.39. With the same notation as in previous theorem, we say that the image of $\rho_{E,m}$ (respectively of ρ_{E,p^∞}, of ρ_E) is *maximal* if it is equal to $\mathcal{G}(E/F,m)$ (respectively to $\mathcal{G}(E/F,p^\infty)$, to $\mathcal{G}(E/F)$).

The algorithm of Sutherland and Zywina to compute images of mod p representations, mentioned in Section 2.4.1, assume that the elliptic curve is non CM.

Example 2.40. The elliptic curve $E: y^2 = x^3 - 11x - 14$ with LMFDB label 32.a1 has CM by $K = \mathbb{Q}(i)$, with endomorphism ring $\mathcal{O} = \mathbb{Z}[2i]$ where $i = \sqrt{-1}$. The conductor f of $\mathcal{O}$ is 2 and $\Delta_K = -4$. Since E is defined over $\mathbb{Q}$, then $K \not\subseteq \mathbb{Q}(j(E)$. Thus

$$\mathcal{G}(E/F) = \mathrm{Aut}_{\mathbb{Z}[2i]}(E_{\mathrm{tors}}), \ltimes \langle \rho_E(\tau) \rangle$$

where $\tau \in G_{\mathbb{Q}}$ satisfies $\tau(i) = -i$. If we consider E defined over K, then

$$\mathcal{G}(E/F) = \mathrm{Aut}_{\mathbb{Z}[2i]}(E_{\mathrm{tors}}).$$

From LMFDB, ρ_{E,p^∞} has maximal image for all p but 2. From Theorem 3.27, $\rho_E(G_{\mathbb{Q}})$ has index 2 in $\mathcal{G}(E/\mathbb{Q})$. We deduce that $\rho_{E,2^\infty}(G_{\mathbb{Q}})$ has index 2 in $\mathcal{G}(E/\mathbb{Q},2^\infty)$.

On the other hand, Lozano-Robledo [LR22] defines a subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, depending on the CM field and on the conductor of $\mathrm{End}(E)$, such that the image of ρ_E is contained with finite index in this group and can be equal to it.

Definition 2.41. Let $\mathcal{O}$ be an order in an imaginary quadratic field K and let f be the conductor of $\mathrm{End}(E)$. For a positive integer m, we define δ and ϕ as follows

- If $\Delta_K f^2 \equiv 0 \pmod 4$ or m is odd, let $\delta = \Delta_K f^2/4$, and $\phi = 0$,
- If $\Delta_K f^2 \equiv 1 \pmod 4$ and m is even, let $\delta = \frac{(\Delta_K - 1)f^2}{4}$ and $\phi = f$.

We set $N_{\delta,\phi}(m) := \left\langle C_{\delta,\phi}(m), \begin{pmatrix} -1 & 0 \\ \phi & 1 \end{pmatrix} \right\rangle$ with

$$C_{\delta,\phi}(m) := \left\{ \begin{pmatrix} a + b\phi & b \\ \delta b & a \end{pmatrix} \mid a, b \in \mathbb{Z}/m\mathbb{Z}, a^2 + ab\phi - \delta b^2 \in (\mathbb{Z}/m\mathbb{Z})^* \right\}.$$

Moreover, we define, for p prime, $N_{\delta,\phi}(p^\infty) = \varprojlim_k N_{\delta,\phi}(p^k)$ and $N_{\delta,\phi}(\hat{\mathbb{Z}}) = \varprojlim_m N_{\delta,\phi}(m)$.

Theorem 2.42. *Let E/F be a CM elliptic curve. Then, for all integers m, there exists a basis of $E[m]$ such that the image of $\rho_{E,m}$ is contained in $N_{\delta,\phi}(m)$ and a compatible system of bases of $E[m]$ for all $m \geq 2$ such that the image of ρ_E is contained in $N_{\delta,\phi}(\hat{\mathbb{Z}})$.*

Proof. This follows from Theorem [LR22, Theorem 1.1], since the inclusion $\mathbb{Q}(j(E)) \subseteq F$ implies $\rho_E(G_F) \leq \rho_E(G_{\mathbb{Q}(j(E))})$. □

If we define the p-adic depth of ρ_E to be the smallest integer k such that $\rho_{E,p^\infty}(G_F)$ is the full inverse image of $\rho_{E,p^k}(G_F)$ in $N_{\delta,\phi}(p^\infty)$, then the p-adic depth of an elliptic curve with CM is equal to 0 or 1 for all p but $2,3$. For $p = 2$, we know that the p-adic depth is less or equal to 5 from [RZB15].

Theorem 2.43 ([LR22, Theorem 1.2.(2)]). *Let $F = \mathbb{Q}(j(E))$. For $p \geq 5$, the group $\rho_{E,p^\infty}(G_F)$ is the full inverse image of $\rho_{E,p}(G_F)$ via the reduction map $N_{\delta,\phi}(p^\infty) \to N_{\delta,\phi}(p)$.*

In *op.cit.*, Lozano-Robledo also gives additional results concerning the 2-adic and 3-adic images.

Example 2.44. For the elliptic curve $E : y^2 = x^3 - 11x - 14$ with LMFDB label 32.a1 of Example 2.40, we have $\Delta_K f^2 = -16 \equiv 0 \pmod 4$. Then $\delta = -4$ and $\phi = 0$ for any m. We have:

$$C_{-4,0}(m) := \left\{ \begin{pmatrix} a & b \\ -4b & a \end{pmatrix}, a, b \in \mathbb{Z}/m\mathbb{Z}, a^2 + 4b^2 \in (\mathbb{Z}/m\mathbb{Z})^* \right\}$$

and $N_{-4,0}(m) := \left\langle C_{-4,0}(m), \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$. Its image modulo 2 is $N_{-4,0}(2) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$. Its image modulo 4 has index 2 in $N_{-4,0}(4)$. By [LR22, Theorem 1.2.(1)], the index of $\rho_E(G_{\mathbb{Q}})$ in $N_{\delta,\phi}(G_{\mathbb{Q}})$ divides 2 and so $\rho_{E,2^\infty}(G_{\mathbb{Q}})$ has index 2 in $N_{\delta,\phi}(\mathbb{Z}_2)$.

Chapter 3

Entanglements and adelic representations

3.1 Entanglement: definitions

The previous chapter concerned local Galois representation at a prime p. In this chapter, we are interested in mod m Galois representation where m is not a prime power. The natural projection $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}_p)$ gives a surjective morphism $\rho_E(G_F) \to \rho_{E,p^\infty}(G_F)$. Hence, knowing $\rho_E(G_F)$, we can deduce $\rho_{E,p^\infty}(G_F)$ for all p. Conversely, knowing the image of ρ_{E,p^∞} for all prime p, we would like to deduce the image of ρ_E, but entanglements give obstructions to determining the global representation from local data.

For an integer m, the natural morphism

$$\rho_{E,m}(G_F) \longrightarrow \prod_{p\in\mathcal{P}} \rho_{E,p^{v_p(m)}}(G_F).$$

is injective but it is not necessary surjective. Equivalently, we have an injective morphism

$$\begin{aligned} \mathrm{Gal}(F(E[m])/F) &\longrightarrow \prod_{p\in\mathcal{P}} \mathrm{Gal}(F(E[p^{v_p(m)}])/F) \\ \sigma &\longmapsto \left(\sigma|_{F(E[p^{v_p(m)}])}\right). \end{aligned} \tag{3.1}$$

By Section 1.2, this morphism is surjective if and only if $F(E[a]) \cap F(E[b]) = F$ for all coprime divisors a, b of m.

Example 3.1. The elliptic curve $E : y^2 = x^3 - 36x + 84$ with LMFDB label 1944.c1 has surjective mod 2 and mod 3 representation, but not mod 6. Thus, the morphism

$$\rho_{E,6}(G_F) \to \rho_{E,2}(G_F) \times \rho_{E,3}(G_F) \simeq \mathrm{GL}_2(6)$$

is not surjective. The index of the mod 6 image in $\mathrm{GL}_2(6)$ is 6, which is the cardinality of

$$\rho_{E,2}(G_F) \simeq \mathrm{GL}_2(2) \simeq S_3.$$

This implies that $\#\rho_{E,6}(G_\mathbb{Q}) = \#\rho_{E,3}(G_\mathbb{Q})$, which is equivalent to having the equality $\mathbb{Q}(E[6]) = \mathbb{Q}(E[3])$, or, equivalently, the inclusion $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$. We say that we have a $(2,3)$-entanglement of non-abelian type S_3, with entanglement field $\mathbb{Q}(E[2]) = \mathbb{Q}(E[2]) \cap \mathbb{Q}(E[3])$. The curve also has a $(4,3)$-entanglement of index 24 (see Definition 3.2). In particular, the field $\mathbb{Q}(E[3])$ is quadratic over the entanglement field $\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[4]))$.

In general, the failure of $\rho_{E,m}$ to be surjective is explained by two phenomena:

1. **Local conditions**: The non-surjectivity of the p-adic image for some $p \mid m$.
2. **Entanglement**: The non-surjectivity of $\rho_E(G_F)$ on $\prod\limits_{p|m} \rho_{E,p^\infty}(G_F)$.

We speak of *vertical entanglement* in the first case. In [DLRM23], this is referred to by *vertical collapsing* or *vertical tanglement*. The latter case is called *horizontal entanglement*, or simply *entanglement* in the literature. We refer to a failure of surjectivity of the injective homomorphism:

$$\mathrm{Gal}(F^{\mathrm{cyc}}/F) \simeq \det(\rho_E(G_F)) \to \prod_{p \in \mathcal{P}} \det(\rho_{E,p^\infty}(G_F)) \simeq \prod_{p \in \mathcal{P}} \mathrm{Gal}(F(\zeta_{\boldsymbol{\mu}_{p^\infty}})/F)$$

as an *arithmetic* or *cyclotomic* contribution to the horizontal entanglement. This cyclotomic entanglement is independent of the curve E/F and concerns the failure of the fields $F(\zeta_{p^\infty})$ to be linearly disjoint over F (see Definition 1.44).

We further define the notion of an (a,b)-entanglement. For m a positive integer, we set $F_m := F(E[m])$. Let a, b two integers with $\gcd(a,b) = d$ and $\mathrm{lcm(a, b)} = m$. We have the following graph of inclusions:

$$\begin{tikzcd}
 & F_m \arrow[dl, dash] \arrow[dr, dash] & \\
F_a \arrow[dr, dash] & & F_b \arrow[dl, dash] \\
 & F_d &
\end{tikzcd}$$

We set

$$\phi_{a,b} : \rho_{E,m}(G_{F_d}) \to \rho_{E,a}(G_{F_d}) \times \rho_{E,b}(G_{F_d})$$

to be the natural map induced by the injective morphism $\mathrm{GL}_2(m) \to \mathrm{GL}_2(a) \times \mathrm{GL}_2(b)$, which gives rise to an injective map

$$\mathrm{Gal}(F_m/F_d) \to \mathrm{Gal}(F_a/F_d) \times \mathrm{Gal}(F_b/F_d)$$

giving $F_m = F_a F_b$ and, from Section 1.2, to an isomorphism

$$\mathrm{Gal}(F_m/F_a \cap F_b) \to \mathrm{Gal}(F_a/F_a \cap F_b) \times \mathrm{Gal}(F_b/F_a \cap F_b).$$

This leads to the following definition:

Definition 3.2. We say that E has an (a,b)*-entanglement* if one of the following equivalent conditions is satisfied:

- $\phi_{a,b}$ is not an isomorphism.
- $F_a \cap F_b \neq F_d$.

In this case, $F_a \cap F_b$ is called the *entanglement field* and the degree $[F_a \cap F_b : F_d]$ is called the *index* (or *degree*) of the (a,b)-entanglement. The extension $(F(\zeta_a) \cap F(\zeta_b))F_d/F_d$ is called the *arithmetic contribution* to the (a,b)-entanglement.

Remark 3.3. Let E/F be an elliptic curve with an (a,b)-entanglement. This entanglement has an arithmetic contribution if and only if F has an (a,b)-cyclotomic entanglement, and $F(\zeta_a)\cap F(\zeta_b)\not\subseteq F(E[d])$.

Remark 3.4. An (a,b)-entanglement for E/F is an obstruction for $\rho_{E,m}$ to be surjective but not necessarily an obstruction to have maximal images. For example, if a and b are coprime, $\rho_{E,a}$ and $\rho_{E,b}$ have maximal images, and $F(E[a])\cap F(E[b]) = F(\zeta_a)\cap F(\zeta_b)\neq F$, then $\rho_{E,m}$ have maximal image.

In particular, when $d=1$ we have an (a,b)-entanglement if and only if $F_a\cap F_b\neq F$.

Remark 3.5. By Remark 1.22, we have

$$[F_a\cap F_b : F_d] = \frac{[F_a:F][F_b:F]}{[F_m:F]} = \frac{\#\rho_{E,a}(G_{F_d})\cdot\#\rho_{E,b}(G_{F_d})}{\#\rho_{E,m}(G_{F_d})}.$$

In particular, if $d=1$ and $L := F(\zeta_a)\cap F(\zeta_b)$ then $\mathcal{G}_{L,ab}\simeq\mathcal{G}_{L,a}\times\mathcal{G}_{L,b}$ and if E/F does not have CM:

$$[F_a\cap F_b : L] = \frac{[\mathcal{G}_{L,ab} : \rho_{E,ab}(G_L)]}{[\mathcal{G}_{L,a}:\rho_{E,a}(G_L)]\cdot[\mathcal{G}_{F,b}:\rho_{E,b}(G_F)]}.$$

The Serre entanglement

Before describing the most common cause of entanglement, we gives a property of 2-torsion fields and set some notations.

Proposition 3.6. *Let E/F be an elliptic curve. We have $F(\sqrt{\Delta_E})\subseteq F(E[2])$.*

Proof. Let $y^2=f(x)$ be a Weierstrass equation for E and let $\alpha_1,\alpha_2,\alpha_3$ be the roots of f. Then

$$\Delta_E = (\alpha_1-\alpha_2)^2(\alpha_2-\alpha_3)^2(\alpha_3-\alpha_1)^2.$$

In particular $F(\sqrt{\Delta_E})\subseteq F(\alpha_1,\alpha_2,\alpha_3)$. The latter is equal to $F(E[2])$ by Proposition 2.6. □

Definition 3.7. Let $E/\mathbb{Q}$ be an elliptic curve and Δ_E its discriminant. We denote by $\Delta_{\mathrm{sf}}(E)$ the squarefree part of Δ_E.

Let $E/\mathbb{Q}$ be an elliptic curve. Since $\mathbb{Q}(\sqrt{\Delta_E})/\mathbb{Q}$ is abelian, the Kronecker-Weber theorem (see [Neu99, V, Theorem 1.10]) implies that there exists n such that $\mathbb{Q}(\sqrt{\Delta_E})\subseteq\mathbb{Q}(\zeta_n)$. If $\Delta_{\mathrm{sf}}(E)\neq 1$, Proposition 3.6 gives that the intersection $\mathbb{Q}(E[2])\cap\mathbb{Q}(\zeta_n)$ is non-trivial and we say that $E/\mathbb{Q}$ has a *Serre entanglement*, because this non-trivial intersection is involved in the proof of Theorem 3.16 by Serre. If $\Delta_{\mathrm{sf}}(E)\in\{\pm1,\pm2\}$, then $\rho_{E,2^\infty}$ is not surjective by [DD11]: if $\Delta_{\mathrm{sf}}(E)=1$ the $\rho_{E,2}$ is not surjective, if $\Delta_{\mathrm{sf}}(E)=-1$ then $\rho_{E,4}$ is not surjective, if $\Delta_{\mathrm{sf}}(E)=\pm2$, then $\rho_{E,8}$ is not surjective. Suppose that $\Delta_{\mathrm{sf}}(E)\notin\{\pm1,\pm2\}$. Then the Serre entanglement gives rise to a non-trivial intersection $\mathbb{Q}(E[2^\infty])\cap\mathbb{Q}(E[m])$ for some odd integer m, as we will show now. By assumption, there exists $p_1,\dots,p_t$ odd primes such that

$$\Delta_{\mathrm{sf}}(E) = 2^*p_1^*\dots p_t^*$$

with

$$2^* = \begin{cases} 1 & \text{if } \Delta_E\equiv 1 \pmod 4,\\ -1 & \text{if } \Delta_E\equiv -1 \pmod 4,\\ 2 & \text{if } \Delta_{\mathrm{sf}}(E)\equiv 2 \pmod 8\\ -2 & \text{if } \Delta_{\mathrm{sf}}(E)\equiv -2 \pmod 8).\end{cases}$$

and for p a prime, $p^* = (-1)^{\frac{p-1}{2}}p$. We set $m = p_1^* \dots p_t^*$. We will show that E has a $(2^k, m)$-entanglement for some $k \leq 3$. By [Neu99, Chapter I, proof of Proposition 10.5], we know that

$$\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(E[p])$$

and so $\mathbb{Q}(\sqrt{m}) \subseteq \mathbb{Q}(E[m])$. Now, we have three cases:

- If $\Delta_{\mathrm{sf}}(E) = p_1^* \dots p_t^*$, *i.e.* $\Delta_{\mathrm{sf}}(E) \equiv 1 \pmod 4$, then

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

  and so $E/\mathbb{Q}$ has a $(2, m)$-entanglement.

- If $\Delta_{\mathrm{sf}}(E) = -p_1^* \dots p_t^*$, *i.e.* $\Delta_{\mathrm{sf}}(E) \equiv -1 \pmod 4$, since $\sqrt{-1} \in \mathbb{Q}(E[4])$ by Weil pairing, we have

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

  and so $E/\mathbb{Q}$ has a $(4, m)$-entanglement.

- If $\Delta_{\mathrm{sf}}(E) = \pm 2 p_1^* \dots p_t^*$, *i.e.* $\Delta_{\mathrm{sf}}(E) \equiv 2 \pmod 4$, since $\sqrt{\pm 2} \in \mathbb{Q}(\zeta_8) \subseteq \mathbb{Q}(E[8])$ by Weil pairing, we have

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

  and so $E/\mathbb{Q}$ has a $(8, m)$-entanglement.

We have proved that:

Theorem 3.8. *Let $E/\mathbb{Q}$ be an elliptic curve.*

- *Suppose that $\Delta_{\mathrm{sf}}(E) \equiv 1 \pmod 4$. If $\Delta_{\mathrm{sf}}(E) = 1$, then $\rho_{E,2}$ is not surjective. Otherwise, $E/\mathbb{Q}$ has a $(2, \Delta_{\mathrm{sf}}(E))$-entanglement.*

- *Suppose that $\Delta_{\mathrm{sf}}(E) \equiv -1 \pmod 4$. If $\Delta_{\mathrm{sf}}(E) = -1$, then $\rho_{E,4}$ is not surjective. Otherwise, $E/\mathbb{Q}$ has a $(4, \Delta_{\mathrm{sf}}(E))$-entanglement.*

- *Suppose that $\Delta_{\mathrm{sf}}(E) \equiv 2 \pmod 4$. If $\Delta_{\mathrm{sf}}(E) = \pm 2$, then $\rho_{E,8}$ is not surjective. Otherwise, $E/\mathbb{Q}$ has a $\left(8, \frac{\Delta_{\mathrm{sf}}(E)}{2}\right)$-entanglement.*

In particular, ρ_E is not surjective. For the listed $(2^k, m)$-entanglement, the entanglement field contain $\mathbb{Q}(\sqrt{m})$.

Almost all elliptic curve over $\mathbb{Q}$ has an horizontal entanglement from the list of Theorem 3.8. Indeed, we saw at the end of Section 2.4.1 that almost all elliptic curves over $\mathbb{Q}$ has surjective p-adic Galois representation for all primes p.

Remark 3.9. The degree of the entanglement field $\mathbb{Q}(E[2^\infty]) \cap \mathbb{Q}(E[m])$ can be greater than 2, as Example 3.1 shows.

Example 3.10. The elliptic curve $E : y^2 = x^3 - 36x + 84$ with LMFDB label 1944.c1 has surjective 2-adic representation. Its discriminant $\Delta_E = -2^8 \times 3^5$ satisfies

$$\mathbb{Q}(\sqrt{\Delta_E}) = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3) \subseteq \mathbb{Q}(E[3])$$

and this causes a $(2, 3)$-entanglement, which is detailed in Example 3.1.

Example 3.11. The elliptic curve with LMFDB label 11.a1 has minimal Weierstrass equation

$$E : y^2 + y = x^3 - x^2 - 7820x - 263580$$

and discriminant $\Delta_E = -11$. Since $11^* = -11$, then $E/\mathbb{Q}$ has a $(2, 11)$-entanglement with entanglement field $\mathbb{Q}(\sqrt{-11})$. On the other hand, ρ_{E,p^∞} is surjective for all p but 5, and the 5-adic depth of ρ_E is 2. The database LMFDB gives that $2 \cdot 5^2 \cdot 11$ is the adelic level of ρ_E.

Example 3.12. The elliptic curve $E/\mathbb{Q}$ with LMFDB label 53.a1 has discriminant -53. Since $53^* = 53$, then $E/\mathbb{Q}$ has a $(4, 53)$-entanglement with entanglement field containing $\mathbb{Q}(\sqrt{53})$. In fact, ρ_E has adelic index 2, and so

$$\mathbb{Q}(E[4]) \cap \mathbb{Q}(E[53]) = \mathbb{Q}(\sqrt{53}).$$

Example 3.13. Let $f(x) = x^3 + x^2 - 77x - 289$ as in Example 1.23. The elliptic curve $E : y^2 = f(x)$ has LMFDB label 44.a1 and discriminant $\Delta_E = -2^8 \cdot 11^3$. There is only one exceptional prime, which is 3, and a $(2, 11)$-entanglement of type $\mathbb{Z}/2\mathbb{Z}$, corresponding to the Serre entanglement, with entanglement field $\mathbb{Q}(\sqrt{-11})$. Over $F = \mathbb{Q}(\sqrt{-11})$, the elliptic curve E/F has no entanglement. However, it has one more exceptional prime, which is 2. The representation $\rho_{E,11}$ is non-surjective for E/F, but has maximal image $\mathcal{G}_F$, which has index 2 in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

The CM entanglement

If E/F has CM by the imaginary quadratic field K, then $K \subseteq F(E[m])$ for any integer m by [BCS17, Lemma 3.15]. In particular, if $K \not\subseteq F$, then for any coprime a, b, the elliptic curve E/F has an (a, b)-entanglement. By Remark 3.5, we have, for $a, b, c \geq 2$ pairwise coprime:

$$[F_{ab} \cap F_c : F][F_a \cap F_b : F] = \frac{\#\rho_{E,a}(G_F) \cdot \#\rho_{E,b}(G_F) \cdot \#\rho_{E,c}(G_F)}{\#\rho_{E,abc}(G_F)}$$

which divides the index of the image of $\rho_E(G_F)$ in $\prod_{p\in\mathcal{P}} \rho_{E,p^\infty}(G_F)$. By induction, we obtain that the index of $\rho_E(G_F)$ in $\prod \rho_{E,p^\infty}(G_F)$ is infinite. But $\rho_E(G_F)$ has finite index in $N_{\delta,\phi}(G_F)$ and in $\mathcal{G}(E/F)$. It follows that the injective maps

$$N_{\delta,\phi}(\hat{\mathbb{Z}}) \to \prod N_{\delta,\phi}(p^\infty) \quad \text{and} \quad \mathcal{G}(E/F) \to \prod \mathcal{G}(E/F, p^\infty)$$

are not surjective. This is the reason why Daniels, Lozano-Robledo and Morrow [DLRM23] define an *horizontal CM entanglement* as the non surjectivity of $\rho_{E,m}(G_F)$ in $N_{\delta,\phi}(m)$ which is not explained by the non-surjectivity in $N_{\delta,\phi}(p^{v_p(m)})$ for any $p \mid m$. The case $K \subseteq F$ is studied in Section 3.3.

3.2 Adelic index

Serre's open image theorem says that, for a non-CM elliptic curve, the adelic index $[\mathcal{G}_F : \rho_E(G_F)]$ is finite. For CM elliptic curves, this index is infinite, but we have defined in Section 2.4.2 the adelic index for CM elliptic curves: it is $[\mathcal{G}(E/F) : \rho_E(G_F)]$, and it is also finite.

Lemma 3.14. *Let E/F be a non-CM elliptic curve. The adelic index is divisible by $[\mathcal{G}_{F,m} : \rho_{E,m}(G_F)]$ for any $m \geq 1$. In particular, it is divisible by $[\mathcal{G}_{F,p^\infty} : \rho_{E,p^\infty}(G_F)]$ for any prime p and by $[F_a \cap F_b : F(\zeta_a) \cap F(\zeta_b)]$ for any coprime integers a, b.*

Proof. Let p be a prime. Then we have a natural surjective morphism $\mathcal{G}_F \to \mathcal{G}_{F,m}/\rho_{E,m}(G_F)$ whose kernel contains $\rho_E(G_F)$. Thus, the morphism

$$\mathcal{G}_F/\rho_E(G_F) \to \mathcal{G}_{F,m}/\rho_{E,m}(G_F)$$

is surjective, and the divisibility

$$[\mathcal{G}_{F,m} : \rho_{E,m}(G_F)] \mid [\mathcal{G}_F : \rho_E(G_F)]$$

follows. Now, let a, b be coprime integers and $L := F(\zeta_a) \cap F(\zeta_b)$. Then

$$[F_a \cap F_b : L] \mid [\mathcal{G}_{L,ab} : \rho_{E,ab}(G_L)] \mid [\mathcal{G}_L : \rho_E(G_L)] \mid [\mathcal{G}_F : \rho_E(G_F)]$$

from Remark 3.5. □

Example 3.15. The elliptic curve with LMFDB label 11.a1 has:

- No vertical entanglement at $p \neq 5$: ρ_{E,p^∞} is surjective for all p but 5,
- A vertical entanglement at 5 with index 120: $[\mathrm{GL}_2(\mathbb{Z}_5) : \rho_{E,5^\infty}(G_F)] = [\mathrm{GL}_2(25) : \rho_{E,25}(G_F)] = 120$,
- An horizontal entanglement at 22: a $(2, 11)$-entanglement (due to the Serre entanglement) of index 2,
- An horizontal entanglement at 275: a $(25, 11)$-entanglement of index 5.

All other entanglements are derived from these one. The adelic level is equal to $550 = 2 \cdot 5^2 \cdot 11$ and the adelic index is equal to $1200 = 120 \cdot 2 \cdot 5$.

Theorem 3.8 implies that for an elliptic curve over $\mathbb{Q}$ the adelic index is never equal to 1. In fact, Serre proved that the adelic index is even, but with a slightly different approach:

Theorem 3.16 ([Ser72, Proposition 22])**.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Then $\rho_{E,2}$ is not surjective or $E/\mathbb{Q}$ has a Serre entanglement. In particular, the adelic index of ρ_E is even.*

Proof. If $\Delta_{\mathrm{sf}}(E) = 1$, then $\rho_{E,2}(G_\mathbb{Q}) \leq \mathbb{Z}/3\mathbb{Z}$ (see [RV01, Proposition 2.1]) and so $[\mathrm{GL}_2(2) : \rho_{E,2}(G_\mathbb{Q})]$ is even. Otherwise, then $\mathbb{Q}(\sqrt{\Delta_E})/\mathbb{Q}$ is a non-trivial abelian extension and so there is $n \geq 1$ such that $\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(\zeta_{2n})$. Thus $\mathbb{Q}(E[2]) \cap \mathbb{Q}(\zeta_{2n})/\mathbb{Q}$ is quadratic. In this case, the restriction morphism

$$\mathrm{Gal}(\mathbb{Q}(E[2n])/\mathbb{Q}(\zeta_{2n})) \to \mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$$

has image $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}(\sqrt{\Delta_E})$, which has index 2 in $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$. Therefore, Proposition 2.13 implies that the image of the natural map

$$\mathrm{SL}_2(2n) \cap \rho_{E,2n}(G_\mathbb{Q}) \to \rho_{E,2}(G_\mathbb{Q})$$

has even index in $\rho_{E,2}(G_\mathbb{Q})$, and so in $\mathrm{GL}_2(2)$. It follows that $\rho_{E,2n}(G_\mathbb{Q})$ has even index in $\mathrm{GL}_2(2n)$. To conclude, we use Proposition 3.14. □

Serre entanglements over $\mathbb{Q}$ are related to the Kronecker-Weber theorem, which is specific to $F = \mathbb{Q}$. For a number field $F \neq \mathbb{Q}$, there are two cases. If $F \cap \mathbb{Q}^{\text{cyc}} = F \cap \mathbb{Q}(\zeta_m) \neq \mathbb{Q}$, then $\rho_{E,m}$, and so ρ_E, cannot be surjective, by the Weil pairing. Otherwise, it can be. This has been proved by Aaron Greicius, who gives necessary and sufficient conditions for the surjectivity of ρ_E, and an example of an elliptic curve with surjective adelic Galois representation.

Theorem 3.17 ([Gre10, Theorem 1.1]). *Let E/F be an elliptic curve. The representation ρ_E is surjective if and only if*

1. *ρ_{E,p^∞} is surjective for all primes p,*
2. *$F \cap \mathbb{Q}^{\text{cyc}} = \mathbb{Q}$, and*
3. *$\sqrt{\Delta_E} \notin F^{\text{cyc}}$.*

Theorem 3.18 ([Gre10, Theorem 1.5]). *Let $F = \mathbb{Q}(\alpha)$ where α is the real root of x^3+x+1. Let E/F be the elliptic curve defined by*

$$E : y^2 + 2xy + \alpha y = x^3 - x^2.$$

Then ρ_E is surjective.

In fact, if $F \cap \mathbb{Q}^{\text{cyc}} = \mathbb{Q}$ and $F \neq \mathbb{Q}$, almost all elliptic curves defined over F have surjective adelic Galois representations:

Theorem 3.19 ([Zyw10, Theorem 1.2]). *Suppose that $F \cap \mathbb{Q}^{\text{cyc}} = \mathbb{Q}$ and $F \neq \mathbb{Q}$. Let $||\cdot||$ be a norm on $\mathbb{R} \otimes_{\mathbb{Z}} \mathcal{O}_F^2$ and, for $(A,B) \in \mathcal{O}_F^2$, $\Delta_{A,B}$ be the discriminant of the elliptic curve $E(A,B)$ with Weierstrass equation $y^2 = x^3 + Ax + B$. We set*

$$B_F(X) = \{(A,B) \in \mathcal{O}_F^2 \mid \Delta_{A,B} \neq 0, ||(a,b)|| \leq X\}.$$

Then

$$\lim_{X\to\infty} \frac{\#\left\{(A,B) \in B_F(X) \mid \rho_{E(A,B)}(G_F) = \mathrm{GL}_2(\hat{\mathbb{Z}})\right\}}{\#B_F(X)} = 1.$$

Also, if $F \cap \mathbb{Q}^{\text{cyc}} \neq \mathbb{Q}$, then $F \cap \mathbb{Q}(\zeta_m) \neq \mathbb{Q}$ for some m and $\rho_{E,m}$, and ρ_E, cannot be surjective. However the image can be maximal. Even more, for $F \cap \mathbb{Q}^{\text{cyc}} \neq \mathbb{Q}$, the proportion of elliptic curves defined over $\mathbb{Q}$ with maximal image quickly approach 1:

Theorem 3.20 ([Zyw10, Theorem 1.3]). *Suppose that $F \neq \mathbb{Q}$. Let $||\cdot||$ and $B_F(X)$ be as in Theorem 3.19. Then there is an effective constant C, depending only on F and on $||\cdot||$, such that*

$$\frac{\#\left\{(A,B) \in B_F(X) \mid \rho_{E(A,B)}(G_F) = \mathcal{G}_F\right\}}{\#B_F(X)} \leq C\frac{\log X}{\sqrt{X}}.$$

In particular, almost elliptic curves E/F do not have any entanglement.

If $F \neq \mathbb{Q}$, the adelic index is equal to 1 for almost elliptic curves. If $F = \mathbb{Q}$, the adelic index is even.

Definition 3.21 ([Jon10]). Let $E/\mathbb{Q}$ be an elliptic curve. If $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})] = 2$, we say that $E/\mathbb{Q}$ is a *Serre curve.*

Example 3.22. The elliptic curve of Example 3.12 with LMFDB label 53.a1 has adelic index 2: it has surjective p-adic representation at all primes p and an entanglement of degree 2, due to the Serre entanglement.

Theorem 3.23 ([Jon10, Theorem 4])**.** *If we order the elliptic curves by their naive height, the proportion of Serre curves is* 1*.*

In other words, in terms of density, almost all elliptic curves defined over $\mathbb{Q}$ are Serre curves. Jones [Jon10, Lemma 5] first gives a sufficient condition for an elliptic curve to be a Serre curve, and later, with Brau, a necessary and sufficient condition:

Theorem 3.24 ([BJ16, Theorem 1.6])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then E is a Serre curve if and only if*

- *E has no exceptional primes,*
- *$\mathbb{Q}(E[2]) \not\subseteq \mathbb{Q}(E[3])$, and*
- *$\rho_{E,4}$ and $\rho_{E,9}$ are surjective.*[1]

If $E/\mathbb{Q}$ is a Serre curve, then E/F has an entanglement of index 2 due to the Serre entanglement, and all other entanglements are derived from this one.

Example 3.25. The elliptic curve $E : y^2 = x^3 - 36x + 84$ with LMFDB label 1944.c1 has maximal p-adic Galois representation for all primes p but it is not a Serre curve since it satisfies $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$. The adelic index of ρ_E is 24.

For elliptic curve with CM, the index of $\rho_E(G_{\mathbb{Q}})$ in $\mathcal{G}(E/\mathbb{Q})$ is also 2 most of the time:

Theorem 3.26 ([DLRM23, Theorem D])**.** *Among the thirteen isomorphism classes over $\overline{\mathbb{Q}}$ of elliptic curves $E/\mathbb{Q}$ with CM, ten are such that, for a good choice of a basis for E_{tors}, the index of $\rho_E(G_F)$ in $N_{\delta,\phi}(\hat{\mathbb{Z}})$ is* 2*.*

Theorem 3.27 ([CP22b])**.** *Let $E/\mathbb{Q}$ be a CM elliptic curve. Then we have*

$$[\mathcal{G}(E/\mathbb{Q}) : \rho_E(G_F)] = \begin{cases} 2 & \textit{if } j(E) \neq 0, 1728, \\ 4 & \textit{if } j(E) = 1728, \\ 6 & \textit{if } j(E) = 0. \end{cases}$$

We just discussed about the minimal possible adelic index, now we turn to upper bounds for this index.

Theorem 3.28 ([Lom15, Corollary 9.3])**.** *Let E/F be a non-CM elliptic curve. The index of the image of ρ_E in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is bounded by*

$$\exp(10^{21483}) \cdot [F : \mathbb{Q}]^{2.4 \cdot 10^{10}} \cdot \max\{1, h(E), \log[F : \mathbb{Q}]\}^{4.8 \cdot 10^{10}}$$

where $h(E)$ is the stable Faltings height of E.

For an elliptic curve E/F with CM by the order $\mathcal{O}$, Lozano-Robledo proved that the index of $\rho_E(G_{\mathbb{Q}(j(E))})$ in $N_{\delta,\phi}(\hat{\mathbb{Z}})$ is a divisor of $|\mathcal{O}^*|$, see [LR22, Theorem 1.2.(1)]. Campagna and Pengo give a formula for the index of $\rho_E(G_F)$ in $\mathcal{G}(E/F)$, valid over every number field F, see [CP22b, Theorem 1.1].

Recently, Zywina classified the possibilities for the index of $\rho_E(G_F)$ in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ for $F = \mathbb{Q}$.

[1] The formulation of Theorem 3.24 is given in [Dan15, Theorem 1.8]. Originally, the second and third points correspond to $j(E) \notin j(X'(4)(\mathbb{Q})) \cup j(X''(4)(\mathbb{Q})) \cup j(X'(9)(\mathbb{Q})) \cup X'(6)$ where $X'(4)$, $X''(4)$, $X'(9)$ and $X'(6)$ are modular curves defined in [BJ16, (14)]

Theorem 3.29 ([Zyw22b, Theorem 1.3]). *There exists a completely determined finite list I (38 elements) such that, for all c, there exists a finite set J_c such that, for all elliptic curve $E/\mathbb{Q}$ such that $j(E) \notin J_c$ and $\rho_{E,p}$ surjective for all $p \geq c$, the index of $\rho_E(G_\mathbb{Q})$ in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ belongs to I.*

The set J_c is not explicit. Very recently, he gives a substantially better bound than that of Lombardo:

Theorem 3.30 ([Zyw24b, Theorem 1.2]). *There is a finite set $J_F \subseteq F$ such that for any non-CM elliptic curve E/F with $j(E) \notin J_F$ and $\rho_{E,p}$ maximal for all primes $p > 19$, we have*

$$[\mathrm{SL}_2(\hat{\mathbb{Z}}) : \rho_E(G_F) \cap \mathrm{SL}_2(\hat{\mathbb{Z}})] \leq \begin{cases} 1382400, & \\ 677376 & \text{if } K \subseteq \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}), \\ 172800 & \text{if } K \cap \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}, \\ 30000 & \text{if } K \cap \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}) \neq \mathbb{Q}, \\ 7200 & \text{if } K \cap \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}) = \mathbb{Q}, \\ 1536 & \text{if } K = \mathbb{Q}. \end{cases}$$

Zywina [Zyw24a] gives an algorithm to compute $\rho_E(G_\mathbb{Q})$ for elliptic curve over $\mathbb{Q}$[2]. Recently, in [Zyw24b], he has studied the question for general number fields. The failure of the Kronecker-Weber theorem is, again, the main change between $F = \mathbb{Q}$ and $F \neq \mathbb{Q}$.

3.3 Radical of the adelic level

Let E/F be an elliptic curve with $K \subseteq \mathbb{Q}(j(E))$ if E has CM by the imaginary quadratic field K. The non-surjectivity of ρ_E in $\mathcal{G}_F$, if E/F does not have CM, and in $\mathcal{G}(E/F)$, if E/F has CM by K with $K \subseteq \mathbb{Q}(j(E))$, is due to two phenomena:

- **Vertical entanglement**: The non-maximality of ρ_{E,p^∞} for some primes p,
- **Horizontal entanglement**: The non-surjectivity of ρ_E on $\prod_{p\in\mathcal{P}} \rho_{E,p^\infty}(G_F)$.

The morphism $\rho_E(G_F) \to \prod_{p\in\mathcal{P}} \rho_{E,p^\infty}(G_F)$ is equivalent to the morphism

$$\mathrm{Gal}(F(E_{\mathrm{tors}})/F) \to \prod_{p\in\mathcal{P}} \mathrm{Gal}(F(E[p^\infty])/F).$$

Proposition 1.20 is about sets $S \subseteq \mathcal{P}$ such that, for all $q \notin S$,

$$F(E[q^\infty]) \cap \left(\prod_{p\in\mathcal{P}\setminus\{q\}} F(E[p^\infty]) \right) = F.$$

Equivalently, we have an isomorphism

$$\mathrm{Gal}(F(E_{\mathrm{tors}})/F) \simeq \mathrm{Gal}(F(E[S^\infty])/F) \times \prod_{p\in\mathcal{P}\setminus S} \mathrm{Gal}(F(E[p^\infty])/F) \tag{3.2}$$

[2] The adelic Galois images data in LMFDB was computed using the algorithm given by [Zyw24a]. For now, their is no data implemented for adelic level of elliptic curves defined over number fields.

where $F(E[S^\infty]) = \prod_{p\in S} F(E[p^\infty])$. From Serre's open image theorem, such a finite set S exists for non-CM elliptic curves, see Proposition 3.14 and Remark 3.5. Campagna and Pengo [CP22a] show that this is also the case for CM elliptic curve. Let S_E be the smallest set S satisfying the isomorphism (3.2). By construction of S_E and definition of M_E, it follows that:

Proposition 3.31. *Let E/F be a non-CM elliptic curve. The primes p such that $\rho_{E,p^\infty}(G_F)$ is non-maximal divides M_E. The other prime divisors of M_E are in S_E.*

Remark 3.32. If $F \cap \mathbb{Q}^{\text{cyc}} = \mathbb{Q}$, then any prime of S_E divides M_E.

Example 3.33. The elliptic curve with LMFDB label 26.b1 has $\Delta_{\text{sf}}(E) = -2\cdot 13$, and so a $(8, 13)$-entanglement. The adelic index is 96 and the index $[\text{GL}_2(7) : \rho_{E,7}(G_\mathbb{Q})]$ is 48. Hence the $(8, 13)$-entanglement has index 2 and all other entanglements are derived from this one, so $S_E = \{2, 13\}$. The adelic level of ρ_E is $M_E = 2^3 \cdot 7 \cdot 13$.

For all $q \in S_E$, we have:

$$F(E[q^\infty]) \cap \left(\prod_{p\in S_E\setminus\{q\}} F(E[p^\infty]) \right) \neq F.$$

In particular, for all $q \in S_E$, the elliptic curve E/F has a (q^k, m)-entanglement for some $k \geq 1$ and some positive integers m with prime divisors in S_E.

Remark 3.34. The previous assumption implies that to study the entanglement of an elliptic curve, it suffices to deal with (p^k, m)-entanglement for p a prime and m a positive integer prime to p. However, we cannot reduce the question of entanglement only to the study of (p^k, q^r)-entanglement for p, q primes. For example, the elliptic curve with LMFDB label 6350400.xr1 has a $(7, 4680)$-entanglement, but for m strictly dividing 4680, we have

$$[\text{GL}_2(7m) : \rho_{E,7m}(G_F)] = [\text{GL}_2(7) : \rho_{E,7}(G_F)] \cdot [\text{GL}_2(m) : \rho_{E,m}(G_F)]$$

and so

$$\rho_{E,7m}(G_F) \simeq \rho_{E,7}(G_F) \times \rho_{E,m}(G_F)$$

i.e. $E/\mathbb{Q}$ does not have a $(7, m)$-entanglement.

In [CS23] and [CP22a], Campagna, Pengo and Stevenhagen determined a set S satisfying (3.2), depending on whether E/F has CM or not. Suppose that $\text{End}(E) \subseteq F$, hypothesis that is automatically satisfied if E/F does not have CM, otherwise it means that $K \subseteq F$ if E/F has CM by K. Let $\mathfrak{f}_E$ be the ideal conductor of E and $\text{N}(\mathfrak{f}_E)$ be its norm over $\mathbb{Q}$.

Theorem 3.35 ([CS23, Theorem 3.2])**.** *If E/F does not have CM, then S_E is contained in the set of the primes p satisfying at least one of the two following conditions:*

- $p \mid 2\cdot 3\cdot 5\cdot \Delta_F \cdot \text{N}(\mathfrak{f}_E)$,
- $\rho_{E,p}$ *is not surjective.*

In the CM case, Campagna and Pengo also determined such a set S.

Theorem 3.36 ([CP22a, Theorem 1.1])**.** *If E/F has CM by $\mathcal{O}$, an order in K, the set S_E is contained in the set of primes dividing $[\mathcal{O}_K : \mathcal{O}] \cdot \Delta_F \cdot \text{N}(\mathfrak{f}_E)$.*

The previous theorem is optimal in the following sense: there exist elliptic curves E/F such that S_E is *exactly* the set of primes dividing $[\mathcal{O}_K : \mathcal{O}] \cdot \Delta_F \cdot \mathrm{N}(\mathfrak{f}_E)$, see [CP22a, Remark 6.4].

Definition 3.37. We say that an integer m is *minimal exceptional* for E if $\rho_{E,m}$ is not surjective and $\rho_{E,a}$ is surjective for all $a \mid m$.

In particular, every minimal exceptional integer divides M_E. If E/F does not have CM, then it has a finite number of minimal exceptional integer. Jones gives a statement about the set of minimal exceptional integers for elliptic curves defined over $\mathbb{Q}$. For a square-free number W, he defines the *Serre number*:

$$M_W = \begin{cases} 2|W| & \text{if } W \equiv 1 \pmod 4 \\ 4|W| & \text{otherwise.} \end{cases}$$

Lemma 3.38 ([Jon10, Lemma 20])**.** *Let $E/\mathbb{Q}$ be an elliptic curve and suppose that m is minimal exceptional for E, then*

$$m \in \mathcal{P} \cup \{M_{\Delta_{\mathrm{sf}}(E)}\} \cup \{4, 8, 9\}.$$

If 8 *is minimal exceptionel for E, then* $[\mathrm{GL}_2(8) : \rho_{E,8}(G_{\mathbb{Q}})] = 2$.

In other words, for $E/\mathbb{Q}$ and m composite, $\rho_{E,m}$ is not surjective if only if m is divisible by $M_{\Delta_{\mathrm{sf}}(E)}$ or a prime p such that ρ_{E,p^∞} is not surjective.

Example 3.39. The elliptic curve with LMFDB label 11.a1 has minimal discriminant $\Delta_E = -11$. Then $M_{\Delta_{fs}(E)} = 2 \cdot 11$. By Lemma 3.38, we know that the minimal exceptional integers are in $\mathcal{P} \cup \{22\} \cup \{4, 8, 9\}$. In fact, the minimal exceptional integers are 5 and 22. The adelic level of ρ_E is $550 = 2 \cdot 5^2 \cdot 11$.

Example 3.40. Let $E/\mathbb{Q}$ be the elliptic curve with LMFDB label 6350400.xr1. The minimal exceptional integers for $E/\mathbb{Q}$ are 10 and 13. The adelic level of ρ_E is $32760 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$.

Theorem 3.41. *If $E/\mathbb{Q}$ is a Serre curve, then the only minimal exceptional integer of E is $M_{\Delta_{\mathrm{sf}}(E)}$. Moreover, $M_E = M_{\Delta_{\mathrm{sf}}(E)}$ and*

$$S_E = \{2\} \cup \{\textit{prime divisors of } \Delta_{\mathrm{sf}}(E)\}.$$

Proof. By Theorem 3.24, the prime numbers and 4 are not minimal exceptional for $E/\mathbb{Q}$. In particular, $E/\mathbb{Q}$ has a Serre entanglement. If $\Delta_{\mathrm{sf}}(E) = \pm 2$ then $\rho_{E,8}(G_F)$ is non maximal and so 8 is minimal exceptional. Otherwise, $E/\mathbb{Q}$ has a $(2, |\Delta_{\mathrm{sf}}(E)|)$-entanglement if $\Delta_{\mathrm{sf}}(E) \equiv 1 \pmod 4$, a $(4, |\Delta_{\mathrm{sf}}(E)|)$-entanglement if $\Delta_{\mathrm{sf}}(E) \equiv -1 \pmod 4$ and a $\left(8, \frac{|\Delta_{\mathrm{sf}}(E))|}{2}\right)$-entanglement if $\Delta_{\mathrm{sf}}(E) \equiv \pm 2 \pmod 4$, by Theorem 3.8. In any case, $M_{\Delta_{\mathrm{sf}}(E)}$ is minimal exceptional for E. But

$$[\mathrm{GL}_2(M_{\Delta_{\mathrm{sf}}(E)}) : \rho_{E,M_{\Delta_{\mathrm{sf}}(E)}}(G_F)] \mid [\mathrm{GL}_2(\hat{\mathbb{Z}}) : \rho_E(G_F)]$$

and E is a Serre curve. Therefore

$$[\mathrm{GL}_2(M_{\Delta_{\mathrm{sf}}(E)}) : \rho_{E,M_{\Delta_{\mathrm{sf}}(E)}}(G_F)] = [\mathrm{GL}_2(\hat{\mathbb{Z}}) : \rho_E(G_F)] = 2.$$

This proves that $M_E = M_{\Delta_{\mathrm{sf}}(E)}$, in particular there is no other minimal exceptional integers. □

Remark 3.42. The previous lemma implies that the p-adic depth of a Serre curve is 0 for all odd prime p, and 0 or 3 for $p = 2$.

Example 3.43. The Serre curve $E/\mathbb{Q}$ with LMFDB label 37.a1 has $\Delta_E = 37 \equiv 1 \pmod 4$, and so $M_{\Delta_E} = 2 \cdot 37 = 74$. Then, by previous theorem, $S_3 = \{2, 37\}$ and the adelic level is $M_E = 74$.

3.4 Types of entanglement

In Section 3.1, we have described the Serre entanglement. In this section, we present results about other possible entanglements. For m a positive integer, we set $F_m := F(E[m])$. Let a, b two integers with $\gcd(a, b) = d$ and $\mathrm{lcm(a, b)} = m$.

Definition 3.44. We say that we have an (a, b)-*entanglement of type* T if the Galois group of the entanglement field over F_d is isomorphic to T where $d = \gcd(a, b)$, *i.e.*

$$\mathrm{Gal}((F_a \cap F_b)/F_d) \simeq T.$$

Example 3.45. Any Serre curve $E/\mathbb{Q}$ has a $(8, m)$-entanglement of type $\mathbb{Z}/2\mathbb{Z}$, for some odd $m \mid \Delta_{\mathrm{sf}}(E)$.

Example 3.1 was about an elliptic curve $E/\mathbb{Q}$ such that $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$. The conditions for having such inclusion is the topic of an article of Jones and Brau:

Theorem 3.46 ([BJ16, Theorem 1.4] and [JM20, Remark 1.9])**.** *There exists an modular curve $X'(6)$, with j-map $j_6 : X'(6) \to X(1)$, such that, for every elliptic curve $E/\mathbb{Q}$, we have $j(E) \in j_6(\mathbb{Q})) - \{0, 1728\}$ if and only if E is isomorphic over $\overline{\mathbb{Q}}$ to an elliptic curve $E'/\mathbb{Q}$ such that $\rho_{E',2}$ is surjective and $\mathbb{Q}(E'[2]) \subseteq \mathbb{Q}(E'[3])$. The modular curve $X'(6)$ is parametrized by $t : X'(6) \to \mathbb{P}^1$ such that $j = 2^{10}3^3t^3(1 - 4t^3)$.*

In particular, $X'(6)$ parameterizes elliptic curves over $\mathbb{Q}$ with a $(2, 3)$-entanglement of type S_3. The theorem above provides an answer to the following question for $F = \mathbb{Q}$ and $(a, b) = (2, 3)$, set by Brau and Jones:

Question 3.47 ([BJ16, Question 1.1])**.** *Can one classify the triple $(E/F, a, b)$ where E/F is an elliptic curve and a, b coprime integers such that* $\mathrm{Gal}(F_a \cap F_b/F)$ *is non abelian?*

Jones and McMurdy provide an answer to this question when the modular curve X_G has genus 0, where $G := \rho_E(G_F)$.

Theorem 3.48 ([JM20, Theorem 1.7])**.** *Let E/F be an elliptic curve with an (a, b)-entanglement of non-abelian type and G be its adelic image. Suppose that X_G has genus* 0*. Then*

$$(a, b) \in \{(2, 3), (2, 5), (3, 5), (2, 9)\} \quad \textit{and} \quad G \leq G_{ab}$$

where G_6, G_{10}, G_{15} and G_{18} are defined by [JM20, (3)]. Moreover, the modular curve X_{G_6}, $X_{G_{10}}$ and $X_{G_{18}}$ are defined over $\mathbb{Q}$, whereas $X_{G_{15}}$ is defined over $\mathbb{Q}(\sqrt{-15})$.

Remark 3.49. We note that $X'(6) = X_{G_6}$. Indeed, an elliptic curve E/F has a $(2, 3)$-entanglement of non-abelian type if and only if $F(E[2]) \cap F(E[3])/F$ has Galois group S_3 if and only if $\rho_{E,2}$ is surjective and $F(E[2]) \subseteq F(E[3])$.

This gives a classification of entanglements of non-abelian type for elliptic curves defined over the function field $F(t)$:

Theorem 3.50 ([JM20, Theorem 1.8])**.** *Let E be an elliptic curve defined over $F(t)$ and a, b be positive integers. Then $E/F(t)$ has an (a, b)-entanglement of non-abelian type T over $F(t)$ if and only if*

$$T = S_3, \quad (a, b) \in \{(2, 3), (2, 5), (3, 5), (2, 9)\} \quad \textit{and} \quad j_E(t) = j_{ab}(f(t))$$

for some $f(t) \in F(t)$ where j_6, j_{10}, j_{15} and j_{18} are the rational functions defined by [JM20, (5)].

By definition, an elliptic curve E/F has an (a,b)-entanglement if $G = \rho_{E,ab}(G_F)$ does not surjects on the product $G_a \times G_b$ where G_a, respectively G_b, is the image of G in $\mathrm{GL}_2(a)$, respectively in $\mathrm{GL}_2(b)$. Then the question of entanglement can be reformulate as studing which subgroups G of $\mathrm{GL}_2(m)$ does not surject on $G_a \times G_b$. Elliptic curves which have $\rho_{E,m}(G_F) = G$ correspond to rational points on the associated modular curve X_G. The groups G_6, G_{10}, G_{15} and G_{18} of Theorem 3.48 are defined in this way. This approach also has been followed by Morrow, in [Mor19], which gives, for each pair

$$(a,b) \in \{(2,3),(4,3),(8,3),(16,3),(2,5),(2,7),(2,11),(2,13)\},$$

a restriction of the possible subgroups G of $\mathrm{GL}_2(ab)$ such that $E/\mathbb{Q}$ has an (a,b)-entanglement for some elliptic curve $E/\mathbb{Q}$. Moreover, he gives a list of index of these subgroups which occurs for infinitely many $E/\mathbb{Q}$.

As seen in Section 3.2, almost all elliptic curve $E/\mathbb{Q}$ have a Serre entanglement, and so a $(8,m)$-entanglement for some odd m. We observe that this entanglement occurs in $\mathbb{Q}^{\mathrm{ab}}$ since $\mathbb{Q}(E[8]) \cap \mathbb{Q}(E[m]) \cap \mathbb{Q}^{\mathrm{ab}} \neq \mathbb{Q}$. More precisely, it occurs in $\mathbb{Q}(\zeta_m)$. For elliptic curves with CM, the CM field is contained in $F(E[m])$ for all m. In particular, all division fields are entangled, and the entanglement occurs in $\mathbb{Q}^{\mathrm{ab}}$.

Definition 3.51. Let E/F be an elliptic curve and S be a non-trivial abelian group. Let $2 \leq a < b$ be positive integers. We say that E/F has:

1. An *abelian (a,b)-entanglement of type S* if $(F_a \cap F_b \cap F^{ab})/(F_d \cap F^{\mathrm{ab}})$ is non-trivial and has Galois group S.
2. A *Weil (a,b)-entanglement of type S* if $\mathrm{Gal}((F_a \cap F(\zeta_b))/F(\zeta_d))$ or $(F_b \cap F(\zeta_a))/F(\zeta_d)$ is non-trivial with Galois group S.
3. A *$(2,b)$-discriminant entanglement* if, setting $m = \mathrm{lcm}(2,b)$, there exists $G \leq \mathrm{GL}_2(m)$ such that $\rho_{E,b}(G_F) \leq G$ has index 2, and $N_2, N_m \leq \mathrm{GL}_2(m)$ two distinct index 2 subgroups such that
   (a) $G_m \cap N_2 = G_m \cap N_b$ and
   (b) $[\pi(G) : \pi(G_2)] = 2$ where $\pi : \mathrm{GL}_2(m) \to \mathrm{GL}_2(2)$ is the natural reduction map.
4. A *Serre entanglement* if E is defined over $\mathbb{Q}$ and has a Weil $(2, 4|\Delta_E|)$-entanglement of type $\mathbb{Z}/2\mathbb{Z}$.
5. A *fake CM entanglement* if E/F is a non-CM elliptic curve, p is an odd prime, $\rho_{E,p}$ is contained in the normalizer of a Cartan subgroup,
$$\mathrm{Gal}(F_p \cap F^{\mathrm{ab}}/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^*$$
and E/F has an abelian (p,q)-entanglement of type $\mathbb{Z}/2\mathbb{Z}$ where $F_p \cap F_q \simeq F(\sqrt{e})$ or $F(\sqrt{ep^*})$ with $e \neq p^*$ a squarefree integer such that $F(\sqrt{e}) \subseteq F_p$.

Remark 3.52. As said in previous sections, the Serre entanglement is not defined over any number field F, because this phenomena is very specific to $\mathbb{Q}$.

These definitions are introduced by [DLRM23] for $F = \mathbb{Q}$.

Remark 3.53. As we observe with the Serre entanglement, a Weil entanglement is not strictly speeking an entanglement: if $a \mid b$, then $\mathrm{lcm}(a,b) = b$ and $\gcd(a,b) = a$. Then the map

$$\rho_{E,b}(G_{F_a}) \to \rho_{E,a}(G_{F_a}) \times \rho_{E,b}(G_{F_a})$$

is an isomorphism. In particular, E/F does not have an (a,b)-entanglement, and yet a non trivial intersection $F_a \cap F(\zeta_b) \neq F(\zeta_a)$ is possible. We describe the entanglements obtained from abelian, Weil, Serre and fake CM entanglements.

1. If E/F has an abelian (a,b)-entanglement of type S, then it has an (a,b)-entanglement of type T and S is a quotient of T. The group T is not necessarily abelian, as seen Example 3.1.

2. Suppose that E/F has a Weil (a,b)-entanglement of type S. If $\gcd(a,b)=1$, then $E/\mathbb{Q}$ has an (a,b)-entanglement of type T and S is a quotient of T. If $\gcd(a,b)=d$ and $F \neq F(E[a]) \cap F(\zeta_b) \not\subseteq F(E[d])$, then E/F has an (a,b)-entanglement. In particular, if $\gcd(a,b)=2$, then either E/F has an (a,b)-entanglement, or $F(E[a]) \cap F(\zeta_b) = F(E[2]) \cap F^{\mathrm{ab}}$.

3. A Serre entanglement is at the same time a Weil entanglement and a discriminant entanglement.

4. If $E/\mathbb{Q}$ has a Serre entanglement and $\Delta_{\mathrm{sf}}(E) \notin \{-1, \pm 2\}$, then $E/\mathbb{Q}$ has a $(8,m)$-entanglement of type T for some odd m and $\mathbb{Z}/2\mathbb{Z}$ is a quotient of T.

5. If E/F has a fake CM entanglement, then, by definition, it has a (p,q)-entanglement for some primes $p \neq q$.

In [DLRM23, Example 3.5 and 3.6], we see that an abelian entanglement is not necessarily Weil, and a Weil entanglement is not necessarily abelian.

Remark 3.54. Let E/F be a non-CM elliptic curve. Let a,b be integers coprime to 6. If $\rho_{E,a}$ has maximal image, then, by Proposition 4.71, we have $F_a \cap F^{\mathrm{ab}} = F(\zeta_a)$. Therefore, if $\rho_{E,a}$ and $\rho_{E,b}$ have both maximal image, then E/F have a Weil (a,b)-entanglement if and only if F has a cyclotomic (a,b)-entanglement.

The following definition is introduced in [DM22] for $F=\mathbb{Q}$.

Definition 3.55. Let E/F be an elliptic curve with an (a,b)-entanglement. This entanglement is said to be *explained* if E/F has a Weil (a,b)-entanglement, and *unexplained* otherwise.

Results below imply that explained entanglement occurs for infinitely many elliptic curves over $\mathbb{Q}$ and infinitely many pairs (a,b), and even infinitely many pairs (p,q) with p and q primes. Whereas unexplained entanglement occurs only for finitely many pairs of primes (p,q) for elliptic curves over $\mathbb{Q}$.

Example 3.56. The elliptic curve $E: y^2 = x^3 - 36x + 84$ with LMFDB label 1944.c1 has a $(2,3)$-entanglement of non-abelian type S_3 and a $(4,6)$-entanglement of abelian type $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/4\mathbb{Z}$. It also has:

- An abelian $(2,3)$-entanglement of type $\mathbb{Z}/2\mathbb{Z}$ since
$$\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[3]) \cap \mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\sqrt{-3}) \neq \mathbb{Q};$$

- A Weil $(2,3)$-entanglement since $\mathbb{Q}(E[2]) \cap \mathbb{Q}(\zeta_3) = \mathbb{Q}(\zeta_3) \neq \mathbb{Q}$, which gives also a Serre entanglement: $\mathbb{Q}(E[2]) \cap \mathbb{Q}(\zeta_{4\times 3}) = \mathbb{Q}(\zeta_3)$.

The second point show that the $(2,3)$-entanglement is explained. However, we see that the Weil pairing explains that $\mathbb{Z}/2\mathbb{Z} \leq \mathrm{Gal}(\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[3])/\mathbb{Q})$ but not that this Galois group is all S_3. On the other hand, the $(4,6)$-entanglement is explained if and only if $\mathbb{Q}(i) \subseteq \mathbb{Q}(E[3])$.

Example 3.57. The elliptic curve with LMFDB label 11.a1 has minimal discriminant $\Delta_E = -11$ and it has surjective image for all primes except 5. It has a $(25, 11)$-entanglement of abelian type $\mathbb{Z}/5\mathbb{Z}$ and a $(2, 11)$-entanglement of abelian type $\mathbb{Z}/2\mathbb{Z}$. It also has:

1. An abelian $(25, 11)$-entanglement of type $\mathbb{Z}/5\mathbb{Z}$ and a $(2, 11)$-entanglement of type $\mathbb{Z}/2\mathbb{Z}$;

2. A Weil $(25, 11)$-entanglement: since $\rho_{E,11}$ is surjective, then $\mathbb{Q}(E[11]) \cap \mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\zeta_{11})$ by Proposition 4.71 and so
$$\mathrm{Gal}(\mathbb{Q}(E[25]) \cap \mathbb{Q}(\zeta_{11})/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(E[25]) \cap \mathbb{Q}(E[11]) \cap \mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z};$$

3. A Serre entanglement since $\mathbb{Q}(E[2]) \cap \mathbb{Q}(\zeta_{4\times 11}) = \mathbb{Q}(\sqrt{-11})$.

In particular, the $(2, 11)$-entanglement is explained. The $(25, 11)$-entanglement is explained if and only if the unique quintic subextension of $\mathbb{Q}(\zeta_{25})$ is in $\mathbb{Q}(E[11])$ or the unique quintic subextension of $\mathbb{Q}(\zeta_{11})$ is in $\mathbb{Q}(E[25])$.

Remark 3.58. The definition of Weil entanglement encompasses also vertical entanglements: an elliptic curve E/F has a Weil (p^k, p^{k+1})-entanglement if the extension $F(E[p^k]) \cap F(\zeta_{p^{k+1}})/F(\zeta_{p^k})$ is non-trivial, which is equivalent to have the inclusions
$$F(\zeta_{p^k}) \subsetneq F(\zeta_{p^{k+1}}) \subseteq F(E[p^k]).$$
If $F \cap \mathbb{Q}(\zeta_{p^{k+1}}) = \mathbb{Q}$ and $p \geq 3$, this never happens by Theorem 4.38. However, the elliptic curve $E : y^2 = x^3 - 11x - 14$ with LMFDB label 32.a1 satisfies $\mathbb{Q}(\zeta_{2^{k+1}}) \subseteq \mathbb{Q}(E[2^k])$ for all $k \geq 1$, see [DLR23, Theorem 1.5]. Jones [Jon23, Theorem 1.1] proves that this is the case for all elliptic curves $E/\mathbb{Q}$ with CM by an order of an imaginary quadratic field K with conductor f such that $\Delta_K f^2$ is even. In particular, these elliptic curves have a $(2^k, 2^{k+1})$-entanglement of Weil type for all $k \geq 1$.

In the case where the extension $\mathbb{Q}(E[p])/\mathbb{Q}$ is abelian, a theorem of Lozano-Robledo provides constraints for the possible type of Weil (p, q^k)-entanglement, for $p < q$ primes:

Theorem 3.59 ([DLR23, Theorem 1.8.(2)]). *Let $E/\mathbb{Q}$ be an elliptic curve and let $p < q$ be prime integers. If $\mathbb{Q}(E[p])/\mathbb{Q}$ is abelian, then $\mathbb{Q}(E[p]) \cap \mathbb{Q}(\zeta_{q^k})$ can be trivial, quadratic, cyclic cubic (for $p = 2$) or cyclic quartic (for $p = 5$).*

The following theorem shows that there is infinitely many isomorphism classes of elliptic curves over $\mathbb{Q}$ with Weil entanglement which are not Serre.

Theorem 3.60 ([DLRM23, Theorem C]). *Each of the following conditions is satisfied by infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over $\mathbb{Q}$:*

1. *a Weil $(3, n)$-entanglement of type $\mathbb{Z}/2\mathbb{Z}$ where $3 \nmid n$,*

2. *a Weil $(5, n)$-entanglement of type $\mathbb{Z}/4\mathbb{Z}$ where $5 \nmid n$,*

3. *a Weil $(7, n)$-entanglement of type $\mathbb{Z}/6\mathbb{Z}$ where $7 \nmid n$,*

4. *a Weil (m, n)-entanglement of type $\mathbb{Z}/2\mathbb{Z}$ where $n \geq 3$, $m \in \{4, 6, 9\}$ and $\gcd(m, n) \leq 2$,*

5. *a Weil $(m, \gcd(4|\Delta_E|, n))$-entanglement of type $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ where $n \geq 3$, $m \in \{8, 10, 12\}$ and $\gcd(m, n) \leq 2$.*

Remark 3.61. Any Weil (a,b)-entanglement of first three points gives rise to an (a,b)-entanglement since $\gcd(a,b)=1$. This is also the case for the last point since the $\gcd(a,b)$ is at most 2 and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ is not a subgroup of $\mathrm{GL}_2(2)$. Let m,n be as in the fourth point. Suppose that $\gcd(m,n)=2$ and that $\mathbb{Q}(E[m])\cap\mathbb{Q}(\zeta_n)=\mathbb{Q}(\sqrt{\Delta_E})$ or $\mathbb{Q}(E[n])\cap\mathbb{Q}(\zeta_m)=\mathbb{Q}(\sqrt{\Delta_E})$, then $E/\mathbb{Q}$ has a Serre entanglement, which gives rise to an $(8,b)$-entanglement for some odd $b\mid\Delta_{\mathrm{sf}}(E)$. Otherwise, $E/\mathbb{Q}$ has an (m,n)-entanglement.

In particular, for $p=3,5,7$ and for all primes $q\neq p$, there are infinitely many elliptic curves defined over $\mathbb{Q}$ with a (p,q)-entanglement. In fact, Daniels and Morrow showed that most of entanglements follow from Weil entanglements: there are infinitely many elliptic curves defined over $\mathbb{Q}$ with a unexplained (p,q)-entanglement of type T only for $(p,q)=(2,3),(2,5),(2,7),(2,13)$ and $(3,5)$ and $T\simeq\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/3\mathbb{Z}$ or S_3. They used a theorem of the first author and Lozano-Robledo, on the extension $\mathbb{Q}(E[p])\cap\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}$ for any prime p, obtained by studying the derived group of $\rho_{E,p}(G_{\mathbb{Q}})$ and by using the classification of subgroups of $\mathrm{GL}_2(p)$. We partially use this method in Section 4.6.

Theorem 3.62 ([DLR23, Theorem 1.7]). *Let $E/\mathbb{Q}$ be an elliptic curve and let $p<q$ be distinct primes.*

1. *The Galois group of $\mathbb{Q}(E[p])\cap\mathbb{Q}^{\mathrm{ab}}$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*\times C$ where C is a cyclic group of order dividing $p-1$.*

2. *Further, if $\rho_E(G_{\mathbb{Q}})$ is not contained in a Borel subgroup, then $\mathbb{Q}(E[p])\cap\mathbb{Q}^{\mathrm{ab}}=L(\zeta_p)$ with $L/\mathbb{Q}$ trivial or quadratic. If $\rho_{E,p}(G_{\mathbb{Q}})$ is exceptional or maximal, then L is trivial.*

3. *In particular, if $\mathbb{Q}(\zeta_{q^k})\subset\mathbb{Q}(E[p])$, then $\mathbb{Q}(E[p])=\mathbb{Q}$, $\mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_3)$, or $\rho_{E,p}(G_{\mathbb{Q}})$ is contained in a Borel subgroup, $p=2,3,5,7,11,13,17,19,37,43,67$ or 163 and $\varphi(q^n)$ divides $p-1$.*

Remark 3.63. Assuming the Serre's uniformity bound, then $\rho_{E,p}(G_{\mathbb{Q}})$ is not contained in a Borel subgroup for any $p\geq 41$.

Theorem 3.64 ([DM22, Theorem A and Section 8]). *There are exactly 9 pairs $((p,q),T)$ with $p<q$ distinct primes and T a finite group such that infinitely many $E/\mathbb{Q}$ has an unexplained (p,q)-entanglement of type T, and they have completely classified these families. The list of the 9 pairs is the following*

$$((2,3),\mathbb{Z}/2\mathbb{Z}),\quad ((2,3),\mathbb{Z}/3\mathbb{Z}),\quad ((2,3),S_3),$$
$$((2,5),\mathbb{Z}/2\mathbb{Z}),\quad ((2,5),\mathbb{Z}/3\mathbb{Z}),\quad ((2,5),S_3),$$
$$((2,7),\mathbb{Z}/2\mathbb{Z}),\quad ((2,7),\mathbb{Z}/3\mathbb{Z}),\quad ((2,13),\mathbb{Z}/2\mathbb{Z}),\quad ((3,5),\mathbb{Z}/2\mathbb{Z})$$

Remark 3.65. For each pair $((p,q),T)$ in the theorem, any elliptic curve having an unexplained (p,q)-entanglement of type T has also a (p,q)-entanglement of type S, where $S\in\{\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/3\mathbb{Z}\}$ is a quotient of T.

Remark 3.66. The pairs $((2,p),\mathbb{Z}/3\mathbb{Z})$ and $((2,p),S_3)$ with $p=3,5,7$ correspond to having the inclusion $\mathbb{Q}(E[2])\subseteq\mathbb{Q}(E[p])$. In the first case, the discriminant is a square and $\rho_{E,2}(G_{\mathbb{Q}})\simeq\mathbb{Z}/3\mathbb{Z}$. In the second case, $\rho_{E,2}$ is surjective and $\mathbb{Q}(\sqrt{\Delta_E})\subseteq\mathbb{Q}(E[p])$. Since the entanglement in unexplained, we have

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

In particular, the squarefree part of Δ_E is not p^*.

The year after, together with Lozano-Robledo, they refine the previous theorem, assuming the Serre's uniformity bound: they classify the elliptic curves $E/\mathbb{Q}$ having an abelian (p,q)-entanglement of type S, with $p<q$ primes, which is not explained, CM or fake CM.

Theorem 3.67 ([DLRM23, Theorem A])**.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve and $p<q$ be primes. There is a finite set $J \subseteq \mathbb{Q}$ such that, if $j(E) \notin J$ and $E/\mathbb{Q}$ has an abelian entanglement of type S which is not Weil, discriminant or fake CM, then*

$$((p,q),S) = ((2,7),\mathbb{Z}/3\mathbb{Z}).$$

Corollary 3.68 ([DLRM23, Corollary B])**.** *Let $E/\mathbb{Q}$ be a non-CM elliptic curve and $p<q$ be primes. Assume a positive answer to Serre's uniformity bound. There is a finite set $J' \subseteq \mathbb{Q}$ such that, if $j(E) \notin J'$ and $E/\mathbb{Q}$ has an abelian (p,q)-entanglement of type S which is not Weil, then*

$$\begin{aligned}((p,q),S) \in \{\,&((2,3),\mathbb{Z}/2\mathbb{Z})\,,((2,5),\mathbb{Z}/2\mathbb{Z})\,,((2,7),\mathbb{Z}/2\mathbb{Z}),\\ &((2,7),\mathbb{Z}/3\mathbb{Z}),((2,13),\mathbb{Z}/2\mathbb{Z}),((3,5),\mathbb{Z}/2\mathbb{Z})\}\end{aligned}$$

The general method for the results of this section is finding an appropriate subgroup G of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ with the desired property, computing the j-line of the associated modular curve X_G, and finding the rational points on this curve and parametric families of elliptic curves E/F with $j(E) \in j(X_G(F))$.

Chapter 4

Coincidence of division fields

We focus on an extreme case of entanglement: the coincidence of two divsion fields. This chapter corresponds in major part to a preprint of the author: available on arXiv [Yvo24].

4.1 Coincidence: definition and approach

For m a positive integer, we set $F_m := F(E[m])$. Let a, b two integers with $\gcd(a,b) = d$ and $\mathrm{lcm(a,b)} = m$.

If $p \geq 5$ and $\rho_{E,p}$ is surjective, then ρ_{E,p^∞} is surjective by Theorem 2.32. Nevertheless, if $\rho_{E,p}$ is not surjective, then we cannot immediately deduce the image of ρ_{E,p^∞} from the image of $\rho_{E,p}$. This image can be the full inverse image of $\rho_{E,p}(G_F)$ in $\mathrm{GL}_2(\mathbb{Z}_p)$, which is equivalent to having

$$[\mathrm{GL}_2(p^k) : \rho_{E,p^k}(G_F)] = [\mathrm{GL}_2(p^{k+1}) : \rho_{E,p^{k+1}}(G_F)],$$

i.e.

$$\mathrm{Gal}(F_{p^{k+1}}/F_{p^k}) \simeq (\mathbb{Z}/p\mathbb{Z})^4$$

for all $k \geq 1$, from 4.2, but it can be smaller.
On the other hand, in the previous chapter on entanglement, we saw that an horizontal entanglement is equivalent to a non trivial intersection

$$F_a \cap F_b \neq F_d.$$

In this chapter, we focus on the case of a coincidence, that is the extreme case of both previous statements.

Definition 4.1. We say that an elliptic curve E/F has an (a,b)-*coincidence* if one of the following equivalent conditions is satisfies:

1. The map $\phi_{a,b}$ introduced in Section 3.1 induces an isomorphism

$$\rho_{E,m}(G_F) \simeq \rho_{E,a}(G_F) \simeq \rho_{E,b}(G_F).$$

2. The equality $F_a = F_b$ holds.

We immediately see that E/F does not have an (a,b)-coincidence if the representations mod a and mod b are both surjective, since $\mathrm{GL}_2(a)$ is never isomorphic to $\mathrm{GL}_2(b)$ for $a \neq b$. In particular, if $\rho_{E,a}$ and $\rho_{E,b}$ are surjective, then E/F can have an (a,b)-entanglement as Example 3.1 shows but not an (a,b)-coincidence. However, this counter-example provides an example of a $(3,6)$-coincidence.

Example 4.2. Let $E/\mathbb{Q}$ be the elliptic curve of Example 3.1 given by the equation

$$y^2 = x^3 - 36x + 84.$$

It satisfies

$$\rho_{E,6}(G_F) \simeq \rho_{E,3}(G_F) \not\simeq \rho_{E,2}(G_F),$$

and, equivalently,

$$\mathbb{Q}(E[2]) \subsetneq \mathbb{Q}(E[3]) = \mathbb{Q}(E[6]).$$

If a coincidence $F_a = F_b$ holds, then, since $F_m = F_a F_b$, it remains true replacing b by m. Thus, to obtain constraints on coincidences, it suffices to consider a dividing b. Furthermore, we can reduce to the question of whether $F_a = F_{p^k a}$ for a prime p and $k \geq 1$. Moreover, considering a set S satisfying the isomorphism (3.2), and using Lemma 4.12, it suffices to consider a with only prime divisors in $S \cup \{p\}$. Then, we consider the following guiding question:

Question 4.3. *Let p be a prime, $k \geq 1$ and m be an integer with only prime divisors in $S \cup \{p\}$. When do we have $F(E[m]) = F(E[p^k m])$?*

We can reformulate this question, considering $p \nmid m$ and the following situations:

- *Horizontal coincidences*
    - $F(E[m]) = F(E[p^k m])$ for some $k \geq 1$
- *Vertical coincidences*
    - $F(E[m]) \neq F(E[pm]) = \cdots = F(E[p^k m])$ for some $k \geq 2$, or
    - $F(E[2m]) \neq F(E[4m]) = \cdots = F(E[2^k m])$ for some $k \geq 3$.

We know by Theorem 4.46 that there are no other cases.

Suppose that E/F has an (a, b)-coincidence. Then it has a *Weil* (a, b)*-coincidence*:

$$F(\zeta_a) \cap F(E[b]) = F(\zeta_a) \quad \text{and} \quad F(\zeta_b) \cap F(E[a]) = F(\zeta_b).$$

In particular E/F has an (a, b)-Weil entanglement. Moreover E/F has an *abelian* (a, b)*-coincidence*:

$$F(E[a]) \cap F^{\mathrm{ab}} = F(E[b]) \cap F^{\mathrm{ab}}.$$

An abelian (a, b)-coincidence is an abelian (a, b)-entanglement if and only if the field $F(E[a]) \cap F^{\mathrm{ab}}$ is not equal to $F(E[d]) \cap F^{\mathrm{ab}}$. Thus, a subquestion of that of coincidence is to know whether Weil coincidences and abelian coincidences occur. This approach has been followed by Daniels and Lozano-Robledo in [DLR23] and will be exploited in this manuscrit, in Section 4.3, 4.4 and 4.5 for the Weil entanglement and in Section 4.6 for the abelian entanglement.

4.2 Coincidence over $\mathbb{Q}$

Stevenhagen asked if elliptic curves over $\mathbb{Q}$ can have a $(2^k, 2^{k+1})$-coincidence and the answer was given by Rouse and Zureick-Brown. Indeed, their classification on 2-adic images for elliptic curves over $\mathbb{Q}$ gives:

Theorem 4.4 ([RZB15, Remark 1.6]). *Let $E/\mathbb{Q}$ be a non-CM elliptic curve. If $E/\mathbb{Q}$ has a $(2^k, 2^{k+1})$-coincidence then $k = 1$ and there exists $t \in \mathbb{Q}$ such that E is $\mathbb{Q}$-isomorphic to $y^2 = x^3 + A(t)x + B(t)$*[1] *where*

$$A(t) = -27t^8 + 648t^7 - 4212t^6 - 2376t^5 + 60102t^4 + 79794t^3 - 105732t^2 - 235224t - 107811,$$

$$\begin{aligned} B(t) = 54t^{12} - 1944t^{11} + 24300t^{10} - 97848t^9 - 251262t^8 + 1722384t^7 + 4821768t^6 \\ -8697456t^5 - 64323558t^4 - 140447736t^3 - 90561240t - 21346578. \end{aligned}$$

Example 4.5. The elliptic curve with LMFDB label 162.d2 with Weierstrass equation

$$E : y^2 + xy + y = x^3 - x^2 + 4x - 1$$

([RZB15, Remark 1.6]) satisfies $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4])$, and the Galois group over $\mathbb{Q}$ of this extension is $\mathrm{GL}_2(2)$. We observe that $\Delta_{\mathrm{sf}}(E) = -1$ gives $\mathbb{Q}(\zeta_4) \subseteq \mathbb{Q}(E[2])$.

Around the same time, Brau and Jones gave a parametrization of elliptic curves $E/\mathbb{Q}$ such that $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[3])$, given in Theorem 3.46, which is equivalent to having a $(3, 6)$-coincidence.

In [DLR23], Daniels and Lozano-Robledo study Weil and abelian coincidences. More precisely, they ask when the inclusion $\mathbb{Q}(\zeta_{p^k}) \subseteq \mathbb{Q}(E[m])$ holds for a prime p and use it to study coincidence. We presented some of their results in Section 3.4, now we focus on what they proved about coincidence. They extend the result of Rouse and Zureick-Brown:

Theorem 4.6 ([DLR23, Theorem 1.4]). *Let $E/\mathbb{Q}$ be an elliptic curve, p be a prime and $k \geq 1$.*

1. *If $\mathbb{Q}(E[p^k]) \cap \mathbb{Q}(\zeta_{p^{k+1}}) = \mathbb{Q}(\zeta_{p^{k+1}})$, then $p = 2$.*
2. *If $\mathbb{Q}(E[p^{k+1}]) = \mathbb{Q}(E[p^k])$, then $(p^k, p^{k+1}) = (2, 4)$ and $E/\mathbb{Q}$ satisfies hypothesis of Theorem 4.4.*

Theorem 4.7 ([DLR23, Theorem 1.7]). *Let $E/\mathbb{Q}$ be an elliptic curve and $p < q$ be distinct primes such that $\mathbb{Q}(E[p^k]) = \mathbb{Q}(E[q^r])$. Then $(p^k, q^r) = (2, 3)$ and there is some $t \in \mathbb{Q}$ such that E is $\mathbb{Q}$-isomorphic to*

$$\begin{aligned} y^2 =& x^3 - 3t^9(t^3 - 2)(t^3 + 2)^3(t^3 + 4)x \\ &- 2t^{12}(t^3 + 2)^4(t^4 - 2t^3 + 4t - 2)(t^8 + 2t^7 + 4t^6 + 8t^5 + 10t^4 + 8t^3 + 16t^2 + 8t + 4). \end{aligned}$$

or its quadratic twist by -3.

Example 4.8. Let $E/\mathbb{Q}$ be the elliptic curve with LMFDB label 486.e2 ([DLR23, Example 1.2]) given by

$$y^2 = x^3 + 405x - 9882.$$

By Proposition 2.6, the field $\mathbb{Q}(E[2])$ is the splitting field of $x^3 + 405x - 9882$, which is isomorphic to $\mathbb{Q}[X]/(x^3 - 3)$. Then $\mathbb{Q}(E[2])$ is equal to $\mathbb{Q}(\zeta_3, \sqrt[3]{3})$, which has Galois group S_3 over $\mathbb{Q}$. From LFMDB, we have

$$\frac{[\mathrm{GL}_2(6) : \rho_{E,6}(G_{\mathbb{Q}})]}{[\mathrm{GL}_2(2) : \rho_{E,2}(G_{\mathbb{Q}})] \cdot [\mathrm{GL}_2(3) : \rho_{E,3}(G_{\mathbb{Q}})]} = \frac{48}{1 \cdot 8} = 6 = [\mathbb{Q}(E[2]) : \mathbb{Q}].$$

This quantity is equal to $[\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[3]) : \mathbb{Q}]$ by Remark 3.5, which gives:

$$\mathbb{Q}(E[2]) = \mathbb{Q}(E[3]) = \mathbb{Q}(E[6]) = \mathbb{Q}(\zeta_3, \sqrt[3]{3}).$$

[1] The modular curve which parameterises elliptic curves with a $(2, 4)$-coincidence is denoted X_{20b} is the notation of Rouse and Zureick-Brown.

Theorem 4.9 ([DLR23, Theorem 1.8]). *Let $E/\mathbb{Q}$ be an elliptic curve and let $nm < n$ be positive integers such that $\mathbb{Q}(E[m])/\mathbb{Q}$ is abelian. Suppose that $\mathbb{Q}(E[m]) = \mathbb{Q}(E[n])$. Then*

1. *Either $(m, n) = (2, 4)$, $\mathbb{Q}(E[2]) = \mathbb{Q}(E[4]) = \mathbb{Q}(i)$ and there is some $t \in \mathbb{Q}$ such that $E/\mathbb{Q}$ is $\mathbb{Q}$-isomorphic to*

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

2. *Or $(m, n) = (3, 6)$, $\mathbb{Q}(E[2]) \subsetneq \mathbb{Q}(E[3]) = \mathbb{Q}(E[6])$ and there is some $t \in \mathbb{Q}$ such that*

$$j(E) = \left(\frac{-(t^3-3t^2-9t-9)(t^3+3t^2+3t-3)(t^6+12t^5+81t^4+216t^3+243t^2+108t+27)}{t(t+1)^2(t+3)^2(t^2+3)^2(t^2+3t+3)}\right)^3.$$

Example 4.10. The elliptic curve with LMFDB label 448.g3 ([DLR23, Example 3.5]) satisfies $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(E[3]) = \mathbb{Q}(E[6]) = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$. Thus we have

$$\rho_{E,6}(G_{\mathbb{Q}}) \simeq \rho_{E,3}(G_{\mathbb{Q}}) \not\simeq \rho_{E,3}(G_{\mathbb{Q}}) \times \rho_{E,2}(G_{\mathbb{Q}}).$$

Theorem 4.11 ([DLR23, Theorem 1.10]). *Let $2 \leq m < n \leq 10$ and $E/\mathbb{Q}$ be an elliptic curve with an (m, n)-coincidence. Then*

$$(m, n) \in \{(2, 3), (2, 4), (2, 6), (3, 6), (4, 6), (6, 8), (6, 9), (5, 10)\}.$$

It is suspected that the only pairs (m, n) such that an elliptic curve $E/\mathbb{Q}$ has an (m, n)-coincidences are $(2, 4), (2, 3), (2, 6)$ and $(3, 6)$.

4.3 Preliminary results over number fields

Let E/F be an elliptic curve. If E/F has CM, we suppose that F contains the CM field. As seen in Section 3.3, there exists a finite set S of rational primes such that

$$\mathrm{Gal}(F(E_{\mathrm{tors}})/F) \simeq \mathrm{Gal}(F(E[S^\infty])/F) \times \prod_{\substack{p \text{ prime} \\ p \notin S}} \mathrm{Gal}(F(E[p^\infty])/F) \tag{4.1}$$

where $F(E[S^\infty])$ is the compositum of $F(E[p^\infty])$ for $p \in S$. As underlined in Section 3.3, Campagna, Pengo and Stevenhagen gave a possible choice of S, distinguishing CM and non-CM case. All tensor products are taken over the base field F.

We deduce the following proposition, which does not depends on the set S. For an integer m, let m_S be the greatest divisor of m with only prime divisors in S.

Lemma 4.12. *Let m and n be two positive integers and suppose that E/F has an (m, n)-coincidence. Then*

$$F(E[m_S]) = F(E[n_S])$$

and

$$\forall p \notin S, \quad F(E[p^{v_p(m)}]) = F(E[p^{v_p(n)}]).$$

Proof. From the isomorphism (4.1), we know that $F(E_{\mathrm{tors}}) = \bigotimes_{i \in I} F(E[i^\infty])$ for

$$I = \{S\} \cup \{p : p \text{ is prime and } p \notin S\}.$$

By linear independance of Galois extensions, we have the following decompositions

$$F(E[m]) = F(E[m_S]) \cdot \prod_{p \notin S} F(E[p^{v_p(m)}]),$$

$$F(E[n]) = F(E[n_S]) \cdot \prod_{p \notin S} F(E[p^{v_p(n)}]).$$

By Remark 1.21 these decompositions are unique, therefore the proposition holds true. □

Proposition 2.13 implies that, if $F(E[n]) = F(E[m])$ for some $n \geq m$, then $F(\zeta_n)$ is contained in $F(E[m])$. A recurring strategy will be to give restrictions on having this inclusion.

Remark 4.13. Let n and m be two integers such that $m < n$. Then there exists a prime p such that $v_p(n) - v_p(m) = k \geq 1$. On the one hand, we have

$$F(E[m]) \subseteq F(E[p^k m]) \subseteq F(E[\operatorname{lcm}(m,n)]) = F(E[m])F(E[n]).$$

On the other hand, we have $F(\zeta_{p^k m}) \subseteq F(E[p^k m])$. Therefore, each time we have $F(\zeta_{p^k m}) \not\subseteq F(E[m])$ for some $k \geq 1$, it follows that $F(E[m]) \neq F(E[n])$ for all n such that $v_p(n) - v_p(m) \geq k$.

As a first attempt, we investigate the possibility of an (m,n)-coincidence, simply by using the inclusions of fields $F(\zeta_m) \subseteq F(E[m])$ and of groups $\rho_{E,m}(G_F) \leq \mathrm{GL}_2(m)$, and the resulting divisibility of degrees and orders. The next proposition tells us that, if $F(E[n]) = F(E[m])$, subject to an additional condition on F, then the primes greater than every prime dividing m can divide n to at most power 1, unless m is a power of 2, in which case 3 can divide n with possibly a greater power than 1.

Proposition 4.14. *Let $m \geq 2$, p be a prime such that $p > q$ for all primes $q \mid m$ and r be the largest integer such that $\mathbb{Q}(\zeta_{p^r}) \subseteq F \cap \mathbb{Q}(\mu_{p^\infty})$. Let E/F be an elliptic curve such that $F(\zeta_{p^k}) \subseteq F(E[m])$ with $k > r$. Then, $k = 1$ (and $r = 0$), unless $(m,p) = (2^j, 3)$ for some $j \geq 1$, in which case either $r = 0$ and $k \leq 2$, or $r = k - 1$.*

Proof. Suppose that $r > 0$, or $r = 0$ and $k \geq 2$. We will prove that $(m,p) = (2^j, 3)$, and $r = k-1$ or $r = 0$ and $k = 2$. By assumption, $p^{k-r} \mid [F(\zeta_{p^k}) : F]$ if $r > 0$ or $p^{k-1} \mid [F(\zeta_{p^k}) : F]$ if $r = 0$. In any case, p divides $[F(\zeta_{p^k}) : F]$. Since $F(\zeta_{p^k}) \subseteq F(E[m])$, we have

$$[F(\zeta_{p^k}) : F] \bigm| [F(E[m]) : F] \bigm| \#\mathrm{GL}_2(m),$$

and

$$\#\mathrm{GL}_2(m) = \prod_{\substack{q^j \mid m \\ j = v_q(m)}} \#\mathrm{GL}_2(q^j) = \prod_{\substack{q^j \mid m \\ j = v_q(m)}} q^{4(j-1)+1}(q-1)^2(q+1).$$

Therefore, since $q < p$ for all $q \mid m$, we obtain $p = q + 1$ for some q dividing m and so $m = 2^j$ for some $j \geq 1$ and $p = 3$. In this case, $k - r = 1$ if $r > 0$ and $k - 1 = 1$ if $r = 0$. □

Corollary 4.15. *Under the hypotheses of Proposition 4.14, let n be an integer such that $v_p(n) = k$ and suppose that E/F has an (m,n)-coincidence. Then, $k = 1$, unless $(m,p) = (2^j, 3)$ for some $j \geq 1$, in which case $r = 0$ and $k \leq 2$, or $r = k - 1$.*

In Corollary 4.24, in the next section, we extend Proposition 4.14 by replacing « $q < p$ for all $q \mid m$ » by « $p \nmid m$ », at the expense of adding conditions on the ramification at p in F or on the reduction type of E at p.

4.4 Horizontal coincidence: ramification behaviour

We talk about *horizontal coincidence* if we have an (m,n)-coincidence and the sets of prime divisors of m and n are not the same. In this section, we study the obstructions to horizontal coincidences given by the type of reduction of the elliptic curve and the resulting ramification.

4.4.1 Ramification and reduction type

Let $\mathfrak{p}$ be a prime of $\mathcal{O}_F$, whose residue characteristic is p. We recall the criterion of Néron-Ogg-Shafarevitch:

Proposition 4.16 ([Sil09, VII, Theorem 7.1])**.** *Let E/F be an elliptic curve. If E/F has good reduction at $\mathfrak{p}$, then $F(E[m])/F$ is unramified at $\mathfrak{p}$ for all m such that $p \nmid m$.*

Moreover, the theory of Tate curves gives constraints on the ramification when the reduction is multiplicative:

Proposition 4.17. *Let E/F be an elliptic curve and $m \geq 2$ such that $p \nmid m$. If E/F has split multiplicative reduction at $\mathfrak{p}$ or if E/F has multiplicative reduction $\mathfrak{p}$ and p is odd, then $F(E[m])/F$ is tamely ramified at $\mathfrak{p}$. If E/F has non split multiplication at $\mathfrak{p}$ and p is even, then $v_p(e_\mathfrak{p}(F(E[m])/F)) \leq 1$.*

Proof. First, we suppose that E/F has split multiplicative reduction at $\mathfrak{p}$. Let $F_\mathfrak{p}$ be the completion of F at $\mathfrak{p}$. We have, from [Sil94, V.Theorem 5.3], that E is isomorphic over $F_\mathfrak{p}$ to the Tate curve E_q for some $q \in F_\mathfrak{p}^*$ (for the definition of E_q, see [Sil94, V.Theorem 3.1]. We consider the $\mathfrak{p}$-adic uniformization:

$$\overline{F_\mathfrak{p}}^*/q^\mathbb{Z} \xrightarrow{\sim} E_q(\overline{F_\mathfrak{p}}).$$

Restricting to the group of m-torsion on each side, we obtain an isomorphism

$$\phi : \left(\zeta_m^\mathbb{Z} Q^\mathbb{Z}\right)/q^\mathbb{Z} \xrightarrow{\sim} E_q[m],$$

where $Q = q^{\frac{1}{m}}$ is a m-th root of q. The action of $\mathrm{Gal}(\overline{F_\mathfrak{p}}/F_\mathfrak{p})$ on $E_q[m]$ is compatible with its action on $\left(\zeta_m^\mathbb{Z} Q^\mathbb{Z}\right)/q^\mathbb{Z}$ (see [Sil09, V, Theorem 5.3]). Let $I_\mathfrak{p}$ be the inertia subgroup of $\mathrm{Gal}(\overline{F_\mathfrak{p}}/F_\mathfrak{p})$ and let $\sigma \in I_\mathfrak{p}$. Since $p \nmid m$, the extension $F_\mathfrak{p}(\zeta_m)/F_\mathfrak{p}$ is unramified, and so $\sigma(\zeta_m) = \zeta_m$. Since Q is a root of $X^m - q$, so is $\sigma(Q)$. Therefore, there exists $a \in \mathbb{Z}/m\mathbb{Z}$ such that $\sigma(Q) = \zeta_m^a Q$. We set $P_1 = \phi(\zeta_m)$ and $P_2 = \phi(Q)$. Then

$$\sigma(P_1) = \sigma(\phi(\zeta_m)) = \phi(\sigma(\zeta_m)) = \phi(\zeta_m) = P_1$$

and,

$$\sigma(P_2) = \sigma(\phi(Q)) = \phi(\sigma(Q)) = \phi(\zeta_m^a Q) = a\phi(\zeta_m) + \phi(Q) = aP_1 + P_2.$$

Hence, for all $\sigma \in I_\mathfrak{p}$, there exists $a \in \mathbb{Z}/m\mathbb{Z}$ such that

$$\rho_{E,p}(\sigma) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

It follows that the image of the wild inertia by $\rho_{E,p}$ is included in a group of order m. However, as observed by Serre in [Ser72, Section 1.1], $I_\mathfrak{p}$ is a pro-p-group, and so its image by $\rho_{E,p}$ is a p-group. So it is trivial. Hence, $F(E[m])/F$ is tamely ramified at $\mathfrak{p}$.

Now, suppose that E/F has non split multiplicative reduction at $\mathfrak{p}$, and let L/F be the quadratic extension where the reduction is split. Then $L(E[m])/L$ is tamely ramified at p. Moreover,

$$e_{\mathfrak{p}}(L(E[m])/F) = e_{\mathfrak{p}}(L(E[m])/L)e_{\mathfrak{p}}(L/F)$$

and so

$$e_{\mathfrak{p}}(F(E[m])/F) \mid e_{\mathfrak{p}}(L(E[m])/F) \mid 2e_{\mathfrak{p}}(L(E[m])/L),$$

which completes the proof. □

Finally, we also have constraints on the ramification in case of additive reduction:

Proposition 4.18. *Let E/F be an elliptic curve and $m \geq 2$ such that $p \nmid m$. If $p > 3$ and E/F has additive reduction at $\mathfrak{p}$, or if $p = 3$ and E/F does not have potential good reduction at $\mathfrak{p}$, then $F(E[m])/F$ is tamely ramified at $\mathfrak{p}$.*

Proof. If E/F has potential good reduction, the proposition follows from [ST68, Section 2, Corollary 2]. If E/F does not have potential good reduction, then the results follows from Proposition 4.17 and [Sil09, Appendix C, Theorem 14.1], since a quadratic extension cannot be widely ramified outside 2. □

Finally, let us recall the following result:

Proposition 4.19 ([Ann14, Section 4.2])**.** *Let E/F be an elliptic curve and $m \geq 2$ such that $p \nmid m$. Suppose that E/F has additive reduction at $\mathfrak{p}$. There exists an extension L/F of degree dividing 24 such that E/L has stable reduction at $\mathfrak{p}$.*

4.4.2 Ramification and entanglement

Let p be a prime and $\mathfrak{p}$ be a prime ideal of F above p. Set $e = e_{\mathfrak{p}}(F/\mathbb{Q})$ the ramification index of $\mathfrak{p}$ in $F/\mathbb{Q}$. We know that, if $F(E[n]) \subseteq F(E[m])$ then $F(\zeta_{p^k}) \subseteq F(E[m])$ for all $p^k \mid n$. In particular, $e_{\mathfrak{p}}(F(\zeta_{p^k})/F)$ divides $e_{\mathfrak{p}}(F(E[m])/F)$ for all $p^k \mid n$. Lemma 4.20 gives information about $e_{\mathfrak{p}}(F(\zeta_{p^k})/F)$.

The map $\varphi : \mathbb{Z} \to \mathbb{Z}$ denotes the Euler totient function.

Lemma 4.20. *We have $v_p(e) \geq k-1-v_p(e_{\mathfrak{p}}(F(\zeta_{p^k})/F))$. Moreover, if $e_{\mathfrak{p}}(F(\zeta_{p^k})/F) = 1$, then $\varphi(p^k) \mid e$.*

Proof. The extension $F(\zeta_{p^k})/F$ is Galois and so the ramification index above $\mathfrak{p}$ only depends on $\mathfrak{p}$. We have

$$\begin{aligned} e_{\mathfrak{p}}(F(\zeta_{p^k})/F)e &= e_{\mathfrak{p}}(F(\zeta_{p^k})/\mathbb{Q}) \\ &= e_{\mathfrak{p}}(F(\zeta_{p^k})/\mathbb{Q}(\zeta_{p^k}))e_{\mathfrak{p}}(\mathbb{Q}(\zeta_{p^k})/\mathbb{Q}) \\ &= e_{\mathfrak{p}}(F(\zeta_{p^k})/\mathbb{Q}(\zeta_{p^k}))\varphi(p^k)\cdot \end{aligned}$$

Since $v_p(\varphi(p^k)) = k-1$ we obtain the first statement. The second follows from the previous equality. □

The previous section gives information about $e_{\mathfrak{p}}(F(E[m])/F)$, summarized in Theorem 4.21. These results give constraints on having an (m,n)-coincidence when m and n do not have the same prime divisors.

Theorem 4.21. *Let $m \geq 2$ such that $p \nmid m$. Let E/F be an elliptic curve. The valuation at $\mathfrak{p}$ of the ramification index $e_{\mathfrak{p}}(F(E[m])/F)$ appears in the table below together with sufficient conditions on the reduction of E/F at $\mathfrak{p}$.*

Sufficient condition on E/F	$t = e_{\mathfrak{p}}(F(E[m])/F)$
good reduction at $\mathfrak{p}$	$t = 1$
multiplicative red. at $\mathfrak{p}$ with p odd *split multiplicative red. at $\mathfrak{p}$ with $p = 2$* *additive red. at $\mathfrak{p}$ with $p > 3$* *additive, not potentially good red. at $\mathfrak{p}$ with $p = 3$*	$v_p(t) = 0$
non split multiplicative red. at $\mathfrak{p}$ with $p = 2$ *additive, potentially good red. at $\mathfrak{p}$ with $p = 3$*	$v_p(t) \leq 1$
additive red. at $\mathfrak{p}$ with $p = 2$	$v_p(t) \leq 3$

Proof. Here is the table, with an additional column with the propositions required for the proof.

Sufficient condition on E/F	$t = e_{\mathfrak{p}}(F(E[m])/F)$	Proof
good red. at $\mathfrak{p}$	$t = 1$	Proposition 4.16
mult. red. at $\mathfrak{p}$ with p odd split mult. red. at $\mathfrak{p}$ with $p = 2$ add. red. at $\mathfrak{p}$, $p > 3$ add., no pot. good red. at $\mathfrak{p}$ with $p = 3$	$v_p(t) = 0$	Proposition 4.17 Proposition 4.17 Proposition 4.18 Proposition 4.18
non split mult. red. at $\mathfrak{p}$ with $p = 2$ add., pot. good red. at $\mathfrak{p}$ with $p = 3$	$v_p(t) \leq 1$	Proposition 4.17 Proposition 4.19
add. red. at $\mathfrak{p}$ with $p = 2$	$v_p(t) \leq 3$	Proposition 4.19

□

Remark 4.22. By Lemma 4.20, we obtain the table below, in which we present the necessary condition on the ramification of $F/\mathbb{Q}$ to obtain the ramification index as in previous theorem.

$s = e_{\mathfrak{p}}(F(\zeta_{p^k})/F)$	Necessary condition on $F/\mathbb{Q}$
$s = 1$	$\varphi(p^k) \mid e$
$v_p(s) = 0$	$v_p(e) \geq k - 1$
$v_p(s) \leq 1$	$v_p(e) \geq k - 2$
$v_p(s) \leq 3$	$v_p(e) \geq k - 4$

With the notation of Theorem 4.21 and Remark 4.22, if $F(\zeta_{p^k}) \subseteq F(E[m])$, then we must have $s \mid t$. Therefore, the tables give restrictions on having $F(\zeta_{p^k}) \subseteq F(E[m])$. For example, if we have this inclusion and E/F has good reduction at $\mathfrak{p}$, then $\varphi(p^k)$ must divide the ramification index of $F/\mathbb{Q}$ at $\mathfrak{p}$. In the following corollary, we consider the case of $F/\mathbb{Q}$ unramified above p.

Corollary 4.23. *Let E/F be an elliptic curve, $m \geq 2$, $k \geq 1$ and suppose that $p \nmid m\Delta_F$. If $F(\zeta_{p^k}) \subseteq F(E[m])$, then we are in one of the following cases:*

- *$k = 1$ and E/F has bad reduction at every ideal above p,*
- *$k = 2$, $p = 2$ and at each prime above p, E/F has either additive or non split multiplicative reduction,*

- *$k = 2$, $p = 3$, and E/F has additive and potential good reduction at every ideal above p,*

- *$k = 3$ or 4, $p = 2$ and E/F has additive and potential good reduction at every ideal above p.*

Proof. Let $\mathfrak{p}$ be a prime ideal above p. Since $p \nmid \Delta_F$, the extension $F(\zeta_{p^k})/F$ is ramified at $\mathfrak{p}$, from Lemma 4.20, so is $F(E[m])/F$ by assumptions. Looking at the tables in Theorem 4.21 and Remark 4.22, with $e = 1$, we see that the possibilities are: $k = 1$, corresponding to the second line of each tables; $k = 2$, corresponding to the third line and in this case $p = 2, 3$; or $k = 3, 4$, corresponding to the fourth line, where $p = 2$. □

The corollary below tells us that if E/F has a (m, n)-coincidence (with some conditions on F), then the primes greater than 5 not dividing m (respectively n) divide n (respectively m) to at most power 1, and E/F must have bad reduction at these primes. Moreover, if $3 \nmid m$, then 3 divides n to at most power 2, and if m is odd, then 2 divides n to at most power 4, and the greater the power, the more restrictive is the reduction type.

Corollary 4.24. *Let E/F be an elliptic curve with an (m, n)-coincidence. Suppose that $p \mid n$ and $p \nmid m\Delta_F$. Then we are in one of the following cases:*

- *$v_p(n) = 1$ and E/F has bad reduction at every ideal above p,*

- *$v_p(n) = 2$, $p = 2$ and at each prime above p, E/F has either additive or non split multiplicative reduction,*

- *$v_p(n) = 2$, $p = 3$, and E/F has additive and potential good reduction at every ideal above p,*

- *$v_p(n) = 3$ or 4, $p = 2$ and E/F has additive and potential good reduction at every ideal above p.*

Remark 4.25. If $e_{\mathfrak{p}}(F/\mathbb{Q})$ is prime to $\varphi(p^k)$ (hypothesis that is satisfied for example if $F/\mathbb{Q}$ is unramified at $\mathfrak{p}$), then Corollaries 4.23 and 4.24 are true replacing « at every ideal above p » by « at $\mathfrak{p}$ ».

Using ramification, we can also deduce a result on vertical coincidences, which is the topic of the next section:

Theorem 4.26. *Let E/F be an elliptic curve, p be a prime and $k \geq 2$. If $p^{k-1} \nmid e_{\mathfrak{p}}(F/\mathbb{Q})$ and E/F has good supersingular reduction at $\mathfrak{p}$, then $F(E[p]) \neq F(E[p^k])$.*

Proof. From Theorem 1.32, the extension $F(E[p])/F$ is tamely ramified at p. Since p^{k-1} does not divide $e_{\mathfrak{p}}(F/\mathbb{Q})$, then Remark 4.22 gives that $F(E(\zeta_{p^2})/F$ is wildly ramified at p. The result follows as a consequence of the Weil pairing 2.13. □

4.5 Coincidences in towers

In this section, we deal with *coincidence in towers*, or *vertical coincidences*, that is to say (p^k, p^{k+1})-coincidences for a prime p and a positive integer k. More generally, the section also contains results about (m, n)-coincidence where $m \mid n$.

4.5.1 Construction of vertical coincidences

Over $\mathbb{Q}$, we know that infinitely many elliptic curves have a $(2,4)$-coincidence and this is the only vertical coincidence which occurs, see Theorem 4.6. Over a number field, there are additional possibilities. Obviously, to obtain an (m,mn)-coincidence for an elliptic curve E/F, it suffices to do a base change of the ground field to $F(E[mn])$. However, such a base change is a trivial construction and so not very relevant. We will say that the base change from F to L is *minimal* for an (m,mn)-coincidence if $L(E[m]) = F(E[mn])$ and $F(E[m]) \cap L = F$. Here is an example of a $(4,8)$-coincidence obtained by a minimal base change:

Theorem 4.27. *There are infinitely many isomorphism classes of elliptic curves $E/\mathbb{Q}$ such that there exists a number field L with Galois group $(\mathbb{Z}/2\mathbb{Z})^r$ over $\mathbb{Q}$ with $1 \leq r \leq 4$ satisfying*

$$L(E[4]) = L(E[8]) \neq L.$$

To prove it, we will use the following theorem on abelian division fields:

Theorem 4.28 ([GLR16, Theorem 1.1])**.** *Let $E/\mathbb{Q}$ be an elliptic curve and let $n \geq 2$. If $\mathbb{Q}(E[m]) = \mathbb{Q}(\zeta_m)$, then $m = 2,3,4$ or 5. More generally, if $\mathbb{Q}(E(E[m])/\mathbb{Q}$ is abelian then $m = 2,3,4,5,6$ or 8 and $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ is isomorphic to one of the following groups:*

m	2	3	4	5	6	8
$\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$	$\{0\}$ $\mathbb{Z}/2\mathbb{Z}$ $\mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$	$\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$ $(\mathbb{Z}/2\mathbb{Z})^3$ $(\mathbb{Z}/2\mathbb{Z})^4$	$\mathbb{Z}/4\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ $(\mathbb{Z}/4\mathbb{Z})^2$	$(\mathbb{Z}/2\mathbb{Z})^2$ $(\mathbb{Z}/2\mathbb{Z})^3$	$(\mathbb{Z}/2\mathbb{Z})^4$ $(\mathbb{Z}/2\mathbb{Z})^5$ $(\mathbb{Z}/2\mathbb{Z})^6$

Furthermore, each listed Galois group occurs for infinitely many distinct j-invariants.

Proof of Theorem 4.27. We apply Proposition 4.33 for $F = \mathbb{Q}$, $m = 4$, $r = 2$ and $E/\mathbb{Q}$ such that $\mathrm{Gal}(\mathbb{Q}(E[8])/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^t$ for some t. Hence, there exists $L/\mathbb{Q}$ of degree dividing $\#\mathrm{GL}_2(8)/\#\mathrm{GL}_2(4) = 2^4$ (by (4.3) in Subsection 4.5.3) such that $L(E[8]) = L(E[4]) \neq L$. By Theorem 4.28, the Galois group $\mathrm{Gal}(\mathbb{Q}(E[8])/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^t$ for some t for infinitely many isomorphism classes of elliptic curves $E/\mathbb{Q}$ and $\mathbb{Q}(E[4])/\mathbb{Q}$ is non trivial since it contains ζ_4, which completes the proof. □

Remark 4.29. The proof of Theorem 4.27 considers only elliptic curves $E/\mathbb{Q}$ such that $\mathbb{Q}(E[8])/\mathbb{Q}$ is abelian. In this case $\mathrm{Gal}(\mathbb{Q}(E[8])/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^t$ with $t \in \{4,5,6\}$ from [GLR16, Theorem 1.1]. Let r be as in Theorem 4.27. We have $2^r = \#\,\mathrm{Gal}(\mathbb{Q}(E[8])/\mathbb{Q}(E[4]))$ by construction of F and $1 \leq r \leq 4$. If $t = 4$, then $1 \leq r \leq 3$ and if $t = 6$ then $2 \leq r \leq 4$.

Remark 4.30. We cannot use the abelian case to construct (p,p^2)-coincidence with p odd, because there is no abelian p^2-division field for p odd and E defined over $\mathbb{Q}$.

We recall the following definitions:

Definition 4.31. A short exact sequence of groups $1 \to H \to G \overset{r}{\to} G/H \to 1$ *split* if there exists an injective morphism $\iota : G/H \to G$ such that $r \circ \iota = \mathrm{id}$.

Definition 4.32. Let G be a group and $H, K \leq G$ such that H is normal in G. We said that G is the *semi-direct product of H by K*, denoted by $G = H \rtimes K$, if, for any $g \in G$, there exists a unique pair $(h,k) \in H \times K$ such that $g = hk$.

Proposition 4.33. *Let m, n be positive integers. Let E/F be an elliptic curve such that the following exact sequence is split:*

$$1 \to \mathrm{Gal}(F(E[mn]/F(E[m])) \to \mathrm{Gal}(F(E[mn]/F) \to \mathrm{Gal}(F(E[m]/F) \to 1$$

with $F(E[m])/F$ non trivial. Then there exists an extension L/F of degree dividing $\#\mathrm{GL}_2(mn)/\#\mathrm{GL}_2(m)$ such that

$$L(E[m]) = L(E[mn]) \neq L.$$

To prove the proposition, we will use the following elementary remark:

Remark 4.34. Let G be a group and H be a subgroup of G of finite index. Let $\phi : G \to G'$ be a surjective morphism (of groups) and set $H' = \phi(H)$. Then ϕ induces a surjective morphism of G-sets $G/H \to G'/H'$, from which

$$[G : H] = [G' : H'][\ker(\phi)H : \ker(\phi)].$$

In particular $[G' : H']$ divides $[G : H]$.

Proof of Proposition 4.33. Since the sequence is split, there exists a morphism

$$\iota : \mathrm{Gal}(F(E[m])/F) \to \mathrm{Gal}(F(E[mn])/F)$$

such that the composition with the restriction map

$$\mathrm{Gal}(F(E[mn])/F) \to \mathrm{Gal}(F(E[m])/F)$$

is the identity. Let L be the fixed field of $\mathrm{Im}(\iota)$. Then $\mathrm{Gal}(F(E[mn])/F)$ is the semi-direct product of $\mathrm{Gal}(F(E[mn])/F(E[m]))$ by $\mathrm{Gal}(F(E[mn])/L)$ and so

$$L(E[m]) = F(E[mn]) = L(E[mn]) \quad \text{and} \quad L \cap F(E[m]) = F.$$

Since $F(E[m])/F$ is nontrivial, then $L(E[m]) \neq L$. Moreover, the extension L/F has degree $[F(E[mn]) : F(E[m])]$, which divides $\#\mathrm{GL}_2(mn)/\#\mathrm{GL}_2(m)$ by point (1) of Remark 4.34, taking for ϕ the natural map $\mathrm{GL}_2(mn) \to \mathrm{GL}_2(m)$ and $H = \rho_{E,mn}(G_F)$. □

Corollary 4.35. *For E/F an elliptic curve, the following are equivalent:*

1. *The following sequence is split*

$$1 \to \mathrm{Gal}(F(E[mn]/F(E[m])) \to \mathrm{Gal}(F(E[mn]/F) \to \mathrm{Gal}(F(E[m]/F) \to 1.$$

2. *There exists an injective morphism*

$$\iota : \mathrm{Gal}(F(E[m])/F) \to \mathrm{Gal}(F(E[mn])/F)$$

such that

$$\mathrm{Gal}(F(E[mn])/F) = \iota(\mathrm{Gal}(F(E[m])/F)) \ltimes \mathrm{Gal}(F(E[mn])/F(E[m])).$$

3. *There exists a minimal base change L/F such that E/L has an (m, mn)-coincidence.*

In this case, $\iota(\mathrm{Gal}(F(E[m])/F) = \mathrm{Gal}(F(E[mn])/L)$.

Proof. The equivalence between point (1) and (2) is immediate from the definitions of split exact sequence and semi-direct product. We know that (1) $\implies$ (3) by Proposition 4.33. It remains to show that (3) $\implies$ (1). Suppose that the conditions of (3) are satisfied. Since $F(E[mn]) = L(E[mn])$, we have the following commutative diagram, where the horizontal arrows are restriction morphisms and the vertical arrows are inclusion morphisms:

$$\begin{tikzcd}
\mathrm{Gal}(F(E[mn])/L) \arrow[r, "\psi"] \arrow[d, hook] & \mathrm{Gal}(L(E[m])/L) \arrow[d, hook, "\phi"] \\
\mathrm{Gal}(F(E[mn])/F) \arrow[r] & \mathrm{Gal}(F(E[m])/F).
\end{tikzcd}$$

By assumption, ψ is a isomorphism, together with ϕ by linear independance of $F(E[m])$ and L over F. It follows that the exact sequence of (1) splits by the morphism

$$\begin{array}{cccc} \iota : & \mathrm{Gal}(F(E[m])/F) & \longrightarrow & \mathrm{Gal}(F(E[mn])/F) \\ & \sigma & \longmapsto & (\phi \circ \psi)^{-1}(\sigma). \end{array}$$

□

As a consequence of the corollary, the elliptic curves satisfying Theorem 4.27 are exactly those such that we have a split exact sequence

$$1 \to (\mathbb{Z}/2\mathbb{Z})^r \to \mathrm{Gal}(\mathbb{Q}(E[8]/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(E[4]/\mathbb{Q}) \to 1.$$

In particular, this is true for $E/\mathbb{Q}$ such that $\mathbb{Q}(E[8])/\mathbb{Q}$ is a $(\mathbb{Z}/2\mathbb{Z})^t$-extension and a classification for such elliptic curves is given in [GLR16, Table 4]. But there are many other possibilities. More generally, we have

$$\mathrm{Gal}(F(E[p^{k+1}]/F(E[p^k])) \simeq (\mathbb{Z}/p\mathbb{Z})^r$$

for some $r \leq 4$. Indeed, the Galois group $\mathrm{Gal}(F(E[p^{k+1}]/F(E[p^k]))$ is isomorphic, for $n = 2$, to a subgroup of

$$\ker\left(\mathrm{GL}_n(p^{k+1}) \to \mathrm{GL}_n(p^k)\right) = I_n + p^k \mathrm{M}_n(\mathbb{Z}/p^{k+1}\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^{n^2}. \tag{4.2}$$

Hence, to construct a (p^k, p^{k+1})-coincidence by minimal base change, we have and it suffices to find elliptic curves E/F such that the following exact sequence is split:

$$1 \to (\mathbb{Z}/p\mathbb{Z})^r \to \mathrm{Gal}(F(E[p^{k+1}]/F) \to \mathrm{Gal}(F(E[p^k]/F) \to 1.$$

4.5.2 Trivial intersection with the cyclotomic field

In this section, we show that, if $F \cap \mathbb{Q}(\zeta_{p^k})$ is trivial, then a (p^k, p^{k+1})-coincidence with p prime is possible only for $p = 2$.

Lemma 4.36. *Let E/F be an elliptic curve, and L/F be a cyclic extension such that $L \subseteq F(E[m])$. Let $\sigma \in G_F$ such that its restriction to L generates* $\mathrm{Gal}(L/F)$. *Then the order of $\rho_{E,m}(\sigma)$ is divisible by $[L : F]$.*

Proof. Let $\overline{\rho_{E,m}}$ be the reduction of $\rho_{E,m}$ modulo $\mathrm{Gal}(\overline{F}/F(E[m]))$. Then

$$[L : F] = \mathrm{ord}(\sigma|_L) \mid \mathrm{ord}(\sigma|_{F(E[m])}) = \mathrm{ord}(\overline{\rho_{E,m}}(\sigma|_{F(E[m])})) = \mathrm{ord}(\rho_{E,m}(\sigma)).$$

The first equality is by assumption, and the second is because of the injectivity of $\overline{\rho_{E,m}}$. □

Lemma 4.37 ([DLR23, Lemma 3.5])**.** *Let $A \in \mathrm{GL}_2(p^k)$ be a matrix with order divisible by $\varphi(p^{k+1})$, then* $\det(A)$ *is a square modulo p.*

From the two previous lemma, we deduce the following result:

Theorem 4.38. *Let E/F be an elliptic curve, p be a prime and k be a positive integer such that $F \cap \mathbb{Q}(\zeta_{p^k}) = \mathbb{Q}$. If $F(\zeta_{p^{k+1}}) \subseteq F(E[p^k])$, then $p = 2$.*

Proof. Suppose that p is odd and $F(\zeta_{p^{k+1}}) \subseteq F(E[p^k])$. Let $\sigma \in G_F$ such that its restriction to $F(\zeta_{p^{k+1}})$ generates $\mathrm{Gal}(F(\zeta_{p^{k+1}})/F)$. Then its restriction to $F(\zeta_{p^k})$ generates $\mathrm{Gal}(F(\zeta_{p^k})/F)$. So $\det \rho_{E,p^k}(\sigma)$ generates $(\mathbb{Z}/p^k\mathbb{Z})^*$. Moreover, Lemma 4.36 says that $\varphi(p^{k+1})$ divides the order of $\rho_{E,p^k}(\sigma)$ and so its determinant is a square mod p, by Lemma 4.37. But, for p odd, a square mod p cannot generate $(\mathbb{Z}/p^k\mathbb{Z})^*$. Hence, p is even. □

Corollary 4.39. *Let E/F be an elliptic curve with $F \cap \mathbb{Q}(\zeta_{p^k}) = \mathbb{Q}$. If E/F has a (p^k, p^{k+1})-coincidence, then $p = 2$.*

Proof. It is immediate from Theorem 4.38, since $F(\zeta_{p^{k+1}}) \subseteq F(E[p^{k+1}])$. □

Remark 4.40. If E/F has an (m, mn)-coincidence, then we must have $F(\zeta_{mn}) \subseteq F(E[m])$. But this does not implies in general that $F(\zeta_{mn}) = F(\zeta_m)$, as we will see in Remark 4.55. Even more, unless m is odd and $n = 2$, this last never happens if $F = \mathbb{Q}$, and yet some coincidences occurs, like $(2, 4)$ and $(2, 6)$-coincidence, as Examples 4.5 and 4.8. As in Remark 4.55, it is due to the non-surjectivity of

$$\mathrm{SL}_2(mn) \cap \rho_{E,mn}(G_F) \to \mathrm{SL}_2(m) \cap \rho_{E,m}(G_F).$$

Remark 4.41. The condition $F(\zeta_{p^{k+1}}) \subseteq F(E[p^k])$ is not sufficient to have the coincidence. For example, the elliptic curve of Remark 3.58 does not satisfy $\mathbb{Q}(E[2^k]) = \mathbb{Q}(E[2^{k+1}])$ for any k. Indeed, this elliptic curve has CM and Theorem 4.6 implies that no CM elliptic curve defined over $\mathbb{Q}$ has a $(2^k, 2^{k+1})$-coincidence.

We are now able to prove the theorem stated in the introduction:

Theorem 4.42. *Let $m, n \geq 1$ and E/F be an elliptic curve with conductor ideal $\mathfrak{f}_E$. Let $\mathrm{N}(\mathfrak{f}_E)$ be the norm of $\mathfrak{f}_E$. Suppose that $F(E[m]) = F(E[n])$. Then, for all primes p such that $v_p(m) \neq v_p(n)$, we have*

$$p \mid 2 \cdot \Delta_F \cdot \mathrm{N}(\mathfrak{f}_E).$$

Proof. First, suppose that p divides n or m but not both. Then, by Corollary 4.24, if p does not divide Δ_F, then E/F has bad reduction above p. Now, suppose that p divides both n and m such that $v_p(m) = k$ and $v_p(m) < v_p(n)$. Since $F(E[m]) = F(E[\mathrm{lcm}(m,n)])$, then $F(E[m]) = F(E[pm])$. Setting $a = \frac{m}{p^k}$ and $L = F(E[a])$, we obtain

$$F(E[p^k a]) = F(E[p^{k+1}a]) \quad \text{and} \quad L(E[p^k]) = L(E[p^{k+1}]).$$

Then Corollary 4.39 implies that $L \cap \mathbb{Q}(\zeta_{p^{k+1}}) \neq \mathbb{Q}$ or $p = 2$. In particular, p is ramified in $L/\mathbb{Q}$ or $p = 2$. But $L = F(E[a])$, so p is ramified in $L/\mathbb{Q}$ if and only if p is ramified in $F/\mathbb{Q}$ or in $F(E[a])/F$. Therefore $p \mid \Delta_F$ or E has bad reduction above p. □

Corollary 4.43. *Let $m, n \geq 1$, $E/\mathbb{Q}$ be an elliptic curve and Δ_E be the minimal discriminant of E. Suppose that $\mathbb{Q}(E[m]) = \mathbb{Q}(E[n])$. Then, for all primes p such that $v_p(m) \neq v_p(n)$, we have $p \mid 2\Delta_E$.*

4.5.3 Index of images

Let p be a prime. Let M be a subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$ and let G be a subgroup of M. In our setting we only need to consider the groups $\mathrm{SL}_2(\mathbb{Z}_p)$, $\mathrm{GL}_2(\mathbb{Z}_p)$ and $(\mathbb{Z}_p)^*$, but we state results in the general case as the approach is the same. For k a positive integer, we denote by M_k the image of M in $\mathrm{GL}_n(\mathbb{Z}/p^k\mathbb{Z})$ and G_k the image of G in M_k. We set $i_k = [M_k : G_k]$. We have $i_k \mid i_{k+1}$ by Remark 4.34. Moreover,

$$\frac{i_{k+1}}{i_k} = \frac{\#M_{k+1}}{\#G_{k+1}} \cdot \frac{\#G_k}{\#M_k} \left| \frac{\#M_{k+1}}{\#M_k} = \begin{cases} p^{n^2} & \text{if } M = \mathrm{GL}_n(\mathbb{Z}_p) \\ p^{n^2-1} & \text{if } M = \mathrm{SL}_n(\mathbb{Z}_p). \end{cases} \right. \tag{4.3}$$

from (4.2). In particular,

$$G_k \simeq G_{k+1} \iff \frac{i_{k+1}}{i_k} = \begin{cases} p^{n^2} & \text{if } M = \mathrm{GL}_n(\mathbb{Z}_p) \\ p^{n^2-1} & \text{if } M = \mathrm{SL}_n(\mathbb{Z}_p). \end{cases} \tag{4.4}$$

The idea of the lemma below and its proof follows [SZ17, Lemma 3.7].

Proposition 4.44. *Suppose that $M = \mathrm{GL}_n(\mathbb{Z}_p)$ or $\mathrm{SL}_n(\mathbb{Z}_p)$. The sequence $(u_k) = \left(\frac{i_{k+1}}{i_k}\right)$ satisfies $u_{k+1} \mid u_k$ for $k \geq 1$ if p is odd and for $k \geq 2$ if $p = 2$.*

Proof. Suppose that p is odd or that $k \geq 2$ and $p = 2$. Let H_k be the kernel of the reduction map $G_k \to G_{k-1}$. Let $h \in G$ whose image in G_k belongs to H_k. Then $h = I + p^{k-1}A$ with $A \in M_n(\mathbb{Z}_p)$. The map

$$\begin{aligned} \phi : H_k &\longrightarrow H_{k+1} \\ \overline{h} &\longmapsto \overline{h^p} \end{aligned}$$

is an injective morphism since

$$(I + p^{k-1}A)^p = I + \binom{p}{1} p^{k-1}A + \binom{p}{2} p^{2k-1}A^2 + \cdots \equiv I + p^k A \pmod{p^{k+1}}.$$

Therefore $\frac{\#G_k}{\#G_{k-1}}$ divides $\frac{\#G_{k+1}}{\#G_k}$ and so, since $\frac{\#M_k}{\#M_{k-1}} = \frac{\#M_{k+1}}{\#M_k}$ from the equation (4.3), we obtain $u_{k+1} \mid u_k$. □

Corollary 4.45. *Let $k \geq 1$ if p is odd and $k \geq 2$ if p is even. If $M = \mathrm{GL}_n(\mathbb{Z}_p)$ or $M = \mathrm{SL}_n(\mathbb{Z}_p)$, and $G_k \simeq G_{k+1}$, then $G_1 \simeq G_2 \simeq \cdots \simeq G_{k+1}$ if p is odd, and $G_2 \simeq G_3 \simeq \cdots \simeq G_{k+1}$ if p is even.*

Proof. Suppose that $M = \mathrm{GL}_n(\mathbb{Z}_p)$. Equivalence (4.3) gives $\frac{i_{k+1}}{i_k} = p^{n^2}$. Since the sequence $\left(\frac{i_{s+1}}{i_s}\right)$ is non-increasing from Lemma 4.44 for $s \geq 1$ and p odd or $s \geq 2$ and $p = 2$, and has values dividing p^{n^2} by Equation (4.4), then $\frac{i_{s+1}}{i_s} = p^4$ for all $s \leq k$. The proof is similar for $M = \mathrm{SL}_n(\mathbb{Z}_p)$. □

Theorem 4.46. *Let $q = p$ and $k \geq 1$ if p is odd, or $q = p^2$ and $k \geq 2$ if p is even. Let E/F be an elliptic curve. If $F(E[p^k]) = F(E[p^{k+1}])$, then $F(E[q]) = F(E[p^{k+1}])$.*

Proof. Let $M = \mathrm{GL}_2(\mathbb{Z}_p)$ and $G = \rho_{E,p^\infty}(G_F)$. So

$$G_k = \rho_{E,p^k}(G_F) \simeq \mathrm{Gal}(F(E[p^k])/F).$$

Therefore, the equality $F(E[p^k]) = F(E[p^{k+1}])$ is equivalent to $G_k \simeq G_{k+1}$, and we use Corollary 4.45. □

Corollary 4.47. *Let $k \geq 2$ if p odd and $k \geq 3$ if p is even. Let E/F be an elliptic curve such that the exact sequence*

$$1 \to \mathrm{Gal}(F(E[p^{k+1}]/F(E[p^k])) \to \mathrm{Gal}(F(E[p^{k+1}]/F) \to \mathrm{Gal}(F(E[p^k]/F) \to 1$$

is split, then $F(E[p^{k-1}]) = F(E[p^k])$.

Proof. By Proposition 4.33, there exists L/F linearly disjoint from $F(E[p^k])/F$ such that $L(E[p^k]) = L(E[p^{k+1}])$. Therefore, by Theorem 4.46, we have $L(E[p^{k-1}]) = L(E[p^k])$. But $L \cap F(E[p^k]) = F$ gives $L(E[p^{k-1}]) \cap F(E[p^k]) = F(E[p^{k-1}])$, from which we obtain

$$[F(E[p^k]) : F(E[p^{k-1}])] = [L(E[p^k]) : L(E[p^{k-1}])] = 1,$$

using Proposition 1.16. □

Remark 4.48. We notice that the assumptions of the theorem are necessary. Indeed, let $E/\mathbb{Q}$ be an elliptic curve satisfying $\mathrm{Gal}(\mathbb{Q}(E[8])/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^6$. Then, the sequence in Corollary 4.47 is split. However, since $\mathrm{Gal}(\mathbb{Q}(E[8])/\mathbb{Q}(E[4])) \leq (\mathbb{Z}/2\mathbb{Z})^4$ by (4.2), we have $(\mathbb{Z}/2\mathbb{Z})2 \leq \mathrm{Gal}(\mathbb{Q}(E[4])/\mathbb{Q})$ and so $\mathbb{Q}(E[2]) \neq \mathbb{Q}(E[4])$.

We obtain the following proposition on the adelic index:

Proposition 4.49. *Let E/F be an elliptic curve without CM, with a (p^k, p^{k+1})-coincidence. Then $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \rho_E(G_F)]$ is divisible by p^{4k} if p is odd, or $\max\left\{2^4, 2^{4k-1}\right\}$ if p is even.*

Proof. With the introduced notation, we consider $M = \mathrm{GL}_2(\mathbb{Z}_p)$ and $G = \rho_{E,p^\infty}(G_F)$. The index i_{k+1} divides $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \rho_E(G_F)]$ by Remark 4.34 and so i_{k+1}/i_k divides the global index $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \rho_E(G_F)]$. But having a (p^k, p^{k+1})-coincidence is equivalent to have $G_k \simeq G_{k+1}$. Then, the proposition follows from Equation 4.4 and Corollary 4.45. □

Remark 4.50. We saw in Theorem 3.29 a set of possible adelic indexes which is generic for elliptic curves E defined over $\mathbb{Q}$ and in Theorem 3.30, upper bounds for the adelic index which is generic for elliptic curves E/F, depending on the number field F, both given by Zywina.

Remark 4.51. Let E/F be an elliptic curve and take $G = \rho_{E,p^\infty}(G_F)$. So we have $G_k = \rho_{E,p^k}(G_F)$ for $k \geq 1$.

1. The sequence (i_k) is increasing, and, if E/F does not have CM, becomes stationary.
2. For elliptic curves $E/\mathbb{Q}$ without CM, let s be the p-adic depth of ρ_E. Then the sequence $\left(\frac{i_{k+1}}{i_k}\right)$ stabilizes at 1 from $\max\{1, s\}$. In particular, if $G = \mathrm{GL}_2(\mathbb{Z}_p)$, then $\left(\frac{i_{k+1}}{i_k}\right)$ is constant equal to 1. The converse is false: the elliptic curve with LMFDB label 11.a2 has non maximal Galois representation at 5 and the sequence $\left(\frac{i_{k+1}}{i_k}\right)$ attached to 5 is constant, equal to 1. In Table 2.1, we find the possible p-adic depth for all p. For example, for $p = 2$, $\left(\frac{i_{k+1}}{i_k}\right)$ stabilizes at 1 from k at most 5.
3. We consider $k \geq 1$ if p is odd, or $k \geq 2$ if p is even. If the first term of $\left(\frac{i_{k+1}}{i_k}\right)$ is different than p^4, then E/F does not have (p^k, p^{k+1})-coincidences for any k. Otherwise, if s is the rank of the first jump of the sequence, then E/F does not have (p^k, p^{k+1})-coincidences for $k \geq s$.

4. We consider $k \geq 1$ if p is odd, or $k \geq 2$ if p is even. We know that the sequences $\left(\frac{i_{k+1}}{i_k}\right)$ is non-increasing, then constant. We can ask if it is decreasing then constant. The answer is no. For example, the elliptic curve with LMFDB label 15.a4 has, for $p = 2$, $\left(\frac{i_{k+1}}{i_k}\right) = (2^2, 2, 2, 2, 1, \dots)$. We can also ask if the graphs are "progressively non-increasing", meaning that $\frac{i_{k+1}}{i_k} \in \left\{\frac{i_k}{i_{k-1}}, \frac{1}{p}\frac{i_k}{i_{k-1}}\right\}$. The answer is also no. For example, the elliptic curve with LMFDB label 15.a8 has, for $p = 2$, $\left(\frac{i_{k+1}}{i_k}\right) = (2^3, 2, 1, \dots)$ and the elliptic curve with LMFDB label 40.a4 has, for $p = 2$, $\left(\frac{i_{k+1}}{i_k}\right) = (2^4, 1, \dots)$.

Example 4.52. Here some examples over $\mathbb{Q}$, computed from [LMF24], illustrate different possibilities for the sequence $\left(\frac{i_{k+1}}{i_k}\right)$. As underlined in Remark 4.51, the sequence $\left(\frac{i_{k+1}}{i_k}\right.$ is constant equal to 1 for $p \geq 13$, and, for $p < 13$, it stabilizes at the rank corresponding to the p-adic depth of ρ_E, which is a most 5 if $p = 2$, at most 3 if $p = 3$, at most 2 if $p = 5, 7, 11$.

LMFDB label	Minimal Weierstrass equation	Non max p	Sequence $\left(\frac{i_{k+1}}{i_k}\right)$ attached to p
14.a6	$y^2 + xy + y = x^3 + 4x - 6$	2	$1, 2, 1, \dots$
15.a1	$y^2 + xy + y = x^3 + x^2 - 2160x - 39540$	2	$2^2, 2^2, 2, 1, \dots$
15.a2	$y^2 + xy + y = x^3 + x^2 - 135x - 660$	2	$2^2, 2^2, 1, \dots$
15.a4	$y^2 + xy + y = x^3 + x^2 - 80x + 242$	2	$2^2, 2, 2, 2, 1, \dots$
15.a5	$y^2 + xy + y = x^3 + x^2 - 10x - 10$	2	$2^3, 2, 1, \dots$
15.a8	$y^2 + xy + y = x^3 + x^2 + 35x - 28$	2	$2^3, 2^2, 1, \dots$
20.a3	$y^2 = x^3 + x^2 - x$	2	$2, 2, 1, \dots$
40.a4	$y^2 = x^3 + 13x - 34$	2	$2^4, 1, \dots$
19.a1	$y^2 + y = x^3 + x^2 - 769x - 8470$	3	$3, 3, 1, \dots$
54.a2	$y^2 + xy = x^3 - x^2 - 3x + 3$	3	$3^2, 1, \dots$
1944.f1	$y^2 = x^3 - 27x - 42$	3	$3^3, 1, \dots$
11.a1	$y^2 + y = x^3 - x^2 - 7820x - 263580$	5	$5, 1, \dots$
11.a2	$y^2 + y = x^3 - x^2 - 10x - 20$	5	$1, 1, \dots$

Remark 4.53. Let E/F be an elliptic curve and take $G = \rho_{E,p^\infty}(G_F)$. Then $\det G$ is a subgroup of $(\mathbb{Z}_p)^*$, with image $\det G_k$ in $(\mathbb{Z}/p^k\mathbb{Z})^*$. We recall that $\det G_k \simeq \mathrm{Gal}(F(\zeta_{p^k})/F)$, by Proposition 2.13. We set $j_k = [(\mathbb{Z}/p^k\mathbb{Z})^* : \det G_k]$. We consider $k \geq 1$ if p is odd, and $k \geq 2$ is p is even. The sequence $\left(\frac{j_{k+1}}{j_k}\right)$ is non-increasing and has value in $\{1, p\}$ by Lemma 4.44 and the equation (4.3). We have $j_{k+1}/j_k = p$ if and only if $\det G_k \simeq \det G_{k+1}$, by the isomorphism (4.4), and this is equivalent to $F(\zeta_{p^{k+1}}) = F(\zeta_{p^k})$. Corollary 4.45 implies that $F(\zeta_q) = F(\zeta_{p^{k+1}})$ with $q = p$ if p is odd and $q = 4$ if p is even. As a consequence, the sequence (j_k) is increasing and becomes stationary from the smallest s such that $\zeta_{p^s} \notin F(\zeta_q)$.

Remark 4.54. A different argument for Remark 4.53 is the following: let r be the greatest integer such that $F(\zeta_q) = F(\zeta_{p^r})$. If $F(\zeta_q)$ is a proper subfield of $F(\zeta_{p^{k+1}})$, then $m < k+1$ and

$$\mathbb{Z}/p^{k+1-r}\mathbb{Z} \simeq \mathrm{Gal}(F(\zeta_{p^{k+1}})/F(\zeta_q))$$

and

$$\mathbb{Z}/p^{k-r}\mathbb{Z} \simeq \mathrm{Gal}(F(\zeta_{p^k})/F(\zeta_q)),$$

so $F(\zeta_{p^{k+1}}) \neq F(\zeta_{p^k})$.

Remark 4.55. Let E/F be an elliptic curve and take $G = \rho_{E,p^\infty}(G_F)$. We observe that $\mathrm{SL}_2(\mathbb{Z}_p) \cap G$ is a subgroup of $\mathrm{SL}_2(Z_p)$ and so we can consider its projection in $\mathrm{SL}_2(p^k)$ for each k. Unfortunately, these projections are not necessarily equal to $\mathrm{SL}_2(p^{k+1}) \cap G_k$ and so we cannot use these groups to deal with the coincidence: if $G_k \simeq G_{k+1}$, we do not necessarily have $\mathrm{SL}_2(p^k) \cap G_k \simeq \mathrm{SL}_2(p^{k+1}) \cap G_{k+1}$. Setting $\ell_k = [\mathrm{SL}_2(p^k) : \mathrm{SL}_2(p^k) \cap G_k]$, we have $i_k = j_k \ell_k$ with j_k defined as in Remark 4.53. Suppose that $G_k \simeq G_{k+1}$. Then $i_{k+1}/i_k = p^4$. Hence

$$\begin{aligned} p^4 = \frac{j_{k+1}\ell_{k+1}}{j_k \ell_k} &= p^4 \frac{\#\det G_k}{\#\det G_{k+1}} \frac{\#(\mathrm{SL}_2(p^k) \cap G_k)}{\#(\mathrm{SL}_2(p^{k+1}) \cap G_{k+1})} \\ &= p^4 \frac{[F(\zeta_{p^k}) : F]}{[F(\zeta_{p^{k+1}}) : F]} \frac{\#(\mathrm{SL}_2(p^k) \cap G_k)}{\#(\mathrm{SL}_2(p^{k+1}) \cap G_{k+1})}. \end{aligned}$$

Then we have two situations:

1. $F(\zeta_{p^k}) = F(\zeta_{p^{k+1}})$, and $\mathrm{SL}_2(p^k) \cap G_k \simeq \mathrm{SL}_2(p^{k+1}) \cap G_{k+1}$,
2. $F(\zeta_{p^{k+1}}) \neq F(\zeta_{p^{k+1}})$, and the reduction map $\mathrm{SL}_2(p^{k+1}) \cap G_{k+1} \to \mathrm{SL}_2(p^k) \cap G_k$ is not surjective.

In the first case, we have seen in Remark 4.53 that $F(\zeta_{p^{k+1}})$ is equal to $F(\zeta_4)$ if $p = 2$ and $F(\zeta_p)$ otherwise. The examples of vertical coincidence we have for elliptic curves over $\mathbb{Q}$ fits, obviously, in the second case. Indeed, the elliptic curve with LMFDB label 40.a4 has a $(2,4)$-coincidence with

$$G_2 = \rho_{E,4}(G_F) \simeq \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle.$$

In this case, we have $G_2 \cap \mathrm{SL}_2(4) = \{\mathrm{id}\}$, whereas

$$G_1 \cap \mathrm{SL}_2(2) = G_1 = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle.$$

4.5.4 Split liftable subgroups

Let m, n be positive integers. If E/F is an elliptic curve with an (m, mn)-coincidence, then $\rho_{E,m}(G_F) \simeq \rho_{E,mn}(G_F)$ and the image of $\rho_{E,mn}(G_F)$ in $\mathrm{GL}_2(m)$ is $\rho_{E,m}(G_F)$. It leads to the following definition. For a subgroup G of $\mathrm{GL}_2(m)$, there are *a priori* several liftings of G in $\mathrm{GL}_2(mn)$.

Definition 4.56. We say that a subgroup G of $\mathrm{GL}_2(m)$ is *split liftable* modulo mn if there exists $G' \leq \mathrm{GL}_2(mn)$ such that G is the image of G' in $\mathrm{GL}_2(m)$ and $G \simeq G'$. We say that an element g of $\mathrm{GL}_2(m)$ is *split liftable* modulo m if there exists $g' \in \mathrm{GL}_2(mn)$ with same order as g and such that g is the image of g' in $\mathrm{GL}_2(m)$.

A subgroup G of $\mathrm{GL}_2(m)$ is split liftable modulo mn is there exists an injective morphism $G \to \mathrm{GL}_2(mn)$ which makes the following diagram commutative:

$$\begin{tikzcd} & \mathrm{GL}_2(mn) \arrow[d] \\ G \arrow[ur, hook] \arrow[r, hook] & \mathrm{GL}_2(m) \end{tikzcd}$$

The definition above is up to conjugation, since two conjugate groups are isomorphic. Therefore:

Proposition 4.57. *Let E/F be an elliptic curve with an (m, mn)-coincidence. Then $\rho_{E,m}(G_F)$ is split liftable modulo mn.*

The aim of this section is to determine the subgroups of $\mathrm{GL}_2(m)$ which are split liftable or not modulo some multiple of m.

Remark 4.58. If G in $\mathrm{GL}_2(m)$ is split liftable modulo mn, then G is split liftable modulo every km such that $1 \leq k \leq n$.

Remark 4.59. In [Elk06], Elkies already use the property of being split liftable to construct the modular curve $\mathcal{X}_9$. It is defined by $\mathcal{X}_9 = X(9)/(G/\langle -\mathrm{id}\rangle)$ where G is a split lifting of $\mathrm{SL}_2(3)$ in $\mathrm{GL}_2(9)$, and more specifically, in $\mathrm{SL}_2(9)$.

Remark 4.60. Corollary 4.45 tells that, if a subgroup of $\mathrm{GL}_2(p^k)$ is split liftable modulo $\mathrm{GL}_2(p^{k+1})$, then its image in $\mathrm{GL}_2(q)$ is also split liftable modulo $\mathrm{GL}_2(p^{k+1})$, where $q = p$ if p is odd or $q = 4$ if p is even.

Lemma 4.61. *Let $G \leq \mathrm{GL}_2(m)$ be split liftable modulo mn. Then, all subgroups of G are split liftable modulo mn.*

Proof. Let G' be a subgroup of $\mathrm{GL}_2(mn)$ such that G is the image of G' in $\mathrm{GL}_2(mn)$ and $G \simeq G'$. Then, the restriction $\pi : G' \to G$ of the natural projection $\mathrm{GL}_2(mn) \to \mathrm{GL}_2(m)$ is an isomorphism. Let $H \leq G$. We set $H' := \pi^{-1}(H)$. Then $H' \simeq H$ and H is the image of H' in $\mathrm{GL}_2(m)$. □

Proposition 4.62. *Let $m \geq 2$. The following subgroups of* $\mathrm{GL}_2(m)$ *are split liftable modulo every multiple of m:*

$$\left\langle \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle, \quad \left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle.$$

Proof. Considering the two groups as subgroups of $\mathrm{GL}_2(\mathbb{Z})$, we observe that they have finite orders, respectively 12 and 8, and their elements only have coefficients in $\{0, 1, -1\}$. Consequently, they are isomorphic to their projection modulo any integers m such that $1 \neq -1 \pmod{m}$, that is for any $m \geq 3$. The case $m = 2$ is given by Example 4.63. □

Example 4.63. The group $\mathrm{GL}_2(2)$ lifts to $\left\langle \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(\mathbb{Z})$, and so is split liftable modulo every even integer.

Remark 4.64. Let E/F be an elliptic curve. To have an (m, mn)-coincidence, it is necessary to have $\rho_{E,m}(G_F)$ split liftable modulo mn, but it is not sufficient. Indeed, $\mathrm{GL}_2(2)$ is split liftable modulo 8, but there are no $(2, 8)$-coincidence for elliptic curve defined over $\mathbb{Q}$, see [DLR23, Theorem 1.4]. This is also the case for $\mathrm{GL}_2(3)$: the subgroup

$$\left\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -2 & 2 \\ -2 & -2 \end{pmatrix}, \begin{pmatrix} 4 & -2 \\ -3 & 4 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(9)$$

is a lifting of $\mathrm{GL}_2(3)$ of order 48. Hence, $\mathrm{GL}_2(3)$ is split liftable modulo 9 and yet there is no $(3, 9)$-coincidence for elliptic curves with surjective mod 3 Galois representation, by Corollary 4.39 and Proposition 2.13.

Now we will present groups which are not split liftable, which give us obtructions having the coincidence. We underline that, by Lemma 4.61, if $g \in \mathrm{GL}_2(m)$ is not split liftable modulo mn, then all groups containing g are not split liftable modulo mn.

From now on, we will denote by T the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Lemma 4.65. *Let p be a prime and $k \geq 1$. The matrix T in $\mathrm{GL}_2(p^k)$ is split liftable modulo p^{k+1} if and only if $p = 2, 3$ and $k = 1$.*

Proof. In $\mathrm{GL}_2(2)$, resp. $\mathrm{GL}_2(3)$, the matrix T is conjugates to $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, resp. $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, and so is split liftable modulo 4, resp. modulo 9, by Lemma 4.62. Set $q = p^2$ if $p = 2, 3$ and $q = p$ otherwise. We know, from Corollary 4.45, that, for $k \geq 1$ if p is odd and $k \geq 2$ if p is even, if T in $\mathrm{GL}_2(p^k)$ is split liftable modulo p^{k+1}, then T in $\mathrm{GL}_2(q)$ is split liftable modulo p^{k+1} and so modulo pq. Now, if T was split liftable modulo pq, then we could find $M \in M_2(\mathbb{Z}_p)$ such that $T + qM$ has order q in $\mathrm{GL}_2(pq)$. But

$$\begin{pmatrix} 1+qa & 1+qb \\ qc & 1+qd \end{pmatrix}^n \equiv \begin{pmatrix} 1+nqa+\frac{n(n-1)}{2}qc & n+nqb+\frac{n(n-1)}{2}q(a+d)+\frac{n(n-1)(n-2)}{6}qc \\ nqc & 1+nqd+\frac{n(n-1)}{2}qc \end{pmatrix} \pmod{pq}.$$

Now, we take $n = q$. Then p divides $\frac{q(q-1)}{2}$ and $\frac{q(q-1)(q-2)}{6}$. We obtain

$$(T + qM)^q \equiv \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \not\equiv \mathrm{id} \pmod{pq}.$$

□

Theorem 4.66. *Let p be a prime. Let $q = p$ if $p \neq 2, 3$, or $q = p^2$ if $p = 2, 3$. Let E/F be an elliptic curve. If $\rho_{E,q}(G_F)$ contains T, then $F(E[q]) \neq F(E[pq])$.*

In particular, if E/F does not have CM and has a (p^k, p^{k+1})-coincidence, then E/F has non maximal image modulo p^2, and even modulo p if $p \neq 2, 3$.

Corollary 4.67. *Let E/F be an elliptic curve with multiplicative reduction at a prime $\mathfrak{r}$ of $\mathcal{O}_F$ and let p be a prime not dividing $2v_{\mathfrak{r}}(j(E))$. Then E/F does not have a (p^k, p^{k+1})-coincidence for any k.*

Proof. If E/F has multiplicative reduction at a prime ideal $\mathfrak{r}$ and p does not divide $2v_{\mathfrak{r}}(j(E))$, then $T \in \rho_{E,p}(G_F)$ by [Sil94, Proposition 1.6]. But this is not possible for a (p^k, p^{k+1})-coincidence from Theorem 4.66. □

Remark 4.68. Suppose that p is odd, and $k \geq 2$ if $p = 3$. To study (p^k, p^{k+1})-coincidences further, it remains to deal with subgroups of $\mathrm{GL}_2(p^k)$ with non-surjective determinant, by Corollary 4.39, and which does not contains T, by Theorem 4.66.

4.5.5 CM case

If E/F has complex multiplication by a quadratic field K and $F \subseteq K(j(E))$, then we can say more.

Proposition 4.69. *Let $E/\overline{\mathbb{Q}}$ be an elliptic curve with CM by a quadratic field K and $F = K(j(E))$. If $F(E[p^k]) = F(E[p^{k+1}])$, then $p = 2$ and $k = 1$.*

Proof. We have the following field inclusions:

$$\begin{tikzcd}
& F(E[p^{k+1}]) \arrow[dl, dash, "a"'] \arrow[dr, dash] & \\
F(E[p^k]) \arrow[dr, dash, "c"'] & & F(h(E[p^{k+1}]) \arrow[dl, dash, "d"] \\
& F(h(E[p^k])) &
\end{tikzcd}$$

where h is a Weber function for E (see [LR22]). Suppose that $k \geq 1$ if p is odd or $k \geq 2$ if $p = 2$ and $a = 1$. By [LR22, Theorem 4.3], we have,

$$d = [F(h(E[p^{k+1}])) : F(h(E[p^k]))] = p^2.$$

This implies that $p^2 \mid c$. Moreover, by [LR22, Theorem 4.1] we have $c \mid \#\mathcal{O}_K^*$. But $\#\mathcal{O}_K^* = 2$, 4 or 6. Thus $p = 2$ and $c = \#\mathcal{O}_K^* = 4$. But $\mathcal{O}_K^* \simeq \mathrm{Aut}(E)$, so $j(E) = 1728$ by [Sil09, III, Theorem 10.1] and $F = K(j(E)) = K = \mathbb{Q}(i)$. In this case, E is defined over $\mathbb{Q}$ and $\mathbb{Q}(E[2^k]) \subsetneq \mathbb{Q}(E[2^{k+1}])$ by Theorem 4.6. Moreover, the Weil pairing implies that

$$F = \mathbb{Q}(i) \subseteq \mathbb{Q}(E[4]) \subseteq \mathbb{Q}(E[2^k]) \subsetneq \mathbb{Q}(E[2^{k+1}])$$

and so $F(E[2^k]) \subsetneq F(E[2^{k+1}])$. We conclude that $p = 2$ and $k = 1$. □

Remark 4.70. If an elliptic curve E/F has a $(2,4)$-coincidence, then $\rho_{E,4}(G_F)$ must be a split lifting of $\rho_{E,2}(G_F)$. Example 4.63 gives such a split lifting and a Magma computation shows that this is the only one up to conjugation ([DLR23, Proof of Proposition 3.9]). The corresponding modular curve is X_{20b} in the notation of Rouse and Zureick-Brown [RZB15, Remark 1.6], whose model is given in Theorem 4.4. We deduce the map to the j-line, explicitely given in [DLR23, Proof of Proposition 3.9]: let E/F be an elliptic curve with a $(2,4)$-coincidence, then there exists $t \in F$ such that

$$j(E) = \frac{-4t^8 + 32t^7 + 80t^6 - 288t^5 - 504t^4 + 864t^3 + 1296t^2 - 864t - 1188}{t^4 + 4t^3 + 6t^2 + 4t + 1}.$$

For rational CM j-invariant, there is no such t.

4.6 Large images

Since $\mathrm{GL}_2(m)$ and $\mathrm{GL}_2(n)$ are not isomorphic for $m \neq n$, then (m,n)-coincidences cannot happen for elliptic curves with surjective mod m and mod n representations. Daniels and Lozano-Robledo compared the abelian part of the division field to show that $E/\mathbb{Q}$ does not have (m,n)-coincidence if only $\rho_{E,m}$ is surjective. In this section, we use the same idea to show a similar result over number fields, in case where $\rho_{E,m}$ is large, *i.e.* it contains the special linear group. In this case, the elliptic curve E/F does not have CM, and it is said that it has maximal image at m. We will only deal with m odd.

For a group G, we denote by $\mathrm{D}(G)$ its commutator subgroup. We know that $D(G)$ is the smallest normal subgroup of G such that $G/\mathrm{D}(G)$ is abelian and this last is called the *abelianization of* G. We will use several well-known results about derived group of $\mathrm{SL}_2(m)$ and $\mathrm{GL}_2(m)$, given with detailed proofs in Appendix A.

We denote by F^{ab} the maximal abelian extension of F. We will compare the maximal abelian extension of $F(E[m])$ and that of $F(E[n])$.

Proposition 4.71. *Let m be an odd integer and E/F be an elliptic curve. Suppose that $\rho_{E,m}(G_F)$ contains $\mathrm{SL}_2(m)$. Then*

$$F(E[m]) \cap F^{\mathrm{ab}} = \begin{cases} F(\zeta_m) & \textit{if } \mathrm{D}(\rho_{E,m}(G_F)) = \mathrm{SL}_2(m) \\ \textit{a } \mathbb{Z}/3\mathbb{Z}\textit{-extension of } F(\zeta_m) & \textit{otherwise.} \end{cases}$$

Proof. Let $G = \rho_{E,m}(G_F)$. We have $\mathrm{SL}_2(m) \leq G \leq \mathrm{GL}_2(m)$. Then, using Proposition A.4,

$$\mathrm{D}(\mathrm{SL}_2(m)) \leq \mathrm{D}(G) \leq \mathrm{SL}_2(m)).$$

Suppose that $\mathrm{D}(G) = \mathrm{SL}_2(m)$. Since

$$G/\mathrm{SL}_2(m) \simeq \det(G),$$

therefore the largest abelian quotient of $F(E[m])/F$ has Galois group isomorphic to $\det(G)$. By the Weil pairing, $F(\zeta_m) \subseteq F(E[m])$ and from Proposition 2.13, we have $\mathrm{Gal}(F(\zeta_m)/F) \simeq \det(G)$. Then the largest abelian subextension of $F(E[m])$ is $F(\zeta_m)$.

Now, suppose that $\mathrm{D}(G) \neq \mathrm{SL}_2(m)$. If $3 \nmid m$, this does not happens, since in this case $\mathrm{D}(\mathrm{SL}_2(m)) = \mathrm{SL}_2(m)$ from Proposition A.2. If $3 \mid m$, then $\mathrm{D}(\mathrm{SL}_2(m))$ has index 3 in $\mathrm{SL}_2(m)$ from Proposition A.2 and so is $\mathrm{D}(G)$. It follows that $F(E[m]) \cap F^{\mathrm{ab}}$ is an extension of degree 3 of $F(\zeta_m)$. □

Remark 4.72. The case $F(E[m]) \cap F^{\mathrm{ab}} \neq F(\zeta_m)$ happens only for $\gcd(m, 12) \neq 1$ by Proposition A.2 and Proposition A.4. Let $k = v_3(m)$. In the previous proposition, m is odd and so $F(E[m]) \cap F^{\mathrm{ab}} \neq F(\zeta_m)$ only if $k > 0$. In this case $L := F(E[3^k]) \cap F^{\mathrm{ab}}$ is a $(\mathbb{Z}/3\mathbb{Z})$-extension of $F(\zeta_{3^k})$ and

$$F(E[m]) \cap F^{\mathrm{ab}} = L \otimes_F F(\zeta_{\frac{m}{3^k}}).$$

Remark 4.73. Let $k = 1$ if $p \geq 5$, $k = 2$ if $p = 3$ and $k = 3$ if $p = 2$. If $\rho_{E,p^k}(G_F)$ contains $\mathrm{SL}_2(p)$, then $\rho_{E,p^\infty}(G_F)$ contains $\mathrm{SL}_2(\mathbb{Z}_p)$, by Theorem 2.32.

Theorem 4.74. *Let m, n be integers such that m is odd, $F(\zeta_n) \not\subseteq F(\zeta_m)$ and E/F be an elliptic curve. Suppose that $\rho_{E,m}(G_F)$ contains $\mathrm{SL}_2(m)$ and that E/F has an (m,n)-coincidence. Then*

$$3 \mid m, \quad \textit{and} \quad \mathrm{D}(\rho_{E,m}(G_F)) \neq \mathrm{SL}_2(m), \quad \textit{and} \quad F(\zeta_n) \subseteq L$$

where L is a $\mathbb{Z}/3\mathbb{Z}$-extension of $F(\zeta_m)$.

Proof. Suppose that $F(E[m]) = F(E[n])$. Then $F(\zeta_n) \subseteq F(E[m]) \cap F^{\mathrm{ab}}$, which is not possible if $F(E[m]) \cap F^{\mathrm{ab}} = F(\zeta_m)$, by assumption. Hence, from Proposition 4.71, the field $F(E[m]) \cap F^{\mathrm{ab}}$ is a $\mathbb{Z}/3\mathbb{Z}$-extension of $F(\zeta_m)$ and the derived group of $\rho_{E,m}(G_F)$ is smaller than $\mathrm{SL}_2(m)$, which only happens if $3 \mid m$ by Remark 4.72. □

Remark 4.75. Under the hypotheses of the previous theorem, for $(m, n) = (p^k, p^{k+1})$, we know by the previous theorem that $p = 2$ or 3. Since $\mathrm{SL}_2(p^k)$ contains the matrix T, this results was already known by Theorem 4.66 and even more: the assumption $\zeta_{p^{k+1}} \notin F$ is unnecessary and $k = 1$.

By [Zyw24a, Lemma 1.7], we have $\mathrm{SL}_2(\hat{\mathbb{Z}}) \cap \rho_E(G_F) = \mathrm{D}(\rho_E(G_F))$. In particular, if $\rho_E(G_F)$ contains $\mathrm{SL}_2(\hat{\mathbb{Z}})$, then $\mathrm{D}(\rho_E(G_F)) = \mathrm{SL}_2(\hat{\mathbb{Z}})$. In particular, if $8 \cdot 9 \mid m$ and $\mathrm{SL}_2(m) \subseteq \rho_{E,m}(G_F)$ then $\mathrm{SL}_2(\hat{\mathbb{Z}}) \subseteq \rho_E(G_F)$ by Theorem 2.32 and so $\mathrm{D}(\rho_{E,m}) = \mathrm{SL}_2(m)$. Hence we deduce from Theorem 4.71 the following:

Theorem 4.76. *Let E/F be an elliptic curve and m be a positive integer. Suppose that $72 \mid m$ and $\rho_{E,m}(G_F)$ contains $\mathrm{SL}_2(m)$. Then $F(E[m]) \cap F^{\mathrm{ab}} = F(\zeta_m)$. In particular, if E/F has an (m,n)-coincidence, then $F(\zeta_n) \subseteq F(\zeta_m)$.*

We finish the section by the following lemma, which contains some additional information about the extension $F(E[3])/F$.

Lemma 4.77. *Let E/F be an elliptic curve with j-invariant $j(E)$. Then we have the inclusion $F(j(E)^{1/3}) \subseteq F(E[3])$. Moreover, if $\mathrm{SL}_2(3) \leq \rho_{E,3}(G_F)$, then $F(j(E)^{1/3})/F$ is non trivial.*

Proof. The inclusion $F(j(E)^{1/3}) \subseteq F(E[3])$ follows from Example B.9. Again from Example *op.cit.*, if $j(E)^{\frac{1}{3}} \in F$, then $\rho_{E,3}(G_F) \leq C_{ns}^{+}(3)$. In particular, in this case, $\rho_{E,3}(G_F)$ cannot contain $\mathrm{SL}_2(3)$. □

Remark 4.78. If $\zeta_3 \in F$, then $F(j(E)^{\frac{1}{3}})/F$ is Galois and so is contained in F^{ab}. If, moreover, $F(j(E)^{\frac{1}{3}}) \cap F(\zeta_m) = F$, then $F(E[m]) \cap F^{\mathrm{ab}} = F(j(E)^{\frac{1}{3}}, \zeta_m)$. Hence, if we have an (m,n)-coincidence, then

$$3 \mid m, \quad \text{and} \quad \mathrm{D}(\rho_{E,m}(G_F)) \neq \mathrm{SL}_2(m), \quad \text{and} \quad F(\zeta_n) \subseteq F(j(E)^{\frac{1}{3}}, \zeta_m).$$

Remark 4.79. If $\zeta_3 \in F$, $3 \mid m$ and $\mathrm{D}(\rho_{E,3^{v_3(m)}}(G_F)) = \mathrm{SL}_2(3^{v_3(m)})$, then $F(j(E)^{\frac{1}{3}}) \subseteq F(\zeta_{3^{v_3(m)}})$ and so we have $r \geq 1$ such that

$$F(j(E)^{\frac{1}{3}}) = F(\zeta_{3^{r+1}}) \quad \text{and} \quad F = F(\zeta_{3^r}) \neq F(\zeta_{3^{r+1}}).$$

4.7 Coincidence of division fields of two elliptic curves

Let E and E' be elliptic curves defined over F. In all this section, we suppose that $F(E[m]) = F(E'[n])$ for two integers m and n. Then $\zeta_n \in F(E[m])$ and in the previous sections we gave constraints to this property. Hence:

Proposition 4.80. *Let p be a prime and r be the largest integer such that $\mathbb{Q}(\zeta_{p^r}) \subseteq F \cap \mathbb{Q}(\mu_{p^\infty})$. Suppose that $p > q$ for all primes $q \mid m$ and $v_p(n) > r$. Then, $v_p(n) = 1$ (and $r = 0$), unless $(m,p) = (2^j, 3)$ for some $j \geq 1$, in which case $r = 0$ and $v_p(n) \leq 2$, or $v_p(n) = r + 1$.*

Proof. This follows from Proposition 4.14 and the fact that $F(\zeta_{p^k}) \subseteq F(E'[p^k]) \subseteq F(E'[n])$. □

We can use Theorem 4.21 and Remark 4.22 in the same way as in Section 4.4 to give constraints on a coincidence $F(E[m]) = F(E'[n])$ using again that we must have $\zeta_n \in F(E[m])$. For example, we give a generalization of Corollary 4.24.

Theorem 4.81. *For all primes p such that $p \mid n$ and $p \nmid m\Delta_F$ we are in one of the following situation:*

- *$v_p(n) = 1$ and E/F has bad reduction at every ideal above p,*
- *$v_p(n) = 2$, $p = 2$ and at each prime above p, E/F has either additive or non split multiplicative reduction,*
- *$v_p(n) = 2$, $p = 3$, and E/F has additive and potential good reduction at every ideal above p,*
- *$v_p(n) = 3$ or 4, $p = 2$ and E/F has additive and potential good reduction at every ideal above p.*

Theorem 4.82. *Let p be a prime and $k \geq 1$ such that $F \cap \mathbb{Q}(\zeta_{p^k}) = \mathbb{Q}$. If $F(E[p^k]) = F(E'[p^{k+1}])$, then $p = 2$.*

Proof. This follows from Theorem 4.38. □

Theorem 4.83. *For all primes p such that $v_p(m) \neq v_p(n)$, we have*

$$p \mid 2 \cdot \Delta_F \cdot \mathrm{N}(\mathfrak{f}_E) \cdot \mathrm{N}(\mathfrak{f}_{E'}).$$

Proof. The proof is the same as for Theorem 4.42, using Proposition 4.81 and Theorem 4.82 instead of Corollary 4.24 and Corollary 4.39. □

Theorem 4.84. *Suppose that m is odd, $F(\zeta_n) \not\subseteq F(\zeta_m)$ and $\rho_{E,m}(G_F)$ contains $\mathrm{SL}_2(m)$. Then*

$$3 \mid m, \quad \textit{and} \quad \mathrm{D}(\rho_{E,m}(G_F)) \neq \mathrm{SL}_2(m), \quad \textit{and} \quad F(\zeta_n) \subseteq L$$

with L a $\mathbb{Z}/3\mathbb{Z}$-extension of $F(\zeta_m)$.

Proof. The proof is exactly the same as Theorem 4.74, replacing $F(E[n])$ by $F(E'[n])$. □

Remark 4.85. Except in Subsection 4.5.2, the results of Section 4.5 use the relationship between $\rho_{E,p^{k+1}}$ and ρ_{E,p^k} on the same elliptic curve. In particular, this method does not apply for different elliptic curves.

Chapter 5

Polynomials realizing mod m images

In this chapter, we return to the inverse Galois problem (IGP), introduced in Chapter 1, which motivated the study of entanglement treated in the previous chapters. We saw in Problem 1.5 that the IGP can be broken down in four problems: the classical IGP, the effective IGP, the IGP with ramification and the explicit IGP. In the context of elliptic curve, we consider $G = \rho_{E,m}(G_F) \leq \mathrm{GL}_2(m)$ for a positive integer m and an elliptic curve E/F. We notice that if E/F is non-CM, m is coprime to the adelic level M_E and $\mathbb{Q}(\zeta_m) \cap F = \mathbb{Q}$, then $\rho_{E,m}$ is surjective. However, if m is divisible by a minimal exceptional integer or if $\mathbb{Q}(\zeta_m) \cap F \neq \mathbb{Q}$, then the group $\rho_{E,m}(G_F)$ is a proper subgroup of $\mathrm{GL}_2(m)$. In Section 1.3, we saw that we have the isomorphism $\mathrm{Gal}(F(E[m])/F) \simeq \rho_{E,m}(G_F)$ and so a solution for the classical IGP and the effective IGP, and also for the IGP with ramification, see Theorem 4.21, more specifically the tame IGP, see Theorem 1.31 and 1.32.

For the explicit IGP, Reverter and Vila provide a solution when m is prime and $\rho_{E,m}$ is surjective:

Theorem 5.1 ([RV00, Theorem 2.1])**.** *Let E/F be an elliptic curve, given by Weierstrass equation $E : y^2 = f(x)$, and let p be an odd prime. Suppose that the Galois representation*

$$\rho_{E,p} : G_F \to \mathrm{Aut}(E[p]) \simeq \mathrm{GL}_2(p)$$

is surjective and let $P \in E[p] \setminus \{\mathcal{O}\}$. Then

1. *The p-division polynomial is irreducible and its Galois group over F is isomorphic to $\rho_{E,p}(G_F)/\{\pm \mathrm{id}\}$.*

2. *The characteristic polynomial $\chi_{E,p}$ of the multiplication by $x(P) + y(P)$ in $F(P) := F(x(P), y(P))$ is irreducible with Galois group isomorphic to $\rho_{E,p}(G_F)$.*

In this chapter, we use their idea to generalize the previous theorem to a general setting. We give families of polynomials realizing the image of the representation $\rho_{E,m} : G_F \to \mathrm{GL}_2(m)$. We also determine a minimum for the valuations of the coefficients of the polynomials arising in our construction.

Most of the results are valid in more general fields, but in our context we restrict our interests to number fields. All results, including Theorem 5.1, are valid for F a field of characteristic 0, except those of Section 5.1.5, because we need that $\mathcal{O}_F$ is a Dedekind domain, and in Proposition 5.41 and Remark 5.42, since we refer to valuation.

This chapter, apart from a few details, corresponds to a paper of the author [Yvo23]. To be consistent with the rest of the manuscrit, we changed some notations. Also, in order to be self-contained, we add the definition of division polynomials and Proposition 5.2 at the begining of Section 5.1.1, a version of Cebotarev density theorem and a corollary in Section 5.1.5, a theorem, a remark, a lemma and a corollary at the end of Section 5.1.2. We add Remark 5.23, linked to the topic of coincidence. Moreover, we explain why $a \neq 0$ is a necessary condition in Section 5.1.4.3.

5.1 Polynomials realizing $\rho_{E,m}(G_F)$

Let E/F be an elliptic curve. For a positive integer m, we define

$$E_m := \{P \in E(\overline{F}) \text{ of order } m\} \subseteq E[m].$$

5.1.1 Primitive division polynomials

Let E/F be an elliptic curve with Weierstrass equation

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

and let b_i as defined in Section 2.1. The family (ψ_m) of division polynomials of E is defined as follow:

$$\psi_1 = 1 \quad \psi_2 = 2y + a_1x + a_3$$
$$\psi_3 = 3x^4 + b_2x^3 + 3b_4x^3 + 3b_6x + b_8$$
$$\psi_4 = \psi_2(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_4)x + (b_4b_8 - b_6^2))$$

$$\begin{aligned}\psi_2\psi_{2m} &= \psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-1}\psi_m\psi_{m+1}^2 \quad \text{for } m \geq 2\\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{for } m \geq 3.\end{aligned}$$

A paper of McKee is about methods to compute faster the coefficients of division polynomials, see [McK94].

The m-division polynomial of an elliptic curve have roots corresponding to first coordinate of m-torsion points:

Proposition 5.2 ([Sil09, Exercice 3.7]). *Let $m \geq 2$ and E/F be an elliptic curve.*

1. *For m odd, respectively even, the polynomial ψ_m, respectively $\frac{\psi_m}{\psi_2}$, is univariate with roots the elements of $x(E[m])$, respectively $x(E[m]) \setminus x(E[2])$, and degree $m^2 - 1$.*

2. *Let ϕ_k be the polynomial defined in [Sil09, Exercice 3.7]. Then we have*

$$x(mQ) = \frac{\phi_m(x(Q))}{\psi_m^2(x(Q))}.$$

Studying the points of order m, where m is not necessary prime, naturally leads to the following definition:

Definition 5.3. Let E/F be an elliptic curve and (ψ_m) the family of its division polynomials. We define the *primitive division polynomial* $(\widetilde{\psi}_m)$ recursively by

$$\psi_m = \prod_{m|n} \widetilde{\psi}_m.$$

Remark 5.4. Clearly $\psi_1 = \widetilde{\psi}_1 = 1$ and, for p prime and $k \geq 1$, we have $\widetilde{\psi}_{p^k} = \frac{\psi_{p^k}}{\psi_{p^{k-1}}}$. In particular, $\widetilde{\psi}_p = \psi_p$ for p prime.

Proposition 5.5. *If $m \neq 2$, the polynomial $\widetilde{\psi}_m$ is in $F[X]$ and its roots are the elements of $x(E_m)$. Moreover, if m is a power of a prime p then the leading coefficient of $\widetilde{\psi}_m$ is p. Otherwise, the polynomial $\widetilde{\psi}_m$ is monic.*

Proof. For m odd, respectively even, the polynomial ψ_m, respectively $\frac{\psi_m}{\psi_2}$, is univariate with roots the elements of $x(E[m])$, respectively $x(E[m]) \setminus x(E[2])$, see Proposition 5.2. Then, by induction, for $m \geq 3$, the polynomial $\widetilde{\psi}_m$ is univariate with roots the elements of $x(E_m)$. Now, the absolute Galois group G_F acts on the m-torsion points, therefore on the points of order m. Indeed, let P be a point of order m and σ in G_F. Suppose that $\sigma(P)$ has order $m < n$. Then, the point $P = \sigma^{-1}(\sigma(P))$ belongs to $E[m]$, which is a contradiction. Therefore, the factorisation

$$\psi_m = \prod_{m|n} \widetilde{\psi}_m$$

is defined over F. For a polynomial f, let $c(f)$ be its leading coefficient. We have

$$c(\psi_m^2) = \prod_{m|n} c(\widetilde{\psi}_m^2).$$

So, using that $c(\psi_m^2) = m^2$ for all m and Remark 5.4, we conclude, by induction that $c(\widetilde{\psi}_{p^k}) = p$ for p prime and k a positive integer, and so that $c(\widetilde{\psi}_m) = 1$ if m is divisible by at least two different primes. □

Remark 5.6. Since we know the degree of ψ_m^2 for all m, we can compute the degree of $\widetilde{\psi}_m$, as a polynomial in x, by induction. For example, if m is the product of two distinct primes p and q, then $\widetilde{\psi}_m$ has degree $(m^2 - p^2 - q^2 + 1)/2$.

The polynomials ψ_m and $\psi_2\psi_m$ are in $F[x]$ when m is odd and even respectively, and ψ_2 is not. In particular, $F(\psi_m)$ is well-defined when m is odd, but not when m is even.

Definition 5.7. For m an even integer, we define $F(\psi_m) := F(\psi_2\psi_m)$.

Lemma 5.8. *For m a positive integer, we have*

$$F(\psi_m) = F(x(E[m])) = F(x(E_m)) = F(\widetilde{\psi}_m).$$

Proof. The last equality is given by Proposition 5.5.

By Proposition 5.5 and the factorization of ψ_m, the roots of ψ_m, for m is odd, are the elements of $x(E[m])$. The same is true for $\psi_2\psi_m$ for m even, noting that $x(E[2])$ are the roots of ψ_2^2, from Propositon 5.2. Then we have the first equality.

Finally, for the second equality, since $E_m \subseteq E[m]$, then $\widetilde{\psi}_m$ divides ψ_m, and we obviously have $F(\widetilde{\psi}_m) \subseteq F(\psi_m)$. For the reverse inclusion, let $x(P) \in F(x(E[m]))$ with P of order $m \mid n$. Then $n = km$ for some k, and $P = kQ$ for some point Q of order n. From Proposition 5.2,

$$x(P) = x(kQ) = \frac{\phi_k(x(Q))}{\psi_k^2(x(Q))},$$

where $\phi_k \in F[X]$. So $x(P) \in F(x(E_m)) = F(\widetilde{\psi}_m)$. □

In fact, we do not need these formulas to prove that $F(x(E[m])) = F(x(E_m))$: see Lemma 5.10 for a proof using only Galois theory.

5.1.2 Galois group of $\widetilde{\psi}_m$

For a positive integer m, let π_n be the canonical projection

$$\pi_n : \mathrm{GL}_2(m) \to \mathrm{GL}_2(m)/\{\pm\,\mathrm{id}\},$$

and define $\overline{\rho_{E,m}} = \pi_n \circ \rho_{E,m}$. If $\rho_{E,m}(G_F)$ does not contain $-\,\mathrm{id}$, it is canonically isomorphic to $\overline{\rho_{E,m}}(G_F)$.

Lemma 5.9. *For $m \geq 2$, we have $\ker \overline{\rho_{E,m}} = \mathrm{Gal}(\overline{F}/F(x(E_m)))$.*

Proof. If $\sigma \in G_F$ satisfies $\overline{\rho_{E,m}}(\sigma) = \mathrm{id}$, then $\sigma(x(P)) = x(P)$ for all $P \in E_m$. Now, let $\sigma \in \mathrm{Gal}(\overline{F}/F(x(E_m)))$. For $P \in E_m$, we have $\sigma(P) \in \{\pm P\}$. Suppose that there are two points $P, Q \in E_m$ such that $\sigma(P) = -P$ and $\sigma(Q) = Q$. Then, on the one hand,

$$\sigma(P+Q) = -P+Q$$

and, on the other hand,

$$\sigma(P+Q) \in \{\pm(P+Q)\}.$$

So either P or Q has order 2, hence $m = 2$, and in this case $P = -P$ for all $P \in E_m$. Consequently, either $\sigma(P) = P$ for all $P \in E_m$, or $\sigma(P) = -P$ for all $P \in E_m$. □

Lemma 5.10. *For $m \geq 2$, we have $F(x(E_m)) = F(x(E[m]))$.*

Proof. The inclusion $F(x(E_m)) \subseteq F(x(E[m]))$ is obvious. Then we have

$$\mathrm{Gal}(\overline{F}/F(x(E[m])) < \mathrm{Gal}(\overline{F}/F(x(E_m)).$$

Now, take $\sigma \in \mathrm{Gal}(\overline{F}/F(x(E_m)))$. By Lemma 5.9, we have $\overline{\rho_{E,m}}(\sigma) = \mathrm{id}$, hence σ fixes $F(x(E[m]))$. □

Theorem 5.11. *Let $m \geq 2$.*

1. *The Galois group of $F(\widetilde{\psi}_m)$ over F is isomorphic to $\overline{\rho_{E,m}}(G_F)$.*
2. *If $\rho_{E,m}(G_F)$ contains $-\,\mathrm{id} \neq \mathrm{id}$, then the extension $F(E[m])/F(x(E[m]))$ has degree 2. Otherwise, $F(E[m]) = F(x(E[m]))$ and the Galois group of $F(\widetilde{\psi}_m)$ is isomorphic to $\rho_{E,m}(G_F)$.*

Proof. Using Lemma 5.9, we obtain

$$\overline{\rho_{E,m}}(G_F) \simeq G_F/\ker \overline{\rho_{E,m}} \simeq \mathrm{Gal}(F(x(E_m))/F) = \mathrm{Gal}(F(\widetilde{\psi}_m)/F).$$

The second point of the proposition is also an immediate consequence of Lemma 5.9. □

When $m = p$ is prime, Reverter and Vila give another sufficient criterion for the Galois group of $\widetilde{\psi}_p = \psi_p$ to be $\rho_{E,p}(G_F)$.

Theorem 5.12. *[RV00, Theorem 1.1] Let E/F be an elliptic curve and p be an odd prime such that $\rho_{E,p}(G_F)$ is conjugates to one of the following groups:*

$$\begin{pmatrix} 1 & * \\ 0 & \chi_p(G_F) \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & \chi_p(G_F) \end{pmatrix}, \begin{pmatrix} \chi_p(G_F) & * \\ 0 & 1 \end{pmatrix}.$$

Then $\mathrm{Gal}(\psi_p) \simeq \rho_{E,p}(G_F)$.

We note that, in the hypothesis of the previous theorem, $-\operatorname{id}$ is not in $\rho_{E,p}(G_F)$.

Remark 5.13. The hypotheses of the previous theorem are satisfies if E/F is a non-p-exceptional elliptic curve which admits a rational isogeny of degree p. An elliptic curve E/F is said to be *p-exceptional* if

1. E/F has no rational points of order p,
2. There exists an elliptic curve E'/F and a F-isogeny $E \to E'$ of degree p,
3. Every elliptic curve F-isogenous to E with isogeny of degree p has no rational point of order p.

For the definition of a F-isogeny, F-isogenous elliptic curves and degree over an isogeny, see [Sil09, Section III.4].

Sutherland proved the following on quadratic twists:

Lemma 5.14 ([Sut16, Lemma 5.24]). *Let E/F be an elliptic curve with Weierstrass equation $y^2 = f(x)$, $m \geq 2$ be an integer, and $d \in F^*\backslash F^{*2}$ be squarefree. Then*

$$F(E[m]) = F(\sqrt{d}, \psi_m) \iff -\operatorname{id} \notin \rho_{E^{(d)},m}(G_F).$$

Corollary 5.15 ([Sut16, Corollary 5.25]). *Let E/F be an elliptic curve with Weierstrass equation $y^2 = f(x)$, $m \geq 2$ be an integer, and $d \in F^*\backslash F^{*2}$. Then $\rho_{E^{(d)},m}(G_F)$ is conjugate to a subgroup of index 1 or 2 of $\langle \rho_{E,m}(G_F), -\operatorname{id}\rangle$. The index 2 occurs when*

1. *$\sqrt{d} \in F(E[m])$ and $\sqrt{d} \notin F(\psi_m)$ if $-\operatorname{id} \in \rho_{E,m}(G_F)$,*
2. *$\sqrt{d} \in F(\psi_m)$ if $-\operatorname{id} \notin \rho_{E,m}(G_F)$.*

5.1.3 Consequence in the case $m = 3$

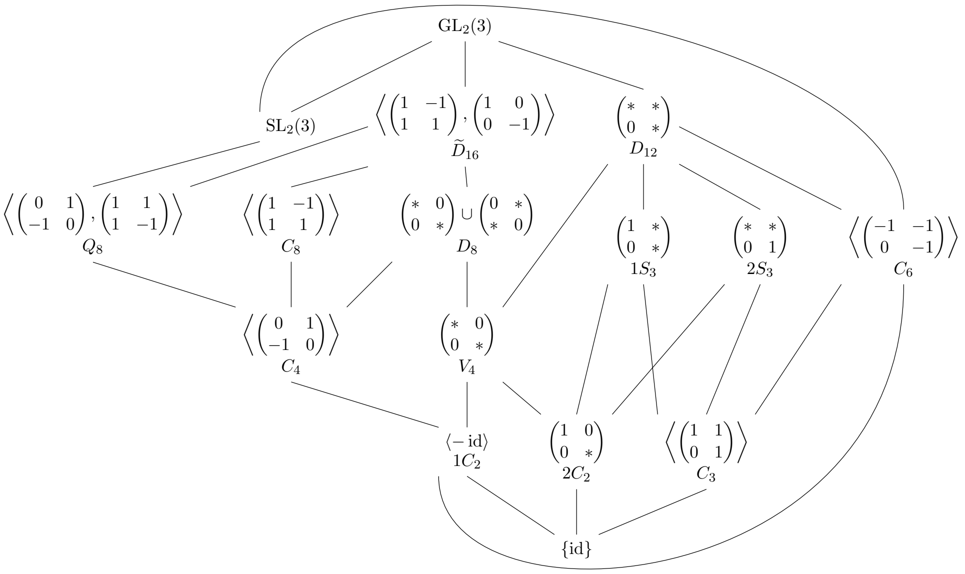
Let E/F be an elliptic curve and let $G := \rho_{E,3}(G_F)$. We denote by ζ_3 a primitive third root of unity.

We recall the following result. Let m be a positive integer and ζ_n be a primitive m-th root of unity. By the Weil pairing, we have $F(\zeta_n) \subseteq F(E[m])$. Hence, for each $\sigma \in \operatorname{Gal}(F(E[m])/F)$, there exists an $\alpha(\sigma) \in (\mathbb{Z}/m\mathbb{Z})^*$ such that $\sigma(\zeta_n) = \zeta_n^{\alpha(\sigma)}$. Thanks to the Weil pairing again, $\alpha(\sigma)$ satisfies $\det \circ \rho_{E,m}(\sigma) = \alpha(\sigma)$. Then the image of $\det \circ \rho_{E,m}$ is equal to the image of the natural embedding of $\operatorname{Gal}(F(\zeta_n)/F)$ in $(\mathbb{Z}/m\mathbb{Z})^*$, which is surjective if and only if F does not contain any m-th roots of unity. In the case $m = 3$, it gives that $\det \circ \rho_{E,3}$ has image $\{\pm 1\}$ if and only if F does not contain ζ_3.

Since G is a subgroup of $\mathrm{GL}_2(3)$, we give a classification of all subgroups of $\mathrm{GL}_2(3)$, up to conjugation, in Figure 5.1. Here, C_m is the cyclic group of order m, S_m is the symmetric group of degree m, D_{2m} is the dihedral group of order $2m$, V_4 is the Klein group, Q_8 is the quaternion group and $\widetilde{D}_{16}$ is the quasi-dihedral group of order 16. The groups $1S_3$ and $2S_3$ are both isomorphic to S_3 but are not conjugate, and similarly for $1C_2$ and $2C_2$, both isomorphic to C_2. The stars $*$ in the matrices means that all choices of elements in $\mathbb{Z}/3\mathbb{Z}$ are possible, provided the matrix is invertible. The graph shows directly

- which subgroups contain $-\operatorname{id}$, so, conversely, which images are isomorphic to the Galois group of ψ_3,
- and which subgroups are in $\mathrm{SL}_2(3)$ or not, which only depends on whether F contains $\mathbb{Q}(\zeta_3)$.

Figure 5.1: Subgroup lattice of $\mathrm{GL}_2(3)$


$\mathrm{GL}_2(3)$
$\mathrm{SL}_2(3)$
$\left\langle \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$
$\widetilde{D}_{16}$
$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$
D_{12}
$\left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right\rangle$
Q_8
$\left\langle \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \right\rangle$
C_8
$\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \cup \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$
D_8
$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$
$1S_3$
$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$
$2S_3$
$\left\langle \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} \right\rangle$
C_6
$\left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$
C_4
$\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$
V_4
$\langle -\mathrm{id} \rangle$
$1C_2$
$\begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$
$2C_2$
$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$
C_3
$\{\mathrm{id}\}$

Remark 5.16. Following the classical description of subgroups of $\mathrm{GL}_2(m)$ given by Serre in [Ser72, Section 2] or Sutherland in [Sut16], $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$ is $C_s(3)$, the split Cartan subgroup; $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \cup \begin{pmatrix} 0 & * \\ * & 0 \end{pmatrix}$ is $N_s(3)$, the normalizer of $C_s(3)$; $\left\langle \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \right\rangle$ is $C_{ns}(3)$, the non split Cartan subgroup; $\left\langle \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$ is $N_{ns}(3)$, the normalizer of $C_{ns}(3)$; and $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ is $B(3)$, the full Borel subgroup.

The next two propositions give all possibilities for G, the image of the mod 3 representation, depending on the factorization of ψ_3.

Theorem 5.17. *If $F \cap \mathbb{Q}(\zeta_3) = \mathbb{Q}$, then, using the classification above,*

1. *If ψ_3 is irreducible, then*
   - *(a) $G = \mathrm{GL}_2(3)$ if $F(\psi_3)/F$ is generated by exactly three roots of ψ_3;*
   - *(b) $G \simeq \widetilde{D}_{16}$ if $F(\psi_3)/F$ is generated by exactly two roots of ψ_3; or*
   - *(c) $G \simeq C_8$ if $F(\psi_3)/F$ is cyclic.*
2. *If ψ_3 can be factorized in two irreducible polynomials of degree 2, then $G \simeq D_8$.*
3. *If ψ_3 has a unique root over F then*
   - *(a) $G \simeq D_{12}$ if $F(E[3])/F(x(E_3))$ has degree 2; or*
   - *(b) $G \simeq 1S_3$ or $2S_3$ if $F(E[3]) = F(x(E_3))$.*

4. If ψ_3 *has exactly two roots over* F*, then*

(a) $G \simeq V_4$ *if* $F(E[3])/F(x(E[3]))$ *has degree* 2*; or*

(b) $G \simeq 2C_2$ *if* $F(E[3]) = F(x(E[3]))$*.*

Theorem 5.18. *If* $F \cap \mathbb{Q}(\zeta_3) \neq \mathbb{Q}$*, then, using the classification above,*

1. If ψ_3 *is irreducible, then*

(a) $G = \mathrm{SL}_2(3)$*; or*

(b) $G \simeq Q_8$ *if* $F(\psi_3)/F$ *is cyclic.*

2. If ψ_3 *factors into two irreducible polynomials of degree* 2 *then* $G \simeq C_4$*.*

3. If ψ_3 *has a unique root in* F*, then*

(a) $G \simeq C_6$ *if* $F(E[3])/F(x(E[3]))$ *has degree* 2*; or*

(b) $G \simeq C_3$ *if* $F(E[3]) = F(x(E[3]))$*.*

4. If ψ_3 *splits completely over* F *then*

(a) $G \simeq C_2$ *if* $F(E[3])/F(x(E[3]))$ *has degree* 2*; or*

(b) $G \simeq C_1$ *if* $F(E[3]) = F(x(E[3]))$*.*

Proof. (of Theorems 5.17 and 5.18). We will consider the Galois action on the x-coordinates on the 3-torsion points, that are the roots of ψ_3, as permutations on these roots. Each $\sigma \in G_F$ corresponds to an element of S_4, seen as permutation representation, and is mapped to $\overline{\rho_{E,3}}(\sigma)$ in $\overline{G} := G/\{\pm \mathrm{id}\}$. So $\overline{G} \simeq \mathrm{Gal}(\psi_3)$ corresponds to a subgroup of $S_4 \simeq \mathrm{Sym}(\{\text{roots of } \psi_3\})$. Then, $G \subseteq B(3)$ is equivalent to ψ_3 having a root in F. The action of the groups not in $B(3)$ or $N_s(3)$ is transitive on $x(E_3)$, so ψ_3 is irreducible. Consequently, $G \subseteq N_s(3)$ is equivalent to ψ_3 factoring into two degree 2 polynomials over F. Moreover, when G does not contain $\{-\mathrm{id}\}$, then $\mathrm{Gal}(\psi_3) \simeq G$, by Thereom 5.11. Otherwise, $\mathrm{Gal}(\psi_3)$ has index 2 in G.

If $F \cap \mathbb{Q}(\zeta_3) = \mathbb{Q}$, we consider only the groups in the above graph with surjective determinant, *i.e.* not contained in $\mathrm{SL}_2(3)$. We just observed that, if ψ_3 splits over F, then $G \subseteq \{\pm \mathrm{id}\} \subseteq \mathrm{SL}_2(3)$. Hence, this cannot happen if $F \cap \mathbb{Q}(\zeta_3) = \mathbb{Q}$.

If $\mathbb{Q}(\zeta_3) \subseteq F$, we only consider the groups in the above graph with non surjective determinant, *i.e.* contained in $\mathrm{SL}_2(3)$. If ψ_3 has at least two roots in F, then there is a basis of $E[3]$ such that $G \subseteq C_s(3)$. Since $\mathbb{Q}(\zeta_3) \subseteq F$, the group G has determinant 1, so $G \subseteq \{\pm \mathrm{id}\}$, hence ψ_3 splits over F.

The different items of each proposition are immediate deductions from these observations. □

Corollary 5.19. *If* ψ_3 *is irreducible or if* ψ_3 *factors into two irreducible polynomials of degree* 2*, then* $-\mathrm{id}$ *belongs to the image.*

5.1.4 Polynomials generating the image of $\rho_{E,m}$

If m divides n, the coordinates of points of order m on an elliptic curve E/F are obtained by adding n/m times a point of order n. The addition of points is given by rational functions over F, then we have

$$F(E[m]) = F(E_m)$$

for all positive integers m.

5.1.4.1 General settings

Let E/F be an elliptic curve defined by a Weierstrass equation $w_E(x,y)=0$, so we have $F(E)=F(x,y)$. Let u be a polynomial of degree 1 in x and y such that

$$F[u,u^*]=F[x,y], \tag{$*$}$$

with $u^*:=[-1]^*u=u\circ[-1]$. In particular, we have $u\neq u^*$. This will be our recurring hypothesis on u.

Let m be a positive integer. Let

$$A=\Big(F[X,Y]/(\widetilde{\psi}_m(X,Y),w_E(X,Y)\Big)\simeq\begin{cases}\frac{F[X]}{(\widetilde{\psi}_m)}\oplus\frac{F[X]}{(\widetilde{\psi}_m)}y & \text{if } m\neq 2\\ \frac{F[X]}{(\psi_2^2(X))} & \text{if } m=2.\end{cases}$$

The dimension of A over F is finite, and equal to $2\deg(\widetilde{\psi}_m)$ for $m\neq 2$ and to 3 for $m=2$, that is, in all cases, equal to cardinality $|E_m|$. We denote by $\chi_{u,m}$ the characteristic polynomial of the multiplication by the polynomial u on the ring A. It is a monic polynomial of degree $|E_m|$ with coefficients in F. We denote by $g_1,\dots,g_s\in F[X]$ the irreducible and monic factors of $\widetilde{\psi}_m$, if $m\neq 2$, or of ψ_2^2 if $m=2$. The polynomials g_i are coprime because the roots of ψ_2^2 and of $\widetilde{\psi}_m$ for $m\neq 2$ all have multiplicity one. We set $A_i=F[X,Y]/(g_i,w_E)$ and denote by χ_i the characteristic polynomial of the class of u in A_i. From the Chinese remainder theorem, we have

$$A\simeq A_1\times\cdots\times A_s.$$

Lemma 5.20. *The roots of χ_i are $u(P)$ where $P\in E_m$ and $g_i(x(P))=0$.*

Proof. Let $S=\{P\in E_m\mid g_i(x(P))=0\}$. We know that the roots of χ_i are in $u(S)$. We have to prove the reverse inclusion. Let $P\in S$. If $m=2$ then $u(P)\in F(x(P))$. Therefore, since the elements of $x(S)$ are conjugate, the elements of $u(S)$ are too. Now, suppose $m\geq 3$. The polynomial w_E has degree 2 over the field $F[X]/(g_i)$. If w_E is irreducible over $F[X]/(g_i)$, take $P'\in S$ such that $u(P')$ is a root of χ_i. The irreducibility of g_i implies that there exists $\sigma\in G_F$ sending $x(P')$ to $x(P)$, and so $u(P')$ to $u(P)$ or $u(-P)$. The irreducibility of w_E over $F(x(P))$ implies that there exists $\tau\in G_F$ which fixes $F(x(P))$ and sends $y(P)$ to $y(-P)$. Therefore $u(P)$ is conjugates to $u(P')$, so it is a root of χ_i.

If w_E is not irreducible, then $w_E=(Y-\alpha)(Y-\beta)$ with $\alpha,\beta\in F[X]/g_i(X)$. So A_i is the product of two extensions of F, that is

$$A_i\simeq(F[X]/g_i(X))[Y]/(Y-\alpha)\times(F[X]/g_i(X))[Y]/(Y-\beta).$$

And the result follows since, if $P\in S$, then $y(P)$ is $\alpha(x(P))$ or $\beta(x(P))$ so $u(P)$ is a root of χ_i. □

Proposition 5.21. *We have*

$$\chi_{u,m}(T)=\prod_{P\in E_m}(T-u(P)).$$

Proof. From the isomorphism of F-vector spaces:

$$A \simeq A_1 \times \cdots \times A_s,$$

the matrix of the multiplication by u in A is conjugated to a block matrix in the F-vector space $A_1 \times \cdots \times A_s$. The characteristic polynomials of these two matrices are the same, and each χ_i is the characteristic polynomial of the block corresponding to A_i. Therefore $\chi_{u,m}$ is the product of characteristic polynomials χ_i for $i = 1, \ldots, s$. The result follows from Lemma 5.20. □

Corollary 5.22. *We have $F(\chi_{u,m}) \simeq F(E[m])$ and $\mathrm{Gal}(\chi_{u,m}) \simeq \rho_{E,m}(G_F)$.*

Proof. By Proposition 5.21 and assumption on u, we have

$$\begin{aligned} F(\chi_{u,m}) = F(u(E_m)) = F(u(E_m), u^*(E_m)) &= F(x(E_m), y(E_m)) \\ &= F(E_m) = F(E[m]) \end{aligned}$$

The group isomorphism follows. □

Remark 5.23. Let E and E' be elliptic curves over F and m, n positive integers such that $F(E[m]) = F(E'[n])$. Then Corollary 5.22 provides two ways of constructing polynomials $f \in F[X]$ with splitting field $F(E[m])$ (and Galois group $\rho_{E,m}(G_F)$): using the characteristic polynomial $\chi_{u,m}$ for some $u \in F(E)$ or the characteristic polynomial $\chi_{u,n}$ for some $u' \in F(E')$.

5.1.4.2 Specialization

If A_i is a field, then

- $A_i \simeq F(P)$ for $P \in E_m$ such that $g_i(x(P)) = 0$.
- from Lemma 5.20, the $u(P)$ with $P \in E_m$ and $g_i(x(P)) = 0$ are all conjugate.

Therefore, the characteristic polynomial of $u(P)$ in $F(P)$ does not depend on the choice of $P \in E_m$ such that $g_i(x(P)) = 0$ and it is equal to χ_i. If A is a field, then $A \simeq F(P)$ for all $P \in E_m$ and the characteristic polynomial of $u(P)$ in $F(P)$ is $\chi_{u,m}$. If $-\mathrm{id}$ belongs to $\rho_{E,m}(G_F)$ then A_i is a field for all i. If the action of G_F on $E[m]$ is transitive, then A is a field.

Proposition 5.24. *Suppose that $\rho_{E,m}(G_F)$ contains $-\mathrm{id}$. Then the splitting field of χ_i over F is the extension generated by the roots of g_i and their y-coordinates. The compositum of the splitting fields of the χ_i is $F(E[m])$, and its Galois group is isomorphic to $\rho_{E,m}(G_F)$.*

Proof. Let $S = \{P \in E_m \mid g_i(x(P)) = 0\}$. We have

$$F(\chi_i) = F(u(S), u^*(S)) = F(x(S), y(S)).$$

Since $K(a, b) = K(a)K(b)$, the compositum of the extensions generated by the χ_i is the extension of F generated by the roots of $\widetilde{\psi}_m$ if $m \geq 3$ or of ψ_2^2, if $m = 2$, and the corresponding y-coordinates, in other words the coordinates of the points of order m. □

5.1.4.3 Condition on u

The function u is linear in x and y so it has the form $u = ay + bx + c$ with $a, b, c \in F$. What are the conditions on a, b, c in terms of E to have $F(u, u^*) = F(x, y)$?

Let (a_i) be the coefficients of E. If $a \neq 0$ and $2b - a_1 a \neq 0$ then

$$x = \frac{u + u^* + aa_3 - 2c}{2b - a_1 a}$$

and

$$y = \frac{(b - a_1 a)u - bu^* - bab - 3 + a_1 ac)}{(2b - a_1 a)a}.$$

So we have $F(u, u^*) = F(x, y)$. We know that the condition $a \neq 0$ is necessary. Indeed, if $u = bx + c$, then $u = u^*$ by [Sil09, Group Law Alorithm 2.3.(a)] and $F(u, u^*) = F(x)$, whereas $F(x, y)/F(x)$ has degree 2. What about the condition $2b - a_1 a \neq 0$? Can we also take (a, b) such that $2b - a_1 a = 0$? The following example shows that this cannot be always the case.

Example 5.25. Let E be an elliptic curve of j-invariant 0, with Weierstrass equation $y^2 = x^3 - B$, with $B \in F \setminus (K^*)^3$. Let $u = y$. In particular, with the previous notations, $a \neq 0$, $b = 0$, $a_1 = 0$ and, then, $2b - a_1 a = 0$. Then $F(u, u^*) = F(y)$. The elliptic curve E admits an automorphism given by $(x, y) \mapsto (\zeta_3 x, y)$. The required condition on B makes the polynomial $x^3 - B$ irreducible over F, then $\zeta_3 x$ is conjugate to x over $F(y)$, and $F(x, y)/F(y)$ has degree 3, and not 1. Hence $F(u, u^*) \neq F(x, y)$.

The required condition for u is $F(u, u^*) = F(x, y)$. Actually, we can assume a weaker condition to obtain $\mathrm{Gal}(\chi_{u,m}) = \rho_{E,m}(G_F)$. For example, if $-\mathrm{id}$ is not in $\rho_{E,m}(G_F)$, then we are not forced to take $a \neq 0$. Indeed, we can take $u = x$ and then $\chi_{u,m}$ is a scalar multiple of ψ_m^2, and its Galois group is $\rho_{E,m}(G_F)$.

5.1.5 Criterion to have $-\mathrm{id}$ in the image

The case where the image contains $-\mathrm{id}$ or not are clearly distinguished. So we can ask under which conditions this happens. Before giving a criterion, here is a theorem of Serre which will be useful. For a prime ideal $\mathfrak{p}$ of the ring of integers $\mathcal{O}_F$ of a number field F, let $k_{\mathfrak{p}}$ be the residue field at $\mathfrak{p}$.

Theorem 5.26. *([Ser89, IV-5]) Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ and ℓ be a prime such that ℓ does not divide* $\mathrm{char}(k_{\mathfrak{p}})$*. If E has good reduction at $\mathfrak{p}$, then the Frobenius automorphism above $\mathfrak{p}$ is defined independently of the chosen prime ideal above $\mathfrak{p}$ and the characteristic polynomial of $\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ is*

$$X^2 - a_{\mathfrak{p}}(E)X + \mathrm{N}(\mathfrak{p}) \pmod{\ell}$$

where $a_{\mathfrak{p}}(E) = \mathrm{N}(\mathfrak{p}) + 1 - |E_{\mathfrak{p}}(k_{\mathfrak{p}})|$ with $E_{\mathfrak{p}}$ the reduction of E modulo $\mathfrak{p}$.

We also give the weak version of the Cebotarov density theorem:

Theorem 5.27 ([DS05, Theorem 9.1.2])**.** *Let K/F be a Galois extension. Let $\sigma \in$* $\mathrm{Gal}(K/F)$*. Then there are infinitely many prime ideals $\mathfrak{p}$ of $\mathcal{O}_F$ such that σ is conjugate to* $\mathrm{Frob}_{\mathfrak{p}}$.

Corollary 5.28. *Let $\sigma \in G_F$. Then there exists infinitely many primes p such that σ is conjugate to* $\mathrm{Frob}_{\mathfrak{p}}$ *for some ideal $\mathfrak{p}$ of $\mathcal{O}_{\overline{F}}$ above p.*

Proof. Let L/F be a finite Galois extension. From Theorem 5.27, there are infinitely many prime ideals $\mathfrak{b}$ of $\mathcal{O}_L$ such that $\sigma|_L = \mathrm{Frob}_{\mathfrak{b}}$. Since L/F is finite, there are only finitely many prime of $\mathcal{O}_L$ above p, and so infinitely many prime integers p such that $\sigma|_L = \mathrm{Frob}_{\mathfrak{b}}$ for some prime $\mathfrak{b}$ above p. The group G_F being the inverse limit of the Galois groups $\mathrm{Gal}(L/F)$ with L/F finite, the results follows. □

We obtain the following proposition, with the same notations:

Proposition 5.29. *Let ℓ be an odd prime. Let E/F be an elliptic curve. The image $\rho_{E,\ell}(G_F)$ contains $-\mathrm{id}$ if and only if there exists a prime ideal $\mathfrak{p}$ of good reduction for E such that $\mathrm{N}(\mathfrak{p}) \equiv 1 \pmod{\ell}$ and $a_{\mathfrak{p}}(E) \equiv -2 \pmod{\ell}$.*

Proof. Suppose that we have $\sigma \in G_F$ such that $\rho_{E,\ell}(\sigma) = -\mathrm{id}$. Since there is only a finite number of primes of bad reduction, Cebotarev's density theorem tell that there exist (infinitely many) prime ideals $\mathfrak{p}$ of good reduction such that $\sigma = \mathrm{Frob}_{\mathfrak{q}}$ for a prime ideal $\mathfrak{q}$ of $\mathcal{O}_{\overline{F}}$ above $\mathfrak{p}$. Hence, the image of $\rho_{E,\ell}$ contains $-\mathrm{id}$ if and only if there exists a prime $\mathfrak{p}$ of good reduction such that $\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{q}}) = -\mathrm{id}$. Since being conjugate to $-\mathrm{id}$ implies being equal to $-\mathrm{id}$, this equality is equivalent to the equality of the corresponding characteristic polynomials:

$$X^2 - a_{\mathfrak{p}}(E)X + \mathrm{N}(\mathfrak{p}) \equiv X^2 + 2X + 1 \pmod{\ell}.$$

The result follows. □

Remark 5.30. The proposition gives us a necessary and sufficient condition for $\rho_{E,\ell}(G_F)$ to contain $-\mathrm{id}$. In particular, it gives a criterion to know whether the image contains $-\mathrm{id}$, as required. In the other direction, if we know the image of the representation, it gives us a criterion on the cardinality of $E_{\mathfrak{p}}(k_{\mathfrak{p}})$ for a certain $\mathfrak{p}$.

Remark 5.31. If F is a number field, we also know that $\rho_{E,\ell}(G_F)$ is surjective for almost all primes ℓ, and so almost always contains $-\mathrm{id}$. In the introduction, we gave some references about the non surjective cases.

Remark 5.32. For a real x and an integer h, Serre ([Ser81a, Theorem 1.20]) gives an estimation of the number of primes $p \leq x$ such that $E/\mathbb{Q}$ has good reduction at p and $a_p(E) = h$. This estimation is

$$\mathcal{O}\left(\left(\frac{\log(x)}{\mathrm{loglog}(x)^2 \mathrm{logloglog}(x)}\right)^{1/4} \int_2^x \frac{dt}{\log(t)}\right),$$

which does not depend on h. This theorem is valid also on a number field, by [Ser81a, 8.2, Remarques 2].

Remark 5.33. Let $q := \mathrm{N}(\mathfrak{p})$. Since we must have $q \equiv 1 \pmod{\ell}$, then q is necessary bigger than ℓ. If $\ell > 2$, then $q \geq 2\ell + 1$. The Hasse-Weil bound

$$-2\sqrt{q} + q + 1 \leq |E_{\mathfrak{p}}(k_{\mathfrak{p}})| \leq 2\sqrt{q} + q + 1.$$

imposes additional conditions on $\mathfrak{p}$.

5.1.6 Transitive case

Theorem 5.34. *Let E/F be an elliptic curve and let $m \geq 2$. Suppose that the Galois action on E_m is transitive. Then*

1. *The polynomial $\widetilde{\psi}_m$, if $m \neq 2$, and ψ_2^2, if $m = 2$, is irreducible and its Galois group is isomorphic to $\overline{\rho_{E,m}}(G_F)$.*

2. *The characteristic polynomial of the multiplication by $u(P)$ in $F(P)$ is irreducible and its Galois group is isomorphic to $\rho_{E,m}(G_F)$.*

Proof. Let $P, Q \in E_m$. Since the action is transitive, then $F[X,Y]/(w_E, \widetilde{\psi}_m)$ is a field, from Subsection 5.1.4.2. In particular, $\widetilde{\psi}_m$, if $m \neq 2$, or ψ_2^2, if $m = 2$, is irreducible and we know its Galois group from Theorem 5.11.

We know that $\mathrm{Gal}(\chi_{u,m}) \simeq \rho_{E,m}(G_F)$, by Proposition 5.22 and Subsection 5.1.4.2. Therefore, we only have to show that $\chi_{u,m}$ is irreducible. In other words, it suffices to prove that its degree, $|E_m|$, is equal to the number of conjugate elements to $u(Q)$, for some $Q \in E_m$. We have

$$\{\sigma(u(Q)), \sigma \in G_F\} = \{u(P), P \in E_m\}.$$

Let us show that the $u(P)$ are pairwise distinct. Suppose that $u(P) = u(P')$. Let $\sigma \in G_F$ be such that $\rho_{E,m}(\sigma) = -\mathrm{id}$. Then $\sigma(u(P)) = \sigma(u(P'))$, in other words $u(-P) = u(-P')$ and

$$u(P) \pm u(-P) = u(P') \pm u(-P').$$

But, by assumption on u, we have $u(P) \neq u(-P)$, unless $P = -P$. Then, in all cases, $x(P) = x(P')$ and $y(P) = y(P')$, so $P = P'$. Therefore, the $u(P)$ are pairwise distinct, so their number is the cardinal of E_m. □

Remark 5.35. In particular, if $\rho_{E,m}$ is surjective, then $\widetilde{\psi}_m$ and $\chi_{u,m}$ are both irreducible and their Galois groups are respectively $\mathrm{GL}_2(m)/\{\pm \mathrm{id}\}$ and $\mathrm{GL}_2(m)$.

5.2 About the valuation of the coefficients of $\chi_{u,m}$

Let E/F be an elliptic curve with Weierstrass equation $w_E(X,Y) = 0$ where

$$w_E(X,Y) = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6. \tag{$\diamond$}$$

Let m be a positive integer. As in the first section, let $u \in F(E)$ be a function of degree 1 in x and y such that $F(u, u^*) = F(x,y)$. We have seen in Subsection 5.1.4.3 that $u = ay + bx + c$ for some $a, b, c \in F$ with $a \neq 0$. Theorem 5.22 says that $\chi_{u,m}$ has Galois group $\rho_{E,m}(G_F)$. This second section gives a minimum for the valuation of the coefficients of $\chi_{u,m}$. As usual, the case $m = 2$ has to be studied separately.

5.2.1 Case $m = 2$

From Theorem 5.11, we have $\mathrm{Gal}(\psi_2^2) \simeq \rho_{E,2}(G_F)$. We can compute ψ_2^2:

$$\psi_2^2(x) = 4x^3 + (a_1^2 + 4a_2)x^2 + (4a_4 + 2a_1a_3)x + a_3^2 + 4a_6.$$

But the polynomial ψ_2^2 is not normalized. We have

$$\chi_{x,2} = \frac{1}{4}\psi_2^2 = x^3 + (\frac{a_1^2}{4} + a_2)x^2 + (a_4 + \frac{a_1a_3}{2})x + \frac{a_3^2}{4} + a_6 \in \frac{1}{2^2}\mathbb{Z}[a_i][x].$$

If we have a short Weierstrass equation, that is $a_1 = a_3 = a_2 = 0$, then we obtain $E : y^2 = \frac{1}{4}\psi_2^2$. Then a short Weierstrass equation for E immediately gives a polynomial realizing $\rho_{E,2}(G_F)$. And the coefficients of ψ_2^2 have the smallest valuations possible at a prime ideal $\mathfrak{p}$ if we take a minimal Weierstrass equation for E at $\mathfrak{p}$. The coefficients of ψ_2^2 have the smallest valuation possible at every prime ideal if we take a global minimal equation for E, that is possible, for example, if F has class number 1.

5.2.2 Minimum of the valuations of the coefficients of $\chi_{u,m}$

Proposition 5.36. *Let p be a prime and k be an integer. Let E/F be an elliptic curve given by ($\diamond$). Let $a, b, c \in F$, with $a \neq 0$, and $R := \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$. Then*

$$\chi_{ay+bx+c,p^k} \in \frac{1}{p^3} R[a^{-1}, b, c][X],$$

and, for m a non prime power integer,

$$\chi_{ay+bx+c,m} \in R[a^{-1}, b, c][X].$$

Proof. We start by showing the result for $(b, c) = (0, 0)$. For $P \in E(\overline{F})$, let be the polynomial

$$w_E(x(P), Y) := Y^2 + (a_1x(P) + a_3)Y - (x(P)^3 + a_2x(P)^2 + a_4x(P) + a_6.$$

For $P \in E(\overline{F})$, the polynomial $w_E(x(P), Y) \in F(x(P))[Y]$ is monic, has degree 2 and has roots $\pm y(P)$. If P has order m, these are also roots of $\chi_{y,m}$. So $\prod_{P \in E_m/\langle -\operatorname{id}\rangle} w_E(x(P), Y)$ and $\chi_{y,m}(Y)$ are monic, both with degree equal to $2 \deg \widetilde{\psi}_m$, and the same roots by Proposition 5.21, so they are equal. The resultant $\operatorname{Res}_X(\widetilde{\psi}_m, w_E)$, where $\widetilde{\psi}_m$ and w_E are considered as polynomials in the first variable, belongs to $R[Y]$: it is a polynomial in Y with coefficients in R. Let r be the leading coefficient of $\widetilde{\psi}_m$. From [Bou81, A IV.75, Corollary 1], we have:

$$\operatorname{Res}_X(\widetilde{\psi}_m, w_E) = r^{\deg_X(w_E)} \prod_{\alpha \text{ roots of } \widetilde{\psi}_m} w_E(\alpha, Y) = r^3 \prod_{P \in E_m/\langle -\operatorname{id}\rangle} w_E(x(P), Y).$$

Therefore

$$\chi_{y,m} \in \frac{1}{r^3} R[Y].$$

Now, consider the elliptic curve E'/F which is the change of variables of E given by $x = x'$ and $y = a^{-1}(y' - bx' - c)$. Then, we have a Weierstrass equation for E', and $\chi_{y',n}$ has coefficients in $\frac{1}{r^3} R[a^{-1}, b, c]$. So

$$\chi_{ay+bx+c,n} = \chi_{y',n} \in \frac{1}{r^3} R[a^{-1}, b, c][Y].$$

By Proposition 5.5, we obtain the desired result. □

Remark 5.37. The lower bound given in the proposition is a minimum, in the sense where there exists elliptic curves such that this bound is reached, as we will observe in Example 5.43.

Remark 5.38. The proof of the previous proposition points out the fact that we can compute $\chi_{u,m}$ in two ways. The first one is, by definition, to compute the characteristic polynomial of a matrix. The second one is, in view of the above, to compute the resultant of two polynomials. In the first case, we have to compute the determinant of a matrix of size $2\deg\widetilde{\psi}_m$, and in the second case the determinant of a matrix of size $\deg\widetilde{\psi}_m+3$. Since $\deg\psi_3=4$, the second matrix is always smaller, and the difference of size increases with m. Moreover, the matrix in the calculus of the resultant is easier to obtain, because we just have to put the coefficients of ψ_m and w_E and some zeros in the matrix. Whereas, to obtain the matrix of the multiplication by u, we have to choose a basis (e_i) and write each $u*e_i$ in terms of the basis.

If $a_1\neq 0$, then we can choose $u=y$ and $\chi_{y,m}$ is equal to

$$\mathrm{Res}_x(\widetilde{\psi}_m, w_E) = \det\begin{pmatrix} r & 0 & 0 & 1 & 0 & \cdots & 0 \\ \times & r & 0 & a_2 & \ddots & \ddots & \vdots \\ \vdots & \times & r & a_4-a_1y & \ddots & \ddots & 0 \\ \vdots & \vdots & \times & a_6-a_3y-y^2 & \ddots & \ddots & 1 \\ \times & \vdots & \vdots & 0 & \ddots & \ddots & a_2 \\ 0 & \times & \vdots & \vdots & \ddots & \ddots & a_4-a_1y \\ 0 & 0 & \times & 0 & \cdots & 0 & a_6-a_3y-y^2 \end{pmatrix}$$

where r and the crosses are elements of F, here corresponding respectively to the leading term of the polynomial $\widetilde{\psi}_m$ and its other coefficients.

If $a_1=0$, we can choose $u=x+y$ and $\chi_{x+y,m}$ is equal to

$$\mathrm{Res}_{x'}(\widetilde{\psi}'_m, w_{E'}) = \det\begin{pmatrix} r & 0 & 0 & 1 & 0 & \cdots & 0 \\ \times & r & 0 & a_2-1 & \ddots & \ddots & \vdots \\ \vdots & \times & r & a_4-a_3-2y & \ddots & \ddots & 0 \\ \vdots & \vdots & \times & a_6-a_3y-y^2 & \ddots & \ddots & 1 \\ \times & \vdots & \vdots & 0 & \ddots & \ddots & a_2-1 \\ 0 & \times & \vdots & \vdots & \ddots & \ddots & a_4-a_3-2y \\ 0 & 0 & \times & 0 & \cdots & 0 & a_6-a_3y-y^2 \end{pmatrix}$$

where E' is an elliptic curve obtained from E setting by the change of variables $(x,y)\mapsto(x,x+y)$, and $\widetilde{\psi}'_m$ is its m-th primitive division polynomial. For comparison, here is the matrix of the multiplication by y,

$$\begin{pmatrix}
0 & 0 & \cdots & \cdots & 0 & \times & a_6 & 0 & \cdots & 0 & \times & \times & \times \\
0 & 0 & \ddots & \ddots & \vdots & \times & a_4 & a_6 & \cdots & 0 & \times & \times & \times \\
0 & 0 & \ddots & \ddots & \vdots & \vdots & a_2 & a_4 & \ddots & \vdots & \vdots & \vdots & \vdots \\
\vdots & 0 & \ddots & \ddots & \vdots & \vdots & 1 & a_2 & \ddots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \ddots & \ddots & \vdots & \vdots & 0 & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots \\
0 & \vdots & \ddots & \ddots & 1 & \times & \vdots & \ddots & \ddots & 1 & \times & \times & \vdots \\
1 & 0 & \ddots & \ddots & 0 & 0 & -a_3 & \vdots & \ddots & 0 & 0 & 0 & \vdots \\
0 & 1 & \ddots & \ddots & \vdots & \vdots & -a_1 & -a_3 & \ddots & \vdots & \vdots & \vdots & \vdots \\
\vdots & 0 & \ddots & \ddots & \vdots & \vdots & 0 & -a_1 & \ddots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \ddots & \ddots & 0 & \vdots & 0 & 0 & \ddots & \ddots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \ddots & \ddots & 1 & 0 & \vdots & \vdots & \ddots & 0 & -a_1 & -a_3 & \vdots \\
0 & 0 & \cdots & \cdots & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & -a_1 & \times
\end{pmatrix}$$

and here is the matrix of the multiplication by $x + y$

$$\begin{pmatrix}
0 & 0 & \cdots & \cdots & 0 & \times & a_6 & 0 & \cdots & 0 & \times & \times & \times \\
1 & 0 & \ddots & \ddots & \vdots & \times & a_4 & a_6 & \cdots & 0 & \times & \times & \times \\
0 & 1 & \ddots & \ddots & \vdots & \vdots & a_2 & a_4 & \ddots & \vdots & \vdots & \vdots & \vdots \\
\vdots & 0 & \ddots & \ddots & \vdots & \vdots & 1 & a_2 & \ddots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \ddots & \ddots & \vdots & \vdots & 0 & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots \\
0 & \vdots & \ddots & \ddots & 1 & \times & \vdots & \ddots & \ddots & 1 & \times & \times & \vdots \\
1 & 0 & \ddots & \ddots & 0 & 0 & -a_3 & \vdots & \ddots & 0 & 0 & 0 & \vdots \\
0 & 1 & \ddots & \ddots & \vdots & \vdots & 1-a_1 & -a_3 & \ddots & \vdots & \vdots & \vdots & \vdots \\
\vdots & 0 & \ddots & \ddots & \vdots & \vdots & 0 & 1-a_1 & \ddots & \vdots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \ddots & \ddots & 0 & \vdots & 0 & 0 & \ddots & \ddots & \vdots & \vdots & \vdots \\
\vdots & \vdots & \ddots & \ddots & 1 & 0 & \vdots & \vdots & \ddots & 0 & 1-a_1 & -a_3 & \vdots \\
0 & 0 & \cdots & \cdots & 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 1-a_1 & \times
\end{pmatrix}.$$

Remark 5.39. Proposition 5.36 tells us that, if we take an equation for E with coefficients in $\mathcal{O}_F$, and $u = ay + bx + c$ such that $a = 1$ and $b, c \in \{0, 1, -1\}$, then

$$\chi_{u,p^k} \in \frac{1}{p^3}\mathcal{O}_F[X]$$

if p is prime and k a positive integer, and

$$\chi_{u,m} \in \mathcal{O}_F[X]$$

if m is not a prime power.

5.2.3 Case $m = 3$

Let $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$ and $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. Since a 3-torsion point (x, y) satisfies $[2](x, y) = -(x, y)$, it satisfies

$$\frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2^2 + 2b_4x + b_6} = x.$$

Then, after simplification,

$$\psi_3(x) = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8.$$

If $a_1 \neq 0$, then $\chi_{y,3}$ has Galois group $\rho_{E,3}(G_F)$ from Corollary 5.22 and Subsection 5.1.4.3. We can compute explicitly $\chi_{y,3}$ by two ways: either as a characteristic polynomial, either as a resultant. In the first way, we compute the determinant of

$$\begin{pmatrix} -X & 0 & 0 & 0 & a_6 & \frac{-b_8}{3} & \frac{-b_8}{3}(a_2-\frac{b_2}{3}) & A_0 \\ 0 & -X & 0 & 0 & a_4 & a_6-b_6 & \frac{-b_8}{3}-b_6(a_2-\frac{b_2}{3}) & A_1 \\ 0 & 0 & -X & 0 & a_2 & a_4-b_4 & a_6-b_6-b_4(a_2-\frac{b_2}{3}) & A_2 \\ 0 & 0 & 0 & -X & 1 & a_2-\frac{b_2}{3} & a_4-b_4-\frac{b_2}{3}(a_2-\frac{b_2}{3}) & A_3 \\ 1 & 0 & 0 & 0 & -X-a_3 & 0 & 0 & \frac{a_1b_8}{3} \\ 0 & 1 & 0 & 0 & -a_1 & -X-a_3 & 0 & a_1b_6 \\ 0 & 0 & 1 & 0 & 0 & -a_1 & -X-a_3 & a_1b_4 \\ 0 & 0 & 0 & 1 & 0 & 0 & -a_1 & -X+\frac{a_1b_2}{3}-a_3 \end{pmatrix}$$

with

$$A_0 = -\frac{b_8}{3}\left(-\frac{b_2}{3}(a_2-\frac{b_2}{3}) + a_4 - b_4\right),$$

$$A_1 = -b_6\left(-\frac{b_2}{3}(a_2-\frac{b_2}{3}) + a_4 - b_4\right) - \frac{b_8}{3}(a_2-\frac{b_2}{3}),$$

$$A_2 = -b_4\left(-\frac{b_2}{3}(a_2-\frac{b_2}{3}) + a_4 - b_4\right) - b_6(a_2-\frac{b_2}{3}) - b_8/3,$$

$$A_3 = -\frac{b_2}{3}\left(-\frac{b_2}{3}(a_2-\frac{b_2}{3}) + a_4 - b_4\right) - b_4(a_2-\frac{b_2}{3}) + a_6 - b_6.$$

By the second way, we compute the determinant

$$\mathrm{Res}_x(\psi_3, w_E) = \det\begin{pmatrix} 3 & 0 & 0 & -1 & 0 & 0 & 0 \\ b_2 & 3 & 0 & -a_2 & -1 & 0 & 0 \\ 3b_4 & b_2 & 3 & a_4-a_1y & -a_2 & -1 & 0 \\ 3b_6 & 3b_4 & b_2 & a_6-a_3-y^2 & a_4-a_1y & -a_2 & -1 \\ b_8 & 3b_6 & 3b_4 & 0 & a_6-a_3-y^2 & a_4-a_1y & a_2 \\ 0 & b_8 & 3b_6 & 0 & 0 & a_6-a_3-y^2 & a_4-a_1y \\ 0 & 0 & b_8 & 0 & 0 & 0 & a_6-a_3-y^2 \end{pmatrix}.$$

Both methods give the same polynomial $\chi_{y,3}$.

Example 5.40. Let $E : y^2 + xy = x^3 - \frac{4}{13}$. Its Galois image modulo 3 is the Borel subgroup $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ and is isomorphic to the Galois group of

$$\chi_{y,3}(x) = x^8 - \frac{1}{3}x^7 - \frac{851}{351}x^6 + \frac{12}{13}x^5 + \frac{760}{507}x^4 + \frac{3076}{4563}x^3 - \frac{16}{169}x^2 + \frac{576}{2197}x - \frac{6912}{28561}$$

If $a_1 = 0$, we can take the function $u = x + y$ for example. With a short Weierstrass equation $E : y^2 = x^2 + Ax + B$, the matrix of the multiplication by $x + y$ is

$$\begin{pmatrix} 0 & 0 & 0 & A^2/3 & B & A^2/3 & 0 & -\frac{A^3}{3} \\ 1 & 0 & 0 & -4B & A & -3B & A^2/3 & 4BA \\ 0 & 1 & 0 & -2A & 0 & -A & -3B & 2A^2 + A^2/3 \\ 0 & 0 & 1 & 0 & 1 & 0 & -A & -3B \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & A^2/3 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & -4B \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & -2A \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

and

$$\operatorname{Res}_x(\psi_3', w_{E'}) = \begin{pmatrix} 3 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 3 & 0 & -1 & -1 & 0 & 0 \\ 6A & 0 & 3 & A-2y & -1 & -1 & 0 \\ 12B & 6A & 0 & B-y^2 & A-2y & -1 & -1 \\ -A^2 & 12B & 6A & 0 & B-y^2 & A-2y & -1 \\ 0 & -A^2 & 12B & 0 & 0 & B-y^2 & A-2y \\ 0 & 0 & -A^2 & 0 & 0 & 0 & B-y^2 \end{pmatrix}.$$

We obtain

$$\begin{aligned}\chi_{x+y,3} = {} & x^8 + (4A+8B)x^6 + (\frac{-32}{3}A^2 + 8B)x^5 + (\frac{8}{3}A^3 + \frac{10}{3}A^2 - 40AB + 18B^2)x^4 \\ & +(16AB - 80B^2)x^3 + (\frac{16}{3}A^4 - \frac{4}{3}A^3 + \frac{40}{3}A^2B + 36AB^2 + 16B^2)x^2 \\ & +(\frac{-32}{9}A^4 + \frac{32}{3}A^3B - \frac{8}{3}A^2B - 16AB^2 + 72B^3)x \\ & -\frac{16}{27}A^6 - \frac{8}{9}A^5 - 8A^3B^2 + \frac{1}{9}A^4 - \frac{8}{3}A^3B - 6A^2B^2 - 27B^4 - 16B^3).\end{aligned}$$

By an appropriate change of variables, we can vary the valuation at a given prime as follows:

Proposition 5.41. *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ which does not contain 3, and let m be an integer. Let E/F be an elliptic curve. We can choose u such that, for $i = 0, \dots, \deg(\chi_{u,3})$, the coefficient of degree i of $\chi_{u,3}$ has valuation at $\mathfrak{p}$ greater or equal than $2m(\deg(\chi_{u,3}) - i)$.*

Proof. Let $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, and let $\lambda = \pi^m$. We have $v_{\mathfrak{p}}(\lambda) = m$. Let the equation $y^2 = x^3 + Ax + B$ be minimal for E at $\mathfrak{p}$. Take $u = \lambda^3 y + \lambda^2 x$. Then $\chi_{u,3}$ is equal to $\chi_{x'+y',3}$ where $y'^2 = x'^3 + \lambda^4 Ax' + \lambda^6 B$. So

$$\begin{aligned}\chi_{u,3} = {} & x^8 + 4\lambda^4(A + 2\lambda^2 B)x^6 + 8\lambda^6\left(\frac{-4}{3}\lambda^2A^2 + B\right)x^5 \\ & +2\lambda^8\left(\frac{4}{3}\lambda^4A^3 + \frac{5}{3}A^2 - 20\lambda^2AB + 9\lambda^4B^2\right)x^4 + 16\lambda^{10}(AB - 5\lambda^2B^2)x^3 \\ & +4\lambda^{12}\left(\frac{4}{3}\lambda^4A^4 - \frac{1}{3}A^3 + \frac{10}{3}\lambda^2A^2B + 9\lambda^4AB^2 + 4B^2\right)x^2 \\ & +8\lambda^{14}\left(\frac{-4}{9}\lambda^2A^4 + \frac{4}{3}\lambda^4A^3B - 2\lambda^2AB^2 + 9\lambda^4AB^3 - \frac{8}{3}A^2B\right)x \\ & +\lambda^{16}\left(\tfrac{-16}{27}\lambda^8A^6 - \tfrac{8}{9}\lambda^4A^5 - 8\lambda^8A^4 + \tfrac{1}{9}A^4 - \tfrac{8}{3}\lambda^2A^3B - 6\lambda^4A^2B^2 - 27\lambda^8B^4 - 16\lambda^2B^2\right).\end{aligned}$$

□

The proof of the previous proposition suggests that we can obtain a polynomial with the smallest possible valuation at a prime $\mathfrak{p}$ taking a minimal equation at $\mathfrak{p}$.

Remark 5.42. Under the same notation as in the previous proposition, we can ask if a similar result holds for $m \geq 5$, with some other equation linking the coefficients and the associated power of π. But, for that, we certainly have to compute $\chi_{x+y,m}$, for $m \geq 5$ and we did not succeed with non-specialized coefficients for E. Nevertheless, we observe that, for $m = 2$, a polynomial generating $F(E[2])$ is $\chi_{E,2} := x^3 + Ax + B$. If we make the change of variables $(A, B) \mapsto (\lambda^4 A, \lambda^6 B)$ with $\lambda = \pi^m$, we obtain $\chi_{E,2} = x^3 + \lambda^4 Ax + \lambda^6 B$. This is an equation for E such that, for all $i = 0, \dots, \deg(\chi_{E,2})$, the coefficient of degree i of $\chi_{E,2}$ is divisible by π at least $2m(\deg(\chi_{E,2}) - i)$ times.

5.3 More examples

In the previous subsection, we have computed, using Sagemath [The22], the polynomial $\chi_{x+y,3}$, for any E/F an elliptic curve with a short Weierstrass equation.

For m larger than 3, let us start by observing that $\deg \widetilde{\psi}_5 = 12 = \deg \widetilde{\psi}_6$. So, thanks to Theorem 5.11, respectively Theorem 5.22, we can construct polynomials of degree 12, respectively degree 24, with different Galois group. There are many others such cases, for example:

$$\begin{aligned}
\deg \widetilde{\psi}_9 &= \deg \widetilde{\psi}_{10} = 36,\\
\deg \widetilde{\psi}_{19} &= \deg \widetilde{\psi}_{22} = 180,\\
\deg \widetilde{\psi}_{31} &= \deg \widetilde{\psi}_{33} = 480,\\
\deg \widetilde{\psi}_{71} &= \deg \widetilde{\psi}_{82} = 2520.
\end{aligned}$$

The interesting point is that, thanks to these theorems, a Sagemath program is enough to compute such polynomials. We remark that an artefact of this method is to find the Galois group of a polynomial of high degree, just by calculating the characteristic polynomial of a matrix, which is easy (although sometimes long) for a computer, whereas numerically finding the Galois group of a polynomial of high degree is not feasible with the current technology. Thanks to Remark 5.38 it is even easier, since it suffices to compute a resultant of two well-known polynomials.

Example 5.43. In [Dan15, Theorem 8.1], Daniels gives a curve $E/\mathbb{Q}(t)$ and a set S such that the specialization E_t of E at t is a Serre curve over $\mathbb{Q}$ if and only if $t \notin S$. In particular, from Theorem 3.24, for $t \notin S$, the representation $\rho_{E_t,m}$ is surjective for all prime, so for all product of pairwise distinct primes, as well as for 4 and 9. This curve is defined by

$$E : y^2 + xy = x^3 + t.$$

Thanks to computations with Sagemath, we obtain, for each integer m where $\rho_{E,m}$ is surjective (and for which the computation is feasible by a computer), a family of irreducible polynomials $(\chi_{u,m})_{t\notin S}$ with Galois group $\mathrm{GL}_2(m)$. For example:

$$\chi_{y_t,3} = x^8 + \tfrac{1}{3}x^7 + (8t + \tfrac{1}{27})x^6 + 3tx^5 + (18t^2 + \tfrac{2}{3}t)x^4 + (-7t^2 + \tfrac{1}{27})x^3 - t^2x^2 + 9t^3x - 27t^4$$

has Galois group $\mathrm{GL}_2(3)$ for all $t \notin S$, and

$$\begin{aligned}
\chi_{y_t,4} = x^{12} - \tfrac{1}{2}x^{11} + \left(54t + \tfrac{1}{8}\right)x^{10} - \tfrac{55}{2}tx^9 + \left(891t^2 + \tfrac{99}{8}t\right)x^8 + \left(27t^2 - 2t\right)x^7\\
+ \left(2916t^3 - \tfrac{219}{4}t^2 + \tfrac{1}{8}t\right)x^6 + \left(-1863t^3 + 6t^2\right)x^5\\
+ \left(-24057t^4 + \tfrac{1107}{4}t^3 + \tfrac{1}{8}t^2\right)x^4 + \left(\tfrac{13851}{2}t^4 + 4t^3\right)x^3\\
+ \left(39366t^5 - \tfrac{891}{8}t^4 - \tfrac{1}{8}t^3\right)x^2 - \tfrac{2187}{2}t^5x - 19683t^6 - \tfrac{729}{8}t^5 - \tfrac{1}{8}t^4
\end{aligned}$$

has Galois group $\mathrm{GL}_2(4)$.

$$\begin{aligned}
\chi_{y_t,5} = x^{24} - x^{23} + \left(216t + \tfrac{3}{5}\right)x^{22} + \left(-217t - \tfrac{3}{25}\right)x^{21} + \left(14742t^2 + \tfrac{877}{5}t + \tfrac{1}{125}\right)x^{20}\\
+ \left(-7695t^2 - \tfrac{1971}{25}t\right)x^{19} + \left(256608t^3 + 1477t^2 + \tfrac{506}{25}t\right)x^{18} + \left(-234495t^3 - \tfrac{3459}{25}t^2 - 3t\right)x^{17}\\
+ \left(-\tfrac{19899513}{5}t^4 + \tfrac{431487}{5}t^3 + \tfrac{1287}{25}t^2 + \tfrac{6}{25}t\right)x^{16} + \left(3083670t^4 - \tfrac{324652}{25}t^3 - \tfrac{448}{25}t^2 - \tfrac{1}{125}t\right)x^{15}\\
+ \left(\tfrac{79046928}{5}t^5 - \tfrac{4052754}{5}t^4 + 190t^3 + \tfrac{62}{25}t^2\right)x^{14} + \left(-\tfrac{23737698}{5}t^5 + \tfrac{2105946}{25}t^4 + \tfrac{3531}{25}t^3 - \tfrac{3}{25}t^2\right)x^{13}\\
+ \left(-\tfrac{88258572}{5}t^6 - \tfrac{3661038}{5}t^5 - \tfrac{15616}{5}t^4 - \tfrac{252}{25}t^3\right)x^{12}\\
+ \left(-\tfrac{36256086}{5}t^6 + \tfrac{10623798}{25}t^5 + \tfrac{11674}{25}t^4 - \tfrac{1}{25}t^3\right)x^{11}\\
+ \left(-17006112t^7 + \tfrac{29406402}{5}t^6 - \tfrac{6267294}{125}t^5 - \tfrac{11448}{125}t^4\right)x^{10}\\
+ \left(48931938t^7 - \tfrac{22323438}{25}t^6 + \tfrac{41099}{25}t^5 + 5t^4\right)x^9\\
+ \left(\tfrac{798755823}{25}t^8 - \tfrac{384172794}{25}t^7 + \tfrac{216756}{25}t^6 - \tfrac{1299}{25}t^5 - \tfrac{3}{25}t^4\right)x^8\\
+ \left(-\tfrac{463947993}{5}t^8 + \tfrac{26690148}{25}t^7 + \tfrac{103356}{25}t^6 + \tfrac{36}{5}t^5\right)x^7\\
+ \left(\tfrac{114791256}{25}t^9 + \tfrac{457452603}{25}t^8 + \tfrac{1010394}{25}t^7 - \tfrac{4106}{25}t^6 - \tfrac{13}{25}t^5\right)x^6\\
+ \left(\tfrac{2157119019}{25}t^9 - \tfrac{80326323}{125}t^8 - \tfrac{796311}{125}t^7 - \tfrac{1046}{125}t^6 + \tfrac{1}{125}t^5\right)x^5\\
+ \left(-\tfrac{86093442}{5}t^{10} - \tfrac{320458923}{25}t^9 - \tfrac{1712421}{25}t^8 + \tfrac{54}{25}t^7 + \tfrac{6}{25}t^6\right)x^4\\
+ \left(-\tfrac{186535791}{5}t^{10} + \tfrac{6121413}{25}t^9 + \tfrac{13122}{5}t^8 + \tfrac{22}{5}t^7\right)x^3 + \left(\tfrac{81310473}{25}t^{10} + \tfrac{236196}{25}t^9 - \tfrac{324}{25}t^8 - \tfrac{1}{25}t^7\right)x^2\\
+ \left(\tfrac{43046721}{5}t^{11} + \tfrac{531441}{25}t^{10}\right)x + \tfrac{387420489}{125}t^{12} + \tfrac{14348907}{125}t^{11} - \tfrac{19683}{25}t^{10} - \tfrac{729}{125}t^9 - \tfrac{1}{125}t^8
\end{aligned}$$

has Galois group $\mathrm{GL}_2(5)$, whereas

$$\begin{aligned}\chi_{y_t,6} = x^{24} - x^{23} + (648t+1)\,x^{22} - 649tx^{21} + \left(132678t^2 + 875t\right)x^{20} + \left(-68607t^2 - 462t\right)x^{19} \\ + \left(6940080t^3 + 25075t^2 + 136t\right)x^{18} + \left(-6152031t^3 - 8067t^2 - 19t\right)x^{17} \\ + \left(-317375253t^4 + 1723113t^3 + 2832t^2 + t\right)x^{16} + \left(256565718t^4 + 157736t^3 - 400t^2\right)x^{15} \\ + \left(4311049392t^5 - 57426246t^4 - 117566t^3 - 4t^2\right)x^{14} \\ + \left(-2135382426t^5 + 2165940t^4 + 12647t^3 + 3t^2\right)x^{13} \\ + \left(-26822181564t^6 + 246120606t^5 + 413098t^4 - 152t^3\right)x^{12} \\ + \left(10811281410t^6 + 22940172t^5 + 1918t^4 - 33t^3\right)x^{11} \\ + \left(85506731136t^7 - 1285601706t^6 - 7285302t^5 - 9201t^4 + 3t^3\right)x^{10} \\ + \left(-30700637982t^7 - 33424650t^6 + 561395t^5 + 1198t^4\right)x^{9} \\ + \left(-159947266329t^8 + 3317254722t^7 + 20098530t^6 + 7890t^5 - 49t^4\right)x^{8} \\ + \left(53354019195t^8 + 71226216t^7 - 1074060t^6 - 1875t^5 + t^4\right)x^{7} \\ + \left(185847043464t^9 - 5354268075t^8 - 26764506t^7 + 4618t^6 + 86t^5\right)x^{6} \\ + \left(-46476109773t^9 + 172186884t^8 + 1826145t^7 + 2342t^6 - t^5\right)x^{5} \\ + \left(-134047489194t^{10} + 2903262183t^9 + 3136158t^8 - 47952t^7 - 89t^6\right)x^{4} \\ + \left(12038732973t^{10} - 115145550t^9 - 572994t^8 - 136t^7 + t^6\right)x^{3} \\ + \left(55788550416t^{11} - 1076168025t^{10} - 2480058t^9 + 8019t^8 + 17t^7\right)x^{2} \\ + \left(1937102445t^{11} + 87687765t^{10} + 367416t^9 + 405t^8\right)x \\ -10460353203t^{12} - 243931419t^{11} - 2480058t^{10} - 8019t^9 - 8t^8\end{aligned}$$

has Galois group $\mathrm{GL}_2(6)$. As we have underlined before, the polynomials $\chi_{y_t,5}$ and $\chi_{y_t,6}$ both have degree 24.

The following two examples were found using the database [LMF24] and come from [Sut16].

Example 5.44. The elliptic curve

$$E : y^2 + xy = x^3 - x^2 - 9x + 3699$$

is defined over $\mathbb{Q}$, and has surjective Galois image over $\mathbb{Q}$ for all primes except for 7. We have

$$G := \rho_{E,7}(G_{\mathbb{Q}}) = \left\langle \begin{pmatrix} 6 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 6 & 6 \\ 0 & 4 \end{pmatrix} \right\rangle.$$

Over $F = \mathbb{Q}(\sqrt{-3})$, the Galois representation is also surjective for all primes except for 7 and we have

$$G' := \rho_{E,7}(G_F) = \left\langle \begin{pmatrix} 1 & 6 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 6 \\ 0 & 5 \end{pmatrix} \right\rangle.$$

Hence, $\chi_{x+y,7}$, which has degree 48, has Galois group G, which has order 84, over $\mathbb{Q}$ and Galois group G', which has order 42, over $\mathbb{Q}(\sqrt{-3})$. In particular, $\chi_{x+y,7}$ has a rational root over $\mathbb{Q}(\sqrt{-3})$. Since G' does not contains $-\,\mathrm{id}$, the polynomial ψ_7, which has degree 24, also has Galois group G over F. It also has a root in $\mathbb{Q}(\sqrt{-3})$.

Example 5.45. Let be the elliptic curve $E : y^2 = f(x)$ where

$$f(x) = x^3 + ix^2 + (2i-2)x - 2i - 1.$$

It is defined over $F = \mathbb{Q}(i)$. The image of $\rho_{E,p}$ is surjective for all primes p except 2 and 5. The image mod 5 is $\left\langle \begin{pmatrix} 0 & 3 \\ 4 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 2 & 3 \end{pmatrix} \right\rangle$. Hence, for all primes p except 2 and 5, the polynomial $\chi_{x+y,p}$, which has degree p^2-1, is irreducible and has Galois group $\mathrm{GL}_2(p)$, which has order $(p^2-1)(p-1)p$. The polynomial $\chi_{x+y,5}$, which has degree 24, has Galois group $\left\langle \begin{pmatrix} 0 & 3 \\ 4 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 2 & 3 \end{pmatrix} \right\rangle$, which has order 96. The image of $\rho_{E,2}$ is $\left\langle \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$, which has order 3, and is the Galois group of $f(x)$. We can find the image modulo 10 from the image modulo 2 and modulo 5. Using that the reduction modulo 5, respectively modulo 2, of $\rho_{E,10}(G_F)$ is $\rho_{E,5}(G_F)$, respectively $\rho_{E,2}(G_F)$, we find that

$$\rho_{E,10}(G_F) = \left\langle \begin{pmatrix} 3 & 3 \\ 7 & 8 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ 9 & 5 \end{pmatrix} \right\rangle .$$

Hence $\chi_{x+y,10}$, which has degree 72, has Galois group $\left\langle \begin{pmatrix} 3 & 3 \\ 7 & 8 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ 9 & 5 \end{pmatrix} \right\rangle$ which has order 288.

Chapter 6

Perspective

6.1 Entanglement and modular curves

In this section, we describe ideas for a future joint work with Anni and Kohel which expands further on topics presented in Section 3.4. For example, we aim to construct $(3,4)$-entanglement of type A_4 using modular curves.

6.2 Entanglement for abelian varieties

Elliptic curves are abelian varieties of dimension 1. Many of the techniques and results presented for elliptic curves can be generalized to abelian varieties of higher dimension. Let F be a number field and A/F be an abelian variety of dimension g. For a positive integer m, the group $A[m](\overline{F})$ of m-torsion points of $A(\overline{F})$ is isomorphic $(\mathbb{Z}/m\mathbb{Z})^{2g}$. As for elliptic curves, the action of G_F on the Tate module give rise to an adelic Galois representations $\rho_A : G_F \to \mathrm{GL}_{2g}(\hat{\mathbb{Z}})$. There is also a Weil pairing

$$e_m : A[m] \times A[m] \to (\mathbb{Z}/m\mathbb{Z})^*.$$

The Galois invariance of e_m gives that the image of ρ_A is contained in a proper subgroup of $\mathrm{GL}_{2g}(\hat{\mathbb{Z}})$: the symplectic group $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$, see [ADRAK$^+$15, Section 2]. For all primes p and all integers m, we have adelic, p-adic and mod m Galois representations:

$$\rho_A : G_F \to \mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$$

$$\rho_{A,p^\infty} : G_F \to \mathrm{GSp}_{2g}(\mathbb{Z}_p)$$

$$\rho_{A,m} : G_F \to \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$$

As for elliptic curves, the failure to the surjectivity of $\rho_{A,m}$ is due to vertical and horizontal entanglements:

- (Vertical entanglement) The non-surjectivity of ρ_{A,p^∞} for some prime $p \mid m$,
- (Horizontal entanglement) The non-surjectivity of $\rho_A(G_F)$ in $\prod\limits_{p \mid m} \rho_{A,p^\infty}(G_F)$.

There are previous work on the topic of entanglement of principally polarized abelian varieties, [DLRM23, Section 7]. Instead of the determinant character in case of elliptic curves, we have the *similitude character*

$$\nu : \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z})^*,$$

which does not always match with the determinant character. The similitude character satisfies $\nu \circ \rho_{A,m} = \chi_m$. In particular, we have $F(\zeta_m) \subseteq F(A[m])$ for all integers m. Thus, we define in a similar way a Weil entanglement:

Definition 6.1. Let T be a non-trivial abelian group. We say that an abelian variety A/F has a *Weil* (a,b)*-entanglement of type* T if $\mathrm{Gal}(F(A[a]) \cap F(\zeta_b)/F(\zeta_d)) \simeq T$ or $\mathrm{Gal}(F(A[b]) \cap F(\zeta_a)/F(\zeta_d)) \simeq T$.

Theorem 6.2 ([DLRM23, Theorem 7.5])**.** *Let $p \geq 5$ be a prime number and $g \geq 1$ such that $p-1 = 2(2g+1)$. There exists infinitely many principally polarized abelian varieties $A/\mathbb{Q}$ of dimension g which has a Weil $(2,p)$-entanglement of type $\mathbb{Z}/(2g+1)\mathbb{Z}$.*

In the case of the study of horizontal coincidence, using the type of reduction of the abelian variety, we can obtain information on the ramification of $F(A[m])/F$, see [ST68] and so we can extend some results of Section 4.4.2 to abelian varieties.

Moreover, since $\mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$ is a subgroup of $\mathrm{GL}_{2g}(\hat{\mathbb{Z}})$, Proposition 4.46 also applies in this case. In other words:

Theorem 6.3. *If $F(A[p^{k+1}] = F(A[p^k])$, then $F(A[p]) = F(A[p^2]) = \cdots = F(A[p^{k+1}])$ if p is odd and $F(E[4]) = F(E[8]) = \cdots = F(A[p^{k+1}]$ if $p = 2$.*

Again, coincidences correspond to subgroups of $\mathrm{GSp}_{2g}(m)$ which are split liftable modulo a multiple of m.

We can also construct coincidences using Corollary 4.47 which are also valid replacing E/F by any abelian variety A/F.

With respect to the explicit IGP for images of mod m Galois representation for abelian varieties, it is not immediate to find an explicit general construction: division polynomials does exist but there is no known generic formula for them.

Appendix A

Derived groups of $\mathrm{GL}_2(m)$ and $\mathrm{SL}_2(m)$

In this appendix, we give elementary and detailed proofs of well-known results about the derived groups of $\mathrm{GL}_2(m)$ and $\mathrm{SL}_2(m)$, for any integer m. They are used in Section 4.6 in the case where m is odd. For a group G, we denote by $\mathrm{D}(G)$ its commutator subgroup, generated by all the elements $[g, h] = ghg^{-1}h^{-1}$ with $g, h \in G$. We know that $\mathrm{D}(G)$ is normal in G and is the smallest group such that $G/\mathrm{D}(G)$ is an abelian group: the *abelianization of* G.

We recall that $\mathrm{SL}_2(\mathbb{Z})$ is generated by $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. They satisfy $S^2 = (ST)^3 = -\mathrm{id}$.

Proposition A.1. *The quotient group* $\mathrm{SL}_2(\mathbb{Z})/\mathrm{D}(\mathrm{SL}_2(\mathbb{Z}))$ *is cyclic of order* 12*, generated by the equivalence class of* T*.*

Proof. Let $\bar{S}$ and $\bar{T}$ the classes of S and T in $\mathrm{SL}_2(\mathbb{Z})/\mathrm{D}(\mathrm{SL}_2(\mathbb{Z}))$ respectively. Since $\mathrm{SL}_2(\mathbb{Z})/\mathrm{D}(\mathrm{SL}_2(\mathbb{Z}))$ is abelian, we have $\bar{S}\bar{T} = \bar{T}\bar{S}$. Hence $(\bar{S}\bar{T})^3 = \bar{S}^3\bar{T}^3 = \bar{S}^2$, which gives $\bar{S} = \bar{T}^{-3}$ and $\bar{T}^{12} = \bar{S}^4 = -\mathrm{id}$. It follows that $\bar{T}$ generated $\mathrm{SL}_2(\mathbb{Z})/\mathrm{D}(\mathrm{SL}_2(\mathbb{Z}))$ and has order 12. □

Let $m \mid n$ be positive integers and, for $i = n, m$, set $X_i = \mathrm{SL}_2(i))/\mathrm{D}(\mathrm{SL}_2(i))$. The following diagram has exact rows and is commutative.

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{D}(\mathrm{SL}_2(\mathbb{Z})) \arrow[r] \arrow[d] & \mathrm{SL}_2(\mathbb{Z}) \arrow[r] \arrow[d, two heads] & \mathbb{Z}/12\mathbb{Z} \arrow[r] \arrow[d] & 0 \\
1 \arrow[r] & \mathrm{D}(\mathrm{SL}_2(n)) \arrow[r] \arrow[d] & \mathrm{SL}_2(n) \arrow[r] \arrow[d, two heads] & X_n \arrow[r] \arrow[d] & 0 \\
1 \arrow[r] & \mathrm{D}(\mathrm{SL}_2(m)) \arrow[r] & \mathrm{SL}_2(m) \arrow[r] & X_m \arrow[r] & 0
\end{tikzcd} \tag{A.1}$$

Proposition A.2. *Let* m *be a positive integer. The abelianization of* $\mathrm{SL}_2(m)$ *is isomorphic to* $\mathbb{Z}/\gcd(m, 12)\mathbb{Z}$*. In particular, if* m *is coprime to* 6*, then* $\mathrm{SL}_2(m)$ *is perfect.*

Proof. By Diagram (A.1) and Proposition A.1, the image of T in $\mathrm{SL}_2(m)$ generates the abelianization of $\mathrm{SL}_2(m)$, whose order divides 12. Moreover, the image of T in $\mathrm{SL}_2(m)$ has order m. Hence the abelianization of $\mathrm{SL}_2(m)$ has order dividing $\gcd(m, 12)$. To prove that its order is exactly $\gcd(m,12)$, it suffices to prove it for $m = 2, 3$ and 4, and then to use again Diagram (A.1). We define the commutators

$$A = \left[\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -2 \\ 1 & -1 \end{pmatrix}\right] = \begin{pmatrix} 3 & -1 \\ 1 & 0 \end{pmatrix},$$

$$B = \left[\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right] = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

Let $G = \langle A, B\rangle \subseteq \mathrm{SL}_2(\mathbb{Z})$. For $m = 2, 3, 4$, let G_m be the image of G is $\mathrm{SL}_2(m)$. By computing explicitely G_2, G_3 and G_4, we find that they have respectively order 3, 8 and 12, and they are normal subgroups of $\mathrm{SL}_2(m)$. Then $\mathrm{SL}_2(m)/G_m$ is an abelian group of order m. Hence, as a subgroup of $\mathbb{Z}/12\mathbb{Z}$, it is isomorphic to $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/\gcd(m,12)\mathbb{Z}$. □

Remark A.3. We also can prove the previous result for $m = p^k$ with $p \geq 5$ prime, just by observing that the diagram A.1 gives that the order of X_m is both a divisor of 12 and a divisor of $\#\mathrm{SL}_2(p^k) = p^{3(k-1)+1}(p-1)(p+1)$. Hence, the order of the abelianization of $\mathrm{SL}_2(p^k)$ is 1, and so its derived group is itself, unless $p = 2$ or 3.

Proposition A.4. *For an odd integer m, the derived group of* $\mathrm{GL}_2(m)$ *is* $\mathrm{SL}_2(m)$*, and so its abelianization is isomorphic to* $(\mathbb{Z}/m\mathbb{Z})^*$*. If m is even, the derived group of* $\mathrm{GL}_2(m)$ *has index* 2 *in* $\mathrm{SL}_2(m)$*.*

Proof. For $A, B \in \mathrm{GL}_2(m)$, we have $\det(ABA^{-1}B^{-1}) = 1$. So $[A,B] \in \mathrm{SL}_2(m)$. Therefore

$$\mathrm{D}(\mathrm{SL}_2(m)) \leq \mathrm{D}(\mathrm{GL}_2(m)) \leq \mathrm{SL}_2(m).$$

For m coprime to 6, we have proven that $\mathrm{D}(\mathrm{SL}_2(m)) = \mathrm{SL}_2(m)$, and so $\mathrm{D}(\mathrm{GL}_2(m)) = \mathrm{SL}_2(m)$. For $m = 3^k$, we know that $\mathrm{D}(\mathrm{SL}_2(3^k))$ has index 3 in $\mathrm{SL}_2(3^k)$, and so $\mathrm{D}(\mathrm{GL}_2(3^k))$ is either $\mathrm{SL}_2(3^k)$ or $\mathrm{D}(\mathrm{SL}_2(3^k))$. For $k = 1$, $\mathrm{D}(\mathrm{SL}_2(3))$ is explicitly know by the proof of Proposition A.2 and

$$\left[\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}\right] = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \notin \mathrm{D}(\mathrm{SL}_2(3)).$$

It follows that $\mathrm{D}(\mathrm{GL}_2(3)) = \mathrm{SL}_2(3)$. We obtain the diagram below:

$$\begin{tikzcd}
\mathrm{D}(\mathrm{SL}_2(3^k)) \arrow[r, hook] \arrow[d, two heads] & \mathrm{D}(\mathrm{GL}_2(3^k)) \arrow[r, hook] \arrow[d, two heads] & \mathrm{SL}_2(3^k) \arrow[d, two heads] \\
\mathrm{D}(\mathrm{SL}_2(3)) \arrow[r, hook, "\text{index } 3"'] & \mathrm{D}(\mathrm{GL}_2(3)) \arrow[r, equal] & \mathrm{SL}_2(3)
\end{tikzcd}$$

showing that $\mathrm{D}(\mathrm{SL}_2(3^k)) \neq \mathrm{D}(\mathrm{GL}_2(3^k))$ and so $\mathrm{D}(\mathrm{GL}_2(3^k)) = \mathrm{SL}_2(3^k)$. For $m = 2^k$, we use the same strategy. From Proposition A.2, we already know that $\mathrm{D}(\mathrm{GL}_2(2))$ has index 2 in $\mathrm{SL}_2(2)$. We have the following diagram:

$$\begin{tikzcd}
\mathrm{D}(\mathrm{SL}_2(2^k)) \arrow[r, hook] \arrow[d, two heads] & \mathrm{D}(\mathrm{GL}_2(2^k)) \arrow[r, hook] \arrow[d, two heads] & \mathrm{SL}_2(2^k) \arrow[d, two heads] \\
\mathrm{D}(\mathrm{SL}_2(4)) \arrow[r, hook] \arrow[d, two heads] & \mathrm{D}(\mathrm{GL}_2(4)) \arrow[r, hook] \arrow[d, two heads] & \mathrm{SL}_2(4) \arrow[d, two heads] \\
\mathrm{D}(\mathrm{SL}_2(2)) \arrow[r, equal] & \mathrm{D}(\mathrm{GL}_2(2)) \arrow[r, hook, "\text{index } 2"'] & \mathrm{SL}_2(2)
\end{tikzcd}$$

The group $\mathrm{D}(\mathrm{SL}_2(4))$ is known by the proof of Proposition A.2, and we have

$$\left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}\right] = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \in \mathrm{D}(\mathrm{GL}_2(4)) \setminus \mathrm{D}(\mathrm{SL}_2(4)).$$

Using that $\mathrm{D}(\mathrm{SL}_2(2^k))$ has index 4 in $\mathrm{SL}_2(2^k)$ for $k \geq 2$, we obtain that $\mathrm{D}(\mathrm{GL}_2(4))$ has exactly index 2 in $\mathrm{SL}_2(4)$ and $\mathrm{D}(\mathrm{GL}_2(2^k))$ has exactly index 2 in $\mathrm{SL}_2(2^k)$ for all $k \geq 2$. The result follows, since the Chinese remainder theorem gives

$$\mathrm{D}(\mathrm{GL}_2(m)) \simeq \prod_{\substack{p^k || m \\ p \text{ prime}}} \mathrm{D}(\mathrm{GL}_2(p^k)).$$

□

Appendix B

Modular curves

This appendix is based on [Maz06, Section 2] and [Sik19].

Let $\mathbb{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$ be the upper-half plane. The group $\mathrm{SL}_2(\mathbb{Z})$ acts on the left on $\mathbb{H}$ by Möbius transformations: for $\tau \in \mathbb{H}$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}.$$

In the same way, $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{P}^1(\mathbb{Q})$. Therefore $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$.

Remark B.1. The matrix $-\mathrm{id}$ acts trivially on $\mathbb{H}^*$.

To a point $\tau \in \mathbb{H}$, we associate a lattice $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau \subseteq \mathbb{C}$ and an elliptic curve $E_\tau \simeq \mathbb{C}/\Lambda_\tau$ (isomorphism of Riemann surfaces which is also a group homomorphism). Every lattice Λ of $\mathbb{C}$ is homothetic to Λ_τ for some $\tau \in \mathbb{H}^*$ *i.e.* there exists $\alpha \in \mathbb{C}$ such that $\alpha\Lambda \subseteq \Lambda_\tau$. We have the following bijections

$$\begin{tikzcd}
\left\{ \begin{array}{l} \text{elliptic curve over } \mathbb{C} \\ \text{up to isomorphism} \end{array} \right\} \arrow[r, leftrightarrow] & \left\{ \begin{array}{l} \text{lattices in } \mathbb{C} \\ \text{up to homothety} \end{array} \right\} \arrow[r, leftrightarrow] & \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H} \arrow[r, "\simeq", "j"'] & \mathbb{C} \\
E_\tau \arrow[r, leftrightarrow] & \Lambda_\tau \arrow[r, leftrightarrow] & \tau \arrow[r, mapsto] & j(E_\tau)
\end{tikzcd}$$

For the first arrow, see [Sil09, VI, Proposition 3.6], [Sil09, VI, Corollary 5.1.1] and [Sil09, VI, Corollary 4.1.1]. The second arrow is easy to check. The surjectivity of the last map follows from:

Theorem B.2 ([Sil09, C, Proposition 12.11])**.** *We set* $X(1) := \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*$. *The map*

$$j : X(1) \to \mathbb{P}^1(\mathbb{C})$$

is a complex analytic isomorphism of compact Riemann surfaces.

For $N \geq 1$, we define

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid a \equiv d \equiv 1 \bmod N,\ b \equiv c \equiv 0 \bmod N \right\}$$

We also define the following typical congruence subgroups:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid b \equiv 0 \bmod N \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid a \equiv d \equiv 1 \bmod N,\ b \equiv 0 \bmod N \right\}.$$

Definition B.3. Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$. We say that Γ is *a congruence subgroup of* $\mathrm{SL}_2(\mathbb{Z})$ if it contains $\Gamma(N)$ for some $N \geq 1$. In this case, the smallest N satisfying this property is called the *level* of Γ.

Definition B.4. Let $G \leq \mathrm{GL}_2(N)$. We associate to G the congruence subgroup

$$\Gamma_G := \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \bmod N \in G\} \supseteq \Gamma(N).$$

Proposition B.5 ([DS05, Section 2.4])**.** *Let $G \leq \mathrm{GL}_2(N)$. The quotient $\Gamma_G \backslash \mathbb{H}^*$ is a compact Riemann surface.*

Definition B.6. Let $G \leq \mathrm{GL}_2(N)$. The *modular curve associated to* G is $X_G := \Gamma_G \backslash \mathbb{H}^*$. The *level of* X_G is the level of Γ_G. A *model* for X_G is a projective curve isomorphic to X_G. The points of $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{Q} \subseteq X_G$ are called the *cusps* of X_G.

We recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^*$ and that $\det G \leq (\mathbb{Z}/N\mathbb{Z})^*$. Let $\mathbb{Q}(\zeta_N)^{\det G}$ be the fixed field of the image of $\det G$ in $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$.

Theorem B.7 ([Maz06, Maz-9])**.** *Let $G \leq \mathrm{GL}_2(N)$. The modular curve X_G has a model defined over the field $\mathbb{Q}(\zeta_N)^{\det(G)}$.*

We have a natural surjective morphism of Riemann surfaces $\Gamma_G \backslash \mathbb{H}^* \to \Gamma(1) \backslash \mathbb{H}^*$ which induces a non-constant morphism of curves $j_G : X_G \to X(1)$, again defined over $\mathbb{Q}(\zeta_N)^{\det(G)}$.

For $G \leq \mathrm{GL}_2(N)$ with determinant $(\mathbb{Z}/N\mathbb{Z})^*$, the modular curve X_G parameterizes isomorphism classes of elliptic curves with image of mod N Galois representation contained in G. A *level N-structure on E* is an isomorphism $E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$, in other words a choice of a $\mathbb{Z}/N\mathbb{Z}$-basis for $E[N]$. Let E_1, E_2 be elliptic curves provided with level N-structures α_1, α_2. We say that the pairs (E_1, α_1) and (E_2, α_2) are *G-isomorphic* if there exists an isomorphism $\phi : E_1 \to E_2$ and an element $g \in G$ such that

$$\alpha_1 = g \circ \alpha_2 \circ \phi.$$

This defines an equivalence relation, and we denote by $[(E, \alpha)]_G$ the G-isomorphism class of (E, α).

Theorem B.8 ([Maz06, Maz-9])**.** *Let $G \leq \mathrm{GL}_2(N)$. There is a bijection between the G-isomorphism classes and the points of X_G. For any elliptic curve E/F such that $\rho_{E,N}(G_F) \leq G$, there exists a non-cuspidal point $Q \in X_G(F)$ such that $j_G(Q) = j(E)$. Conversally, for any non-cuspidal point $Q \in X_G(F)$ such that $j_G(Q) \neq 0, 1728$, there exists an elliptic curve E/F such that $\rho_{E,N}(G_F) \leq G$ and $j_G(Q) = j(E)$.*

Typical examples are the modular curves

$$X(N) = X_{\Gamma(N)}, \quad X_0(N) = X_{\Gamma_0(N)} \quad \text{and} \quad X_1(N) = X_{\Gamma_1(N)},$$

which parameterize elliptic curves with mod N image contained in a subgroup of $\mathrm{GL}_2(N)$ conjugate to

$$\{\mathrm{id}\}, \quad \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

respectively, see for example [Sil09, Appendix C, Theorem 13.1]). In the context of entanglement, we focus on other examples, which appear in the manuscript, see below.

Example B.9. Let $X_{ns}^+(3) = X_G$ where $G = C_{ns}^+(3)$ is the normalizer of the non-split Cartan subgroup of $\mathrm{GL}_2(3)$. From [Che99, Proposition 4.1], the modular curve $X_{ns}^+(3)$ has genus 0 and the corresponding j-line is given by

$$X_{ns}^+(3) \to X(1) \quad t \mapsto t^3.$$

In other words, a non-cuspidal point $t \in X_{ns}^+(3)(F)$ corresponds to an elliptic curve over F with j-invariant t^3 and mod 3 Galois image contained in $C_{ns}^+(3)$, and conversely. From the graph 5.1, the group $C_{ns}^+(3)$ is conjugate to

$$\left\langle \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle.$$

Let E/F be an elliptic curve. As an elliptic curve over $F(E[3])$, it has trivial mod 3 Galois image, so contained in $C_{ns}^+(3)$. In particular, we have $j(E)^{\frac{1}{3}} \in F(E[3])$. Conversely, if $j(E)^{\frac{1}{3}} \in F$, then E/F has mod 3 image contained in $C_{ns}^+(3)$. These facts are used in the proof of Proposition 4.77.

Example B.10 (Section 2.4.1, [Elk06]). Let $G = \left\langle \begin{pmatrix} 0 & 5 \\ 7 & 0 \end{pmatrix}, \begin{pmatrix} 4 & 1 \\ -3 & 4 \end{pmatrix} \right\rangle \leq \mathrm{SL}_2(9)$. The group G is a split lifting of $\mathrm{SL}_2(3)$, see Section 4.5.4. Elkies defines $\mathcal{X}_9 = X_G$. This modular curve has genus 0 and the corresponding j-map

$$\mathcal{X}_9 \to X(1) \quad x \mapsto f(x)$$

is given in [Elk06, Section 2]. The points of $\mathcal{X}_9(\mathbb{Q})$ correspond to elliptic curves $E/\mathbb{Q}$ satisfying $\rho_{E,9}(G_{\mathbb{Q}}) \cap \mathrm{SL}_2(9) \leq G$. In particular, using (4.3), we obtain that

$$3^3 = [\mathrm{SL}_2(9) : G] \mid [\mathrm{SL}_2(9) : \rho_{E,9}(G_{\mathbb{Q}}) \cap \mathrm{SL}_2(9)] \mid [\mathrm{GL}_2(9) : \rho_{E,9}(G_{\mathbb{Q}})].$$

Elkies shows that there exists elliptic curves $E/\mathbb{Q}$ with $j(E) = f(x)$ for some $x \in \mathbb{P}^1(\mathbb{Q})$ and $\rho_{E,3}$ surjective. This provides examples of elliptic curves $E/\mathbb{Q}$ with surjective mod 3 Galois representation but not mod 9. We observe that in the above case, $\frac{i_2}{i_1} = 3^3$ where i_k is defined in Section 4.5.3 and taking $p = 3$.

We say that $G \leq \mathrm{GL}_2(m)$ is a *group of entanglement* if there exist a, b coprime such that $ab = m$ and G does not surject on the product $G_a \times G_b$ where G_a and G_b are the images of G in $\mathrm{GL}_2(a)$ and $\mathrm{GL}_2(b)$ respectively. In the manuscript are mentioned modular curves corresponding to groups of entanglement: $X'(6)$ in Theorem 3.46, and $X_{G_6} = X'(6)$, $X_{G_{10}}$, $X_{G_{15}}$ and $X_{G_{18}}$ in Theorem 3.48. They all have genus 0 and the corresponding j-maps are given in [JM20, Theorem 1.8].

We focuse now on the case of coincidences. As seen in Section 4.1, we can reduce the question to $(m, p^k m)$-coincidence where m is an integer and p is a prime, as formulated in Question 4.3. In this case, if an elliptic curve E/F has an $(m, p^k m)$-coincidence, then the group $G := \rho_{E,p^k m}(G_F)$ must be isomorphic to its image in $\mathrm{GL}_2(m)$. Hence, the study of coincidences amounts to find such groups G and then F-rational points on X_G.

Remark B.11. In Example B.10, the group $G \leq \mathrm{GL}_2(9)$ is isomorphic to its image in $\mathrm{GL}_2(3)$, which is $\mathrm{SL}_2(3)$, but does not correspond to a coincidence for some elliptic curve over $\mathbb{Q}$ since it has non surjective determinant. However, over a number field F such that $\zeta_9 \in F$, the points on $\mathcal{X}_9(F)$ could give elliptic curves over F with a $(3, 9)$-coincidence.

Example B.12. If an elliptic curve over F has a $(2, 3)$-coincidence, then it has a $(2, 6)$-coincidence and a $(3, 6)$-coincidence. Therefore, the image mod 6 must be a subgroup G

of $\mathrm{GL}_2(6)$ which is isomorphic to its image in $\mathrm{GL}_2(2)$ and in $\mathrm{GL}_2(3)$. In case where $F \cap \mathbb{Q}(\zeta_6) = \mathbb{Q}$, the subgroup G must have surjective determinant and, from [DLR23, Section 6, end], there are only two possibilities for G:

$$G_1 = \left\langle \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix} \right\rangle \quad \text{and} \quad G_2 = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 2 & -1 \\ 1 & 3 \end{pmatrix} \right\rangle.$$

In both case X_G has genus 0. Thus, if an elliptic E/F with $F \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$ has a $(2,3)$-coincidence, then $j(E) = j_{G_1}(t)$ or $j(E) = j_{G_2}(t)$ for some $t \in F$. The parametrization of such elliptic curves is given in Theorem 4.7.

Example B.13 ([RZB15]). Let

$$G = \left\langle \begin{pmatrix} 1 & 0 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 1 & 0 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(4).$$

Any subgroup of $\mathrm{GL}_2(4)$ isomorphic to its image in $\mathrm{GL}_2(2)$ is, up to conjugation, a subgroup of G. The modular curve X_G corresponds to X_{20b} is the notation of Rouse and Zureick-Brown. It has genus 0 and the j-line $j_G : X_G \to \mathbb{P}^1$ maps t to

$$j_G(t) = \frac{-4t^8 + 32t^7 + 80t^6 - 288t^5 - 504t^4 + 864t^3 + 1296t^2 - 864t - 1188}{t^4 + 4t^3 + 6t^2 + 4t + 1}$$

In particular, X_{20b} gives a parametrization of elliptic curves with a $(2,4)$-coincidence, which is given in Theorem 4.4. Since there are no CM j-invariant in $\mathbb{Q}$ on X_{20b}, then there are no elliptic curves over $\mathbb{Q}$ with CM and a $(2,4)$-coincidence. We can use the same approach to see if they are CM j-invariant over more general number field F which maps to $j_G(t)$ for some $t \in F$.

Nomenclature

$[m]$	multiplication by m map, page 34
χ_{cyc}	adelic cyclotomic character, page 29
χ_m	mod m cyclotomic character, page 29
χ_{p^∞}	p-adic cyclotomic character, page 29
$\Delta_{\mathrm{sf}}(E)$	squarefree part of Δ_E, page 49
$\Gamma(N)$	principal congruence subgroup of level N, page 115
Γ_G	congruence subgroup associated to G, page 116
$\mathfrak{f}_E$	conductor ideal of E, page 33
$\mathcal{G}(E/F)$	maximal adelic subgroup, page 43
$\mathcal{G}(E/F, m)$	maximal mod m subgroup, page 43
$\mathcal{G}(E/F, p^\infty)$	maximal p-adic subgroup, page 43
$\mathcal{G}_{F,m}$	maximal mod m subgroup, page 37
$\mathcal{G}_{F,p^\infty}$	maximal p-adic subgroup, page 37
$\mathcal{G}_F$	maximal adelic subgroup, page 37
O	point at infinity, page 31
ψ_m	m-th division polynomial, page 90
$\rho_{E,m}$	mod m Galois representation of E, page 35
ρ_{E,p^∞}	p-adic Galois representation of E, page 35
ρ_E	adelic Galois representation of E, page 35
$\sigma(P)$	the point with coordinates $(x(P), y(P))$, page 35
$\widetilde{\psi}_m$	m-th primitive division polynomial, page 90
$a_p(E)$	trace of Frobenius at p, page 33
$D(G)$	commutator subgroup of G, page 111
$E[p^\infty]$	group of p^k torsion points of E for $k \geq 1$, page 34

$E^{(d)}$	quadratic twist of E by d, page 32
E_{tors}	group of torsion points of E, page 34
f_E	conductor of $E/\mathbb{Q}$, page 33
M_Δ	Serre number associated to Δ, page 57
M_E	adelic level of E, page 38
$N_{\delta,\phi}(\hat{\mathbb{Z}})$	Cartan normalizer subgroup, page 44
$N_{\delta,\phi}(m)$	Cartan normalizer subgroup, page 44
$N_{\delta,\phi}(p^\infty)$	Cartan normalizer subgroup, page 44
S_n	symmetric group of degree n, page 22
$T(E)$	adelic Tate module of E, page 34
$T_p(E)$	p-adic Tate module of E, page 34
X_G	modular curve associated to G, page 116
$\Delta(E)$	discriminant of E, page 32
$F(E[m])$	m-division field of E/F, page 35
$j(E)$	j-invariant of E, page 32
$v_{\mathfrak{p}}(a)$	$\mathfrak{p}$-adic valuation of a, page 33

Index

Bibliography

[AD20] Samuele Anni and Vladimir Dokchitser. Constructing hyperelliptic curves with surjective Galois representations. *Transactions of the American Mathematical Society*, 373(2):1477–1500, 2020.

[ADRAK+15] Sara Arias-De-Reyna, Cécile Armana, Valentijn Karemaker, Marusia Rebolledo, Lara Thomas, and Núria Vila. *Galois representations and Galois groups over Q*, chapter 2. Association for Women in Mathematics series. Springer International Publishing, 2015.

[AdRV09] Sara Arias-de Reyna and Núria Vila. Tame Galois realizations of $\mathrm{GL}_2(\mathbb{F}_\ell)$ over $\mathbb{Q}$. *Journal of number theory*, 129(5):1056–1065, 2009.

[Ann14] Samuele Anni. A local-global principle for isogenies of prime degree over number fields. *Journal of the London Mathematical Society*, 89(3):745–761, 2014.

[BCS17] Abbey Bourdon, Pete L. Clark, and James Stankewicz. Torsion points on CM elliptic curves over real number fields. *Transactions of the American Mathematical Society*, 369(12):8457–8496, 2017.

[BDM+19] Jennifer S. Balakrishnan, Netan Dogra, J. S. Müller, Jan Tuitman, and Jan Vonk. Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Annals of mathematics*, 189(3):885–944, 2019.

[BDM+23] Jennifer S. Balakrishnan, Netan Dogra, J. S. Müller, Jan Tuitman, and Jan Vonk. Quadratic chabauty for modular curves: algorithms and examples. *Compositio mathematica*, 159(6):1111–1152, 2023.

[BFGR06] Nils Briun, E. V. Flynn, Josep Gonzalez, and Victor Rotger. On finiteness conjectures for endomorphism algebras of abelian surfaces. *Mathematical proceedings of the Cambridge Philosophical Society*, 141(3):383–408, 2006.

[BJ16] Julio Brau and Nathan Jones. Elliptic curves with 2-torsion contained in the 3-torsion field. *Proceedings of the American Mathematical Society*, 144(3):925–936, 2016.

[Bou81] Nicolas Bourbaki. *Algebra II.* Springer Berlin, Heidelberg, 1981.

[BP11] Yuri Bilu and Pierre Parent. Serre's uniformity problem in the split Cartan case. *Annals of mathematics*, 173(1):569–584, 2011.

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo. Rational points on $X_0^+(p^r)$. *Annales de l'Institut Fourier*, 63(3):957–984, 2013.

[Che99] Imin Chen. On Siegel's modular curve of level 5 and the class number one problem. *Journal of Number Theory*, 74(2):278–297, 1999.

[CK05] Alina C. Cojocaru and Ernst Kani. On the surjectivity of the Galois representations associated to non-CM elliptic curves. *Canadian mathematical bulletin*, 48(1):16–31, 2005.

[Coh79] S. D. Cohen. The distribution of the Galois groups of integral polynomials. *Illinois journal of mathematics*, 23(1), 1979.

[Coh12] P. M. Cohn. *Basic Algebra: Groups, Rings and Fields.* Springer Nature, Netherlands, 2012.

[CP22a] Francesco Campagna and Riccardo Pengo. Entanglement in the family of division fields of elliptic curves with complex multiplication. *Pacific Journal of Mathematics*, 317(1):21–66, 2022.

[CP22b] Francesco Campagna and Riccardo Pengo. How big is the image of the Galois representations attached to CM elliptic curves? *arXiv: Number Theory (Cornell University)*, 2022.

[CS23] Francesco Campagna and Peter Stevenhagen. Cyclic reduction densities for elliptic curves. *Research in number theory*, 9(3), 2023.

[Dan15] Harris B. Daniels. An infinite family of Serre curves. *Journal of Number Theory*, 155:226–247, 2015.

[DD11] Tim Dokchitser and Vladimir Dokchitser. Surjectivity of mod 2^n representations of elliptic curves. *Mathematische Zeitschrift*, 272, 2011.

[DLR23] Harris Daniels and Álvaro Lozano-Robledo. Coincidences of division fields. *Annales de l'Institut Fourier*, 2023.

[DLRM23] Harris B. Daniels, Alvaro Lozano-Robledo, and Jackson S. Morrow. Towards a classification of entanglements of Galois representations attached to elliptic curves. *Revista matemática iberoamericana*, 39(3):803–844, 2023.

[DM22] Harris Daniels and Jackson Morrow. A group theoretic perspective on entanglements of division fields. *Transactions of the American Mathematical Society. Series B*, 9(27):827–858, 2022.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[Duk97] William Duke. Elliptic curves with no exceptional primes. *Comptes rendus de l'Académie des sciences. Série I. Mathématique*, 325(8):813–818, 1997.

[Elk06] Noam D. Elkies. Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9. *arXiv (Cornell University)*, 2006.

[GLR16] Enrique GonzálezJiménez and Álvaro Lozano-Robledo. Elliptic curves with abelian division fields. *Mathematische Zeitschrift*, 283(3-4):835–859, 2016.

[Gre10] Aaron Greicius. Elliptic curves with surjective adelic Galois representations. *Experimental mathematics*, 19(4):495–507, 2010.

[Jac12] Nathan Jacobson. *Lectures in Abstract Algebra I: Basic Concepts*. Springer Nature, Netherlands, 2012.

[JM20] Nathan Jones and Ken McMurdy. Elliptic curves with non-abelian entanglements. *arXiv: Number Theory (Cornell University)*, 2020.

[Jon10] Nathan Jones. Almost all elliptic curves are Serre curves. *Transactions of the American Mathematical Society*, 362(3):1547–1570, 2010.

[Jon23] Nathan Jones. CM elliptic curves and vertically entangled 2-adic groups. *arXiv: Number Theory (Cornell University)*, 2023.

[KM04] J. Klüners and G. Malle. Counting nilpotent Galois extensions. *Journal für die reine und angewandte Mathematik*, 2004(572):1–26, 2004.

[KS09] Willem Kuyk and Jean-Pierre Serre. *Modular Functions of One Variable III: Proceedings International Summer School, University of Antwerp, RUCA, July 17 - August 3, 1972*, volume 350. Springer, 1st 1973. corr. 2nd printing 1986. edition, 2009.

[LMF24] The LMFDB Collaboration. The L-functions and modular forms database. `https://www.lmfdb.org`, 2024. [Online; accessed 24 September 2024].

[Lom15] Davide Lombardo. Bounds for Serre's open image theorem for elliptic curves over number fields. *Algebra & Number Theory*, 9(10):2347–2395, 2015.

[Lom16] Davide Lombardo. Explicit surjectivity of Galois representations for abelian surfaces and GL_2-varieties. *Journal of algebra*, 460:26–59, 2016.

[LR22] Álvaro Lozano-Robledo. Galois representations attached to elliptic curves with complex multiplication. *Algebra and Number Theory*, 16:777–837, 2022.

[LV13] Eric Larson and Dmitry Vaintrob. On the surjectivity of Galois representations associated to elliptic curves over number fields. *Bulletin of the London Mathematical Society*, 46(1):197–209, 2013.

[Maz78] Barry Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[Maz06] Barry Mazur. *Rational points on modular curves*, pages 107–148. Modular Functions of one Variable V. Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.

[McK94] James F. McKee. Computing division polynomials. *Mathematics of Computation*, 63:767–771, 1994.

[Mor19] Jackson S. Morrow. Composite images of Galois for elliptic curves over $\mathbf{Q}$ and entanglement fields. *Mathematics of computation*, 88(319):2389–2421, 2019.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[NSN07] Nikolay Nikolov, Dan Segal, and Nikolay Nikolav. On finitely generated profinite groups, I: Strong completeness and uniform bounds. *Annals of mathematics*, 165(1):171–238, 2007.

[Pla03] Bernat Plans. Central embedding problems, the arithmetic lifting property, and tame extensions of $\mathbb{Q}$. *International mathematics research notices*, 2003(23):1249–1267, 2003.

[PV03] Bernat Plans and Núria Vila. Tame A_n-extensions of $\mathbb{Q}$. *Journal of algebra*, 266(1):27–33, 2003.

[RSZB22] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown. ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with john voight). *Forum of Mathematics, Sigma*, 10:e62, 2022.

[RV00] Amadeu Reverter and Núria Vila. Polynomials of Galois representations attached to elliptic curves. *Revista de la Real Academia de Ciencias Exactas Físicas y Naturales*, 94(3):417–421, 2000.

[RV01] Amadeu Reverter and Núria Vila. Images of mod p Galois representations associated to elliptic curves. *Canad. Math. Bull.*, 44(3):313–322, 2001.

[RZB15] Jeremy Rouse and David Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. *Research in number theory*, 1(1), 2015.

[SD08] Jean-Pierre Serre and Henri Darmon. *Topics in Galois theory.* Wellesley (Mass.): AK Peters, 2nd edition, 2008.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser81a] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 54:123–201, 1981.

[Ser81b] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Publications mathématiques. Institut des hautes études scientifiques*, 54(1):123–201, 1981.

[Ser89] Jean-Pierre Serre. Abelian ℓ-adic representation and elliptic curves. In *Advanced book classics*, 1989.

[Ser13] Jean-Pierre Serre. *Cohomologie Galoisienne: Cours Au College de France, 1962-1963*, volume 5. Springer Berlin / Heidelberg, Berlin, Heidelberg, 3 edition, 2013.

[Sik19] Samir Siksek. Lecture notes "Explicit arithmetic of modular curves". University of Warwick, 2019.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1994.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics.* Springer, Dordrecht, second edition, 2009.

[ST68] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *JSTOR*, 88(3):492–517, 1968.

[Sut16] Andrew V. Sutherland. Computing images of Galois representations attached to elliptic curves. *Forum of mathematics. Sigma*, 4, 2016.

[SZ17] Andrew V. Sutherland and David Zywina. Modular curves of prime-power level with infinitely many rational points. *Algebra & Number Theory*, 11(5):1199–1229, 2017.

[The22] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.6)*, 2022. `https://www.sagemath.org`.

[Yvo23] Zoé Yvon. Polynomials realizing images of Galois representations of an elliptic curve. *Functiones et Approximatio Commentarii Mathematici*, 69(1), 2023.

[Yvo24] Zoé Yvon. Coincidences of division fields of an elliptic curve defined over a number field. *arXiv: Number Theory (Cornell University)*, 2024.

[Zyw10] David Zywina. Elliptic curves with maximal Galois action on their torsion points. *Bulletin of the London Mathematical Society*, 42(5):811–826, 2010.

[Zyw15] David Zywina. On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$. *arXiv: Number Theory (Cornell University)*, 2015.

[Zyw22a] David Zywina. On the surjectivity of mod ℓ representations associated to elliptic curves. *Bulletin of the London Mathematical Society*, 54(6):2404–2417, 2022.

[Zyw22b] David Zywina. Possible indices for the Galois image of elliptic curves over $\mathbb{Q}$. *arXiv: Number Theory (Cornell University)*, 2022.

[Zyw24a] David Zywina. Explicit open images for elliptic curves over $\mathbb{Q}$. *arXiv: Number Theory (Cornell University)*, 2024.

[Zyw24b] David Zywina. Open image computations for elliptic curves over number fields. *arXiv: Number Theory (Cornell University)*, 2024.