New York Journal of Mathematics

New York J. Math. **28** (2022) 182–229.

Elliptic curves with non-abelian entanglements

Nathan Jones and Ken McMurdy

ABSTRACT. In this paper we consider the problem of classifying quadruples (K, E, m_1, m_2) where K is a number field, E is an elliptic curve defined over K and (m_1, m_2) is a pair of relatively prime positive integers for which the intersection $K(E[m_1]) \cap K(E[m_2])$ is a non-abelian extension of K. There is an infinite set $\mathcal{S}$ of modular curves whose K-rational points capture all elliptic curves over K without complex multiplication that have this property. Our main theorem explicitly describes the subset $\mathcal{S}_0 \subseteq \mathcal{S}$ consisting of those modular curves having genus zero. The subset $\mathcal{S}_0$ turns out to consist of four modular curves, each isomorphic to $\mathbb{P}^1$ over its field of definition. In the case $K = \mathbb{Q}$, this has applications to the problem of determining when the Galois representation on the torsion of E is as large as possible modulo a prescribed obstruction; we illustrate this application with a specific example.

CONTENTS

1. Introduction

Let K be a field of characteristic zero and E an elliptic curve over K. For a positive integer m, let $E[m]$ denote the m-torsion of E and

$$K(E[m]) := K\left(\left\{x, y \in \overline{K} : (x, y) \in E[m]\right\}\right)$$

the m-th division field of E over K, obtained by adjoining to K the x and y coordinates of the m-torsion of some (any) Weierstrass model of E. The restriction

Received February 23, 2021.

2010 *Mathematics Subject Classification.* Primary 11G05, 11F80.

Key words and phrases. Elliptic curve, Galois representation, entanglement, division field, Serre curve.

ISSN 1076-9803/2022

of $\mathrm{Gal}(K(E[m])/K)$ to $E[m]$ gives rise to an embedding

$$\mathrm{Gal}(K(E[m])/K) \hookrightarrow \mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

the latter isomorphism induced by the choice of a $\mathbb{Z}/m\mathbb{Z}$-basis for $E[m]$, which is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank 2. It is of interest to understand the image of this embedding as m varies over all positive integers, for K and E fixed. In the present paper, we are focused on the case where m has more than one distinct prime factor. Writing $m = m_1m_2$ where $\gcd(m_1, m_2) = 1$ and each m_i is greater than 1, we have

$$\begin{aligned}\mathrm{Gal}(K(E[m])/K) &\subseteq \mathrm{Gal}(K(E[m_1])/K) \times \mathrm{Gal}(K(E[m_2])/K)\\ &\subseteq \mathrm{GL}_2(\mathbb{Z}/m_1\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/m_2\mathbb{Z}).\end{aligned}$$

By Galois theory, the first inclusion is proper if and only if $K(E[m_1]) \cap K(E[m_2]) \neq K$. In particular, understanding $\mathrm{Gal}(K(E[m])/K)$ amounts to understanding each of the groups $\mathrm{Gal}(K(E[m_1])/K)$, $\mathrm{Gal}(K(E[m_2])/K)$ as well as the *entanglement* $K(E[m_1]) \cap K(E[m_2])$, and "how it sits" inside $K(E[m_1])$ and $K(E[m_2])$. In recent years, there has been significant interest in both the nature of division fields $K(E[m])$ for composite level m (see for instance [22], [25] and [20]) and the nature of entanglements (see [10], [6] and [9]).

Definition 1.1. Let E be an elliptic curve defined over a field K and let $m \in \mathbb{N}$ be a positive integer that is divisible by at least two primes. We call a factorization $m = m_1m_2$ of m **permissible** if the factors m_1 and m_2 are co-prime and each greater than one. Given a permissible factorization $m = m_1m_2$, we call the field extension $K(E[m_1]) \cap K(E[m_2])/K$ the **entanglement associated to** E/K **and** (m_1, m_2). We say that E **has a non-abelian entanglement over** K **at level** m if, for some permissible factorization $m = m_1m_2$, the entanglement associated to E/K and (m_1, m_2) is a non-abelian extension of K. Finally, we say that E **has a non-abelian entanglement over** K if it has a non-abelian entanglement over K at some level m.

Remark 1.2. In case the pair (m_1, m_2) is uniquely determined by m (i.e. in case m has exactly 2 distinct prime factors), we call the extension $K(E[m_1]) \cap K(E[m_2])/K$ the **entanglement at** m **associated to** E/K.

In the present paper, we are concerned with the following problem.

Problem 1.3. For a given number field K, classify the elliptic curves E over K that have a non-abelian entanglement over K. (This is a restatement of [5, Question 1.1].)

Remark 1.4. Mazur's Program B [19] asks for a classification of elliptic curves E over a number field K for which $\rho_E\left(\mathrm{Gal}(\overline{K}/K)\right) \subseteq G$, where $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is a given open (or equivalently, finite index) subgroup and

$$\rho_E : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}_2(\hat{\mathbb{Z}})$$

is the Galois representation defined by letting $\mathrm{Gal}(\overline{K}/K)$ act on the torsion subgroup $E_{\mathrm{tors}} := \bigcup_{m=1}^{\infty} E[m]$ of E and fixing a compatible system of $\mathbb{Z}/m\mathbb{Z}$-bases. (In the above, $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z} \simeq \prod_{\ell \text{ prime}} \mathbb{Z}_\ell$ is the inverse limit of the rings $\{\mathbb{Z}/m\mathbb{Z} : m \in \mathbb{N}\}$, ordered by divisibility.) The present paper settles a particular case of this problem, namely the case where G is a non-abelian entanglement group (see Definition 1.5 below) for which the associated modular curve has genus zero.

It is difficult to address Problem 1.3 completely, since non-abelian entanglements can correspond to K-rational points on modular curves of genus greater than 1, and could thus occur "sporadically" for large m, a la Faltings' Theorem. We therefore focus at present on classifying all "one-parameter families" of non-abelian entanglements, or in other words on the case where the associated modular curve has genus zero.

To state our main theorem precisely, we need to recall a few fundamentals about modular curves. For an arbitrary level $m \in \mathbb{N}$, we let $X(m)$ denote the complete modular curve of level m, which parametrizes pairs $(E, \mathcal{B})$, where E is an elliptic curve and $\mathcal{B} \subseteq E[m]$ is an ordered $\mathbb{Z}/m\mathbb{Z}$-basis of $E[m]$. The modular curve $X(m)$ is equipped with a natural "forgetful map," $j_m : X(m) \longrightarrow X(1) \simeq \mathbb{P}^1$, whose modular interpretation is $j_m((E, \mathcal{B})) = E$. The group $\mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ acts on $X(m)$, and the kernel of this action is $\{I, -I\} \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. For any $G(m) \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, we enlarge $G(m)$ by setting

$$\tilde{G}(m) := \langle G(m), -I \rangle$$

and define the modular curve $X_{\tilde{G}(m)}$ to be the quotient curve of orbits under the action of $\tilde{G}(m)$:

$$X_{\tilde{G}(m)} := X(m)/\tilde{G}(m).$$

Let $F = \mathbb{Q}(\mu_m)^{\det(G(m))}$ be the subfield of $\mathbb{Q}(\mu_m)$ fixed by the subgroup

$$\det(G(m)) = \det(\tilde{G}(m)) \subseteq (\mathbb{Z}/m\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}).$$

The modular curve $X_{\tilde{G}(m)}$ is defined over F. In particular, $X_{\tilde{G}(m)}$ is defined over $\mathbb{Q}$ if and only if $\det(G(m)) = (\mathbb{Z}/m\mathbb{Z})^\times$. Furthermore, the forgetful map j_m on $X(m)$ induces a map

$$j_{\tilde{G}(m)} : X_{\tilde{G}(m)} \longrightarrow X(1) \simeq \mathbb{P}^1.$$

Note that in the above construction, the modular curves $X_{\tilde{G}_1(m)}$ and $X_{\tilde{G}_2(m)}$ are isomorphic over $\mathbb{Q}$ whenever $G_1(m)$ and $G_2(m)$ are conjugate inside $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. It is thus sensible to coarsen the relations of equality and subset inclusion on the set of subgroups of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ to $\doteq$ and $\dot{\subseteq}$, where

$$\begin{aligned} G_1(m) \doteq G_2(m) &\overset{\text{def}}{\iff} \exists g \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \text{ with } G_1(m) = gG_2(m)g^{-1} \\ G_1(m) \dot{\subseteq} G_2(m) &\overset{\text{def}}{\iff} \exists g \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \text{ with } G_1(m) \subseteq gG_2(m)g^{-1}. \end{aligned} \tag{1}$$

Using this notation, a modular interpretation of rational points on $X_{\tilde{G}(m)}$ can be phrased as follows: For any number field K with $F \subseteq K$ and $x \in K - \{0, 1728\}$, $x \in j_{\tilde{G}(m)}(X_{\tilde{G}(m)}(K))$ if and only if there is an elliptic curve E defined over K with j-invariant equal to x and for which $\mathrm{Gal}(K(E[m])/K) \dot{\subseteq} \tilde{G}(m)^t$. In particular, we are choosing to let $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ act on $X(m)$ on *the left*[1]. For a helpful discussion about this issue, see [22, Remark 2.2]. For full background details, see [11].

There is an infinite set of modular curves (see $\mathcal{G}^{\max}_{\mathrm{non-ab}}$ below) whose K-rational points capture all elliptic curves over K without complex multiplication that have a non-abelian entanglement. Our main theorem explicitly describes the (finite) subset consisting of those modular curves having genus zero. Because the level m will vary, we rephrase our definitions in terms of finite index (i.e. open) subgroups $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, where

$$\mathrm{GL}_2(\hat{\mathbb{Z}}) = \varprojlim \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \simeq \prod_p \mathrm{GL}_2(\mathbb{Z}_p).$$

For any open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, we denote by m_G its *level*, i.e. the smallest $m \in \mathbb{N}$ for which $\ker\big(\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})\big) \subseteq G$, and for any $m \in \mathbb{N}$ we define $G(m) := G \mod m \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. We extend our notation for the associated modular curve by setting

$$\tilde{G} := \langle G, -I \rangle \tag{2}$$

and setting the notation

$$X_{\tilde{G}} := X_{\tilde{G}(m_{\tilde{G}})}, \qquad j_{\tilde{G}} := j_{\tilde{G}(m_{\tilde{G}})} : X_{\tilde{G}} \longrightarrow X(1).$$

Definition 1.5. Let $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ be an open subgroup of level m_G. We say that G is a **non-abelian entanglement group** if there is a number field K and an elliptic curve E over K having a non-abelian entanglement at level m_G and satisfying $G(m_G) \doteq \mathrm{Gal}(K(E[m_G])/K)$. We call G a **maximal non-abelian entanglement group** if G is a non-abelian entanglement group that is maximal with respect to $\dot{\subseteq}$ among all non-abelian entanglement groups.

Remark 1.6. Note that non-abelian entanglement groups may be defined in terms of fibered products. Indeed, let $\psi_1 : G_1 \to \Gamma$ and $\psi_2 : G_2 \to \Gamma$ be surjective homomorphisms onto a common quotient group Γ, let ψ denote the ordered pair (ψ_1, ψ_2) and let

$$G_1 \times_\psi G_2 := \{(g_1, g_2) \in G_1 \times G_2 : \psi_1(g_1) = \psi_2(g_2)\}$$

denote the corresponding fibered product group. By considering Definition 1.5 and the Galois correspondence, we may see that an open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$

[1]As is easily verified by direct computation, all subgroups $G(m) \subseteq \mathrm{GL}(\mathbb{Z}/m\mathbb{Z})$ produced in the present paper satisfy the property that

$$G(m)^t := \{g^t : g \in G(m)\}$$

is $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$-conjugate to $G(m)$, and so our results are not affected by the choice of left action versus right action.

is a non-abelian entanglement group if and only if there is a level $m \in \mathbb{N}$ that admits a permissible factorization $m = m_1 m_2$ and, under the isomorphism $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{Z}/m_1\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/m_2\mathbb{Z})$ of the Chinese Remainder Theorem, we have $G(m) \simeq G(m_1) \times_\psi G(m_2)$, where the associated common quotient Γ is a non-abelian group.

Next we elaborate on a technicality that arises from the distinction between G and $\tilde{G}$ in the case when $-I \notin G$. For a given elliptic curve E over K and open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, the property of whether or not $\mathrm{Gal}(K(E[m])/K) \dot{\subseteq} \tilde{G}(m)$ is independent of twisting in the sense that it is a function just of the j-invariant of E (i.e. of the $\overline{K}$-isomorphism class of E). By contrast, in case $-I \notin G(m)$, the finer question of whether or not $\mathrm{Gal}(K(E[m])/K) \dot{\subseteq} G(m)$ for E corresponding to a point of $X_{\tilde{G}}(K)$ may change as we twist E (i.e. as we vary E within a fixed $\overline{K}$-isomorphism class). This motivates the following terminology.

Definition 1.7. We say that a subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is **twist-independent** if $-I \in G$; otherwise we say that G is **twist-dependent**.

We now fix notation used in the main theorem. Define the following subgroups $G_m \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$:

$$\begin{aligned}
G_6 &:= \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : g \mod 6 \in \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 1 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 5 & 4 \\ 4 & 1 \end{pmatrix} \right\rangle \right\}, \\
G_{10} &:= \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : g \mod 10 \in \left\langle \begin{pmatrix} 5 & 6 \\ 4 & 5 \end{pmatrix}, \begin{pmatrix} 4 & 9 \\ 9 & 6 \end{pmatrix}, \begin{pmatrix} 7 & 3 \\ 9 & 4 \end{pmatrix} \right\rangle \right\}, \\
G_{15} &:= \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : g \mod 15 \in \left\langle \begin{pmatrix} 2 & 3 \\ 14 & 14 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 14 & 0 \end{pmatrix} \right\rangle \right\}, \\
G_{18} &:= \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : g \mod 18 \in \left\langle \begin{pmatrix} 7 & 17 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 17 & 3 \\ 3 & 14 \end{pmatrix}, \begin{pmatrix} 4 & 3 \\ 3 & 14 \end{pmatrix} \right\rangle \right\}.
\end{aligned} \tag{3}$$

Note that each of the underlying levels is divisible by exactly 2 primes, and thus we have the unique permissible factorizations

$$6 = 2 \cdot 3, \qquad 10 = 2 \cdot 5, \qquad 15 = 3 \cdot 5, \qquad 18 = 2 \cdot 9. \tag{4}$$

Also, each of these groups is checked to be twist-independent. Next, we define the rational functions j_6, j_{10}, j_{15} and j_{18} by

$$\begin{aligned}
j_6(t) &:= 2^{10}\, 3^3\, t^3(1 - 4t^3) \\
j_{10}(t) &:= s_{10}^3(s_{10}^2 + 5s_{10} + 40), \qquad s_{10} = \frac{3t^6 + 12t^5 + 80t^4 + 50t^3 - 20t^2 - 8t + 8}{(t-1)^2(t^2 + 3t + 1)^2} \\
j_{15}(t) &:= s_{15}^3(s_{15}^2 + 5s_{15} + 40), \qquad s_{15} = t^3 - \frac{5 - 3\sqrt{-15}}{2} \\
j_{18}(t) &:= \frac{-3^3\, t^3(t^3 - 2)(3t^3 - 4)^3(3t^3 - 2)^3}{(t^3 - 1)^2}.
\end{aligned} \tag{5}$$

For $g \in \mathbb{Z}_{\geq 0}$ we set

$$\begin{aligned}
\mathcal{G} &:= \{G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}}) : \ G \text{ open}\} \\
\mathcal{G}(g) &:= \{G \in \mathcal{G} : \mathrm{genus}(X_{\tilde{G}}) = g\} \\
\mathcal{G}_{\mathrm{non-ab}} &:= \{G \in \mathcal{G} : G \text{ a non-abelian entanglement group}\} \\
\mathcal{G}_{\mathrm{non-ab}}(g) &:= \mathcal{G}_{\mathrm{non-ab}} \cap \mathcal{G}(g) \\
\mathcal{G}^{\max}_{\mathrm{non-ab}} &:= \{G \in \mathcal{G}_{\mathrm{non-ab}} : \nexists H \in \mathcal{G}_{\mathrm{non-ab}} \text{ with } G \dot{\subsetneq} H\} \\
\mathcal{G}^{\max}_{\mathrm{non-ab}}(g) &:= \mathcal{G}^{\max}_{\mathrm{non-ab}} \cap \mathcal{G}(g),
\end{aligned}$$

where we are extending the definitions (1) of $\doteq$ and $\dot{\subseteq}$ in the obvious way to subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, and $G \dot{\subsetneq} H$ means that $G \dot{\subseteq} H$ and $G \not\doteq H$. Furthermore, we extend the relations $\dot{\subseteq}$ and $\doteq$ to subsets $\mathcal{S}_1, \mathcal{S}_2 \subseteq \mathcal{G}$ by declaring that

$$\begin{aligned}
\mathcal{S}_1 \dot{\subseteq} \mathcal{S}_2 &\overset{\text{def}}{\iff} \forall G_1 \in \mathcal{S}_1 \, \exists G_2 \in \mathcal{S}_2 \text{ with } G_1 \doteq G_2 \\
\mathcal{S}_1 \doteq \mathcal{S}_2 &\overset{\text{def}}{\iff} \mathcal{S}_1 \dot{\subseteq} \mathcal{S}_2 \text{ and } \mathcal{S}_2 \dot{\subseteq} \mathcal{S}_1.
\end{aligned}$$

In particular, note that one could have $\mathcal{S}_1 \doteq \mathcal{S}_2$ even though $\#\mathcal{S}_1 \neq \#\mathcal{S}_2$, since for any single element $G_1 \in \mathcal{S}_1$, we could have $G_1 \doteq G_2$ for many different $G_2 \in \mathcal{S}_2$.

Theorem 1.8. *We have*

$$\mathcal{G}^{\max}_{\mathrm{non-ab}}(0) \doteq \{G_6, G_{10}, G_{15}, G_{18}\}, \tag{6}$$

where the groups G_m are as in (3)*. In other words, every $G \in \mathcal{G}^{\max}_{\mathrm{non-ab}}(0)$ is $\mathrm{GL}_2(\hat{\mathbb{Z}})$-conjugate to exactly one of the groups G_m appearing in the right-hand set. Furthermore, each group G_m is twist-independent of level m, and there is a parameter t on X_{G_m} for which*

$$j_{G_m}(t) = j_m(t),$$

where $j_m(t)$ is as in (5)*. The modular curves X_{G_6}, $X_{G_{10}}$, and $X_{G_{18}}$ are defined over $\mathbb{Q}$, whereas the modular curve $X_{G_{15}}$ is defined over $\mathbb{Q}(\sqrt{-15})$. Finally, in all cases the underlying entanglement is an S_3-entanglement, i.e. for each $G_m \in \mathcal{G}^{\max}_{\mathrm{non-ab}}(0)$ and for each elliptic curve E over a number field K satisfying $j(E) \in j_{G_m}(X_{G_m}(K))$ and $\mathrm{Gal}(K(E[m])/K) \doteq G_m(m)$, we have*

$$\mathrm{Gal}(K(E[m_1]) \cap K(E[m_2])/K) \simeq S_3,$$

where $m = m_1 m_2$ is the unique permissible factorization of m as in (4) *and S_3 denotes the symmetric group of order 6.*

Remark 1.9. The infinite family of j-invariants $j_6(t) = 2^{10}\, 3^3\, t^3(1 - 4t^3)$ was considered in previous work of the first author (see [5]). In that paper, it is incorrectly stated that, for any elliptic curve E over $\mathbb{Q}$ with j-invariant j_E, we have $j_E = j_6(t_0)$ for some $t_0 \in \mathbb{Q}$ if and only if $E \simeq_{\overline{\mathbb{Q}}} E'$ for some elliptic curve E' over $\mathbb{Q}$ satisfying $\mathbb{Q}(E'[2]) \subseteq \mathbb{Q}(E'[3])$. Although the "only if" part is correct, the converse can fail for elliptic curves $E/\mathbb{Q}$ satisfying $\mathbb{Q}(E[2]) = \mathbb{Q}$. A correct

biconditional statement is as follows: For each elliptic curve E over $\mathbb{Q}$ with j-invariant $j_E \in \mathbb{Q} - \{0, 1728\}$, $j_E = j_6(t_0)$ for some $t_0 \in \mathbb{Q}$ if and only if there exists $E'/\mathbb{Q}$ with

$$E' \simeq_{\overline{\mathbb{Q}}} E,\ [\mathbb{Q}(E'[2]) : \mathbb{Q}] = 6 \text{ and } \mathbb{Q}(E'[2]) \subseteq \mathbb{Q}(E'[3]).$$

The first author thanks Maarten Derickx for pointing out this correction. It was also identified in [20, Theorem 8.6].

Remark 1.10. When $K = \mathbb{Q}$, Theorem 1.8 leads in some cases to precise criteria for detecting elliptic curves over $\mathbb{Q}$ for which every $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ is as large as possible, relative to a given obstruction. We discuss this in more detail in Section 4. Another motivation to consider Problem 1.3 is its relationship to constants decorating the main term in various conjectures attached to elliptic curves (see [4]).

The proof of Theorem 1.8 breaks up into two main steps. The first is to establish Proposition 1.12 below, which reduces the problem to a finite search and hence enables us to verify (6) by explicit computation. The proposition is established in Section 2 by a series of technical group-theoretical lemmas, essentially deriving properties of G that are visible at the lower SL_2-level whenever the GL_2-level and SL_2-level differ (see Definition 1.11 below). For $g \geq 1$, the latter statement of Proposition 1.12 is false, in that even *maximal* non-abelian entanglement groups can have distinct SL_2-level and GL_2-level. The proposition also fails to hold, even for $g = 0$, if we remove the maximality assumption. To illustrate this fact, we have included in Section 5 an infinite family of (non-maximal) genus 0 non-abelian entanglement groups with unbounded GL_2-level. The second main step in the proof of Theorem 1.8 is to derive explicit models for the modular curves, as well as the corresponding maps to the j-line. This work is done in Section 3.

For any open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, we recall and extend the concept of its level m_G in the following definition.

Definition 1.11. For an open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, we define the positive integer

$$m_{\mathrm{GL}_2}(G) := \min\left\{m \in \mathbb{N} : \ker\left(\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})\right) \subseteq G\right\}$$

and call it the GL_2-**level of** G. Furthermore, we define the SL_2-**level of** G by

$$m_{\mathrm{SL}_2}(G) := \min\left\{m \in \mathbb{N} : \ker\left(\mathrm{SL}_2(\hat{\mathbb{Z}}) \to \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})\right) \subseteq G\right\}.$$

It is straightforward to see that $m_{\mathrm{SL}_2}(G)$ always divides $m_{\mathrm{GL}_2}(G)$; they may or may not be equal. Next, for any level $m \in \mathbb{N}$, we define

$$\mathcal{G}_{\mathrm{non-ab}}^{m_{\mathrm{SL}_2}=m} := \{G \in \mathcal{G}_{\mathrm{non-ab}} : m_{\mathrm{SL}_2}(G) = m\},\ \mathcal{G}_{\mathrm{non-ab}}^{m_{\mathrm{SL}_2}=m}(g) := \mathcal{G}_{\mathrm{non-ab}}^{m_{\mathrm{SL}_2}=m} \cap \mathcal{G}(g),$$
$$\mathcal{G}_{\mathrm{non-ab}}^{m_{\mathrm{GL}_2}=m} := \{G \in \mathcal{G}_{\mathrm{non-ab}} : m_{\mathrm{GL}_2}(G) = m\},\ \mathcal{G}_{\mathrm{non-ab}}^{m_{\mathrm{GL}_2}=m}(g) := \mathcal{G}_{\mathrm{non-ab}}^{m_{\mathrm{GL}_2}=m} \cap \mathcal{G}(g).$$

Proposition 1.12. *With the notation just outlined, we have*

$$\mathcal{G}_{\mathrm{non-ab}}(0) = \bigsqcup_{m\in\mathcal{L}} \mathcal{G}_{\mathrm{non-ab}}^{m_{\mathrm{SL}_2}=m}(0), \tag{7}$$

where $\mathcal{L} = \{6, 10, 12, 15, 18, 20, 24, 30, 36, 40, 48, 60, 72, 96\}$. *Furthermore, for every* $G \in \mathcal{G}_{\mathrm{non-ab}}^{\max}(0)$, *we have* $m_{\mathrm{GL}_2}(G) = m_{\mathrm{SL}_2}(G)$.

As a byproduct of the computations involved in the proof of Proposition 1.12, we obtain, for each $m \in \mathcal{L}$, an explicit list of the groups $G \in \mathcal{G}_{\mathrm{non-ab}}^{m_{\mathrm{GL}_2}=m}(0)/\doteq$. Tables 1–3 list the number of $G \in \mathcal{G}_{\mathrm{non-ab}}^{m_{\mathrm{GL}_2}=m}(0)/\doteq$, sorted according to the Galois group of the underlying entanglement. More precisely, for any non-abelian entanglement group G of level m and elliptic curve E over K satisfying

$$G(m) \doteq \mathrm{Gal}(K(E[m])/K), \tag{8}$$

there exists by definition a permissible factorization $m = m_1m_2$ so that

$$\Gamma := \mathrm{Gal}(K(E[m_1]) \cap K(E[m_2])/K) \tag{9}$$

is a non-abelian group. By (8) and the Galois correspondence, the group Γ in (9) is uniquely determined by G and the pair (m_1, m_2); we call Γ *the quotient associated to* G *and* (m_1, m_2). In case the level m has only two distinct primes in its factorization, the co-prime integers m_1 and m_2 satisfying $m = m_1m_2$ are uniquely determined; in this case we simply call Γ *the quotient associated to* G and define $\mathcal{G}_{\mathrm{non-ab}}^{m_{\mathrm{GL}_2}=m}(g, \Gamma)$ to be the set of all $G \in \mathcal{G}_{\mathrm{non-ab}}^{m_{\mathrm{GL}_2}=m}(g)$ for which Γ is the quotient associated to G. There are exactly three groups Γ that arise as non-abelian quotients associated to $G \in \bigcup_{m\in\mathcal{L}} \mathcal{G}_{\mathrm{non-ab}}^{m_{\mathrm{GL}_2}=m}(0)$, namely the dihedral groups D_3 ($\simeq S_3$) and D_6, of orders 6 and 12 respectively, and the dicyclic group[2] Dic_3 of order 12. For levels $m \in \mathcal{L}$ that are divisible by just two distinct primes, our results give the data displayed in Table 1.

For the remaining levels $m \in \{30, 60\}$, we must refine the definition of $\mathcal{G}_{\mathrm{non-ab}}^{m_{\mathrm{GL}_2}=m}(g, \Gamma)$ to reflect the dependence on the pair (m_1, m_2) occurring in the permissible factorization $m = m_1m_2$, which is not unique in this case. Hence, for any finite non-abelian group Γ, we define $\mathcal{G}_{\mathrm{non-ab}}^{m_{\mathrm{GL}_2}=m}(g, (m_1, m_2), \Gamma)$ to be the set of all $G \in \mathcal{G}_{\mathrm{non-ab}}^{m_{\mathrm{GL}_2}=m}(g)$ for which Γ is the quotient associated to G and (m_1, m_2). Regarding $m \in \{30, 60\}$, the non-abelian group Γ above is found to be either D_3 or D_6, and these groups occur with the frequencies indicated in Table 2 and Table 3.

What can we say about groups $G \in \mathcal{G}_{\mathrm{non-ab}}(0)$ satisfying $m_{\mathrm{GL}_2(G)} > 96$? As mentioned earlier, we will see that the set

$$\{G \in \mathcal{G}_{\mathrm{non-ab}}(0) : m_{\mathrm{SL}_2}(G) = m,\ m_{\mathrm{GL}_2}(G) > m\}$$

[2]The dicyclic group satisfies $\mathrm{Dic}_3 \simeq \mathbb{Z}/4\mathbb{Z} \ltimes \mathbb{Z}/3\mathbb{Z}$, where the map $\mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ defining the semidirect product structure is the unique non-trivial group homomorphism.

m	$\left\lvert \mathcal{G}_{\text{non-ab}}^{m_{\text{GL}_2}=m}(0, D_3) \,/\doteq \right\rvert$	$\left\lvert \mathcal{G}_{\text{non-ab}}^{m_{\text{GL}_2}=m}(0, D_6) \,/\doteq \right\rvert$	$\left\lvert \mathcal{G}_{\text{non-ab}}^{m_{\text{GL}_2}=m}(0, \text{Dic}_3) \,/\doteq \right\rvert$
6	4	0	0
10	1	0	0
12	10	2	0
15	1	0	0
18	10	0	0
20	3	0	1
24	38	16	0
36	24	6	0
40	1	0	1
48	40	16	0
72	6	32	0
96	4	8	0

TABLE 1. Frequencies of genus zero non-abelian entanglement groups of level $\in \mathcal{L} \backslash \{30, 60\}$

(m_1, m_2)	$\left\lvert \mathcal{G}_{\text{non-ab}}^{m_{\text{GL}_2}=30}(0, (m_1, m_2), D_3) \,/\doteq \right\rvert$	$\left\lvert \mathcal{G}_{\text{non-ab}}^{m_{\text{GL}_2}=30}(0, (m_1, m_2), D_6) \,/\doteq \right\rvert$
(2, 15)	22	0
(3, 10)	16	4
(5, 6)	2	0

TABLE 2. Frequencies of genus zero non-abelian entanglement groups of level $= 30$

(m_1, m_2)	$\left\lvert \mathcal{G}_{\text{non-ab}}^{m_{\text{GL}_2}=60}(0, (m_1, m_2), D_3) \,/\doteq \right\rvert$	$\left\lvert \mathcal{G}_{\text{non-ab}}^{m_{\text{GL}_2}=60}(0, (m_1, m_2), D_6) \,/\doteq \right\rvert$
(4, 15)	0	14
(3, 20)	0	14
(5, 12)	0	0

TABLE 3. Frequencies of genus zero non-abelian entanglement groups of level $= 60$

is infinite for some $m \in \mathcal{L}$ (see Section 5). We emphasize that, according to Proposition 1.12, this does not happen when we restrict to $\mathcal{G}_{\text{non-ab}}^{\max}(0)$, i.e. we

have

$$\{G \in \mathcal{G}_{\mathrm{non-ab}}^{\max}(0) : m_{\mathrm{SL}_2}(G) < m_{\mathrm{GL}_2}(G)\} = \emptyset.$$

1.1. Remarks on computation. All of the computations necessary to justify the theorems in this paper were performed using the computational software package MAGMA [2]. The code used to perform these computations can be found at the following link:

`https://github.com/ncjones-uic/NonabelianEntanglements`

Additional computations related to the development of the results in Section 3 were performed using SageMath [26]. However, those computations are not necessary for verifying said results.

Acknowledgements. The authors would like to thank David Zureick-Brown for insightful conversations and also Jackson Morrow and Harris Daniels, as well as Andrew Sutherland, for helpful comments on an earlier version of the paper. Finally, we thank the anonymous referee for a careful reading of the manuscript and many helpful suggestions for improvement.

2. Reducing to a finite search

In this section we prove Proposition 1.12, which reduces the computation of $\mathcal{G}_{\mathrm{non-ab}}^{\max}(0)/\doteq$ to a finite search. We consider the quotient set

$$\mathcal{G}_{\mathrm{non-ab}}(0)/\doteq$$

of all open subgroups $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ of genus zero that are non-abelian entanglement groups in the sense of Definition 1.5, up to conjugation inside $\mathrm{GL}_2(\hat{\mathbb{Z}})$. More generally, we may fix an arbitrary genus g and consider the quotient set $\mathcal{G}(g)/\doteq$. In what follows, we will be discussing the corresponding set of modular curves $\{X_{\tilde{G}} : G \in \mathcal{G}(g)/\doteq\}$, so it will be natural to introduce the notation

$$\tilde{\mathcal{G}} := \{\tilde{G} : G \in \mathcal{G}\}, \qquad \tilde{\mathcal{G}}(g) := \{\tilde{G} : G \in \mathcal{G}(g)\},$$

and the associated set of modular curves

$$\{X_{\tilde{G}} : \tilde{G} \in \tilde{\mathcal{G}}/\doteq\}.$$

If we view these modular curves *geometrically*, i.e. if we regard two such curves as equivalent if they are isomorphic over $\overline{K}$, then the further quotient set

$$\{X_{\tilde{G}} : \tilde{G} \in \tilde{\mathcal{G}}(g)/\doteq\}/\simeq_{\overline{K}} \tag{10}$$

of geometric modular curves is finite, for any fixed $g \in \mathbb{Z}_{\geq 0}$. This may be restated in terms of the groups $\tilde{G} \in \tilde{\mathcal{G}}(g)/\doteq$ as follows. We have

$$X_{\tilde{G}_1} \simeq_{\overline{K}} X_{\tilde{G}_2} \iff \tilde{G}_1 \cap \mathrm{SL}_2(\hat{\mathbb{Z}}) \doteq \tilde{G}_2 \cap \mathrm{SL}_2(\hat{\mathbb{Z}}).$$

Thus, coarsening the relation $\doteq$ to $\doteq_{\mathrm{SL}_2}$, defined by

$$\tilde{G}_1 \doteq_{\mathrm{SL}_2} \tilde{G}_2 \overset{\text{def}}{\iff} \tilde{G}_1 \cap \mathrm{SL}_2(\hat{\mathbb{Z}}) \doteq \tilde{G}_2 \cap \mathrm{SL}_2(\hat{\mathbb{Z}}),$$

we have that

$$\left|\tilde{\mathcal{G}}(g)/\doteq_{\mathrm{SL}_2}\right| < \infty \qquad \left(g \in \mathbb{Z}_{\geq 0}\right). \tag{11}$$

However, within each $\doteq_{\mathrm{SL}_2}$-equivalence class, there are infinitely many $\doteq$-equivalence classes, which corresponds in part to the fact that any given $\overline{K}$-isomorphism class in (10) contains infinitely many twists, i.e. infinitely many K-isomorphism classes. The case $g = 0$ of (11) is equivalent to a well-known conjecture of Rademacher that was proven by Dennin (see [12]). More generally, in [27] and [28], the same is shown for a general $g \in \mathbb{Z}_{\geq 0}$. In addition, there is a fair amount of literature on the *effective* resolution of Rademacher's conjecture. In particular, Cummins and Pauli [8] have produced the complete list of the elements of $\tilde{\mathcal{G}}(g)/\doteq_{\mathrm{SL}_2}$ for $g \leq 24$; it can be seen in the tables therein that

$$G \in \mathcal{G}(0) \implies m_{\mathrm{SL}_2}(\tilde{G}) \in \begin{Bmatrix} 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15, \\ 16,18,20,21,24,25,26,27,28,30,32,36,48 \end{Bmatrix}. \tag{12}$$

It is possible that $m_{\mathrm{SL}_2}(G) > m_{\mathrm{SL}_2}(\tilde{G})$, and the following lemma controls this difference.

Lemma 2.1. *Let $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ be an open subgroup. We then have*

$$\frac{m_{\mathrm{SL}_2}(G)}{m_{\mathrm{SL}_2}(\tilde{G})} \in \{1,2\}, \tag{13}$$

where $\tilde{G}$ is as in (2)*.*

Lemma 2.1 will be established as a corollary of the Lemmas 2.4 and 2.5 below, which are in turn aided by the next two lemmas.

Lemma 2.2. *There is no proper subgroup $S \subsetneq \mathrm{SL}_2(\hat{\mathbb{Z}})$ satisfying $\tilde{S} = \mathrm{SL}_2(\hat{\mathbb{Z}})$.*

Proof. See [30, Lemma 2.3]. □

Lemma 2.3. *(Goursat's Lemma) Let G_1, G_2 be groups and for $i \in \{1,2\}$ denote by $\mathrm{pr}_i : G_1 \times G_2 \longrightarrow G_i$ the projection map onto the i-th factor. Let $G \subseteq G_1 \times G_2$ be a subgroup and assume that*

$$\mathrm{pr}_1(G) = G_1, \ \mathrm{pr}_2(G) = G_2.$$

Then there exists a group Γ together with a pair of surjective homomorphisms

$$\psi_1 : G_1 \longrightarrow \Gamma$$
$$\psi_2 : G_2 \longrightarrow \Gamma$$

so that

$$G = G_1 \times_\psi G_2 := \{(g_1, g_2) \in G_1 \times G_2 : \psi_1(g_1) = \psi_2(g_2)\}.$$

Proof. See [21, Lemma (5.2.1)]. □

Lemma 2.4. *Suppose that $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is an open subgroup satisfying*

$$m_{\mathrm{SL}_2}(\tilde{G}) < m_{\mathrm{SL}_2}(G)$$

and that there is a prime p dividing $m_{\mathrm{SL}_2}(G)$ that does not divide $m_{\mathrm{SL}_2}(\tilde{G})$. Then $p = 2$ (so $m_{\mathrm{SL}_2}(\tilde{G})$ is odd) and $m_{\mathrm{SL}_2}(G) = 2m_{\mathrm{SL}_2}(\tilde{G})$.

Proof. First, we set $S := G \cap \mathrm{SL}_2(\hat{\mathbb{Z}})$, so that $\tilde{S} = \tilde{G} \cap \mathrm{SL}_2(\hat{\mathbb{Z}})$ as well; furthermore, we make the abbreviations

$$\begin{aligned} m_S :=& m_{\mathrm{SL}_2}(S) & m_{\tilde{S}} :=& \ m_{\mathrm{SL}_2}(\tilde{S}) \\ =& m_{\mathrm{SL}_2}(G) & =& \ m_{\mathrm{SL}_2}(\tilde{G}). \end{aligned} \tag{14}$$

Let p be a prime as in the statement of the lemma, let p^α be the exact power of p dividing m_S and let us write $m_S = p^\alpha m'_S$, where $p \nmid m'_S$ and $m_{\tilde{S}} \mid m'_S$. By definition of $m_{\tilde{S}}$, under the isomorphism of the Chinese Remainder Theorem, we have

$$S(m_S) \subseteq \tilde{S}(m_S) \simeq \tilde{S}(m'_S) \times \mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}).$$

In light of Lemma 2.3, there are three possibilities for the index two subgroup $S(m) \subseteq \tilde{S}(m_S)$:

$$\begin{aligned} &S(m_S) = S(m'_S) \times \mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) && [\tilde{S}(m'_S) : S(m'_S)] = 2 \\ &S(m_S) = \tilde{S}(m'_S) \times S(p^\alpha) && [\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) : S(p^\alpha)] = 2 \\ &S(m_S) = \tilde{S}(m'_S) \times_\psi \mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) && |\psi_{p^\alpha}(\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}))| = 2. \end{aligned} \tag{15}$$

The first possibility in (15) would imply that m_S divides m'_S, a contradiction. The second possibility would imply the existence of a proper subgroup $S := \pi^{-1}_{\mathrm{SL}_2}(S(p^\alpha)) \subsetneq \mathrm{SL}_2(\hat{\mathbb{Z}})$ satisfying $\tilde{S} = \mathrm{SL}_2(\hat{\mathbb{Z}})$, contradicting Lemma 2.2. We thus conclude that only the third possibility can occur:

$$S(m_S) = \tilde{S}(m'_S) \times_\psi \mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \qquad |\psi_{p^\alpha}(\mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}))| = 2.$$

We now consider the map $\psi_{p^\alpha} : \mathrm{SL}_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \longrightarrow \{\pm 1\}$. Using the well-known fact that the abelianization map $\mathrm{SL}_2(\hat{\mathbb{Z}}) \longrightarrow \mathbb{Z}/12\mathbb{Z}$ factors as

$$\mathrm{SL}_2(\hat{\mathbb{Z}}) \xrightarrow{\mathrm{red}\times\mathrm{red}} \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}) \xrightarrow{\mathrm{ab}\times\mathrm{ab}} \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, \tag{16}$$

it follows that $p = 2$ and $\ker \psi_{p^\alpha} = \pi^{-1}_{\mathrm{SL}_2}(A_3)$, where $A_3 \subseteq S_3 \simeq \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ is the unique subgroup of index 2. Since the SL_2-level of S is $2^\alpha m'_S$ and the map ψ_{2^α} factors through reduction modulo 2, we must then have $\alpha = 1$. To finish the proof, we will show that $m'_S = m_{\tilde{S}}$. Suppose for the sake of contradiction that

$$m'_S > m_{\tilde{S}}. \tag{17}$$

The hypothesis that $m_S = 2m'_S$ implies that $\ker \psi_{m'_S} \subseteq \tilde{S}(m'_S)$ is an index 2 subgroup whose image at any lower level m''_S is all of $\tilde{S}(m''_S)$. In particular, fixing any (necessarily odd) prime p dividing m'_S, we have that $\ker \psi_{m'_S}(m'_S/p) = \tilde{S}(m'_S/p)$, and since $\ker\big(\mathrm{SL}_2(\mathbb{Z}/p^2\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})\big)$ is a p-group and $\ker \psi_{m'_S}(m'_S) \subseteq \tilde{S}(m'_S)$ is an index two subgroup, it follows that

m'_S must be square-free. Thus, by (17) there must be a square-free number m''_S satisfying $m'_S = m_{\tilde{S}} m''_S$ and with

$$\ker \psi_{m'_S} \simeq \tilde{S}(m_{\tilde{S}}) \times_{\phi} \mathrm{SL}_2(\mathbb{Z}/m''_S\mathbb{Z}), \tag{18}$$

where the image of ϕ is a group of order 2. Again by (16), any non-trivial image of $\mathrm{SL}_2(\mathbb{Z}/m''_S\mathbb{Z})$ must have order divisible by 3, and thus the fibered product (18) is a full cartesian product, so that $\ker \psi_{m'_S} = \tilde{S}(m'_S)$, a contradiction. This implies that $m'_S = m_{\tilde{S}}$, proving the lemma. □

We now prove a lemma that handles the "vertical" situation.

Lemma 2.5. *Let $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ be an open subgroup. Suppose that*

$$m_{\mathrm{SL}_2}(\tilde{G}) < m_{\mathrm{SL}_2}(G)$$

and that any prime p dividing $m_{\mathrm{SL}_2}(G)$ also divides $m_{\mathrm{SL}_2}(\tilde{G})$. We then have that $m_{\mathrm{SL}_2}(\tilde{G})$ is even and $m_{\mathrm{SL}_2}(G) = 2m_{\mathrm{SL}_2}(\tilde{G})$.

Proof. As before, we set $S := G \cap \mathrm{SL}_2(\hat{\mathbb{Z}})$, so that $\tilde{S} = \tilde{G} \cap \mathrm{SL}_2(\hat{\mathbb{Z}})$, and also define m_S and $m_{\tilde{S}}$ by (14). Since $[\tilde{S} : S] = 2$ and by definitions of m_S and $m_{\tilde{S}}$, for any divisor d of m_S, we have

$$m_{\tilde{S}} \mid d \mid m_S \text{ and } d < m_S \implies S(d) = \tilde{S}(d). \tag{19}$$

Let p be any prime for which

$$m_{\tilde{S}} \text{ divides } \frac{m_S}{p}. \tag{20}$$

Since the kernel

$$\ker\left(\mathrm{SL}_2(\mathbb{Z}/m_S\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/(m_S/p)\mathbb{Z})\right)$$

is an abelian p-group, it follows from (19) that any p satisfying (20) must be even, and thus $m_S = 2^{\alpha} m_{\tilde{S}}$ for some $\alpha \geq 1$. We now show that $\alpha = 1$. Note that each matrix X in the set

$$\mathcal{K} := \left\{ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} \right\} \subseteq M_{2\times 2}(\mathbb{Z})$$

satisfies $X^2 = 0$, and also (recall that $2 \mid m_{\tilde{S}}$) that

$$\ker\left(\mathrm{SL}_2(\mathbb{Z}/2^n m_{\tilde{S}}\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/2^{n-1} m_{\tilde{S}}\mathbb{Z})\right) = \left\langle \{ I + 2^{n-1} m_{\tilde{S}} X \mod 2^n m_{\tilde{S}} : X \in \mathcal{K} \} \right\rangle \qquad (n \geq 1). \tag{21}$$

If $\alpha > 1$ then, by (19), $\ker\left(\mathrm{SL}_2(\mathbb{Z}/2m_{\tilde{S}}\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/m_{\tilde{S}}\mathbb{Z})\right) \subseteq S(2m_{\tilde{S}})$. Fixing any $X \in \mathcal{K}$, we then have

$$I + m_{\tilde{S}} X \mod 2m_{\tilde{S}} \in S(2m_{\tilde{S}}).$$

Replacing X by an appropriate lift in $M_{2\times 2}(\mathbb{Z}_2)$ of $X \mod 2$ (which must still satisfy $X^2 \equiv 0 \mod 2$), we may assume that $I + m_{\tilde{S}} X \mod 4m_{\tilde{S}} \in S(4m_{\tilde{S}})$, and so then

$$(I + m_{\tilde{S}} X)^2 = I + 2m_{\tilde{S}} X + m_{\tilde{S}}^2 X^2 \equiv I + 2m_{\tilde{S}} X \mod 4m_{\tilde{S}} \in S(4m_{\tilde{S}}),$$

and by (21), we see that $\ker(\mathrm{SL}_2(\mathbb{Z}/4m_{\tilde{S}}\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/2m_{\tilde{S}}\mathbb{Z})) \subseteq S(4m_{\tilde{S}})$. Continuing inductively, we would then conclude that

$$S(2^\alpha m_{\tilde{S}}) = \pi_{\mathrm{SL}_2}^{-1}(S(m_{\tilde{S}})) = \tilde{S}(2^\alpha m_{\tilde{S}}),$$

a contradiction. Thus, we must have $S(2m_{\tilde{S}}) \subsetneq \tilde{S}(2m_{\tilde{S}})$, and so $m_S = 2m_{\tilde{S}}$, as asserted. □

Proof of Lemma 2.1. Lemma 2.1 follows immediately from Lemmas 2.4 and 2.5. □

Applying Lemma 2.1 to (12), we obtain the following corollary.

Corollary 2.6. *Let $G \in \mathcal{G}(0)$. We then have*

$$m_{\mathrm{SL}_2}(G) \in \begin{Bmatrix} 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,18,20,21,22,24, \\ 25,26,27,28,30,32,36,40,42,48,50,52,54,56,60,64,72,96 \end{Bmatrix}.$$

The proof of Proposition 1.12 involves a group theoretical analysis together with a MAGMA computation. We now develop the group theory part.

2.1. Lemmas on fibered products. Let G_1 and G_2 be groups, let

$$\phi_i : G_i \longrightarrow \Gamma_\phi$$
$$\psi_i : G_i \longrightarrow \Gamma_\psi$$

be surjective group homomorphisms and let

$$G_1 \times_\phi G_2 := \{(g_1, g_2) \in G_1 \times G_2 : \ \phi_1(g_1) = \phi_2(g_2)\},$$
$$G_1 \times_\psi G_2 := \{(g_1, g_2) \in G_1 \times G_2 : \ \psi_1(g_1) = \psi_2(g_2)\}$$

be the associated fibered products. We call Γ_ϕ the *common quotient* associated to $G_1 \times_\phi G_2$, and likewise with Γ_ψ.

Lemma 2.7. *In the above setting, we have*

$$G_1 \times_\phi G_2 = G_1 \times_\psi G_2 \iff \ker\psi_1 \times \ker\psi_2 \subseteq G_1 \times_\phi G_2 \subseteq G_1 \times_\psi G_2. \tag{22}$$

Proof. Since "⇒" is trivial, we prove the "⇐" direction. The condition

$$\ker\psi_1 \times \ker\psi_2 \subseteq G_1 \times_\phi G_2$$

implies that $\ker\psi_i \subseteq \ker\phi_i$ for each $i \in \{1,2\}$. On the other hand, the containment $G_1 \times_\phi G_2 \subseteq G_1 \times_\psi G_2$ implies that $\ker\phi_1 \times \ker\phi_2 \subseteq G_1 \times_\psi G_2$, which forces $\ker\phi_i \subseteq \ker\psi_i$ for each i. Thus we have

$$\ker\phi_i = \ker\psi_i \qquad (i \in \{1,2\}).$$

It follows that there are isomorphisms $\eta_i : \Gamma_\phi \to \Gamma_\psi$ such that, for each $i \in \{1,2\}$, we have $\psi_i = \eta_i\phi_i$. Now, if there exists $\gamma \in \Gamma_\phi$ with $\eta_1(\gamma) \neq \eta_2(\gamma)$, then, by choosing $g_i \in G_i$ with $\phi_i(g_i) = \gamma$, we find that $(g_1, g_2) \in G_1 \times_\phi G_2$ but $(g_1, g_2) \notin G_1 \times_\psi G_2$, a contradiction. Thus, $\eta_1 = \eta_2 =: \eta$, and it follows that

$$G_1 \times_\phi G_2 = G_1 \times_{(\eta\phi_1, \eta\phi_2)} G_2 = G_1 \times_\psi G_2,$$

as asserted, establishing the "⇐" direction and proving the lemma. □

The following lemma is key throughout. Let G_1 and G_2 be groups, together with surjective group homomorphisms

$$\psi_i : G_i \longrightarrow \Gamma$$

onto a common group Γ, and let $G_1 \times_\psi G_2$ be the corresponding fibered product. For $i \in \{1,2\}$, let $\pi_i : G_i \twoheadrightarrow \overline{G}_i$ be a surjective group homomorphisms (which we will denote by $g_i \mapsto \overline{g}_i$) and consider the induced surjection

$$\pi : G_1 \times G_2 \longrightarrow \overline{G}_1 \times \overline{G}_2, \quad (g_1, g_2) \mapsto (\overline{g}_1, \overline{g}_2)$$

(in other words, $\pi := \pi_1 \times \pi_2$). The following lemma describes explicitly the image of $G_1 \times_\psi G_2$ under π. Define the quotient group $\overline{\Gamma}$ by

$$\overline{\Gamma} := \frac{\Gamma}{\psi_1(\ker \pi_1)\psi_2(\ker \pi_2)},$$

let $\varpi : \Gamma \longrightarrow \overline{\Gamma}$ be the canonical surjection and let $\overline{\psi}_i := \varpi \circ \psi_i$. Note that $\overline{\psi}_i$ induces a well defined surjective homomorphism $\overline{G}_i \longrightarrow \overline{\Gamma}$ (via $\overline{g}_i \mapsto \overline{\psi}_i(g_i)$), which we will continue to denote by $\overline{\psi}_i$. Note the functional equation

$$\varpi \circ \psi_i = \overline{\psi}_i \circ \pi_i. \tag{23}$$

We let $\overline{\psi}$ denote the pair $(\overline{\psi}_1, \overline{\psi}_2)$ and $\overline{G}_1 \times_{\overline{\psi}} \overline{G}_2$ the corresponding fibered product group.

Lemma 2.8. *Let G_1 and G_2 be groups and consider the fibered product $G_1 \times_\psi G_2$ as described above. Then, with the notation just outlined, we have*

$$\pi(G_1 \times_\psi G_2) = \overline{G}_1 \times_{\overline{\psi}} \overline{G}_2.$$

Proof. The containment "$\subseteq$" is immediate, since $\psi_1(g_1) = \psi_2(g_2)$ implies that $\varpi(\psi_1(g_1)) = \varpi(\psi_2(g_2))$, and so $\overline{\psi}_1(\overline{g}_1) = \overline{\psi}_2(\overline{g}_2)$. Furthermore, it follows from the surjectivity of each π_i that $\pi(G_1 \times_\psi G_2) \subseteq \overline{G}_1 \times \overline{G}_2$ is a subgroup that projects onto $\overline{G}_1$ and onto $\overline{G}_2$ via the canonical projections. Thus, by Lemma 2.3, $\pi(G_1 \times_\psi G_2)$ is equal to $\overline{G}_1 \times_\eta \overline{G}_2$ for some fibering maps (η_1, η_2). Furthermore, we claim that

$$\ker \overline{\psi}_1 \times \ker \overline{\psi}_2 \subseteq \overline{G}_1 \times_\eta \overline{G}_2. \tag{24}$$

Indeed, it is sufficient to show that

$$\ker \overline{\psi}_1 \times \{1\} \subseteq \overline{G}_1 \times_\eta \overline{G}_2,$$
$$\{1\} \times \ker \overline{\psi}_2 \subseteq \overline{G}_1 \times_\eta \overline{G}_2.$$

Let $\overline{x}_1 \in \ker \overline{\psi}_1$ and let $x_1 \in G_1$ be any lift under π_1 of $\overline{x}_1$. By definition of $\overline{\psi}_1$, we may adjust $x_1 \in \pi_1^{-1}(\overline{x}_1)$ so that $\psi_1(x_1) \in \psi_2(\ker \pi_2)$, and thus there exists $k_2 \in \ker \pi_2$ for which $(x_1, k_2) \in G_1 \times_\psi G_2$. Applying π, it follows that $(\overline{x}_1, 1) \in \overline{G}_1 \times_\eta \overline{G}_2$, and so $\ker \overline{\psi}_1 \times \{1\} \subseteq \overline{G}_1 \times_\eta \overline{G}_2$; the argument that $\{1\} \times \ker \overline{\psi}_2 \subseteq \overline{G}_1 \times_\eta \overline{G}_2$ is similar. The containment (24) follows.

Having established that

$$\ker \overline{\psi}_1 \times \ker \overline{\psi}_2 \subseteq \overline{G}_1 \times_\eta \overline{G}_2 \subseteq \overline{G}_1 \times_{\overline{\psi}} \overline{G}_2,$$

Lemma 2.7 now finishes the proof. □

Our final lemma has to do with intersecting fibered products with full cartesian products, and will later be applied to the situation of intersecting with SL_2. Let $G_1 \times_\psi G_2$ be a fibered product and let $S_i \subseteq G_i$ be subgroups. It is clear that

$$\big(G_1 \times_\psi G_2\big) \cap (S_1 \times S_2) = S_1 \times_\psi S_2,$$

but the canonical projection maps in the right-hand expression may not be surjective, which can cause confusion. To remedy this, let us say that Γ is the common quotient group associated to the fibered product $G_1 \times_\psi G_2$ and put

$$\Gamma_S := \psi_1(S_1) \cap \psi_2(S_2).$$

Lemma 2.9. *Let $G_1 \times_\psi G_2$ be a fibered product and let $S_i \subseteq G_i$ be subgroups. Then*

$$\big(G_1 \times_\psi G_2\big) \cap (S_1 \times S_2) = \psi_1|_{S_1}^{-1}(\Gamma_S) \times_\psi \psi_2|_{S_2}^{-1}(\Gamma_S),$$

and the canonical projection maps in the right-hand expression are surjective. Moreover,

$$\psi_1\left(\psi_1|_{S_1}^{-1}(\Gamma_S)\right) = \Gamma_S = \psi_2\left(\psi_2|_{S_2}^{-1}(\Gamma_S)\right).$$

2.2. Pre-twist groups and how we search for them. We will now define the notion of a pre-twist group, as a means to aid in the search for $G \in \mathcal{G}$ which satisfy $m_{\mathrm{SL}_2}(G) < m_{\mathrm{GL}_2}(G)$. Our goal to prove Proposition 1.12 may be stated more broadly as follows.

Goal 2.10. *To find all (maximal) non-abelian entanglement groups of genus* 0 *(or, more generally, of fixed genus $g \geq 0$).*

For any given non-abelian entanglement group G, either $m_{\mathrm{GL}_2}(G)$ is equal to $m_{\mathrm{SL}_2}(G)$ or not. If $m_{\mathrm{GL}_2}(G) = m_{\mathrm{SL}_2}(G)$, then G will be found when we search through all groups with GL_2-level appearing in the list from Corollary 2.6. If $m_{\mathrm{GL}_2}(G) \neq m_{\mathrm{SL}_2}(G)$, then we will view G as being a *twist cover* of some group $\overline{G}$ whose GL_2-level appears in that list.

Definition 2.11. A subgroup $\overline{G} \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is called a **pre-twist group** if there exists a non-abelian entanglement group $G \subsetneq \overline{G}$ such that

$$\begin{aligned} m_{\mathrm{SL}_2}(G) = m_{\mathrm{GL}_2}(\overline{G}) =: \overline{m}, \\ m_{\mathrm{GL}_2}(G) =: m > \overline{m}, \quad \text{and} \\ G(\overline{m}) = \overline{G}(\overline{m}). \end{aligned} \tag{25}$$

If $\overline{G}$ is a pre-twist group, then a **twist cover of** $\overline{G}$ refers to any non-abelian entanglement group $G \subsetneq \overline{G}$ satisfying (25) .

If G is a non-abelian entanglement group with $m_{\mathrm{GL}_2}(G) > m_{\mathrm{SL}_2}(G) =: \overline{m}$, then we define

$$\overline{G} := \pi_{\mathrm{GL}_2}^{-1}(G(\overline{m})) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}}).$$

Clearly $\overline{G}$ is a pre-twist group and G is a twist cover of $\overline{G}$. Thus, to find all non-abelian entanglement groups whose GL_2-level and SL_2-level are different, it suffices to first find all pre-twist groups $\overline{G}$ and then describe the process of constructing twist covers G of $\overline{G}$.

Our next lemma will aid in the proof of Proposition 2.14 below, which in turn implies a somewhat restrictive necessary condition on pre-twist groups that allows us to deduce Proposition 1.12. First we observe two elementary lemmas about twist covers. The set-up is as follows: $\overline{G}$ will be a pre-twist group of GL_2-level $\overline{m}$ and $G \subsetneq \overline{G}$ will be a twist cover of $\overline{G}$ with GL_2-level $m > \overline{m}$. Suppose that $m = m_1 m_2$ with $\gcd(m_1, m_2) = 1$, that $\overline{m}_i := \gcd(\overline{m}, m_i)$ and that

$$G(m) = G(m_1) \times_{\psi} G(m_2),$$
$$G(\overline{m}) = G(\overline{m}_1) \times_{\overline{\psi}} G(\overline{m}_2),$$

where the fibering maps $\psi_i : G(m_i) \twoheadrightarrow \Gamma$ surject onto a non-abelian group Γ and $\overline{\psi}_i : G(\overline{m}_i) \twoheadrightarrow \overline{\Gamma}$ surject onto the corresponding quotient $\overline{\Gamma}$ of Γ as described above in Lemma 2.8. Let $\varpi : \Gamma \twoheadrightarrow \overline{\Gamma}$ denote the canonical surjection. Here and throughout this section, we let $\pi_i : G(m_i) \twoheadrightarrow G(\overline{m}_i)$ denote the reduction modulo $\overline{m}_i$ map restricted to $G(m_i)$ and

$$N^G(m_i) := \ker \psi_i, \quad N^{\overline{G}}(\overline{m}_i) := \ker \overline{\psi}_i. \tag{26}$$

To view things more globally, we define the open subgroups $N^G \subseteq G$ and $N^{\overline{G}} \subseteq \overline{G}$ by

$$N^G := \pi_{\mathrm{GL}_2}^{-1}\left(N^G(m_1) \times N^G(m_2)\right), \quad N^{\overline{G}} := \pi_{\mathrm{GL}_2}^{-1}\left(N^{\overline{G}}(\overline{m}_1) \times N^{\overline{G}}(\overline{m}_2)\right)$$

and the maps

$$\psi : G \longrightarrow \Gamma,$$
$$\overline{\psi} : \overline{G} \longrightarrow \overline{\Gamma}$$

by

$$\psi(g) := \psi_1(g \bmod m_1) = \psi_2(g \bmod m_2),$$
$$\overline{\psi}(g) := \overline{\psi}_1(g \bmod \overline{m}_1) = \overline{\psi}_2(g \bmod \overline{m}_2).$$

Then $N^G = \ker \psi$, $N^{\overline{G}} = \ker \overline{\psi}$, and we have a commuting diagram of exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N^G & \longrightarrow & G & \xrightarrow{\psi} & \Gamma & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \varpi} & & \\ 1 & \longrightarrow & N^{\overline{G}} & \longrightarrow & \overline{G} & \xrightarrow{\overline{\psi}} & \overline{\Gamma} & \longrightarrow & 1 \end{array} \tag{27}$$

in which all unlabeled arrows denote either inclusion maps or trivial surjections. For any positive integer n, we may now consider the subgroups $N^G(n) \subseteq G(n) \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and $N^{\overline{G}}(n) \subseteq \overline{G}(n) \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$; we note that $N^G(n) \subseteq N^{\overline{G}}(n)$ and caution the reader that this containment may be proper, especially when $n = \overline{m}$. Since we are considering the genus of G, we are interested in its intersection with $\mathrm{SL}_2(\hat{\mathbb{Z}})$. Here and throughout the rest of this section, we will employ the following notation: for any open subgroup $H \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, we define

$$H_{\mathrm{SL}_2} := H \cap \mathrm{SL}_2(\hat{\mathbb{Z}}). \tag{28}$$

Note that, for any $n \in \mathbb{N}$,

$$H_{\mathrm{SL}_2}(n) \subseteq H(n) \cap \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}).$$

We caution the reader that this containment may be proper when n isn't a multiple of $m_{\mathrm{GL}_2}(H)$. The analogue of (27) obtained after intersecting with $\mathrm{SL}_2(\hat{\mathbb{Z}})$ is

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N^G_{\mathrm{SL}_2} & \longrightarrow & G_{\mathrm{SL}_2} & \xrightarrow{\psi|_{G_{\mathrm{SL}_2}}} & \Gamma_{\mathrm{SL}_2} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \varpi|_{\Gamma_{\mathrm{SL}_2}}} & & \\ 1 & \longrightarrow & N^{\overline{G}}_{\mathrm{SL}_2} & \longrightarrow & \overline{G}_{\mathrm{SL}_2} & \xrightarrow{\overline{\psi}|_{\overline{G}_{\mathrm{SL}_2}}} & \overline{\Gamma}_{\mathrm{SL}_2} & \longrightarrow & 1, \end{array} \tag{29}$$

where

$$\begin{aligned} \Gamma_{\mathrm{SL}_2} &:= \psi_1\left(G_{\mathrm{SL}_2}(m_1)\right) \cap \psi_2\left(G_{\mathrm{SL}_2}(m_2)\right) \\ \overline{\Gamma}_{\mathrm{SL}_2} &:= \overline{\psi}_1\left(\overline{G}_{\mathrm{SL}_2}(\overline{m}_1)\right) \cap \overline{\psi}_2\left(\overline{G}_{\mathrm{SL}_2}(\overline{m}_2)\right) \end{aligned}$$

are as in Lemma 2.9. (Actually, by the definition (28), we in fact have

$$\Gamma_{\mathrm{SL}_2} := \psi_1\left(G_{\mathrm{SL}_2}(m_1)\right) = \psi_2\left(G_{\mathrm{SL}_2}(m_2)\right)$$

and likewise with $\overline{\Gamma}_{\mathrm{SL}_2}$.) In what follows, our goal is to understand the image of G_{SL_2} inside $\overline{G}_{\mathrm{SL}_2}$, which is equivalent to understanding the image of $G_{\mathrm{SL}_2}(\overline{m})$ inside $\overline{G}_{\mathrm{SL}_2}(\overline{m})$.

Lemma 2.12. *Assume the notation outlined above (in particular, assume that G is a non-abelian entanglement group with SL_2-level dividing $\overline{m}$). We have*

$$\ker \varpi \subseteq Z(\Gamma) \tag{30}$$

(where $Z(\Gamma)$ denotes the center of Γ); in particular, $\psi_i\left(N^{\overline{G}}(m_i)\right) \subseteq Z(\Gamma)$ for each $i \in \{1, 2\}$. Furthermore, we have

$$\begin{aligned} \left[G(\overline{m}_i), N^{\overline{G}}(\overline{m}_i)\right] &\subseteq N^G_{\mathrm{SL}_2}(\overline{m}_i), \\ \left[G(\overline{m}_i), G(\overline{m}_i)\right] &\nsubseteq N^G_{\mathrm{SL}_2}(\overline{m}_i). \end{aligned} \tag{31}$$

Proof. Since $m_{\mathrm{SL}_2}(G)$ divides $\overline{m}$, we have that, for each $i \in \{1,2\}$,

$$\psi_i(\ker \pi_i \cap \mathrm{SL}_2(\mathbb{Z}/m_i\mathbb{Z})) = 1_\Gamma,$$

and so $\psi_i|_{\ker \pi_i}$ factors through the determinant map. It follows that, for each $g \in G(m_i)$ and $k \in \ker \pi_i$, we have

$$\psi_i(gkg^{-1}) = \psi_i(k),$$

and by surjectivity of ψ_i we thus see that $\psi_i(\ker \pi_i)$ is contained in the center of Γ. Since $\ker \varpi = \psi_1(\ker \pi_1)\psi_2(\ker \pi_2)$, this establishes (30), and it follows from $\varpi \circ \psi_i = \overline{\psi}_i \circ \pi_i$ that $\psi_i\left(N^{\overline{G}}(m_i)\right) \subseteq Z(\Gamma)$. The first containment in (31) follows from this by further considering the isomorphism $G(m_i)/N^G(m_i) \simeq \Gamma$ and then projecting modulo $\overline{m}_i$. To see why $[G(\overline{m}_i), G(\overline{m}_i)] \not\subseteq N^G_{\mathrm{SL}_2}(\overline{m}_i)$, suppose not, i.e., suppose that $[G(\overline{m}_i), G(\overline{m}_i)] \subseteq N^G_{\mathrm{SL}_2}(\overline{m}_i)$. Since $N^G_{\mathrm{SL}_2}(m_i) = \pi^{-1}_{\mathrm{SL}_2}(N^G_{\mathrm{SL}_2}(\overline{m}_i))$, we then see that

$$[G(m_i), G(m_i)] \subseteq \pi^{-1}_{\mathrm{SL}_2}([G(\overline{m}_i), G(\overline{m}_i)]) \subseteq N^G_{\mathrm{SL}_2}(m_i) \subseteq N^G(m_i),$$

contradicting the fact that $\Gamma \simeq G(m_i)/N^G(m_i)$ is non-abelian. This establishes that $[G(\overline{m}_i), G(\overline{m}_i)] \not\subseteq N^G_{\mathrm{SL}_2}(\overline{m}_i)$, finishing the proof. □

Corollary 2.13. *Let $\overline{G}$ be a pre-twist group, let $G \in \mathcal{G}_{\mathrm{non-ab}}$ be a twist cover of $\overline{G}$ and let m, $\overline{m}$ be as in* (25)*. Suppose that $m = m_1 m_2$ is a permissible factorization for which $G(m) \simeq G(m_1) \times_\psi G(m_2)$ has a non-abelian common quotient Γ. Then, defining $\overline{m}_i := \gcd(\overline{m}, m_i)$ for $i \in \{1,2\}$, the common quotient $\overline{\Gamma}$ associated to $\overline{G}(\overline{m}) \simeq \overline{G}(\overline{m}_1) \times_{\overline{\psi}} \overline{G}(\overline{m}_2)$ satisfies $\overline{\Gamma} \neq \{1\}$. Consequently we have*

$$G \in \mathcal{G}_{\mathrm{non-ab}}(0) \;\Rightarrow\; m_{\mathrm{SL}_2}(G) \in \left\{ \begin{matrix} 6, 10, 12, 14, 15, 18, 20, 21, 22, \\ 24, 26, 28, 30, 36, 40, 42, 48, \\ 50, 52, 54, 56, 60, 64, 72, 96 \end{matrix} \right\}. \tag{32}$$

If we further assume that $G \in \mathcal{G}^{\max}_{\mathrm{non-ab}}$, then $\overline{\Gamma}$ is abelian.

Proof. By Lemma 2.8 and (30), we have that

$$\ker \varpi \subseteq Z(\Gamma) \neq \Gamma,$$

since Γ is non-abelian. This establishes that $\overline{\Gamma} \neq \{1\}$. It follows that the factorization $\overline{m} = \overline{m}_1 \overline{m}_2$ must be permissible, and therefore $m_{\mathrm{SL}_2}(G) = \overline{m}$ must belong to the subset of those levels listed in Corollary 2.6 which admit permissible factorizations, leading to (32). Finally, if $\overline{\Gamma}$ were non-abelian, then $\overline{G} \in \mathcal{G}_{\mathrm{non-ab}}$ and $G \subsetneq \overline{G}$, contradicting the hypothesis that $G \in \mathcal{G}^{\max}_{\mathrm{non-ab}}$. □

Proposition 2.14. *Let $\overline{G}$ be a pre-twist group, let G be a twist cover of $\overline{G}$, and assume the notation set above. Then there exists a pair of surjective group homomorphisms $\tilde{\psi}_i : G(\overline{m}_i) \twoheadrightarrow \tilde{\Gamma}_i$ onto non-abelian groups $\tilde{\Gamma}_i$ with the following properties:*

(1) *There exist surjective group homomorphisms* $\tilde{\varpi}_i : \tilde{\Gamma}_i \twoheadrightarrow \overline{\Gamma}$ *with*

$$\overline{\psi}_i = \tilde{\varpi}_i \circ \tilde{\psi}_i \text{ and } \ker \tilde{\varpi}_i \subseteq Z(\tilde{\Gamma}_i). \tag{33}$$

(2) *Defining* Γ_{SL_2} *to be the common value of* $\psi_i\left(G_{\mathrm{SL}_2}(m_i)\right)$*, and* $\tilde{\Gamma}_{i,\mathrm{SL}_2} := \tilde{\psi}_i\left(G_{\mathrm{SL}_2}(\overline{m}_i)\right)$*, there are isomorphisms* $\theta_i : \Gamma_{\mathrm{SL}_2} \to \tilde{\Gamma}_{i,\mathrm{SL}_2}$ *satisfying* $\tilde{\varpi}_i|_{\tilde{\Gamma}_{i,\mathrm{SL}_2}} \circ \theta_i = \varpi|_{\Gamma_{\mathrm{SL}_2}}$ *and*

$$\theta_i \circ \psi_i|_{G_{\mathrm{SL}_2}(m_i)} = \tilde{\psi}_i|_{G_{\mathrm{SL}_2}(\overline{m}_i)} \circ \pi_i|_{G_{\mathrm{SL}_2}(m_i)}.$$

Finally, under the isomorphism $G(m) \simeq G(m_1) \times_{\psi} G(m_2)$ *we have that*

$$G_{\mathrm{SL}_2}(m) \simeq \pi_{\mathrm{SL}_2}^{-1}\left(\tilde{\psi}_1|^{-1}_{G_{\mathrm{SL}_2}(\overline{m}_1)}(\theta_1(\Gamma_{\mathrm{SL}_2})) \times_{\theta^{-1}\circ\tilde{\psi}} \tilde{\psi}_2|^{-1}_{G_{\mathrm{SL}_2}(\overline{m}_2)}(\theta_2(\Gamma_{\mathrm{SL}_2}))\right). \tag{34}$$

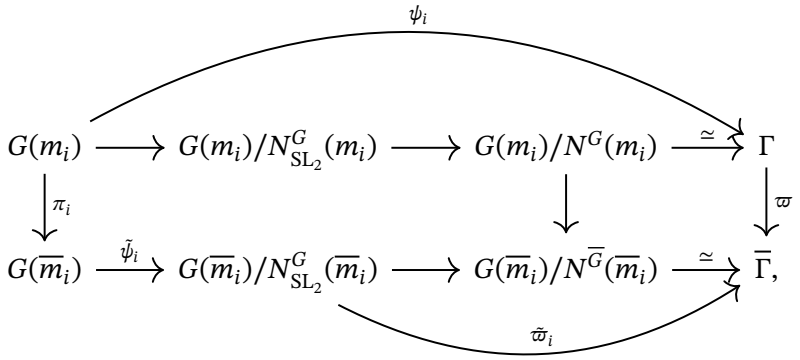
Proof. We define

$$\tilde{\Gamma}_i := G(\overline{m}_i)/N^G_{\mathrm{SL}_2}(\overline{m}_i)$$

and let $\tilde{\psi}_i : G(\overline{m}_i) \twoheadrightarrow \tilde{\Gamma}_i$ be the canonical surjection. By Lemma 2.12, $\tilde{\Gamma}_i$ is non-abelian. By the definition (26), we see that $N^G_{\mathrm{SL}_2}(\overline{m}_i) \subseteq N^{\overline{G}}(\overline{m}_i)$, so there is a natural map

$$\tilde{\varpi}_i : \tilde{\Gamma}_i := G(\overline{m}_i)/N^G_{\mathrm{SL}_2}(\overline{m}_i) \longrightarrow G(\overline{m}_i)/N^{\overline{G}}(\overline{m}_i) \simeq \overline{\Gamma}.$$

We note the commuting diagram



which implies that $\varpi \circ \psi_i = \tilde{\varpi}_i \circ \tilde{\psi}_i \circ \pi_i$. Using this together with (23), the functional equation (33) is then established. Furthermore, it follows from the first containment in (31) that $\ker \tilde{\varpi}_i \subseteq Z(\tilde{\Gamma}_i)$.

We now construct the maps θ_i. We have

$$\Gamma_{\mathrm{SL}_2} := \psi_i(G_{\mathrm{SL}_2}(m_i)) \simeq G_{\mathrm{SL}_2}(m_i)/N^G_{\mathrm{SL}_2}(m_i),$$

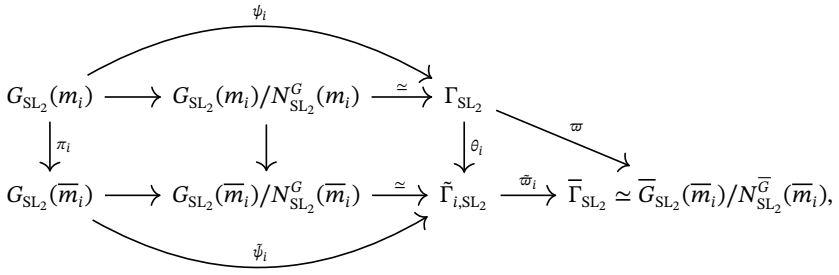
and since $m_{\mathrm{SL}_2}(G) = \overline{m}$ and by definition of $N^G_{\mathrm{SL}_2}$, we have

$$\begin{aligned} G_{\mathrm{SL}_2}(m_i) &= \pi_{\mathrm{SL}_2}^{-1}\left(G_{\mathrm{SL}_2}(\overline{m}_i)\right) \\ N^G_{\mathrm{SL}_2}(m_i) &= \pi_{\mathrm{SL}_2}^{-1}\left(N^G_{\mathrm{SL}_2}(\overline{m}_i)\right). \end{aligned}$$

Thus, we see that the reduction modulo $\overline{m}_i$ map induces an isomorphism that defines θ_i:

$$\theta_i : \Gamma_{\mathrm{SL}_2} \simeq \frac{G_{\mathrm{SL}_2}(m_i)}{N^G_{\mathrm{SL}_2}(m_i)} \to \frac{G_{\mathrm{SL}_2}(\overline{m}_i)}{N^G_{\mathrm{SL}_2}(\overline{m}_i)} \simeq \tilde{\psi}_i\left(G_{\mathrm{SL}_2}(\overline{m}_i)\right) = \tilde{\Gamma}_{i,\mathrm{SL}_2}.$$

Furthermore, the commuting diagram



illustrates that $\tilde{\varpi}_i|_{\tilde{\Gamma}_{i,\mathrm{SL}_2}} \circ \theta_i = \varpi|_{\Gamma_{\mathrm{SL}_2}}$ and

$$\theta_i \circ \psi_i|_{G_{\mathrm{SL}_2}(m_i)} = \tilde{\psi}_i|_{G_{\mathrm{SL}_2}(\overline{m}_i)} \circ \pi_i|_{G_{\mathrm{SL}_2}(m_i)}. \tag{35}$$

Finally, Lemma 2.9, together with (35) and $G_{\mathrm{SL}_2}(m) = \pi^{-1}_{\mathrm{SL}_2}\left(G_{\mathrm{SL}_2}(\overline{m})\right)$, imply that

$$\begin{aligned} G_{\mathrm{SL}_2}(m) &\simeq \psi_1|^{-1}_{G_{\mathrm{SL}_2}(m_1)}\left(\Gamma_{\mathrm{SL}_2}\right) \times_\psi \psi_2|^{-1}_{G_{\mathrm{SL}_2}(m_2)}\left(\Gamma_{\mathrm{SL}_2}\right) \\ &= \pi_1|^{-1}_{G_{\mathrm{SL}_2}(m_1)} \tilde{\psi}_1|^{-1}_{G_{\mathrm{SL}_2}(\overline{m}_1)} \theta_1\left(\Gamma_{\mathrm{SL}_2}\right) \times_{\theta^{-1}\tilde{\psi}\pi} \pi_2|^{-1}_{G_{\mathrm{SL}_2}(m_2)} \tilde{\psi}_2|^{-1}_{G_{\mathrm{SL}_2}(\overline{m}_2)} \theta_2\left(\Gamma_{\mathrm{SL}_2}\right) \\ &= \pi^{-1}_{\mathrm{SL}_2}\left(\tilde{\psi}_1|^{-1}_{G_{\mathrm{SL}_2}(\overline{m}_1)}(\theta_1(\Gamma_{\mathrm{SL}_2})) \times_{\theta^{-1}\tilde{\psi}} \tilde{\psi}_2|^{-1}_{G_{\mathrm{SL}_2}(\overline{m}_2)}(\theta_2(\Gamma_{\mathrm{SL}_2}))\right). \end{aligned}$$

□

The main point of Proposition 2.14 is that the right-hand side of (34) involves information just from level $\overline{m}$, with the only exceptions being the two subgroups $\tilde{H}_i := G_{\mathrm{SL}_2}(\overline{m}_i) \subseteq \overline{G}_{\mathrm{SL}_2}(\overline{m}_i)$, which satisfy the condition

$$\tilde{\psi}_1\left(\tilde{H}_1\right) \simeq \tilde{\psi}_2\left(\tilde{H}_2\right). \tag{36}$$

In our search for pre-twist groups, we can thus take $\tilde{H}_i \subseteq \overline{G}_{\mathrm{SL}_2}(\overline{m}_i)$ to be arbitrary subgroups that happen to satisfy (36). Thus, we have derived necessary conditions for $\overline{G}$ to be a pre-twist group, which can be checked from $\overline{G}$ alone (at level $\overline{m}$). We emphasize this point in the following corollary, which is then used to prove Proposition 1.12.

Corollary 2.15. *Let $\overline{G}$ be a pre-twist group, let G be a twist cover of $\overline{G}$ and let*

$$m := m_{\mathrm{GL}_2}(G), \quad \overline{m} := m_{\mathrm{GL}_2}(\overline{G}).$$

Suppose that $m = m_1 m_2$ is a permissible factorization for which the group $G(m) \simeq G(m_1) \times_\psi G(m_2)$ has a non-abelian common quotient Γ. For each $i \in \{1, 2\}$, define $\overline{m}_i := \gcd(\overline{m}, m_i)$, write $\overline{G}(\overline{m}) \simeq \overline{G}(\overline{m}_1) \times_{\overline{\psi}} \overline{G}(\overline{m}_2)$ and set

$N^{\overline{G}}(\overline{m}_i) = \ker \overline{\psi}_i$. *Then there exist subgroups* $\tilde{N}_i \subseteq N^{\overline{G}}(\overline{m}_i) \cap \mathrm{SL}_2(\mathbb{Z}/\overline{m}_i\mathbb{Z})$ *(with* $\tilde{N}_i \neq N^{\overline{G}}(\overline{m}_i) \cap \mathrm{SL}_2(\mathbb{Z}/\overline{m}_i\mathbb{Z})$ *in case* $G \in \mathcal{G}^{\max}_{\mathrm{non-ab}}$*), with each* $\tilde{N}_i$ *normal in* $\overline{G}(\overline{m}_i)$*, satisfying*

$$[\overline{G}(\overline{m}_i), N^{\overline{G}}(\overline{m}_i)] \subseteq \tilde{N}_i \not\supseteq [\overline{G}(\overline{m}_i), \overline{G}(\overline{m}_i)]. \tag{37}$$

Furthermore, setting $\tilde{\psi}_i : \overline{G}(\overline{m}_i) \to \overline{G}(\overline{m}_i)/\tilde{N}_i$*, there exist subgroups* $\tilde{H}_i \subseteq \overline{G}_{\mathrm{SL}_2}(\overline{m}_i)$ *and isomorphisms* $\theta_i : B \to \tilde{\psi}_i(\tilde{H}_i)$ *(for some group* B*) satisfying*

$$\forall b \in B, \quad \tilde{\varpi}_1(\theta_1(b)) = \tilde{\varpi}_2(\theta_2(b)) \tag{38}$$

and such that, if

$$S := \tilde{\psi}_1|^{-1}_{\tilde{H}_1}(\theta_1(B)) \times_{\theta^{-1}\circ\tilde{\psi}} \tilde{\psi}_2|^{-1}_{\tilde{H}_2}(\theta_2(B)),$$

then the modular curve $X_{\tilde{G}}$ *is isomorphic over* $\overline{\mathbb{Q}}$ *to the modular curve* $X_{\tilde{S}}$*. In particular, there are embeddings* $\theta_i : B \hookrightarrow \tilde{\psi}_i\left(\overline{G}_{\mathrm{SL}_2}(\overline{m}_i)\right)$ *satisfying* (38) *and such that, if*

$$S' := \tilde{\psi}_1|^{-1}_{\overline{G}_{\mathrm{SL}_2}(\overline{m}_1)}(\theta_1(B)) \times_{\theta^{-1}\circ\tilde{\psi}} \tilde{\psi}_2|^{-1}_{\overline{G}_{\mathrm{SL}_2}(\overline{m}_1)}(\theta_2(B)), \tag{39}$$

then $X_{\tilde{G}}$ *is a geometric cover of* $X_{\tilde{S}'}$*, which in turn is a geometric cover of* $X_{\tilde{\overline{G}}}$*.*

Proof. This is essentially a direct translation of Proposition 2.14, taking

$$\tilde{N}_i = N^G_{\mathrm{SL}_2}(\overline{m}_i),\ B = \Gamma_{\mathrm{SL}_2},\ \text{ and }\ \tilde{H}_i = G_{\mathrm{SL}_2}(\overline{m}_i).$$

It is straightforward to verify that $\tilde{N}_i \trianglelefteq \overline{G}(\overline{m}_i)$ and that $\tilde{N}_i$ is contained in $N^{\overline{G}}(\overline{m}_i) \cap \mathrm{SL}_2(\mathbb{Z}/\overline{m}_i\mathbb{Z})$. The fact that $[\overline{G}(\overline{m}_i), N^{\overline{G}}(\overline{m}_i)] \subseteq \tilde{N}_i$ and $[\overline{G}(\overline{m}_i), \overline{G}(\overline{m}_i)] \not\subseteq \tilde{N}_i$ can be seen directly from Lemma 2.12. Finally, in case $G \in \mathcal{G}^{\max}_{\mathrm{non-ab}}$, we have

$$[\overline{G}(\overline{m}_i), \overline{G}(\overline{m}_i)] \subseteq N^{\overline{G}}(\overline{m}_i) \cap \mathrm{SL}_2(\mathbb{Z}/\overline{m}_i\mathbb{Z}),$$

which by (37) forces $\tilde{N}_i$ to be a proper subgroup of $N^{\overline{G}}(\overline{m}_i) \cap \mathrm{SL}_2(\mathbb{Z}/\overline{m}_i\mathbb{Z})$.

Regarding the modular curve $X_{\tilde{S}'}$, it is straightforward to see that $S \subseteq S'$, so it follows immediately from $X_{\tilde{G}} \simeq_{\overline{\mathbb{Q}}} X_{\tilde{S}}$ that $X_{\tilde{G}}$ is a geometric cover of $X_{\tilde{S}'}$. Finally, we claim that $S' \subseteq \overline{G}_{\mathrm{SL}_2}(\overline{m})$. Indeed, if $(s_1, s_2) \in S'$, then for each $i \in \{1, 2\}$, we have $\tilde{\psi}_i(s_i) = \theta(b)$ for some (fixed) $b \in B$. Now using (33) together with (38), we find that

$$\overline{\psi}_1(s_1) = \tilde{\varpi}_1\left(\tilde{\psi}_1(s_1)\right) = \tilde{\varpi}_1(\theta_1(b)) = \tilde{\varpi}_2(\theta_2(b)) = \tilde{\varpi}_2\left(\tilde{\psi}_2(s_2)\right) = \overline{\psi}_2(s_2).$$

Thus $(s_1, s_2) \in \overline{G}_{\mathrm{SL}_2}(\overline{m})$, which establishes that $X_{\tilde{S}'}$ is a geometric cover of $X_{\tilde{\overline{G}}}$, finishing the proof. □

Remark 2.16. We included the group $S' \supseteq S$ in the statement of Corollary 2.15 since it simplifies our computer search. Indeed, since $\mathrm{genus}(X_{\tilde{G}})$ is at least $\mathrm{genus}(X_{\tilde{S}'})$, if for a given $\overline{G}$ our search produces no S' as in (39) with $\mathrm{genus}(X_{\tilde{S}'}) = 0$, then it follows that there are no twist covers $G \in \mathcal{G}^{\max}_{\mathrm{non-ab}}$ of $\overline{G}$ with $\mathrm{genus}(X_{\tilde{G}}) = 0$.

2.3. A search algorithm for pre-twist groups with maximal twist covers. We now describe the algorithm used to search for pre-twist groups of genus zero that have maximal twist covers of genus zero.

Step 1. For a fixed level

$$\overline{m} \in \left\{ \begin{matrix} 6, 10, 12, 14, 15, 18, 20, 21, 22, 24, 26, 28, 30, \\ 36, 40, 42, 48, 50, 52, 54, 56, 60, 64, 72, 96 \end{matrix} \right\}, \tag{40}$$

we construct (as a list) the set $\mathcal{G}^{m_{\mathrm{GL}_2}=\overline{m}}(0)$ of open subgroups $\overline{G} \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ of genus zero and GL_2-level $\overline{m}$ (see Corollary 2.13 and Definition 2.11).

Step 2. For each permissible factorization $\overline{m} = \overline{m}_1\overline{m}_2$, we construct the subset $\mathcal{G}_{\mathrm{ab}}^{m_{\mathrm{GL}_2}=\overline{m}}\left(0, (\overline{m}_1, \overline{m}_2)\right)$ of all $\overline{G} \in \mathcal{G}^{m_{\mathrm{GL}_2}=\overline{m}}(0)$ with the property that, under $\overline{G}(\overline{m}) \subseteq \overline{G}(\overline{m}_1) \times \overline{G}(\overline{m}_2)$, the common quotient in the fibered product associated to $\overline{G}(\overline{m})$ via Lemma 2.3 is a non-trivial abelian group (see Corollary 2.13).

Step 3. For each $\overline{G} \in \mathcal{G}_{\mathrm{ab}}^{m_{\mathrm{GL}_2}=\overline{m}}\left(0, (\overline{m}_1, \overline{m}_2)\right)$, denoting by $\overline{\psi} = (\overline{\psi}_1, \overline{\psi}_2)$ the pair of surjective group homomorphisms implicit in the fibered product $\overline{G}(\overline{m}) \simeq \overline{G}(\overline{m}_1) \times_{\overline{\psi}} \overline{G}(\overline{m}_2)$ and by $N^{\overline{G}}(\overline{m}_i) := \ker \overline{\psi}_i \subseteq \overline{G}(\overline{m}_i)$, we search for normal subgroups $\tilde{N}_i \trianglelefteq \overline{G}(\overline{m}_i)$ satisfying $\tilde{N}_i \subsetneq N^{\overline{G}}(\overline{m}_i) \cap \mathrm{SL}_2(\mathbb{Z}/\overline{m}_i\mathbb{Z})$ and the property (37). We create a new list $\mathcal{G}_{\mathrm{ab,\,pot.}}^{m_{\mathrm{GL}_2}=\overline{m}}\left(0, (\overline{m}_1, \overline{m}_2)\right)$ of *potential* pre-twist groups, consisting of the triples $(\overline{G}(\overline{m}), \tilde{N}_1, \tilde{N}_2)$ found by this search. Note that a given group $\overline{G}(\overline{m})$ may belong to more than one triple in this list.

Step 4. For each triple $(\overline{G}(\overline{m}), \tilde{N}_1, \tilde{N}_2) \in \mathcal{G}_{\mathrm{ab,\,pot.}}^{m_{\mathrm{GL}_2}=\overline{m}}\left(0, (\overline{m}_1, \overline{m}_2)\right)$, denoting by $\tilde{\Gamma}_i := \overline{G}(\overline{m}_i)/\tilde{N}_i$ and by $\tilde{\psi}_i : \overline{G}(\overline{m}_i) \twoheadrightarrow \tilde{\Gamma}_i$ the canonical projection, we search for finite groups B together with embeddings $\theta_i : B \hookrightarrow \tilde{\psi}_i\left(\overline{G}_{\mathrm{SL}_2}(\overline{m}_i)\right)$ satisfying (38). For each such pair $(B, \theta = (\theta_1, \theta_2))$, we form the fibered product

$$S' := \tilde{\psi}_1|^{-1}_{\overline{G}_{\mathrm{SL}_2}(\overline{m}_1)}(\theta_1(B)) \times_{\theta^{-1}\tilde{\psi}} \tilde{\psi}_2|^{-1}_{\overline{G}_{\mathrm{SL}_2}(\overline{m}_2)}(\theta_2(B))$$

and form a new *final* list $\mathcal{G}_{\mathrm{ab,\,fin.}}^{m_{\mathrm{GL}_2}=\overline{m}}\left(0, (\overline{m}_1, \overline{m}_2)\right)$ consisting of those quadruples $(\overline{G}(\overline{m}), \tilde{N}_1, \tilde{N}_2, S')$ for which the genus of $X_{\tilde{S}'}$ is zero (see Corollary 2.15 and Remark 2.16).

Remark 2.17. When computing the list of genus zero subgroups $\overline{G}$ of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ in Step 1, we make use of the following memory-saving measures:

(1) For any level $\overline{m}$ that does not appear in the list (12), by Lemma 2.6, any G of genus zero and GL_2-level $\overline{m}$ must satisfy $-I \notin G$ and $m_{\mathrm{GL}_2}(\tilde{G}) = \overline{m}/2$. We therefore first construct the list of subgroups G_0 of GL_2-level $\overline{m}/2$

satisfying $-I \in G_0$ and then, for each such G_0, search for index two subgroups $G \subseteq G_0$ of GL_2-level $\overline{m}$ with $-I \notin G$.

(2) Searching directly among all subgroups of GL_2-level 48 is memory-intensive enough to be prohibitively difficult on most machines. To work around this problem, we instead started with the single unique subgroup $S(48) \subseteq \mathrm{SL}_2(\mathbb{Z}/48\mathbb{Z})$ of SL_2-level 48 and genus zero and constructed all other subgroups $G(48) \subseteq \mathrm{GL}_2(\mathbb{Z}/48\mathbb{Z})$ by initializing $G_0 := S(48)$ and recursively defining $G_{n+1} := \langle g, G_n \rangle$ with g any matrix in $\mathrm{GL}_2(\mathbb{Z}/48\mathbb{Z})$ for which $G_{n+1} \cap \mathrm{SL}_2(\mathbb{Z}/48\mathbb{Z}) = S(48)$. This process generates all subgroups $G(48) \subseteq \mathrm{GL}_2(\mathbb{Z}/48\mathbb{Z})$ of SL_2-level 48 and genus zero.

Proof of Proposition 1.12. The above algorithm was implemented on a computer, using the MAGMA computational algebra system [2] (see Section 1.1). For each level $\overline{m}$ from Step 1 and permissible factorization $\overline{m} = \overline{m}_1\overline{m}_2$, the search concluded that $\mathcal{G}_{\text{ab, fin.}}^{m_{\mathrm{GL}_2}=\overline{m}}\left(0, (\overline{m}_1, \overline{m}_2)\right) = \emptyset$. By Remark 2.16, we conclude that

$$G \in \mathcal{G}_{\text{non-ab}}^{\max}(0) \implies m_{\mathrm{GL}_2}(G) = m_{\mathrm{SL}_2}(G).$$

Finally, the assertion (7) follows from (32), together with a straightforward computer search that we also carried out using MAGMA. This search also yielded the data in Tables 1, 2 and 3 of Section 1. □

Remark 2.18. The key takeaway from Proposition 1.12 is that we have a finite list of GL_2-levels to consider when searching for maximal genus 0 non-abelian entanglement groups G (each necessarily satisfying the condition, $m_{\mathrm{GL}_2}(G) = m_{\mathrm{SL}_2}(G)$, by the proposition). This second search is then what establishes (6) in Theorem 1.8.

3. Explicit models for modular curves

In the previous section, we proved the first part of Theorem 1.8, which is that (up to conjugation) there are exactly four maximal non-abelian entanglement groups, $G \in \{G_6, G_{10}, G_{15}, G_{18}\}$, for which the associated modular curve $X_{\tilde{G}}$ has genus 0. In all four cases the underlying entanglement is S_3, and in all four cases $-I \in G$ so that $\tilde{G} = G$. Three of the curves are defined over $\mathbb{Q}$, while $X_{G_{15}}$ is defined over $\mathbb{Q}(\sqrt{-15})$. In this section, we complete the proof of the theorem by determining explicit equations for the modular curves. More precisely, we determine a rational parameter t on each X_G as well as an explicit formula for $j_G(t)$. Work for one of the curves, X_{G_6}, is omitted, as this curve was previously studied in [5].

Our approach to finding the explicit models is essentially one of "gluing" along the common non-abelian quotient Γ, in the decomposition of $G = G_m$ into the fiber product $G(m) = G(m_1) \times_\psi G(m_2)$. This process is described *in*

general in Section 3.1, which will also serve as a foundation for future work (when $g > 0$). However, for each of the curves being considered here, the specific underlying entanglement group is $\Gamma \cong S_3$. Hence, we prove in Section 3.2 a lemma that explicitly describes the gluing mechanism in that special case. Once the computational framework is fully developed in principle, it is then implemented in each of the three cases using SageMath [26].

Since the groups $G(m_1)$ and $G(m_2)$ play such a crucial role in our analysis, this data is collected below in Table 3. Note that B(3) refers to the Borel group at 3, while $\mathcal{E}_{S_4}(5)$ refers to the unique index 5 subgroup of $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$ containing $\mathcal{N}_s(5)$ (the normalizer of split Cartan). We also include for reference the usual modular curve data vector (d, c_2, c_3, c_∞) in each case, as well as the Cummins-Pauli label for the curve.

m	$G(m_1), G(m_2)$	(d, c_2, c_3, c_∞)	C-P Label
6	$\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$	$(6, 0, 3, 1)$	$6A^0$
10	$\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}), \mathcal{E}_{S_4}(5)$	$(30, 0, 6, 3)$	$10E^0$
15	$\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}), \mathcal{E}_{S_4}(5)$	$(15, 3, 3, 1)$	$15A^0$
18	$\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}), \pi_9^{-1}(\mathrm{B}(3))$	$(24, 0, 3, 4)$	$18C^0$

TABLE 4. Maximal Genus 0 Non-Abelian Entanglement Curves

Remark 3.1. There are several other methods for obtaining an explicit model for $X_{\tilde{G}}$ when G is an arbitrary open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$. For example, one can use Siegel functions as was done in [10] and [25]. (See [22] for an alternative method, or [29] when $X_{\tilde{G}}$ is not hyperelliptic.) The method developed here for entanglement modular curves has the advantage of resulting in a model that explicitly reflects the entanglement structure. Moreover, it places the modular curve atop a natural tower, which then breaks down desingularization and related analysis into smaller steps.

3.1. General Entanglement Curve Yoga. Fix a non-abelian entanglement scenario, i.e., two subgroups, $G(m_i) \subseteq \mathrm{GL}_2(\mathbb{Z}/m_i\mathbb{Z})$, $i \in \{1, 2\}$ (where $(m_1, m_2) = 1$), which surject onto a common non-abelian quotient Γ with kernels $N(m_1)$ and $N(m_2)$. For simplicity, assume that $-I$ is contained in each $N(m_i)$. We say that an elliptic curve E/K has an entanglement of type

$$(G(m_1), N(m_1), G(m_2), N(m_2))$$

if bases for $E[m_1]$ and $E[m_2]$ may be chosen over $\overline{K}$ such that

(1) $\mathrm{Gal}(K(E[m_1])/K) \cong G(m_1)$
(2) $\mathrm{Gal}(K(E[m_2])/K) \cong G(m_2)$ and
(3) $K(E[m_1]) \cap K(E[m_2]) = K(E[m_1])^{N(m_1)} = K(E[m_2])^{N(m_2)}$.

The isomorphisms in (1) and (2) are induced by the isomorphisms of $\mathrm{Aut}(E[m_i])$ with $\mathrm{GL}_2(\mathbb{Z}/m_i\mathbb{Z})$ that are determined by the choice of bases. Then the fixed fields in (3) are defined via those isomorphisms. Whenever the kernels $N(m_1)$ and $N(m_2)$ are uniquely determined by $G(m_1)$, $G(m_2)$ and Γ, we say that E/K has an entanglement of type $(G(m_1), G(m_2), \Gamma)$ and simplify (3) to the following equivalent condition.

(3') $\mathrm{Gal}(K(E[m_1]) \cap K(E[m_2])/K) \cong \Gamma$

In this section, we develop a method for determining explicit equations for a finite set of modular curves whose K-rational points "correspond generically" to elliptic curves E/K that have an entanglement of type $(G(m_1), N(m_1), G(m_2), N(m_2))$, meaning that every such elliptic curve must correspond to a K-rational point on one of the modular curves. More precisely, after an appropriate choice of basis for $E[m_1m_2]$ over $\overline{K}$ we have

$$\mathrm{Gal}(K(E[m_1m_2])/K) \subseteq G(m_1) \times_\psi G(m_2)$$

for some $\psi_i : G(m_i) \twoheadrightarrow \Gamma$ with $\ker \psi_i = N(m_i)$ if and only if $j(E)$ lifts to a K-rational point on one of the modular curves.

The first step is to find an explicit model for the "full product" curve, the modular curve $X := X_{G(m_1),G(m_2)}$ whose K-rational points correspond generically to elliptic curves E/K that satisfy properties (1) and (2) from above. Since $-I$ is contained in both groups, X can be obtained by crossing the modular curves $X_{G(m_1)}$ and $X_{G(m_2)}$ over the j-line. Next, we determine explicit models for the modular curves, $Y_{\Gamma,i}$ $(i = 1, 2)$, which lie over X and whose K-rational points correspond generically to elliptic curves E/K for which $\mathrm{Gal}(K(E[m_i])/K) = N(m_i)$. Then each $Y_{\Gamma,i}$ is a Galois cover of X, whose Galois group, i.e., the Galois group of the corresponding extension of function fields, is isomorphic to Γ. For each choice of isomorphisms, $\sigma_i : \mathrm{Gal}(Y_{\Gamma,i}/X) \to \Gamma$, it makes sense to form the diagonal quotient $\mathcal{X}_{\sigma_1,\sigma_2}$ of the fiber product of $Y_{\Gamma,1}$ and $Y_{\Gamma,2}$ over X.

$$\mathcal{X}_{\sigma_1,\sigma_2} := Y_{\Gamma,1} \times_X Y_{\Gamma,2} / \left\{(\sigma_1^{-1}(g), \sigma_2^{-1}(g)) | g \in \Gamma\right\}$$

Theorem 3.2. *Let P be a K-rational point on $X_{G(m_1),G(m_2)}$, corresponding to an elliptic curve E/K satisfying properties (1) and (2) from above. Then E satisfies condition (3) if and only if P lifts to a K-rational point on some $\mathcal{X}_{\sigma_1,\sigma_2}$.*

Proof. First suppose that E/K satisfies property (3) from above. Then for some Galois extension L/K there are injections, $\alpha_i : L \hookrightarrow K(E[m_i])$ (over K), which identify L with the fixed field of $N(m_i)$. But this fixed field is precisely the specialization of the function field of $Y_{\Gamma,i}$ to P. Thus, α_i induces an L-valued point, $\hat{\alpha}_i : \mathrm{Spec}(L) \to Y_{\Gamma,i}$, which restricts to an isomorphism (over K) on the fiber over P. Identifying $\mathrm{Gal}(L/K)$ with Γ, we define σ_1 and σ_2 as follows. For $\tau \in \mathrm{Gal}(Y_{\Gamma,i}/X)$, we set $\sigma_i(\tau) = \alpha_i^{-1}\tau\alpha_i$. Consider the L-valued point of $\mathcal{X}_{\sigma_1,\sigma_2}$ given by $\hat{P} = (\hat{\alpha}_1, \hat{\alpha}_2)$, which clearly lies over P. For any $g \in \mathrm{Gal}(L/K)$, we have $g(\hat{P}) = (\hat{\alpha}_1\hat{g}, \hat{\alpha}_2\hat{g})$, where $\hat{g}$ is the induced automorphism on $\mathrm{Spec}(L)$ over K.

On the other hand, if we act on $\hat{P}$ geometrically by $(\sigma_1^{-1}(g), \sigma_2^{-1}(g))$, we get

$$(\hat{\alpha}_1 \hat{g} \hat{\alpha}_1^{-1} \hat{\alpha}_1, \hat{\alpha}_2 \hat{g} \hat{\alpha}_2^{-1} \hat{\alpha}_2) = (\hat{\alpha}_1 \hat{g}, \hat{\alpha}_2 \hat{g}) = g(\hat{P}).$$

Thus, $\hat{P}$ is actually fixed by $\mathrm{Gal}(L/K)$ and hence K-rational.

Conversely, suppose P lifts to a K-rational point $\hat{P}$ on some $\mathcal{X}_{\sigma_1,\sigma_2}$. The key observation in this direction is that regardless of the choice of (σ_1, σ_2), no non-trivial diagonal element (g, g) fixes either $Y_{\Gamma,i}$. So the three function fields of $Y_{\Gamma,1}$, $Y_{\Gamma,2}$ and $\mathcal{X}_{\sigma_1,\sigma_2}$ are all linearly disjoint inside the overall extension, and the compositum of any two contains the third.

$$Y_{\Gamma,1} \times_X \mathcal{X}_{\sigma_1,\sigma_2} = Y_{\Gamma,1} \times_X Y_{\Gamma,2} = Y_{\Gamma,2} \times_X \mathcal{X}_{\sigma_1,\sigma_2}$$

Specialization to $\hat{P}$ determines an isomorphism between the fibers of $Y_{\Gamma,1}$ and $Y_{\Gamma,2}$ over P. As noted above, this is equivalent to an isomorphism between the fixed fields of $K(E[m_1])$ and $K(E[m_2])$ by $N(m_1)$ and $N(m_2)$. So Condition (3) holds for E/K. □

While there are clearly $(\mathrm{Aut}\,\Gamma)^2$ choices for (σ_1, σ_2), not all of the corresponding curves (i.e., function fields) of the form $\mathcal{X}_{\sigma_1,\sigma_2}$ are distinct. Moreover, the elements of the Galois group of $Y_{\Gamma,1} \times_X Y_{\Gamma,2}$ over X may restrict to isomorphisms between some of these (distinct) intermediate fields. Therefore, it is not immediately clear from Theorem 3.2 how many distinct *modular curves* exist for each fixed entanglement type. The following theorem answers this question.

Theorem 3.3. *There are* $|\mathrm{Aut}\,\Gamma|$ *distinct curves of the form* $\mathcal{X}_{\sigma_1,\sigma_2}$ *lying over* $X_{G(m_1),G(m_2)}$. *However, each isomorphism class (over* $X_{G(m_1),G(m_2)}$*) is acted on faithfully by* $\mathrm{Inn}\,\Gamma$. *Hence, there are no more than* $[\mathrm{Aut}\,\Gamma : \mathrm{Inn}\,\Gamma]$ *modular curves for each fixed* $(G(m_1), N(m_1), G(m_2), N(m_2))$ *entanglement type.*

Proof. The group, $\mathrm{Aut}\,\Gamma \times \mathrm{Aut}\,\Gamma$ acts transitively on the set of curves, $\mathcal{X}_{\sigma_1,\sigma_2}$, by post-composition on both sides.

$$(\tau_1, \tau_2) : \mathcal{X}_{\sigma_1,\sigma_2} \mapsto \mathcal{X}_{\tau_1\sigma_1,\tau_2\sigma_2}$$

However, the diagonal subgroup acts trivially, since the group of geometric transformations by which the quotient of $Y_{\Gamma,1} \times_X Y_{\Gamma,2}$ is being taken remains the same. In fact, for any $\tau_1, \tau_2 \in \mathrm{Aut}\,\Gamma \times \mathrm{Aut}\,\Gamma$ we have

$$\{(\sigma_1^{-1}(g), \sigma_2^{-1}(g))\} = \{((\tau_1\sigma_1)^{-1}(g), (\tau_2\sigma_2)^{-1}(g))\} \longleftrightarrow \tau_1 = \tau_2.$$

So, the set $\{\mathcal{X}_{\sigma_1,\sigma_2}\}$ actually only contains $|\mathrm{Aut}\,\Gamma|$ distinct curves, i.e, diagonal quotients of $Y_{\Gamma,1} \times_X Y_{\Gamma,2}$.

Now, fix the pair, (σ_1, σ_2), which in turn fixes an isomorphism between $\mathrm{Gal}(Y_{\Gamma,1} \times_X Y_{\Gamma,2}/X)$ and $\Gamma \times \Gamma$. With this perspective, we may view the function field of $\mathcal{X}_{\sigma_1,\sigma_2}$ as the fixed field of the diagonal subgroup, $\{(g, g)\}$. Moreover, any element (g_1, g_2) then defines an isomorphism (via Galois) from this curve onto the one whose function field is fixed by $\{(g_1 g g_1^{-1}, g_2 g g_2^{-1})\}$. It is easy to check that this curve is none other than $\mathcal{X}_{\tau_1\sigma_1,\tau_2\sigma_2}$, where $\tau_1, \tau_2 \in \mathrm{Aut}\,\Gamma$ are given by

$$\tau_1(g) = g_1^{-1} g g_1 \qquad \tau_2(g) = g_2^{-1} g g_2.$$

So, when $\tau_1, \tau_2 \in \operatorname{Inn}\Gamma$, the aforementioned action of $\operatorname{Aut}\Gamma \times \operatorname{Aut}\Gamma$ actually corresponds to an isomorphism between the two curves. Clearly, if we fix τ_2 to be the identity, the resulting action of $\operatorname{Inn}\Gamma$ is faithful, which proves the theorem. □

Remark 3.4. Any specific choice of *maps*, (ψ_1, ψ_2), determines exactly one of the above modular curves. We have specified only the kernels in the entanglement type in order to highlight the distinction and facilitate the counting of the modular curves. In addition, it is often more difficult in practice to nail down the maps than it is to specify the kernels.

3.2. S_3 Entanglement Modular Curves. The above construction can be made completely explicit in the case where $\Gamma = S_3$. Recall that the first step in the process is to determine the function field L for the full product modular curve $X_{G(m_1),G(m_2)}$ by crossing the modular curves $X_{G(m_1)}$ and $X_{G(m_2)}$ over the j-line. Then, the ψ maps on either side of the fiber product, $G(m_1) \times_\psi G(m_2)$, or more precisely their kernels, $N(m_1)$ and $N(m_2)$, will give rise to two S_3 extensions L_1 and L_2 of L. Without loss of generality, we may assume that these extensions are the splitting fields of two irreducible cubic polynomials over L, $x^3 + Ax^2 + Bx + C$ and $x^3 + Dx^2 + Ex + F$, whose roots in $\bar{L}$ are $\{s_1, s_2, s_3\}$ and $\{t_1, t_2, t_3\}$ (respectively). Identifying the Galois group of the compositum L_1L_2 over L with $S_3 \times S_3$, the function field for the entanglement modular curve will then be the subfield fixed by the diagonal subgroup. But this subfield is clearly generated over L by the element $r := s_1t_1 + s_2t_2 + s_3t_3$. Hence, an explicit equation for the S_3 entanglement modular curve, as an extension of $X_{G(m_1),G(m_2)}$, will be given by the minimal polynomial for r over L. The following lemma provides an explicit formula for that minimal polynomial.

Lemma 3.5. *Let $\{s_1, s_2, s_3\}$ and $\{t_1, t_2, t_3\}$ be the roots of the polynomials $x^3 + Ax^2 + Bx + C$ and $x^3 + Dx^2 + Ex + F$, respectively, in the compositum of the two splitting fields. In the same field, set*

$$\delta = (s_1 - s_2)(s_1 - s_3)(s_2 - s_3)(t_1 - t_2)(t_1 - t_3)(t_2 - t_3)$$

and $r = s_1t_1 + s_2t_2 + s_3t_3$. (So, δ^2 is the product of the two cubic discriminants.) Then r is a root of the cubic, $x^3 + Gx^2 + Hx + I$, where

$$\begin{aligned} G &= -AD \\ H &= A^2E + D^2B - 3BE \\ I &= -\tfrac{1}{2}\left(2CD^3 + ABDE + 2A^3F - 9CDE - 9ABF + 27CF + \delta\right). \end{aligned}$$

Proof. This is easily verified by interpreting the coefficients as symmetric functions in the roots.

A	B	C
$-s_1 - s_2 - s_3$	$s_1s_2 + s_1s_3 + s_2s_3$	$-s_1s_2s_3$
D	E	F
$-t_1 - t_2 - t_3$	$t_1t_2 + t_1t_3 + t_2t_3$	$-t_1t_2t_3$
G	H	I
$-r_1 - r_2 - r_3$	$r_1r_2 + r_1r_3 + r_2r_3$	$-r_1r_2r_3$

Take $r_1 = r$, $r_2 = s_1t_2 + s_2t_3 + s_3t_1$ and $r_3 = s_1t_3 + s_2t_1 + s_3t_2$. □

Remark 3.6. It is irrelevant how we identify with S_3 on each side, i.e., which "diagonal quotient" we choose. Once the kernels of ψ_1 and ψ_2 are specified, there is only one entanglement modular curve up to isomorphism by Theorem 3.3, since $[\mathrm{Aut}\,\Gamma : \mathrm{Inn}\,\Gamma] = 1$ when $\Gamma = S_3$.

Remark 3.7. A similar technique was applied in [3, pg. 19]. The main difference in our Lemma 3.5 is that we have not generated the desired S_3 extension with an irreducible degree 6 polynomial over the base field, but rather with a cubic polynomial over the quadratic subextension generated by δ (the square root of the discriminant).

3.3. Level 10. Let $G(m_1) = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, and let $G(m_2) \subseteq \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$ be the unique index 5 subgroup $\mathcal{E}_{S_4}(5)$ containing $\mathcal{N}_s(5)$ (the normalizer of split Cartan) as an index 3 subgroup. The group $\mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ contains as a subgroup an isomorphic copy of S_4, and $\mathcal{E}_{S_4}(5)$ may also be described as the full pre-image of that copy of S_4 under the canonical projection $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z}) \twoheadrightarrow \mathrm{PGL}_2(\mathbb{Z}/5\mathbb{Z})$ (it is often referred to as an *exceptional* subgroup). We may fix an isomorphism $\psi_1 : G(m_1) \xrightarrow{\sim} S_3$ and a surjection $\psi_2 : G(m_2) \twoheadrightarrow S_3$ whose kernel is contained in $\mathcal{N}_s(5)$ with index 2. Moreover, $G := \pi_{\mathrm{GL}_2}^{-1}\left(G(m_1) \times_\psi G(m_2)\right)$ is conjugate to the non-abelian entanglement group G_{10} in Theorem 1.8. In this section we determine a parameter on the genus 0 modular curve $\mathcal{X} := X_G$, as well as an explicit formula for the map from $\mathcal{X}$ down to the j-line.

Closely following the general yoga of Section 3.1, our first step is to find an explicit model for the full product modular curve. However, since $G(m_1)$ is "full," i.e., all of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, this is simply the curve $X = X_{G(m_2)}$. From [30] we know that $X_{G(m_2)}$ is a genus 0 curve with parameter t, such that the map to the j-line is as follows.[3]

$$j(t) = t^3(t^2 + 5t + 40). \tag{41}$$

The next step is to define a universal family of elliptic curves E_t over $K(t)$, and then find two cubic polynomials over $K(t)$ that generically generate the S_3

[3]Our group $G(m_2)$ is referred to as G_9 in [30].

subextensions of $K(E_t[2])$ and $K(E_t[5])$, respectively. A convenient family can be found by substituting $j(t)$ into the following universal family over the j-line.

$$y^2 = x^3 + \tfrac{1}{4}x^2 - \frac{36}{j-1728}x - \frac{1}{j-1728} \tag{42}$$

After a linear change of variables over $\mathbb{Q}$, we arrive at the family E_t given by $y^2 = x^3 + B(t)x + C(t)$, where $B(t)$ and $C(t)$ are as follows.

$$B(t) = -3(t-3)t(t^2+5t+40) \quad C(t) = 2(t-3)^2(t^2+4t+24)(t^2+5t+40) \tag{43}$$

The cubic polynomial that generically generates the S_3 subextension of $K(E_t[2])$, i.e., the full 2-torsion field of E_t, is simply the Weierstrass polynomial. In the next lemma, we determine a cubic polynomial over $\mathbb{Q}(t)$ that generically generates the S_3 subextension of $K(E_t[5])$. Thus we are in position to apply Lemma 3.5 to determine first a singular equation for the genus 0 entanglement curve, $\mathcal{X}$, and then a parameter over $\mathbb{Q}$.

Lemma 3.8. *The S_3 subextension of $K(E_t[5])/K$ is (generically) generated by the roots of the cubic polynomial, $x^3 + E(t)x + F(t)$, where*

$$E(t) = -3\left(t^2 + 5t + 40\right)$$
$$F(t) = -2\left(t + \tfrac{5}{2}\right)\left(t^2 + 5t + 40\right).$$

Proof. Recall that $\ker\psi_2 \subseteq \mathcal{N}_s(5) \subseteq G(m_2)$, with indices of 2 and 3, respectively. Therefore, the S_3 subextension of $K(E_t[5])$ that is determined by $\ker\psi_2$ must be generated (generically) by the natural extension from $X_{G(m_2)}$ up to $X_s^+(5) = X_{\mathcal{N}_s(5)}$. More precisely and in the language of Section 3.1, the function field of the modular curve, $Y_{S_3,2}$, in this case, is just the normal closure of the function field of $X_s^+(5)$ in the function field of $X(5)$, once $X_s^+(5)$ is viewed as a degree 3 extension of $X_{G(m_2)}$.

So, essentially, we just need to find an explicit equation for the natural projection from $X_s^+(5)$ to $X_{G(m_2)}$. One way to do this is to think of the desired extension as an irreducible component of $X_s^+(5) \times_{X(1)} X_{G(m_2)}$ that lies over $X_{G(m_2)}$ with degree 3 by the canonical map (projection onto the second factor). The j-map for the genus 0 curve, $X_s^+(5)$, is also given in [30] and copied below for convenience.

$$j(s) = \frac{(s+5)^3\left(s^2-5\right)^3\left(s^2+5s+10\right)^3}{\left(s^2+5s+5\right)^5} \tag{44}$$

Setting $j(s) = j(t)$ to compute the fiber product, we then factor to find two irreducible components, which lie over $X_{G(m_2)}$ with degrees 3 and 12. The former is given by

$$s^3 + (-t+5)s^2 + (-5t-5)s - 5t - 25 = 0.$$

The substitution, $x = 3s - t + 5$, yields the polynomial that is given in the statement of the lemma. □

Theorem 3.9. *Let $\mathcal{X}$ be the modular curve of level 10 whose K-rational points correspond generically to elliptic curves E/K satisfying:*

(1) $Gal(K(E[2])/K) \cong \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$
(2) $Gal(K(E[5])/K) \cong \mathcal{E}_{S_4}(5)$ (from above)
(3) $Gal(K(E[5]) \cap K(E[2])/K) \cong S_3$.

Then $\mathcal{X}$ is isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$, and a (degree 1) parameter u may be chosen on $\mathcal{X}$ so that the natural map from $\mathcal{X}$ to $X_{G(m_2)}$ is described as follows.

$$t = \frac{3u^6 + 12u^5 + 80u^4 + 50u^3 - 20u^2 - 8u + 8}{(u-1)^2\left(u^2+3u+1\right)^2}$$

Proof. When we begin to apply the construction of Lemma 3.5 to the cubic polynomial from the previous lemma and the Weierstrass polynomial of E_t, we find that

$$\delta^2 = 2^8 \cdot 3^{12} \cdot 5(t-3)^3\left(t^2+5t+40\right)^4.$$

For simplicity, we make the substitution, $\delta = 2^4 \cdot 3^6(t-3)\left(t^2+5t+40\right)^2 y$. Then y is a parameter on the genus 0 modular curve (lying over $X_{G(m_2)}$) whose K-rational points correspond generically to elliptic curves E/K for which $E[2]$ and $E[5]$ have the desired quadratic entanglement. The map from this curve to $X_{G(m_2)}$ is given by $y^2 = 5(t-3)$.

Continuing on with Lemma 3.5, we then compute the coefficients of the cubic equation, $x^3 + Gx^2 + Hx + I = 0$, over $\mathbb{Q}(t,\delta) = \mathbb{Q}(y)$, which describes the full S_3 entanglement modular curve. After making the simplifying substitution $x = 3 \cdot 5^{-3} y\left(y^2 - 5y + 40\right) x_0$, we arrive at the equation, $x_0^3 + H_0 x_0 + I_0 = 0$, where

$$H_0(y) = -3\left(y^2+15\right)\left(y^2+5y+40\right)^2$$
$$I_0(y) = \left(y^2+5y+40\right)^2\left(2y^5+10y^4+125y^3+225y^2+1125y-3375\right).$$

It is easy to check that the equations given below define a map from $\mathbb{P}^1$ (with parameter u) to this singular curve.

$$y = \frac{-5\left(4u^2+2u-1\right)}{(u-1)\left(u^2+3u+1\right)}$$
$$x_0 = \frac{25\left(2u^2+u+2\right)^2\left(3u^5+10u^4+25u^3+10u^2+2\right)}{(u-1)^3\left(u^2+3u+1\right)^3}$$

The map must be a birational isomorphism, as y defines a degree 3 function on both curves. Composing with $t = \frac{1}{5}y^2 + 3$ yields the formula for t in terms of u that is given in the statement of the theorem. □

Example 3.10. If we substitute $u = 0$ into Theorem 3.9, we arrive at $j = 73728$ and the following elliptic curve.

$$E : y^2 = x^3 - 120x + 500$$

Let $p(x)$ be the 5-torsion polynomial of E, which has degree 12. Then $p(x)$ is irreducible over $\mathbb{Q}$, and its splitting field is a degree 48 extension. Adjoining the corresponding y coordinate for any particular root of $p(x)$ generates a further quadratic extension. Since $\mathrm{Gal}(\mathbb{Q}(E[5])/\mathbb{Q}) \subseteq \mathcal{E}_{S_4}(5)$ (up to conjugation), and the order of $\mathcal{E}_{S_4}(5)$ is 96, this confirms that $\mathrm{Gal}(\mathbb{Q}(E[5])/\mathbb{Q}) \cong \mathcal{E}_{S_4}(5)$. However, over $\mathbb{Q}(\alpha)$ for any root α of the Weierstrass polynomial, $p(x)$ factors into the product of a degree 4 polynomial and a degree 8 polynomial. Hence, we must have $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(E[5])$. But $\mathbb{Q}(E[2])$ is just the Galois closure of $\mathbb{Q}(\alpha)$. Therefore, since the intersection of Galois extensions must be Galois, it follows that $\mathbb{Q}(E[2]) \subseteq \mathbb{Q}(E[5])$, i.e, $\mathrm{Gal}(\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[5])/\mathbb{Q}) \cong S_3$.

3.4. Level 15. Let $G(m_1) = \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$, and let $G(m_2) \subseteq \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$ be the same subgroup $\mathcal{E}_{S_4}(5)$ as in Section 3.3. Each $G(m_i)$ surjects via some ψ_i onto S_3, so that $G := \pi_{\mathrm{GL}_2}^{-1}\big(G(m_1) \times_\psi G(m_2)\big)$ is conjugate to the group G_{15} in Theorem 1.8. In this section we derive an explicit equation for the modular curve $\mathcal{X} := X_G$ that corresponds to this scenario. All of the essential information on the 5-side carries over directly from the previous section. In particular, there is a genus 0 modular curve, $X_{G(m_2)}$, whose K-rational points correspond generically to elliptic curves E/K for which $\mathrm{Gal}(K(E[5])/K) \cong G(m_2)$. The map from $X_{G(m_2)}$ (with parameter t) to the j-line is given in (41), and we have a universal family of elliptic curves E_t over $K(t)$, which is described by (43). In the language of Section 3.1, we may once again view $X = X_{G(m_2)}$ as the full product curve, since we have $G(m_1) = \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$.

The cubic polynomial over $K(t)$ that generically generates the S_3 subextension of $K(E_t[5])$ was derived in Lemma 3.8. On the other hand, we have the classical result that for elliptic curves E/K with $\mathrm{Gal}(K(E[3])/K)$ isomorphic to $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$, the S_3 subextension of $K(E[3])$ is the splitting field of $x^3 - j$. Therefore, in order to find an explicit model for the entanglement modular curve in this case, we work over $K(t)$ and apply Lemma 3.5, using the cubic polynomial from Lemma 3.8 and the cubic polynomial $x^3 - j(t)$ (where $j(t)$ is as given in (41)). Note that we already know, a priori, when the *quadratic* subfields of $K(E_t[3])$ and $K(E_t[5])$ coincide. The two quadratic subfields are $K(\sqrt{-3})$ and $K(\sqrt{5})$, respectively. Hence, they will coincide if and only if $\sqrt{-15} \in K$.

Theorem 3.11. *Let $\mathcal{X}$ be the modular curve of level* 15 *whose K-rational points correspond generically to elliptic curves E/K satisfying:*

(1) Gal$(K(E[3])/K) \cong \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$
(2) Gal$(K(E[5])/K) \cong \mathcal{E}_{S_4}(5)$ *(from above)*
(3) Gal$(K(E[5]) \cap K(E[3])/K) \cong S_3$.

Then $\mathcal{X}$ is isomorphic to $\mathbb{P}^1$ over its field of definition, $\mathbb{Q}(\sqrt{-15})$, and a (degree 1) parameter u may be chosen on $\mathcal{X}$ so that the natural map from $\mathcal{X}$ to $X_{G(m_2)}$ is described as follows.

$$t = u^3 - \frac{5-3\sqrt{-15}}{2}$$

Proof. We begin by computing the discriminants of the two cubic polynomials over $K(t)$.

$$\Delta_1 = -3^3 \cdot t^6(t^2+5t+40)^2 \qquad \Delta_2 = 3^6 \cdot 5 \cdot (t^2+5t+40)^2$$

Then the first step in applying Lemma 3.5 is to adjoin δ to $\mathbb{Q}(t)$, where

$$\delta^2 = \Delta_1\Delta_2 = -3^9 \cdot 5 \cdot t^6(t^2+5t+40)^4.$$

This clearly implies, as was noted above, that $\mathbb{Q}(t,\delta) = \mathbb{Q}(t,\sqrt{-15})$, and so we may continue by taking $\delta = 3^4\sqrt{-15} \cdot t^3(t^2+5t+40)^2$. Applying Lemma 3.5, we arrive at the model,

$$x^3 - 3^3 \cdot t^3\left(t + \frac{5-3\sqrt{-15}}{2}\right)^2\left(t + \frac{5+3\sqrt{-15}}{2}\right)^3 = 0.$$

The model given in the statement of the theorem can be obtained by letting

$$x = 3 \cdot t\left(t + \frac{5-3\sqrt{-15}}{2}\right)\left(t + \frac{5+3\sqrt{-15}}{2}\right)u^{-1}.$$

□

3.5. Level 18. Let $G(m_1) = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and let $G(m_2)$ be the full pre-image of the Borel group B(3) under the canonical projection from $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ onto $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. Then $G(m_2)$ has an index 6 normal subgroup $N(m_2)$ consisting of all upper triangular invertible matrices for which the diagonal entries are congruent mod 3. Moreover, the quotient is isomorphic to S_3. Fixing a surjection $\psi_2 : G(m_2) \twoheadrightarrow S_3$ with $\ker\psi_2 = N(m_2)$, and an isomorphism $\psi_1 : G(m_1) \xrightarrow{\sim} S_3$, we arrive at a group $G := \pi_{\mathrm{GL}_2}^{-1}\left(G(m_1) \times_\psi G(m_2)\right)$ which is conjugate to the group G_{18} in the statement of Theorem 1.8. In this section we derive an explicit equation for the corresponding genus 0 modular curve $\mathcal{X} := X_G$.

Following the yoga, we want to build $\mathcal{X}$ as an extension of the full product curve $X := X_{G(m_1),G(m_2)}$, but this is once again just $X_{G(m_2)}$ since $G(m_1) = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. Hence, X is canonically isomorphic to the well-known modular curve $X_0(3)$, for which we may choose the following parameter and map to the j-line.

$$t = \left(\frac{\eta_1}{\eta_3}\right)^{12} \qquad j(t) = \frac{(t+27)(t+243)^3}{t^3}$$

Substituting $j(t)$ into (42) as before, and making a linear change of variables, we arrive at the family E_t of elliptic curves over X given by the Weierstrass polynomial, $y^2 = x^3 + B(t)x + C(t)$, where

$$B(t) = -3(t+27)(t+243) \qquad C(t) = 2(t+27)(t^2-486t-19683).$$

Our next step is to determine the two cubic polynomials with coefficients in $\mathbb{Q}(t)$ that generically generate the corresponding S_3 subextensions of $K(E_t[2])$ and $K(E_t[9])$ over K, respectively, for a given K-rational point of X. The first is simply the Weierstrass polynomial, while the second is addressed in the following lemma.

Lemma 3.12. *The S_3 subextension of $K(E_t[9])/K$ which is fixed by $N(m_2)$ (as above) is generically generated by the roots of the cubic polynomial, $x^3 + E(t)x + F(t)$, where*

$$E(t) = -3t(t + 27)$$
$$F(t) = -t(2t + 27)(t + 27).$$

Proof. Note that $N(m_2)$, the kernel of the map from $G(m_2)$ to S_3, is contained in the Borel group B(9). Hence, the corresponding S_3 subextension of $\mathrm{Gal}(K(E_t[9])/K)$ will be (generically) generated by a certain degree 3 factor in the fiber product of $X_{G(m_2)}$ with $X_0(9)$ over the j-line. Identifying $X_{G(m_2)}$ with $X_0(3)$, it is the factor whose points correspond in moduli-theoretic terms with triples (E, C, D), where D is cyclic of order 9 and $C = 3D$. In order to determine this factor explicitly, we need an explicit parameter on the genus 0 modular curve $X_0(9)$, along with an equation for the map to the j-line. One choice of parameter is given by the eta product function $s = (\eta_1/\eta_9)^3$, for which the map is as follows.

$$j(s) = \frac{(s + 9)^3 \left(s^3 + 243s^2 + 2187s + 6561\right)^3}{s^9 \left(s^2 + 9s + 27\right)}$$

Factoring $j(s) - j(t)$, we find a unique factor of degree 3 over $K(t)$.

$$s^3 - ts^2 - 9ts - 27t$$

So the roots of this polynomial in s would indeed (generically) generate the desired S_3 subextension of $K(E_t[9])$ over K. The substitution, $s = \frac{1}{3}(x + t)$, yields the equivalent cubic given in the statement of the lemma. □

Theorem 3.13. *Let $\mathcal{X}$ be the modular curve of level* 18 *whose K-rational points correspond (generically) to elliptic curves E/K satisfying:*

(1) Gal$(K(E[2])/K) \cong \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$
(2) Gal$(K(E[9])/K) \cong G(m_2)$ (the full pre-image of B(3) in $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$)
(3) Gal$(K(E[9]) \cap K(E[2])/K) \cong S_3$ (the fixed field of $N(m_2)$ as above).

Then $\mathcal{X}$ is isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$, and a (degree 1) parameter u may be chosen on $\mathcal{X}$ so that the natural map from $\mathcal{X}$ to $X_{G(m_2)}$ is described as follows.

$$t = -27\left(u^3 - 1\right)^{-2}.$$

Proof. In order to apply Lemma 3.5, we first set δ^2 equal to the product of the discriminants of the cubic polynomial in Lemma 3.12 and the Weierstrass polynomial of E_t. Then δ generates the quadratic entanglement curve over X.

$$\delta^2 = -2^8 \cdot 3^{15}(t+27)^4 t^5$$

If we set $\delta = 2^4 \cdot 3^7 (t+27)^2 t^2 y$, this simplifies to $y^2 = -3t$, so that y is clearly a parameter (over $\mathbb{Q}$) for the genus 0 curve.

Now that we have δ, we are able to apply Lemma 3.5 to obtain an initial singular equation for $\mathcal{X}$ of the form, $x^3 + H(y)x + I(y) = 0$. After making the linear substitution, $x = -\frac{1}{3}(y+9)x_0$, we arrive at the equation, $x_0^3 + H_0(y)x_0 + I_0(y) = 0$, where $H_0(y)$ and $I_0(y)$ are as follows.

$$H_0(y) = -3y^2(y-27)(y+27)(y-9)^2$$
$$I_0(y) = -y^2(y-9)^2(2y^5 - 18y^4 + 2997y^3 - 32805y^2 - 177147y + 1594323)$$

It is easy to check that a birational isomorphism over $\mathbb{Q}$ from $\mathbb{P}^1$ to this singular curve is given by the following equations.

$$y = \frac{-9}{u^3 - 1} \qquad x_0 = \frac{729u^2\left(3u^5 - 3u^3 - 4u^2 + 2\right)}{\left(u^3 - 1\right)^3}$$

Composing with $t = -\frac{1}{3}y^2$ results in the formula for the forgetful map from $\mathcal{X}$ to $X_{G(m_2)}$ that is given in the statement of the theorem. □

4. An application to counting elliptic curves over $\mathbb{Q}$ with maximal Galois image modulo a prescribed obstruction

In this section we discuss an application of Theorem 1.8 to the problem of determining which elliptic curves defined over $\mathbb{Q}$ have Galois image as large as possible relative to a given obstruction, and also of counting elliptic curves with this property. More precisely, as in Remark 1.4, let $E_{\text{tors}} := \bigcup_{m=1}^{\infty} E[m]$ denote the torsion subgroup of E over $\overline{\mathbb{Q}}$, let $G_{\mathbb{Q}} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ denote the absolute Galois group of $\mathbb{Q}$ and let

$$\rho_E : G_{\mathbb{Q}} \longrightarrow \text{Aut}(E_{\text{tors}}) \simeq \text{GL}_2(\hat{\mathbb{Z}}),$$
$$\rho_{E,m} : G_{\mathbb{Q}} \longrightarrow \text{Aut}(E[m]) \simeq \text{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

be the Galois representations defined by letting $G_{\mathbb{Q}}$ act on E_{tors} (resp. on $E[m]$) and fixing $\mathbb{Z}/m\mathbb{Z}$-bases compatibly. Furthermore, let $G \subseteq \text{GL}_2(\hat{\mathbb{Z}})$ be an open subgroup and suppose that there is an elliptic curve E over $\mathbb{Q}$ satisfying $\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G$. In fact, this will imply that G is *admissible* in the sense of the following definition, which is inspired by that found in [25, p. 1209] but is a slight modification thereof.

Definition 4.1. An open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is called **admissible** if

(1) $\det G = \hat{\mathbb{Z}}^\times$, and
(2) $\exists g \in G$ that is $\mathrm{GL}_2(\hat{\mathbb{Z}})$-conjugate to either $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ or $\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$.

By considering the Weil pairing and the image under ρ_E of a complex conjugation, we may see that

$$\exists \text{ an elliptic curve } E/\mathbb{Q} \text{ with } \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G \implies G \text{ is admissible.}$$

Remark 4.2. Our restriction to considering only elliptic curves defined over $\mathbb{Q}$ applies only to this section of the paper, and not to other sections. In particular, the computer search associated to Theorem 1.8 is not restricted to admissible subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$, and indeed the group G_{15} of (3) is not admissible, failing each of the conditions in Definition 4.1.

Remark 4.3. As mentioned above, Definition 4.1 differs slightly from the definition of admissible found in [25, p. 1209], wherein it is also demanded that $-I \in G$ and that G be of prime power level. As a consequence of the Hasse-Minkowski theorem, assuming $-I \in G$ and X_G has genus zero, they prove that

$$G \text{ is admissible and of prime power level} \implies |X_G(\mathbb{Q})| = \infty.$$

Given an admissible open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, it is natural to wonder whether or not there exists an elliptic curve E over $\mathbb{Q}$ satisfying

$$\rho_E(G_{\mathbb{Q}}) \doteq G. \tag{45}$$

Because we are working over $\mathbb{Q}$, classical class field theory motivates the following definition.

Definition 4.4. We say that a subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is **commutator-thick** if

$$[G, G] = G \cap \mathrm{SL}_2(\hat{\mathbb{Z}}).$$

Note that we clearly have $[G, G] \subseteq G \cap \mathrm{SL}_2(\hat{\mathbb{Z}})$ for any subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$, and this containment can be proper (indeed, it is proper even for $G = \mathrm{GL}_2(\hat{\mathbb{Z}})$)[4]. Furthermore, it follows from the Kronecker-Weber Theorem that, for any elliptic curve E over $\mathbb{Q}$, the subgroup $\rho_E(G_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is commutator-thick. Indeed, identifying $\rho_E(G_{\mathbb{Q}})$ with $\mathrm{Gal}(\mathbb{Q}(E_{\mathrm{tors}})/\mathbb{Q})$, we have

$$\begin{aligned} \mathbb{Q}(\mu_\infty) &= \mathbb{Q}(E_{\mathrm{tors}})^{\rho_E(G_{\mathbb{Q}}) \cap \mathrm{SL}_2(\hat{\mathbb{Z}})} \\ &\subseteq \mathbb{Q}(E_{\mathrm{tors}})^{[\rho_E(G_{\mathbb{Q}}), \rho_E(G_{\mathbb{Q}})]} \subseteq \mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\mu_\infty), \end{aligned} \tag{46}$$

and so we must have equality at each inclusion. In particular, (45) can only happen if G is itself commutator-thick. In case G is not commutator-thick, we are motivated to consider what it should mean for $\rho_E(G_{\mathbb{Q}}) \subseteq G$ to be "as large as possible." Following [17], we make the following definition.

[4]Here we are defining the commutator subgroup $[G, G]$ to be the *closure* of the subgroup generated by commutators.

Definition 4.5. Let $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$. Given a subgroup $H \subseteq G$, we say that H is **commutator-maximal in** G if

$$[H, H] = [G, G].$$

If $H \dot{\subseteq} G$, we say that H is commutator-maximal in G if gHg^{-1} is commutator-maximal in G for some (any) $g \in \mathrm{GL}_2(\hat{\mathbb{Z}})$ for which $gHg^{-1} \subseteq G$.

We will use commutator-maximality of $H = \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G$ to define the concept of $\rho_E(G_{\mathbb{Q}})$ having maximal image inside G. Since we are assuming that $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ is an open subgroup, it follows that $[G, G] \subseteq \mathrm{SL}_2(\hat{\mathbb{Z}})$ is open, which implies that the index of $[G, G]$ in $G \cap \mathrm{SL}_2(\hat{\mathbb{Z}})$ is finite. As discussed in [17], in case $\det H = \hat{\mathbb{Z}}^\times$, Definition 4.5 is equivalent to the statement that

$$[H : G] = \big[[G, G] : G \cap \mathrm{SL}_2(\hat{\mathbb{Z}})\big]. \tag{47}$$

In case $G = \mathrm{GL}_2(\hat{\mathbb{Z}})$, the index on the right-hand side of (47) is 2; thus in this case $\rho_E(G_{\mathbb{Q}})$ is commutator-maximal in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ if and only if $\rho_E(G_{\mathbb{Q}})$ has index two inside $\mathrm{GL}_2(\hat{\mathbb{Z}})$. An elliptic curve E for which $\big[\rho_E(G_{\mathbb{Q}}) : \mathrm{GL}_2(\hat{\mathbb{Z}})\big] = 2$ is typically called a *Serre curve*, and so this motivates the following nomenclature.

Definition 4.6. Let $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ be an admissible open subgroup and suppose that E is an elliptic curve over $\mathbb{Q}$ that satisfies $\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G$. We call E a G-**Serre curve** if $\rho_E(G_{\mathbb{Q}})$ is commutator-maximal in G, in the sense of Definition 4.5.

Remark 4.7. Definition 4.6 is *stronger* than (and in particular not equivalent to) the condition that $\rho_E(G_{\mathbb{Q}})$ be maximal among commutator-thick subgroups. For example, there exist elliptic curves E over $\mathbb{Q}$ for which

$$\mathbb{Q}(\sqrt{\Delta_E}) = \mathbb{Q}(i) \tag{48}$$

and with $\rho_E(G_{\mathbb{Q}}) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ maximal among commutator-thick subgroups, but, since the index two subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ corresponding to (48) is not commutator-thick, none of these elliptic curves will be Serre curves. (In this case, $\rho_E(G_{\mathbb{Q}})$ must be contained in an index four subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$.)

If E is an elliptic curve over $\mathbb{Q}$ with $\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G$, how can we tell whether or not E is a G-Serre curve? We define the following two sets of proper subgroups of G:

$$\begin{aligned} \mathfrak{S}(G) &:= \left\{ H \subsetneq G : \begin{array}{c} H \text{ admissible but not} \\ \text{commutator-maximal in } G \end{array} \right\} \\ \mathfrak{S}^{\max}(G) &:= \big\{ H \in \mathfrak{S}(G) : \nexists H_1 \in \mathfrak{S}(G) \text{ for which } H \subsetneq H_1 \subsetneq G \big\}. \end{aligned} \tag{49}$$

Since we obviously have

$$E \text{ is not } G\text{-Serre} \iff \exists H \in \mathfrak{S}^{\max}(G) \text{ for which } \rho_E(G_{\mathbb{Q}}) \dot{\subseteq} H, \tag{50}$$

it is of natural interest to determine the set $\mathfrak{S}^{\max}(G)$. The following theorem does so, for a particular open subgroup $G \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$. As we will see, for each $H \in \{G_6, G_{18}\}$ (the two non-abelian entanglement groups featured in Theorem 1.8), we have $H \cap G \in \mathfrak{S}^{\max}(G)$. To begin with, we will observe that this is

not unexpected, since whenever $H \subseteq G$ is a fibered product over a non-abelian quotient and G is merely a fibered product over a cyclic quotient, then H is not commutator-maximal in G. In particular, consider the following two lemmas, where G_1 and G_2 are finite groups and $\psi_i : G_i \longrightarrow \Gamma_\psi$ are surjective group homomorphisms onto a common quotient group Γ_ψ, and recall that

$$G_1 \times_\psi G_2 := \{(g_1, g_2) \in G_1 \times G_2 : \psi_1(g_1) = \psi_2(g_2)\}$$

denotes the fibered product group.

Lemma 4.8. *With the notation as above, if the group Γ_ψ is cyclic, then we have*

$$\left[G_1 \times_\psi G_2, G_1 \times_\psi G_2\right] = [G_1, G_1] \times [G_2, G_2]\,.$$

Proof. This follows from [18, Lemma 1, p. 174]. □

By contrast, we have

Lemma 4.9. *With the notation as above, if the group Γ_ψ is non-abelian, then*

$$\left[G_1 \times_\psi G_2, G_1 \times_\psi G_2\right] \subsetneq [G_1, G_1] \times [G_2, G_2]\,.$$

Proof. Since Γ_ψ is non-abelian, we have $[\Gamma_\psi, \Gamma_\psi] \neq \{1\}$. Since each ψ_i is onto, we have

$$\{1\} \neq [\Gamma_\psi, \Gamma_\psi] = \psi_i\left([G_i, G_i]\right) \subseteq \Gamma_\psi \qquad (i \in \{1, 2\})\,,$$

and so the commutator subgroup

$$\left[G_1 \times_\psi G_2, G_1 \times_\psi G_2\right] \subseteq [G_1, G_1] \times_\psi [G_2, G_2]$$

is contained in a fibered product over the non-trivial group $[\Gamma_\psi, \Gamma_\psi]$, and is therefore a proper subgroup of $[G_1, G_1] \times [G_2, G_2]$. □

Combining Lemma 4.8 with Lemma 4.9, we obtain the following corollary.

Corollary 4.10. *Let $G = G_1 \times_\psi G_2$ be a fibered product over a* cyclic *group Γ_ψ and, for each $i \in \{1, 2\}$, let $H_i \subseteq G_i$ be a subgroup. Suppose that $H \subseteq G$ is a subgroup of the form $H = H_1 \times_\phi H_2$, where each $\phi_i : H_i \to \Gamma_\phi$ is a surjective homomorphism onto a* non-abelian *group Γ_ϕ. Then H is* not *commutator-maximal in G.*

We now take $G_1 := \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and $G_2 := \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. We let $\gamma := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, and define the maps ψ_2 and ψ_3 as follows:

$$\psi_2 : \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \xrightarrow{\text{can}} \frac{\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})}{\langle\gamma\rangle} \xrightarrow{\simeq} \{\pm 1\},$$

$$\psi_3 : \left\{\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}\right\} \xrightarrow{\det} (\mathbb{Z}/3\mathbb{Z})^\times \xrightarrow{\simeq} \{\pm 1\}.$$

We define the index eight subgroup $G(6) \subseteq \mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z})$ to be the fibered product

$$G(6) := \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times_{\psi} \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \tag{51}$$

and define $G := \pi_{\mathrm{GL}_2}^{-1}(G(6)) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ to be the associated open subgroup. Let E be an elliptic curve satisfying $\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G$. Our next theorem determines precisely the conditions under which E is a G-Serre curve[5]. First, let us denote by

$$\mathrm{B}(\ell) := \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}), \qquad (\ell \text{ prime}),$$

$$\mathcal{N}_{\mathrm{ns}}(\ell) := \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} x & y \\ y & -x \end{pmatrix} \right\} \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \qquad (\ell \geq 3 \text{ prime})$$

respectively, the Borel subgroup and the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Next, we define the following subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

$$\begin{aligned}
G_{2,1} &:= \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : g \mod 2 \in \mathrm{B}(2) \right\}, \\
G_{3,1} &:= \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : g \mod 3 \in \mathcal{N}_{\mathrm{ns}}(3) \right\}, \\
G_{4,1} &:= \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : g \mod 4 \in \left\langle \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} \right\rangle \right\}, \\
G_{6,1} &:= \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : g \mod 6 \in \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 1 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 5 & 4 \\ 4 & 1 \end{pmatrix} \right\rangle \right\}, \\
G_{9,1} &:= \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : g \mod 9 \in \left\langle \begin{pmatrix} 4 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle \right\}, \\
G_{9,2} &:= \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : g \mod 9 \in \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right\rangle \right\}, \\
G_{9,3} &:= \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : g \mod 9 \in \left\langle \begin{pmatrix} 2 & 2 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 7 \\ 0 & 8 \end{pmatrix}, \begin{pmatrix} 5 & 4 \\ 3 & 4 \end{pmatrix} \right\rangle \right\}, \\
G_{18,1} &:= \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : g \mod 18 \in \left\langle \begin{pmatrix} 7 & 17 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 17 & 3 \\ 3 & 14 \end{pmatrix}, \begin{pmatrix} 4 & 3 \\ 3 & 14 \end{pmatrix} \right\rangle \right\}, \\
G_{18,2} &:= \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : g \mod 18 \in \left\langle \begin{pmatrix} 1 & 10 \\ 3 & 11 \end{pmatrix}, \begin{pmatrix} 16 & 3 \\ 9 & 8 \end{pmatrix}, \begin{pmatrix} 11 & 4 \\ 12 & 11 \end{pmatrix} \right\rangle \right\}, \\
G_{18,3} &:= \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : g \mod 18 \in \left\langle \begin{pmatrix} 16 & 9 \\ 9 & 8 \end{pmatrix}, \begin{pmatrix} 5 & 16 \\ 6 & 5 \end{pmatrix}, \begin{pmatrix} 7 & 13 \\ 3 & 10 \end{pmatrix} \right\rangle \right\}.
\end{aligned} \tag{52}$$

By (50), we see that, when E is not a G-Serre curve, $\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} H$ for some $H \in \mathfrak{S}^{\max}(G)$. Assuming that such a group H satisfies $H(\ell) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for each $\ell \notin \{2, 3\}$, [17, Theorem 2.7 & Remark 2.8] establishes in this case that

[5] We have $\left[G \cap \mathrm{SL}_2(\hat{\mathbb{Z}}) : [G, G] \right] = 2$, and thus, E is a G-Serre curve if and only if $\rho_E(G_{\mathbb{Q}})$ is an index two subgroup of G.

$G_{i,j}$ from (52)	$G_{2,1}$	$G_{3,1}$	$G_{4,1}$	$G_{6,1}$	$G_{9,1}$	$G_{9,2}$	$G_{9,3}$	$G_{18,1}$	$G_{18,2}$	$G_{18,3}$
genus($X_{\tilde{G}_{i,j}}$)	0	0	0	0	0	0	1	0	1	2
genus($X_{\tilde{G}\cap\tilde{G}_{i,j}}$)	0	1	1	0	0	1	2	0	1	2

TABLE 5. Genera of modular curves associated to $G_{i,j}$ from (52)

$[H(216), H(216)] \neq [G(216), G(216)]$. Thus, it becomes a finite search to determine the set $\mathfrak{S}^{\max}(G)$, and, carrying out this computation, we arrive at the following theorem.

Theorem 4.11. *Let $G(6) \subseteq \mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z})$ be the index two subgroup defined by* (51) *and let $G = \pi^{-1}_{\mathrm{GL}_2}(G(6))$ be the associated open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$. For each elliptic curve E over $\mathbb{Q}$ for which $\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G$, we have that E is* not *a G-Serre curve if and only if*

(1) *there exists a group $G_{i,j}$ appearing in* (52) *for which $\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G_{i,j}$, or*
(2) *there exists a prime $\ell \geq 5$ for which $\rho_{E,\ell}(G_{\mathbb{Q}}) \neq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*

Remark 4.12. The subgroups $G_{6,1}$ and $G_{18,1}$ of (52) are the subgroups G_6 and G_{18}, respectively, that appear in Theorem 1.8. In particular, Theorem 4.11 highlights the role played by non-abelian entanglement groups in this problem. The group $G_{4,1}$ has appeared in various previous papers (see [16], [13] and [25]); the groups $G_{9,1}$ and $G_{9,2}$ correspond, respectively, to the curves labeled $9C^0-9a$ and $9B^0 - 9a$ in the Table 1 of [25].

Remark 4.13. In the language introduced in (49), we have that

$$\mathfrak{S}^{\max}(G) = \{H \cap G \,:\, H = G_{i,j} \text{ as in (52)}\} \cup \bigcup_{\ell \geq 5} \{H \cap G \,:\, H \in \mathfrak{S}^{\max}(\ell)\},$$

where the set $\mathfrak{S}^{\max}(\ell)$ is defined as follows: we let $\mathfrak{S}(\ell)$ denote the set of all admissible open subgroups $H \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ for which $H(\ell) \neq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and define $\mathfrak{S}^{\max}(\ell) \subseteq \mathfrak{S}(\ell)$ to be the subset of those $H \in \mathfrak{S}(\ell)$ that are maximal with respect to subset inclusion. The genera of the modular curves $X_{G_{i,j}}$ and $X_{G\cap G_{i,j}}$ associated to each of the groups $G_{i,j}$ in (52) are listed in Table 5.

We now turn to the question: In case $\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G$, how *likely* is it that E is a G-Serre curve? More precisely, assume for simplicity that $-I \in G$, and suppose that the modular curve X_G has genus zero and that $X_G(\mathbb{Q}) \neq \emptyset$. Projecting from any rational point then yields a *generic* point in $X_G(\mathbb{Q}(t))$, whose specializations give rise to all points in $X_G(\mathbb{Q})$. Applying the forgetful map to the j-line

$$j_G \,:\, \mathbb{P}^1_{\mathbb{Q}}(t) \simeq X_G \longrightarrow X(1) \simeq \mathbb{P}^1_{\mathbb{Q}}(j),$$

we may then construct a Weierstrass model $\mathcal{E}$ defined over $\mathbb{Q}(t)$:

$$\mathcal{E} \,:\, y^2 = x^3 + a(t)x + b(t) \qquad (a(t), b(t) \in \mathbb{Q}(t)),$$

with j-invariant $j_{\mathcal{E}}(t) = j_G(t)$. The generic Galois representation

$$\rho_{\mathcal{E}} : G_{\mathbb{Q}(t)} \longrightarrow \mathrm{GL}_2(\hat{\mathbb{Z}})$$

satisfies $\rho_{\mathcal{E}}(G_{\mathbb{Q}(t)}) \subsetneq G$. One can show independently that in fact, $\rho_{\mathcal{E}}(G_{\mathbb{Q}(t)}) \doteq G$, but this may also be deduced from the following argument.

We are interested in understanding the nature of the specializations of $\mathcal{E}$ and their associated Galois representations. More precisely, let $\Delta_{\mathcal{E}}(t) \in \mathbb{Q}(t)$ denote the discriminant of $\mathcal{E}$ and define the finite subset $B_{\mathcal{E}} \subseteq \mathbb{Q}$ by

$$B_{\mathcal{E}} := \{t_0 \in \mathbb{Q} : a(t) \text{ or } b(t) \text{ is not regular at } t_0, \\ \Delta_{\mathcal{E}}(t_0) = 0, \text{ or } j_{\mathcal{E}}(t_0) \in \{0, 1728\}\}. \quad (53)$$

For each $t_0 \in \mathbb{Q} - B_{\mathcal{E}}$, we denote by $\mathcal{E}_{t_0}$ the specialized Weierstrass model

$$y^2 = x^3 + a(t_0)x + b(t_0),$$

which is an elliptic curve over $\mathbb{Q}$. We always have $\rho_{\mathcal{E}_{t_0}}(G_{\mathbb{Q}}) \dot{\subseteq} G$, and we would like to ask how *often* a specialization $\mathcal{E}_{t_0}$ is a G-Serre curve. More precisely, for $t_0 \in \mathbb{Q}$, we denote by

$$H(t_0) := \max\left\{|x_0|, |y_0| : t_0 = \frac{x_0}{y_0} \text{ in lowest terms}\right\}.$$

A standard exercise in analytic number theory (see for instance [1, Theorem 3.9]) shows that

$$\left|\{t_0 \in \mathbb{Q} : H(t_0) \le T\}\right| \sim \frac{1}{2\zeta(2)} T^2 \quad \text{as} \quad T \longrightarrow \infty. \quad (54)$$

It is reasonable to ask whether the ratio

$$\frac{\left|\left\{t_0 \in \mathbb{Q} - B_{\mathcal{E}} : H(t_0) \le T,\ \mathcal{E}_{t_0} \text{ is a } G\text{-Serre curve}\right\}\right|}{\left|\{t_0 \in \mathbb{Q} - B_{\mathcal{E}} : H(t_0) \le T\}\right|}$$

tends to 1 as $T \to \infty$. As discussed in [17] (see also [7]), this is indeed the case; in the spirit of [15] and [7], one might want to compute an asymptotic formula as $T \to \infty$ for the size of the truncated exceptional set

$$\mathcal{S}(T) := \left\{t_0 \in \mathbb{Q} - B_{\mathcal{E}} : H(t_0) \le T,\ \mathcal{E}_{t_0} \text{ is not a } G\text{-Serre curve}\right\}. \quad (55)$$

By (50), we see that

$$\mathcal{S}(T) = \bigcup_{H \in \mathfrak{S}^{\max}(G)} \mathcal{S}_H(T), \quad (56)$$

where

$$\mathcal{S}_H(T) := \left\{t_0 \in \mathbb{Q} - B_{\mathcal{E}} : H(t_0) \le T,\ \rho_{\mathcal{E}_{t_0}}(G_{\mathbb{Q}}) \dot{\subseteq} H\right\}.$$

A straightforward commutator calculation shows that, for any subgroup $H \subseteq G$ with $\tilde{H} = G$, $[H, H] = [G, G]$. Thus, for any $H \in \mathfrak{S}^{\max}(G)$, we must have $\tilde{H} \neq G$. This observation shows that the sets $\mathcal{S}_H(T)$ above are (truncations of) "thin sets" in the sense of [23]. Indeed, for $H \in \mathfrak{S}^{\max}(G)$, let $f_H : X_H \to X_G$

denote the forgetful map and $d_H := \deg f_H = [G : H]$ its degree. We have the commuting diagram

$$X_H \xrightarrow{f_H} X_G \xrightarrow{j_G} \mathbb{P}^1_{\mathbb{Q}}(j), \qquad X_H \xrightarrow{j_H} \mathbb{P}^1_{\mathbb{Q}}(j).$$

For each $t_0 \in \mathbb{Q} - B_{\mathcal{E}}$, we have

$$\rho_{\mathcal{E}_{t_0}}(G_{\mathbb{Q}}) \dot{\subseteq} H \iff j_{\mathcal{E}_{t_0}} \in j_H(X_H(\mathbb{Q})),$$

and thus

$$\mathcal{S}_H(T) := \left\{ t_0 \in \mathbb{Q} - B_{\mathcal{E}} : H(t_0) \le T,\ j_{\mathcal{E}_{t_0}} \in j_H\left(X_H(\mathbb{Q})\right) \right\}.$$

It follows from this (see [23, p. 133]) that, as $T \to \infty$, we have

$$\left|\mathcal{S}_H(T)\right| \quad \begin{cases} \sim C_H T^{2/d_H} & \text{if genus}(X_H) = 0 \text{ and } |X_H(\mathbb{Q})| = \infty, \\ \sim C_H (\log T)^{\rho_H/2} & \text{if genus}(X_H) = 1 \text{ and } |X_H(\mathbb{Q})| = \infty, \\ \ll_H 1 & \text{if } |X_H(\mathbb{Q})| < \infty, \end{cases} \tag{57}$$

where $C_H > 0$ denotes a constant, d_H is the degree of f_H in case genus$(X_H) = 0$, and $\rho_H \ge 1$ denotes the Mordell-Weil rank of X_H in case genus$(X_H) = 1$ and $|X_H(\mathbb{Q})| = \infty$. Furthermore, in [7] it is shown that the infinite tail occurring in (56) may be bounded, so that for any $\varepsilon > 0$, we may write

$$\mathcal{S}(T) = \mathcal{S}'(T) \cup \bigcup_{\substack{H \in \mathfrak{S}^{\max}(G) \\ m_{\mathrm{GL}_2}(H) \le r}} \mathcal{S}_H(T)$$

for some $r = r_{\mathcal{E},\varepsilon} \in \mathbb{N}$, where

$$\mathcal{S}'(T) = \begin{cases} O_{\mathcal{E},\varepsilon}\left(T^{1+\varepsilon}\right) & \text{if } \exists \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}) \text{ and } P(x) \in \mathbb{Z}[x] \\ & \quad \text{with } j_{\mathcal{E}}(t) = P\left(\frac{at+b}{ct+d}\right), \\ O_{\mathcal{E},\varepsilon}\left(T^{\varepsilon}\right) & \text{otherwise.} \end{cases}$$

Thus, we see that the asymptotic growth in T of the truncated exceptional set $\mathcal{S}(T)$ is governed by the arithmetic of the curves X_H for subgroups $H \in \mathfrak{S}^{\max}(G)$; in particular, such growth is governed by those $H \in \mathfrak{S}^{\max}(G)$ satisfying genus$(X_H) = 0$, if such subgroups exist; we refine (49) by defining

$$\mathfrak{S}(G, g) := \{H \in \mathfrak{S}(G) : \text{ genus}(X_H) = g\}.$$

In case $\mathfrak{S}(G, 0) \neq \emptyset$, (57) leads us to the definitions

$$d_{\min}(G, 0) := \min\{d_H : H \in \mathfrak{S}(G, 0)\},$$
$$\mathfrak{S}_{\min}(G, 0) := \{H \in \mathfrak{S}(G, 0) \text{ and } d_H = d_{\min}(G, 0)\}.$$

In our case of the group G appearing in Theorem 4.11, a computation shows that, for each prime $\ell \ge 5$ and each $H \in \mathfrak{S}^{\max}(\ell)$ (see Remark 4.13), the

modular curve $X_{\tilde{G}\cap\tilde{H}}$ has genus at least one. A bit more computation shows that $d_{\min}(G,0)=3$ and

$$\mathfrak{S}_{\min}(G,0)=\{G_{2,1},G_{6,1},G_{9,1},G_{18,1}\}$$

(see Table 5). Finally, by considering the divisor $\mathrm{div}(j_{\mathcal{E}})$, it is straightforward to verify that $j_{\mathcal{E}}(t)$ is not of the form $P\left(\frac{at+b}{ct+d}\right)$ for any $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in \mathrm{GL}_2(\mathbb{Q})$ and any $P(x)\in\mathbb{Z}[x]$. Thus, the above analysis leads to the following second theorem. We define the rational functions

$$t_2(u):=\frac{3u^2+1}{u(u^2+3)},\quad t_6(u):=u^3+1,\quad t_9(u):=1/u^3,\quad t_{18}(u):=\frac{1}{u^3-1}, \tag{58}$$

and the elliptic curve

$$\mathcal{E}:\ y^2=x^3-\frac{108(t^2-1)(t^2-9)^3}{(t^4+18t^2-27)^2}x-\frac{432(t^2-1)(t^2-9)^3}{(t^4+18t^2-27)^2}. \tag{59}$$

Theorem 4.14. *Let $G(6)\subseteq \mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z})$ be the index eight subgroup defined by* (51) *and let $G=\pi^{-1}_{\mathrm{GL}_2}(G(6))$ be the associated open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$. Let $\mathcal{E}$ be the elliptic curve over $\mathbb{Q}(t)$ defined by* (59) *and define the corresponding finite subset $B_{\mathcal{E}}\subset\mathbb{Q}$ by* (53)*. We have*

(1) *For any $t_0\in\mathbb{Q}-B_{\mathcal{E}}$, the specialized curve $\mathcal{E}_{t_0}$ satisfies*

$$\rho_{\mathcal{E}_{t_0}}(G_{\mathbb{Q}})\dot{\subsetneq}G.$$

(2) *For any $\varepsilon>0$, the truncated exceptional set $\mathcal{S}(T)$, defined in* (55)*, satisfies*

$$|\mathcal{S}(T)|=CT^{2/3}+O_{\varepsilon}(T^{\varepsilon}),$$

for some constant $C>0$. More precisely, we have

$$\mathcal{S}(T)=\mathcal{S}'(T)\cup\bigcup_{i\in\{2,6,9,18\}}\left\{t_0\in\mathbb{Q}-B_{\mathcal{E}}:\begin{array}{c}H(t_0)\le T,\ t_0=t_i(u_0)\\ \text{for some } u_0\in\mathbb{Q}\end{array}\right\}, \tag{60}$$

where $t_2(u),t_6(u),t_9(u),t_{18}(u)\in\mathbb{Q}(u)$ are as in (58) *and the set $\mathcal{S}'(T)$ satisfies $|\mathcal{S}'(T)|=O_{\varepsilon}(T^{\varepsilon})$.*

(3) *In particular, we have*

$$\lim_{T\to\infty}\frac{\left|\left\{t_0\in\mathbb{Q}-B_{\mathcal{E}}:H(t_0)\le T \text{ and } \mathcal{E}_{t_0} \text{ is a } G\text{-Serre curve}\right\}\right|}{\left|\{t_0\in\mathbb{Q}-B_{\mathcal{E}}:H(t_0)\le T\}\right|}=1,$$

i.e. almost all specializations of $\mathcal{E}$ are G-Serre curves.

Remark 4.15. Part (3) of Theorem 4.11 follows immediately from part (2) and (54). It is also is a special case of [17, Theorem 2.11], the relevance to this paper being (60), which highlights the involvement of non-abelian entanglement modular curves in this problem, since $t_6(u)$ (resp. $t_{18}(u)$) corresponds to the

forgetful map associated to the curve $X_{G_6\cap G}$ (resp. the curve $X_{G_{18}}$) featured in Theorem 1.8:

$$\begin{array}{ccccccc} & & & \overset{\text{forgetful map}}{\curvearrowright} & & & \\ X_{G_6\cap G} & \xrightarrow{\simeq} & \mathbb{P}^1_{\mathbb{Q}}(u) & \xrightarrow{t_6} & \mathbb{P}^1_{\mathbb{Q}}(t) & \xrightarrow{\simeq} & X_G, \\ X_{G_{18}} & \xrightarrow{\simeq} & \mathbb{P}^1_{\mathbb{Q}}(u) & \xrightarrow{t_{18}} & \mathbb{P}^1_{\mathbb{Q}}(t) & \xrightarrow{\simeq} & X_G. \\ & & & \underset{\text{forgetful map}}{\curvearrowright} & & & \end{array}$$

In particular, we see that non-abelian entanglement groups arise naturally in the problem of determining and counting elliptic curves over $\mathbb{Q}$ for which $\rho_E(G_{\mathbb{Q}}) \dot{\subseteq} G$ is as large as possible, given the constraints dictated by the Kronecker-Weber theorem.

5. An infinite family of D_6-entanglements

In this section, we exhibit an infinite family of D_6-entanglements, which in particular demonstrates that, for fixed $G_0 \in \mathcal{G}_{\text{non-ab}}(0)$, the set

$$\{m_{\mathrm{GL}_2}(G) : G \in \mathcal{G}_{\text{non-ab}}(0),\ G \doteq_{\mathrm{SL}_2} G_0\} \tag{61}$$

is in general unbounded. First, let $G_3 \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ be defined by

$$G_3 := \left\{ g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : \pi_3(g) \in \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \right\},$$

where here and in what follows we denote by $\pi_m : \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ the canonical projection map. Next, fix an arbitrary fundamental discriminant $D \in \mathbb{Z}$ and define

$$\chi_D : \mathrm{GL}_2(\hat{\mathbb{Z}}) \longrightarrow \{\pm 1\}, \qquad \chi_D(g) := \left(\frac{D}{\det g}\right).$$

We fix isomorphisms

$$\pi_3(G_3) \simeq S_3 \times \{\pm 1\}, \quad \pi_2(G_3) \simeq S_3, \tag{62}$$

and define the fibering maps ψ_3 and ψ_D by

$$\psi_3 : G_3 \xrightarrow{\pi_3} \pi_3(G_3) \xrightarrow{\simeq} S_3 \times \{\pm 1\}$$

$$\psi_D : G_3 \xrightarrow{\pi_2\times\chi_D} \pi_2(G_3) \times \{\pm 1\} \xrightarrow{\simeq} S_3 \times \{\pm 1\};$$

we note that ψ_D is surjective, provided $D \neq 1$. Finally, we define the open subgroup $G_{6,D} \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ by

$$G_{6,D} := \{g \in G_3 : \psi_3(g) = \psi_D(g)\}.$$

It is straightforward to see that, under (62), we have

$$\psi_3\left(G_3 \cap \mathrm{SL}_2(\hat{\mathbb{Z}})\right) = A_3 \times \{\pm 1\},$$
$$\psi_D\left(G_3 \cap \mathrm{SL}_2(\hat{\mathbb{Z}})\right) = S_3 \times \{1\},$$

and it follows from this that

$$G_{6,D} \cap \mathrm{SL}_2(\hat{\mathbb{Z}}) = \psi_3|^{-1}_{\mathrm{SL}_2(\hat{\mathbb{Z}})}(A_3 \times \{1\}) \cap \psi_D|^{-1}_{\mathrm{SL}_2(\hat{\mathbb{Z}})}(A_3 \times \{1\}).$$

Thus, the groups $G_{6,D}$ all have SL_2-level 6. Since the GL_2-level of $G_{6,D}$ is $\mathrm{lcm}\,(6, |D|)$, this example demonstrates that the set (61) is indeed unbounded. Furthermore, we note that $-I \notin G_{6,D}$, and that the group $\tilde{G}_{6,D}$ has level 6. Since this group does not depend on D, let us denote it by $\tilde{G}_6$.

Under what conditions do we have $\rho_E(G_K) \dot{\subseteq} G_{6,D}$? Define the map

$$\eta : \pi_3(G_3) \longrightarrow \{\pm 1\}, \qquad \eta\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right) = a \in (\mathbb{Z}/3\mathbb{Z})^\times \simeq \{\pm 1\}.$$

Assume for simplicity that

$$\mu_3 \not\subseteq K, \qquad \sqrt{D} \notin K(\mu_3). \tag{63}$$

Then, for an appropriate choice of the isomorphism $\pi_3(G) \simeq S_3 \times \{\pm 1\}$ in (62), we have that for any elliptic curve E over K, $\rho_E(G_K) \dot{\subseteq} G_{6,D}$ if and only if E admits a K-rational isogeny of degree 3 and also satisfies the three conditions

$$K(\mu_3) \subseteq K(E[2]), \quad K(E[3]) = K(E[2], \sqrt{D}), \quad K(E[3])^{\ker \eta} = K(\sqrt{D}).$$

Thus, setting $m_D := \mathrm{lcm}\,(2, |D|)$, we have that, under the hypothesis (63), elliptic curves E/K with $\rho_E(G_K) \dot{\subseteq} G_{6,D}$ have the entanglement $K(E[3]) \subseteq K(E[m_D])$. Furthermore, since generically we have

$$\mathrm{Gal}(K(E[3])/K) \simeq \pi_3(G_3) \simeq S_3 \times \{\pm 1\} \simeq D_6,$$

this is an example of a D_6-entanglement.

For each fundamental discriminant D, there is an elliptic curve $\mathcal{E}_D$ over $\mathbb{Q}(t)$ satisfying $\rho_{\mathcal{E}}(G_{\mathbb{Q}(t)}) \doteq G_{6,D}$. To describe it, we first define

$$A(t) := -3t^9(t^3 - 2)(t^3 + 2)^3(t^3 + 4)$$
$$B(t) := -2t^{12}(t^3 + 2)^4(t^4 - 2t^3 + 4t - 2) \cdot (t^8 + 2t^7 + 4t^6 + 8t^5 + 10t^4 + 8t^3 + 16t^2 + 8t + 4),$$

and then set

$$\mathcal{E}_D : y^2 = x^3 + D^2A(t)x + D^3B(t). \tag{64}$$

The discriminant $\Delta_{\mathcal{E}_D}(t)$ and j-invariant $j_{\mathcal{E}_D}(t)$ are given by

$$\Delta_{\mathcal{E}_D}(t) = 2^{12}3^3D^6t^{24}(t+1)^6(t^2-t+1)^6(t^3+2)^8,$$
$$j_{\mathcal{E}_D}(t) = \frac{-27t^3(t^3-2)^3(t^3+2)(t^3+4)^3}{(t+1)^6(t^2-t+1)^6}.$$

By [9, Theorem 1.6], the elliptic curve $\mathcal{E}_1/\mathbb{Q}(t)$ has the property that $\rho_{\mathcal{E}_1,6}(G_{\mathbb{Q}(t)})$ belongs to one of the two index two subgroups of the level 6 group $\tilde{G}_6$ corresponding to elliptic curves $E/\mathbb{Q}$ satisfying $\mathbb{Q}(E[2]) = \mathbb{Q}(E[3])$; its twist $\mathcal{E}_{-3}$ by $\mathbb{Q}(\sqrt{-3})$ has mod 6 image belonging to the other such index two subgroup. Given this, it is straightforward to verify (e.g. by explicitly computing a Galois-stable cyclic subgroup $\mathcal{C} \subseteq \mathcal{E}_D[3]$) that $\mathcal{E}_D$ admits a $\mathbb{Q}(t)$-rational isogeny of degree three and that the following three conditions hold.

$$\mathbb{Q}(t)(\mu_3) \subseteq \mathbb{Q}(t)(\mathcal{E}_D[2])$$
$$\mathbb{Q}(t)(\mathcal{E}_D[3]) = \mathbb{Q}(t)\left(\mathcal{E}_D[2], \sqrt{D}\right)$$
$$\mathbb{Q}(t)(\mathcal{E}_D[3])^{\ker\eta} = \mathbb{Q}(t)\left(\sqrt{D}\right)$$

Thus, $\rho_{\mathcal{E}_D}(G_{\mathbb{Q}(t)}) \dot{\subseteq} G_{6,D}$, and by examining specializations, we may see that in fact $\rho_{\mathcal{E}_D}(G_{\mathbb{Q}(t)}) \doteq G_{6,D}$.

Remark 5.1. A curious feature of the underlying group $\tilde{G}_6$ in the above example is that, given any elliptic curve E over $\mathbb{Q}$ for which $\rho_E(G_{\mathbb{Q}}) \subseteq \tilde{G}_6$, we have $-I \notin \rho_E(G_{\mathbb{Q}})$, in spite of the fact that $-I \in \tilde{G}_6$. The reason for this is as follows: a computation shows that

$$-I \notin \left[\tilde{G}_6(6), \tilde{G}_6(6)\right].$$

In the language of Section 4, this implies that there are no commutator-thick subgroups of $\tilde{G}_6$ that contain $-I$. In particular, since $\rho_E(G_{\mathbb{Q}})$ is commutator-thick (see (46)), we conclude that $-I \notin \rho_E(G_{\mathbb{Q}})$. By the same reasoning, the same conclusion holds for the group G appearing in Theorem 4.11.

Remark 5.2. In the language of Section 4, the collection of groups

$$\{G_{6,D} \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}}) : D \text{ is a fundamental discriminant}\}$$

is exactly the set of all commutator-maximal subgroups of $\tilde{G}_6$. Thus, in case $K = \mathbb{Q}$, any $\tilde{G}_6$-Serre curve E over $\mathbb{Q}$ satisfies $\rho_E(G_{\mathbb{Q}}) = G_{6,D}$ for some fundamental discriminant D. In the language of [10], the quadratic entanglement $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(E[3]) \cap \mathbb{Q}(E[|D|])$ is an *explained* entanglement, in the sense that it is forced by the Kronecker-Weber Theorem. Thus, this example is similar in nature to the set of all index two "Serre subgroups" described in [25, Remark 1.3]; the reason we include it here is to emphasize that the same "unbounded GL_2-level with fixed SL_2-level" phenomenon can happen when considering non-abelian entanglement groups.

References

[1] APOSTOL, T. Introduction to Analytic Number Theory. Undergraduate Texts in Mathematics. *Springer-Verlag, New York-Heidelberg* (1976). MR0434929, Zbl 1154.11300. 222

[2] BOSMA, W.; CANNON, J.; PLAYOUST, C. The Magma algebra system. I. The user language. Computational algebra and number theory (London, 1993). *J. Symbolic Comput.* **24** (1997), No. 3-4, 235–265. MR1484478, Zbl 0898.68039. 191, 205

[3] BOURDON, A.; GILL, D.; ROUSE, J.; WATSON, L. Odd degree isolated points on $X_1(N)$ with rational j-invariant. Preprint, available at `https://arxiv.org/abs/2006.14966` 210

[4] BRAU, J. Selmer groups of elliptic curves and Galois representations. Ph.D. Dissertation, University of Cambridge (2014). 188

[5] BRAU, J.; JONES, N. Elliptic curves with 2-torsion contained in the 3-torsion field. *Proc. Amer. Math. Soc.* **144** (2016), 925–936. MR3447646, Zbl 1333.11050. 183, 187, 205

[6] CAMPAGNA, F.; PENGO, R. Entanglement in the family of division fields of elliptic curves with complex multiplication. Preprint, available at `https://arxiv.org/abs/2006.00883` 183

[7] COJOCARU, A.C.; GRANT, D.; JONES, N. One-parameter families of elliptic curves over $\mathbb{Q}$ with maximal Galois representations. *Proc. Lond. Math. Soc.* **103** (2011), No. 3, 654–675. MR2837018, Zbl 1284.11090. 222, 223

[8] CUMMINS, C. J.; PAULI, S. Congruence subgroups of PSL(2, $\mathbb{Z}$) of genus less than or equal to 24. *Exp. Math.* **12** (2003), No. 2, 243–255. MR2016709, Zbl 1060.11021. 192

[9] DANIELS, H.; LOZANO-ROBLEDO, Á. Coincidences of division fields. Preprint, available at `https://arxiv.org/abs/1912.05618` 183, 227

[10] DANIELS, H.; MORROW, J. S. A group theoretic perspective on entanglements of division fields. Preprint, available at `https://arxiv.org/abs/2008.09886` 183, 206, 227

[11] DELIGNE, P.; RAPOPORT, M. Les schémas de modules de courbes elliptiques. Modular Functions of One Variable II (Antwerp, 1972). *Lecture Notes in Mathematics* **349** (1973) 143–316. MR0337993, Zbl 0281.14010. 185

[12] DENNIN, J. B. The genus of subfields of $K(n)$. *Proc. Amer. Math. Soc.* **51** (1975) 282–288. MR384698 (52 #5571), Zbl 0313.10022. 192

[13] DOKCHITSER, T.; DOKCHITSER, V. Surjectivity of mod 2^n representations of elliptic curves. *Math. Z.* **272** (2012) 961–964. MR2995149, Zbl 1315.11046. 221

[14] ELKIES, N. Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9. Preprint, available at `https://arxiv.org/abs/math/0612734`

[15] GRANT, D. A formula for the number of elliptic curves with exceptional primes. *Compos. Math.* **122** (2000), No. 2, 151–164. MR1775416, Zbl 1011.11039. 222

[16] JONES, N. Almost all elliptic curves are Serre curves. *Trans. Amer. Math. Soc.* **362** (2010), No. 3, 1547–1570. MR2563740, Zbl 1204.11088. 221

[17] JONES, N. GL_2-representations with maximal image. *Math. Res. Lett.* **22** (2015), No. 3, 803–839. MR3350106, Zbl 1380.11080. 217, 218, 220, 222, 224

[18] LANG, S.; TROTTER, H. Frobenius distribution in GL_2 extensions. Distribution of Frobenius automorphisms in GL2-extensions of the rational numbers. *Lecture Notes in Math.* **504**, *Springer-Verlag, Berlin-New York* (1976). MR0568299, Zbl 0329.12015. 219

[19] MAZUR, B. Rational points on modular curves. Modular functions of one variable, V, Proc. Second Internat. Conf. (Bonn, 1976). *Lecture Notes in Math.* **601** (1977) 107–148. MR0450283, Zbl 0357.14005. 183

[20] MORROW, J. S. Composite images of Galois for elliptic curves over Q and entanglement fields. *Math. Comp.* **88** (2019), No. 319, 2389–2421. MR3957898, Zbl 1470.11154. 183, 188

[21] RIBET, K. Galois action on division points of Abelian varieties with real multiplications. *Amer. J. Math.* **98** (1976), No. 3, 751–804. MR0457455, Zbl 0348.14022. 192

[22] ROUSE, J.; ZUREICK-BROWN, D. Elliptic curves over Q and 2-adic images of Galois. *Res. Number Theory* **1** (2015), Paper No. 12, 34 pp. MR3500996, Zbl 1397.11095. 183, 185, 206

[23] SERRE, J-P. Lectures on the Mordell-Weil Theorem. Aspects of Mathematics. *Friedr. Vieweg & Sohn, Braunschweig* (1989). MR1002324, Zbl 0676.14005. 222, 223

[24] SERRE, J-P. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.* **15** (1972) 259–331. MR0387283, Zbl 0235.14012.

[25] SUTHERLAND, A.; ZYWINA, D. Modular curves of prime-power level with infinitely many rational points. *Algebra and Number Theory* **11** (2017), No. 5, 1199–1229. MR3671434, Zbl 1374.14022. 183, 206, 216, 217, 221, 227

[26] THE SAGE DEVELOPERS. SageMath, the Sage Mathematics Software System (Version 9.0). `https://www.sagemath.org`. 2020. 191, 206

[27] THOMPSON, J. G. A finiteness theorem for subgroups of PSL(2, $\mathbb{R}$) which are commensurable with PSL(2, $\mathbb{Z}$). Santa Cruz Conference on Finite Groups (Santa Cruz, CA, 1979), 533–555, Proc. Symp. Pure Math. **37**, *Amer. Math. Soc., Providence, RI* (1980). MR0604632, Zbl 0448.20044. 192

[28] ZOGRAF, P. A spectral proof of Rademacher's conjecture for congruence subgroups of the modular group. *J. Reine Angew. Math.* **414** (1991) 113–116. MR1092625, Zbl 0709.11031. 192

[29] ZYWINA, D. Computing actions on cusp forms. Preprint, available at `https://arxiv.org/abs/2001.07270` 206

[30] ZYWINA, D. On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$. Preprint, available at `https://arxiv.org/abs/1508.07660` 192, 210, 211

(Nathan Jones) DEPARTMENT OF MATHEMATICS, STATISTICS AND COMPUTER SCIENCE, UNIVERSITY OF ILLINOIS AT CHICAGO, 851 S MORGAN ST, 322 SEO, CHICAGO, IL 60607, USA
`ncjones@uic.edu`

(Ken McMurdy) DEPARTMENT OF MATHEMATICS, RAMAPO COLLEGE OF NEW JERSEY, 505 RAMAPO VALLEY ROAD, MAHWAH, NJ 07430, USA
`kmcmurdy@ramapo.edu`

This paper is available via `http://nyjm.albany.edu/j/2022/28-9.html`.