ALGEBRAIC CURVES UNIFORMIZED BY CONGRUENCE SUBGROUPS OF TRIANGLE GROUPS

PETE L. CLARK AND JOHN VOIGHT

Abstract. We construct certain subgroups of hyperbolic triangle groups which we call "congruence" subgroups. These groups include the classical congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, Hecke triangle groups, and 19 families of arithmetic triangle groups associated to Shimura curves. We determine the field of moduli of the curves associated to these groups and thereby realize the groups $\mathrm{PSL}_2(\mathbb{F}_q)$ and $\mathrm{PGL}_2(\mathbb{F}_q)$ regularly as Galois groups.

Contents

1. Introduction

Motivation. The rich arithmetic and geometric theory of classical modular curves, quotients of the upper half-plane by subgroups of $\mathrm{SL}_2(\mathbb{Z})$ defined by congruence conditions, has fascinated mathematicians since at least the nineteenth century. One can see these curves as special cases of several distinguished classes of curves. Fricke and Klein [25] investigated curves obtained as quotients by Fuchsian groups arising from unit groups of certain quaternion algebras, now called arithmetic groups. Later, Hecke [32] investigated his triangle groups, arising from reflections in the sides of a hyperbolic triangle with angles $0, \pi/2, \pi/n$ for $n \geq 3$. Then in the 1960s, amidst a flurry of activity studying the modular curves, Atkin and Swinnerton-Dyer [1] pioneered the study of noncongruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. In this paper, we consider a further direction: we introduce a class of curves arising from certain subgroups of hyperbolic triangle groups. These curves appear to share many appealing properties in common with classical modular curves despite the fact that their uniformizing Fuchsian groups are in general *not* arithmetic groups.

Date: August 4, 2022.

To motivate the definition of this class of curves, we begin with the modular curves, defined as follows. Let p be prime and let $\Gamma(p) \subseteq \mathrm{PSL}_2(\mathbb{Z}) = \Gamma(1)$ be the subgroup of matrices congruent to (plus or minus) the identity modulo p. Then $\Gamma(p)$ acts on the completed upper half-plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$, and the quotient $X(p) = \Gamma(p)\backslash\mathcal{H}^*$ can be given the structure of a Riemann surface. The subgroup $G = \Gamma(1)/\Gamma(p) \subseteq \mathrm{Aut}(X(p))$ satisfies $G \simeq \mathrm{PSL}_2(\mathbb{F}_p)$ and the natural map $j\colon X(p) \to X(p)/G \simeq \mathbb{P}^1_{\mathbb{C}}$ is a Galois branched cover ramified only above the points $0, 1728, \infty$.

So we are led to study the class of (smooth, projective) curves X over $\mathbb{C}$ with the property that there exists a subgroup $G \subseteq \mathrm{Aut}(X)$ with $G \simeq \mathrm{PSL}_2(\mathbb{F}_q)$ or $G \simeq \mathrm{PGL}_2(\mathbb{F}_q)$ for a prime power q such that the map $X/G \simeq \mathbb{P}^1$ and the map $X \to X/G$ is a Galois branched cover ramified at exactly three points.

Belyĭ [4, 5] proved that a curve X over $\mathbb{C}$ can be defined over the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ if and only if X admits a Belyĭ map, a nonconstant morphism $f\colon X \to \mathbb{P}^1_{\mathbb{C}}$ unramified away from $0, 1, \infty$. So, on the one hand, three-point branched covers are indeed ubiquitous. On the other hand, there are only *finitely* many curves X up to isomorphism of given genus $g \geq 2$ which admit a *Galois* Belyĭ map (Remark 3.10). We call a curve which admits a Galois Belyĭ map a Galois Belyĭ curve. In other contexts, Galois Belyĭ curves are also called quasiplatonic surfaces [26, 88], owing to their connection with the Platonic solids, or curves with many automorphisms because their locus is equivalently characterized on the moduli space $\mathcal{M}_g(\mathbb{C})$ of curves of genus g by the condition that the function $[C] \mapsto \#\,\mathrm{Aut}(C)$ attains a strict local maximum. For example, the Hurwitz curves, those curves X with maximal automorphism group $\#\,\mathrm{Aut}(X) = 84(g-1)$ for their genus g, are Galois Belyĭ curves, as are the Fermat curves $x^n + y^n = z^n$ for $n \geq 3$. (Part of the beauty of this subject is that the same object can be viewed from many different perspectives, and the natural name for an object depends on this view.)

So Galois Belyĭ curves with Galois group $G = \mathrm{PSL}_2(\mathbb{F}_q)$ and $G = \mathrm{PGL}_2(\mathbb{F}_q)$ generalize the classical modular curves and bear further investigation. In this article, we study the existence of these curves, and we then consider one of the most basic properties about them: the fields over which they are defined.

Existence. To state our first result concerning existence we use the following notation. For $s \in \mathbb{Z}_{\geq 2}$, let $\zeta_s = \exp(2\pi i/s)$ and $\lambda_s = \zeta_s + 1/\zeta_s = 2\cos(2\pi/s)$; by convention we let $\zeta_\infty = 1$ and $\lambda_\infty = 2$.

Let $a, b, c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$ satisfy $a \leq b \leq c$. Then we have the following tower of fields:

(*)
$$\begin{array}{c} F(a,b,c) = \mathbb{Q}(\lambda_{2a}, \lambda_{2b}, \lambda_{2c}) \\ | \\ E(a,b,c) = \mathbb{Q}(\lambda_a, \lambda_b, \lambda_c, \lambda_{2a}\lambda_{2b}\lambda_{2c}) \\ | \\ D(a,b,c) = \mathbb{Q}(\lambda_a, \lambda_b, \lambda_c) \\ | \\ \mathbb{Q} \end{array}$$

We have $E(a,b,c) \subseteq F(a,b,c)$ since $\lambda_{2a}^2 = \lambda_a + 2$ (the half-angle formula), and consequently this extension has degree at most 4 and exponent at most 2. Accordingly, a prime $\mathfrak{p}$ of $E(a,b,c)$ (by which we mean a nonzero prime ideal in the ring of integers of $E(a,b,c)$) that is unramified in $F(a,b,c)$ either splits completely or has inertial degree 2.

The triple (a,b,c) is hyperbolic if

$$\chi(a,b,c) = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1 < 0.$$

Our first main result is as follows.

Theorem A. *Let (a,b,c) be a hyperbolic triple with $a,b,c \in \mathbb{Z}_{\geq 2}$. Let $\mathfrak{p}$ be a prime of $E(a,b,c)$ with residue field $\mathbb{F}_\mathfrak{p}$ and suppose $\mathfrak{p} \nmid 2abc$. Then there exists a G-Galois Belyĭ map*

$$X(a,b,c;\mathfrak{p}) \to \mathbb{P}^1$$

with ramification indices (a,b,c), where

$$G = \begin{cases} \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p}), & \text{if } \mathfrak{p} \text{ splits completely in } F(a,b,c); \\ \mathrm{PGL}_2(\mathbb{F}_\mathfrak{p}), & \text{otherwise.} \end{cases}$$

We have stated Theorem A in a simpler form; for a more general statement, including the case when $\mathfrak{p} \mid 2$ or when one or more of a,b,c is equal to ∞, see Theorem 9.1. In some circumstances (depending on a norm residue symbol), one can also take primes dividing abc (see Remark 5.24).

Theorem A generalizes work of Lang, Lim, and Tan [40] who treat the case of Hecke triangle groups using an explicit presentation of the group (see also Example 10.4), and work of Marion [47] who treats the case a,b,c prime. This also complements celebrated work of Macbeath [43], providing an explicit way to distinguish between projective two-generated subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ by a simple splitting criterion. Theorem A overlaps with work of Conder, Potočnik, and Širáň [16] (they also give several other references to work of this kind), and more recent work of Broughton [9].

The construction of Galois Belyĭ maps in Theorem A arises from another equivalent characterization of Galois Belyĭ curves (of genus ≥ 2) as compact Riemann surfaces of the form $\Gamma\backslash\mathcal{H}$, where Γ is a finite index normal subgroup of the hyperbolic triangle group

$$\overline{\Delta}(a,b,c) = \langle \bar{\delta}_a, \bar{\delta}_b, \bar{\delta}_c \mid \bar{\delta}_a^a = \bar{\delta}_b^b = \bar{\delta}_c^c = \bar{\delta}_a\bar{\delta}_b\bar{\delta}_c = 1 \rangle \subset \mathrm{PSL}_2(\mathbb{R})$$

for some $a,b,c \in \mathbb{Z}_{\geq 2}$, where by convention we let $\bar{\delta}_\infty^\infty = 1$. (See Sections 1–2 for more detail. The bars may seem heavy-handed here, but signs play a delicate and somewhat important role in the development, so we include this as part of the notation for emphasis.) Phrased in this way, Theorem A asserts the existence of a normal subgroup

$$\overline{\Delta}(\mathfrak{p}) = \overline{\Delta}(a,b,c;\mathfrak{p}) \trianglelefteq \overline{\Delta}(a,b,c) = \overline{\Delta}$$

with quotient $\overline{\Delta}/\overline{\Delta}(\mathfrak{p}) = G$ as above. In a similar way, one obtains curves $X_0(a,b,c;\mathfrak{p})$ by considering the quotient of $X(a,b,c;\mathfrak{p})$ by the subgroup of upper-triangular matrices—these curves are analogous to the classical modular curves $X_0(p)$ as quotients of $X(p)$.

Arithmeticity. A Fuchsian group is arithmetic if it is commensurable with the group of units of reduced norm 1 of a maximal order in a quaternion algebra. A deep theorem of Margulis [46] states that a Fuchsian group is arithmetic if and only if it is of infinite index in its commensurator. By work of Takeuchi [80], only finitely many of the groups $\Delta(a,b,c)$ are arithmetic: in these cases, the curves $X(a,b,c;\mathfrak{p})$ are Shimura curves (arising from full congruence subgroups) and canonical models were studied by Shimura [65] and Deligne [19]. Indeed, the curves $X(2,3,\infty;p)$ are the classical modular curves $X(p)$ and the Galois Belyĭ map $j\colon X(p)\to\mathbb{P}^1$ is associated to the congruence subgroup $\Gamma(p)\subseteq \mathrm{PSL}_2(\mathbb{Z})$. Several other arithmetic families of Galois Belyĭ curves have seen more detailed study, most notably the family $X(2,3,7;\mathfrak{p})$ of Hurwitz curves. (The arithmetic triangle groups are considered as examples given by Shimura [65, Example 3.18].) Aside from these finitely many triples, the triangle group $\Delta=\Delta(a,b,c)$ is *not* arithmetic, and our results can be seen as a generalization in this nonarithmetic context.

However, we still have an embedding inside an arithmetic group Γ, following Takeuchi [80] and later work of Tretkoff (née Cohen) and Wolfart [12]: our curves are obtained via pullback

$$\begin{array}{ccc} \overline{\Delta}(\mathfrak{p})\backslash\mathcal{H} & \hookrightarrow & \Gamma(\mathfrak{p})\backslash\mathcal{H}^s \\ \downarrow & & \downarrow \\ \mathbb{P}^1=\overline{\Delta}\backslash\mathcal{H} & \hookrightarrow & \Gamma(1)\backslash\mathcal{H}^s \end{array} \tag{1.1}$$

from a branched cover of quaternionic Shimura varieties, and this promises further arithmetic applications. Accordingly, we call the subgroups $\overline{\Delta}(a,b,c;\mathfrak{p})$ we construct congruence subgroups of $\overline{\Delta}$ in analogy with the classical case of modular curves, since they arise from certain congruence conditions on matrix entries, and we call the curves $X(a,b,c;\mathfrak{p})$ and their cousins $X_0(a,b,c;\mathfrak{p})$ triangle modular curves. (In some contexts, the term *congruence* is used only for arithmetic groups; we propose the above extension of this terminology to non-arithmetic groups.) For a fuller discussion of the arithmetic cases of Theorem A, see Example 10.3.

Field of definition. Our second main result studies fields of definition. The modular curve $X(p)$, a Riemann surface defined over $\mathbb{C}$, has a model as an algebraic curve defined over $\mathbb{Q}$; we seek a similar (nice, explicit) result for our class of curves. For a curve X defined over $\mathbb{C}$, the field of moduli $M(X)$ of X is the fixed field of the group $\{\sigma\in\mathrm{Aut}(\mathbb{C})\colon X^\sigma\simeq X\}$, where X^σ is the base change of X by the automorphism $\sigma\in\mathrm{Aut}(\mathbb{C})$. A field of definition for X clearly contains the field of moduli of X, so if X has a (unique) minimal field of definition F, then F is necessarily equal to the field of moduli.

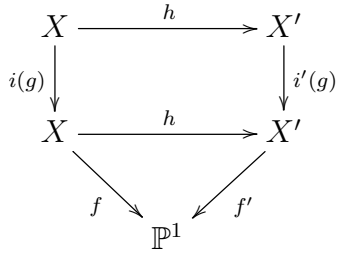
We will need two refinements of this notion. First, we define the notion for branched covers. We say that two Belyĭ maps $f\colon X\to\mathbb{P}^1$ and $f'\colon X'\to\mathbb{P}^1$ are isomorphic (over $\mathbb{C}$ or $\overline{\mathbb{Q}}$) if there exists an isomorphism $h\colon X\xrightarrow{\sim}X'$ that respects the branched covers, i.e., such that $f=f'\circ h$. We define the field of moduli $M(X,f)$ of a Belyĭ map analogously. A Galois Belyĭ map can always be defined over its field of moduli (Lemma 4.1) as mere cover.

But we will also want to keep track of the Galois automorphisms of the branched cover. For a finite group G, a G-Galois Belyĭ map is a Belyĭ map $f\colon X\to\mathbb{P}^1$ equipped with an isomorphism $i\colon G\xrightarrow{\sim}\mathrm{Gal}(f)$ between G and the Galois (monodromy) group of f, and an

isomorphism of G-Galois Belyĭ maps is an isomorphism h of Belyĭ maps that identifies i with i', i.e.,

$$h(i(g)x) = i'(g)h(x) \text{ for all } g \in G \text{ and } x \in X(\mathbb{C})$$

so the diagram



commutes. We define the field of moduli $M(X, f, G)$ of a G-Galois Belyĭ map f accordingly. For example, we have

$$M(X(p), j, \mathrm{PSL}_2(\mathbb{F}_p)) = \mathbb{Q}(\sqrt{p^*}) \quad \text{where } p^* = (-1)^{(p-1)/2}p$$

(see Example 4.6). A G-Galois Belyĭ map f can be defined over its field of moduli $M(X, f, G)$ if G has trivial center $Z(G) = \{1\}$ and $G = \mathrm{Aut}(X)$ (see Lemma 4.3).

On the one hand, we observe (Remark 4.8) that for any number field K there is a G-Galois Belyĭ map f for some finite group G such that the field of moduli of (X, f, G) contains K. On the other hand, we will show that our curves have quite nice fields of definition. (See also work of Streit and Wolfart [75] who consider the case $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$.)

We need one further bit of notation. For a prime p and integers $a, b, c \in \mathbb{Z}_{\geq 2}$, let $D_{p'}(a, b, c)$ be the compositum of the fields $\mathbb{Q}(\lambda_s)$ with $s \in \{a, b, c\}$ prime to p. (For example, if all of a, b, c are divisible by p, then $D_{p'}(a, b, c) = \mathbb{Q}$.) Similarly define $F_{p'}(a, b, c)$.

Theorem B. *Let X be a curve of genus $g \geq 2$ and let $f\colon X \to \mathbb{P}^1$ be a G-Galois Belyĭ map with $G \simeq \mathrm{PGL}_2(\mathbb{F}_q)$ or $G \simeq \mathrm{PSL}_2(\mathbb{F}_q)$. Let (a, b, c) be the ramification indices of f.*

Then the following statements hold.

(a) *Let r be the order of* Frob_p *in* $\mathrm{Gal}(F_{p'}(a, b, c)/\mathbb{Q})$. *Then*

$$q = \begin{cases} \sqrt{p^r}, & \text{if } G \simeq \mathrm{PGL}_2(\mathbb{F}_q); \\ p^r, & \text{if } G \simeq \mathrm{PSL}_2(\mathbb{F}_q). \end{cases}$$

(b) *The map f as a mere cover is defined over its field of moduli $M(X, f)$. Moreover, $M(X, f)$ is an extension of $D_{p'}(a, b, c)^{\langle \mathrm{Frob}_p \rangle}$ of degree $d_{(X,f)} \leq 2$. If $a = 2$ or q is even, then $d_{(X,f)} = 1$.*

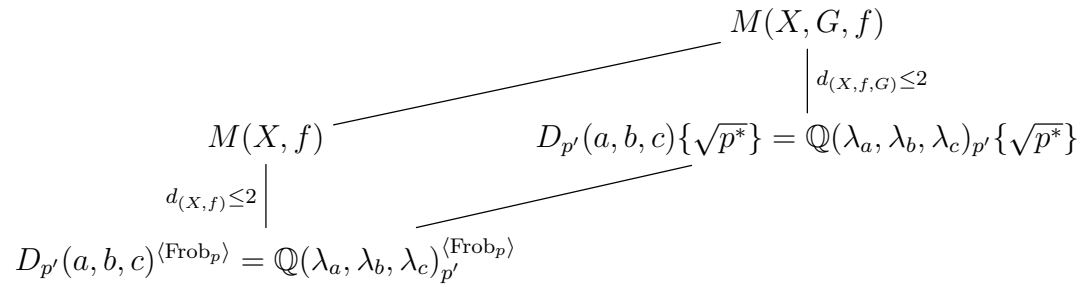
(c) *The map f as a G-Galois Belyĭ map is defined over its field of moduli $M(X, f, G)$. Let*

$$D_{p'}(a, b, c)\{\sqrt{p^*}\} = \begin{cases} D_{p'}(a, b, c)(\sqrt{p^*}), & \text{if } p \mid abc,\ pr \text{ is odd, and } G \simeq \mathrm{PSL}_2(\mathbb{F}_q); \\ D_{p'}(a, b, c) & \text{otherwise.} \end{cases}$$

Then $M(X, f, G)$ is an extension of $D_{p'}(a, b, c)\{\sqrt{p^*}\}$ of degree $d_{(X,f,G)} \leq 2$. If q is even or $p \mid abc$ or $G \simeq \mathrm{PGL}_2(\mathbb{F}_q)$, then $d_{(X,f,G)} = 1$.

Not all G-Galois Belyĭ maps with $G \simeq \mathrm{PGL}_2(\mathbb{F}_q)$ or $G \simeq \mathrm{PSL}_2(\mathbb{F}_q)$ arise from the construction in Theorem A, but Theorem B applies to them all: see Remark 10.6.

The various fields of moduli fit into the following diagram.



As a simple special case of Theorem B, we have the following corollary.

Corollary. *Suppose $f\colon X \to \mathbb{P}^1$ is a $\mathrm{PSL}_2(\mathbb{F}_q)$-Galois Belyĭ map with ramification indices $(2,3,c)$ and suppose $p \nmid 6c$ is prime and a primitive root modulo $2c$. Then $q = p^r$ where $r = \phi(2c)/2$ and f is defined over $\mathbb{Q}$. Moreover, the monodromy group $\mathrm{Gal}(f)$ is defined over an at most quadratic extension of $\mathbb{Q}(\lambda_p)$.*

To prove Theorem B, we use a variant of the rigidity and rationality results which arise in the study of the inverse Galois problem [45, 86] and apply them to the groups $\mathrm{PSL}_2(\mathbb{F}_q)$ and $\mathrm{PGL}_2(\mathbb{F}_q)$. We use the classification of subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ generated by two elements provided by Macbeath [43]. The statements $q = \sqrt{p^r}$ and $q = p^r$, respectively, can be found in earlier work of Langer and Rosenberger [41, Satz (4.2)]; our proof follows similar lines. Theorem B generalizes work of Schmidt and Smith [59, Section 3] who consider the case of Hecke triangle groups as well as work of Streit [73] and Džambić [20] who consider Hurwitz groups, where $(a,b,c) = (2,3,7)$.

Composite level. The congruence subgroups so defined naturally extend to composite ideals, and so they form a projective system (Proposition 9.7). For a prime $\mathfrak{p}$ of E and $e \geq 1$, let $P(\mathfrak{p}^e)$ be the group

$$P(\mathfrak{p}^e) = \begin{cases} \mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{p}^e), & \text{if } \mathfrak{p} \text{ splits completely in } F; \\ \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{p}^e), & \text{otherwise} \end{cases}$$

where $\mathbb{Z}_E$ denotes the ring of integers of E. For an ideal $\mathfrak{n}$ of $\mathbb{Z}_E$, let $P(\mathfrak{n}) = \prod_{\mathfrak{p}^e \| \mathfrak{n}} P(\mathfrak{p}^e)$, and let $\widehat{P} = \varprojlim_{\mathfrak{n}} P(\mathfrak{n})$ be the projective limit of $P(\mathfrak{n})$ with respect to the ideals $\mathfrak{n}$ with $\mathfrak{n}$ coprime to $6abc$.

Theorem C. *$\overline{\Delta}(a,b,c) \leq \widehat{P}$ contains a dense subgroup of $\prod_{\mathfrak{p}} \mathrm{PSL}_2(\mathbb{Z}_{E,\mathfrak{p}})$.*

Kucharczyk [38] uses superstrong approximation for thin subgroups of arithmetic groups to prove a version of Theorem C that shows that the closure of the image of $\overline{\Delta}(a,b,c)$ is an open subgroup of $\widehat{P}$, in particular of finite index; our Theorem C is more refined, giving effective control over the closure of the image.

Applications. The construction and analysis of these curves has several interesting applications. Combining Theorems A and B, we see that the branched cover $X(a,b,c;\mathfrak{p}) \to \mathbb{P}^1$ realizes the group $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$ or $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{p})$ regularly over the field $M(X,f,G)$, a small extension of a totally real abelian number field. (See Malle and Matzat [45], Serre [61, Chapters

7–8], and Völklein [86] for more information and groups realized regularly by rigidity and other methods.)

Moreover, the branched covers $X(a,b,c;\mathfrak{p}) \to X(a,b,c)$ have applications in the Diophantine study of generalized Fermat equations. When $c = \infty$, Darmon [17] has constructed a family of hypergeometric abelian varieties associated to the triangle group $\overline{\Delta}(a,b,c)$. The analogous construction when $c \neq \infty$ we believe will likewise have important arithmetic applications. (See also work of Tyszkowska [82], who studies the fixed points of a particular symmetry of $\mathrm{PSL}_2(\mathbb{F}_p)$-Galois Belyĭ curves.)

Finally, it is natural to consider applications to the arithmetic theory of elliptic curves. Every elliptic curve E over $\mathbb{Q}$ is uniformized by a modular curve $X_0(N) \to E$, and the theory of Heegner points govern facets of the arithmetic of E: in particular, it controls the rank of $E(\mathbb{Q})$ when this rank is at most 1. By analogy, we are led to consider those elliptic curves over a totally real field that are uniformized by a curve $X(a,b,c;\mathfrak{p})$—there is some evidence [84] that the images of CM points generate subgroups of rank at least 2.

Organization. The paper is organized as follows. In Sections 2–4, we introduce triangle groups, Belyĭ maps, Galois Belyĭ curves, and fields of moduli. In Section 5, we investigate in detail a construction of Takeuchi, later explored by Cohen and Wolfart, which realizes the curves associated to triangle groups as subvarieties of quaternionic Shimura varieties, and from this modular embedding we define congruence subgroups of triangle groups. We next introduce in Section 6 the theory of weak rigidity which provides the statement of Galois descent we will employ. In Section 7, we set up the basic theory of $\mathrm{PSL}_2(\mathbb{F}_q)$, and in Section 8 we recall Macbeath's theory of two-generated subgroups of $\mathrm{SL}_2(\mathbb{F}_q)$. In Section 9, we put the pieces together and prove Theorems A, B, and C. We conclude in Section 10 with several explicit examples.

The authors would like to thank Henri Darmon, Richard Foote, David Harbater, Hilaf Hasson, Robert Kucharczyk, Jennifer Paulhus, Michael Schein, Jeroen Sijsling, Jürgen Wolfart, and several anonymous referees for very helpful comments and suggestions, as well as Noam Elkies for his valuable comments and encouragement. The second author was supported by an NSF CAREER Award (DMS-1151047).

2. Triangle groups

In this section, we review the basic theory of triangle groups. We refer to Magnus [44, Chapter II] and Ratcliffe [53, §7.2] for further reading.

Let $a,b,c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$ satisfy $a \leq b \leq c$. We say that the triple (a,b,c) is spherical, Euclidean, or hyperbolic according as the quantity

$$\chi(a,b,c) = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1$$

is positive, zero, or negative. The spherical triples are $(2,3,3)$, $(2,3,4)$, $(2,3,5)$, and $(2,2,c)$ with $c \in \mathbb{Z}_{\geq 2}$. The Euclidean triples are $(2,2,\infty)$, $(2,4,4)$, $(2,3,6)$, and $(3,3,3)$. All other triples are hyperbolic.

We associate to a triple (a,b,c) the extended triangle group $\Delta = \Delta(a,b,c)$, the group generated by elements $-1, \delta_a, \delta_b, \delta_c$, with -1 central in Δ, subject to the relations $(-1)^2 = 1$ and

$$\delta_a^a = \delta_b^b = \delta_c^c = \delta_a\delta_b\delta_c = -1; \tag{2.1}$$

by convention we let $\delta_\infty^\infty = -1$. We define the quotient

$$\overline{\Delta} = \overline{\Delta}(a,b,c) = \Delta(a,b,c)/\{\pm 1\}$$

and call $\overline{\Delta}$ a triangle group. We denote by $\bar{\delta}$ the image of $\delta \in \Delta(a,b,c)$ in $\overline{\Delta}(a,b,c)$.

Remark 2.2. Reordering generators permits our assumption that $a \leq b \leq c$ without loss of generality. Indeed, the defining condition $\delta_a\delta_b\delta_c = -1$ is invariant under cyclic permutations so $\Delta(a,b,c) \simeq \Delta(b,c,a) \simeq \Delta(c,a,b)$, and similarly the map which sends a generator to its inverse gives an isomorphism $\Delta(a,b,c) \simeq \Delta(c,b,a)$. The same is true for the quotients $\overline{\Delta}(a,b,c)$.

The triangle groups $\overline{\Delta}(a,b,c)$ with (a,b,c) earn their name from the following geometric interpretation. Associated to $\overline{\Delta}$ is a triangle T with angles π/a, π/b, and π/c on the Riemann sphere, the Euclidean plane, or the hyperbolic plane according as the triple is spherical, Euclidean, or hyperbolic, where by convention we let $1/\infty = 0$. (The case $(a,b,c) = (2,2,\infty)$ is admittedly a bit weird; one must understand the term *triangle* generously in this case.) The group of isometries generated by reflections $\overline{\tau}_a, \overline{\tau}_b, \overline{\tau}_c$ in the three sides of the triangle T is a discrete group with T itself as a fundamental domain. The subgroup of orientation-preserving isometries is generated by the elements $\bar{\delta}_a = \overline{\tau}_b\overline{\tau}_c$, $\bar{\delta}_b = \overline{\tau}_c\overline{\tau}_a$, and $\bar{\delta}_c = \overline{\tau}_a\overline{\tau}_b$ and these elements generate a group isomorphic to $\overline{\Delta}(a,b,c)$. A fundamental domain for $\overline{\Delta}(a,b,c)$ is obtained by taking the union of the triangle T with its reflection in one of its sides. The sides of this fundamental domain are identified by the elements $\bar{\delta}_a$, $\bar{\delta}_b$, and $\bar{\delta}_c$, and consequently the quotient space is a Riemann surface of genus zero. This surface is compact if and only if $a, b, c \neq \infty$ (i.e., $c \neq \infty$ since $a \leq b \leq c$). We analogously classify the groups $\overline{\Delta}(a,b,c)$ as spherical, Euclidean, or hyperbolic. We make the convention $\mathbb{Z}/\infty\mathbb{Z} = \mathbb{Z}$.

Example 2.3. For all $a, b \geq 2$, $\overline{\Delta}(a,b,\infty)$ is canonically isomorphic to the free product $\mathbb{Z}/a\mathbb{Z} * \mathbb{Z}/b\mathbb{Z}$. This group is Euclidean when $a = b = 2$ and otherwise hyperbolic.

(a) The group $\overline{\Delta}(2,2,\infty) \simeq \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$ can be geometrically realized as the group of isometries of the Euclidean plane generated by reflections through two distinct points. This yields the alternate presentation

$$\overline{\Delta}(2,2,\infty) \simeq \langle \sigma, \tau \mid \sigma^2 = 1,\ \sigma\tau\sigma = \tau^{-1} \rangle.$$

The group $\overline{\Delta}(2,2,\infty)$ is sometimes called the infinite dihedral group.

(b) We have $\Delta(2,3,\infty) \simeq \mathbb{Z}/4\mathbb{Z} *_{\mathbb{Z}/2\mathbb{Z}} \mathbb{Z}/6\mathbb{Z} \simeq \mathrm{SL}_2(\mathbb{Z})$. It follows that $\overline{\Delta}(2,3,\infty) \simeq \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/3\mathbb{Z} \simeq \mathrm{PSL}_2(\mathbb{Z})$.

(c) The group $\overline{\Delta}(\infty,\infty,\infty) \simeq \mathbb{Z} * \mathbb{Z}$ is free on two generators. We have $\overline{\Delta}(\infty,\infty,\infty) \simeq \mathrm{Ker}(\mathrm{PSL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/2\mathbb{Z}))$.

(d) For $n \in \mathbb{Z}_{\geq 2}$, the groups $\Delta(2,n,\infty) \simeq \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/n\mathbb{Z}$ are called Hecke groups [32].

Example 2.4. The spherical triangle groups are all finite groups: we have $\overline{\Delta}(2,2,c) \simeq D_{2c}$, the dihedral group on $2c$ elements, and

$$\overline{\Delta}(2,3,3) \simeq A_4, \quad \overline{\Delta}(2,3,4) \simeq S_4, \quad \overline{\Delta}(2,3,5) \simeq A_5.$$

We have the exact sequence

$$1 \to [\overline{\Delta}, \overline{\Delta}] \to \overline{\Delta} \to \overline{\Delta}^{\mathrm{ab}} \to 1 \tag{2.5}$$

where $[\overline{\Delta},\overline{\Delta}]$ denotes the commutator subgroup. If $c \neq \infty$, then $\overline{\Delta}^{\mathrm{ab}} = \overline{\Delta}/[\overline{\Delta},\overline{\Delta}]$ is isomorphic to the quotient of $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ by the cyclic subgroup generated by (c,c); when $c = \infty$, we have $\overline{\Delta}^{\mathrm{ab}} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Thus, the group $\overline{\Delta}$ is perfect (i.e. $\overline{\Delta}^{\mathrm{ab}} = \{1\}$) if and only if a, b, c are relatively prime in pairs. We have $[\overline{\Delta},\overline{\Delta}] \simeq \mathbb{Z}$ for $(a,b,c) = (2,\infty,\infty)$, whereas for the other Euclidean triples we have $[\overline{\Delta},\overline{\Delta}] \simeq \mathbb{Z}^2$ [44, §II.4]. In particular, the Euclidean triangle groups are infinite and nonabelian, but solvable.

From now on, suppose (a,b,c) is hyperbolic. Then by the previous paragraph we can realize $\overline{\Delta} = \overline{\Delta}(a,b,c) \hookrightarrow \mathrm{PSL}_2(\mathbb{R})$ as a Fuchsian group, a discrete subgroup of orientation-preserving isometries of the upper half-plane $\mathcal{H}$. Let $\mathcal{H}^{(*)}$ denote $\mathcal{H}$ together with the cusps of $\overline{\Delta}(a,b,c)$. We write $X(a,b,c) = \overline{\Delta}(a,b,c)\backslash\mathcal{H}^{(*)} \simeq \mathbb{P}^1_{\mathbb{C}}$ for the quotient space.

We lift this embedding to $\mathrm{SL}_2(\mathbb{R})$ as follows. Suppose that $b < \infty$: this excludes the cases (a,∞,∞) and (∞,∞,∞), which can be analyzed after making appropriate modifications. Then Takeuchi [80, Proposition 1] has shown that there exists an embedding

$$\Delta(a,b,c) \hookrightarrow \mathrm{SL}_2(\mathbb{R})$$

which is unique up to conjugacy in $\mathrm{SL}_2(\mathbb{R})$. In fact, this embedding can be made explicit as follows [52]. As in the introduction, for $s \in \mathbb{Z}_{\geq 2}$, let $\zeta_s = \exp(2\pi i/s)$ and

$$\lambda_s = \zeta_s + \frac{1}{\zeta_s} = 2\cos\left(\frac{2\pi}{s}\right) \quad \text{and} \quad \mu_s = 2\sin\left(\frac{2\pi}{s}\right) = -i\left(\zeta_s - \frac{1}{\zeta_s}\right) \tag{2.6}$$

where by convention $\zeta_\infty = 1$, $\lambda_\infty = 2$, and $\mu_\infty = 0$.

Then we have a map

$$\begin{aligned} \Delta(a,b,c) &\hookrightarrow \mathrm{SL}_2(\mathbb{R}) \\ \delta_a &\mapsto \frac{1}{2}\begin{pmatrix} \lambda_{2a} & \mu_{2a} \\ -\mu_{2a} & \lambda_{2a} \end{pmatrix} \\ \delta_b &\mapsto \frac{1}{2}\begin{pmatrix} \lambda_{2b} & t\mu_{2b} \\ -\mu_{2b}/t & \lambda_{2b} \end{pmatrix} \end{aligned} \tag{2.7}$$

where

$$t + 1/t = 2\frac{\lambda_{2a}\lambda_{2b} + 2\lambda_{2c}}{\mu_{2a}\mu_{2b}}.$$

The embedding (2.7) then also gives rise to an explicit embedding $\overline{\Delta}(a,b,c) \hookrightarrow \mathrm{PSL}_2(\mathbb{R})$.

A triangle group $\overline{\Delta} = \overline{\Delta}(a,b,c)$ is maximal (we also say that the triple (a,b,c) is maximal) if $\overline{\Delta}$ cannot be properly embedded in any Fuchsian group. By a result of Singerman [64] (see also Greenberg [29, Theorem 3B]), any Fuchsian group containing $\overline{\Delta}(a,b,c)$ is itself a triangle group. All inclusion relations between triangle groups can be generated (by concatenation) from the relations [26, (2)]

$$\begin{aligned} \overline{\Delta}(2,7,7) &\leq_9 \overline{\Delta}(2,3,7) & \overline{\Delta}(3,8,8) &\leq_{10} \overline{\Delta}(2,3,8) \\ \overline{\Delta}(4,4,5) &\leq_6 \overline{\Delta}(2,4,5) & \overline{\Delta}(3,3,7) &\leq_8 \overline{\Delta}(2,3,7) \end{aligned} \tag{2.8}$$

and the families

$$\begin{aligned} \overline{\Delta}(a,a,a) &\trianglelefteq_3 \overline{\Delta}(3,3,a) & \overline{\Delta}(a,a,c) &\trianglelefteq_2 \overline{\Delta}(2,a,2c) \\ \overline{\Delta}(2,b,2b) &\leq_3 \overline{\Delta}(2,3,2b) & \overline{\Delta}(3,b,3b) &\leq_4 \overline{\Delta}(2,3,3b). \end{aligned} \tag{2.9}$$

Here $H \leq_n G$ (resp. $H \trianglelefteq_n G$) means that H is an index n subgroup of G (resp. an index n normal subgroup of G). Moreover, to avoid tedious proliferation of cases, we have in (2.9)

removed our assumption that $a \leq b \leq c$. It follows from (2.8)–(2.9) that $\overline{\Delta}(a,b,c)$ is maximal if and only if (a,b,c) is not of the form

$$(a,b,b), (2,b,2b), \text{ or } (3,b,3b) \tag{2.10}$$

with again $a,b,c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$ not necessarily in increasing order.

A Fuchsian group Γ is arithmetic [7] if there exists a quaternion algebra B over a totally real field F that is unramified at precisely one real place of F such that Γ is commensurable with the image of the units of reduced norm 1 in an order $\mathcal{O} \subseteq B$. Takeuchi [80, Theorem 3] has enumerated the arithmetic triangle groups $\overline{\Delta}(a,b,c)$: there are 85 of them, falling into 19 commensurability classes [81, Table (1)].

3. Galois Belyĭ maps

In this section, we discuss Belyĭ maps and Galois Belyĭ curves and we relate these curves to those uniformized by subgroups of triangle groups. For an encyclopedic reference on Belyĭ maps, see the tome by Lando and Zvonkin [39]; for general reference, see the book by Jones and Wolfart [34], in particular for a full expository account of Galois Belyĭ maps.

A branched cover of curves over a field k is a finite morphism of curves $f\colon X \to Y$ defined over k. A Belyĭ map is a branched cover $f\colon X \to \mathbb{P}^1$ over $\mathbb{C}$ which is unramified away from $\{0,1,\infty\}$. An isomorphism of branched covers between f and f' is an isomorphism $h\colon X \xrightarrow{\sim} X'$ that respects the covers, i.e., such that $f = f' \circ h$.

Remark 3.1. Let $f\colon X \to \mathbb{P}^1$ be a morphism of degree $d > 1$. By Riemann-Hurwitz, f is ramified over at least two points of $\mathbb{P}^1$, and if f is ramified over exactly two points then $X \simeq \mathbb{P}^1$. In the latter case, after identifying X with $\mathbb{P}^1$ we may adjust the source and target by an automorphism (linear fractional transformation) so as to have $f(z) = z^d$.

A branched cover that is Galois, i.e. a covering whose corresponding extension of function fields is Galois, is called a Galois branched cover. A curve X that possesses a Galois Belyĭ map is called a Galois Belyĭ curve. For a Galois branched cover $f\colon X \to \mathbb{P}^1$, the ramification index of $P \in X(\mathbb{C})$ depends only on $f(P)$, so we record these indices as an n-tuple $(a_1, \ldots, a_n)$ of integers $1 < a_1 \leq \cdots \leq a_n$ and say that $(a_1, \ldots, a_n)$ is the ramification type of f.

Now let G be a finite group. A G-Galois branched cover branched cover is a branched cover equipped with an isomorphism

$$i\colon G \xrightarrow{\sim} \mathrm{Gal}(f) = \mathrm{Aut}(X,f) \subseteq \mathrm{Aut}(X).$$

An isomorphism of G-Galois branched covers over k is an isomorphism h of branched covers that identifies i with i', i.e.,

$$h(i(g)x) = i'(g)h(x) \text{ for all } g \in G \text{ and } x \in X(\overline{k})$$

where $\overline{k}$ is an algebraic closure of k. (This distinction may seem irrelevant at first, but it is important if one wants to study properties not just the cover but also the Galois group of the branched cover.)

Remark 3.2. If X has genus at least 2 and $X \to X/G$ is a G-Galois Belyĭ map, then the quotient $X \to X/\mathrm{Aut}(X)$ is an $\mathrm{Aut}(X)$-Galois Belyĭ map.

Example 3.3. The map

$$f\colon \mathbb{P}^1 \to \mathbb{P}^1$$
$$f(t) = \frac{t^2(t+3)}{4} = 1 + \frac{(t-1)(t+2)^2}{4}$$

is a Belyĭ map, a branched cover ramified only over $0, 1, \infty$, with ramification indices $(2, 2, 3)$. The Galois closure of f is a Galois Belyĭ map $g\colon \mathbb{P}^1 \to \mathbb{P}^1$ with Galois group S_3 corresponding to the simplest spherical triangle group $\overline{\Delta}(2, 2, 3)$: it is given by

$$g(t) = \frac{27t^2(t-1)^2}{4(t^2-t+1)^3} \quad \text{with} \quad g(t) - 1 = -\frac{(t-2)^2(2t-1)^2(t+1)^2}{4(t^2-t+1)^3}.$$

It becomes an S_3-Galois Belyĭ map when it is equipped with the isomorphism

$$S_3 \xrightarrow{\sim} \mathrm{Gal}(f) \leq \mathrm{Aut}(\mathbb{P}^1) \simeq \mathrm{PGL}_2(\mathbb{C})$$
$$(1\ 2) \mapsto (t \mapsto 1-t) \leftrightarrow \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$$
$$(1\ 2\ 3) \mapsto \left(t \mapsto \frac{1}{1-t}\right) \leftrightarrow \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}.$$

All examples of Galois Belyĭ maps $\mathbb{P}^1 \to \mathbb{P}^1$ arise in this way from the spherical triangle groups, as in Example 2.4.

Example 3.4. We now consider Galois Belyĭ maps $E \to \mathbb{P}^1$ where E is a curve of genus 1 over $\mathbb{C}$. There is no loss in assuming that E has the structure of elliptic curve with neutral element $\infty \in E(\mathbb{C})$. The elliptic curves with extra automorphisms present candidates for such maps.

The curve $E\colon y^2 = x^3 - x$ with $j(E) = 1728$ has $G = \mathrm{Aut}(E, \infty)$ cyclic of order 4, and the quotient $x^2\colon E \to E/G \simeq \mathbb{P}^1$ yields a Galois Belyĭ map of degree 4 with ramification type $(2, 4, 4)$ by a direct computation. This map as a G-Galois Belyĭ map is minimally defined over $\mathbb{Q}(\sqrt{-1})$; the Belyi map itself is defined over $\mathbb{Q}$.

Next we consider the curve with $j(E) = 0$ with $G = \mathrm{Aut}(E, \infty)$ cyclic of order 6, from which we obtain two Galois Belyĭ maps. The first map is obtained by writing $E\colon y^2 = x^3 - 1$ and taking the map $x^3\colon E \to E/G \simeq \mathbb{P}^1$, a Galois Belyĭ map of degree 6 with ramification type $(2, 3, 6)$. The second is obtained by writing instead $E\colon y^2 - y = x^3$ (isomorphically) and the unique subgroup $H < G$ of order 3, corresponding to the map $y\colon E \to E/H \simeq \mathbb{P}^1$ with ramification type $(3, 3, 3)$. These maps are minimally defined over $\mathbb{Q}(\sqrt{-3})$ as Galois Belyĭ maps. Indeed, the inclusions (2.9) imply an inclusion $\overline{\Delta}(3, 3, 3) \trianglelefteq_2 \overline{\Delta}(2, 3, 6)$, so the former is the composition of the latter together with the squaring map.

One obtains further Galois Belyĭ maps by precomposing these with an isogeny $E \to E$.

Lemma 3.5. *Up to isomorphism, the only Galois Belyĭ maps $E \to \mathbb{P}^1$ with E a genus 1 curve over $\mathbb{C}$ are of the form*

$$E \xrightarrow{\phi} E \xrightarrow{f} \mathbb{P}^1$$

where ϕ is an isogeny and f is one of the three Galois Belyĭ maps in Example 3.4. In particular, the only Galois Belyĭ curves E of genus 1 have $j(E) = 0, 1728$.

Proof. Let $E \to \mathbb{P}^1$ be a Galois Belyĭ map, where without loss of generality we may assume $E\colon y^2 = h(x)$ is an elliptic curve in Weierstrass form with neutral element ∞. We claim that $j(E) = 0, 1728$. We always have $\operatorname{Aut} E = E(\mathbb{C}) \rtimes \operatorname{Aut}(E, \infty)$. If $G < \operatorname{Aut} E$ is a finite subgroup, then $G' = G \cap E(\mathbb{C}) \trianglelefteq G$ and $G/G' \subseteq \operatorname{Aut}(E, \infty)$, so $E' = E/G'$ is an elliptic curve and $E/G \simeq E/(G/G')$. However, if $j(E) \neq 0, 1728$, then $\operatorname{Aut}(E, \infty) = \{\pm 1\}$, so either $G = G'$ and E/G is an elliptic curve, or $G = \pm G'$ and the map $E \to E/G' \xrightarrow{x} E/G \simeq \mathbb{P}^1$ is ramified at four points, the roots of $h(x)$ and ∞. □

In view of Examples 3.3 and 3.4 and Lemma 3.5, from now on we may restrict our attention to Galois Belyĭ maps $f\colon X \to \mathbb{P}^1$ with X of genus $g \geq 2$. These curves can be characterized in several equivalent ways.

Proposition 3.6 (Wolfart [88, 90])**.** *Let X be a compact Riemann surface of genus $g \geq 2$. Then the following are equivalent.*

(i) *X is a Galois Belyĭ curve;*
(ii) *The map $X \to X/\operatorname{Aut}(X)$ is a Belyĭ map;*
(iii) *There exists a finite index, torsion-free normal subgroup $\Gamma \trianglelefteq \overline{\Delta}(a, b, c)$ with $a, b, c \in \mathbb{Z}_{\geq 2}$ and a complex uniformization $\Gamma\backslash\mathcal{H} \xrightarrow{\sim} X$; and*
(iv) *There exists an open neighborhood U of $[X]$ (with respect to the complex analytic topology) in the moduli space $\mathcal{M}_g(\mathbb{C})$ of curves of genus g such that $\#\operatorname{Aut}(X) > \#\operatorname{Aut}(Y)$ for all $[Y] \in U \smallsetminus \{[X]\}$.*

Remark 3.7. Proposition 3.6 implies that Riemann surfaces uniformized by subgroups of non-cocompact hyerperbolic triangle groups are also uniformized by subgroups of cocompact hyperbolic triangle groups. More precisely: let $a', b' \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$, $(a', b') \neq (2, 2)$, and let $\Gamma' \subset \overline{\Delta}(a', b', \infty)$ be a finite index subgroup (*not* necessarily torsionfree). Then $\Gamma'\backslash\mathcal{H}^{(*)} \to \overline{\Delta}(a', b', \infty)\backslash\mathcal{H}^{(*)}$ is a Galois Belyĭ map, so by Proposition 3.6 there are $a, b, c \in \mathbb{Z}_{\geq 2}$ and a finite index, normal torsionfree subgroup $\Gamma \subset \overline{\Delta}(a, b, c)$ such that $\Gamma'\backslash\mathcal{H}^{(*)} \simeq \Gamma\backslash\mathcal{H}$. The case of $\mathrm{PSL}_2(\mathbb{F}_q)$-Galois Belyĭ curves uniformized by subgroups of Hecke triangle groups is treated in detail by Schmidt and Smith [59, Prop. 4].

By the Riemann-Hurwitz formula, if X is a G-Galois Belyĭ curve of type (a, b, c), then X has genus

$$g(X) = 1 + \frac{\#G}{2}\left(1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}\right) = 1 - \frac{\#G}{2}\chi(a, b, c). \tag{3.8}$$

Remark 3.9. The function of $\#G$ in (3.8) is maximized when $(a, b, c) = (2, 3, 7)$. Combining this with Proposition 3.6(iv) we recover the Hurwitz bound

$$\#\operatorname{Aut}(X) \leq 84(g(X) - 1)$$

for Galois Belyĭ curves; the Hurwitz bound for all smooth projective curves then follows from the fact that $\#\operatorname{Aut}(X)$ achieves its maximum on $\mathcal{M}_g(\mathbb{C})$ at an isolated point.

Remark 3.10. There are only finitely many Galois Belyĭ curves of any given genus g. By the Hurwitz bound (3.9), we can bound $\#G$ given $g \geq 2$, and for fixed g and $\#G$ there are only finitely many triples (a, b, c) satisfying (3.8). Each $\overline{\Delta}(a, b, c)$ is finitely generated so has only finitely many subgroups of index $\#G$. From this, one can extract an explicit upper bound; using a more refined approach, Schlage-Puchta and Wolfart [58, Theorem 1] showed that the number of isomorphism classes of Galois Belyĭ curves of genus at most g grows like $g^{\log g}$.

Remark 3.11. Wolfart [90] gives a complete list of all Galois Belyĭ curves of genus $g = 2, 3, 4$. Further examples of Galois Belyĭ curves can be found in the work of Shabat and Voevodsky [62]. See Table 10.5 for the determination of all $\mathrm{PSL}_2(\mathbb{F}_q)$-Galois Belyĭ curves with genus $g \leq 24$.

Example 3.12. Let $f\colon X \to \mathbb{P}^1$ be a Belyĭ map and let $g\colon Y \to \mathbb{P}^1$ be its Galois closure. Then g is also a Belyĭ map and hence Y is a Galois Belyĭ curve. Note however that the genus of Y may be much larger than the genus of X!

Condition (iii) in Proposition 3.6 leads us to consider curves arising from finite index normal subgroups of the hyperbolic triangle groups $\overline{\Delta}(a, b, c)$. If $\overline{\Gamma} \subseteq \mathrm{PSL}_2(\mathbb{R})$ is a Fuchsian group, write $X(\overline{\Gamma}) = \overline{\Gamma} \setminus \mathcal{H}^{(*)}$. If X is a compact Riemann surface of genus $g \geq 2$ with uniformizing subgroup $\overline{\Gamma} \subseteq \mathrm{PSL}_2(\mathbb{R})$, so that $X = X(\overline{\Gamma})$, then $\mathrm{Aut}(X) = N(\overline{\Gamma})/\overline{\Gamma}$, where $N(\overline{\Gamma})$ is the normalizer of $\overline{\Gamma}$ in $\mathrm{PSL}_2(\mathbb{R})$. Moreover, the quotient $X \to X/\mathrm{Aut}(X)$, obtained from the map $X(\overline{\Gamma}) \to X(N(\overline{\Gamma}))$, is a Galois cover with Galois group $\mathrm{Aut}(X)$. By the results of Section 1, if $\overline{\Gamma} \subseteq \overline{\Delta}(a, b, c)$ is a finite index normal subgroup then $\mathrm{Aut}(X(\overline{\Gamma}))$ is of the form $\overline{\Delta}'/\overline{\Gamma}$ with an inclusion $\overline{\Delta} \subseteq \overline{\Delta}'$ as in (2.8)–(2.9); if $\overline{\Delta}$ is maximal, then we have

$$\mathrm{Aut}(X(\overline{\Gamma})) \simeq \overline{\Delta}(a, b, c)/\overline{\Gamma}. \tag{3.13}$$

4. Fields of moduli

In this section, we briefly review the theory of fields of moduli and fields of definition. See Coombes and Harbater [15] and Köck [37] for more detail.

The field of moduli $M(X)$ of a curve X over $\mathbb{C}$ is the fixed field of the group

$$\{\sigma \in \mathrm{Aut}(\mathbb{C})\colon X^\sigma \simeq X\}.$$

In a similar way, we define the fields of moduli $M(X, f)$ of a Belyĭ map $f\colon X \to \mathbb{P}^1$ and $M(X, f, G)$ of a G-Galois Belyĭ map.

Owing to a lack of rigidity, not every curve can be defined over its field of moduli. However, in our situation we have the following lemma.

Lemma 4.1. *Let $f\colon X \to \mathbb{P}^1$ be a Galois Belyĭ map. Then the following statements hold.*

(a) *f is defined over its field of moduli $M(X, f)$.*
(b) *Suppose f is given by the quotient $f\colon X \to X/\mathrm{Aut}(X) \simeq \mathbb{P}^1$ and that the associated triangle group Δ is maximal (i.e., not of the form (2.10)). Then $M(X, f) = M(X)$ and X is defined over its field of moduli $M(X)$.*

Proof. Dèbes and Emsalem [18, §1] remark that statement (a) follows from results of Coombes and Harbater [15]. A proof of (a) was written down by Köck [37, Theorem 2.2].

Now we prove (b). By Dèbes and Emsalem [18, Theorem 3.1], one always has $M(X, g) = M(X)$ where $g\colon X \to X/\mathrm{Aut}(X) = V$: indeed, any automorphism $\sigma(X) \to X$ with $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ induces an isomorphism of automorphism groups and hence of the pair (X, g). (Or, the field of $M(X)$ is the intersection of all fields of definition of X, but over any field K where X is defined, so is g (since $\mathrm{Aut}(X)$ as a scheme is defined over K), so $M(X, g) = M(X)$.) The subtlety in statement (b) is that a Belyĭ map f is rigidified so that an automorphism of f is required to act as the identity on $\mathbb{P}^1$. If one allows automorphisms of $\mathbb{P}^1$, then there may be additional descent of f and X, and in particular the quotient $X \to X/\mathrm{Aut}(X)$ may

be a branched cover of a genus zero curve ramified above at most three points but would then not be a Belyĭ map, according to our definition.

So to conclude (b), we will show that the map g is a Belyĭ map according to our definition, and for that it suffices to show that each ramification point on the target curve V is $M(X)$-rational (so in particular V is defined over $M(X)$ and isomorphic over $M(X)$ to $\mathbb{P}^1$). To do this, we note that since the associated triangle group $\Delta(a,b,c)$ is maximal, by (2.10) the three indices a,b,c are distinct; any automorphism of g preserves ramification indices and thus necessarily fixes these ramification points, so the base descends with these three points marked and so in the canonical model of Dèbes and Emsalem they are defined over $M(X,g) = M(X)$. □

Remark 4.2. The subtlety in Lemma 4.1 is noted by Streit and Wolfart [75, Theorem 1, Remark 1], and they discuss the possible misinterpretation of the proof in Wolfart [91, Theorem 5] and the subtlety in rigidifying the base curve. Girondo, Torres-Teigell, and Wolfart [27, Lemma 1, Remark 1, Lemma 2] also give a proof of the second statement and discuss descent for certain non-maximal triangle groups.

Keeping track of the action of the automorphism group, we also have the following result.

Lemma 4.3. *Let $f : X \to \mathbb{P}^1$ be a G-Galois Belyĭ map. Suppose that $C_{\mathrm{Aut}(X)}(G) = \{1\}$, i.e., the centralizer of G in $\mathrm{Aut}(X)$ is trivial. Then f and the action of $\mathrm{Gal}(f) \simeq G$ can be defined over the field of moduli $M(X,f,G)$.*

Proof. By definition, an automorphism of f as a G-Galois Belyĭ map is given by $h \in \mathrm{Aut}(X)$ such that $hi(g)h^{-1} = i(g)$ for all $g \in G$, so under the hypothesis of the lemma, f has no automorphisms. Thus f and $\mathrm{Gal}(f)$ can be defined over $M(X,f,G)$ by the Weil cocycle criterion for descent. □

Remark 4.4. Let X be a curve which can be defined over its field of moduli $F = M(X)$. Then the set of F-isomorphism classes of models for X over F is in bijection with the Galois cohomology set $H^1(\mathrm{Gal}(\overline{F}/F), \mathrm{Aut}(X))$, where $\mathrm{Aut}(X)$ is equipped with the natural action of the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$. Similar statements are true more generally for the other objects considered here, including Belyĭ maps and G-Galois Belyĭ maps.

Corollary 4.5. *If $G \simeq \mathrm{Aut}(X)$ and G has trivial center $Z(G) = \{1\}$, then f as a G-Galois Belyĭ map can be defined over $K = M(X,f,G)$, and G occurs infinitely often as a Galois group over K.*

Proof. The first conclusion is an immediate consequence of Lemma 4.3. For the second conclusion, by definition the group G occurs as a Galois group over $K(t)$, and applying Hilbert's irreducibility theorem [61, Chapter 3] we find that G occurs infinitely often as a Galois group over K. □

Example 4.6. Let p be prime and let $X(p) = \Gamma(p)\backslash\mathcal{H}^*$ be the classical modular curve (over $\mathbb{C}$), parametrizing (generalized) elliptic curves E equipped with a basis of $E[p]$ which is symplectic with respect to the Weil pairing. Then $\mathrm{Aut}(X(p)) \supseteq G = \mathrm{PSL}_2(\mathbb{F}_p)$, and the quotient map $j\colon X \to X/G \simeq \mathbb{P}^1$, corresponding to the inclusion $\Gamma(p) \subseteq \mathrm{PSL}_2(\mathbb{Z})$, is ramified over $j = 0, 1728, \infty$ with indices $2, 3, p$, so $X(p)$ is a Galois Belyĭ curve.

For $p \leq 5$, the curve $X(p)$ has genus 0 and thus $\mathrm{Aut}\, X(p) = \mathrm{PGL}_2(\mathbb{C})$. For $p \geq 7$, the curve $X(p)$ has genus at least three (the curve $X(7)$ has genus 3 and is considered in more

detail in the following example), so $\operatorname{Aut} X(p)$ is a finite group containing $\mathrm{PSL}_2(\mathbb{F}_p)$. In fact we have $\operatorname{Aut} X(p) = \mathrm{PSL}_2(\mathbb{F}_p)$, as was shown by Mazur, following Serre [48, p. 255]. Later we will recover this fact as a special case of a more general result.

The field of moduli of $j\colon X \to \mathbb{P}^1$ is $\mathbb{Q}$, and indeed this map (and hence X) admits a canonical model over $\mathbb{Q}$ [36]. This model is not unique, since the set $H^1(\mathbb{Q}, \operatorname{Aut}(X))$ is infinite: in fact, every isomorphism class of Galois modules $E[p]$ with E an elliptic curve gives a different element in this set.

For $p > 2$, let $p^* = p(-1)^{(p-1)/2}$ (so $\mathbb{Q}(\sqrt{p^*})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$). The field of moduli of the $\mathrm{PSL}_2(\mathbb{F}_p)$-Galois Belyĭ map j is $\mathbb{Q}(\sqrt{p^*})$ when $p > 2$ and $\mathbb{Q}$ when $p = 2$, and in each case the field of moduli is a field of definition [63, pp. 108-109]. Indeed, this follows from Weil descent when $p \geq 7$ and can be seen directly when $p = 2, 3, 5$ as these correspond to spherical triples $(2, 3, p)$ (cf. Example 3.3).

Example 4.7. The Klein quartic curve [23] defined by the equation

$$x^3y + y^3z + z^3x = 0$$

has field of definition equal to its field of moduli $\mathbb{Q}$, and all elements of $\operatorname{Aut}(X)$ can be defined over $\mathbb{Q}(\sqrt{-7}) = \mathbb{Q}(\sqrt{7^*})$. Although the Klein quartic is isomorphic to $X(7)$ over $\overline{\mathbb{Q}}$, as remarked by Livné, the Katz-Mazur canonical model of $X(7)$ agrees with the Klein quartic only over $\mathbb{Q}(\sqrt{-3})$. The issue here concerns the fields of definition of the special points giving rise to the canonical model. We do not go further into this issue here, but for more on this in the case of genus 1, see work of Sijsling [70].

Remark 4.8. We consider again Remark 3.12. If the field of moduli of a Belyĭ map $f\colon X \to \mathbb{P}^1$ is F, then the field of moduli of its Galois closure $g\colon Y \to \mathbb{P}^1$ as a Belyĭ map contains F. Consequently, let F be a number field and let X be an elliptic curve such that $\mathbb{Q}(j(X)) = F$. Then X admits a Belyĭ map defined over F. The Galois closure $g\colon Y \to \mathbb{P}^1$ with its automorphism group G therefore has field of moduli $M(Y, g, G)$ containing F. Therefore, for any number field F, there exists a G-Galois Belyĭ map such that any field of definition of this Galois map, including its automorphism group, contains F. Note that from Lemma 3.5 that outside of a handful of cases, the associated Galois Belyĭ curve Y has genus $g(X) \geq 2$. This shows that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on the set of isomorphism classes of G-Galois Belyĭ curves. However if $X \to \mathbb{P}^1$ is a G-Galois Belyĭ map and $H \leq G$ is a subgroup, then the field of moduli of $X \to X/H$ can be smaller than the $M(X, f, G)$.

Nevertheless, González-Diez and Jaikin-Zapirain [28] have recently shown that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts faithfully on the set of Galois Belyĭ curves. See also related work of Bauer, Catanese, and Grunewald [3].

In view of Remark 4.8, we restrict our attention from the general setup to the special class of G-Galois Belyĭ curves X where $G = \mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$.

Remark 4.9. Conder, Jones, Streit, and Wolfart [14] give the fields of definition of Galois Belyi maps for genus $g \leq 18$.

5. Congruence subgroups of triangle groups

In this section, we associate a quaternion algebra over a totally real field to a triangle group following Takeuchi [79]. This idea was also pursued by Cohen and Wolfart [12] with an eye toward results in transcendence theory, and further elaborated by Cohen, Itzykson,

and Wolfart [10]. Here, we use this embedding to construct congruence subgroups of Δ. We refer to Vignéras [83] for the facts we will use about quaternion algebras and Katok [35] as a reference on Fuchsian groups.

Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{R})$ be a discrete subgroup such that $\overline{\Gamma} = \Gamma/\{\pm 1\} \subseteq \mathrm{PSL}_2(\mathbb{R})$ has finite coarea, so in particular is Γ is finitely generated. Let

$$F = \mathbb{Q}(\operatorname{tr}\Gamma) = \mathbb{Q}(\operatorname{tr}\gamma)_{\gamma\in\Gamma}$$

be the trace field of Γ. Then F is a finitely generated extension of $\mathbb{Q}$.

Suppose further that F is a number field, so F has finite degree over $\mathbb{Q}$, and let $\mathbb{Z}_F$ be its ring of integers. Let $F[\Gamma]$ be the F-vector space generated by Γ in $\mathrm{M}_2(\mathbb{R})$, and let $\mathbb{Z}_F[\Gamma]$ denote the $\mathbb{Z}_F$-submodule of $F[\Gamma]$ generated by Γ. By work of Takeuchi [78, Propositions 2–3], the ring $F[\Gamma]$ is a quaternion algebra over F. If further $\operatorname{tr}(\Gamma) \subseteq \mathbb{Z}_F$, then $\mathbb{Z}_F[\Gamma]$ is an order in $F[\Gamma]$.

Remark 5.1. Let $\Gamma \leq \mathrm{SL}_2(\mathbb{R})$ be a Fuchsian group of finite coarea. We introduce terminology following Schaller and Wolfart [57, Definition 1, p. 14]: a modular embedding of Γ consists of a holomorphic embedding $F : \mathcal{H} \to \mathcal{H}^r$ (for some $r \in \mathbb{Z}_{\geq 1}$) together with an inclusion $\iota : \Gamma \hookrightarrow \Pi \subseteq \mathrm{SL}_2(\mathbb{R})$ such that Π is an arithmetic group acting on $\mathcal{H}^r$, with the compatibility

$$F(\gamma z) = \iota(\gamma)F(z) \quad \text{for all } \gamma \in \Gamma,\ \ z \in \mathcal{H}.$$

Thus Γ admits a modular embedding if Γ is arithmetic or is a subgroup of a triangle group. Schaller and Wolfart ask whether the converse holds [57, Problem 1, p. 23]. As has been pointed out by Kucharczyk [38, item (iv), p. 79], work of McMullen [49] gives a negative answer to this question, but none of the known counterexamples are cocompact. See also work of Ricker [55], which answers the question in the affirmative for a certain class of cocompact Fuchsian groups.

Let (a, b, c) be a hyperbolic triple with $2 \leq a \leq b \leq c \leq \infty$. As in section 2, associated to the triple (a, b, c) is the triangle group $\Delta(a, b, c) \subseteq \mathrm{SL}_2(\mathbb{R})$ with $\Delta(a, b, c)/\{\pm 1\} \simeq \overline{\Delta}(a, b, c) \subseteq \mathrm{PSL}_2(\mathbb{R})$. Let $F = \mathbb{Q}(\operatorname{tr}\Delta(a, b, c))$ be the trace field of $\Delta(a, b, c)$. The generating elements $\delta_s \in \Delta(a, b, c)$ for $s = a, b, c$ satisfy the quadratic equations

$$\delta_s^2 - \lambda_{2s}\delta_s + 1 = 0$$

in B where λ_{2s} is defined in (2.6).

Lemma 5.2 ([80, Lemma 2])**.** *Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{R})$. If $\gamma_1, \ldots, \gamma_r$ generate Γ, then $\mathbb{Q}(\operatorname{tr}\Gamma)$ is generated by $\operatorname{tr}(\gamma_{i_1} \cdots \gamma_{i_s})$ for $\{i_1, \ldots, i_s\} \subseteq \{1, \ldots, r\}$.*

By Lemma 5.2, we deduce

$$F = \mathbb{Q}(\operatorname{tr}\Delta(a, b, c)) = \mathbb{Q}(\lambda_{2a}, \lambda_{2b}, \lambda_{2c}).$$

Taking traces in the equation

$$\delta_a\delta_b = -\delta_c^{-1} = \delta_c - \lambda_{2c},$$

yields

$$-\operatorname{tr}(\delta_c^{-1}) = -\lambda_{2c} = \operatorname{tr}(\delta_a\delta_b) = \delta_a\delta_b + (\lambda_{2b} - \delta_b)(\lambda_{2a} - \delta_a).$$

Also we have

$$\delta_a\delta_b + \delta_b\delta_a = \lambda_{2b}\delta_a + \lambda_{2a}\delta_b - \lambda_{2c} - \lambda_{2a}\lambda_{2b}. \tag{5.3}$$

Together with the cyclic permutations of these equations, we conclude that the elements $1, \delta_a, \delta_b, \delta_c$ form a $\mathbb{Z}_F$-basis for the order $\mathcal{O} = \mathbb{Z}_F[\Delta] \subseteq B = F[\Delta]$ (see also Takeuchi [80, Proposition 3]).

Lemma 5.4. *The reduced discriminant of $\mathcal{O}$ is a principal $\mathbb{Z}_F$-ideal generated by*

$$\beta = \lambda_{2a}^2 + \lambda_{2b}^2 + \lambda_{2c}^2 + \lambda_{2a}\lambda_{2b}\lambda_{2c} - 4 = \lambda_a + \lambda_b + \lambda_c + \lambda_{2a}\lambda_{2b}\lambda_{2c} + 2.$$

Proof. Let $\mathfrak{d}$ be the discriminant of $\mathcal{O}$. Then we calculate from the definition that

$$\mathfrak{d}^2 = \det \begin{pmatrix} 2 & \lambda_{2a} & \lambda_{2b} & \lambda_{2c} \\ \lambda_{2a} & \lambda_{2a}^2 - 2 & -\lambda_{2c} & -\lambda_{2b} \\ \lambda_{2b} & -\lambda_{2c} & \lambda_{2b}^2 - 2 & -\lambda_{2a} \\ \lambda_{2c} & -\lambda_{2b} & -\lambda_{2a} & \lambda_{2c}^2 - 2 \end{pmatrix} \mathbb{Z}_F = \beta^2 \mathbb{Z}_F.$$

Alternatively, we compute a generator for $\mathfrak{d}$ using the scalar triple product and (5.3) as

$$\begin{aligned} \operatorname{tr}([\delta_a, \delta_b]\delta_c) &= \operatorname{tr}((\delta_a\delta_b - \delta_b\delta_a)\delta_c) = \operatorname{tr}(2\delta_a\delta_b - (\lambda_{2b}\delta_a + \lambda_{2a}\delta_b - \lambda_{2c} - \lambda_{2a}\lambda_{2b})\delta_c) \\ &= -4 - \lambda_{2b}\operatorname{tr}(\delta_a\delta_c) - \lambda_{2a}\operatorname{tr}(\delta_b\delta_c) + \lambda_{2c}^2 + \lambda_{2a}\lambda_{2b}\lambda_{2c} = \beta \end{aligned}$$

since $\delta_a\delta_c = -\delta_b^{-1}$ and $\delta_b\delta_c = -\delta_a^{-1}$. □

Lemma 5.5. *If $\mathfrak{P}$ is a prime of $\mathbb{Z}_F$ with $\mathfrak{P} \nmid 2abc$, then $\mathfrak{P} \nmid \beta$. If further (a, b, c) is not of the form $(mz, m(z+1), mz(z+1))$ with $z, m \in \mathbb{Z}$, then $\mathfrak{P} \nmid \beta$ for all $\mathfrak{P} \nmid abc$.*

Proof. Let $\mathfrak{P}$ be a prime of F such that $\mathfrak{P} \nmid abc$. We have the following identity in the field $\mathbb{Q}(\zeta_{2a}, \zeta_{2b}, \zeta_{2c}) = K$:

$$\beta = \left(\frac{\zeta_{2b}\zeta_{2c}}{\zeta_{2a}} + 1\right)\left(\frac{\zeta_{2a}\zeta_{2c}}{\zeta_{2b}} + 1\right)\left(\frac{\zeta_{2a}\zeta_{2b}}{\zeta_{2c}} + 1\right)\left(\frac{1}{\zeta_{2a}\zeta_{2b}\zeta_{2c}} + 1\right). \tag{5.6}$$

Let $\mathfrak{P}_K$ be a prime above $\mathfrak{P}$ in K and suppose that $\mathfrak{P}_K \mid \beta$. Then $\mathfrak{P}_K$ divides one of the factors in (5.6).

First, suppose that $\mathfrak{P}_K \mid (\zeta_{2b}\zeta_{2c}\zeta_{2a}^{-1} + 1)$, i.e., we have $\zeta_{2b}\zeta_{2c} \equiv -\zeta_{2a} \pmod{\mathfrak{P}_K}$. Suppose that $\mathfrak{P}_K \nmid 2abc$. Then the map $(\mathbb{Z}_K^\times)_{\text{tors}} \to \mathbb{F}_{\mathfrak{P}_K}^\times$ is injective. Hence $\zeta_{2b}\zeta_{2c} = -\zeta_{2a} \in K$. But then embedding $K \hookrightarrow \mathbb{C}$ by $\zeta_s \mapsto e^{2\pi i/s}$ in the usual way, this equality would then read

$$\frac{1}{b} + \frac{1}{c} = 1 + \frac{1}{a} \in \mathbb{Q}/2\mathbb{Z}. \tag{5.7}$$

However, we have

$$0 \leq \frac{1}{b} + \frac{1}{c} \leq 1 < 1 + \frac{1}{a} < 2$$

for any $a, b, c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$ when $a \neq \infty$, a contradiction, and when $a = \infty$ we have $b = c = \infty$ which again contradicts (5.7).

Now suppose $\mathfrak{P}_K \mid 2$ but still $\mathfrak{P}_K \nmid abc$. Then $\ker((\mathbb{Z}_K^\times)_{\text{tors}} \to \mathbb{F}_{\mathfrak{P}}^\times) = \{\pm 1\}$, so instead we have the equation $\zeta_{2b}\zeta_{2c} = \pm\zeta_{2a} \in K$. Arguing as above, it is enough to consider the equation with the $+$-sign, which is equivalent to

$$\frac{1}{b} + \frac{1}{c} = \frac{1}{a}.$$

Looking at this equation under a common denominator we find that $b \mid c$, say $c = zb$. Substituting this back in we find that $(z+1) \mid b$ so $b = m(z+1)$ and hence $a = zm$ and $c = mz(z+1)$, and in this case we indeed have equality.

The case where $\mathfrak{P}_K$ divides the middle two factors is similar. The case where $\mathfrak{P}_K$ divides the final factor follows from the impossibility of

$$0 = 1 + \frac{1}{a} + \frac{1}{b} + \frac{1}{c} \in \mathbb{Q}/2\mathbb{Z}$$

since (a, b, c) is hyperbolic. □

We have by definition an embedding

$$\Delta \hookrightarrow \mathcal{O}_1^\times = \{\gamma \in \mathcal{O} \colon \operatorname{nrd}(\gamma) = 1\}$$

(where nrd denotes the reduced norm) and hence an embedding

$$\overline{\Delta} = \Delta/\{\pm 1\} \hookrightarrow \mathcal{O}_1^\times/\{\pm 1\}. \tag{5.8}$$

In fact, the image of this map arises from a quaternion algebra over a smaller field, as follows. Let $\Delta^{(2)}$ denote the subgroup of Δ generated by -1 and γ^2 for $\gamma \in \Delta$. Then $\Delta^{(2)}$ is a normal subgroup of Δ, and the quotient $\Delta/\Delta^{(2)}$ is an elementary abelian 2-group. We have an embedding

$$\Delta^{(2)}/\{\pm 1\} \hookrightarrow \Delta/\{\pm 1\} = \overline{\Delta}.$$

Recall the exact sequence (2.5):

$$1 \to [\overline{\Delta}, \overline{\Delta}] \to \overline{\Delta} \to \overline{\Delta}^{\mathrm{ab}} \to 1.$$

Here, $\overline{\Delta}^{\mathrm{ab}}$ is the quotient of $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z}$ by the subgroup $(1, 1, 1)$. We obtain $\Delta^{(2)} \supseteq [\overline{\Delta}, \overline{\Delta}]$ as the kernel of the (further) maximal elementary 2-quotient of $\overline{\Delta}^{\mathrm{ab}}$. It follows that the quotient $\Delta/\Delta^{(2)}$ is generated by the elements δ_s for $s \in \{a, b, c\}$ such that either $s = \infty$ or s is even, and

$$\Delta/\Delta^{(2)} \simeq \begin{cases} \{0\}, & \text{if at least two of } a, b, c \text{ are odd;} \\ \mathbb{Z}/2\mathbb{Z}, & \text{if exactly one of } a, b, c \text{ is odd;} \\ (\mathbb{Z}/2\mathbb{Z})^2, & \text{if all of } a, b, c \text{ are even or } \infty. \end{cases} \tag{5.9}$$

(See also Takeuchi [80, Proposition 5].)

We have

$$\operatorname{tr} \delta_s^2 = \operatorname{tr}(\lambda_{2s}\delta_s - 1) = \lambda_{2s}^2 - 2 = \lambda_s - 2$$

for $s \in \{a, b, c\}$ and similarly

$$\operatorname{tr}(\delta_a^2\delta_b^2) = \operatorname{tr}((\lambda_{2a}\delta_a - 1)(\lambda_{2b}\delta_b - 1)) = \lambda_{2a}\lambda_{2b}\lambda_{2c} - \lambda_{2b}^2 - \lambda_{2a}^2 + 2$$

and

$$\operatorname{tr}(\delta_a^2\delta_b^2\delta_c^2) = \operatorname{tr}((\lambda_{2a}\delta_a - 1)(\lambda_{2b}\delta_b - 1)(\lambda_{2c}\delta_c - 1)) = \lambda_{2a}^2 + \lambda_{2b}^2 + \lambda_{2c}^2 + \lambda_{2a}\lambda_{2b}\lambda_{2c} - 2;$$

from these we conclude that the trace field of $\Delta^{(2)}$ contains

$$E = E(a, b, c) = \mathbb{Q}(\lambda_{2a}^2, \lambda_{2b}^2, \lambda_{2c}^2, \lambda_{2a}\lambda_{2b}\lambda_{2c}) = \mathbb{Q}(\lambda_a, \lambda_b, \lambda_c, \lambda_{2a}\lambda_{2b}\lambda_{2c}). \tag{5.10}$$

By work of Takeuchi [80, Propositions 4–5], this containment is an equality, so the trace field of $\Delta^{(2)}$ is equal to E.

Example 5.11. The Hecke triangle groups $\Delta(2, n, \infty)$ for $n \geq 3$ have trace field $F = \mathbb{Q}(\lambda_{2n})$ whereas the corresponding groups $\Delta^{(2)}$ have trace field $E = \mathbb{Q}(\lambda_n)$, which is strictly contained in F if and only if n is even.

Let $\Lambda = \mathbb{Z}_E[\Delta^{(2)}] \subseteq A = E[\Delta^{(2)}]$ be the order and quaternion algebra associated to $\Delta^{(2)}$. By construction we have

$$\Delta^{(2)}/\{\pm 1\} \hookrightarrow \Lambda_1^\times/\{\pm 1\}. \tag{5.12}$$

We then have the following fundamental result.

Proposition 5.13. *The image of the natural homomorphism*

$$\overline{\Delta} \hookrightarrow \frac{\mathcal{O}_1^\times}{\{\pm 1\}} \hookrightarrow \frac{N_B(\mathcal{O})}{F^\times}$$

lies in the subgroup $N_A(\Lambda^\times)/E^\times$ via

$$\begin{aligned} &\overline{\Delta} \hookrightarrow \frac{N_A(\Lambda)}{E^\times} \hookrightarrow \frac{N_B(\mathcal{O})}{F^\times} \\ &\bar{\delta}_s \mapsto \delta_s^2 + 1, && \text{if } s \neq 2; \\ &\bar{\delta}_a \mapsto (\delta_b^2+1)(\delta_c^2+1), && \text{if } a = 2. \end{aligned} \tag{5.14}$$

where $s = a, b, c$ and N denotes the normalizer. The map (5.14) *extends the natural embedding* (5.12)*.*

Proof of Proposition 5.13. First, suppose $a \neq 2$ (whence $b, c \neq 2$, by the assumption that $a \leq b \leq c$). In B, for each $s = a, b, c$, we have

$$\delta_s^2 + 1 = \lambda_{2s}\delta_s; \tag{5.15}$$

since $s \neq 2$, so that $\lambda_{2s} \neq 0$, this implies that $\delta_s^2 + 1$ has order s in $A^\times/E^\times \subseteq B^\times/F^\times$ and

$$(\delta_a^2+1)(\delta_b^2+1)(\delta_c^2+1) = \lambda_{2a}\lambda_{2b}\lambda_{2c}\delta_a\delta_b\delta_c = -\lambda_{2a}\lambda_{2b}\lambda_{2c} \in E^\times,$$

so (5.14) defines a group homomorphism $\overline{\Delta} \hookrightarrow A^\times/E^\times$. The image lies in the normalizer $N_A(\Lambda)$ because $\Delta^{(2)}$ generates Λ and Δ normalizes $\Delta^{(2)}$. Finally, we have

$$(\delta_s^2+1)^2 = \lambda_{2s}^2\delta_s^2 \in A,$$

so the map extends the natural embedding of $\Delta^{(2)}/\{\pm 1\}$.

If $a = 2$, the same argument applies, with instead

$$\bar{\delta}_a \mapsto (\delta_b^2+1)(\delta_c^2+1)$$

since $(\delta_b^2+1)(\delta_c^2+1) = \lambda_{2b}\lambda_{2c}(-\delta_a^{-1}) = \lambda_{2b}\lambda_{2c}\delta_a$ now has order 2 in $A^\times/E^\times$, and necessarily $b, c > 2$ since the triple is hyperbolic. □

Example 5.16. The triangle group $\Delta(2,4,6)$ has trace field $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. However, the group $\Delta(2,4,6)^{(2)}$ has trace field $E = \mathbb{Q}$ and indeed we find an embedding $\overline{\Delta}(2,4,6) \hookrightarrow N_A(\Lambda)/\mathbb{Q}^\times$ where Λ is a maximal order in a quaternion algebra A of discriminant 6 over $\mathbb{Q}$.

Corollary 5.17. *The following statements hold.*

(a) *We have $\Lambda \otimes_{\mathbb{Z}_E} \mathbb{Z}_F \subseteq \mathcal{O}$.*
(b) *If $a \neq 2$, the quotient $\mathcal{O}/(\Lambda \otimes_{\mathbb{Z}_E} \mathbb{Z}_F)$ is annihilated by $\lambda_{2a}\lambda_{2b}\lambda_{2c}$.*
(c) *If $a = 2$, the quotient $\mathcal{O}/(\Lambda \otimes_{\mathbb{Z}_E} \mathbb{Z}_F)$ is annihilated by $\lambda_{2b}\lambda_{2c}$.*

Proof. This follows from (5.15) since a basis for $\mathcal{O}$ is given by $1, \delta_a, \delta_b, \delta_c$. □

We now define congruence subgroups of triangle groups. Let $\mathfrak{N}$ be an ideal of $\mathbb{Z}_F$ such that $\mathfrak{N}$ is coprime to abc and either $\mathfrak{N}$ is coprime to 2 or

$$(a,b,c) \neq (mz, m(z+1), mz(z+1)) \text{ with } m,z \in \mathbb{Z}.$$

Then by Lemma 5.5, we have an isomorphism

$$\mathcal{O} \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{N}} \simeq \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{N}}) \tag{5.18}$$

where $\mathbb{Z}_{F,\mathfrak{N}}$ denotes the $\mathfrak{N}$-adic completion of the ring $\mathbb{Z}_F$: this is the product of the completions at $\mathfrak{P}$ for $\mathfrak{P} \mid \mathfrak{N}$ and thus is a finite product of discrete valuation rings. Any two maximal orders in a split quaternion algebra over a discrete valuation ring R with fraction field K are conjugate by an element of $M_2(K)$ [83, Théorème II.2.3], and it follows easily that the isomorphism (5.18) is unique up to conjugation by an element of $\mathrm{GL}_2(\mathbb{Z}_{F,\mathfrak{N}})$. Alternately (and perhaps more fundamentally) since the ring $\mathbb{Z}_{F,\mathfrak{N}}$ has trivial Picard group, the result follows from a generalization of the Noether–Skolem Theorem [56, Corollary 12].

Let

$$\mathcal{O}(\mathfrak{N}) = \{\alpha \in \mathcal{O} \colon \alpha \equiv 1 \pmod{\mathfrak{N}\mathcal{O}}\}. \tag{5.19}$$

The definition of $\mathcal{O}(\mathfrak{N})$ does not depend on the choice of isomorphism in (5.18). Let

$$\mathcal{O}_1^\times = \{\gamma \in \mathcal{O} \colon \mathrm{nrd}(\gamma) = 1\} \tag{5.20}$$

and similarly $\mathcal{O}(\mathfrak{N})_1^\times$. Then $\mathcal{O}(\mathfrak{N})_1^\times \trianglelefteq \mathcal{O}_1^\times$ is normal and we have an exact sequence

$$1 \to \mathcal{O}(\mathfrak{N})_1^\times \to \mathcal{O}_1^\times/\{\pm 1\} \to \mathrm{PSL}_2(\mathbb{Z}_F/\mathfrak{N}) \to 1$$

where surjectivity follows from strong approximation [83, Théorème III.4.3]. Let

$$\overline{\Delta}(\mathfrak{N}) = \overline{\Delta} \cap \mathcal{O}(\mathfrak{N})_1^\times.$$

Then we have

$$\frac{\overline{\Delta}}{\overline{\Delta}(\mathfrak{N})} \hookrightarrow \frac{\mathcal{O}_1^\times/\{\pm 1\}}{\mathcal{O}(\mathfrak{N})_1^\times} \simeq \mathrm{SL}_2(\mathbb{Z}_F/\mathfrak{N})/\{\pm 1\}. \tag{5.21}$$

We conclude by considering the image of the embedding (5.21). Let $\mathfrak{n} = \mathbb{Z}_E \cap \mathfrak{N}$ be the prime of E below $\mathfrak{N}$. Then $\mathfrak{n}$ is coprime to the discriminant of Λ since the latter divides $(\lambda_{2a}\lambda_{2b}\lambda_{2c})\beta$ by Corollary 5.17. Therefore, we may define $\Lambda(\mathfrak{n})$ analogously. Then by Proposition 5.13, we have an embedding

$$\overline{\Delta} \hookrightarrow \frac{N_A(\Lambda)}{E^\times} \hookrightarrow \frac{A^\times}{E^\times} \hookrightarrow \frac{A_{\mathfrak{n}}^\times}{E_{\mathfrak{n}}^\times} \simeq \mathrm{PGL}_2(E_{\mathfrak{n}}) \tag{5.22}$$

where $E_{\mathfrak{n}}$ denotes the completion of E at $\mathfrak{n}$. The image of $\overline{\Delta}$ in this map lies in $\mathrm{PGL}_2(\mathbb{Z}_{E,\mathfrak{n}})$ by (5.15) since $\lambda_{2s} \in \mathbb{Z}_{E,\mathfrak{n}}^\times$ for $s = a, b, c$ (since $\mathfrak{n}$ is coprime to abc). Reducing the image in (5.22) modulo $\mathfrak{n}$, we obtain a map

$$\overline{\Delta} \to \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{n}).$$

This map is compatible with the map $\overline{\Delta} \to \mathrm{PSL}_2(\mathbb{Z}_F/\mathfrak{N})$ inside $\mathrm{PGL}_2(\mathbb{Z}_F/\mathfrak{N})$, obtained by comparing the images in the reduction modulo $\mathfrak{N}$ of $B^\times/F^\times$, by Proposition 5.13.

We summarize the main result of this section.

Proposition 5.23. *Let $a, b, c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$. Let $\mathfrak{N}$ be an ideal of $\mathbb{Z}_F$ with $\mathfrak{N}$ prime to abc and such that either $\mathfrak{N}$ is prime to 2 or $(a,b,c) \neq (mz, m(z+1), mz(z+1))$ with $m, z \in \mathbb{Z}$. Let $\mathfrak{n} = \mathbb{Z}_E \cap \mathfrak{N}$. Then there exists a homomorphism*

$$\phi \colon \overline{\Delta}(a,b,c) \to \mathrm{PSL}_2(\mathbb{Z}_F/\mathfrak{N})$$

such that $\operatorname{tr}\phi(\bar{\delta}_s) \equiv \pm\lambda_{2s} \pmod{\mathfrak{N}}$ *for* $s = a, b, c$. *The image of* ϕ *lies in the subgroup*

$$\mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{n}) \cap \mathrm{PSL}_2(\mathbb{Z}_F/\mathfrak{N}) \subseteq \mathrm{PGL}_2(\mathbb{Z}_F/\mathfrak{N}).$$

Remark 5.24. We conclude this section with some remarks extending the primes $\mathfrak{P}$ of F (equivalently, primes $\mathfrak{p}$ of E) for which the construction applies.

First, we note that whenever $\mathfrak{P} \nmid \beta$, the order $\mathcal{O}$ is maximal at $\mathfrak{P}$.

Second, even for a ramified prime $\mathfrak{P}$ (or $\mathfrak{p}$), we still can consider the natural map to the completion; however, instead of $\mathrm{PGL}_2(F_\mathfrak{P})$ we instead obtain the units of an order in a division algebra over $F_\mathfrak{P}$, a prosolvable group. Our interest remains in the groups PSL_2 and PGL_2, but this case also bears further investigation: see Takei [77] for some results in the case where $b = c = \infty$.

Third, we claim that

$$B \simeq \left(\frac{\lambda_{2s}^2 - 4, \beta}{F}\right)$$

for any $s \in \{a, b, c\} \setminus \{\infty\}$. Indeed, given the basis $1, \delta_a, \delta_b, \delta_c$, we construct the orthogonal elements for B

$$1, 2\delta_a - \lambda_{2a}, (\lambda_{2a}^2 - 4)\delta_b + (\lambda_{2a}\lambda_{2b} + 2\lambda_{2c})\delta_a - (\lambda_{2a}^2\lambda_{2b} + \lambda_{2a}\lambda_{2c} - 2\lambda_{2b})$$

which gives rise to the presentation $B \simeq \left(\frac{\lambda_{2a}^2 - 4, -(\lambda_{2a}^2 - 4)\beta}{F}\right) \simeq \left(\frac{\lambda_{2a}^2 - 4, \beta}{F}\right)$, sensible as long as $a \neq \infty$. The others follow by symmetry. It follows that a prime $\mathfrak{P}$ of $\mathbb{Z}_F$ ramifies in B according to the Hilbert symbol on this quaternion algebra. For example, if $(a, b, c) = (2, 3, c)$ (with $c \geq 7$), one can show that the quaternion algebra B is ramified at no finite place.

A similar argument [81, Proposition 2] shows that

$$A \simeq \left(\frac{\lambda_{2b}^2(\lambda_{2b}^2 - 4), \lambda_{2b}^2\lambda_{2c}^2\beta}{E}\right)$$

whenever $b \neq \infty$: Takeuchi only claims this for arithmetic, cocompact triples but the argument extends. (Indeed, if $\infty \in \{a, b, c\}$, then the corresponding generator δ_a is parabolic, so A has a zerodivisor and necessarily $A \simeq \mathrm{M}_2(E)$.) For any prime $\mathfrak{p}$ of E which is unramified in A, we can repeat the above construction, and we obtain a homomorphism ϕ as in (5.23); the image can be analyzed by considering the isomorphism class of the local order $\Lambda_\mathfrak{p}$, measured in part by the divisibility of β by $\mathfrak{p}$.

6. Weak rigidity

In this section, we investigate some weak forms of rigidity and rationality for Galois covers of $\mathbb{P}^1$. We refer to work of Coombes and Harbater [15], Malle and Matzat [45], Serre [61, Chapters 7–8], and Völklein [86] for references. Our main result concerns three-point covers, but we begin by briefly considering more general covers.

Let G be a finite group. An n-tuple for G is a finite sequence $\underline{g} = (g_1, \ldots, g_n)$ of elements of G such that $g_1 \cdots g_n = 1$. In our applications we will take $n = 3$, so we will not emphasize the dependence on n, and refer to *tuples*. A tuple is generating if $\langle g_1, \ldots, g_n \rangle = G$. Let $\underline{C} = (C_1, \ldots, C_n)$ be a finite sequence of conjugacy classes of G. Let $\Sigma(\underline{C})$ be the set of generating tuples $\underline{g} = (g_1, \ldots, g_n)$ such that $g_i \in C_i$ for all i.

The group $\mathrm{Inn}(G) = G/Z(G)$ of inner automorphims of G acts on G^n via

$$x \cdot \underline{g} = x \cdot (g_1, \ldots, g_n) = \underline{g}^x = (xg_1x^{-1}, \ldots, xg_nx^{-1})$$

and restricts to an action of $\mathrm{Inn}(G)$ on $\underline{C}$.

To avoid trivialities, suppose that $\Sigma(\underline{C}) \neq \emptyset$. Then the action of $\mathrm{Inn}(G) \simeq G/Z(G)$ on $\Sigma(\underline{C})$ has no fixed points: if $z \in G$ fixes $\underline{g}$, then z commutes with each g_i hence with $\langle g_1, \ldots, g_n \rangle = G$, so $z \in Z(G)$. If in addition $Z(G) = \{1\}$, then the action of G by conjugation on $\Sigma(\underline{C})$ is free.

Now suppose that $n = 3$; we call a 3-tuple a triple. For every generating triple $\underline{g}$, we obtain from the Riemann Existence Theorem [86, Theorem 2.13] a G-Galois branched covering $X(\underline{g}) \to \mathbb{P}^1$ defined over $\overline{\mathbb{Q}}$ with ramification type $\underline{g}$ over $0, 1, \infty$ and Galois group G. Two such covers $f\colon X(\underline{g}) \to \mathbb{P}^1$ and $f'\colon X(\underline{g}') \to \mathbb{P}^1$ are isomorphic as covers if and only if there exists $\varphi \in \mathrm{Aut}(G)$ such that $\varphi(\underline{g}) = (\varphi(g_1), \ldots, \varphi(g_n)) = \underline{g}'$, and as G-Galois covers if and only if there exists $x \in G$ such that $\underline{g}^x = (\underline{g}')^x$.

The group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the set of generating tuples for G up to automorphism (or simply inner automorphism) via its action on the covers. Coming to grips with the mysteries of this action in general is part of Grothendieck's program of *dessin d'enfants* [30]: to understand $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ via its faithful action on the fundamental group of $\mathbb{P}^1_{\overline{\mathbb{Q}}} \smallsetminus \{0, 1, \infty\}$. There is one aspect of the action which is partially understood, coming from the maximal abelian extension of $\mathbb{Q}$ generated by roots of unity.

Let $\zeta_s = \exp(2\pi i/s) \in \mathbb{C}$ be a primitive sth root of unity for $s \in \mathbb{Z}_{\geq 2}$. The group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ acts on conjugacy classes of G via the cyclotomic character χ, as follows. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ and let C be a conjugacy class of G represented by $g \in C$ with g of order m. Then $\sigma(\zeta_m) = \zeta_m^a$ for some $a = \chi(\sigma) \in (\mathbb{Z}/m\mathbb{Z})^\times$ and $\sigma \cdot C$ is the conjugacy class of $g^{\chi(\sigma)}$ in G. Put another way, let m be the exponent of G. Then the group $(\mathbb{Z}/m\mathbb{Z})^\times$ acts on G by $s \cdot g = g^s$ for $s \in (\mathbb{Z}/m\mathbb{Z})^\times$ and $g \in G$ and this induces an action on conjugacy classes. Pulling back by the canonical isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^\times$ defines the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ and hence also $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ on conjugacy classes of G.

Let $H_{\mathrm{r}} \subseteq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ be the kernel of this action:

$$H_{\mathrm{r}}(G) = \{s \in (\mathbb{Z}/m\mathbb{Z})^\times\colon C^s = C \text{ for all conjugacy classes } C \text{ of } G\}.$$

The fixed field $F_{\mathrm{r}}(G) = \mathbb{Q}(\zeta_m)^{H_{\mathrm{r}}}$ is called the field of rationality of G. The field $F_{\mathrm{r}}(G)$ can also be characterized as the field obtained by adjoining to $\mathbb{Q}$ the values of the character table of G. Let

$$H_{\mathrm{r}}(\underline{C}) = \{s \in (\mathbb{Z}/m\mathbb{Z})^\times\colon\ C_i^s = C_i \text{ for all } i\}$$

be the stabilizer of $\underline{C}$ under this action. We define the field of rationality of $\underline{C}$ to be

$$F_{\mathrm{r}}(\underline{C}) = \mathbb{Q}(\zeta_m)^{H_{\mathrm{r}}(\underline{C})}.$$

Similarly, let

$$H_{\mathrm{wr}}(\underline{C}) = \{s \in (\mathbb{Z}/m\mathbb{Z})^\times\colon \underline{C}^s = \varphi(\underline{C}) \text{ for some } \varphi \in \mathrm{Aut}(G)\}.$$

We define the field of weak rationality of $\underline{C}$ to be $F_{\mathrm{wr}}(\underline{C}) = \mathbb{Q}(\zeta_m)^{H_{\mathrm{wr}}(\underline{C})}$. Then

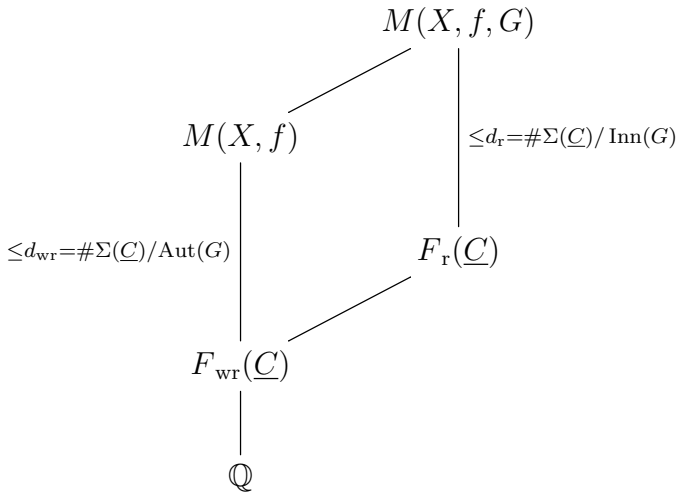
$$F_{\mathrm{wr}}(\underline{C}) \subseteq F_{\mathrm{r}}(\underline{C}) \subseteq F_{\mathrm{r}}(G).$$

The group $\mathrm{Gal}(\overline{\mathbb{Q}}/F_{\mathrm{wr}}(\underline{C}))$ acts on the set of generating tuples $\underline{g} \in \Sigma(\underline{C})$ up to uniform automorphism, which we denote $\Sigma(\underline{C})/\mathrm{Aut}(G)$. For $\underline{g} \in \Sigma(\underline{C})$, the cover $f\colon X = X(\underline{g}) \to \mathbb{P}^1$

has field of moduli $M(X,f)$ equal to the fixed field of the kernel of this action, a number field of degree at most $d_{\mathrm{wr}} = \#\Sigma(\underline{C})/\mathrm{Aut}(G)$ over $F_{\mathrm{wr}}(\underline{C})$.

Similarly, a G-Galois branched cover $f\colon X \to \mathbb{P}^1$ (equipped with its isomorphism $i\colon G \xrightarrow{\sim} \mathrm{Aut}(X,f)$) has field of moduli $M(X,f,G)$ equal to the fixed field of the stabilizer of the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/F_{\mathrm{r}}(\underline{C}))$, a number field of degree $\leq d_{\mathrm{r}} = \#\Sigma(\underline{C})/\operatorname{Inn}(G)$ over $F_{\mathrm{r}}(\underline{C})$.

Therefore, we have the following diagram of fields.



The simplest case of this setup is as follows. We say that $\underline{C}$ is rigid if the action of $\mathrm{Inn}(G)$ on $\Sigma(\underline{C})$ is transitive. By the above, if $\Sigma(\underline{C})$ is rigid then this action is simply transitive and so endows $\Sigma(\underline{C})$ with the structure of a torsor under $G = \mathrm{Inn}(G)$. In this case, the diagram collapses to

$$M(X,f,G) = F_{\mathrm{r}}(\underline{C}) \supseteq M(X,f) = F_{\mathrm{wr}}(\underline{C}).$$

More generally, we say that $\underline{C}$ is weakly rigid if for all $\underline{g}, \underline{g}' \in \Sigma(\underline{C})$ there exists $\varphi \in \mathrm{Aut}(G)$ such that $\varphi(\underline{g}) = \underline{g}'$. (Coombes and Harbater [15] say inner rigid and outer rigid for rigid and weakly rigid, respectively.) If $\underline{C}$ is weakly rigid, and $X = X(\underline{g})$ with $\underline{g} \in \underline{C}$, then $M(X,f) = F_{\mathrm{wr}}(\underline{C})$ and the group $\mathrm{Gal}(M(X,f,G)/F_{\mathrm{r}})$ injects canonically into the outer automorphism group $\mathrm{Out}(G) = \mathrm{Aut}(G)/\operatorname{Inn}(G)$.

We summarize the above discussion in the following proposition.

Proposition 6.1. *Let G be a group with trivial center. Let $\underline{g} = (g_1, \ldots, g_n)$ be a generating tuple for G and let $\underline{C} = (C_1, \ldots, C_n)$, where C_i is the conjugacy class of g_i. Let $P_1, \ldots, P_n \in \mathbb{P}^1(\overline{\mathbb{Q}})$. Then the following statements hold.*

(a) *There exists a branched covering $f\colon X \to \mathbb{P}^1$ with ramification type $\underline{C} = (C_1, \ldots, C_n)$ over the points $P_1, \ldots, P_n$ and an isomorphism $G \xrightarrow{\sim} \mathrm{Aut}(X,f)$, all defined over $\overline{\mathbb{Q}}$.*

(b) *The field of moduli $M(X,f)$ of f is a number field of degree at most*

$$d_{\mathrm{wr}} = \#\Sigma(\underline{C})/\mathrm{Aut}(G)$$

over $F_{\mathrm{wr}}(\underline{C})$.

(c) *The field of moduli $M(X,f,G)$ of f as a G-Galois branched cover is a number field of degree at most*

$$d_{\mathrm{r}} = \#\Sigma(\underline{C})/\operatorname{Inn}(G)$$

over $F_{\mathrm{r}}(\underline{C})$.

7. Conjugacy classes, fields of rationality

Let p be a prime number and $q = p^r$ a prime power. Let $\mathbb{F}_q$ be a field with q elements and algebraic closure $\overline{\mathbb{F}}_q$. In this section, we record some basic but crucial facts concerning conjugacy classes and automorphisms in the finite matrix groups arising from $\mathrm{GL}_2(\mathbb{F}_q)$; see Huppert [33, §II.8] for a reference.

First let $g \in \mathrm{GL}_2(\mathbb{F}_q)$. By the Jordan canonical form, exactly one of the following holds:

(1) The characteristic polynomial $f(g;T) \in \mathbb{F}_q[T]$ has two repeated roots (in $\mathbb{F}_q$), and hence g is either a scalar matrix (central in $\mathrm{GL}_2(\mathbb{F}_q)$) or g is conjugate to a matrix of the form $\begin{pmatrix} t & 1 \\ 0 & t \end{pmatrix}$ with $t \in \mathbb{F}_q^\times$; or

(2) $f(g;T)$ has distinct roots (in $\overline{\mathbb{F}}_q$) and the conjugacy class of g is uniquely determined by $f(g;T)$, and we say g is semisimple.

Let $\mathrm{PGL}_2(\mathbb{F}_q) = \mathrm{GL}_2(\mathbb{F}_q)/\mathbb{F}_q^\times$ and let $\overline{g}$ be the image of g under the natural reduction map $\mathrm{GL}_2(\mathbb{F}_q) \to \mathrm{PGL}_2(\mathbb{F}_q)$. We have $\overline{g} = \overline{1}$ iff g is a scalar matrix. If g is conjugate to $\begin{pmatrix} t & 1 \\ 0 & t \end{pmatrix}$, then $\overline{g}$ is conjugate to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and we say that $\overline{g}$ is unipotent. If $f(g;T)$ is semisimple, then in the quotient the conjugacy classes associated to $f(g;T)$ and $f(cg;T) = c^2 f(g;c^{-1}T)$ for $c \in \mathbb{F}_q^\times$ become identified. If $f(g;T)$ factors over $\mathbb{F}_q$ then $\overline{g}$ is conjugate in $\mathrm{PGL}_2(\mathbb{F}_q)$ to the image of a matrix $\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}$ with $x \in \mathbb{F}_q^\times \smallsetminus \{1\}$, and we say that $\overline{g}$ is split (semisimple). The set of split semisimple conjugacy classes in $\mathrm{PGL}_2(\mathbb{F}_q)$ is therefore in bijection with the set

$$\{\{x, x^{-1}\} \colon x \in \mathbb{F}_q^\times \smallsetminus \{1\}\}. \tag{7.1}$$

There are $(q-3)/2+1 = (q-1)/2$ such classes if q is odd, and $(q-2)/2 = q/2-1$ such classes if q is even. On the other hand, the conjugacy classes of semisimple elements with irreducible $f(g;T)$ are in bijection with the set of monic, irreducible polynomials $f(T) \in \mathbb{F}_q[T]$ of degree 2 up to rescaling $x \mapsto ax$ with $a \in \mathbb{F}_q^\times$. There are $q(q-1)/2$ such monic irreducible quadratic polynomials $T^2 - aT + b$; for any such polynomial with $a \neq 0$, there is a unique rescaling such that $a = 1$; when q is odd, there is a unique such polynomial with $a = 0$ up to rescaling. Therefore, the total number of conjugacy classes is $(q(q-1)/2)/(q-1) = q/2$ when q is even and $(q(q-1)/2 - (q-1)/2)/(q-1) + 1 = (q-1)/2$ when q is odd. Equivalently, the set of nonsplit semisimple conjugacy classes in $\mathrm{PGL}_2(\mathbb{F}_q)$ is in bijection with the set

$$\{\{y, y^q\} \colon y \in (\mathbb{F}_{q^2} \smallsetminus \mathbb{F}_q)/\mathbb{F}_q^\times\} \tag{7.2}$$

by taking roots.

Now let $g \in \mathrm{SL}_2(\mathbb{F}_q)$ with $g \neq \pm 1$. Suppose first that $f(g;T)$ has a repeated root, necessarily ± 1; then we say that g is unipotent. For $u \in \mathbb{F}_q$, let $U(u) = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$. Using Jordan canonical form we find that g is conjugate to $\pm U(u)$ for some $u \in \mathbb{F}_q^\times$. The matrices $U(u)$ and $U(v)$ are conjugate if and only if $uv^{-1} \in \mathbb{F}_q^{\times 2}$. Thus, if q is odd there are four nontrivial conjugacy classes associated to characteristic polynomials with repeated roots, whereas if q is even there is a single such conjugacy class.

Otherwise the element g is semisimple and so g is conjugate in $\mathrm{SL}_2(\mathbb{F}_q)$ to the matrix $\begin{pmatrix} 0 & -1 \\ 1 & \mathrm{tr}(g) \end{pmatrix}$ by rational canonical form, and the trace map provides a bijection between the set of conjugacy classes of semisimple elements of $\mathrm{SL}_2(\mathbb{F}_q)$ and elements $\alpha \in \mathbb{F}_q$ with $\alpha \neq \pm 2$.

Finally, we give the corresponding description in $\mathrm{PSL}_2(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)/\{\pm 1\}$. When $p = 2$ we have $\mathrm{PSL}_2(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)$, so assume that p is odd. Then the conjugacy classes of the matrices $U(u)$ and $-U(u)$ in $\mathrm{SL}_2(\mathbb{F}_q)$ become identified in $\mathrm{PSL}_2(\mathbb{F}_q)$, so there are precisely two nontrivial unipotent conjugacy classes, each consisting of elements of order p. If g is a semisimple element of $\mathrm{SL}_2(\mathbb{F}_q)$ of order a, then the order of its image $\pm g$ in $\mathrm{PSL}_2(\mathbb{F}_q)$ is $a/\gcd(a, 2)$. We define the trace of an element $\pm g \in \mathrm{PSL}_2(\mathbb{F}_q)$ to be $\mathrm{tr}(\pm g) = \{\mathrm{tr}(g), -\mathrm{tr}(g)\} \subseteq \mathbb{F}_q$ and define the trace field of $\pm g$ to be $\mathbb{F}_p(\mathrm{tr}(\pm g))$. The conjugacy class, and therefore the order, of a semisimple element of $\mathrm{PSL}_2(\mathbb{F}_q)$ is then again uniquely determined by its trace. (This is particular to $\mathrm{PSL}_2(\mathbb{F}_q)$—the trace does not determine a conjugacy class in $\mathrm{PGL}_2(\mathbb{F}_q)$!)

We now describe outer automorphism groups (see e.g. Suzuki [76]). The p-power Frobenius map σ, acting on the entries of a matrix by $a \mapsto a^p$, gives an outer automorphism of $\mathrm{PSL}_2(\mathbb{F}_q)$ and $\mathrm{PGL}_2(\mathbb{F}_q)$, and in fact $\mathrm{Out}(\mathrm{PGL}_2(\mathbb{F}_q)) = \langle \sigma \rangle$. When p is odd, the map τ given by conjugation by an element in $\mathrm{PGL}_2(\mathbb{F}_q) \smallsetminus \mathrm{PSL}_2(\mathbb{F}_q)$ is also an outer automorphism of $\mathrm{PSL}_2(\mathbb{F}_q)$, and these maps generate $\mathrm{Out}(\mathrm{PSL}_2(\mathbb{F}_q))$:

$$\mathrm{Out}(\mathrm{PSL}_2(\mathbb{F}_q)) \simeq \begin{cases} \langle \sigma, \tau \rangle, & \text{if } p \text{ is odd;} \\ \langle \sigma \rangle, & \text{if } p = 2. \end{cases} \tag{7.3}$$

In particular, the order of $\mathrm{Out}(\mathrm{PSL}_2(\mathbb{F}_q))$ is $2r$ if p is odd and r if $p = 2$. From the embedding $\mathrm{PGL}_2(\mathbb{F}_q) \hookrightarrow \mathrm{PSL}_2(\mathbb{F}_{q^2})$, given explicitly by $\pm g \mapsto \pm(\det g)^{-1/2} g$, we may also view the outer automorphism τ as conjugation by an element of $\mathrm{PSL}_2(\mathbb{F}_{q^2}) \smallsetminus \mathrm{PSL}_2(\mathbb{F}_q)$.

We conclude this section by describing the field of rationality (as defined in section 6) for these conjugacy classes.

Lemma 7.4. *Let $\overline{g} \in \mathrm{PGL}_2(\mathbb{F}_q)$ have order m. Then the field of rationality of the conjugacy class C of $\overline{g}$ is*

$$F_{\mathrm{r}}(C) = \begin{cases} \mathbb{Q}(\lambda_m), & \text{if } \overline{g} \text{ is semisimple;} \\ \mathbb{Q}, & \text{if } \overline{g} \text{ is unipotent;} \end{cases}$$

and the field of weak rationality of C is

$$F_{\mathrm{wr}}(C) = \begin{cases} \mathbb{Q}(\lambda_m)^{\langle \mathrm{Frob}_p \rangle}, & \text{if } \overline{g} \text{ is semisimple;} \\ \mathbb{Q}, & \text{if } \overline{g} \text{ is unipotent.} \end{cases}$$

Proof. A power of a unipotent conjugacy class is unipotent or trivial so its field of rationality and weak rationality is $\mathbb{Q}$.

If C is split semisimple, corresponding to $\{x, x^{-1}\}$ by (7.1) with $x \in \mathbb{F}_q^\times \smallsetminus \{1\}$ then $\overline{g} \mapsto \overline{g}^s$ for $s \in (\mathbb{Z}/m\mathbb{Z})^\times$ corresponds to the map $x \mapsto x^s$ and it stabilizes the set $\{x, x^{-1}\}$ (resp. up to an automorphism of $\mathrm{PGL}_2(\mathbb{F}_q)$) if and only if $s \in \langle -1 \rangle \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$ (resp. $s \in \langle -1, p \rangle$).

Next consider the case where C is nonsplit semisimple, corresponding to $\{y, y^q\}$ by (7.2) with $y \in (\mathbb{F}_{q^2} \smallsetminus \mathbb{F}_q)/\mathbb{F}_q^\times$. Then the map $\overline{g} \mapsto g^s$ again with $s \in (\mathbb{Z}/m\mathbb{Z})^\times$ corresponds to the map $y \mapsto y^s$. We have $y \in \mathbb{F}_{q^2}^\times \simeq \mathbb{Z}/(q^2 - 1)\mathbb{Z}$, with the image of $\mathbb{F}_q^\times$ the subgroup

$(q+1)\mathbb{Z}/(q^2-1)\mathbb{Z}$, so the set $\{y, y^q\}$ is stable if and only if $s \in \{1, q\} = \langle -1 \rangle \pmod m$, and the set is stable up to an automorphism of $\mathrm{PGL}_2(\mathbb{F}_q)$ if and only if $s \in \langle -1, p \rangle \subset \mathbb{Z}/m\mathbb{Z}$, so we have the same result as in the split case. □

For an odd prime p, we abbreviate $p^* = (-1)^{(p-1)/2}p$. Recall that $q = p^r$.

Lemma 7.5. *Let $\pm g \in \mathrm{PSL}_2(\mathbb{F}_q)$ have order m. Then the field of rationality of the conjugacy class C of g is*

$$F_{\mathrm{r}}(C) = \begin{cases} \mathbb{Q}(\lambda_m), & \text{if } g \text{ is semisimple;} \\ \mathbb{Q}(\sqrt{p^*}), & \text{if } g \text{ is unipotent and } pr \text{ is odd;} \\ \mathbb{Q}, & \text{otherwise.} \end{cases}$$

The field of weak rationality of C is

$$F_{\mathrm{wr}}(C) = \begin{cases} \mathbb{Q}(\lambda_m)^{\langle \mathrm{Frob}_p \rangle}, & \text{if } g \text{ is semisimple;} \\ \mathbb{Q}, & \text{otherwise,} \end{cases}$$

where $\mathrm{Frob}_p \in \mathrm{Gal}(\mathbb{Q}(\lambda_m)/\mathbb{Q})$ is the Frobenius element associated to the prime p.

Proof. First, suppose $\pm g = \pm U(u)$ is unipotent with $u \in \mathbb{F}_q^\times$. Then for all integers s prime to p, we have $(\pm g)^s = \pm U(su)$. Thus, the subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times$ stabilizing C is precisely the set of elements of $\mathbb{F}_p^\times$ which are squares in $\mathbb{F}_q^\times$. Thus if $p = 2$ or r is even, this subgroup is all of $\mathbb{F}_p^\times$ so that the field of rationality of C is $\mathbb{Q}$, whereas if pr is odd this subgroup is the unique index two subgroup of $\mathbb{F}_p^\times$ and the corresponding field of rationality for C in $\mathrm{PSL}_2(\mathbb{F}_q)$ is $\mathbb{Q}(\sqrt{p^*})$.

Next we consider semisimple conjugacy classes. By the trace map, these classes are in bijection with $\pm t \in \pm\mathbb{F}_q \smallsetminus \{\pm 2\}$. The induced action on the set of traces is given by $\pm t = \pm(z + 1/z) \mapsto \pm(z^s + 1/z^s)$ for $s \in (\mathbb{Z}/m\mathbb{Z})^\times$ where z is a primitive mth root of unity. From this description, we see that the stabilizer is $\langle -1 \rangle \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$.

A similar analysis yields the field of weak rationality. If C is unipotent then τ identifies the two unipotent conjugacy classes so the field of weak rationality is always $\mathbb{Q}$. If C is semisimple then σ identifies C with C^p so the stabilizer of $\pm t$ is $\langle -1, p \rangle \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$, the field fixed further under the Frobenius Frob_p. □

8. Subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ and $\mathrm{PGL}_2(\mathbb{F}_q)$ and weak rigidity

The general theory developed for triples in section 6 can be further applied to the groups $\mathrm{PSL}_2(\mathbb{F}_q)$ (and consequently $\mathrm{PGL}_2(\mathbb{F}_q)$) using work of Macbeath [43], which we recall in this section. See also Langer and Rosenberger [41], who give an exposition of Macbeath's work in our context.

Let q be a prime power. We begin by considering triples $\underline{g} = (g_1, g_2, g_3)$ with $g_i \in \mathrm{SL}_2(\mathbb{F}_q)$ – we remind the reader that the terminology implies $g_1g_2g_3 = 1$ and does not imply that $\langle g_1, g_2, g_3 \rangle = \mathrm{SL}_2(\mathbb{F}_q)$ – with an eye to understanding the image of the subgroup generated by g_1, g_2, g_3 in $\mathrm{PSL}_2(\mathbb{F}_q)$ according to the traces of the corresponding elements. Long periods of consternation have taught us that the difference between a matrix and a matrix up to sign plays an important role here, and so we keep this in our notation. Moreover, because we will be considering other kinds of triples, we refer to $\underline{g} = (g_1, g_2, g_3)$ as a group triple.

A trace triple is a triple $\underline{t} = (t_1, t_2, t_3) \in \mathbb{F}_q^3$. For a trace triple $\underline{t}$, let $T(\underline{t})$ denote the set of group triples $\underline{g}$ such that $\mathrm{tr}(g_i) = t_i$ for $i = 1, 2, 3$. The group $\mathrm{Inn}(\mathrm{SL}_2(\mathbb{F}_q)) = \mathrm{PSL}_2(\mathbb{F}_q)$ acts on $T(\underline{t})$ by conjugation.

Proposition 8.1 (Macbeath [43, Theorem 1])**.** *For all trace triples $\underline{t}$, the set $T(\underline{t})$ is nonempty.*

To a group triple $\underline{g} = (g_1, g_2, g_3) \in \mathrm{SL}_2(\mathbb{F}_q)^3$, we associate the order triple (a, b, c) by letting a be the order of $\pm g_1 \in \mathrm{PSL}_2(\mathbb{F}_q)$, and similarly b the order of $\pm g_2$ and c the order of $\pm g_3$. Without loss of generality, as in the definition of the triangle group (2.2) we may assume that an order triple (a, b, c) has $a \leq b \leq c$.

Our goal is to give conditions under which we can be assured that a group triple generates $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$ and not a smaller group. We do this by placing restrictions on the associated trace triples, which come in three kinds.

A trace triple $\underline{t}$ is commutative if there exists $\underline{g} \in T(\underline{t})$ such that the group $\pm\langle g_1, g_2, g_3\rangle \subseteq \mathrm{PSL}_2(\mathbb{F}_q)$ is commutative. By a direct calculation, Macbeath proves that a triple $\underline{t}$ is commutative if and only if the ternary $\mathbb{F}_q$-quadratic form

$$x^2 + y^2 + z^2 + t_1 yz + t_2 xz + t_3 xy$$

is singular [43, Corollary 1, p. 21], i.e. if and only if its (half-)discriminant

$$d(\underline{t}) = d(t_1, t_2, t_3) = t_1^2 + t_2^2 + t_3^2 - t_1 t_2 t_3 - 4 \tag{8.2}$$

is zero. If a trace triple $\underline{t}$ is not commutative, then the order triple (a, b, c) is the same for any $\underline{g} \in T(\underline{t})$: the trace uniquely defines the order of a semisimple or unipotent element, and if some g_i is scalar in $\underline{g} \in T(\underline{t})$ then the group it generates is necessarily commutative.

A trace triple $\underline{t}$ is exceptional if there exists a triple $\underline{g} \in T(\underline{t})$ with order triple equal to $(2, 2, c)$ with $c \geq 2$ or one of

$$(2,3,3), (3,3,3), (3,4,4), (2,3,4), (2,5,5), (5,5,5), (3,3,5), (3,5,5), (2,3,5). \tag{8.3}$$

Put another way, a trace triple $\underline{t}$ is exceptional if there exists $\underline{g} \in T(\underline{t})$ whose order triple is the same as that of a triple of elements of $\mathrm{SL}_2(\mathbb{F}_q)$ that generates a finite spherical triangle group in $\mathrm{PSL}_2(\mathbb{F}_q)$.

Finally, a trace triple $\underline{t}$ is projective if for all $\underline{g} = (g_1, g_2, g_3) \in T(\underline{t})$, the subgroup $\pm\langle g_1, g_2, g_3\rangle \subseteq \mathrm{PSL}_2(\mathbb{F}_q)$ is conjugate to a subgroup of the form $\mathrm{PSL}_2(k)$ or $\mathrm{PGL}_2(k)$ for $k \subseteq \mathbb{F}_q$ a subfield.

Remark 8.4. There are no trace triples which are both projective and commutative. A projective trace triple may be exceptional, but the possibilities can be explicitly described as follows. A trace triple is exceptional if there is a homomorphism from a finite spherical group to $\mathrm{PSL}_2(\mathbb{F}_q)$ with order triple as given in (8.3); a trace triple is projective if the image is conjugate to $\mathrm{PSL}_2(k)$ or $\mathrm{PGL}_2(k)$ for $k \subseteq \mathbb{F}_q$ a subfield. From the classification of finite spherical groups, this homomorphism must be one of the following exceptional isomorphisms:

$$D_6 \simeq \mathrm{GL}_2(\mathbb{F}_2),\ A_4 \simeq \mathrm{PSL}_2(\mathbb{F}_3),\ S_4 \simeq \mathrm{PGL}_2(\mathbb{F}_3),\ \text{or } A_5 \simeq \mathrm{PGL}_2(\mathbb{F}_4) \simeq \mathrm{PSL}_2(\mathbb{F}_5).$$

Any trace triple $\underline{t}$ with $\mathbb{F}_p(\underline{t}) = \mathbb{F}_p(t_1, t_2, t_3) = \mathbb{F}_q$ that is both exceptional and projective corresponds to one of these isomorphisms.

We now come to Macbeath's classification of subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ generated by two elements.

Theorem 8.5 ([43, Theorem 4])**.** *Every trace triple $\underline{t}$ is exceptional, commutative or projective.*

Example 8.6. We illustrate the above with the case $q = 7$. There are a total of $7^3 = 243$ trace triples.

First, the trace triples where the order triple is *not* well-defined are the trace triples

$$(2, 2, 2), (2, -2, -2), (-2, 2, -2), (-2, -2, 2)$$

which are commutative. Multiplication by -1 plays an obvious role here, so in this example, for a trace triple $\underline{t} = (t_1, t_2, t_3)$ we say that a trace triple agrees with $\underline{t}$ with an even number of signs if it is one of

$$(t_1, t_2, t_3), (t_1, -t_2, -t_3), (-t_1, t_2, -t_3), (-t_1, -t_2, t_3).$$

Put this way, the trace triples where the order triple is not well-defined are those agreeing with $(2, 2, 2)$ with an even number of signs. We define odd number of signs analogously. For each of these four trace triples, there exists a group triple $\underline{g}$ with order triple $(1, 1, 1)$, $(1, 7, 7)$, or $(7, 7, 7)$.

The other commutative trace triples are:

$(2, 0, 0)$, with any signs	having orders $(1, 2, 2)$
$(2, 1, 1)$, with even number of signs	having orders $(1, 3, 3)$
$(2, 3, 3)$, with even number of signs	having orders $(1, 4, 4)$
$(0, 0, 0)$, with any signs	having orders $(2, 2, 2)$
$(0, 3, 3)$, with any signs	having orders $(2, 4, 4)$
$(1, 1, -1)$, with odd number of signs	having orders $(3, 3, 3)$

Indeed, these are all values $(t_1, t_2, t_3) \in \mathbb{F}_q^3$ such that

$$d(t_1, t_2, t_3) = t_1^2 + t_2^2 + t_3^2 - t_1 t_2 t_3 - 4 = 0.$$

The three commutative trace triples $(0, 0, 0), (0, 3, 3), (1, 1, -1)$ are also exceptional. The remaining exceptional triples are:

$(0, 0, 1)$, with any signs	having orders $(2, 2, 3)$
$(0, 0, 3)$, with any signs	having orders $(2, 2, 4)$
$(0, 1, 1)$, with any signs	having orders $(2, 3, 3)$
$(0, 1, 3)$, with any signs	having orders $(2, 3, 4)$
$(1, 1, 1)$, with even number of signs	having orders $(3, 3, 3)$
$(1, 3, 3)$, with any signs	having orders $(3, 4, 4)$

All other triples are projective:

$(0,1,2)$, with any signs	having orders $(2,3,7)$
$(0,3,2)$, with any signs	having orders $(2,4,7)$
$(0,2,2)$, with any signs	having orders $(2,7,7)$
$(1,1,3)$, with any signs	having orders $(3,3,4)$
$(1,1,2)$, with any signs	having orders $(3,3,7)$
$(1,3,2)$, with any signs	having orders $(3,4,7)$
$(1,2,2)$, with any signs	having orders $(3,7,7)$
$(3,3,3)$, with any signs	having orders $(4,4,4)$
$(3,3,-2)$, with odd number of signs	having orders $(4,4,7)$
$(3,2,2)$, with any signs	having orders $(4,7,7)$
$(2,2,-2)$, with odd number of signs	having orders $(7,7,7)$

We note that the triples $(1,3,-3)$ with an odd number of signs in fact generate $\mathrm{PSL}_2(\mathbb{F}_7)$—but the triple is not projective. In particular, we observe that one cannot deduce that a nonsingular trace triple is projective by looking only at its order triple.

Finally, the issue that this example is supposed to make clear is that changing signs on a trace triple may change the subgroup of $\mathrm{PSL}_2(\mathbb{F}_q)$ that a corresponding group triple generates. Indeed, changing an odd number of signs on a group triple does not yield a group triple!

We now consider the role of -1 and the parity of these signs (taking an even or odd number).

Lemma 8.7. *Let $\underline{t} = (t_1, t_2, t_3) \in \mathbb{F}_q^3$ be a trace triple.*

(a) *There are bijections*

$$T(\underline{t}) \leftrightarrow T(t_1, -t_2, -t_3) \leftrightarrow T(-t_1, t_2, -t_3) \leftrightarrow T(-t_1, -t_2, t_3)$$
$$(g_1, g_2, g_3) \mapsto (g_1, -g_2, -g_3) \mapsto (-g_1, g_2, -g_3) \mapsto (-g_1, -g_2, g_3)$$

which preserve the subgroups generated by each triple. In particular, if $\underline{t}$ is commutative (resp. exceptional, projective), then so is each of

$$(t_1, -t_2, -t_3), (-t_1, t_2, -t_3), (-t_1, -t_2, t_3).$$

(b) *Suppose q is odd. If $\underline{t}$ is commutative, then $(-t_1, t_2, t_3)$ is commutative if and only if $t_1 t_2 t_3 = 0$.*

Proof. Part (a) is clear. As for part (b): the trace triple $\underline{t}$ is commutative if and only if $d(t_1, t_2, t_3) = 0$. So $(-t_1, t_2, t_3)$ is also commutative if and only if $d(-t_1, t_2, t_3) = 0$ if and only if $d(t_1, t_2, t_3) - d(-t_1, t_2, t_3) = 2t_1 t_2 t_3 = 0$, as claimed. □

Let ℓ/k be a separable quadratic extension. We say that $t \in \ell$ is a square root from k if $t = 0$ or $t = \sqrt{u}$ with $u \in k^\times \smallsetminus k^{\times 2}$. A trace triple $\underline{t}$ is irregular [43, p. 28] if the field $\mathbb{F}_p(\underline{t}) = \mathbb{F}_p(t_1, t_2, t_3) \subseteq \mathbb{F}_q$ has a subfield $k \subseteq \mathbb{F}_p(\underline{t})$ such that

(i) $[\mathbb{F}_p(\underline{t}) : k] = 2$ and
(ii) after reordering, we have $t_1 \in k$ and t_2, t_3 are square roots from k.

Otherwise, $\underline{t}$ is regular. Of course, if $[\mathbb{F}_p(\underline{t}) : \mathbb{F}_p]$ is odd—e.g., if $[\mathbb{F}_q : \mathbb{F}_p]$ is odd—then $\underline{t}$ is necessarily regular.

Proposition 8.8 ([43, Theorem 3])**.** *Let $\underline{g}$ generate a projective subgroup $G = \pm\langle g_1, g_2, g_3\rangle \subseteq \mathrm{PSL}_2(\mathbb{F}_q)$ and let $\underline{t}$ be its trace triple.*

(a) *Suppose $\underline{t}$ is regular. Then G is conjugate in $\mathrm{PSL}_2(\mathbb{F}_q)$ to $\mathrm{PSL}_2(\mathbb{F}_p(\underline{t}))$.*
(b) *Suppose $\underline{t}$ is irregular, and let k_0 be the unique index 2 subfield of $\mathbb{F}_p(\underline{t})$. Then G is conjugate in $\mathrm{PSL}_2(\mathbb{F}_q)$ to either $\mathrm{PSL}_2(\mathbb{F}_p(\underline{t}))$ or $\mathrm{PGL}_2(k_0)$.*
(c) *Suppose $k = \mathbb{F}_q$. Then the number of orbits of $\mathrm{Inn}(\mathrm{SL}_2(\mathbb{F}_q)) = \mathrm{PSL}_2(\mathbb{F}_q)$ on $T(\underline{t})$ is 2 or 1 according as p is odd or $p = 2$.*
(d) *For all $\underline{g}' \in T(\underline{t})$, there exists $m \in \mathrm{SL}_2(\overline{\mathbb{F}}_q)$ such that $m^{-1}\underline{g}m = \underline{g}'$.*

We say that a trace triple $\underline{t}$ is of PSL_2-type (resp. of PGL_2-type) if $\underline{t}$ is projective and for all $\underline{g} \in T(\underline{t})$ the group $\pm\langle g_1, g_2, g_3\rangle$ is conjugate to $\mathrm{PSL}_2(k)$ (resp. $\mathrm{PGL}_2(k_0)$); by Proposition 8.8(a), every projective triple is either of PSL_2-type or of PGL_2-type.

We now transfer these results to trace triples in the projective groups $\mathrm{PSL}_2(\mathbb{F}_q)$. The passage from $\mathrm{SL}_2(\mathbb{F}_q)$ to $\mathrm{PSL}_2(\mathbb{F}_q)$ identifies conjugacy classes whose traces have opposite signs, so associated to a triple of conjugacy classes $\underline{C}$ in $\mathrm{PSL}_2(\mathbb{F}_q)$ is a trace triple $(\pm t_1, \pm t_2, \pm t_3)$, which we abbreviate $\pm\underline{t}$ (remembering that the signs may be taken independently). We call $\pm\underline{t}$ a trace triple up to signs.

Let $\pm\underline{t}$ be a trace triple up to signs. We say $\pm\underline{t}$ is commutative if there exists $\pm\underline{g} \in T(\pm\underline{t})$ such that $\pm\langle g_1, g_2, g_3\rangle$ is commutative. We say $\pm\underline{t}$ is exceptional if there exists a lift of $\pm\underline{t}$ to a trace triple $\underline{t}$ such that the associated order triple (a, b, c) is exceptional. Finally, we say $\pm\underline{t}$ is projective if all lifts $\underline{t}$ of $\pm\underline{t}$ are projective, and partly projective if there exists a lift $\underline{t}$ of $\pm\underline{t}$ that is projective.

Lemma 8.9. *Every trace triple up to signs is exceptional, commutative, or partly projective.*

Proof. This follows from Theorem 8.5 and Lemma 8.7. □

To a nonsingular trace triple up to signs $\pm\underline{t}$, we associate the order triple (a, b, c) as the order triple associated to any lift $\underline{t}$ of $\pm\underline{t} = (\pm t_1, \pm t_2, \pm t_3)$; this is well defined because we took orders of elements in $\mathrm{PSL}_2(\mathbb{F}_q)$ from the very beginning. Similarly, we write $\mathbb{F}_p(\pm\underline{t})$ for the field generated by any lift of t_i, so that $\mathbb{F}_p(\underline{t}) = \mathbb{F}_p(\pm\underline{t}) = \mathbb{F}_q$. We assume that $a \le b \le c$; Remark 2.2 explains why this is no loss of generality.

For a triple of conjugacy classes $\underline{C} = (C_1, C_2, C_3)$ of $\mathrm{PSL}_2(\mathbb{F}_q)$, recall we have defined $\Sigma(\underline{C})$ to be the set of generating triples $\underline{g} = (g_1, g_2, g_3)$ such that $g_i \in C_i$.

Proposition 8.10. *Let $\underline{C}$ be a triple of conjugacy classes in $\mathrm{PSL}_2(\mathbb{F}_q)$. Let $\pm\underline{t}$ be the associated trace triple up to signs, let $\mathbb{F}_q = \mathbb{F}_p(\pm\underline{t})$, and let (a, b, c) the associated order triple. Suppose that $\pm\underline{t}$ is partly projective and not exceptional, and let $G = \pm\langle g_1, g_2, g_3\rangle \subseteq \mathrm{PSL}_2(\mathbb{F}_q)$.*

Then the values $\#\Sigma(\underline{C})/\operatorname{Inn}(G)$ *and* $\#\Sigma(\underline{C})/\operatorname{Aut}(G)$ *are given in the following table:*

p	a	abc	G	$\#\Sigma(\underline{C})/\operatorname{Inn}(G)$	$\#\Sigma(\underline{C})/\operatorname{Aut}(G)$
$p=2$	$-$	$-$	$-$	1	1
$p>2$	$a=2$	$p \mid abc$	$-$	1	1
		$p \nmid abc$	PGL_2	1	1
		$p \nmid abc$	PSL_2	2	1
$p>2$	$a\neq 2$	$p \mid abc$	$-$	≤ 2	≤ 2
		$p \nmid abc$	PGL_2	≤ 2	≤ 2
		$p \nmid abc$	PSL_2	≤ 4	≤ 2

Proof. Suppose $p=2$. Then $\mathrm{PSL}_2(\mathbb{F}_q)=\mathrm{SL}_2(\mathbb{F}_q)$ and by Proposition 8.8(b) the triple $\underline{C}$ is rigid, i.e. we have $\#\Sigma(G)/\operatorname{Inn}(G)=\#\Sigma(G)/\operatorname{Aut}(G)=1$. This gives the first row of the table. So from now on we suppose $p>2$.

Let $\underline{t}=(t_1,t_2,t_3)\in\mathbb{F}_q^3$ be a lift of $\pm\underline{t}$. Let $\pm\underline{g},\pm\underline{g}'\in\Sigma(\underline{C})$; lift them to $\underline{g},\underline{g}'$ in $\mathrm{SL}_2(\mathbb{F}_q)^3$ such that $g_1g_2g_3=\pm 1$ and $g_1'g_2'g_3'=\pm 1$ and such that $\operatorname{tr}(g_i)=\operatorname{tr}(g_i')=t_i$.

Case 1: *Suppose* $a=2$. Then $t_1=\operatorname{tr}(g_1)=0=-\operatorname{tr}(g_1)$, so changing the signs of g_1 and g_1' if necessary, we may assume that $\underline{g},\underline{g}'$ are triples (that is, $g_1g_2g_3=g_1'g_2'g_3'=1$). Then by Proposition 8.8(c), there exists $m\in\mathrm{SL}_2(\overline{\mathbb{F}}_q)$ such that m conjugates $\underline{g}$ to $\underline{g}'$. Since the elements of $\pm\underline{g}$ generate G by hypothesis and the elements of $\pm\underline{g}'$ lie in G, it follows that conjugation by m induces an automorphism φ of G, so $\varphi(\underline{g})=\underline{g}'$, and $\underline{C}$ is weakly rigid. This gives the entries in the last column for $p>2$ and $a=2$.

Case 1(a): *Suppose* $a=2$ *and* $p\mid abc$. Then at least one conjugacy class is unipotent and so the two orbits of the set $T(\underline{t})$ under $\operatorname{Out}(\mathrm{PSL}_2(\mathbb{F}_q))$ correspond to two different conjugacy class triples and only one belongs to $\underline{C}$. Therefore the triple is in fact rigid.

Case 1(b): *Suppose* $a=2$ *and* $p\nmid abc$. First, suppose that G is of PGL_2-type. Then $G\simeq\mathrm{PGL}_2(\mathbb{F}_{\sqrt{q}})$ and $\operatorname{Out}(\mathrm{PGL}_2(\mathbb{F}_{\sqrt{q}}))=\langle\sigma\rangle$; and since $\mathbb{F}_q=\mathbb{F}_p(\underline{t})$, the stabilizer of $\langle\sigma\rangle$ acting on $\underline{t}$ is trivial as in the analysis following (7.3), and hence the orbits must be already identified by conjugation in $\mathrm{PGL}_2(\mathbb{F}_q)$, so the triple is in fact rigid.

Second, suppose that G is of PSL_2-type. Then since $\mathbb{F}_q=\mathbb{F}_p(\pm\underline{t})$ we have $G=\mathrm{PSL}_2(\mathbb{F}_q)$. Because $p\nmid abc$, all conjugacy classes $C_i\in\underline{C}$ are semisimple and so are preserved under automorphism. From Proposition 8.8(b), we see that there are two orbits of $\mathrm{PSL}_2(\mathbb{F}_q)$ acting by conjugation on $\Sigma(\underline{C})$ and the element $\tau\in\operatorname{Out}(\mathrm{PSL}_2(\mathbb{F}_q))$ induced by conjugation by an element of $\mathrm{PGL}_2(\mathbb{F}_q)\smallsetminus\mathrm{PSL}_2(\mathbb{F}_q)$ identifies these orbits: they are identifed by some element of $\operatorname{Out}(\mathrm{PSL}_2(\mathbb{F}_q))$, but since $\mathbb{F}_q=\mathbb{F}_p(\underline{t})$ the stabilizer of $\langle\sigma\rangle$ acting on $\underline{t}$ is again trivial.

This completes Case 1 and the table for $p>2$ and $a=2$. Note that in this case, the choice of the lift $\underline{t}$ does not figure in the analysis.

Case 2: *Suppose* $a>2$. Now either $\underline{g}'$ is already a triple, or changing the sign of g_1 we have $\underline{g}'$ is a triple with trace triple $\underline{t}'=(-t_1,t_2,t_3)$. By Lemma 8.7, this is without loss of generality.

Case 2(a): *Suppose* $\underline{t}'=\underline{t}$. Then the same analysis as in Case 1 shows that $\underline{g}'$ is obtained from $\underline{g}$ by an automorphism φ of G, and this automorphism can be taken to be inner except when $p\nmid abc$ and $G=\mathrm{PSL}_2(\mathbb{F}_q)$, in which case up to conjugation there are two triples.

Case 2(b): *Suppose* $\underline{t}'\neq\underline{t}$. Then clearly $\underline{g}'$ is not obtained from $\underline{g}$ by an inner automorphism. If $\underline{g}'=\varphi(\underline{g})$ with φ an outer automorphism, then after conjugation in $\mathrm{SL}_2(\overline{\mathbb{F}}_q)$, as in Case 2(a), we may assume that $\varphi=\sigma^j$ is a power of the p-power Frobenius automorphism

σ, with $\sigma^j(t_1) = -t_1$ and $\sigma^j(t_2) = t_2$ and $\sigma^j(t_3) = t_3$ (with slight abuse of notation). But again $\mathbb{F}_q$ is generated by the trace triple, so the fixed field k of σ^j contains t_2, t_3 and $\mathbb{F}_q$ is a quadratic extension of k, generated by t_1, and t_1 is a square root from k.

This concludes Case 2, with the stated inequalities: we have at most twice as many triples as in Cases 1(a) and 1(b).

We have equality in the first column if and only if $\underline{t}'$ is projective: otherwise, $\underline{t}'$ is commutative, as in the proof of Proposition 8.10, and all $\underline{g}' \in \underline{t}'$ generate affine or commutative subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ since they are singular [43, Theorem 2], and any such triple does not belong to $\Sigma(\underline{C})$—the trace triple up to signs is not exceptional so any group generated by a corresponding triple is not projective. In the second column, we have equality if and only if $\underline{t}'$ is projective and we are not in the special case described in 2(b). □

9. Proof of Theorems

In this section, we give proofs of the main theorems A, B, and C.

We begin with Theorem A, which follows from the following theorem.

Theorem 9.1. *Let (a, b, c) be a hyperbolic triple with $a, b, c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$. Let $\mathfrak{p}$ be a prime of $E(a, b, c)$ with residue field $\mathbb{F}_\mathfrak{p}$ lying above the rational prime p, and suppose $\mathfrak{p}$ does not divide any of $\{a, b, c\} \smallsetminus \{\infty\}$. If $\mathfrak{p} \mid 2$, suppose further that (a, b, c) is not of the form $(mz, m(z+1), mz(z+1))$ with $z, m \in \mathbb{Z}$. Let $a^\sharp = p$ if $a = \infty$ and $a^\sharp = a$ otherwise, and similarly with b, c, and suppose that $(a^\sharp, b^\sharp, c^\sharp)$ is not spherical or Euclidean.*

Then there exists a G-Galois Belyĭ map

$$X(a, b, c; \mathfrak{p}) \to \mathbb{P}^1$$

with ramification indices $(a^\sharp, b^\sharp, c^\sharp)$, where

$$G = \begin{cases} \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p}), & \text{if } \mathfrak{p} \text{ splits completely in } F(a, b, c); \\ \mathrm{PGL}_2(\mathbb{F}_\mathfrak{p}), & \text{otherwise.} \end{cases}$$

Proof. Let (a, b, c) be a hyperbolic triple with $a, b, c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$. Let $\mathfrak{p}$ be a prime of the field

$$E(a, b, c) = \mathbb{Q}(\lambda_a, \lambda_b, \lambda_c, \lambda_{2a}\lambda_{2b}\lambda_{2c})$$

above the rational prime $p \nmid abc$ and let $\mathfrak{P}$ be a prime of

$$F(a, b, c) = \mathbb{Q}(\lambda_{2a}, \lambda_{2b}, \lambda_{2c})$$

above $\mathfrak{p}$.

Then by Proposition 5.23, we have a homomorphism

$$\phi \colon \overline{\Delta}(a, b, c) \to \mathrm{PSL}_2(\mathbb{F}_\mathfrak{P})$$

with $\operatorname{tr} \phi(\bar{\delta}_s) \equiv \pm\lambda_{2s} \pmod{\mathfrak{P}}$ for $s = a, b, c$ whose image lies in $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{P}) \cap \mathrm{PGL}_2(\mathbb{F}_\mathfrak{p})$. We have $[\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}] \leq 2$ and

$$\mathrm{PSL}_2(\mathbb{F}_\mathfrak{P}) \cap \mathrm{PGL}_2(\mathbb{F}_\mathfrak{p}) = \begin{cases} \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p}), & \text{if } \mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{p}; \\ \mathrm{PGL}_2(\mathbb{F}_\mathfrak{p}), & \text{if } [\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}] = 2. \end{cases} \tag{9.2}$$

Let $\overline{\Delta}(a,b,c;\mathfrak{p})$ be the kernel of the homomorphism $\phi\colon \overline{\Delta}(a,b,c) \to \mathrm{PSL}_2(\mathbb{F}_\mathfrak{P})$. The generators $\bar{\delta}_s$ of $\overline{\Delta}$ (for $s = a,b,c$) give rise to a triple $\underline{g} = (g_1,g_2,g_3)$, namely $g_1 = \phi(\bar{\delta}_a)$, $g_2 = \phi(\bar{\delta}_b)$, $g_3 = \phi(\bar{\delta}_c)$, with trace triple up to signs

$$\pm\underline{t} = (\pm t_1, \pm t_2, \pm t_3) \equiv (\pm\lambda_{2a}, \pm\lambda_{2b}, \pm\lambda_{2c}) \pmod{\mathfrak{P}}.$$

The map of complex algebraic curves

$$f\colon X = X(a,b,c;\mathfrak{p}) = \overline{\Delta}(a,b,c;\mathfrak{p})\backslash\mathcal{H} \to \overline{\Delta}(a,b,c)\backslash\mathcal{H} \simeq \mathbb{P}^1$$

is a G-Galois Belyĭ map by construction, where $G = \overline{\Delta}(a,b,c)/\overline{\Delta}(a,b,c;\mathfrak{p})$. It is our task to specify G by our understanding of subgroups of $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{P})$.

First, we dispose of the exceptional triples. Since (a,b,c) is hyperbolic, this leaves the five triples

$$(a^\sharp, b^\sharp, c^\sharp) = (3,4,4), (2,5,5), (5,5,5), (3,3,5), (3,5,5).$$

Each of these triples is arithmetic, by work of Takeuchi [80], and the result follows from well-known properties of Shimura curves—something that could be made quite explicit in each case, if desired.

Second, we claim that the triple $\pm\underline{t}$ is not commutative. From (8.2), the triple $\underline{t}$ is commutative if and only if

$$\beta = \lambda_{2a}^2 + \lambda_{2b}^2 + \lambda_{2c}^2 - \lambda_{2a}\lambda_{2b}\lambda_{2c} - 4 = 0$$

in k. But $\beta\mathbb{Z}_F$ is the reduced discriminant of the order $\mathcal{O}$ arising in Section 5! And as in the proof of Lemma 5.5, from the factorization

$$\beta = \left(\frac{\zeta_{2b}\zeta_{2c}}{\zeta_{2a}} - 1\right)\left(\frac{\zeta_{2a}\zeta_{2c}}{\zeta_{2b}} - 1\right)\left(\frac{\zeta_{2a}\zeta_{2b}}{\zeta_{2c}} - 1\right)\left(\frac{1}{\zeta_{2a}\zeta_{2b}\zeta_{2c}} - 1\right)$$

we see that the argument in the case $\mathfrak{P}_K \mid 2$ applies to show that $\beta \not\equiv 0 \pmod{\mathfrak{P}}$.

Next, we show that orders of g_1, g_2, g_3 are $a^\sharp, b^\sharp, c^\sharp$. Let $s = a,b,c$ and write g for the corresponding element. We have $\operatorname{tr}\phi(\bar{\delta}_s) \equiv \pm\lambda_{2s} \pmod{\mathfrak{P}}$. If $g = 1$, then the image is commutative, and this possibility was just ruled out. If $s = \infty$, then since $g \neq 1$ and $\lambda_\infty = 2$ we must have g unipotent, so g has order $p = s^\sharp$. So we are left with only the possibility that g is a semisimple element of $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{P})$: but then the order is indeed determined by the trace (see Section 7), and an element with trace λ_{2s} necessarily has order s. The fact that the orders of the images are a,b,c then implies that the ramification indices are (a,b,c).

We continue now with the remainder of the proof of the theorem. By Theorem 8.5, we conclude that the triple $\underline{g}$ is projective. Then, by Proposition 8.8(a)–(b), we have either that the image of ϕ is either equal to $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{P})$, or that the trace triple is irregular and the image of ϕ is equal to $\mathrm{PGL}_2(k)$, where k is the unique subfield of $\mathbb{F}_\mathfrak{P}$ with $[\mathbb{F}_\mathfrak{P} : k] = 2$. In the first case, by (9.2) we must have $\mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{p}$ and so the result holds. In the second case, if $[\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}] = 2$ then again by (9.2) the image is already contained in $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{p})$ so we must have $k = \mathbb{F}_\mathfrak{p}$ and again the result holds.

So to conclude, we must rule out the possibility that the trace triple is irregular and that $\mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{p}$. Since $\mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{p}$, we have

$$\mathbb{F}_p(t_1,t_2,t_3) = \mathbb{F}_p(t_1^2, t_2^2, t_3^2, t_1t_2t_3).$$

Now let k be the subfield of $\mathbb{F}_\mathfrak{p}$ with $[\mathbb{F}_\mathfrak{p} : k] = 2$. Then we have

$$\mathbb{F}_p(\underline{t}^2) = \mathbb{F}_p(t_1^2, t_2^2, t_3^2) \subseteq k \subseteq \mathbb{F}_p(t_1,t_2,t_3) = \mathbb{F}_\mathfrak{p}.$$

But we have $[\mathbb{F}_{\mathfrak{p}} : \mathbb{F}_p(\underline{t}^2)] \leq 2$ so $k = \mathbb{F}_p(\underline{t}^2)$. If now the triple $\underline{t}$ is irregular, then without loss of generality (in this argument) we may suppose that $t_1 \in k$ and t_2, t_3 are either zero or square roots of nonsquares in k. But then $t_1 t_2 t_3 \in k$, so

$$k = \mathbb{F}_p(\underline{t}^2) = \mathbb{F}_p(\underline{t}^2, t_1 t_2 t_3) = \mathbb{F}_p(t_1, t_2, t_3),$$

a contradiction. □

Corollary 9.3. *We have*

$$[\overline{\Delta} : \overline{\Delta}(\mathfrak{p})] = [\mathcal{O}_1^\times/\{\pm 1\} : \mathcal{O}_1(\mathfrak{P})^\times/\{\pm 1\}] \cdot \begin{cases} 1, & \text{if } \mathbb{F}_{\mathfrak{P}} = \mathbb{F}_{\mathfrak{p}}; \\ 2, & \text{if } [\mathbb{F}_{\mathfrak{P}} : \mathbb{F}_{\mathfrak{p}}] = 2. \end{cases}$$

Next, we prove statements (a)–(c) of Theorem B, in two parts. (In the next section, we will show that the corresponding field extension is unramified away from p.) To this end, let X be a curve of genus $g \geq 2$ and let $f\colon X \to \mathbb{P}^1$ be a G-Galois Belyĭ map with $G \simeq \mathrm{PGL}_2(\mathbb{F}_q)$ or $G \simeq \mathrm{PSL}_2(\mathbb{F}_q)$. Let (a, b, c) be the ramification indices of f.

Theorem 9.4. *Let r be the order of* Frob_p *in* $\mathrm{Gal}(F_{p'}(a, b, c)/\mathbb{Q})$. *Then*

$$q = \begin{cases} \sqrt{p^r}, & \text{if } G \simeq \mathrm{PGL}_2(\mathbb{F}_q); \\ p^r, & \text{if } G \simeq \mathrm{PSL}_2(\mathbb{F}_q). \end{cases}$$

Proof. By work in Section 2, there exists a finite index, normal subgroup $\overline{\Gamma} \subseteq \overline{\Delta}(a, b, c)$ such that $\overline{\Delta}(a, b, c)/\overline{\Gamma} \simeq G$ and the map $X \to \mathbb{P}^1$ is the map $\overline{\Gamma}\backslash\mathcal{H} \to \overline{\Delta}(a, b, c)\backslash\mathcal{H}$. In this way, we have identified the images in G of the monodromy at the three ramification points with the elements $\bar{\delta}_a, \bar{\delta}_b, \bar{\delta}_c$. Thus, by hypothesis, the images of the triple $(\bar{\delta}_a\overline{\Gamma}, \bar{\delta}_b\overline{\Gamma}, \bar{\delta}_c\overline{\Gamma})$ in G generate G. This triple lifts to the triple $(-\delta_a\overline{\Gamma}, \delta_b\overline{\Gamma}, \delta_c\overline{\Gamma})$ in $\mathrm{SL}_2(\mathbb{F}_q)$ with corresponding trace triple

$$\underline{t} \equiv (-\lambda_{2a}, \lambda_{2b}, \lambda_{2c}) \pmod{\mathfrak{p}}$$

for $\mathfrak{p}$ a prime above p in the field $F_{p'}(a, b, c)$.

If $G \simeq \mathrm{PSL}_2(\mathbb{F}_q)$, then Proposition 8.8(a) implies that $q = \#\mathbb{F}_p(\underline{t}) = p^r$; this is the residue class field of the prime $\mathfrak{p}$ above and so r is equal to its residue degree, equal to the order of the Frobenius Frob_p in the field. Put another way, $r = \log_p q$ is the least common multiple of the orders of p in $(\mathbb{Z}/2s\mathbb{Z})^\times/\{\pm 1\}$ for $s = a, b, c$, which is the order of Frob_p in $\mathrm{Gal}(F_{p'}(a, b, c)/\mathbb{Q})$, as claimed. If instead $G \simeq \mathrm{PGL}_2(\mathbb{F}_{\sqrt{q}})$, then r is twice this degree. □

Now we prove statements (b)–(c) of Theorem B concerning fields of moduli.

Theorem 9.5. *The map f is defined over its field of moduli $M(X, f)$ and $M(X, f)$ is an extension of $D_{p'}(a, b, c)^{\langle \mathrm{Frob}_p \rangle}$ of degree $d_{(X,f)} \leq 2$. If $a = 2$ or q is even, then $d_{(X,f)} = 1$.*

The map f together with its Galois group $\mathrm{Gal}(f) \simeq G$ *is defined over its field of moduli $M(X, f, G)$. Let r be the order of* Frob_p *in* $\mathrm{Gal}(F_{p'}(a, b, c)/\mathbb{Q})$, *and let*

$$D_{p'}(a, b, c)\{\sqrt{p^*}\} = \begin{cases} D_{p'}(a, b, c)(\sqrt{p^*}), & \text{if } p \mid abc, \text{ } pr \text{ is odd, and } G \simeq \mathrm{PSL}_2(\mathbb{F}_q); \\ D_{p'}(a, b, c) & \text{otherwise.} \end{cases}$$

Then $M(X, f, G)$ is an extension of $D_{p'}(a, b, c)\{\sqrt{p^*}\}$ of degree $d_{(X,f,G)} \leq 2$. If q is even or $p \mid abc$ or $G \simeq \mathrm{PGL}_2(\mathbb{F}_q)$, then $d_{(X,f,G)} = 1$.

Proof. As in the proof of Theorem 9.1, we may identify the images in G of the monodromy at the three ramification points with the elements $\bar{\delta}_a, \bar{\delta}_b, \bar{\delta}_c \in \overline{\Delta}(a,b,c)$. Let $\underline{g} = (\bar{\delta}_a\overline{\Gamma}, \bar{\delta}_b\overline{\Gamma}, \bar{\delta}_c\overline{\Gamma})$ and let $\underline{C}$ be the corresponding conjugacy class triple in G.

We refer to the discussion in Section 5, specifically Proposition 6.1, and recall the calculation of the field of weak rationality in Section 6 (Lemmas 7.4 and 7.5). Then by Proposition 8.10, we have $d_{(X,f)} = \#\Sigma(\underline{C})/\mathrm{Aut}(G) \leq 2$ and $d_{(X,f,G)} = \#\Sigma(\underline{C})/\operatorname{Inn}(G) \leq 4$, with the various cases as listed.

Finally, the map f is defined over its field of moduli by Lemma 4.1. And we would know that f together with $\mathrm{Gal}(f) \simeq G$ is defined over its field of moduli when the centralizer of G in $\operatorname{Aut} X$ is trivial by Lemma 4.3. This holds for any maximal triple (see the discussion surrounding (2.8)–(2.9)). We conclude in fact that it is therefore true for a nonmaximal triple, by the following reasoning. We need only concern ourselves with the presence of extra automorphisms of the G-Galois Belyĭ map; such an automorphism is given by an element of the maximal group centralizing G, and in particular it must normalize the nonmaximal triangle group. So we reduce to the case where we have a normal inclusion of triangle groups, and this leaves only the three cases in (2.9) (the third obtained by a concatenation). But the desired Belyĭ map is defined over the field obtained from the maximal triple simply by taking the quotient by the smaller group, and the relevant fields $D_{p'}(a,b,c)^{\langle \mathrm{Frob}_{p'}\rangle})$ and $D_{p'}(a,b,c)\{\sqrt{p^*}\}$ are the *same* in each of these three cases! □

We now prepare for the proof of Theorem C with a discussion of the extension to composite $\mathfrak{N}$. Let $\mathfrak{N}$ be an ideal of $\mathbb{Z}_F$ coprime to $6abc$. Let $\mathfrak{n} = \mathfrak{N} \cap \mathbb{Z}_E$. Then by Proposition 5.23, we have a homomorphism

$$\phi_{\mathfrak{N}} \colon \overline{\Delta} \to \mathrm{PSL}_2(\mathbb{Z}_F/\mathfrak{N}). \tag{9.6}$$

If $\mathfrak{M} \mid \mathfrak{N}$ then $\phi_{\mathfrak{M}}$ is obtained by the composition of $\phi_{\mathfrak{N}}$ with the natural reduction map modulo $\mathfrak{M}$. Therefore these maps form a projective system and so we obtain in the limit a map

$$\widehat{\phi} \colon \overline{\Delta} \to \prod_{\mathfrak{P} \nmid 6abc} \mathrm{PSL}_2(\mathbb{Z}_{F,\mathfrak{P}})$$

after composing with the Chinese remainder theorem. The map $\widehat{\phi}$ is injective because $\overline{\Delta} \hookrightarrow \mathcal{O}_1^\times/\{\pm 1\} \hookrightarrow \mathrm{PSL}_2(\mathbb{Z}_{F,\mathfrak{P}})$ for any prime $\mathfrak{P}$.

For a prime $\mathfrak{P}$ of $\mathbb{Z}_F$ with $\mathfrak{p} = \mathfrak{P} \cap \mathbb{Z}_E$ and an integer $e \geq 1$, let $P(\mathfrak{P}^e) \subseteq \mathrm{PSL}_2(\mathbb{Z}_F/\mathfrak{P}^e)$ be the group

$$P(\mathfrak{P}^e) = \begin{cases} \mathrm{PSL}_2(\mathbb{Z}_E/\mathfrak{p}^e), & \text{if } \mathbb{F}_{\mathfrak{P}} = \mathbb{F}_{\mathfrak{p}}; \\ \mathrm{PGL}_2(\mathbb{Z}_E/\mathfrak{p}^e), & \text{if } [\mathbb{F}_{\mathfrak{P}} : \mathbb{F}_{\mathfrak{p}}] = 2. \end{cases}$$

For an ideal $\mathfrak{N}$ of $\mathbb{Z}_F$ let $P(\mathfrak{N}) = \prod_{\mathfrak{P}^e \| \mathfrak{N}} P(\mathfrak{P}^e)$, and let $\widehat{P} = \varprojlim_{\mathfrak{N}} P(\mathfrak{N})$ be the projective limit of $P(\mathfrak{N})$ with respect to the $\mathfrak{N}$ for $N \nmid 6abc$. Then $\widehat{P}$ is a subgroup of $\prod_{\mathfrak{P} \nmid 6abc} \mathrm{PSL}_2(\mathbb{Z}_{F,\mathfrak{P}})$.

Proposition 9.7. *The image of $\widehat{\phi}$ contains a dense subgroup of $\mathrm{PSL}_2(\mathbb{Z}_{E,\mathfrak{p}})$.*

We will use the following lemma in the proof.

Lemma 9.8. *Let P denote either PSL_2 or PGL_2. Let H be a closed subgroup of $P(\mathbb{Z}_{F,\mathfrak{p}})$, and suppose that H projects surjectively onto $P(\mathbb{Z}_F/\mathfrak{p})$. If $\#\mathbb{Z}_F/\mathfrak{p} \geq 4$, then $H = P(\mathbb{Z}_{F,\mathfrak{p}})$.*

Proof. Serre [60, Lemmas 3.4.2–3.4.3] proves this when $\mathbb{Z}_F = \mathbb{Z}$ and $P = \mathrm{PSL}_2$, but his Lie-theoretic proof generalizes to an arbitrary number ring $\mathbb{Z}_F$. One can deduce the statement for $P = \mathrm{PGL}_2$ from this statement as follows. The preimage of H under the map $\mathrm{GL}_2(\mathbb{Z}_{F,\mathfrak{p}}) \to \mathrm{PGL}_2(\mathbb{Z}_{F,\mathfrak{p}})$ intersected with $\mathrm{SL}_2(\mathbb{Z}_{F,\mathfrak{p}})$ maps surjectively to $\mathrm{SL}_2(\mathbb{Z}_F/\mathfrak{p})$ so $H \supseteq \mathrm{PSL}_2(\mathbb{Z}_{F,\mathfrak{p}})$. But

$$\mathrm{PGL}_2(\mathbb{Z}_{F,\mathfrak{p}})/\mathrm{PSL}_2(\mathbb{Z}_{F,\mathfrak{p}}) \simeq \mathbb{Z}_{F,\mathfrak{p}}^\times/\mathbb{Z}_{F,\mathfrak{p}}^{\times 2} \simeq (\mathbb{Z}_F/\mathfrak{p})^\times/(\mathbb{Z}_F/\mathfrak{p})^{\times 2}$$

and so since H maps surjectively to $\mathrm{PGL}_2(\mathbb{Z}_F/\mathfrak{p})$ we must have $H = \mathrm{PGL}_2(\mathbb{Z}_{F,\mathfrak{p}})$.

An alternate proof for both cases runs as follows. Let $k = \mathbb{Z}_F/\mathfrak{p}$. One proves the statement by induction; we have an exact sequence

$$0 \to M_2(k) \to \mathrm{GL}_2(\mathbb{Z}_F/\mathfrak{p}^e) \to \mathrm{GL}_2(\mathbb{Z}_F/\mathfrak{p}^{e-1}) \to 1 \tag{9.9}$$

via the isomorphism

$$1 + M_2(\mathfrak{p}^{e-1}/\mathfrak{p}^e) \simeq M_2(\mathfrak{p}^{e-1}/\mathfrak{p}^e) \simeq M_2(k).$$

The group $\mathrm{GL}_2(\mathbb{Z}_F/\mathfrak{p}^{e-1})$ acts by conjugation on $M_2(k)$ and factors through $\mathrm{GL}_2(k)$. Since $\operatorname{char} k$ is odd, $M_2(k)$ decomposes into irreducible subspaces under this action as $M_2(k) = k \oplus M_2(k)_0$ where $M_2(k)_0$ denotes the subspace of matrices of trace zero. Restricting to SL_2 or PGL_2, one then reduces to an exercise showing that the above sequence does not split (and indeed, it splits for $k = \mathbb{F}_2$ for $e \leq 3$ and for $k = \mathbb{F}_3$ for $e = 2$ [60, Exercise 1, p. IV-27]). □

Proof of Proposition 9.7. We show that $\phi_{\mathfrak{N}}$ has image $P(\mathfrak{N})$. We have shown that this statement is true if $\mathfrak{N}$ is prime. Using Lemma 9.8 and basic topological considerations, we find that the image of $\phi_{\mathfrak{N}}$ is equal to $P(\mathfrak{N})$ when $\mathfrak{N} = \mathfrak{P}^e$ is a prime power.

Suppose that $\mathfrak{M}$ and $\mathfrak{N}$ are coprime ideals of $\mathbb{Z}_F$. The kernel of the map

$$\overline{\Delta} \to \frac{\overline{\Delta}}{\overline{\Delta}(\mathfrak{M})} \times \frac{\overline{\Delta}}{\overline{\Delta}(\mathfrak{N})}$$

is equal to

$$\overline{\Delta}(\mathfrak{M}) \cap \overline{\Delta}(\mathfrak{N}) = \overline{\Delta} \cap (\mathcal{O}(\mathfrak{M})_1^\times \cap \mathcal{O}(\mathfrak{N})_1^\times) = \overline{\Delta} \cap \mathcal{O}(\mathfrak{M}\mathfrak{N})_1^\times = \overline{\Delta}(\mathfrak{M}\mathfrak{N}).$$

The cokernel of this map is $\dfrac{\overline{\Delta}}{\overline{\Delta}(\mathfrak{M})\overline{\Delta}(\mathfrak{N})}$. We claim that this cokernel is trivial. Since $\mathcal{O}$ is dense in $\mathcal{O}_{\mathfrak{N}} = \mathcal{O} \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{N}}$ it follows that $\mathcal{O}(\mathfrak{M})$ is dense in $\mathcal{O}_{\mathfrak{N}}$, so $\mathcal{O}(\mathfrak{M})_1^\times$ maps surjectively modulo $\mathfrak{N}$ onto $\mathcal{O}_1^\times/\mathcal{O}(\mathfrak{N})_1^\times \simeq \mathrm{SL}_2(\mathbb{Z}_F/\mathfrak{N})$. Thus $\mathcal{O}(\mathfrak{M})_1^\times \mathcal{O}(\mathfrak{N})_1^\times = \mathcal{O}_1^\times$, and so $\overline{\Delta}(\mathfrak{M})\overline{\Delta}(\mathfrak{N}) = \overline{\Delta}$. Composing with the map $(\phi_{\mathfrak{M}}, \phi_{\mathfrak{N}})$, we obtain a map

$$\overline{\Delta} \to \mathrm{PSL}_2(\mathbb{Z}_F/\mathfrak{M}) \times \mathrm{PSL}_2(\mathbb{Z}_F/\mathfrak{N});$$

by induction on the number of prime factors, we may suppose that the image of the this map contains a dense subgroup of $P(\mathfrak{M}) \times P(\mathfrak{N}) \simeq P(\mathfrak{M}\mathfrak{N})$, and the result follows. □

Having now defined the curve $X(a, b, c; \mathfrak{N}) = X(\mathfrak{N}) = \overline{\Delta}(\mathfrak{N})\backslash\mathcal{H}$ and identified its Galois group as a cover of $X(1) = \overline{\Delta}\backslash\mathcal{H}$, to conclude this section we also define certain intermediate quotients in analogy with the classical modular curves. Recall by (9.6) we have a homomorphism $\phi_{\mathfrak{N}} \colon \overline{\Delta} \to \mathrm{PSL}_2(\mathbb{Z}_F/\mathfrak{N}) = P$; we let $H_0 \leq P$ be the image in P of subgroup

of upper-triangular matrices in $\mathrm{SL}_2(\mathbb{Z}_F/\mathfrak{N})$ and similarly $H_1 \leq P$ the image of the subgroup of upper-trianglar matrices with both diagonal entries equal to 1. Let

$$\Delta(\mathfrak{N}) \leq \Delta_1(\mathfrak{N}) = \phi_{\mathfrak{N}}^{-1}(H_1) \leq \Delta_0(\mathfrak{N}) = \phi_{\mathfrak{N}}^{-1}(H_0) \leq \overline{\Delta},$$

be the preimages of H_0 and H_1 under $\phi_{\mathfrak{N}}$; then we define

$$X_0(\mathfrak{N}) = \Delta_0(\mathfrak{N})\backslash\mathcal{H}, \qquad X_1(\mathfrak{N}) = \Delta_1(\mathfrak{N})\backslash\mathcal{H}$$

and we obtain maps

$$X(\mathfrak{N}) \to X_1(\mathfrak{N}) \to X_0(\mathfrak{N}) \to X(1). \tag{9.10}$$

Although the definition of these curves depends on a choice of isomorphism $\phi_{\mathfrak{N}}$, any two such choices are conjugate in $G = \mathrm{Aut}(X_0(\mathfrak{N})/X(1))$, so the resulting tower (9.10) does not depend on any choices up to isomorphism. The curves $X_0(\mathfrak{N}), X_1(\mathfrak{N})$ are defined over any field of definition of $(X(\mathfrak{N}), G)$.

10. Examples

In this section, we give many examples of Theorems A and B and show how these theorems recover some familiar families of curves.

Our notation $X(a, b, c; \mathfrak{p})$ becomes awkward in the consideration of specific cases: given $a, b, c \in \mathbb{Z}_{\geq 2}$ and a prime number $p \nmid 2abc$, we need to choose a prime ideal $\mathfrak{p}$ of $E(a, b, c)$ lying over p. By Theorem B, the curve $X(a, b, c; \mathfrak{p})$ only depends upon the choice of $\mathfrak{p}$ lying over p up to Galois conjugacy, and there is in general no canonical choice of $\mathfrak{p}$. Therefore in what follows we will write $X(a, b, c; p)$ for $X(a, b, c; \mathfrak{p})$ for some unspecified $\mathfrak{p} \mid p$.

Example 10.1. We take $(a, b, c) = (2, 3, \infty)$ as $\mathrm{SL}_2(\mathbb{Z}) \simeq \Delta(2, 3, \infty)$. For $N \in \mathbb{Z}_{\geq 1}$, our construction from triangle groups gives exactly the congruence subgroup $\Delta(2, 3, \infty; N) = \Gamma(N)$ of matrices congruent to the identity modulo N, and we find the modular curve $X(2, 3, \infty; N) = X(N) = \Gamma(N)\backslash\mathcal{H}^*$ of level N, where $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ is the completed upper half-plane. Suppose $N = p$ is prime. The cover $X(p) \to X(1)$ is a $G = \mathrm{PSL}_2(\mathbb{F}_p)$-cover with ramification indices $(2, 3, p)$; this verifies the statement of Theorem B, since $F = F(a, b, c) = \mathbb{Q}(\lambda_4, \lambda_6, \lambda_\infty) = \mathbb{Q} = E$. The statement of Theorem A says that $M(X(p)) = \mathbb{Q}$ since $a = 2$. As discussed in Example 4.6, in fact we have $M(X(p), G) = \mathbb{Q}(\sqrt{p^*})$.

Example 10.2. We take $(a, b, c) = (2, 3, p)$ with $p \geq 7$ prime. We want to consider the case where q is a power of p; for this, we will need the slight extension of Theorem B given in Remark 5.24. We have $F = F(\lambda_4, \lambda_6, \lambda_{2p}) = F(\lambda_{2p}) = E$; the discriminant

$$\beta = \lambda_4^2 + \lambda_6^2 + \lambda_{2p}^2 + \lambda_4\lambda_6\lambda_{2p} - 4 = \lambda_{2p}^2 - 3 = \lambda_p - 1$$

is a unit in $\mathbb{Z}_E$. Therefore we can consider $X(2, 3, p; \mathfrak{p})$ where $\mathfrak{p}^{(p-1)/2} = (p)$, which gives a $\mathrm{PSL}_2(\mathbb{F}_p)$-cover $X(2, 3, p; \mathfrak{p}) \to X(2, 3, p) \simeq \mathbb{P}^1$.

We verify Theorem A: we have $\mathbb{Q}(\lambda_4, \lambda_6, \lambda_{2p})_{p'} = \mathbb{Q}$ so $r = 1$. Since $a = 2$ and $p \mid abc$, we have $d_X = d_{(X,G)} = 1$; consequently, $M(X) = \mathbb{Q}$ and $M(X, G) = \mathbb{Q}(\sqrt{p^*})$.

The proof in this situation comes down to the following. There are two unipotent conjugacy classes which are in the same Galois orbit (taking an odd power moves from quadratic residues to nonresidues) and so the field of rationality of such a conjugacy class is the quadratic subfield $\mathbb{Q}(\sqrt{p^*}) \subseteq \mathbb{Q}(\zeta_p)$, where $p^* = (-1)^{(p-1)/2}p$. Since the other two conjugacy

classes representing elements of orders 2 and 3 are $\mathbb{Q}$-rational, the field of rationality of $\underline{C}$ is $F(\underline{C}) = \mathbb{Q}(\sqrt{p^*})$. As above, the outer automorphism τ interchanges the two unipotent conjugacy classes, so $F_{\mathrm{wr}}(\underline{C}) = \mathbb{Q}$.

In fact, the classical modular cover $j\colon X(p) \to X(1)$ is also a $\mathrm{PSL}_2(\mathbb{F}_p)$-Galois Belyĭ map, with ramification points $0, 1728, \infty$. It follows that $X(2,3,p;p) \simeq X(p)$ over $\overline{\mathbb{Q}}$.

We could equally well consider the covers $X = X(2,3,p;2) \to X(2,3,p)$, which for the same reasons can be defined over $\mathbb{Q}$ and gives rise to $\mathrm{SL}_2(\mathbb{F}_{2^r}) = \mathrm{PSL}_2(\mathbb{F}_{2^r}) = \mathrm{PSL}_2(\mathbb{F}_{2^r})$ covers where r is the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$; from Theorem A, we have $M(X,G) = \mathbb{Q}(\lambda_p)$.

Example 10.3. Finitely many families of curves $X(a,b,c;p)$ correspond to Shimura curves, where the group $\Delta(a,b,c)$ is arithmetic. The arithmetic triples were classified by Takeuchi in a sequence of papers [78, 79, 80, 81]: there are 85 triples (a,b,c) and 26 maximal triples which fall into 19 commensurability classes. As Takeuchi explains (in the notation of Section 5), the triple (a,b,c) gives rise to arithmetic groups if and only if the quaternion algebra A over E is split at exactly one real place of E, and the triangle group $\Delta(a,b,c)$ is commensurable with the unit group of a maximal order in A.

This covers as a special case the previous example of the modular curves, which include the maximal triples $(2,3,\infty), (2,4,\infty), (2,6,\infty)$ and the nonmaximal triples

$$(3,3,\infty), (3,\infty,\infty), (4,4,\infty), (6,6,\infty), (\infty,\infty,\infty).$$

So in this example, we restrict to the case $a,b,c \in \mathbb{Z}$.

The minimal field of definition of these curves was studied by Elkies [24, §5.3] and later by the second author [85, Proposition 5.1.2]. Each base field E is Galois over $\mathbb{Q}$, and it turns out that at least one of the triangle groups in each commensurability class has distinct indices a,b,c: therefore, by identifying the corresponding elliptic points with $0,1,\infty$, any Galois-invariant construction (such as taking Galois invariant level) yields a curve which is fixed by $\mathrm{Gal}(E/\mathbb{Q})$, providing extra descent in some cases.

This argument can be made directly using the language of canonical models of Shimura curves, which has the advantage that it applies in other circumstances as well (see e.g. Hallouin [31, Proposition 1]). Let B be a quaternion algebra over a totally real field F which is split at a unique real place and let $\mathcal{O}$ be a maximal order in B. Associated to this datum is a Shimura curve $X(\mathbb{C}) = B_+^\times\backslash\mathcal{H} \times \widehat{B}^\times/\widehat{\mathcal{O}}^\times$ which has a model X over the reflex field $F^\flat = F$. Suppose F has strict class number 1, so $X(\mathbb{C})$ is irreducible (otherwise consider a component over the strict class field of F). Suppose further that F is Galois over $\mathbb{Q}$. Then for any $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$, the conjugate curve X^σ is given by

$$X^\sigma(\mathbb{C}) = (B^\sigma)_+^\times\backslash\mathcal{H} \times (\widehat{B}^\sigma)^\times/\widehat{\mathcal{O}}^\sigma)^\times.$$

Now if $B^\sigma \simeq_{\mathbb{Q}} B$, which means precisely that the discriminant of B is invariant under σ, and there exists an analytic isomorphism $X(\mathbb{C}) = \Gamma(1)\backslash\mathcal{H} \xrightarrow{\sim} \Gamma(1)^\sigma\backslash\mathcal{H} = X^\sigma(\mathbb{C})$, then this yields exactly the descent datum needed to descend X to $\mathbb{Q}$. In the case of triangle groups, the quotients $X^\sigma(\mathbb{C})$ have fundamental domain given by the union of two hyperbolic triangles with angles $\pi/a, \pi/b, \pi/c$, and any two hyperbolic triangles with the same angles are congruent; hence the curves descend. This argument works with the maximal order replaced by any order $\mathcal{O}$ which is defined by Galois invariant means, e.g. the order $\mathcal{O}(N)$ for $N \geq 1$.

Many of these triples will occur in specific examples below.

Example 10.4. Consider the case of Hecke triangle groups treated by Lang, Lim, and Tan [40], the groups with $\overline{\Delta}(a,b,c) = \overline{\Delta}(2,b,\infty)$. We make the additional assumption that b is odd. Then we have

$$F(4,2b,\infty) = \mathbb{Q}(\lambda_4, \lambda_{2b}, \lambda_\infty) = \mathbb{Q}(\lambda_{2b}) = E(2,b,\infty)$$

since b is odd. Then for all primes $\mathfrak{p}$ of $\mathbb{Q}(\lambda_q)$ we have $\mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{p}$ in the notation of Section 5, so $\overline{\Delta}/\overline{\Delta}(\mathfrak{p}) \simeq \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$. Note that when $q \neq p$ we have that $[\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]$ is indeed equal to the smallest positive integer r such that $p^r \equiv \pm 1 \pmod{q}$, or equivalently the order of Frob_p in $\mathrm{Gal}(\mathbb{Q}(\lambda_q)/\mathbb{Q})$.

Lang, Lim, and Tan [40, Main Theorem, part (iii)] obtain a group of PGL_2-type in the case that r is even and $[\mathbb{F}_p(t) : \mathbb{F}_p(t^2)] = 2$, where $t \equiv \lambda_q \pmod{\mathfrak{p}}$. But this latter equality cannot hold: the map $\zeta_q \mapsto \zeta_q^2$ is a Galois automorphism of $\mathbb{Q}(\zeta_q)$ and restricts to the automorphism $\lambda_q \mapsto \lambda_q^2 - 2$. It follows in fact that $\mathbb{F}_p(t) = \mathbb{F}_p(t^2)$.

To give further examples, we list all G-Galois Belyĭ curves with $a, b, c \neq \infty$ with genus $g \leq 24$ with $G = \mathrm{PSL}_2(\mathbb{F}_q)$ or $G = \mathrm{PGL}_2(\mathbb{F}_q)$. The formula for the genus (Remark 3.10) gives a bound for a, b, c and $\#G$ in terms of g (in fact, for arbitrary groups G). From the bound $\#\mathrm{PSL}_2(\mathbb{F}_q) \leq 84(g-1) \leq 1932$ we obtain $q \leq 16$; and for each group G we find only finitely many triples of possible orders (a,b,c). We then enumerate the triples in Magma [8]; the curves of genus $g \leq 24$ are listed in Table 10.5. We list also if the triple (a,b,c) is arithmetic (after Takeuchi) and the genus g_0 of the subcover $X_0(a,b,c;\mathfrak{p})$ whose Galois closure is $X(a,b,c;\mathfrak{p})$, as defined at the end of Section 9; we also give the corresponding fields $F(a,b,c) \supseteq E(a,b,c)$, defined in (*).

We now discuss many of these curves in turn, highlighting those curves with interesting features. We note first that all curves but the last two (of genus 24) are arithmetic. Our computations are performed in Magma [8]. We are grateful to Elkies for allowing us to record several computations and other remarks in these examples.

Genus 3, $(2,3,7)$, $\mathrm{PSL}_2(\mathbb{F}_7)$. This curve is the beloved Klein quartic, the projective plane curve given by the equation $x^3y + y^3z + z^3x = 0$. For a detailed discussion of this curve and its arithmetic, see Elkies [23]. The map $f\colon X_0(2,3,7;7) \simeq \mathbb{P}^1 \to X(2,3,7) = \mathbb{P}^1$ is given by the rational function

$$\frac{(t^4 + 14t^3 + 63t^2 + 70t - 7)^2}{1728t} = \frac{(t^2 + 5t + 1)^3(t^2 + 13t + 49)}{1728t} + 1.$$

As predicted by part (b) of Theorem B, the curve is defined over $\mathbb{Q}$ (since $a = 2$); its automorphism group is defined over $\mathbb{Q}(\sqrt{-7})$, the quadratic extension allowed by part (c) of Theorem B.

Genus 3, $(3,4,4)$, $\mathrm{PGL}_2(\mathbb{F}_3)$. The triple $(3,4,4)$ is exceptional, and so has been excluded from our analysis. But since $\mathrm{PGL}_2(\mathbb{F}_3) \simeq S_4$ is the full group, it is worth identifying this cover. The quaternion algebra A associated to the triple $(3,4,4)$ is defined over $E = \mathbb{Q}(\lambda_3, \lambda_4, \lambda_6\lambda_8^2) = \mathbb{Q}$ and has discriminant 6. The group $\Delta(3,4,4)$ is not maximal: it is contained in $\Delta(2,4,6)$ with index 2. The curve $X(2,4,6)$ is associated to the arithmetic group $N(\Lambda)/\mathbb{Q}^\times$ for $\Lambda \subseteq A$ a maximal order, and the quotient $X(3,4,4) \to X(2,4,6)$ is obtained as the quotient by an Atkin-Lehner involution; the Shimura curve associated to

g	(a,b,c)	G	arithmetic?	g_0	$F(a,b,c)$	$E(a,b,c)$	$D_{p'}(a,b,c)^{\langle \mathrm{Frob}_p \rangle}$
3	$(2,3,7)$	$\mathrm{PSL}_2(\mathbb{F}_7)$	T	0	$\mathbb{Q}(\lambda_7)$	$\mathbb{Q}(\lambda_7)$	$\mathbb{Q}$
3	$(3,4,4)$	$\mathrm{PGL}_2(\mathbb{F}_3)$	T	1	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}$	$\mathbb{Q}$
4	$(2,4,5)$	$\mathrm{PGL}_2(\mathbb{F}_5)$	T	0	$\mathbb{Q}(\sqrt{2},\sqrt{5})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}$
4	$(2,5,5)$	$\mathrm{PGL}_2(\mathbb{F}_4)$	T	1	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}$
4	$(2,5,5)$	$\mathrm{PSL}_2(\mathbb{F}_5)$	T	0	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}$
5	$(3,3,5)$	$\mathrm{PGL}_2(\mathbb{F}_4)$	T	0	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}$
5	$(3,3,5)$	$\mathrm{PSL}_2(\mathbb{F}_5)$	T	1	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}$
6	$(2,4,6)$	$\mathrm{PGL}_2(\mathbb{F}_5)$	T	0	$\mathbb{Q}(\sqrt{2},\sqrt{3})$	$\mathbb{Q}$	$\mathbb{Q}$
7	$(2,3,7)$	$\mathrm{PGL}_2(\mathbb{F}_8)$	T	0	$\mathbb{Q}(\lambda_7)$	$\mathbb{Q}(\lambda_7)$	$\mathbb{Q}$
8	$(2,3,8)$	$\mathrm{PGL}_2(\mathbb{F}_7)$	T	0	$\mathbb{Q}(\lambda_{16})$	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}$
8	$(3,3,4)$	$\mathrm{PSL}_2(\mathbb{F}_7)$	T	0	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\sqrt{2})$
9	$(2,5,6)$	$\mathrm{PGL}_2(\mathbb{F}_5)$	T	1	$\mathbb{Q}(\sqrt{3},\sqrt{5})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}$
9	$(3,5,5)$	$\mathrm{PGL}_2(\mathbb{F}_4)$	T	1	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}$
9	$(3,5,5)$	$\mathrm{PSL}_2(\mathbb{F}_5)$	T	1	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}$
10	$(2,4,5)$	$\mathrm{PSL}_2(\mathbb{F}_9)$	T	0	$\mathbb{Q}(\sqrt{2},\sqrt{5})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}$
10	$(2,4,7)$	$\mathrm{PSL}_2(\mathbb{F}_7)$	T	1	$\mathbb{Q}(\lambda_7,\sqrt{2})$	$\mathbb{Q}(\lambda_7)$	$\mathbb{Q}$
11	$(2,6,6)$	$\mathrm{PGL}_2(\mathbb{F}_5)$	T	1	$\mathbb{Q}(\sqrt{3})$	$\mathbb{Q}$	$\mathbb{Q}$
11	$(3,4,4)$	$\mathrm{PGL}_2(\mathbb{F}_5)$	T	0	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}$	$\mathbb{Q}$
13	$(5,5,5)$	$\mathrm{PGL}_2(\mathbb{F}_4)$	T	2	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}$
13	$(5,5,5)$	$\mathrm{PSL}_2(\mathbb{F}_5)$	T	1	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}$
14	$(2,3,7)$	$\mathrm{PSL}_2(\mathbb{F}_{13})$	T	0	$\mathbb{Q}(\lambda_7)$	$\mathbb{Q}(\lambda_7)$	$\mathbb{Q}(\lambda_7)$
15	$(2,3,9)$	$\mathrm{PGL}_2(\mathbb{F}_8)$	T	1	$\mathbb{Q}(\lambda_9)$	$\mathbb{Q}(\lambda_9)$	$\mathbb{Q}$
15	$(2,4,6)$	$\mathrm{PGL}_2(\mathbb{F}_7)$	T	0	$\mathbb{Q}(\sqrt{2},\sqrt{3})$	$\mathbb{Q}$	$\mathbb{Q}$
15	$(3,4,4)$	$\mathrm{PSL}_2(\mathbb{F}_7)$	T	1	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}$	$\mathbb{Q}$
16	$(2,3,8)$	$\mathrm{PGL}_2(\mathbb{F}_9)$	T	0	$\mathbb{Q}(\lambda_{16})$	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}$
16	$(3,3,4)$	$\mathrm{PSL}_2(\mathbb{F}_9)$	T	0	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}$
16	$(3,4,6)$	$\mathrm{PGL}_2(\mathbb{F}_5)$	T	1	$\mathbb{Q}(\sqrt{2},\sqrt{3})$	$\mathbb{Q}(\sqrt{6})$	$\mathbb{Q}$
17	$(3,3,7)$	$\mathrm{PSL}_2(\mathbb{F}_7)$	T	0	$\mathbb{Q}(\lambda_7)$	$\mathbb{Q}(\lambda_7)$	$\mathbb{Q}$
19	$(2,7,7)$	$\mathrm{PSL}_2(\mathbb{F}_7)$	T	0	$\mathbb{Q}(\lambda_7)$	$\mathbb{Q}(\lambda_7)$	$\mathbb{Q}$
19	$(2,5,5)$	$\mathrm{PSL}_2(\mathbb{F}_9)$	T	1	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}$
19	$(4,4,5)$	$\mathrm{PGL}_2(\mathbb{F}_5)$	T	0	$\mathbb{Q}(\sqrt{2},\sqrt{5})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}$
21	$(3,6,6)$	$\mathrm{PGL}_2(\mathbb{F}_5)$	T	2	$\mathbb{Q}(\sqrt{3})$	$\mathbb{Q}$	$\mathbb{Q}$
22	$(2,4,8)$	$\mathrm{PGL}_2(\mathbb{F}_7)$	T	1	$\mathbb{Q}(\lambda_{16})$	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\sqrt{2})$
22	$(4,4,4)$	$\mathrm{PSL}_2(\mathbb{F}_7)$	T	2	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}$
24	$(3,4,7)$	$\mathrm{PSL}_2(\mathbb{F}_7)$	F	1	$\mathbb{Q}(\lambda_7,\sqrt{2})$	$\mathbb{Q}(\lambda_7,\sqrt{2})$	$\mathbb{Q}$
24	$(4,5,6)$	$\mathrm{PGL}_2(\mathbb{F}_5)$	F	1	$\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$	$\mathbb{Q}(\sqrt{30})$	$\mathbb{Q}$

Table 10.5: $\mathrm{PSL}_2(\mathbb{F}_q)$-Galois Belyĭ curves of genus $g \leq 24$

a maximal order has signature $(0; 2, 2, 3, 3)$. See work of Baba and Granath [2] as well as Elkies [24, §3.1] for a detailed discussion of these triangle groups and their relationships.

Theorem B does not apply nor does Remark 5.24 since 3 is ramified in this quaternion algebra. Consequently, the algebra $A \otimes_{\mathbb{Q}} \mathbb{Q}_3$ is a division algebra and $\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}_3$ is the unique maximal order. There is a unique two-sided prime ideal $P \subset \Lambda$ with $\mathrm{nrd}(P) = 3$. The quotient Λ/P is isomorphic to $\mathbb{F}_9 = \mathbb{F}_3(i)$, and $\Lambda/P^2 = \Lambda/3\Lambda$ is isomorphic to the algebra over $\mathbb{F}_3$ generated by i, j subject to $i^2 = -1$, $j^2 = 0$, and $ji = -ij$. We have an exact sequence

$$1 \to (1+P)/(1+3\Lambda) \to (\Lambda/3\Lambda)^\times/\{\pm 1\} \to (\Lambda/P)^\times/\{\pm 1\} \to 1$$

which as finite groups is

$$1 \to \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \to (\Lambda/3\Lambda)^\times/\{\pm 1\} \to \mathbb{Z}/4\mathbb{Z} \to 1.$$

There is a dicyclic group of order 12, a subgroup of $(\Lambda/3\Lambda)^\times/\{\pm 1\}$ that maps surjectively onto $\mathbb{Z}/4\mathbb{Z}$ with kernel $\mathbb{Z}/3\mathbb{Z}$; this gives a cover $X(3, 4, 4; 3) \to X(\Lambda)$ of degree 12. There is an Atkin-Lehner involution (normalizing Λ) whose quotient then yields the cover $f\colon X(3, 4, 4; 3) \to X(3, 4, 4)$ with Galois group $\mathrm{PGL}_2(\mathbb{F}_3)$.

The conjugacy classes of elements of orders 3 and 4 in S_4 are unique, and one can check by hand that the corresponding triple is rigid, so the curve $X(3, 4, 4; 3)$ (with its automorphism group) is defined over $\mathbb{Q}$.

Wolfart [89, §6.3] identifies $X(3, 4, 4; 3)$ as the hyperelliptic curve

$$y^2 = x^8 - 14x^4 + 1 = (x^4 - 4x^2 + 1)(x^4 + 4x^2 + 1)$$

with automorphism group $S_4 \times C_2$. The roots of the polynomial in x are the vertices of a cube in the Riemann sphere. The genus 1 curve $X_0(3, 4, 4; 3)$ is a degree 4 cover of $X(3, 4, 4)$ and corresponds to the fixed field under a subgroup $S_3 \subseteq S_4$: it is the elliptic curve with minimal model

$$y^2 = x^3 + x^2 + 16x + 180$$

of conductor 48 and the map $X_0(3, 4, 4; 3) \to X(3, 4, 4)$ is the map

$$\phi(x, y) = 56 + x^2 - 4y$$

with divisor $4(4, 18) - 4\infty$ and the divisor of $\phi - 108$ is $3(-2, -12) + (22, 108) - 4\infty$. Via $\phi(x, y) = t$, this cover gives rise to the family of S_4-extensions

$$(x^2 + 56 - t)^2 - 16(x^3 + x^2 + 16x + 180) = x^4 - 16x^3 + (96 - 2t)x^2 - 256x + (t^2 - 112t + 256).$$

Remark 10.6. This shows that for exceptional (or commutative) triples there may be normal subgroups of $\overline{\Delta}(a, b, c)$ with quotient isomorphic to $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$ which are not obtained by the construction of Theorem A. In general, covers obtained by considering suborders of index supported at primes dividing the discriminant of the quaternion algebra will give only solvable extensions.

Genus 4, $(2, 4, 5)$*,* $\mathrm{PGL}_2(\mathbb{F}_5)$*;* $(2, 5, 5)$*,* $\mathrm{PGL}_2(\mathbb{F}_4) = \mathrm{PSL}_2(\mathbb{F}_5)$*.* The triangle group $\overline{\Delta}(2, 4, 5)$ is maximal, associated to a quaternion algebra defined over $\mathbb{Q}(\sqrt{5})$ ramified at the prime (2) (obtained as the full Atkin-Lehner quotient), and this group contains $\overline{\Delta}(2, 5, 5)$ as a subgroup of index 2. We have an exceptional isomorphism $\mathrm{PGL}_2(\mathbb{F}_4) = \mathrm{PSL}_2(\mathbb{F}_4) \simeq \mathrm{PSL}_2(\mathbb{F}_5)$, so this curve arises from the congruence subgroup with $\mathfrak{p} = (\sqrt{5})$. The triple $(2, 5, 5)$ is exceptional, but the spherical triangle group that it generates is the full group ($\mathrm{PSL}_2(\mathbb{F}_5) \simeq A_5$; note $\mathrm{PGL}_2(\mathbb{F}_5) \simeq S_5$).

The curve is the Bring curve (see Wolfart [89, §6.4] and also Edge [21]), defined by the equations

$$x_0 + x_1 + ... + x_4 = x_0^2 + x_1^2 + ... + x_4^2 = x_0^3 + x_1^3 + ... + x_4^3 = 0$$

in $\mathbb{P}^4$.

The significance in Theorem B about the splitting behavior of primes is illustrated here. We have $F_5(2,4,5) = \mathbb{Q}(\sqrt{2})$ and $F_5(2,5,5) = \mathbb{Q}$, whereas the trace field of the square subgroup is $E_5(2,4,5) = \mathbb{Q} = E_5(2,5,5) = E$; the prime 5 is inert in $\mathbb{Q}(\sqrt{2})$, so in the former case we obtain a $\mathrm{PGL}_2(\mathbb{F}_5)$-extension and in the latter we obtain a $\mathrm{PSL}_2(\mathbb{F}_5)$-extension.

Genus 5, $(3,3,5)$*,* $\mathrm{PGL}_2(\mathbb{F}_4) \simeq \mathrm{PSL}_2(\mathbb{F}_5)$. The triple $(3,3,5)$ is exceptional but again generates the full group. However, the quaternion algebra A is defined over $\mathbb{Q}(\sqrt{5})$ and is ramified at $(\sqrt{5})$, and $\overline{\Delta}(3,3,5)$ corresponds to the group of units of reduced norm 1 in a maximal order. (The Atkin-Lehner quotient is uniformized by the triangle group $\overline{\Delta}(2,3,10)$—the composite gives a G-Galois Belyĭ map, but $G \not\simeq \mathrm{PGL}_2(\mathbb{F}_5)$, since there is no element of order 10 in this group!)

The conjugacy class of order 3 is unique and there are two of order 5; we check directly that this cover is rigid, even though it is exceptional. Therefore the curve $X = X(3,3,5;5)$ is defined over $\mathbb{Q}$ and its automorphism group is defined over $\mathbb{Q}(\sqrt{5})$.

The cover $X_0(3,3,5;4)$ has genus 0, and is given by

$$t^3(6t^2 - 15t + 10) - 1 = (t-1)^3(6t^2 + 3t + 1).$$

Genus 6, $(2,4,6)$*,* $\mathrm{PGL}_2(\mathbb{F}_5)$. As in the $(3,4,4;3)$ case above, the curve $X(2,4,6)$ is the full $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$-Atkin-Lehner quotient of the curve corresponding to the discriminant 6 quaternion algebra over $\mathbb{Q}$. The curve $X = X(2,4,6;5)$ is rather exotic, in that it does not arise from a congruence subgroup in the usual sense: the usual (Shimura curve) congruence subgroup of level 5 gives a $\mathrm{PSL}_2(\mathbb{F}_5)$-cover of genus 11 mapping to a conic $X(1)$ defined by $x^2 + 3y^2 + z^2 = 0$ and its quotients by Atkin-Lehner involutions give $\mathrm{PGL}_2(\mathbb{F}_5)$-covers, as below. In particular, the curve $X(1)$ does not occur intermediate to $X(2,4,6;5) \to X(2,4,6)$.

Here in Theorem B we have $F(2,4,6) = \mathbb{Q}(\sqrt{2},\sqrt{3})$ and $E(2,4,6) = \mathbb{Q}$; the prime 5 has inertial degree 2 in this extension, hence we get $\mathrm{PGL}_2(\mathbb{F}_5)$. In Theorem A we have $a = 2$ and $G \simeq \mathrm{PGL}_2(\mathbb{F}_5)$ so $d_X = d_{(X,G)} = 1$, hence $M(X) = M(X,G) = \mathbb{Q}$.

The map $X_0(2,4,6;5) \to X(2,4,6)$ is computed by Elkies [24]:

$$(540t^6 + 324t^5 + 135t^4 + 1) - 1 = 27t^4(20t^2 + 12t + 5).$$

And as Elkies observes, by the invariant theory of $\mathrm{PGL}_2(\mathbb{F}_5)$, there are invariants of degree 12, 20, and 30, and a relation of degree 60, so the cover can be written invariantly as

$$y^2 = F_{12}^5/F_{30}^2$$

and this gives the quotient.

Genus 7, $(2,3,7)$*,* $\mathrm{PGL}_2(\mathbb{F}_8)(= \mathrm{SL}_2(\mathbb{F}_8))$. The curve $X = X(2,3,7;2)$ is the Fricke-Macbeath curve [42] of genus 7, the second smallest genus for a Hurwitz curve: i.e., a curve uniformized by a subgroup of the Hurwitz group $\Delta(2,3,7)$ (and therefore having maximal automorphism group for its genus). The curve X has field of moduli equal to $\mathbb{Q}$ and the minimal field of definition of (X,G) is $\mathbb{Q}(\lambda_7)$. Berry and Tretkoff [6] show that the Jacobian J of X is isogenous to E^7, where E is a non-CM elliptic curve with j-invariant equal to $2^8 \cdot 7 = 1792$. (See also Wolfart [89, §6.5] and Wohlfahrt [87].)

Genus 8, $(2,3,8)$*,* $\mathrm{PGL}_2(\mathbb{F}_7)$ *and* $(3,3,4)$*,* $\mathrm{PSL}_2(\mathbb{F}_7)$*.* The curve $X_0(2,3,8;7)$ has genus 0, and the triangle group $\overline{\Delta}(2,3,8)$ arises from the quaternion algebra over $\mathbb{Q}(\sqrt{2})$ ramified at the prime above 2: the map is

$$\phi(t) = t^8 + \frac{1}{7}(-4\sqrt{2}-16)t^7 + (-4\sqrt{2}+6)t^6 + 6\sqrt{2}t^5 + \frac{1}{2}(-36\sqrt{2}+39)t^4 + (3\sqrt{2}-12)t^3 + \frac{1}{2}(-46\sqrt{2}+79)t^2 + \frac{1}{2}(9\sqrt{2}-8)t + \frac{1}{16}(-248\sqrt{2}+313)$$

which factors as

$$\phi(t) = \left(t^2 + \frac{1}{2}(-2\sqrt{2}+1)\right)^3 \left(t^2 + \frac{1}{7}(-4\sqrt{2}-16)t + \frac{1}{2}(-2\sqrt{2}+9)\right)$$

and

$$\phi(t) - \frac{1}{27}(4\sqrt{2}+5) = \left(t^2 + \frac{1}{7}(3\sqrt{2}+12)t + \frac{1}{14}(-8\sqrt{2}+31)\right) \cdot \left(t^3 + \frac{1}{2}(-\sqrt{2}-4)t^2 + \frac{1}{2}(-2\sqrt{2}+7)t + \frac{1}{4}\sqrt{2}\right)^2.$$

We have $\Delta(3,3,4) \subseteq \Delta(2,3,8)$ with index 2 and given by the quotient of the Atkin-Lehner involution, so this gives us also a $\mathrm{PSL}_2(\mathbb{F}_7)$-subcover.

Since $a = 2$ we have $d_X = 1$ and so $M(X) = \mathbb{Q}(\lambda_8)^{\langle \mathrm{Frob}_7 \rangle} = \mathbb{Q}(\sqrt{2})$, in agreement. We only know $d_{(X,G)} \leq 2$, so this is the first example of a curve where the automorphism group may be defined over a quadratic extension of $\mathbb{Q}(\sqrt{2})$.

Genus 14, $(2,3,7)$*,* $\mathrm{PSL}_2(\mathbb{F}_{13})$*.* The curve $X(2,3,7;13)$ is a Hurwitz curve. Some progress has been made in writing down equations for this curve: see work by Moreno-Mejía [51] (and work in progress by Streit; methods of Streit [74] apply in general). The curve can be defined over $\mathbb{Q}(\lambda_7)$ and its automorphism group can be defined over an at most quadratic extension of $\mathbb{Q}(\lambda_7)$ ramified only at 13.

Genus 15, $(2,3,9)$*,* $\mathrm{PGL}_2(\mathbb{F}_8)(= \mathrm{SL}_2(\mathbb{F}_8))$*.* Elkies [22, §2] computed an equation for the genus 1 curve $X_0(2,3,9;2)$, which happens to be an elliptic curve: it is the curve 162b3:

$$y^2 + xy + y = x^3 - x^2 - 95x - 697.$$

Genus 16, $(3,4,6)$*,* $\mathrm{PGL}_2(\mathbb{F}_5)$*.* By Theorem A, the field $M(X)$ it is a degree $d_X \leq 2$ extension of $\mathbb{Q}(\lambda_3,\lambda_4,\lambda_6)^{\langle \mathrm{Frob}_5 \rangle} = \mathbb{Q}$. But since $G \simeq \mathrm{PGL}_2(\mathbb{F}_5)$, we have $d_{(X,G)} = 1$ so $M(X,G) = M(X)$.

This example is interesting because the quaternion algebra A is defined over $E = \mathbb{Q}(\sqrt{6})$ and ramified at the prime $(\sqrt{6}+2)$ over 2. The field E has narrow class number 2 though class number 1—the extension $\mathbb{Q}(\sqrt{-2},\sqrt{-3})$ over $\mathbb{Q}(\sqrt{6})$ is ramified only at ∞. This implies that the Shimura curve is in fact a disjoint union of two curves with an action of this strict class group. The group $\Delta(3,4,6)$ is obtained by an Atkin-Lehner quotient, and since the prime above 2 represents the nontrivial class in the strict class group, the involution interchanges these two curves; consequently, the quotient is something that will be defined canonically over $E = \mathbb{Q}(\sqrt{6})$.

The genus 1 curve $X_0 = X_0(3,4,6;5)$ can be computed as follows. The ramification datum above the designated points $0, 1, \infty$ is $3^2, 4^1 1^2, 6^1$. We take the point above ∞ to be the origin

of the group law on X_0 and take the point $(0,1)$ to be the ramification point of order 4. The curve X_0 is then described by an equation

$$y^2 = x^3 + \lambda_2 x^2 + \lambda_1 x + 1 = f(x)$$

and the map $\phi(x,y) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + (b_0 + b_1 x)y = a(x) + b(x)y$ is of degree 6. By ramification, we must have

$$N\phi(x,y) = a(x)^2 - b(x)^2 f(x) = a_3^2 x^4 (x^2 + c_1 x + c_0)$$

and

$$N(\phi(x,y) - 1) = (a(x) - 1)^2 - b(x)^2 f(x) = a_3^2 (x^2 + d_1 x + d_0)^3$$

for some values c_0, c_1, d_0, d_1. We solve the corresponding system of equations for the values $a_0, \dots, \lambda_2$ and find a unique solution defined over $E = \mathbb{Q}(\sqrt{6})$: after simplifying, the elliptic curve X has minimal model

$$X_0 \colon y^2 + (\sqrt{6}+1)xy = x^3 + (-8\sqrt{6}+23)x + (-2\sqrt{6}+7)$$

with j-invariant

$$j(X_0) = \frac{-21355471243\sqrt{6} + 55502166112}{2^5 5^9} \in \mathbb{Q}(\sqrt{6}) \smallsetminus \mathbb{Q},$$

showing that $M(X) = M(X,G) = \mathbb{Q}(\sqrt{6})$, and

$$\begin{aligned}\phi(x,y) = {} & (186\sqrt{6}+351)x^3 + (9504\sqrt{6}+21564)x^2 + (25350\sqrt{6}+58725)x + 11280\sqrt{6} + 26730 \\ & + ((1611\sqrt{6}+4401)x + (7602\sqrt{6}+18882))y\end{aligned}$$

with ramification at $0, 50000, \infty$.

Genus 24, $(4,5,6)$*,* $\mathrm{PGL}_2(\mathbb{F}_5)$. Finally we arrive at the first of two nonarithmetic curves.

Elkies has computed another interesting subcover of genus 1, namely, the curve E corresponding to the permutation representation of $\mathrm{PGL}_2(\mathbb{F}_5)$ as S_5: it is the curve

$$y^2 + (17 + 2\sqrt{6})xy + 36(7 - 3\sqrt{6})y = x^3 - 36(1 + \sqrt{6})x^2$$

and the Belyĭ function is

$$\phi(x,y) = xy + (-9 + 6\sqrt{6})x^2 + (117 - 48\sqrt{6})y$$

with a pole of degree 5 at infinity, a zero at $P = (0,0)$ of degree 4, and taking the value $2^8 3^3(-5 + 2\sqrt{6})$ with multiplicity 3 at $-6P = (12(\sqrt{6}-1), -144)$ and multiplicity 2 at $9P = (12(9 - 4\sqrt{6}), 48(27 - 10\sqrt{6}))$.

This was computed as follows. The ramification type is 4 $1,5,3$ 2. Put the point of ramification index 5 as the origin of the group law and the 4 point above 0; let P and $P' = -4P$ be the preimages with multiplicities $4,1$. The preimages of multiplicity 3 and 2 are $2Q$ and $-3Q$ for some point Q. But the divisor of $d\phi/\omega$, where ω is a holomorphic differential, is $3P + 2(2Q) + (-3Q) - 6\infty$ hence $Q = -3P$, so these preimages are $-6P$ and $9P$.

We take $E \colon y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2$ so that P is at $(0,0)$ with a horizontal tangent; we scale so $a_2 = a_3$ and let $a_1 = a + 1$ and $a_2 = a_3 = b$. Then $\phi = axy - bx^2 + by$. The condition that $f - f(-6P)$ vanishes to order at least 2 at $-6P$ and vanish at $9P$ leaves a factor $a^2 - 216a + 48$ giving $(a,b) = (108 + 44\sqrt{6}, -(6084 + 2484\sqrt{6}))$.

Genus 24, $(3,4,7)$*,* $\mathrm{PSL}_2(\mathbb{F}_7)$. We have $F = F(3,4,7) = \mathbb{Q}(\lambda_6, \lambda_8, \lambda_{14}) = \mathbb{Q}(\sqrt{2}, \lambda_7)$ and $E = E(3,4,7) = \mathbb{Q}(\lambda_3, \lambda_4, \lambda_7, \lambda_6\lambda_8\lambda_{14}) = \mathbb{Q}(\sqrt{2}, \lambda_7) = F$, and $F_7(3,4,7) = \mathbb{Q}$.

The curve $X(3,4,7;7)$, according to Theorem A, is defined over an at most quadratic extension $M(X)$ of $\mathbb{Q}$; the curve with its automorphism group is defined over $M(X)(\sqrt{-7})$.

We find that the curve $X_0(3,4,7;7)$ has genus one and is defined over $\mathbb{Q}(\sqrt{2})$:

$$E\colon y^2 + (\sqrt{6}+1)xy + (\sqrt{6}+1)y = x^3 + (-14\nu + 3)x + (-78\nu + 128)$$

with j-invariant

$$j(E) = -\frac{14000471420\sqrt{6} + 19227826689}{2^3 3^4 7^5}$$

and good reduction away from $2, 3, 7$. The specialization $\phi = -1$ gives a Galois extension of $\mathbb{Q}(\sqrt{2}, \sqrt{-7})$ with Galois group $\mathrm{PSL}_2(\mathbb{F}_7)$. This gives reason to believe that $M(X) = \mathbb{Q}(\sqrt{2})$ and $M(X, G) = \mathbb{Q}(\sqrt{2}, \sqrt{-7})$.

Another genus 1 quotient of $X(3,4,7;7)$ was computed by Elkies by "turning a p-adic crank" (for an exposition of this method, see the survey by Sijsling–Voight [71, §5]). This curve is defined only over $\mathbb{Q}(\sqrt{2}, \sqrt{-7})$, and already the j-invariant of the curve

$$\frac{-28505956008\sqrt{2}\sqrt{-7} + 39863931701\sqrt{-7} + 120291604664\sqrt{2} + 15630829689}{107495424}$$

generates this field. The subgroup $H \leq \mathrm{PSL}_2(\mathbb{F}_7)$ that gives rise to this curve is not stable under $\sigma\colon \sqrt{-7} \mapsto -\sqrt{-7}$; however, this elliptic curve is 2-isogenous to its Galois conjugate by σ, and so defines a $\mathbb{Q}(\sqrt{2})$-curve, giving further evidence for this hypothesis.

We conclude with an example which extends beyond our table but illustrates an important point.

Example 10.7. Consider the triple $(3,5,6)$ and the prime 11. We obtain from Theorem B a $\mathrm{PSL}_2(\mathbb{F}_{11})$-cover, and this is the curve with smallest genus in the list of all PSL_2-covers such that $a \neq 2$ and $p \nmid abc$. This is the extreme case of Theorem A, where no hypothesis allows us to reduce d_X or $d_{(X,G)}$ or deduce something about $M(X)$ from $M(X, G)$.

We compute that

$$F_{11}(3,5,6)^{\langle \mathrm{Frob}_{11} \rangle} = \mathbb{Q}(\lambda_3, \lambda_5, \lambda_6)^{\langle \mathrm{Frob}_{11} \rangle} = \mathbb{Q}(\lambda_5) = \mathbb{Q}(\sqrt{5})$$

and so $M(X)$ is an extension of

$$E(3,5,6) = \mathbb{Q}(\lambda_3, \lambda_5, \lambda_6, \lambda_6\lambda_{10}\lambda_{12}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$$

of degree at most 2.

The curve $X_0(3,5,6;11)$ has genus 2, and so offers additional computational difficulties. We instead compute the curve E which arises from the quotient by the subgroup $A_5 \subseteq \mathrm{PSL}_2(\mathbb{F}_{11})$. This subcover $E \to \mathbb{P}^1$ is of genus 1 and has degree $11 = \#\,\mathrm{PSL}_2(\mathbb{F}_{11})/\#A_5$.

An equation for this curve was computed by Sijsling and the second author [71]: we find a single Galois orbit of curves defined over the field $\mathbb{Q}(\sqrt{5}, \sqrt{3}, \sqrt{b})$ where

$$b = 4\sqrt{3} + \frac{1}{2}(11 + \sqrt{5});$$

with $N(b) = 11^2$; alternately, it is given by extending by a root β of the equation

$$T^2 - \frac{1+\sqrt{5}}{2}T - (\sqrt{3}+1) = 0.$$

The elliptic curve has minimal model:

$$\begin{aligned}
&y^2 + ((1/2(13\sqrt{5}+33)\sqrt{3} + 1/2(25\sqrt{5}+65))\beta + (1/2(15\sqrt{5}+37)\sqrt{3} + (12\sqrt{5}+30)))xy \\
&\quad + (((8\sqrt{5}+15)\sqrt{3} + 1/2(31\sqrt{5}+59))\beta + (1/2(13\sqrt{5}+47)\sqrt{3} + 1/2(21\sqrt{5}+77)))y \\
&\quad = x^3 + ((1/2(5\sqrt{5}+7)\sqrt{3} + 1/2(11\sqrt{5}+19))\beta + (1/2(3\sqrt{5}+17)\sqrt{3} + (2\sqrt{5}+15)))x^2 \\
&\quad + ((1/2(20828483\sqrt{5}+46584927)\sqrt{3} + 1/2(36075985\sqrt{5}+80687449))\beta \\
&\qquad + (1/2(21480319\sqrt{5}+48017585)\sqrt{3} + 1/2(37205009\sqrt{5}+83168909)))x \\
&\quad + (((43904530993\sqrt{5}+98173054995)\sqrt{3} + 1/2(152089756713\sqrt{5}+340081438345))\beta \\
&\qquad + ((45275857298\sqrt{5}+101240533364)\sqrt{3} + (78420085205\sqrt{5}+175353747591)))
\end{aligned}$$

The j-invariant of this curve generates the field $\mathbb{Q}(\sqrt{5}, \sqrt{3}, \sqrt{\beta})$. So in Theorem B, we see that the possible quadratic extension that may arise from the failure of (weak) rigidity does actually occur.

Remark 10.8. Elkies has suggested that further examples could be obtained by considering triangle covers which are arithmetic, but not congruence.

References

[1] A.O.L. Atkin and H.P.F. Swinnerton-Dyer, *Modular forms on noncongruence subgroups*, Combinatorics (Proc. Sympos. Pure Math., Vol. XIX, Univ. California, Los Angeles, Calif., 1968), Amer. Math. Soc., Providence, R.I., 1971, pp. 1–25.

[2] S. Baba and H. Granath, *Genus 2 curves with quaternionic multiplication*, Canadian J. Math. **60** (2008), no. 4, 734–757.

[3] Ingrid Bauer, Fabrizio Catanese, and Fritz Grunewald, *Faithful actions of the absolute Galois group on connected components of moduli spaces*, Invent. Math. **199** (2015), no. 3, 859–888.

[4] G.V. Belyĭ, *Galois extensions of a maximal cyclotomic field*, Math. USSR-Izv. **14** (1980), no. 2, 247–256.

[5] G.V. Belyĭ, *A new proof of the three-point theorem*, translation in Sb. Math. **193** (2002), no. 3–4, 329–332.

[6] K. Berry and M. Tretkoff, M., *The period matrix of Macbeath's curve of genus seven*, Curves, Jacobians, and abelian varieties, Amherst, MA, 1990, Providence, RI: Contemp. Math., vol. 136, Amer. Math. Soc., 31–40.

[7] A. Borel, *Introduction aux groupes arithmétiques*, Hermann, Paris, 1969.

[8] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language.*, J. Symbolic Comput., **24** (3–4), 1997, 235–265.

[9] S. Allen Broughton, *Quasi-platonic $PSL_2(q)$-actions on closed Riemann surfaces*, Albanian J. Math. **9** (2015), no. 1, 31–61.

[10] Paula Beazley Cohen, Claude Itzykson, and Jürgen Wolfart, *Fuchsian triangle groups and Grothendieck dessins*, Comm. Math. Phys. **163** (1994), no. 3, 605–627.

[11] Paul B. Cohen and Gisbert Wüstholz, *Application of the André–Oort conjecture to some questions in transcendence*, A panorama of number theory or the view from Baker's garden (Zürich, 1999), Cambridge Univ. Press, Cambridge, 2002, 89–106.

[12] Paula Cohen and Jürgen Wolfart, *Modular embeddings for some non-arithmetic Fuchsian groups*, Acta Arith. **56** (1990), 93–110.

[13] Paula Beazley Cohen and Jürgen Wolfart, *Dessins de Grothendieck et variétés de Shimura*, C. R. Acad. Sci. Paris, Serie I, vol. 315, 1992, 1025–1028.
[14] Marston D. E. Conder, Gareth A. Jones, Manfred Streit, and Jürgen Wolfart, *Galois actions on regular dessins of small genera*, Rev. Mat. Iberoam. **29** (2013), no. 1, 163–181.
[15] Kevin Coombes and David Harbater, *Hurwitz families and arithmetic Galois groups*, Duke Math. J. **52** (1985), no. 4, 821–839.
[16] Marston Conder, Primož Potočnik, and Jozef Širáň, *Regular hypermaps over projective linear groups*, J. Aust. Math. Soc. **85** (2008), 155–175.
[17] Henri Darmon, *Rigid local systems, Hilbert modular forms, and Fermat's last theorem*, Duke Math. J. **102** (2000), no. 3, 413–449.
[18] Dèbes and Emsalem, *On fields of moduli of curves*, J. Algebra **211** (1999), no. 1, 42–56.
[19] Pierre Deligne, *Travaux de Shimura*, Séminaire Bourbaki, 23ème année (1970/71), Exp. No. 389, 123–165, Lecture Notes in Math., vol. 244, Springer, Berlin, 1971.
[20] Amir Džambić, *Macbeath's infinite series of Hurwitz groups*, Arithmetic and geometry around hypergeometric functions, Progr. Math., vol. 260, Birkhäuser, Basel, 2007, 101–108.
[21] W.L. Edge, *Bring's curve*, J. London Math. Soc. **2** (1978), no. 3, 539–545.
[22] Noam Elkies, *Shimura curves for level-3 subgroups of the* $(2, 3, 7)$ *triangle group, and some other examples*, Algorithmic number theory, Springer, 2006, 302–316.
[23] Noam Elkies, *The Klein quartic in number theory*, The eightfold way, Math. Sci. Res. Inst. Publ., vol. 35, Cambridge Univ. Press, Cambridge, 1999, 51–101.
[24] Noam Elkies, *Shimura curve computations*, Algorithmic number theory (Portland, OR, 1998), Lecture notes in Comput. Sci., vol. 1423, 1–47.
[25] R. Fricke and F. Klein, *Vorlesungen ueber die Theorie der automorphen Funktionen*, vols. 1–2, Teubner, Leipzig, 1897, 1912.
[26] Ernesto Girondo and Jürgen Wolfart, *Conjugators of Fuchsian groups and quasiplatonic surfaces*, Quart. J. Math. **56** (2005), 525–540.
[27] Ernesto Girondo, David Torres-Teigell, and Jürgen Wolfart, *Fields of definitions of uniform dessins on quasiplatonic surfaces*, Riemann and Klein surfaces, automorphisms, symmetries and moduli spaces, (eds. Milagros Izquierdo, S. Allen Broughton, Antonio F. Costa, and Rubi E. Rodriquez), Contemp. Math. **629**, American Math. Soc., 2014.
[28] Gabino González-Diez and Andrei Jaikin-Zapirain, *The absolute Galois group acts faithfully on regular dessins and on Beauville surfaces*, Proc. Lond. Math. Soc. (3) **111** (2015), no. 4, 775–796.
[29] Leon Greenberg, *Maximal Fuchsian groups*, Bull. Amer. Math. Soc. **69** (1963), 569–573.
[30] Alexandre Grothendieck, *Sketch of a programme (translation into English)*, in *Geometric Galois actions 1*, eds. Leila Schneps and Pierre Lochak, London Math. Soc. Lect. Note Series, vol. 242, Cambridge University Press, Cambridge, 1997, 243–283.
[31] E. Hallouin, *Computation of a cover of Shimura curves using a Hurwitz space*, J. of Algebra **321** (2009), no. 2, 558–566.
[32] E. Hecke, *Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichungen*, Math. Ann. **112** (1936), 664–699.
[33] Huppert, *Endliche Gruppen I*, Grundlehren Math. Wiss., vol. 134, Springer-Verlag, Berlin, 1967.
[34] Gareth A. Jones and Jürgen Wolfart, *Dessins d'enfants on Riemann surfaces*, Springer Monographs in Mathematics, Springer, Cham, 2016.
[35] Svetlana Katok, *Fuchsian groups*, University of Chicago Press, Chicago, 1992.
[36] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, 1985.
[37] Bernhard Köck, *Belyĭ's theorem revisited*, Beiträge Algebra Geom. **45** (2004), no. 1, 253–265.
[38] Robert Kucharczyk, *Modular embeddings and rigidity for Fuchsian groups*, Acta Arith. **169** (2015), no. 1, 77–100.
[39] Sergei K. Lando and Alexander K. Zvonkin, *Graphs on surfaces and their applications*, with an appendix by D. Zagier, Encyclopaedia of Mathematical Sciences, Low-Dimensional Topology, II, Springer-Verlag, Berlin, 2004.

[40] Mong-Lung Lang, Chong-Hai Lim, and Ser-Peow Tan, *Principal congruence subgroups of the Hecke groups*, J. Number Theory **85** (2000) 220–230.
[41] Ulrich Langer and Gerhard Rosenberger, *Erzeugende endlicher projektiver linearer Gruppen*, Results Math. **15** (1989), no. 1–2, 119–148.
[42] A.M. Macbeath, *On a curve of genus* 7, Proc. London Math. Soc. (3) **15** (1965), 527–542.
[43] A.M. Macbeath, *Generators of the linear fractional groups*, Number Theory (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967), Amer. Math. Soc., Providence, 14–32.
[44] Wilhelm Magnus, *Noneuclidean tesselations and their groups*, Pure and Applied Mathematics, vol. 61, Academic Press, New York, 1974.
[45] Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999.
[46] G. Margulis, *Discrete subgroups of semisimple Lie groups*, Springer, Berlin, 1991.
[47] Claude Marion, *Triangle groups and* $\mathrm{PSL}_2(q)$, J. Group Theory **12** (2009) 689–708.
[48] Barry Mazur, Open problems regarding rational points on curves and varieties, Galois representations in arithmetic algebraic geometry (Durham, 1996), London Math. Soc. Lecture Note Ser., vol. 254, Cambridge Univ. Press, Cambridge, 1998, 239–265.
[49] Curtis T. McMullen, *Billiards and Teichmüller curves on Hilbert modular surfaces.* J. Amer. Math. Soc. 16 (2003), 857–885.
[50] J.S. Milne, *Introduction to Shimura Varieties*, Clay Mathematic Proceedings, vol. 4, 2005.
[51] Israel Moreno-Mejía, *The quadrics through the Hurwitz curves of genus 14*, London Math. Soc. **81** (2010), 374–388.
[52] Hans Petersson, *Über die eindeutige Bestimmung und die Erweiterungsfähigkeit von gewissen Grenzkreisgruppen*, Abh. Math. Semin. Univ. Hambg. **12** (1937), no. 1, 180–199.
[53] John G. Ratcliffe, *Foundations of hyperbolic manifolds*, 2nd ed., Graduate Texts in Mathematics, vol. 149, Springer, New York, 2006.
[54] Harry Reimann, *The semi-simple zeta function of quaternionic Shimura varieties*, Lecture Notes in Mathematics, vol. 1657, Springer-Verlag, Berlin, 1997.
[55] Sabine Ricker, *Symmetric Fuchsian quadrilateral groups and modular embeddings*, Quart. J. Math **53** (2002), 75–86.
[56] Alex Rosenberg and Daniel Zelinsky, *Automorphisms of separable algebras*, Pacific J. Math. 11 (1961), 1109–1117.
[57] Paul Schmutz Schaller and Jürgen Wolfart, *Semi-arithmetic Fuchsian groups and modular embeddings*, J. London Math. Soc. (2) **61** (2000), 13–24.
[58] Jan-Christoph Schlage-Puchta and Jürgen Wolfart, *How many quasiplatonic surfaces?*, Arch. Math. (Basel) **86** (2006), no. 2, 129–132.
[59] Thomas A. Schmidt and Katherine Smith, *Galois orbits of principal congruence Hecke curves*, J. London Math. Soc. (2) **67** (2003), no. 3, 673–685.
[60] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, Research Notes in Math., vol. 7. A.K. Peters, Wellesley, MA, 1998.
[61] J.-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics 1, Jones and Bartlett, 1992.
[62] G.B. Shabat and V. Voevodsky, *Drawing curves over number fields*, Grothendieck Festchrift, vol. III, Birkhauser, Boston, 1990, 199–227.
[63] Kuang-yen Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann. **207** (1974), 99–120.
[64] D. Singerman, *Finitely maximal Fuchsian groups*, J. London Math. Soc. (2) **6** (1972), 29–38.
[65] Goro Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. (2) **85** (1967), 58–159.
[66] Goro Shimura, *On canonical models of arithmetic quotients by bounded symmetric domains*, Annals of Math. **91** (1970), no. 1, 144–222.
[67] Goro Shimura, *On canonical models of arithmetic quotients by bounded symmetric domains, II*, Annals of Math. **92** (1970), no. 3, 528–549.
[68] Goro Shimura, *On some arithmetic properties of modular forms of one and several variables*, Ann. of Math. **102** (1975), 491–515.

[69] Goro Shimura, Collected papers, Vol. I–IV, Springer-Verlag, New York, 2002–2003.
[70] Jeroen Sijsling, *Canonical models of arithmetic* $(1; e)$*-curves*, Math. Z. **271** (2012), 173–210.
[71] Jeroen Sijsling and John Voight, *On computing Belyĭ maps*, Publ. Math. Besançon: Algèbre Théorie Nr. 2014/1, Presses Univ. Franche-Comté, Besançon, 73–131.
[72] D. Singerman and R.I. Syddall, *Belyĭ uniformization of elliptic curves*, Bull. London Math. Soc. **139** (1997), 443–451.
[73] Manfred Streit, *Field of definition and Galois orbits for the Macbeath-Hurwitz curves*, Arch. Math. (Basel) **74** (2000), no. 5, 342–349.
[74] Manfred Streit, *Homology, Belyĭ functions and canonical curves*, Manuscripta Math. **90** (1996), 489–509.
[75] Manfred Streit and Jürgen Wolfart, *Characters and Galois invariants of regular dessins*, Rev. Mat. Complut. **13** (2000), no. 1, 49–81.
[76] Michio Suzuki, *Group theory. II*, Grundlehren der Mathematischen Wissenschaften, vol. 248, Springer-Verlag, New York, 1986.
[77] Luiz Takei, *Congruence covers of triangular modular curves and their Galois groups*, preprint, 2015, `1503.00557`.
[78] Kisao Takeuchi, *On some discrete subgroups of* $\mathrm{SL}_2(\mathbb{R})$, J. Fac. Sci. Univ. Tokyo Sect. I **16** (1969), 97–100.
[79] Kisao Takeuchi, *A characterization of arithmetic Fuchsian groups*, J. Math. Soc. Japan **27** (1975), no. 4, 600–612.
[80] Kisao Takeuchi, *Arithmetic triangle groups*, J. Math. Soc. Japan **29** (1977), no. 1, 91–106.
[81] Kisao Takeuchi, *Commensurability classes of arithmetic triangle groups*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **24** (1977), no. 1, 201–212.
[82] Ewa Tyszkowska, *On Macbeath-Singerman symmetries of Belyi surfaces with* $\mathrm{PSL}(2, p)$ *as a group of automorphisms*, Cent. Eur. J. Math. **1** (2003), no. 2, 208–220.
[83] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980.
[84] John Voight, *Semi-arithmetic points on elliptic curves*, in preparation.
[85] John Voight, *Quadratic forms and quaternion algebras: Algorithms and arithmetic*, Ph.D. thesis, University of California, Berkeley, 2005.
[86] Helmut Völklein, *Groups as Galois groups. An introduction*, Cambridge Studies in Advanced Mathematics, vol. 53, Cambridge University Press, Cambridge, 1996.
[87] K. Wohlfahrt, *Macbeath's curve and the modular group*, Glasgow Math. J. **27** (1985), 239–247.
[88] Jürgen Wolfart, *The 'obvious' part of Belyi's theorem and Riemann surfaces with many automorphisms*, Geometric Galois actions, 1, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge Univ. Press, Cambridge, 1997, 97–112.
[89] Jürgen Wolfart, *Triangle groups and Jacobians of CM type*, manuscript, 2000.
[90] Jürgen Wolfart, *Regular dessins, endomorphisms of Jacobians, and transcendence*, A panorama of number theory or the view from Baker's garden (Zürich, 1999), Cambridge Univ. Press, Cambridge, 2002, 107–120.
[91] Jürgen Wolfart, *ABC for polynomials, dessin d'enfants, and uniformization: a survey*, Elementare und analytische Zahlentheorie, Schr. Wiss. Ges. Johann Wolfgang Goethe Univ. Frankfurt am Main, vol. 20, Franz Steiner Verlag Stuttgart, Stuttgart, 2006, 313–345.

Department of Mathematics, University of Georgia, Athens, GA 30602, USA
Email address: `pete@math.uga.edu`

Department of Mathematics and Statistics, University of Vermont, 16 Colchester Ave, Burlington, VT 05401, USA; Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA
Email address: `jvoight@gmail.com`