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.

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 [20] investigated curves obtained as quotients by Fuchsian groups which arise from the unit group of certain quaternion algebras, now called arithmetic groups. Later, Hecke [24] 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 share many appealing properties in common with classical modular curves despite the fact that their uniformizing Fuchsian groups are in general not arithmetic groups.

To motivate the definition of this class of curves, we begin with the modular curves. 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 $\mathcal{H}^*$, and the quotient $X(p) = \Gamma(p)\backslash\mathcal{H}^*$ can be given the structure of Riemann surface, a modular curve. The subgroup $G = \Gamma(1)/\Gamma(p) \subseteq \mathrm{Aut}(X(p))$ satisfies $G \cong \mathrm{PSL}_2(\mathbb{F}_p)$ and the natural map $j : X(p) \to X(p)/G \cong \mathbb{P}^1_{\mathbb{C}}$ is a Galois cover ramified at the points $\{0, 1728, \infty\}$.

In this paper, we will be interested in the class of (algebraic) curves X over $\mathbb{C}$ with the property that there exists a subgroup $G \subseteq \mathrm{Aut}(X)$ with $G \cong \mathrm{PSL}_2(\mathbb{F}_q)$ or $G \cong \mathrm{PGL}_2(\mathbb{F}_q)$ (for some prime power q) such that the map $X \to X/G \cong \mathbb{P}^1$ is a Galois cover ramified at exactly three points.

On the one hand, Belyĭ [3, 4] proved that a curve X over $\mathbb{C}$ admits a *Belyĭ map*, a map $X \to \mathbb{P}^1_{\mathbb{C}}$ ramified at exactly three points, if and only if X can be defined

Date: August 3, 2011.

over the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. On the other hand, there are only finitely many curves X (up to isomorphism) of any genus $g \geq 2$ which admit a Galois Belyĭ map (Remark 2.7). We call a Galois Belyĭ map $f : X \to \mathbb{P}^1$ (with Galois group G) a *(G-)Wolfart map*, and we call a curve which admits a (G-)Wolfart map a *(G-)Wolfart curve*, after Wolfart [66]. These curves are called *curves with many automorphisms* by Wolfart because they are also equivalently characterized as the locus on the moduli space $\mathcal{M}_g(\mathbb{C})$ of curves of genus g at which the function $[C] \mapsto \#\operatorname{Aut}(C)$ attains a strict local maximum. For example, the Hurwitz curves, those curves X with maximal automorphism group $\#\operatorname{Aut}(X) = 84(g-1)$ for their genus g, are Wolfart curves, as are the Fermat curves $x^n + y^n = z^n$ for $n \geq 2$. These curves are also called *quasiplatonic surfaces* [21] owing to their connection with the Platonic solids. (See below for other equivalent characterizations of Wolfart curves.)

The modular curve $X(p)$, a Riemann surface defined over $\mathbb{C}$, has a model as an algebraic curve defined over $\mathbb{Q}$. For a curve X defined over $\mathbb{C}$, the *field of moduli* $M(X)$ of X is the fixed field of the group $\{\sigma \in \operatorname{Aut}(\mathbb{C}) : X^\sigma \cong X\}$, where X^σ is the base change of X by the automorphism $\sigma \in \operatorname{Aut}(\mathbb{C})$. If F is a field of definition for X then clearly F contains the field of moduli of X. If X has a minimal field of definition F then F is necessarily equal to the field of moduli. In fact, a Wolfart curve can always be defined over its field of moduli (Lemma 3.3).

However, in the presence of automorphisms, even if a curve X can be defined over its field of moduli this model need not be unique. We consider therefore also the field of moduli $M(X, \operatorname{Aut}(X))$ of the pair $(X, \operatorname{Aut}(X))$. For example $M(X(p), \operatorname{Aut}(X(p))) = \mathbb{Q}(\sqrt{p^*})$ where $p^* = (-1)^{(p-1)/2}p$. We observe (Remark 3.7) that for any number field K there is a Wolfart curve such that the field of moduli of $(X, \operatorname{Aut}(X))$ contains K. At the same time, we will show that the distinguished class of G-Wolfart curves with $G = \mathrm{PSL}_2(\mathbb{F}_q)$ or $G = \mathrm{PGL}_2(\mathbb{F}_q)$ considered herein have fields of definition which can be explicitly characterized. (See also work of Streit and Wolfart [55] who consider the case $G \cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$.)

To state our first result we use the following notation. For $s \in \mathbb{Z}_{>0}$, let $\zeta_s = \exp(2\pi i/s)$ and $\lambda_s = \zeta_s + 1/\zeta_s = 2\cos(2\pi/s)$. For a prime p and integers $a, b, c \in \mathbb{Z}_{\geq 2}$, let $F_p(a,b,c) = \mathbb{Q}(\lambda_a, \lambda_b, \lambda_c)_{p'}$ be the compositum of the fields $\mathbb{Q}(\lambda_s)$ (resp. $\mathbb{Q}(\zeta_s)$) with $s \in \{a,b,c\}$ prime to p. Let Frob_p be a representative of the conjugacy class of the p-power Frobenius in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

We now consider the following diagram of fields:

$$\begin{array}{c} F(a,b,c) = \mathbb{Q}(\lambda_{2a}, \lambda_{2b}, \lambda_{2c}) \\ | \\ E(a,b,c) = \mathbb{Q}(\lambda_a, \lambda_b, \lambda_c, \lambda_{2a}\lambda_{2b}\lambda_{2c}) \\ | \\ \mathbb{Q}(\lambda_a, \lambda_b, \lambda_c) \\ | \\ F_p(a,b,c) = \mathbb{Q}(\lambda_a, \lambda_b, \lambda_c)_{p'}^{\langle \mathrm{Frob}_p \rangle} \end{array}$$

By convention we let $\zeta_\infty = 1$ and $\lambda_\infty = 2$. Note that indeed $E \subseteq F$ since $\lambda_{2a}^2 = \lambda_a + 2$, and consequently the extension $E \subseteq F$ has degree at most 4 and exponent at most 2. By a *prime* of a number field we mean a nonzero prime ideal of its ring of integers. Note that a prime $\mathfrak{p}$ of E either splits completely or has inertial degree 2 in F. For a prime $\mathfrak{p}$ of a number field, let $\mathbb{F}_\mathfrak{p}$ denote its residue class field. Since these fields are abelian, Frob_p is well-defined.

A triple (a,b,c) is *exceptional* if (a,b,c) is one of

$$(2,3,3), (3,3,3), (3,4,4), (2,3,4), (2,5,5), (5,5,5), (3,3,5), (3,5,5), (2,3,5).$$

(These triples are precisely the orders of elements which generate finite spherical triangle groups.)

A triple (a,b,c) is *commutative* if there is an abelian group generated by two elements of orders a, b whose product has order c; if a triple is commutative, then

$$\frac{\mathrm{lcm}(a,b)}{\gcd(a,b)} \mid c \mid \mathrm{lcm}(a,b).$$

Theorem A. *Let X be a curve of genus $g \geq 2$ and let $f : X \to \mathbb{P}^1$ be a G-Wolfart map with ramification indices (a,b,c). Let p be prime and let q be a power of p. Suppose that (a,b,c) is neither exceptional nor commutative.*

Let r be the order of the Frobenius Frob_p in $\mathrm{Gal}(\mathbb{Q}(\lambda_{2a}, \lambda_{2b}, \lambda_{2c})_{p'}/\mathbb{Q})$. If $G \cong \mathrm{PGL}_2(\mathbb{F}_q)$, then $q = \sqrt{p^r}$; otherwise, if $G \cong \mathrm{PSL}_2(\mathbb{F}_q)$, then $q = p^r$.

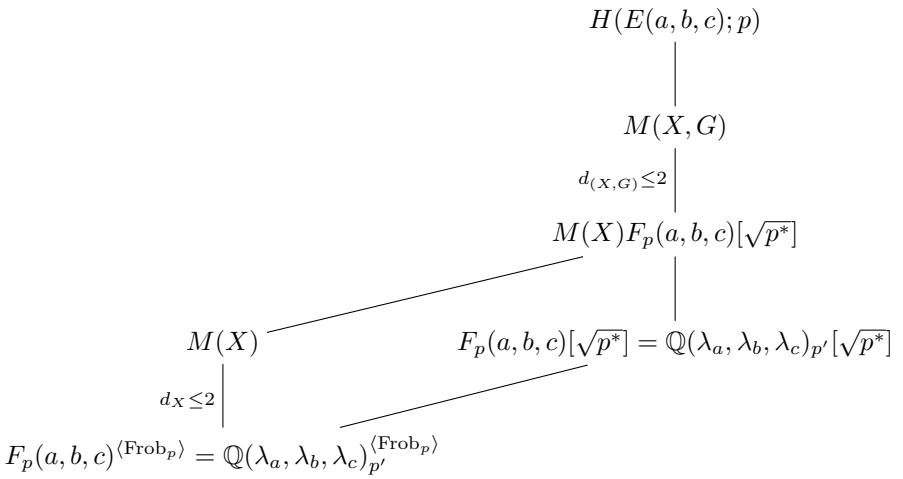
(a) *$M(X)$ is an extension of $F_p(a,b,c)^{\langle \mathrm{Frob}_p \rangle}$ of degree $d_X \leq 2$.*
(b) *$M(X,G)$ is an extension of the compositum of $M(X)$ and $F_p(a,b,c)[\sqrt{p^*}]$ of degree $d_{(X,G)} \leq 2$, where*

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

Each of the fields $M(X) \subseteq M(X,G)$ is contained in the ray class field of $E(a,b,c)$ of conductor p.

Finally, if $a = 2$ or q is even, then $d_X = 1$. If q is even or $p \mid abc$ or $G \cong \mathrm{PGL}_2(\mathbb{F}_q)$, then $d_{(X,G)} = 1$.

These fields fit into the following diagram.



Here $H(E(a,b,c);p)$ is the ray class field of $E(a,b,c)$ of conductor p.

To prove Theorem A, we use a variant of the rigidity and rationality results which arise in the study of the inverse Galois problem [33, 64] 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 [31]. The statements $q = \sqrt{p^r}$ and $q = p^r$, respectively, can be found in earlier work of Langer and Rosenberg [29, Satz (4.2)]; our proof follows similar lines. Theorem A generalizes work of Schmidt and Smith [44, Section 3] who consider the case of Hecke triangle groups as well as work of Streit [53] who considers Hurwitz groups, where $(a,b,c) = (2,3,7)$.

As a complement to Theorem A, we explicitly construct the corresponding Wolfart maps. Let $a,b,c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$ satisfy $a \leq b \leq c$ and let p be a prime with $p \nmid abc$. The triple (a,b,c) is *hyperbolic* if

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

Theorem B. *Let (a,b,c) be a hyperbolic triple with $a,b \in \mathbb{Z}_{\geq 2}$ and $c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$. Suppose that (a,b,c) is neither exceptional nor commutative. Let $\mathfrak{p}$ be a prime of $E(a,b,c)$ above the rational prime $p \nmid abc$.*

Then there exists a G-Wolfart map

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

with ramification indices (a,b,c) or (a,b,p) according as $c \in \mathbb{Z}$ or $c = \infty$, where

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

Aside from the excluded triples, this construction gives all possible G-Wolfart maps with $G \cong \mathrm{PSL}_2(\mathbb{F}_q)$ or $G \cong \mathrm{PGL}_2(\mathbb{F}_q)$.

We make the convention that no prime p divides ∞, so if $c = \infty$ then we may take any prime $\mathfrak{p}$ above $p \nmid ab$. In some circumstances (depending on a norm residue symbol), one can take primes dividing abc (see Section 4).

The construction of Wolfart maps in Theorem B arises from another equivalent characterization of Wolfart curves (of genus ≥ 2) as compact Riemann surfaces of the form $\Gamma\backslash\mathcal{H}$, where Γ is a finite index normal subgroup of a hyperbolic triangle group $\overline{\Delta}(a,b,c)$, defined as the abstract group generated by elements $\overline{\gamma}_a, \overline{\gamma}_b, \overline{\gamma}_c$ subject to the relations

$$\overline{\gamma}_a^a = \overline{\gamma}_b^b = \overline{\gamma}_c^c = \overline{\gamma}_a\overline{\gamma}_b\overline{\gamma}_c = 1$$

where by convention we let $\overline{\gamma}^\infty = 1$. (See Sections 1–2 for more detail.) Phrased in this way, Theorem B asserts the existence of a normal subgroup $\overline{\Delta}(a,b,c;\mathfrak{p}) \trianglelefteq \overline{\Delta}(a,b,c)$ with quotient isomorphic to G as above. We call such a subgroup a *congruence* subgroup of $\overline{\Delta}(a,b,c)$ in analogy with the classical case of modular curves, since these subgroups arise from certain congruence conditions. The proof uses a modular embedding of the triangle group $\overline{\Delta}(a,b,c)$ into an arithmetic group, following Takeuchi [59] and later work of Cohen and Wolfart [10].

Theorem B generalizes work of Lang, Lim, and Tan [28] who treat the case of Hecke triangle groups using an explicit presentation of the group (see also Example 10.4).

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 defined over a totally real field which is split at a unique real place. A deep theorem of Margulis [34] states that a Fuchsian group is arithmetic if and only if it is of infinite index in its commensurator group. By work of Takeuchi [59], 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 a canonical model was given by Shimura [50] and Deligne [15]. Indeed, the curves $X(2,3,\infty;p)$ are the classical modular curves $X(p)$ and the Wolfart map $j : X(p) \to \mathbb{P}^1$ is associated to the congruence subgroup $\Gamma(p) \subseteq \mathrm{PSL}_2(\mathbb{Z})$. Several other arithmetic families of Wolfart curves have seen more detailed study, most notably the family $X(2,3,7;\mathfrak{p})$ of Hurwitz curves. Aside from these finitely many cases, the groups $\Delta(a,b,c;\mathfrak{p})$ are not arithmetic; at the same time, based upon the result of Theorem B we believe that these curves carry a rich geometry which is worthy of study. In particular, the curves obtained by considering the quotient $X_0(a,b,c;\mathfrak{p})$ of $X(a,b,c;\mathfrak{p})$ by the subgroup of upper-triangular matrices are analogous to the classical modular curves $X_0(p)$.

The congruence subgroups so defined naturally extend to composite ideals, and so they form a projective system (Proposition 9.4). 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 $\mathfrak{n} \nmid 6abc$.

Theorem C. *$\overline{\Delta}(a,b,c)$ is a dense open subgroup of $\widehat{P}$.*

The construction of these curves has several interesting applications. Combining Theorems A and B we see that the 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 $M(X,G)$. (See Malle and Matzat [33], Serre [46, Chapters 7–8], and Volklein [64] for more information and groups realized regularly by rigidity and other methods.)

Moreover, the 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 [13] 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 [61], who studies the fixed points of a particular symmetry of $\mathrm{PSL}_2(\mathbb{F}_p)$-Wolfart curves.)

The paper is organized as follows. In Sections 1 and 2, we introduce triangle groups, Belyĭ maps, and Wolfart curves. In Section 3 we briefly review the basic theory of fields of moduli. In Section 4, 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 5 the theory of weak rigidity which provides the statement of Galois descent we will employ; in Sections 6, we set up the basic theory of $\mathrm{PSL}_2(\mathbb{F}_q)$ and in Section 7 we use Macbeath's theory of two-generated subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ to prove most of Theorem A. In Section 8, we use the reflex field of the quaternionic Shimura variety to further specify the field of moduli and complete the proof of Theorem A. In Section 9, we prove Theorems B and C. Finally, we conclude in Section 10 with many explicit examples and pose some final questions.

The second author would like to thank Henri Darmon, Richard Foote, David Harbater, Hilaf Hasson, Jennifer Paulhus, and Jeroen Sijsling for helpful discussions and is especially grateful to Noam Elkies for his valuable comments and encouragement.

1. Triangle groups

In this section, we review the basic theory of triangle groups. We refer to Magnus [32, Chapter II] and Ratcliffe [39, §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 $-1, \gamma_a, \gamma_b, \gamma_c$, with -1 central in Δ, subject to the

relations $(-1)^2 = 1$ and

$$\gamma_a^a = \gamma_b^b = \gamma_c^c = \gamma_a\gamma_b\gamma_c = -1; \tag{1.1}$$

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

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

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

Remark 1.2. Reordering generators permits our assumption that $a \leq b \leq c$ without loss of generality. Indeed, the defining condition $\gamma_a\gamma_b\gamma_c = -1$ is invariant under cyclic permutations so $\Delta(a,b,c) \cong \Delta(b,c,a) \cong \Delta(c,a,b)$, and similarly the map which sends a generator to its inverse gives an isomorphism $\Delta(a,b,c) \cong \Delta(c,b,a)$.

We analogously classify the groups $\overline{\Delta}(a,b,c)$ as spherical, Euclidean, or hyperbolic.

Example 1.3. The spherical triangle groups are all finite groups: indeed, we have $\overline{\Delta}(2,2,c) \cong D_{2c}$ (the dihedral group of order $2c$), $\overline{\Delta}(2,3,3) \cong A_4$, $\overline{\Delta}(2,3,4) \cong S_4$, and $\overline{\Delta}(2,3,5) \cong S_5$.

Example 1.4. For $a, b \in \mathbb{Z}_{\geq 2}$, the group $\overline{\Delta}(a,b,\infty)$ is the free product $\mathbb{Z}/a\mathbb{Z} * \mathbb{Z}/b\mathbb{Z}$ of the groups $\mathbb{Z}/a\mathbb{Z}$ and $\mathbb{Z}/b\mathbb{Z}$.

We have an exact sequence

$$1 \to [\overline{\Delta}, \overline{\Delta}] \to \overline{\Delta} \to \overline{\Delta}^{\mathrm{ab}} \to 1. \tag{1.5}$$

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 $\overline{\Delta}^{\mathrm{ab}} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. 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 $[\overline{\Delta}(2,2,\infty), \overline{\Delta}(2,2,\infty)] \cong \mathbb{Z}$, whereas for the other Euclidean triples we have $[\overline{\Delta}, \overline{\Delta}] \cong \mathbb{Z}^2$ [32, §II.4]. In particular, the Euclidean triangle groups are infinite and nonabelian, but solvable.

The triangle groups $\overline{\Delta}(a,b,c)$ with $(a,b,c) \neq (2,2,\infty)$ have 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 accordingly, where by convention we let $\pi/\infty = 0$. 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 $\overline{\gamma}_a = \overline{\tau}_a\overline{\tau}_b$, $\overline{\gamma}_b = \overline{\tau}_b\overline{\tau}_c$, and $\overline{\gamma}_c = \overline{\tau}_c\overline{\tau}_a$ 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 reflecting the triangle T in one of its sides. The sides of this fundamental domain are identified by the elements $\overline{\gamma}_a$, $\overline{\gamma}_b$, and $\overline{\gamma}_c$, and consequently the quotient space is a Riemann surface of genus zero. This surface is compact if and only if $a, b, c \neq \infty$ (equivalently, $c \neq \infty$ since $a \leq b \leq c$).

Example 1.6. We have the isomorphism $\Delta(2,3,\infty) \cong \mathrm{SL}_2(\mathbb{Z})$ and consequently $\overline{\Delta}(2,3,\infty) \cong \mathrm{PSL}_2(\mathbb{Z})$.

The Hecke triangle groups [24] are given by $\overline{\Delta}(2,n,\infty) \cong \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/n\mathbb{Z}$ for $n \geq 3$.

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 acting discretely on the (completed) upper half-plane $\mathcal{H}^{(*)}$; we write $X(a,b,c) = \overline{\Delta}(a,b,c)\backslash\mathcal{H}^{(*)} \cong \mathbb{P}^1_{\mathbb{C}}$ for the quotient space. The embedding $\overline{\Delta}(a,b,c) \hookrightarrow \mathrm{PSL}_2(\mathbb{R})$ is unique up to conjugacy in $\mathrm{PSL}_2(\mathbb{R})$ since any two hyperbolic triangles with the same angles are congruent (or isometric).

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 (but will be excluded anyway for other reasons later). Then Takeuchi [59, 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 [38]. As in the introduction, for $s \in \mathbb{Z}_{\geq 2}$, let $\zeta_s = \exp(2\pi i/s)$ and

$$\lambda_s = \zeta_s + \frac{1}{\zeta_s} = 2\cos\left(\frac{2\pi}{s}\right) \quad \text{and} \quad \mu_s = 2\sin\left(\frac{2\pi}{s}\right) = -i\left(\zeta_s - \frac{1}{\zeta_s}\right) \tag{1.7}$$

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

Then we have a map

$$\begin{aligned} \Delta(a,b,c) &\hookrightarrow \mathrm{SL}_2(\mathbb{R}) \\ \gamma_a &\mapsto \frac{1}{2}\begin{pmatrix} \lambda_{2a} & \mu_{2a} \\ -\mu_{2a} & \lambda_{2a} \end{pmatrix} \\ \gamma_b &\mapsto \frac{1}{2}\begin{pmatrix} \lambda_{2b} & t\mu_{2b} \\ -\mu_{2b}/t & \lambda_{2b} \end{pmatrix} \end{aligned} \tag{1.8}$$

where

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

The embedding (1.8) then also gives rise to an explicit embedding $\overline{\Delta}(a,b,c) \hookrightarrow \mathrm{PSL}_2(\mathbb{R})$.

A triangle group $\overline{\Delta}$ is *maximal* if it cannot be properly embedded in any other Fuchsian group (as a subgroup with finite index). By a result of Singerman [49] (see also Greenberg [22, Theorem 3B]), if $\overline{\Delta}(a,b,c)$ is not maximal then in fact $\overline{\Delta}$ is contained in another triangle group $\overline{\Delta}'$. All inclusion relations between triangle groups can be generated (by concatenation) from the relations [21, (2)]

$$\begin{array}{ll} \overline{\Delta}(2,7,7) \subseteq_9 \overline{\Delta}(2,3,7) & \overline{\Delta}(3,8,8) \subseteq_{10} \overline{\Delta}(2,3,8) \\ \overline{\Delta}(4,4,5) \subseteq_6 \overline{\Delta}(2,4,5) & \overline{\Delta}(3,3,7) \subseteq_8 \overline{\Delta}(2,3,7) \end{array} \tag{1.9}$$

or one of the families

$$\begin{array}{ll} \overline{\Delta}(a,a,a) \subseteq_3 \overline{\Delta}(3,3,a) & \overline{\Delta}(a,a,c) \subseteq_2 \overline{\Delta}(2,a,2c) \\ \overline{\Delta}(2,b,2b) \subseteq_3 \overline{\Delta}(2,3,2b) & \overline{\Delta}(3,b,3b) \subseteq_4 \overline{\Delta}(2,3,3b), \end{array} \tag{1.10}$$

where in (1.10) (and here alone) for notational simplicity we relax our assumption that $a \leq b \leq c$. The notation $\overline{\Delta} \subseteq_n \overline{\Delta}'$ is an abbreviation for $[\overline{\Delta}' : \overline{\Delta}] = n$. It follows that $\Delta(a,b,c)$ is maximal if and only if (a,b,c) is not of the form

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

with again $a, b, c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$, and in this case we say the triple (a, b, c) is *maximal*.

A Fuchsian group Γ is *arithmetic* [6] if there exists a quaternion algebra B over a totally real field F which is ramified at all but one real place (and possibly some finite places) such that Γ is commensurable with the image of the units of reduced norm 1 in a maximal order $\mathcal{O} \subseteq B$. Takeuchi [59, Theorem 3] has classified all triples (a, b, c) such that $\overline{\Delta}(a, b, c)$ is arithmetic; there are 85 such triples and they fall into 19 commensurability classes [60, Table (1)].

Remark 1.11. For arithmetic triples, our result on the existence of congruence subgroups and fields of definition of their (canonical) models is well-known, due to Shimura [50] and Deligne [15]: see Remark 10.3.

2. Wolfart curves, Belyĭ maps

In this section, we discuss Belyĭ maps and Wolfart curves and we relate these curves to those uniformized by subgroups of triangle groups.

A *Belyĭ map* is a morphism $f : X \to \mathbb{P}^1$ of Riemann surfaces (equivalently, algebraic curves over $\mathbb{C}$) which is ramified at exactly 3 points. A Belyĭ map which is a Galois covering (with Galois group G), i.e. a covering whose corresponding extension of function fields is Galois (with Galois group G), is called a *(G-)Wolfart map*, named after Wolfart who studied these curves in detail [66, 68]. We note that if $X \to X/G$ realizes X as a Wolfart curve of genus $g \geq 2$, then $X \to X/\mathrm{Aut}(X)$ does as well.

Example 2.1. The map $f : \mathbb{P}^1 \to \mathbb{P}^1$ given by $f(t) = t^2(t + 3)$ has $f(t) - 4 = (t - 1)(t + 2)^2$ and thus gives a Belyĭ map ramified over $0, 4, \infty$ with ramification indices $(2, 2, 3)$. The Galois closure of the map f gives an S_3-Wolfart map $\mathbb{P}^1 \to \mathbb{P}^1$ corresponding to the simplest spherical triangle group $\overline{\Delta}(2, 2, 3)$. All examples of Belyĭ maps $\mathbb{P}^1 \to \mathbb{P}^1$ arise in this way from the spherical triangle groups.

Example 2.2. An elliptic curve E (over $\overline{\mathbb{Q}}$ or $\mathbb{C}$) is a Wolfart curve if and only if E has CM by either $\mathbb{Q}(\omega)$ or $\mathbb{Q}(i)$. Indeed, if $f : E \to E/G \cong \mathbb{P}^1$ is a Wolfart map with $G \subseteq \mathrm{Aut}(E)$ (automorphisms as a genus 1 curve), then we can factor f into the composition of an isogeny $E \to E'$ (an unramified map) and a quotient $E' \to E'/G' \cong \mathbb{P}^1$, where now G' is a subgroup of automorphisms of E' as an elliptic curve. In particular, if $j(E') \neq 0, 1728$, then $G' = \{\pm 1\}$, but the quotient of E' by -1 is ramified at the four 2-torsion points of E', a contradiction.

Indeed, for $j = 0$ we have the curve $E : y^2 - y = x^3$ with CM by $K = \mathbb{Z}[\omega]$ where$\omega^3 = 1$, and the quotient by $\omega : E \to E$ gives the Wolfart map $y : E \to \mathbb{P}^1$ of degree 3 ramified over $0, 1, \infty$. If $j = 1728$, then $E : y^2 = x^3 - x$ has CM by $K = \mathbb{Z}[i]$ and the quotient by $i : E \to E$ gives a Galois Belyĭ map of degree 4 defined by x^2. Note that in each case $(X, \mathrm{Aut}(X))$ is minimally defined over its CM field K.

These curves arise as the quotients by the Euclidean triangle groups $\overline{\Delta}(2, 4, 4)$ and $\overline{\Delta}(3, 3, 3) \hookrightarrow \overline{\Delta}(2, 3, 6)$. We refer to work of Singerman and Syddall [52] for a more complete treatment.

In view of Examples 2.1 and 2.2, from now on we consider Wolfart maps $f : X \to \mathbb{P}^1$ with X of genus $g \geq 2$. These curves can be characterized in several equivalent ways.

Proposition 2.3 (Wolfart [66, 68])**.** *Let X be a compact Riemann surface of genus $g \geq 2$. Then the following are equivalent.*

(i) *X is a Wolfart curve;*
(ii) *The map $X \to X/\mathrm{Aut}(X)$ is a Belyĭ map;*
(iii) *There exists a finite index, normal subgroup $\Gamma \subseteq \overline{\Delta}(a,b,c)$ 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 $[X]$ in the moduli space $\mathcal{M}_g(\mathbb{C})$ of curves of genus g such that $\#\mathrm{Aut}(X) > \#\mathrm{Aut}(Y)$ for all $[Y] \in U \setminus \{[X]\}$.*

Remark 2.4. We note the following interesting consequence of Proposition 2.3. If $\Gamma' \subseteq \mathrm{PSL}_2(\mathbb{Z}) \cong \overline{\Delta}(2,3,\infty)$ is a normal subgroup and $X = \Gamma'\backslash\mathcal{H}^{(*)}$ is a Wolfart curve, then in fact X is uniformized by a group $\Gamma \subseteq \overline{\Delta}(a,b,c)$ with $a,b,c \in \mathbb{Z}_{\geq 2}$. A similar statement holds for any subgroup of a triangle group $\overline{\Delta}(a,b,c)$ with $c = \infty$, including the Hecke triangle groups [44, Proposition 4].

By the Riemann-Hurwitz formula, if X is a G-Wolfart curve with ramification degrees (a,b,c), then X has genus

$$g(X) = 1 + \frac{\#G}{2}\left(1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}\right) = 1 - \frac{\#G}{2}\chi(a,b,c). \tag{2.5}$$

Remark 2.6. The function of $\#G$ in (2.5) is maximized when $(a,b,c) = (2,3,7)$. Combining this with Proposition 2.3(iv) we recover the Hurwitz bound

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

Remark 2.7. There are only finitely many Wolfart curves of any given genus g. By the Hurwitz bound (2.6), we can bound $\#G$ given $g \geq 2$, and for of the finitely many possible groups G there are only finitely possible values of a,b,c by (2.5). See Table 10.5 for the determination of all $\mathrm{PSL}_2(\mathbb{F}_q)$-Wolfart curves with genus $g \leq 100$.

In fact, according to Schlage-Puchta and Wolfart [43], the number of isomorphism classes of Wolfart curves of genus $\leq g$ grows like $g^{\log g}$. Wolfart [68] gives a complete list of all Wolfart curves of genus $g = 2, 3, 4$. Further examples of Wolfart curves can be found in the work of Shabat and Voevodsky [47].

Example 2.8. Let $f : V \to \mathbb{P}^1$ be a Belyĭ map and let $g : X \to \mathbb{P}^1$ be its Galois closure. Then g is also a Belyĭ map and hence X is a Wolfart curve. Note however that the genus of X may be much larger than the genus of V!

Condition Proposition 2.3(iii) leads us to consider curves arising from finite index normal subgroups of the hyperbolic triangle groups $\overline{\Delta}(a,b,c)$. If $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{R})$ is a Fuchsian group, write $X(\Gamma) = \Gamma \setminus \mathcal{H}^{(*)}$. If X is a compact Riemann surface of genus $g \geq 2$ with uniformizing subgroup $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{R})$, so that $X = X(\Gamma)$, then $\mathrm{Aut}(X) = N(\Gamma)/\Gamma$, where $N(\Gamma)$ is the normalizer of Γ in $\mathrm{PSL}_2(\mathbb{R})$. Moreover, the quotient $X \to X/\mathrm{Aut}(X)$, obtained from the map $X(\Gamma) \to X(N(\Gamma))$, is a Galois

cover with Galois group $\mathrm{Aut}(X)$. By the results of Section 1, if $\Gamma \subseteq \overline{\Delta}(a,b,c)$ is a finite index normal subgroup then $\mathrm{Aut}(X(\Gamma))$ is of the form $\overline{\Delta}'/\Gamma$ with an inclusion $\overline{\Delta} \subseteq \overline{\Delta}'$ as in (1.9)–(1.10); if $\overline{\Delta}$ is maximal, then we conclude simply

$$\mathrm{Aut}(X(\Gamma)) \cong \overline{\Delta}(a,b,c)/\Gamma. \tag{2.9}$$

3. Fields of moduli

In this section, we briefly review the theory of fields of moduli and fields of definition. See Coombes and Harbater [12] and Köck [27] for more detail.

The *field of moduli* $M(X)$ of a curve X over $\mathbb{C}$ is the fixed field of the group $\{\sigma \in \mathrm{Aut}(X) : X^\sigma \cong X\}$. If F is a field of definition for X then clearly F contains the field of moduli of X. If X has a minimal field of definition F, then F is necessarily equal to the field of moduli.

Remark 3.1. Belyĭ's theorem can be rephrased as saying that field of moduli of a curve is a number field if and only if the curve admits a Belyĭ map.

Remark 3.2. Let $f : X \to C$ be a separable morphism over a field F which ramified at three points where C has genus 0. Then in fact $C \cong \mathbb{P}^1$ over F, since the ramification divisor on C has odd degree and is defined over F.

It is well-known that not every curve can be defined over its field of moduli. However, in our situation we have the following lemma.

Lemma 3.3. *Let X be a Wolfart curve. Then X is defined over its field of moduli.*

Proof. Debes and Emsalem [14] remark that this lemma follows from results of Coombes and Harbater [12]. The proof was written down by Köck [27, Theorem 2.2]: in fact, he shows that any Galois covering of curves $X \to \mathbb{P}^1$ can be defined over the field of moduli of the cover (similarly defined), and the field of moduli of X as a curve is equal to the field of moduli of the covering $X \to X/\mathrm{Aut}(X)$. See also the proof in Wolfart [69, Theorem 5]. □

Let X be a curve which can be defined over its field of moduli $F = M(X)$. Then the set of models for X over F is given by the Galois cohomology set $H^1(F, \mathrm{Aut}(X))$, where $\mathrm{Aut}(X)$ is viewed as a module over the absolute Galois group $\mathcal{G}_F = \mathrm{Gal}(\overline{F}/F)$. The action of $\mathcal{G}_F$ on $\mathrm{Aut}(X)$ cuts out a finite Galois extension $K \supseteq F$ which is the minimal field such that all elements of $\mathrm{Aut}(X)$ are defined over K; in other words, the pair $(X, \mathrm{Aut}(X))$ has field of moduli equal to its minimal field of definition K.

Remark 3.4. Let X be a G-Wolfart curve with $G = \mathrm{Aut}(X)$ and let K be the minimal field of definition for $(X, \mathrm{Aut}(X))$. Then by definition the group G occurs as a Galois group over $K(t)$, and in particular applying Hilbert's irreducibility theorem [46, Chapter 3] we find that G occurs infinitely often as a Galois group over K.

Example 3.5. Let p be prime and let $X = X(p) = \Gamma(p)\backslash\mathcal{H}^*$ be the classical modular curve, parametrizing (generalized) elliptic curves with full p-level structure. Then $\mathrm{Aut}(X) \supseteq G = \mathrm{PSL}_2(\mathbb{F}_p)$ (with equality when $p \geq 7$, so that the genus of $X(p)$ is ≥ 2), and the quotient map $j : X \to X/G \cong \mathbb{P}^1$, corresponding to the inclusion $\Gamma(p) \subseteq \mathrm{PSL}_2(\mathbb{Z})$, is ramified over $j = 0, 1728, \infty$ with indices $2, 3, p$. In particular, $X(p)$ is a Wolfart curve.

The field of moduli of X is $\mathbb{Q}$, and indeed X admits a model over $\mathbb{Q}$ [26]. This model is not unique, since the set $H^1(\mathbb{Q}, \mathrm{Aut}(X))$ is infinite: in fact, every isomorphism class of Galois modules $E[p]$ with E an elliptic curve gives a distinct class in this set.

In any case, the field of rational numbers $\mathbb{Q}$ is not a field of definition for $\mathrm{Aut}(X)$. Rather, letting $p^* = (-1)^{(p-1)/2}p$, Shih showed that the pair $(X, \mathrm{Aut}(X))$ has minimal field of definition $\mathbb{Q}(\sqrt{p^*})$. Note that the naive moduli interpretation of X gives a model over $\mathbb{Q}(\zeta_p)$.

Example 3.6. The Klein quartic has field of definition equal to field of moduli which is $\mathbb{Q}$. The field of definition of $(X, \mathrm{Aut}\, X)$ is $\mathbb{Q}(\zeta_7)^+$. Although the Klein quartic is isomorphic to $X(7)$ over $\overline{\mathbb{Q}}$, as remarked by Livné, in fact the canonical model of $X(7)$ agrees with the Klein quartic only over $\mathbb{Q}(\sqrt{-3})$—the two are quadratic twists. The issue here concerns the fields of definition of the special points giving rise to the canonical model; happily, this issue will not concern us.

Remark 3.7. We consider again Remark 2.8. If the field of moduli of a Belyĭ map $f : V \to \mathbb{P}^1$ is F then the field of moduli of its Galois closure $g : X \to \mathbb{P}^1$ is also F. It follows that for any number field F, there exists a Wolfart curve X such that any field of definition of X (hence also of $(X, \mathrm{Aut}\, X)$) contains F. Indeed, we obtain such an X from any curve V with field of moduli F, e.g. an elliptic curve such that $\mathbb{Q}(j(V)) = F$, since any such curve admits a Belyĭ map (defined over F)! Note that from Example 2.2 that outside of a handful of cases, the Wolfart curve X corresponding to V has genus $g(X) \geq 2$.

In view of Remark 3.7, we restrict our attention from now on to the special class of G-Wolfart curves X where $G = \mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$, which we will show have distinguished arithmetic and geometric properties.

4. Congruence subgroups of triangle groups

In this section, we associate a quaternion algebra over a totally real field to a triangle group following Takeuchi [58]. This idea was also pursued by Cohen and Wolfart [10] with an eye toward results in transcendence theory, and further elaborated by Cohen, Itzykson and Wolfart [9]. Here, we use this embedding to construct congruence subgroups of Δ. We refer to Vignéras [62] for the facts we will use about quaternion algebras and Katok [25] as a reference on Fuchsian groups.

Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{R})$ be a subgroup such that $\Gamma/\{\pm 1\} \subseteq \mathrm{PSL}_2(\mathbb{R})$ is a finitely generated Fuchsian group of the first kind. Let

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

be the *trace field* of Γ. Then in fact F is finitely generated over $\mathbb{Q}$ and hence F is a totally real number field. 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 [57, Propositions 2–3], the ring $F[\Gamma]$ is a quaternion algebra over F. If further $\mathrm{tr}(\Gamma) \subseteq \mathbb{Z}_F$, then $\mathbb{Z}_F[\Gamma]$ is an order in $F[\Gamma]$.

Remark 4.1. This construction can be made more general. Schaller and Wolfart [42] call a Fuchsian group Γ *semi-arithmetic* if its trace field $F = \mathbb{Q}(\mathrm{tr}\,\Gamma)$ is a totally real number field and $\{\mathrm{tr}\,\gamma^2 : \gamma \in \Gamma\}$ is contained in the ring of integers of F. They ask if all semi-arithmetic groups are either arithmetic or subgroups of triangle groups, and the answer to this question is affirmative if a certain general conjecture of Chudnovsky and Chudnovsky [8, Section 7] holds. See also work of Ricker [41].

Now let (a, b, c) be a hyperbolic triple with $2 \leq a \leq b \leq c \leq \infty$. As in §1, associated to the triple (a, b, c) is the triangle group $\Delta(a, b, c) \subseteq \mathrm{SL}_2(\mathbb{R})$ with $\Delta(a, b, c)/\{\pm 1\} \cong \overline{\Delta}(a, b, c) \subseteq \mathrm{PSL}_2(\mathbb{R})$. Let $F = \mathbb{Q}(\mathrm{tr}\,\Delta(a, b, c))$ be the trace field of $\Delta(a, b, c)$.

The generating elements $\gamma_s \in \Delta(a, b, c)$ for $s = a, b, c$ satisfy the quadratic equations

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

in B where λ_{2s} is defined in (1.7).

Lemma 4.2. *If $\gamma_1, \ldots, \gamma_r$ generate Γ, then $\mathbb{Q}(\mathrm{tr}\,\Gamma)$ is generated by $\mathrm{tr}(\gamma_{i_1} \cdots \gamma_{i_s})$ for $\{i_1, \ldots, i_s\} \subseteq \{1, \ldots, r\}$.*

From the lemma, we compute that

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

Since

$$\gamma_a\gamma_b = -\gamma_c^{-1} = \gamma_c - \lambda_{2c},$$

taking traces we have

$$-\mathrm{tr}(\gamma_c^{-1}) = -\lambda_{2c} = \mathrm{tr}(\gamma_a\gamma_b) = \gamma_a\gamma_b + (\lambda_{2b} - \gamma_b)(\lambda_{2a} - \gamma_a)$$

we have

$$\gamma_a\gamma_b + \gamma_b\gamma_a = \lambda_{2b}\gamma_a + \lambda_{2a}\gamma_b - \lambda_{2c} - \lambda_{2a}\lambda_{2b}. \tag{4.3}$$

Together with the cyclic permutations of these equations, we conclude that the elements $1, \gamma_a, \gamma_b, \gamma_c$ form a $\mathbb{Z}_F$-basis for the order $\mathcal{O} = \mathbb{Z}_F[\Delta] \subseteq B = F[\Delta]$ (see also Takeuchi [59, Proposition 3]).

Lemma 4.4. *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 (4.3) as

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

since $\gamma_a\gamma_c = -\gamma_b^{-1}$ and $\gamma_b\gamma_c = -\gamma_a^{-1}$. □

Lemma 4.5. *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 $(mk, m(k+1), mk(k+1))$ with $k, m \in \mathbb{Z}$, 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 (beautiful) identity in the field $\mathbb{Q}(\zeta_{2a}, \zeta_{2b}, \zeta_{2c}) = K$:

$$\beta = \left(\frac{\zeta_{2b}\zeta_{2c}}{\zeta_{2a}} + 1\right)\left(\frac{\zeta_{2a}\zeta_{2c}}{\zeta_{2b}} + 1\right)\left(\frac{\zeta_{2a}\zeta_{2b}}{\zeta_{2c}} + 1\right)\left(\frac{1}{\zeta_{2a}\zeta_{2b}\zeta_{2c}} + 1\right). \tag{4.6}$$

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 (4.6).

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

$$\frac{1}{b} + \frac{1}{c} = 1 + \frac{1}{a} \in \mathbb{Q}/2\mathbb{Z}. \tag{4.7}$$

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 (4.7).

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 $c = kb$. Substituting this back in we find that $(k+1) \mid b$ so $b = m(k+1)$ and hence $a = km$ and $c = mk(k+1)$, 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

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

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

$$\overline{\Delta} = \Delta/\{\pm 1\} \hookrightarrow \mathcal{O}_1^\times/\{\pm 1\}. \tag{4.8}$$

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 (1.5):

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

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 $(1,1,1)$ (by convention, if $c = \infty$ then we take $\mathbb{Z}/c\mathbb{Z} = \{0\}$). 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 γ_s for $s \in \{a, b, c\}$ such that either $s = \infty$ or s is even, and

$$\Delta/\Delta^{(2)} \cong \begin{cases} \{0\}, & \text{if at least two of } a, b, c \text{ are odd;} \\ \mathbb{Z}/2\mathbb{Z}, & \text{if exactly one of } a, b, c \text{ is odd;} \\ (\mathbb{Z}/2\mathbb{Z})^2, & \text{if all of } a, b, c \text{ are even or } \infty. \end{cases} \tag{4.9}$$

(See also Takeuchi [59, Proposition 5].)

Consequently, $\Delta^{(2)}$ is the normal closure of the set $\{-1, \gamma_a^2, \gamma_b^2, \gamma_c^2\}$ in Δ. A modification of the proof of Lemma 4.2 shows that the trace field of $\Delta^{(2)}$ can be computed on these generators (trace is invariant under conjugation). We have

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

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

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

and

$$\operatorname{tr}(\gamma_a^2\gamma_b^2\gamma_c^2) = \operatorname{tr}((\lambda_{2a}\gamma_a - 1)(\lambda_{2b}\gamma_b - 1)(\lambda_{2c}\gamma_c - 1)) = \lambda_{2a}^2 + \lambda_{2b}^2 + \lambda_{2c}^2 + \lambda_{2a}\lambda_{2b}\lambda_{2c} - 2;$$

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

$$E = F(a,b,c) = \mathbb{Q}(\lambda_{2a}^2, \lambda_{2b}^2, \lambda_{2c}^2, \lambda_{2a}\lambda_{2b}\lambda_{2c}) = \mathbb{Q}(\lambda_a, \lambda_b, \lambda_c, \lambda_{2a}\lambda_{2b}\lambda_{2c}). \tag{4.10}$$

(See also Takeuchi [59, Propositions 4–5].)

Example 4.11. 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

$$\Delta^{(2)}/\{\pm 1\} \hookrightarrow \mathcal{O}_1^{(2)\times}/\{\pm 1\}. \tag{4.12}$$

We then have the following fundamental result.

Proposition 4.13. *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 group $N_A(\mathcal{O}^{(2)\times})/F^{(2)\times}$ *via*

$$\begin{aligned} \overline{\Delta} &\hookrightarrow \frac{N_A(\Lambda)}{F^{(2)\times}} \hookrightarrow \frac{N_B(\mathcal{O})}{F^\times} \\ \overline{\gamma}_s &\mapsto \gamma_s^2 + 1 \end{aligned} \tag{4.14}$$

where $s = a, b, c$ *and* N *denotes the normalizer. The map* (4.14) *extends the natural embedding* (4.12)*.*

Example 4.15. 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 $\mathbb{Q}$.

Proof of Proposition 4.13. First, suppose $a \neq 2$ (for a hyperbolic triple, we always have $2 < b \leq c$). In B we have

$$\gamma_s^2 + 1 = \lambda_{2s}\gamma_s; \tag{4.16}$$

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

$$(\gamma_a^2+1)(\gamma_b^2+1)(\gamma_c^2+1) = \lambda_{2a}\lambda_{2b}\lambda_{2c}\gamma_a\gamma_b\gamma_c = -\lambda_{2a}\lambda_{2b}\lambda_{2c} \in F^\times$$

so the map (4.14) indeed defines a group homomorphism $\overline{\Delta} \hookrightarrow B^{(2)\times}/F^{(2)\times}$. The image lies in the normalizer $N_A(\Lambda)$ because $\Delta^{(2)}$ generates Λ and Δ normalizes $\Delta^{(2)}$. Finally, we have

$$(\gamma_s^2+1)^2 = \lambda_{2s}^2\gamma_s^2 \in E[\Delta^{(2)}]$$

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

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

$$\overline{\gamma}_a \mapsto (\gamma_b^2+1)(\gamma_c^2+1)$$

since $(\gamma_b^2+1)(\gamma_c^2+1) = \lambda_{2b}\lambda_{2c}(-\gamma_a^{-1}) = \lambda_{2b}\lambda_{2c}\gamma_a$ now has order 2 in $B^{(2)\times}/F^{(2)\times}$. □

Corollary 4.17. *We have* $\Lambda \otimes_{\mathbb{Z}_E} \mathbb{Z}_F \subseteq \mathcal{O}$ *with index dividing* $\lambda_{2a}\lambda_{2b}\lambda_{2c}$ *if* $a \neq 2$ *and dividing* $\lambda_{2b}\lambda_{2c}$ *if* $a = 2$*.*

Proof. This statement follows from (4.16) since a basis for $\mathcal{O}$ is given by $1, \gamma_a, \gamma_b, \gamma_c$. □

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) is not of the form $(mk, m(k+1), mk(k+1))$. Then by Lemma 4.5, we have a splitting

$$\mathcal{O} \hookrightarrow \mathcal{O} \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{N}} \cong \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{N}}) \tag{4.18}$$

where $\mathbb{Z}_{F,\mathfrak{N}}$ denotes the completion of $\mathbb{Z}_F$ at $\mathfrak{N}$ (the product of the completions at $\mathfrak{P}$ for $\mathfrak{P} \mid \mathfrak{N}$). Let

$$\mathcal{O}(\mathfrak{N}) = \{\gamma \in \mathcal{O} : \gamma \equiv 1 \pmod{\mathfrak{N}\mathcal{O}}\}.$$

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

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

Let

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

Then we have an embedding

$$\frac{\overline{\Delta}}{\overline{\Delta}(\mathfrak{N})} \hookrightarrow \frac{\mathcal{O}_1^\times/\{\pm 1\}}{\mathcal{O}(\mathfrak{N})_1^\times} \cong \mathrm{PSL}_2(\mathbb{F}_{\mathfrak{N}}). \tag{4.19}$$

We conclude by considering the image of the embedding (4.19). Let $\mathfrak{n}$ be the prime of $E = F(a,b,c)$ 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 (4.17). Therefore, we may define $\Lambda(\mathfrak{n})$ analogously. Then by Proposition 4.13, we have an embedding

$$\overline{\Delta} \hookrightarrow \frac{N_A(\Lambda)}{F^{(2)\times}} \hookrightarrow \frac{B^{(2)\times}}{F^{(2)\times}} \hookrightarrow \frac{B_{\mathfrak{n}}^{(2)\times}}{F_{\mathfrak{n}}^{(2)\times}} \cong \mathrm{PGL}_2(F_{\mathfrak{n}}^{(2)}) \tag{4.20}$$

where $F_{\mathfrak{n}}$ denotes the completion of F at $\mathfrak{n}$. The image of $\overline{\Delta}$ in this map lies in $\mathrm{PGL}_2(\mathbb{Z}_{E,\mathfrak{n}})$ 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 (4.20) 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 4.13.

We summarize the main result of this section.

Proposition 4.21. *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) is not of the form $(mk, m(k+1), mk(k+1))$. Let $\mathfrak{n} = \mathbb{Z}_E \cap \mathfrak{N}$. Then there exists a homomorphism ϕ with*

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

such that $\operatorname{tr}\phi(\overline{\gamma}_s) \equiv \pm\lambda_{2s} \pmod{\mathfrak{N}}$ 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 4.22. 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 claim that

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

for any $s \in \{a,b,c\}$. Indeed, given the basis $1, \gamma_a, \gamma_b, \gamma_c$, we construct an orthogonal basis for B as

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

which gives rise to the presentation $B \cong \left(\frac{4-\lambda_{2a}^2, \beta}{F}\right)$. The others follow by symmetry.

It follows that a prime $\mathfrak{P}$ of $\mathbb{Z}_F$ ramifies in B if and only if $(\lambda_{2s}^2 - 4, \beta)_{\mathfrak{P}} = -1$ for all $s \in \{a,b,c\}$. 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 [60, Proposition 2] shows that

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

For any prime $\mathfrak{p}$ of E which is unramified in A, we can repeat the above construction, replacing Λ and $\mathcal{O}$ with maximal orders containing them, respectively; we obtain again a homomorphism ϕ as in (4.21).

5. 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 [12], Malle and Matzat [33], Serre [46, Chapters 7–8], and Volklein [64] for references.

Let G be a finite group. A *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.) 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 natural (diagonal) action of $\mathrm{Inn}(G) = G/Z(G)$ on G^n stabilizes $\Sigma(\underline{C})$ and thus gives an action of $\mathrm{Inn}(G)$ on $\Sigma(\underline{C})$.

From now on we assume that G has trivial center, so $\mathrm{Inn}(G) = G$. Suppose that $\Sigma(\underline{C}) \neq \emptyset$. Then the action of $\mathrm{Inn}(G)$ 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 $z \in Z(G) = \{1\}$.

Let $P_1, \ldots, P_n \in \mathbb{P}^1(\mathbb{Q})$ be distinct points. For every generating tuple $\underline{g}$, we obtain from the Riemann existence theorem a branched covering $X(\underline{g}) \to \mathbb{P}^1$ with ramification type $\underline{g}$ over $P_1, \ldots, P_n$ and and Galois group G defined over $\overline{\mathbb{Q}}$. Two such covers $X(\underline{g}) \to \mathbb{P}^1$ and $X(\underline{g}') \to \mathbb{P}^1$ are isomorphic as covers if and only if there exists an automorphism $\varphi \in \mathrm{Aut}(G)$ such that $\varphi(\underline{g}) = (\varphi(g_1), \ldots, \varphi(g_n)) = \varphi(\underline{g}')$. Two covers equipped with maps $G \hookrightarrow \mathrm{Aut}(X(\underline{g}))$ such that $X(\underline{g}) \to X(\underline{g})/G \cong \mathbb{P}^1$ are isomorphic if and only if $\underline{g}, \underline{g}'$ are uniformly conjugate in G, i.e. there exists $x \in G$ such that

$$\underline{g}^x = (xg_1x^{-1}, \ldots, xg_nx^{-1}) = (\underline{g}')^x.$$

In this way, 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.

In general, this action is mysterious: in fact, to understand it in general is part of Grothendieck's program to understand $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ via its faithful action on the fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$. There is one part of the action which is understood, coming from the maximal abelian extension of $\mathbb{Q}$ generated by roots of unity.

Let $\zeta_n = \exp(2\pi i/n) \in \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ be the usual primitive nth root of unity, and use this compatible system of roots of unity to normalize the inertia groups of a cover. With this normalization, the group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ acts on a tuple via the cyclotomic character χ: for $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ and a triple $\underline{g}$, we have $\sigma \cdot \underline{g}$ is uniformly conjugate to $(g_1^{\chi(\sigma)}, \ldots, g_n^{\chi(\sigma)})$ where if g_i has order m_i then $g_i^{\chi(\sigma)}$ is conjugate to $g_i^{a_i}$, where $\sigma(\zeta_{m_i}) = \zeta_{m_i}^{a_i}$.

This action becomes an action on conjugacy classes in purely group theoretic language as follows. 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 the set of triples for G.

Let $H_{\mathrm{rat}} \subseteq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is the kernel of this action, i.e.

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

The fixed field $F_{\mathrm{rat}}(G) = \mathbb{Q}(\zeta_m)^{H_{\mathrm{rat}}}$ is called the *field of rationality* of G. The field $F_{\mathrm{rat}}(G)$ can also be characterized as the field obtained by adjoining to $\mathbb{Q}$ the values of the character table of G [46, §7.1]. Let $H(\underline{C}) \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$ be the stabilizer of $\underline{C}$ under this action, i.e.

$$H(\underline{C}) = \{s \in (\mathbb{Z}/m\mathbb{Z})^\times : \ C_i^s = C_i \text{ for all } i\}.$$

We define the *field of rationality* of $\underline{C}$ to be

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

Similarly, let

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

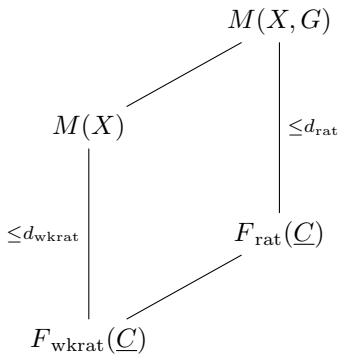
We define the *field of weak rationality* of $\underline{C}$ to be the fixed field $F_{\mathrm{wkrat}}(\underline{C}) = \mathbb{Q}(\zeta_m)^{H_{\mathrm{wkrat}}(\underline{C})}$. Evidently we have

$$F_{\mathrm{wkrat}}(\underline{C}) \subseteq F_{\mathrm{rat}}(\underline{C}) \subseteq F_{\mathrm{rat}}(G).$$

Having identified the stabilizer in this way, we now have an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/F_{\mathrm{wkrat}}(\underline{C}))$ on the set of generating tuples $\underline{g} \in \Sigma(\underline{C})$ up to uniform automorphism, which we denote $\Sigma(\underline{C})/\mathrm{Aut}(G)$. Let $X = X(\underline{g}) \to \mathbb{P}^1$ be such a cover. Then X has field of moduli $M(X)$ equal to the fixed field of the stabilizer of this action, a number field of degree $\leq d_{\mathrm{wkrat}} = \#\Sigma(\underline{C})/\mathrm{Aut}(G)$ over $F_{\mathrm{wkrat}}(\underline{C})$.

Similarly, the field of moduli of (X, G), i.e. X equipped with an embedding $G \hookrightarrow \mathrm{Aut}(X)$ such that the cover is given by $X \to X/G \cong \mathbb{P}^1$, has field of moduli

$M(X,G)$ equal to the fixed field of the stabilizer of the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/F_{\mathrm{rat}}(\underline{C}))$, a number field of degree $\leq d_{\mathrm{rat}} = (\#\Sigma(\underline{C})/\mathrm{Inn}(G))/d_{\mathrm{wkrat}}$ over $F_{\mathrm{wkrat}}(\underline{C})$.



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: we have

$$M(X,G) = F_{\mathrm{rat}}(\underline{C}) \supseteq M(X) = F_{\mathrm{wkrat}}(\underline{C}).$$

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 [12] say *inner rigid* and *outer rigid* for rigid and weakly rigid, respectively.) In this case, we have $M(X) = F_{\mathrm{wkrat}}(\underline{C})$ and the group $\mathrm{Gal}(M(X,G)/F_{\mathrm{rat}})$ injects canonically into the group $\mathrm{Out}(G)$.

We summarize the above discussion in the following proposition.

Proposition 5.1. *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 $P_1, \ldots, P_n \in \mathbb{P}^1(\mathbb{Q})$. Then the following statements hold.*

(a) *There exists a curve X (over $\overline{\mathbb{Q}}$) and an embedding $G \hookrightarrow \mathrm{Aut}(X)$ such that the map*

$$f : X \to X/G \cong \mathbb{P}^1$$

is a branched covering with ramification type $\underline{C} = (C_1, \ldots, C_n)$ over the points $P_1, \ldots, P_n$.

(b) *The curve X can be defined over its field of moduli $M(X)$, a number field of degree $\leq d_{\mathrm{wkrat}} = \#\Sigma(\underline{C})/\mathrm{Aut}(G)$ over $F_{\mathrm{wkrat}}(\underline{C})$.*

(c) *There is a (unique) minimal field of definition $M(X,G)$ for X together with the subgroup $G \hookrightarrow \mathrm{Aut}(X)$, a number field of degree at most*

$$d_{\mathrm{rat}} = \frac{\#\Sigma(\underline{C})/\mathrm{Inn}(G)}{d_{\mathrm{wkrat}}}$$

over $F_{\mathrm{wkrat}}(\underline{C})$ containing $F_{\mathrm{rat}}(\underline{C})$.

6. Basic theory of $\mathrm{GL}_2(\mathbb{F}_q)$

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 derived from $\mathrm{GL}_2(\mathbb{F}_q)$.

First let $g \in \mathrm{GL}_2(\mathbb{F}_q)$. By the Jordan canonical form, either the characteristic polynomial $f(g;T) \in \mathbb{F}_q[T]$ has two repeated roots (in $\mathbb{F}_q$)—and hence g is a scalar matrix (central in $\mathrm{GL}_2(\mathbb{F}_q)$), or g is conjugate to a matrix of the form $\begin{pmatrix} t & 1 \\ 0 & t \end{pmatrix}$ for $t \in \mathbb{F}_q^\times$ in which case we say g is *unipotent*—or $f(g;T)$ 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*.

Now we consider the reduction $\overline{g} \in \mathrm{PGL}_2(\mathbb{F}_q) = \mathrm{GL}_2(\mathbb{F}_q)/\mathbb{F}_q^*$. If g is scalar then $\overline{g} = \overline{1}$. If g is unipotent then $\overline{g}$ is conjugate to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. 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 $c \in \mathbb{F}_q^*$ become identified. If $f(g;T)$ factors over $\mathbb{F}_q$ then g is conjugate to a matrix $\begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}$ with $x \in \mathbb{F}_q^* \setminus \{1\}$, and we say that g is *split*. The set of split semisimple conjugacy classes is therefore in bijection with the set of classes $[x]$ with $x \in \mathbb{F}_q^* \setminus \{1\}$ where we identify x with x^{-1}: there are $(q-3)/2 + 1 = (q-1)/2$ such classes. If $f(g;T)$ is irreducible over $\mathbb{F}_q$ then taking a root of this characteristic polynomial gives a bijection between the set of *nonsplit* conjugacy classes and equivalence classes $[y]$ with $y \in (\mathbb{F}_{q^2} \setminus \mathbb{F}_q)/\mathbb{F}_q^*$, totalling q in all.

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 g is conjugate to either $U(u) = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ or $-U(u)$ 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 is q is even there is a single such conjugacy class.

Otherwise, g is semisimple and so g is conjugate in $\mathrm{SL}_2(\mathbb{F}_q)$ to the matrix $\begin{pmatrix} 0 & -1 \\ 1 & \mathrm{tr}(g) \end{pmatrix}$, 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 of a semisimple element of $\mathrm{PSL}_2(\mathbb{F}_q)$ is then

again uniquely determined by its trace. (Note that this is unique to $\mathrm{PSL}_2(\mathbb{F}_q)$—the trace no longer determines a conjugacy class in $\mathrm{PGL}_2(\mathbb{F}_q)$!)

We now describe the outer automorphism group $\mathrm{Out}(\mathrm{PSL}_2(\mathbb{F}_q))$ (see e.g. Suzuki [56]). The p-power Frobenius map σ, acting on the entries of a matrix by $a \mapsto a^p$, gives such an outer automorphism. When p is odd, the map τ given by conjugation by an element in $\mathrm{PGL}_2(\mathbb{F}_q) \setminus \mathrm{PSL}_2(\mathbb{F}_q)$ is also such an automorphism. In fact, these maps generate $\mathrm{Out}(\mathrm{PSL}_2(\mathbb{F}_q))$:

$$\mathrm{Out}(\mathrm{PSL}_2(\mathbb{F}_q)) \cong \begin{cases} \langle \sigma, \tau \rangle, & \text{if } p \text{ is odd;} \\ \langle \sigma \rangle, & \text{if } p = 2. \end{cases} \tag{6.1}$$

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 $\mathrm{PSL}_2(\mathbb{F}_{q^2}) \setminus \mathrm{PSL}_2(\mathbb{F}_q)$. The stabilizer in $\mathrm{Out}(\mathrm{PSL}_2(\mathbb{F}_q))$ of a unipotent conjugacy class is equal to $\langle \sigma \rangle$. For the semisimple conjugacy classes, we note that if g is semisimple then (diagonalizing over $\overline{\mathbb{F}}_p$) we see that $\sigma(g)$ is conjugate to g^p, and since $f(g^p; T) = f^{\sigma^{-1}}(g; T)$ where σ acts on the coefficients of f, we see directly that the stabilizer of a semisimple class is $\langle \sigma^s, \tau \rangle$ where $\mathbb{F}_{q^s}$ is its trace field if p is odd and $\langle \sigma^s \rangle$ if $p = 2$.

In a similar way, we have simply $\mathrm{Out}(\mathrm{PGL}_2(\mathbb{F}_q)) \cong \langle \sigma \rangle$. Here again the stabilizer of a unipotent conjugacy classes is $\langle \sigma \rangle$. If C is a split semisimple conjugacy class corresponding to $[x]$ with $x \in \mathbb{F}_q^* \setminus \{1\}$ then the stabilizer of C is equal to $\langle \sigma^s \rangle$ where $\mathbb{F}_{q^s} = \mathbb{F}_q(x)$. If C is nonsplit and semisimple then we claim that its stabilizer is trivial. Indeed, suppose the class corresponds to $[y]$ with $y\mathbb{F}_q^* \in (\mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*)/\mathbb{F}_q^*$, then $[y] = [y^p]$ implies that $y^{p-1} \in \mathbb{F}_q^*$ or $y^{q/p-1} \in \mathbb{F}_q^*$. Without loss of generality (replacing σ by σ^{-1}) we may assume that $y^{p-1} \in \mathbb{F}_q^*$. Then $y^{q-1} \in \mathbb{F}_p^\times$, which is a contradiction since then $\mathrm{tr}(y) \in y\mathbb{F}_p \notin \mathbb{F}_q$. A similar argument for the powers of σ then proves the claim.

We conclude this section by describing the field of rationality (as defined in §5) for these conjugacy classes. For an odd prime p, we abbreviate $p^* = (-1)^{(p-1)/2} p$. Recall that $q = p^r$.

Lemma 6.2. *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*

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

The field of weak rationality of C is

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

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

Proof. We first prove the result for $g \in \mathrm{SL}_2(\mathbb{F}_q)$ and then use this to derive the result for $\pm g \in \mathrm{PSL}_2(\mathbb{F}_q)$. So suppose that $g \in \mathrm{SL}_2(\mathbb{F}_q)$ has order $2m$. If $g = \pm 1$, the result is clear.

First, suppose $g = U(u)$ is unipotent with $u \in \mathbb{F}_q^\times$. Then for all $s \in \mathbb{Z}$ prime to p, we have $g^s = U(su)$. 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 $\mathrm{SL}_2(\mathbb{F}_q)$ is $\mathbb{Q}(\sqrt{p^*})$. The same result holds for $g = -U(u)$, and these are identified in the quotient $\mathrm{PSL}_2(\mathbb{F}_q)$, so the field of rationality of C in $\mathrm{PSL}_2(\mathbb{F}_q)$ is also $\mathbb{Q}(\sqrt{p^*})$.

Next we consider semisimple conjugacy classes. By the trace map, these classes are in bijection with $t \in \mathbb{F}_q \setminus \{\pm 2\}$. The induced action on the set of traces is given by $t = z + 1/z \mapsto z^s + 1/z^s$ for $s \in (\mathbb{Z}/2m\mathbb{Z})^\times$ where z is a primitive $2m$th root of unity. From this description, we see that the stabilizer of t is $\langle -1 \rangle \subseteq (\mathbb{Z}/2m\mathbb{Z})^\times$. Now we consider $\mathrm{PSL}_2(\mathbb{F}_q)$; we may assume that p is odd. We then have instead an action on traces $\pm t$. If m is odd then $\pm g$ also has order m and the stabilizer is again $\langle -1 \rangle \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$. If m is even, then $\pm g$ has order m; since then $\zeta^m = -1$, we see that the stabilizer of $\pm t$ is $\langle -1, m+1 \rangle \subseteq (\mathbb{Z}/2m\mathbb{Z})^\times$; this is the preimage of the subgroup $\langle -1 \rangle \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$, so the fixed field remains $\mathbb{Q}(\lambda_m)$.

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 t up to isomorphism is $\langle -1, p \rangle \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$, the field fixed further under the Frobenius Frob_p. □

Corollary 6.3. *The field of rationality of* $\mathrm{PSL}_2(\mathbb{F}_q)$ *is*

$$F_{\mathrm{rat}}(\mathrm{PSL}_2(\mathbb{F}_q)) = \begin{cases} \mathbb{Q}(\lambda_{(q-1)/2}, \lambda_{(q+1)/2}, \sqrt{p^*}), & \text{if } pr \text{ is odd;} \\ \mathbb{Q}(\lambda_{(q-1)/2}, \lambda_{(q+1)/2}), & \text{if } p \text{ is odd and } r \text{ is even;} \\ \mathbb{Q}(\lambda_{q-1}, \lambda_{q+1}), & \text{if } p = 2. \end{cases}$$

Proof. The exponent of $\mathrm{SL}_2(\mathbb{F}_q)$ is $m = (q^2-1)p/2$ if p is odd and $m = (q^2-1)p$ if $p = 2$. By the above, there exist $g \in \mathrm{SL}_2(\mathbb{F}_q)$ with orders $q+1, q-1$, so the stabilizer of all semisimple conjugacy classes is $\langle -1 \rangle \subseteq (\mathbb{Z}/(m/p)\mathbb{Z})^\times$. The corresponding elements of $\mathrm{PSL}_2(\mathbb{F}_q)$ for q odd have orders $(q+1)/2, (q-1)/2$. □

Lemma 6.4. *Let* $\overline{g} \in \mathrm{PGL}_2(\mathbb{F}_q)$ *have order* m*. Then the field of rationality of the conjugacy class* C *of* g *is*

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

and the field of weak rationality of C *is*

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

Proof. The power of a unipotent conjugacy class is unipotent (or scalar) so its field of rationality is $\mathbb{Q}$. If C is split semisimple, corresponding to $[x]$ with $x \in \mathbb{F}_q^* \setminus \{1\}$ (identifying x with x^{-1}) then $x \mapsto x^s$ for $s \in (\mathbb{Z}/m\mathbb{Z})^\times$ and the stabilizer is $\langle -1 \rangle \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$. If C is nonsplit, corresponding to $[y]$ with $y\mathbb{F}_q^\times \in (\mathbb{F}_{q^2}^\times \setminus \mathbb{F}_q^\times)/\mathbb{F}_q^\times$ then again $y \mapsto y^s$ for $s \in (\mathbb{Z}/m\mathbb{Z})^\times$ and the stabilizer is $\langle q \rangle \subseteq (\mathbb{Z}/m\mathbb{Z})^\times$. But $m \mid (q+1)$ so $q \equiv -1 \pmod{m}$, so we have the same result as in the split case.

A similar proof gives the field of weak rationality, where now $\sigma(C) = C^p$. □

7. 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 §5 can be further applied to the groups $\mathrm{PSL}_2(\mathbb{F}_q)$ (and consequently $\mathrm{PGL}_2(\mathbb{F}_q)$) using celebrated work of Macbeath [31], which we recall in this section. See also Langer and Rosenberg [29], who give an exposition of Macbeath's work in our context.

Let q be a prime power. We begin by considering (not necessarily generating) triples $\underline{g} = (g_1, g_2, g_3)$ with $g_i \in \mathrm{SL}_2(\mathbb{F}_q)$, so $g_1 g_2 g_3 = 1$, with an eye to understanding the image of the subgroup generated by g_1, g_2, g_3 in $\mathrm{PSL}_2(\mathbb{F}_q)$. These will be characterized by the traces of the corresponding elements.

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 triples $\underline{g}$ such that $\mathrm{tr}(g_i) = t_i$ for $i = 1, 2, 3$. The group $\mathrm{Inn}(\mathrm{SL}_2(\mathbb{F}_q)) \cong \mathrm{PSL}_2(\mathbb{F}_q)$ acts on $T(\underline{t})$ by conjugating triples.

Proposition 7.1 (Macbeath [31, Theorem 1])**.** *For all trace triples $\underline{t}$, the set $T(\underline{t})$ is nonempty.*

To a triple $\underline{g} = (g_1, g_2, g_3) \in \mathrm{SL}_2(\mathbb{F}_q)^3$, we associate an *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 (1.2) we restrict to order triples (a, b, c) with $a \leq b \leq c$.

Our goal is to give conditions under which we can be assured that a 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 quadratic form

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

is singular [31, Corollary 1, p. 21], i.e. if

$$d(t_1, t_2, t_3) = t_1^2 + t_2^2 + t_3^2 - t_1 t_2 t_3 - 4 = 0. \tag{7.2}$$

If a trace triple $\underline{t}$ is not commutative, then we associate the triple of orders (a, b, c) for any $\underline{g} \in T(\underline{t})$. This is well-defined because the trace uniquely defines the order

of a semisimple or unipotent element: we cannot have ± 1 in $\underline{g} \in T(\underline{t})$ since then the group it generates is necessarily commutative.

Remark 7.3. It appears that the only time that this actually happens is when the trace triple is $(2,2,2)$ with any even number of signs.

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 the following:

$$(2,3,3),(3,3,3),(3,4,4),(2,3,4),(2,5,5),(5,5,5),(3,3,5),(3,5,5),(2,3,5). \tag{7.4}$$

The exceptional triples are precisely the orders of triples of elements of $\mathrm{SL}_2(\mathbb{F}_q)$ which generate finite spherical triangle groups in $\mathrm{PSL}_2(\mathbb{F}_q)$.

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.

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

Proposition 7.5 ([31, Theorem 4])**.** *Every trace triple $\underline{t}$ is either exceptional, commutative or projective.*

Example 7.6. For illustration, we consider the case $q = 7$. The only trace triples where the order triple is not well-defined are $(2,2,2)$ *with an even number of signs*, by which we mean

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

In each of these four cases, there exist triples $\underline{g}$ with order triples $(1,1,1)$, $(1,7,7)$, and $(7,7,7)$. The other commutative trace triples are:

The 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) such that

$$d(t_1,t_2,t_3) = t_1^2 + t_2^2 + t_3^2 - t_1t_2t_3 - 4 = 0.$$

The latter three are exceptional, as 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 $(3,3,3)$
$(1,1,2)$, with even number of signs	having orders $(3,3,7)$
$(1,3,3)$, 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 odd number of 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 note that one cannot deduce that a trace triple is projective by looking only at its order triple.

The issue of the nonuniqueness of signs (taking an even or odd number) is a key issue that will arise and so we address it now.

Lemma 7.7. *Let $\underline{t} = (t_1, t_2, t_3)$ be a trace triple. Then 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

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

Moreover, 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. The first statement is clear.

If $\underline{t}$ is commutative, then $d(t_1, t_2, t_3) = 0$. 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 $d(t_1, t_2, t_3) - d(-t_1, t_2, t_3) = 2t_1t_2t_3 = 0$, as claimed. □

In particular, it follows from Lemma 7.7 that if $\underline{t}$ is commutative, and $t_1t_2t_3 \neq 0$, then $(-t_1, t_2, t_3)$ is projective.

A trace triple $\underline{t}$ is *irregular* if the subfield $\mathbb{F}_p(\underline{t}) = \mathbb{F}_p(t_1, t_2, t_3)$ is a quadratic extension of a subfield k with $[\mathbb{F}_p(\underline{t}) : k] = 2$ with the property that t_i belongs to k for some i whereas t_j for $j \neq i$ is either zero or a square root in $\mathbb{F}_p(\underline{t})$ of a nonsquare in k.

Proposition 7.8 ([31, 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) *The group G is conjugate to either $\mathrm{PSL}_2(k)$ or $\mathrm{PGL}_2(k_0)$, where $k = \mathbb{F}_p(t_1, t_2, t_3)$ and $[k : k_0] = 2$ (independent of $\underline{g}$); the latter can occur only if $\underline{t}$ is irregular.*
(b) *Suppose $k = \mathbb{F}_q$. Then the number of orbits of $\mathrm{Inn}(\mathrm{SL}_2(\mathbb{F}_q)) \cong \mathrm{PSL}_2(\mathbb{F}_q)$ on $T(\underline{t})$ is 2 or 1 according as p is odd or $p = 2$.*
(c) *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. 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 7.8(a), every projective triple is either of PSL_2-type or of PGL_2-type.

Using this lemma, we can prove the first part of Theorem A.

Proposition 7.9. *Let X be a curve of genus $g \geq 2$ and let $f : X \to \mathbb{P}^1$ be a G-Wolfart map with ramification indices (a, b, c). Let p be prime and let q be a power of p.*

Let r be the order of the Frobenius Frob_p in $\mathrm{Gal}(\mathbb{Q}(\lambda_{2a}, \lambda_{2b}, \lambda_{2c})_{p'}/\mathbb{Q})$. If $G \cong \mathrm{PGL}_2(\mathbb{F}_q)$, then $q = \sqrt{p^r}$; otherwise, if $G \cong \mathrm{PSL}_2(\mathbb{F}_q)$, then $q = p^r$.

Proof. By work in Section 2, there exists a finite index, normal subgroup $\Gamma \subseteq \overline{\Delta}(a, b, c)$ such that $\overline{\Delta}(a, b, c)/\Gamma \cong G \subset \mathrm{PSL}_2(\mathbb{F}_q)$ the map $X \to \mathbb{P}^1$ is the map $\Gamma\backslash\mathcal{H} \to \overline{\Delta}(a, b, c)\backslash\mathcal{H}$. In this way, we have identified the images in G of the monodromy at the three ramification points with the elements $\overline{\gamma}_a, \overline{\gamma}_b, \overline{\gamma}_c$. Thus, by hypothesis, the triple $(\overline{\gamma}_a\Gamma, \overline{\gamma}_b\Gamma, \overline{\gamma}_c\Gamma)$ in G generates G. This triple lifts to the triple $(-\gamma_a, \gamma_b, \gamma_c)$ 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 $\mathbb{Q}(\lambda_{2a}, \lambda_{2b}, \lambda_{2c})_{p'}$.

If $G \cong \mathrm{PSL}_2(\mathbb{F}_q)$, then Proposition 7.8(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 $\mathrm{Gal}(\mathbb{Q}(\lambda_{2a}, \lambda_{2b}, \lambda_{2c})_{p'}/\mathbb{Q})$, as claimed. If instead $G \cong \mathrm{PGL}_2(\mathbb{F}_{\sqrt{q}})$, then r is half of this degree. □

We now transfer these results to 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 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.

Lemma 7.10. *Every trace triple up to signs $\pm\underline{t}$ is either exceptional, commutative, or projective.*

Proof. This follows from Lemma 7.7. □

To a projective trace triple up to signs $\pm\underline{t}$, we associate the order triple (a, b, c) (assuming $a \leq b \leq c$) as the order triple associated to any lift $\underline{t}$ of $\pm\underline{t} = (\pm t_1, \pm t_2, \pm t_3)$.

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 7.11. *Let $\underline{C}$ be a triple of conjugacy classes in $\mathrm{PSL}_2(\mathbb{F}_q)$ with q odd. Let $\pm\underline{t}$ be the associated trace triple and (a, b, c) the associated order triple. Suppose that $\pm\underline{t}$ is projective and $\mathbb{F}_q = \mathbb{F}_p(\underline{t})$. Let $G = \pm\langle g_1, g_2, g_3\rangle \subseteq \mathrm{PSL}_2(\mathbb{F}_q)$.*

(a) *Suppose $a = 2$ and $p \mid abc$. Then $\underline{C}$ is rigid, i.e. $\#\Sigma(\underline{C})/\mathrm{Inn}(G) = 1$.*
(b) *Suppose $a = 2$ and $p \nmid abc$. If $\underline{t}$ is of PSL_2-type, then $\#\Sigma(\underline{C})/\mathrm{Inn}(G) = 2$ and $\underline{C}$ is weakly rigid, i.e. $\#\Sigma(\underline{C})/\mathrm{Aut}(G) = 1$. If $\underline{t}$ is of PGL_2-type, then $\underline{C}$ is rigid.*
(c) *Suppose $a \neq 2$ and $p \mid abc$. Then $\#\Sigma(\underline{C})/\mathrm{Inn}(G) = \#\Sigma(G)/\mathrm{Aut}(G) = 2$.*
(d) *Suppose $a \neq 2$ and $p \nmid abc$. If $\underline{t}$ is of PSL_2-type, then $\#\Sigma(\underline{C})/\mathrm{Inn}(G) = 4$ and $\#\Sigma(\underline{C})/\mathrm{Aut}(G) = 2$. If $\underline{t}$ is of PGL_2-type, then $\#\Sigma(\underline{C})/\mathrm{Inn}(G) = \#\Sigma(G)/\mathrm{Aut}(G) = 2$.*

If $p = 2$, then $\mathrm{PSL}_2(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)$ and by Proposition 7.8(b) $\underline{C}$ is rigid, i.e. $\#\Sigma(G)/\mathrm{Inn}(G) = 1$. So this proposition handles the general case.

Proof. Let $\underline{t} = (t_1, t_2, t_3) \in \mathbb{F}_q^3$ lift $\pm\underline{t}$. 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 $\mathrm{tr}(g_i) = \mathrm{tr}(g_i') = t_i$.

Suppose $a = 2$. Then $t_1 = \mathrm{tr}(g_1) = 0 = -\mathrm{tr}(g_1)$, 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 7.8(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.

Suppose $p \nmid abc$. If G is of PSL_2-type, then $G = \mathrm{PSL}_2(\mathbb{F}_q)$. By hypothesis, all conjugacy classes $C_i \in \underline{C}$ are semisimple and so are preserved under automorphism. From Proposition 7.8(b), we see that there are two orbits of $\mathrm{PSL}_2(\mathbb{F}_q)$ acting by conjugation on $\Sigma(\underline{C})$ and $\tau \in \mathrm{Out}(\mathrm{PSL}_2(\mathbb{F}_q))$ identifies these orbits: they are identifed by some element of $\mathrm{Out}(\mathrm{PSL}_2(\mathbb{F}_q))$ but since $\mathbb{F}_q = \mathbb{F}_p(\underline{t})$ the stabilizer of $\langle\sigma\rangle$ acting on $\underline{t}$ is trivial (see the analysis following (6.1)). If instead G is of PGL_2-type, then $G \cong \mathrm{PGL}_2(\mathbb{F}_{\sqrt{q}})$, then $\mathrm{Out}(\mathrm{PGL}_2(\mathbb{F}_{\sqrt{q}})) = \langle\sigma\rangle$ and since $\mathbb{F}_q = \mathbb{F}_p(\underline{t})$ the stabilizer of $\langle\sigma\rangle$ acting on $\underline{t}$ is again trivial, and hence the orbits must be already identified by conjugation in $\mathrm{PGL}_2(\mathbb{F}_q)$, so the triple is in fact rigid.

Similarly, if $p \mid abc$ then at least one conjugacy class is unipotent and so the two orbits of the set $T(\underline{t})$ under $\mathrm{Out}(\mathrm{PSL}_2(\mathbb{F}_q))$ correspond to two different conjugacy class triples—only one belongs to $\underline{C}$. Therefore the triple is in fact rigid.

Now suppose $a \neq 2$. There are 8 possible trace triples $\underline{t}$ lifting $\pm\underline{t}$, but by Lemma 7.7 it suffices to consider only $\underline{t} = (t_1, t_2, t_3)$ and $(-t_1, t_2, t_3)$. By Proposition 7.1, there exist a triple $\underline{g}$ with trace triple $\underline{t}$ and a triple $\underline{g}'$ with trace triple $\underline{t}'$ with $\pm\underline{g}, \pm\underline{g}' \in \Sigma(\underline{C})$, and up to conjugation in $\mathrm{SL}_2(\overline{\mathbb{F}_q})$ these are unique. (Up to conjugation in $\mathrm{PSL}_2(\mathbb{F}_q)$, there are four which are identified in pairs, as in the previous paragraph.) By hypothesis, each of these triples is projective. To finish the proof of the claim, we need to show that $\pm\underline{g}$ and $\pm\underline{g}'$ are not identified by an automorphism of $\mathrm{PSL}_2(\mathbb{F}_q)$ (the case of PGL_2-type is similar), and this follows from the fact that any automorphism of $\mathrm{PSL}_2(\mathbb{F}_q)$ lifts to an automorphism of $\mathrm{SL}_2(\mathbb{F}_q)$ which preserves traces. We have a similar breakdown as in the previous paragraph when $p \mid abc$ and one of the conjugacy classes is unipotent. □

We are now in a position to prove a statement which nearly completes Theorem A (in the next section, we will show that the corresponding field extension is unramified away p.)

Recall our notation: for the prime p and integers $a, b, c \in \mathbb{Z}_{\geq 2}$, let $F_p(a,b,c) = \mathbb{Q}(\lambda_a, \lambda_b, \lambda_c)_{p'}$ be the compositum of the fields $\mathbb{Q}(\lambda_s)$ (resp. $\mathbb{Q}(\zeta_s)$) with $s \in \{a, b, c\}$ prime to p.

Theorem 7.12. *Let X be a curve of genus $g \geq 2$ and let $f : X \to \mathbb{P}^1$ be a G-Wolfart map with ramification indices (a, b, c). Let p be prime and let q be a power of p.*

(a) *The field of moduli $M(X)$ is an extension of $F_p(a,b,c)^{\langle \mathrm{Frob}_p \rangle}$ of degree $d_X \leq 2$.*
(b) *If $p \mid abc$, pr is odd, and $G \cong \mathrm{PSL}_2(\mathbb{F}_q)$, then $M(X,G)$ is an extension of $F_p(a,b,c)(\sqrt{p^*})$ of degree $d_{(X,G)} \leq 2$; otherwise, $M(X,G)$ is an extension of $F_p(a,b,c)$ of degree $d_{(X,G)} \leq 2$.*

Finally, if $a = 2$ or q is even or $p \mid abc$, then $d_X = 1$; if q is even or $G \cong \mathrm{PGL}_2(\mathbb{F}_q)$, then $d_{(X,G)} = 1$.

Proof. Let $a, b, c \in \mathbb{Z}_{\geq 2}$, and let $X \to \mathbb{P}^1$ be a G-Wolfart map with ramification indices (a, b, c). As in the proof of Proposition 7.9, we may identify the images in G of the monodromy at the three ramification points with the elements $\overline{\gamma}_a, \overline{\gamma}_b, \overline{\gamma}_c \in \overline{\Delta}(a, b, c)$. Let $\underline{g} = (\overline{\gamma}_a\Gamma, \overline{\gamma}_b\Gamma, \overline{\gamma}_c\Gamma)$ and let $\underline{C}$ be the corresponding conjugacy class triple in G.

We refer to the discussion in Section 5, specifically Proposition 5.1, and recall the calculation of the field of weak rationality in Section 6 (Lemmas 6.2 and 6.4). By Proposition 7.11, we have $d_X = \#\Sigma(\underline{C})/\mathrm{Aut}(G) \leq 2$ and $d_{(X,G)} = \#\Sigma(\underline{C})/\mathrm{Inn}(G) \leq 4$; moreover, $d_X = 1$ when $t_1t_2t_3 = 0$, i.e., $a = 0$. □

Remark 7.13. We conclude with some comment on an extension of Proposition 7.11. We take nearly the same hypotheses. Suppose that $\underline{C}$ is a triple of conjugacy classes in $\mathrm{PSL}_2(\mathbb{F}_q)$ with q odd. Suppose that $\pm t$ is the associated trace triple and $\mathbb{F}_q = \mathbb{F}_p(\underline{t})$. Let $G = \pm\langle g_1, g_2, g_3\rangle \subseteq \mathrm{PSL}_2(\mathbb{F}_q)$.

Here, we do not insist that $\pm t$ is projective; only that there exists a lift $\underline{t}$ such that $\underline{t}$ is projective. As in the proof of this proposition, this allows the possibility that $\underline{t}' = (-t_1, t_2, t_3)$ is commutative (so $\pm t$ is "mixed commutative-projective"); necessarily, $t_1 \neq 0$. In this situation, in fact all $\underline{g}' \in \underline{t}'$ generate affine (or commutative) subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ since they are *singular* [31, Theorem 2]. Since these no longer contribute to the count of $\Sigma(\underline{C})$, all sets are halved.

8. Reflex field

In this section, we use the reflex field of the quaternionic Shimura variety introduced in Section 4 that gives rise to the construction of Wolfart curves to further control its field of moduli. We refer the reader to Milne [36] and Reimann [40] as references.

Let F be a totally real field of degree $n = [F : \mathbb{Q}]$ with ring of integer $\mathbb{Z}_F$. Let B be a quaternion algebra over F. Let $v_1, \ldots, v_n$ be the real places of F, abbreviating $x_i = v_i(x)$ for $x \in F$, and suppose that B is split at $v_1, \ldots, v_r$ with $r > 1$ and ramified at $v_{r+1}, \ldots, v_n$, i.e.

$$B \hookrightarrow B_\infty = B \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} \mathrm{M}_2(\mathbb{R})^r \times \mathbb{H}^{n-r}. \tag{8.1}$$

Let ι_i denote the ith projection $B \to \mathrm{M}_2(\mathbb{R})$ and $\iota = (\iota_1, \ldots, \iota_r)$. Let

$$F_+^\times = \{x \in F : x_i > 0 \text{ for all } i\}$$

be the group of totally positive elements of F and let $\mathbb{Z}_{F,+}^\times = \mathbb{Z}_F^\times \cap F_+^\times$.

Let $\mathcal{O} \subseteq B$ be an order. Let $\mathcal{H}^\pm = \mathbb{C} \setminus \mathbb{R}$ be the union of the upper and lower half-planes. Via the embeddings $v_1, \ldots, v_r$, corresponding to the first r factors in (8.1), the group $B_\infty^\times$ acts on $(\mathcal{H}^\pm)^r$ on the right transitively with the stabilizer of $(\sqrt{-1}, \ldots, \sqrt{-1}) \in \mathcal{H}^r$ being

$$K_\infty = (\mathbb{R}^\times \mathrm{SO}_2(\mathbb{R}))^r \times (\mathbb{H}^\times)^{n-r}.$$

Therefore we can identify

$$\begin{aligned} B_\infty^\times/K_\infty &\to (\mathcal{H}^\pm)^r \\ g &\mapsto z = g(\sqrt{-1}, \ldots, \sqrt{-1}). \end{aligned} \tag{8.2}$$

Let

$$\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \prod_p{}' \mathbb{Z}_p$$

(where $'$ denotes the restricted direct product) and let $\widehat{\ }$ denote tensor with $\widehat{\mathbb{Z}}$ over $\mathbb{Z}$. We define the *quaternionic Shimura variety* associated to $\mathcal{O} \subseteq B$ as the double coset

$$V(\mathbb{C}) = B^\times \backslash (B_\infty^\times / K_\infty \times \widehat{B}^\times / \widehat{\mathcal{O}}^\times) = B^\times \backslash ((\mathcal{H}^\pm)^r \times \widehat{B}^\times / \widehat{\mathcal{O}}^\times).$$

By Eichler's theorem of norms, we can identify

$$V(\mathbb{C}) = B_+^\times \backslash (\mathcal{H}^r \times \widehat{B}^\times / \widehat{\mathcal{O}}^\times)$$

where

$$B_+^\times = \{\gamma \in B : \mathrm{nrd}(\gamma) \in F_+^\times\}$$

is the subgroup of $B^\times$ whose elements have totally positive reduced norm. Now we have a natural (continuous) projection map

$$V(\mathfrak{N})(\mathbb{C}) \to B_+^\times \backslash \widehat{B}^\times / \widehat{\mathcal{O}}^\times$$

which via the reduced norm gives a bijection

$$\mathrm{nrd} : B_+^\times \backslash \widehat{B}^\times / \widehat{\mathcal{O}}^\times \to F_+^\times \backslash \widehat{F}^\times / \mathrm{nrd}(\widehat{\mathcal{O}}^\times) = C$$

by the theorem of strong approximation. The latter is a class group of F: if, for example, $\mathrm{nrd}(\widehat{\mathcal{O}}^\times) = \widehat{\mathbb{Z}}_F$, then it is canonically identified with $C \cong \mathrm{Cl}^+(\mathbb{Z}_F)$, the strict class group of $\mathbb{Z}_F$, i.e. the ray class group of $\mathbb{Z}_F$ with modulus equal to the product of all real (infinite) places of F.

Therefore, the space $X(\mathbb{C})$ is the disjoint union of connected Riemannian manifolds indexed by a class group C, which we identify explicitly as follows. Let the ideals $\mathfrak{a} \subseteq \mathbb{Z}_F$ form a set of representatives for C, and let $\widehat{a} = (a_v)_v \in \widehat{\mathbb{Z}}_F$ be such that $\widehat{a}\,\widehat{\mathbb{Z}}_F \cap \mathbb{Z}_F = \mathfrak{a}$. By the above bijection, there exists $\widehat{\alpha} \in \widehat{B}^\times$ such that $\mathrm{nrd}(\widehat{\alpha}) = \widehat{a}$. We let $\mathcal{O}_\mathfrak{a} = \widehat{\alpha}\widehat{\mathcal{O}}\widehat{\alpha}^{-1} \cap B$ so that $\mathcal{O}_{(1)} = \mathcal{O}$, and we put $\Gamma_\mathfrak{a}(1) = (\mathcal{O}_\mathfrak{a})_1^\times / \{\pm 1\} = (\widehat{\mathcal{O}}_\mathfrak{a}^\times \cap B_1^\times)/\{\pm 1\}$. Then we have

$$V(\mathbb{C}) = \bigsqcup_{[\mathfrak{a}] \in C} B_+^\times (\mathcal{H}^r \times \widehat{\alpha}\widehat{\mathcal{O}}^\times) \xrightarrow{\sim} \bigsqcup_{[\mathfrak{a}] \in C} \Gamma_\mathfrak{a} \backslash \mathcal{H}^r, \tag{8.3}$$

where the last identification is obtained via the bijection

$$\begin{aligned} B_+^\times \setminus (\mathcal{H}^r \times \widehat{\alpha}\widehat{\mathcal{O}}^\times) &\xrightarrow{\sim} \Gamma_\mathfrak{a} \backslash \mathcal{H}^r \\ B_+^\times (z, \widehat{\alpha}\widehat{\mathcal{O}}^\times) &\mapsto z \end{aligned} \tag{8.4}$$

In light of this setup, we reconsider the construction of the Wolfart curves given in Section 4, with $F = \mathbb{Q}(\mathrm{tr}\,\Delta) = \mathbb{Q}(\lambda_{2a}, \lambda_{2b}, \lambda_{2c})$ and $B = F[\Delta]$. We worked with the order $\mathbb{Z}_F[\Delta]$, but it is more convenient here to work with a maximal order $\mathcal{O}(1) \supseteq \mathcal{O}$—the two orders are isomorphic locally at all primes $\mathfrak{P} \nmid \beta$, and we work with these primes. The uniformizing subgroups arose from pullback as in the

following diagram:

$$\begin{array}{ccc} \overline{\Delta}(\mathfrak{N}) = \overline{\Delta} \cap \mathcal{O}(\mathfrak{N})^\times & \hookrightarrow & \mathcal{O}(\mathfrak{N})_1^\times/\{\pm 1\} \\ \downarrow & & \downarrow \\ \overline{\Delta} & \hookrightarrow & \mathcal{O}(1)_1^\times/\{\pm 1\}. \end{array}$$

Embed $\Gamma(1) \hookrightarrow \mathrm{PSL}_2(\mathbb{R})^r$ by the split places $v_1, \dots, v_r$ and similarly with $\Gamma(\mathfrak{N})$; embed $\overline{\Delta} \hookrightarrow \mathrm{PSL}_2(\mathbb{R})$ by (1.8). Then we have a diagram

$$\begin{array}{ccc} X(\mathfrak{N})(\mathbb{C}) = \overline{\Delta}(\mathfrak{N})\backslash\mathcal{H} & \hookrightarrow & \Gamma(\mathfrak{N})\backslash\mathcal{H}^r \\ \downarrow & & \downarrow \\ X(\mathbb{C}) = \overline{\Delta}\backslash\mathcal{H} & \hookrightarrow & \Gamma(1)\backslash\mathcal{H}^r. \end{array} \tag{8.5}$$

via the quotient of the diagonal map $\mathcal{H} \hookrightarrow \mathcal{H}^r$.

Remark 8.6. The number of split real places r is equal to the number of real embeddings v of F such that

$$v(\lambda_{2a}^2 + \lambda_{2b}^2 + \lambda_{2c}^2 + 2\lambda_{2a}\lambda_{2b}\lambda_{2c} - 1) < 0$$

given by Takeuchi [59, Theorem 1(ii)] in his characterization of arithmetic triangle groups: indeed, the triangle group $\overline{\Delta}(a, b, c)$ is arithmetic if and only if $r = 1$.

From the above, it is more natural to embed not just in one Riemann surface but the complete disjoint union. This can be achieved as follows.

Lemma 8.7. *For all $[\mathfrak{a}] \in \mathrm{Cl}^+(\mathbb{Z}_F)$, there exists an embedding $\overline{\Delta} \hookrightarrow (\mathcal{O}_\mathfrak{a})_1^\times$.*

Proof. Let $\mathcal{O}' = \mathcal{O}_\mathfrak{a}$. We have an embedding $\mathbb{Z}_F[\zeta_{2a}] \hookrightarrow \mathcal{O}$ by $\zeta_{2a} \mapsto \gamma_a$. Since B is indefinite, we also have an embedding $\mathbb{Z}_F[\zeta_{2a}] \hookrightarrow \mathcal{O}_\mathfrak{a}$; let γ_a' be the image. By the Noether-Skolem theorem, there exists $\nu \in B^\times$ such that $\nu\gamma_a\nu^{-1} = \gamma_a'$, and ν is unique up to $K^\times = F(\zeta_{2a})^\times$. Let $\gamma_b' = \nu\gamma_b\nu^{-1}$. We claim there exists $\mu \in K^\times$ such that $\mu\gamma_b'\mu^{-1} \in \mathcal{O}'$. Indeed, let $\mu_0 \in B^\times$ be any element such that $\mu\gamma_b'\mu^{-1} \in \mathcal{O}'$; then $(\mathcal{O}')^\times\mu_0 F(\gamma_b')^\times = B^\times \supset K^\times \ni \mu$. Then the elements $\mu\gamma_a'\mu^{-1}$ and $\mu\gamma_b'\mu^{-1}$ yield the desired embedding of $\overline{\Delta}$. □

With this lemma in hand, we can extend (8.5) as follows:

$$\begin{array}{ccc} \bigsqcup X(\mathfrak{N})(\mathbb{C}) = \bigsqcup_{[\mathfrak{a}] \in \mathrm{Cl}^+_\mathfrak{N}(\mathbb{Z}_F)/\mathrm{Cl}^+(\mathbb{Z}_F)} \overline{\Delta}(\mathfrak{N})\backslash\mathcal{H} & \hookrightarrow & V(\mathfrak{N})(\mathbb{C}) = \bigsqcup_{[\mathfrak{a}] \in \mathrm{Cl}^+_\mathfrak{N}(\mathbb{Z}_F)} \Gamma_\mathfrak{a}(\mathfrak{N})\backslash\mathcal{H}^r \\ \downarrow & & \downarrow \\ X(\mathbb{C}) = \overline{\Delta}\backslash\mathcal{H} & \hookrightarrow & V(1)(\mathbb{C}) = \bigsqcup_{[\mathfrak{a}] \in \mathrm{Cl}^+(\mathbb{Z}_F)} \Gamma_\mathfrak{a}(1)\backslash\mathcal{H}^r. \end{array} \tag{8.8}$$

In the second row of this diagram, we have identified the class group with $\mathrm{Cl}^+(\mathbb{Z}_F)$; in the first row, in the reduced norm we have only those elements which are congruent to 1 modulo $\mathfrak{N}$, so we instead get the (strict) ray class group with modulus equal to $\mathfrak{N}$ times the product of the real places of F.

From the theory of canonical models of Shimura [50, 51] and Deligne [15] (see also Milne [36]), the disjoint unions $V(1)(\mathbb{C})$ and $V(\mathfrak{N})(\mathbb{C})$ have a canonical model $V(1)$ defined over the reflex field E of F, which is the field

$$E = \mathbb{Q}(\sum_{i=1}^{r} v_i(x))_{x \in F}.$$

Equivalently, since F is Galois over $\mathbb{Q}$, we have $E = F^H$ where $H \subset \mathrm{Gal}(F/\mathbb{Q})$ is the set of σ such that $\{\sigma v_1, \ldots, \sigma v_r\} = \{v_1, \ldots, v_r\}$. In any case, since F is Galois over $\mathbb{Q}$, the reflex field E is a subfield of F. The action of the Galois group on the connected components is given by a reciprocity homomorphism

$$\mathrm{Gal}(\overline{\mathbb{Q}}/E) \to C \cong \mathrm{Cl}^+(\mathbb{Z}_F).$$

The canonical model $V(1)$ is obtained by an analysis of the field of definition of the reciprocity law on the special points in $V(1)$. Since the Galois action pulls back to $X(\mathbb{C})$ compatibly, and $X(\mathbb{C})$ itself has a model X over E (it is isomorphic to $\mathbb{P}^1$ over $\mathbb{C}$), it follows that the embedding $X \hookrightarrow V(1)$ is defined over E.

This same theory of canonical models shows that $V(\mathfrak{N})$ is defined over E. Since $\bigsqcup X(\mathfrak{N})(\mathbb{C})$ is obtained via pullback, it is also defined over E.

The field of moduli of an individual component of $V(\mathfrak{N})(\mathbb{C})$ will tell us the field of moduli of $X(\mathfrak{N})(\mathbb{C})$. For this, we need to understand the reciprocity map

$$\mathrm{Gal}(\overline{\mathbb{Q}}/E) \to \mathrm{Cl}^+_{\mathfrak{N}}(\mathbb{Z}_F).$$

We use only the fact that if one base extends the above diagram (8.8) to F (here we use that F is Galois, so $E \subseteq F$), then this "generalized" reciprocity map is just a quotient of the usual reciprocity map (Artin map), and consequently its kernel is contained in the ray class field associated to $\mathrm{Cl}^+_{\mathfrak{N}}(\mathbb{Z}_F)$ which is ramified only at primes dividing the norm of $\mathfrak{N}$; since $E \subseteq F$ we can take a field of definition of $X(\mathfrak{N})$ to be such an extension of F. This completes the proof of Theorem A.

Remark 8.9. In fact, we have the necessary elements to squeeze more out of the reciprocity map, namely CM (special) points: the fixed points of $\gamma_a, \gamma_b, \gamma_c$! Using these, one could obtain more information about the field of moduli.

9. Fields of definition

In this section, we prove Theorems B and C.

We begin with Theorem B, which we restate as the following theorem. We recall that $\pm\underline{t}$ is not exceptional if it is not one in the list (7.4).

Theorem 9.1. *Let (a, b, c) be a hyperbolic triple with $a, b \in \mathbb{Z}_{\geq 2}$ and $c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$. Suppose that (a, b, c) is not exceptional nor of the form $(mk, m(k+1), mk(k+1))$ with $m, k \in \mathbb{Z}_{\geq 1}$. Let $\mathfrak{p}$ be a prime of $E(a, b, c)$ above the rational prime $p \nmid abc$.*

Then there exists a G-Wolfart map

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

with ramification indices (a,b,c) *or* (a,b,p) *according as* $c \in \mathbb{Z}$ *or* $c = \infty$*, 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, so that $a,b,c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$ satisfy $a \leq b \leq c$ and $\chi(a,b,c) = 1/a + 1/b + 1/c - 1 < 0$. Let $\mathfrak{p}$ be a prime of the field

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

and let $\mathfrak{P}$ be a prime of

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

above $\mathfrak{p}$ above the rational prime $p \nmid abc$.

Then by Proposition 4.21, we have a homomorphism

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

with $\operatorname{tr} \phi(\overline{\gamma}_s) \equiv \pm\lambda_{2s} \pmod{\mathfrak{P}}$ for $s = a,b,c$ whose image lies in the subgroup $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{P}) \cap \mathrm{PGL}_2(\mathbb{F}_\mathfrak{p})$. We note that $[\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}] \leq 2$ and that this intersection is given by

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

We note from (4.9) that $\mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{p}$ if at least two of a,b,c are odd.

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

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

The Riemann surface $X = X(a,b,c;\mathfrak{p}) = \overline{\Delta}(a,b,c;\mathfrak{p})\backslash\mathcal{H}$ is a Wolfart curve by construction, with quotient $\overline{\Delta}(a,b,c;\mathfrak{p})\backslash\mathcal{H} \to \overline{\Delta}(a,b,c)\backslash\mathcal{H}$.

We now show that the triple $\pm\underline{t}$ is not commutative. From (7.2), 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 β is the reduced discriminant of the order $\mathcal{O}$ arising in Section 4! And as in the proof of Lemma 4.5, 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 $\beta \not\equiv 0 \pmod{\mathfrak{P}}$.

By Proposition 7.5, we conclude that the triple $\underline{g}$ is projective. Then, by Proposition 7.8(a), we have that the image of ϕ is equal to $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{P})$ or $\mathrm{PGL}_2(k)$ where $[\mathbb{F}_\mathfrak{P} : k] = 2$. If $[\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}] = 2$ then by (9.2) we have already that the image is contained in $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{p})$ so we have the second case with $k = \mathbb{F}_\mathfrak{p}$. If $\mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{p}$, i.e.

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

we must rule out the possibility that the image is of PGL_2-type. 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 the extension $[\mathbb{F}_\mathfrak{p} : \mathbb{F}_p(\underline{t}^2)] \leq 2$ so we must have $k = \mathbb{F}_p(\underline{t}^2)$. 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 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*

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

We conclude with a discussion of the natural extension to composite $\mathfrak{N}$. Let $\mathfrak{N}$ be an ideal of $\mathbb{Z}_F$ coprime to $2abc$. Let $\mathfrak{n} = \mathfrak{N} \cap \mathbb{Z}_E$. Then by Proposition 4.21, we have a homomorphism

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

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

$$\widehat{\phi} : \overline{\Delta} \to \prod_{\mathfrak{P} \nmid 2abc} \mathrm{PSL}_2(\mathbb{Z}_{F,\mathfrak{P}}).$$

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 $\prod_{\mathfrak{P} \nmid 2abc} \mathrm{PSL}_2(\mathbb{Z}_{F,\mathfrak{P}})$.

Proposition 9.4. *The image of $\widehat{\phi}$ is a dense subgroup of $\widehat{P}$.*

We will use the following lemma in the proof.

Lemma 9.5. *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 $\operatorname{char} R/\mathfrak{p} \geq 5$, then $H = P(\mathbb{Z}_{F,\mathfrak{p}})$.*

Proof. Serre [45, 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 arbitrary number rings $\mathbb{Z}_F$.

For the case $P = \mathrm{PGL}_2$, 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

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

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

We sketch an alternative proof as follows. One proves the statement by induction; we have an exact sequence

$$1 \to M_2(k) \to \mathrm{GL}_2(R/\mathfrak{p}^e) \to \mathrm{GL}_2(R/\mathfrak{p}^{e-1}) \to 1$$

via the isomorphism $1+M_2(\mathfrak{p}^{e-1}/\mathfrak{p}^e) \cong M_2(\mathfrak{p}^{e-1}/\mathfrak{p}^e) \cong M_2(k)$. The group $\mathrm{GL}_2(R/\mathfrak{p}^{e-1})$ acts by conjugation $M_2(k)$ and factors through $\mathrm{GL}_2(k)$. Since $\mathrm{char}\, k$ 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 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 $e = 2$ [45, Exercise 1, p. IV-27]). □

Proof of Proposition 9.4. We show that $\phi_{\mathfrak{N}}$ has image $P(\mathfrak{N})$. By Proposition 9.1, this statement is true if $\mathfrak{N}$ is prime. The fact that the image of $\phi_{\mathfrak{N}}$ is equal to $P(\mathfrak{N})$ when $\mathfrak{N} = \mathfrak{P}^e$ is a prime power follows from Lemma 9.5.

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

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

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 $\mathcal{O}_1^\times/\mathcal{O}(\mathfrak{N})_1^\times \cong \mathrm{PSL}_2(\mathbb{Z}_F/\mathfrak{N})$. 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 is equal to $P(\mathfrak{M}) \times P(\mathfrak{N}) \cong P(\mathfrak{M}\mathfrak{N})$, and the result follows. □

10. Examples

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

Example 10.1. The well-known statements about modular curves can be recovered from our theorem. We take $(a, b, c) = (2, 3, \infty)$ since $\mathrm{SL}_2(\mathbb{Z}) \cong \Delta(2, 3, \infty)$. 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. It is obvious here that 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 $F = F(a,b,c) = \mathbb{Q}(\lambda_4, \lambda_6, \lambda_\infty) = \mathbb{Q} = E = F_0$. The statement of Theorem A says that $M(X(p)) = \mathbb{Q}$ since $a = 2$ and $M(X(p), G) = \mathbb{Q}(\sqrt{p^*})$ since $c = p$. This recovers the result of Mazur and Shih.

Example 10.2. Consider the special case $(a,b,c) = (2,3,p)$ with $p \geq 7$ prime. We want to consider the case where q is a power of p; for this, we will need the extension of Theorem B given in 4.22. We compute $F = F(\lambda_4, \lambda_6, \lambda_{2p}) = F(\lambda_{2p}) = E$ and 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 $X(2,3,p;\mathfrak{p}) \to X(2,3,p) \cong \mathbb{P}^1$.

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 $F_{\mathrm{wkrat}}(\underline{C}) = \mathbb{Q}$.

In fact, the classical modular cover $j : X(p) \to X(1)$ is also a $\mathrm{PSL}_2(\mathbb{F}_p)$-Wolfart map, with the three ramification points being $0, 1728, \infty$, and so it follows that $X(2,3,p;p) \cong X(p)$ over $\overline{\mathbb{Q}}$. In particular, it follows from the above analysis that $\mathrm{PSL}_2(\mathbb{F}_p)$ is the full automorphism group of $X(p)$ [35] and that the minimal field of definition of $(X(p), \mathrm{Aut}(X(p)))$ is $\mathbb{Q}(\sqrt{p^*})$. In particular, we note that this interpretation is quite different than the moduli interpretation of "naïve" level p-structure [26] for $X(p)$ which gives a model of $\mathbb{Q}(\zeta_p)$. Indeed, this model is used by Shih [48] to show that $\mathrm{PSL}_2(\mathbb{F}_p)$ occurs regularly as a Galois group over K.

We could equally well consider the covers $X = X(2,3,p;2) \to X(2,3,p)$ (warning, the notation p is overloaded), 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: in the notation of Section 4, this means simply that the quaternion algebra A over E is split at exactly one real place of E—it follows that the triangle group $\Delta(a,b,c)$ is commensurable with the unit group of a maximal order in A. The arithmetic triples were classified by Takeuchi in a sequence of papers [57, 58, 59, 60]: there are 85 triples (a,b,c) and 26 maximal triples which fall into 19 commensurability classes.

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

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

In view of the previous example, it suffices to consider only those with $a, b, c \in \mathbb{Z}$.

The minimal field of definition of these curves was studied by Elkies [19, §5.3] and later by the second author [63, 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 $\mathrm{Gal}(E/\mathbb{Q})$.

This argument can be made directly using the language of canonical models of Shimura curves: this has the advantage that it applies in other circumstances as well (see e.g. Hallouin [23, 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 data 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 $E = F$. 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 $B^\sigma \cong B$, 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 data 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 it is an elementary theorem in hyperbolic geometry that 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 $\mathcal{O}(N)$ where $N \in \mathbb{Z}_{>0}$.

Many of these triples will occur in specific examples below.

Example 10.4. Consider the case of (odd) Hecke triangle groups treated by Lang, Lim, and Tan [28], the groups with $\overline{\Delta}(a,b,c) = \overline{\Delta}(2,q,\infty)$ with q odd. Then we have

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

since q is odd. It follows from our analysis that $\mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{p}$, so for all primes $\mathfrak{p}$ of $\mathbb{Q}(\lambda_q)$ we have $\overline{\Delta}/\overline{\Delta}(\mathfrak{p}) \cong \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$. 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 $\mathrm{Gal}(\mathbb{Q}(\lambda_q)/\mathbb{Q})$.

In their Main Theorem, part (iii), they 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 by elementary considerations: 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 then that $\mathbb{F}_p(t) = \mathbb{F}_p(t^2)$.

To give further examples, we list all G-Wolfart curves with $a, b, c \neq \infty$ up to 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 2.7) 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). The curves of genus $g \leq 24$ are listed in Table 10.5. For clarity, we use the group theorist's notation $\mathrm{P^*L}_2(q) = \mathrm{P^*L}_2(\mathbb{F}_q)$. 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 $X(a, b, c; \mathfrak{p})$.

Remark 10.6. It is remarkable that the curves $X_0(a, b, c; \mathfrak{p})$ have such low genus even as the curves $X(a, b, c; \mathfrak{p})$ grow in genus! A simple-minded application of the Riemann-Hurwitz theorem does not immediately give the result that there are only finitely many of bounded genus. If this is true, one instead will have to understand the cycle decomposition of the corresponding elements $g_a, g_b, g_c \in \mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$.

We now discuss each of these curves in turn. We note first that all curves but the last two (of genus 24) are arithmetic. Our computations are performed in Magma [7].

We are grateful to Elkies for allowing us to record several computations and other remarks in these examples.

Genus 3, $(2, 3, 7)$*,* $\mathrm{PSL}_2(7)$*.* 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 [18]. The map $f : X_0(2, 3, 7; 7) \cong \mathbb{P}^1 \to X(2, 3, 7) = \mathbb{P}^1$ is given by the rational function

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

This verifies in Theorem A that the curve is defined over $\mathbb{Q}$ (since $a = 2$) and its automorphism group is defined over $\mathbb{Q}(\sqrt{-7})$.

Genus 3, $(3, 4, 4)$*,* $\mathrm{PGL}_2(3)$*.* The triple $(3, 4, 4)$ is exceptional, and so has been excluded from our analysis. But since $\mathrm{PGL}_2(\mathbb{F}_3) \cong S_4$ 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 $N(\mathcal{O})/\mathbb{Q}^\times$ 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 a maximal order has signature $(0; 2, 2, 3, 3)$. See work of Baba and Granath [2] as well as Elkies [19, §3.1] for a detailed discussion of these triangle groups and their relationships.

Theorem B does not apply nor does Remark 4.22 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

g	(a,b,c)	G	arithmetic?	g_0
3	$(2,3,7)$	$\mathrm{PSL}_2(7)$	T	0
3	$(3,4,4)$	$\mathrm{PGL}_2(3)$	T	1
4	$(2,4,5)$	$\mathrm{PGL}_2(5)$	T	0
4	$(2,5,5)$	$\mathrm{PGL}_2(4)$	T	1
4	$(2,5,5)$	$\mathrm{PSL}_2(5)$	T	0
5	$(3,3,5)$	$\mathrm{PGL}_2(4)$	T	0
5	$(3,3,5)$	$\mathrm{PSL}_2(5)$	T	1
6	$(2,4,6)$	$\mathrm{PGL}_2(5)$	T	0
7	$(2,3,7)$	$\mathrm{PGL}_2(8)$	T	0
8	$(2,3,8)$	$\mathrm{PGL}_2(7)$	T	0
8	$(3,3,4)$	$\mathrm{PSL}_2(7)$	T	0
9	$(2,5,6)$	$\mathrm{PGL}_2(5)$	T	1
9	$(3,5,5)$	$\mathrm{PGL}_2(4)$	T	1
9	$(3,5,5)$	$\mathrm{PSL}_2(5)$	T	1
10	$(2,4,5)$	$\mathrm{PSL}_2(9)$	T	0
10	$(2,4,7)$	$\mathrm{PSL}_2(7)$	T	1
11	$(2,6,6)$	$\mathrm{PGL}_2(5)$	T	1
11	$(3,4,4)$	$\mathrm{PGL}_2(5)$	T	0
13	$(5,5,5)$	$\mathrm{PGL}_2(4)$	T	2
13	$(5,5,5)$	$\mathrm{PSL}_2(5)$	T	1
14	$(2,3,7)$	$\mathrm{PSL}_2(13)$	T	0
15	$(2,3,9)$	$\mathrm{PGL}_2(8)$	T	1
15	$(2,4,6)$	$\mathrm{PGL}_2(7)$	T	0
15	$(3,4,4)$	$\mathrm{PSL}_2(7)$	T	1
16	$(2,3,8)$	$\mathrm{PGL}_2(9)$	T	0
16	$(3,3,4)$	$\mathrm{PSL}_2(9)$	T	0
16	$(3,4,6)$	$\mathrm{PGL}_2(5)$	T	1
17	$(3,3,7)$	$\mathrm{PSL}_2(7)$	T	0
19	$(2,7,7)$	$\mathrm{PSL}_2(7)$	T	0
19	$(2,5,5)$	$\mathrm{PSL}_2(9)$	T	1
19	$(4,4,5)$	$\mathrm{PGL}_2(5)$	T	0
21	$(3,6,6)$	$\mathrm{PGL}_2(5)$	T	2
22	$(2,4,8)$	$\mathrm{PGL}_2(7)$	T	1
22	$(4,4,4)$	$\mathrm{PSL}_2(7)$	T	2
24	$(3,4,7)$	$\mathrm{PSL}_2(7)$	F	1
24	$(4,5,6)$	$\mathrm{PGL}_2(5)$	F	1

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

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

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

Choosing a factor $\mathbb{Z}/3\mathbb{Z}$ gives a cover $X(3,4,4;3) \to X(\Lambda)$ of degree 12, and choosing a factor stable under the Atkin-Lehner involution (which normalizes Λ) we find the cover $f : X(3,4,4;3) \to X(3,4,4)$ 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 (with its automorphism group) is defined over $\mathbb{Q}$.

Wolfart [67, §6.3] identifies the curve $X(3,4,4;3)$ 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. 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

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

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 our construction. 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, $(2,4,5)$, $\mathrm{PGL}_2(5)$*;* $(2,5,5)$, $\mathrm{PGL}_2(4) = \mathrm{PSL}_2(5)$. 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 $\mathrm{PGL}_2(\mathbb{F}_4) = \mathrm{PSL}_2(\mathbb{F}_4) \cong \mathrm{PSL}_2(FF_5)$, 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 ($\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$; note $\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$).

The curve is the Bring curve (see Wolfart [67, §6.4] and also Edge [16]), 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, $(3,3,5)$*,* $\mathrm{PGL}_2(4) = \mathrm{PSL}_2(5)$. 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 the triangle group $\overline{\Delta}(2,3,10)$—the composite gives a G-Wolfart map, but $G \ncong \mathrm{PGL}_2(\mathbb{F}_5)$, since there is no element of order 10 in this group!)

As usual, 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

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

Elkies pointed out to us that this curve should be given by a hyperelliptic cover whose hyperelliptic branch points are the 12 vertices of an icosahedron inscribed in the Riemann sphere, in analogy to the $(3,4,4;3)$ case, such as

$$C : y^2 = x^{11} - 11x^6 - x.$$

However, the automorphism group of C is minimally defined over $\mathbb{Q}(\zeta_5)$; therefore, if this is correct, the curve C is a twist of $X(3,3,5;5)$ over $\mathbb{Q}(\zeta_5)$.

Genus 6, (2,4,6), $\mathrm{PGL}_2(5)$. 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 $X(2,4,6;5)$ 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 $G \cong \mathrm{PGL}_2(\mathbb{F}_5)$ 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 [19]:

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

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, $(2,3,7)$*,* $\mathrm{PGL}_2(8)(= \mathrm{SL}_2(8))$. The curve $X = X(2,3,7;2)$ is the Fricke-Macbeath curve [30] of genus 7, the second smallest genus for 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 [5] show that the Jacobian J of X is isogenous to E^7, where E is a non-CM elliptic curve with rational j-invariant. (See also Wolfart [67, §6.5] and Wohlfahrt [65].)

Genus 8, $(2, 3, 8)$*,* $\mathrm{PGL}_2(7)$*.*

Genus 8, $(3, 3, 4)$*,* $\mathrm{PSL}_2(7)$. 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

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

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

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

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 $\mathbb{Q}(\sqrt{2})$. Such a field will have to be ramified only at 7 and so

$$M(X, G) \subset \mathbb{Q}(\sqrt{2})\left(\sqrt{-7}, \sqrt{2\sqrt{2} - 1}\right).$$

Genus 9, $(2, 5, 6)$*,* $\mathrm{PGL}_2(5)$*;* $(3, 5, 5)$*,* $\mathrm{PGL}_2(4) = \mathrm{PSL}_2(5)$. The triangle group $\overline{\Delta}(2, 5, 6)$ is maximal and contains $\overline{\Delta}(3, 5, 5)$ with index 2. The triple $(3, 5, 5)$ is exceptional, so it falls out of the purview of our theorems—nevertheless, it arises as a subcover of the nonexceptional triple $(2, 5, 6)$, so we can describe this triple instead.

Applying Theorem A, we have $a = 2$ and $p \mid abc$ (and $G \cong \mathrm{PGL}_2(\mathbb{F}_5)$!) so we have $M(X) = \mathbb{Q}(\lambda_2, \lambda_6)^{\langle \mathrm{Frob}_5 \rangle} = \mathbb{Q}$ and $M(X, G) = \mathbb{Q}(\sqrt{5})$.

Elkies suggests two candidates for this curve: start with the Bring equation and replace the sum of cubes with a sum of fourth powers; or consider the hyperelliptic curve

$$y^2 = x^{20} + 228x^{15} + 494x^{10} - 228x^5 + 1$$

with 20 branch points at the vertices of a regular dodecahedron. The former curve is not hyperelliptic, so these curves are not isomorphic.

Genus 10, $(2,4,5)$, $\mathrm{PSL}_2(9)$. Elkies suggests the first invariant polynomial of the complex reflection group $3A_6$ (also known as the *Valentiner group*).

Genus 10, (2,4,7), $\mathrm{PSL}_2(7)$. Elkies suggests the Hessian of the Klein quartic

$$x^5y + y^5z + z^5x - 5(xyz)^2.$$

Genus 11, $(2,6,6)$, $\mathrm{PGL}_2(5)$*; (3,4,4),* $\mathrm{PGL}_2(5)$. See also the genus 6 $(2,4,6)$ $\mathrm{PGL}_2(\mathbb{F}_5)$-cover. This cover arises from the usual (Shimura curve) congruence subgroup $X(5) \to X(1)$ by further quotient by Atkin-Lehner involutions, extending the $\mathrm{PSL}_2(\mathbb{F}_5)$-cover.

Genus 13, $(5,5,5)$, $\mathrm{PGL}_2(4) = \mathrm{PSL}_2(5)$. The triple $(5,5,5)$ is exceptional.

Genus 14, $(2,3,7)$, $\mathrm{PSL}_2(13)$. 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 [37] (and work in progress by Streit; methods of Streit [54] apply in general). The curve is defined over $\mathbb{Q}(\lambda_7)$ and its automorphism group is defined over an at most quadratic extension of $\mathbb{Q}(\lambda_7)$ ramified only at 13.

Genus 15, $(2,3,9)$, $\mathrm{PGL}_2(8)(= \mathrm{SL}_2(8))$. Elkies [17, §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 15, $(2,4,6)$, $\mathrm{PGL}_2(7)$*;* $(3,4,4)$, $\mathrm{PSL}_2(7)$. No comment.

Genus 16, $(2,3,8)$, $\mathrm{PGL}_2(9)$*;* $(3,3,4)$, $\mathrm{PSL}_2(9)$. No comment.

Genus 16, $(3,4,6)$, $\mathrm{PGL}_2(5)$. 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 $G \cong \mathrm{PGL}_2(\mathbb{F}_5)$, we have that $d_{(X,G)} = 1$ so $M(X,G) = M(X)$.

This example is also unusual 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. (Is it possible that this action is trivial?) In any case, 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 over $E = \mathbb{Q}(\sqrt{6})$.

The genus 1 curve $X = X_0(3,4,6;5)$ can be computed as follows. The ramification data above the designated points $0, 1, \infty$ is $3^2, 4\,1^2, 6$. We take the point above ∞ to be the origin of the group law on X and take the point $(0,1)$ to be the ramification point of order 4. The curve X 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 $a_0, \ldots, \lambda_2$ and find a unique solution defined over $E = \mathbb{Q}(\sqrt{6})$: after simplifying, the elliptic curve X has minimal model

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

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 $0, 50000, \infty$.

This confirms that $M(X)$ is contained in the ray class field of E of conductor 5, as predicted by Theorem A–in fact, it is already contained in E.

Genus 17, $(3,3,7)$, $\mathrm{PSL}_2(7)$. We refer back to Example 7.6. The corresponding projective trace triple is a "mixed commutative-projective" triple, so should have some extra descent.

Genus 19, $(2,7,7)$, $\mathrm{PSL}_2(7)$. No comment.

Genus 19, $(2,5,5)$, $\mathrm{PSL}_2(9)$; $(4,4,5)$, $\mathrm{PGL}_2(5)$. The maximal triangle group $\overline{\Delta}(2,4,5)$ contains $\overline{\Delta}(2,5,5)$ with index 2 and $\overline{\Delta}(4,4,5)$ with index 6. The quaternion algebra A is defined over $E = \mathbb{Q}(\sqrt{5})$ and is ramified at (2); the group associated to units in the maximal order is $\overline{\Delta}(2,5,5)$, and the quotient by the Atkin-Lehner involution is $\Delta(2,4,5)$. The cover $X(2,5,5;9)$ is thus obtained by the usual congruence subgroup of level (3).

Interestingly, the extension of this cover is a group containing $\mathrm{PSL}_2(\mathbb{F}_9)$ with index 2 which appears to contain $\mathrm{PGL}_2(\mathbb{F}_5)$ as a subgroup! (Maybe this group is $\mathrm{SL}_2(\mathbb{F}_9)$?) Consequently the curve $X(4,4,5;5)$ appears in between.

Genus 21, $(3,6,6)$, $\mathrm{PGL}_2(5)$. No comment.

Genus 22, $(2,4,8)$, $\mathrm{PGL}_2(7)$; $(4,4,4)$, $\mathrm{PSL}_2(7)$. No comment.

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

Elkies has computed 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 Belyi 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 $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2$ 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, $(3,4,7)$*,* $\mathrm{PSL}_2(7)$. 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 $\mathbb{Q}$ contained in the ray class field of E of conductor 7; the curve with its automorphism group is defined over $M(X)(\sqrt{-7})$.

Elkies has computed the curve $X_0(3,4,7;7)$; it is a genus 1 curve. His methods "turning a p-adic crank", which we explain in detail in the final example. He finds that the curve is defined only over $\mathbb{Q}(\sqrt{2}, \sqrt{-7})$, and already the j-invariant of the curve

$$\frac{1}{107495424}(-28505956008\sqrt{2}\sqrt{-7} + 39863931701\sqrt{-7} + 120291604664\sqrt{2} + 15630829689)$$

generates this field. This suggests that $M(X) = \mathbb{Q}(\sqrt{2})$ and $M(X,G) = \mathbb{Q}(\sqrt{2}, \sqrt{-7})$ and the subgroup of upper-triangular matrices, which gives rise to the curve $X_0(3,4,7;7)$, is not stable under $\sigma : \sqrt{-7} \mapsto -\sqrt{-7}$. Elkies also observes that 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. (He also computes that the action of $G = \mathrm{PSL}_2(\mathbb{F}_7)$ on the Jacobian of this $X(3,4,7)$ should contain the Jacobian of the Klein curve as a G-isogeny factor.)

We include one other example which extends beyond our table but illustrates an important final 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- or PGL_2-covers such that $a \neq 2$, $p \nmid abc$, and G is not obtained from PGL_2 or its quotient. 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

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

and so $M(X)$ is a degree at most 2 extension of $\mathbb{Q}(\lambda_5)$ which is contained in the ray class field 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 conductor 11∞. More precisely, from Section 8, for a choice of prime $\mathfrak{p}$ in $E(3,5,6)$ of norm 11 (of which there are two, it is contained in the ray class extension of $E(3,5,6)$ of conductor $\mathfrak{p}\infty$, where ∞ is the product of all 4 real places. The field $M(X,G)$ is a degree at most 2 extension of $M(X)$ contained in the same field.

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 $11 = \#\,\mathrm{PSL}_2(\mathbb{F}_{11})/\#A_5 = 660/60$.

We compute that the ramification type is $3^3\ 1^2, 5^2\ 1, 6\ 3\ 2$, and we place these above $0, 1, \infty$, respectively. We choose the point of ramification degree 6 above ∞ to be the origin of the group law on E. We label the other points above ∞ as $(0,1)$ and $(1,\gamma)$ with ramification indices 3 and 2, respectively. Thus we have an equation

$$y^2 = \delta x^3 + \lambda x^2 + (\gamma^2 - \lambda - \delta - 1)x + 1 = f(x)$$

The Belyi function ϕ has the form

$$\phi(x,y) = \frac{a(x) + b(x)y}{(x-1)^2x^3}$$

where $a(x) = a_0 + \cdots + a_8x^8$ and $b(x) = b_0 + \cdots + b_6x^6$ have degree $8, 6$ respectively and the numerator $\phi_{\mathrm{num}}(x,y) = a(x) + b(x)y$ vanishes to degree 3 at $(0,-1)$ and 2 at $(0,-\gamma)$.

By the ramification description above 0, we must have

$$N\phi_{\mathrm{num}}(x,y) = a(x)^2 - b(x)^2f(x) = a_8^2(x-1)^2x^3c(x)^3d(x) \tag{10.8}$$

where $c(x) = c_0 + c_1x + c_2x^2 + x^3$ and $d(x) = x^2 + d_1x + d_0$, and

$$N(\phi(x,y)-1)_{\mathrm{num}} = (a(x)-(x-1)^2x^3)^2 - b(x)^2f(x) = (x-1)^2x^3a_8^2e(x)g(x) \tag{10.9}$$

where $e(x) = x^2 + e_1x + e_0$ and $g(x) = x + g_0$.

In principal, one could simply solve these equations over $\overline{\mathbb{Q}}$, as was done in previous examples, using Gröbner basis techniques or other simplifications. This utterly fails here given the number of variables involved. This calculation is also made more difficult by the possibility that other Belyi covers will intervene: the Matthieu

group $M_{11} \hookrightarrow S_{11}$ also has a $(3,5,6)$ triple of genus 1, and it is conceivable that S_{11} also occurs. Discarding these solutions is a nontrivial task until one has already computed them!

So we instead by "turning the ℓ-adic crank": we search for a solution in a finite field $\mathbb{F}_\ell$, lift such a solution using Hensel's lemma (when it applies), and then attempt to recognize the solution ℓ-adically as an algebraic number using the LLL-lattice reduction algorithm. This method was pursued by Elkies [17] and its variants have been rediscovered and used by many people in different contexts.

We guess that this curve will be defined over $M(X,G)$ and that this field is a quadratic extension of $\mathbb{Q}(\sqrt{3},\sqrt{5})$ ramified only at 11. The primes of smallest norm which is coprime to $\#\operatorname{PSL}_2(\mathbb{F}_{11})$ are $49, 59$.

We speed up the search with a few tricks. Subtracting the two equations (10.8)–(10.9), we have

$$a_8^2 c(x)^3 d(x) - 2a(x) + (x-1)^2 x^3 = a_8^2 e(x)^5 g(x).$$

Comparing coefficients on both sides, by degree we see that the coefficients of x^9 and x^{10} of $c(x)^3 d(x)$ and $e(x)^5 g(x)$ must agree. So we precompute a table of the possible polynomials of the form $e(x)^5 g(x)$: there are $O(\ell^3)$ such, and we sort them for easy table lookup. Then, for each of the possible polynomials of the form $c(x)^3 d(x)$, of which there are $O(\ell^5)$, we match the above coefficients—typically there are few matches. Then for each $a_8^2 \in \mathbb{F}_\ell^{\times 2}$, we compute $a(x)$ as

$$a(x) = \frac{1}{2}\left(a_8^2 c(x)^3 d(x) - a_8^2 e(x)^5 g(x) - (x-1)^2 x^3\right).$$

From equation (10.8) we have

$$a(x)^2 - a_8^2 (x-1)^2 x^3 c(x)^3 d(x) = f(x) b(x)^2$$

so we compute the polynomial on the right and factor it into squarefree parts. If $f(x)$ has degree 3, then we find $b(x)$ as well, and we have found our solution.

Putting this on a cluster (hosted graciously at the Vermont Advanced Computing Center), and using Magma, after a few days we have our answer. We find some solutions in $\mathbb{F}_{49}$ but only one solution lifts ℓ-adically (the Jacobian of the corresponding system of equations drops rank): after some effort, we recognize this cover as an M_{11}-cover with ramification $(3,5,6)$, defined over the number field $\mathbb{Q}(\alpha)$ where

$$\alpha^7 - \alpha^6 - 8\alpha^5 + 21\alpha^4 + 6\alpha^3 - 90\alpha^2 + 60\alpha + 60 = 0.$$

We find 62 solutions in $\mathbb{F}_{59}$, but only 8 of these yield covers with the correct ramification data: our above conditions are necessary, but not sufficient, as we have only specified the x-coordinates and not the y-coordinates. (The M_{11}-cover does not reappear as there is no prime of norm 59 in $\mathbb{Q}(\alpha)$.) These covers lift to 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 $N(b) = 11^2$; more beautifully, it is given by extending by a root β of the equation

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

For what it's worth, 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, barring computational error, this gives strong evidence for our Theorem A, and shows that it is "best possible" in that one may indeed obtain a nontrivial extension in one of the unknown quadratic extensions which arise from the failure of (weak) rigidity.

Remark 10.10. 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] Srinath Baba and Hakan Granath, *Genus 2 curves with quaternionic multiplication*, Canadian J. of Math. **60** (2008), no. 4, 734–757.

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

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

[5] 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.

[6] A. Borel, *Introduction aux groupes arithmetiques*, Hermann, Paris, 1969.

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

[8] D.V. Chudnovsky and G.V. Chudnovsky, *Computer algebra in the service of mathematical physics and number theory*, Computers and Mathematics (Stanford, CA, 1986), Lecture Notes in Pure and Appl. Math., vol. 125, Dekker, New York, 1990, 109–232.

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

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

[11] 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.

[12] Kevin Coombes and David Harbater, *Hurwitz families and arithmetic Galois groups*, Duke Math. J. **52** (1985), no. 4, 821–839.

[13] Henri Darmon, *Rigid local systems, Hilbert modular forms, and Fermat's last theorem*, Duke Math. J. **102** (2000), no. 3, 413–449.

[14] Debes and Emsalem, *On fields of moduli of curves*, **211** (1999), no. 1, 42–56.

[15] 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.

[16] W.L. Edge, *Bring's curve*, J. London Math. Soc. **2** (1978), no. 3, 539–545.

[17] 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.
[18] 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.
[19] Noam Elkies, *Shimura curve computations*, Algorithmic number theory (Portland, OR, 1998), Lecture notes in Comput. Sci., vol. 1423, 1–47.
[20] R. Fricke and F. Klein, *Vorlesungen ueber die Theorie der automorphen Funktionen*, vols. 1–2, Teubner, Leipzig, 1897, 1912.
[21] Ernesto Girondo and Jürgen Wolfart, *Conjugators of Fuchsian groups and quasiplatonic surfaces*, Quart. J. Math. **56** (2005), 525–540.
[22] Leon Greenberg, *Maximal Fuchsian groups*, Bull. Amer. Math. Soc. **69** (1963), 569–573.
[23] E. Hallouin, *Computation of a cover of Shimura curves using a Hurwitz space*, J. of Algebra **321** (2009), no. 2, 558–566.
[24] E. Hecke, *Über die Bestimmung Direchletscher Reihen durch ihre Funktionalgleichungen*, Math. Ann. **112** (1936), 664–699.
[25] Svetlana Katok, *Fuchsian groups*, University of Chicago Press, Chicago, 1992.
[26] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, 1985.
[27] Bernhard Köck, *Belyĭ's theorem revisited*, Beiträge Algebra Geom. **45** (2004), no. 1, 253–265.
[28] Mong-Lung Lang, Chong-Hai Lim, and Ser-Peow Tan, *Principal congruence subgroups of the Hecke groups*, J. Number Theory **85** (2000) 220–230.
[29] Ulrich Langer and Gerhard Rosenberger, *Erzeugende endlicher projektiver linearer Gruppen*, Results Math. **15** (1989), no. 1–2, 119–148.
[30] Macbeath, *On a curve of genus* 7, Proc. London Math. Soc. (3) **15** (1965), 527–542.
[31] Macbeath, *Generators of the linear fractional groups*, Number Theory (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967), Amer. Math. Soc., Providence, 14–32.
[32] Wilhelm Magnus, *Noneuclidean tesselations and their groups*, Pure and Applied Mathematics, vol. 61, Academic Press, New York, 1974.
[33] Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999.
[34] G. Margulis, *Discrete subgroups of semisimple Lie groups*, Springer, Berlin, 1991.
[35] 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.
[36] J.S. Milne, *Introduction to Shimura Varieties*, Clay Mathematic Proceedings, vol. 4, 2005.
[37] Israel Moreno-Mejía, *The quadrics through the Hurwitz curves of genus 14*, London Math. Soc. **81** (2010), 374–388.
[38] Hans Petersson, *Über die eindeutige Bestimmung und die Erweiterungsfähigkeit von gewissen Grenzkreisgruppen*, Abh. Math. Semin. Univ. Hambg. **12** (1937), no. 1, 180–199.
[39] John G. Ratcliffe, *Foundations of hyperbolic manifolds*, 2nd ed., Graduate Texts in Mathematics, vol. 149, Springer, New York, 2006.
[40] Harry Reimann, *The semi-simple zeta function of quaternionic Shimura varieties*, Lecture Notes in Mathematics, vol. 1657, Springer-Verlag, Berlin, 1997.
[41] Sabine Ricker, *Symmetric Fuchsian quadrilateral groups and modular embeddings*, Quart. J. Math **53** (2002), 75–86.
[42] Paul Schmutz Schaller and Jürgen Wolfart, *Semi-arithmetic Fuchsian groups and modular embeddings*, J. London Math. Soc. (2) **61** (2000), 13–24.
[43] Jan-Christoph Schlage-Puchta and Jürgen Wolfart, *How many quasiplatonic surfaces?*, Arch. Math. (Basel) **86** (2006), no. 2, 129–132.
[44] Thomas A. Schmidt and Katherine Smith, *Galois orbits of principal congruence Hecke curves*, J. London Math. Soc. (2) **67** (2003), no. 3, 673–685.
[45] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, Research Notes in Math., vol. 7. A.K. Peters, Wellesley, MA, 1998.
[46] J.-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics 1, Jones and Bartlett, 1992.
[47] G.B. Shabat and V. Voevodsky, *Drawing curves over number fields*, Grothendieck Festchrift, vol. III, Birkhauser, Boston, 1990, 199–227.

[48] Kuang-yen Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann. **207** (1974), 99–120.
[49] D. Singerman, *Finitely maximal Fuchsian groups*, J. London Math. Soc. (2) **6** (1972), 29–38.
[50] Goro Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. (2) **85** (1967), 58–159.
[51] Goro Shimura, *On canonical models of arithmetic quotients by bounded symmetric domains*, Annals of Math. **91** (1970), no. 1, 144–222.
[52] D. Singerman and R.I. Syddall, *Belyĭ uniformization of elliptic curves*, Bull. London Math. Soc. **139** (1997), 443–451.
[53] Manfred Streit, *Field of definition and Galois orbits for the Macbeath-Hurwitz curves*, Arch. Math. (Basel) **74** (2000), no. 5, 342–349.
[54] Manfred Streit, *Homology, Belyĭ functions and canonical curves*, Manuscripta Math. **90** (1996), 489–509.
[55] Manfred Streit and Jürgen Wolfart, *Galois actions on some series of Riemann surfaces with many automorphisms*, preprint, available at `www.math.uni-frankfurt.de/~wolfart/Artikel/gal.ps`.
[56] Michio Suzuki, *Group theory. II*, Grundlehren der Mathematischen Wissenschaften, vol. 248, Springer-Verlag, New York, 1986.
[57] Kisao Takeuchi, *On some discrete subgroups of* $\mathrm{SL}_2(\mathbb{R})$, J. Fac. Sci. Univ. Tokyo Sect. I **16** (1969), 97–100.
[58] Kisao Takuechi, *A characterization of arithmetic Fuchsian groups*, J. Math. Soc. Japan **27** (1975), no. 4, 600–612.
[59] Kisao Takeuchi, *Arithmetic triangle groups*, J. Math. Soc. Japan **29** (1977), no. 1, 91–106.
[60] Kisao Takeuchi, *Commensurability classes of arithmetic triangle groups*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **24** (1977), no. 1, 201–212.
[61] 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.
[62] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980.
[63] John Voight, *Quadratic forms and quaternion algebras: Algorithms and arithmetic*, Ph.D. thesis, University of California, Berkeley, 2005.
[64] Helmut Völklein, *Groups as Galois groups. An introduction*, Cambridge Studies in Advanced Mathematics, vol. 53, Cambridge University Press, Cambridge, 1996.
[65] K. Wohlfahrt, *Macbeath's curve and the modular group*, Glasgow Math. J. **27** (1985), 239–247.
[66] 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.
[67] Jürgen Wolfart, *Triangle groups and Jacobians of CM type*, manuscript, 2000.
[68] 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.
[69] 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

E-mail address: `pete@math.uga.edu`

Department of Mathematics and Statistics, University of Vermont, 16 Colchester Ave, Burlington, VT 05401, USA

E-mail address: `jvoight@gmail.com`