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 Shimura curves associated to arithmetic triangle groups. We determine the field of moduli of the curves associated to these groups and thereby realize the Galois groups $\mathrm{PSL}_2(\mathbb{F}_q)$ and $\mathrm{PGL}_2(\mathbb{F}_q)$ regularly in many cases over explicitly given abelian number fields.

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 [12] investigated curves arising from subgroups which we now recognize among the class of arithmetic Fuchsian groups. Later, Hecke [15] investigated his triangle groups, generalizing the presentation of $\mathrm{SL}_2(\mathbb{Z})$ as the free product of the groups $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$. In the 1960s, Atkin and Swinnerton-Dyer [1] pioneered the study of noncongruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. In this paper, we pursue a different direction and 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 consider again the classical modular curves. Let $p \geq 3$ be prime and let $\Gamma(p) \subset \mathrm{PSL}_2(\mathbb{Z}) = \Gamma(1)$ be the subgroup of matrices congruent to the identity modulo p. Then $\Gamma(p)$ acts on the completed upper half-plane $\mathfrak{H}^*$, and the quotient $X(p) = \Gamma(p)\backslash\mathfrak{H}^*$ is a modular curve which parametrizes (generalized) elliptic curves with full level p-structure. The subgroup $G = \Gamma(1)/\Gamma(p) \subset \mathrm{Aut}(X(p))$ 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 $G \subset \mathrm{Aut}(X)$ with $G \cong \mathrm{PSL}_2(\mathbb{F}_q)$ or $G \cong \mathrm{PGL}_2(\mathbb{F}_q)$ (for some prime power q) and the map $X \to X/G \cong \mathbb{P}^1$ is a Galois cover ramified at three points.

This class of curves is indeed an appealing class to study. On the one hand, Belyĭ [2, 3] proved that a curve X over $\mathbb{C}$ admits a map $X \to \mathbb{P}^1_{\mathbb{C}}$ ramified at three points, known as a *Belyĭ map*, if and only if X can be defined 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 2.3). We call a Galois Belyĭ map $f : X \to \mathbb{P}^1$ with Galois group G a *(G-)Wolfart map* and a curve which admits a G-Wolfart map a *(G-)Wolfart curve*, after Wolfart [50]. These curves are called *curves with many automorphisms*

Date: September 14, 2009.

by Wolfart because they are also characterized as being 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 $n \geq 3$. These curves are also called *quasiplatonic surfaces* [13] owing to their connection with the Platonic solids, given by the spherical triangle groups. (See below for other equivalent characterizations of Wolfart curves.)

Our main goal is to investigate the basic arithmetic of Wolfart curves. For a curve X defined over $\mathbb{C}$, the *field of moduli* of X is the fixed field of the group $\{\sigma \in \operatorname{Aut}(X) : X^\sigma \cong X\}$, where X^σ is the base change of X by the automorphism $\sigma \in \operatorname{Aut}(X)$. 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. In fact, a Wolfart curve can 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 of the pair $(X, \operatorname{Aut}(X))$. 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 [39] who considers $G \cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$.)

To state our first result we use the following notation. For an integer $s \in \mathbb{Z}_{>0}$, write $\zeta_s = \exp(2\pi i/s)$ and $\lambda_s = \zeta_s + 1/\zeta_s = 2\cos(2\pi/s)$. Let $E_\lambda(a,b,c)$ (resp. $E_\zeta(a,b,c)$) be the compositum of fields $\mathbb{Q}(\lambda_s)$ (resp. $\mathbb{Q}(\zeta_s)$) for $s \in \{a,b,c\}$ with $p \nmid s$. Let $E(a,b,c;p) = E(a,b,c)^{\langle \mathrm{Frob}_p \rangle}$.

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) with $a,b,c \in \mathbb{Z}_{\geq 2}$. Let r be the order of Frob_p in $\mathrm{Gal}(E(2a,2b,2c)/\mathbb{Q})$, and let K be the minimal field of definition of $(X, \operatorname{Aut}(X))$.*

(a) *Suppose that $G \cong \mathrm{PSL}_2(\mathbb{F}_q)$. Then $q = p^r$. The field of moduli of X is $E_\lambda(a,b,c;p)$. If p is odd then K contains $E_\lambda(a,b,c)$ with $[K : E(a,b,c)] = 2$, and if $p = 2$ then $K = E_\lambda(a,b,c)$.*

(b) *Suppose that $G \cong \mathrm{PGL}_2(\mathbb{F}_q)$. Then $q = \sqrt{p^r}$, the field of moduli of X is $E_\zeta(a,b,c;p)$, and $K = E_\zeta(a,b,c)$.*

The statements $q = p^r$ and $q = \sqrt{p^r}$, accordingly, can be extracted from work of Langer and Rosenberg [20]; we give a similar but slightly more streamlined proof. Theorem A also generalizes work of Schmidt and Smith [32, Section 3] in the case of Hecke triangle groups where $(a,b,c) = (2,n,\infty)$ for $n \geq 5$, and Streit [37] who covers Hurwitz groups, those with $(a,b,c) = (2,3,7)$.

To prove Theorem A, we use a variant of the rigidity and rationality results which arise in the study of the inverse Galois problem [24, 49] 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 [22].

In light of Theorem A, a result which follows mainly from group theory, we then consider a method for constructing such Wolfart maps which arises from arithmetic geometry. Wolfart curves of genus $g \geq 2$ admit a further description as compact Riemann surfaces of the form $\Gamma \backslash \mathfrak{H}$, where Γ is a torsion-free finite-index normal subgroup of a hyperbolic triangle

group $\Delta(a,b,c)$ with $a,b,c \in \mathbb{Z}_{\geq 2}$ (see Section 1 for definitions and Proposition 2.4 for this equivalence).

Let $a,b,c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$ satisfy $a \leq b \leq c$. The triple (a,b,c) is *hyperbolic* if

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}-1<0.$$

A triple is *maximal* if it is not of the form

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

Let

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

by convention we let $\zeta_\infty = 1$ and $\lambda_\infty = 2$. By a *prime* of a number field F we mean a nonzero prime ideal of the ring of integers of F. For a prime $\mathfrak{p}$ of F, let $\mathbb{F}_\mathfrak{p}$ denote its residue class field.

Theorem B. *Let (a,b,c) be a hyperbolic triple with $a,b,c \in \mathbb{Z}_{\geq 2}\cup\{\infty\}$. Suppose that (a,b,c) is maximal and that either*

$$\frac{\operatorname{lcm}(a,b)}{\gcd(a,b)} \nmid c \quad \text{or} \quad c \nmid \operatorname{lcm}(a,b).$$

Let $\mathfrak{P}$ be a prime of $F^{(2)}(a,b,c)$ with $\mathfrak{p} \nmid 2abc$, let $\mathfrak{p}$ be the prime of $F^{(2)}$ below $\mathfrak{p}$, and let p be the rational prime below $\mathfrak{p}$.

Then there is 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

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

The curve $X(a,b,c;\mathfrak{p})$ is unique up to (nonunique) isomorphism.

This Theorem generalizes work of Lang, Lim, and Tan [19] who treat the case of Hecke triangle groups $(a,b,c) = (2,q,\infty)$ using an explicit presentation of the group. (But see also Example 9.3.) To prove Theorem B, we use a modular embedding of the triangle group $\overline{\Delta}(a,b,c)$ into an arithmetic group, following Takeuchi [45], later developed by Cohen and Wolfart [6].

When $\infty \in \{a,b,c\}$, Darmon [8] has constructed a family of so-called hypergeometric abelian varieties associated to the triangle group $\overline{\Delta}(a,b,c)$ with consequences for generalized Fermat equations. The construction of the covers above we believe will likewise have similarly important arithmetic applications. See also work of Tyszkowska [47], who studies the fixed points of a particular symmetry of $\mathrm{PSL}_2(\mathbb{F}_p)$-Wolfart curves.

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 [25] states that a Fuchsian group is arithmetic if and only if it is of infinite index in its commensurator group. Only finitely many of the groups $\Delta(a,b,c)$ are arithmetic by work of Takeuchi [45]. In these cases, the curves $X(a,b,c;\mathfrak{p})$ are *Shimura curves* (arising from congruence subgroups) and a canonical model was given by Shimura [40] and Deligne [10]. Indeed, the curves $X(2,3,\infty;p)$ are

the classical modular curves $X(p)$ and the Wolfart map $X(p) \to \mathbb{P}^1$ is associated to the congruence subgroup $\Gamma(p) \subset \mathrm{PSL}_2(\mathbb{Z})$. 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; nevertheless, based upon the theorems above we believe that these curves carry a rich geometry which is worthy of study.

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 either $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$ or $\mathrm{SL}_2(\mathbb{F}_\mathfrak{p})$ regularly over the field $F(a,b,c;p)$. Moreover, by considering the curves corresponding to the subgroups of upper-triangular matrices modulo $\mathfrak{p}$, one obtains covers $X_0(a,b,c;\mathfrak{p}) \to X(a,b,c)$ which can be used in the arithmetic study generalized Fermat equations.

The paper is organized as follows. In Sections 1 and 2, we introduce the triangle groups $\Delta(a,b,c)$, 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 we then 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; then in Sections 6 and 7 we review Macbeath's theory of subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ and thereby prove Theorem A. In Section 8, we prove Theorem B. Finally, we conclude in Section 9 with some explicit examples and pose some final questions.

1. Triangle groups

In this section, we review the basic theory of triangle groups. We refer to Magnus [23, Chapter II] and Ratcliffe [28, §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

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1$$

is positive, zero, or negative. The spherical triples are $(2,2,c)$ with $c \in \mathbb{Z}_{\geq 2}$, $(2,3,3)$, $(2,3,4)$, and $(2,3,5)$. 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 $\gamma^\infty = 1$. 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 $\overline{\Delta}(a,b,c)$ by the triple (a,b,c).

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 of the groups $\mathbb{Z}/a\mathbb{Z}$ and $\mathbb{Z}/b\mathbb{Z}$.

We have an exact sequence

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

and we see that $\overline{\Delta}^{\mathrm{ab}} = \overline{\Delta}/[\overline{\Delta},\overline{\Delta}]$ 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 $c \neq \infty$. Thus, the group $\overline{\Delta}$ is perfect (i.e. $\overline{\Delta}^{\mathrm{ab}} = \{1\}$) if and only if $c = \infty$ or 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 $[\overline{\Delta},\overline{\Delta}] \cong \mathbb{Z}^2$ [23, §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 τ_a, τ_b, τ_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 $\gamma_a = \tau_a\tau_b$, $\gamma_b = \tau_b\tau_c$, and $\gamma_c = \tau_c\tau_a$ 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 γ_a, γ_b, and γ_c, and consequently the quotient space is a Riemann surface of genus zero. This surface is compact if and only if $c < \infty$.

Example 1.5. 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 [15] are given by $\overline{\Delta}(2,n,\infty)$ 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 $\mathfrak{H}^{(*)}$; we write $X(a,b,c) = \overline{\Delta}(a,b,c)\backslash\mathfrak{H}^{(*)} \cong \mathbb{P}^1_{\mathbb{C}}$ 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 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 and will also be excluded for other reasons later. Then Takeuchi [45, 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 [27]. For $s \in \mathbb{Z}_{\geq 2}$ we let $\zeta_s = \exp(2\pi i/s)$ and

$$\lambda_s = \zeta_s + \frac{1}{\zeta_s} = 2\cos\left(\frac{2\pi}{s}\right) \quad \text{and} \quad \mu_s = 2\sin\left(\frac{2\pi}{s}\right) = -i\left(\zeta_s - \frac{1}{\zeta_s}\right) \tag{1.6}$$

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

Then we have a map

$$\begin{aligned} \Delta(a,b,c) &\hookrightarrow \mathrm{SL}_2(\mathbb{R}) \\ \gamma_a &\mapsto \frac{1}{4}\begin{pmatrix} \lambda_{2a} & \mu_{2a} \\ -\mu_{2a} & \lambda_{2a} \end{pmatrix} \\ \gamma_b &\mapsto \frac{1}{4}\begin{pmatrix} \lambda_{2b} & t\mu_{2b} \\ -\mu_{2b}/t & \lambda_{2b} \end{pmatrix} \end{aligned} \tag{1.7}$$

where

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

The embedding (1.7) then also gives rise to an explicit embedding $\Delta(a,b,c) \hookrightarrow \mathrm{PSL}_2(\mathbb{R})$.

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 [36] (see also Greenberg [14, 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 [13, (2)]

$$\begin{aligned} \overline{\Delta}(2,7,7) &\subset_9 \overline{\Delta}(2,3,7) & \overline{\Delta}(3,8,8) &\subset_{10} \overline{\Delta}(2,3,8) \\ \overline{\Delta}(4,4,5) &\subset_6 \overline{\Delta}(2,4,5) & \overline{\Delta}(3,3,7) &\subset_8 \overline{\Delta}(2,3,7) \end{aligned} \tag{1.8}$$

or one of the families

$$\begin{aligned} \overline{\Delta}(a,a,a) &\subset_3 \overline{\Delta}(3,3,a) & \overline{\Delta}(a,a,c) &\subset_2 \overline{\Delta}(2,a,2c) \\ \overline{\Delta}(2,b,2b) &\subset_3 \overline{\Delta}(2,3,2b) & \overline{\Delta}(3,b,3b) &\subset_4 \overline{\Delta}(2,3,3b), \end{aligned} \tag{1.9}$$

where in (1.9) (and here alone) for notational simplicity we relax our assumption that $a \leq b \leq c$. The notation $\overline{\Delta} \subset_n \overline{\Delta}'$ 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* [4] 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 units of reduced norm 1 in a maximal order $\mathcal{O} \subset B$. Takeuchi [45, Theorem 3] has classified all triples (a,b,c) such that $X(a,b,c)$ is arithmetic; there are 85 such triples and they fall into 19 commensurability classes [46, Table (1)].

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 [50, 51]. 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 $\overline{\Delta}(2, 2, 3)$. Further examples of Belyĭ maps $\mathbb{P}^1 \to \mathbb{P}^1$ are given by the other spherical triangle groups.

Example 2.2. An elliptic curve E (over $\overline{\mathbb{Q}}$ or $\mathbb{C}$) is a Wolfart curve 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 $G \subset \mathrm{Aut}(E)$ (automorphisms as a genus 1 curve), then we can factor f into the composition of an isogeny $E \to E'$ 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 $K = \mathbb{Z}[\omega]$ with $\omega^3 = 1$ 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 [41] for a more complete treatment.

Remark 2.3. There are only finitely many Wolfart curves of given genus. [♠♠ **TO DO** : Argument here.] In fact, according to Schlage-Puchta and Wolfart [31], the number of isomorphism classes of Wolfart curves of genus $\leq g$ grows like $g^{\log g}$. Wolfart [51] 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 [34].

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 2.4 (Wolfart [50, 51])**.** *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) *X is uniformized by a Fuchsian group Γ which is a finite-index, normal subgroup of a hyperbolic triangle group $\overline{\Delta}(a, b, c)$ with $a, b, c \in \mathbb{Z}_{\geq 2}$;*
(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 2.5. We note the following interesting consequence of Proposition 2.4. If $\Gamma' \subset \mathrm{PSL}_2(\mathbb{Z}) \cong \overline{\Delta}(2, 3, \infty)$ is a torsion-free normal subgroup and $X = \Gamma' \backslash \mathfrak{H}^{(*)}$ is a Wolfart curve, then in fact X is uniformized by a group $\Gamma \subset \overline{\Delta}(a, b, c)$ 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 [32, Proposition 4].

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

$$g(X) = 1 + \frac{\#G}{2}\left(1 - \frac{1}{a} - \frac{1}{b} - \frac{1}{c}\right). \tag{2.6}$$

Remark 2.7. The function of $\#G$ in (2.6) is maximized when $(a, b, c) = (2, 3, 7)$. Combining this with Proposition 2.4(iv) we recover the Hurwitz bound

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

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 2.4(iii) leads us to consider curves arising from finite-index normal subgroups of the hyperbolic triangle groups $\overline{\Delta}(a, b, c)$. If $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$ is a Fuchsian group, write $X(\Gamma) = \Gamma \setminus \mathfrak{H}^{(*)}$. If X is a compact Riemann surface of genus $g \geq 2$ with uniformizing subgroup $\Gamma \subset \mathrm{PSL}_2(\mathbb{R})$, so that $X = X(\Gamma)$, then $\operatorname{Aut}(X) = N(\Gamma)/\Gamma$, where $N(\Gamma)$ is the normalizer of Γ in $\mathrm{PSL}_2(\mathbb{R})$. Moreover, the quotient $X \to X/\operatorname{Aut}(X)$, obtained from the map $X(\Gamma) \to X(N(\Gamma))$, is a Galois cover with Galois group $\operatorname{Aut}(X)$. By the results of Section 1, if $\Gamma \subset \overline{\Delta}(a, b, c)$ is a finite-index normal subgroup then $\operatorname{Aut}(X(\Gamma))$ is of the form $\overline{\Delta}'/\Gamma$ with an inclusion $\overline{\Delta} \subset \overline{\Delta}'$ as in (1.8)–(1.9); if $\overline{\Delta}$ is maximal, then we conclude

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

3. Fields of moduli

In this section, we briefly review the theory of fields of moduli and fields of definition. See Köck [18] and the references contained therein for more detail.

The *field of moduli* of a curve X over $\mathbb{C}$ is the fixed field of the group $\{\sigma \in \operatorname{Aut}(X) : X^\sigma \cong X\}$. 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 a curve has a number field as field of moduli if and only if it 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 $C \cong \mathbb{P}^1$, 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 [9] remark that this lemma follows from results of Coombes and Harbater [7]. The proof was written down by Köck [18, 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 $X \to X/\operatorname{Aut}(X)$. □

Let X be a curve which can be defined over its field of moduli F. Then the set of models for X over F is given by the Galois cohomology set $H^1(F, \operatorname{Aut}(X))$, where $\operatorname{Aut}(X)$ is viewed as a module over the absolute Galois group $\mathcal{G}_F = \operatorname{Gal}(\overline{F}/F)$. The action of $\mathcal{G}_F$ on $\operatorname{Aut}(X)$ cuts out a finite Galois extension $K \supset F$ which is the minimal field such that all elements of $\operatorname{Aut}(X)$ are defined over K; in other words, the pair $(X, \operatorname{Aut}(X))$ 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 [33, Chapter 3] we find that G occurs infinitely often as a Galois group over K.

Example 3.5. Let $p \geq 7$ be prime and let $X = X(p) = \Gamma(p)\backslash\mathfrak{H}^*$ be the classical modular curve, parametrizing (generalized) elliptic curves with full p-level structure. Then $\mathrm{Aut}(X) \cong \mathrm{PSL}_2(\mathbb{F}_p)$ and the quotient map $j : X \to X/\mathrm{Aut}(X) \cong \mathbb{P}^1$, corresponding to the inclusion $\Gamma(p) \subset \mathrm{PSL}_2(\mathbb{Z})$, 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 $\mathbb{Q}$ [♠♠ **TO DO** : Cite Shimura-Deligne or Katz-Mazur for this? It's a common point of confusion, so we should state it cleanly, briefly here. One gets a 'canonical' model by defining the right moduli problem and we should address this.] 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 [♠♠ **TO DO** : Cite] 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 [♠♠ **TO DO** : Cite Katz-Mazur or whatever] gives a model over $\mathbb{Q}(\zeta_p)$.

Example 3.6. [♠♠ **TO DO** : 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 $\mathbb{Q}(\zeta_7)^+$? The canonical model is not the Klein quartic, though: it is a twist by $\mathbb{Q}(\sqrt{-3})$? This was remarked by Livné.]

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 [44]. This idea was also pursued by Cohen and Wolfart [6] with an eye toward results in transcendence theory, and further elaborated by Cohen, Itzykson and Wolfart [5]. Here, we use this embedding to construct congruence subgroups of Δ. We refer to Vignéras [48] for the facts we will use about quaternion algebras and Katok [16] as a reference on Fuchsian groups.

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ be a Fuchsian group of the first kind. Let

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

be the *trace field* of Γ. Suppose that F is a number field and let $\mathbb{Z}_F$ be its ring of integers. Let $F[\Gamma]$ be the F-vector space generated by Γ in $\mathrm{M}_2(\mathbb{R})$ and let $\mathbb{Z}_F[\Gamma]$ denote the $\mathbb{Z}_F$-submodule of $F[\Gamma]$ generated by Γ. Then by work of Takeuchi [43, Propositions 2–3], the ring $F[\Gamma]$ is a quaternion algebra over F and $\mathbb{Z}_F[\Gamma]$ is an order in $F[\Gamma]$.

Remark 4.1. This construction can be made more general. Schaller and Wolfart [30] call a Fuchsian group Γ *semi-arithmetic* if its trace field $F = \mathbb{Q}(\operatorname{tr}\Gamma)$ is a totally real number field and $\operatorname{tr}\Gamma^2$ 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 holds. See also work of Ricker [29].

Now let (a,b,c) be a hyperbolic triple with $2 \le a \le b \le c \le \infty$. As in §1, associated to the triple (a,b,c) is the triangle group $\Delta(a,b,c) \subset \mathrm{SL}_2(\mathbb{R})$ with $\Delta(a,b,c)/\{\pm 1\} \cong \overline{\Delta}(a,b,c) \subset \mathrm{PSL}_2(\mathbb{R})$. Let $F = \mathbb{Q}(\operatorname{tr}\Delta(a,b,c))$ be the trace field of $\Delta(a,b,c)$. By Takeuchi [45, Proposition 2], we have

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

Since

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

and

$$\gamma_a\gamma_b + \gamma_b\gamma_a = \lambda_{2b}\gamma_a + \lambda_{2a}\gamma_b + \lambda_{2c} - \lambda_{2a}\lambda_{2b},$$

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 $\mathcal{O} = \mathbb{Z}_F[\Delta] \subset B = F[\Delta]$ (see also Takeuchi [45, Proposition 3]). The 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 (1.6).

Lemma 4.2. *The (reduced) discriminant of $\mathcal{O}$ is a principal $\mathbb{Z}_F$-ideal generated by*

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

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

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

The result follows. □

Lemma 4.3. *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 identity in the field $\mathbb{Q}(\zeta_{2a}, \zeta_{2b}, \zeta_{2c}) = K$:

$$\beta = \left(\frac{\zeta_{2b}\zeta_{2c}}{\zeta_{2a}} + 1\right)\left(\frac{\zeta_{2a}\zeta_{2c}}{\zeta_{2b}} + 1\right)\left(\frac{\zeta_{2a}\zeta_{2b}}{\zeta_{2c}} + 1\right)\left(\frac{1}{\zeta_{2a}\zeta_{2b}\zeta_{2c}} + 1\right). \tag{4.4}$$

Let $\mathfrak{q}$ be a prime above $\mathfrak{P}$ in K and suppose that $\mathfrak{q} \mid \beta$. Then $\mathfrak{q}$ divides one of the factors in (4.4).

First, suppose that $\mathfrak{q} \mid (\zeta_{2b}\zeta_{2c}\zeta_{2a}^{-1} + 1)$, i.e., we have $\zeta_{2b}\zeta_{2c} \equiv -\zeta_{2a} \pmod{\mathfrak{q}}$. Suppose that $\mathfrak{q} \nmid 2abc$. Then the map $(\mathbb{Z}_K^\times)_{\mathrm{tors}} \to \mathbb{F}_\mathfrak{q}^\times$ 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

$$\frac{1}{b} + \frac{1}{c} = 1 + \frac{1}{a} \in \mathbb{Q}/2\mathbb{Z}. \tag{4.5}$$

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 (4.5).

Now suppose $\mathfrak{q} \mid 2$ but still $\mathfrak{q} \nmid abc$. Then $\ker((\mathbb{Z}_K^\times)_{\mathrm{tors}} \to \mathbb{F}_\mathfrak{P}^\times) = \{\pm 1\}$, 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 it is easy to see 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 $\mathfrak{q}$ divides the middle two factors is similar. The case where $\mathfrak{q}$ 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. □

Remark 4.6. It would be interesting to analyze the case where $\mathfrak{p} \mid abc$ and to characterize when $\mathfrak{p}$ is in fact ramified in the algebra B (even if the order $\mathcal{O}$ is not $\mathfrak{p}$-maximal).

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

$$\overline{\Delta} = \Delta/\{\pm 1\} \hookrightarrow \mathcal{O}_1^\times/\{\pm 1\}. \tag{4.7}$$

In fact, the image of this map arises from a quaternion algebra over a smaller field, as follows. Let Δ^2 denote the subgroup of Δ generated by γ^2 for $\gamma \in \Delta$. Then Δ^2 is a normal

subgroup of Δ, and the quotient Δ/Δ^2 is an elementary abelian 2-group. We have [45, Proposition 5]

$$\Delta/\Delta^2 \cong \begin{cases} \{0\}, & \text{if at least two of } a,b,c \text{ are odd;} \\ \mathbb{Z}/2\mathbb{Z}, & \text{if exactly one of } a,b,c \text{ is odd;} \\ (\mathbb{Z}/2\mathbb{Z})^2, & \text{if all of } a,b,c \text{ are even or } \infty. \end{cases} \tag{4.8}$$

We note that

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

(and hence $\Delta^2 \hookrightarrow \overline{\Delta}$ if all of a,b,c are odd). To ease notation, we abbreviate $[\pm 1] = \Delta^2 \cap \{\pm 1\}$.

Again by Takeuchi [45, Propositions 4–5], we have that the trace field of Δ^2 is

$$F^{(2)} = F(a,b,c) = \mathbb{Q}(\lambda_{2a}^2, \lambda_{2b}^2, \lambda_{2c}^2, \lambda_{2a}\lambda_{2b}\lambda_{2c}) = \mathbb{Q}(\lambda_a, \lambda_b, \lambda_c, \lambda_{2a}\lambda_{2b}\lambda_{2c}), \tag{4.9}$$

where the latter equality holds since $\lambda_{2s}^2 = \lambda_s + 2$ for $k \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$.

Example 4.10. The Hecke triangle groups $\Delta(2,n,\infty)$ for $n \geq 3$ have trace field $F = \mathbb{Q}(\lambda_{2n})$ whereas the corresponding groups Δ^2 have trace field $F^{(2)} = \mathbb{Q}(\lambda_n)$.

Let $\mathcal{O}^{(2)} \subset B^{(2)}$ be the order and quaternion algebra associated to Δ^2. By construction we have

$$\Delta^2/[\pm 1] \hookrightarrow \mathcal{O}_1^{(2)\times}/\{\pm 1\}. \tag{4.11}$$

We then have the following fundamental result.

Proposition 4.12. *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 $N_{B^{(2)}}(\mathcal{O}^{(2)\times})/F^{(2)\times}$ *via*

$$\begin{aligned} \overline{\Delta} &\hookrightarrow \frac{N_{B^{(2)}}(\mathcal{O}^{(2)})}{F^{(2)\times}} \hookrightarrow \frac{N_B(\mathcal{O})}{F^\times} \\ \overline{\gamma}_s &\mapsto \gamma_s^2 + 1 \end{aligned} \tag{4.13}$$

where $k = a,b,c$ *and* N *denotes the normalizer. The map* (4.13) *extends the natural embedding* (4.11).

Example 4.14. 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 $F^{(2)} = \mathbb{Q}$ and indeed we find an embedding $\overline{\Delta}(2,4,6) \hookrightarrow N_{B^{(2)}}(\mathcal{O}^{(2)})/\mathbb{Q}^\times$ where $\mathcal{O}^{(2)}$ is a maximal order in a quaternion algebra $B^{(2)}$ of discriminant 6 over $\mathbb{Q}$.

Proof of Proposition 4.12. In B we have

$$\gamma_s^2 + 1 = \lambda_{2s}\gamma_s. \tag{4.15}$$

This implies that $\gamma_s^2 + 1$ has order k in $B^{(2)\times}/F^{(2)\times} \subset B^\times/F^\times$, and that

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

so the map (4.13) indeed defines a group homomorphism $\overline{\Delta} \hookrightarrow B^{(2)\times}/F^{(2)\times}$. The image lies in the normalizer $N_{B^{(2)}}(\mathcal{O}^{(2)})$ because Δ^2 generates $\mathcal{O}^{(2)}$ and Δ normalizes Δ^2.

Finally, we have

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

so the map extends the natural embedding of $\Delta^2/[\pm 1]$. □

Corollary 4.16. *We have $\mathcal{O}^{(2)} \otimes_{\mathbb{Z}_{F^{(2)}}} \mathbb{Z}_F = \mathcal{O}$. A prime $\mathfrak{p}$ of $F^{(2)}$ with $\mathfrak{p} \nmid 2abc$ is unramified in $B^{(2)}$.*

Proof. This statement follows from (4.15) since we have the obvious inclusion $\mathcal{O}^{(2)} \otimes_{\mathbb{Z}_{F^{(2)}}} \mathbb{Z}_F = \mathbb{Z}_{F^{(2)}}[\Delta^2] \subset \mathbb{Z}_F[\Delta]$. □

We now define congruence subgroups of triangle groups. Let $\mathfrak{P}$ be a prime of F with $\mathfrak{P} \nmid 2abc$. Then by Lemma 4.3, we have that $\mathfrak{P}$ is not ramified in B hence we have a splitting

$$\mathcal{O} \hookrightarrow \mathcal{O} \otimes_{\mathbb{Z}_F} \mathbb{Z}_{F,\mathfrak{P}} \cong \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{P}}) \tag{4.17}$$

where $\mathbb{Z}_{F,\mathfrak{P}}$ denotes the completion of $\mathbb{Z}_F$ at $\mathfrak{P}$. Let

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

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

$$1 \to \mathcal{O}(\mathfrak{P})_1^\times \to \mathcal{O}_1^\times/\{\pm 1\} \to \mathrm{PSL}_2(\mathbb{F}_{\mathfrak{P}}) \to 1,$$

where $\mathbb{F}_{\mathfrak{P}}$ denotes the residue class field of $\mathfrak{P}$. Let

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

Then we have an embedding

$$\frac{\overline{\Delta}}{\overline{\Delta}(\mathfrak{P})} \hookrightarrow \frac{\mathcal{O}_1^\times/\{\pm 1\}}{\mathcal{O}(\mathfrak{P})_1^\times} \cong \mathrm{PSL}_2(\mathbb{F}_{\mathfrak{P}}). \tag{4.18}$$

We conclude by considering the image of the embedding (4.18). Let $\mathfrak{p}$ be the prime of $F^{(2)} = F(a,b,c)$ below $\mathfrak{P}$ and define $\mathcal{O}^{(2)}(\mathfrak{p})$ analogously. Then by Proposition 4.12, we have an embedding

$$\overline{\Delta} \hookrightarrow \frac{N_{B^{(2)}}(\mathcal{O}^{(2)})}{F^{(2)\times}} \hookrightarrow \frac{B^{(2)\times}}{F^{(2)\times}} \hookrightarrow \frac{B_{\mathfrak{p}}^{(2)\times}}{F_{\mathfrak{p}}^{(2)\times}} \cong \mathrm{PGL}_2(F_{\mathfrak{p}}^{(2)}). \tag{4.19}$$

The image of $\overline{\Delta}$ in this map lies in $\mathrm{PGL}_2(\mathbb{Z}_{F^{(2)},\mathfrak{p}})$ since $\lambda_{2k} \in \mathbb{Z}_{F^{(2)},\mathfrak{p}}^\times$ for $k = a,b,c$ (since $\mathfrak{p} \nmid abc$). Then reducing the image in (4.19) modulo $\mathfrak{p}$, we obtain a map

$$\overline{\Delta} \to \mathrm{PGL}_2(\mathbb{F}_{\mathfrak{p}}).$$

This map is compatible with the map $\overline{\Delta} \to \mathrm{PSL}_2(\mathbb{F}_{\mathfrak{P}})$ inside $\mathrm{PGL}_2(\mathbb{F}_{\mathfrak{P}})$, obtained by comparing the images in the reduction modulo $\mathfrak{P}$ of $B^\times/F^\times$, by Proposition 4.12.

We record this result in the following proposition.

Proposition 4.20. *Let $a,b,c \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$. Let $\mathfrak{P}$ be a prime of F with $\mathfrak{P} \nmid 2abc$, and let $\mathfrak{p}$ be the prime of $F(a,b,c)$ below $\mathfrak{P}$. Then there exists a homomorphism ϕ with*

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

such that $\operatorname{tr}\phi(\overline{\gamma}_s) \equiv \pm\lambda_{2s} \pmod{\mathfrak{p}}$ for $s = a,b,c$. The image of ϕ lies in the subgroup $\mathrm{PGL}_2(\mathbb{F}_{\mathfrak{p}}) \cap \mathrm{PSL}_2(\mathbb{F}_{\mathfrak{P}}) \subset \mathrm{PGL}_2(\mathbb{F}_{\mathfrak{P}})$.

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 Malle and Matzat [24] and Serre [33, Chapters 7–8] for references.

Let G be a finite group. A *tuple* for G is a finite sequence $\underline{g} = (g_1, \dots, g_n)$ 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 $\langle g_1, \dots, g_n \rangle = G$. Let $\underline{C} = (C_1, \dots, C_n)$ be a finite sequence of conjugacy classes of G. Let $\Sigma(\underline{C})$ be the set of generating tuples $\underline{g} = (g_1, \dots, g_n)$ 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 $\mathrm{Inn}(G) = G$, and that $\underline{g}$ is generating. Suppose that $\Sigma(\underline{C}) \neq \emptyset$. Then the action of $\mathrm{Inn}(G)$ on $\Sigma(\underline{C})$ has no fixed points: if $x \in G$ fixes $\underline{g}$, then x commutes with each g_i hence with $\langle g_1, \dots, g_n \rangle = G$, so $g \in Z(G) = \{1\}$.

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 $G = \mathrm{Inn}(G)$. 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 $\varphi(\underline{g}) = \underline{g}'$.

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 $g \in G$. This action induces an action on conjugacy classes. If $\underline{C}$ is rigid and $s \in (\mathbb{Z}/m\mathbb{Z})^\times$ then $\underline{C}^s = (C_1^s, \dots, C_n^s)$ is rigid [33, Corollary 7.3.2]. Pulling back by the canonical isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/m\mathbb{Z})^\times$ gives an action of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ and hence also $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the set of conjugacy classes of G. If $H_{\mathrm{rat}} \subset \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is the kernel of this action, then 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 [33, §7.1].

Let $H(\underline{C}) \subset (\mathbb{Z}/m\mathbb{Z})^\times$ be the stabilizer of $\underline{C}$ under this action, i.e. the subgroup of $s \in (\mathbb{Z}/m\mathbb{Z})^\times$ such that $C_i^s = C_i$ 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 $H_{\mathrm{wkrat}}(\underline{C})$ denote the subgroup of $s \in (\mathbb{Z}/m\mathbb{Z})^\times$ such that there exists $\phi \in \mathrm{Aut}(G)$ with $\phi(\underline{C}) = \underline{C}^s$. 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

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

Proposition 5.1 (Weak rigidity-weak rationality (WRWR))**.** *Let G be a group with trivial center. Let $\underline{g} = (g_1, \dots, g_n)$ be a generating tuple for G and let $\underline{C} = (C_1, \dots, C_n)$, where C_i is the conjugacy class of g_i. Suppose that $\underline{C}$ is weakly rigid. 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 $\underline{C}$. The curve X together with the subgroup $G \subset \mathrm{Aut}(X)$ is unique up to (nonunique) isomorphism.

(b) *The curve X can be defined over its field of moduli which is equal to the field of weak rationality $F_{\mathrm{wkrat}}(\underline{C})$.*

(c) *There is a canonical bijection between the* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-orbits of* X *and the orbits of* $\underline{C}$.
(d) *There is a (unique) minimial field of definition* K *for* (X, G). *We have* $F_{\mathrm{wkrat}}(\underline{C}) \subset K$ *and the group* $\mathrm{Gal}(K/F_{\mathrm{wkrat}})$ *embeds into the stabilizer of* $\underline{C}$ *by the group* $\mathrm{Out}(G)$.

Proof. The proof can be extracted from work of Volklein [49, Remark 3.9, Proposition 9.2(b)].
[♠♠ **TO DO** : Write out proof. Maybe not here, but in some other document for our reference.]
□

Remark 5.2. [♠♠ **TO DO** : What are the field of definition of the branch points of the map $f : X \to X/G$? The ramification divisor of f itself?]

Remark 5.3. [♠♠ **TO DO** : Insert remark here about the consequence that only $\mathrm{PSL}_2(\mathbb{F}_q)$ with $[\mathbb{F}_q : \mathbb{F}_p] \leq 3$ can occur as the Galois group of a Wolfart map $X \to \mathbb{P}^1$ with $(X, \mathrm{Aut}(X))$ defined over $\mathbb{Q}$.]

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 $x \in \mathbb{F}_q^* \backslash \{1\}$, 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 $x \in \mathbb{F}_q^* \backslash \{1\}$ where we identify x with x^{-1}. The set of *nonsplit* conjugacy classes are in bijection with equivalence classes $[y]$ with $y \in (\mathbb{F}_{q^2}^* \setminus \mathbb{F}_q)/\mathbb{F}_q^*$ where we identify y and y^q.

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 $\mathrm{tr}(\pm g) = \{\mathrm{tr}(g), -\mathrm{tr}(g)\} \subset \mathbb{F}_q$ 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.

We now describe the outer automorphism group $\mathrm{Out}(\mathrm{PSL}_2(\mathbb{F}_q))$ (see e.g. Suzuki [42]). 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 $\mathrm{PSL}_2(\mathbb{F}_{q^2})$. 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 $\sigma(g) = g^p$, 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 s. Then the field of rationality of the conjugacy class C of g is*

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

The field of weak rationality of C is

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

where $\mathrm{Frob}_p \in \mathrm{Gal}(\mathbb{Q}(\lambda_s)/\mathbb{Q})$ *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 $\pm g \in \mathrm{PSL}_2(\mathbb{F}_q)$. 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 is conjugate $U(su)$. 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 field of rationality is $\mathbb{Q}(\sqrt{p^*})$.

Next we consider semisimple conjugacy classes. By the trace map, these classes are in bijection with $\lambda \in \mathbb{F}_q \setminus \{\pm 2\}$. The induced action on the set of traces is given by $\lambda = t + 1/t \mapsto t^m + 1/t^m$ for $m \in (\mathbb{Z}/s\mathbb{Z})^\times$ where $t + 1/t = \lambda$ and t is a primitive sth root of unity. From this description, we see that the stabilizer of λ is $\langle -1 \rangle \subset (\mathbb{Z}/s\mathbb{Z})^\times$. The result then follows for $\mathrm{SL}_2(\mathbb{F}_q)$.

For $\mathrm{PSL}_2(\mathbb{F}_q)$, we may assume that p is odd. We then have instead an action on traces $\pm\lambda$. If s is odd then $\pm g$ also has order s and the stabilizer is again $\langle -1 \rangle \subset (\mathbb{Z}/s\mathbb{Z})^\times$. If s is even, then $\pm g$ has order $s/2$; since then $t^{s/2} = -1$, we see that the stabilizer of $\pm\lambda$ is $\langle -1, s/2 + 1 \rangle \subset (\mathbb{Z}/s\mathbb{Z})^\times$ with fixed field $\mathbb{Q}(\lambda_{s/2})$, as claimed.

A similar analysis yields the field of weak rationality, where here if C is semisimple we have the stabilizing automorphism σ which has $\sigma(C) = C^p$, whereas if C is unipotent then τ identifies the two unipotent conjugacy classes. □

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

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

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 $\langle -1 \rangle \subset (\mathbb{Z}/(m/p)\mathbb{Z})^\times$. The corresponding elements of $\mathrm{PSL}_2(\mathbb{F}_q)$ for q odd have orders $(q+1)/2, (q-1)/2$ but now $\mathrm{lcm}((q+1)/2, (q-1)/2) = (q^2-1)/2$ so the result again holds. □

[♠♠ **TO DO** : In §5, you say that according to §7.1 of Serre, this field of rationality is also the field obtained by adjoining to $\mathbb{Q}$ the values of the character table. I couldn't find this exact statement. Anyway, something is wrong with either this remark or the above corollary. Already the character table of $\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$ for example has values in $\mathbb{Q}(\sqrt{5})$, whereas the above corollary gives its field of rationality as $\mathbb{Q}(\sqrt{5}, \lambda_{12}) = \mathbb{Q}(\sqrt{5}, \sqrt{3})$. I don't think it's just a factor of 2 off...]

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

$$F_{\mathrm{rat}}(C) = \begin{cases} \mathbb{Q}(\lambda_s), & \text{if } g \text{ is split semisimple;} \\ \mathbb{Q}(\zeta_s)^{\langle \mathrm{Frob}_q \rangle}, & \text{if } g \text{ is nonsplit semisimple;} \\ \mathbb{Q}, & \text{if } g \text{ is unipotent} \end{cases}$$

where $\mathrm{Frob}_q = \mathrm{Frob}_p^r \in \mathrm{Gal}(\mathbb{Q}(\zeta_s)/\mathbb{Q})$ denotes the Frobenius associated to q. The field of weak rationality of C is

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

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 $x \in \mathbb{F}_q^* \setminus \{1\}$ then $x \mapsto x^s$ for $s \in (\mathbb{Z}/a\mathbb{Z})^\times$ and the stabilizer is $\langle -1 \rangle \subset (\mathbb{Z}/a\mathbb{Z})^\times$. 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 $y \mapsto y^m$ for $m \in (\mathbb{Z}/s\mathbb{Z})^\times$ and the stabilizer is $\langle q \rangle \subset (\mathbb{Z}/s\mathbb{Z})^\times$.

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 of weak rigidity for triples (§5) can be applied to the groups $\mathrm{PSL}_2(\mathbb{F}_q)$ (and consequently $\mathrm{PGL}_2(\mathbb{F}_q)$) using celebrated work of Macbeath [22], which we recall in this section. See also [20], who gives an exposition of Macbeath's work in our context.

We begin by considering triples $\underline{g} = (g_1, g_2, g_3)$ with $g_i \in \mathrm{SL}_2(\mathbb{F}_q)$, so $g_1 g_2 g_3 = 1$. For $\underline{t} = \underline{t} \in \mathbb{F}_q^3$, 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 [22, Theorem 1])**.** *Let $\underline{t} \in \mathbb{F}_q^3$. Then $T(\underline{t})$ is nonempty.*

Since the trace of an element of $\mathrm{SL}_2(\mathbb{F}_q)$ determines its order, to each $\mathbb{F}_q$-triple $\underline{t}$ we associate an *order triple* (a, b, c) such that for any triple $\underline{g} \in T(\underline{t})$, the order of $\pm g_1 \in \mathrm{PSL}_2(\mathbb{F}_q)$ is a, the order of $\pm g_2$ is b and the order of $\pm g_3$ is c.

Without loss of generality, as in the definition of the triangle group (1.2) we restrict to order triples (a, b, c) with $a \leq b \leq c$.

An $\mathbb{F}_q$-triple $\underline{t}$ is *commutative* if there exists $\underline{g} \in T(\underline{t})$ such that the group $\pm\langle g_1, g_2, g_3 \rangle \subset \mathrm{PSL}_2(\mathbb{F}_q)$ is commutative. 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 [22, Corollary 1, p. 21], i.e. if

$$t_1^2 + t_2^2 + t_3^2 - t_1 t_2 t_3 - 4 = 0.$$

For the sake of simplicity we will content ourselves with the following necessary condition for commutativity in terms of the order triple (a, b, c).

Lemma 7.2. *Let g and h be commuting elements of a finite group. Let a, b and c be the orders of g, h and gh, respectively. Then*

$$\frac{\operatorname{lcm}(a,b)}{\gcd(a,b)} \mid c \mid \operatorname{lcm}(a,b). \tag{7.3}$$

An $\mathbb{F}_q$-triple $\underline{t}$ is *exceptional* if the associated sequence (a,b,c) of orders is 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 subgroup of $\mathrm{PSL}_2(\mathbb{F}_q)$ is *projective* if it is conjugate to a subgroup of the form $\mathrm{PSL}_2(k)$ or $\mathrm{PGL}_2(k)$ for $k \subset \mathbb{F}_q$ a subfield. A triple $\underline{t}$ is *projective* if for any $\underline{g} = (g_1,g_2,g_3) \in T(\underline{t})$, the subgroup $\pm\langle g_1,g_2,g_3\rangle \subset \mathrm{PSL}_2(\mathbb{F}_q)$ is projective.

Proposition 7.5 ([22, Theorem 4])**.** *Every $\mathbb{F}_q$-triple $\underline{t}$ is either exceptional, commutative or projective.*

Proposition 7.6 ([22, Theorem 3, p. 28])**.** *Let $\underline{t}$ be a projective $\mathbb{F}_q$-triple.*

(a) *For any $\underline{g} \in T(\underline{t})$, the group $\pm\langle g_1,g_2,g_3\rangle$ 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 $\underline{g}$).*
(b) *The number of orbits of $\mathrm{PSL}_2(\mathbb{F}_q)$ on $T(\underline{t})$ is 2 or 1 according as p is odd or $p = 2$.*
(c) *For all $\underline{g},\underline{g}' \in T(\underline{t})$, there exists $m \in \mathrm{SL}_2(\overline{\mathbb{F}}_q)$ such that $m^{-1}\underline{g}m = \underline{g}'$.*

We say that a conjugacy class $\underline{C}$ with associated trace triple $\underline{t}$ is *of* PSL_2*-type* (resp. PGL_2-type) if there exists $\underline{g} \in T(\underline{t})$ such that $\pm\langle g_1,g_2,g_3\rangle$ is conjugate to $\mathrm{PSL}_2(k)$ (resp. $\mathrm{PGL}_2(k_0)$); by Proposition 7.6(a), the type is independent of the choice of $\underline{g}$ and so depends only on $\underline{t}$. If a triple $\underline{t}$ is of PGL_2-type, then necessarily it is *irregular*, which is defined as follows: the subfield $\mathbb{F}_p(\underline{t})$ is a quadratic extension of a subfield k with $[\mathbb{F}_p(\underline{t}):k] = 2$, $t_i \in k$ for some i and t_j for $j \neq i$ are zero or squareroots in $\mathbb{F}_p(\underline{t})$ of nonsquares in k.

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 define $T(\pm\underline{t})$ to be the set of triples $\pm g = (\pm g_1,\pm g_2,\pm g_3)$ with $\pm g_i \in \mathrm{PSL}_2(\mathbb{F}_q)$ such that $\pm g_1g_2g_3 = \pm 1$ and $\operatorname{tr}(\pm g_i) = \pm t_i$ for $i = 1,2,3$. We say that a trace triple $\pm\underline{t}$ is *commutative* if there exists $\pm\underline{g} T(\pm\underline{t})$ such that $\pm\langle g_1,g_2,g_3\rangle$ is commutative, and analogously define *exceptional* and *projective* (as well as the *type*).

Corollary 7.7. *Let $\underline{C}$ be a conjugacy class triple in $\mathrm{PSL}_2(\mathbb{F}_q)$ with $\Sigma(\underline{C}) \neq \emptyset$. Let $\pm\underline{t}$ be the associated trace triple and suppose that $\mathbb{F}_q = \mathbb{F}_p(\underline{t})$. Then $\underline{C}$ is weakly rigid.*

Moreover, if p is odd and $\underline{C}$ is of PSL_2-type, then the action of $\mathrm{Inn}(\mathrm{PSL}_2(\mathbb{F}_q))$ on $\Sigma(\underline{C})$ has exactly two orbits; otherwise, $\underline{C}$ is in fact rigid.

Proof. If $p = 2$, then $\mathrm{PSL}_2(\mathbb{F}_q) = \mathrm{SL}_2(\mathbb{F}_q)$ and the corollary is a restatement of Proposition 7.6(b).

So suppose that p is odd and first suppose that $\underline{C}$ is of PSL_2-type. Let $\pm\underline{g},\pm\underline{g}' \in \Sigma(\underline{C})$. Choose signs appropriately so that $\underline{g},\underline{g}'$ are triples in $\mathrm{SL}_2(\mathbb{F}_q)$ (and such that $\operatorname{tr} g_i = \operatorname{tr} g_i'$ for

$i = 1, 2, 3$). Then by Proposition 7.6(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 $\mathrm{PSL}_2(\mathbb{F}_q)$ and the elements of $\pm\underline{g}'$ lie in $\mathrm{PSL}_2(\mathbb{F}_q)$, it follows that conjugation by m induces an automorphism of $\mathrm{PSL}_2(\mathbb{F}_q)$, so $\underline{C}$ is weakly rigid. Since $\mathrm{Inn}(\mathrm{PSL}_2(\mathbb{F}_q)) = \mathrm{Inn}(\mathrm{SL}_2(\mathbb{F}_q))$, from Proposition 7.6(b), we see that there are two orbits of $\mathrm{PSL}_2(\mathbb{F}_q)$ acting by conjugation on $\Sigma(\underline{C})$. It is not hard to see that $\tau \in \mathrm{Out}(\mathrm{PSL}_2(\mathbb{F}_q))$ 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.

The same argument applies if $\underline{C}$ is of PGL_2-type. In this case, conjugation by m induces an automorphism of $\mathrm{PGL}_2(\mathbb{F}_{\sqrt{q}}) \subset \mathrm{PSL}_2(\mathbb{F}_q)$. But now $\mathrm{Out}(\mathrm{PGL}_2(\mathbb{F}_{\sqrt{q}})) = \langle\sigma\rangle$ and from the analysis following (6.1), if $\mathbb{F}_q = \mathbb{F}_p(\underline{t})$ then the stabilizer of $\langle\sigma\rangle$ acting on $\underline{t}$ is trivial, and hence the orbits must be already identified by conjugation by $\mathrm{PGL}_2(\mathbb{F}_q)$. □

We are now in a position to prove Theorem A.

Proof of Theorem A. 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). First suppose that $G \cong \mathrm{PSL}_2(\mathbb{F}_q)$ with q a power of a prime p. Let $\pm\underline{g} = (\pm g_1, \pm g_2, \pm g_3)$ be the images in G of the monodromy at the three ramification points. Choosing signs appropriately, lift $\pm\underline{g}$ to a triple $\underline{g}$ with $g_i \in \mathrm{SL}_2(\mathbb{F}_q)$. Let $\underline{t} = \mathrm{tr}\,\underline{g}$. Then by Proposition 7.6(a), we have $\mathbb{F}_q = \mathbb{F}_p(\underline{t})$, and this is independent of the choice of lift $\underline{g}$. Now $r = \log_p q$ 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 $\mathrm{Gal}(E(2a, 2b, 2c)/\mathbb{Q})$, as claimed.

Now let $\underline{C}$ be the corresponding conjugacy class triple in G. By Corollary 7.7, the triple $\underline{C}$ is weakly rigid and so Proposition 5.1 (WRWR) applies. By Proposition 5.1(b), the field of moduli of X is equal to the field $F_{\mathrm{wkrat}}(\underline{C})$ of weak rationality of $\underline{C}$, and it follows from Lemma 6.2, that $F_{\mathrm{wkrat}}(\underline{C})$ is equal to $E(a, b, c; p)$, the fixed field under Frob_p of the compositum of $\mathbb{Q}(\lambda_s)$ for $s \in \{a, b, c\}$ with $p \nmid s$. Finally, part (d) of this Proposition and Corollary 7.7 yields that the minimal field of definition K of $(X, \mathrm{Aut}(X))$ satisfies $[K : E(a, b, c; p)] = 2$ when p is odd and $K = E(a, b, c; p)$ if $p = 2$.

The same reasoning applies in the case $G \cong \mathrm{PGL}_2(\mathbb{F}_q)$, where now we apply Lemma 6.2 and find that the cover is in fact rigid, so $K = E(a, b, c; p)$. □

8. Fields of definition

In this section, we combine the results of the sections §4–7 in the cases relevant to our application.

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 $1/a + 1/b + 1/c - 1 < 0$. Let $\mathfrak{P}$ be a prime of the field

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

and let $\mathfrak{p}$ be the prime of

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

below $\mathfrak{P}$. Suppose that $\mathfrak{P} \nmid 2abc$. Then by Proposition 4.20, 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

$$\mathrm{PSL}_2(\mathbb{F}_\mathfrak{P}) \cap \mathrm{PGL}_2(\mathbb{F}_\mathfrak{p}) = \begin{cases} \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p}), & \text{if } \mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{p}; \\ \mathrm{PGL}_2(\mathbb{F}_\mathfrak{p}), & \text{if } [\mathbb{F}_\mathfrak{P} : \mathbb{F}_\mathfrak{p}] = 2. \end{cases} \tag{8.1}$$

We note from (4.8) 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 $X = X(a, b, c; \mathfrak{p}) = \overline{\Delta}(a, b, c; \mathfrak{p})\backslash\mathfrak{H}$ is a Wolfart curve by construction. We now prove Theorem B, which we restate as the following proposition.

Proposition 8.2. *If (a, b, c) is maximal and not exceptional and $\pm\underline{t}$ is noncommutative, then $\mathrm{Aut}(X(a, b, c; \mathfrak{p})) \cong \mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$ or $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{p})$ according as in* (8.1).

Remark 8.3. We recall that $\pm\underline{t}$ is noncommutative for example if the condition (7.3) is violated and that (a, b, c) is not exceptional if it is not one in the list (7.4).

Proof. First, by Proposition 7.5 we conclude that the triple $\underline{g}$ is projective. Then, by Proposition 7.6(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 (8.1) 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

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

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 $t_1t_2t_3 \in k$, so

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

a contradiction.

Finally, by the results of Section 2, since (a, b, c) is maximal we have

$$\mathrm{Aut}(X(a, b, c; \mathfrak{p})) \cong \frac{N(\overline{\Delta}(a, b, c; \mathfrak{p}))}{\overline{\Delta}(a, b, c; \mathfrak{p})} = \frac{N(\overline{\Delta}(a, b, c))}{\overline{\Delta}(a, b, c; \mathfrak{p})} \cong \frac{\overline{\Delta}(a, b, c)}{\overline{\Delta}(a, b, c; \mathfrak{p})}$$

and the result follows. □

Corollary 8.4. *We have*

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

9. Examples

Example 9.1. Finitely many families of curves $X(a,b,c;p)$ correspond to Shimura curves, where the groups $\Delta(a,b,c)$ are arithmetic, associated to unit groups of maximal orders in quaternion algebras over totally real fields. [♠♠ **TO DO** : Cite Takeuchi. Check the canonical models of these Shimura curves.]

[♠♠ **TO DO** : Galois descent for triangle Shimura curves which I used and that $\mathrm{PSL}_2(\mathbb{F}_8)$ example guy.]

Example 9.2. Suppose that the triple (a,b,c) has $p \mid abc$. There are two unipotent conjugacy classes of order p, [♠♠ **TO DO** : Analysis here].

As a special case, we consider the case $(a,b,c) = (2,3,p)$ with $p \geq 7$. There are two unipotent conjugacy classes which are in the same $\mathcal{G}_{\mathbb{Q}}$-orbit (taking the ith power moves from quadratic residues to nonresidues) and so the field of rationality of such a conjugacy class is the quadratic subfield $K = \mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$, 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 $F(\underline{C}) = K$. As above, the outer automorphism τ interchanges the two unipotent conjugacy classes, so $F_{\mathrm{wkrat}}(\underline{C}) = \mathbb{Q}$. Hence we obtain a $\mathrm{PSL}_2(\mathbb{F}_p)$-curve $X(2,3,p;p)$ which is defined (noncanonically) over $\mathbb{Q}$ and with $(X(2,3,p;p), \mathrm{Aut}(X))$ defined over K.

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 $X(p)$ [26] and that the minimal field of definition of $(X(p), \mathrm{Aut}(X(p)))$ is K. In particular, we note that this interpretation is quite different than the moduli interpretation of "naïve" level p-structure [17] for $X(p)$ which gives a model of $\mathbb{Q}(\zeta_p)$. Indeed, this model is used by Shih [35] to show that $\mathrm{PSL}_2(\mathbb{F}_p)$ occurs regularly as a Galois group over K [♠♠ **TO DO** : And do we want to mention that by twisting he gets it as a Galois group over $\mathbb{Q}$ subject to congruence conditions on p?]

As further example, we mention the case $p = 7$ is the Klein quartic curve $X(2,3,7;7) = X(7)$ of genus 3 given by the equation $x^3y + y^3z + x^3z = 0$ in $\mathbb{P}^2$ (see Elkies [11] for further detail).

Example 9.3. Consider the case of (odd) Hecke triangle groups treated by Lang, Lim, and Tan [19], the groups with $\overline{\Delta}(a,b,c) = \overline{\Delta}(2,q,\infty)$ with q odd. Then we have

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

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 $\mathbb{F}_p(t) = \mathbb{F}_p(t^2)$.

Example 9.4. Consider the case $(a, b, c) = (2, 3, 7)$ with $p = 2$. Then $G = \mathrm{PSL}_2(\mathbb{F}_8)$ and $X = X(2, 3, 7; 2)$ is the Fricke-Macbeath curve [21] of genus 7, the second smallest genus for a curve uniformized by a subgroup of the Hurwitz group $\Delta(2, 3, 7)$. The curve X has field of moduli equal to $\mathbb{Q}$ and the minimal field of definition of (X, G) is $\mathbb{Q}(\lambda_7)$. Macbeath shows that the Jacobian J of X is isogenous to E^7, where E is a non-CM elliptic curve with rational j-invariant.

We could equally well consider the curves $X = X(2, 3, p; 2)$ for $p \geq 7$ prime, which can be defined over $\mathbb{Q}$. If r is the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$ then $\mathrm{Aut}(X) \cong \mathrm{PSL}_2(\mathbb{F}_{p^r})$ and $(X, \mathrm{Aut}(X))$ is defined over $\mathbb{Q}(\lambda_p)^+$. Unfortunately, already $p = 11$ gives a curve of genus 1241 so these curves are not amenable to explicit computations as in the case $p = 7$. [♠♠ **TO DO** : What about other intermediate values of p which are not prime? The case $p = 9$ is a Shimura curve...]

To give further examples, we list all $\mathrm{PSL}_2(\mathbb{F}_q)$-Wolfart curves with $a, b, c \neq \infty$ by increasing genus. Using the Hurwitz bound (Remark 2.7), which follows from (2.6), we can bound $\#G$ (equivalently q) in terms of g and then for each group G there are only finitely many triples of possible orders (a, b, c). The curves of genus $g \leq 24$ are listed in Table 9.5.

g	(a, b, c)	q
3	$(2, 3, 7)$	7
4	$(2, 5, 5)$	$4, 5$
5	$(3, 3, 5)$	$4, 5$
7	$(2, 3, 7)$	8
8	$(3, 3, 4)$	7
9	$(3, 5, 5)$	$4, 5$
10	$(2, 4, 7)$	7
10	$(2, 4, 5)$	9
13	$(5, 5, 5)$	$4, 5$
15	$(3, 4, 4)$	7
15	$(2, 3, 9)$	8
16	$(3, 3, 4)$	9
19	$(2, 5, 5)$	9
24	$(3, 4, 7)$	7

Table 9.5: $\mathrm{PSL}_2(\mathbb{F}_q)$-Wolfart curves of genus $g \leq 24$

Note there is an exceptional isomorphism $\mathrm{PSL}_2(\mathbb{F}_4) \cong \mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$. We also note that all of the curves in this table are arithmetic (Shimura curves) with the exception of the last curve, a curve of genus 24 with Galois group $\mathrm{PSL}_2(\mathbb{F}_7)$ and associated triple $(3, 4, 7)$.

Equations for these curves can be found using the methods of Streit [38].

[♠♠ **TO DO** : It might be fun to compute equations for the curves of genus 4 and 5, if they're not already known? They'd have plane models as quintics with either two or one nodes. Elkies finds these curves by finding them modulo a prime of good reduction of the curve and then

lifting p-adically, which is possible by rigidity. Or we could just make a remark about this and leave it for future work...]

Remark 9.6. [♠♠ **TO DO** : Remark about other groups G for which the G-Wolfart curves have nice properties? Like G abelian?]

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

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

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

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

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

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

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

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

[10] 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.

[11] 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.

[12] R. Fricke and F. Klein, *Vorlesungen ueber die Theorie der automorphen Funktionen*, vols. 1–2, Teubner, Leipzig, 1897, 1912.

[13] Ernesto Girondo and Jürgen Wolfart, *Conjugators of Fuchsian groups and quasiplatonic surfaces*, Quart. J. Math. **56** (2005), 525–540.

[14] Leon Greenberg, *Maximal Fuchsian groups*, Bull. Amer. Math. Soc. **69** (1963), 569–573.

[15] E. Hecke, *Über die Bestimmung Direchletscher Reihen durch ihre Funktionalgleichungen*, Math. Ann. **112** (1936), 664–699.

[16] Svetlana Katok, *Fuchsian groups*, University of Chicago Press, Chicago, 1992.

[17] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, 1985.

[18] Bernhard Köck, *Belyĭ's theorem revisited*, Beiträge Algebra Geom. **45** (2004), no. 1, 253–265.

[19] Mong-Lung Lang, Chong-Hai Lim, and Ser-Peow Tan, *Principal congruence subgroups of the Hecke groups*, J. Number Theory **85** (2000) 220–230.

[20] Ulrich Langer and Gerhard Rosenberger, *Erzeugende endlicher projektiver linearer Gruppen*, Results Math. **15** (1989), no. 1–2, 119–148.

[21] Macbeath, *On a curve of genus* 7, Proc. London Math. Soc. (3) **15** (1965), 527–542.

[22] Macbeath, *Generators of the linear fractional groups*, Number Theory (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967), Amer. Math. Soc., Providence, 14–32.

[23] Wilhelm Magnus, *Noneuclidean tesselations and their groups*, Pure and Applied Mathematics, vol. 61, Academic Press, New York, 1974.

[24] Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999.

[25] G. Margulis, *Discrete subgroups of semisimple Lie groups*, Springer, Berlin, 1991.

[26] 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.
[27] Hans Petersson, *Über die eindeutige Bestimmung und die Erweiterungsfähigkeit von gewissen Grenzkreisgruppen*, Abh. Math. Semin. Univ. Hambg. **12** (1937), no. 1, 180–199.
[28] John G. Ratcliffe, *Foundations of hyperbolic manifolds*, 2nd ed., Graduate Texts in Mathematics, vol. 149, Springer, New York, 2006.
[29] Sabine Ricker, *Symmetric Fuchsian quadrilateral groups and modular embeddings*, Quart. J. Math **53** (2002), 75–86.
[30] Paul Schmutz Schaller and Jürgen Wolfart, *Semi-arithmetic Fuchsian groups and modular embeddings*, J. London Math. Soc. (2) **61** (2000), 13–24.
[31] Jan-Christoph Schlage-Puchta and Jürgen Wolfart, *How many quasiplatonic surfaces?*, Arch. Math. (Basel) **86** (2006), no. 2, 129–132.
[32] Thomas A. Schmidt and Katherine Smith, *Galois orbits of principal congruence Hecke curves*, J. London Math. Soc. (2) **67** (2003), no. 3, 673–685.
[33] J.-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics 1, Jones and Bartlett, 1992.
[34] G.B. Shabat and V. Voevodsky, *Drawing curves over number fields*, Grothendieck Festchrift, vol. III, Birkhauser, Boston, 1990, 199–227.
[35] Kuang-yen Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann. **207** (1974), 99–120.
[36] D. Singerman, *Finitely maximal Fuchsian groups*, J. London Math. Soc. (2) **6** (1972), 29–38.
[37] Manfred Streit, *Field of definition and Galois orbits for the Macbeath-Hurwitz curves*, Arch. Math. (Basel) **74** (2000), no. 5, 342–349.
[38] Manfred Streit, *Homology, Belyĭ functions and canonical curves*, Manuscripta Math. **90** (1996), 489–509.
[39] 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`.
[40] Goro Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. (2) **85** (1967), 58–159.
[41] D. Singerman and R.I. Syddall, *Belyĭ uniformization of elliptic curves*, Bull. London Math. Soc. **139** (1997), 443–451.
[42] Michio Suzuki, *Group theory. II*, Grundlehren der Mathematischen Wissenschaften, vol. 248, Springer-Verlag, New York, 1986.
[43] Kisao Takeuchi, *On some discrete subgroups of* $\mathrm{SL}_2(\mathbb{R})$, J. Fac. Sci. Univ. Tokyo Sect. I **16** (1969), 97–100.
[44] Kisao Takuechi, *A characterization of arithmetic Fuchsian groups*, J. Math. Soc. Japan **27** (1975), no. 4, 600–612.
[45] Kisao Takeuchi, *Arithmetic triangle groups*, J. Math. Soc. Japan **29** (1977), no. 1, 91–106.
[46] Kisao Takeuchi, *Commensurability classes of arithmetic triangle groups*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **24** (1977), no. 1, 201–212.
[47] 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.
[48] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980.
[49] Helmut Völklein, *Groups as Galois groups. An introduction*, Cambridge Studies in Advanced Mathematics, vol. 53, Cambridge University Press, Cambridge, 1996.
[50] 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.
[51] 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.

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