ALGEBRAIC CURVES UNIFORMIZED BY CONGRUENCE SUBGROUPS OF TRIANGLE GROUPS

PETE L. CLARK AND JOHN VOIGHT

Abstract. We define congruence subgroups of hyperbolic triangle groups. These groups include the classical congruence subgroups of 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 in many cases thereby explicitly realize the Galois group $\text{PSL}_2(\mathbb{F}_q)$ regularly over an explicitly given number field.

The rich geometric and arithmetic theory of classical modular curves, quotients of the upper half-plane by congruence subgroups of SL$_2(\mathbb{Z})$, has intrigued mathematicians since the nineteenth century. One can see these curves as special cases of several distinguished classes of curves. Fricke and Klein [8] investigated curves arising from subgroups which we now recognize among the class of arithmetic Fuchsian groups. Later, Hecke [10] investigated his triangle groups, generalizing the presentation of SL$_2(\mathbb{Z})$ as the free product of the groups $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$. More recently, higher-dimensional generalizations known as Shimura varieties have seen further fruitful number-theoretical investigation. In this paper, we introduce a class of curves arising from congruence subgroups of triangle groups; these curves share many appealing properties in common with modular curves, despite the fact that their uniformizing Fuchsian groups are not in general arithmetic.

To motivate the definition of this class of curves, we consider again the classical modular curves. Let $p$ be prime and let $X(p)_{\mathbb{C}} = \Gamma(p)\backslash \mathcal{H}$ be the modular curve which parametrizes (generalized) elliptic curves with full level $p$-structure. Then there is a model $X(p) = X(p)_{\mathbb{Q}}$ for $X(p)_{\mathbb{C}}$ defined over $\mathbb{Q}$ (see Example 3.5), and there exists a subgroup $G \subset \text{Aut}(X(p))$ with $G \cong \text{PSL}_2(\mathbb{F}_p)$ such that the natural map $j : X(p) \to X(p)/G \cong \mathbb{P}^1$ 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 $G \subset \text{Aut}(X)$ such that $G \cong \text{PSL}_2(\mathbb{F}_q)$ 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 an appealing class to study for several reasons. On the one hand, Belyi [1] 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 Belyi map, if and only if $X$ can be defined over the algebraic closure $\mathbb{Q}$ 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 Belyi map (Remark 2.3). We call a Galois Belyi 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 [34]. Wolfart called such curves curves with many automorphisms because they are also characterized as being the locus on the moduli space $M_g(\mathbb{C})$ of curves of genus $g$ at which the function $[C] \mapsto \# \text{Aut}(C)$ attains a strict local maximum.

Date: August 25, 2009.
For example, the Hurwitz curves, those curves with maximal automorphism group \# Aut(X) = 84(g−1) for their genus g, are Wolfart curves, as are the Fermat curves \( x^n + y^n = z^n \) for \( n \geq 3 \). (See below for an alternative equivalent characterizations of Wolfart curves.)

We now proceed to investigate some basic arithmetic properties of Wolfart curves. For a curve \( X \) defined over \( \mathbb{C} \), the field of moduli of \( X \) is the field of constants of any \( \overline{\mathbb{C}} \)-model of \( X \). We instead consider the field of moduli of the pair \( (X,F) \), where \( F \) is a field of constants of any \( \overline{\mathbb{F}}_q \)-model of \( X \). 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, and indeed a Wolfart curve can be defined over its field of moduli (Lemma 3.3).

Even if a curve \( X \) can be defined over its field of moduli, this model need not be unique. We instead consider the field of moduli of the pair \( (X,\text{Aut}(X)) \). We observe (Remark 3.6) that for any number field \( K \) over its field of moduli (Lemma 3.3).

To state our first result we use the following notation. Let \( a, b, c \in \mathbb{Z}_{>0} \) and let \( m = \text{lcm}(a,b,c) \). We have an injective map
\[
\iota : (\mathbb{Z}/m\mathbb{Z})^\times \hookrightarrow (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times \times (\mathbb{Z}/c\mathbb{Z})^\times.
\]
Define
\[
\epsilon_a = (-1,1,1), \quad \epsilon_b = (1,-1,1), \quad \epsilon_c = (1,1,-1) \in (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times \times (\mathbb{Z}/c\mathbb{Z})^\times
\]
and let
\[
H(a,b,c) = (\mathbb{Z}/m\mathbb{Z})^\times \cap \iota^{-1}\langle \epsilon_a, \epsilon_b, \epsilon_c \rangle.
\]
For a prime number \( p \) with \( \gcd(p,abc) = 1 \), let
\[
H(a,b,c;p) = (\mathbb{Z}/m\mathbb{Z})^\times \cap \iota^{-1}\langle \epsilon_a, \epsilon_b, \epsilon_c, (p,p,p) \rangle.
\]
Let
\[
F(a,b,c) = \mathbb{Q}(\zeta_m)^{H(a,b,c)} = \mathbb{Q}(\zeta_a, \zeta_b, \zeta_c)^{H(a,b,c)}
\]
and \( F(a,b,c;p) = \mathbb{Q}(\zeta_a, \zeta_b, \zeta_c)^{H(a,b,c;p)} \), where we have the canonical identification \( \text{Gal}(\mathbb{Z}/m\mathbb{Z}) \cong (\mathbb{Z}/m\mathbb{Z})^\times \). Our first result is as follows.

**Theorem A.** Let \( X \) be a curve of genus \( g \geq 2 \) and let \( f : X \to \mathbb{P}^1 \) be a \( \text{PSL}_2(\mathbb{F}_q) \)-Wolfart map with ramification indices \( (a,b,c) \). Then:

(a) We have \( q = p^r \), where \( r \) is the order of \( p \) in \( (\mathbb{Z}/m\mathbb{Z})^\times / H(a,b,c) \).

(b) The field of moduli of \( X \) is the real abelian number field \( F(a,b,c;p) \).

(c) The minimal field of definition \( K \) of \( (X,\text{Aut}(X)) \) contains \( F(a,b,c) \), and we have \([K : F(a,b,c)] \leq 2\).

\[\text{TO DO : Relate to result of Streit [24] who does (2,3,7).}\]

To prove Theorem A, we use a variant of the rigidity and rationality results which arise in the study of the inverse Galois problem [16, 33] and apply them to the groups \( \text{PSL}_2(\mathbb{F}_q) \). We use the classification of subgroups of \( \text{PSL}_2(\mathbb{F}_q) \) generated by two elements provided by Macbeath [14].

Wolfart curves of genus \( g \geq 2 \) admit a further description as compact Riemann surfaces of the form \( \Gamma \backslash \mathcal{H} \), where \( \Gamma \) is a torsion-free finite-index normal subgroup of a hyperbolic triangle group \( \Delta(a,b,c) \) (see Section 1 for definitions and Proposition
2.4 for this equivalence). In our analysis, we construct such normal subgroups \( \Gamma \subset \Delta(a,b,c) \) with quotient \( \text{PSL}_2(\mathbb{F}_p) \) as follows. For an integer \( k \in \mathbb{Z}_{>0} \), let \( \zeta_k \) be a primitive \( k \)th root of unity and let \( \lambda_k = \zeta_{2k} + 1/\zeta_{2k} = 2 \cos(\pi/k) \). By convention, we let \( \lambda_\infty = 1 \). To the triple \( a,b,c \) we associate the totally real field

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

By a prime of \( F \) we mean a nonzero prime ideal of the ring of integers of \( F \). For a prime \( p \) of \( F \), let \( \mathbb{F}_p \) denote its residue class field.

Our main theorem is as follows.

**Theorem B.** For every triple \( a,b,c \in \mathbb{Z}_{\geq 2} \cup \{\infty\} \) and every prime \( p \) of \( F(a,b,c) \), there is a \( \text{PSL}_2(\mathbb{F}_p) \)-Wolfart curve \( X = X(a,b,c;p) \) with field of moduli \( F(a,b,c;p) \) and such that \((X,\text{Aut}(X))\) has minimal field of definition \( K \supseteq \mathbb{Q} \). The curve \( X \) is unique up to (nonunique) isomorphism [\( \spadesuit \) TO DO : Over \( \overline{\mathbb{Q}} \)]

\[
\left[ \spadesuit \spadesuit \text{ TO DO : Cite other papers: Lang, Lim, and Tan} \right]
\]

In particular, the cover \( X(a,b,c;p) \to X(a,b,c) \) realizes the group \( \text{PSL}_2(\mathbb{F}_p) \) regularly over the field \( K \). [\( \spadesuit \spadesuit \text{ TO DO : In certain rigid cases, we get better results...} \)

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 unramified at a unique real place. A deep theorem of Margulis [\( \spadesuit \spadesuit \text{ TO DO : cite Margulis} \)] gives a necessary and sufficient condition for a group to be arithmetic [\( \spadesuit \spadesuit \text{ TO DO : In terms of the Hecke algebra, but really its about the commensurator being of infinite superindex} \)]. Only finitely many of the groups \( \Delta(a,b,c) \) are arithmetic by work of Takeuchi [30]. In these cases, the curves \( X(a,b,c;p) \) are Shimura curves and a canonical model was given by Shimura [25] and Deligne [6]. 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 the one associated to the congruence subgroup \( \Gamma(p) \subset \text{PSL}_2(\mathbb{Z}) \). In fact, the same can be seen for the curves \( X(2,3,p;p) \) for \( p \geq 7 \) (see Example 9.3). Several other arithmetic families have seen more detailed study, most notably the family \( X(2,3,7;p) \) of Hurwitz curves. In general, however, the groups \( \Delta(a,b,c;p) \) are not arithmetic; nevertheless we believe that these curves carry a rich geometry which is worthy of study.

The paper is organized as follows. In Sections 1 and 2, we introduce the triangle groups \( \Delta(a,b,c) \) and the theory of Wolfart curves and Belyš maps. In Section 3, we reinterpret a construction of Takeuchi which realizes the curves associated to triangle groups as subvarieties of quaternionic Shimura varieties and define their congruence subgroups. After reviewing Macbeath’s theory of subgroups of \( \text{PSL}_2(\mathbb{F}_q) \) in Section 4, we introduce in Section 5 the theory of weak rigidity which implies the relevant Galois descent. In Section 6, we discuss the field of definition of congruence triangle curves and then in Section 7 we prove that congruence triangle curves realize the Galois group \( \text{PSL}_2(\mathbb{F}_q) \) regularly. Finally, in Section 8 we conclude with some explicit examples of triangle Shimura curves and pose some final questions.
1. Triangle Groups

In this section, we review the basic theory of triangle groups. We refer to Magnus [15, Chapter II] and Ratcliffe [19, §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

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

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 triangle group $\Delta = \Delta(a, b, c)$ to be the (abstract) group generated by $\gamma_a, \gamma_b, \gamma_c$ subject to the relations

$$(1.1) \quad \gamma_a^a = \gamma_b^b = \gamma_c^c = 1;$$

by convention we let $\gamma^\infty = 1$. We analogously classify the groups $\Delta(a, b, c)$ by the triple $(a, b, c)$.

**Example 1.2.** The spherical triangle groups are all finite groups: indeed, we have $\Delta(2, 2, c) \cong D_{2c}$, the dihedral group of order $2c$, $\Delta(2, 3, 3) \cong A_4$, $\Delta(2, 3, 4) \cong S_4$, and $\Delta(2, 3, 5) \cong S_5$.

**Example 1.3.** The group $\Delta(a, b, \infty)$ is the free product of $\mathbb{Z}/a\mathbb{Z}$ and $\mathbb{Z}/b\mathbb{Z}$.

We have an exact sequence

$$1 \rightarrow [\Delta, \Delta] \rightarrow \Delta \rightarrow \Delta^{ab} \rightarrow 1;$$

we identify $\Delta^{ab} = \Delta/[\Delta, \Delta]$ as the quotient of $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ by the cyclic subgroup generated by $(c, c)$. Thus, the group $\Delta$ is perfect (i.e. $\Delta^{ab} = \{1\}$) if and only if $a, b, c$ are relatively prime in pairs. We have $[\Delta(2, 2, \infty), \Delta(2, 2, \infty)] \cong \mathbb{Z}$, whereas for the other Euclidean triples we have $[\Delta, \Delta] \cong \mathbb{Z}^2$ [15, § II.4]. In particular, the Euclidean triangle groups are infinite, nonabelian but solvable.

The triangle groups $\Delta(a, b, c)$ with $(a, b, c) \neq (2, 2, \infty)$ have the following geometric interpretation. Associated to $\Delta$ is a triangle $T$ with angles $\pi/a$, $\pi/b$, and $\pi/c$ 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 $\tau_a, \tau_b, \tau_c$ in the three sides of the triangle $T$ is a discrete group with $T$ itself as a fundamental domain. The subgroup of orientation-preserving isometries is generated by the elements $\gamma_a = \tau_a \tau_b$, $\gamma_b = \tau_b \tau_c$, and $\gamma_c = \tau_c \tau_a$ and these elements generate a group isomorphic to $\Delta(a, b, c)$. A fundamental domain for $\Delta(a, b, c)$ is obtained by reflecting the triangle $T$ in one of its sides. The sides of this fundamental domain are identified by the elements $\gamma_a, \gamma_b$, and $\gamma_c$, and consequently the quotient space is a Riemann surface of genus zero. This surface is compact if and only if $c < \infty$.

From now on, suppose $(a, b, c)$ is hyperbolic. Then $\Delta = \Delta(a, b, c) \subset \text{PSL}_2(\mathbb{R})$ is a Fuchsian group acting discretely on the (completed) upper half-plane $\mathbb{H}^{(*)}$; we write $X(a, b, c) = \Delta(a, b, c) \backslash \mathbb{H}^{(*)} \cong \mathbb{H}_c$ for the quotient space.

By the preceding geometric construction, we have a natural embedding

$$\Delta(a, b, c) \hookrightarrow \text{PSL}_2(\mathbb{R}).$$
and this embedding is unique up to conjugacy in $\operatorname{PSL}_2(\mathbb{R})$ since any two hyperbolic triangles with the same angles are isometric. We lift this embedding to $\operatorname{SL}_2(\mathbb{R})$ as follows. Define the group $\Delta(a, b, c)$ to be the group generated by elements $-1, \tilde{\gamma}_a, \tilde{\gamma}_b, \tilde{\gamma}_c$ with $-1$ central in $\Delta(a, b, c)$ subject to the relations $(-1)^2 = 1$ and

$$\tilde{\gamma}_a = \tilde{\gamma}_b = \tilde{\gamma}_c = \tilde{\gamma}_a \tilde{\gamma}_b \tilde{\gamma}_c = -1.$$  

Note that $\tilde{\Delta}(a, b, c)/\langle \pm 1 \rangle \cong \Delta(a, b, c)$.

Further, suppose that $b < \infty$: this excludes the cases $(a, \infty, \infty)$ and $(\infty, \infty, \infty)$ which can be analyzed after making appropriate modifications. Then Takeuchi [30, Proposition 1] has shown that there exists an embedding

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

which is unique up to conjugacy in $\operatorname{SL}_2(\mathbb{R})$. In fact, this embedding can be made explicit as follows [18]. For $k \in \mathbb{Z}_{\geq 2}$ we let

$$(1.4) \quad \lambda_k = 2 \cos \left( \frac{2\pi}{k} \right) \quad \text{and} \quad \mu_k = 2 \sin \left( \frac{2\pi}{k} \right)$$

and by convention $\lambda_{\infty} = 2$ and $\mu_{\infty} = 0$. Note that $\lambda_k = \zeta_k + 1/\zeta_k$ where $\zeta_k = \exp(2\pi i/k)$. Then we have a map

$$(1.5) \quad \tilde{\Delta}(a, b, c) \hookrightarrow \operatorname{SL}_2(\mathbb{R})$$

$$\gamma_a \mapsto \frac{1}{2} \begin{pmatrix} \lambda_{2a} & \mu_{2a} \\ -\mu_{2a} & \lambda_{2a} \end{pmatrix} = \begin{pmatrix} \cos(\pi/a) & \sin(\pi/a) \\ -\sin(\pi/a) & \cos(\pi/a) \end{pmatrix}$$

$$\gamma_b \mapsto \frac{1}{2} \begin{pmatrix} \lambda_{2b} & t\mu_{2b} \\ -t\mu_{2b}/t & \lambda_{2b} \end{pmatrix} = \begin{pmatrix} \cos(\pi/b) & t\sin(\pi/b) \\ -(1/t)\sin(\pi/b) & \cos(\pi/b) \end{pmatrix}$$

where

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

A triangle group $\Delta$ is maximal if it cannot be properly embedded in any other Fuchsian group (as a subgroup with finite index). By a result of Greenberg [9, Theorem 3B] [♠♠ TO DO : Wolfart says this is due to Singerman?], if $\Delta(a, b, c)$ is not maximal then in fact $\Delta$ is contained in another triangle group $\Delta'$. All inclusion relations between triangle groups belong to one of the families

$$(1.6) \quad \Delta(a, a, c) \subset_2 \Delta(2, a, 2c) \quad \Delta(2, b, 2b) \subset_3 \Delta(2, 3, 2b) \quad \Delta(3, b, 3b) \subset_4 \Delta(2, 3, 3b),$$

where in (1.6) (and here alone) we do not assume that $a \leq b \leq c$, or one of the exceptional inclusions

$$(1.7) \quad \Delta(\infty, \infty, \infty) \subset_3 \Delta(3, 3, \infty) \quad \Delta(7, 7, 7) \subset_2 \Delta(2, 3, 7)$$

$$\Delta(4, 4, 5) \subset_0 \Delta(2, 4, 5);$$

the notation $\Delta \subset_n \Delta'$ is an abbreviation for $|\Delta' : \Delta| = n$.

As in the introduction, a Fuchsian group $\Gamma$ is arithmetic [2] 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 $\Gamma$ is commensurable with the units of reduced norm 1 in a maximal order $\mathcal{O} \subset B$. Takeuchi [30, Theorem 3] has classified all triples $(a, b, c)$ such that $\mathcal{X}(a, b, c)$ is arithmetic; there are 85 such triples and they fall into 19 commensurability classes [31, Table (1)].
2. Wolfart curves, Belyi maps

In this section, we discuss Belyi maps and Wolfart curves, and we relate these curves to triangle curves.

As in the introduction, we define a Belyi map to be a morphism \( f : X \to \mathbb{P}^1 \) of Riemann surfaces (equivalently, algebraic curves) which is ramified at 3 points. A Belyi map which is a Galois covering (with Galois group \( \text{Aut}(E) \)) named after Wolfart who studied these curves in detail [34, 35]. We note that if \( X \to X/G \) realizes \( X \) as a Wolfart curve of genus \( g \geq 2 \), then \( X \to X/\text{Aut}(X) \) 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 Belyi 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 spherical triangle group \( \Delta(2, 2, 3) \). Further examples of Belyi 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 if and only if \( j(E) = 0, 1728 \). If \( f : E \to E/G \cong \mathbb{P}^1 \) is a Wolfart map with \( G \subset \text{Aut}(E) \) (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 \( j \neq 0, 1728 \), 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 Belyi map of degree 4 defined by \( x^2 \). Note that in each case \((X, \text{Aut}(X))\) is minimally defined over its CM field \( K \).

Indeed, these curves arise as the quotients by the Euclidean triangle groups \( \Delta(2, 4, 4) \) and \( \Delta(3, 3, 3) \hookrightarrow \Delta(2, 3, 6) \). We refer to work of Singerman and Syddall [26] for further discussion.

Remark 2.3. There are only finitely many Wolfart curves of given genus. \[ \text{DO: Make argument here.} \]

Wolfart [35] 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 [22].

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 have several alternative characterizations.

Proposition 2.4 (Wolfart [34, 35]). 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 \( X \to X/\text{Aut}(X) \) is a Belyi map;
(iii) \( X \) is uniformized by a Fuchsian group \( \Gamma \) which is a finite-index, normal subgroup of a hyperbolic triangle group \( \Delta(a, b, c) \) with \( 2 \leq a \leq b \leq c < \infty \).
(iv) There exists an open neighborhood \( U \) of \( [X] \) in the moduli space \( M_g(\mathbb{C}) \) of curves of genus \( g \) such that \( \# \text{Aut}(X) > \# \text{Aut}(Y) \) for all \( [Y] \in U \setminus \{ [X] \} \).
Remark 2.5. We note the following consequence of Proposition 2.4. If $\Gamma' \subset \text{PSL}_2(\mathbb{Z}) \cong \Delta(2, 3, \infty)$ is a torsion-free normal subgroup and $X = \Gamma' \backslash \mathbb{H}^\ast$ is a Wolfart curve, then in fact $X$ is uniformized by a group $\Gamma \subset \Delta(a, b, c)$ with $a, b, c \in \mathbb{Z}_{\geq 2}$. \hspace{1cm} ♠♠ TO DO: Dig this up in that Streit-Smith paper. \hspace{1cm} ♠♠ TO DO: Also works for Hecke triangle groups! So maybe should say this for the noncompact case.

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

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

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

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

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

Condition Proposition 2.4(iii) leads us to consider curves arising from finite-index normal subgroups of the hyperbolic triangle groups $\Delta(a, b, c)$. If $\Gamma \subset \text{PSL}_2(\mathbb{R})$ is a Fuchsian group, write $X(\Gamma) = \Gamma \backslash \mathbb{H}^\ast$. Recall that if $X$ is a compact Riemann surface of genus $g \geq 2$ with uniformizing subgroup $\Gamma \subset \text{PSL}_2(\mathbb{R})$, so that $X = X(\Gamma)$, then $\text{Aut}(X) = N(\Gamma)/\Gamma$, where $N(\Gamma)$ is the normalizer of $\Gamma$ in $\text{PSL}_2(\mathbb{R})$. Moreover, the quotient $X \rightarrow X/\text{Aut}(X)$, obtained from the map $X(\Gamma) \twoheadrightarrow X(N(\Gamma))$, is a Galois cover with Galois group $\text{Aut}(X)$. By the results of Section 1, if $\Gamma \subset \Delta(a, b, c)$ is a finite-index normal subgroup then $\text{Aut}(X(\Gamma))$ is of the form $\Delta' / \Gamma$ with an inclusion $\Delta \subset \Delta'$ as in (1.6)–(1.7); if $\Delta$ is maximal, then we conclude

$$\text{Aut}(X(\Gamma)) \cong \Delta(a, b, c) / \Gamma.$$

3. Fields of moduli

In this section, we briefly review the theory of fields of moduli and fields of definition. \hspace{1cm} ♠♠ TO DO: Give reference.

Recall from the introduction that the field of moduli of a curve $X$ over $\mathbb{C}$ is the fixed field of the group $\{ \sigma \in \text{Aut}(X) : X^\sigma \cong X \}$. 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. Belyï’s theorem can be rephrased as saying that a curve has field of moduli given by a number field if and only if it admits a Belyï map.

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

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 [5] remark that this lemma follows from results of Coombes and Harbater [4]. The proof was written down by Köck [12, 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 $X \to X/\text{Aut}(X)$. \qed

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 $H^1(F, \text{Aut}(X))$, where $\text{Aut}(X)$ is viewed as a module over $G_F = \text{Gal}(\overline{F}/F)$. The action of $G_F$ on $\text{Aut}(X)$ cuts out a finite Galois extension $K \supset F$ which is the minimal field such that all elements of $\text{Aut}(X)$ are defined over $K$; in other words, $(X, \text{Aut}(X))$ has field of moduli equal to its minimal field of definition $K$.

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

Example 3.5. Let $p \geq 7$ be prime and let $X = X(p) = \Gamma(p)/\mathcal{O}^*$ be the classical modular curve, parametrizing (generalized) elliptic curves with full $p$-level structure. Then $\text{Aut}(X) \cong \text{PSL}_2(\mathbb{F}_p)$ and the quotient map $X \to X/\text{Aut}(X) \cong \mathbb{P}^1 = \mathbb{C}(j)$, corresponding to the inclusion $\Gamma(p) \subset \text{PSL}_2(\mathbb{Z})$, 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 $\mathbb{Q}$ [\color{red}{\text{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 $H^1(\mathbb{Q}, \text{Aut}(X))$ is infinite: in fact, every isomorphism class of Galois modules $E[p]$ with $E$ an elliptic curve gives a distinct class in this set. However, the field of rational numbers $\mathbb{Q}$ is not a field of definition for $\text{Aut}(X)$. Rather, letting $p^* = (-1)^{(p-1)/2}/p$, Shih [\color{red}{\text{TO DO : Cite}}] showed that the pair $(X, \text{Aut}(X))$ has minimal field of definition $\mathbb{Q}(\sqrt{p^*})$. Note that the naïve modular interpretation of $X$ [\color{red}{\text{TO DO : Cite Katz-Mazur or whatever}}] gives a model over $\mathbb{Q}(\zeta_p)$.

Remark 3.6. We consider again Remark 2.8. If the field of moduli of a Belyï 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 $(X, \text{Aut}(X))$ 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 Belyï map! Note that unless $F = \mathbb{Q}$ and $j(V) = 0, 1728$, we have from Example 2.2 that the Wolfart curve $X$ corresponding to $V$ has genus $g(X) \geq 2$.

In view of Remark 3.6, we restrict our attention from now on to the special class of $\text{PSL}_2(\mathbb{F}_p)$-Wolfart curves $X$, which 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 [29]. This idea was also pursued by Cohen and Wolfart [3] with an eye toward results in transcendence theory. Here, we use this embedding to construct congruence subgroups of $\Delta$. We refer to Vignéras [32] for the facts we will use about quaternion algebras.

Throughout, we let $\Delta = \Delta(a, b, c)$ be a hyperbolic triangle group with $2 \leq a \leq b \leq c \leq \infty$. By Takeuchi [30, Proposition 2] with an eye toward results in transcendence theory. Here, we use this triangle group following Takeuchi [29]. This idea was also pursued by Cohen and

Let $\alpha = \lambda_2 b - 4$ and $\beta = (\lambda_a - 2)(\lambda_c - 2)(\lambda_a + \lambda_b + \lambda_c + \lambda_2a\lambda_2b\lambda_2c + 2)$. Moreover, $\tilde{O} = \mathbb{Z}_F[\tilde{\Delta}]$ is an order in $\bar{F} [\tilde{\Delta}]$.

Lemma 4.1. The algebra $F[\tilde{\Delta}]$ is isomorphic to the quaternion algebra $\left( \frac{\alpha, \beta}{F} \right)$ where $\alpha = \lambda_2 b - 4$ and $\beta = (\lambda_a - 2)(\lambda_c - 2)(\lambda_a + \lambda_b + \lambda_c + \lambda_2a\lambda_2b\lambda_2c + 2)$. Moreover, $\tilde{O} = \mathbb{Z}_F[\tilde{\Delta}]$ is an order in $\bar{F} [\tilde{\Delta}]$.

Proof. Combine the explicit computation in Takeuchi [30, Proposition 2] with the classification in his earlier work [28].

In fact, we note that $Q(\alpha, \beta) = Q(\lambda_a, \lambda_b, \lambda_c, \lambda_2a, \lambda_2b, \lambda_2c) = F$, so we have $B = \left( \frac{\alpha, \beta}{F} \right) \otimes F \bar{F}$. Let $O = \tilde{O} \cap B$. Then we have an embedding $\tilde{\Delta} \hookrightarrow \tilde{O}_1^*$ and an embedding $\Delta \hookrightarrow O_1^*/\{\pm 1\}$.

Lemma 4.2. The (reduced) discriminant of $O$ is generated (as a $\mathbb{Z}_F$-ideal) by $\beta = \lambda_a + \lambda_b + \lambda_c + \lambda_2a\lambda_2b\lambda_2c + 2$.

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

$$\mathfrak{d}^2 = \det \begin{pmatrix} 2 & \lambda_2a & \lambda_2b & \lambda_2c \\ \lambda_2a & \lambda_a & -\lambda_2c & -\lambda_2b \\ \lambda_2b & -\lambda_2c & \lambda_b & -\lambda_2a \\ \lambda_2c & -\lambda_2b & -\lambda_2a & \lambda_c \end{pmatrix} \mathbb{Z}_F = \beta^2 \mathbb{Z}_F.$$
Remark 4.4. More generally [28], if $\Gamma$ is any Fuchsian group of the first kind, then the algebra $B(\Gamma)$ generated over $\mathbb{Q}(\text{tr } \Gamma) = \mathbb{Q}(\text{tr } \gamma \in \Gamma)$ by $\Gamma$ is a quaternion algebra over $\mathbb{Q}(\text{tr } \Gamma)$. If $\text{tr}(\Gamma) \subset \mathbb{Z}_F$, then $\mathbb{Z}_F[\Gamma]$ is an order in $B(\Gamma)$.

\[ \star \star \text{ TO DO : Comment about semiarithmetic groups that also have embeddings?} \]

Let $O \supset \mathbb{Z}[\Delta]$ be a maximal order in $B$. From Lemma 4.1, realized by the embedding (1.5), we have an embedding

$\Delta(a, b, c) \hookrightarrow O_1^*$

where $O_1^* = \{ \gamma \in O : \text{nr}(O) = 1 \}$ denotes the group of units of reduced norm 1 in $O$.

\[ \star \star \text{ TO DO : Some experiments indicate that very often } B(a, b, c) = F[\Delta] \text{ is everywhere unramified; we should be able to prove this using a careful direct computation. Same with the discriminant of } \mathbb{Z}_F[\Delta]. \text{ Note that} \]

$\beta = \left( \frac{\zeta_b \zeta_c}{\zeta_a} + 1 \right) \left( \frac{\zeta_a \zeta_c}{\zeta_b} + 1 \right) \left( \frac{\zeta_a \zeta_b}{\zeta_c} + 1 \right) \left( \frac{1}{\zeta_a \zeta_b \zeta_c} + 1 \right).$

\[ \ldots \]

Example 4.5. \[ \star \star \text{ TO DO : Reference some examples of arithmetic triangle groups, specifically } \text{SL}_2(\mathbb{Z}). \]

Example 4.6. \[ \star \star \text{ TO DO : Explain the specific case of Hecke triangle groups.} \]

We now define congruence subgroups of these groups. For a prime $p$ of $\mathbb{Z}_F$ which is unramified in $\mathbb{Z}_F[\Delta]$ \[ \star \star \text{ TO DO : Or just in } F[\Delta]? \], let

$O(p) = \{ \gamma \in O : \gamma \equiv 1 \pmod{p} \}$

and

$\Delta(p) = \Delta(a, b, c; p) = O(p)_1^* \cap \Delta.$

Then $\Delta(p) \subset \Delta$ is a normal subgroup of finite index. Let $X(p) = X(a, b, c; p) = \Delta(p) \setminus \mathcal{H}$ be the associated (complex) curve.

5. Field of definition of congruence triangle curves

In this section, we let $(a, b, c)$ be a hyperbolic triple and continue the notation from Section 4. In particular, we let $p$ be a prime of $F = F(a, b, c)$. Let $F_p$ denote the residue class field of $p$ and let $\mathbb{Z}_{F,p}$ be the completion of $\mathbb{Z}_F$ at $p$.

Proposition 5.1. If $(a, b, c)$ is maximal and not exceptional, then $\text{Aut}(X(p)) \cong \text{PSL}_2(F_p)$.

Proof. By the results of Section 2, since $(a, b, c)$ is maximal we have

$\text{Aut}(X(p)) \cong N(\Delta(p))/\Delta(p) \cong \Delta/\Delta(p).$

Furthermore, we have an inclusion

$\Delta/\Delta(p) \hookrightarrow O_1^*/O(p)_1^* \cong \text{PSL}_2(F_p),$
where the latter follows since $O \otimes_{\mathbb{Z}_p} \mathbb{Z}_{F_\mathfrak{p}} \cong M_2(\mathbb{Z}_{F_\mathfrak{p}})$. Hence we obtain a triple $g = (\tau_a, \tau_b, \tau_c) \in \text{PSL}_2(F_\mathfrak{p})$, where $\tau$ denotes reduction modulo $\mathfrak{p}$, with trace triple $(\lambda_a, \lambda_b, \lambda_c)$.

But since further $(a, b, c)$ is not exceptional (7.4), by Macbeath’s classification (Proposition 7.5) the triple $g$ is projective and hence the triple generates a subgroup $\text{PSL}_2(k) \subset \text{PSL}_2(F_\mathfrak{p})$ with $k \subset F_\mathfrak{p}$. Moreover, by Corollary 7.8, we have $k = F_\mathfrak{p}$. Hence we obtain a triple $(\lambda_a, \lambda_b, \lambda_c)$.

\[ \text{\textbullet\textbullet \ TO DO : The result then holds because by definition when } p \nmid abc, \text{ but ‘oh! I think we just need to analyze carefully the } p \text{-maximality of the (commutative) order } Z[\lambda_a, \lambda_b, \lambda_c]. \]

\[
\text{\textbullet\textbullet \ TO DO : What is established in the proof here – namely, the index equality } \left[ \Delta : \Delta(p) \right] = \left[ O^1 : O^1(\mathfrak{p}) \right] \text{ – is, to my mind, at least as important as the consequence that is stated in this proposition. This index equality should be stated as a result in its own right (even a theorem, perhaps) and this should be a corollary.}
\]

6. Weak rigidity

In this section, we investigate some weak forms of rigidity and rationality for Galois covers of $\mathbb{P}^1$. \[ \text{\textbullet\textbullet \ TO DO : References} \].

Let $G$ be a finite group. A \textbf{(n-)tuple} is a finite sequence $g = (g_1, \ldots, g_n)$ of elements of $G$ such that $g_1 \cdots g_n = 1$. (Since all of our applications concern the case $n = 3$, we do not feel the need to emphasize the dependence on $n$.) The tuple is \textbf{generating} if $(g_1, \ldots, g_n) = G$. Let $C = (C_1, \ldots, C_n)$ be a tuple of conjugacy classes of $G$. Let $\Sigma(G)$ be the set of generating tuples $g = (g_1, \ldots, g_n)$ such that for all $i$, $C(g_i) = C_i$.

The natural (diagonal) action of $\text{Inn}(G) = G/Z(G)$ on $G^n$ stabilizes $\Sigma(G)$ and thus gives an action of $\text{Inn}(G)$ on $\Sigma(G)$.

From now on we assume that $G$ has trivial center, so $\text{Inn}(G) = G$. Let $C$ be a conjugacy class tuple such that $\Sigma(G) \neq \emptyset$. Then the action of $\text{Inn}(G)$ on $\Sigma(G)$ is fixed point free: if $g \cdot (g_1, \ldots, g_n) = (g_1, \ldots, g_n)$, then $g$ commutes with each $g_i$ hence with $(g_1, \ldots, g_n) = G$, so $g \in Z(G) = 1$.

We say that $\Sigma(G)$ is \textbf{rigid} if the action of $\text{Inn}(G)$ on $\Sigma(G)$ is transitive. By the above discussion, the action is then simply transitive, i.e., endows $\Sigma(G)$ with the structure of a torsor under $G = \text{Inn}(G)$. We say that $\Sigma(G)$ is \textbf{weakly rigid} if for any two tuples $g, g' \in \Sigma(G)$, there exists $\varphi \in \text{Aut}(G)$ such that $\varphi(g) = g'$.

Now let $G$ be any finite group, and let $N$ be the exponent of $G$. Then the group $(\mathbb{Z}/N\mathbb{Z})^\times$ acts on $G$: $a \cdot g = g^a$. There is an induced action on conjugacy classes and thus on conjugacy class tuples. If $C$ is a rigid tuple and $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, then also $C^a = (C_1^a, \ldots, C_n^a)$ is rigid [21, Cor. 7.3.2]. Pulling back by the canonical isomorphism $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \sim (\mathbb{Z}/N\mathbb{Z})^\times$ gives an action of $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ on the set of conjugacy classes of $G$. If $H$ is the kernel of this action, then the fixed field
\[ F(G) = \mathbb{Q}(\zeta_N)^H \] is called the field of rationality of \( G \). The field \( F(G) \) can also be characterized as the field obtained by adjoining to \( \mathbb{Q} \) the values of the character table of \( G \) [21, §7.1].

Let \( H(\mathcal{C}) \subset (\mathbb{Z}/N\mathbb{Z})^\times \) be the stabilizer of \( \mathcal{C} \), i.e., the set of \( \alpha \in \mathbb{Z}/N\mathbb{Z}^\times \) such that \( C^\alpha_i = C_i \) for all \( 1 \leq i \leq n \). We define the field of rationality as
\[
F(\mathcal{C}) = \mathbb{Q}(\zeta_N)^H(\mathcal{C}).
\]

Similarly, we put
\[
\{H_{wk}(\mathcal{C}) = \{\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times \mid \exists \phi \in \text{Aut}(G) \phi(\mathcal{C}) = C^\alpha\}
\]
and define the field of weak rationality as
\[
F_{wk}(\mathcal{C}) = \mathbb{Q}(\zeta_N)^{H_{wk}(\mathcal{C})}.
\]
Evidently we have
\[
F_{wk}(\mathcal{C}) \subset F(\mathcal{C}) \subset F(G).
\]

\[\text{Proposition 6.1 (Weak rigidity-weak rationality (WRWR))}\]

Let \( G \) be a group of order \( \#G = m \) with trivial center. Let \( g = (g_1, \ldots, g_n) \) be a generating tuple for \( G \) with associated tuple of conjugacy classes \( \mathcal{C} \). Suppose that \( \mathcal{C} \) is weakly rigid. Then the following statements hold.

(a) There exists a curve over \( \overline{\mathbb{Q}} \) and an embedding \( G \rightarrow \text{Aut}(X) \) such that the map
\[
f : X \rightarrow X/G \cong \mathbb{P}^1
\]
is a branched covering with ramification type \( \mathcal{C} \), and the pair \( (X,G) \) 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 \( F_{wk}(\mathcal{C}) \).

(c) There is a canonical bijection between the \( G_\mathbb{Q} \)-orbits of \( X \) and the orbits of \( \mathcal{C} \).

(d) There is a (unique) minimal field of definition \( K \) for \( (X,G) \). We have \( F(\mathcal{C}) \subset K \) and an embedding \( \text{Gal}(K/F_{wk}) \) into the stabilizer of \( \mathcal{C} \) in the group \( \text{Out}(G) \).

\[\text{Proposition 6.1 (Weak rigidity-weak rationality (WRWR)). Let G be a group of order #G = m with trivial center. Let g = (g_1, \ldots, g_n) be a generating tuple for G with associated tuple of conjugacy classes C. Suppose that C is weakly rigid. Then the following statements hold.}\]

\[(a) \text{ There exists a curve over \( \overline{\mathbb{Q}} \) and an embedding } G \rightarrow \text{Aut}(X) \text{ such that the map } f : X \rightarrow X/G \cong \mathbb{P}^1 \text{ is a branched covering with ramification type } C, \text{ and the pair } (X,G) \text{ is unique up to (nonunique) isomorphism.}\]

\[(b) \text{ The curve } X \text{ can be defined over its field of moduli which is equal to the field of weak rationality } F_{wk}(C).\]

\[(c) \text{ There is a canonical bijection between the } G_\mathbb{Q}-\text{orbits of } X \text{ and the orbits of } C.\]

\[(d) \text{ There is a (unique) minimal field of definition } K \text{ for } (X,G). \text{ We have } F(C) \subset K \text{ and an embedding } \text{Gal}(K/F_{wk}) \text{ into the stabilizer of } C \text{ in the group } \text{Out}(G).\]

\[\text{Proof. The proof can be extracted from work of Volklein [33, Remark 3.9, Proposition 9.2(b)].} \]

\[\text{Proposition 6.1 (Weak rigidity-weak rationality (WRWR)). Let G be a group of order #G = m with trivial center. Let g = (g_1, \ldots, g_n) be a generating tuple for G with associated tuple of conjugacy classes C. Suppose that C is weakly rigid. Then the following statements hold.}\]

\[(a) \text{ There exists a curve over \( \overline{\mathbb{Q}} \) and an embedding } G \rightarrow \text{Aut}(X) \text{ such that the map } f : X \rightarrow X/G \cong \mathbb{P}^1 \text{ is a branched covering with ramification type } C, \text{ and the pair } (X,G) \text{ is unique up to (nonunique) isomorphism.}\]

\[(b) \text{ The curve } X \text{ can be defined over its field of moduli which is equal to the field of weak rationality } F_{wk}(C).\]

\[(c) \text{ There is a canonical bijection between the } G_\mathbb{Q}-\text{orbits of } X \text{ and the orbits of } C.\]

\[(d) \text{ There is a (unique) minimal field of definition } K \text{ for } (X,G). \text{ We have } F(C) \subset K \text{ and an embedding } \text{Gal}(K/F_{wk}) \text{ into the stabilizer of } C \text{ in the group } \text{Out}(G).\]

\[\text{Proof. The proof can be extracted from work of Volklein [33, Remark 3.9, Proposition 9.2(b)].} \]

\[\text{Proposition 6.1 (Weak rigidity-weak rationality (WRWR)). Let G be a group of order #G = m with trivial center. Let g = (g_1, \ldots, g_n) be a generating tuple for G with associated tuple of conjugacy classes C. Suppose that C is weakly rigid. Then the following statements hold.}\]

\[(a) \text{ There exists a curve over \( \overline{\mathbb{Q}} \) and an embedding } G \rightarrow \text{Aut}(X) \text{ such that the map } f : X \rightarrow X/G \cong \mathbb{P}^1 \text{ is a branched covering with ramification type } C, \text{ and the pair } (X,G) \text{ is unique up to (nonunique) isomorphism.}\]

\[(b) \text{ The curve } X \text{ can be defined over its field of moduli which is equal to the field of weak rationality } F_{wk}(C).\]

\[(c) \text{ There is a canonical bijection between the } G_\mathbb{Q}-\text{orbits of } X \text{ and the orbits of } C.\]

\[(d) \text{ There is a (unique) minimal field of definition } K \text{ for } (X,G). \text{ We have } F(C) \subset K \text{ and an embedding } \text{Gal}(K/F_{wk}) \text{ into the stabilizer of } C \text{ in the group } \text{Out}(G).\]

\[\text{Proof. The proof can be extracted from work of Volklein [33, Remark 3.9, Proposition 9.2(b)].} \]
believe it’s correct. I will need to go back to Volklein’s book, which I have back in Athens but not online.

Remark 6.2. [♠♠ TO DO : Remark here about the branch points being defined over \(\mathbb{Q}\), and not just the divisor. But I’m not sure how you’re using that in the above proposition. And you write “\(C'_{P_j} = C_{\sigma(P_j)}\), but what do you mean by this? The conjugacy classes are indexed not by points.]

[♠♠ TO DO : The cases where \(a, b, c\) are distinct seem very natural, and I’d hate to exclude them from our analysis unless things really do get hairy.]

[♠♠ TO DO : Insert remark here about the consequence that only \(\text{PSL}_2(\mathbb{F}_q)\) 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 \((X, \text{Aut}(X))\) defined over \(\mathbb{Q}\).]

We now apply this result to the case of generating triples for \(\text{PSL}_2(k)\) as in the previous section. Let \(g\) be any generating triple in \(\text{PSL}_2(k)\) which is not exceptional, so that the associated triple of orders \((a, b, c)\) is not one in the list (7.4). Then the triple \(g\) is not commutative, since \(\text{PSL}_2(k)\) is never an abelian group. Then by Corollary 7.7, the associated conjugacy class triple \(C\) is weakly rigid, and so Proposition 6.1 (WRWR) applies; let \(X(g)\) be the curve associated to \(g\).

**Proposition 6.3.** Let \(g\) be a nonexceptional generating triple in \(G = \text{PSL}_2(k)\) with associated triples of orders \((a, b, c)\) and conjugacy classes \(C\), and let \(X = X(g)\) be the curve associated to \(g\).

Then the minimal field of definition of \(X\) is the field of weak rationality \(F_{wk}(C)\) and the minimal field of definition \(K\) of \((X, G)\) satisfies \([K : F_{wk}(C)] \leq 2\).

Moreover, the triple \(C\) is rigid if and only if \(p = 2\) or \(p | abc\), and if so then the minimal field of definition of \((X, G)\) (hence also of \(X\)) is equal to its field of rationality \(F(C)\).

**Proof.** The first statement follows from (WRWR), Proposition 6.1(b). To prove the other statements, we consider part (d) of this Proposition in view of (??). By Corollary 7.8, the traces \(\text{tr}(g)\) generate \(k\) over \(\mathbb{F}_p\), therefore the \(p\)-power Frobenius \(\sigma\) acts nontrivially on \(C\). So the only nontrivial automorphism which might stabilize \(C\) is \(\tau\), of order 2, and hence \([K : F_{wk}(C)] \leq 2\).

We now prove the last statement. We claim that \(C\) is rigid if and only if \(p = 2\) or \(\tau\) does not stabilize \(C\). Indeed, by Proposition 7.5, the number of conjugacy classes with given trace triples is 1 or 2 according as \(p = 2\) or not, and yet by Corollary 7.7 we have that \(\text{Aut}(G)\) acts transitively on these triples. Hence if \(p = 2\) then \(C\) is rigid, and if \(p \neq 2\) then \(\tau\) stabilizes \(C\) if and only if \(G\) does not act transitively on \(\Sigma(C)\), which is to say that \(C\) is not rigid.

But by the results of Section 5, we see that conjugacy classes are determined by their trace except when the conjugacy class is unipotent (equivalently, \(p | abc\) or in fact \(p\) is equal to one of \(a, b, c\)), in which case we see easily that \(\tau\) interchanges the two unipotent conjugacy classes. The result follows. \(\square\)
7. Subgroups of $\text{PSL}_2(\mathbb{F}_q)$

Let $p$ be a prime number and $q = p^r$ a prime power. We denote by $\mathbb{F}_q$ “the” finite field of order $q$ and by $\overline{\mathbb{F}}_q$ “the” algebraic closure of $\mathbb{F}_q$. Our goal in this section is to record some basic, but crucial, facts concerning conjugacy classes and automorphisms in the finite matrix groups $\text{SL}_2(\mathbb{F}_q)$ and $\text{PSL}_2(\mathbb{F}_q)$.

Let $g \in \text{SL}_2(\mathbb{F}_q)$. Then $g$ has characteristic polynomial $P(g) = t^2 - \text{tr}(g)t + 1$. Suppose first that the characteristic polynomial has a repeated root, which therefore must be $\pm 1$. In particular the characteristic values are $\mathbb{F}_q$-rational, so the Jordan canonical form exists over $\mathbb{F}_q$. Excluding the trivial cases $g = \pm 1$, the Jordan form is either $U(u) = \begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix}$ or $-U(u) = \begin{bmatrix} -1 & u \\ 0 & -1 \end{bmatrix}$ for some $u \in \mathbb{F}$.

One checks easily that for any $u, v \in \mathbb{F}_q^\times$, the matrices $U(u)$ and $U(v)$ are conjugate iff $uv^{-1} \in k^\times$. In particular, if $q$ is odd there are two conjugacy classes of nontrivial matrices with characteristic polynomial $(t - 1)^2$, whereas is $q$ is even there is a single such conjugacy class. Such conjugacy classes are called unipotent.

Now we suppose that the characteristic polynomial of $g$ has distinct roots in $\overline{\mathbb{F}}$: we say that $g$ is semisimple. Then $g$ is conjugate in $\text{SL}_2(\mathbb{F}_q)$ to a diagonal matrix $\begin{bmatrix} a & 0 \\ 0 & \frac{1}{a} \end{bmatrix}$. Moreover, $g$ is diagonalizable over $\mathbb{F}_q$ iff the roots of $P(g)$ are $\mathbb{F}_q$-rational: if this occurs we say that $g$ is split semisimple; otherwise we say $g$ is nonsplit semisimple. In the nonsplit case there is a unique $\mathbb{F}_q$-rational invariant factor, so $g$ is conjugate to the matrix $\begin{bmatrix} 0 & -1 \\ 1 & \text{tr}(g) \end{bmatrix}$. Further, $g$ lies in the unit group of a nonsplit Cartan subalgebra $C_{ns} \cong \mathbb{F}_q^2$ of $\mathcal{M}_2(\mathbb{F}_q)$. The restriction of the determinant map to $C_{ns}$ is precisely the norm map $\mathbb{F}_q^2 \to \mathbb{F}_q$, so it is surjective. It follows that $C_{ns} \cap \text{SL}_2(\mathbb{F}_q)$ is a cyclic group of order $q + 1$.

The conjugacy class of a semisimple element of $\text{SL}_2(\mathbb{F}_q)$ is determined by its trace. Conversely, for any $\alpha \in \mathbb{F}_q$, $\alpha \neq \pm 2$, there exists a nontrivial (necessarily semisimple) element of $\text{SL}_2(\mathbb{F}_q)$ with trace $\alpha$, namely $\begin{bmatrix} 0 & -1 \\ 1 & \text{tr}(g) \end{bmatrix}$.

Moreover, if a semisimple element $g \in \text{SL}_2(\mathbb{F}_q)$ has order $a$, then $a$ is prime to $p$ and the eigenvalues of $g$ consist of a primitive $a$th root of unity and its inverse. Let $\zeta_a$ denote a fixed choice of primitive $a$th root of unity (not necessarily equal to the eigenvalue of $g$!) and put $\lambda_a = \zeta_a + \zeta_a^{-1}$. It is easy to see that the field extension of $\mathbb{F}_p$ obtained by adjoining the trace of $g$ is $\mathbb{F}_p(\lambda_a)$.

Let us now give the corresponding description of orders, traces and conjugacy classes in $\text{PSL}_2(\mathbb{F}_q) = \text{SL}_2(\mathbb{F}_q)/\{\pm 1\}$. When $q$ is even, $\text{PSL}_2(\mathbb{F}_q) = \text{SL}_2(\mathbb{F}_q)$ has just been described, so assume that $q$ is odd. Then, the conjugacy classes of the matrices $U(u)$ and $-U(u)$ in $\text{SL}_2(\mathbb{F}_q)$ become identified in $\text{PSL}_2(\mathbb{F}_q)$, so there are precisely two nontrivial unipotent conjugacy classes, each consisting of elements of order $p$.

If $\bar{g}$ is a semisimple element of $\text{SL}_2(\mathbb{F}_q)$ of order $a$, then the order of its image $g$ in $\text{PSL}_2(\mathbb{F}_q)$ is $\frac{a}{\gcd(a,2)}$. We define the trace of an element $g$ as the pair $\{\text{tr}(\bar{g}), \text{tr}(-\bar{g})\} = \{\pm \text{tr}(g)\}$ of elements of $\mathbb{F}_q$. We further define the trace field of $g$ as $\mathbb{F}_p(\bar{g}) = \mathbb{F}_p(\pm \bar{g})$. (Thus the trace field of any unipotent element is simply $\mathbb{F}_p$.)
As above, the conjugacy class of a semisimple element of $\text{PSL}_2(\mathbb{F}_q)$ is uniquely determined by its trace, whereas the trace field of a semisimple element of order $a$ is $\mathbb{F}_p(\lambda_{2a}) = \mathbb{F}_p(\zeta_{2a} + \zeta_{2a}^{-1})$. Here $\zeta_{2a}$ denotes a fixed primitive $2$-th root of unity in $\mathbb{F}_q$.

For later use, let us count the number of conjugacy classes of elements in $\text{PSL}_2(\mathbb{F}_q)$ of order $a$ prime to $p$. By the considerations just above, we may assume that $\mathbb{F}_q$ contains $\mathbb{F}_p(\lambda_{2a})$, since otherwise $\text{PSL}_2(\mathbb{F}_q)$ does not have elements of order $a$.

Case 1: Suppose $a$ is odd. Then these conjugacy classes correspond to elements of order $a$ or $2a$ in $\text{SL}_2(\mathbb{F}_q)$. The number of conjugacy classes of order $a$ in $\text{SL}_2(\mathbb{F}_q)$ is equal to the number of distinct expressions $\zeta + \zeta^{-1}$ as $\zeta$ runs through the primitive $a$th roots of unity in $\mathbb{F}_q$, namely $\frac{\varphi(a)}{2}$. Similarly, the number of conjugacy classes of order $2a$ in $\text{SL}_2(\mathbb{F}_q)$ is $\frac{\varphi(2a)}{2}$. So if $q$ is even, there are $\varphi(a)$ conjugacy classes in $\text{PSL}_2(\mathbb{F}_q) = \text{SL}_2(\mathbb{F}_q)$. If $q$ is odd, then passage from $\text{SL}_2(\mathbb{F}_q)$ to $\text{PSL}_2(\mathbb{F}_q)$ identifies the traces $\zeta + \zeta^{-1}$ and $-\zeta - \zeta^{-1}$ (which is also a sum of a primitive $a$ or $2a$th root of unity and its inverse), giving a final count of $\frac{\varphi(a)}{2}$.

Case 2: Suppose $a$ is even. The discussion is completely analogous but simplified by the fact that all the lifts of $g$ to $\text{SL}_2(\mathbb{F}_q)$ have order $2a$, so we get $\varphi(2a)$ conjugacy classes if $q$ is even and $\varphi(2a)/2$ conjugacy classes if $q$ is odd.

Note that since $\varphi(2a) = \varphi(a)$ when $a$ is odd, it is possible to consolidate the two cases: the total number of conjugacy classes of order $a$ in $\text{PSL}_2(\mathbb{F}_q)$ is $\frac{\varphi(2a)}{2}$ if $q$ is odd and $\varphi(2a)$ if $q$ is even.

7.1. Cyclotomic action on conjugacy classes. We will compute the field of rationality of each conjugacy class in the sense of §X.X.

First, let $g$ be a nontrivial unipotent element of $\text{PSL}_2(\mathbb{F}_q)$, so that $g \sim U(u)$ for $u \in \mathbb{F}_q^\times$. Then for all $a$ prime to $p$, $g^a \sim U(au)$. From this it follows easily that the subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times$ stabilizing the conjugacy class is precisely the set of elements of $\mathbb{F}_p^\times$ which are squares in $\mathbb{F}_p^\times$. Thus if $p = 2$ or $r$ is even, this subgroup is all of $\mathbb{F}_p^\times$, so that the field of rationality of $g$ is $\mathbb{Q}$, whereas if $p$ is odd this is the unique index two subgroup of $\mathbb{F}_p^\times$ and the field of rationality is $\mathbb{Q}(\sqrt{\mathbb{F}_p})$.

Next, let $g$ be a nontrivial semisimple element of $\text{PSL}_2(\mathbb{F}_q)$, and let $\pm \tilde{g}$ be the lifts of $g$ to $SL_2(\mathbb{F}_q)$. As above, there exists a primitive $2a$th root of unity $\zeta$ such that the traces of $\tilde{g}$ are $\pm(\zeta + \zeta^{-1})$.

Case: $q$ is even. Then the fixed field is $\mathbb{Q}(\lambda_a)$, the real subfield of the $a$th cyclotomic field.

Case: $q$ is odd, $a$ is even. Then the field of rationality is best viewed as the fixed field of the subgroup $\langle -1, a + 1 \rangle$ of $(\mathbb{Z}/2a\mathbb{Z})^\times = \text{Gal}(\mathbb{Q}(\zeta_{2a})/\mathbb{Q})$. An easy calculation shows this field to be equal to $\mathbb{Q}(\lambda_a)$.

Case: $qa$ is odd. Then we can choose the lift $\tilde{g}$ of $g$ to have order $a$, so that the field of rationality is $\mathbb{Q}(\lambda_a)$. 
Thus in all cases the field of rationality of a semisimple conjugacy class of order $a$ is $Q(\lambda_a) = Q(\zeta_a + \zeta_a^{-1})$.

7.2. The group $\text{Out}(\text{PSL}_2(F_q))$. We recall (e.g. [27]) that the outer automorphism group $\text{Out}(\text{PSL}_2(F_q'))$ has order $2r$ if $p$ is odd and order $r$ if $p$ is even. It is generated by the $p$-power Frobenius map $\sigma$ which acts on the entries of a matrix by $a \mapsto a^p$, together with (when $p$ is odd) conjugation $\tau$ by an element $h \in \text{PGL}_2(F_q) \setminus \text{PSL}_2(F_q)$. If $q$ is odd, there is a natural embedding $\text{PGL}_2(F_q) \hookrightarrow \text{PSL}_2(F_q^2)$, given explicitly by $g \mapsto \left(\frac{1}{\det g}\right)g$. Therefore we may view the outer automorphism $\tau$ as being given by conjugation by a matrix $m_\tau \in \text{PSL}_2(F_q^2)$. It follows from this description that outer automorphisms need not preserve the traces, but – by the Galois theory of finite fields – they must preserve the trace fields of all elements of $\text{PSL}_2(F_q)$.

7.3. Macbeath theory. In order to apply the general theory of $\xi X$ to the group $\text{PSL}_2(F_q)$, we need sufficient conditions for a triple to generate $\text{PSL}_2(F_q)$ and to be (at least) weakly rigid. Both of these problems are addressed by a celebrated work of A.M. Macbeath [14], which we will now recall in some detail.

As above, it is natural to consider $\text{PSL}_2(F_q)$ by way of $\text{SL}_2(F_q)$. So we consider triples $g = (g_1, g_2, g_3) \in \text{SL}_2(F_q)$. (Recall that according to the standard conventions of $\xi X.X$, the term “triple” implies the relation $g_1 g_2 g_3 = 1$.) For $\alpha, \beta, \gamma \in F_q^3$, let $E(\alpha, \beta, \gamma)$ denote the set of triples $g$ such that $\text{tr}(g) = (\alpha, \beta, \gamma)$.

**Theorem 7.1.** (Macbeath, [14, Thm. 1]) Let $\alpha, \beta, \gamma \in F_q^3$. Then there exists at least one triple $g = (g_1, g_2, g_3)$ in $\text{SL}_2(F_q)$ such that $\text{tr}(g_1) = \alpha$, $\text{tr}(g_2) = \beta$, $\text{tr}(g_3) = \gamma$. In other words, the set $T(\alpha, \beta, \gamma)$ is nonempty.

Since the trace field – a fortiori, the trace – of a semisimple element of $\text{SL}_2(F_q)$ determines its order, to each $F_q$-triple $(\alpha, \beta, \gamma)$ we may associate a unique order triple $(a, b, c)$ such that for any triple $(g_1, g_2, g_3) \in E(\alpha, \beta, \gamma)$, the order of $g_1$ is $a$, the order of $g_2$ is $b$ and the order of $g_3$ is $c$.

There is no loss of generality in restricting to order triples $(a, b, c)$ with $a \leq b \leq c$. Indeed, (i) the defining condition of a triple, that $g_1 g_2 g_3 = 1$, is invariant under cyclic permutations, and (ii) if $(g_1, g_2, g_3)$ is a triple with orders $(a, b, c)$, then $(g_3^{-1}, g_2^{-1}, g_1^{-1})$ is a triple generating the same subgroup, and with order triple $(c, b, a)$. We make this assumption throughout.

An $F_q$-triple $(\alpha, \beta, \gamma)$ is commutative if there exists $(g_1, g_2, g_3) \in E(\alpha, \beta, \gamma)$ such that $(g_1, g_2, g_3)$ is a commutative group. Macbeath gives a pretty characterization of commutative triples $(\alpha, \beta, \gamma)$: they are such that the naturally associated ternary quadratic form

$$Q(x, y, z) = x^2 + y^2 + z^2 + \alpha yz + \beta xz + \gamma xy$$

is singular [14, Corollary 1, p. 21]. However, for the sake of simplicity we will not use this sharp result but rather content ourselves with the following necessary condition for commutativity in terms of the order triple.
Lemma 7.2. Let \( x \) and \( y \) be commuting elements of a finite group. Let \( a, b \) and \( c \) be the orders of \( x, y \) and \( xy \), respectively. Then

\[
\text{lcm}(a, b) \quad \text{gcd}(a, b) \mid c \mid \text{lcm}(a, b).
\]

The simple, elementary proof is left to the reader. In our applications, we will generally restrict to the case in which \((a, b, c)\) does not satisfy (7.3) and thus any triple \( g \) with order triple \((a, b, c)\) generates a non-commutative subgroup of \( \text{PSL}_2(\mathbb{F}_q) \).

An \( \mathbb{F}_q \)-triple \((\alpha, \beta, \gamma)\) is exceptional if the associated sequence \((a, b, c)\) of orders is equal to \((2, 2, c)\) for \( c \geq 2 \) or one of the following:

\[
(7.4) \quad (2, 3, 3), (3, 3, 3), (3, 4, 4), (2, 3, 4), (2, 5, 5), (5, 5, 5), (3, 3, 5), (3, 5, 5), (2, 3, 5).
\]

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

A subgroup of \( \text{PSL}_2(\mathbb{F}_q) \) is projective if it is conjugate to a subgroup of the form \( \text{PSL}_2(\mathbb{F}_q) \) or \( \text{PGL}_2(\mathbb{F}_q) \) for \( \mathbb{F}_q \subset \mathbb{F}_q \) a subfield.

Theorem 7.5. (Macbeath [14, Thm. 4]) Every triple \( g \) in \( \text{PSL}_2(\mathbb{F}_q) \) is either exceptional, commutative or projective.

Theorem 7.6. (Macbeath [14, Thm. 3]) Let \((\alpha, \beta, \gamma)\) be a nonsingular \( \mathbb{F}_q \)-triple.

(a) The number of orbits of \( \text{Inn}(\text{SL}_2(\mathbb{F}_q)) = \text{SL}_2(\mathbb{F}_q) \) on \( E(\alpha, \beta, \gamma) \) is 2 or 1 according as \( q \) is odd or even.

(b) For \( g, g' \in E(\alpha, \beta, \gamma) \) there exists \( m \in \text{SL}_2(\mathbb{F}_q) \) such that \( mg = mg' \).

In order to transfer these results to the projective groups \( \text{PSL}_2(\mathbb{F}_q) \), we introduce a fourth notion of a triple (which does not explicitly appear in Macbeath’s work): a projective trace triple. By this we mean equivalence classes \([\alpha, \beta, \gamma]\) of \( \mathbb{F}_q \)-triples \((\alpha, \beta, \gamma)\) under the relation \((\alpha, \beta, \gamma) \sim (\alpha', \beta', \gamma')\) iff \( \alpha' = \pm \alpha, \beta' = \pm \beta, \gamma' = \pm \gamma \). Here all \( \pm \) signs are taken independently, so if \( q \) is odd most fibers of this equivalence relation have cardinality 8. (When \( q \) is even, projective trace triples are just trace triples.) Let us say that a trace triple \([\alpha, \beta, \gamma]\) is semisimple if none of \( \alpha, \beta, \gamma \) are \( \pm 1 \). Then the semisimple trace triples are naturally in bijection with triples of semisimple conjugacy classes \((C_1, C_2, C_3)\) in \( \text{PSL}_2(\mathbb{F}_q) \).

Now we rephrase Macbeath’s work in the language and notation of the previous section. Let \( C = (C_1, C_2, C_3) \) be a triple of conjugacy classes, which we will generally assume to be semisimple and nontrivial.

Corollary 7.7. Let \([\alpha, \beta, \gamma]\) be a nonsingular, semisimple \( \mathbb{F}_q \)-triple, e.g. one whose associated order triple \((a, b, c)\) does not satisfy the relations (7.3). Let \( \Sigma(C) = (C_1, C_2, C_3) \) be the corresponding conjugacy class triple in \( \text{PSL}_2(\mathbb{F}_q) \). Recall that \( \Sigma(C) \) is the set of ordered triples \((g_1, g_2, g_3)\) with \( g_1, g_2, g_3 \in \text{PSL}_2(\mathbb{F}_q) \), \( g_1g_2g_3 = 1 \), \( \langle g_1, g_2 \rangle = \text{PSL}_2(\mathbb{F}_q) \), \( C(g_1) = C_1 \). We suppose that \( \Sigma(C) \neq \emptyset \).

(a) If \( q \) is even, \( \Sigma(C) \) is rigid.

(b) If \( q \) is odd, then the action of \( \text{Out}(\text{PSL}_2(\mathbb{F}_q)) \) on \( \Sigma(C) \) has exactly two orbits.

(c) In all cases, \( \Sigma(C) \) is weakly rigid.

Proof. Since, as usual, we have \( \text{PSL}_2(\mathbb{F}_q) = \text{SL}_2(\mathbb{F}_q) \) when \( q \) is even, part a) is simply a restatement of Theorem 7.6a). As for part b), it follows from Theorem
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.  \[ \Box \Box \text{ TO DO : Cite Takeuchi. Check the canonical models of these Shimura curves.} \]

Example 9.2.  \[ \Box \Box \text{ TO DO : Galois descent for triangle Shimura curves which I used and that PSL}_2(\mathbb{F}_8) \text{ example guy.} \]

Example 9.3. Suppose that the triple $(a, b, c)$ has $p \mid abc$. There are two unipotent conjugacy classes of order $p$.  \[ \Box \Box \text{ TO DO : Analysis here.} \]

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 $G_0$-orbit (taking the $i$th power moves from quadratic residues to nonresidues) and so the field of rationality of such a conjugacy class is the quadratic subfield $K = \mathbb{Q}(\sqrt[1/p]{p^*}) \subset \mathbb{Q}(\zeta_p)$, 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 $C$ is $F(C) = K$. As above, the outer automorphism $\tau$ interchanges the two unipotent conjugacy classes, so $F_{\text{we}}(C) = \mathbb{Q}$. Hence we obtain a $\text{PSL}_2(\mathbb{F}_p)$-curve $X(2, 3; p; p)$ which is defined (noncanonically) over $\mathbb{Q}$ and with $(X(2, 3; p; p), \text{Aut}(X))$ defined over $K$.

In fact, the classical modular cover $j : X(p) \to X(1)$ is also a $\text{PSL}_2(\mathbb{F}_p)$-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 $\mathbb{F}_p$. In particular, it follows from the above analysis that
PSL$_2(F_p)$ is the full automorphism group of $X(p)$ \cite{17} and that the minimal field of definition of $(X(p), \text{Aut}(X(p)))$ is $K$. In particular, we note that this interpretation is quite different than the moduli interpretation of “naïve” level $p$-structure \cite{11} for $X(p)$ which gives a model of $\mathbb{Q}(\zeta_p)$. Indeed, this model is used by Shih \cite{23} to show that PSL$_2(F_p)$ occurs regularly as a Galois group over $K$.

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 \cite{7} for further detail).

Example 9.4. Consider the case $(a, b, c) = (2, 3, 7)$ with $p = 2$. Then $G = PSL_2(F_8)$ and $X = X'(2, 3, 7; 2)$ is the Fricke-Macbeath curve \cite{13} 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 $(\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\}$ then $\text{Aut}(X) \cong PSL_2(F_{p^r})$ and $(X, \text{Aut}(X))$ 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 give further examples, we list all PSL$_2(F_q)$-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.

<table>
<thead>
<tr>
<th>$g$</th>
<th>$(a, b, c)$</th>
<th>$q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>(2, 3, 7)</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>(2, 5, 5)</td>
<td>4, 5</td>
</tr>
<tr>
<td>5</td>
<td>(3, 3, 5)</td>
<td>4, 5</td>
</tr>
<tr>
<td>7</td>
<td>(2, 3, 7)</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>(3, 3, 4)</td>
<td>7</td>
</tr>
<tr>
<td>9</td>
<td>(3, 5, 5)</td>
<td>4, 5</td>
</tr>
<tr>
<td>10</td>
<td>(2, 4, 7)</td>
<td>7</td>
</tr>
<tr>
<td>10</td>
<td>(2, 4, 5)</td>
<td>9</td>
</tr>
<tr>
<td>13</td>
<td>(5, 5, 5)</td>
<td>4, 5</td>
</tr>
<tr>
<td>15</td>
<td>(3, 4, 4)</td>
<td>7</td>
</tr>
<tr>
<td>15</td>
<td>(2, 3, 9)</td>
<td>8</td>
</tr>
<tr>
<td>16</td>
<td>(3, 3, 4)</td>
<td>9</td>
</tr>
<tr>
<td>19</td>
<td>(2, 5, 5)</td>
<td>9</td>
</tr>
<tr>
<td>24</td>
<td>(3, 4, 7)</td>
<td>7</td>
</tr>
</tbody>
</table>

Table 9.5: PSL$_2(F_q)$-Wolfart curves of genus $g \leq 24$
Note there is an exceptional isomorphism $\text{PSL}_2(\mathbb{F}_4) \cong \text{PSL}_2(\mathbb{F}_5) \cong A_5$. 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 $\text{PSL}_2(\mathbb{F}_7)$ and associated triple $(3,4,7)$.

♠♠ 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


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