

AUTOMORPHISMS OF HARBATER–KATZ–GABBER CURVES

FRAUKE M. BLEHER*, TED CHINBURG**, BJORN POONEN†, AND PETER SYMONDS

ABSTRACT. Let k be a perfect field of characteristic $p > 0$, and let G be a finite group. We consider the pointed G -curves over k associated by Harbater, Katz, and Gabber to faithful actions of G on $k[[t]]$ over k . We use such “HKG G -curves” to classify the automorphisms of $k[[t]]$ of p -power order that can be expressed by particularly explicit formulas, namely those mapping t to a power series lying in a $\mathbb{Z}/p\mathbb{Z}$ Artin–Schreier extension of $k(t)$. In addition, we give necessary and sufficient criteria to decide when an HKG G -curve with an action of a larger finite group J is also an HKG J -curve.

1. INTRODUCTION

Let k be a field, let $k[[t]]$ be the power series ring, and let $\text{Aut}(k[[t]])$ be its automorphism group as a k -algebra. When the characteristic of k is positive, $\text{Aut}(k[[t]])$ contains many interesting finite subgroups. One way to construct such subgroups is to start with an algebraic curve X on which a finite group G acts with a fixed point x having residue field k ; then G acts on the completion $\hat{\mathcal{O}}_{X,x}$ of the local ring of x at X , and $\hat{\mathcal{O}}_{X,x}$ is isomorphic to $k[[t]]$ for any choice of uniformizing parameter t at x . In fact, results of Harbater [14, §2] and of Katz and Gabber [19, Main Theorem 1.4.1] show that *every* finite subgroup G of $\text{Aut}(k[[t]])$ arises in this way. Their results connect the étale fundamental group of $\text{Spec}(k((t)))$ to that of $\mathbb{P}_k^1 - \{0, \infty\}$. See Section 4.C for further discussion. The value of this technique is that one can study local questions about elements of $\text{Aut}(k[[t]])$ using global tools such as the Hurwitz formula for covers of curves over k .

In this paper we use the above method to study two closely related problems when k is a perfect field of characteristic $p > 0$, which we assume for the rest of this paper. The first problem, described in Section 1.A, is to find explicit formulas for p -power-order elements σ of $\text{Aut}(k[[t]])$. In particular, we study σ that are “almost rational” in the sense of Definition 1.1. Our main result in this direction, Theorem 1.2, classifies all such σ .

Date: August 2, 2016.

2010 *Mathematics Subject Classification.* Primary 14H37; Secondary 14G17, 20F29.

*Supported by NSA Grant # H98230-11-1-0131 and NSF Grant # DMS-1360621.

**Supported by NSF Grants # DMS-1265290 and DMS-1360767, SaTC grant CNS-15136718 and a grant from the Simons Foundation (338379 to Ted Chinburg).

†Supported by NSF Grants # DMS-1069236 and DMS-1601946 and a grant from the Simons Foundation (340694 to Bjorn Poonen).

Published in *Math. Annalen* on October 31, 2016. DOI: 10.1007/s00208-016-1490-2.

The second problem, described in Sections 1.B and 1.C, is to study the full automorphism group of the so-called Harbater–Katz–Gabber G -curves (HKG G -curves), which are certain curves X with a G -action as above. One reason for this study is that it turns out that almost rational automorphisms arise from HKG G -curves X for which $\text{Aut}(X)$ is strictly larger than G . In fact, our Theorems 5.1(c) and 5.9 concerning such X are needed for our proof of Theorem 1.2 on almost rational automorphisms of $k[[t]]$.

For some other applications of HKG G -curves, e.g., to the problem of lifting automorphisms of $k[[t]]$ to characteristic 0, see [4] and its references.

1.A. Finite-order automorphisms of $k[[t]]$. Every order p element of $\text{Aut}(k[[t]])$ is conjugate to $t \mapsto t(1 + ct^m)^{-1/m}$ for some $c \in k^\times$ and some positive integer m prime to p (see [20, Proposition 1.2], [21, §4], and Theorem 2.2).

The natural question arises whether there is an equally explicit description of automorphisms of order p^n for $n > 1$. Each such automorphism is conjugate to $t \mapsto \sigma(t)$ for some $\sigma(t) \in k[[t]]$ that is algebraic over $k(t)$ (see Corollary 4.11). In this case, the field $L := k(t, \sigma(t), \dots, \sigma^{p^n-1}(t)) \subseteq k((t))$ is algebraic over $k(t)$. When $n > 1$, we cannot have $L = k(t)$, because the group $\text{Aut}_k(k(t)) \simeq \text{PGL}_2(k)$ has no element of order p^2 . The next simplest case from the point of view of explicit power series is the following:

Definition 1.1. Call $\sigma \in \text{Aut}(k[[t]])$ **almost rational** if the field $L := k(\{\sigma(t) : \sigma \in G\})$ is a $\mathbb{Z}/p\mathbb{Z}$ Artin–Schreier extension of $k(t)$; i.e., $L = k(t, \beta)$ where $\beta \in k((t))$ satisfies $\wp(\beta) = \alpha$ for some $\alpha \in k(t)$; here $\wp$ is the Artin–Schreier operator defined by $\wp(x) := x^p - x$.

By subtracting an element of $k[t^{-1}]$ from β , we may assume that $\beta \in tk[[t]]$ and hence $\alpha \in k(t) \cap tk[[t]]$. Then we have an explicit formula for β , namely

$$\beta = - \sum_{i=0}^{\infty} \alpha^{p^i},$$

and $\sigma(t)$ is a rational function in t and β . This is the sense in which almost rational automorphisms have explicit power series.

Prior to the present article, two of us found one explicit example of an almost rational σ of order $p^n > p$ (and its inverse); see [5]. Our first main theorem describes *all* such σ up to conjugacy.

Theorem 1.2. *Suppose that σ is an almost rational automorphism of $k[[t]]$ of order p^n for some $n > 1$. Then $p = 2$, $n = 2$, and there exists $b \in k$ (unique modulo $\wp(k) = \{\wp(a) : a \in k\}$) such that σ is conjugate to the order 4 almost rational automorphism*

$$\sigma_b(t) := \frac{b^2t + (b+1)t^2 + \beta}{b^2 + t^2}, \tag{1.3}$$

where β is the unique solution to $\beta^2 - \beta = t^3 + (b^2 + b + 1)t^2$ in $tk[[t]]$.

Remark 1.4. If k is algebraically closed, then $\wp(k) = k$, so Theorem 1.2 implies that all almost rational automorphisms of order 4 lie in one conjugacy class in $\text{Aut}(k[[t]])$.

Remark 1.5. The example in [5] was

$$\begin{aligned}\sigma_0(t) &= t + t^2 + \sum_{j=0}^{\infty} \sum_{\ell=0}^{2^j-1} t^{6 \cdot 2^j + 2\ell} \\ &= t + t^2 + (t^6) + (t^{12} + t^{14}) + (t^{24} + t^{26} + t^{28} + t^{30}) + \dots \\ &= \frac{t}{1+t} + \frac{\gamma}{(1+t)^2}\end{aligned}$$

over $\mathbb{F}_2$, where the series $\gamma := \sum_{i=0}^{\infty} (t^3 + t^4)^{2^i}$ satisfies $\gamma^2 - \gamma = t^3 + t^4$. (If β is as in Theorem 1.2, then $\gamma = \beta + t^2$.) Zieve and Scherr communicated to us that the inverse of σ_0 has a simpler series, namely

$$\sigma_1(t) = t^{-2} \sum_{i=0}^{\infty} (t^3 + t^4)^{2^i} = \sum_{i=0}^{\infty} t^{3 \cdot 2^i - 2} + \sum_{j=2}^{\infty} t^{2^j - 2}.$$

In general, the inverse of σ_b is σ_{b+1} (Remark 5.14).

Remark 1.6. Let σ be any element of finite order in $\text{Aut}(k[[t]])$. Even if σ is not almost rational, we can assume after conjugation that the power series $\sigma(t) = \sum_{i \geq 1} a_i t^i$ is algebraic over $k(t)$, as mentioned above. When k is finite, this implies that the sequence (a_i) is Turing computable, and even *p-automatic*; i.e., there is a finite automaton that calculates a_i when supplied with the base p expansion of i [6, 7].

1.B. Harbater–Katz–Gabber G -curves. An order p^n element of $\text{Aut}(k[[t]])$ induces an injective homomorphism $\mathbb{Z}/p^n\mathbb{Z} \rightarrow \text{Aut}(k[[t]])$. Suppose that we now replace $\mathbb{Z}/p^n\mathbb{Z}$ with any finite group G . Results of Harbater [14, §2] when G is a p -group, and of Katz and Gabber [19, Main Theorem 1.4.1] in general, show that any injective $\alpha: G \rightarrow \text{Aut}(k[[t]])$ arises from a G -action on a curve. More precisely, α arises from a triple (X, x, ϕ) consisting of a smooth projective curve X , a point $x \in X(k)$, and an injective homomorphism $\phi: G \rightarrow \text{Aut}(X)$ such that G fixes x : here α expresses the induced action of G on the completed local ring $\widehat{\mathcal{O}}_{X,x}$ with respect to some uniformizer t . In Section 4.B we will define a Harbater–Katz–Gabber G -curve (HKG G -curve) to be a triple (X, x, ϕ) as above with $X/G \simeq \mathbb{P}_k^1$ such that apart from x there is at most one non-free G -orbit, which is tamely ramified if it exists. We will sometimes omit ϕ from the notation.

HKG G -curves play a key role in our proof of Theorem 1.2. Our overall strategy is to reduce Theorem 1.2 to the classification of certain HKG G -curves, and then to use geometric tools such as the Hurwitz formula to complete the classification.

1.C. Harbater–Katz–Gabber G -curves with extra automorphisms. In this section, (X, x) is an HKG G -curve and J is a finite group such that $G \leq J \leq \text{Aut}(X)$. We do not assume a priori that J fixes x . Let g_X be the genus of X .

Question 1.7. *Must (X, x) be an HKG J -curve?*

The answer is sometimes yes, sometimes no. Here we state our three main theorems in this direction; we prove them in Section 7.

Theorem 1.8. *We have that (X, x) is an HKG J -curve if and only if J fixes x .*

When $g_X > 1$, Theorem 1.10 below gives a weaker hypothesis that still is sufficient to imply that (X, x) is an HKG J -curve. Let J_x be the decomposition group $\text{Stab}_J(x)$.

Definition 1.9. We call the action of J **mixed** if there exists $\sigma \in J$ such that $\sigma(x) \neq x$ and $\sigma(x)$ is nontrivially but tamely ramified with respect to the action of J_x , and **unmixed** otherwise.

Theorem 1.10. *If $g_X > 1$ and the action of J is unmixed, then (X, x) is an HKG J -curve.*

We will also answer Question 1.7 in an explicit way when $g_X \leq 1$, whether or not the action of J is mixed.

Finally, if J is solvable, the answer to Question 1.7 is almost always yes, as the next theorem shows. For the rest of the paper, $\bar{k}$ denotes an algebraic closure of k .

Theorem 1.11. *If J is solvable and (X, x) is not an HKG J -curve, then one of the following holds:*

- $X \simeq \mathbb{P}^1$;
- p is 2 or 3, and X is an elliptic curve of j -invariant 0;
- $p = 3$, and X is isomorphic over $\bar{k}$ to the genus 3 curve $z^4 = t^3u - tu^3$ in $\mathbb{P}^2$; or
- $p = 2$, and X is isomorphic over $\bar{k}$ to the smooth projective model of the genus 10 affine curve $z^9 = (u^2 + u)(u^2 + u + 1)^3$.

Each case in Theorem 1.11 actually arises. We prove a stronger version of Theorem 1.11 in Theorem 7.13 using the examples discussed in Section 6.

2. AUTOMORPHISMS OF $k[[t]]$

The purpose of this section is to recall some basic results about $\text{Aut}(k[[t]])$.

2.A. Groups that are cyclic mod p . A p' -group is a finite group of order prime to p . A finite group G is called **cyclic mod p** if it has a normal Sylow p -subgroup such that the quotient is cyclic. Equivalently, G is cyclic mod p if G is a semidirect product $P \rtimes C$ with P a p -group and C a cyclic p' -group. In this case, P is the unique Sylow p -subgroup of G , and the Schur–Zassenhaus theorem [18, Theorem 3.12] implies that every subgroup of G isomorphic to C is conjugate to C .

2.B. The Nottingham group. Any k -algebra automorphism σ of $k[[t]]$ preserves the maximal ideal and its powers, and hence is t -adically continuous, so σ is uniquely determined by specifying the power series $\sigma(t) = \sum_{n \geq 1} a_n t^n$ (with $a_1 \in k^\times$). The map $\text{Aut}(k[[t]]) \rightarrow k^\times$ sending σ to a_1 is a surjective homomorphism. The Nottingham group $\mathcal{N}(k)$ is the kernel of this homomorphism; it consists of the power series $t + \sum_{n \geq 2} a_n t^n$ under composition. Then $\text{Aut}(k[[t]])$ is a semidirect product $\mathcal{N}(k) \rtimes k^\times$. For background on $\mathcal{N}(k)$, see, e.g., [3].

If k is finite, then $\mathcal{N}(k)$ is a pro- p group. In general, $\mathcal{N}(k)$ is pro-solvable with a filtration whose quotients are isomorphic to k under addition; thus every finite subgroup of $\mathcal{N}(k)$ is a p -group. Conversely, Leedham-Green and Weiss, using techniques of Witt, showed that any finite p -group can be embedded in $\mathcal{N}(\mathbb{F}_p)$; indeed, so can any countably based pro- p group [2]. The embeddability of finite p -groups follows alternatively from the fact that the maximal pro- p quotient of the absolute Galois group of $k((t^{-1}))$ is a free pro- p group of infinite rank [19, (1.4.4)].

On the other hand, any finite subgroup of $k^\times$ is a cyclic p' -group. Thus any finite subgroup of $\text{Aut}(k[[t]])$ is cyclic mod p , and any finite p -group in $\text{Aut}(k[[t]])$ is contained in $\mathcal{N}(k)$.

2.C. Algebraic automorphisms of $k[[t]]$. Call $\sigma \in \text{Aut}(k[[t]])$ algebraic if $\sigma(t)$ is algebraic over $k(t)$.

Proposition 2.1. *The set $\text{Aut}_{\text{alg}}(k[[t]])$ of all algebraic automorphisms of $k[[t]]$ over k is a subgroup of $\text{Aut}(k[[t]])$.*

Proof. Suppose that $\sigma \in \text{Aut}_{\text{alg}}(k[[t]])$, so $\sigma(t)$ is algebraic over $k(t)$. Applying another automorphism $\tau \in \text{Aut}(k[[t]])$ to the algebraic relation shows that $\sigma(\tau(t))$ is algebraic over $k(\tau(t))$. So if τ is algebraic, so is $\sigma \circ \tau$. On the other hand, taking $\tau = \sigma^{-1}$ shows that t is algebraic over $k(\sigma^{-1}(t))$. Since t is not algebraic over k , this implies that $\sigma^{-1}(t)$ is algebraic over $k(t)$. $\square$

2.D. Automorphisms of order p . The following theorem was proved by Klopsch [20, Proposition 1.2] and reproved by Lubin [21, §4] (they assumed that k was finite, but this is not crucial). Over algebraically closed fields it was shown in [1, p. 211] by Bertin and Mézard, who mention related work of Oort, Sekiguchi and Suwa in [22]. For completeness, we give here a short proof, similar to the proofs in [20, Appendix] and [1, p. 211]; it works over any perfect field k of characteristic $p > 0$.

Theorem 2.2. *Every $\sigma \in \mathcal{N}(k)$ of order p is conjugate in $\mathcal{N}(k)$ to $t \mapsto t(1 + ct^m)^{-1/m}$ for a unique positive integer m prime to p and a unique $c \in k^\times$. The automorphisms given by (m, c) and (m', c') are conjugate in $\text{Aut}(k[[t]])$ if and only if $m = m'$ and $c/c' \in k^{\times m}$.*

Proof. Extend σ to the fraction field $k((t))$. By Artin-Schreier theory, there exists $y \in k((t))$ such that $\sigma(y) = y + 1$. This y is unique modulo $k((t))^\sigma$. Since σ acts trivially on the residue field of $k[[t]]$, we have $y \notin k[[t]]$. Thus $y = ct^{-m} + \dots$ for some $m \in \mathbb{Z}_{>0}$ and $c \in k^\times$. Choose y

so that m is minimal. If the ramification index p divided m , then we could subtract from y an element of $k((t))^\sigma$ with the same leading term, contradicting the minimality of m . Thus $p \nmid m$. By Hensel's lemma, $y = c(t')^{-m}$ for some $t' = t + \dots$. Conjugating by the automorphism $t \mapsto t'$ lets us assume instead that $y = ct^{-m}$. Substituting this into $\sigma(y) = y + 1$ yields $c\sigma(t)^{-m} = ct^{-m} + 1$. Equivalently, $\sigma(t) = t(1 + c^{-1}t^m)^{-1/m}$. Rename c^{-1} as c .

Although y is determined only modulo $\wp(k((t)))$, the leading term of a minimal y is determined. Conjugating σ in $\text{Aut}(k[[t]])$ amounts to expressing σ with respect to a new uniformizer $u = u_1t + u_2t^2 + \dots$. This does not change m , but it multiplies c by u_1^m . Conjugating σ in $\mathcal{N}(k)$ has the same effect, except that $u_1 = 1$, so c is unchanged too. $\square$

Remark 2.3. For each positive integer m prime to p , let $\text{Disp}_m: \mathcal{N}(k) \rightarrow \mathcal{N}(k)$ be the map sending $t \mapsto f(t)$ to $t \mapsto f(t^m)^{1/m}$ (we take the m th root of the form $t + \dots$). This is an injective endomorphism of the group $\mathcal{N}(k)$, called m -**dispersal** in [21]. It would be conjugation by $t \mapsto t^m$, except that $t \mapsto t^m$ is not in $\text{Aut}(k[[t]])$ (for $m > 1$). The automorphisms in Theorem 2.2 may be obtained from $t \mapsto t(1+t)^{-1}$ by conjugating by $t \mapsto ct$ and then dispersing.

3. RAMIFICATION AND THE HURWITZ FORMULA

Here we review the Hurwitz formula and related facts we need later.

3.A. Notation. By a **curve** over k we mean a 1-dimensional smooth projective geometrically integral scheme X of finite type over k . For a curve X , let $k(X)$ denote its function field, and let g_X or $g_{k(X)}$ denote its genus. If G is a finite group acting on a curve X , then X/G denotes the curve whose function field is the invariant subfield $k(X)^G$.

3.B. The local different. Let G be a finite subgroup of $\text{Aut}(k[[t]])$. For $i \geq 0$, define the **ramification subgroup** $G_i := \{g \in G \mid g \text{ acts trivially on } k[[t]]/(t^{i+1})\}$ as usual. Let $\mathfrak{d}(G) := \sum_{i=0}^{\infty} (|G_i| - 1) \in \mathbb{Z}_{\geq 0}$; this is the exponent of the **local different** [24, IV, Proposition 4].

3.C. The Hurwitz formula. In this paragraph we assume that k is an algebraically closed field of characteristic $p > 0$. Let H be a finite group acting faithfully on a curve X over k . For each $s \in X(k)$, let $H_s \leq H$ be the inertia group. We may identify $\widehat{\mathcal{O}}_{X,s}$ with $k[[t]]$ and H_s with a finite subgroup $G \leq \text{Aut}(k[[t]])$; then define $\mathfrak{d}_s = \mathfrak{d}_s(H) := \mathfrak{d}(H_s)$. We have $\mathfrak{d}_s > 0$ if and only if s is ramified. If s is tamely ramified, meaning that H_s is a p' -group, then $\mathfrak{d}_s = |H_s| - 1$. The Hurwitz formula [15, IV, 2.4] is

$$2g_X - 2 = |H|(2g_{X/H} - 2) + \sum_{s \in X(k)} \mathfrak{d}_s.$$

Remark 3.1. When we apply the Hurwitz formula to a curve over a perfect field that is not algebraically closed, it is understood that we first extend scalars to an algebraic closure.

3.D. Lower bound on the different. We continue to assume that k is an algebraically closed field of characteristic $p > 0$. The following material is taken from [24, IV], as interpreted by Lubin in [21]. Let G and the G_i be as in Section 3.B. An integer $i \geq 0$ is a **break** in the lower numbering of the ramification groups of G if $G_i \neq G_{i+1}$. Let $b_0, b_1, \dots$ be the breaks in increasing order; they are all congruent modulo p . The group G_0/G_1 embeds into $k^\times$, while G_i/G_{i+1} embeds in the additive group of k if $i \geq 1$.

From now on, assume that G is a cyclic group of order p^n with generator σ . Then $G_0 = G_1$ and each quotient G_i/G_{i+1} is killed by p . Thus there must be exactly n breaks $b_0, \dots, b_{n-1}$. If $0 \leq i \leq b_0$, then $G_i = G$; if $1 \leq j \leq n-1$ and $b_{j-1} < i \leq b_j$, then $|G_i| = p^{n-j}$; and if $b_{n-1} < i$, then $G_i = \{e\}$. According to the Hasse–Arf theorem, there exist positive integers $i_0, \dots, i_{n-1}$ such that $b_j = i_0 + pi_1 + \dots + p^j i_j$ for $0 \leq j \leq n-1$. Then

$$\mathfrak{d}(G) = (i_0 + 1)(p^n - 1) + i_1(p^n - p) + \dots + i_{n-1}(p^n - p^{n-1}). \quad (3.2)$$

The upper breaks $b^{(j)}$ we do not need to define here, but they have the property that in the cyclic case, $b^{(j)} = i_0 + \dots + i_j$ for $0 \leq j \leq n-1$.

Local class field theory shows that $p \nmid b^{(0)}$, that $b^{(j)} \geq pb^{(j-1)}$ for $1 \leq j \leq n-1$, and that if this inequality is strict then $p \nmid b^{(j)}$; this is proved in [24, XV, §2 Thm. 2] for quasi-finite residue fields, and extended to algebraically closed residue fields in [4, Prop. 13.2]. Conversely, any sequence of positive numbers $b^{(0)}, \dots, b^{(n-1)}$ that satisfies these three conditions is realized by some element of order p^n in $\text{Aut}(k[[t]])$ [21, Observation 5].

Thus $i_0 \geq 1$, and $i_j \geq (p-1)p^{j-1}$ for $1 \leq j \leq n-1$. Substituting into (3.2) yields the following result.

Lemma 3.3. *If G is cyclic of order p^n , then*

$$\mathfrak{d}(G) \geq \frac{p^{2n} + p^{n+1} + p^n - p - 2}{p + 1}$$

and this bound is sharp.

Remark 3.4. Lemma 3.3 is valid over any perfect field k of characteristic p , because extending scalars to $\bar{k}$ does not change $\mathfrak{d}(G)$.

4. HARBATER–KATZ–GABBER G -CURVES

Let k be a perfect field of characteristic $p > 0$.

4.A. Pointed G -curves.

Definition 4.1. A **pointed G -curve** over k is a triple (X, x, ϕ) consisting of a curve X , a point $x \in X(k)$, and an injective homomorphism $\phi: G \rightarrow \text{Aut}(X)$ such that G fixes x . (We will sometimes omit ϕ from the notation.)

Suppose that (X, x, ϕ) is a pointed G -curve. The faithful action of G on X induces a faithful action on $k(X)$. Since G fixes x , the latter action induces a G -action on the k -algebras $\mathcal{O}_{X,x}$ and $\widehat{\mathcal{O}}_{X,x}$. Since $\text{Frac}(\mathcal{O}_{X,x}) = k(X)$ and $\mathcal{O}_{X,x} \subseteq \widehat{\mathcal{O}}_{X,x}$, the G -action on $\widehat{\mathcal{O}}_{X,x}$ is faithful too. Since $x \in X(k)$, a choice of uniformizer t at x gives a k -isomorphism $\widehat{\mathcal{O}}_{X,x} \simeq k[[t]]$. Thus we obtain an embedding $\rho_{X,x,\phi}: G \hookrightarrow \text{Aut}(k[[t]])$. Changing the isomorphism $\widehat{\mathcal{O}}_{X,x} \simeq k[[t]]$ conjugates $\rho_{X,x,\phi}$ by an element of $\text{Aut}(k[[t]])$, so we obtain a map

$$\begin{aligned} \{\text{pointed } G\text{-curves}\} &\longrightarrow \{\text{conjugacy classes of embeddings } G \hookrightarrow \text{Aut}(k[[t]])\} \\ (X, x, \phi) &\longmapsto [\rho_{X,x,\phi}]. \end{aligned} \quad (4.2)$$

Also, G is the inertia group of $X \rightarrow X/G$ at x .

Lemma 4.3. *If (X, x, ϕ) is a pointed G -curve, then G is cyclic mod p .*

Proof. The group G is embedded as a finite subgroup of $\text{Aut}(k[[t]])$. □

4.B. Harbater–Katz–Gabber G -curves.

Definition 4.4. A pointed G -curve (X, x, ϕ) over k is called a **Harbater–Katz–Gabber G -curve** (HKG G -curve) if both of the following conditions hold:

- (i) The quotient X/G is of genus 0. (This is equivalent to $X/G \simeq \mathbb{P}_k^1$, since x maps to a k -point of X/G .)
- (ii) The action of G on $X - \{x\}$ is either unramified everywhere, or tamely and nontrivially ramified at one G -orbit in $X(\bar{k}) - \{x\}$ and unramified everywhere else.

Remark 4.5. Katz in [19, Main Theorem 1.4.1] focused on the *base curve* X/G as starting curve. He fixed an isomorphism of X/G with $\mathbb{P}_k^1$ identifying the image of x with ∞ and the image of a tamely and nontrivially ramified point of $X(\bar{k}) - \{x\}$ (if such exists) with 0. He then considered Galois covers $X \rightarrow X/G = \mathbb{P}_k^1$ satisfying properties as above; these were called Katz–Gabber covers in [4]. For our applications, however, it is more natural to focus on the upper curve X .

HKG curves have some good functoriality properties that follow directly from the definition:

- *Base change:* Let X be a curve over k , let $x \in X(k)$, and let $\phi: G \rightarrow \text{Aut}(X)$ be a homomorphism. Let $k' \supseteq k$ be a field extension. Then (X, x, ϕ) is an HKG G -curve over k if and only if its base change to k' is an HKG G -curve over k' .
- *Quotient:* If (X, x, ϕ) is an HKG G -curve, and H is a normal subgroup of G , then X/H equipped with the image of x and the induced G/H -action is an HKG G/H -curve.

Example 4.6. Let P be a finite subgroup of the additive group of k , so P is an elementary abelian p -group. Then the addition action of P on $\mathbb{A}_k^1$ extends to an action $\phi: P \rightarrow \text{Aut}(\mathbb{P}_k^1)$ totally ramified at ∞ and unramified elsewhere, so $(\mathbb{P}_k^1, \infty, \phi)$ is an HKG P -curve.

Example 4.7. Suppose that C is a p' -group and that (X, x, ϕ) is an HKG C -curve. By Lemma 4.3, C is cyclic. By the Hurwitz formula, X must have genus 0 since there are at most two C -orbits of ramified points and all the ramification is tame. Moreover, X has a k -point (namely, x), so $X \simeq \mathbb{P}_k^1$, and C is a p' -subgroup of the stabilizer of x inside $\text{Aut}(X) \simeq \text{Aut}(\mathbb{P}_k^1) \simeq \text{PGL}_2(k)$. It follows that after applying an automorphism of $X = \mathbb{P}_k^1$, we can assume that C fixes the points 0 and ∞ and corresponds to the multiplication action of a finite subgroup of $k^\times$ on $\mathbb{A}_k^1$. Conversely, such an action gives rise to an HKG C -curve $(\mathbb{P}_k^1, \infty, \phi)$.

The following gives alternative criteria for testing whether a pointed G -curve is an HKG G -curve.

Proposition 4.8. *Let (X, x, ϕ) be a pointed G -curve. Let P be the Sylow p -subgroup of G . Then the following are equivalent:*

- (i) (X, x, ϕ) is an HKG G -curve.
- (ii) $(X, x, \phi|_P)$ is an HKG P -curve.
- (iii) The quotient X/P is of genus 0, and the action of P on $X - \{x\}$ is unramified.
- (iv) Equality holds in the inequality $g_X \geq 1 - |P| + \mathfrak{d}_x(P)/2$.

Proof. Let $C = G/P$.

(iii) $\Rightarrow$ (ii): Trivial.

(i) $\Rightarrow$ (iii): By the quotient property of HKG curves, X/P is an HKG C -curve, so $X/P \simeq \mathbb{P}_k^1$ by Example 4.7. At each $y \in X(\bar{k}) - \{x\}$, the ramification index e_y for the P -action divides $|P|$ but is prime to p , so $e_y = 1$. Thus the action of P on $X - \{x\}$ is unramified.

(ii) $\Rightarrow$ (i): Applying the result (i) $\Rightarrow$ (iii) to P shows that $X \rightarrow X/P$ is unramified outside x . There is a covering $\mathbb{P}_k^1 \simeq X/P \rightarrow X/G$, so $X/G \simeq \mathbb{P}_k^1$. We may assume that $C \neq \{1\}$. By Example 4.7, the cover $X/P \rightarrow X/G$ is totally tamely ramified above two k -points, and unramified elsewhere. One of the two points must be the image of x ; the other is the image of the unique tamely ramified G -orbit in $X(\bar{k})$, since $X \rightarrow X/P$ is unramified outside x .

(iii) $\Leftrightarrow$ (iv): The Hurwitz formula (see Remark 3.1) for the action of P simplifies to the inequality in (iv) if we use $g_{X/P} \geq 0$ and discard ramification in $X - \{x\}$. Thus equality holds in (iv) if and only if $g_{X/P} = 0$ and the action of P on $X - \{x\}$ is unramified. $\square$

4.C. The Harbater–Katz–Gabber theorem. The following is a consequence of work of Harbater [14, §2] when G is a p -group and of Katz and Gabber [19, Main Theorem 1.4.1] when G is arbitrary.

Theorem 4.9 (Harbater, Katz–Gabber). *The assignment $(X, x, \phi) \mapsto \rho_{X, x, \phi}$ induces a surjection from the set of HKG G -curves over k up to equivariant isomorphism to the set of conjugacy classes of embeddings of G into $\text{Aut}(k[[t]])$.*

Corollary 4.10. *Any finite subgroup of $\text{Aut}_{\bar{k}}(\bar{k}[[t]])$ can be conjugated into $\text{Aut}_k(k'[[t]])$ for some finite extension k' of k in $\bar{k}$.*

Proof. The subgroup is realized by some HKG curve over $\bar{k}$. Any such curve is defined over some finite extension k' of k . $\square$

Corollary 4.11. *Any finite subgroup of $\text{Aut}(k[[t]])$ can be conjugated into $\text{Aut}_{\text{alg}}(k[[t]])$.*

Proof. The subgroup is realized by some HKG curve X . By conjugating, we may assume that the uniformizer t is a rational function on X . Then each power series $\sigma(t)$ represents another rational function on X , so $\sigma(t)$ is algebraic over $k(t)$. $\square$

5. ALMOST RATIONAL AUTOMORPHISMS

5.A. The field generated by a group of algebraic automorphisms. Let G be a finite subgroup of $\text{Aut}_{\text{alg}}(k[[t]])$. Let $L := k(\{\sigma(t) : \sigma \in G\}) \subseteq k((t))$. Then L is a finite extension of $k(t)$, so $L \simeq k(X)$ for some curve X . The t -adic valuation on $k((t))$ restricts to a valuation on L associated to a point $x \in X(k)$. The G -action on $k((t))$ preserves L . This induces an embedding $\phi : G \rightarrow \text{Aut}(X)$ such that G fixes x , so (X, x, ϕ) is a pointed G -curve over k .

Theorem 5.1. *Let G be a finite subgroup of $\text{Aut}_{\text{alg}}(k[[t]])$. Let L and (X, x, ϕ) be as above. Let $d := [L : k(t)]$.*

- (a) *We have $g_X \leq (d - 1)^2$.*
- (b) *If G is cyclic of order p^n , then $g_X \geq \frac{p(p^n - 1)(p^{n-1} - 1)}{2(p + 1)}$. Moreover, if equality holds, then (X, x, ϕ) is an HKG G -curve.*
- (c) *Suppose that G is cyclic of order p^n . Then*

$$d \geq 1 + \sqrt{\frac{p(p^n - 1)(p^{n-1} - 1)}{2(p + 1)}}. \quad (5.2)$$

In particular, if $d \leq p$ and $n \geq 2$, then $d = p = n = 2$ and (X, x, ϕ) is an HKG $\mathbb{Z}/4\mathbb{Z}$ -curve of genus 1.

Proof.

- (a) In [23, §2], a subfield $F \subseteq L$ is called d -controlled if there exists $e \in \mathbb{Z}_{>0}$ such that $[L : F] \leq d/e$ and $g_F \leq (e - 1)^2$. In our setting, the G -action on $k((t))$ preserves L , so $[L : k(\sigma(t))] = d$ for every $\sigma \in G$. By [23, Corollary 2.2], $L \subseteq L$ is d -controlled. Here $d/e = 1$, so $g_L \leq (e - 1)^2 = (d - 1)^2$.
- (b) In the inequality $g_X \geq 1 - |G| + \mathfrak{d}_x(G)/2$ of Proposition 4.8(iv), substitute $|G| = p^n$ and the bound of Lemma 3.3. If equality holds, then Proposition 4.8(iv) $\Rightarrow$ (i) shows that (X, x, ϕ) is an HKG G -curve.

(c) Combine the upper and lower bounds on g_X in (a) and (b). If $d \leq p$ and $n \geq 2$, then

$$p \geq d \geq 1 + \sqrt{\frac{p(p^2 - 1)(p - 1)}{2(p + 1)}} = 1 + (p - 1)\sqrt{\frac{p}{2}} \geq 1 + (p - 1) = p,$$

so equality holds everywhere. In particular, $p = d$, $n = 2$, and $p/2 = 1$, so $d = p = n = 2$.

Also, (b) shows that (X, x, ϕ) is an HKG G -curve, and $g_X = (d - 1)^2 = 1$. $\square$

Remark 5.3. Part (c) of Theorem 5.1 implies the first statement in Theorem 1.2, namely that if σ is an almost rational automorphism of order $p^n > p$, then $p = n = 2$. To complete the proof of Theorem 1.2 we will classify in Section 5.B the σ when $p = n = 2$.

5.B. Almost rational automorphisms of order 4. In this section, k is a perfect field of characteristic 2, and $G = \mathbb{Z}/4\mathbb{Z}$.

Definition 5.4. For $a, b \in k$, let $E_{a,b}$ be the projective closure of

$$z^2 - z = w^3 + (b^2 + b + 1)w^2 + a.$$

Let $O \in E_{a,b}(k)$ be the point at infinity, and let $\phi: \mathbb{Z}/4\mathbb{Z} \rightarrow \text{Aut}(E_{a,b})$ send 1 to the order 4 automorphism

$$\sigma: (w, z) \mapsto (w + 1, z + w + b).$$

Proposition 5.5. *Each $(E_{a,b}, O, \phi)$ in Definition 5.4 is an HKG $\mathbb{Z}/4\mathbb{Z}$ -curve over k .*

Proof. The automorphism σ fixes O . Also, σ^2 maps (w, z) to $(w, z + 1)$, so σ^2 fixes only O ; hence the G -action on $E_{a,b} - \{O\}$ is unramified. Since $E_{a,b} \rightarrow E_{a,b}/G$ is ramified, the genus of $E_{a,b}/G$ is 0. $\square$

Proposition 5.6. *Let k be a perfect field of characteristic 2. Let $G = \mathbb{Z}/4\mathbb{Z}$. For an HKG G -curve (X, x, ϕ') over k , the following are equivalent:*

- (i) *The genus of X is 1.*
- (ii) *The lower ramification groups for $X \rightarrow X/G$ at x satisfy $|G_0| = |G_1| = 4$, $|G_2| = |G_3| = 2$, and $|G_i| = 1$ for $i \geq 4$.*
- (iii) *The ramification group G_4 equals $\{1\}$.*
- (iv) *There exist $a, b \in k$ such that (X, x, ϕ') is isomorphic to the HKG G -curve $(E_{a,b}, O, \phi)$ of Definition 5.4.*

Proof. Let g be the genus of X . Since G is a 2-group, $|G_0| = |G_1| = 4$.

(ii) $\Rightarrow$ (i): This follows from the Hurwitz formula (see Remark 3.1)

$$2g - 2 = 4(-2) + \sum_{i \geq 0} (|G_i| - 1).$$

(i) $\Rightarrow$ (ii): If $g = 1$, then the Hurwitz formula yields $0 = -8 + 3 + 3 + \sum_{i \geq 2} (|G_i| - 1)$. Since the $|G_i|$ form a decreasing sequence of powers of 2 and include all the numbers 4, 2, and 1 (see Section 3.D), the only possibility is as in (ii).

(ii) $\Rightarrow$ (iii): Trivial.

(iii) $\Rightarrow$ (ii): The lower breaks (see Section 3.D) satisfy $1 \leq b_0 < b_1 < 4$. Since $b_0 \equiv b_1 \pmod{2}$, (ii) follows.

(iv) $\Rightarrow$ (i): The formulas in [25, III.§1] show that $E_{a,b}$ is an elliptic curve, hence of genus 1.

(i) $\Rightarrow$ (iv): By [25, A.1.2(c)], an elliptic curve with an order 4 automorphism has j -invariant $1728 = 0 \in k$. By [25, A.1.1(c)], it has an equation $y^2 + a_3y = x^3 + a_4x + a_6$. Substituting $y \mapsto y + a_3^{-1}a_4x$ leads to an alternative form $y^2 + a_3y = x^3 + a_2x^2 + a$. Let $u \in k^\times$ be such that σ^* acts on $H^0(X, \Omega^1)$ by multiplication by u^{-1} . Then $u^4 = 1$, so $u = 1$. By [25, p. 49], σ has the form $(x, y) \mapsto (x + r, y + sx + t)$ for some $r, s, t \in k$. Since $\sigma^2 \neq 1$, we have $s \neq 0$. Conjugating by a change of variable $(x, y) \mapsto (\epsilon^2x, \epsilon^3y)$ lets us assume that $s = 1$. The condition that $(x, y) \mapsto (x + r, y + x + t)$ preserves $y^2 + a_3y = x^3 + a_2x^2 + a$ implies that $a_3 = r = 1$ and $a_2 = t^2 + t + 1$. Rename t, x, y as b, w, z . $\square$

Corollary 5.7. *The HKG $\mathbb{Z}/4\mathbb{Z}$ -curves that are minimally ramified in the sense of having the smallest value of $\inf\{i : G_i = \{1\}\}$ are those satisfying the equivalent conditions in Proposition 5.6.*

Let $\wp(x) := x^2 - x$ be the Artin–Schreier operator in characteristic 2. The following lemma is clear.

Lemma 5.8. *Let L/K be a $\mathbb{Z}/2\mathbb{Z}$ Artin–Schreier extension, so there exist $a \in K$ and $b \in L - K$ such that $\wp(b) = a$. If $x \in L - K$ satisfies $\wp(x) \in K$, then $x \in b + K$.*

Theorem 5.9. *Let k be a perfect field of characteristic 2. Let $G = \mathbb{Z}/4\mathbb{Z}$. Let $\mathcal{X}$ be the set of HKG G -curves satisfying the equivalent conditions in Proposition 5.6. Then*

- (a) *The map (4.2) restricts to a surjection from $\mathcal{X}$ to the set of conjugacy classes in $\text{Aut}(k[[t]])$ containing an almost rational automorphism of order 4.*
- (b) *Explicitly, $E_{a,b}$ (made into an HKG G -curve as in Proposition 5.5) maps to the conjugacy class of*

$$\sigma_b(t) := \frac{b^2t + (b+1)t^2 + \beta}{b^2 + t^2}, \quad (5.10)$$

where $\beta := \sum_{i=0}^{\infty} (t^3 + (b^2 + b + 1)t^2)^{2^i}$ is the unique solution to $\beta^2 - \beta = t^3 + (b^2 + b + 1)t^2$ in $tk[[t]]$.

- (c) *For $b, b' \in k$, the automorphisms $\sigma_b, \sigma_{b'} \in \text{Aut}(k[[t]])$ are conjugate if and only if $b \equiv b' \pmod{\wp(k)}$.*

Proof.

(a) First we show that each $E_{0,b}$ maps to a conjugacy class containing an almost rational automorphism; the same will follow for $E_{a,b}$ for $a \neq 0$ once we show in the proof of (c) that $E_{a,b}$ gives rise to the same conjugacy class as $E_{0,b}$. Let $P := (0, 0) \in E_{0,b}(k)$. Composing w with translation-by- P yields a new rational function $w_P = z/w^2$ on $E_{0,b}$; define z_P similarly, so $z_P = 1 - z^2/w^3$. Since w has a simple zero at P , the function $t := w_P$ has a simple

zero at O . Also, $\sigma^j(t) \in k(E_{0,b}) = k(t, z_P)$, which shows that σ is almost rational since $z_P^2 - z_P = w_P^3 + (b^2 + b + 1)w_P^2$.

Now suppose that σ is any almost rational automorphism of order 4. Theorem 5.1(c) shows that σ arises from an HKG $\mathbb{Z}/4\mathbb{Z}$ -curve of genus 1, i.e., a curve as in Proposition 5.6(i).

(b) Again by referring to the proof of (c), we may assume $a = 0$. Follow the first half of the proof of (a) for $E_{0,b}$. In terms of the translated coordinates (w_P, z_P) on $E_{0,b}$, the order 4 automorphism of the elliptic curve is

$$(t, \beta) \longmapsto \sigma((t, \beta) - P) + P.$$

It is a straightforward but lengthy exercise to show that the first coordinate equals the expression $\sigma_b(t)$ in (5.10). One uses $t = w_P = z/w^2$, $\beta = z_P = 1 - z^2/w^3$, and the formulas $\sigma(w) = w + 1$ and $\sigma(z) = z + w + b$. In verifying equalities in the field $k(t, \beta)$, one can use the fact that $k(t, \beta)$ is the quadratic Artin–Schreier extension of $k(t)$ defined by $\beta^2 - \beta = t^3 + (b^2 + b + 1)t^2$.

(c) Let $v := w^2 - w$. Let $\widehat{\mathcal{O}}$ be the completion of the local ring of $E_{a,b}$ at the point O at infinity, and let $\widehat{K} := \text{Frac}(\widehat{\mathcal{O}}) = k((w^{-1}))(z^{-1})$. With respect to the discrete valuation on $\widehat{K}$, the valuations of w , z and v are -2 , -3 and -4 , respectively. With respect to the discrete valuation on $k((w^{-1}))$, the valuation of w is -1 and the valuation of v is -2 . We have $\widehat{K}^G = k((v^{-1}))$. Define w' , z' , v' , σ' , $\widehat{\mathcal{O}}'$, and $\widehat{K}' = k((w'^{-1}))(z'^{-1})$ similarly for $E_{a',b'}$. By definition of the map (4.2), $E_{a,b}$ and $E_{a',b'}$ give rise to the same conjugacy class if and only if there exists a G -equivariant continuous isomorphism $\widehat{\mathcal{O}} \xrightarrow{\sim} \widehat{\mathcal{O}}'$ or equivalently $\alpha: \widehat{K} \xrightarrow{\sim} \widehat{K}'$. It remains to prove that α exists if and only if $b \equiv b' \pmod{\wp(k)}$.

$\implies$: Suppose that α exists. Lemma 5.8 shows that $\alpha(w) = w' + f$ for some $f \in k((v'^{-1}))$. Since α preserves valuations, $f \in k[[v'^{-1}]]$. Since v' has valuation -2 in $k((w'^{-1}))$, the valuation of v'^{-1} in this field is 2. Therefore $f \in k[[v'^{-1}]]$ implies $f = c + \sum_{i \geq 2} f_i w'^{-i}$ for some $c, f_i \in k$. Similarly, $\alpha(z) = z' + h$ for some $h = \sum_{i \geq -1} h_i w'^{-i} \in w'k[[w'^{-1}]]$. Subtracting the equations

$$\begin{aligned} \alpha(z)^2 - \alpha(z) &= \alpha(w)^3 + (b^2 + b + 1)\alpha(w)^2 + a \\ z'^2 - z' &= w'^3 + (b'^2 + b' + 1)w'^2 + a' \end{aligned}$$

yields

$$h^2 - h = (w' + f)^3 - w'^3 + (b^2 + b + 1)(w' + f)^2 - (b'^2 + b' + 1)w'^2 + a - a' \quad (5.11)$$

$$= w'^2 f + w' f^2 + f^3 + \wp(b - b')w'^2 + (b^2 + b + 1)f^2 + a - a'$$

$$h^2 - h \equiv (c + \wp(b - b'))w'^2 + c^2 w' + (f_2 + c^3 + (b^2 + b + 1)c^2 + a - a') \pmod{w'^{-1}k[[w'^{-1}]]}. \quad (5.12)$$

Equating coefficients of w' yields $h_{-1} = c^2$. The G -equivariance of α implies

$$\begin{aligned}
\alpha(\sigma(z)) &= \sigma'(\alpha(z)) \\
(z' + h) + (w' + f) + b &= (z' + w' + b') + \sigma'(h) \\
h + f + b &= b' + \sigma'(h) \\
h_{-1}w' + h_0 + c + b &\equiv b' + h_{-1}(w' + 1) + h_0 \pmod{w'^{-1}k[[w'^{-1}]]} \\
b - b' &= h_{-1} - c = c^2 - c = \wp(c).
\end{aligned} \tag{5.13}$$

$\Leftarrow$: Conversely, suppose that $b - b' = \wp(c)$ for some $c \in k$. We must build a G -equivariant continuous isomorphism $\alpha: \widehat{K} \xrightarrow{\sim} \widehat{K}'$. Choose $f := c + \sum_{i \geq 2} f_i w'^{-i}$ in $k[[w'^{-1}]]$ so that the value of f_2 makes the coefficient of w'^0 in (5.12), namely the constant term, equal to 0. The coefficient of w'^2 in (5.12) is $c + \wp(\wp(c)) = c^4$. So (5.12) simplifies to

$$h^2 - h \equiv c^4 w'^2 + c^2 w' \pmod{w'^{-1}k[[w'^{-1}]]}.$$

Thus we may choose $h := c^2 w' + \sum_{i \geq 1} h_i w'^{-i}$ so that (5.11) holds. Define $\alpha: k((w^{-1})) \rightarrow k((w'^{-1}))$ by $\alpha(w) := w' + f$. Equation (5.11) implies that α extends to $\alpha: \widehat{K} \rightarrow \widehat{K}'$ by setting $\alpha(z) := z' + h$. Then $\alpha|_{k((w^{-1}))}$ is G -equivariant since $(w' + 1) + f = (w' + f) + 1$. In other words, $\sigma^{-1}\alpha^{-1}\sigma'\alpha \in \text{Gal}(\widehat{K}/k((w^{-1}))) = \{1, \sigma^2\}$. If $\sigma^{-1}\alpha^{-1}\sigma'\alpha = \sigma^2$, then

$$\begin{aligned}
\alpha\sigma^3 &= \sigma'\alpha \\
\alpha(\sigma^3(z)) &= \sigma'(\alpha(z)) \\
\alpha(z + w + b + 1) &= \sigma'(z' + h) \\
(z' + h) + (w' + f) + b + 1 &= (z' + w' + b') + \sigma'(h);
\end{aligned}$$

by the calculation leading to (5.13), this is off by 1 modulo $w'^{-1}k[[w'^{-1}]]$. Thus $\sigma^{-1}\alpha^{-1}\sigma'\alpha = 1$ instead. In other words, α is G -equivariant. $\square$

Remark 5.14. Changing b to $b + 1$ does not change the curve $E_{a,b}$, but it changes σ to σ^{-1} . Thus σ and σ^{-1} are conjugate in $\text{Aut}(k[[t]])$ if and only if $1 \in \wp(k)$, i.e., if and only if k contains a primitive cube root of unity.

Combining Theorems 5.1(c) and 5.9 proves Theorem 1.2 (and a little more).

6. CONSTRUCTIONS OF HARBATER–KATZ–GABBER CURVES

In this section we construct some examples needed for the proofs of Theorems 1.11 and 7.13. Let k be an algebraically closed field of characteristic $p > 0$. Let (Y, y) be an HKG H -curve over k . If the H -action on $Y - \{y\}$ has a tamely ramified orbit, let S be that orbit; otherwise let S be any H -orbit in $Y - \{y\}$. Let $S' = S \cup \{y\}$. Let $m, n \in \mathbb{Z}_{\geq 1}$. Suppose that $p \nmid n$, that mn divides $|S'|$, that the divisor $\sum_{s \in S'} (s - y)$ is principal, and that for all $s \in S'$, the divisor $m(s - y)$ is principal.

Choose $f \in k(Y)^\times$ with divisor $\sum_{s \in S'} (s - y)$. Let $\pi: X \rightarrow Y$ be the cover with $k(X) = k(Y)(z)$, where z satisfies $z^n = f$. Let $C := \text{Aut}(X/Y)$, so C is cyclic of order n . Let x be the point of $X(k)$ such that $\pi(x) = y$. Let $G := \{\gamma \in \text{Aut}(X) : \gamma|_{k(Y)} \in H\}$.

Proposition 6.1. *Let k, Y, H, S', n, X, C, G be as above.*

- (a) *Every automorphism of Y preserving S' lifts to an automorphism of X (in n ways).*
- (b) *The sequence $1 \rightarrow C \rightarrow G \rightarrow H \rightarrow 1$ is exact.*
- (c) *We have that (X, x) is an HKG G -curve.*

Proof.

- (a) Suppose that $\alpha \in \text{Aut}(Y)$ preserves S' . Then $\text{div}({}^\alpha f/f) = (|S'| + 1)({}^\alpha y - y)$, which is n times an integer multiple of the principal divisor $m({}^\alpha y - y)$, so ${}^\alpha f/f = g^n$ for some $g \in k(Y)^\times$. Extend α to an automorphism of $k(X)$ by defining ${}^\alpha z := gz$; this is well-defined since the relation $z^n = f$ is preserved. Given one lift, all others are obtained by composing with elements of C .
- (b) Only the surjectivity of $G \rightarrow H$ is nontrivial, and that follows from (a).
- (c) The quotient X/G is isomorphic to $(X/C)/(G/C) = Y/H$, which is of genus 0. In the covers $X \rightarrow X/C \simeq Y \rightarrow X/G \simeq Y/H$, all the ramification occurs above and below S' . The valuation of f at each point of S' is $1 \bmod n$, so $X \rightarrow Y$ is totally ramified above S' . Hence each ramified G -orbit in X maps bijectively to an H -orbit in Y , and each nontrivial inertia group in G is an extension of a nontrivial inertia group of H by C . Thus, outside the totally ramified G -orbit $\{x\}$, there is at most one ramified G -orbit and it is tamely ramified. $\square$

Example 6.2. Let $(Y, y) = (\mathbb{P}^1, \infty)$, with coordinate function $t \in k(\mathbb{P}^1)$. Let $H \leq \text{PGL}_2(\mathbb{F}_q)$ be a group fixing ∞ and acting transitively on $\mathbb{A}^1(\mathbb{F}_q)$. (One example is $H := \begin{pmatrix} 1 & \mathbb{F}_q \\ 0 & 1 \end{pmatrix}$.) Let n be a positive divisor of $q + 1$. Then the curve $z^n = t^q - t$ equipped with the point above ∞ is an HKG G -curve, where G is the set of automorphisms lifting those in H . (Here $S' = \mathbb{P}^1(\mathbb{F}_q)$, $m = 1$, and $f = t^q - t \in k(\mathbb{P}^1)$. Degree 0 divisors on $\mathbb{P}^1$ are automatically principal.)

Example 6.3. Let $p = 2$. Let (Y, y) be the j -invariant 0 elliptic curve $u^2 + u = t^3$ with its identity, so $\# \text{Aut}(Y, y) = 24$ [16, Chapter 3, §6]. Let H be $\text{Aut}(Y, y)$ or its Sylow 2-subgroup. Then $k(Y)(\sqrt[3]{t^4 + t})$ is the function field of an HKG G -curve X , for an extension G of H by a cyclic group of order 3. (Here $S' = Y(\mathbb{F}_4)$, which is also the set of 3-torsion points on Y , and $m = n = 3$, and $f = t^4 + t$.) Eliminating t by cubing $z^3 = t^4 + t$ and substituting $t^3 = u^2 + u$ leads to the equation $z^9 = (u^2 + u)(u^2 + u + 1)^3$ for X .

Example 6.4. Let $p = 3$. Let (Y, y) be the j -invariant 0 elliptic curve $u^2 = t^3 - t$ with its identity, so $\# \text{Aut}(Y, y) = 12$ [16, Chapter 3, §5]. Let H be a group between $\text{Aut}(Y, y)$ and

its Sylow 3-subgroup. Then $k(Y)(\sqrt{u})$ is the function field of an HKG G -curve X , for an extension G of H by a cyclic group of order 2. (Here S' is the set of 2-torsion points on Y , and $m = n = 2$, and $f = u$.) Thus X has affine equation $z^4 = t^3 - t$. (This curve is isomorphic to the curve in Example 6.2 for $q = 3$, but $|C|$ here is 2 instead of 4.)

7. HARBATER–KATZ–GABBER CURVES WITH EXTRA AUTOMORPHISMS

We return to assuming only that k is perfect of characteristic p . Throughout this section, (X, x) is an HKG G -curve over k , and J is a finite group such that $G \leq J \leq \text{Aut}(X)$. Let J_x be the decomposition group of x in J . Choose Sylow p -subgroups $P \leq P_x \leq P_J$ of $G \leq J_x \leq J$, respectively. In fact, $P \leq G$ is uniquely determined since G is cyclic mod p by Lemma 4.3; similarly $P_x \leq J_x$ is uniquely determined.

7.A. General results.

Proof of Theorem 1.8. If (X, x) is an HKG J -curve, then J fixes x , by definition.

Now suppose that J fixes x . By Lemma 4.3, J is cyclic mod p . By Proposition 4.8(i) $\Rightarrow$ (ii), (X, x) is an HKG P -curve. Identify X/P with $\mathbb{P}_k^1$ so that x maps to $\infty \in X/P \simeq \mathbb{P}_k^1$.

Case 1: J normalizes G . Then J normalizes also the unique Sylow p -subgroup P of G . In particular, P is normal in P_J . If a p -group acts on $\mathbb{P}_k^1$ fixing ∞ , it must act by translations on $\mathbb{A}_k^1$; applying this to the action of P_J/P on X/P shows that $X/P \rightarrow X/P_J$ is unramified outside ∞ . Also, $X \rightarrow X/P$ is unramified outside x . Thus the composition $X \rightarrow X/P \rightarrow X/P_J$ is unramified outside x . On the other hand, X/P_J is dominated by X/P , so $g_{X/P_J} = 0$. By Proposition 4.8(iii) $\Rightarrow$ (i), (X, x) is an HKG J -curve.

Case 2: J is arbitrary. There exists a chain of subgroups beginning at P and ending at P_J , each normal in the next. Ascending the chain, applying Case 1 at each step, shows that (X, x) is an HKG curve for each group in this chain, and in particular for P_J . By Proposition 4.8(ii) $\Rightarrow$ (i), (X, x) is also an HKG J -curve. $\square$

Corollary 7.1. *We have that (X, x) is an HKG J_x -curve and an HKG P_x -curve.*

Proof. Apply Theorem 1.8 with J_x in place of J . Then apply Proposition 4.8(i) $\Rightarrow$ (ii). $\square$

Lemma 7.2. *Among p' -subgroups of J_x that are normal in J , there is a unique maximal one; call it C . Then C is cyclic, and central in J_x .*

Proof. Let C be the group generated by all p' -subgroups of J_x that are normal in J . Then C is another group of the same type, so it is the unique maximal one. By Lemma 4.3, J_x is cyclic mod p , so J_x/P_x is cyclic. Since C is a p' -group, $C \rightarrow J_x/P_x$ is injective. Thus C is cyclic. The injective homomorphism $C \rightarrow J_x/P_x$ respects the conjugation action of J_x on each group. Since J_x/P_x is abelian, the action on J_x/P_x is trivial. Thus the action on C is trivial too; i.e., C is central in J_x . $\square$

7.B. Low genus cases. Define $A := \text{Aut}(X, x)$, so $G \leq A$. By Theorem 1.8, (X, x) is an HKG J -curve if and only if $J \leq A$. When $g_X \leq 1$, we can describe A very explicitly.

Example 7.3. Suppose that $g_X = 0$. Then $(X, x) \simeq (\mathbb{P}_k^1, \infty)$. Thus $\text{Aut}(X) \simeq \text{PGL}_2(k)$, and A is identified with the image in $\text{PGL}_2(k)$ of the group of upper triangular matrices in $\text{GL}_2(k)$.

Example 7.4. Suppose that $g_X = 1$. Then (X, x) is an elliptic curve, and $\text{Aut}(X) \simeq X(k) \rtimes A$. Let $\mathcal{A} := \text{Aut}(X_{\bar{k}}, x)$ be the automorphism group of the elliptic curve over $\bar{k}$. Now p divides $|G|$, since otherwise it follows from Example 4.7 that $g_X = 0$. Thus G contains an order p element, which by the HKG property has a unique fixed point. Since $G \leq A \leq \mathcal{A}$, the group $\mathcal{A}$ also contains such an element. By the computation of $\mathcal{A}$ (in [16, Chapter 3], for instance), p is 2 or 3, and X is supersingular, so X has j -invariant 0. Explicitly:

- If $p = 2$, then $\mathcal{A} \simeq \text{SL}_2(\mathbb{F}_3) \simeq Q_8 \rtimes \mathbb{Z}/3\mathbb{Z}$ (order 24), and G is $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, Q_8 , or $\text{SL}_2(\mathbb{F}_3)$.
- If $p = 3$, then $\mathcal{A} \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ (order 12), and G is $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, or $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$.

Because of Corollary 7.1, the statement about G is valid also for J_x .

7.C. Cases in which p divides $|G|$. If p divides $|G|$, then we can strengthen Theorem 1.8: see Theorem 7.6 and Corollary 7.7 below.

Lemma 7.5. *If p divides $|G|$ and G is normal in J , then J fixes x .*

Proof. Ramification outside x is tame, so if p divides $|G|$, then x is the unique point fixed by G . If, in addition, J normalizes G , then J must fix this point. $\square$

Theorem 7.6. *If p divides $|G|$, then the following are equivalent:*

- (i) (X, x) is an HKG J -curve.
- (ii) J fixes x .
- (iii) J is cyclic mod p .

Proof.

(i) $\Leftrightarrow$ (ii): This is Theorem 1.8.

(ii) $\Rightarrow$ (iii): This is Lemma 4.3.

(iii) $\Rightarrow$ (i): By Proposition 4.8(i) $\Rightarrow$ (ii), (X, x) is an HKG P -curve. Again choose a chain of subgroups beginning at P and ending at P_J , each normal in the next. Since J is cyclic mod p , we may append J to the end of this chain. Applying Lemma 7.5 and Theorem 1.8 to each step of this chain shows that for each group K in this chain, K fixes x and (X, x) is an HKG K -curve. $\square$

Corollary 7.7. *If p divides $|G|$, then*

- (a) $P_x = P_J$.

- (b) The prime p does not divide the index $(J : J_x)$.
- (c) If $j \in J_x$, then ${}^jP_x = P_x$.
- (d) If $j \notin J_x$, then ${}^jP_x \cap P_x = 1$.
- (e) If J contains a nontrivial normal p -subgroup A , then (X, x) is an HKG J -curve.

Proof.

- (a) Since p divides $|P_x|$ and P_J is cyclic mod p , Corollary 7.1 and Theorem 7.6(iii) $\Rightarrow$ (ii) imply that P_J fixes x . Thus $P_J \leq P_x$, so $P_x = P_J$.
- (b) The exponent of p in each of $|J_x|$, $|P_x|$, $|P_J|$, $|J|$ is the same.
- (c) By Lemma 4.3, J_x is cyclic mod p , so P_x is normal in J_x .
- (d) A nontrivial element of $P_x \cap {}^jP_x$ would be an element of p -power order fixing both x and jx , contradicting the definition of HKG J_x -curve.
- (e) The group A is contained in every Sylow p -subgroup of J ; in particular, $A \leq P_J = P_x$. This contradicts (d) unless $J_x = J$. By Theorem 7.6(ii) $\Rightarrow$ (i), (X, x) is an HKG J -curve. $\square$

Lemma 7.8. *Suppose that $g_X > 1$. Let $A \leq J$ be an elementary abelian ℓ -subgroup for some prime ℓ . Suppose that P_x normalizes A . Then $A \leq J_x$.*

Proof. It follows from Example 4.7 that p divides $|G|$. If $\ell = p$, then $P_x A$ is a p -subgroup of J , but P_x is a Sylow p -subgroup of J by Corollary 7.7(a), so $A \leq P_x \leq J_x$.

Now suppose that $\ell \neq p$. The conjugation action of P_x on A leaves the group $A_x = J_x \cap A$ invariant. By Maschke's theorem, $A = A_x \times C$ for some other subgroup C normalized by P_x . Then $C_x = 1$. By Corollary 7.1, (X, x) is an HKG P_x -curve. Since P_x normalizes C , the quotient X/C equipped with the image y of x and the induced P_x -action is another HKG P_x -curve. Since $C_x = 1$, we have $\mathfrak{d}_x(P_x) = \mathfrak{d}_y(P_x)$; thus Proposition 4.8(i) $\Rightarrow$ (iv) implies that $g_X = g_{X/C}$. Since $g_X > 1$, this implies that $C = 1$. So $A = A_x \leq J_x$. $\square$

7.D. Unmixed actions.

Proof of Theorem 1.10. By the base change property mentioned after Remark 4.5, we may assume that k is algebraically closed. By Corollary 7.1, we may enlarge G to assume that $G = J_x$.

First suppose that the action of G has a nontrivially and tamely ramified orbit, say Gy , where $y \in X(k)$. The Hurwitz formula applied to (X, G) gives

$$2g_X - 2 = -2|G| + \mathfrak{d}_x(G) + |G/G_y|(|G_y| - 1). \quad (7.9)$$

Since the action of J is unmixed, Jx and Jy are disjoint. The Hurwitz formula for (X, J) therefore gives

$$2g_X - 2 \geq -2|J| + |J/G|\mathfrak{d}_x(G) + |J/J_y|(|J_y| - 1). \quad (7.10)$$

Calculating $|J/G|$ times the equation (7.9) minus the inequality (7.10) yields

$$(|J/G| - 1)(2g_X - 2) \leq |J/J_y| - |J/G_y| \leq 0,$$

because $G_y \leq J_y$. Since $g_X > 1$, this forces $J = G$.

If a nontrivially and tamely ramified orbit does not exist, we repeat the proof while omitting the terms involving y . $\square$

7.E. Mixed actions. Here is an example, mentioned to us by Rachel Pries, that shows that Theorem 1.10 need not hold if the action of J is mixed.

Example 7.11. Let n be a power of p ; assume that $n > 2$. Let $k = \mathbb{F}_{n^6}$. Let $\mathcal{X}$ be the curve over k constructed by Giulietti and Korchmáros in [11]; it is denoted $\mathcal{C}_3$ in [13]. Let $J = \text{Aut}(\mathcal{X})$. Let G be a Sylow p -subgroup of J ; by [11, Theorem 7], $|G| = n^3$. Then $\mathcal{X}$ is an HKG G -curve by [13, Lemma 2.5 and proof of Proposition 3.12], and $g_{\mathcal{X}} > 1$ by [11, Thm. 2]. Taking σ in Definition 1.9 to be the automorphism denoted $\tilde{W}$ on [11, p. 238] shows that the action of J on $\mathcal{X}$ is mixed. In fact, [11, Theorem 7] shows that J fixes no k -point of $\mathcal{X}$, so the conclusion of Theorem 1.10 does not hold.

7.F. Solvable groups. Here we prove Theorem 1.11. If p does not divide $|G|$, then Example 4.7 shows that $X \simeq \mathbb{P}_k^1$, so the conclusion of Theorem 1.11 holds. For the remainder of this section, we assume that p divides $|G|$. In this case we prove Theorem 1.11 in the stronger form of Theorem 7.13, which assumes a hypothesis weaker than solvability of J . We retain the notation set at the beginning of Section 7, and let C denote the maximal p' -subgroup of J_x that is normal in J , as in Lemma 7.2.

Lemma 7.12. *Suppose that $g_X > 1$ and that (X, x) is not an HKG J -curve. If J contains a nontrivial normal abelian subgroup, then $C \neq 1$.*

Proof. The last hypothesis implies that J contains a nontrivial normal elementary abelian ℓ -subgroup A for some prime ℓ . By Corollary 7.7(e), $\ell \neq p$. By Lemma 7.8, $A \leq J_x$. Thus $1 \neq A \leq C$. $\square$

Theorem 7.13. *Suppose that p divides $|G|$ and (X, x) is not an HKG J -curve.*

(a) *Suppose that $g_X = 0$, so $\text{Aut}(X) \simeq \text{Aut}(\mathbb{P}_k^1) \simeq \text{PGL}_2(k)$. Then J is conjugate in $\text{PGL}_2(k)$ to precisely one of the following groups:*

- $\text{PSL}_2(\mathbb{F}_q)$ or $\text{PGL}_2(\mathbb{F}_q)$ for some finite subfield $\mathbb{F}_q \leq k$ (these groups are the same if $p = 2$); note that $\text{PSL}_2(\mathbb{F}_q)$ is simple when $q > 3$.
- If $p = 2$ and m is an odd integer at least 5 such that a primitive m th root of unity $\zeta \in \bar{k}$ satisfies $\zeta + \zeta^{-1} \in k$, the dihedral group of order $2m$ generated by $\begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ if $\zeta \in k$, and generated by $\begin{pmatrix} \zeta + \zeta^{-1} + 1 & 1 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ if $\zeta \notin k$. (The case $m = 3$ is listed already, as $\text{PSL}_2(\mathbb{F}_2)$.)
- If $p = 3$ and $\mathbb{F}_9 \leq k$, a particular copy of the alternating group A_5 in $\text{PSL}_2(\mathbb{F}_9)$ (all such copies are conjugate in $\text{PGL}_2(\mathbb{F}_9)$); the group A_5 is simple.

Suppose, in addition, that J contains a nontrivial normal abelian subgroup; then $p \in \{2, 3\}$ and $|P_J| = p$, and if J is conjugate to $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$, then $q = p$.

- (b) Suppose that $g_X = 1$. Then p is 2 or 3, and the limited possibilities for X and J_x are described in Example 7.4. The group J is a semidirect product of J_x with a finite abelian subgroup $T \leq X(k)$.
- (c) Suppose that $g_X > 1$. Let $C \leq J$ be as in Lemma 7.2. Let $Y = X/C$, let y be the image of x under $X \rightarrow Y$, and let $U = \mathrm{Stab}_{J/C}(y)$. If J/C contains a nontrivial normal abelian subgroup (automatic if J is solvable), then one of the following holds:
- i. $p = 3$, $g_X = 3$, $g_Y = 0$, $C \simeq \mathbb{Z}/4\mathbb{Z}$, $P_x \simeq \mathbb{Z}/3\mathbb{Z}$, $(J : J_x) = 4$, and (X, x) is isomorphic over $\bar{k}$ to the curve $z^4 = t^3u - tu^3$ in $\mathbb{P}^2$ equipped with $(t : u : z) = (1 : 0 : 0)$, which is the curve in Example 6.2 with $q = 3$. Moreover,

$$\mathrm{PSL}_2(\mathbb{F}_3) \leq J/C \leq \mathrm{PGL}_2(\mathbb{F}_3).$$

- ii. $p = 2$, $g_X = 10$, $g_Y = 1$, $C \simeq \mathbb{Z}/3\mathbb{Z}$, $P_x \simeq Q_8$, $(J : J_x) = 9$, and (X, x) is isomorphic over $\bar{k}$ to the curve in Example 6.3. The homomorphism $J \rightarrow J/C$ sends the subgroups $J_x \supset P_x$ to subgroups $J_x/C \supset P_xC/C$ of U . Also, $P_xC/C \simeq P_x \simeq Q_8$ and $U \simeq \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, and U acts faithfully on the 3-torsion subgroup $Y[3] \simeq (\mathbb{Z}/3\mathbb{Z})^2$ of the elliptic curve (Y, y) . The group J/C satisfies

$$Y[3] \rtimes Q_8 \simeq (\mathbb{Z}/3\mathbb{Z})^2 \rtimes Q_8 \leq J/C \leq (\mathbb{Z}/3\mathbb{Z})^2 \rtimes \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}) \simeq Y[3] \rtimes U.$$

- iii. $p = 3$, $g_X = 3$, $g_Y = 1$, $C \simeq \mathbb{Z}/2\mathbb{Z}$, $P_x \simeq \mathbb{Z}/3\mathbb{Z}$, $(J : J_x) = 4$, and (X, x) is isomorphic over $\bar{k}$ to the curve $z^4 = t^3u - tu^3$ in $\mathbb{P}^2$ equipped with $(t : u : z) = (1 : 0 : 0)$ as in Example 6.4. The homomorphism $J \rightarrow J/C$ sends the subgroups $J_x \supset P_x$ to subgroups $J_x/C \supset P_xC/C$ of U . Also $P_xC/C \simeq P_x \simeq \mathbb{Z}/3\mathbb{Z}$ and $U \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, and $U/Z(U)$ acts faithfully on the group $Y[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2$. The group J/C satisfies

$$Y[2] \rtimes \mathbb{Z}/3\mathbb{Z} = (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z} \leq J/C \leq (\mathbb{Z}/2\mathbb{Z})^2 \rtimes (\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}) = Y[2] \rtimes U.$$

In each of i., ii., and iii., if (X, x) is the curve over $\bar{k}$ specified, from Examples 6.2–6.4, then any group satisfying the displayed upper and lower bounds for J/C is actually realized as J/C for some subgroup $J \leq \mathrm{Aut}(X)$ satisfying all the hypotheses.

Proof.

(a) The groups listed in the statement of (a) are pairwise non-isomorphic, hence not conjugate. Thus it remains to prove that J is conjugate to one of them. By Corollary 7.7(e), J has no normal Sylow p -subgroup. We will show that *every* finite subgroup $J \leq \mathrm{PGL}_2(k)$ with no normal Sylow p -subgroup is conjugate to a group listed in (a). This would follow immediately from [9, Theorem B], but [9] has not yet been published, so we now give a proof not relying on it. We will use the exact sequence

$$1 \longrightarrow \mathrm{PSL}_2(k) \longrightarrow \mathrm{PGL}_2(k) \xrightarrow{\det} k^\times/k^{\times 2} \longrightarrow 1.$$

Case 1: k is finite and $J \leq \mathrm{PSL}_2(k)$. For finite k , the subgroups of $\mathrm{PSL}_2(k)$ up to conjugacy were calculated by Dickson [8, §260]; see also [17, Ch.2 §8], [26, Ch.3 §6]. The ones with no normal Sylow p -subgroup are among those listed in (a). (Dickson sometimes lists *two* $\mathrm{PSL}_2(k)$ -conjugacy classes of subgroups of certain types, but his proof shows that they map to a single $\mathrm{PGL}_2(k)$ -conjugacy class.)

Case 2: k is infinite and $J \leq \mathrm{PSL}_2(k)$. Let $\tilde{J}$ be the inverse image of J under the finite extension $\mathrm{SL}_2(k) \twoheadrightarrow \mathrm{PSL}_2(k)$. So $\tilde{J}$ is finite. The representation of $\tilde{J}$ on k^2 is absolutely irreducible, since otherwise $\tilde{J}$ would inject into the group $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ of 2×2 upper triangular

invertible matrices over $\bar{k}$, and $\tilde{J}$ would have a normal Sylow p -subgroup $\tilde{J} \cap \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, and J would have one too, contrary to assumption. By [10, Theorem 19.3], this representation is definable over the field k_0 generated by the traces of the elements of $\tilde{J}$. Each trace is a sum of roots of unity, so k_0 is finite. Thus J is conjugate in $\mathrm{PGL}_2(k)$ to a subgroup $J_0 \leq \mathrm{PGL}_2(k_0)$. Conjugation does not change the determinant, so $J_0 \leq \mathrm{PSL}_2(k_0)$. By Case 1, J_0 is conjugate to a group in our list, so J is too.

Case 3: k is finite or infinite, and $J \leq \mathrm{PGL}_2(k)$, but $J \not\leq \mathrm{PSL}_2(k)$. If $p = 2$, then, since k is perfect, $k^\times = k^{\times 2}$, so $\mathrm{PGL}_2(k) = \mathrm{PSL}_2(k)$. Thus $p > 2$. Let $J' := J \cap \mathrm{PSL}_2(k)$. Then J/J' injects into $k^\times/k^{\times 2}$, so $p \nmid (J : J')$. The Sylow p -subgroups of J' are the same as those of J , so J' has exactly one if and only if J has exactly one; i.e., J' has a normal Sylow p -subgroup if and only if J has one. Since J does not have one, neither does J' . By Case 1, we may assume that J' appears in our list.

The group J is contained in the normalizer $N_{\mathrm{PGL}_2(k)}(J')$. We now break into cases according to J' . If J' is $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$ for some subfield $\mathbb{F}_q \leq k$, then $N_{\mathrm{PGL}_2(k)}(J') = \mathrm{PGL}_2(\mathbb{F}_q)$ by [8, §255] (the proof there works even if k is infinite), so $J = \mathrm{PGL}_2(\mathbb{F}_q)$, which is in our list. Recall that $p > 2$, so J' is not dihedral. Thus the only remaining possibility is that $J' \simeq A_5 \leq \mathrm{PSL}_2(\mathbb{F}_9) \leq \mathrm{PGL}_2(k)$. Let $\{1, a\}$ be a subgroup of order 2 in the image of J in $k^\times/k^{\times 2}$ and let J'' be its inverse image in J . Then $J'' < \mathrm{PSL}_2(k(\sqrt{a}))$, so J'' should appear in our list, but $|J''| = 120$ and there is no group of order 120 there for $p = 3$.

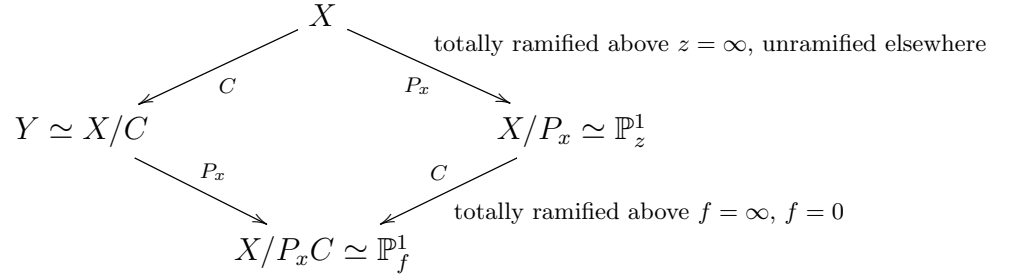
(b) In the notation of Example 7.4, let $\psi: J \rightarrow A$ be the projection. Let $T := \ker \psi \leq X(k)$. Since X is supersingular, T is a p' -group. Let $\bar{J} := \psi(J) \leq A$. Since $G \leq \bar{J} \leq A$, the group $\bar{J}$ is in the list of possibilities in Example 7.4 for G given p . Checking each case shows that its Sylow p -subgroup $\bar{P}_J := \psi(P_J)$ is normal in $\bar{J}$. The action of $\mathrm{Aut}(X)$ on $X(k)$ restricts to the conjugation action of J on the abelian group T , which factors through $\bar{J}$, so $H^0(\bar{P}_J, T) = T^{\bar{P}_J} = T^{P_J} = 0$, since P_J has a unique fixed point on X . Also, $H^i(\bar{P}_J, T) = 0$ for all $i \geq 1$, since $|\bar{P}_J|$ and $|T|$ are coprime. Thus, by the Lyndon–Hochschild–Serre spectral sequence applied to $\bar{P}_J \triangleleft \bar{J}$, we have $H^i(\bar{J}, T) = 0$ for all $i \geq 1$. Therefore the short exact sequence $0 \rightarrow T \rightarrow J \rightarrow \bar{J} \rightarrow 1$ is split, and all splittings are conjugate. Let K be the

image of a splitting $\bar{J} \rightarrow J$. Then K contains a Sylow p -subgroup of J . Equivalently, some conjugate K' of K contains P_J . Since $K' \simeq \bar{J}$ and $\bar{P}_J$ is normal in $\bar{J}$, the group P_J is normal in K' . Since x is the unique fixed point of P_J , this implies that K' fixes x ; i.e., $K' \leq J_x$. On the other hand, $|K'| = |\bar{J}| \geq |J_x|$ since $J_x \cap T = \{e\}$. Hence $K' = J_x$ and $J = T \rtimes J_x$.

(c) We may assume that k is algebraically closed. By Theorem 1.8, (X, x) is an HKG J_x -curve. Then (Y, y) is an HKG J_x/C -curve, but not an HKG J/C -curve since J/C does not fix y . If $g_Y > 1$, then Lemma 7.12 applied to Y yields a nontrivial p' -subgroup $C_1 \leq J_x/C$ that is normal in J/C , and the inverse image of C_1 in J is a p' -subgroup $C_2 \leq J_x$ normal in J with $C_2 \not\supseteq C$, contradicting the maximality of C . Thus $g_Y \leq 1$. Since $g_X > 1$, we have $C \neq 1$. Let $n = |C|$. Let ζ be a primitive n th root of unity in k . Let c be a generator of C .

By Lemma 7.2, C is central in J_x , so $P_x C$ is a direct product. By Corollary 7.1, X is an HKG P_x -curve. Thus $X/P_x \simeq \mathbb{P}^1$, and the P_x -action on X is totally ramified at x and unramified elsewhere. The action of C on X/P_x fixes the image of x , so by Example 4.7, the curves in the covering $X/P_x \rightarrow X/P_x C$ have function fields $k(z) \supseteq k(f)$, where $z^n = f$ and $c z = \zeta z$. Powers of z form a $k(X/P_x C)$ -basis of eigenvectors for the action of c on $k(X/P_x)$.

We may assume that the (totally ramified) image of x in X/P_x is the point $z = \infty$. We obtain a diagram of curves



where the subscript on each $\mathbb{P}^1$ indicates the generator of its function field, and the group labeling each morphism is the Galois group. The field $k(X)$ is the compositum of its subfields $k(Y)$ and $k(X/P_x)$.

Let S be the preimage of the point $f = 0$ under $Y \rightarrow X/P_x C$, and let $S' := S \cup \{y\}$. Comparing the p -power and prime-to- p ramification on both sides of the diagram shows that the point $f = \infty$ totally ramifies in $X \rightarrow Y \rightarrow X/P_x C$, while the point $f = 0$ splits completely into a set S of $|P_x|$ points of Y , each of which is totally ramified in $X \rightarrow Y$. Thus the extension $k(X) \supseteq k(Y)$ is Kummer and generated by the same z as above, and powers of z form a $k(Y)$ -basis of eigenvectors for the action of c on $k(X)$. This extension is totally ramified above S' and unramified elsewhere. The divisor of f on Y is $S - |S|y = S' - |S'|y$, where S here denotes the divisor $\sum_{s \in S} s$, and so on.

Let $j \in J$. Since $C \triangleleft J$, the element j acts on Y and preserves the branch locus S' of $X \rightarrow Y$. Since $X \rightarrow Y$ is totally ramified above S' , the automorphism j fixes x if and only if it fixes y . Since P_x acts transitively on S , and J does not fix x or y , the set S' is the

J -orbit of y . Thus

$$(J : J_x) = |Jx| = |Jy| = |S'| = |P_x| + 1.$$

Suppose that $j \in J - J_x$, so $^jy \neq y$. Then the divisor of $^jf/f$ on Y is

$$(S' - |S'|^jy) - (S' - |S'|y) = |S'|(y - ^jy),$$

which is nonzero. Since C is cyclic and normal, $j^{-1}cj = c^r$ for some r , and hence $^c(jz/z) = ^{jc^r}z/^cz = \zeta^{r-1}(^jz/z)$. Thus $^jz/z$ is a ζ^{r-1} -eigenvector, so $^jz/z = z^{r-1}g$ for some $g \in k(Y)^\times$. Taking n th powers yields $^jf/f = f^{r-1}g^n$. The corresponding equation on divisors is

$$|S'|(y - ^jy) = (r - 1)(S' - |S'|y) + n \operatorname{div}(g). \quad (7.14)$$

Considering the coefficient of a point of $S' - \{y, ^jy\}$ shows that $r - 1 \equiv 0 \pmod{n}$. Then, considering the coefficient of y shows that n divides $|S'|$, and dividing equation (7.14) through by n shows that $(|S'|/n)(y - ^jy)$ is $\operatorname{div}(f^{(r-1)/n}g)$, a principal divisor. If, moreover, $g_Y > 0$, then a difference of points on Y cannot be a principal divisor, so $n \neq |S'|$.

Case 1: $g_Y = 0$. Applying (a) to Y shows that $p \in \{2, 3\}$ and any Sylow p -subgroup of J/C has order p . Since C is a p' -group, $|P_J| = p$ too. By Corollary 7.7(a), $P_x = P_J$, so $|P_x| = p$, and n divides $|S'| = p + 1$. Thus (p, n) is $(2, 3)$, $(3, 2)$, or $(3, 4)$. The Hurwitz formula for $X \rightarrow Y$ yields

$$2g_X - 2 = n(2 \cdot 0 - 2) + \sum_{s \in S'} (n - 1) = -2n + (p + 1)(n - 1).$$

Only the case $(p, n) = (3, 4)$ yields $g_X > 1$. By (a), we may choose an isomorphism $Y \simeq \mathbb{P}_t^1$ mapping y to ∞ such that the J/C -action on Y becomes the standard action of $\operatorname{PSL}_2(\mathbb{F}_3)$ or $\operatorname{PGL}_2(\mathbb{F}_3)$ on $\mathbb{P}_t^1$. Then $S' = Jy = \mathbb{P}^1(\mathbb{F}_3)$. Then f has divisor $S' - 4y = \mathbb{A}^1(\mathbb{F}_3) - 3 \cdot \infty$ on $\mathbb{P}^1$, so $f = t^3 - t$ up to an irrelevant scalar. Since $k(X) = k(Y)(\sqrt[n]{f})$, the curve X has affine equation $z^4 = t^3 - t$. This is the same as the $q = 3$ case of Example 6.2.

Case 2: $g_Y = 1$. Applying (b) (i.e., Example 7.4) to Y shows that either p is 2 and $|P_x|$ divides 8, or $p = 3$ and $|P_x| = 3$; also, Y has j -invariant 0. Also, n divides $|S'| = |P_x| + 1$, but n is not 1 or $|S'|$. Thus $(p, n, |P_x|, |S'|)$ is $(2, 3, 8, 9)$ or $(3, 2, 3, 4)$. The Hurwitz formula as before gives $g_X = 10$ or $g_X = 3$, respectively. Let $m = |S'|/n$. Since $m(y - ^jy)$ is principal for all $j \in J$, if y is chosen as the identity of the elliptic curve, then the J -orbit S' of y is contained in the group $Y[m]$ of m -torsion points. But in both cases, these sets have the same size $|S'| = m^2$. Thus $S' = Y[m]$.

If $p = 2$, the j -invariant 0 curve Y has equation $u^2 + u = t^3$, and $Y[3] - \{y\}$ is the set of points with $t \in \mathbb{F}_4$, so $f = t^4 + t$ up to an irrelevant scalar, and $k(X) = k(Y)(\sqrt[3]{t^4 + t})$. Thus X is the curve of Example 6.3.

If $p = 3$, the j -invariant 0 curve Y has equation $u^2 = t^3 - t$, and $Y[2] - \{y\}$ is the set of points with $u = 0$, so $f = u$ up to an irrelevant scalar, and $k(X) = k(Y)(\sqrt{u}) = k(t)(\sqrt[4]{t^3 - t})$. Thus X is the curve of Example 6.4.

Finally, Proposition 6.1 implies that in each of i., ii., and iii., any group satisfying the displayed upper and lower bounds, viewed as a subgroup of $\text{Aut}(Y)$, can be lifted to a suitable group J of $\text{Aut}(X)$. $\square$

Remark 7.15. Suppose that (X, x) is not an HKG J -curve, $g_X > 1$, and P_J is not cyclic or generalized quaternion. Then [13, Theorem 3.16] shows that J/C is almost simple with socle from a certain list of finite simple groups.

ACKNOWLEDGEMENT

We thank the referee for suggestions on the exposition.

REFERENCES

- [1] J. Bertin and A. Mézard, Déformations formelles des revêtements sauvagement ramifiés de courbes algébriques. *Invent. Math.* 141 (2000), no. 1, 195 – 238.
- [2] R. Camina. Subgroups of the Nottingham group, *J. Algebra* 196, (1997), 101–113.
- [3] R. Camina. The Nottingham group. In: *New horizons in pro- p groups*, pp. 205–221, *Progr. Math.*, 184, Birkhäuser Verlag, Boston, MA, 2000.
- [4] T. Chinburg, R. Guralnick, D. Harbater. The local lifting problem for actions of finite groups on curves. *Annales scientifiques de l'ENS*, 44, (2011), 537-605.
- [5] T. Chinburg, P. Symonds. An element of order 4 in the Nottingham group at the prime 2. [arXiv:1009.5135v1](https://arxiv.org/abs/1009.5135v1)
- [6] G. Christol. Ensembles presque périodiques k -reconnaisables. *Theoret. Comput. Sci.* 9 (1979), 141–145.
- [7] G. Christol, T. Kamae, M. Mendès-France, G. Rauzy. Suites algébriques, automates et substitutions. *Bull. Math. Soc. France* 108 (1980), 401–419.
- [8] L.E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*. Teubner, Leipzig, 1901.
- [9] X. Faber. Finite p -irregular subgroups of $\text{PGL}_2(k)$. [arXiv:1112.1999v2](https://arxiv.org/abs/1112.1999v2).
- [10] W. Feit. *The Representation Theory of Finite Groups*. North Holland, Amsterdam, 1982.
- [11] M. Giulietti, G. Korchmáros. A new family of maximal curves over a finite field. *Math. Ann.* 343 (2009), 229–245.
- [12] B. Green. Realizing deformations of curves using Lubin-Tate formal groups. *Israel J. Math.* 139 (2004), 139–148.
- [13] R. Guralnick, B. Malmskog, R. Pries. The automorphism groups of a family of maximal curves. *J. Algebra* 361 (2012), 92–106.
- [14] D. Harbater. Moduli of p -covers of curves. *Comm. Algebra* 8 (1980), 1095–1122.
- [15] R. Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.
- [16] D. Husemöller. *Elliptic curves*. Graduate Texts in Mathematics, No. 111. Springer-Verlag, New York-Heidelberg, 1987.
- [17] B. Huppert. *Endliche Gruppen I*, *Grundlehren der mathematischen Wissenschaften* 134, Springer-Verlag, New York-Heidelberg, 1967.
- [18] I. M. Isaacs. *Finite group theory*. Graduate Studies in Mathematics, Vol. 92. American Mathematical Society, Providence, 2008.
- [19] N. M. Katz. Local-to-global extensions of representations of fundamental groups. *Ann. Inst. Fourier (Grenoble)* 36 (1986), 69–106

- [20] B. Klopsch. Automorphisms of the Nottingham group. *J. Algebra* 223 (2000), 37–56.
- [21] J. Lubin. Torsion in the Nottingham group. *Bull. London Math. Soc.* 43 (2011), 547–560.
- [22] F. Oort, T. Sekiguchi, and N. Suwa. On the deformation of Artin–Schreier to Kummer. *Ann. Sci. École Norm. Sup. (4)* 22 (1989), no. 3, 345–375.
- [23] B. Poonen. Gonality of modular curves in characteristic p . *Math. Res. Letters* 15 (2008), no. 2, 265–271.
- [24] J.-P. Serre. *Corps locaux*. Publications de l’Institut de Mathématique de l’Université de Nancago, VIII Actualités Sci. Indust., No. 1296. Hermann, Paris, 1962.
- [25] J.H. Silverman. *The arithmetic of elliptic curves*. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.
- [26] M. Suzuki. *Group Theory*. Grundlehren der mathematischen Wissenschaften 247, Springer-Verlag, New York-Heidelberg, 1982.

FRAUKE M. BLEHER, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF IOWA, IOWA CITY, IA 52242, U.S.A.

E-mail address: frauke-bleher@uiowa.edu

TED CHINBURG, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF PENNSYLVANIA, PHILADELPHIA, PA 19104, U.S.A.

E-mail address: ted@math.upenn.edu

BJORN POONEN, DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA 02139, U.S.A.

E-mail address: poonen@math.mit.edu

PETER SYMONDS, SCHOOL OF MATHEMATICS, UNIVERSITY OF MANCHESTER, OXFORD ROAD, MANCHESTER M13 9PL, MANCHESTER M13 9PL UNITED KINGDOM

E-mail address: Peter.Symonds@manchester.ac.uk