

# Algebraic curves with many automorphisms

Massimo Giulietti and Gábor Korchmáros

**This is a post-peer-review, pre-copyedit version of an article published in *Advances in Mathematics*. The final authenticated version is available online at <https://doi.org/10.1016/j.aim.2019.04.003>  
Copyright © 2019. This manuscript version is made available under the CC BY-NC-ND 4.0 license <http://creativecommons.org/licenses/by-nc-nd/4.0>**

## Abstract

Let  $\mathcal{X}$  be a (projective, geometrically irreducible, non-singular) algebraic curve of genus  $g \geq 2$  defined over an algebraically closed field  $\mathbb{K}$  of odd characteristic  $p$ . Let  $\text{Aut}(\mathcal{X})$  be the group of all automorphisms of  $\mathcal{X}$  which fix  $\mathbb{K}$  element-wise. It is known that if  $|\text{Aut}(\mathcal{X})| \geq 8g^3$  then the  $p$ -rank (equivalently, the Hasse-Witt invariant) of  $\mathcal{X}$  is zero. This raises the problem of determining the (minimum-value) function  $f(g)$  such that whenever  $|\text{Aut}(\mathcal{X})| \geq f(g)$  then  $\mathcal{X}$  has zero  $p$ -rank. For *even*  $g$  we prove that  $f(g) \leq 900g^2$ . The *odd* genus case appears to be much more difficult although, for any genus  $g \geq 2$ , if  $\text{Aut}(\mathcal{X})$  has a solvable subgroup  $G$  such that  $|G| > 252g^2$  then  $\mathcal{X}$  has zero  $p$ -rank and  $G$  fixes a point of  $\mathcal{X}$ . Our proofs use the Hurwitz genus formula and the Deuring Shafarevich formula together with a few deep results from Group theory characterizing finite simple groups whose Sylow 2-subgroups have a cyclic subgroup of index 2. We also point out some connections with the Abhyankar conjecture and the Katz-Gabber covers.

## 1 Introduction

Numerous deep results on automorphism groups of algebraic curves, defined over a groundfield of characteristic zero, have been achieved in the passed 125 years following up the seminal work by Hurwitz who was the first to prove that complex curves, other than the rational and elliptic ones, can only have a finite number of automorphisms. Later, Hurwitz's result was given a characteristic-free proof and the fundamental treatment of the theory of automorphisms from the view point of Galois coverings of curves was expanded to include groundfields of positive characteristic. Nevertheless, the theory of automorphism groups of curves present several different features in positive characteristic. This is especially apparent when the curve has many automorphisms, since the classical Hurwitz bound  $|G| \leq 84(g-1)$  on the order of the automorphism group  $\text{Aut}(\mathcal{X})$  of a curve with genus  $g \geq 2$ , may fail in positive characteristic when  $|G|$  is divisible by the characteristic of the groundfield  $\mathbb{K}$ . As a matter of fact, curves in positive characteristic may happen to have much larger  $\mathbb{K}$ -automorphism group compared to their genus. From previous works by Roquette [41], Stichtenoth [42, 47], Henn [28], and Hansen [24], we know infinite families of curves with  $|\text{Aut}(\mathcal{X})| \approx cg^3$  and it is plausible that there exist many others with  $|\text{Aut}(\mathcal{X})| \approx cg^2$ . Although curves with large automorphism groups may have rather different features, they seem to share a common property, namely their  $p$ -rank is equal to zero. This raises the problem of determining a function  $f(g)$  such that if a curve  $\mathcal{X}$  defined over a field of characteristic  $p > 0$  has an automorphism group  $G$  with  $|G| \geq f(g)$  then  $\mathcal{X}$  has zero  $p$ -rank. An

upper bound on  $f(\mathfrak{g})$  is  $8\mathfrak{g}^3$ , as a corollary to Henn's classification [28], see also [29, Theorem 11.127]. Our results stated in Theorems 1.1 and 1.2 show for **odd**  $p$  that if either  $\text{Aut}(\mathcal{X})$  is solvable or  $\mathfrak{g}$  is even then  $f(\mathfrak{g}) > c\mathfrak{g}^2$  for some constant  $c$  independent of  $\mathfrak{g}$  and  $p$ .

For a subgroup  $G$  of  $\text{Aut}(\mathcal{X})$ , a related question is to determine  $p(G)$  and  $G/p(G)$  where  $p(G)$  is the (normal) subgroup of  $G$  generated by its  $p$ -subgroups. The necessary part of the *Abhyankar conjecture for affine curves* states that if  $G$  has exactly  $r$  short orbits then the factor group  $G/p(G)$  has a generating set of size at most  $2\bar{\mathfrak{g}} + r - 1$  where  $\bar{\mathfrak{g}}$  is the genus of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/G$ . If  $\bar{\mathcal{X}}/G$  is rational (in particular when  $G$  is large), then  $G = p(G)$  for  $r = 1$ , and  $G/p(G)$  is cyclic for  $r = 2$ . The Abhyankar conjecture was stated in [1] and proven by Harbater [25]. Recent surveys on this conjecture are found in [39] and [26]. Theorems 1.1 and 1.2 provide a complete description of  $p(G)$  when  $|G| > 900\mathfrak{g}^2$  and either  $G$  is solvable or  $\mathfrak{g}$  is even.

For a subgroup  $G$  of  $\text{Aut}(\mathcal{X})$  the associated Galois cover is a Katz-Gabber  $G$ -cover if  $\mathcal{X}/G$  is rational,  $G$  fixes a point  $P \in \mathcal{X}$ , it has at most one more short orbit  $o$  and  $o$  is tame. Such covers are related with the Nottingham groups consisting of power series over a field  $\mathbb{K}$  of positive characteristic with substitution as group operation, and are useful to understand how the Nottingham groups can be realized as automorphisms of a curve over  $\mathbb{K}$ ; see [6].

**Theorem 1.1.** *Let  $G$  be a solvable automorphism group of an algebraic curve  $\mathcal{X}$  of genus  $\mathfrak{g} \geq 2$ . If*

$$|G| > \frac{p}{p-2} 84\mathfrak{g}^2$$

*then  $\mathcal{X}$  has zero  $p$ -rank. Furthermore,  $G$  fixes a point of  $\mathcal{X}$  and  $G = p(G) \rtimes C$  where  $p(G)$  is a Sylow  $p$ -subgroup of  $G$  and  $C$  is a cyclic group. In particular, the cover  $\mathcal{X}|(\mathcal{X}/G)$  is a Katz-Gabber  $G$ -cover.*

**Theorem 1.2.** *Let  $G$  be a non-solvable automorphism group of an algebraic curve  $\mathcal{X}$  of even genus  $\mathfrak{g} \geq 2$ . If  $|G| > 900\mathfrak{g}^2$  then  $\mathcal{X}$  has zero  $p$ -rank, and  $p(G)$  is isomorphic to one of the following linear groups:  $PSL(2, q)$  for  $q \geq 5$ ,  $PSU(3, q)$  for  $q \equiv 1 \pmod{4}$ ,  $SL(2, q)$  for  $q \geq 5$ ,  $SU(3, q)$  for  $q \equiv 5 \pmod{12}$ , for a power  $q$  of  $p$ .*

In particular,  $G/p(G)$  is a cyclic group according to the Abhyankar conjecture; see Proposition 6.21 and Theorem 7.1. Certain quotient curves of the Hermitian and of the GK curves [12] provide examples covering all cases in Theorem 1.2; see Section 9.

From the framework of this paper, it emerges that the automorphism groups of curves with even genus are subject to several constraints which allow to determine their structures completely; see Theorem 6.1. In some sense, this is an unexpected result since each finite group is the automorphism group of some curve defined over  $\mathbb{K}$ .

The ingredients of the proofs are the Hurwitz genus formula and the Deuring-Shafarevich formula together with a few deep results from Group theory characterizing finite simple groups whose Sylow 2-subgroups have a cyclic subgroup of index 2. We also point out that some of our lemmas are related to the Abhyankar conjecture for curves, although our proof of Theorem 1.2 is independent of it.

The paper is organized as follows.

Section 2 provides the necessary background on Galois coverings of algebraic curves in positive characteristic, it also collects results from Group theory which play a role in the paper.

Section 3 contains the proof of Theorem 1.1 which is carried out by induction on  $\mathfrak{g}$ . In proving the first statement, two cases are distinguished according to whether  $G$  has a normal subgroup of order prime to  $p$ , or all its normal subgroups are  $p$ -groups. In either case we show that if a curve satisfies the hypothesis of Theorem 1.1 but has positive  $p$ -rank, then a quotient curve with respect to a well chosen normal subgroup of  $G$  also satisfies the hypotheses of Theorem 1.1 with genus less than  $\mathfrak{g}$ ; see Propositions 3.3 and 3.5. The

proof of the second statement of Theorem 1.1 is given at the end of the section as a consequence of Lemmas 3.4 and 3.9.

Section 4 gives some new sufficient conditions for a curve to have  $p$ -rank zero; see Lemmas 4.1, 4.6, 4.8, and 4.9. The key achievement is Lemma 4.1, which can be viewed as an improvement on the bound of Theorem 1.1 for a large family of solvable groups. These results are used in several proofs in this paper, and appear to be of independent interest.

The rest of the paper is dedicated to the proof of Theorem 1.2.

The main ingredient is the classification given in Theorem 6.1 where the abstract structure of  $G$  is determined without any assumption on the order of  $G$ . The key point is Lemma 6.2 which together with the classification of 2-groups containing a cyclic subgroup of index 2 allow us to use several deeper results from Group theory obtained within the classification project of finite simple groups. Theorem 6.1 is proved first for solvable groups, then for groups without non-trivial normal subgroups of odd order (see Subsection 6.1), and finally for the general case (see Subsection 6.2).

From Theorem 6.1 it is apparent the central role of a few low dimensional linear and semilinear groups in the study of curves with even genus. This motivates the previous accurate analysis in Section 5 in which a series of rather technical lemmas shows that if the group is large enough with respect to the genus of the curve, then it is linear (and cannot be semilinear) and the  $p$ -rank of the curve must be zero.

For large automorphism groups compared to the genera of the curves, the list in Theorem 6.1 shortens. This is showed in Subsection 6.3; see Lemma 6.19 for odd-core free groups, that is, for groups containing no non-trivial normal subgroup of odd order, and see Proposition 6.21 for the general case.

The proof of the first statement of Theorem 1.2 is given in Section 7. A certain effort is made to fully understand how  $O(G)$  and the center  $Z(G)$  and are related; see Theorem 7.1. The proof is divided into three cases, according to the list given in Proposition 6.21, and also uses deeper result from Group theory.

The second part of Theorem 1.2 is proved in Section 8. It essentially depends on Theorem 7.1 which allows to use Hering's classification [30] of certain 2-transitive group spaces in order to determine the possibilities for  $p(G)$ . Finally, Section 9 provides examples that illustrate Theorem 1.2.

## 2 Background and Preliminary Results

In this paper,  $\text{Aut}(\mathcal{X})$  stands for the automorphism group of a (projective, non-singular, geometrically irreducible, algebraic) curve  $\mathcal{X}$  of genus  $g \geq 2$  defined over an algebraically closed field  $\mathbb{K}$  of odd characteristic  $p$ .

For a subgroup  $G$  of  $\text{Aut}(\mathcal{X})$ , let  $\bar{\mathcal{X}}$  denote a non-singular model of  $\mathbb{K}(\mathcal{X})^G$ , that is, a projective non-singular geometrically irreducible algebraic curve with function field  $\mathbb{K}(\mathcal{X})^G$ , where  $\mathbb{K}(\mathcal{X})^G$  consists of all elements of  $\mathbb{K}(\mathcal{X})$  fixed by every element in  $G$ . Usually,  $\bar{\mathcal{X}}$  is called the quotient curve of  $\mathcal{X}$  by  $G$  and denoted by  $\mathcal{X}/G$ . The field extension  $\mathbb{K}(\mathcal{X})|\mathbb{K}(\mathcal{X})^G$  is Galois of degree  $|G|$ .

Since our approach is mostly group theoretical, we prefer to use notation and terminology from Group theory rather than from Function field theory.

Let  $\Phi$  be the cover of  $\mathcal{X} \rightarrow \bar{\mathcal{X}}$  where  $\bar{\mathcal{X}} = \mathcal{X}/G$  is a quotient curve of  $\mathcal{X}$  with respect to  $G$ . A point  $P \in \mathcal{X}$  is a ramification point of  $G$  if the stabilizer  $G_P$  of  $P$  in  $G$  is non-trivial; the ramification index  $e_P$  is  $|G_P|$ ; a point  $\bar{Q} \in \bar{\mathcal{X}}$  is a branch point of  $G$  if there is a ramification point  $P \in \mathcal{X}$  such that  $\Phi(P) = \bar{Q}$ ; the ramification (branch) locus of  $G$  is the set of all ramification (branch) points. The  $G$ -orbit of  $P \in \mathcal{X}$  is the subset of  $\mathcal{X}$   $o = \{R \mid R = g(P), g \in G\}$ , and it is *long* if  $|o| = |G|$ , otherwise  $o$  is *short*. For a point  $\bar{Q}$ , the  $G$ -orbit  $o$  lying over  $\bar{Q}$  consists of all points  $P \in \mathcal{X}$  such that  $\Phi(P) = \bar{Q}$ . If  $P \in o$  then  $|o| = |G|/|G_P|$  and hence  $\bar{Q}$  is a branch point if and only if  $o$  is a short  $G$ -orbit. It may be that  $G$  has no short orbits.

This is the case if and only if every non-trivial element in  $G$  is fixed-point-free on  $\mathcal{X}$ , that is, the cover  $\Phi$  is unramified. On the other hand,  $G$  has a finite number of short orbits. For a non-negative integer  $i$ , the  $i$ -th ramification group of  $\mathcal{X}$  at  $P$  is denoted by  $G_P^{(i)}$  (or  $G_i(P)$  as in [43, Chapter IV]) and defined to be

$$G_P^{(i)} = \{g \mid \text{ord}_P(g(t) - t) \geq i + 1, g \in G_P\},$$

where  $t$  is a uniformizing element (local parameter) at  $P$ . Here  $G_P^{(0)} = G_P$ . The structure of  $G_P$  is well known; see for instance [43, Chapter IV, Corollary 4] or [29, Theorem 11.49].

**Result 2.1.** *The stabilizer  $G_P$  of a point  $P \in \mathcal{X}$  in  $G$  has the following properties.*

- (i)  $G_P^{(1)}$  is the unique Sylow  $p$ -subgroup of  $G_P$ ;
- (ii) For  $i \geq 1$ ,  $G_P^{(i)}$  is a normal subgroup of  $G_P$  and the quotient group  $G_P^{(i)}/G_P^{(i+1)}$  is an elementary abelian  $p$ -group.
- (iii)  $G_P = G_P^{(1)} \rtimes U$  where the complement  $U$  is a cyclic group whose order is prime to  $p$ .

Let  $\bar{g}$  be the genus of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/G$ . The Hurwitz genus formula gives the following equation

$$2\bar{g} - 2 = |G|(2\bar{g} - 2) + \sum_{P \in \mathcal{X}} d_P. \quad (1)$$

where

$$d_P = \sum_{i \geq 0} (|G_P^{(i)}| - 1). \quad (2)$$

Here  $D(\mathcal{X}|\bar{\mathcal{X}}) = \sum_{P \in \mathcal{X}} d_P$  is the *different*. For a tame subgroup  $G$  of  $\text{Aut}(\mathcal{X})$ , that is for  $p \nmid |G_P|$ ,

$$\sum_{P \in \mathcal{X}} d_P = \sum_{i=1}^m (|G| - \ell_i)$$

where  $\ell_1, \dots, \ell_m$  are the sizes of the short orbits of  $G$ .

A subgroup of  $\text{Aut}(\mathcal{X})$  is a  $p'$ -group (or a prime to  $p$  group) if its order is prime to  $p$ . A subgroup  $G$  of  $\text{Aut}(\mathcal{X})$  is *tame* if the 1-point stabilizer of any point in  $G$  is a  $p'$ -group. Otherwise,  $G$  is *non-tame* (or *wild*). Obviously, every  $p'$ -subgroup of  $\text{Aut}(\mathcal{X})$  is tame, but the converse is not always true. From the classical Hurwitz's bound, if  $|G| > 84(\mathfrak{g}(\mathcal{X}) - 1)$  then  $G$  is non-tame; see [47] or [29, Theorems 11.56]. An orbit  $o$  of  $G$  is *tame* if  $G_P$  is a  $p'$ -group for  $P \in o$ , otherwise  $o$  is a *non-tame orbit* of  $G$ .

**Result 2.2** (Stichtenoth's result on the number of short orbits of large automorphism groups [47]; see also Theorems 11.56 and 11.116 in [29]). *Let  $G$  be a subgroup of  $\text{Aut}(\mathcal{X})$  whose order exceeds  $84(\mathfrak{g}(\mathcal{X}) - 1)$ . Then  $G$  has*

- (a) *exactly three short orbits, two tame and one non-tame, and  $|G| < 24\mathfrak{g}(\mathcal{X})^2$ ;*
- (b) *exactly two short orbits, both non-tame, and  $|G| < 16\mathfrak{g}(\mathcal{X})^2$ ;*
- (c) *only one short orbit which is non-tame;*
- (d) *exactly two short orbits, one tame and one non-tame.*

If  $|G| > 4(\mathfrak{g}(\mathcal{X}) - 1)$  then the quotient curve  $\mathcal{X}/G$  is rational.

**Result 2.3** (Roquette's result [41]). *If the size of  $\text{Aut}(\mathcal{X})$  exceeds  $84(\mathfrak{g}(\mathcal{X}) - 1)$ , then  $\mathfrak{g}(\mathcal{X}) \geq p - 1$ .*

The  $p$ -rank of  $\mathcal{X}$  is defined to be the rank of the (elementary abelian) group of the  $p$ -torsion points in the Jacobian variety of  $\mathcal{X}$ , and it coincides with the Hasse-Witt invariant of  $\mathcal{X}$ . The  $p$ -rank of  $\mathcal{X}$  does not exceed the genus  $\mathfrak{g}(\mathcal{X})$ . Let  $\gamma$  be the  $p$ -rank of  $\mathcal{X}$ , and let  $\bar{\gamma}$  be the  $p$ -rank of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/S$  for a  $p$ -subgroup  $S$  of  $\text{Aut}(\mathcal{X})$ . The Deuring-Shafarevich formula, see [46] or [29, Theorem 11.62], states that

$$\gamma - 1 = |S|(\bar{\gamma} - 1) + \sum_{i=1}^k (|S| - \ell_i) \quad (3)$$

where  $\ell_1, \dots, \ell_k$  are the sizes of the short orbits of  $S$ .

**Result 2.4.** *If  $\mathcal{X}$  has zero  $p$ -rank then  $\text{Aut}(\mathcal{X})$  has the following properties:*

- (i) *a Sylow  $p$ -subgroup of  $\text{Aut}(\mathcal{X})$  fixes a point  $P \in \mathcal{X}$  but its non-trivial elements have no fixed point other than  $P$ ;*
- (ii) *the normalizer of a Sylow  $p$ -subgroup fixes a point of  $\mathcal{X}$ ;*
- (iii) *any two distinct Sylow  $p$ -subgroups have trivial intersection.*

Claim (i) is [29, Theorem 11.129]. Claim (ii) follows from Claim (i). Claim (iii) is [29, Theorem 11.133].

**Result 2.5** (Nakajima's bound [36]; see also [16] and Theorem 11.84 in [29]). *If  $\mathcal{X}$  has positive  $p$ -rank and  $S$  is a  $p$ -subgroup of  $\text{Aut}(\mathcal{X})$  then*

$$|S| \leq \begin{cases} \frac{p}{p-2} (\mathfrak{g}(\mathcal{X}) - 1) & \text{for } \gamma(\mathcal{X}) > 1, \\ \mathfrak{g}(\mathcal{X}) - 1 & \text{for } \gamma(\mathcal{X}) = 1. \end{cases} \quad (4)$$

*If, in addition,  $S$  fixes a point of  $\mathcal{X}$  then  $|S| \leq \frac{p}{p-1} \mathfrak{g}(\mathcal{X})$ .*

We quote a result on the orders of Sylow  $p$ -subgroups in large automorphism groups.

**Result 2.6** (Proposition 11.138 in [29]; see also Theorem 1.1 in [14]). *Let  $\mathcal{X}$  be a curve with  $p$ -rank 0, genus  $\mathfrak{g}(\mathcal{X}) \geq 2$ , and such that  $G$  is a solvable automorphism group of  $\mathcal{X}$  with  $|G| > 24\mathfrak{g}(\mathcal{X})(\mathfrak{g}(\mathcal{X}) - 1)$ . Let  $S$  be a Sylow  $p$ -subgroup of  $G$ . If  $G$  has no fixed point then  $|S| < p^2$ .*

For automorphism groups with special structures or actions on  $\mathcal{X}$ , the classical Hurwitz bound can be improved; see for instance [29, Theorems 11.108, 11.79, 11.60].

**Result 2.7.** (i) *If  $G$  is abelian then  $|G| \leq 4\mathfrak{g}(\mathcal{X}) + 4$ .*

(ii) *If  $G$  has prime order other than  $p$  then  $|G| \leq 2\mathfrak{g}(\mathcal{X}) + 1$ .*

(iii) *If  $G$  fixes a point  $P$  of  $\mathcal{X}$  and its order is prime to  $p$  then  $|G| \leq 4\mathfrak{g}(\mathcal{X}) + 2$ .*

**Result 2.8** (Automorphism groups of elliptic curves and genus 2 curves; see Theorem 11.94, Theorem 11.98, and Proposition 11.99 in [29], and Theorem 2 in [45]). *If  $G$  is an automorphism group of an elliptic curve  $\mathcal{E}$  over  $\mathbb{K}$  then for every point  $P \in \mathcal{E}$  the stabilizer  $G_P$  has order at most 6 when  $p > 3$  and at most 12 when  $p = 3$ . If  $G$  is an automorphism group of an hyperelliptic curve  $\mathcal{H}$  over  $\mathbb{K}$  with hyperelliptic involution  $\omega$  and  $\omega \in G$  then  $G/\langle \omega \rangle$  is isomorphic to a finite subgroup of  $\text{PGL}(2, \mathbb{K})$ . If  $\mathcal{X}$  has genus 2 then  $G/\langle \omega \rangle$  is not isomorphic to either  $\text{PSL}(2, q)$  with  $q \geq 5$ , or  $\text{Alt}_7$ , or the Mathieu group  $M_{11}$ , or  $\text{PSU}(3, q)$  with  $q \geq 5$ , or  $\text{PGU}(3, q)$  with  $q \geq 5$ .*

The results from Group theory which play a role in the paper are quoted below, where  $G$  denotes any abstract finite group. We use standard notation and terminology; see [19, 31, 27]. In particular,  $O(G)$  stands for the largest normal subgroup of  $G$  of odd order. Furthermore,  $q$  denotes a power of an odd prime  $d$ .

**Result 2.9** (Dickson's classification of finite subgroups of the projective linear group  $PGL(2, \mathbb{K})$ ; see [49] and also Theorem A.8 in [29]). *Any finite subgroup of the group  $PGL(2, \mathbb{K})$  is isomorphic to one of the following groups:*

- (i) *prime to  $p$  cyclic groups;*
- (ii) *elementary abelian  $p$ -groups;*
- (iii) *prime to  $p$  dihedral groups;*
- (iv) *the alternating group  $\text{Alt}_4$ ;*
- (v) *the symmetric group  $\text{Sym}_4$ ;*
- (vi) *the alternating group  $\text{Alt}_5$ ;*
- (vii) *the semidirect product of an elementary abelian  $p$ -group of order  $p^h$  by a cyclic group of order  $n > 1$  with  $n \mid (p^h - 1)$ ;*
- (viii)  *$PSL(2, p^f)$ ;*
- (ix)  *$PGL(2, p^f)$ .*

*For  $q > 11$ , the minimal size of a set on which  $PSL(2, q)$  can act transitively is  $q + 1$ ; see [31, Kapitel II, Satz 8.28].*

The maximal subgroups of  $PSU(3, q)$  for  $q$  odd were classified by Mitchell [35]; see also [37] and [29, Theorem A.10]. In this paper we only need the following corollaries of Mitchell's classification; see [35, Theorem 30].

**Result 2.10.** *Let  $\mu = \gcd(3, q + 1)$ . The subgroups of  $PSU(3, q)$  of order  $q^3(q^2 - 1)/\mu$  are maximal. For  $q > 5$ , they are the largest subgroups of  $PSU(3, q)$ . For  $q = 5$  the largest subgroups of  $PSU(3, q)$  have order 2520 and are isomorphic to  $\text{Alt}_7$ . Let  $\Omega$  be a set of smallest size on which  $PSU(3, q)$  has a non-trivial action. Then  $|\Omega| \geq q^3 + 1$  with an exception for  $q = 5$  and  $|\Omega| = 60$ .*

**Result 2.11** (Classification of 2-groups with a cyclic subgroup of index 2; see Theorem 12.5.1 in [27], or Kapitel I, Satz 14.9 in [31]). *The non-cyclic groups of order  $2^n$  which contain a cyclic subgroup of index 2 are generated by two elements  $a, b$  and are of the following types:*

- $a^{2^{n-1}} = 1, b^2 = 1, ba = ab$  (direct product of two cyclic groups);
- $n \geq 3, a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, ba = a^{-1}b$  (generalized quaternion group);
- $n \geq 2, a^{2^{n-1}} = 1, b^2 = 1, ba = a^{-1}b$  (dihedral group);
- $n \geq 4, a^{2^{n-1}} = 1, b^2 = 1, ba = a^{-1+2^{n-2}}b$  (semidihedral - also called quasidihedral - group);
- $n \geq 4, a^{2^{n-1}} = 1, b^2 = 1, ba = a^{1+2^{n-2}}b$  (modular maximal-cyclic group, that is type (3) group with notation as in [31]).

Observe that the dihedral group for  $n = 2$  is an elementary abelian group of order 4. Some elementary properties of the above 2-groups are as follows; see [31, Kapitel I, Satz 14.9]. A generalized quaternion group has rank 1, the other groups listed in Result 2.11 have rank 2 as they contain an elementary abelian group of order 4 but no elementary abelian group of order 8. Generalized quaternion groups, as well as dihedral and semidihedral groups, have center of order 2. Dihedral, semidihedral and modular maximal-cyclic groups have non-central involutions. The quotient groups of a generalized quaternion group, as well as of a semidihedral group, with respect to its center is a dihedral group. A modular maximal-cyclic group has exactly three involutions and four elements of order 4. In particular, it contains neither a dihedral group of order  $2^n \geq 8$  nor a generalized quaternion group.

**Result 2.12** (The Schur-Zassenhaus theorem; see Kapitel I, Hauptsatz 18.1 in [31]). *Let  $N$  be a normal subgroup of  $G$  such that  $|N|$  and  $[G : N]$  are coprime. Then  $N$  has a complement in  $G$ , that is,  $G = N \rtimes U$  for a subgroup  $U$  of  $G$ .*

**Result 2.13** (The Gorenstein-Walter theorem [20, 21]; see also Chapter 16 in [19]). *Let  $G$  be a group with a dihedral Sylow 2-subgroup  $S_2$ . Then, either  $G = O(G) \rtimes S_2$ , or  $G/O(G) \cong \text{Alt}_7$ , or  $G/O(G)$  is isomorphic to a subgroup of  $\text{PGL}(2, q)$  containing  $\text{PSL}(2, q)$ .*

**Result 2.14** (The Brauer-Suzuki theorem [8]; see also Chapter 12 in [19]). *Let  $G$  be a group with a generalized quaternion Sylow 2-subgroup. Then the center of  $G/O(G)$  has order 2.*

Observe that a Sylow 2-subgroup of  $SL(2, q)$  is a generalized quaternion group.

**Result 2.15** (The Alperin-Brauer-Gorenstein theorem [4]). *Let  $G$  be a non-abelian simple group with a semidihedral Sylow 2-subgroup  $S_2$ . Then, either  $G \cong \text{PSL}(3, q)$  with  $q \equiv 3 \pmod{4}$ , or  $G \cong \text{PSU}(3, q)$  with  $q \equiv 1 \pmod{4}$ , or  $G = M_{11}$ , where  $q$  is an odd prime power.*

The 2-rank of a group  $G$  is, by definition, the maximum rank of an abelian 2-subgroup of  $G$ . We also recall that a 2-group is said to be wreathed if it contains the direct product of two cyclic groups of the same order greater than 2 as a subgroup of index 2 and possesses an involution which interchanges the two cyclic groups by conjugation.

**Result 2.16** (The Alperin theorem [3]). *A Sylow 2-subgroup of a non-abelian simple group with 2-rank equal to 2 is either dihedral, or semidihedral, or wreathed, or isomorphic to a Sylow 2-subgroup of  $SU(3, 2)$ .*

A group  $G$  of even order is said to have a normal 2-complement if  $G = O(G) \rtimes S_2$  with a Sylow 2-subgroup  $S_2$  of  $G$ . By an elementary result, see for instance [31, Kapitel I, Aufgaben I.21], the groups of even order with a cyclic Sylow 2-subgroup have a normal 2-complement. More generally, groups with a Sylow 2-subgroup containing a cyclic subgroup of index 2 have a normal 2-complement, apart from some exceptions; see [53, 52].

**Result 2.17.** *If a group  $G$  has no 2-complement but a Sylow 2-subgroup  $S_2$  of  $G$  has a cyclic subgroup of index  $\leq 2$  then  $S_2$  is either a generalized quaternion, or a dihedral group, or a semidihedral group. If, in addition,  $G$  is also solvable then one of the following cases occurs.*

- $S_2$  is dihedral and  $G/O(G) \cong \text{PSL}(2, 3)$ ,  $\text{PGL}(2, 3)$ .
- $S_2$  is semidihedral and  $G/O(G) \cong \text{GL}(2, 3)$ .

**Result 2.18.** *If a group  $G$  has no 2-complement but it has a semidihedral Sylow 2-subgroup, then one of the following holds.*

- (i)  $G$  has a (normal) subgroup of index 2, which has no normal subgroup of index 2 and has a dihedral Sylow 2-subgroup.
- (ii)  $G$  has a (normal) subgroup of index 2, which has no normal subgroup of index 2 and has a generalized quaternion Sylow 2-subgroup.
- (iii)  $G$  has no normal subgroup of index 2, and the involutions of  $G$  form a single conjugacy class.

Let  $G$  be a group with non-trivial center  $Z(G)$ . If  $N$  is a subgroup of  $Z(G)$  with quotient group  $U = G/N$ , then  $G$  is called a central extension of  $U$  by  $N$ . When the sequence splits, that is  $G$  has a subgroup isomorphic to  $U$  that meets  $N$  trivially,  $G$  is called a split extension of  $U$  by  $N$ , and  $G = N \rtimes U$ . If  $N \leq G'$  then the central extension is *stem*, and if  $G$  is *perfect*, that is  $G = G'$ , the central extension is *perfect*.

**Result 2.19** (Schur's result on perfect central extensions of  $PSL(2, q)$ ; see Kapitel V, Satz 25.7 in [31]). *Let  $G$  be a perfect central extension of  $PSL(2, q)$  with  $q \geq 5$ . If  $q \neq 9$  then  $G = SL(2, q)$ . This holds true for  $q = 9$  provided that extension is by a group of order 2.*

**Result 2.20** (Griess' result on perfect central extensions of  $PSU(3, q)$ ; see Theorem 2 in [23]). *The unique perfect central extension of  $PSU(3, q)$  is  $SU(3, q)$ .*

A linear group containing  $SL(2, q)$  as an index 2 subgroups is  $SL^\pm(2, q)$ , that is, the subgroup of  $GL(2, q)$  consisting of all matrices with determinant equal to  $\pm 1$ .  $SL^\pm(2, q)$  contains an involution other than the central involution of  $SL(2, q)$ , and hence its Sylow 2-subgroups are not generalized quaternion groups. More precisely, for  $q \equiv -1 \pmod{4}$  they are semidihedral groups. Similarly, the subgroup  $SU^\pm(2, q)$  of  $GU(2, q)$  consisting of all matrices with determinant equal to  $\pm 1$  contains  $SU(2, q)$  as an index 2 subgroup. Furthermore,  $SL(2, q) \cong SU(2, q)$ . The center of  $SU^\pm(2, q)$  has order either 2 or 4 according to  $q \equiv 1 \pmod{4}$  or  $q \equiv -1 \pmod{4}$ , and in the former case the Sylow 2-subgroups of  $SU^\pm(2, q)$  are semidihedral.

**Result 2.21** (Schur's classification of non-split central extension of  $PGL(2, q)$  by an involution; see p. 176 in [18]). *Let  $G$  be a group with a Sylow 2-subgroup not isomorphic to a generalized quaternion group. If  $G$  is a stem non-split central extension of  $PGL(2, q)$  by a group of order 2 then a Sylow 2-subgroup of  $G$  is semidihedral, and either  $G \cong SL^\pm(2, q)$  or  $G \cong SU^\pm(2, q)$  according to  $q \equiv -1 \pmod{4}$  or  $q \equiv 1 \pmod{4}$ . For each odd  $q$ ,  $PGL(2, q)$  has two non-isomorphic stem non-split central extension by a group of order 2. One has semidihedral Sylow 2-subgroups, the other has generalized quaternion and is denoted by  $SL^{(2)}(2, q)$ .*

**Result 2.22** (Thompson's transfer lemma; see Lemma 5.38 in [48]). *Let  $G$  be a finite group of even order. Let  $M$  be an index 2 subgroup of a Sylow 2-subgroup  $S_2$  of  $G$ . If  $G$  has no subgroup of index 2, then every involution in  $S_2 \setminus M$  is conjugate to an involution in  $M$ .*

**Result 2.23** (The Landázuri and Seitz bound on the degree of cross-representations of  $PSU(3, q)$ ; see [33]). *Assume that  $PSU(3, q)$  has an irreducible, faithful representation as a projective group of the projective space  $PG(r-1, t)$ . If  $t > 2$  is an odd prime and  $q$  is not a  $t$ -power, then  $r-1 \geq q(q-1)$ .*

A group space  $(\Omega, G)$  is a pair where  $\Omega$  is a non-empty set and  $G$  is a group acting on  $\Omega$ . This action is not supposed to be faithful, that is, the permutation representation of  $G$  on  $\Omega$  may have non-trivial kernel. A group space  $(\Omega, G)$  is called transitive if  $G$  induces on  $\Omega$  a transitive permutation group.

**Result 2.24** (Hering's classification on doubly transitive group spaces; see Theorem 2.4 in [30]). *Let  $(\Omega, G)$  be a finite transitive group space, where  $|\Omega| > 2$ . Assume that for some  $\alpha \in \Omega$  the stabiliser  $G_\alpha$  contains a normal subgroup  $Q$  which is sharply transitive on  $\Omega \setminus \{\alpha\}$ . If  $S$  is the normal closure of  $Q$  in  $G$ , then one of the following holds:*

- (i)  $S \cong PSL(2, q), SL(2, q), Sz(q), PSU(3, q), SU(3, q)$  or a group of Ree type of order  $q^3(q^3 + 1)(q - 1)$ , where  $q$  is a prime power and the size of  $\Omega$  is  $q + 1$  in the linear case,  $q^2 + 1$  in the Suzuki case and  $q^3 + 1$  in the unitary and Ree case.
- (ii)  $S \cong PGL(2, 8)$  and  $|\Omega| = 28$ .
- (iii)  $(\Omega, S)$  is sharply 2-transitive.
- (iv)  $|\Omega| = p^2$  for a prime  $p \in \{3, 5, 7, 11, 23, 29, 59\}$ ,

**Result 2.25** (The Gow-Burnside theorem [22]; see Theorem 11.134 in [29]). *If a Sylow  $d$ -subgroup  $S_d$  of a solvable group  $G$  meets any other Sylow  $d$ -subgroup of  $G$  trivially then  $S_d$  is either cyclic, or a normal subgroup of  $G$ , or  $d = 2$  and  $S_d$  is generalized quaternion group.*

**Result 2.26** (The Feit-Thompson theorem [11]). *Every group of odd order is solvable.*

### 3 Large solvable automorphism groups of curves

In this section, our goal is to provide a proof for Theorem 1.1. We begin with the first claim.

**Proposition 3.1.** *Let  $\mathcal{X}$  be an algebraic curve of genus  $\mathfrak{g} \geq 2$  with a solvable subgroup  $G$  of  $\text{Aut}(\mathcal{X})$  such that*

$$|G| > 84 \frac{p}{p-2} \mathfrak{g}^2. \quad (5)$$

*Then the  $p$ -rank of  $\mathcal{X}$  is equal to zero.*

The proof of Proposition 3.1 is by induction on the genus of  $\mathcal{X}$ , and is carried out by a series of lemmas and propositions. By (i) of Result 2.7, the group  $G$  is assumed to be non-abelian. Then, one of the following cases occurs:

- (A)  $G$  has some non-trivial normal  $p'$ -subgroup;
- (B)  $G$  has some non-trivial normal  $p$ -subgroup, but it does not have any non-trivial normal  $p'$ -subgroup.

We investigate Case (A).

**Lemma 3.2.** *Under the hypotheses of Proposition 3.1, if (A) holds then one of the following cases occurs.*

- (C) *For any normal  $p'$ -subgroup  $N$  of  $G$  of maximal order the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/N$  has zero  $p$ -rank.*
- (D) *Some curve of genus less than  $\mathfrak{g}$  is a counterexample to Proposition 3.1 for an automorphism group satisfying Property (B).*

*Proof.* Claim (C) certainly holds if  $\bar{\mathcal{X}}$  is rational.

If  $\bar{\mathcal{X}}$  is elliptic, take a Sylow  $p$ -subgroup  $S$  of  $G$ . Since (5) yields  $|G| > 84(\mathfrak{g} - 1)$ , Result 2.2 shows that  $G$  has a non-tame orbit on  $\mathcal{X}$ . Hence, some non-trivial subgroup of  $S$  fixes a point of  $\mathcal{X}$ . Let  $\bar{S} = SN/N$ . Then  $\bar{S}$  is a Sylow  $p$ -subgroup of  $\bar{G} = G/N$ , and some non-trivial subgroup  $\bar{T}$  of  $\bar{S}$  fixes a point of  $\bar{\mathcal{X}}$ . From Result 2.8,  $|\bar{T}| = 3$  (and  $p = 3$ ). The Deuring-Shafarevich formula applied to  $\bar{T}$  gives  $\gamma(\bar{\mathcal{X}}) - 1 = 3(\gamma(\bar{\mathcal{Y}}) - 1) + 2\lambda$  where  $\bar{\mathcal{Y}}$  is the quotient curve of  $\bar{\mathcal{X}}$  by  $\bar{T}$  while  $\lambda > 0$  is the number of fixed points of  $\bar{T}$  on  $\bar{\mathcal{X}}$ . Since  $0 \leq \gamma(\bar{\mathcal{Y}}) \leq \gamma(\bar{\mathcal{X}}) \leq \mathfrak{g}(\bar{\mathcal{X}}) = 1$ , this equation implies  $\gamma(\bar{\mathcal{X}}) = 0$ . Then Claim (C) also holds for  $\mathfrak{g}(\bar{\mathcal{X}}) = 1$ . If  $\mathfrak{g} = 2$ , then  $\mathcal{X}$  is either rational or elliptic and both cases have already been considered.

Therefore,  $\mathfrak{g} \geq 3$  and  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 2$  are assumed. From the Hurwitz genus formula applied to  $N$ ,

$$\mathfrak{g} \geq |N|(\mathfrak{g}(\bar{\mathcal{X}}) - 1) + 1.$$

This together with  $(|N|(\mathfrak{g}(\bar{\mathcal{X}}) - 1) + 1)^2 > |N|\mathfrak{g}(\bar{\mathcal{X}})^2$  yield

$$|\bar{G}| = \frac{|G|}{|N|} > \frac{p}{p-2} 84 \frac{\mathfrak{g}^2}{|N|} > \frac{p}{p-2} 84 \mathfrak{g}(\bar{\mathcal{X}})^2.$$

The group  $\bar{G}$  is a non-abelian solvable group and hence it has a non-trivial minimal normal subgroup  $\bar{M}$ . Let  $M$  be the normal subgroup of  $G$  containing  $N$  such that  $M/N = \bar{M}$ . Then  $p$  divides  $|M|$  as  $N$  has been chosen to be a maximal normal  $p'$ -subgroup of  $G$ . Since  $p \nmid |N|$ , this yields that  $p$  divides  $|\bar{M}|$ , as well. Since  $\bar{M}$  is a minimal normal subgroup, and  $G$  is solvable,  $\bar{M}$  is a normal (elementary abelian)  $p$ -subgroup of  $\bar{G}$ . If the  $p$ -rank of  $\bar{\mathcal{X}}$  is positive,  $\bar{\mathcal{X}}$  turns out to be a counterexample to Proposition 3.1 for its automorphism group  $\bar{G}$  satisfying property (B).  $\square$

**Proposition 3.3.** *Under the hypotheses of Proposition 3.1, if (A) holds then either  $\mathcal{X}$  has zero  $p$ -rank, or (D) holds.*

*Proof.* Among the normal  $p'$ -subgroups of  $G$  choose one, say  $N$ , of maximal order. Let  $\bar{M}$  be a normal (elementary abelian)  $p$ -subgroup of  $\bar{G}$  defined as in the final part of the proof of Lemma 3.2.

By Lemma 3.2 we may assume that (C) holds. Then  $\gamma(\bar{\mathcal{X}}) = 0$ , and hence  $\bar{M}$  fixes a unique point  $\bar{P} \in \bar{\mathcal{X}}$ , by (i) of Result 2.4.

Let  $\theta$  be the  $N$ -orbit consisting of all points of  $\mathcal{X}$  lying over  $\bar{P}$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ . Since  $p \nmid |N|$ , we also have  $p \nmid |\theta|$ . Furthermore, as  $\bar{M}$  is a normal subgroup of  $\bar{G}$ ,  $\bar{P}$  is fixed by  $\bar{G}$ , as well. Therefore,  $\theta$  is a  $G$ -orbit. Choose a point  $P \in \theta$ . Then  $|G| = |G_P||\theta|$  and (iii) of Result 2.1 shows that the stabilizer  $G_P$  of  $P$  in  $G$  is the semidirect product of a Sylow  $p$ -subgroup  $S$  of  $G_P$  by a cyclic group  $H$  of order  $h$  with  $p \nmid h$ . Actually,  $S$  is a Sylow  $p$ -subgroup of  $G$  since  $p$  does not divide  $|\theta|$ .

If  $\theta = \{P\}$  then  $G = G_P = S \rtimes H$ . From this and (5),  $24\mathfrak{g}^2 < |G| = |S||H| \leq |S|(4\mathfrak{g} + 2)$  by (iii) of Result 2.7 whence

$$|S| > \frac{24\mathfrak{g}^2}{4\mathfrak{g} + 2} > 6 \frac{\mathfrak{g}^2}{\mathfrak{g} + 1} > 4\mathfrak{g}.$$

From Result 2.5,  $\mathcal{X}$  has zero  $p$ -rank.

Therefore,  $|\theta| \geq 2$  is assumed. Since  $N$  is a normal subgroup of  $G$ , the set  $L = NH$  is a subgroup of  $G$  whose order  $|L|$  is equal to  $|H||N|/|H \cap N|$ . Obviously,  $\theta$  is an  $L$ -orbit, and hence  $|L| = |L_P||\theta|$  with  $L_P$  being the stabilizer of  $P$  in  $L$  and  $H \leq L_P$ . Since  $|G| = |G_P||\theta| = |S||H||\theta|$ , the Lagrange theorem yields that

$$\frac{|G|}{|L|} = |S| \frac{|H|}{|L_P|}$$

is an integer. Since  $|S|$  and  $|L_P|$  are coprime, this yields that  $|L_P|$  must divide  $|H|$ . Hence,  $L_P$  cannot contain  $H$  properly. Therefore,  $H = L_P$ , and  $|G| = |S||L_P||\theta| = |S||L|$ . As  $p$  does not divide  $|L|$ , Result 2.2 yields  $|L| \leq 84(\mathfrak{g} - 1)$ . It turns out that

$$84 \frac{p}{p-2} \mathfrak{g}^2 < |G| = |S||L| \leq |S|84(\mathfrak{g} - 1) < 84|S|\mathfrak{g}, \quad (6)$$

whence  $|S| > \frac{p}{p-2}\mathfrak{g}$ . From Result 2.5,  $\mathcal{X}$  has zero  $p$ -rank.  $\square$

**Lemma 3.4.** *Under the hypotheses of Proposition 3.1, if (A) holds and  $\mathcal{X}$  has zero  $p$ -rank then  $G$  fixes a point.*

*Proof.* Among the normal  $p'$ -subgroups of  $G$  choose one, say  $N$ , of maximal order and let  $\bar{\mathcal{X}} = \mathcal{X}/N$ . Let  $M$  and  $\bar{M}$  be as in the final part of the proof of Lemma 3.2. We first show that  $\bar{M}$  fixes a unique point  $\bar{P} \in \bar{\mathcal{X}}$ . Since  $|M| = |\bar{M}||N|$ , from Result 2.12, there exists a  $p$ -subgroup  $T$  in  $G$  such that  $M = N \rtimes T$ . Clearly,  $\bar{T} = T/N$  coincides with  $\bar{M}$ . By (i) of Result 2.4,  $T$  fixes a point  $P \in \mathcal{X}$  and no non-trivial element of  $T$  fixes a point other than  $P$ . Therefore,  $\bar{T}$  fixes the point  $\bar{P}$  lying under  $P$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ . Assume that  $\bar{T}$  fixes a point  $\bar{Q} \neq \bar{P}$ . The  $N$ -orbit  $\omega$  consisting of all points lying over  $\bar{Q}$  is left invariant by  $M$ . Since  $|\omega|$  divides  $|N|$  and  $p$  is prime to  $|N|$ ,  $p$  is prime to  $|\omega|$  as well. Then  $T$  must fix a point  $Q \in \omega$ . Since  $P \notin \omega$ , this contradicts (i) of Result 2.4. Therefore,  $\bar{P}$  is the unique fixed point of  $\bar{M}$ . Since  $\bar{M}$  is a normal subgroup of  $\bar{G}$ ,  $\bar{P}$  is the unique fixed point of  $\bar{G}$ , as well. This shows that  $\omega$  is a non-tame short orbit of  $G$ . If  $\omega = \{P\}$ , then  $G$  fixes  $P$ . Otherwise, the final part in the proof of Proposition 3.3 shows that  $|G| \leq |S|84(\mathfrak{g} - 1)$  where  $S$  is the Sylow  $p$ -subgroup of  $G$  fixing  $P$ . This together with our hypothesis (5) give  $|S| > \frac{p}{p-1}\mathfrak{g}$ . On the other hand,  $\mathfrak{g} \geq p-1$  by Result 2.3. Therefore  $|S| > p$  and hence  $|S| \geq p^2$ . By Result 2.6  $G$  fixes a point.  $\square$

So far, we have proven that if a counterexample for Proposition 3.1 exists then Case (D) must hold. Therefore, we are left with Case (B).

**Proposition 3.5.** *Under the hypotheses of Proposition 3.1, if (B) holds then either  $\mathcal{X}$  has zero  $p$ -rank, or (D) occurs.*

*Proof.* Choose a maximal normal  $p$ -subgroup  $N$  of  $G$ . Then  $|N| = p^h$  with  $h \geq t$ , and the factor group  $\bar{G} = G/N$  contains no normal  $p$ -subgroup. If  $\bar{G}$  is trivial then  $G = N$ , that is,  $G$  is a  $p$ -group, and  $\gamma(\mathcal{X}) = 0$  by Result 2.5. Therefore  $|\bar{G}| > 1$  is assumed. Let  $S$  be a Sylow  $p$ -subgroup of  $G$ . Then  $S \geq N$ . From Result 2.2,  $G$  has a unique non-tame short orbit, say  $\theta$ . Since  $N$  is a normal subgroup,  $\theta$  is partitioned into  $N$ -orbits, each of the same length  $p^{h-k}$  where  $p^k = |N_P|$  for any point  $P \in \theta$ . If  $\lambda$  counts the components of the partition, then  $N$  has exactly  $\lambda$  short orbits and  $|\theta| = \lambda p^{h-k}$ .

Now we prove three preliminary claims that will be useful when dealing separately, as usual, with the cases  $\mathfrak{g}(\bar{\mathcal{X}}) = 0, 1, \geq 2$  for the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/N$ .

**Claim 3.6.** *If  $S = N$ , or  $|\theta| = 1$  then  $\mathcal{X}$  has zero  $p$ -rank.*

*Proof.* If  $S = N$  then by Result 2.12,  $G = S \rtimes L$  with a  $p'$ -subgroup  $L$  of  $G$ . Therefore,  $|G| = |S||L| \leq |S|84(\mathfrak{g} - 1)$  whence  $|S| > \frac{p}{p-2} \cdot \frac{\mathfrak{g}(\mathcal{X})^2}{\mathfrak{g}(\bar{\mathcal{X}})-1}$ . Hence  $\mathcal{X}$  has zero  $p$ -rank by Result 2.5. Therefore,  $S \supsetneq N$  is assumed. Then  $\bar{S} = S/N$  is a non-trivial  $p$ -subgroup of  $\text{Aut}(\bar{\mathcal{X}})$ . If  $|\theta| = 1$  then  $G$  would fix a point and Result 2.1 would imply  $S = N$ .  $\square$

Therefore,  $S \supsetneq N$  and  $|\theta| > 1$  are assumed.

**Claim 3.7.** *If  $\lambda = 1$  then  $\gamma(\bar{\mathcal{X}}) \geq 2$ .*

*Proof.* For  $\lambda = 1$ , the Deuring-Shafarevich formula applied to  $N$  gives  $\gamma(\mathcal{X}) - 1 = p^h(\gamma(\bar{\mathcal{X}}) - 1) + (p^h - p^{h-k})$ . From this  $\gamma(\bar{\mathcal{X}}) - 1 \geq 0$ , otherwise  $\gamma(\mathcal{X}) = 0$ . Furthermore, if  $\gamma(\bar{\mathcal{X}}) = 1$  then  $\gamma(\mathcal{X}) - 1 = p^h - p^{h-k}$ . On the other hand, if  $\mathcal{X}$  has positive  $p$ -rank then Result 2.5 together with  $|S| > |N|$  yield  $\gamma(\mathcal{X}) - 1 \geq \frac{p-2}{p}|S| \geq \frac{p-2}{p}p^{h+1}$ . Therefore,

$$p^h - p^{h-k} \geq (p-2)p^h,$$

a contradiction with  $p > 2$ .  $\square$

**Claim 3.8.** *If  $\lambda > 1$ , then some non-trivial subgroup of  $\bar{S} = S/N$  has a fixed point on  $\bar{\mathcal{X}}$ .*

*Proof.* We show that if  $\lambda > 1$  then  $G_P^{(1)} \not\cong N_P$  for any point  $P \in \theta$ . For  $|N_P| = 1$ , this is trivial. Thus  $k > 0$  is assumed. From the Deuring-Shafarevich formula applied to  $N$ ,  $\gamma(\mathcal{X}) - 1 = p^h(\gamma(\bar{\mathcal{X}}) - 1) + \lambda(p^h - p^{h-k}) \geq -p^h + \lambda(p^h - p^{h-k})$  whence

$$\gamma(\mathcal{X}) - 1 \geq \lambda p^h \left(1 - \frac{1}{\lambda} - \frac{1}{p^k}\right) \geq \lambda p^h \left(1 - \frac{1}{2} - \frac{1}{3}\right) \geq \frac{1}{6} \lambda p^h = \frac{1}{6} p^k |\theta|. \quad (7)$$

According to (iii) of Result 2.7, for a point  $P \in \theta$  write  $G_P = G_P^{(1)} \rtimes H$  where  $H$  is a  $p'$ -subgroup of  $G$  fixing  $P$ . Then  $|H| \leq 4\mathfrak{g} + 2$  by (iii) of Result 2.7. Now if  $G_P^{(1)} = N_P$ , this together with (7) would yield  $6(\mathfrak{g}(\mathcal{X}) - 1) \geq 6(\gamma(\mathcal{X}) - 1) \geq |G_P^{(1)}| |\theta|$  whence

$$24\mathfrak{g}(\mathcal{X})^2 > 6(4\mathfrak{g}(\mathcal{X}) + 2)(\mathfrak{g}(\mathcal{X}) - 1) \geq |G_P^{(1)}| |H| |\theta| = |G|,$$

a contradiction. □

Since Case (B) occurs and  $G$  is not  $p$ -group,  $\bar{G}$  has a non-trivial minimal normal subgroup  $\bar{T}$  which is an elementary abelian group of order  $d^j$  with a prime  $d \neq p$ . Let  $T$  be the subgroup of  $G$  containing  $N$  such that  $\bar{T} = T/N$ . Three cases are investigated separately according to the values of  $\mathfrak{g}(\bar{\mathcal{X}})$ .

If  $\bar{\mathcal{X}}$  is rational, then  $\bar{G}$  is isomorphic to a subgroup of  $PGL(2, \mathbb{K})$  of order divisible by  $p$  which has a normal  $p'$ -subgroup isomorphic to  $\bar{T}$ . From Result 2.9,  $p = 3$  and  $\bar{G} \cong \text{Alt}_4$  or  $\bar{G} \cong \text{Sym}_4$ . Therefore,  $24\mathfrak{g}(\bar{\mathcal{X}})^2 < |G| \leq 3^h |\bar{G}| \leq 8 \cdot 3^{h+1}$  whence  $|S| = 3^{h+1} \geq 3\mathfrak{g}(\bar{\mathcal{X}})^2 > 3\mathfrak{g}(\bar{\mathcal{X}})$ . From Result 2.5,  $\bar{\mathcal{X}}$  has zero  $p$ -rank.

If  $\bar{\mathcal{X}}$  is elliptic then  $\lambda > 1$  by Claim 3.7. Hence  $\bar{S}$  is a subgroup of  $\bar{\mathcal{X}}$  with a non-trivial subgroup  $\bar{R}$  fixing a point of  $\bar{\mathcal{X}}$ . From Result 2.8,  $|\bar{R}| = 3$  (and  $p = 3$ ). The Deuring-Shafarevich formula applied to  $\bar{R}$  gives  $\gamma(\bar{\mathcal{X}}) - 1 = 3(\gamma(\bar{\mathcal{Y}}) - 1) + 2\tau$  where  $\bar{\mathcal{Y}}$  is the quotient curve of  $\bar{\mathcal{X}}$  by  $\bar{R}$  while  $\tau > 0$  is the number of fixed points of  $\bar{R}$  on  $\bar{\mathcal{X}}$ . This equation is only consistent with  $\gamma(\bar{\mathcal{X}}) = 0$  and  $\tau = 1$ . As a consequence,  $\bar{S}$  fixes a unique point  $\bar{P}$ . Also,  $\bar{S} = \bar{R}$  and hence  $|S| = 3|N|$ . Furthermore, the  $N$ -orbit  $\omega$  consisting of all points of  $\mathcal{X}$  lying over  $\bar{P}$  is an  $S$ -orbit. Therefore,  $|S_P|/|N_P| = |S|/|N| = 3$  for  $P \in \omega$ . Write  $G_P = S_P \rtimes H$  with a  $p'$ -subgroup fixing  $P$ . If  $k = 0$  then no non-trivial element of  $N$  fixes a point, and  $\gamma(\bar{\mathcal{X}}) = 0$  gives a contradiction. Therefore  $k > 0$  and (7) holds as in the proof of Claim 3.8. From (7),  $18(\gamma(\mathcal{X}) - 1) \geq 3 \cdot 3^k |\theta| = |S_P| |\theta|$  which together with (iii) of Result 2.7 give

$$|G| = |S_P| |\theta| |H| \leq 18(\gamma(\mathcal{X}) - 1)(4\mathfrak{g}(\mathcal{X}) + 2) \leq 18(4\mathfrak{g}(\mathcal{X}) + 2)(\mathfrak{g}(\mathcal{X}) - 1).$$

But this contradicts our hypothesis (5).

If  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 2$ , we may argue as in the proof of Lemma 3.2 to prove

$$|\bar{G}| > 84 \frac{p}{p-2} \mathfrak{g}(\bar{\mathcal{X}})^2.$$

Since  $\bar{T}$  is a normal  $p'$ -subgroup of  $\bar{G}$ , Proposition 3.3 applies to  $\bar{\mathcal{X}}$ . Therefore, either (D) occurs, or  $\bar{\mathcal{X}}$  has zero  $p$ -rank. In the latter case, from Lemma 3.4,  $\bar{G}$  fixes a point  $\bar{P} \in \bar{\mathcal{X}}$ . Hence, the  $N$ -orbit consisting of all points of  $\mathcal{X}$  lying over  $\bar{P}$  coincides with  $\theta$ . Then  $\theta$  is also an  $S$ -orbit and  $|\theta| = |N|/|N_P| = |S|/|S_P|$  holds. Write  $G_P = G_P^{(1)} \rtimes H$  with a  $p'$ -subgroup  $H$ . Since  $|H| \leq 4\mathfrak{g}(\mathcal{X}) + 2$  by (iii) of Result 2.7, this yields

$$|G| = |G_P| |\theta| \leq |S_P| |H| \frac{|S|}{|S_P|} \leq |S| (4\mathfrak{g}(\mathcal{X}) + 2).$$

From this and (5),

$$|S| > \frac{c\mathfrak{g}(\mathcal{X})^2}{4\mathfrak{g}(\mathcal{X}) + 2} > 3\mathfrak{g}(\mathcal{X}).$$

Therefore  $\mathcal{X}$  has zero  $p$ -rank by Result 2.5.  $\square$

Proposition 3.1 is a corollary of the above lemmas and propositions. In fact, let  $\mathcal{X}$  be a counterexample of minimal genus. From Proposition 3.3 and Lemma 3.4, case (B) occurs for  $\mathcal{X}$ . But this is ruled out by Proposition 3.5.

A further ingredient of the proof of Theorem 1.1 is the following lemma.

**Lemma 3.9.** *Let  $\mathcal{X}$  be an algebraic curve of genus  $\mathfrak{g} \geq 2$  and  $p$ -rank zero. Let  $G$  be a solvable subgroup of  $\text{Aut}(\mathcal{X})$ . If  $G$  has no non-trivial normal  $p'$ -subgroup then  $G$  fixes a point of  $\mathcal{X}$ .*

*Proof.* Let  $N$  be a minimal normal subgroup of  $G$ . Since  $G$  is solvable,  $N$  is an elementary abelian group. By our hypothesis,  $p \mid |N|$ . Therefore  $N$  is a normal  $p$ -subgroup of  $G$ . Since  $\mathcal{X}$  has zero  $p$ -rank,  $N$  fixes a unique point  $P \in \mathcal{X}$  by (i) of Result 2.4. Therefore  $G$  fixes  $P$ .  $\square$

Now we are in a position to give a proof for Theorem 1.1. From Proposition 3.1 together with Lemmas 3.4 and 3.9, the  $p$ -rank of  $\mathcal{X}$  is zero and  $G$  fixes a point of  $\mathcal{X}$ . Then  $G = S \rtimes C$  with a Sylow  $p$ -subgroup  $S$  and a cyclic group  $C$ . From (i) of Result 2.4, no non-trivial element in  $S$  fixes a point other than  $P$ . Therefore, if  $G$  has a short orbit distinct from  $\{P\}$  then it is tame. Actually, it is also unique by Result 2.2 by virtue of the hypothesis  $|G| > 24\mathfrak{g}^2$ . Then the cover  $\mathcal{X}|(\mathcal{X}/G)$  is a Katz-Gabber  $G$ -cover.

## 4 Automorphism groups and $p$ -rank

In this section, we provide some sufficient conditions for a curve to have  $p$ -rank equal to zero, which will be useful for the proof of Theorem 1.2. Throughout the section  $d$  stands for an odd prime and  $\mathcal{X}$  is an algebraic curve of genus  $\mathfrak{g} \geq 2$ . We first show that for special solvable groups, the bound of Theorem 1.1 can be improved.

**Lemma 4.1.** *Let  $H$  be an automorphism group of an algebraic curve of genus  $\mathfrak{g} \geq 2$  with a normal Sylow  $d$ -subgroup  $Q$  of odd order. Suppose that a complement  $U$  of  $Q$  in  $H$  is abelian, and that  $N_H(U) \cap Q = \{1\}$ . If*

$$|H| \geq 30(\mathfrak{g} - 1), \tag{8}$$

*then  $d = p$  and  $U$  is cyclic. Moreover, the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/Q$  is rational and either*

- (i)  $\mathcal{X}$  has positive  $p$ -rank,  $Q$  has exactly two (non-tame) short orbits, and they are also the only short orbits of  $H$ ; or
- (ii)  $\mathcal{X}$  has zero  $p$ -rank and  $H$  fixes a point.

*Proof.* We have  $H = Q \rtimes U$ . Set  $|Q| = d^k$ ,  $|U| = u$ . Then  $u \neq d$ . If  $u = 2$  then (8) reads  $|Q| > 15(\mathfrak{g} - 1)$ . If  $d = p$  then  $\mathcal{X}$  has zero  $p$ -rank by Result 2.5; then (ii) holds, since  $Q$  fixes a point by (i) of Result 2.4 and  $Q$  is normal in  $H$ . Otherwise,  $Q$  is a prime to  $p$  subgroup of  $H$ . The Hurwitz genus formula applied to  $Q$  gives  $|Q| < 6(\mathfrak{g} - 1)$  for  $d \neq 3$  and  $|Q| < 12(\mathfrak{g} - 1)$  for  $d = 3$ , contradicting (8). Therefore we may assume that  $u \geq 3$ .

Three cases are treated separately according to the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/Q$  has genus  $\bar{g}$  at least 2, or  $\bar{\mathcal{X}}$  is elliptic, or rational.

If  $g(\bar{\mathcal{X}}) \geq 2$ , then  $\text{Aut}(\bar{\mathcal{X}})$  has a subgroup isomorphic to  $U$ , and (i) of Result 2.7 yields  $4g(\bar{\mathcal{X}}) + 4 \geq |U|$ . Furthermore, from the Hurwitz genus formula applied to  $Q$ ,  $g - 1 \geq |Q|(g(\bar{\mathcal{X}}) - 1)$ . Therefore,

$$(4g(\bar{\mathcal{X}}) + 4)|Q| \geq |U||Q| = |H| \geq 30(g - 1) \geq 30|Q|(g(\bar{\mathcal{X}}) - 1),$$

whence

$$30 \leq 4 \frac{g(\bar{\mathcal{X}}) + 1}{g(\bar{\mathcal{X}}) - 1} \leq 12$$

contradicting (8).

If  $\bar{\mathcal{X}}$  is elliptic, then the cover  $\mathcal{X}|\bar{\mathcal{X}}$  ramifies, otherwise  $\mathcal{X}$  itself would be elliptic. Thus,  $Q$  has some short orbits. Take one of them together with its images  $o_1, \dots, o_u$  under the action of  $H$ . Since  $Q$  is a normal subgroup of  $H$ ,  $o = o_1 \cup \dots \cup o_m$  is a  $H$ -orbit of size  $u_1 d^v$  where  $d^v = |o_1| = \dots |o_m|$ . Equivalently, the stabilizer of a point  $P \in o$  has order  $d^{k-m} u / u_1$ , and it is the semidirect product  $Q_1 \rtimes U_1$  where  $|Q_1| = d^{k-v}$  and  $|U_1| = u / u_1$  for a subgroup  $Q_1$  of  $Q$  and  $U_1$  of  $U$  respectively. The point  $\bar{P}$  lying under  $P$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$  is fixed by the factor group  $\bar{U}_1 = U_1 Q / Q$ . Since  $\bar{\mathcal{X}}$  is elliptic, Result 2.8 implies  $|\bar{U}_1| \leq 12$  for  $p = 3$  and  $|\bar{U}_1| \leq 6$  for  $p > 3$ . As  $\bar{U}_1 \cong U_1$ , this yields the same bound for  $|U_1|$ , that is,  $u \leq 12u_1$  for  $p = 3$  and  $u \leq 6u_1$  for  $p > 3$ . Furthermore, if  $p = 3$  then  $d > 3$ , and  $d_P \geq d^{k-m} - 1 \geq \frac{4}{5}d^{k-m}$ . If  $p > 3$  then  $d_P \geq d^{k-m} - 1 \geq \frac{2}{3}d^{k-m}$ . From the Hurwitz genus formula applied to  $Q$ , if  $p = 3$  then

$$2g - 2 \geq d^m u_1 d_P \geq d^m u_1 \left(\frac{4}{5}d^{k-m}\right) \geq \frac{4}{5}d^m u_1 \geq \frac{1}{15}d^m u = \frac{1}{15}|Q||U| = \frac{1}{15}|H|,$$

while for  $p > 3$ ,

$$2g - 2 \geq d^m u_1 d_P \geq d^m u_1 \left(\frac{2}{3}d^{k-m}\right) \geq \frac{2}{3}d^m u_1 \geq \frac{1}{9}d^m u = \frac{1}{9}|Q||U| = \frac{1}{9}|H|,$$

But this contradicts (8).

If  $\bar{\mathcal{X}}$  is rational, then  $Q$  has at least one short orbit. Furthermore,  $\bar{U} = UQ/Q$  is isomorphic to a subgroup of  $PGL(2, \mathbb{K}) \cong \text{Aut}(\bar{\mathcal{X}})$ . Since  $U \cong \bar{U}$ , Result 2.9 shows that either

- (I)  $U$  is an elementary abelian  $p$ -group and  $\bar{U}$  fixes a point  $\bar{P}_\infty$  but no non-trivial element of  $\bar{U}$  fixes a point other than  $\bar{P}_\infty$ , or
- (II)  $U$  is a cyclic group of order prime to  $p$ ,  $\bar{U}$  fixes two points  $\bar{P}_0$  and  $\bar{P}_\infty$  but no non-trivial element in  $\bar{U}$  fixes a point other than  $\bar{P}_0$  and  $\bar{P}_\infty$ .

Let  $o_\infty$  and  $o_0$  be the  $Q$ -orbits lying over  $\bar{P}_0$  and  $\bar{P}_\infty$ , respectively. Obviously,  $o_\infty$  (and in case (II) also  $o_0$ ) is a short orbit of  $H$ . We show that  $Q$  has at most one or two short orbits according to cases (I) and (II), the candidates being  $o_\infty$  and in case (II) also  $o_0$ . By absurd, there is a  $Q$ -orbit  $o$  of size  $d^m$  with  $m < k$  which lies over a point  $\bar{P} \in \bar{\mathcal{X}}$  different from  $\bar{P}_\infty$  (in case (II) from both  $\bar{P}_0$  and  $\bar{P}_\infty$ ). Since the orbit of  $\bar{P}$  in  $\bar{U}$  has length  $u$ , then the  $H$ -orbit of a point  $P \in o$  has length  $ud^m$ . If  $u > 3$ , the Hurwitz genus applied to  $Q$  gives

$$2g - 2 \geq -2d^k + ud^m(d^{k-m} - 1) \geq -2d^k + ud^m \frac{2}{3}d^{k-m} \geq -2d^k + \frac{2}{3}ud^k \geq \frac{2}{3}(u - 3)d^k > \frac{1}{6}ud^k \geq \frac{1}{6}|H|,$$

a contradiction with  $|H| > cg$  for  $c = 36$ . If  $u = 3$  then  $d \geq 3$ , and hence

$$2g - 2 \geq -2d^k + 3d^m(d^{k-m} - 1) = d^k - 3d^m > \frac{1}{3}d^k,$$

whence  $|H| = 3d^k < 9\mathfrak{g}$ , a contradiction with (8).

In case (I),  $u$  is a power of  $p$  with  $p \neq d$  while  $|o_\infty| = d^k$ . Hence  $U$  must fix a point  $P_\infty \in o_\infty$ . As  $o_\infty$  is a short  $Q$ -orbit,  $H_P$  contains a non-trivial element  $v$  from  $Q$ . From (i) of Result 2.1,  $U$  is a normal subgroup of  $H_P$ . Therefore,  $w \in N_H(U) \cap Q$ , a contradiction.

We are left with case (II). Since  $H$  has exactly two short orbits, (8) together with Result 2.2 yield that  $p$ -divides  $|H|$ . Therefore,  $d = p$ . Assume that  $Q$  has two short orbits. They are  $o_\infty$  and  $o_0$ . If their lengths are  $p^a$  and  $p^b$  with  $a, b < k$ , the Deuring-Shafarevich formula applied to  $Q$  gives

$$\gamma(\mathcal{X}) - 1 = -p^k + (p^k - p^a) + p^k - p^b$$

whence  $\gamma(\mathcal{X}) = p^k - (p^a + p^b) + 1 > 0$ . The same argument shows that if  $Q$  has just one short orbit, then  $\gamma(\mathcal{X}) = 0$  and the short orbit consists of a single point  $P$ . Since  $Q$  is a normal subgroup of  $H$ ,  $P$  is also fixed by  $H$ .  $\square$

**Remark 4.2.** As a byproduct of the the above proof, if the hypotheses of Lemma 4.1 are satisfied then Case (II) occurs, that is,  $\mathfrak{g}(\tilde{\mathcal{X}}) = 0$ ,  $U$  is a cyclic group of order prime to  $p$ ,  $\bar{U} = UQ/Q$  fixes two points  $\bar{P}_0$  and  $\bar{P}_\infty$  in  $\tilde{\mathcal{X}}$  but no non-trivial element in  $\bar{U}$  fixes a point other than  $\bar{P}_0$  and  $\bar{P}_\infty$ . In fact, the other possibilities have explicitly been ruled out in that proof for  $u \geq 3$ . The claim is true also for  $u = 2$  since  $|Q| > 15(\mathfrak{g} - 1)$  yields  $\mathfrak{g}(\tilde{\mathcal{X}}) = 0$  by the last statement of Result 2.2.

**Remark 4.3.** In Lemma 4.1, if  $d = p$  is assumed then the extra-hypothesis  $N_H(U) \cap Q = \{1\}$  is unnecessary, since in the proof of Lemma 4.1 the hypothesis  $N_H(U) \cap Q = \{1\}$  is only used to rule out Case (I), in which  $d \neq p$  holds. In fact, if  $Q$  is a  $p$ -subgroup then  $U$  is a  $p'$ -subgroup, and (I) cannot occur. Furthermore, Lemma 4.1 applies whenever  $H$  is taken for a group stabilizing a point of  $\mathcal{X}$  and satisfying (8).

**Remark 4.4.** Both Cases (i) and (ii) in Lemma 4.1 occur as the following examples show. For Case (i), let  $\mathcal{X}$  be a non-singular model  $\mathcal{X}$  of the Artin-Mumford curve where  $\mathcal{C}$  is the plane irreducible (singular) curve  $\mathcal{C}$  of affine equation  $(X^p - X)(Y^p - Y) - 1 = 0$ . The main properties of  $\mathcal{X}$  are well known; see [9, 5, 32]:  $\mathcal{X}$  is an ordinary curve  $\mathcal{X}$  of genus  $\mathfrak{g}$  (and  $p$ -rank) equal to  $(p - 1)^2$ . Furthermore,  $\mathcal{C}$  has two (ordinary) singular points  $X_\infty$  and  $Y_\infty$  both  $p$ -fold points. Each of them is the center of  $p$  places of  $\mathbb{K}(\mathcal{X})$ . Let  $o_\infty$  be the set of the  $p$  points of  $\mathcal{X}$  associated to the  $p$  places centered at  $X_\infty$ , and  $o_0$  that arising from  $Y_\infty$  in the same way. For every  $a, b \in \mathbb{F}_p$ , the linear map  $(X, Y) \rightarrow (X + a, Y + b)$  is an automorphism of  $\mathcal{C}$  and hence of  $\mathcal{X}$ . The linear maps form an (elementary abelian) group  $Q = C_p \times C_p$  of order  $p^2$ , and  $Q$  has two (short) orbits of length  $p$ , namely  $o_\infty$  and  $o_0$ . Also, for every  $c \in \mathbb{F}_p^*$  the linear map  $(X, Y) \rightarrow (cX, c^{-1}Y)$  is an automorphism of  $\mathcal{C}$  and hence of  $\mathcal{X}$ . They form a cyclic group  $C_{p-1}$  of order  $p - 1$  that preserves both  $o_\infty$  and  $o_0$ . A further (linear) automorphism is  $\varphi : (X, Y) \rightarrow (Y, X)$  which interchanges  $o_\infty$  and  $o_0$ . The group generated by  $C_{p-1}$  together with  $\varphi$  is a dihedral group  $D_{p-1}$ . Therefore,  $\text{Aut}(\mathcal{X})$  has a subgroup  $G = (C_p \times C_p) \rtimes D_{p-1}$  with a dihedral group of order  $2(p - 1)$ . If  $\mathbb{K} = \overline{\mathbb{F}_p}$  or  $(\mathbb{K}, |\cdot|)$  is non-Archimedean valued field of characteristic  $p$ , then  $\text{Aut}(\mathcal{X}) = G$ ; see [5] and [9]. For  $p \geq 31$ ,  $|H| = p^2(p - 1) \geq 30(\mathfrak{g} - 1)$  and  $H = (C_p \times C_p) \rtimes C_{p-1}$  satisfies the hypotheses of Lemma 4.1, and we have Case (i). For Case (ii), let  $\mathcal{X}$  be a non-singular model  $\mathcal{X}$  of the the plane irreducible (singular) curve  $\mathcal{C}$  of affine equation  $Y^p + Y - X^m = 0$  with  $m < p$ . For the main properties of  $\mathcal{X}$  see [47], and [29, Theorems 12.9 and 12.11]. If  $m$  does not divide  $p + 1$  then  $\mathcal{X}$  has genus  $\frac{1}{2}(p - 1)m$  and  $p$ -rank zero while  $H = \text{Aut}(\mathcal{X})$  fixes the infinite point and  $H = S \rtimes C$  with  $|S| = p$  and  $|C| = m(p - 1)$ . If  $p \geq 17$  then  $|H| > 30(\mathfrak{g} - 1)$ , and we have Case (ii).

**Remark 4.5.** In Lemma 4.1, if we assume  $d \neq p$  and  $[H : Q] \geq 3$  but drop the extra-hypothesis  $N_H(U) \cap Q = \{1\}$  then Case (I) in the proof of Lemma 4.1 occurs. Then  $H$  has a unique short orbit  $o_\infty$  and the quotient curve  $\tilde{\mathcal{X}} = X/H$  is rational. From the Abhyankar conjecture as stated in Section 2,  $H$  is generated by  $U$

together with its conjugates in  $H$ . In particular,  $H$  is not a direct product of  $Q$  and  $U$ . We do not use this fact in the forthcoming proofs.

**Lemma 4.6.** *Let  $T$  be a subgroup of  $\text{Aut}(\mathcal{X})$  containing a normal subgroup  $H$  that satisfies the hypotheses of Lemma 4.1. Then  $T = Q \rtimes V$  where  $Q$  is a  $p$ -group,  $V$  is a cyclic or a dihedral group, and  $p$  is prime to  $|V|$ . If in addition  $\mathcal{X}$  has positive  $p$ -rank and  $T$  fuses two short  $H$ -orbits together into one orbit then  $V$  is dihedral.*

*Proof.* By Remark 4.2 we may suppose that (II) in the proof of Lemma 4.1 holds. Since  $H$  is a normal subgroup of  $T$ , and  $o_\infty$  and  $o_0$  are the only short orbits of  $H$ , two possibilities arise, namely either  $T$  preserves both  $o_\infty$  and  $o_0$ , or  $o_\infty \cup o_0$  is a  $T$ -orbit. On the other hand,  $Q$  is the unique Sylow  $p$ -subgroup of  $H$ . Thus  $Q$  is a characteristic subgroup of  $H$ , and hence  $Q$  is a normal subgroup of  $T$ . Therefore,  $\bar{T} = G/Q$  is a subgroup of  $PGL(2, \mathbb{K})$ . It turns out that either  $\bar{T}$  fixes both points  $\bar{P}_0$  and  $\bar{P}_\infty$ , or  $\bar{T}$  interchanges them. From Result 2.9,  $\bar{T}$  is cyclic in the former case, and it is a dihedral group in the latter case. In both cases  $p$  is prime to  $|\bar{T}|$ . Therefore  $Q$  is prime to  $[T : Q]$ , and hence  $T = Q \rtimes V$  where  $V$  is either cyclic or dihedral, and  $p$  is prime to  $|V|$ .  $\square$

**Remark 4.7.** In the dihedral case, some (involutory) elements of  $\bar{T}$  fixes a point  $\bar{P}$  distinct from  $P_\infty$  and  $P_0$ . This agrees with the Abhyankar conjecture as stated in Section 2 which shows that the possibility for  $T$  to be dihedral in Lemma 4.6 can only occur when  $T$  has a short orbit other than the fused one. This is the case when  $\mathcal{X}$  is a non-singular model of the Artin-Mumford curve  $\mathcal{C}$ ; see Remark 4.4. In fact, the automorphism  $\varphi : (X, Y) \rightarrow (Y, X)$  of  $\mathcal{C}$  fixes each point  $P(a, a) \in \mathcal{C}$  with  $a^p - a \pm 1 = 0$  and these points are outside  $o_\infty$  and  $o_0$ . We do not use this fact in the forthcoming proofs.

**Lemma 4.8.** *Let  $G$  be a subgroup of  $\text{Aut}(\mathcal{X})$  of order at least  $16g^2$  which satisfies property (iii) of Result 2.4. If  $G$  has a Sylow  $d$ -subgroup  $Q$  of odd order such that the normalizer  $N_G(Q)$  satisfies the hypotheses on  $H$  in Lemma 4.1, that is  $Q$  has an abelian complement  $U$  in  $N_G(Q)$  with  $N_{N_G(Q)}(U) \cap Q = \{1\}$  and  $|N_G(Q)| \geq 30(g-1)$ , then  $\mathcal{X}$  has zero  $p$ -rank.*

*Proof.* By Lemma 4.1,  $d = p$ . From Remark 4.2 Case (II) in the proof of Lemma 4.1 occurs. Assume by contradiction that  $\mathcal{X}$  has positive  $p$ -rank. Then from the proof of Lemma 4.1, there exist exactly two short  $Q$ -orbits  $o_\infty$  and  $o_0$ . Each is left invariant by  $N_G(Q)$ , as well. If they are in two different orbits of  $G$  then Case (b) in Result 2.2 with  $|G| < 16g^2$  holds, a contradiction. Therefore, if  $P_\infty \in o_\infty$  and  $P_0 \in o_0$  then there exists  $w \in G$  taking  $P_\infty$  to  $P_0$ . Take two non-trivial elements  $r_\infty, r_0 \in Q$  fixing  $P_\infty$  and  $P_0$ , respectively. The conjugate  $r$  of  $r_\infty$  by  $w$  fixes  $P_0$ . Hence both  $r$  and  $r_0$  are in the stabilizer of  $P_0$  in  $G$ . From (i) of Result 2.1, a  $p$ -subgroup  $R$  of  $G$  contains both  $r$  and  $r_0$ . Since the conjugate  $Q'$  of  $Q$  by  $w$  is a Sylow  $p$ -subgroup of  $G$ ,  $R$  has non-trivial elements from both two Sylow  $p$ -subgroups  $Q$  and  $Q'$ . Since  $G$  is a group in which any two distinct Sylow  $p$ -subgroups have trivial intersection, it turns out that  $Q = Q'$ , that is,  $w \in N_G(Q)$ . This is a contradiction as  $o_\infty$  is an  $N_G(Q)$ -orbit.  $\square$

**Lemma 4.9.** *Let  $G$  be a subgroup of  $\text{Aut}(\mathcal{X})$  with a non-trivial  $p$ -subgroup  $Q$  that satisfies the following properties.*

- (i)  $Z(G)$  has a non-trivial element  $g$  of order  $t$  with  $t < p$ ,
- (ii) The normalizer of  $Q$  in  $G$  contains a subgroup  $N$  such that  $N = Q \rtimes M$  with an abelian group  $M$  of order prime to  $p$  properly containing  $\langle g \rangle$ .

*If  $\bar{\mathcal{X}} = \mathcal{X}/\langle g \rangle$  has zero  $p$ -rank and  $\tilde{\mathcal{X}} = \mathcal{X}/Q$  is rational then  $\mathcal{X}$  has also zero  $p$ -rank.*

*Proof.* Let  $U = \langle g \rangle$ . The quotient group  $\bar{Q} = QU/U$  is a  $p$ -subgroup of  $\text{Aut}(\bar{\mathcal{X}})$ . Since  $\gamma(\bar{\mathcal{X}}) = 0$ , there exists a point  $\bar{P} \in \bar{\mathcal{X}}$  fixed by  $\bar{Q}$  but no non-trivial element in  $\bar{Q}$  fixes a point of  $\bar{\mathcal{X}}$  other than  $\bar{P}$ . Let  $o$  be the  $U$ -orbit in  $\mathcal{X}$  lying over  $\bar{P}$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ . Since  $|o| \leq t$  and  $t < p$ ,  $Q$  fixes  $o$  pointwise. No point  $R \in \mathcal{X}$  other than those in  $o$  is fixed by  $Q$ , otherwise the point  $\bar{R}$  lying under  $R$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$  would be a fixed point of  $\bar{Q}$  distinct from  $\bar{P}$ . Therefore,  $N$  preserves  $o$ . From (ii),  $|o| \leq t < |M|$ . Hence, some non-trivial element  $m \in M$  fixes a point in  $o$ . Since  $M$  is abelian and contains  $U$ ,  $m$  fixes  $o$  pointwise.

Furthermore, the cover  $\mathcal{X}|\bar{\mathcal{X}}$  totally ramifies at the points of  $\bar{\mathcal{X}}$  lying under those in  $o$  while it is unramified elsewhere. Now look at the action of the quotient group  $\bar{N} = N/Q$  as a subgroup of  $\text{Aut}(\bar{\mathcal{X}})$ . In the natural group homomorphism  $N \rightarrow \bar{N}$ , the image  $\bar{m}$  of  $m$  is a non-trivial automorphism of  $\bar{\mathcal{X}}$  which fixes each of the  $|o|$  points of  $\bar{\mathcal{X}}$  lying under the points of  $o$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ . Since  $\bar{\mathcal{X}}$  is rational,  $\bar{N}$  is isomorphic to a subgroup of  $PGL(2, \mathbb{K})$ . Moreover,  $\bar{N}$  is abelian by  $M \cong \bar{N}$ . From Result 2.9,  $\bar{N}$  is a cyclic group of order prime to  $p$  and hence it fixes exactly two points in  $\bar{\mathcal{X}}$ , and no non-trivial element of  $\bar{N}$  fixes a further point in  $\bar{\mathcal{X}}$ ; see [49, Theorem 1]. In particular, the image  $\bar{g}$  of  $g$  has exactly two fixed points in  $\bar{\mathcal{X}}$ , and they are also the fixed points of  $\bar{m}$ . From this,  $|o| \leq 2$ . If equality holds then both points in  $o$  must be fixed by  $N$ . But this is impossible since  $o$  is an  $U$ -orbit and  $U \leq N$ . Therefore,  $|o| = 1$ , and hence  $Q$  has exactly one fixed point in  $\mathcal{X}$ . Since  $\gamma(\bar{\mathcal{X}}) = 0$ , the Deuring-Shafarevich formula yields that  $\gamma(\mathcal{X}) = 0$  also holds.  $\square$

## 5 Some low dimensional linear groups as automorphism groups of curves

For a prime power  $q = d^k$  with an odd prime  $d$ , let  $W$  denote one of the following non-solvable linear groups

$$PSL(2, q), PGL(2, q), \text{ with } q \geq 5, PSU(3, q), PGU(3, q), PSL(3, q), PGL(3, q). \quad (9)$$

Choose a Sylow  $d$ -subgroup  $Q$  of  $W$ . If  $W \neq PSL(3, q), PGL(3, q)$  then the normalizer  $H$  of  $Q$  is a semidirect product  $Q \rtimes C_m$  with a cyclic complement  $C_m$  of order  $m$ . Here  $(|Q|, m)$  is  $(q, \frac{1}{2}(q-1))$ , or  $(q, q-1)$ , or  $(q^3, (q^2-1)/\mu)$ , or  $(q^3, q^2-1)$  according to  $W$  is  $PSL(2, q)$ , or  $PGL(2, q)$ , or  $PSU(3, q)$  or  $PGU(3, q)$  where  $\mu = \gcd(3, q+1)$ . In these cases,  $W$  satisfies property (iii) of Result 2.4. Some but not all of these facts remain true for  $PSL(3, q)$  and  $PGL(3, q)$ . For  $PSL(3, q)$  with  $q = d^k$  and  $d > 2$  prime, the normalizer  $H$  of a Sylow  $d$ -subgroup  $Q$  is a semidirect product of  $Q$  by  $C_{q-1} \times C_{(q-1)/\mu}$  where  $\mu$  is the greatest common divisor of 3 and  $q-1$ . The same holds for  $PGL(3, q)$  with  $\mu = 1$  for any  $q$ .  $PSL(3, q)$  (and hence  $PGL(3, q)$ ) does not satisfy property (iii) of Result 2.4.

Throughout the section  $d$  stands for an odd prime and  $\mathcal{X}$  is an algebraic curve of genus  $\mathfrak{g} \geq 2$ .

**Lemma 5.1.** *Let  $W$  be one of the groups on the list (9),  $W \neq PSL(3, q), PGL(3, q)$ . If  $W$  is isomorphic to a subgroup of  $\text{Aut}(\mathcal{X})$  with*

$$|W| > 900\mathfrak{g}^2, \quad (10)$$

*then  $\mathcal{X}$  has zero  $p$ -rank and  $q$  is a power of  $p$ .*

*Proof.* Let  $H$  be the normalizer of a Sylow  $d$ -subgroup  $Q$  of  $W$ . For  $W \cong PSL(2, q)$ , we have  $|W| = (q+1)|H|$  with  $|H| = \frac{1}{2}q(q-1)$  whence  $|H|^2 > |W| > 900\mathfrak{g}(\mathcal{X})^2$  which yields  $|H| > 30(\mathfrak{g}(\mathcal{X}) - 1)$ . As  $900 > 16$ , the assertions follow from Lemmas 4.8 and 4.1. Similar arguments apply to the other cases. In particular,

- for  $W \cong PGL(2, q)$ , we have  $|W| = (q+1)|H|$  with  $|H| = q(q-1)$  whence  $|H|^2 > |W| > 900\mathfrak{g}(\mathcal{X})^2$ ;
- for  $W \cong PSU(3, q)$ , we have  $|W| = (q^3+1)|H|$  with  $|H| = \frac{1}{\mu}q^3(q^2-1)$ , where  $\mu = \gcd(3, q+1)$ , whence  $|H|^2 > |W| > 900\mathfrak{g}(\mathcal{X})^2$ ;

- for  $W \cong PGU(3, q)$ , we have  $|W| = (q^3 + 1)|H|$  with  $|H| = q^3(q^2 - 1)$  whence  $|H|^2 > |W| > 900\mathfrak{g}(\mathcal{X})^2$ .

□

Recall that  $\text{Aut}(W) = P\Gamma L(2, q)$  when  $W = PSL(2, q)$ , or  $W = PGL(2, q)$  while  $\text{Aut}(W) = P\Gamma L(3, q)$  when  $W = PSU(3, q)$  or  $W = PGU(3, q)$ ; see for instance [51, Sections 3.3.4, 3.6.3]. So,  $W \leq \text{Aut}(W)$  may be assumed.

**Remark 5.2.** We point out that in the natural representation of  $P\Gamma L(2, q)$ , the 2-point stabilizer is neither abelian nor dihedral. More precisely, a semilinear subgroup of  $P\Gamma L(2, q)$  containing  $PSL(2, q)$  is non-abelian and, apart from the smallest value of  $q$ , namely  $q = 9$  (and  $|G| = 720$ ), it is also non-dihedral. The same result is valid for the 2-point stabilizer of  $P\Gamma U(3, q)$  including all cases.

In its natural representation,  $P\Gamma L(2, q)$  is the semilinear group on the projective line  $PG(1, q)$  over  $\mathbb{F}_q$ . Its subgroup  $PSL(2, q)$  acts on  $PG(1, q)$  as a doubly transitive permutation group such that its stabilizer  $M$  of the origin  $O$  and the infinite point  $\infty$  has order  $\frac{1}{2}(q - 1)$  and consists of all permutations  $x \mapsto ax$  with a non-zero quadratic element  $a$  in  $\mathbb{F}_q$ . The stabilizer of  $\infty$  is  $H = Q \rtimes M$  where  $Q$  is the Sylow  $d$ -subgroup of  $PSL(2, q)$  consisting of all translations  $x \mapsto x + c$  with  $c \in \mathbb{F}_q$ . If a subgroup  $G$  of  $P\Gamma L(2, q)$  contains  $PSL(2, q)$  then the stabilizer of  $\infty$  in  $G$  is  $G_{\infty, O} \rtimes Q$  where  $G_{\infty, O}$  is the stabilizer of  $\infty$  and  $O$  in  $G$ , and  $M$  is a normal subgroup of  $G_{\infty, O}$ . Suppose that  $G$  contains  $PSL(2, q)$  properly. Then  $G_{\infty, O}$  has an element  $v$  other than those in  $M$ . If  $v \in PGL(2, q)$  then  $G$  also contains  $PGL(2, q) = \langle PSL(2, q), v \rangle$ . Since  $PGL(2, q)$  is the only linear subgroup of  $P\Gamma L(2, q)$  containing  $PSL(2, q)$  properly, it turns out that if  $G$  is not linear then  $G_{\infty, O}$  contains a permutation  $\varphi : x \mapsto \alpha x^\sigma$  where  $\alpha \in \mathbb{F}_q$  and  $\sigma$  is a non-trivial automorphism of  $\mathbb{F}_q$ . Then  $\varphi\psi_a \neq \psi_a\varphi$  for  $\psi_a : x \mapsto ax$  with  $a \in \mathbb{F}_q$  such that  $\sigma(a) \neq a$ . Hence  $G_{\infty, O}$  is not abelian. We show that  $G_{\infty, O}$  is neither dihedral for  $|G| > 720$ . Since  $M$  is a cyclic subgroup of order  $\frac{1}{2}(q - 1)/2 \geq 4$ , the index 2 cyclic subgroup of any dihedral group containing  $M$  also contains  $M$ . As we have already showed the centralizer of  $M$  does not contain  $\varphi$ . Therefore, if  $G_{\infty, O}$  is assumed to be dihedral then  $\varphi$  is an element in the coset of the index 2 cyclic subgroup of  $G_{\infty, O}$ . Thus  $\varphi^2 = 1$ , that is,  $\sigma$  is involutory and  $\alpha^{\sigma+1} = 1$ . Furthermore,  $\varphi\psi_a\varphi = (\psi_a)^{-1} = \psi_{a^{-1}}$  holds for every  $a \in D$ . Therefore,  $a^{\sigma+1} = 1$  for every non-zero quadratic element  $a \in \mathbb{F}_q$ . Since the number of such elements is  $\frac{1}{2}(q - 1)$ , this occurs if and only if  $d = 3, q = 9$ . Hence, either  $G = P\Gamma L(2, 9)$ , and  $|G| = 1440$ , or  $G$  has order 720. The former case  $G = P\Gamma L(2, 9)$ , as  $P\Gamma L(2, 9)_{\infty, O}$  is a semi-dihedral group of order 16. In the latter case,  $G$  is one of the two subgroups of  $P\Gamma L(2, 9)$  of order 720, other than  $PGL(2, 9)$ . Therefore, if  $G_{\infty, O}$  is dihedral then  $|G| = 720$ .

In its natural representation,  $P\Gamma U(3, q)$  is the semilinear group preserving the set of all  $\mathbb{F}_{q^2}$ -rational points of the Hermitian curve  $\mathcal{H}$  with equation  $y^q + y = x^{q+1}$ . Its subgroup  $PSU(3, q)$  acts as a doubly transitive permutation group. Let  $D$  be the subgroup of index  $\mu$  in the multiplicative group of  $\mathbb{F}_{q^2}$ . Then a Sylow  $d$ -subgroup  $Q$  of  $PSU(3, q)$  consists of all maps  $(x, y) \mapsto (x + a, y + a^q x + b)$  with  $a, b \in \mathbb{F}_{q^2}$  and  $b^q + b = a^{q+1}$ . The subgroup  $PSU(3, q)$  acts on  $\mathcal{H}$  as a doubly transitive permutation group such that its stabilizer  $M$  of the origin  $O = (0, 0)$  and the infinite point  $\infty$  of the  $y$ -axis has order  $(q^2 - 1)/\mu$  and it consists of all maps  $\psi_{a, b} : (x, y) \mapsto (ax, by)$  with  $a \in D$  and  $b = a^{q+1}$ . Suppose that a subgroup  $G$  of  $P\Gamma U(3, q)$  contains  $PSU(3, q)$  properly. Then the stabilizer  $G_{\infty, O}$  of  $G$  contains an element  $v$  other than those in  $M$ . If  $v \in PGU(3, q)$  (and  $\mu = 3$ ) then  $G$  also contains  $PGU(3, q) = \langle PSU(3, q), v \rangle$ . Since  $PGU(3, q)$  is the only linear subgroup of  $P\Gamma U(3, q)$  containing  $PSU(3, q)$  properly, it turns out that if  $G$  is not linear then  $G_{\infty, O}$  contains a map  $\varphi : (x, y) \mapsto (\alpha x^\sigma, \beta y^\sigma)$  where  $\alpha \in D$ ,  $\beta = \alpha^{q+1}$  and  $\sigma$  is a non-trivial automorphism of  $\mathbb{F}_q$ . Then  $\varphi\psi_{a, b} \neq \psi_{a, b}\varphi$  for  $a \in \mathbb{F}_q$  such that  $\sigma(a) \neq a$ . Hence  $G_{\infty, O}$  is not abelian. We show that  $G_{\infty, O}$  is neither dihedral. Since  $M$  is a cyclic subgroup of order  $(q^2 - 1)/\mu \geq 3$ , the index 2 cyclic subgroup of any dihedral group containing  $M$  also contains  $M$ . The centralizer of  $M$  does not contain  $\varphi$ . Therefore, if  $G_{\infty, O}$  is dihedral by absurd, then  $\varphi$  is in the coset of the index 2 cyclic subgroup of  $G_{\infty, O}$ . Hence  $\sigma$  is involutory,

$\alpha^{\sigma+1} = 1$ , and  $\varphi\psi_{a,b}\varphi = (\psi_{a,b})^{-1} = \psi_{a^{-1},b^{-1}}$  holds for every  $\psi_{a,b} \in M$ . From this,  $a^{\sigma+1} = 1$  follows for every  $a \in D$ . Since  $|D| = (q^2 - 1)/\mu$  this yields  $d^h + 1 = (d^{2k} - 1)/\mu$  with  $\sigma = d^h$ . As  $\mu = 1$  or  $\mu = 3$ , this is impossible. Therefore  $G_{\infty, O}$  is not dihedral.

**Lemma 5.3.** *Let  $G$  be a subgroup of  $\text{Aut}(W)$  containing  $W$  where  $W$  is one of the groups on the list (9), for some prime power  $q = d^k$  with an odd prime  $d$ . If  $G$  is also a subgroup of  $\text{Aut}(\mathcal{X})$  up to isomorphism, and*

$$|G| > c \cdot 900\mathfrak{g}^2 \quad (11)$$

with

$$c = \begin{cases} \frac{2k(q+1)}{(q-1)q} & \text{if } W = PSL(2, q), \\ \frac{k(q+1)}{(q-1)q} & \text{if } W = PGL(2, q), \\ \frac{2k\mu(q^3+1)}{(q^2-1)q^3} & \text{if } W = PSU(3, q), \\ \frac{2k(q^3+1)}{(q^2-1)q^3} & \text{if } W = PGU(3, q), \\ \frac{k\mu(q^2+q+1)(q+1)}{(q^2-1)q^3} & \text{if } W = PSL(3, q), \\ \frac{k(q^2+q+1)(q+1)}{(q^2-1)q^3} & \text{if } W = PGL(3, q), \end{cases}$$

then  $G$  is linear, and  $W \neq PSL(3, q), PGL(3, q)$ .

*Proof.* We begin with the case  $W = PSL(2, q)$ . Let  $Q$  be a Sylow  $d$ -subgroup of  $PSL(2, q)$  and  $H$  its normalizer in  $PSL(2, q)$ . We may assume that  $Q$  and  $H$  are taken as in Remark 5.2. Then  $T = G_{\infty}$  is a subgroup of  $G$  containing  $H$  as a normal subgroup such that  $T = Q \rtimes G_{\infty, O}$ . Assume that  $G$  is nonlinear. From Remark 5.2,  $G_{\infty, O}$  is not cyclic and it is dihedral only for  $d = 3$  and  $|G| = 720$ . On the other hand,  $k \geq 2$  and  $|G| = \frac{1}{2}h(q-1)q(q+1)$  where  $h > 1$  is a divisor of  $k$ . The assumption  $|G| > 900c\mathfrak{g}^2$  yields

$$|H| = \frac{1}{2}(q-1)q > 30\sqrt{\frac{c(q-1)q}{2h(q+1)}}\mathfrak{g} > 30\mathfrak{g}. \quad (12)$$

By (11),  $H$  satisfies the hypotheses of Lemma 4.1. By Lemma 4.6,  $G_{\infty, O}$  is either cyclic or dihedral. Since  $|G| > 720$  this is impossible.

Now, let  $W = PSU(3, q)$ . By the above argument applied to a subgroup  $G$  of  $P\Gamma L(3, q)$  containing  $PSU(3, q)$  properly, Remark 5.2 shows that  $T = G_{\infty}$  is a subgroup of  $G$  containing  $H$  as a normal subgroup such that  $T = Q \rtimes G_{\infty, O}$  where  $G_{\infty, O}$  is neither cyclic nor dihedral when  $G$  is nonlinear. On the other hand,  $|G| = \frac{1}{\mu}h(q^2-1)q^3(q^3+1)$  where  $h$  is a divisor of  $2k$ . Assumption  $|G| > 900c\mathfrak{g}^2$  yields

$$|H| = \frac{1}{\mu}(q^2-1)q^3 > 30\sqrt{\frac{c(q^2-1)q^3}{\mu h(q^3+1)}}\mathfrak{g} > 30\mathfrak{g}. \quad (13)$$

By (11),  $H$  satisfies the hypotheses of Lemma 4.1. From Lemma 4.6,  $T = Q \rtimes G_{\infty, O}$  where  $V$  is either cyclic or dihedral, a contradiction.

Finally, let  $W = PSL(3, q)$ . Then  $|W| = \frac{1}{\mu}h(q-1)^2q^3(q^2+q+1)(q+1)$  where  $h$  is a divisor of  $k$ . Then

$$|H| = \frac{1}{\mu}(q-1)^2q^3 > 30\sqrt{\frac{c(q-1)^2q^3}{\mu h(q^2+q+1)(q+1)}}\mathfrak{g} > 30\mathfrak{g}. \quad (14)$$

By (10), the hypotheses on  $H$  in Lemma 4.1 are satisfied. From Lemma 4.6,  $T = Q \rtimes V$  where  $V$  is either cyclic or dihedral. However,  $H$  contains the direct product of two cyclic groups, and hence  $V$  is neither cyclic, nor a dihedral group. This contradiction shows that  $W \neq PSL(3, q)$ . A similar argument shows that  $W = PGL(3, q)$  cannot occur.  $\square$

**Remark 5.4.** In Lemma 5.3  $c \leq 1$  holds in each case.

**Remark 5.5.** In some but not all cases, Lemma 5.3 follows from the Abhyankar conjecture under a bit weaker condition, namely  $|G| > 24\mathfrak{g}^2$ . This condition yields one of the Cases (c) and (d) in Result 2.2. Furthermore, the quotient curve  $\mathcal{X}/G$  is rational, and the Abhyankar conjecture stated in Introduction applies to  $G$ . If  $G$  has one short orbit, that is in Case (c), then  $G$  is generated by its Sylow  $p$ -subgroups and hence  $G \geq W$  implies  $G = W$ ; thus  $G$  is linear, and Lemma 5.3 follows. If  $G$  has two short orbits, that is in Case (d), then  $G/W$  is a cyclic group. For instance, this occurs when  $G \cong PGL(2, q)$  or  $G \cong PGU(3, q)$ . The Abhyankar conjecture rules out the possibility that in Case (d)  $G$  properly contains  $PGL(2, q)$  or  $PGU(3, q)$ , as  $G/W$  is not cyclic in these cases.

The following lemma shows that the hypothesis  $W \neq PSL(3, q), PGL(3, q)$  in Lemma 5.1 is meaningful.

**Lemma 5.6.** *If  $W = PSL(3, q)$  with  $q > 3$  is a subgroup of  $\text{Aut}(\mathcal{X})$  then  $|G| < 72\mathfrak{g}^2$ .*

*Proof.* As we have already pointed out  $H = Q \rtimes (C_{q-1} \times C_{(q-1)/\mu})$ . Let  $M$  be the subgroup of  $C_{(q-1)/\mu}$  of index 2. Then the factor group  $\bar{T} = (C_{q-1} \times C_{(q-1)/\mu})/M$  has order  $2(q-1)$ . Here  $\bar{T}$  is a non-cyclic abelian group of order greater than 4. Obviously, the subgroup  $U = Q \rtimes M$  is a normal subgroup of  $H$ . Therefore,  $\bar{H} = H/U$  is an automorphism group of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/U$ . Since  $\bar{H} \cong \bar{T}$ , no subgroup of  $PGL(2, \mathbb{K})$  is isomorphic to  $\bar{H}$  by Result 2.9. Therefore  $\bar{\mathcal{X}}$  is not rational. If  $\bar{\mathcal{X}}$  is elliptic then  $U$  has a short orbit  $o$ , and for a point  $P \in o$ , the contribution of  $o$  to the different  $D(\mathcal{X}|\bar{\mathcal{X}})$  is at least  $|o|(|U_P| - 1) \geq \frac{1}{2}|o|U_P = \frac{1}{2}|U|$ . Assume that  $o$  is the unique short orbit of  $U$ . Then  $o$  is also an  $H$ -orbit. Thus  $|H_P|/|U_P| = |H|/|U|$  whence

$$|H_P U/U| = \frac{|H_P U|}{|U|} = \frac{|H_P||U|}{|H_P \cap U|} \cdot \frac{1}{|U|} = \frac{|H_P|}{|U_P|} = \frac{|H|}{|U|} = |\bar{T}| = 2(q-1).$$

This shows that  $H_P U/U$  has order  $2(q-1)$ . Furthermore,  $H_P U/U$  viewed as an automorphism group of  $\bar{\mathcal{X}}$  fixes the point  $\bar{P} \in \bar{\mathcal{X}}$  lying under  $o$ . But then  $q < 5$ , as  $\bar{\mathcal{X}}$  is elliptic, see Result 2.8. Therefore, there is another such orbit, and the Hurwitz genus formula gives  $2(\mathfrak{g}-1) \geq |U|$  whence

$$\mathfrak{g}-1 \geq \frac{1}{2}|U| = \frac{1}{4} \frac{q-1}{\mu} q^3.$$

This holds true for  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 2$ , by the Hurwitz genus formula. Therefore,

$$72\mathfrak{g}^2 > 72(\mathfrak{g}-1)^2 \geq \frac{24}{16\mu} \frac{(q-1)^2}{\mu} q^6 \geq \frac{3}{2} q^3 q^3 \frac{(q-1)^2}{\mu} > (q^2 + q + 1)(q+1)q^3 \frac{(q-1)^2}{\mu} = |G|,$$

a contradiction with the hypothesis of the lemma.  $\square$

A variant of the proof of Lemma 5.3 can be used to prove a similar result for the group  $SL(2, q)$  with  $q = d^k$  and  $d$  an odd prime. In the natural representation of  $SL(2, q)$  as a linear group of the vector space  $V(2, \mathbb{F}_q)$ , a Sylow  $d$ -subgroup is the subgroup  $Q$  consisting of all maps  $(x, y) \mapsto (x + ry, y)$  with  $r \in \mathbb{F}_q$ , and the normalizer of  $Q$  in  $SL(2, q)$  is the semidirect product  $Q \rtimes M$  where  $M \cong C_{q-1}$  consists of all transformations  $(x, y) \mapsto (ax, a^{-1}y)$  with  $a \in \mathbb{F}_q^*$ .

**Lemma 5.7.** *Let  $G$  be a group with commutator subgroup  $G' = SL(2, q)$  such that the centralizer of  $G'$  in  $G$  has order 2. If  $G$  is also a subgroup of  $\text{Aut}(\mathcal{X})$ , and*

$$|G| > 900\mathfrak{g}^2 \tag{15}$$

then  $\mathcal{X}$  has zero  $p$ -rank and  $q$  is a power of  $p$ .

*Proof.* For every  $g \in G$ , let  $\varphi_g$  denote the automorphism of  $G'$  taking the element  $h \in G'$  to its conjugate  $h^g$ . The map from  $G$  to  $\text{Aut}(G')$  which takes  $g$  to  $\varphi_g$  is a group homomorphism whose kernel consists of the elements in  $G$  which centralize  $G'$ . Hence,  $|G| = 2|L|$  with a subgroup  $L$  of  $\text{Aut}(G')$ . From  $\text{Aut}(SL(2, q)) \cong PGL(2, q)$ , we have that  $|G| \leq 2k(q+1)q(q-1)$  where  $q = d^k$  and  $d$  is an odd prime. Observe that if  $4k(q+1) > (q-1)q$  then  $q = 3, 5, 9$ , but for these values of  $q$ ,  $|G| \leq 2880 < 3600 \leq 900\mathfrak{g}^2$ . Hence

$$\frac{4k(q+1)}{(q-1)q} \leq 1. \tag{16}$$

For the normalizer  $H = Q \rtimes U$  of  $Q$  in  $SL(2, q)$ , assumption  $|G| > 900\mathfrak{g}^2$  yields

$$|H| = (q-1)q > 30\mathfrak{g}, \tag{17}$$

which shows that  $H$  satisfies the hypotheses in Lemma 4.1. Therefore,  $d = p$  and the quotient curve  $\tilde{\mathcal{X}} = \mathcal{X}/Q$  is rational. Take a point  $P$  from one of the short orbits  $\Omega_1$  of  $H$ . Then  $|H_P| = |H||Q_P| = (q-1)p^r$  with a positive integer  $r$ . By absurd,  $\mathcal{X}$  has positive  $p$ -rank and hence (i) of Lemma 4.1 occurs. We prove that Lemma 4.9 applies to  $G$  where  $g$  is the central involution of  $G'$ . Obviously,  $g \in Z(G)$  as  $G'$  is a characteristic subgroup of  $G$ .

It remains to show that the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/V$  with  $V = \langle g \rangle$  has zero  $p$ -rank. For this purpose, we need three facts:

- (i)  $\bar{G} = G/V$  is isomorphic to a subgroup of  $PGL(2, q)$  containing  $PSL(2, q)$ .
- (ii)  $\bar{G}$  is a subgroup of  $\text{Aut}(\bar{\mathcal{X}})$ .
- (iii) Let  $\bar{H} = H/V$ . If  $\bar{P}$  is a point of  $\bar{\mathcal{X}}$  lying under  $P \in \Omega_1$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ , then  $|\bar{H}_{\bar{P}}| = \frac{1}{2}(q-1)p^r$  with a positive integer  $r$ .

By (16), Lemma 5.3 for  $W = PSL(2, q)$  applies to  $\bar{G}$ . Therefore, either  $\bar{G} = PSL(2, q)$ , or  $\bar{G} = PGL(2, q)$ . If  $\bar{\mathfrak{g}} = \mathfrak{g}(\bar{\mathcal{X}}) \geq 2$  then  $\mathfrak{g} - 1 \geq 2(\bar{\mathfrak{g}} - 1)$  and hence

$$|\bar{G}| = \frac{1}{2}|G| \geq 900\mathfrak{g}^2 \geq 900 \cdot \frac{1}{2}(2\bar{\mathfrak{g}} - 1)^2 > 900\bar{\mathfrak{g}}^2,$$

which yields  $\bar{\mathfrak{g}} = 0$  by Lemma 5.1 applied to  $\bar{G}$ . If  $\bar{\mathcal{X}}$  is elliptic, (iii) together with Result 2.8 yield  $p = 3$  and  $\frac{1}{4}(q-1) = |\bar{H}_{\bar{P}}| \in \{6, 12\}$  whence  $q = 9$ . On the other hand  $|PGL(2, 9)| = 2|PSL(2, 9)| = 720$ . Hence  $|G| \leq 1440 < 900\mathfrak{g}^2$  as  $\mathfrak{g} \geq 2$ . Therefore,  $\bar{\mathcal{X}}$  is not elliptic.  $\square$

## 6 Structure of automorphism groups of curves of even genus

In this section we prove a classification theorem on the abstract structure of automorphism groups of algebraic curves with even genus. It is worth mentioning that the list of the possible structures is quite short. As a consequence, the inverse Galois problem restricted to curves with even genus is not solvable in general.

**Theorem 6.1.** *If  $G$  is a subgroup of the automorphism group of some non-rational algebraic curve with even genus, defined over an algebraically closed field of odd characteristic  $p$ , then one of the following cases occurs up to isomorphism:*

- (i)  $G$  has odd order;
- (ii)  $G = O(G) \rtimes S_2$  where  $S_2$  is a 2-group described in Result 2.11;
- (iii) the commutator subgroup of  $G/O(G)$  is isomorphic to  $SL(2, q)$  with  $q \geq 5$ ;
- (iv)  $PSL(2, q) \leq G/O(G) \leq P\Gamma L(2, q)$  with  $q \geq 3$ ;
- (v)  $PSL(3, q) \leq G/O(G) \leq P\Gamma L(3, q)$  with  $q \equiv 3 \pmod{4}$ ;
- (vi)  $PSU(3, q) \leq G/O(G) \leq P\Gamma U(3, q)$  with  $q \equiv 1 \pmod{4}$ ;
- (vii)  $G/O(G) = \text{Alt}_7$ ;
- (viii)  $G/O(G) = M_{11}$ ;
- (ix)  $G/O(G) = GL(2, 3)$ ;
- (x)  $G/O(G)$  is the unique perfect group of order 5040 and  $(G/O(G))/Z(G) \cong \text{Alt}_7$ ;
- (xi)  $G/O(G)$  is the group of order 48 named  $\text{SmallGroup}(48, 28)$  in the GAP-database.

In Subsection 6.3 refinements of Theorem 6.1 are obtained under the additional hypothesis that the order of  $G$  is large enough compared to genus  $\mathfrak{g}$  of the curve; more precisely when  $|G|$  is assumed to exceed  $900\mathfrak{g}(\mathcal{X})^2$ ; see Proposition 6.21.

Throughout the section,  $\mathcal{X}$  stands for an algebraic curve defined over an algebraically closed field  $\mathbb{K}$  of odd characteristic  $p$ , whose genus  $\mathfrak{g}$  is a (nonzero) even integer, and  $G$  denotes a subgroup of  $\text{Aut}(\mathcal{X})$ .

For  $G$  of even order, a key property is given in the following lemma.

**Lemma 6.2.** *If  $G$  has even order, then any 2-subgroup of  $G$  has a cyclic subgroup of index 2.*

*Proof.* Let  $U$  be a subgroup of  $\text{Aut}(\mathcal{X})$  of order  $2^u \geq 2$ . Since  $p$  is odd,  $U$  is tame. Therefore, the Hurwitz genus formula applied to  $U$  gives

$$2\mathfrak{g} - 2 = 2^u(2\bar{\mathfrak{g}} - 2) + \sum_{i=1}^m (2^u - \ell_i)$$

where  $\bar{\mathfrak{g}}$  is the genus of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/U$  and  $\ell_1, \dots, \ell_m$  are the short orbits of  $U$  on  $\mathcal{X}$ . Since  $2(\mathfrak{g}(\mathcal{X}) - 1) \equiv 2 \pmod{4}$  while  $2^u(2\bar{\mathfrak{g}} - 2) \equiv 0 \pmod{4}$ , some  $\ell_i$  ( $1 \leq i \leq m$ ) must be either 1 or 2. Therefore,  $U$  or a subgroup of  $U$  of index 2 fixes a point of  $\mathcal{X}$  and hence is cyclic.  $\square$

**Remark 6.3.** Lemma 6.2 shows that Result 2.11 applies to any 2-subgroup of  $\text{Aut}(\mathcal{X})$ .

Note that Lemma 6.2 holds also for curves with odd genus, provided that a Sylow 2-subgroup of  $G$  either fixes a point or has a short orbit of size 2. Actually, Theorem 6.1 holds under this weaker assumption.

For solvable  $G$ , Theorem 6.1 is obtained as a corollary of Lemma 6.2 together with Results 2.11 and 2.17.

**Proposition 6.4.** *If  $G$  is solvable then one of the following cases occurs.*

- (i)  $G = O(G) \rtimes S_2$  where  $S_2$  is a Sylow 2-subgroup of  $G$ .
- (ii)  $G/O(G) \cong PSL(2, 3)$ , or  $G/O(G) \cong PGL(2, 3)$ .
- (iii)  $G/O(G) \cong GL(2, 3)$ .

If  $G$  contains no non-trivial normal subgroup of odd order, then  $G$  is an *odd core-free* group. We first prove Theorem 6.1 in this case.

### 6.1 The case $|O(G)| = 1$

We show that the hypothesis of  $\mathfrak{g}$  to be even gives a heavy restriction on the structure of the minimal normal subgroups of an odd-core free subgroup of  $\text{Aut}(\mathcal{X})$ .

**Lemma 6.5.** *If  $G$  is odd core-free, then a minimal normal subgroup  $N$  of  $G$  is either a 2-group with  $|N| \leq 4$ , or a non-abelian simple group.*

*Proof.* Since  $N$  is characteristically simple, if  $N$  is solvable then  $N$  is an elementary abelian group, otherwise it is a direct product of pairwise isomorphic non-abelian simple groups; see, for instance, [31, Kapitel I, Satz 9.13]. In the former case,  $N \cong \mathbb{Z}_2^h$  since  $G$  is odd core-free, and  $h \leq 2$  otherwise  $N$  would be a 2-group without a cyclic subgroup of index 2. If  $N$  is the direct product of pairwise isomorphic simple groups, let  $M$  be one of these simple subgroups of  $N$ . From Result 2.14,  $M$  is neither cyclic nor a generalized quaternion group. By the remarks made after Result 2.11, a Sylow 2-subgroup of  $N$  contains an elementary abelian group of order 4, say  $V$ . Then  $M = N$ , otherwise  $V$  and any involution from another factor in that direct product would generate an elementary abelian subgroup of  $N$  of order 8, which is a 2-group without a cyclic subgroup of index 2.  $\square$

Three cases are now treated separately, according to whether a minimal normal subgroup  $N$  has order 2, 4, or is a simple group.

**Lemma 6.6.** *If  $G$  has a (minimal) normal subgroup  $N$  of order 2 then  $G$  has a 2-complement, unless a Sylow 2-subgroup of  $G$  is either a generalized quaternion group, or a semidihedral group. In the semidihedral case,  $G$  has an index 2 subgroup  $M$  such that either  $M$  has a 2-complement, or a Sylow 2-subgroup of  $M$  is a generalized quaternion group. If, in addition,  $G$  is solvable and has no 2-complement then  $G/O(G) \cong GL(2, 3)$  and  $G$  has a semidihedral Sylow 2-subgroup of order 16.*

*Proof.* If a Sylow 2-subgroup  $S_2$  of  $G$  is dihedral then Result 2.13 yields that  $G$  has a normal 2-complement. In fact,  $NO(G)/O(G)$  is a non-trivial subgroup of  $G/O(G)$  contained in the center of  $G/O(G)$  whereas any subgroup of  $P\Gamma L(2, q)$  containing  $PSL(2, q)$ , as well as  $\text{Alt}_7$ , have trivial center. By the first claim in Result 2.17, we are left with the case where  $S_2$  is a semidihedral group. Then  $S_2$  has a cyclic subgroup  $U$  of index 2 such that  $S_2 \setminus U$  contains an involution  $v$ . From Result 2.22, either  $G$  has a subgroup of index 2 containing  $U$ , or  $v$  is conjugate to an involution in  $U$ . The latter case cannot actually occur in our situation, since the normal subgroup  $N$  consists of the unique involution of  $U$  together with the identity. Therefore,  $G$  has a subgroup of index 2, and either (i) or (ii) in Result 2.18 holds. In case (i),  $G$  has an index 2 subgroup  $M$  with a dihedral Sylow 2-subgroup, and hence  $M$  has a 2-complement. In case (ii),  $G$  has an index 2 subgroup  $M$  with a generalized quaternion Sylow 2-subgroup. If  $G$  is solvable, the second claim in Result 2.17 applies.  $\square$

**Remark 6.7.** Lemma 6.6 applies to  $SL^\pm(2, q)$  and  $SU^\pm(2, q)$  and shows that  $\text{Aut}(\mathcal{X})$  has no subgroup isomorphic to  $SL^\pm(2, q)$  for  $q \equiv 1 \pmod{4}$  and to  $SU^\pm(2, q)$  for  $q \equiv -1 \pmod{4}$ .

**Lemma 6.8.** *If  $G$  has a minimal normal subgroup  $N$  of order 4, then either  $G = O(G) \rtimes S_2$  where  $S_2$  is the direct product of a cyclic group by a group of order 2, or  $G/O(G) \cong PSL(2, 3), PGL(2, 3)$ .*

*Proof.* Let  $V$  be a Sylow 2-subgroup of the centralizer  $T = C_G(N)$  of  $N$  in  $G$ . Then  $N \leq V$ . Since  $N \cong C_2 \times C_2$ , Result 2.11 shows that  $V$  must be abelian. Hence  $V \cong C_{2^m} \times C_2$  with  $m \geq 1$ . From Result 2.17,  $T$  has a normal 2-complement. We investigate the case where  $T$  is a proper subgroup of  $G$ . In this case,  $G/T$  is isomorphic to subgroup of  $\text{Sym}_3$  and hence it is solvable. Since  $T$  is also solvable, this yields that  $G$  is itself solvable. Since  $GL(2, 3)$  has no normal subgroup of order 4, Result 2.17 shows that either  $G/O(G) \cong PSL(2, 3)$  or  $G/O(G) \cong PGL(2, 3)$ .  $\square$

**Lemma 6.9.** *If  $G$  is an odd core-free group and has a non-abelian minimal normal subgroup  $N$  then one of the following cases occurs.*

- (i)  $N \cong PSL(2, q)$  with  $q \geq 5$  odd, and a Sylow 2-subgroup of  $N$  is dihedral;
- (ii)  $N \cong PSL(3, q)$  with  $q \equiv 3 \pmod{4}$ , and a Sylow 2-subgroup of  $N$  is semidihedral;
- (iii)  $N \cong PSU(3, q)$  with  $q \equiv 1 \pmod{4}$ , and a Sylow 2-subgroup of  $N$  is semidihedral;
- (iv)  $N \cong \text{Alt}_7$ , and a Sylow 2-subgroup of  $N$  is dihedral;
- (v)  $N \cong M_{11}$ , the Mathieu group on 11 letters, and a Sylow 2-subgroup of  $N$  is semidihedral.

*Proof.* By Lemma 6.5  $N$  is simple. From Result 2.16, a Sylow 2-subgroup of  $N$  is either dihedral, or semidihedral, or wreathed, or isomorphic to a Sylow 2-subgroup of  $SU(3, 2)$ . Actually, by Lemma 6.2 and Result 2.11, the latter two cases cannot occur in our situation. Now, the claim follows from Results 2.13 and 2.15.  $\square$

Theorem 6.1 for odd core-free groups is a corollary of Lemmas 6.10, 6.11, and 6.13.

**Lemma 6.10.** *Let  $G$  be an odd core-free group with generalized quaternion Sylow 2-subgroups. Then its commutator subgroup  $G'$  is isomorphic to  $SL(2, q)$  with  $q \geq 5$ , apart from three cases:*

- (i)  $G$  is a generalized quaternion group,
- (ii)  $G$  is isomorphic to the unique perfect group of order 5040 and  $G/Z(G) \cong \text{Alt}_7$ ,
- (iii)  $G$  is isomorphic to the group of order 48 named `SmallGroup(48, 28)` in the GAP-database.

*Proof.* If  $G$  is a 2-group, Case (i) holds. From now on  $|G|$  is assumed to have some odd divisor.

From Result 2.14,  $|Z(G)| = 2$ . We point out that the factor group  $\bar{G} = G/Z(G)$  is also odd core-free. By absurd, let  $\bar{N}$  be a non-trivial normal subgroup of  $\bar{G}$  of odd order. Then there exists a normal subgroup  $N$  of  $G$  such that  $\varphi(N) = \bar{N}$  where  $\varphi$  is the natural homomorphism  $G \rightarrow \bar{G}$ . Since  $G$  is odd core-free,  $N$  has even order. Since the involution  $z$  generating  $Z(G)$  is the unique involution in  $G$ ,  $N$  must contain  $z$ . Since  $|\bar{N}|$  is odd,  $|N|$  is twice an odd number bigger than 1. By  $z \in N$ , this yields  $N = Z(G) \times O(N)$ . Therefore,  $O(N)$  is non-trivial. Since  $N$  is a normal subgroup of  $G$  and  $O(N)$  is a characteristic subgroup of  $N$ , this yields that  $O(N)$  is a normal subgroup of  $G$ , a contradiction as  $G$  is odd core-free. Hence  $\bar{G}$  is odd core-free, as well. Furthermore, a Sylow 2-subgroup of  $\bar{G}$  is  $\bar{S}_2 = S_2/Z(S)$  which is a dihedral group as  $S_2$  a generalized quaternion group.

From Result 2.13,  $\bar{G}$  is either a dihedral group whose order is a power of 2 in which Case (i) holds, or  $\bar{G} \cong \text{Alt}_7$ , or  $PSL(2, q) \leq \bar{G} \leq P\Gamma L(2, q)$  with  $q$  odd, up to isomorphism. For  $q \geq 5$ ,  $PSL(2, q)$  is a perfect group, while the commutator subgroup of  $PSL(2, 3)$  is an elementary abelian group of order 4.

If  $q = 3$  then either  $\bar{G} \cong PSL(2, 3)$ , or  $\bar{G} \cong PGL(2, 3)$ . By direct GAP-aided computation,  $G \cong SL(2, 3)$  in the former case while if  $\bar{G} \cong PGL(2, 3)$ , the only possibility for  $G$  is the group *SmallGroup*(48, 28) in the GAP database. This gives (iii).

Suppose  $q \geq 5$ . As  $G'$  is a normal subgroup of  $G$ , and  $G$  is odd core-free,  $G'$  has even order. Since  $z$  is the unique involution of  $G$ ,  $z$  is contained in  $G'$ , that is,  $Z(G) \leq G'$ . Thus,  $G'/Z(G) = G'Z(G)/Z(G)$ . On the other hand,  $G'Z(G)/Z(G)$  is the commutator subgroup of  $\bar{G}$ , see [31, Kapitel I, Hilfssatz 8.4], and, since  $q \geq 5$ , either  $G'/Z(G) \cong PSL(2, q)$ , or  $G'/Z(G) \cong \text{Alt}_7$ .

The commutator subgroup  $H$  of  $G'$  is a characteristic subgroup of  $G'$ , and hence a normal subgroup of  $G$ . Therefore,  $H$  has even order, and hence contains  $Z(G)$ . From this, either  $H/Z(G) \cong PSL(2, q)$ , or  $H/Z(G) \cong \text{Alt}_7$ . Since  $H \leq G'$ , this yields  $H = G'$  showing that  $G'$  is a perfect group, and hence  $G'$  is perfect non-split extension of either  $PSL(2, q)$  or  $\text{Alt}_7$ . Now, the first claim in Lemma 6.10 follows from Result 2.19. Finally,  $\text{Alt}_7$  has a unique non-split central extension by a cyclic group of order 2 which is the group of order 5040 given in (ii).  $\square$

**Lemma 6.11.** *Let  $G$  be an odd core-free group with a semidihedral Sylow 2-subgroup  $S_2$ . If  $G$  has a (minimal) normal subgroup of order 2 then either  $G = S_2$ , or its commutator group  $G'$  is isomorphic to  $SL(2, q)$ .*

*Proof.* If  $G$  is solvable the assertion follows from Lemma 6.6. Assume that  $G$  has even order, and take a minimal normal subgroup  $N$  of  $G$  such that  $|N| = 2$ . Since  $S_2$  is semidihedral, the quotient group  $S_2/N$  is dihedral. Therefore, the quotient group  $\bar{G} = G/N$  has a dihedral Sylow 2-subgroup, and Result 2.13 applies. First the case where  $\bar{G}$  is isomorphic to a subgroup of  $P\Gamma L(2, q)$  containing  $PSL(2, q)$  is investigated. In this case, the commutator group  $\bar{G}'$  of  $\bar{G}$  is isomorphic to  $PSL(2, q)$  with  $q \geq 5$ . From Lemma 6.6,  $G$  has a (normal) subgroup  $M$  of index 2, and we may assume that its commutator group  $M'$  is isomorphic to  $SL(2, q)$ . Then  $N \geq M'$ , and the factor group  $\bar{M} = M/N$  is a subgroup of  $\bar{G}$ . In particular, the commutator subgroup  $\bar{M}'$  is contained in  $\bar{G}'$ . Since  $\bar{M}$  is normal in  $\bar{G}$  and  $\bar{M}'$  is a characteristic subgroup of  $\bar{M}$ , we have that  $\bar{M}'$  is normal in  $\bar{G}$ . Therefore,  $\bar{M}'$  is a normal subgroup of  $\bar{G}'$ . As  $q \geq 5$ ,  $\bar{G}'$  is simple, and hence  $\bar{M}' = \bar{G}'$ . From [31, Kapitel I, Hilfssatz 8.4],  $\bar{G}' = G'/N$  and  $\bar{M}' = M'/N$  whence  $G' = M' \cong SL(2, q)$ . Finally, since  $[G : M] = 2$  together with  $N \leq M \leq G$  yield  $[\bar{G} : \bar{M}] = 2$ , the case  $\bar{G} \cong \text{Alt}_7$  does not occur.  $\square$

**Lemma 6.12.** *If  $G$  is an odd core-free group with commutator subgroup  $G' \cong SL(2, q)$  then the centralizer of  $G'$  in  $G$  has order 2.*

*Proof.* Since  $G'$  is a normal subgroup of  $G$ , the centralizer  $C_G(G')$  of  $G'$  in  $G$  is a normal subgroup of  $G$ . As  $G$  is odd core-free,  $C_G(G')$  has even order. Assume by contradiction that  $|C_G(G')| > 2$ . Therefore  $|C_G(G')|$  must be divisible by four, otherwise  $|C_G(G')|$  is twice an odd number and hence  $C_G(G') = Z(G') \times O(C_G(G'))$  where  $O(C_G(G'))$  is a characteristic subgroup of  $C_G(G')$  of odd order contradicting the hypothesis that  $G$  is odd core-free. Therefore,  $C_G(G')$  has a Sylow 2-subgroup  $R$  of order at least 4.

Take a Sylow 2-subgroup  $V$  of  $G'$ , and let  $U = VR$ . Then  $|Z(U)| \geq 4$ . Since  $V$  is a generalized quaternion group, we also have  $|Z(V)| = 2$ . Therefore,  $U \not\cong V$ . From  $|Z(U)| \geq 4$ ,  $U$  is neither a generalized quaternion, nor a dihedral nor a semidihedral group. As we pointed out after Result 2.11, a modular maximal-cyclic group contains no generalized quaternion group. Therefore  $U \not\cong V$  cannot actually occur, and the assertion follows by absurd.  $\square$

**Lemma 6.13.** *If  $G$  is an odd core-free group with a non-abelian simple minimal normal subgroup, then one of the following cases occurs, up to isomorphisms, where  $q$  is an odd prime power  $d^k$ :*

- (i)  $PSL(2, q) \leq G \leq P\Gamma L(2, q)$  with  $q \geq 5$ ;
- (ii)  $PSL(3, q) \leq G \leq P\Gamma L(3, q)$  with  $q \equiv 3 \pmod{4}$ ;
- (iii)  $PSU(3, q) \leq G \leq P\Gamma U(3, q)$  with  $q \equiv 1 \pmod{4}$ ;
- (iv)  $G = \text{Alt}_7$ ;
- (v)  $G = M_{11}$ .

*Proof.* Let  $N$  be a non-abelian simple minimal normal subgroup of  $G$ . We prove that the centralizer  $C_G(N)$  of  $N$  in  $G$  is trivial. Obviously,  $C_G(N) \cap N$  is trivial. If  $C_G(N)$  has an involution  $u$  then  $u \notin N$  and hence the 2-subgroup of  $G$  generated by  $u$  and a Sylow 2-subgroup of  $N$  has rank at least 3, a contradiction. Therefore  $C_G(N)$  has odd order. Then  $C_G(N)$  is trivial, since  $C_G(N)$  is a normal subgroup of  $G$ , and  $G$  is odd core-free. Therefore,  $G$  is isomorphic to an automorphism group of  $N$ . By Lemma 6.9 all possibilities for  $N$  are determined. The cases  $N \cong PSL(2, q)$  with  $q \geq 5$ ,  $N \cong PSL(3, q)$  and  $N \cong PSU(3, q)$  give (i), (ii) and (iii), respectively. If  $N = \text{Alt}_7$  then either  $G = N$ , or  $G \cong \text{Sym}_7$ . The latter case cannot actually occur as a Sylow 2-subgroup of  $\text{Sym}_7$  has 2-rank 3. Hence (iv) holds. Finally,  $M_{11}$  is isomorphic to its automorphism group, and hence (v) holds.  $\square$

**Remark 6.14.** The subgroups of  $P\Gamma L(2, q)$  containing  $PSL(2, q)$  whose Sylow 2-subgroups have 2-rank 2 are  $PSL(2, q)$ ,  $PGL(2, q)$  and, when  $q = d^h$  with an odd prime  $d$  and  $h \geq 2$ , the semidirect product of  $PSL(2, q)$  or  $PGL(2, q)$  with a cyclic group whose order is an odd divisor of  $h$ . Analog results are valid for  $PSL(3, q)$  and  $PSU(3, q)$ . These groups are all the candidates for  $G$  in (i),(ii),(iii) of Lemma 6.13. It is not true that  $d$  must be equal to  $p$ . For instance, the Hermitian curve of equation  $X^{q+1} + Y^{q+1} + Z^{q+1} = 0$  defined over  $\mathbb{F}_q$  has genus  $\frac{1}{2}q(q-1)$  and if either  $p = 7$  or  $\sqrt{-7} \in \mathbb{F}_q$  it has an automorphism group isomorphic to  $PSL(2, 7)$ .

**Remark 6.15.** The Hermitian curve of equation  $X^6 + Y^6 + 1 = 0$  defined over  $\mathbb{F}_5$  has genus 10 and an automorphism group isomorphic to  $\text{Alt}_7$ . Over an algebraically closed field of characteristic 3, the modular curve  $X(11)$  has genus 26, and its automorphism group is isomorphic to  $M_{11}$ ; see [2, 40].

## 6.2 The case $|O(G)| > 1$

To prove Theorem 6.1 for any automorphism groups the following lemma is useful.

**Lemma 6.16.** *Let  $N$  be any subgroup of  $G$  of odd order. If a Sylow 2-subgroup of  $G$  fixes no point of  $\mathcal{X}$  then the quotient curve  $\mathcal{Y} = \mathcal{X}/N$  has also even genus.*

*Proof.* If the cover  $\mathcal{X}|\mathcal{Y}$  is unramified then the claim follows from the Hurwitz genus formula applied to  $N$ . For a point  $\bar{P} \in \mathcal{Y}$  where  $\mathcal{X}|\mathcal{Y}$  ramifies, take a point  $P \in \mathcal{X}$  lying over  $\bar{P}$ . Since  $|N|$  is odd, all ramification groups of  $N_P$  at  $P$  have odd order. By (2),  $d_P$  is even. Let  $\theta$  be the  $G$ -orbit containing  $P$ . Then,  $|G_P||\theta| = |G|$ . Take a Sylow 2-subgroup  $S$  of  $G$  containing a Sylow 2-subgroup  $S_P$  of  $G_P$ . Then  $S \neq S_P$ , as  $S$  does not fix  $P$ . Therefore,  $|S|$  does not divide  $|G_P|$  showing that  $|\theta|$  must be even. This yields that  $d_P|\theta|$  is divisible by four. Since  $N$  is a normal subgroup of  $G$ , the different  $D(\mathcal{X}|\mathcal{Y})$  is also divisible by four, that is,  $D(\mathcal{X}|\mathcal{Y})/2$  is even. Therefore, the Hurwitz genus formula applied to  $N$  yields  $\mathfrak{g}(\mathcal{X}) - 1 = |V|(\mathfrak{g}(\bar{\mathcal{X}}) - 1) + (D(\mathcal{X}|\mathcal{Y})/2)$  whence  $\mathfrak{g}(\mathcal{Y}) - 1$  is odd.  $\square$

**Remark 6.17.** If a Sylow 2-subgroup of  $G$  is not cyclic, then (iii) of Result 2.1 shows that the hypothesis of Lemma 6.16 is satisfied.

**Lemma 6.18.** *If  $|O(G)| > 1$  and  $G/O(G)$  is a subgroup of  $PGL(2, \mathbb{K})$ , then Theorem 6.1 holds for  $G$ .*

*Proof.* By Proposition 6.4,  $G/O(G)$  may be supposed to be non-solvable. Then Result 2.9 yields that either  $G/O(G) \cong PSL(2, q)$ , or  $G \cong PGL(2, q)$  with  $q \geq 5$ .  $\square$

We are now in a position to prove Theorem 6.1 for the case  $|O(G)| > 1$ . If  $G$  is any subgroup of  $\text{Aut}(\mathcal{X})$  then the factor group  $G/O(G)$  is an odd core-free automorphism group of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/O(G)$ . If a Sylow 2-subgroup fixes a point of  $\mathcal{X}$  then  $S_2$  is cyclic, and hence  $G = O(G) \rtimes S_2$ . Dismissing this case allows us to use Lemma 6.16. Doing so, either  $\bar{\mathcal{X}}$  is rational and  $\bar{G} = G/O(G)$  is a subgroup of  $PGL(2, \mathbb{K})$ , and Lemma 6.18 applies, or  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 2$  and Lemmas 6.6, 6.8, 6.10, 6.11 and 6.13 apply.

### 6.3 Refinements of Theorem 6.1 for large $G$

For large automorphism groups compared to the genera of the curves, the list in Theorem 6.1 shortens. For the odd core-free case this is shown in the following lemma.

**Lemma 6.19.** *If  $G$  is an odd core-free group of automorphisms of a curve  $\mathcal{X}$  of even genus  $\mathfrak{g}(\mathcal{X}) \geq 2$  such that*

$$|G| > 900\mathfrak{g}(\mathcal{X})^2, \tag{18}$$

*then  $\mathcal{X}$  has zero  $p$ -rank, and one of the following three cases occurs for  $G$ , up to group isomorphisms*

- (i)  $PSL(2, q)$ ,  $PGL(2, q)$ ,  $q = p^k \geq 5$ ;
- (ii)  $PSU(3, q)$ ,  $q = p^k$  and  $q \equiv 1 \pmod{4}$ ,  $PGU(3, q)$ ,  $q = p^k$  and  $q \equiv 5 \pmod{12}$ ;
- (iii)  $SL(2, q)$ ,  $SL^{(2)}(2, q)$ ,  $SU^\pm(2, q)$ ,  $q \equiv 1 \pmod{4}$ ,  $SL^\pm(2, q)$ ,  $q \equiv -1 \pmod{4}$ ,  $q = p^k \geq 5$ .

*Proof.* Theorem 6.1 with  $O(G) = \{1\}$  applies. Obviously,  $|G|$  is even, otherwise  $G$  is not odd-core free, because it is solvable by Result 2.26. If  $G$  is solvable, Theorem 6.1 shows that  $G$  is a 2-group apart from four sporadic cases, namely when  $G \cong PSL(2, 3)$ ,  $PGL(2, 3)$ ,  $GL(2, 3)$ ,  $\text{SmallGroup}(48, 28)$  whose orders are 12, 24, 48, and 48 respectively. If  $G$  is a 2-group then Lemma 6.2 yields that  $G$  has a cyclic subgroup  $N$  of index 2. From (i) of Result 2.7 applied to  $N$ ,  $|G| = 2|N| \leq 8(\mathfrak{g}(\mathcal{X}) + 1)$  whence  $|G| < 900\mathfrak{g}(\mathcal{X})^2$ . Therefore,  $G$  is assumed to be non-solvable.

The sporadic cases  $G \cong \text{Alt}_7$ ,  $G \cong M_{11}$  and  $G/Z(G) \cong \text{Alt}_7$  do not occur. In fact, for  $G \cong \text{Alt}_7$ , (18) yields  $\mathfrak{g}(\mathcal{X})^2 < 4$  which contradicts  $\mathfrak{g}(\mathcal{X}) \geq 2$ . For  $G \cong M_{11}$ , we have  $|G| = 7920$ . From (18), it follows  $\mathfrak{g}(\mathcal{X})^2 < 9$  whence  $\mathfrak{g}(\mathcal{X}) = 2$ . In this case the hyperelliptic involution  $\omega$  does not belong to  $G$ , since  $G$  is simple; hence,  $G\langle\omega\rangle/\langle\omega\rangle \cong M_{11}$ , which contradicts the last claim in Result 2.8. For  $G/Z(G) \cong \text{Alt}_7$ , we have  $|G| = 5040$ , and (18) yields  $\mathfrak{g}(\mathcal{X}) = 2$  which shows that the quotient curve  $\mathcal{X}/Z(G)$  is rational by Remark 6.3. But this contradicts Result 2.9 as no subgroup of  $PGL(2, \mathbb{K})$  is isomorphic to  $\text{Alt}_7$ .

Furthermore, the case  $PSL(3, q) \leq G \leq P\Gamma L(3, q)$  is ruled out by Lemma 5.3 and Remark 5.4.

Now, from Theorem 6.1 with  $|O(G)| = 1$ , either  $G' \cong SL(2, q)$ , or one of the Cases (iv) or (vi) of Theorem 6.1 hold. In the latter two cases,  $\mathcal{X}$  has zero  $p$ -rank and  $q$  is a power of  $p$  from Lemma 5.1. Also, by Lemma 5.3 and Remark 5.4, either (i) or (ii) of Lemma 6.19 holds.

Hence  $G' = SL(2, q)$  can be assumed. In this case a Sylow 2-subgroup of  $G$  is either a generalized quaternion group or a semidihedral group; in fact, the subgroup  $N = Z(G')$  generated by the central

involution in  $G' = SL(2, q)$  is normal in  $G$  since  $G'$  is a characteristic subgroup of  $G$ , and hence Lemma 6.6 applies. From Lemmas 6.12 and 5.7,  $\mathcal{X}$  has zero  $p$ -rank.

Also, since  $N$  is normal in  $G$ , the central involution in  $G'$  commutes with each element in  $G$  and hence  $Z(G') \subseteq Z(G)$ . Actually,  $Z(G') = Z(G)$  by Lemma 6.12. From Lemma 5.7  $d = p$ , that is,  $q$  is a power of  $p$ .

To prove that Case (iii) must occur, consider the quotient group  $\bar{G} = G/Z(G)$  regarded as an automorphism group of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/Z(G)$ . Since the Sylow 2-subgroups of  $G$  are either semidihedral groups or generalized quaternion groups, those of  $\bar{G}$  are dihedral groups. Furthermore, as  $G' \cong SL(2, q)$ , we have  $G'/Z(G) \cong PSL(2, q)$ . Since  $G'/Z(G) = G'Z(G)/Z(G)$  and, by [31, Kapitel I, Hilfssatz 8.4],  $\bar{G}' \cong G'Z(G)/Z(G)$ , this yields  $\bar{G}' \cong PSL(2, q)$ .

First we prove that  $\bar{G}$  is also odd core-free. By absurd, let  $\bar{N}$  be a non-trivial odd order normal subgroup of  $\bar{G}$ . The subgroup  $N$  of  $G$  containing  $Z(G)$  such that  $N/Z(G) = \bar{N}$  has order twice an odd number. Hence, its maximal normal subgroup of odd order is non-trivial. Since such a maximal subgroup is a characteristic subgroup of  $N$ , it must be a normal subgroup of  $G$ , a contradiction as  $G$  is odd core-free.

Next we prove that  $\bar{G}$  is isomorphic to a subgroup of  $PGL(2, q)$  containing  $PSL(2, q)$ . Since  $\bar{G}$  is odd core-free and its Sylow 2-subgroups are dihedral, Result 2.13 applies to  $\bar{G}$  showing that either  $\bar{G} \cong \text{Alt}_7$ , or, up to an isomorphism,  $PSL(2, n) \leq \bar{G} \leq PGL(2, n)$  with an odd prime power  $n \geq 5$ . As we have already shown,  $\bar{G}' \cong PSL(2, q)$  is the commutator group of  $\bar{G}$ . Therefore  $n = q$ , since  $PSL(2, n)$  is the commutator subgroup of any subgroup of  $PGL(2, n)$  containing  $PSL(2, n)$ . The case  $\bar{G} \cong \text{Alt}_7$  does not occur. In fact, from  $2|\text{Alt}_7| = 5040 > 900\mathfrak{g}(\bar{\mathcal{X}})^2$ , we would have  $\mathfrak{g}(\bar{\mathcal{X}}) = 2$  which contradicts Result 2.8.

To finish the proof, three cases are distinguished according to the value  $\mathfrak{g}(\bar{\mathcal{X}})$ .

If  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 2$  then the Hurwitz genus formula together with (18) yield  $|\bar{G}| > 900\mathfrak{g}(\bar{\mathcal{X}})^2$ . From Lemma 5.3 and Remark 5.4 applied to  $\bar{G}$ , either  $\bar{G} \cong PSL(2, q)$  or  $\bar{G} \cong PGL(2, q)$ . In the former case,  $|\bar{G}| = 2|\bar{G}'| = 2|PSL(2, q)| = |SL(2, q)| = |G'|$  whence  $G = G'$  follows. This gives the first possibility in (iii). In the latter case,  $G$  is isomorphic to a central extension of  $PGL(2, q)$  by a group of order 2. If this is a split extension then  $G$  contains a subgroup  $T \cong PGL(2, q)$  such that  $G = Z(G) \times T$ . Then a Sylow 2-subgroup of  $G$  is the direct product of a dihedral group and a cyclic group of order 2. But such a direct product contains neither a generalized quaternion group nor a semidihedral group. Therefore, Result 2.21 applies, and either the second, or the third, or the fourth case in (iii) must occur.

If  $\mathfrak{g}(\bar{\mathcal{X}}) = 0$ , Result 2.9 gives the same possibilities for  $\bar{G}$ , namely  $\bar{G} = PSL(2, q)$  or  $\bar{G} = PGL(2, q)$ , and the same conclusion can be made.

If  $\mathfrak{g}(\bar{\mathcal{X}}) = 1$  then the Hurwitz genus formula shows that the set  $\theta$  of all points fixed by  $Z(G)$  has size  $2\mathfrak{g}(\bar{\mathcal{X}}) - 2$ . Further,  $\bar{G}$  leaves  $\theta$  invariant. For a point  $\bar{P} \in \theta$ , the stabilizer  $\bar{G}_{\bar{P}}$  of  $\bar{P}$  has order at most 12 by Result 2.8. Therefore,  $|\bar{G}| \leq 12|\theta|$  whence  $|\bar{G}| \leq 24(\mathfrak{g}(\bar{\mathcal{X}}) - 1)$ . Thus  $|\bar{G}| \leq 48(\mathfrak{g}(\bar{\mathcal{X}}) - 1)$ . Comparing with (18) shows that this is impossible.  $\square$

**Remark 6.20.** The Hermitian curve of equation  $Y^q + Y = X^{q+1}$  with  $q \equiv 1 \pmod{4}$  is an example for (ii). If  $q \geq 125$ , the Roquette curve  $\mathcal{X}$  of equation  $Y^2 = X^q - X$  provides an example for (iii) with  $G \cong SL(2, q)$  where  $q \equiv 1 \pmod{4}$ .

The general case  $|O(G)| \geq 1$  is described in the following proposition.

**Proposition 6.21.** *Let  $G$  be a non-solvable group of automorphisms of a curve  $\mathcal{X}$  of even genus  $\mathfrak{g}(\mathcal{X}) \geq 2$  such that (18) holds. Then either  $G/O(G)$  has a non-abelian simple minimal normal subgroup, and one of the following two cases occurs, up to group isomorphisms*

- (A)  $G/O(G) \cong PSL(2, q)$ ,  $G/O(G) \cong PGL(2, q)$ ,  $q = p^k \geq 5$ ;
- (B)  $G/O(G) \cong PSU(3, q)$ ,  $q = p^k$  and  $q \equiv 1 \pmod{4}$ ,  $G/O(G) \cong PGU(3, q)$ ,  $q = p^k$  and  $q \equiv 5 \pmod{12}$ ;

or

(C)  $G/O(G) \cong SL(2, q), SL^{(2)}(2, q), G/O(G) \cong SU^\pm(2, q), q \equiv 1 \pmod{4}, G/O(G) \cong SL^\pm(2, q), q \equiv -1 \pmod{4}$ , where, in all cases,  $q = p^k \geq 5$ .

*Proof.*  $G/O(G)$  is an odd core-free automorphism group of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/O(G)$ . If  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 2$ , the assertion follows from Lemma 6.19. Furthermore, from Lemma 6.16 and Remark 6.17,  $\bar{\mathcal{X}}$  is not elliptic. If  $\bar{\mathcal{X}}$  is rational then  $G/O(G)$  is a subgroup of  $PGL(2, q)$  with  $q = p^k$ . Since  $G/O(G)$  is supposed to be non-solvable, Result 2.9 yields that case (A) occurs with only two possible exceptions for  $p \neq 5$ , namely  $G/O(G) \cong PSL(2, 5)$  and  $G/O(G) \cong PGL(2, 5)$ . We rule out both exceptions. Both  $PSL(2, 5)$  and  $PGL(2, 5)$  contain a maximal, solvable non-abelian subgroup of index 6. As  $O(G)$  is solvable by Result 2.26,  $G$  also has a solvable non-abelian subgroup  $N$  of index 6. This together with (18) give  $|N| > 150\mathfrak{g}(\mathcal{X})^2$ . As  $N$  is solvable, Theorem 1.1 yields that  $N$  fixes a point  $P \in \mathcal{X}$ . Since  $G$  does not fix  $P$ , and  $N$  is a maximal subgroup of  $G$ , the  $G$ -orbit  $o$  of  $P$  has length 6. By Theorem 1.1,  $\mathcal{X}$  has zero  $p$ -rank. If  $N$  has some elements of order  $p$ , then a  $p$ -subgroup of  $N$  fixes  $P$  and acts transitively on the remaining 5 points in  $o$ . But this yields  $p = 5$ , a contradiction. Otherwise,  $N$  is a prime to  $p$  subgroup, and the classical Hurwitz bound yields  $|N| < 84(\mathfrak{g} - 1)$  whence  $|G| < 504(\mathfrak{g} - 1)$  contradicting (18).  $\square$

Finally, a useful bound on the size of  $O(G)$  is given in the lemma below.

**Lemma 6.22.** *Let  $G$  be a non-solvable group of automorphisms of a curve  $\mathcal{X}$  of even genus  $\mathfrak{g} \geq 2$  such that (18) holds. Let  $\bar{\mathcal{X}} = \mathcal{X}/O(G)$ . If  $\mathfrak{g}(\bar{\mathcal{X}}) > 0$  then  $900|O(G)| < |G/O(G)|$ .*

*Proof.* From Lemma 6.16 and Remark 6.17,  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 2$ . The Hurwitz genus formula applied to  $O(G)$  gives  $\mathfrak{g}(\bar{\mathcal{X}}) - 1 \geq |O(G)|$ . This together with (18) show  $|G/O(G)||O(G)| > 900\mathfrak{g}(\mathcal{X})^2 > 900|O(G)|^2$  whence the claim follows.  $\square$

## 7 Large automorphism groups of curves with even genus

An important step towards our second main result is the following theorem.

**Theorem 7.1.** *Let  $G$  be a non-solvable automorphism group of an algebraic curve  $\mathcal{X}$  of even genus  $\mathfrak{g}(\mathcal{X}) \geq 2$  such that*

$$|G| > 900\mathfrak{g}(\mathcal{X})^2.$$

*Then  $\mathcal{X}$  has zero  $p$ -rank. Furthermore,  $O(G)$  is a cyclic prime to  $p$  subgroup, and either  $O(G) = Z(G)$  or  $[Z(G) : O(G)] = 2$  according to whether Cases (A), (B), or (C) in Proposition 6.21 hold.*

The proof of Theorem 7.1 requires a careful analysis of the Cases (A), (B), (C) in Proposition 6.21. The basic idea is to find an appropriate upper bound on  $|O(G)|$  depending on  $q$  so that the linear bound given in Lemma 4.1 may be applied to show that  $\mathcal{X}$  has zero  $p$ -rank. Once this is done, the relationship between  $O(G)$  and  $Z(G)$  can thoroughly been worked out.

### 7.1 Proof of Theorem 7.1 in Case (A) of Proposition 6.21

Let  $L = G'O(G)$  where  $G'$  is the commutator subgroup of  $G$ . Since  $G'O(G)/O(G) \cong (G/O(G))'$  by [31, Kapitel I, Hilfssatz 8.4], we have that  $\bar{L} = L/O(G)$  is the commutator subgroup  $\bar{G}'$  of  $\bar{G}$ . In particular  $\bar{L} = \bar{G}' \cong PSL(2, q)$ , and either  $\bar{G}' = \bar{G}$ , or  $\bar{G}'$  is the unique normal subgroup of  $\bar{G}$  and  $\bar{G} \cong PGL(2, q)$ . Furthermore, either  $L = G$  or the index of  $L$  in  $G$  is equal to 2.

**Lemma 7.2.** *If Case (A) in Proposition 6.21 holds then*

$$\frac{(q-1)q}{|O(G)|(q+1)} > \frac{25}{4}. \quad (19)$$

*In particular,*

$$|O(G)| < \frac{4}{25}q \quad (20)$$

and  $q > 11$ .

*Proof.* Consider  $\bar{L} = L/O(G)$  as an automorphism group of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/O(G)$ . Since  $\bar{L} \cong PSL(2, q)$  its Sylow 2-subgroups are dihedral and hence not cyclic. Result 2.1 shows that  $L$  fixes no point of  $\mathcal{X}$ . From Lemma 6.16,  $\mathfrak{g}(\bar{\mathcal{X}})$  is even. Therefore, either  $\bar{\mathcal{X}}$  is rational, or  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 2$ . In the latter case, since  $\bar{L}$  contains an abelian subgroup of odd order  $q$ , see Result 2.9, we have  $4\mathfrak{g}(\bar{\mathcal{X}}) + 3 \geq q$  by (i) of Result 2.7. Thus  $4\mathfrak{g}(\bar{\mathcal{X}}) + 4 \geq q + 1$ .

If  $\bar{\mathcal{X}}$  is not rational, the Hurwitz genus formula applied to  $O(G)$  gives  $\mathfrak{g}(\mathcal{X}) - 1 \geq |O(G)|(\mathfrak{g}(\bar{\mathcal{X}}) - 1)$ . From (18),

$$(q-1)q > 900 \frac{\mathfrak{g}(\mathcal{X})^2}{|O(G)|(q+1)}.$$

Since  $\mathfrak{g}(\mathcal{X}) > \mathfrak{g}(\mathcal{X}) - 1$ ,

$$\frac{(q-1)q}{|O(G)|(q+1)} > 900 \left( \frac{\mathfrak{g}(\bar{\mathcal{X}}) - 1}{q+1} \right)^2 > 900 \left( \frac{\mathfrak{g}(\bar{\mathcal{X}}) - 1}{4(\mathfrak{g}(\bar{\mathcal{X}}) + 1)} \right)^2 > \frac{900}{144} = \frac{25}{4},$$

whence (19) follows. A direct computation shows that this yields (20) and  $q > 11$ .

If  $\bar{\mathcal{X}}$  is rational, then  $\bar{L}$  acts on  $\bar{\mathcal{X}}$  as  $PSL(2, q)$  on the projective line  $PG(1, \mathbb{K})$ . Take any point  $\bar{P} \in \bar{\mathcal{X}}$ . As  $PSL(2, q)$  is non-solvable,  $\bar{L}$  does not fix  $\bar{P}$  by (iii) of Result 2.1. Hence, the  $\bar{L}$ -orbit of  $\bar{P}$  has length at least  $q$ . In fact,  $|\bar{L}_{\bar{P}}| \leq \frac{1}{2}q(q-1)$  as the order of the largest proper subgroup of  $PSL(2, q)$  is  $\frac{1}{2}q(q-1)$  by Result 2.9. Now take a point  $P \in \mathcal{X}$  where the cover  $\mathcal{X}|\bar{\mathcal{X}}$  ramifies. Then the  $G$ -orbit  $o$  of  $P$  has length at least  $qu$  where  $u = |O(G)|/|O(G)_P|$ . The Hurwitz genus formula applied to  $O(G)$  yields

$$2\mathfrak{g} - 2 \geq -2|O(G)| + |o|(|O(G)_P| - 1) \geq -2|O(G)| + |o|\frac{2}{3}|O(G)_P| \geq |O(G)|(\frac{2}{3}q - 2).$$

Hence  $\mathfrak{g}(\mathcal{X}) > \frac{1}{3}(q-3)|O(G)|$ . From this and  $(q+1)q(q-1)|O(G)| > 900\mathfrak{g}^2$ ,

$$|O(G)| < \frac{9}{900} \frac{(q+1)(q-1)}{(q-3)^2} q < \frac{3}{50}q$$

Therefore, both (19) and (20) hold for any  $\bar{\mathcal{X}}$ . Also,  $q > 11$  must hold.  $\square$

**Lemma 7.3.** *If Case (A) in Proposition 6.21 holds then the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/O(G)$  has zero  $p$ -rank.*

*Proof.* We may assume that  $\bar{\mathcal{X}}$  is not rational. As we have already observed in the proof of Lemma 7.2,  $\mathfrak{g}(\bar{\mathcal{X}})$  is even by Lemma 6.16.

Since  $\bar{L}$  contains a subgroup  $\bar{Q}$  of odd order  $q \geq 13$ , see Result 2.9, if  $\bar{\mathcal{X}}$  has positive  $p$ -rank then  $\mathfrak{g}(\bar{\mathcal{X}}) - 1 \geq \frac{p-2}{p}q \geq \frac{13}{3}$  by Result 2.5 applied to  $\bar{Q}$ . Thus we can assume  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 6$  and hence

$$\mathfrak{g}(\mathcal{X}) > \mathfrak{g}(\mathcal{X}) - 1 \geq |O(G)|(\mathfrak{g}(\bar{\mathcal{X}}) - 1) \geq \frac{5}{6}|O(G)|\mathfrak{g}(\bar{\mathcal{X}}). \quad (21)$$

As  $|\bar{L}| \geq \frac{|G|}{2|O(G)|}$  holds, taking into account (18) we then have

$$|\bar{L}| \geq \frac{450\mathfrak{g}(\mathcal{X})^2}{|O(G)|} > 450 \cdot \frac{25}{36} |O(G)|\mathfrak{g}(\bar{\mathcal{X}})^2 > 900\mathfrak{g}(\bar{\mathcal{X}})^2.$$

From Lemma 6.19 applied to  $\bar{L}$ , the  $p$ -rank of  $\bar{\mathcal{X}}$  is equal to zero.  $\square$

**Lemma 7.4.** *If Case (A) in Proposition 6.21 holds then  $\mathcal{X}$  has zero  $p$ -rank.*

*Proof.* Lemma 7.3 together with Result 2.4 applied to  $\bar{\mathcal{X}}$  show that a Sylow  $p$ -subgroup  $\bar{Q}$  of  $\bar{L}$ , as well as its normalizer in  $\bar{L}$ , fixes a unique point  $\bar{P} \in \bar{\mathcal{X}}$ . Here  $|\bar{Q}| = q$ , and the normalizer of  $\bar{Q}$  in  $\bar{L}$  is the semidirect product  $\bar{Q} \rtimes \bar{T}$  with a cyclic group  $\bar{T}$  of order  $\frac{1}{2}(q-1)$  by Result 2.9. Since this normalizer is a maximal subgroup of  $\bar{G}$ , see again Result 2.9, it is the stabilizer of  $\bar{P}$  in  $\bar{L}$ . Let  $o$  be the  $O(G)$ -orbit lying over  $\bar{P}$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ . The counter-image of  $\bar{Q} \rtimes \bar{T}$  in the homomorphism  $L \rightarrow \bar{L}$  is a subgroup  $N$  of order  $\frac{1}{2}(q-1)q|O(G)|$  where  $N$  is the subgroup of  $G$  which preserves  $o$ . For a point  $P \in o$ , the stabilizer  $H$  of  $P$  in  $N$  has order  $\frac{1}{2}(q-1)q|O(G)_P|$ . Therefore, the (unique) Sylow  $p$ -subgroup  $Q_1$  of  $H$  has order  $q_1 = qp^a$  and a complement of  $Q_1$  in  $H$  is a cyclic subgroup  $C_t$  of order  $t = \frac{1}{2}(q-1)b$  with  $p \nmid b$  by (iii) of Result 2.1. Hence  $H = Q_1 \rtimes C_t$ , and  $|o|p^ab = |O(G)|$ . Now, since by (18)  $q(q-1)(q+1)|O(G)| > 900\mathfrak{g}(\mathcal{X})^2$ ,

$$|H|^2 > (p^ab)^2 \frac{\frac{1}{4}(q-1)q}{|O(G)|(q+1)} 900\mathfrak{g}(\mathcal{X})^2.$$

This together with (19) give  $|H|^2 > 900\mathfrak{g}(\mathcal{X})^2$  whence

$$|H| = q_1t > 30\mathfrak{g}(\mathcal{X}).$$

From Lemma 4.1 and Remark 4.3, either  $\mathcal{X}$  has zero  $p$ -rank, or  $Q_1$  has just one short orbit  $\theta$  other than its fixed point  $P$ . Observe that  $\theta$  is contained in  $o$ . In fact, each  $Q_1$ -orbit in  $o$  is short as  $|o| \leq |O(G)| < q < q_1$  by (20). Therefore  $o = \theta \cup \{P\}$ , and hence  $|o| = 1 + p^h$  for some  $h \geq 0$ . Since  $|o|$  divides  $|O(G)|$  this implies that  $|O(G)|$  is even, a contradiction. Thus  $\mathcal{X}$  has zero  $p$ -rank.  $\square$

To complete our investigation of Case (A) in Proposition 6.21, we only need the following result.

**Lemma 7.5.** *If Case (A) in Proposition 6.21 holds then  $O(G)$  is a prime to  $p$  cyclic group, and  $Z(G) = O(G)$ .*

*Proof.* For every  $h \in G$  the map  $\varphi_h$  taking  $u \in O(G)$  to  $h^{-1}uh$  is an automorphism of  $O(G)$ , and hence the map  $\Phi : h \mapsto \varphi_h$  is a homomorphism from  $G$  into  $\text{Aut}(O(G))$ . Take a Sylow  $p$ -subgroup  $Q$  of  $G$ . From Lemma 7.4 and Result 2.4,  $Q$  fixes a unique point  $P \in \mathcal{X}$  but no non-trivial element of  $Q$  fixes a point other than  $P$ . If  $g$  is any element in  $O(G)$ , then (20) yields that the  $Q$ -orbit of  $g$  in the action of  $\Phi$  has length smaller than  $|Q|$ . Hence,  $g$  commutes with a non-trivial element of  $Q$ . Therefore,  $g$  fixes  $P$ , and hence  $O(G)$  does, as well. Repeating this argument with another Sylow  $p$ -subgroup of  $G$ , it turns out that  $O(G)$  fixes a point  $P' \in \mathcal{X}$  other than  $P$ . From (i) of Result 2.4,  $O(G)$  contains no element of order  $p$ . Therefore, from (iii) of Result 2.1,  $O(G)$  is a cyclic prime to  $p$  group. In particular,  $\ker(\Phi) \geq O(G)$ . Since  $\bar{G}$  is either simple, or  $\bar{L} \cong PSL(2, q)$  is the only non-trivial normal subgroup of  $\bar{G}$ , two cases arise namely  $\ker(\Phi) = O(G)$  and  $\ker(\Phi) \geq L$ .

In the former case,  $\Phi$  induces a faithful action of  $\bar{L}$  on  $O(G)$ . If  $\Lambda$  is a non-trivial orbit then  $|\Lambda| < q$  by (20). On the other hand, since  $q > 11$ , Result 2.9 yields  $|\Lambda| \geq q+1$ , a contradiction.

In the latter case,  $\ker(\Phi) \geq L$  and hence  $O(G) \subseteq Z(L)$ ; actually,  $O(G) = Z(L)$  since  $Z(\bar{L})$  is trivial. As we have shown,  $O(G)$  fixes a point  $P \in \mathcal{X}$ . Since  $\gamma(\mathcal{X}) = 0$ , (ii) of Result 2.4 shows that  $G_P$  coincides with the normalizer  $N_{\bar{G}}(Q)$  of  $Q$  in  $G$ . From Result 2.12, a complement  $C$  of  $Q$  contains  $O(G)$ . If  $L \not\leq G$  then  $C$  contains an element of  $G \setminus L$ . Therefore, some element in  $G \setminus L$  centralizes  $O(G)$ . This shows that  $Z(G) = O(G)$ , since  $Z(\bar{G})$  is trivial.  $\square$

## 7.2 Proof of Theorem 7.1 in Case (B) of Proposition 6.21

The quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/O(G)$  is not rational as  $\bar{G} = G/O(G)$  is an automorphism group of the quotient curve  $\bar{\mathcal{X}} = \mathcal{X}/O(G)$  but  $PGL(2, \mathbb{K})$  has no subgroup isomorphic to  $\bar{G} \cong PSU(3, q)$  by Result 2.9. Also,  $\bar{\mathcal{X}}$  is neither elliptic by Lemma 6.16. Then  $\mathfrak{g}(\bar{\mathcal{X}}) > 2$  by Result 2.8.

In particular,  $\mathfrak{g}(\bar{\mathcal{X}}) > 2$ . From  $|O(G)| \geq 3$  and  $\mathfrak{g}(\mathcal{X}) > \mathfrak{g}(\mathcal{X}) - 1 \geq |O(G)|(\mathfrak{g}(\bar{\mathcal{X}}) - 1)$ , we have by (18)

$$|\bar{G}| = \frac{|G|}{|O(G)|} > \frac{900}{|O(G)|} \mathfrak{g}(\mathcal{X})^2 > 900|O(G)|(\mathfrak{g}(\bar{\mathcal{X}}) - 1)^2 \geq 900 \frac{|O(G)|}{3} \mathfrak{g}(\bar{\mathcal{X}})^2 \geq 900 \mathfrak{g}(\bar{\mathcal{X}})^2$$

which together with Lemma 5.1 show that  $\bar{\mathcal{X}}$  has zero  $p$ -rank.

Let  $L = G'O(G)$  where  $G'$  is the commutator subgroup of  $G$ . By [31, Kapitel I, Hilfssatz 8.4],  $\bar{L} = L/O(G)$  is the commutator subgroup  $\bar{G}'$  of  $\bar{G}$ . In particular  $\bar{L} = \bar{G}' \cong PSU(3, q)$ , and either  $\bar{G}' = \bar{G}$ , or  $\bar{G}'$  is the unique proper normal subgroup of  $\bar{G}$  and  $\bar{G} \cong PGU(3, q)$ . First we show how the arguments used in Section 7.1 can be adapted as far as

$$\frac{(q^2 - 1)q^3}{|O(G)|(q^3 + 1)} > \mu^2 \tag{22}$$

where, as in Result 2.10,  $\mu = \gcd(3, q + 1)$ .

**Lemma 7.6.** *If (22) is assumed then Theorem 7.1 holds.*

*Proof.* Since the  $p$ -rank of  $\bar{\mathcal{X}}$  is equal to zero, (i) of Result 2.4 shows that a Sylow  $p$ -subgroup  $\bar{Q}$  of  $\bar{L}$  fixes a unique point  $\bar{P} \in \bar{\mathcal{X}}$ . The normalizer of  $\bar{Q}$  in  $\bar{L}$  is the semidirect product  $\bar{Q} \rtimes \bar{T}$  where  $\bar{Q}$  is a non-abelian  $p$ -group of order  $q^3$  while  $\bar{T}$  is a cyclic group of order  $(q^2 - 1)/\mu$ . From Result 2.10, this normalizer is a maximal subgroup of  $\bar{L}$ . Hence it coincides with the stabilizer of  $\bar{P}$  in  $\bar{L}$ . Let  $o$  be the  $O(G)$ -orbit lying over  $\bar{P}$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ . The counter-image of  $\bar{Q} \rtimes \bar{T}$  in the homomorphism  $L \rightarrow \bar{L}$  is a subgroup  $N$  of order  $(q^2 - 1)q^3|O(G)|/\mu$ . For a point  $P \in o$ , the stabilizer of  $P$  in  $N$  is a subgroup  $H$  of order  $(q^2 - 1)q^3|O(G)_P|/\mu$ . Therefore, the (unique) Sylow  $p$ -subgroup  $Q_1$  of  $H$  has order  $q_1 = q^3p^a$  and a complement of  $Q_1$  in  $H$  is a cyclic subgroup  $C_t$  of order  $t = b(q^2 - 1)/\mu$  with  $p \nmid b$ . Hence  $H = Q_1 \rtimes C_t$ , and  $|o|p^ab = |O(L)|$ . From (18),

$$(q^2 - 1)q^3 > \frac{900\mathfrak{g}(\mathcal{X})^2}{(q^3 + 1)|O(G)|}.$$

Therefore,

$$|H|^2 = (q_1t)^2 > (p^ab)^2 \frac{(q^2 - 1)q^3}{\mu^2|O(G)|(q^3 + 1)} 900\mathfrak{g}(\mathcal{X})^2$$

This together with (22) give

$$|H| > 30\mathfrak{g}(\mathcal{X}).$$

From Lemma 4.1 and Remark 4.3, either  $\mathcal{X}$  has zero  $p$ -rank, or  $Q_1$  has just one short orbit  $\theta$  other than its fixed point  $P$ . Observe that  $\theta$  is contained in  $o$ . In fact, each  $Q_1$ -orbit in  $o$  is short as  $|o| \leq |O(G)| <$

$(q^2 - 1)/\mu^2 < q^3 < q_1$  by (22). Therefore  $o = \theta \cup \{P\}$ , and hence  $|o| = 1 + p^h$  for some  $h \geq 0$ . Since  $|o|$  divides  $|O(G)|$  this implies that  $|O(G)|$  is even, a contradiction. Thus  $\mathcal{X}$  has zero  $p$ -rank.

Finally,  $O(G) = Z(G)$  and  $O(G)$  is a cyclic prime to  $p$  group. We point out that this can be shown by the arguments used in the final part of the proof of Lemma 7.5. It is enough to deal with the case where  $\Phi$  induces a faithful action of  $\bar{L} \cong PSU(3, q)$  on  $O(G)$ . If  $\Lambda$  is a non-trivial orbit then  $|\Lambda| < |O(G)| < (q^2 - 1)/\mu^2$  by (22). On the other hand,  $|\Lambda|$  is at least as large as the index of the largest subgroup of  $PSU(3, q)$ , and, from Result 2.10,  $|\Lambda| \geq q^3 + 1$  for  $q \neq 5$  while  $|\Lambda| \geq 60$  for  $q = 5$ . In both cases, this gives a contradiction.  $\square$

Next we show that (22) is not heavily restrictive. Throughout this section, let  $\bar{\mathcal{X}} = \mathcal{X}/O(G)$ .

### 7.2.1 The case of ramified cover $\mathcal{X}|\bar{\mathcal{X}}$

**Lemma 7.7.** *If the cover  $\mathcal{X}|\bar{\mathcal{X}}$  ramifies then (22) holds.*

*Proof.* Take a ramification point  $\bar{P} \in \bar{\mathcal{X}}$ . As  $PSU(3, q)$  is non-solvable,  $\bar{G}$  does not fix  $\bar{P}$  by (iii) of Result 2.1. Let  $\bar{o}$  be the  $\bar{G}$ -orbit of  $\bar{P}$ . Note that  $q \neq 3$  by  $q \equiv 1 \pmod{4}$ . From Result 2.10, either  $|\bar{o}| \geq q^3 + 1$ , or  $|\bar{o}| \geq 60$  and  $q = 5$ . Assume  $q \neq 5$ . Then the cover  $\mathcal{X}|\bar{\mathcal{X}}$  has at least  $q^3 + 1$  ramification points with the same ramification index. If the  $O(G)$ -orbit lying over  $\bar{P}$  has length  $\ell$  then  $|O(G)| - \ell \geq \frac{2}{3}|O(G)|$ . Recall that  $g(\bar{\mathcal{X}}) > 2$ . Therefore, if  $q \neq 5$  then

$$2g(\mathcal{X}) - 2 > (q^3 + 1)(|O(G)| - \ell) \geq |O(G)|\frac{2}{3}(q^3 + 1), \quad (23)$$

whence

$$g(\mathcal{X}) > g(\bar{\mathcal{X}}) - 1 > \frac{4}{9}(q^3 + 1)|O(G)|.$$

This together with (18) give

$$900((q^3 + 1)|O(G)|\frac{4}{9})^2 < 900g(\mathcal{X})^2 < |O(G)|(q^3 + 1)(q^2 - 1)q^3$$

and hence (22) holds. Similarly, if  $q = 5$  we have

$$g(\mathcal{X}) > g(\bar{\mathcal{X}}) - 1 > 20|O(G)|,$$

and

$$900(20|O(G)|)^2 < 900g(\mathcal{X})^2 < |O(G)| \cdot |PGU(3, 5)|$$

gives (22) for  $q = 5$ .  $\square$

By Lemmas 7.6 and 7.7, Theorem 7.1 holds for ramified covers  $\mathcal{X}|\bar{\mathcal{X}}$ . We will show below that the unramified case cannot actually occur. Unfortunately, this case appears to be more involved and our proof requires deeper results from Group theory.

### 7.2.2 The case of unramified cover $\mathcal{X}|\bar{\mathcal{X}}$

It has already been noticed that  $\bar{\mathcal{X}}$  has zero  $p$ -rank and that  $g(\bar{\mathcal{X}}) > 2$ . Also, by Lemma 6.16 the genus of  $\bar{\mathcal{X}}$  is even.

**Lemma 7.8.** *If the cover  $\mathcal{X}|\bar{\mathcal{X}}$  is unramified then  $O(G)$  is not characteristically simple.*

*Proof.* Assume on the contrary that  $O(G)$  is characteristically simple. From Result 2.22  $O(G)$  is solvable. Hence  $O(G)$  is the direct product of  $r \geq 1$  cyclic groups of odd prime order  $v$ ; see [31, Kapitel I, Satz 9.12]. We show that  $v \neq p$ . Let  $\bar{Q}$  be a Sylow  $p$ -subgroup of  $\bar{G}$ . From (i) of Result 2.4, there is a point  $\bar{P} \in \bar{\mathcal{X}}$  which is fixed by  $\bar{Q}$ . Assume on the contrary that  $v = p$ . Then  $|O(G)| = p^r$ . Let  $Q$  be a Sylow  $p$ -subgroup of  $G$  containing  $O(G)$  such that  $\bar{Q} = Q/O(G)$ . Let  $o$  be the  $O(G)$ -orbit lying over  $\bar{P}$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ . Since  $|o| = p^r$ , for each  $P \in O$  the stabilizer of  $P$  in  $Q$  has order  $q^3 = |\bar{Q}|$ . On the other hand, no non-trivial element of  $Q$  fixes a point in  $\mathcal{X} \setminus o$ . In fact, if  $h \in Q$  fixes a point  $P'$  in  $\mathcal{X} \setminus o$ , then  $h \notin O(G)$  since  $\mathcal{X}|\bar{\mathcal{X}}$  is unramified. Let  $\bar{h}$  be the image of  $h$  under the homomorphism  $G \rightarrow \bar{G}$ . Then  $\bar{h}$  is not the trivial automorphism of  $\bar{\mathcal{X}}$ , and fixes two distinct points, namely  $\bar{P}$  and the point  $\bar{P}'$  lying under  $P'$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ . Since  $\bar{h}$  is a  $p$ -element, the  $p$ -rank of  $\bar{\mathcal{X}}$  is not zero by (i) of Result 2.4, a contradiction. Note that  $\bar{\mathcal{X}} = \mathcal{X}/O(G)$  is an unramified  $p$ -cover of  $\bar{\mathcal{X}}/Q$ , and hence the  $p$ -rank of  $\mathcal{X}/Q$  is zero. From the Deuring-Shafarevich formula applied to  $Q$ ,

$$\gamma(\mathcal{X}) - 1 = -|Q| + |O(G)|(q^3 - 1) = -p^r q^3 + p^r(q^3 - 1) = -p^r,$$

a contradiction. Thus,  $v \neq p$ .

Let  $\Phi$  denote the homomorphism from  $G$  to the automorphism group of  $O(G)$  arising from conjugacy. Since  $O(G)$  is abelian,  $\ker(\Phi)$  contains  $O(G)$ . Two cases are distinguished according to  $\ker(\Phi) = O(G)$  or  $\ker(\Phi)$  contains  $O(G)$  properly.

In the former case,  $\Phi$  gives rise to a faithful representation of  $\bar{G}$  by a matrix group of the vector space  $V = \mathbb{F}_v^r$ . As we have shown at the beginning of the proof, no non-trivial normal subgroup of  $G$  is contained in  $O(G)$ . Therefore,  $\Phi$  is irreducible. Let  $PG(r-1, v)$  be the projective space arising from  $V$ . Since  $\bar{L} \cong PSU(3, q)$  is simple,  $\bar{L}$  also has an irreducible, faithful representation as a projective group of  $PG(r-1, v)$ . Since  $v \neq p$ , this yields  $r-1 \geq q(q-1)$  by Result 2.23. Hence  $|O(G)| \geq v^{q(q-1)+1}$ . But this contradicts Lemma 6.22.

In the latter case,  $\ker(\Phi)/O(G)$  is a proper normal subgroup of  $\bar{G}$ . Since  $\bar{G} \cong PSU(3, q)$ , or  $\bar{G} \cong PGU(3, q)$ , this yields that  $\ker(\Phi)$  contains  $L$ , that is,  $O(G) \subseteq Z(L)$ ; actually  $O(G) = Z(L)$  holds since the center of  $\bar{L}$  is trivial. Two cases arise according to  $O(G) \leq G''$  or  $O(G) \not\leq G''$ .

If  $G''$  contains  $O(G)$ , then  $Z(G') = O(G)$  and  $G'/O(G) = \bar{L} \cong PSU(3, q)$ . Therefore,  $G'$  is a perfect central extension of  $PSU(3, q)$ . From Result 2.20,  $G' = SU(3, q)$ . In particular,  $|Z(G')| = 3$  whence  $|O(G)| = 3$ . This shows that (22) holds. From Lemma 7.6,  $\mathcal{X}$  has zero  $p$ -rank. As any  $p$ -subgroup of  $G$  is contained in  $G'$ , we have that a Sylow  $p$ -subgroup of  $G$ , say  $S_p$  is contained in  $G'$ . Since  $\mathcal{X}$  has zero  $p$ -rank,  $S_p$  fixes a point  $P$  in  $\mathcal{X}$  and no non-trivial element of  $S_p$  fixes another point; see Result 2.4. Each  $h \in O(G)$  commutes with every element in  $S_p$ , and hence fixes  $P$ , which contradicts the hypothesis that the cover  $\mathcal{X}|\bar{\mathcal{X}}$  is unramified.

If  $G''$  does not contain  $O(G)$  then they intersect trivially as  $O(G)$  contains no proper normal subgroup of  $G$ . Therefore,  $G'' \times O(G)$  is a normal subgroup of  $G$ . Since  $PSU(3, q) \leq G/O(G) \leq PGU(3, q)$  up to an isomorphism, this implies  $G'' \cong PSU(3, q)$ . In particular, any  $p$ -subgroup of  $G$  is contained in  $G''$ . Take a point  $\bar{P} \in \bar{\mathcal{X}}$ . Since  $\bar{\mathcal{X}}$  has zero  $p$ -rank, (i) of Result 2.4 yields that  $\bar{P}$  is fixed by a Sylow  $p$ -subgroup  $\bar{Q}$  of  $\bar{G}$ . The  $O(G)$ -orbit  $o$  lying over  $\bar{P}$  is left invariant by a subgroup  $Q$  of  $G$  such that  $Q/O(G) = \bar{Q}$ . Since  $|O(G)|$  is prime to  $|\bar{Q}| = q^3$ , Result 2.12 shows that  $Q = O(G) \rtimes R$  where  $|R| = |\bar{Q}|$  with  $R \leq G''$ , and that  $R$  fixes a point  $P \in o$ . Since  $O(G)$  is contained in the centralizer of  $G'$  in  $G$ , this yields that  $R$  fixes  $o$  pointwise. From the Deuring-Shafarevich formula applied to  $R$ ,

$$\gamma(\mathcal{X}) \geq -q^3 + |O(G)|(q^3 - 1) + 1 > \frac{1}{3}(q^3 + 1)|O(G)|. \quad (24)$$

This together with  $\mathfrak{g}(\mathcal{X}) \geq \gamma(\mathcal{X})$  yields (22). From Lemma 7.6,  $\gamma(\mathcal{X}) = 0$ , but this contradicts (24).

□

**Lemma 7.9.** *The cover  $\mathcal{X}|\bar{\mathcal{X}}$  is ramified.*

*Proof.* Assume that  $\mathcal{X}$  is a counter-example with minimal genus. Since by Lemma 7.8  $O(G)$  is not characteristically simple,  $G$  has a normal subgroup  $N$  properly contained in  $O(G)$ . Consider the quotient curve  $\tilde{\mathcal{X}} = \mathcal{X}/N$ . From  $N < O(G)$ , we have  $4 \leq \mathfrak{g}(\tilde{\mathcal{X}}) < \mathfrak{g}(\mathcal{X})$ . From the Hurwitz genus formula applied to  $N$ ,

$$\mathfrak{g}(\mathcal{X}) > \mathfrak{g}(\tilde{\mathcal{X}}) - 1 = |N|(\mathfrak{g}(\tilde{\mathcal{X}}) - 1) \geq \frac{4}{3}|N|\mathfrak{g}(\tilde{\mathcal{X}}).$$

Since  $\tilde{G} = G/N$  is a subgroup of  $\text{Aut}(\tilde{\mathcal{X}})$ , and  $|N| \geq 3$ ,

$$|\tilde{G}| > \frac{900 \cdot 16}{25}|N^2|\mathfrak{g}(\tilde{\mathcal{X}})^2 \geq \frac{146}{25} \cdot 900\mathfrak{g}(\tilde{\mathcal{X}})^2.$$

Note that  $\tilde{G}$  is a non-solvable group and that the quotient group  $O(G)/N$  is the largest normal subgroup  $O(\tilde{G})$  of  $\tilde{G}$  of odd order. Then  $\bar{\mathcal{X}} = \tilde{\mathcal{X}}/O(\tilde{G})$  and the cover  $\tilde{\mathcal{X}}|\bar{\mathcal{X}}$  is unramified. Therefore,  $\bar{\mathcal{X}}$  with respect to  $\tilde{G}$  satisfies Condition (B) in Proposition 6.21. As  $\mathcal{X}$  is assumed to be a counter-example with minimal genus, we obtain a contradiction. □

### 7.3 Proof of Theorem 7.1 in Case (C) in Proposition 6.21

We use the idea worked out in Section 7.1. Note that in this case the commutator subgroup  $\bar{G}'$  contains  $SL(2, q)$ . Let  $L$  be the subgroup of  $G$  such that  $\bar{L} = SL(2, q)$ .

**Lemma 7.10.** *In Case (C) of Proposition 6.21,  $\mathcal{X}$  has zero  $p$ -rank.*

*Proof.* As  $\bar{L} \cong SL(2, q)$  is a subgroup of  $\text{Aut}(\bar{\mathcal{X}})$ , Result 2.9 yields that  $\bar{\mathcal{X}}$  is not rational. Furthermore, since a Sylow 2-subgroup of  $SL(2, q)$  is not cyclic, Lemma 6.16 and Remark 6.3 yield that  $\bar{\mathcal{X}}$  is neither elliptic. Therefore,  $\mathfrak{g}(\bar{\mathcal{X}}) \geq 2$ . If equality holds then Result 2.5 applied to  $\mathfrak{g}(\bar{\mathcal{X}}) = 2$  yields  $\gamma(\bar{\mathcal{X}}) = 0$ , with just one exception, namely when  $p = 3$ , and a Sylow  $p$ -subgroup of  $\bar{L}$  has order 3. This exception does not actually occur here as  $q \geq 5$  in Case (C). Therefore,  $\bar{\mathcal{X}}$  has zero  $p$ -rank. We show that this holds true for  $\mathfrak{g}(\bar{\mathcal{X}}) > 2$ . From the Hurwitz genus formula applied to  $O(G)$ ,  $\mathfrak{g}(\mathcal{X}) - 1 \geq |O(G)|(\mathfrak{g}(\bar{\mathcal{X}}) - 1)$ . This and (18) give

$$|\bar{G}'||O(G)| > 900(\mathfrak{g}(\bar{\mathcal{X}}) - 1)^2|O(G)|^2 \geq 900\mathfrak{g}(\bar{\mathcal{X}})^2\frac{4}{9}|O(G)|^2 \geq 900\mathfrak{g}(\bar{\mathcal{X}})^2|O(G)|$$

whence  $|\bar{G}'| > 900\mathfrak{g}(\bar{\mathcal{X}})^2$ . From Lemma 6.19,  $\bar{\mathcal{X}}$  has zero  $p$ -rank.

Furthermore, since  $|\bar{G}'| \leq 2(q+1)q(q-1)$  and  $SL(2, q)$  has an abelian subgroup of order  $q+1$ ,

$$\frac{2(q-1)q}{|O(G)|(q+1)} \geq \frac{|G|}{(|O(G)|(q+1))^2} > 900 \left( \frac{\mathfrak{g}(\mathcal{X}) - 1}{|O(G)|(q+1)} \right)^2 \geq 900 \left( \frac{\mathfrak{g}(\bar{\mathcal{X}}) - 1}{4(\mathfrak{g}(\bar{\mathcal{X}}) + 1)} \right)^2 \geq \frac{900}{64} = \frac{225}{16}. \quad (25)$$

This yields

$$|O(G)| < \frac{32}{225}q. \quad (26)$$

Also,  $q \geq 23$  holds.

From (i) of Result 2.4, a Sylow  $p$ -subgroup  $\bar{Q}$  of  $\bar{L} \cong SL(2, q)$  fixes a unique point  $\bar{P} \in \bar{\mathcal{X}}$ . Here  $|\bar{Q}| = q$ , and the normalizer of  $\bar{Q}$  in  $\bar{L}$  is the semidirect product  $\bar{Q} \rtimes \bar{T}$  with a cyclic group  $\bar{T}$  of order  $q-1$ . Since this

normalizer is a maximal subgroup of  $\bar{L}$ , it is the stabilizer of  $\bar{P}$  in  $\bar{L}$  otherwise  $\bar{G}$  would fix  $\bar{P}$  contradicting (iii) of Result 2.1.

Let  $o$  be the  $O(G)$ -orbit lying over  $\bar{P}$  in the cover  $\mathcal{X}|\bar{\mathcal{X}}$ . The counter-image of  $\bar{Q} \rtimes \bar{T}$  in the homomorphism  $G \rightarrow \bar{G}$  is a subgroup  $N$  of order  $(q-1)q|O(G)|$  where  $N$  is the subgroup of  $G$  which preserves  $o$ . For a point  $P \in o$ , the stabilizer  $H$  of  $P$  in  $N$  has order  $(q-1)q|O(G)_P|$ . Therefore, the (unique) Sylow  $p$ -subgroup  $Q_1$  of  $H$  has order  $q_1 = qp^a$  and a complement of  $Q_1$  in  $H$  is a cyclic subgroup  $C_t$  of order  $t = (q-1)b$  with  $p \nmid b$ . Hence  $H = Q_1 \rtimes C_t$ , and  $|o|p^ab = |O(G)|$ . Now, (18) yields  $q(q-1)p^ab(q+1)|o| > 450\mathfrak{g}(\mathcal{X})^2$  whence

$$|H|^2 = (q_1t)^2 > \frac{(q-1)qp^ab}{(q+1)|o|} 450\mathfrak{g}^2 = \frac{1}{4}(p^ab)^2 \frac{2(q-1)q}{|O(G)|(q+1)} 900\mathfrak{g}(\mathcal{X})^2.$$

This together with (25) give

$$|H| = q_1t > 30\mathfrak{g}(\mathcal{X}).$$

From Lemma 4.1 and Remark 4.3, either  $\mathcal{X}$  has zero  $p$ -rank, or  $Q_1$  has just one short orbit  $\theta$  other than its fixed point  $P$ . Observe that  $\theta$  is contained in  $o$ . In fact, each  $Q_1$ -orbit in  $o$  is short as  $|o| \leq |O(G)| < q < q_1$  by (26). Therefore  $o = \theta \cup \{P\}$ , and hence  $|o| = 1 + p^h$  for some  $h \geq 0$ . Since  $|o|$  divides  $|O(G)|$  this implies that  $|O(G)|$  is even, a contradiction. Thus  $\mathcal{X}$  has zero  $p$ -rank.  $\square$

**Lemma 7.11.** *In Case (C) of Proposition 6.21,  $Z(G)$  is a cyclic prime to  $p$  group and contains  $O(G)$  as an index 2 subgroup.*

*Proof.* We adapt the arguments used in Section 7.1. For this purpose, let  $M$  be the normal subgroup of  $G$  containing  $O(G)$  such that  $M/O(G) = Z(G/O(G))$ . Since  $\bar{G} = G/O(G)$  is isomorphic to either  $SL(2, q)$ , or  $SL^{(2)}(2, q)$ , or  $SL^\pm(2, q)$ , or  $SU^\pm(2, q)$ , we have  $|Z(\bar{G})| = 2$ . Thus  $|M| = 2|O(G)|$ . Since  $\bar{L} \cong SL(2, q)$ , we have that  $\bar{L}$  contains  $Z(\bar{G})$ . Hence  $M \leq L$ , and  $\hat{L} = L/M \cong (L/O(G))/(M/O(G)) \cong PSL(2, q)$ . From Lemma 6.19 applied to  $\mathcal{X}/M$ , we have that  $\hat{G} = G/M$  is isomorphic to either  $PSL(2, q)$  or  $PGL(2, q)$  according to  $\hat{G} = \hat{L}$  or  $[\hat{G} : \hat{L}] = 2$ .

For every  $h \in G$  the map  $\varphi_h$  taking  $u \in M$  to  $h^{-1}uh$  is an automorphism of  $M$ . Thus the map  $\Phi : h \mapsto \varphi_h$  is a homomorphism from  $G$  into  $\text{Aut}(M)$ . Now, after replacing  $O(G)$  by  $M$  and Lemma 7.5 by Lemma 7.10, the analog argument used in the proof of Lemma 7.5 shows that  $M$  is a cyclic prime to  $p$  group. In particular,  $\ker(\Phi) \geq M$ . Since either  $\hat{G} = \hat{L}$ , or  $\hat{L}$  is the only non-trivial normal subgroup of  $\hat{G}$ , two cases arise namely  $\ker(\Phi) = M$  and  $\ker(\Phi) \geq L$ .

In the former case,  $\Phi$  induces a faithful action of  $\hat{L}$  on  $M$ . If  $\Lambda$  is a non-trivial orbit then  $|\Lambda| < 2|O(G)|$ , and hence  $|\Lambda| < q$  by (26). On the other hand,  $|\Lambda| \leq q+1$  by the analog argument in the proof of Lemma 7.5; a contradiction.

In the latter case,  $\ker(\Phi) \geq L$  and hence  $Z(L) = M$ . Let  $Q$  be a Sylow  $p$ -subgroup of  $G$ . Then  $Q \leq L$  as either  $G = L$  or  $[G : L] = 2$ . From Lemma 7.10 and (i) of Result 2.4,  $Q$  fixes a unique point  $P$ . Since  $Z(L) = M$ ,  $M$  fixes  $P$ . From Lemma 7.10 and (ii) of Result 2.4,  $G_P$  coincides with the normalizer  $N_G(Q)$  of  $Q$  in  $G$ . From Result 2.12, a complement  $C$  of  $Q$  contains  $M$ . If  $L \not\leq G$  then  $C$  contains an element of  $G \setminus L$ . Therefore, some element in  $G \setminus L$  centralizes  $O(G)$ . This shows that  $Z(G) = M$ .  $\square$

## 8 Proof of Theorem 1.2

From Theorem 7.1,  $\gamma(\mathcal{X}) = 0$ . If  $O(G) = \{1\}$ , Theorem 1.2 is a corollary of Lemma 6.19, taking into account that for the groups  $G$  listed in Lemma 6.19  $p(G)$  is  $PGL(2, q)$ ,  $PSL(2, q)$  or  $SL(2, q)$ .

Therefore,  $O(G)$  is assumed to be non-trivial. From (i) of Result 2.4, each Sylow  $p$ -subgroup fixes a point of  $\mathcal{X}$ . Therefore, the set  $\Omega$  consisting of the fixed points of the Sylow  $p$ -subgroups of  $G$  is non-empty. There is a bijection between  $\Omega$  and the set of all Sylow  $p$ -subgroups of  $G$ . Since the Sylow  $p$ -subgroups of  $G$  are pairwise conjugate in  $G$ ,  $\Omega$  is a  $G$ -orbit. Therefore,  $G$  has a transitive permutation representation  $\Phi$  on  $\Omega$ . Let  $\tilde{G} = G/\ker(\Phi)$ . Then  $Z(G) \leq \ker(\Phi)$  as  $Z(G)$  fixes  $\Omega$  pointwise. Also, from Theorem 7.1,  $Z(G)$  is a prime to  $p$  subgroup, and hence Sylow  $p$ -subgroups of  $G$  are isomorphic to those of  $G/Z(G)$ . Note that  $\ker(\Phi)$  is a proper subgroup of  $G$  as otherwise  $G$  would have just one Sylow  $p$ -subgroup.

If Case (A) or Case (B) in Proposition 6.21 holds, then  $\tilde{G} = G/O(G)$  has trivial center and  $Z(G) = O(G)$  by Theorem 7.1. Therefore,  $Z(G) = \ker \Phi$  since  $\ker(\Phi)/O(G)$  is a normal subgroup of  $\tilde{G}$ . Then  $\tilde{G} = \tilde{G}$  acts (by conjugation) on  $\Omega$  faithfully in the same way as either  $PSL(2, q)$ , or  $PGL(2, q)$ , or  $PSU(3, q)$ , or  $PGU(3, q)$ , on the set of their Sylow  $p$ -subgroups, that is, in their usual doubly transitive permutation representation. In particular,  $q = |\Omega| - 1$  for  $PSL(2, q)$  and  $PGL(2, q)$  while  $q^3 = |\Omega| - 1$  for  $PSU(3, q)$  and  $PGU(3, q)$ .

If case (C) in Proposition 6.21 occurs, then either  $G/Z(G) \cong PSL(2, q)$ , or  $G/Z(G) \cong PGL(2, q)$ , and  $[Z(G) : O(G)] = 2$  by Theorem 7.1. In the former case,  $G/Z(G)$  is simple, in the latter one  $G/Z(G)$  has a unique proper normal subgroup, and this subgroup is isomorphic to  $PSL(2, q)$ . Therefore,  $\ker(\Phi) = Z(G)$ , and  $\tilde{G}$  acts on  $\Omega$  faithfully as either  $PSL(2, q)$ , or  $PGL(2, q)$ , on the set of their Sylow  $p$ -subgroups, that is, in their usual doubly transitive permutation representation.

Let  $S_p$  be a Sylow  $p$ -subgroup of  $G$ , and look at the action of  $S_p$  on  $\Omega$ . Obviously  $S_p$  fixes the point  $P \in \Omega$  represented by  $S_p$  itself. From (i) of Result 2.4, no non-trivial element of  $S_p$  fixes another point, that is,  $S_p$  acts semiregularly on the points of  $\Omega$  other than  $P$ . Actually,  $S_p$  is regular on  $\Omega \setminus \{P\}$ , as  $|S_p| = |\Omega| - 1$ . Furthermore, from (i) of Result 2.1,  $S_p$  is a normal subgroup of the stabilizer  $G_P$  of  $P$  in  $G$ .

Therefore, the pair  $(\Omega, G)$  is a group space satisfying the hypothesis of Result 2.24 where the normal closure  $S$  of  $Q$  is the subgroup  $p(G)$  of  $G$  generated by all Sylow  $p$ -subgroups of  $G$ . In Result 2.24, there are several possibilities for  $S$  and hence for our  $p(G)$ , but those consistent with Proposition 6.21 are only four, namely  $PSL(2, q)$ ,  $SL(2, q)$ ,  $PSU(3, q)$  with  $q \equiv 1 \pmod{4}$  and  $SU(3, q)$  with  $q \equiv 5 \pmod{12}$ . This completes the proof of Theorem 1.2.

## 9 Examples for Theorem 1.2

In Remark 6.20 we have already pointed out that Hermitian curves and Roquette curves provide example for the cases  $p(G) = PSU(3, q)$ ,  $PSL(2, q)$ ,  $SL(2, q)$ .

We show that the GK curves [12] have quotient curves that provide more examples for Theorem 1.2.

Let  $q$  be a power of  $p$  such that  $q \equiv 1 \pmod{4}$ .

From [12], the GK curve  $\mathcal{Z}$  has genus  $\mathfrak{g}(\mathcal{Z}) = \frac{1}{2}(q^3 + 1)(q^2 - 2) + 1$  which is even for  $q \equiv 1 \pmod{4}$ , and  $\text{Aut}(\mathcal{Z})$  has order  $(q^3 + 1)q^3(q^2 - 1)(q^2 - q + 1)$ . More precisely,  $\text{Aut}(\mathcal{Z}) \cong PSU(3, q) \times C_{q^2 - q + 1}$  for  $q \not\equiv -1 \pmod{3}$  while  $\text{Aut}(\mathcal{Z})$  has an index 3 subgroup  $G \cong SU(3, q) \times C_{(q^2 - q + 1)/3}$  for  $q \equiv -1 \pmod{3}$ ; see [12]. In particular,  $|\text{Aut}(\mathcal{Z})| \approx 8\mathfrak{g}(\mathcal{X})^2$ . Furthermore,  $\text{Aut}(\mathcal{Z})$  has exactly two short orbits. One of them has size  $q^3 + 1$  and the kernel of the permutation representation of  $\text{Aut}(\mathcal{Z})$  on it is the cyclic subgroup  $C_{q^2 - q + 1}$  of  $\text{Aut}(\mathcal{Z})$  while no non-trivial element of  $C_{q^2 - q + 1}$  fixes a point in the other short orbit. The quotient curves of  $\mathcal{Z}$  have been under investigations; see [10, 17]. Here we limit ourselves to a special case, also discussed in [12].

For a divisor  $u$  of  $q^2 - q + 1$ , the group  $C_{q^2 - q + 1}$  contains a subgroup  $C_u$  of order  $u$ . Let  $\mathcal{X}_u = \mathcal{Z}/C_u$  be the quotient curve of  $\mathcal{X}$  with respect to  $C_u$ . Since  $C_u$  is tame, the Hurwitz genus formula gives

$$(q^3 + 1)(q^2 - 2) = 2\mathfrak{g}(\mathcal{Y}) - 2 = u(2\mathfrak{g}(\mathcal{X}_d) - 2) + (d - 1)(q^3 + 1),$$

whence

$$\mathfrak{g}(\mathcal{X}_d) = \frac{1}{2} \left( \frac{(q^3 + 1)(q^2 - u - 1)}{u} + 2 \right).$$

In particular,  $\mathfrak{g}(\mathcal{X}_u)$  is even. Furthermore, since  $C_u$  is a normal subgroup of  $\text{Aut}(\mathcal{X})$ ,  $\text{Aut}(\mathcal{X})/C_u$  is a subgroup  $G_u$  of  $\text{Aut}(\mathcal{X}_u)$  such that

$$|G_u| = \frac{q^3(q^3 + 1)(q^2 - 1)(q^2 - q + 1)}{u}.$$

Comparison  $|G_u|$  with  $\mathfrak{g}(\mathcal{X}_d)$  shows that if  $u \geq 450$  then  $|\text{Aut}(\mathcal{X}_u)| \geq |G_u| > 900\mathfrak{g}(\mathcal{X}_u)^2$ .

If  $q \not\equiv -1 \pmod{3}$  then both  $(PSU(3, q) \times C_u)/C_u \cong PSU(3, q)$  and  $C_{q^2-q+1}/C_u \cong C_{(q^2-q+1)/u}$  are subgroups of  $G_u$ , and their intersection is trivial. Therefore, they generate a group isomorphic to  $PSU(3, q) \times C_{(q^2-q+1)/u}$  whose order is equal to that of  $G_u$ . Thus  $G_d \cong PSU(3, q) \times C_{(q^2-q+1)/u}$ . This gives an example, not isomorphic to the Hermitian curve, for the case  $p(G) \cong PSU(3, q)$  with  $q \equiv 1 \pmod{3}$  in Theorem 1.2.

If  $q \equiv -1 \pmod{3}$ , take the index 3 subgroup  $G \cong SU(3, q) \times C_{(q^2-q+1)/3}$  together with a subgroup  $C_u$  of  $C_{(q^2-q+1)/3}$ . Then  $u$  is not divisible by 3 and we may replace  $G_u = \text{Aut}(\mathcal{X})/C_u$  with  $G/C_u$  in the above argument. This time we obtain  $G/C_u \cong SU(3, q) \times C_{(q^2-q+1)/3u}$  which gives an example for the case  $p(G) \cong SU(3, q)$  with  $q \equiv -1 \pmod{3}$  in Theorem 1.2.

## Acknowledgments

The research was partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM). M. Giulietti was supported by *Università degli Studi di Perugia - Fondo ricerca di base Esercizio 2015 - Project: Geometrie di Galois, Curve Algebriche su campi finiti e loro Applicazioni*.

## References

- [1] S. Abhyankar, Coverings of algebraic curves, *Amer. J. Math.*, **79** (1957), 825-856.
- [2] A. Adler, The Mathieu group  $M(11)$  and the modular curve  $X(11)$ , *Proc. London Math. Soc.* **74** (1997), 1-28.
- [3] L. Alperin, R. Brauer and D. Gorenstein, Finite simple groups of 2-rank two, *Scripta Math.* **29** (1973), 191-214.
- [4] J.L. Alperin, R. Brauer and D. Gorenstein, Finite groups with quasi-dihedral and wreathed Sylow 2-subgroups, *Trans. Amer. Math. Soc.* **151** (1970), 1-261.
- [5] N. Arakelian and G. Korchmáros, A characterization of the Artin-Mumford curve, *J. Number Theory* **154** (2015), 278-291.
- [6] F.M. Bleher, T. Chinburg, B. Poonen and P. Symonds, Automorphisms of Harbater-Katz-Gabber curves, ArXiv:1509.02139.
- [7] I.I. Bouw, The  $p$ -rank of ramified covers, *Compositio Math.* **126** (2001), 209–322.

- [8] R. Brauer and M. Suzuki, On finite groups of even order whose 2-Sylow group is a quaternion group, *Proceedings of the National Academy of Sciences of the United States of America* **45** (1959), 1757-1759.
- [9] G. Cornelissen, F. Kato and A. Kontogeorgis, Discontinuous groups in positive characteristic and automorphisms of Mumford curves, *Math. Ann.* **320** (2001), 55-85.
- [10] S. Fanali and M. Giulietti, Quotient curves of the GK curve, *Adv. Geom.* **12** (2012), 239-268.
- [11] W. Feit and J.G. Thompson, Solvability of groups of odd order, *Pac. Jour. Math.* **13** (1963), 775-1029.
- [12] M. Giulietti and G. Korchmáros, A new family of maximal curves, *Math. Ann.* (2009) **343**, 229-245.
- [13] M. Giulietti and G. Korchmáros, Large 2-groups of automorphisms of curves with positive 2-rank, *J. Algebra*, **427** (2015), 264-294.
- [14] M. Giulietti and G. Korchmáros, Algebraic curves with a large non-tame automorphism group fixing no point, *Trans. Amer. Math. Soc.* **362** (2010), 5983–6001.
- [15] M. Giulietti and G. Korchmáros, Automorphism groups of algebraic curves with  $p$ -rank zero, *J. London Math. Soc.*, (2) **81** (2010) 277-296.
- [16] M. Giulietti and G. Korchmáros, Large  $p$ -groups of automorphisms of algebraic curves in characteristic  $p$ , *J. Algebra* **481** (2017), 215-249.
- [17] M. Giulietti, L. Quoos, Luciane and G. Zini, Maximal curves from subcovers of the GK-curve, *J. Pure Appl. Algebra* **220** (2016), 3372-3383.
- [18] D. Gorenstein and K. Harada, *Finite Groups Whose 2-Subgroups Are Generated by at Most 4 Elements*, Memoirs of the American Mathematical Society, No. **147**, American Mathematical Society, Providence, R.I., 1974. vii+464 pp.
- [19] D. Gorenstein, *Finite groups*, Second edition. Chelsea Publishing Co., New York, 1980. xvii+519 pp. ISBN: 0-8284-0301-5 20-02 (20Dxx).
- [20] D. Gorenstein and J.H. Walter, The characterization of finite groups with dihedral Sylow 2-subgroups. I. *J. Algebra* **2** (1965), 85-151.
- [21] D. Gorenstein and J.H. Walter, The characterization of finite groups with dihedral Sylow 2-subgroups. II. *J. Algebra* **2** (1965), 218-270.
- [22] R. Gow, Some  $TI$  subgroups of solvable groups, *J. London Math. Soc.* **12** (1976), 285–286.
- [23] R. L. Griess, Jr., Schur multipliers of finite simple groups of Lie type, *Trans. Amer. Math. Soc.*, **183** (1973), 355–421.
- [24] J.P. Hansen and J.P. Pedersen, Automorphism group of Ree type, Deligne-Lusztig curves and function fields, *J. Reine Angew. Math.* **440** (1993), 99–109.
- [25] D. Harbater, Abhyankar’s conjecture on Galois groups over curves, *Invent. Math.*, **117** (1994), 1-25.
- [26] D. Harbater, A. Obus, R. Pries, and K. Stevenson, Abhyankar’s conjectures in galois theory: current status and future directions, arXiv:1408.0859 [math.AG].

- [27] M. Hall, Jr. *The theory of groups*, The Macmillan Co., New York, N.Y. 1959 xiii+434 pp.
- [28] H.W. Henn, Funktionenkörper mit großer Automorphismengruppe, *J. Reine Angew. Math.* **302** (1978), 96–115.
- [29] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves Over a Finite Field*, Princeton Univ. Press, Princeton and Oxford, 2008, xx+696 pp.
- [30] C. Hering, A theorem on group space, *Hokkaido Math. J.* **8** (1979), 115–120.
- [31] B. Huppert, *Endliche Gruppen. I*, Grundlehren der Mathematischen Wissenschaften **134**, Springer, Berlin, 1967, xii+793 pp.
- [32] G. Korchmáros and M. Montanucci, The geometry of the Artin-Schreier-Mumford curves over an algebraically closed field, *Acta Sci. Math. (Szeged)* **83** (2017), 673–681.
- [33] V. Landázuri and G.M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, *J. Algebra* **32** (1974), 418–443.
- [34] L.M. Isaacs, *Character theory of finite groups*, Corrected reprint of the 1976 original [Academic Press, New York; MR0460423]. Dover Publications, Inc., New York, 1994. xii+303 pp.
- [35] H.H. Mitchell, Determination of the ordinary and modular ternary linear groups. *Trans. Amer. Math. Soc.* **12** (1911), 207–242.
- [36] S. Nakajima,  $p$ -ranks and automorphism groups of algebraic curves, *Trans. Amer. Math. Soc.* **303** (1987), 595–607.
- [37] M.E. O’Nan, On unitary collineation group, *J. Algebra* **22** (1972), 211–218.
- [38] R.J. Pries, Wildly ramified covers with large genus *J. Number Theory* **119** (2006), 194–209.
- [39] R. Pries and K. Stevenson, A survey of Galois theory of curves in characteristic  $p$ , WIN–women in numbers, 169–191, Fields Inst. Commun., **60**, Amer. Math. Soc., Providence, RI, 2011.
- [40] C.S. Rajan, Automorphisms of  $X(11)$  over characteristic 3 and the Mathieu group  $M(11)$ , *Ramanujan Math. Soc.* **13**, (1998), 63–72
- [41] P. Roquette, Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik, *Math. Z.* **117** (1970), 157–163.
- [42] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe, *Arch. Math.* **24** (1973), 527–544.
- [43] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics **67**, Springer, New York, 1979. viii+241 pp.
- [44] I.R. Shafarevich, On  $p$ -extensions, *Amer. Math. Soc. Transl.* **4** (1954), 59–71.
- [45] T. Shaska and H. Völklein, Elliptic subfields and automorphisms of genus 2 function fields, in *Algebra, arithmetic and geometry with applications* (West Lafayette, IN, 2000), 703–723, Springer, Berlin, 2004.

- [46] F. Sullivan,  $p$ -torsion in the class group of curves with many automorphisms, *Arch. Math.* **26** (1975), 253–261.
- [47] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern, *Arch. Math.* **24** (1973), 615–631.
- [48] J.G. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.* **74** (1968), 383–437.
- [49] R.C. Valentini and M.L. Madan, A Hauptsatz of L.E. Dickson and Artin–Schreier extensions, *J. Reine Angew. Math.* **318** (1980), 156–177.
- [50] J.H. Walter, The characterization of finite groups with abelian Sylow 2-subgroups, *Ann. of Math.* **89** (1969), 405–514.
- [51] R.A. Wilson, *The finite simple groups*, Graduate Texts in Mathematics, **251**, Springer-Verlag London, Ltd., London, 2009. xvi+298 pp.
- [52] W.J. Wong, On finite groups with semi-dihedral Sylow 2-subgroups. *J. Algebra* **4** (1966), 52–63.
- [53] W.J. Wong, On finite groups whose 2-sylow subgroups have cyclic subgroups of index 2, *J. Austral. Math. Soc.* **4** (1964), 90–112.

*Authors' addresses:*

Massimo GIULIETTI  
 Dipartimento di Matematica e Informatica  
 Università degli Studi di Perugia  
 Via Vanvitelli, 1  
 06123 Perugia (Italy).  
 E-mail: `massimo.giulietti@unipg.it`

Gábor KORCHMÁROS  
 Dipartimento di Matematica  
 Università della Basilicata  
 Contrada Macchia Romana  
 85100 Potenza (Italy).  
 E-mail: `gabor.korchmaros@unibas.it`