Algebra & Number Theory

Volume 13
2019
No. 1

Ordinary algebraic curves with many automorphisms in positive characteristic

Gábor Korchmáros and Maria Montanucci

msp

ALGEBRA AND NUMBER THEORY 13:1 (2019)
dx.doi.org/10.2140/ant.2019.13.1

Ordinary algebraic curves with many automorphisms in positive characteristic

Gábor Korchmáros and Maria Montanucci

Let $\mathscr{X}$ be an ordinary (projective, geometrically irreducible, nonsingular) algebraic curve of genus $\mathfrak{g}(\mathscr{X}) \ge 2$ defined over an algebraically closed field $\mathbb{K}$ of odd characteristic p. Let $\mathrm{Aut}(\mathscr{X})$ be the group of all automorphisms of $\mathscr{X}$ which fix $\mathbb{K}$ elementwise. For any solvable subgroup G of $\mathrm{Aut}(\mathscr{X})$ we prove that $|G| \le 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$. There are known curves attaining this bound up to the constant 34. For p odd, our result improves the classical Nakajima bound $|G| \le 84(\mathfrak{g}(\mathscr{X})-1)\mathfrak{g}(\mathscr{X})$ and, for solvable groups G, the Gunby–Smith–Yuan bound $|G| \le 6(\mathfrak{g}(\mathscr{X})^2 + 12\sqrt{21}\,\mathfrak{g}(\mathscr{X})^{3/2})$ where $\mathfrak{g}(\mathscr{X}) > cp^2$ for some positive constant c.

1. Introduction

In this paper, $\mathscr{X}$ stands for a (projective, geometrically irreducible, nonsingular) algebraic curve of genus $\mathfrak{g}(\mathscr{X}) \ge 2$ defined over an algebraically closed field $\mathbb{K}$ of odd characteristic p. Let $\mathrm{Aut}(\mathscr{X})$ be the group of all automorphisms of $\mathscr{X}$ which fix $\mathbb{K}$ elementwise. The assumption $\mathfrak{g}(\mathscr{X}) \ge 2$ ensures that $\mathrm{Aut}(\mathscr{X})$ is finite. However, the classical Hurwitz bound $|\mathrm{Aut}(\mathscr{X})| \le 84(\mathfrak{g}(\mathscr{X})-1)$ for complex curves fails in positive characteristic, and there exist four families of curves satisfying $|\mathrm{Aut}(\mathscr{X})| \ge 8\mathfrak{g}^3(\mathscr{X})$ [Stichtenoth 1973; Henn 1978; Hirschfeld et al. 2008, §11.12]. Each of them has p-rank $\gamma(\mathscr{X})$ (equivalently, its Hasse–Witt invariant) equal to zero; see for instance [Giulietti and Korchmáros 2014]. On the other hand, if $\mathscr{X}$ is ordinary, i.e., $\mathfrak{g}(\mathscr{X}) = \gamma(\mathscr{X})$, Guralnick and Zieve announced in 2004, as reported in [Gunby et al. 2015; Kontogeorgis and Rotger 2008], that for odd p there exists a sharper bound, namely $|\mathrm{Aut}(\mathscr{X})| \le c_p\mathfrak{g}(\mathscr{X})^{8/5}$ with some constant c_p depending on p. It should be noticed that no proof of this sharper bound is available in the literature. In this paper, we concern ourselves with solvable automorphism groups G of an ordinary curve $\mathscr{X}$, and for odd p we prove the even sharper bound:

Theorem 1.1. *Let $\mathscr{X}$ be an algebraic curve of genus $\mathfrak{g}(\mathscr{X}) \ge 2$ defined over an algebraically closed field $\mathbb{K}$ of odd characteristic p. If $\mathscr{X}$ is ordinary and G is a solvable subgroup of* $\mathrm{Aut}(\mathscr{X})$, *then*

$$|G| \le 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}. \tag{1}$$

For odd p, our result provides an improvement on the classical Nakajima bound $|G| \le 84(\mathfrak{g}(\mathscr{X})-1)\mathfrak{g}(\mathscr{X})$ [1987] and, for solvable groups, on the recent Gunby–Smith–Yuan bound $|G| \le 6(\mathfrak{g}(\mathscr{X})^2+12\sqrt{21}\,\mathfrak{g}(\mathscr{X})^{3/2})$ proven in [Gunby et al. 2015] under the hypothesis that $\mathfrak{g}(\mathscr{X}) > cp^2$ for some positive constant c.

MSC2010: primary 14H37; secondary 14H05.
Keywords: algebraic curves, algebraic function fields, positive characteristic, automorphism groups.

The following example is due to Stichtenoth, and it shows that (1) is the best possible bound apart from the constant c [Korchmáros et al. 2018]. Let $\mathbb{F}_q$ be a finite field of order $q=p^h$, and let $\mathbb{K}=\overline{\mathbb{F}_q}$ denote its algebraic closure. For a positive integer m prime to p, let $\mathscr{Y}$ be the irreducible curve with affine equation

$$y^q+y=x^m+\frac{1}{x^m} \tag{2}$$

and $F=\mathbb{K}(\mathscr{Y})$ its function field. Let $t=x^{m(q-1)}$. The extension $F|\mathbb{K}(t)$ is a non-Galois extension as the Galois closure of F with respect to H is the function field $\mathbb{K}(x,y,z)$ where x,y,z are linked by (2) and $z^q+z=x^m$. Furthermore, $\mathfrak{g}(\mathscr{Y})=(q-1)(qm-1)$, $\gamma(\mathscr{Y})=(q-1)^2$, and $\mathrm{Aut}(\mathscr{Y})$ contains a subgroup $Q\rtimes U$ of index 2 where Q is an elementary abelian normal subgroup of order q^2 and the complement U is a cyclic group of order $m(q-1)$. If $m=1$, then $\mathscr{Y}$ is an ordinary curve, and in this case $2\mathfrak{g}(\mathscr{Y})^{3/2}=2(q-1)^3<2q^2(q-1)=|\mathrm{Aut}(\mathscr{X})|$, which shows indeed that (1) is sharp up to the constant c.

Lower bounds on the order of solvable automorphism groups of algebraic curves depending on their genera are due to Neftin and Zieve. Their [2015, Theorem 4.1] states that for every integer $\ell>0$ there exists a curve $\mathscr{X}$ together with a solvable subgroup of $\mathrm{Aut}(\mathscr{X})$ of order d and derived length ℓ such that

$$\mathfrak{g}(\mathscr{X})\le c_\ell d\log^{o\ell}(d),$$

where c_ℓ is a constant and $\log^{o\ell}$ denotes log iterated ℓ times. The curve $\mathscr{X}$ is constructed as a solvable cover of a curve with at least one rational point, in which a given set S of rational points splits completely.

2. Background and preliminary results

For a subgroup G of $\mathrm{Aut}(\mathscr{X})$, let $\overline{\mathscr{X}}$ denote a nonsingular model of $\mathbb{K}(\mathscr{X})^G$, that is, a (projective, nonsingular, geometrically irreducible) algebraic curve with function field $\mathbb{K}(\mathscr{X})^G$, where $\mathbb{K}(\mathscr{X})^G$ consists of all elements of $\mathbb{K}(\mathscr{X})$ fixed by every element in G. Usually, $\overline{\mathscr{X}}$ is called the quotient curve of $\mathscr{X}$ by G and denoted by $\mathscr{X}/G$. The field extension $\mathbb{K}(\mathscr{X})|\mathbb{K}(\mathscr{X})^G$ 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 Φ be the cover of $\mathscr{X}|\overline{\mathscr{X}}$ where $\overline{\mathscr{X}}=\mathscr{X}/G$. A point $P\in\mathscr{X}$ is a ramification point of G if the stabilizer G_P of P in G is nontrivial; the ramification index e_P is $|G_P|$; a point $\overline{Q}\in\overline{\mathscr{X}}$ is a branch point of G if there is a ramification point $P\in\mathscr{X}$ such that $\Phi(P)=\overline{Q}$; the ramification (branch) locus of G is the set of all ramification (branch) points. The G-orbit of $P\in\mathscr{X}$ is the subset $o=\{R\mid R=g(P),\ g\in G\}$ of $\mathscr{X}$, and it is *long* if $|o|=|G|$; otherwise o is *short*. For a point $\overline{Q}$, the G-orbit o lying over $\overline{Q}$ consists of all points $P\in\mathscr{X}$ such that $\Phi(P)=\overline{Q}$. If $P\in o$, then $|o|=|G|/|G_P|$ and hence $\overline{Q}$ 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 nontrivial element in G is fixed-point-free on $\mathscr{X}$, that is, the cover Φ is unramified. On the other hand, G has a finite number of short orbits. For a nonnegative integer i, the i-th ramification group of $\mathscr{X}$ at P is denoted by $G_P^{(i)}$ (or $G_i(P)$ as in [Serre 1979, Chapter IV]) and defined to be

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

where t is a uniformizing element (local parameter) at P. Here $G_P^{(0)}=G_P$.

Let $\bar{\mathfrak{g}}$ be the genus of the quotient curve $\overline{\mathcal{X}} = \mathcal{X}/G$. The Riemann–Hurwitz genus formula gives

$$2\mathfrak{g} - 2 = |G|(2\bar{\mathfrak{g}} - 2) + \sum_{P\in\mathcal{X}} d_P, \tag{3}$$

where the different d_P at P is given by

$$d_P = \sum_{i\geq 0}(|G_P^{(i)}| - 1). \tag{4}$$

If $|G_P|$ is prime to p, then $d_P = |G_P| - 1$.

Let γ be the p-rank of $\mathcal{X}$, and let $\bar{\gamma}$ be the p-rank of the quotient curve $\overline{\mathcal{X}} = \mathcal{X}/G$. The Deuring–Shafarevich formula (see [Sullivan 1975] or [Hirschfeld et al. 2008, Theorem 11.62]) states that if G is a p-group then

$$\gamma - 1 = |G|(\bar{\gamma} - 1) + \sum_{i=1}^{k}(|G| - \ell_i) \tag{5}$$

where $\ell_1, \ldots, \ell_k$ are the sizes of the short orbits of G. If $\mathcal{X}$ is ordinary (and hence $G_P^{(2)}$ is trivial for every $P \in \mathcal{X}$; see Result 2.5(i)), then $d_P = |G_P^{(0)}| - 1 + |G_P^{(1)}| - 1 = 2(|G_P^{(0)}| - 1) = 2(|G_P| - 1)$ and hence (5) follows from (3) and vice versa.

The Nakajima bound (see [1987, Theorem 1] or [Hirschfeld et al. 2008, Theorem 11.84]) states that the existence of large p-groups of automorphisms implies that $\gamma = 0$.

Result 2.1. *If $\mathcal{X}$ has positive p-rank γ, then every p-subgroup of* $\mathrm{Aut}(\mathcal{X})$ *has order* $\leq p(\gamma - 1)/(p - 2)$.

A subgroup of $\mathrm{Aut}(\mathcal{X})$ is a prime to p group (or a p'-subgroup) if its order is prime to p. A subgroup G of $\mathrm{Aut}(\mathcal{X})$ is *tame* if the 1-point stabilizer of any point in G is p'-group. Otherwise, G is *nontame* (or *wild*). Obviously, every p'-subgroup of $\mathrm{Aut}(\mathcal{X})$ is tame, but the converse is not always true.

Result 2.2. *The following claims hold.*

(i) *If $|G| > 84(\mathfrak{g}(\mathcal{X}) - 1)$, then G is nontame.*

(ii) *If G is abelian, then $|G| \leq 4\mathfrak{g} + 4$.*

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

The first two claims are due to Stichtenoth [1973]; see also [Hirschfeld et al. 2008, Theorems 11.56 and 11.79]. For a proof of claim (iii), see [Homma 1980] or [Hirschfeld et al. 2008, Theorem 11.108].

Henn's bound [1978] (see also [Hirschfeld et al. 2008, Theorem 11.127]) has the following corollary.

Result 2.3. *If $|G| > 8\mathfrak{g}^3$, then $\mathcal{X}$ has zero p-rank, and G is not solvable.*

An orbit o of G is *tame* if G_P is a p'-group for $P \in o$. The structure of G_P is well known; see for instance [Serre 1979, Chapter IV, Corollary 4] or [Hirschfeld et al. 2008, Theorem 11.49].

Result 2.4. *The stabilizer G_P of a point $P \in \mathcal{X}$ in G is a semidirect product $G_P = Q_P \rtimes U$ where the normal subgroup Q_P is a p-group while the complement U is a cyclic prime to p group.*

If $\mathcal{X}$ is ordinary, some more results are available; those used in this paper are collected below.

Result 2.5. *If $\mathcal{X}$ is an ordinary curve, then*

(i) $Q_P^{(2)}$ *is trivial,*

(ii) Q_P *is elementary abelian,*

(iii) *no nontrivial element of U commutes with a nontrivial element of Q_P,*

(iv) $|U|$ *divides* $|Q_P|-1$, *and*

(v) *the quotient curve $\mathcal{X}/G$ for a p-group G of automorphisms is also ordinary.*

Claim (i) is due to Nakajima [1987, Theorem 2.1]. Claim (ii) follows from claim (i) by Serre's result [1979, Corollary 3, p. 67] stating that the factor groups $Q_P^{(i)}/Q_P^{(i+1)}$ for $i \geq 1$ are elementary abelian; see also [Hirschfeld et al. 2008, Theorem 11.74]. Claim (iii) follows from claim (ii) by Serre's result [1979, Corollary 1, p. 69]; see also [Hirschfeld et al. 2008, Theorem 11.75(ii)]. Claim (iv) is a consequence of claim (iii) since the latter claim together with Result 2.4 imply that U induces an automorphism group of Q_P. Claim (v) follows from comparison of (3) to (5) taking into account claim (i).

For a nontrivial p-subgroup G of $\mathrm{Aut}(\mathcal{X})$, divide both sides in (3) by 2 and then subtract the result from (5). If $G_P^{(2)}$ is trivial for every $P \in \mathcal{X}$, then this computation gives

$$\mathfrak{g}(\mathcal{X}) - \gamma(\mathcal{X}) = |G|(\mathfrak{g}(\bar{\mathcal{X}}) - \gamma(\bar{\mathcal{X}})) \tag{6}$$

where $\bar{\mathcal{X}} = \mathcal{X}/Q$ [Nakajima 1987]. This shows the first two claims of the following result hold. The third one is due to Stichtenoth [1973]; see also [Hirschfeld et al. 2008, Theorem 11.79].

Result 2.6. *Let Q be nontrivial p-subgroup of* $\mathrm{Aut}(\mathcal{X})$. *Assume that $Q_P^{(2)}$ is trivial for every $P \in \mathcal{X}$. Then*

(i) (6) *holds,*

(ii) *$\mathcal{X}$ and its quotient curve $\mathcal{X}/Q$ are simultaneously ordinary or not, and*

(iii) $|Q_P| \leq p\mathfrak{g}(\mathcal{X})/(p-1)$.

The first two claims below on low-genus curves are well known; see for instance [Hirschfeld et al. 2008, Theorems 11.94 and 11.99]. The third one is a corollary of Henn's bound.

Result 2.7. *If G is an automorphism group of an elliptic curve $\mathscr{E}$ over $\mathbb{K}$, then for every point $P \in \mathscr{E}$ the order of the stabilizer G_P of P in G divides* 6 *when* $p > 3$ *and* 12 *when* $p = 3$. *The solvable automorphism groups of a genus-*2 *curve over $\mathbb{K}$ have order at most* 48. *For genus-*3 *curves the latter bound is* 216.

We also need a technical result.

Result 2.8. *Assume that* $\mathrm{Aut}(\mathcal{X})$ *has a solvable subgroup G of order larger than* $34(\mathfrak{g}(\mathcal{X})+1)^{3/2}$. *If N is a normal subgroup of G and the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$ is neither rational nor elliptic, then the automorphism group $\bar{G} = G/N$ of $\bar{\mathcal{X}}$ has order larger than* $34(\mathfrak{g}(\bar{\mathcal{X}})+1)^{3/2}$, *as well.*

Since $|N| = |G|/|\bar{G}|$, the claim is a straightforward consequence of (3) except for the cases where $\mathfrak{g}(\bar{\mathscr{X}}) = 2$, or $\mathfrak{g}(\bar{\mathscr{X}}) = 3$, $\mathfrak{g}(\mathscr{X}) = 5$, $|N| = 2$, and the cover $\mathscr{X}|\bar{\mathscr{X}}$ is unramified. Actually, the exceptional cases do not occur. In fact, $|\bar{G}| \geq |G|(\mathfrak{g}(\bar{\mathscr{X}}) - 1)/(\mathfrak{g}(\mathscr{X}) - 1) > 34(\mathfrak{g}(\mathscr{X}) + 1)^{3/2}(\mathfrak{g}(\bar{\mathscr{X}}) - 1)/(\mathfrak{g}(\mathscr{X}) - 1)$ is bigger than 48 and $8 \cdot 27 = 216$ for $\mathfrak{g}(\bar{\mathscr{X}}) = 2$ and $\mathfrak{g}(\bar{\mathscr{X}}) = 3$, contradicting Results 2.7 and 2.3, respectively.

From group theory we use Dickson's classification of finite subgroups of the projective linear group $PGL(2, \mathbb{K})$; see [Valentini and Madan 1980] or [Hirschfeld et al. 2008, Theorem A.8].

Result 2.9. *The following is a complete list of finite solvable subgroups of $PGL(2, \mathbb{K})$ up to conjugacy*:

(i) *cyclic groups of order prime to p*,

(ii) *elementary abelian p-groups*,

(iii) *dihedral groups with an index-2 cyclic subgroup of order prime to p*,

(iv) *the alternating group* A_4,

(v) *the symmetric group* S_4,

(vi) *semidirect products of an elementary abelian p-group of order p^h by a cyclic group of order n with $n \mid (p^h - 1)$.*

If $PGL(2, \mathbb{K})$ is viewed as the automorphism group of the line over $\mathbb{K}$, any cyclic subgroup of order prime to p has exactly two points, while any p-subgroup has a unique fixed point [Valentini and Madan 1980].

We also use the Schur–Zassenhaus theorem; see for instance [Machì 2012, Corollary 7.5].

Result 2.10. *Let G be a finite group with a normal subgroup N. If $|N|$ is prime to the index $[G : N]$ of N, then N has a complement in G, that is, $G = N \rtimes M$ for a subgroup M of G. Such complements are pairwise conjugate in G.*

From representation theory, we need the Maschke theorem; see for instance [Machì 2012, Theorem 6.1].

Result 2.11. *Any representation of a finite group over a field whose characteristic is prime to the order of the group is completely reducible.*

The following two lemmas of independent interest play a role in our proof of Theorem 1.1.

Lemma 2.12. *Let $\mathscr{X}$ be an ordinary algebraic curve of genus $\mathfrak{g}(\mathscr{X}) \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of odd characteristic p. Let H be a solvable automorphism group of $\mathrm{Aut}(\mathscr{X})$ containing a normal p-subgroup Q such that $|Q|$ and $[H : Q]$ are coprime. Suppose that a complement U of Q in H is abelian and that*

$$|H| > \begin{cases} 18(\mathfrak{g} - 1) & \text{for } |U| = 3, \\ 12(\mathfrak{g} - 1) & \text{otherwise}. \end{cases} \tag{7}$$

Then U is cyclic, and the quotient curve $\bar{\mathscr{X}} = \mathscr{X}/Q$ is rational. Furthermore, Q has exactly two (nontame) short orbits, say Ω_1, Ω_2. They are also the only short orbits of H, and $\mathfrak{g}(\mathscr{X}) = |Q| - (|\Omega_1| + |\Omega_2|) + 1$.

Proof. From Result 2.10, $H = Q \rtimes U$. Set $|Q| = p^k$ and $|U| = u$. Then $p \nmid u$. Furthermore, if $u = 2$, then $|H| = 2|Q| > 9\mathfrak{g}(\mathscr{X})$ whence $|Q| > 4.5\mathfrak{g}(\mathscr{X})$. From Result 2.1, $\mathscr{X}$ has zero p-rank, which is not possible as $\mathscr{X}$ is assumed to be ordinary of genus at least 2. Therefore, $u \geq 3$.

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

If $\mathfrak{g}(\bar{\mathscr{X}}) \geq 2$, then $\mathrm{Aut}(\bar{\mathscr{X}})$ has a subgroup isomorphic to U, and Result 2.2(ii) yields $4\mathfrak{g}(\bar{\mathscr{X}}) + 4 \geq |U|$. Furthermore, from (3) applied to Q, $\mathfrak{g} - 1 \geq |Q|(\mathfrak{g}(\bar{\mathscr{X}}) - 1)$. Let $c = 12$ or $c = 18$, according as $|U| > 3$ or $|U| = 3$, so that $|H| > c(\mathfrak{g} - 1)$ from (7). Then

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

whence

$$c \leq 4\frac{\mathfrak{g}(\bar{\mathscr{X}}) + 1}{\mathfrak{g}(\bar{\mathscr{X}}) - 1}.$$

As the right-hand side is smaller than 12, a contradiction to the choice of the constant c is obtained.

If $\bar{\mathscr{X}}$ is elliptic, then the cover $\mathscr{X}|\bar{\mathscr{X}}$ ramifies; otherwise $\mathscr{X}$ itself would be elliptic. Thus, Q has some short orbits. The group H acts on the set of short orbits of Q. In this action, an orbit of a given short orbit o of Q with respect to H is a set of short orbits of Q having the same length of o. We will refer to these short orbits as images of o. Take a short orbit of Q together with its images $o_1, \ldots, o_{u_1}$ under the action of H. Since Q is a normal subgroup of H, $o = o_1 \cup \cdots \cup o_{u_1}$ is an H-orbit of size $u_1 p^v$ where $p^v = |o_1| = \cdots = |o_{u_1}|$. Equivalently, the stabilizer of a point $P \in o$ has order $p^{k-v}u/u_1$, and by Result 2.4, it is the semidirect product $Q_1 \rtimes U_1$ where $|Q_1| = p^{k-v}$ and $|U_1| = u/u_1$ for subgroups Q_1 of Q and U_1 of U, respectively. The point $\bar{P}$ lying under P in the cover $\mathscr{X}|\bar{\mathscr{X}}$ is fixed by the factor group $\bar{U}_1 = U_1Q/Q$. Since $\bar{\mathscr{X}}$ is elliptic, and p is prime to $|\bar{U}_1|$, Result 2.7 yields $|\bar{U}_1| \leq 4$ 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, $u \leq 4u_1$ for $p = 3$ and $u \leq 6u_1$ for $p > 3$. Furthermore, since the p-group Q_1 fixes P, and ${Q_1}^{(0)} = Q_1^{(1)} = Q_1$, we have $d_P = \sum_{i \geq 0}(|{Q_1}^{(i)}| - 1) \geq 2(|Q_1| - 1) = 2(p^{k-v} - 1) \geq \frac{4}{3}p^{k-v}$. From (3) applied to Q, since $P \in o$ and $|o| = p^v u_1$, if $p = 3$, then

$$2\mathfrak{g} - 2 \geq 3^v u_1 d_P \geq 3^v u_1\left(\tfrac{4}{3}3^{k-v}\right) = \tfrac{4}{3}3^k u_1 \geq \tfrac{1}{3}3^k u = \tfrac{1}{3}|Q||U| = \tfrac{1}{3}|H|,$$

while for $p > 3$,

$$2\mathfrak{g} - 2 \geq p^v u_1 d_P \geq p^v u_1\left(\tfrac{4}{3}p^{k-v}\right) = \tfrac{4}{3}p^k u_1 \geq \tfrac{2}{9}p^k u = \tfrac{2}{9}|Q||U| = \tfrac{2}{9}|H|,$$

but this contradicts (7).

If $\bar{\mathscr{X}}$ is rational, then Q has at least one short orbit. Furthermore, $\bar{U} = UQ/Q$ is isomorphic to a subgroup of $PGL(2, \mathbb{K}) \cong \mathrm{Aut}(\bar{\mathscr{X}})$. Since $U \cong \bar{U}$ and U is abelian, from Result 2.9, $\bar{U}$ is cyclic, $\bar{U}$ fixes two points $\bar{P}_0$ and $\bar{P}_\infty$, but no nontrivial element in $\bar{U}$ fixes a point other than $\bar{P}_0$ or $\bar{P}_\infty$. Let o_∞ and o_0 be the Q-orbits lying over $\bar{P}_0$ and $\bar{P}_\infty$, respectively. Obviously, o_∞ and o_0 are short orbits of H. We show that Q has at most two short orbits, the candidates being o_∞ and o_0. By absurd, there is a Q-orbit o

of size p^m with $m < k$ which lies over a point $\bar{P} \in \bar{\mathscr{X}}$ different 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 up^m. If $u > 3$, (3) applied to Q gives

$$2\mathfrak{g}-2 \geq -2p^k + up^m(p^{k-m}-1) \geq -2p^k + up^m\tfrac{2}{3}p^{k-m} = -2p^k + \tfrac{2}{3}up^k = \tfrac{2}{3}(u-3)p^k > \tfrac{1}{6}up^k = \tfrac{1}{6}|H|,$$

a contradiction with $|H| > 12(\mathfrak{g}-1)$. If $u = 3$, then $p > 3$, and hence,

$$2\mathfrak{g}-2 \geq -2p^k + 3p^m(p^{k-m}-1) = p^k - 3p^m > \tfrac{1}{3}p^k,$$

whence $|H| = 3p^k < 18(\mathfrak{g}-1)$, a contradiction with (7). This proves that H has exactly two short orbits. Since, as we have showed, Q has either one or two short orbits, and they are contained in $o_\infty \cup o_0$, two cases arise correspondingly. Assume first that Q has two short orbits. They are o_∞ and o_0. If their lengths are p^a and p^b with $a, b < k$, then (5) (or (3)) applied to Q gives

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

whence $\mathfrak{g}(\mathscr{X}) = p^k - (p^a + p^b) + 1 > 0$. The same argument shows that if Q has just one short orbit, then $\gamma(\mathscr{X}) = 0$, a contradiction. □

Lemma 2.13. *Let N be an automorphism group of an algebraic curve of even genus such that $|N|$ is even. Then any 2-subgroup of N has a cyclic subgroup of index 2.*

Proof. Let U be a subgroup of N of order $d = 2^u \geq 2$, and $\bar{\mathscr{X}} = \mathscr{X}/U$ the arising quotient curve. From (3) applied to U,

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

where $\ell_1, \ldots, \ell_m$ are the short orbits of U on $\mathscr{X}$. Since $\mathfrak{g}(\mathscr{X})$ is even, $2\mathfrak{g}(\mathscr{X}) - 2 \equiv 2 \pmod 4$. On the other hand, $2^u(2\mathfrak{g}(\bar{\mathscr{X}}) - 2) \equiv 0 \pmod 4$. Therefore, some ℓ_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 $\mathscr{X}$ and hence is cyclic. □

3. The proof of Theorem 1.1

Our proof is by induction on the genus. Theorem 1.1 holds for $\mathfrak{g}(\mathscr{X}) = 2$, as $|G| \leq 48$ for any solvable automorphism group G of a genus-2 curve; see Result 2.7. For $\mathfrak{g}(\mathscr{X}) > 2$, $\mathscr{X}$ is taken by absurd for a minimal counterexample with respect the genera so that for any solvable subgroup of $\mathrm{Aut}(\bar{\mathscr{X}})$ of an ordinary curve $\bar{\mathscr{X}}$ of genus $\mathfrak{g}(\bar{\mathscr{X}}) \geq 2$ we have $|\bar{G}| \leq 34(\mathfrak{g}+1)^{3/2}$. Two cases are treated separately.

Case I. G contains a minimal normal p-subgroup.

Proposition 3.1. *Let $\mathscr{X}$ be an ordinary algebraic curve of genus $\mathfrak{g}$ defined over an algebraically closed field $\mathbb{K}$ of odd characteristic $p > 0$. If G is a solvable subgroup of* $\mathrm{Aut}(\mathscr{X})$ *containing a minimal normal p-subgroup N, then $|G| \leq 34(\mathfrak{g}+1)^{3/2}$.*

Proof. Before going through the proof we describe the main steps in it.

Take the largest normal p-subgroup Q of G. Let $\bar{\mathcal{X}}$ be the quotient curve of $\mathcal{X}$ with respect to Q, and let $\bar{G} = G/Q$. The first step is to show that $\bar{\mathcal{X}}$ is rational. Then we derive from the classification in Result 2.9 that G is a semidirect product of Q by cyclic group U of order prime to p. Therefore, Lemma 2.12 applies to G. This gives us enough information on the action of Q on $\mathcal{X}$: Q has exactly two (nontame) orbits, say Ω_1 and Ω_2, and they are also the only short orbits of G. Then a subgroup H of G of index ≤ 2 preserves both Ω_1 and Ω_2, inducing a permutation group on each of them. If both Ω_1 and Ω_2 are nontrivial, that is, $|\Omega_1| > 1$ and $|\Omega_2| > 1$, then two cases are possible, according as Q_P with $P \in \Omega_1$ is sharply transitive and faithful on Ω_2 or some nontrivial element in Q_P fixes Ω_2 pointwise. So the next step is to rule out both these possibilities using elementary permutation group theory together with Results 2.2 and 2.4. If $\Omega_1 = \{P\}$ and $|\Omega_2| > 1$, then G fixes P, and the structure of G is given by Result 2.4 where Q is an elementary abelian group, that is, a vector space over the prime field of $\mathbb{K}$ and G is a linear group so that some appropriate result from representation theory can be used. In fact, combining Result 2.11 with (5) allows us to rule out this possibility. If $\Omega_1 = \{P\}$ and $\Omega_2 = \{Q\}$, we are able to prove a much stronger bound, namely $|G| \leq 2(\mathfrak{g}(\mathcal{X}) + 1)$. In this final step, our approach is function field theory rather than group theory as it uses some ideas from Nakajima's paper [1987] and the Riemann–Roch theorem together with some results on linearized polynomials over finite fields.

The quotient group $\bar{G}$ is a subgroup of $\mathrm{Aut}(\bar{\mathcal{X}})$, and it has no normal p-subgroup; otherwise G would have a normal p-subgroup properly containing Q. For $\bar{\mathfrak{g}} = \mathfrak{g}(\bar{\mathcal{X}})$ three cases may occur, namely $\bar{\mathfrak{g}} \geq 2$, $\bar{\mathfrak{g}} = 1$, or $\bar{\mathfrak{g}} = 0$. If $\bar{\mathfrak{g}} \geq 2$, then Result 2.8 shows that $|\bar{G}| > 34(\bar{\mathfrak{g}} + 1)^{3/2}$. Since $\bar{\mathcal{X}}$ is still ordinary by Result 2.5(v), this contradicts our choice of $\mathcal{X}$ to be a minimal counterexample. If $\bar{\mathfrak{g}} = 1$, then the cover $\mathbb{K}(\mathcal{X})|\mathbb{K}(\bar{\mathcal{X}})$ ramifies. Take a short orbit Δ of Q. Let Γ be the nontame short orbit of G that contains Δ. Since Q is normal in G, the orbit Γ partitions into short orbits of Q whose components have the same length, which is equal to $|\Delta|$. Let k be the number of the Q-orbits contained in Γ. Then

$$|G_P| = \frac{|G|}{k|\Delta|}$$

holds for every $P \in \Gamma$. Moreover, the quotient group $G_P Q/Q$ fixes a place on $\bar{\mathcal{X}}$. Now, from Result 2.7,

$$\frac{|G_P Q|}{|Q|} = \frac{|G_P|}{|G_P \cap Q|} = \frac{|G_P|}{|Q_P|} \leq 12.$$

From this together with (3) and Result 2.5(i),

$$2\mathfrak{g} - 2 \geq 2k|\Delta|(|Q_P| - 1) \geq 2k|\Delta|\frac{|Q_P|}{2} \geq \frac{k|\Delta||G_P|}{12} = \frac{|G|}{12},$$

which contradicts our hypothesis $|G| > 34(\mathfrak{g} + 1)^{3/2}$.

It turns out that $\bar{\mathcal{X}}$ is rational. Therefore, $\bar{G}$ is isomorphic to a subgroup of $PGL(2, \mathbb{K})$ which contains no normal p-subgroup. From Result 2.9, $\bar{G}$ is a prime to p subgroup which is either cyclic, or dihedral, or isomorphic to one of the groups Alt_4, Sym_4. In all cases, $\bar{G}$ has a cyclic subgroup U of index ≤ 6 and of order distinct from 3. We may dismiss all cases but the cyclic one up to replacing $\bar{G}$ with U, that is, up to assuming that $G = Q \rtimes U$ with $|G| \geq \frac{34}{6}(\mathfrak{g}(\mathscr{X})+1)^{3/2}$. Then $|G| > 12(\mathfrak{g}-1)$. Therefore, Lemma 2.12 applies to G. Thus, Q has exactly two (nontame) orbits, say Ω_1 and Ω_2, and they are also the only short orbits of G. More precisely,

$$\gamma - 1 = |Q| - (|\Omega_1| + |\Omega_2|). \tag{8}$$

We may also observe that G_P with $P \in \Omega_1$ contains a subgroup V isomorphic to U. In fact, $|Q||U| = |G| = |G_P||\Omega_1| = |Q_P \rtimes V||\Omega_1| = |V||Q_P||\Omega_1|$ with a prime to p subgroup V fixing P, whence $|U| = |V|$. Since V is cyclic the claim follows.

We proceed with the case where both Ω_1 and Ω_2 are nontrivial, that is, their lengths are at least 2.

Assume that Q is nonabelian, and look at the action of its center $Z(Q)$ on $\mathscr{X}$. Since $Z(Q)$ is a nontrivial normal subgroup of G, we can argue as before to show that quotient curve $\mathscr{X}/Z(Q)$ is rational, and hence that the Galois cover $\mathscr{X}|(\mathscr{X}/Z(Q))$ ramifies at some points. Indeed, observe that in the previous arguments normality of Q was only used to dismiss all cases but the rational one, and hence we may simply replace Q with $Z(Q)$. In other words, there is a point $P \in \Omega_1$ (or $R \in \Omega_2$) such that some nontrivial subgroup T of $Z(Q)$ fixes P (or R). Suppose that the former case occurs. Since Ω_1 is a Q-orbit, T fixes Ω_1 pointwise.

The group G has an index ≤ 2 subgroup H that induces a permutation group on Ω_1. Let M_1 be the kernel of this permutation representation. Obviously, T is a nontrivial p-subgroup of M_1. Therefore, M contains some but not all elements from Q. Since both M_1 and Q are normal subgroups of G, $N = M_1 \cap Q$ is a nontrivial normal p-subgroup of G. As we have proven before, the quotient curve $\widetilde{\mathscr{X}} = \mathscr{X}/N$ is rational, and hence the factor group $\widetilde{G} = G/N$ is isomorphic to a subgroup of $PGL(2, \mathbb{K})$. Since $1 \lneqq N \lneqq Q$, the order of $\widetilde{G}$ is divisible by p. From Result 2.9, $\widetilde{G} = \widetilde{Q} \rtimes \widetilde{U}$ where $\widetilde{Q}$ is an elementary abelian p-group of order q and $\widetilde{U} \cong UN/N \cong U$ with $|\widetilde{U}| = |U|$ is a divisor of $q-1$.

This shows that Q acts on Ω_1 as an abelian transitive permutation group. Obviously this holds true when Q is abelian. Therefore, the action of Q on Ω_1 is sharply transitive. In terms of 1-point stabilizers of Q on Ω_1, we have $Q_P = Q_{P'}$ for any $P, P' \in \Omega_1$. Moreover, $Q_P = N$, and hence Q_P is a normal subgroup of G.

Furthermore, since $\mathscr{X}$ is an ordinary curve, Q_P is an elementary abelian group by Result 2.5(ii).

The quotient curve $\mathscr{X}/Q_P$ is rational, and its automorphism group contains the factor group Q/Q_P. Hence, exactly one of the Q_P-orbits is preserved by Q. Since Ω_1 is a Q-orbit consisting of fixed points of Q_P, Ω_2 must be a Q_P-orbit. Similarly, if $Z(Q) \neq Q_P$, the factor group $Z(Q)Q_P/Q_P$ is an automorphism group of $\mathscr{X}/Q_P$ and hence exactly one of the Q_P-orbits is preserved by $Z(Q)$. Either $Z(Q)$ fixes a point in Ω_1 but then $Z(Q) = Q_P$, or Ω_2 is a $Z(Q)$-orbit. This shows that either $Z(Q) = Q_P$, or $Z(G)$ acts transitively on Ω_2.

Two cases arise according as Q_P is sharply transitive and faithful on Ω_2 or some nontrivial element in Q_P fixes Ω_2 pointwise.

If some nontrivial element in Q_P fixes Ω_2 pointwise, then the kernel M_2 of the permutation representation of H on Ω_2 contains a nontrivial p-subgroup. Hence, the above results extend from Ω_1 to Ω_2, and Q_R is a normal subgroup of Q.

If Q_P is (sharply) transitive on Ω_2, then the abelian group $Z(Q)Q_P$ acts on Ω_2 as a sharply transitive permutation group, as well. Hence, either $Z(Q) = Q_P$, or as before M_2 contains a nontrivial p-subgroup, and Q_R is a normal subgroup of Q. In the former case, $Q = Q_P Q_R$ with $Q_R \cap Q_P = \{1\}$, and $Z(Q) = Q_P$ yields that

$$Q = Q_P \times Q_R. \tag{9}$$

This shows that Q is abelian, and hence $|Q| \leq 4\mathfrak{g}+4$ by Result 2.2(ii). Also, either $|Q_P|$ or $|Q_R|$ is at most $\sqrt{4\mathfrak{g}+4}$. From Result 2.5(i), $G_P^{(2)}$ at $P \in \Omega_1$ is trivial. Furthermore, for $G_P = Q_P \rtimes V$, Result 2.5(iv) gives $|U| = |V| \leq |Q_P| - 1$. Hence, $|U| < |Q_P| \leq \sqrt{|Q|} \leq \sqrt{4\mathfrak{g}+4}$ whence

$$|G| = |U||Q| \leq 8(\mathfrak{g}+1)^{3/2}. \tag{10}$$

If Q_R is a normal subgroup, take a point R from Ω_2, and look at the subgroup $Q_{P,R}$ of Q_P fixing R. Actually, we prove that either $Q_{P,R} = Q_P$ or $Q_{P,R}$ is trivial. Suppose that $Q_{P,R} \neq \{1\}$. Since $Q_{P,R} = Q_P \cap Q_R$ and both Q_P and Q_R are normal subgroups of G; the same holds for $Q_{P,R}$. By (ii), the quotient curve $\mathscr{X}/Q_{P,R}$ is rational and hence its automorphism group $Q/Q_{P,R}$ fixes exactly one point. Furthermore, each point in Ω_2 is totally ramified. Therefore, $Q_R = Q_{P,R}$; otherwise $Q_R/Q_{P,R}$ would fix any point lying under a point in Ω_1 in the cover $\mathscr{X}|(\mathscr{X}/Q_{P,R})$.

It turns out that either $Q_P = Q_R$ or $Q_P \cap Q_R = \{1\}$, whenever $P \in \Omega_1$ and $R \in \Omega_2$.

In the former case, from (5) applied to Q_P,

$$\gamma - 1 = -|Q_P| + |\Omega_1|(|Q_P| - 1) + |\Omega_2|(|Q_P| - 1) = -|Q_P| + |Q| - |\Omega_1| + |Q| - |\Omega_2|.$$

This together with (8) give $Q = Q_P$, a contradiction.

Therefore, the latter case must hold. Thus, $Q = Q_P \times Q_R$ and Q_P (and also Q_R) is an elementary abelian group since it is isomorphic to a p-subgroup of $PGL(2, \mathbb{K})$. Also, $|Q_P| = |Q_R| = \sqrt{|Q|}$. Since Q is abelian, this yields $|Q_P| \leq \sqrt{4\mathfrak{g}+4}$ by Result 2.2(ii). Now, the argument used after (9) can be employed to prove (10). This ends the proof in the case where both Ω_1 and Ω_2 are nontrivial.

Suppose next $\Omega_1 = \{P\}$ and $|\Omega_2| \geq 2$. Then G fixes P, and hence $G = Q \rtimes U$ with an elementary abelian p-group Q. Furthermore, G has a permutation representation on Ω_2 with kernel K. As Ω_2 is a short orbit of Q, the stabilizer Q_R of $R \in \Omega_2$ in Q is nontrivial. Since Q is abelian, this yields that K is nontrivial, and hence it is a nontrivial elementary abelian normal subgroup of G. In other words, Q is an r-dimensional vector space $V(r, p)$ over a finite field $\mathbb{F}_p$ with $|Q| = p^r$, the action of each nontrivial element of U by conjugacy is a nontrivial automorphism of $V(r, p)$, and K is a U-invariant subspace. By Result 2.11, K has a complementary U-invariant subspace. Therefore, Q has a subgroup M such that $Q = K \times M$, and M is a normal subgroup of G. Since $K \cap M = \{1\}$, and Ω_2 is an orbit of Q, this yields $|M| = |\Omega_2|$. The factor group G/M is an automorphism group of the quotient curve $\mathscr{X}/M$, and Q/M is a nontrivial p-subgroup of G/M whereas G/M fixes two points on $\mathscr{X}/M$. Therefore the quotient curve $\mathscr{X}/M$ is not rational since the 2-point stabilizer in the representation of $PGL(2, \mathbb{K})$ as an automorphism group of the rational function field is a prime to p (cyclic) group. We show that $\mathscr{X}/M$ is not elliptic either.

From (5), $\mathfrak{g}(\mathscr{X})-1=\gamma(\mathscr{X})-1=-|Q|+1+|\Omega_2|$, and so $\mathfrak{g}(\mathscr{X})$ is even. Since M is a normal subgroup of odd order, $\mathfrak{g}(\mathscr{X})\equiv 0 \pmod 2$ yields that $\mathfrak{g}(\mathscr{X}/M)\equiv 0 \pmod 2$. In particular, $\mathfrak{g}(\mathscr{X}/M)\neq 1$. Therefore, $\mathfrak{g}(\mathscr{X}/M)\geq 2$. At this point we may repeat our previous argument and prove $|G/M|>34(\mathfrak{g}(\mathscr{X}/M)+1)^{3/2}$. Again, we get a contradiction with our choice of $\mathscr{X}$ to be a minimal counterexample, which ends the proof in the case where just one of Ω_1 and Ω_2 is trivial.

We are left with the case where both short orbits of Q are trivial. Our goal is to prove a much stronger bound for this case, namely $|U|\leq 2$ whence

$$|G|\leq 2(\mathfrak{g}(\mathscr{X})+1). \tag{11}$$

We also show that if equality holds then $\mathscr{X}$ is a hyperelliptic curve with equation

$$f(U)=aT+b+cT^{-1}, \quad a,b,c\in\mathbb{K}^*, \tag{12}$$

where $f(U)\in\mathbb{K}[U]$ is an additive polynomial of degree $|Q|$.

Let $\Omega_1=\{P_1\}$ and $\Omega_2=\{P_2\}$. Then Q has two fixed points P_1 and P_2, but no nontrivial element in Q fixes a point of $\mathscr{X}$ other than P_1 and P_2. From (5),

$$\mathfrak{g}(\mathscr{X})+1=\gamma(\mathscr{X})+1=|Q|. \tag{13}$$

Therefore, $|U|\leq\mathfrak{g}(\mathscr{X})$. Actually, for our purpose, we need a stronger estimate, namely $|U|\leq 2$. To prove the latter bound, we use some ideas from Nakajima's paper [1987] regarding the Riemann–Roch spaces $\mathscr{L}(\boldsymbol{D})$ of certain divisors $\boldsymbol{D}$ of $\mathbb{K}(\mathscr{X})$. Our first step is to show

(i) $\dim_{\mathbb{K}}\mathscr{L}((|Q|-1)P_1)=1$ and

(ii) $\dim_{\mathbb{K}}\mathscr{L}((|Q|-1)P_1+P_2)\geq 2$.

Let $\ell\geq 1$ be the smallest integer such that $\dim_{\mathbb{K}}\mathscr{L}(\ell P_1)=2$, and take $x\in\mathscr{L}(\ell P_1)$ with $v_{P_1}(x)=-\ell$. As $Q=Q_{P_1}$, the Riemann–Roch space $\mathscr{L}(\ell P_1)$ contains all $c_\sigma=\sigma(x)-x$ with $\sigma\in Q$. This yields $c_\sigma\in\mathbb{K}$ by $v_{P_1}(c_\sigma)\geq-\ell+1$ and our choice of ℓ to be minimal. Also, $Q=Q_{P_2}$ together with $v_{P_2}(x)\geq 0$ show $v_{P_2}(c_\sigma)\geq 1$. Therefore, $c_\sigma=0$ for all $\sigma\in Q$, that is, x is fixed by Q. From $\ell=[\mathbb{K}(\mathscr{X}):\mathbb{K}(x)]=[\mathbb{K}:\mathbb{K}(\mathscr{X})^Q][\mathbb{K}(\mathscr{X})^Q:\mathbb{K}(x)]$ and $|Q|=[\mathbb{K}:\mathbb{K}(\mathscr{X})^Q]$, it turns out that ℓ is a multiple of $|Q|$. Thus $\ell>|Q|-1$ whence (i) follows. From the Riemann–Roch theorem, $\dim_{\mathbb{K}}\mathscr{L}((|Q|-1)P_1+P_2)\geq|Q|-g+1=2$, which proves (ii).

Let $d\geq 1$ be the smallest integer such that $\dim_{\mathbb{K}}\mathscr{L}(dP_1+P_2)=2$. From (ii)

$$d\leq|Q|-1. \tag{14}$$

Let α be a generator of the cyclic group U. Since α fixes both points P_1 and P_2, it acts on $\mathscr{L}(dP_1+P_2)$ as a $\mathbb{K}$-vector space automorphism $\bar{\alpha}$. If $\bar{\alpha}$ is trivial, then $\alpha(u)=u$ for all $u\in\mathscr{L}(dP_1+P_2)$. Suppose that $\bar{\alpha}$ is nontrivial. Since U is a prime to p cyclic group, $\bar{\alpha}$ has two distinct eigenspaces, so that $\mathscr{L}(dP_1+P_2)=\mathbb{K}\oplus\mathbb{K}u$ where $u\in\mathscr{L}(dP_1+P_2)$ is an eigenvector of $\bar{\alpha}$ with eigenvalue $\xi\in\mathbb{K}^*$ so that

$\bar{\alpha}(u) = \xi u$ with $\xi^{|U|} = 1$. Therefore, there is $u \in \mathscr{L}(dP_1 + P_2)$ with $u \neq 0$ such that $\alpha(u) = \xi u$ with $\xi^{|U|} = 1$. The pole divisor of u is

$$\mathrm{div}(u)_\infty = dP_1 + P_2. \tag{15}$$

Since $Q = Q_{P_1} = Q_{P_2}$, the Riemann–Roch space $\mathscr{L}(dP_1 + P_2)$ contains $\sigma(u)$ and hence contains all

$$\theta_\sigma = \sigma(u) - u, \quad \sigma \in Q.$$

By our choice of d to be minimal, this yields $\theta_\sigma \in \mathbb{K}$, and then defines the map θ from Q into $\mathbb{K}$ that takes σ to θ_σ. More precisely, θ is a homomorphism from Q into the additive group $(\mathbb{K}, +)$ of $\mathbb{K}$ as the following computation shows:

$$\theta_{\sigma_1 \circ \sigma_2} = (\sigma_1 \circ \sigma_2)(u) - u = \sigma_1(\sigma_2(u) - u + u) - u = \sigma_1(\theta_{\sigma_2}) + \sigma_1(u) - u = \theta_{\sigma_2} + \theta_{\sigma_1} = \theta_{\sigma_1} + \theta_{\sigma_2}.$$

Also, θ is injective. In fact, if $\theta_{\sigma_0} = 0$ for some $\sigma_0 \in Q \setminus \{1\}$, then u is in the fixed field of σ_0, which is impossible since $v_{P_2}(u) = -1$ whereas P_2 is totally ramified in the cover $\mathscr{X}|(\mathscr{X}/\langle\sigma_p\rangle)$. The image $\theta(Q)$ of θ is an additive subgroup of $\mathbb{K}$ of order $|Q|$. The smallest subfield of $\mathbb{K}$ containing $\theta(Q)$ is a finite field $\mathbb{F}_{p^m}$ and hence $\theta(Q)$ can be viewed as a linear subspace of $\mathbb{F}_{p^m}$ considered as a vector space over $\mathbb{F}_p$. Therefore, the polynomial

$$f(U) = \prod_{\sigma \in Q} (U - \theta_\sigma) \tag{16}$$

is a linearized polynomial over $\mathbb{F}_p$ [Lidl and Niederreiter 1983, §4, Theorem 3.52]. In particular, $f(U)$ is an additive polynomial of degree $|Q|$; see also [Serre 1962, Chapter V, §5]. Also, $f(U)$ is separable as θ is injective. From (16), the pole divisor of $f(u) \in \mathbb{K}(\mathscr{X})$ is

$$\mathrm{div}(f(u))_\infty = |Q|(dP_1 + P_2). \tag{17}$$

For every $\sigma_0 \in Q$,

$$\sigma_0(f(u)) = \prod_{\sigma \in Q}(\sigma_0(u) - \theta_\sigma) = \prod_{\sigma \in Q}(u + \theta_{\sigma_0} - \theta_\sigma) = \prod_{\sigma \in Q}(u - \theta_{\sigma\sigma_0^{-1}}) = \prod_{\sigma \in Q}(u - \theta_\sigma) = f(u).$$

Thus, $f(u) \in \mathbb{K}(\mathscr{X})^Q$. Furthermore, from $\alpha \in N_G(Q)$, for every $\sigma \in Q$ there is $\sigma' \in Q$ such that $\alpha\sigma = \sigma'\alpha$. Therefore,

$$\alpha(f(u)) = \prod_{\sigma \in Q}(\alpha(\sigma(u) - u)) = \prod_{\sigma \in Q}(\alpha(\sigma(u)) - \xi u) = \prod_{\sigma \in Q}(\sigma'(\alpha(u)) - \xi u) = \prod_{\sigma \in Q}(\sigma'(\xi u) - \xi u) = \xi f(u).$$

This shows that if $R \in \mathscr{X}$ is a zero of $f(u)$ then $\mathrm{Supp}(\mathrm{div}(f(u)_0))$ contains the U-orbit of R of length $|U|$. Actually, since $\sigma(f(u)) = f(u)$ for $\sigma \in Q$, $\mathrm{Supp}(\mathrm{div}(f(u)_0))$ contains the G-orbit of R of length $|G| = |Q||U|$. This together with (17) give

$$|U| | (d+1). \tag{18}$$

On the other hand, $\mathbb{K}(\mathscr{X})^Q$ is rational. Let $\bar{P}_1$ and $\bar{P}_2$ be the points lying under P_1 and P_2, respectively, and let $\bar{R}_1, \bar{R}_2, \dots, \bar{R}_k$ with $k = (d+1)/|U|$ be the points lying under the zeros of $f(u)$ in the cover $\mathscr{X}|(\mathscr{X}/Q)$. We may represent $\mathbb{K}(\mathscr{X})^Q$ as the projective line $\mathbb{K} \cup \{\infty\}$ over $\mathbb{K}$ so that $\bar{P}_1 = \infty$, $\bar{P}_1 = 0$, and $\bar{R}_i = t_i$ for $1 \le i \le k$. Let $g(t) = t^d + t^{-1} + h(t)$ where $h(t) \in \mathbb{K}[t]$ is a polynomial of degree $k = (d+1)/|U|$ whose roots are $r_1, \dots, r_k$. It turns out that $f(u), g(t) \in \mathbb{K}(\mathscr{X})$ have the same pole and zero divisors, and hence

$$cf(u) = t^d + t^{-1} + h(t), \quad c \in \mathbb{K}^*. \tag{19}$$

We prove that $\mathbb{K}(\mathscr{X}) = \mathbb{K}(u, t)$. From [Sullivan 1975] (see also [Hirschfeld et al. 2008, Remark 12.12]), the polynomial $cTf(X) - T^{d+1} - 1 - h(T)T$ is irreducible, and the plane curve $\mathscr{C}$ has genus $\mathfrak{g}(\mathscr{C}) = \frac{1}{2}(q-1)(d+1)$. Comparison with (13) shows $\mathbb{K}(\mathscr{X}) = \mathscr{C}$ and $d = 1$ whence $|U| \le 2$. If equality holds, then $\deg h(T) = 1$ and $\mathscr{X}$ is a hyperelliptic curve with Equation (12). □

Case II. G contains no minimal normal p-subgroup.

Proposition 3.2. *Let $\mathscr{X}$ be an ordinary algebraic curve of genus $\mathfrak{g}$ defined over a field $\mathbb{K}$ of odd characteristic $p > 0$. If G is a solvable subgroup of $\mathrm{Aut}(\mathscr{X})$ with a minimal normal subgroup N, then $|G| \le 34(\mathfrak{g}(\mathscr{X}) + 1)^{3/2}$.*

Proof. We begin with an outline of the proof.

Since $\mathscr{X}$ is chosen to be a (minimal) counterexample, Proposition 3.1 yields that G contains no nontrivial normal p-subgroup. The factor group $\bar{G} = G/N$ is a subgroup of $\mathrm{Aut}(\bar{\mathscr{X}})$ where $\bar{\mathscr{X}} = \mathscr{X}/N$. As in the proof of Proposition 3.1, we begin by showing that $\bar{\mathscr{X}}$ must be rational. This time Result 2.6(ii) does not apply and some more effort is needed to rule out the possibility of $\mathfrak{g}(\bar{\mathscr{X}}) \ge 2$ while the elliptic case does not require a different approach. If $\bar{\mathscr{X}}$ is rational, the classification in Result 2.9 gives the possibility of the structure of $\bar{G}$ and its action on $\bar{\mathscr{X}}$. A careful analysis shows that $\bar{G}$ must be of type (vi) in Result 2.9. From this we obtain the possibilities for the action of G on $\mathscr{X}$. After that, (3) and (5) together with straightforward computation are sufficient to end the proof although the case where N is an elementary abelian 2-group requires some additional facts from group theory.

We prove that $\mathfrak{g}(\bar{\mathscr{X}}) \ge 2$. By Result 2.2(ii), $|N| \le 4\mathfrak{g}(\mathscr{X}) + 4$ as N is abelian. If $\bar{\mathscr{X}}$ is also ordinary, then the choice of $\mathscr{X}$ to have minimal genus implies that $|\bar{G}| \le 34(\mathfrak{g}(\bar{\mathscr{X}}) + 1)^{3/2}$. Comparing this with Result 2.8 shows a contradiction. Therefore, the possibility for $\bar{\mathscr{X}}$ to be nonordinary is investigated.

From Result 2.5(i), any p-subgroup S of G has trivial second ramification group at any point $\mathscr{X}$. The latter property remains true when $\mathscr{X}$ and S are replaced by $\bar{\mathscr{X}}$ and the factor group $\bar{S} = SN/N$, respectively. To show this claim, take $\bar{P} \in \bar{\mathscr{X}}$ and let $\bar{S}_{\bar{P}}$ be the subgroup of $\bar{S}$ fixing $\bar{P}$. Since $p \nmid |N|$ there is a point $P \in \mathscr{X}$ lying over $\bar{P}$ which is fixed by S. Hence, the stabilizer S_P of P in S is a nontrivial normal subgroup of G_P. Since N is a normal subgroup in G, so is N_P in G_P. This yields that the product $N_P S_P$ is actually a direct product. Therefore, N_P is trivial by Result 2.5(iii), that is, the cover $\mathscr{X}|\bar{\mathscr{X}}$ is unramified at $\bar{P}$. From this, the claim follows.

Actually, N may be taken to be the largest normal subgroup N_1 of G whose order is prime to p. Also, by our hypothesis, the quotient curve $\mathscr{X}_1 = \mathscr{X}/N_1$ is neither rational, nor elliptic. From Result 2.8, its

$\mathbb{K}$-automorphism group $G_1 = G/N_1$ has order bigger than $34(\mathfrak{g}(\mathscr{X}_1)+1)^{3/2}$. Since G and hence G_1 are solvable, G_1 has a minimal normal d-subgroup where d must be equal to p by the choice of N_1 to be the largest normal, prime to p subgroup of G. Take the largest normal p-subgroup N_2 of G_1. Observe that $N_2 \neq G_1$. In fact, if $N_2 = G_1$, then G_1 is p-group of order bigger than $34(\mathfrak{g}(\mathscr{X}_1)+1)^{3/2} > p\mathfrak{g}(\mathscr{X}_1)/(p-2)$. From Result 2.1, $\mathscr{X}_1$ has zero p-rank, and hence G_1 fixes a point $P_1 \in \mathscr{X}_1$. On the other hand, since $G_1^{(2)}$ is trivial, Result 2.6(iii) shows $|G_1| \leq p\mathfrak{g}(\mathscr{X}_1)/(p-1)$, a contradiction. Now, define $\mathscr{X}_2$ to be the quotient curve $\mathscr{X}_1/N_2$. Since the second ramification group of N_1 at any point of $\mathscr{X}_1$ is trivial, Result 2.6(i) gives $\mathfrak{g}(\mathscr{X}_1) - \gamma(\mathscr{X}_1) = |N_2|(\mathfrak{g}(\mathscr{X}_2) - \gamma(\mathscr{X}_2))$. In particular, if $\mathscr{X}_2$ is ordinary or rational, then $\mathscr{X}_1$ is an ordinary curve. From the proof of Proposition 3.1, the case $\mathfrak{g}(\mathscr{X}_2) = 1$ cannot occur as $|G_1| > 34(\mathfrak{g}(\mathscr{X}_1)+1)^{3/2}$. Therefore, $\mathfrak{g}(\mathscr{X}_2) \geq 2$ with $\mathfrak{g}(\mathscr{X}_2) > \gamma(\mathscr{X}_2)$ may be assumed. The factor group $G_2 = G_1/N_2$ is a $\mathbb{K}$-automorphism group of the quotient curve $\mathscr{X}_2 = \mathscr{X}_1/N_2$, and it has a minimal normal d-subgroup with $d \neq p$, by the choice of N_2. Define N_3 to be the largest normal, prime to p subgroup of G_2. Observe that N_3 must be a proper subgroup of G_2; otherwise G_2 itself would be a prime to p subgroup of $\mathrm{Aut}(\mathscr{X}_2)$ of order bigger than $34(\mathfrak{g}(\mathscr{X}_2)+1)^{3/2}$, contradicting Result 2.2(i). Therefore, there exists a (maximal) nontrivial normal p-subgroup N_4 in the factor group $G_3 = G_2/N_3$. Now, the above argument remains valid whenever $G, N_1, G_1, N_2, \mathscr{X}_1, \mathscr{X}_2$ are replaced by $G_2, N_3, G_3, N_4, \mathscr{X}_3, \mathscr{X}_4$ where the quotient curves are $\mathscr{X}_3 = G_2/N_3$ and $\mathscr{X}_4 = G_3/N_4$. In particular, $\mathfrak{g}(\mathscr{X}_4) \neq 1$ and $\mathfrak{g}(\mathscr{X}_3) - \gamma(\mathscr{X}_3) = |N_4|(\mathfrak{g}(\mathscr{X}_4) - \gamma(\mathscr{X}_4))$. Repeating the above argument, a finite sharply decreasing sequence $\mathfrak{g}(\mathscr{X}_1) > \mathfrak{g}(\mathscr{X}_2) > \mathfrak{g}(\mathscr{X}_3) > \mathfrak{g}(\mathscr{X}_4) > \cdots$ arises. If this sequence has $n+1$ members, then $\mathfrak{g}(\mathscr{X}_n) - \gamma(\mathscr{X}_n) = |N_{n+1}|(\mathfrak{g}(\mathscr{X}_{n+1}) - \gamma(\mathscr{X}_{n+1}))$ with $\mathfrak{g}(\mathscr{X}_{n+1}) = \gamma(\mathscr{X}_{n+1}) = 0$. Therefore, for some (odd) index $m \leq n$, the curve $\mathscr{X}_m$ would not be ordinary, but the successive member $\mathscr{X}_{m+1}$ would be an ordinary curve. Since $\mathscr{X}_{m+1}$ is a quotient curve of $\mathscr{X}_m$ with respect to a p-subgroup, this is impossible by Result 2.6(ii).

We continue with the elliptic case. Since $\mathfrak{g}(\mathscr{X}) \geq 2$, (3) applied to $\bar{X}$ ensures that N has a short orbit. Let Γ be a short orbit of G containing a short orbit of N. Since N is a normal subgroup of G, Γ is partitioned into short orbits $\Sigma_1, \ldots, \Sigma_k$ of N each of length $|\Sigma_1|$. Take a point R_i from Σ_i for $i = 1, 2, \ldots, k$, and set $\Sigma = \Sigma_1$ and $S = S_1$. With this notation, $|G| = |G_S||\Gamma| = |G_S|k|\Sigma|$, and (3) gives

$$2\mathfrak{g}(\mathscr{X}) - 2 \geq \sum_{i=1}^{k} |\Sigma_i|(|N_{S_i}| - 1) = k|\Sigma|(|N_S| - 1) \geq +\tfrac{1}{2}k|\Sigma||N_S| = \tfrac{1}{2}|G|\frac{|N_S|}{|G_S|}. \tag{20}$$

Also, the factor group $G_S N/N$ is a subgroup of $\mathrm{Aut}(\bar{\mathscr{X}})$ fixing the point of $\bar{\mathscr{X}}$ lying under S in the cover $\mathscr{X}|\bar{\mathscr{X}}$. From Result 2.7,

$$\frac{|G_S N|}{|N|} = \frac{|G_S|}{|G_S \cap N|} = \frac{|G_S|}{|N_S|} \leq 12.$$

This and (20) yield $|G| \leq 48(\mathfrak{g}(\mathscr{X}) - 1)$, a contradiction with our hypothesis $34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$.

Therefore, $\bar{\mathscr{X}}$ is rational. Thus, $\bar{G}$ is isomorphic to a subgroup of $PGL(2,\mathbb{K})$. Since p divides $|G|$ but not $|N|$, $\bar{G}$ contains a nontrivial p-subgroup. From Result 2.9, either $p = 3$ and $\bar{G} \cong \mathrm{Alt}_4, \mathrm{Sym}_4$, or $\bar{G} = \bar{Q} \rtimes \bar{C}$ where $\bar{Q}$ is a normal p-subgroup and its complement $\bar{C}$ is a cyclic prime to p subgroup and $|\bar{C}|$ divides $|\bar{Q}| - 1$.

If $\bar{G} \cong \mathrm{Alt}_4, \mathrm{Sym}_4$, then $|\bar{G}| \le 24$ whence $|G| \le 24|N| \le 96(\mathfrak{g}(\mathscr{X})+1)$ as N is abelian. Comparison with our hypothesis $|G| \ge 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$ shows that $\mathfrak{g}(\mathscr{X}) \le 6$. For small genera we need a little more. If $|N|$ is prime, then $|N| \le 2\mathfrak{g}(\mathscr{X})+1$ by Result 2.2(iii), and hence $|G| \le 48(\mathfrak{g}(\mathscr{X})+1)$, which is inconsistent with $|G| \ge 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$. Otherwise, since $p=3$ and $|N|$ has order a power of prime distinct from p, the bound $|N| \le 4(\mathfrak{g}(\mathscr{X})+1)$ with $\mathfrak{g}(\mathscr{X}) \le 6$ is only possible for $(\mathfrak{g}(\mathscr{X}), |N|) \in \{(3,16),(4,16),(5,16),(6,16),(6,25)\}$. Comparison of $|G| \le 24|N|$ with $|G| \ge 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$ rule out the latter three cases. Furthermore, since N is an elementary abelian group of order 16, $\mathfrak{g}(\mathscr{X})$ must be odd by Lemma 2.13. Finally, $\mathfrak{g}(\mathscr{X})=3$, $|N|=16$, and $G/N \cong \mathrm{Sym}_4$ is impossible as Result 2.3 would imply that $\mathscr{X}$ has zero p-rank.

Therefore, the case $\bar{G} = \bar{Q} \rtimes \bar{C}$ occurs. Also, $\bar{G}$ fixes a unique place $\bar{P} \in \bar{\mathscr{X}}$. Let Δ be the N-orbits in $\mathscr{X}$ that lie over $\bar{P}$ in the cover $\mathscr{X}|\bar{\mathscr{X}}$. We prove that Δ is a long orbit of N. By absurd, the permutation representation of G on Δ has a nontrivial 1-point stabilizer containing a nontrivial subgroup M of N. Since N is abelian, M is in the kernel. In particular, M is a normal subgroup of G contradicting our choice of N to be minimal.

Take a Sylow p-subgroup Q of G of order $|Q| = p^h$ with $h \ge 1$, and look at the action of Q on Δ. Since $|\Delta| = |N|$ is prime to p, Q fixes a point $P \in \Delta$, that is, $Q = Q_P$. Since $\mathscr{X}$ is an ordinary curve, Result 2.5(ii) shows that Q_P and hence Q are elementary abelian. Therefore, $G_P = Q \rtimes U$ where U is a prime to p cyclic group. Thus,

$$|\bar{Q}||\bar{C}||N| = |\bar{G}||N| = |G| = |G_P||\Delta| = |Q||U||\Delta| = |Q||U||N|, \tag{21}$$

whence $|Q| = |\bar{Q}|$ and $|U| = |\bar{C}|$. Consider the subgroup H of G generated by G_P and N. Since Δ is a long N-orbit, $G_P \cap N = \{1\}$. As N is normal in H this implies that $H = N \rtimes G_P = N \rtimes (Q \rtimes U)$ and hence $|H| = |N||Q||U|$, which proves $G = H = N \rtimes (Q \rtimes U)$.

Since $\bar{\mathscr{X}}$ is rational and $\bar{P}$ is the unique fixed point of nontrivial elements of $\bar{Q}$, each $\bar{Q}$-orbit other than $\{\bar{P}\}$ is long. Furthermore, $\bar{C}$ fixes a point $\bar{R}$ other than $\bar{P}$ and no nontrivial element of $\bar{C}$ fixes a point distinct from $\bar{P}$ and $\bar{R}$. This shows that the $\bar{G}$-orbit $\bar{\Omega}_1$ of $\bar{R}$ has length $|Q|$. In terms of the action of G on $\mathscr{X}$, there exist as many as $|Q|$ orbits of N, say $\Delta_1, \ldots, \Delta_{|Q|}$, whose union Λ is a short G-orbit lying over $\bar{\Omega}_1$ in the cover $\mathscr{X}|\bar{\mathscr{X}}$. Obviously, if at least one of Δ_i is a short N-orbit, then so are all.

We show that this actually occurs. Since the cover $\mathscr{X}|\bar{\mathscr{X}}$ ramifies, N has some short orbits, and by absurd there exists a short N-orbit Σ not contained in Λ. Then Σ and Λ are disjoint. Let Γ denote the (short) G-orbit containing Σ. Since N is a normal subgroup of G, Γ is partitioned into N-orbits, say $\Sigma = \Sigma_1, \ldots, \Sigma_k$, each of them of the same length $|\Sigma|$. Here $k = |Q||U|$ since the set of points of $\bar{\mathscr{X}}$ lying under these k short N-orbits is a long $\bar{G}$-orbit. Also, $|N| = |\Sigma_i||N_{R_i}|$ for $\le i \le k$ and $R_i \in \Sigma_i$. In particular, $|\Sigma_1| = |\Sigma_i|$ and $|N_{R_1}| = |B_{R_i}|$. From (3),

$$2\mathfrak{g}(\mathscr{X}) - 2 \ge -2|N| + \sum_{i=1}^{k} |\Sigma_i|(|N_{R_i}|-1) = -2|N| + |Q||U||\Sigma_1|(|N_{R_1}|-1).$$

Since N_{R_1} is nontrivial, $|N_{R_1}|-1 \geq \frac{1}{2}|N_{R_1}|$. Therefore,

$$2\mathfrak{g}(\mathscr{X})-2 \geq -2|N|+\tfrac{1}{2}|Q||U||\Sigma_1||N_{R_1}| = -2|N|+\tfrac{1}{2}|Q||U||N| = |N|\big(\tfrac{1}{2}(|Q||U|-2)\big) = \tfrac{1}{2}|N|(|Q||U|-4).$$

As $|Q||U|-4 \geq \frac{1}{2}|Q||U|$ by $|Q||U| \geq 4$, this gives

$$2\mathfrak{g}(\mathscr{X})-2 \geq \tfrac{1}{4}|N||U||Q| = \tfrac{1}{4}|G|.$$

But this contradicts our hypothesis $|G| > 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$.

Therefore, the short orbits of N are exactly $\Delta_1,\ldots,\Delta_{|Q|}$. Take a point S_i from Δ_i for $i=1,\ldots,|Q|$. Then N_{S_1} and N_{S_i} are conjugate in G, and hence $|N_{S_1}| = |N_{S_i}|$. From (3) applied to N,

$$2\mathfrak{g}(\mathscr{X})-2 = -2|N| + \sum_{i=1}^{|Q|} |\Delta_i|(|N_{S_i}|-1) = -2|N| + |Q||\Delta_1|(|N_{S_1}|-1) \geq -2|N| + \tfrac{1}{2}|Q||\Delta_1||N_{S_1}|.$$

Since $|N| = |\Delta_1||N_{S_1}|$, this gives $2\mathfrak{g}(\mathscr{X})-2 \geq \frac{1}{2}|N|(|Q|-4)$ whence $2\mathfrak{g}(\mathscr{X})-2 \geq \frac{1}{4}|N||Q|$ provided that $|Q| \geq 5$. The missing case, $|Q|=3$, cannot actually occur since in this case $|\bar{C}| = |U| \leq |Q|-1 = 2$, whence $|G| = |Q||U||N| \leq 6|N| \leq 24(\mathfrak{g}(\mathscr{X})+1)$, a contradiction with $|G| > 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$. Thus,

$$|N||Q| \leq 8(\mathfrak{g}(\mathscr{X})-1). \tag{22}$$

Since $|N||U| < |N||Q|$, this also shows

$$|N||U| < 8(\mathfrak{g}(\mathscr{X})-1). \tag{23}$$

Therefore,

$$|G||N| = |N|^2|U||Q| < 64(\mathfrak{g}(\mathscr{X})-1)^2.$$

Equations (22) and (23) together with our hypothesis $|G| \geq 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$ yield

$$|N| < \tfrac{64}{34}\sqrt{\mathfrak{g}(\mathscr{X})-1}. \tag{24}$$

From (24) and $|G| = |N||Q||U| \geq 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$ we obtain

$$|Q||U| > \frac{34^2}{64}(\mathfrak{g}(\mathscr{X})-1) > 18(\mathfrak{g}(\mathscr{X})-1),$$

which shows that Lemma 2.12 applies to the subgroup $Q \rtimes U$ of $\mathrm{Aut}(\mathscr{X})$. With the notation in Lemma 2.12, this gives that $Q \rtimes U$ and Q have the same two short orbits, $\Omega_1 = \{P\}$ and Ω_2. In the cover $\mathscr{X}|\bar{\mathscr{X}}$, the point $\bar{P} \in \bar{\mathscr{X}}$ lying under P is fixed by Q. We prove that Ω_2 is a subset of the N-orbit Δ containing P. For this purpose, it suffices to show that for any point $R \in \Omega_2$, the point $\bar{R} \in \bar{\mathscr{X}}$ lying under R in the cover $\mathscr{X}|\bar{\mathscr{X}}$ coincides with $\bar{P}$. Since Ω_2 is a Q-short orbit, the stabilizer Q_R is nontrivial, and hence $\bar{Q}$ fixes $\bar{R}$. Since $\bar{\mathscr{X}}$ is rational, this yields $\bar{P} = \bar{R}$. Therefore, $\Omega_2 \cup \{P\}$ is contained in Δ, and either $\Delta = \Omega_2 \cup \{P\}$ or Δ contains a long Q-orbit. In the latter case, $|U| < |Q| < |N|$, and hence

$$|G|^2 = |N||Q||N||U||Q||U| < |N||Q||N||U||N|^2 \leq \frac{64^2}{34}(\mathfrak{g}(\mathscr{X})-1)^3$$

whence $|G| < 34(\mathfrak{g}(\mathscr{X})+1)^{3/2}$, a contradiction with our hypothesis. Otherwise $|N| = |\Delta| = 1 + |\Omega_2|$. In particular, $|N|$ is even, and hence it is a power of 2. Also, by (5), $\mathfrak{g}(\mathscr{X}) - 1 = \gamma(\mathscr{X}) - 1 = -|Q| + 1 + |\Omega_2|$ where $|\Omega_2| \geq 1$ is a power of p. This implies that $\mathfrak{g}(\mathscr{X})$ is also even. Since N is an elementary abelian 2-group, Lemma 2.13 yields that either $|N| = 2$ or $|N| = 4$.

If $|N| = 2$, then Ω_2 consists of a unique point R and $Q \rtimes U$ fixes both points P and R. Since $\Delta = \{P, R\}$, and Δ is a G-orbit, the stabilizer $G_{P,R}$ is an index-2 (normal) subgroup of G. On the other hand, $G_{P,R} = Q \rtimes U$ and hence Q is the unique Sylow p-subgroup of $Q \rtimes U$. Thus, Q is a characteristic subgroup of the normal subgroup $G_{P,R}$ of G. But then Q is a normal subgroup of G, a contradiction with our hypothesis.

If $|N| = 4$, then $|\Delta| = 4$ and $p = 3$. The permutation representation of G of degree 4 on Δ contains a 4-cycle induced by N but also a 3-cycle induced by Q. Hence, if $K = \ker$, then $G/K \cong \mathrm{Sym}_4$. On the other hand, since both N and Ker are normal subgroups of G, their product NK is normal, as well. Hence, NK/K is a normal subgroup of G/K, but this contradicts $G/K \cong \mathrm{Sym}_4$. □

References

[Giulietti and Korchmáros 2014] M. Giulietti and G. Korchmáros, "Garden of curves with many automorphisms", pp. 93–120 in *Algebraic curves and finite fields*, edited by H. Niederreiter et al., Radon Ser. Comput. Appl. Math. **16**, de Gruyter, Berlin, 2014. MR Zbl

[Gunby et al. 2015] B. Gunby, A. Smith, and A. Yuan, "Irreducible canonical representations in positive characteristic", *Res. Number Theory* **1** (2015), art. id. 3. MR Zbl

[Henn 1978] H.-W. Henn, "Funktionenkörper mit großer Automorphismengruppe", *J. Reine Angew. Math.* **302** (1978), 96–115. MR Zbl

[Hirschfeld et al. 2008] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*, Princeton Univ., 2008. MR Zbl

[Homma 1980] M. Homma, "Automorphisms of prime order of curves", *Manuscripta Math.* **33**:1 (1980), 99–109. MR Zbl

[Kontogeorgis and Rotger 2008] A. Kontogeorgis and V. Rotger, "On abelian automorphism groups of Mumford curves", *Bull. Lond. Math. Soc.* **40**:3 (2008), 353–362. MR Zbl

[Korchmáros et al. 2018] G. Korchmáros, M. Montanucci, and P. Speziali, "Transcendence degree one function fields over a finite field with many automorphisms", *J. Pure Appl. Algebra* **222**:7 (2018), 1810–1826. MR Zbl

[Lidl and Niederreiter 1983] R. Lidl and H. Niederreiter, *Finite fields*, Encycl. Math. Appl. **20**, Addison-Wesley, Reading, MA, 1983. MR Zbl

[Machì 2012] A. Machì, *Groups: an introduction to ideas and methods of the theory of groups*, Unitext **58**, Springer, 2012. MR Zbl

[Nakajima 1987] S. Nakajima, "p-ranks and automorphism groups of algebraic curves", *Trans. Amer. Math. Soc.* **303**:2 (1987), 595–607. MR Zbl

[Neftin and Zieve 2015] D. Neftin and M. E. Zieve, "Solvable covers with many rational points", preprint, 2015, Available at https://neftin.net.technion.ac.il/files/2015/10/many-12-9-13.pdf.

[Serre 1962] J.-P. Serre, *Corps locaux*, Publ. Inst. Math. Univ. Nancago **8**, Hermann, Paris, 1962. MR Zbl

[Serre 1979] J.-P. Serre, *Local fields*, Graduate Texts in Math. **67**, Springer, 1979. MR Zbl

[Stichtenoth 1973] H. Stichtenoth, "Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik, II: Ein spezieller Typ von Funktionenkörpern", *Arch. Math.* (*Basel*) **24** (1973), 615–631. MR Zbl

[Sullivan 1975] F. J. Sullivan, "p-torsion in the class group of curves with too many automorphisms", *Arch. Math.* (*Basel*) **26** (1975), 253–261. MR Zbl

[Valentini and Madan 1980] 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. MR Zbl

Communicated by Gavril Farkas
Received 2016-10-25 Revised 2018-10-18 Accepted 2018-11-20

gabor.korchmaros@unibas.it *Dipartimento di Matematica, Informatica ed Economia, Università degli Studi della Basilicata, Potenza, Italy*

mariamontanucci@gmail.com *Dipartimento di Tecnica e Gestione dei Sistemi Industriali, Università degli Studi di Padova, Vicenza, Italy*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2019 is US \$385/year for the electronic version, and \$590/year (+\$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 13 No. 1 2019