Large 3-groups of automorphisms of algebraic curves in characteristic 3

Massimo Giulietti and Gábor Korchmáros

December 19, 2013

Abstract

Let S be a p-subgroup of the $\mathbb{K}$-automorphism group $\mathrm{Aut}(\mathcal{X})$ of an algebraic curve $\mathcal{X}$ of genus $\mathfrak{g} \geq 2$ and p-rank γ defined over an algebraically closed field $\mathbb{K}$ of characteristic $p \geq 3$. In this paper we prove that if $|S| > 2(\mathfrak{g}-1)$ then one of the following cases occurs.

(i) $\gamma = 0$ and the extension $\mathbb{K}(\mathcal{X})/\mathbb{K}(\mathcal{X})^S$ completely ramifies at a unique place, and does not ramify elsewhere.

(ii) $\gamma > 0$, $p = 3$, $\mathcal{X}$ is a general curve, S attains the Nakajima's upper bound $3(\gamma-1)$ and $\mathbb{K}(\mathcal{X})$ is an unramified Galois extension of the function field of a general curve of genus 2 with equation $Y^2 = cX^6 + X^4 + X^2 + 1$ where $c \in \mathbb{K}^*$.

Case (i) was investigated by Stichtenoth, Lehr, Matignon, and Rocher, see [18, 11, 12, 15, 16].

1 Introduction

In the present paper, $\mathbb{K}$ is an algebraically closed field of characteristic $p \geq 3$, $\mathcal{X}$ is a (projective, non-singular, geometrically irreducible, algebraic) curve of genus $\mathfrak{g}(\mathcal{X}) \geq 2$ with function field $\mathbb{K}(\mathcal{X})$, $\mathrm{Aut}(\mathcal{X})$ is the $\mathbb{K}$-automorphism group of $\mathcal{X}$, and S is a (non-trivial) subgroup of $\mathrm{Aut}(\mathcal{X})$ whose order is a power of p.

The earliest results on the maximum size of S date back to the 1970's and have played an important role in the study of curves with large automorphism groups exceeding the classical Hurwitz bound $84(\mathfrak{g}(\mathcal{X})-1)$. Stichtenoth proved that if S fixes a place $\mathcal{P}$ of $\mathbb{K}(\mathcal{X})$ then

$$|S| \leq \frac{p}{p-1}\,\mathfrak{g}(\mathcal{X}) \tag{1}$$

unless the extension $\mathbb{K}(\mathcal{X}) : \mathbb{K}(\mathcal{X})^S$ completely ramifies at $\mathcal{P}$, and does not ramify elsewhere; in geometric terms, S fixes a point P of $\mathcal{X}$ and acts on $\mathcal{X} \setminus \{P\}$ as a semiregular permutation group; see [18] and also [10, Theorem 11.78]. In the latter case, the Stichtenoth bound is

$$|S| \leq \frac{4p}{p-1}\,\mathfrak{g}(\mathcal{X})^2. \tag{2}$$

In his 1987 paper [13] Nakajima pointed out that the maximum size of S is related to the Hasse-Witt invariant $\gamma(\mathcal{X})$ of $\mathcal{X}$. It is known that $\gamma(\mathcal{X})$ coincides with the p-rank of $\mathcal{X}$ defined to be the rank of the (elementary abelian) group of the p-torsion points in the Jacobian variety of $\mathcal{X}$; moreover, $\gamma(\mathcal{X}) \leq \mathfrak{g}(\mathcal{X})$

and when equality holds then $\mathcal{X}$ is called an *ordinary* (or *general*) curve; see [10, Section 6.7]. If S fixes a point and (1) fails then $\gamma(\mathcal{X}) = 0$; conversely, if $\gamma(\mathcal{X}) = 0$, then S fixes a point, see [10, Lemma 11.129]. For $\gamma(\mathcal{X}) > 0$, Nakajima proved that $|S|$ divides $\mathfrak{g}(\mathcal{X}) - 1$ when $\gamma(\mathcal{X}) = 1$, and $|S| \leq p/(p-2)(\gamma(\mathcal{X}) - 1)$ otherwise; see [13] and also [10, Theorem 11.84]. Therefore, the Nakajima bound [13, Theorem 1] is

$$|S| \leq \begin{cases} p/(p-2)\,(\mathfrak{g}(\mathcal{X}) - 1) & \text{for} \quad \gamma(\mathcal{X}) > 1, \\ \mathfrak{g}(\mathcal{X}) - 1 \quad \text{for} \quad \gamma(\mathcal{X}) = 1. \end{cases} \tag{3}$$

In this context, a major issue is to determine the possibilities for $\mathcal{X}$, $\mathfrak{g}$ and S when either $|S|$ is close to the Stichtenoth bound (2), or $|S|$ is close to the Nakajima bound (3).

Lehr and Matignon [11] investigated the case where S fixes a point and were able to determine all curves $\mathcal{X}$ with

$$|S| > \frac{4}{(p-1)^2}\, g^2, \tag{4}$$

proving that (4) only occurs when the curve is birationally equivalent over $\mathbb{K}$ to an Artin-Schreier curve of equation $Y^q - Y = f(X)$ such that $f(X) = XS(X) + cX$ where $S(X)$ is an additive polynomial of $\mathbb{K}[X]$. Later on, Matignon and Rocher [12] showed that the action of a p-subgroup of $\mathbb{K}$-automorphisms S satisfying

$$|S| > \frac{4}{(p^2-1)^2}\, g^2,$$

corresponds to the étale cover of the affine line with Galois group $S \cong (\mathbb{Z}/p\mathbb{Z})^n$ for $n \leq 3$. These results have been refined by Rocher, see [15] and [16]. The essential tools used in the above mentioned papers are ramification theory and some structure theorems about finite p-groups.

Curves close to the Nakajima bound are investigated in this paper. The main result is stated in the following theorem.

Theorem 1.1. *Let S be a p-subgroup of the $\mathbb{K}$-automorphism group* $\mathrm{Aut}(\mathcal{X})$ *of an algebraic curve $\mathcal{X}$ of genus $\mathfrak{g}(\mathcal{X}) \geq 2$ defined over an algebraically closed field $\mathbb{K}$ of characteristic $p \geq 3$. If*

$$|S| > 2(\mathfrak{g}(\mathcal{X}) - 1) \tag{5}$$

then one of the following cases occurs:

(i) $\gamma = 0$ *and the extension $\mathbb{K}(\mathcal{X})/\mathbb{K}(\mathcal{X})^S$ completely ramifies at a unique place, and does not ramify elsewhere.*

(ii) $\gamma > 0$*, $p = 3$, $\mathcal{X}$ is a general curve, S attains the Nakajima's upper bound* $3(\gamma - 1)$ *and* $\mathbb{K}(\mathcal{X})$ *is an unramified Galois extension of the function field of a general curve of genus* 2 *with equation* $Y^2 = cX^6 + X^4 + X^2 + 1$ *where $c \in \mathbb{K}^*$.*

The analogous problem for 2-groups of automorphisms S in characteristic $p = 2$ was investigated in [4].

One may also ask how the above results may be refined when $\mathrm{Aut}(\mathcal{X})$ is larger than S. So far, this problem has been investigated for zero p-rank curves $\mathcal{X}$ such that $\mathrm{Aut}(\mathcal{X})$ fixes no point of $\mathcal{X}$; see [5, 6, 7].

2 Background and Preliminary Results

Let $\bar{\mathcal{X}}$ be a non-singular model of $\mathbb{K}(\mathcal{X})^S$, that is, a projective non-singular geometrically irreducible algebraic curve with function field $\mathbb{K}(\mathcal{X})^S$, where $\mathbb{K}(\mathcal{X})^S$ consists of all elements of $\mathbb{K}(\mathcal{X})$ fixed by every element in S.

Usually, $\bar{\mathcal{X}}$ is called the quotient curve of $\mathcal{X}$ by S and denoted by $\mathcal{X}/S$. The field extension $\mathbb{K}(\mathcal{X})/\mathbb{K}(\mathcal{X})^S$ is Galois of degree $|S|$.

Let $\bar{P}_1,\ldots,\bar{P}_k$ be the points of the quotient curve $\bar{\mathcal{X}}=\mathcal{X}/S$ where the cover $\mathcal{X}\mapsto\bar{\mathcal{X}}$ ramifies. For $1\le i\le k$, let L_i denote the set of points of $\mathcal{X}$ which lie over $\bar{P}_i$. In other words, $L_1,\ldots,L_k$ are the short orbits of S on its faithful action on $\mathcal{X}$. Here the orbit of $P\in\mathcal{X}$

$$o(P)=\{Q\mid Q=P^g,\, g\in S\}$$

is *long* if $|o(P)|=|S|$, otherwise $o(P)$ is *short*. It may be that S has no short orbits. This is the case if and only if every non-trivial element in S is fixed–point-free on $\mathcal{X}$. On the other hand, S has a finite number of short orbits.

If P is a point of $\mathcal{X}$, the stabilizer S_P of P in S is the subgroup of S consisting of all elements fixing P. For a non-negative integer i, the i-th ramification group of $\mathcal{X}$ at P is denoted by $S_P^{(i)}$ (or $S_i(P)$ as in [19, Chapter IV]) and defined to be

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

where t is a uniformizing element (local parameter) at P. Here $S_P^{(0)}=S_P^{(1)}=S_P$.

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

$$2\mathfrak{g}-2=|S|(2\bar{\mathfrak{g}}-2)+\sum_{P\in\mathcal{X}}d_P. \tag{6}$$

where

$$d_P=\sum_{i\ge 0}(|S_P^{(i)}|-1). \tag{7}$$

Let γ be the p-rank of $\mathcal{X}$, and let $\bar{\gamma}$ be the p-rank of the quotient curve $\bar{\mathcal{X}}=\mathcal{X}/S$. The Deuring-Shafarevich formula, see [23] or [10, Theorem 11,62], states that

$$\gamma-1=|S|(\bar{\gamma}-1)+\sum_{i=1}^{k}(|S|-\ell_i) \tag{8}$$

where $\ell_1,\ldots,\ell_k$ are the sizes of the short orbits of S. If G has no short orbits, that is, the Galois extension $\mathbb{K}(\mathcal{X})$ of $\mathbb{K}(\bar{\mathcal{X}})$ is unramified, then G can be generated by $\bar{\gamma}$ elements by Shafarevich's theorem [20, Theorem 2], whereas the largest elementary abelian subgroup of G has rank at most $\bar{\gamma}$ see [14, Section 4.7].

The following result is a special case of the classification of automorphism groups of genus 2 curves due to Igusa [9, Section 8] and refined in [2, Section 1]; see also [21, Lemma 1], and [3].

Proposition 2.1. *Let G be the automorphism group of a genus 2 curve $\mathcal{C}$ in characteristic 3. If 3 divides $|G|$, then either $G\cong D_{12}$, or $G\cong GL(2,3)$, and $\mathcal{C}$ is a non-singular model of an irreducible plane curve of equation $Y^2=cX^6+X^4+X^2+1$ where $c\in\mathbb{K}^*$ with $c=1$ when $G\cong GL(2,3)$.*

Remark 2.2. An equivalent equation for $\mathcal{C}$ in Proposition 2.1 is

$$X(Y^3-Y)-X^2+c=0, \tag{9}$$

and the linear map $(X,Y)\mapsto(X,Y+1)$ is an automorphism of $\mathcal{C}$.

From group theory we use the following results, see for instance [24].

Proposition 2.3. *Let G be a non-abelian group of order 27. Then either $G \cong C_9 \rtimes C_3$ or $G \cong UT(3,3)$ where $UT(r,3)$ denotes the group of upper-triangular unipotent $r \times r$ matrices over the field with three elements.*

From Projective geometry, the following known result is used. For the sake of completeness we include a proof.

Lemma 2.4. *In the r-dimensional projective space $PG(r,\mathbb{K})$ over an algebraically closed field $\mathbb{K}$ of characteristic p, let S be a finite p-subgroup of $PGL(r+1,\mathbb{K})$. If $r \geq 2$ then S preserves a flag*

$$\Pi_0 \subset \Pi_1 \subset \ldots \subset \Pi_{r-1}$$

where Π_i is an i-dimensional projective subspace of $PG(r,\mathbb{K})$.

Proof. In $PG(2,\mathbb{K})$, any p-subgroup of $PGL(3,\mathbb{K})$ fixes an incident point-line pair. Hence, the claim holds for $r = 2$. We prove it for $r \geq 3$ by induction on r.

We first show that S fixes a point of $PG(r,\mathbb{K})$. Take a non-trivial element s in the center $Z(S)$ of S. Since $\mathbb{K}$ is algebraically closed, s fixes some points of $PG(r,\mathbb{K})$. If s has a unique fixed point, then S itself fix that point. Therefore, we may assume that s has more than one fixed point. Since s has order a power of p, the set of its fixed points is a proper projective subspace Π of $PG(r,\mathbb{K})$. From $s \in Z(S)$ it follows that S preserves Π. By the inductive hypothesis, S fixes a point in Π, and hence in $PG(r,\mathbb{K})$.

Now, let $P \in PG(r,\mathbb{K})$ be a fixed point of S. The linear system of hyperplanes through P is a projective space $PG(r-1,\mathbb{K})$ over $\mathbb{K}$, and S acts on $PG(r-1,\mathbb{K})$, not necessarily faithfully, as a p-subgroup S_1 of $PGL(r,\mathbb{K})$. From what we have already proven, S_1 fixes a point Q of $PG(r-1,\mathbb{K})$. Therefore, Q regarded as a hyperplane Π_{r-1} of $PG(r,\mathbb{K})$ through P is preserved by S. From the inductive hypothesis on r, S has an invariant flag $\Pi_0 \subset \Pi_1 \subset \ldots \subset \Pi_{r-2}$. This together with Π_{r-1} gives an S-invariant flag in $PG(r,\mathbb{K})$. □

3 The action of S on $\mathcal{X}$

In this section, $\mathcal{X}$ stands for a curve which satisfies the hypotheses of Theorem 1.1 but does not have the property given in (i) of Theorem 1.1.

Proposition 3.1. *The following results hold:*

(I) $p = 3$,

(II) *S fixes no point in $\mathcal{X}$,*

(III) $\gamma(\mathcal{X}) > 0$.

Proof. (II) holds, otherwise comparing (5) with (1) would yield (i) of Theorem 1.1. From this (III) follows by [10, Lemma 11.129]. In particular, (3) applies, and comparing (5) with (3) gives (I). □

Proposition 3.2. *$\mathcal{X}$ is an ordinary curve with $\mathfrak{g}(\mathcal{X}) - 1 = \frac{1}{3}|S|$. Moreover, S has exactly two short orbits on $\mathcal{X}$, both of length $\frac{1}{3}|S|$, and if $|S| > 3$ then the identity is the unique element in S fixing every point of $\Omega_1 \cup \Omega_2$.*

Proof. Let $\mathfrak{g} = \mathfrak{g}(\mathcal{X})$ and $\gamma = \gamma(\mathcal{X})$. Our hypothesis (5) yields $\gamma \geq 2$ by (3). Let $\bar{\gamma}$ be the 3-rank of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/S$. From (8),

$$\gamma - 1 = \bar{\gamma}|S| - |S| + \sum_{i=1}^{k}(|S| - \ell_i) = (\bar{\gamma} + k - 1)|S| - \sum_{i=1}^{k} \ell_i \geq (\bar{\gamma} + \frac{2}{3}k - 1)|S|, \tag{10}$$

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

If no such short orbits exist, then $\gamma - 1 = |S|(\bar{\gamma} - 1)$ whence $\bar{\gamma} > 1$ by $\gamma \geq 2$. Therefore, $|S| \leq \gamma - 1 \leq \mathfrak{g} - 1$ contradicting (5).

Hence $k \geq 1$, and if $\bar{\gamma} \geq 1$ then (10) yields that $|S| \leq \frac{3}{2}(\gamma - 1) \leq \frac{3}{2}(\mathfrak{g} - 1)$ contradicting (5). So, $\bar{\gamma} = 0$, and (10) together with (5) imply that $k < \frac{9}{4}$ whence $1 \leq k \leq 2$. The case $k = 1$ cannot actually occur by (10).

Therefore, $\bar{\gamma} = 0$ and $k = 2$. Let Ω_1 and Ω_2 be the short orbits of S, and let $\ell_i = |\Omega_i|$ for $i = 1, 2$. Then (10) reads

$$\gamma - 1 = |S| - (\ell_1 + \ell_2) \tag{11}$$

whence $|S| > 2(\gamma - 1) = 2|S| - 2(\ell_1 + \ell_2)$. Also, $\ell_1 + \ell_2 < |S|$. Write $|S| = 3^h, \ell_1 = 3^m, \ell_2 = 3^r$ with $h > m \geq r$. Then $3^m + 3^r < 3^h < 2(3^m + 3^r)$. Here $r > 0$ by (II) of Proposition 3.1. Therefore $3^{m-r} + 1 < 3^{h-r} < 2(3^{m-r} + 1)$. Since $h > m \geq r$, this yields $m = r$, that is, $\ell_1 = \ell_2$, and $h = r + 1$. In other words, $\ell_1 = \ell_2 = \frac{1}{3}|S|$. From (11), $\gamma - 1 = \frac{1}{3}|S|$.

Let $\bar{\mathfrak{g}}$ be the genus of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/S$. The Hurwitz genus formula, (6) and (7), applied to S gives

$$2\mathfrak{g} - 2 = |S|(2\bar{\mathfrak{g}} - 2) + \tfrac{2}{3}|S|(4 + k_1 + k_2) \tag{12}$$

where, for a point $P_i \in \Omega_i$, k_i is the smallest non-negative integer such that $|S_{P_i}^{2+k_i}| = 1$. Suppose on the contrary that $\mathcal{X}$ is not an ordinary curve, that is, $\mathfrak{g} > \gamma$. Then $k_1 + k_2 \geq 1$. From (12), $2\mathfrak{g} - 2 \geq -2|S| + \frac{10}{3}|S| = \frac{4}{3}|S|$ contradicting (5).

Assume that a non-trivial element s of S fixes $\Omega_1 \cup \Omega_2$ pointwise. From the Deuring-Shafarevic formula (8) applied to $\langle s \rangle$,

$$|s| = \frac{1}{3}\,|S|(2|s| - 3),$$

which is only possible for $|s| = |S| = 3$. □

From now on, Ω_1 and Ω_2 denote the short orbits of S on $\mathcal{X}$. By the second claim of Proposition 3.2,

$$|S_P| = 3 \text{ for } P \in \Omega_1 \cup \Omega_2. \tag{13}$$

Proposition 3.3. *If S is abelian then either $|S| = 3$, or $|S| = 9$ and S is elementary abelian.*

Proof. For a point $P \in \Omega_1$, the stabilizer S_P of P in S is a subgroup of order 3. Since S is abelian, S_P fixes every point in Ω_1. Let γ^* be the 3-rank of the quotient curve $\mathcal{X}/S_P$. From (8) and Proposition 3.2,

$$\tfrac{1}{3}|S| = \gamma - 1 \geq 3(\gamma^* - 1) + \tfrac{2}{3}|S| \geq \tfrac{2}{3}|S| - 3$$

whence $|S| = 9$ and $\mathfrak{g} = \gamma = 4$. Assume on the contrary that S is cyclic. For a point $Q \in \Omega_2$ the stabilizer S_Q is a subgroup of S of order 3. Since S is cyclic, it has only one subgroup of order 3. Therefore $S_P = S_Q$, and

$$\tfrac{1}{3}|S| = \gamma - 1 \geq 3(\gamma^* - 1) + \tfrac{2}{3}|S| + \tfrac{2}{3}|S| \geq \tfrac{4}{3}|S| - 3,$$

which implies $|S| = 1$, a contradiction. □

Proposition 3.4. *Assume that $|S| \geq 9$. Let N be a non-trivial normal subgroup of S. Then either N is semiregular on $\mathcal{X}$, or $S = N \rtimes \langle \varepsilon \rangle$ with $\varepsilon^3 = 1$.*

Proof. The assertion trivially holds for $|S| = 9$. Assume that some non-trivial element in N fixes point P. From the Hurwitz genus formula applied to N, we have $\frac{1}{3}|S| > |N|(\bar{\mathfrak{g}} - 1)$ where $\bar{\mathfrak{g}}$ is the 3-rank of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$. Let $\bar{S}$ be the automorphism group of $\bar{\mathcal{X}}$ induced by S. Then $|\bar{S}||N| = |S|$ and hence $\frac{1}{3}|\bar{S}| > \bar{\mathfrak{g}} - 1$. Assume that $\bar{\mathfrak{g}} \geq 2$. Then (I) holds for $\bar{S}$. If (II) were also true for $\bar{S}$ then Proposition 3.2 would imply $|\bar{S}| = 3(\mathfrak{g} - 1)$. So, $\bar{S}$ fixes a point in $\bar{\mathcal{X}}$. This remains true when $\bar{\gamma} = 0$. Let $\bar{Q} \in \bar{\mathcal{X}}$ be such a fixed point. Then the orbit $\mathcal{O}$ of N consisting of all points of $\mathcal{X}$ lying over $\bar{Q}$ is also an orbit of S. Since Ω_1 and Ω_2 are the only short orbits of S, this yields that either $\mathcal{O}$ coincides with one of them, say Ω_1 Therefore, $|N| = \frac{1}{3}|S|$. The stabilizer ε of a point $R \in \Omega_2$ on S has order 3 and $\varepsilon \notin N$. Therefore $S = N \rtimes \langle \varepsilon \rangle$. We are left with the case $\bar{\mathfrak{g}} = \bar{\gamma} = 1$. Let $\mathcal{O}_1, \ldots, \mathcal{O}_m$ be the short orbits of N. Since the stabilizer N_Q of any point $Q \in \mathcal{O}_i$ has order 3, (8) applied to N gives

$$\frac{1}{3}|S| = |\gamma - 1) = \frac{2}{3}|N|m$$

whence $|S| = 2|N|m$. But this is impossible as $|S|$ is a power of 3. □

Proposition 3.5. *If $|S| > 9$ then the center $Z(S)$ of S is semiregular on $\mathcal{X}$.*

Proof. Since $Z(S)$ is a normal subgroup of S, Proposition 3.4 applies to $Z(S)$. The case $S = Z(S) \rtimes \langle \varepsilon \rangle$ cannot actually occur since this semidirect product would be direct and S would be abelian contradicting Proposition 3.3. □

Proposition 3.6. *Let N be a normal subgroup of G such that $|N| \leq \frac{1}{9}|S|$. Then the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$ with $\bar{S} = S/N$ and $\mathfrak{g}(\bar{\mathcal{X}}) - 1 = (\mathfrak{g} - 1)/|N|$ satisfies the hypotheses of Theorem 1.1 but does not have the property given in* (i) *of Theorem 1.1.*

Proof. By Proposition 3.4, the Galois p-extension of $\bar{\mathcal{X}}$ with Galois group $\bar{G}$ is unramified. Therefore, the Deuring-Shafarevic formula applied to $\bar{G}$ gives that $\mathfrak{g} - 1 = |\bar{G}|(\bar{\mathfrak{g}} - 1)$. □

Since the center of any p-group is non-trivial, a straightforward inductive argument on $|S|$ depending on Proposition 3.6 gives the following result.

Proposition 3.7. *If there exists a curve which satisfies the hypothesis of Theorem 1.1 for $|S| = 3^k$ but does not have the property* (i)*, then for any $1 \leq j < k$ there also exists a curve which satisfies the hypothesis of Theorem 1.1 for $|S| = 3^j$ but does not have the property* (i).

Proposition 3.8. *Let N be a non-trivial normal subgroup of S. If the factor group S/N is a abelian then either $|N| = \frac{1}{3}|S|$ or $|N| = \frac{1}{9}|S|$, and in the latter case, S/N is an elementary abelian group.*

Proof. The assertion is a corollary of Propositions 3.4 and 3.6. □

Proposition 3.9. *If $|S| \geq 9$ then the following hold.*

(i) $\Phi(S) = S'$.

(ii) $|\Phi(S)| = \frac{1}{9}|S|$.

(iii) *S contains exactly four maximal subgroups, each being a normal subgroup of S of index* 3.

(iv) *Exactly two of the four maximal subgroups of S are semiregular on $\mathcal{X}$.*

(v) *S can be generated by two elements.*

Proof. From Proposition 3.8, either $|S'| = \frac{1}{3}|S|$, or $|S'| = \frac{1}{9}|S|$. In the former case, S is cyclic by [8, Hilfssatz 7.1.b] but this contradicts Proposition 3.3. Therefore, $|S'| = \frac{1}{9}|S|$. Since S/S' is elementary abelian by Proposition 3.8, (i) holds. From this (ii) follows. Let φ be the natural homomorphism $S \mapsto S/\Phi(S)$. Since every maximal subgroup of S contains $\Phi(S)$, there is a one-to-one correspondence between the maximal subgroups of S and the subgroups of $S/\Phi(S)$. By (ii), $S/\Phi(S)$ is an elementary abelian group of order 9 with exactly four proper subgroups. Therefore there are exactly four maximal subgroups in S. Also, the subgroups of $S/\Phi(S)$ are normal, and hence each of the four maximal subgroups of S is normal, as well. Furthermore, the four maximal subgroups of $S/\Phi(S)$ partition the set of non-trivial elements of $S/\Phi(S)$. Hence every element of $S \setminus \Phi(S)$ belongs to exactly one of the four maximal subgroups of S. Take a point $P \in \Omega_1$, and let M_1 be the maximal subgroup of S containing S_P. Since M is a normal subgroup of S and Ω_1 is an S-orbit, this yields that M contains S_Q for every $Q \in \Omega_1$. Repeating the above argument for a point in Ω_2 shows that a maximal normal subgroup contains the stabilizer of each point in Ω_2. From the last claim of Proposition 3.2, these two maximal subgroups are distinct. Therefore, the remaining two maximal subgroups are both semiregular on $\mathcal{X}$.

Finally, (i) together with the Burnside fundamental theorem, [8, Chapter III, Satz 3.15] imply that S can be generated by two elements. $\square$

From now on, the following notation is used: For $i = 1, 2$, M_i denotes the maximal normal subgroup of S containing the stabilizer of a point of Ω_i while M_3 and M_4 stand for the semiregular maximal subgroups of S, respectively. Proposition 3.4 has the following corollary.

Proposition 3.10. *Neither M_1 nor M_2 is cyclic.*

Proposition 3.11. *Every normal subgroup of S whose order is at most $\frac{1}{9}|S|$ is contained in $\Phi(S)$.*

Proof. Let N be a normal subgroup of S. From [8, Chapter III, Hilfssatz 3.4.a], $\Phi(S)N/N$ is a subgroup of $\Phi(S/N)$. From Propositions 3.6 and Proposition 3.9 applied to $\bar{\mathcal{X}} = \mathcal{X}/N$, we have $|\Phi(S/N)| = \frac{1}{9}|S|/|N|$. Since $\Phi(S)/(\Phi(S) \cap N) \cong \Phi(S)N/N$, this yields $|N| \leq |\Phi(S) \cap N|$. Therefore, if $|N| \leq |\Phi(S)|$ then N is contained in $\Phi(S)$. $\square$

Proposition 3.12. *If M_i is abelian for some $1 \leq i \leq 4$, then S has maximal class.*

Proof. By (i) of Proposition 3.9, the assertion follows from an elementary result, see for instance [27, Theorem 5.2]. $\square$

It should be noted that p-groups of maximal class have intensively investigated, see [8] and [1].

Proposition 3.13. *If $|S| > 3$ then $\mathcal{X}$ is not hyperelliptic.*

Proof. Since the length of any S-orbit in $\mathcal{X}$ is divisible by 3, the number of distinct Weierstrass points of $\mathcal{X}$ is also divisible by 3. On the other hand, a hyperelliptic curve of genus g defined over a field of zero or odd characteristic has as many as $2g + 2$ Weierstrass points, see [10, Theorem 7.103]. Therefore, if $\mathcal{X}$ were hyperelliptic, both numbers $2g + 2$ and $2g - 2 = \frac{2}{3}|S|$ would be divisible by 3, a contradiction. $\square$

Proposition 3.14. *If $|S| = 27$ then $S \cong UT(3, 3)$.*

Proof. If $|S| = 27$ then either $S = C_9 \rtimes C_3$, or S is isomorphic to the group $UT(3,3)$ of all upper-triangular unipotent 3×3 matrices over the field with three elements. Since the group $C_9 \rtimes C_3$ has only one non-cyclic maximal subgroup, the assertion follows from Proposition 3.10. $\square$

Proposition 3.15. *If $|S| \geq 81$ then S is not metacyclic.*

Proof. We show that S has a normal subgroup of index 27. This is certainly true when M_3 is cyclic. Otherwise, M_3 can be generated by two elements, and its Frattini subgroup $\Phi(M_3)$ has index 27 in S. Since $\Phi(M_3)$ is a characteristic subgroup of M_3 and M_3 is a normal subgroup of S, $\Phi(M_3)$ has the required property. From Proposition 3.6 applied to $N = \Phi(M_3)$ shows that $\bar{S} = S/\Phi(M_3)$ is a subgroup of $\mathrm{Aut}(\bar{\mathcal{X}})$ with $\mathcal{X}$ the quotient curve of $\bar{\mathcal{X}} = \mathcal{X}/\Phi(M_3)$. Since $\Phi(M_3)$ is semiregular on $\mathcal{X}$ by Proposition 3.4, $\bar{\mathcal{X}}$ has genus 10. As $|\bar{S}| = 27$, Proposition 3.14 implies that $\bar{S} \cong UT(3,3)$. In particular, $\bar{S}$ is not metacyclic. Since every factor group of a metacylic group is still metacyclic, the assertion follows. $\square$

4 Small genera

4.1 Cases $|S| = 3, 9$

We prove that if $\mathcal{X}$ satisfies the hypotheses of Theorem 1.1 for $|S| = 3$ then (ii) holds. For this case, our hypothesis (5) yields $\mathfrak{g} = 2$. From (8), every automorphism of $\mathrm{Aut}(\mathcal{X})$ of order 3 has two fixed points on $\mathcal{X}$. Therefore, (i) of Theorem 1.1 cannot occur, and the assertion follows from Proposition 2.1.

From now on, $|S| = 9$ and $\mathcal{X}$ is a curve satisfying the hypotheses of Theorem 1.1 but does not have the property given in (i) of Theorem 1.1. We prove that then (iii) holds. From Propositions 3.2 and 3.3, $\mathcal{X}$ is an ordinary curve of genus $\mathfrak{g} = 4$ with an elementary abelian subgroup S of $\mathrm{Aut}(\mathcal{X})$ of order 9.

Let N be the kernel of the permutation representation of S on $\Omega_1 \cup \Omega_2$. If N is not trivial then it has order 3, and the Hurwitz genus formula (6) and (7) applied to N gives $6 = 2(\mathfrak{g}-1) \geq 6(\bar{\mathfrak{g}}-1)+24$. Therefore S acts on $\Omega_1 \cup \Omega_2$ faithfully.

By Proposition 3.13, $\mathcal{X}$ is assumed to be a canonical curve embedded in $PG(3,\mathbb{K})$. Then S extends to a subgroup of $PG(3,\mathbb{K})$ which preserves $\mathcal{X}$ and acts on $\mathcal{X}$ faithfully.

According to Lemma 2.4, choose the projective coordinate system $(X_0 : X_1 : X_2 : X_3)$ in $PG(3,\mathbb{K})$ in such a way that S preserves the canonical flag

$$P_0 \subset \Pi_1 \subset \Pi_2$$

where $P_0 = (1:0:0:0)$, Π_1 is the line through P_0 and $P_1 = (0:1:0:0)$ while Π_2 is the plane of equation $X_3 = 0$. Here $P_0 \notin \mathcal{X}$, since S fixes no point in $\mathcal{X}$. Moreover, $\Pi_2 \cap \mathcal{X} = \Omega_1 \cup \Omega_2$. In fact, for any point $R \in \Pi_2 \cap \mathcal{X}$, Proposition 3.2 implies that the S-orbit of R has size 9 unless $R \in \Omega_1 \cup \Omega_2$. On the other hand S preserves $\Pi_2 \cap \mathcal{X}$, and this implies that the S-orbit of R cannot exceed 6.

Lemma 4.1. *Both Ω_1 and Ω_2 consist of three collinear points.*

Proof. Assume on the contrary that Ω_1 is a triangle. Take $g \in S$ such that g fixes each vertex of Ω_1. Since g is a projectivity of $PG(3,\mathbb{K})$ it fixes Π_2 pointwise. As Π_2 also contains Ω_2, g must fix Ω_2 pointwise. But this is impossible as S acts on $\mathcal{X}$ faithfully. $\square$

As a corollary, $I(R, \mathcal{X} \cap \Pi_2) = 1$ for every point $R \in \Omega_1 \cup \Omega_2$. For $i = 1,2$, let r_i denote the line containing Ω_i. Their common point is fixed by S, and may be chosen for P_0. Let M be the subgroup of S which preserves every line through P_0. Since $\deg \mathcal{X} = 6$, no line meets $\mathcal{X}$ in more than six distinct points.

Therefore, either $|M| = 1$ or $|M| = 3$. In the latter case, M is an elation group of order 3 with center P_0. If Δ is its axis then every point in $\Delta \cap \mathcal{X}$ is fixed by M. Therefore Δ is not Π_2 and contains either r_1 or r_2. Since S is abelian, it preserves Δ and hence every plane through r_1. But then every S-orbit has length at most 3. A contradiction with Proposition 3.2. Hence M is trivial.

Since $P_0 \notin \mathcal{X}$, the linear system Σ of all planes through P_0 cuts out on $\mathcal{X}$ a linear series without fixed point. Therefore this effective linear series has dimension 2 and degree 6, and is denoted by g_2^6.

It might happen that g_2^6 is composed of an involution, and we investigate such a possibility. From [10, Section 7.4], there is a curve $\mathcal{Z}$ whose function field $\mathbb{K}(\mathcal{X})$ is an S-invariant proper subfield of $\mathbb{K}(\mathcal{X})$. Since no non-trivial element in S fixes every line through P_0 and hence every plane through P_0, S acts on $\mathcal{Z}$ faithfully. As the genus of $\mathcal{Z}$ is less than 4, applying (3) to $\mathcal{Z}$ gives $\gamma(\mathcal{Z}) = 0$. Therefore, every non-trivial element in S has a unique fixed point $\bar{T}$, see [10, Lemma 11.129]. From this, the support of the divisor of $K(\mathcal{X})$ lying over $\bar{T}$ contains the points in $\Omega_1 \cup \Omega_2$. Therefore, the line through P_0 and a point in $\Omega_1 \cup \Omega_2$ must contain all the points in $\Omega_1 \cup \Omega_2$. But this would imply that $r_1 = r_2$, a contradiction.

Therefore, g_2^6 is simple and without fixed point. The projection of $\mathcal{X}$ from P_0 is an irreducible plane curve $\mathcal{C}$ of degree 6 and genus 4 with two triple points R_1 and R_2 arising from Ω_1 and Ω_2, respectively. Here $\mathcal{C}$ and $\mathcal{X}$ are birationally equivalent, and S is a subgroup of $PGL(3, \mathbb{K})$ preserving $\mathcal{C}$. For $i = 1, 2$, a non-trivial projectivity $s_i \in S$ fixing Ω_i pointwise acts on $\mathcal{C}$ fixing the point R_i.

Choose the projective coordinate system $(X_0 : X_1 : X_2)$ in $PG(2, \mathbb{K})$ so that $R_1 = (0 : 0 : 1)$ and $R_2 = (0 : 1 : 0)$. In affine coordinates (X, Y) with $X = X_1/X_0$, $Y = X_2/X_0$, an equation of $\mathcal{C}$ is $f = 0$ with an irreducible polynomial $f \in \mathbb{K}[X, Y]$ of degree six. W.l.o.g. the origin $O = (0, 0)$ is the common point of two tangents to $\mathcal{C}$, say t_1 at R_1 and t_2 at R_2. Furthermore, $s_1(O) = (\lambda, 0)$, $s_2(O) = (0, \mu)$ with $\lambda, \mu \in \mathbb{K}^*$, and $\lambda = \mu = 1$ may be assumed. Thus $s_1 : (X, Y) \mapsto (X + 1, Y)$ and $s_2 : (X, Y) \mapsto (X, Y + 1)$. Hence

$$f(X + 1, Y) = f(X, Y), \quad f(X, Y + 1) = f(X, Y). \tag{14}$$

Since R_1 is a triple point of $\mathcal{C}$, there exist $h_0, h_1, h_2, h_3 \in \mathbb{K}[Y]$ such that

$$f(X, Y) = h_3X^3 + h_2X^2 + h_1X + h_0 = 0,$$

where $\deg h_0 \leq 2$ by the particular choice of t_2. From this and (14), the polynomial

$$f(X + 1, Y) - f(X, Y) = h_3 - h_2X + h_2 + h_1 \tag{15}$$

vanishes at every affine point of $\mathcal{C}$. Since $\mathcal{C}$ is not rational, this is only possible when (15) is the zero polynomial, that is, $h_2 = h_3 + h_1 = 0$. Thus $f(X, Y) = h_3(X^3 - X) + h_0$. The second mixed partial derivate is $f_{X,Y} = -dh_3/dY$. Similarly, as R_2 is a triple point of $\mathcal{C}$ there exist $k_0, k_3 \in \mathbb{K}[X]$ with $\deg k_0 \leq 2$ such that $f(Y, X) = k_3(Y^3 - Y) + k_0$. Since $f_{X,Y} = f_{Y,X}$, this yields $dh_3/dY = dk_3/dX$, whence dh_3/dY and dk_3/dX both have degree 0. Thus

$$h_3 = c_3Y^3 + c_1Y + c_0, \quad k_3 = d_3X^3 + d_1X + d_0$$

where $c_0, c_1, c_3, d_0, d_1, d_3 \in \mathbb{K}$. Therefore

$$(c_3Y^3 + c_1Y + c_0)(X^3 - X) + h_0 = (d_3X^3 + d_1X + d_0)(Y^3 - Y) + k_0.$$

Comparison of the coefficients of X^3 shows that $c_3 = -c_1, c_0 = 0$. Similarly, $d_3 = -d_1, d_0 = 0$. Thus

$$f(X, Y) = c(X^3 - X)(Y^3 - Y) + h_0 = d(Y^3 - Y)(X^3 - X) + k_0$$

where $c, d \in \mathbb{K}$. From this $(c-d)(X^3-X)(Y^3-Y) = k_0 - h_0$ whence $c = d$ and $k_0 = h_0 = u$ with $u \in \mathbb{K}^*$. Therefore

$$f(X,Y) = (X^3-X)(Y^3-Y) + c = 0$$

where $c \in \mathbb{K}^*$. This ends the proof of Theorem 1.1 for $|S| = 9$.

4.2 Case $|S| = 27$

We exhibit an explicit example. Let $\mathcal{X}$ be a non-singular model of the irreducible curve $\mathcal{Y}$ embedded in $PG(3,\mathbb{K})$ defined by the affine equations

(i) $(X^3-X)(Y^3-Y) - 1 = 0$;

(ii) $Z^3 - Z + X^3Y - XY^3 = 0$.

A straightforward Magma computation shows that $\mathfrak{g}(\mathcal{X}) = \gamma(\mathcal{X}) = 10$. Moreover, both maps

$$g: (X,Y,Z) \mapsto (X+1, Y, Z+Y) \quad h: (X,Y,Z) \mapsto (X, Y-1, Z+X)$$

are in $\mathrm{Aut}(\mathcal{X})$. They generate a non-abelian group S of order 27 and exponent 3. Therefore $S \cong UT(3,3)$. Actually, $\mathrm{Aut}(\mathcal{X})$ is larger than S since it also contains $r: (X,Y,Z) \mapsto (Y,X,Z)$. This shows that $\mathcal{X}$ satisfies the hypotheses of Theorem 1.1 with $S \cong UT(3,3)$.

4.3 Case $|S| = 81$

Proposition 4.2. *For $|S| = 81$ there are only two possibilities for S, namely*

(a) $S \cong S(81,7)$ *where* $S(81,7) = C_3 \wr C_3$ *is the Sylow* 3*-subgroup of the symmetric group of degree* 9*, moreover* $M_1 \cong C_3 \times C_3 \times C_3$, $M_2 \cong UT(3,3)$, $M_3 \cong M_4 \cong C_9 \rtimes C_3$.

(b) $S \cong S(81,9) = \langle a,b,c | a^9 = b^3 = c^3 = 1, ab = ba, cac^{-1} = ab^{-1}, cbc^{-1} = a^3b \rangle$ *with exactly* 62 *elements of order* 3*; moreover* $M_1 \cong M_2 \cong M_3 \cong UT(3,3)$, $M_4 \cong C_9 \times C_3$.

Proof. There exist exactly seven groups of order 81 generated by two elements, namely $S(81,i)$ with $i = 1,\ldots,7$, and each of them has an abelian normal subgroup of index 3. By Proposition 3.12, S is of maximal class. There are four pairwise non-isomorphic groups of order 81 and maximal class, namely (a), (b) and

(c) $S(81,8) \cong \langle a,b,c | a^9 = b^3 = c^3 = 1, ab = ba, cac^{-1} = ab, cbc^{-1} = a^3b \rangle$ with 26 elements of order 3;

(d) $S(81,10) \cong (C_9 \rtimes C_3) \rtimes C_3$ with 8 elements of order 3.

One of the four maximal normal subgroups of $S(81,8)$ is isomorphic to $U(3,3)$ and hence it contains all elements of order 3. On the other hand, (iv) of Proposition 3.9 yields that two of the maximal normal subgroups of S, namely M_1 and M_2, have non-trivial 1-point stabilizer in Ω_1 and Ω_2, respectively. Hence, both must have an element of order 3 not contained in $\Phi(S)$. Since $M_1 \cap M_2 = \Phi(S)$, these elements are not in the same maximal normal subgroup. This contradiction shows that (c) cannot actually occur in our situation. Regarding $S(81,10)$, all elements of order 3 lie in $\Phi(S)$ as $\Phi(S)$ is an elementary abelian group of order 9. But this is impossible in our situation since M_1 must have an element of order 3 not in $\Phi(S)$ by Propositions 3.9 and 3.11. □

We exhibit an explicit example. Let $\mathcal{X}$ be a non-singular model of the irreducible curve $\mathcal{Y}$ embedded in $PG(4,\mathbb{K})$ defined by the affine equations

(i) $(X^3-X)(Y^3-Y)-1=0$;

(ii) $X(U^3-U)-1=0$;

(iii) $(X+1)(V^3-V)-1=0$.

A straightforward Magma computation shows that $\mathfrak{g}(\mathcal{X})=\gamma(\mathcal{X})=28$. Furthermore, each of the following four maps

$$\begin{array}{ll} g_1:\ (X,Y,U,V)\mapsto(X,Y+1,U,V), & g_2:\ (X,Y,U,V)\mapsto(X,Y,U+1,V),\\ g_3:\ (X,Y,U,V)\mapsto(X,Y,U,V+1), & g_4:\ (X,Y,U,V)\mapsto(X+1,Y,V,-Y-U-V), \end{array}$$

are in $\mathrm{Aut}(\mathcal{X})$. They generate a non-abelian group S of order 81 isomorphic to $S(81,7)$.

4.4 Case $|S|=243$

Proposition 4.3. *If $|S|=243$ and S has a maximal abelian subgroup, then there are only two possibilities for S, namely*

(i) *S is isomorphic to the unique group $S(243,26)$ of order 243 with 170 elements of order 3, moreover $M_2\cong M_3\cong M_4\cong S(81,9)$, and $M_1\cong C_9\times C_9$,*

(ii) *S is isomorphic to the unique group $S(243,28)$ of order 243 with 116 elements of order 3, moreover $M_1\cong M_2\cong S(81,9)$ while $M_3\cong S(81,4)$, and $M_4\cong S(81,10)$.*

Proof. There exist exactly six pairwise non-isomorphic groups of order 81 and maximal class, namely (i), (ii) and $S(243,25)$ with 62 elements of order 3; $S(243,27)$ with 8 elements of order 3; $S(243,29)$ with 8 elements of order 3; $S(243,30)$ with 62 elements of order 3.

One of the four maximal normal subgroups of $S(243,28)$ (and of $S(243,30)$) is isomorphic to $S(81,8)$ and hence it contains all elements of order 3. The argument in the proof of Proposition 4.2 ruling out possibility (c) also works in this case. Therefore, neither $S\cong S(243,25)$ nor $S\cong S(243,28)$ is possible. Regarding $S(243,27)$ and $S(243,29)$, we may use the argument from the proof of Proposition 4.2 that ruled out possibility (d). Therefore, $S\cong S(243,25)$ and $S\cong S(243,28)$ cannot occur in our situation. $\square$

5 Infinite Family of Examples

Let $\mathcal{C}$ be a general curve of genus 2 as given in Remark 2.1 with function field $F=\mathbb{K}(\mathcal{X})=\mathbb{K}(x,y)$ where

$$x(y^3-y)-x^2+c=0. \tag{16}$$

For a positive integer N, let F_N be the largest unramified abelian extension of F of exponent N; that is, $F_N|F$ has the following three properties:

(i) $F_N|F$ is an unramified Galois extension;

(ii) F_N is generated by all function fields which are cyclic unramified extensions of F of degree p^N,

(iii) $\mathrm{Gal}(F_N|F)$ is abelian and $u^{3^N}=1$ for every element $u\in \mathrm{Gal}(F_N|F)$.

From classical results due to Schmid and Witt [17], $\deg(F_N|F)=3^{2N}$ and $\mathrm{Gal}(F_N|F)$ is the direct product of two copies of the cyclic group of order 3^N. Let $\mathcal{X}$ be the curve such that $F_N=\mathbb{K}(\mathcal{X})$. Since F_N is an unramified extension of F, from the Deuring-Shafarevic formula (8) we have that $\gamma(\mathcal{X})-1=3^{2N}(2-1)=3^{2N}$. Our aim is to prove that $\mathrm{Aut}(\mathcal{X})$ contains a 3-group of order 3^{2N+1}.

Let $\mathbb{K}(x)$ be rational the subfield of F generated by x. Obviously, $\mathbb{K}(x)$ is a subfield of F_N and we are going to consider the Galois closure M of $F_N|\mathbb{K}(x)$. Let $M=\mathbb{K}(\mathcal{Y})$ where $\mathcal{Y}$ is an algebraic curve defined over $\mathbb{K}$. Take any $\mu\in \mathrm{Gal}(M|\mathbb{K}(x))$. Then μ is a $\mathbb{K}$-automorphism of $\mathcal{Y}$ fixing x. Let $v=\mu(y)$. Since $\mu(x(y^3-y)-x^2+c)=x(v^3-v)-x^2+c$, from (16)

$$x(v^3-v)-x^2+c=0.$$

This together with (16) yield that either $v=y$ or $v=y\pm 1$. In both cases $v\in F$. Therefore, $\mathrm{Gal}(M|\mathbb{K}(x))$ viewed as a subgroup S of $\mathrm{Aut}(\mathcal{Y})$ preserves F. From the definition of F_N, this implies that S also preserves F_N, that is S is a subgroup of $\mathrm{Aut}(\mathcal{X})$. Since $F_N\subseteq M$, we have that

$$[F_N:\mathbb{K}(x)]\le[M:\mathbb{K}(x)]=|S|.$$

Furthermore,

$$[F_N:\mathbb{K}(x)]=[F_N:F][F:\mathbb{K}(x)]=3^{2N}3=3^{2N+1}.$$

On the other hand $|S|>3^{2N+1}$ is impossible by the Nakajima's bound.

As a corollary, $\mathrm{Aut}(\mathcal{X})$ has a subgroup S so that the Hasse-Witt invariant $\gamma(\mathcal{X})$ is equal to $|S|/3$.

Our construction together with Proposition 3.7 provides a curve of type (ii) in Theorem 1.1, for every power of 3.

In particular, if $N=1$ then the resulting curve is isomorphic to that given in Subsection 3.7. For $N=2$, we have $S\cong S(243,26)$ and case (i) in Proposition 4.3 occurs; furthermore, $S/Z(S)$ is isomorphic to $S(81,9)$, and the quotient curve $\mathcal{X}/Z(S)$ provides an example for type (b) in Proposition 4.2.

References

[1] Y. Berkovich, On subgroups and epimorphih images of finite p-groups, *J. Alg.* **248** (2002) 472-353.

[2] G. Cardona, On the number of curves of genus 2 over a finite field, *Finite Fields Appl.* **9** (2003), 505–526.

[3] G. Cardona and J. Quer, Curves of genus 2 with group of automorphisms isomorphic to D_8 or D_{12}, *Trans. Amer. Math. Soc.* **359** (2007), 2831–2849.

[4] M. Giulietti and G. Korchmáros, Large 2-groups of automorphisms of curves with positive 2-rank, arXiv:1104.5159 [math.AG].

[5] 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.

[6] M. Giulietti and G. Korchmáros, Automorphism groups of algebraic curves with p-rank zero, *J. London Math. Soc.*, (2) **81** (2010), 277–296.

[7] R. Guralnick, B. Malmskog and R. Pries, The automorphism groups of a family of maximal curves, *J. Algebra* **361** (2012), 92–106.

[8] B. Huppert, *Endliche Gruppen. I*, Grundlehren der Mathematischen wissenschaften **134**, Springer, Berlin, 1967, xii+793 pp.

[9] J. Igusa, Arithmetic Variety Moduli for genus 2, *Ann. of Math.* (2), **72** (1960), 612–649.

[10] 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.

[11] C. Lehr and M. Matignon, Automorphism groups for p-cyclic covers of the affine line, *Compositio Math.* **141** (2005), 1213–1237.

[12] M. Matignon and M. Rocher, On smooth curves endowed with a large automorphism p-group in characteristic $p > 0$, *Algebra & Number Theory* **2** (2008), 887–926.

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

[14] R. Pries and K. Stevenson, Katherine, A survey of Galois theory of curves in characteristic p, WINwomen in numbers, 169191, Fields Inst. Commun., **60**, Amer. Math. Soc., Providence, RI, 2011.

[15] M. Rocher, Large p-groups actions with a p-elementary abelian second ramification group, *J. Alg.* **321** (2009), 704–740.

[16] M. Rocher, Large p-groups actions with $|G|/g^2 > 4/(p^2-1)^2$, arXiv:0801.3494v1[math.A.G.], 2008.

[17] H.L. Schmid and E. Witt, Ünverzweigte abelsche Körper vom Exponenten p^n über einem algebraischen Funktionenkörper der Charakteristik p, *J. Reine Angew. Math.* **176** (1936), 168-173.

[18] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe, *Arch. Math.* **24** (1973), 527–544.

[19] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics **67**, Springer, New York, 1979. viii+241 pp.

[20] I.R. Shafarevich, On p-extensions, *Amer. Math. Soc. Transl.* **4** (1954), 59–71.

[21] T. Shaska and L. Beshaj, The arithmetic of genus two curves, in *Information security, coding theory and related combinatorics*, 59-98, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., 29, IOS, Amsterdam, 2011.

[22] H. Stichtenoth, *Algebraic Function Fields and Codes, 2nd Edition*, Springer, 2009.

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

[24] A.D. Thomas and G.V. Wood, *Group Tables*, Shiva Publishing 1980.

[25] E. Witt, Der Existenzsatz für abelsche Funktionenkörper, *J. Reine Angew. Math.* **173** (1935), 43–51.

[26] E. Witt, Konstruktion von galoischen Körpern der Characteristik p zu vorgegebener Gruppe der Ordnung p^f, *J. Reine Angew. Math.* **174** (1936), 237–245.

[27] Mingyao Xu, Lijian An, and Qinhai Zhang, Finite p-groups all of whose non-abelian proper subgroups are generated by two elements, *J. Alg.* **319** (2008), 3603-3620.

Authors' addresses:

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

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