Journal of Algebra 481 (2017) 215–249

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Large p-groups of automorphisms of algebraic curves in characteristic p ☆

Massimo Giulietti [a,*], Gábor Korchmáros [b]

[a] *Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, 06123 Perugia, Italy*
[b] *Dipartimento di Matematica, Informatica ed Economia, Università della Basilicata, Contrada Macchia Romana, 85100 Potenza, Italy*

ARTICLE INFO

Article history:
Received 26 April 2016
Available online 16 March 2017
Communicated by Steven Dale Cutkosky

MSC:
14H37

Keywords:
Algebraic curves
Positive characteristic
Automorphism groups

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 $p \geq 3$. Nakajima [27] proved that if $\gamma \geq 2$ then $|S| \leq \frac{p}{p-2}(\mathfrak{g}-1)$. If equality holds, $\mathcal{X}$ is a *Nakajima extremal curve*. We prove that if

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

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) $|S| = p$, and $\mathcal{X}$ is an ordinary curve of genus $\mathfrak{g} = p-1$.
(iii) $\mathcal{X}$ is an ordinary, Nakajima extremal curve, and $\mathbb{K}(\mathcal{X})$ is an unramified Galois extension of a function field of a curve given in (ii).
(iii) $\mathcal{X}$ is an ordinary, Nakajima extremal curve, and $\mathbb{K}(\mathcal{X})$ is an unramified Galois extension of a function field of a curve given in (ii). There are exactly $p-1$ subgroups M of S such that $\mathbb{K}(\mathcal{X})|\mathbb{K}(\mathcal{X})^M$ is such a Galois extension.

☆ The research was supported by Ministry for Education, University and Research of Italy MIUR (Project PRIN 2012 "Geometrie di Galois e strutture di incidenza") and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA-INdAM).

* Corresponding author.
E-mail addresses: giuliet@dmi.unipg.it (M. Giulietti), gabor.korchmaros@unibas.it (G. Korchmáros).

http://dx.doi.org/10.1016/j.jalgebra.2017.02.024

Moreover, if some of them is an abelian extension then S has maximal nilpotency class.

The full $\mathbb{K}$-automorphism group of any Nakajima extremal curve is determined, and several infinite families of Nakajima extremal curves are constructed by using their pro-p fundamental groups.

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 $\mathfrak{g}(\mathcal{X}) \geq 2$, $\mathbb{K}(\mathcal{X})$ is the function field of $\mathcal{X}$, and $\mathrm{Aut}(\mathcal{X})$ 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 1970s 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

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

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 [34] and also [21, Theorem 11.78]. In the latter case, the Stichtenoth bound is

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

In his paper [27] Nakajima pointed out that the maximum size of S is also 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 [21, 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 [21, Lemma 11.129]. For $\gamma(\mathcal{X}) > 0$, Nakajima proved that $|S|$ divides $\mathfrak{g}(\mathcal{X}) - 1$ when $\gamma(\mathcal{X}) = 1$, and $|S| \leq \frac{p}{p-2}(\gamma(\mathcal{X}) - 1)$ otherwise; see [27] and also [21, Theorem 11.84]. Therefore, the Nakajima bound [27, Theorem 1] is

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

A *Nakajima extremal curve* is a curve $\mathcal{X}$ with p-rank $\gamma(\mathcal{X}) \geq 2$ which attains the bound (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 [25] investigated the case where S fixes a point and were able to determine all curves $\mathcal{X}$ with

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

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 [26] showed that the action of a p-subgroup of $\mathbb{K}$-automorphisms S satisfying

$$|S| > \tfrac{4}{(p^2-1)^2}\,\mathfrak{g}(\mathcal{X})^2,$$

corresponds to the étale cover of the affine line with Galois group $S \cong (\mathbb{Z}/p\mathbb{Z})^n$ for $n \le 3$. These results have been refined by Rocher, see [31] and [32]. 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, and in particular Nakajima extremal curves, are investigated in this paper. Our main results are stated in the following theorems.

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 $\mathfrak{g}(\mathcal{X}) \ge 2$ defined over an algebraically closed field $\mathbb{K}$ of characteristic $p \ge 3$. If*

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

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) *$|S| = p$, and $\mathcal{X}$ is an ordinary curve of genus $\mathfrak{g} = p - 1$.*
(iii) *$\mathcal{X}$ is an ordinary Nakajima extremal curve, and $\mathbb{K}(\mathcal{X})$ is an unramified Galois extension of a function field of a curve given in* (ii)*. There are exactly $p-1$ subgroups M of S such that $\mathbb{K}(\mathcal{X})|\mathbb{K}(\mathcal{X})^M$ is such a Galois extension.*

Theorem 1.2. *In case* (iii) *of Theorem 1.1, S is generated by two elements and if one of those $p - 1$ Galois extensions is abelian, then S has maximal nilpotency class. If there are more than one such abelian extensions, then one of the following two cases occurs:*

(A) *$\mathfrak{g} = p(p - 2) + 1$, $|S| = p^2$ and $S = C_p \times C_p$;*
(B) *$\mathfrak{g} = p^2(p - 2) + 1$, $|S| = p^3$ and $S \cong UT(3, p)$ where $UT(3, p)$ is the group of all upper-triangular unipotent 3×3 matrices over the field with p elements.*

Theorem 1.3. *Let $\mathcal{X}$ be an Nakajima extremal curve, and S a Sylow p-subgroup of* $\mathrm{Aut}(\mathcal{X})$*. Then either S is a normal subgroup of* $\mathrm{Aut}(\mathcal{X})$ *and* $\mathrm{Aut}(\mathcal{X})$ *is the semidirect product of S by a subgroup of a dihedral group of order* $2(p-1)$*, or $p = 3$ and, for some subgroup M of S of index* 3*, M is a normal subgroup of* $\mathrm{Aut}(\mathcal{X})$ *and* $\mathrm{Aut}(\mathcal{X})/M$ *is isomorphic to a subgroup of* $GL(2,3)$.

We also construct several infinite families of Nakajima extremal curves, and provide explicit equations, especially for $p = 3$ and small genera.

The analogous problem for 2-groups of automorphisms S makes sense in characteristic $p = 2$ but the investigation gave rather different results, see [12,15].

One may also ask how the above results may be refined when $\mathrm{Aut}(\mathcal{X})$ is much 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 [13,14,19].

The present paper is also related with the study of automorphism groups of curves in terms of quotients of fundamental groups, see [9,28,29].

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, in other words, the cover $\mathcal{X}|\mathcal{X}^S$ is unramified. 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. Any unramified cover of an ordinary curve is also ordinary. 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 $S_i(P)$ in lower numbering as in [35, 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

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

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 [39] or [21, 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 S has no short orbits, that is, the Galois extension $\mathbb{K}(\mathcal{X})$ of $\mathbb{K}(\bar{\mathcal{X}})$ is unramified, then S can be generated by $\bar{\gamma}$ elements by Shafarevich's theorem [36, Theorem 2], whereas the largest elementary abelian subgroup of S has rank at most $\bar{\gamma}$ see [30, Section 4.7].

The Artin–Mumford curve $\mathcal{M}_c$ over a field $\mathbb{K}$ of characteristic $p>2$ is the curve birationally equivalent over $\mathbb{K}$ to the plane curve with affine equation

$$(x^p-x)(y^p-y)=c, \quad c\in\mathbb{K}^*. \tag{9}$$

$\mathcal{M}_c$ is an ordinary curve with genus $\mathfrak{g}=(p-1)^2$ and its $\mathbb{K}$-automorphism group is isomorphic to $(C_p\times C_p)\rtimes D_{p-1}$, where C_p is a cyclic group of order p and D_{p-1} is a dihedral group of order $2(p-1)$; see [40], and [21, Theorem 11.93].

Proposition 2.1. *Let $\mathcal{Y}$ be a curve of genus $p-1$ and positive p-rank such that p divides* $\mathrm{Aut}(\mathcal{Y})$*. If G is a subgroup of* $\mathrm{Aut}(\mathcal{Y})$ *containing a subgroup T of order p, then either T is a normal subgroup and $G=T\rtimes H$ with H a subgroup of a dihedral group of order $2(p-1)$, or $p=3$ and $\mathcal{Y}$ is a non-singular model of the plane curve with affine equation*

$$Y^3-Y=-X+\frac{1}{X}, \tag{10}$$

and $\mathrm{Aut}(\mathcal{Y})\cong GL(2,3)$*.*

Proof. Let T be a subgroup of $\mathrm{Aut}(\mathcal{Y})$ of order p. The Hurwitz genus formula applied to T yields that the number λ of fixed points of T on $\mathcal{Y}$ is positive. From the Deuring–Shafarevich formula applied to T, $p-2\geq\gamma-1=p(\bar{\gamma}-1)+\lambda(p-1)$ whence $\bar{\gamma}=0$ and $\lambda=2$. Now, from the Hurwitz genus formula applied to T, $2(p-2)\geq 2p(\bar{\mathfrak{g}}-1)+4(p-1)$ which yields $\bar{\mathfrak{g}}=0$. Therefore, T is a normal subgroup of G with four exceptions by a result of Madan and Valentini [40]; see also [21, Theorem 11.93]. One exception occurs for $p=3$ when $\mathcal{Y}$ is a non-singular model of a plane curve $\mathcal{C}$ of affine equation

$X(X-1)(Y^3-Y)=\alpha$ with $\alpha^2=2$, equivalently (10), and G is isomorphic to a subgroup of $GL(2,3)$. This shows that Proposition 2.1 holds in this case. Two of the other three exceptions have zero p-rank, while the fourth is the Artin–Mumford curve of genus $(p-1)^2$. Therefore, they cannot actually occur in our case.

We may assume that T is a normal subgroup of G. By the Nakajima bound (3) applied to $\mathcal{Y}$, T is a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{Y})$. Therefore, $G = T \rtimes H$ with H of order prime to p. Therefore, H can be viewed as an automorphism group of the rational curve fixing two points. Hence, H is a subgroup of a dihedral group of order $2(p-1)$. $\square$

Remark 1. Apart from the exceptional case $p=3$ and $a=-1$, a non-singular model of the plane curve $\mathcal{C}_a$ with affine equation

$$Y^p - Y = aX + \frac{1}{X}, \quad a \in \mathbb{K}^* \tag{11}$$

is a general (hyperelliptic) curve of genus $p-1$ which provides an example for the curve $\mathcal{Y}$ in Proposition 2.1 with an elementary abelian group H of order 4, so that $G = \langle h \rangle \times D_p$ where h is the hyperelliptic involution and D_p is the dihedral group of order $2p$. If $\mathbb{K}$ is the algebraic closure of the finite field $\mathbb{F}_p$, then $G = \mathrm{Aut}(\mathcal{Y})$ by a result due to van der Geer and der Vlugt [42]. As far as we know, no curve $\mathcal{Y}$ of genus $p-1$ and positive p-rank with an automorphism group containing a p-element whose order is larger than $4p$ is available in the literature.

Remark 2. Let $p=3$. The plane curve $\mathcal{C}_a$ in Remark 1 has also an affine equation of type

$$Y^2 = cX^6 + X^4 + X^2 + 1 \tag{12}$$

with some $c \in \mathbb{K}^*$, and provides a further plane model of the curve $\mathcal{Y}$ defined in Proposition 2.1, see [23, Section 8], and [10, Section 1]; see also [37, Lemma 1], and [11]. In particular, $\mathrm{Aut}(\mathcal{Y})$ is a dihedral group of order 12, apart from the exceptional case (10) occurring here for $c=1$. It is an open problem to decide whether an analog result may hold for $p \geq 5$.

From Galois theory we use results on the pro-p fundamental group $\pi_1^p(\bar{\mathcal{X}})$ of an algebraic curve $\bar{\mathcal{X}}$ with p-rank $\bar{\gamma}$ greater than 1; see [30] and [36]. The (finite, Galois) p-extensions of $\mathbb{K}(\bar{\mathcal{X}})$ are taken in a given separable algebraic closure of $\mathbb{K}(\bar{\mathcal{X}})$.

Proposition 2.2. *The pro-p fundamental group $\pi_1^p(\bar{\mathcal{X}})$ is a free group Γ generated by $\bar{\gamma}$ generators. The unramified p-extensions of $\mathbb{K}(\bar{\mathcal{X}})$ are in one-to-one correspondence with the normal subgroups of $\pi_1^p(\bar{\mathcal{X}})$ whose indices are powers of p. Moreover, if an unramified p-extension F corresponds to the normal subgroup N then the Galois group* $\mathrm{Gal}(F|\mathbb{K}(\bar{\mathcal{X}}))$ *is isomorphic to the factor group Γ/N. If two unramified p-extensions*

F and F_1 correspond to N and N_1, respectively, then $F \supseteq F_1$ implies $N \subseteq N_1$ and conversely.

Proposition 2.3. *Let G be a group of order p^n. If $d(G)$ is the minimum size of the generator sets of G, and $\alpha(G)$ is the order of the automorphism group of G, then the following statements hold.*

(i) *There exists an unramified p-extension of $\mathbb{K}(\bar{\mathcal{X}})$ with Galois group isomorphic to G if and only if $d(G) \le \gamma$.*
(ii) *If $d(G) = \gamma$ then the number of different unramified p-extensions of $\mathbb{K}(\bar{\mathcal{X}})$ with Galois group isomorphic to G is equal to*

$$\frac{p^{\gamma(n-d(G))}(p^\gamma - 1)(p^\gamma - p)\cdots(p^\gamma - p^{d(G)-1})}{\alpha(G)}. \tag{13}$$

From group theory we use the following results; see [20, Theorem 12.2.2] and [22, Chapter III, 3.19 Satz].

Proposition 2.4 *(Burnside–Hall bound). Let G be a p-group of order p^n. If $d(G)$ is the minimum size of the generator sets of G and $\alpha(G)$ is the order of the automorphism group of G, then $\alpha(G)$ divides*

$$p^{d(G)(n-d(G))}\,(p^{d(G)} - 1)(p^{d(G)} - p)\cdots(p^{d(G)} - p^{d(G)-1}). \tag{14}$$

In particular, the order of a Sylow p-subgroup of the automorphism group of G divides

$$p^{d(G)(n-d(G))+\frac{1}{2}d(G)(d(G)-1)}. \tag{15}$$

Comparison of the above two propositions, especially (15) with (13), gives the following result.

Corollary 2.5. *Let G be any finite p-group. If the minimum size of the generator sets of G is equal to the Hasse–Witt invariant of $\bar{\mathcal{X}}$ then the number of unramified p-extensions of $\mathbb{K}(\bar{\mathcal{X}})$ with Galois group isomorphic to G is not divisible by p.*

Remark 3. Well known groups G whose automorphism groups attain (14) are the direct product of $d(G)$ copies of the cyclic group of order p^N where N is any positive integer. Furthermore, the Sylow p-subgroup of the special linear group $SL(p,p)$ is isomorphic to the group $UT(p,p)$ of all non-degenerate upper unitriangular $(p \times p)$-matrices over $\mathbb{F}_p$ and the minimum size of the generator sets of $UT(p,p)$ is equal $p-1$. Therefore, Corollary 2.5 applies to any curve $\bar{\mathcal{X}}$ with Hasse–Witt invariant equal to $p-1$. Using the database of GAP, more such examples can be obtained for smaller p.

3. Proof of Theorem 1.1

In this section, $\mathcal{X}$ stands for a curve which satisfies the hypotheses of Theorem 1.1.

3.1. General results on $\mathcal{X}$

From [21, Lemma 11.129], we have the following result.

Lemma 3.1. *If $\gamma = 0$ then* (i) *of Theorem 1.1 holds.*

Moreover, (3) rules out the possibility that case $\gamma = 1$ occurs in Theorem 1.1. Therefore,

$$\gamma \geq 2. \tag{16}$$

Lemma 3.2. *If S fixes a point of $\mathcal{X}$ then* (ii) *of Theorem 1.1 holds.*

Proof. Comparison of (5) with (1) gives

$$|S| < p^2 + \tfrac{p(p-1)}{p-2}.$$

Since the right hand side is smaller than p^3, either $|S| = p$ or $|S| = p^2$ holds. In the latter case, (5) yields $g < p(p-1)$ but this contradicts (1). If $|S| = p$, then (5) reads $(p^2 - p - 1) > p(\mathfrak{g}(\mathcal{X}) - 1)$ while (1) yields $\mathfrak{g}(\mathcal{X}) - 1 \geq p - 2$. Therefore $\mathfrak{g}(\mathcal{X}) - 1$ is an integer in the interval $[p-2, (p^2-p-1)/p)$ whose length is smaller than 2. This is only possible when either $\mathfrak{g}(\mathcal{X}) - 1 = p - 2$ or $\mathfrak{g}(\mathcal{X}) - 1 = p - 1$. Comparison with (5) rules out the latter case. So $\mathfrak{g}(\mathcal{X}) = p - 1$. From Nakajima's bound $|S| \leq p/(p-2)(\gamma(\mathcal{X}) - 1)$, we have $\gamma(\mathcal{X}) \geq p - 1$. Therefore $\gamma(\mathcal{X}) = \mathfrak{g}(\mathcal{X}) = p - 1$. $\square$

From now on we assume that neither (i) or (ii) of Theorem 1.1 hold for $\mathcal{X}$. In particular,

$$|S| \geq p^2. \tag{17}$$

Proposition 3.3. *$\mathcal{X}$ is an ordinary Nakajima extremal curve. Moreover, S has exactly two short orbits on $\mathcal{X}$, both of length $\frac{1}{p}|S|$, and the identity is the unique element in S fixing every point of the short orbits.*

Proof. Let $\mathfrak{g} = \mathfrak{g}(\mathcal{X})$ and $\gamma = \gamma(\mathcal{X})$ where $\gamma \geq 2$ by (16). Let $\bar{\gamma}$ be the p-rank of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/S$. From (8),

$$\gamma - 1 = \bar{\gamma}|S| - |S| + \sum_{i=1}^{k}(|S| - \ell_i) = (\bar{\gamma} + k - 1)|S| - \sum_{i=1}^{k} \ell_i \geq (\bar{\gamma} + \tfrac{p-1}{p}k - 1)|S|, \tag{18}$$

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 (18) yields that $|S|\leq\frac{p}{p-1}(\gamma-1)$ contradicting (5). So, $\bar\gamma=0$, and (18) together with (5) implies that

$$k<\tfrac{2p^2-p-1}{p^2-p}=2+\tfrac{1}{p}$$

whence $1\leq k\leq 2$. The case $k=1$ cannot actually occur by (18).

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 (18) reads

$$\gamma-1=|S|-(\ell_1+\ell_2). \tag{19}$$

Also, $\ell_1+\ell_2<|S|$. Write $|S|=p^h$, $\ell_1=p^m$, $\ell_2=p^r$ with $h>m\geq r$. Here $r>0$ by Lemma 3.2. From (5) and (19),

$$\tfrac{p^2}{p^2-p-1}(p^m+p^r)>p^h(\tfrac{p^2}{p^2-p-1}-1),$$

whence $p^{2+m-h}+p^{2+r-h}>p+1$. Since $m\geq r$, this yields $m=h-1$. Hence, $p^{2+r-h}>1$, and $h-1=m\geq r\geq h-1$. Therefore,

$$\ell_1=\ell_2=\tfrac{|S|}{p}.$$

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

$$2\mathfrak{g}-2=|S|(2\bar{\mathfrak{g}}-2)+\tfrac{p-1}{p}|S|(4+k_1+k_2) \tag{20}$$

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. Then $k_1+k_2\geq 1$. From (20),

$$2g-2\geq -2|S|+5|S|\tfrac{p-1}{p}=|S|(\tfrac{3p-5}{p}).$$

Comparing this with (5) yields

$$\frac{2p}{3p-5}\geq\frac{|S|}{g-1}\geq\frac{p^2}{p^2-p-1},$$

a contradiction.

Assume that a non-trivial element $s\in S$ of order p fixes $\Omega_1\cup\Omega_2$ pointwise. From the Deuring–Shafarevich formula applied to $\langle s\rangle$,

$$\tfrac{p-2}{p}|S|\geq -p+2\tfrac{|S|}{p}(p-1),$$

which is only possible for $|S|=p$. $\square$

We stress that the first claim of Proposition 3.3 means that

$$\mathfrak{g}-1=\gamma-1=\tfrac{p-2}{p}|S|, \tag{21}$$

and hence $\mathcal{X}$ is a Nakajima extremal curve.

Proposition 3.4. *$\mathcal{X}$ is not hyperelliptic.*

Proof. Since the length of any S-orbit in $\mathcal{X}$ is divisible by p, the number of distinct Weierstrass points of $\mathcal{X}$ is also divisible by p. On the other hand, a hyperelliptic curve of genus $\mathfrak{g}$ defined over a field of zero or odd characteristic has as many as $2\mathfrak{g}+2$ Weierstrass points, see [21, Theorem 7.103]. Therefore, if $\mathcal{X}$ were hyperelliptic, both numbers $\mathfrak{g}+1$ and $\mathfrak{g}-1=\frac{p-2}{p}|S|$ would be divisible by p, a contradiction with $|S|\geq p^2$. $\square$

3.2. The short orbits of S

From the rest of the paper, we keep up our notation; in particular Ω_1 and Ω_2 denote the short orbits of S on $\mathcal{X}$. By the second claim of Proposition 3.3, the following hold.

Lemma 3.5. *For every point $P\in\Omega_1\cup\Omega_2$, the stabilizer S_P of P has order p.*

Proposition 3.6. *If S is abelian then $|S|=p^2$ and S is elementary abelian.*

Proof. Choose a point $P\in\Omega_1$. From Lemma 3.5, $|S_P|=p$. Since S is abelian S_P fixes every point in Ω_1. Let γ^* be the p-rank of the quotient curve $\mathcal{X}/S_P$. The Deuring–Shafarevich formula applied to S_P together with (21) gives

$$\tfrac{p-2}{p}|S|=\gamma-1\geq -p+\tfrac{p-1}{p}|S|$$

whence $|S|\leq p^2$. Then $|S|=p^2$ by (17). 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 p. Since S is cyclic, it has only one subgroup of order p. Therefore $S_P=S_Q$, and

$$\tfrac{p-2}{p}|S|=\gamma-1\geq -p+2\tfrac{p-1}{p}|S|$$

which implies $|S|\leq p$, a contradiction. $\square$

Proposition 3.7. *Let N be a non-trivial normal subgroup of S. Then either N is semiregular on $\mathcal{X}$, or N has order $\frac{|S|}{p}$ and there is point $P\in\Omega_1\cup\Omega_2$ such that $S=N\rtimes S_P$.*

Proof. The assertion trivially holds for $|S|=p^2$ with $S=N\times S_P$. Assume that some non-trivial element in N fixes point P. From the Hurwitz genus formula applied to N, we have $\frac{p-2}{p}|S|>|N|(\bar{\mathfrak{g}}-1)$ where $\bar{\mathfrak{g}}$ is the genus 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 $\frac{p-2}{p}|\bar{S}| > \bar{\mathfrak{g}} - 1$. If $\bar{\mathfrak{g}} \geq 2$, Nakajima's bound (3) applied to $\bar{\mathcal{X}}$ implies that $\bar{\gamma} = 0$. From [21, Lemma 11.129], $\bar{S}$ fixes a point $\bar{Q}$ in $\bar{\mathcal{X}}$. 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 $\mathcal{O}$ coincides with one of them, say Ω_1. Therefore, $|N| = \frac{1}{p}|S|$. The stabilizer ε of a point $R \in \Omega_2$ on S has order p and $\varepsilon \notin N$. Therefore $S = N \rtimes \langle\varepsilon\rangle$. This argument also works when $\bar{\mathfrak{g}} \leq 1$ and $\bar{\gamma} = 0$. 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 p, the Deuring–Shafarevich formula applied to N together with (21) gives

$$\tfrac{p-2}{p}|S| = \tfrac{p-1}{p}|N|m$$

whence $|S| = \frac{p-1}{p-2}|N|m$. But this is impossible as both $|S|$ and $|N|$ are powers of p. □

3.3. The structure of S

Proposition 3.8. *The center $Z(S)$ of S is semiregular on $\mathcal{X}$.*

Proof. Since $Z(S)$ is a normal subgroup of S, Proposition 3.7 applies to $Z(S)$. The case $S = Z(S) \rtimes S_P$ cannot actually occur since this semidirect product would be direct and S would be abelian contradicting Proposition 3.6. □

Proposition 3.9. *Let N be a non-trivial normal subgroup of S such that $|N| \leq \frac{1}{p^2}|S|$. 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 either* (i) *or* (ii) *of Theorem 1.1. In particular, if $\mathcal{X}$ is a Nakajima extremal curve then $\bar{\mathcal{X}}$ is also a Nakajima extremal curve.*

Proof. By Proposition 3.7, the extension $\mathbb{K}(\mathcal{X})|\mathbb{K}(\bar{\mathcal{X}})$ is an unramified p-extension with Galois group N. Therefore, the Hurwitz formula applied to N gives that $\mathfrak{g} - 1 = |N|(\mathfrak{g}(\bar{\mathcal{X}}) - 1)$. In Theorem 1.1 referred to $\bar{\mathcal{X}}$ and $\bar{S}$, case (i) is impossible by $\bar{\gamma} \neq 0$, while case (ii) cannot occur since $|\bar{S}| > p$. □

Since the center of any p-group is non-trivial, a straightforward inductive argument on $|S|$ depending on Proposition 3.9 gives the following result.

Proposition 3.10. *If there exists a curve $\mathcal{X}$ which satisfies the hypothesis of Theorem 1.1 for $|S| = p^k$ but does not have the properties* (i) *and* (ii)*, then for any $1 < j < k$ the curve $\mathcal{X}$ has a quotient curve $\bar{\mathcal{X}}$ which satisfies the hypothesis of Theorem 1.1 for $|\bar{S}| = p^j$ but has none of the properties* (i) *and* (ii).

A corollary of Propositions 3.7 and 3.9 is stated in the following proposition.

Proposition 3.11. *Let N be a non-trivial normal subgroup of S. If the factor group S/N is abelian then either $|N| = \frac{1}{p}|S|$ or $|N| = \frac{1}{p^2}|S|$, and in the latter case, S/N is an elementary abelian group.*

Proposition 3.11 together with classical results from Group theory gives some useful results on S.

Proposition 3.12. *Let $\Phi(S)$ and S' be the Frattini subgroup and the commutator subgroup of S, respectively. Then the following hold.*

(i) $\Phi(S) = S'$.
(ii) $|\Phi(S)| = \frac{1}{p^2}|S|$.
(iii) *S contains exactly $p+1$ maximal subgroups, each being a normal subgroup of S of index p.*
(iv) *Exactly two of the $p+1$ maximal subgroups of S are not semiregular on $\mathcal{X}$.*
(v) *Two elements of S of order p, one fixing a point in Ω_1 and the other in Ω_2, always generate S.*

Proof. From Proposition 3.11, either $|\Phi(S)| = \frac{1}{p}|S|$, or $|\Phi(S)| = \frac{1}{p^2}|S|$. In the former case, S is cyclic by [22, Hilfssatz 7.1.b] but this contradicts Proposition 3.6. Therefore, (ii) holds. Since $S/\Phi(S)$ is (elementary) abelian, $\Phi(S)$ contains S'. Hence, Proposition 3.11 yields (i). 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 p^2 which have exactly $p+1$ proper subgroups. Therefore there are exactly $p+1$ maximal subgroups in S. Also, the subgroups of $S/\Phi(S)$ are normal, and hence each of the $p+1$ maximal subgroups of S is normal, as well. Furthermore, the $p+1$ 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 $p+1$ 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 3.3, these two maximal subgroups are distinct. Therefore, the remaining $p-1$ maximal subgroups are semiregular on $\mathcal{X}$.

Finally, (i) together with the Burnside fundamental theorem, [22, Chapter III, Satz 3.15] implies that S can be generated by two elements. Here any two non-trivial elements from different maximal subgroups of S generate S. Since some element g_1 of order p fixes a point Ω_1, and the same holds for some element g_2 fixing a point of Ω_2 where g_1, g_2 are in two distinct maximal subgroups of S, it turns out that $S = \langle g_1, g_2 \rangle$. □

3.4. Some quotient curves of $\mathcal{X}$

For $i = 1, 2,,$ let M_i be the maximal normal subgroup of S containing the stabilizer of a point of Ω_i, while let $M_3, \ldots, M_{p+1}$ be the semiregular maximal subgroups of S, respectively.

Proposition 3.13. *Every normal subgroup of S whose order is at most $\frac{1}{p^2}|S|$ is contained in $\Phi(S)$.*

Proof. Let N be a normal subgroup of S. From [22, Chapter III, Hilfssatz 3.4.a], $\Phi(S)N/N$ is a subgroup of $\Phi(S/N)$. From Propositions 3.9 and Proposition 3.12 applied to $\bar{\mathcal{X}} = \mathcal{X}/N$, we have $|\Phi(S/N)| = \frac{1}{p^2}|S|/|N|$. 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 $\Phi(S)$. □

Proposition 3.14. *For $i = 1, 2$, the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/M_i$ is rational.*

Proof. Every point in Ω_i is fixed by an element of M_i order p. From the Hurwitz genus formula applied to M_i,

$$\tfrac{p-2}{p}|S| \geq \tfrac{|S|}{p}(\bar{\mathfrak{g}} - 1) + \tfrac{|S|}{p}(p - 1)$$

where $\bar{\mathfrak{g}}$ is the genus of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/M_i$. This yields $\bar{\mathfrak{g}} = 0$. □

Proposition 3.15. *For $3 \leq i \leq p + 1$, the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/M_i$ is a curve given in (ii) of Theorem 1.1, and the extension $\mathbb{K}(\mathcal{X})|\mathbb{K}(\bar{\mathcal{X}})$ is an unramified p-extension with Galois group isomorphic to M_i.*

Proof. Since M_i is semiregular on $\mathcal{X}$, the extension $\mathbb{K}(\mathcal{X})|\mathbb{K}(\bar{\mathcal{X}})$ is unramified. Furthermore, since M_i is a subgroup of S of index p, (21) together with the Hurwitz and the Deuring–Shafarevich formulas gives $\bar{\mathfrak{g}} - 1 = \bar{\gamma} - 1 = p - 2$ where $\bar{\mathfrak{g}}$ is the genus and $\bar{\gamma}$ is the p-rank of $\bar{\mathcal{X}}$. □

Remark 4. From Propositions 3.15 and 2.3(i), every minimal generator set of M_i with $3 \leq i \leq p+1$ has size at most $p-1$. We will show curves attaining this bound $p-1$.

Theorem 1.1 follows from Lemmas 3.1 and 3.2 together with Propositions 3.3, 3.10 and 3.15. For the rest of the paper, $\mathcal{X}$ *always denotes an extremal Nakajima curve. Also, we keep our notation and terminology adopted in Section 3. In particular,* $\mathfrak{g} = \mathfrak{g}(\mathcal{X}) = (p-2)p^{n-1} + 1$ *and S is a Sylow subgroup of* $\mathrm{Aut}(\mathcal{X})$ *of order p^n with its subgroups $M_1, M_2, \ldots, M_{p+1}$ of index p where M_i with $i = 1, 2$ stands for the maximal normal subgroup of S containing the stabilizer of a point of Ω_i.*

4. Infinite family of examples

Let $\bar{\mathcal{X}}$ be a general curve of genus $p-1$ defined in Remark 1 with function field $F = \mathbb{K}(\bar{\mathcal{X}}) = \mathbb{K}(x, y)$ where

$$x(y^p - y) - ax^2 - 1 = 0, \;\; a \in \mathbb{K}^*. \tag{22}$$

For a positive integer N, let F_N be the largest unramified abelian extension of F of exponent p^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 $u^{p^N} = 1$ for every element $u \in \mathrm{Gal}(F_N|F)$.

From classical results due to Schmid and Witt [33], we have that $\deg(F_N|F) = p^{(p-1)N}$ and that $\mathrm{Gal}(F_N|F)$ is the direct product of $p-1$ copies of the cyclic group of order p^N. Let $\mathcal{X}$ be the curve such that $F_N = \mathbb{K}(\mathcal{X})$. Since F_N is an unramified extension of F, the Deuring–Shafarevich formula yields $\gamma(\mathcal{X}) - 1 = p^{(p-1)N}(p-2)$. Our aim is to prove that $\mathrm{Aut}(\mathcal{X})$ contains a p-group of order $p^{(p-1)N+1}$.

Let $\mathbb{K}(x)$ be the rational 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 $\mu(x(y^p - y) - ax^2 - 1) = x(v^p - v) - ax^2 - 1$, from (22)

$$x(v^p - v) - ax^2 - 1 = 0.$$

This together with (22) yields that either $v = y$ or $v = y + s$ with $s \in \mathbb{F}_p^*$. In both cases $v \in F$. Therefore, $\mathrm{Gal}(M|\mathbb{K}(x))$ viewed as a subgroup G of $\mathrm{Aut}(\mathcal{Y})$ preserves F. From the definition of F_N, this implies that G also preserves F_N. If L is the (normal) subgroup of G fixing F_N elementwise, this yields that $H = G/L$ is a subgroup of $\mathrm{Aut}(\mathcal{X})$. Let T be the subfield of M consisting of all elements which are fixed by L. Since $F_N \subseteq T \subseteq M$ and $M|T$ is a Galois extension, we have that

$$|G| = [M : \mathbb{K}(x)] = [M : T][T : F_N][F_N : F][F : \mathbb{K}(x)] = |L|[T : F_N]p^{(p-1)N}p,$$

whence $|H| = |G|/|L|$ is divisible by $p^{(p-1)N+1}$. Let S be a Sylow p-subgroup of H. Then S is a subgroup of $\mathrm{Aut}(\mathcal{X})$ so that $\gamma(\mathcal{X}) - 1 = (p-2)\frac{|S|}{p}$. In particular, S is a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X})$. By construction, $U = \mathrm{Gal}(F_N|F)$ is an index p subgroup of S containing no nontrivial element fixing a point on $\mathcal{X}$. From Proposition 3.3, the stabilizer S_P for some point $P \in \mathcal{X}$ has order p. From (iii) of Proposition 3.12, U is a normal subgroup of S, and hence $S = U \rtimes S_P$. Therefore, the following result is obtained.

Theorem 4.1. *For $N \geq 1$, let $\mathcal{X}$ be the curve whose function field $\mathbb{K}(\mathcal{X})$ is generated by all cyclic unramified p-extensions of degree p^N of the function field of the curve $\bar{\mathcal{X}}$ with affine equation (22). Then $\mathcal{X}$ is an extremal Nakajima curve of genus $\mathfrak{g}(\mathcal{X}) = p^{(p-1)N}(p-2)+1$ whose p-group of automorphisms S is a semidirect product $U \rtimes \langle s \rangle$ where U is the direct product of $p-1$ cyclic groups of order p^N and s has order p.*

Theorem 4.1 together with Proposition 3.10 provides a curve of type (iii) in Theorem 1.1, for every proper power of p. An explicit example, for $p = 3$ and $N = 1$, is given in Section 8.2.

In our construction, F_N may be replaced by any unramified Galois extension F' under the condition that $G = \mathrm{Gal}(F'|F)$ is a finite group of order p^m with $d(G) = p-1$, whose automorphism group $\mathrm{Aut}(G)$ attains (14). In fact, Proposition 2.3 shows that F' is the unique unramified Galois extension of F with Galois group G in the separable algebraic closure of F. Therefore, if $\mathcal{X}$ is a curve with function field F', the above argument shows that $\mathcal{X}$ is a Nakajima extremal curve with p-rank equal to $p^{m+1}(p-2)$. This proves the following result.

Theorem 4.2. *Let G be a finite p-group of order p^n such that the minimum size of its generator sets equals $p-1$. Assume that the automorphism group of G attains (14). Then, for every $a \in \mathbb{K}^*$, there exists a unique Nakajima extremal curve $\mathcal{X}$ which is an unramified p-extension of the curve $\bar{\mathcal{X}}$, as in Remark 1, with* $\mathrm{Gal}(\mathbb{K}(\mathcal{X})|\mathbb{K}(\bar{\mathcal{X}})) \cong G$.

From Remark 3, Theorem 4.2 applies to the above considered direct product of $p-1$ copies of the cyclic group of order p^N, and to the group $UT(r,p)$ for $r = p$. A further refinement of the above construction is given in the following theorem.

Theorem 4.3. *Existence (but not necessarily uniqueness) of a Nakajima extremal curve stated in Theorem 4.2 holds true under the weaker hypothesis that a Sylow p-subgroup of the automorphism group of G attains (15).*

Proof. Let $|G| = p^m$. In a separable algebraic closure of F, let $\{F_1, \dots, F_k\}$ be the set of all unramified Galois extension $F_i|F$ with $G \cong \mathrm{Gal}(F_i|F)$, and let F' be their compositum. Obviously, the Galois closure M of $F'|\mathbb{K}(x)$ contains each F_i. Since $d(G) = p-1$, Corollary 2.5 yields that k is not divisible by p. Our arguments leading to Theorem 4.2 show that $\mathrm{Gal}(M|\mathbb{K}(x))$ preserves F, and hence leaves the set $\{F_1, \dots, F_k\}$ invariant. Since $p \nmid k$, any p-subgroup of $\mathrm{Gal}(M|\mathbb{K}(x))$ preserves at least one of them, say F_1. As

$$|\mathrm{Gal}(M|\mathbb{K}(x))| = [M : F'][F' : F_1][F_1 : F][F : \mathbb{K}(x)] = [M : F'][F' : F_1]p^{m+1},$$

$\mathrm{Gal}(M|\mathbb{K}(x))$ has a subgroup of index p^{m+1} that preserves F_1. This shows that if $\mathcal{X}$ is a curve with $\mathbb{K}(\mathcal{X}) = F_1$, then $\mathrm{Aut}(\mathcal{X})$ has a subgroup of order p^{m+1}. Since $[F_1 : F]$ is an unramified Galois extension with Galois group of order p^m and $\bar{\mathcal{X}}$ has p-rank $p-1$, the Deuring–Shafarevich formula yields that $\mathcal{X}$ has p-rank $p^m(p-2)+1$. Therefore, $\mathcal{X}$ is a Nakajima extremal curve with an automorphism group of order p^{m+1}. Our argument also shows that uniqueness might not hold when $k \not\equiv 1 \pmod{p}$. $\square$

With some changes, the above construction also applies to the Artin–Mumford curve $\mathcal{M}_c = \bar{\mathcal{X}}$ with affine equation (9). As we have already mentioned, $\mathfrak{g}(\bar{\mathcal{X}}) = \gamma(\bar{\mathcal{X}}) = (p-1)^2$ and $\mathrm{Aut}(\bar{\mathcal{X}})$ has an elementary abelian subgroup of order p^2 generated by $\alpha = (x, y) \to (x + 1, y)$ and $\beta = (x, y) \to (x, y + 1)$. In fact, if $F = \mathbb{K}(t)$ is the rational field generated by $t = x^p - x$, and M is the Galois closure of $F_N|\mathbb{K}(t)$ then every $\mu \in \mathrm{Gal}(M|\mathbb{K}(t))$ preserves the Artin–Mumford curve $\bar{\mathcal{X}}$. Therefore, the following result holds.

Theorem 4.4. *For $N \geq 1$, let $\mathcal{X}$ be the curve whose function field $\mathbb{K}(\bar{\mathcal{X}})$ is generated by all cyclic unramified p-extensions of degree p^N of the function field of the Artin–Mumford curve $\bar{\mathcal{X}}$ with affine equation (9). Then $\mathcal{X}$ is an extremal Nakajima curve of genus $\mathfrak{g}(\mathcal{X}) = p^{N(p-1)^2+1}(p-2)+1$ with a p-group of automorphisms S whose Frattini subgroup $\Phi(S)$ of order $p^{N(p-1)^2}$ is the direct product of $(p-1)^2$ copies of the cyclic group of order p^N, so that the factor group $S/\Phi(S)$ is elementary abelian of order p^2.*

5. The structure of S for $|S| \leq p^{p+1}$

Proposition 5.1. *If $|S| \leq p^p$ then S has exponent p.*

Proof. From [22, Chapter III, 10.2 b) Satz], S is a regular p-group. By (v) of Proposition 3.12, S is generated by (two) elements of order p. Therefore, the subgroup $\Omega_1(S)$ generated by all elements of order p is the whole group S. From [22, Chapter III, 10.7 a) Satz], the subgroup of S generated by all elements which are proper p-powers of elements in S is trivial. Hence, every non-trivial element of S has order p. $\square$

Proposition 5.2. *If $|S| = p^3$ then S isomorphic to $UT(3, p)$, the unique non-abelian group of order p^3 and exponent p. Furthermore, the non-trivial elements of S which have fixed points are at most $2(p^2 - p)$.*

Proof. From the classification of groups of order p^3, see [22, Chapter I, 14.10 Satz], either $S = C_{p^2} \rtimes C_p$, or $S \cong UT(3, p)$. Since the group $C_{p^2} \rtimes C_p$ has exponent p^2, the first assertion follows from Proposition 5.1. The elements of S with fixed points fall into two subgroups, namely M_1 and M_2, both elementary abelian of order p^2. Since $Z(S)$ is a subgroup of M_1 of order p, Proposition 3.8 shows that M_1 (and M_2) has at most as many as $p^2 - p$ non-trivial elements with a fixed points. $\square$

Proposition 5.3. *For $c \in \mathbb{K}^*$, the curve $\mathcal{X}_c$ with function field $\mathbb{K}(x, y, z)$ defined by the equations*

(i) $(x^p - x)(y^p - y) - c = 0$;
(ii) $z^p - z + x^p y - x y^p = 0$

is a Nakajima extremal curve whose automorphism group has order p^3, and its $\mathbb{K}$-automorphism group is a semidirect product of $UT(p,3)$ by a dihedral group of order $2(p-1)$.

Proof. As before, let $\mathcal{M}_c$ denote the Artin–Mumford curve with affine equation (9). We first show that $\mathbb{K}(\mathcal{X}_c)$ is an unramified Artin–Schreier extension of $\mathbb{K}(\mathcal{M}_c)$. This will imply that $\mathfrak{g}(\mathcal{X}_c) = \gamma(\mathcal{X}_c) = (p-2)p^2 + 1$.

Since $\mathfrak{g}(\mathcal{M}_c) = (p-1)^2$ and $\mathbb{K}(\mathcal{M}_c) = \mathbb{K}(x,y)$ with x, y as in (9), there exist places $P_0, \ldots, P_{p-1}$, $Q_0, \ldots, Q_{p-1}$ such that

$$(y)_0 = pP_0, \qquad (y)_\infty = Q_0 + \ldots + Q_{p-1},$$
$$(x)_0 = pQ_0, \qquad (x)_\infty = P_0 + \ldots + P_{p-1},$$

and for each $i = 1, \ldots, p-1$

$$v_{P_i}(y-i) = v_{Q_i}(x-i) = p.$$

Let $u = xy^p - x^p y$. Then $u = xy \prod_{a \in \mathbb{F}_p^*}(y - ax)$. The pole divisor of u is

$$(u)_\infty = p(P_1 + \ldots + P_{p-1} + Q_1 + \ldots + Q_{p-1}).$$

Also,

$$v_{P_0}(u) = 0, \qquad v_{Q_0}(u) = 0.$$

In order to prove that the equation $z^3 - z = u$ defines an Artin–Schreier extension of $\mathbb{K}(x,y)$, we first show that $u \neq w^p - w$ for every $w \in \mathbb{K}(x,y)$; see [38, Proposition III.7.8]. A canonical divisor of $\mathbb{K}(x,y)$ is

$$W = (p-2)(P_0 + \ldots + P_{p-1} + Q_0 + \ldots + Q_{p-1}),$$

and a $\mathbb{K}$-basis of $\mathcal{L}(W)$ is

$$\{x^i y^j \mid 0 \le i \le p-2,\ 0 \le j \le p-2\}.$$

Assume that $u = w^p - w$ for some $w \in \mathbb{K}(x,y)$. Then

$$(w)_\infty = P_1 + \ldots + P_{p-1} + Q_1 + \ldots + Q_{p-1}.$$

Therefore, $w \in \mathcal{L}(W)$, and hence

$$w = \sum_{i=0,\ldots,p-1} x^i f_i(y),$$

for f_i a polynomial in $\mathbb{K}[T]$ of degree less than or equal to $p-2$. Note that for each $k=1,\dots,p-1$

$$v_{P_k}(x^i f_i(y)) = -i + ps_{i,k},$$

where $s_{i,k}$ is the multiplicity of k as a root of f_i. As the degree of f_i is less than $p-1$, for each $i>0$ with $f_i(y)\neq 0$ there is some k with $s_{i,k}=0$. Let k_i be the minimum of such k's. Then

$$-1 = v_{P_{k_i}}(w) = -i,$$

which shows that $f_i(y)=0$ for each $i\geq 2$. Then

$$w = f_0(y) + xf_1(y).$$

Analogously, it can be proved that

$$w = g_0(x) + yg_1(x)$$

for some polynomials $g_0, g_1 \in \mathbb{K}[T]$ of degree less than or equal to $p-2$. The only possibility is that

$$w = \alpha + \beta x + \gamma y + \delta xy, \text{ for some } \alpha,\beta,\gamma,\delta \in \mathbb{K}.$$

Therefore,

$$u = xy^p - x^p y = w^p - w = \alpha^p - \alpha - \beta x + \beta^p x^p - \gamma y + \gamma^p y^p - \delta xy + \delta^p x^p y^p.$$

If $\beta \neq 0$, then

$$v_{P_0}(u) = v_{P_0}(\beta^p x^p) = -p;$$

similarly, if $\gamma \neq 0$ then

$$v_{Q_0}(u) = v_{Q_0}(\gamma^p y^p) = -p.$$

As $v_{P_0}(u) = v_{Q_0}(u) = 0$, we have $\beta=\gamma=0$ and hence $u = \alpha^p - \alpha - \delta xy + \delta^p x^p y^p$. From $(x^p - x)(y^p - y) = c$ it follows $x^p y^p = x^p y + xy^p - xy + c$, whence $u = \delta^p(x^p y + xy^p - xy + c) - \delta xy + \alpha^3 - \alpha$, and

$$(1-\delta^p)xy^p - (1+\delta^p)x^p y + (\delta^p + \delta)xy - (\delta^p c + \alpha^p - \alpha) = 0.$$

Valuating at P_1 and Q_1 gives $\delta^p = 1$ and $\delta^p = -1$, a contradiction.

In order to prove that the extension $\mathbb{K}(x,y,z)|\mathbb{K}(x,y)$ is unramified, we need to show that for each $i=1,\dots,p-1$ there exist t_i and v_i such that

$$v_{P_i}(xy^p - x^p y - (t_i^p - t_i)) \geq 0, \qquad v_{Q_i}(xy^p - x^p y - (v_i^p - v_i)) \geq 0. \tag{23}$$

Let $t_i = ix$. Then

$$xy^p - x^p y - (t_i^p - t_i) = xy^p - x^p y + ix^p - ix = x(i-y) \prod_{a \in \mathbb{F}_p^\star} (x - a(i-y))$$

and hence

$$v_{P_i}(xy^p - x^p y - (t_i^p - t_i)) = v_{P_i}(y-i) - p = 0.$$

Similarly, one can show that $v_{Q_i}(xy^p - x^p y - ((iy)^p - (iy))) = 0$ for each $i = 1, \ldots, p-1$. This completes the proof of the first assertion.

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 p^3 and exponent p. Therefore $S \cong UT(p,3)$. Furthermore, $\mathrm{Aut}(\mathcal{X})$ contains the maps $r : (x,y,z) \mapsto (y, x, -z)$, and $t := (x,y,z) \mapsto (\omega x, \omega^{-1} y, z)$ where ω is primitive element of $\mathbb{F}_p$. By a straightforward computation, $\langle r, t \rangle \cong D_{p-1}$ and

$$rgr = h^{-1},\, rhr = g^{-1},\, t^{-1}gt = g^{\omega^{-1}},\, t^{-1}ht = h^{\omega}.$$

Thus $G = \langle g, h, r, t \rangle \cong UT(p,3) \rtimes D_{p-1}$. Actually G is the full $\mathbb{K}$-automorphism group of $\mathcal{X}$ for $p > 3$. This follows from Theorem 1.3. For $p = 3$, a Magma computation shows that $\mathrm{Aut}(\mathcal{X})$ is larger as it has order 432 and $\mathrm{Aut}(\mathcal{X}) \cong UT(3,3) \rtimes V$ where V is a semidihedral group of order 16. □

Proposition 5.4. *If $|S| = p^{p+1}$, then S has exponent p or p^2. In the latter case, M_1 and M_2 have exponent p, and if M_i with $3 \leq i \leq p+1$ has exponent p^2 then all elements of M_i of order p are in $\Phi(S)$. Moreover, the maximal normal subgroups M_i of exponent p^2 are as many as k, then the number of elements of S of order p is equal to $(p+1-k)(p^p - p^{p-1}) + p^{p-1} - 1$.*

Proof. The subgroup N_1 generated by the elements of M_1 of order p is a characteristic subgroup of M_1. Since M_1 is a normal subgroup of S, this yields that N_1 is a normal subgroup of S. By Lemma 3.5, the stabilizer of a point $P \in \Omega_1$ is in N_1. Hence Proposition 3.7 yields $N_1 = M_1$. Since M_1 has order p^p its exponent is equal to p. Therefore, [22, Chapter III, 10.7 a) Satz] yields no non-trivial element of M_1 is a p-power of an element of M_1, that is, M_1 has exponent p. This remains true for M_2. If S has exponent p^h with $h > 1$ then some M_i with $3 \leq i \leq p+1$ contains an element u of order p^i. Since $\Phi(S)$ is a subgroup of M_i of index p, $\Phi(S)$ contains u^p. On the other hand $\Phi(S)$ is a subgroup of

M_1 and M_1 has exponent p. Therefore, $u^{p^2} = 1$ whence $h = 2$. Moreover, if M_i had an element v of order p other than those in $\Phi(S)$, then $\Phi(S)$ together with v would generate M_i. Since M_i is a p-regular subgroup, this would yield M_i to have exponent p, again by [22, Chapter III, 10.7 a) Satz]; a contradiction. Therefore, no element of $M_i \setminus \Phi(S)$ has order p. If we have k such M_i, then S has exactly $(p+1-k)(p^p - p^{p-1}) + p^{p-1} - 1$ whence the last claim follows. □

6. Particular families of groups and a proof of Theorem 1.2

Metacyclic, regular p-groups and p-groups with maximal nilpotency class play an important role in Group theory; the main references are [22, Section III.14], and [5–7]. This gives us a motivation for the study of Nakajima extremal curves whose p-automorphism group S falls in one of those families, exploiting the well developed theory of finite p-groups. Our results provide not only the necessary technical lemmas for a proof for Theorem 1.2 but also useful properties of Nakajima extremal curves with small genera, especially those considered in Section 8.

Proposition 6.1. *If $|S| \geq p^4$ then S is not metacyclic.*

Proof. Assume on the contrary that S is metacyclic. From Proposition 3.12 and [8, Lemma 2.2], S'/S is cyclic. Therefore S' contains a characteristic subgroup N of index p. By (i) of Proposition 3.12, N has index p^3 in S. From Proposition 3.9 applied to N, $\bar{S} = S/N$ is a subgroup of $\mathrm{Aut}(\bar{\mathcal{X}})$ with $\bar{\mathcal{X}} = \mathcal{X}/N$ such that $|\bar{S}| = p^3$, Proposition 5.2 implies that $\bar{S} \cong UT(3,p)$. On the other hand, as S is metacyclic, [4, Theorem 2] yields that $\bar{S} = S/N$ is also a metacyclic group. But $UT(3,p)$ is not a metacyclic group by Proposition 5.2, a contradiction. □

Proposition 6.2. *S is a regular p-group if and only if S has exponent p.*

Proof. The proof of Proposition 5.1 shows that if S is regular then it has exponent p. The converse also holds, see [22, Chapter III, 10.2 d) Satz]. □

Proposition 6.3. *If $|S| > p^2$ then none of the subgroups M_i is cyclic.*

Proof. For $i = 1, 2$ the assertion follows from Proposition 3.7. For $3 \leq i \leq p+1$ the proof is by induction on $|S|$. In the smallest case, $|S| = p^3$, the assertion is a consequence of Proposition 5.2. Assume that $M = M_i$ is cyclic for some $3 \leq i \leq p+1$. Let T be the unique subgroup of M of order p. Since M is a normal subgroup of S, T is a normal subgroup of S, as well. As T is semiregular, the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/T$ is a Nakajima extremal curve with Sylow p-subgroup S/T. Since $|S/T| = \frac{1}{p}|S|$ and $|M/T| = \frac{1}{p}|M|$, the inductive hypothesis yields that M/T is not cyclic. But then M itself is not cyclic. □

Proposition 6.4. *If at least two of the $p+1$ maximal normal subgroups M_i of S are abelian then $|S| = p^2$ or $|S| = p^3$.*

Proof. Assume that $|S| \neq p^2$. From [22, Chapter I, Aufgabe 21)], every p-group with at least two abelian maximal normal subgroup has class at most 2. On the other hand, if a non-abelian group G of order p^n has an abelian maximal normal subgroup and the commutator subgroup of G has index p^2 then G has (maximal) class $n-1$; see [43, Theorem 2.5]. This applies to S in our case by (i) and (ii) of Proposition 3.12. Therefore, $n-1=2$. □

The result on G quoted in the proof of Proposition 6.4 together with (i) and (ii) of Proposition 3.12 also gives the following result.

Proposition 6.5. *If M_i is abelian for some $3 \le i \le p+1$, then S has maximal nilpotency class.*

The subgroup U in Theorem 4.1 is an abelian subgroup of S of index p. Therefore, the proof of Proposition 6.4 can be used to prove the first assertion.

Proposition 6.6. *The p-automorphism group S of the Nakajima extremal curve given in Theorem 4.1 has maximal nilpotency class.*

Proof. The subgroup U in Theorem 4.1 is an abelian subgroup of S of index p. Therefore, the proof of Proposition 6.4 can be used to prove the assertion. □

Remark 5. According to Proposition 3.10, the quotient curves of the curve given in Theorem 4.1 are also Nakajima extremal curves. Their p-automorphism groups have maximal nilpotency class, as well, by [22, Section III, 14.2 Hilfssatz].

Proposition 6.7. *The p-automorphism group S of the Nakajima extremal curve given in Theorem 4.4 has no maximal nilpotency class.*

Proof. From Theorem 4.4, the minimum size of a generator set of $\Phi(S)$ is $(p-1)^2$. Since $(p-1)^2 > p-1$, $\Phi(S)$ cannot be generated by $p-1$ elements. If S has maximal nilpotency class, this implies that S must be of order p^{p+1} and isomorphic to the Sylow p-subgroup of the symmetric group of degree p^2, see [3, Theorem 5.2]. Since $|S| = p^{N(p-1)^2+2}$, this yields $N(p-1)^2 + 2 = p+1$, a contradiction which proves the assertion. □

By [22, Chapter III, 14.22 Satz], any p-group of maximal nilpotency class and order bigger than p^{p+1} has exactly one maximal subgroup M which is a regular p-group, namely $M = C_S(\mathbf{K}_2(S)/\mathbf{K}_4(S))$, see [22, Chapter III, 14.3 Definition]. This subgroup, called the *fundamental subgroup*, plays a relevant role in the study of p-groups.

Proposition 6.8. *Let S be the p-automorphism group of a Nakajima extremal curve such that S has maximal nilpotency class and order bigger than p^{p+1}. If $s \in S$ is an element of order p then number of fixed points of s is either zero, or p. Accordingly, the relative quotient curve $\mathcal{Z} = \mathcal{X}/\langle s \rangle$ of $\mathcal{X}$ has genus*

$$\mathfrak{g}(\mathcal{Z}) = \begin{cases} (p-2)p^{n-2}+1, \\ (p-2)p^{n-2}-(p-1)+1. \end{cases} \tag{24}$$

Proof. If s has no fixed point in Ω, then the Hurwitz genus formula together with Proposition 3.3 yields $\mathfrak{g}(\mathcal{Z}) = (p-2)p^{n-2}+1$. Therefore, we focus on an element $s \in S$ which fixes a point in Ω. Then $s \in M_1$ or $s \in M_2$, according as the set Ω_s of the fixed points of s is contained in Ω_1 or in Ω_2. Assume that $\Omega_s \subset \Omega_1$, and let P_1, P_2 be any two distinct points in Ω_s. Since Ω_1 is an S-orbit, there exists $h \in S$ that takes P_1 to P_2. Then hsh^{-1} fixes P_1, and Lemma 3.5 implies that either $hsh^{-1} = s$ or $hsh^{-1} = s^{-1}$. The latter case cannot actually occur as in a p-group a non-trivial element and its inverse are in different conjugacy classes. Therefore, h is in the centralizer $C_S(s)$ of s. The converse also holds. Thus $p|\Omega_s| = |C_S(s)|$.

We show that the fundamental subgroup of S is neither M_1 nor M_2. Assume on the contrary that it is M_1. The argument at the beginning of the proof of Proposition 5.4 shows that M_1 is generated by its elements of order p. Since M_1 is a regular p-group, [22, Chapter III, 10.7 a) Satz] applied to M_1 and $k = 1$, shows that M_1 has exponent p. Now, the last claim of [22, Chapter III, 14.16 Satz] yields $|M_1| = p^{p-1}$, a contradiction. Therefore, one of the other maximal normal subgroups, say M_3, is the fundamental subgroup of S, and $s \in S \setminus M_3$.

From [22, Chapter III, 14.6 a) Satz], $M_3 = C_S(S_i/S_{i+2})$ for $2 \le i \le n-3$. Here $|S| = p^n$, $S_i = \mathbf{K}_i(S)$ for $i = 2, \dots n$, in particular, $|S_{n-2}| = p^2$, $S_{n-1} = Z(S)$, $S_n = \{1\}$, see [22, Chapter III, 14.3 Definition]. If $s \notin C_S(S_{n-2})$, [22, Chapter III, 14.13 Hilfssatz b)] yields $|C_S(s)| = p^2$. Otherwise, $s \in C_S(S_{n-2})$, and since $C_S(S_{n-2})$ is a normal subgroup of S, Proposition 3.7 implies $M_1 = C_S(S_{n-2})$. Take a maximal normal subgroup of S, say M_4, other than M_1, M_3. From [22, Chapter III, 14.3 Hilfssatz, Bemerkung] applied to $\mathfrak{U} = M_4$, the hypothesis on s in [22, Chapter III, 14.3 Hilfssatz] is fulfilled. Hence $|C_S(s)| = p^2$ by [22, Chapter III, 14.13 Hilfssatz b)]. Therefore, $|\Omega_s| = p$.

Finally, the Hurwitz genus formula together with Proposition 3.3 yields $\mathfrak{g}(\mathcal{Z}) = (p-2)p^{n-2}-(p-1)+1$. □

The converse of Proposition 6.8 also holds.

Proposition 6.9. *Let S be the p-automorphism group of a Nakajima extremal curve with $|S| = p^n$, $n \ge 3$. If some element $s \in S$ has exactly p fixed points, then S has maximal nilpotency class.*

Proof. The first part of the proof of Proposition 6.8 also shows that if an element $s \in S$ has exactly p fixed points then $|C_S(s)| = p^2$. The latter condition means that the conjugacy class of s in S has size p^{n-2}. Therefore, the claim follows from [22, Chapter III, 14.23 Satz]. $\square$

Theorem 1.2 is corollary of (v) of Proposition 3.12 and Propositions 6.5 and 6.4 together with Propositions 3.6 and 5.2

7. Proof of Theorem 1.3

Lemma 7.1. *Let N be a normal subgroup of $\mathrm{Aut}(\mathcal{X})$ such that the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$ is neither rational nor elliptic. Then the order of N is a power of p. Furthermore, $\bar{\mathcal{X}}$ is an extremal Nakajima curve provided that its genus is bigger than $p-1$.*

Proof. Let $|N| = ap^b$ with a prime to p. We may assume that $S \cap N$ is a Sylow subgroup of N. From the Hurwitz genus formula applied to N, $\mathfrak{g} - 1 = p^{n-1}(p-2) \geq ap^b(\bar{\mathfrak{g}} - 1)$. On the other hand, since $SN/N \cong S/S \cap N$ is a $\mathbb{K}$-automorphism group of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$ whose order is p^{n-b}, the Nakajima bound gives $p^{n-b-1}(p-2) \leq \bar{\mathfrak{g}} - 1$. Then,

$$\tfrac{p-2}{a} p^{n-1-b} \geq \bar{\mathfrak{g}} - 1 \geq p^{n-1-b}(p-2).$$

Therefore $a = 1$ and this proves the assertion. $\square$

Lemma 7.2. *Let N be a normal subgroup of $\mathrm{Aut}(\mathcal{X})$ such that the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$ is rational. Then the order of N is a divisible by p^{n-1}.*

Proof. By Proposition 3.3 S has two short orbits, Ω_1 and Ω_2, both of size p^{n-1}. Since S normalizes N, the Hurwitz genus formula applied to N gives

$$2\mathfrak{g} - 2 = 2(p-2)p^{n-1} = -2|N| + p^{n-1}(d_P + d_Q) + \kappa p^n$$

with $P \in \Omega_1$, $Q \in \Omega_2$ and κ non-negative integer. From this the assertion follows. $\square$

To obtain a similar result for the case where $\bar{\mathcal{X}}$ is elliptic, we need some technical results.

Lemma 7.3. *Assume that S is not a normal subgroup of $\mathrm{Aut}(\mathcal{X})$ and that T is a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X})$ other than S. If there exists a point $P \in \Omega_1$ fixed by a non-trivial element of T then no point in Ω_2 is fixed by a non-trivial element of T.*

Proof. Let $G = \mathrm{Aut}(\mathcal{X})$. In G_P, all $\mathbb{K}$-automorphisms of order a power of p lie in the first ramification group $G_P^{(1)}$. Obviously, $G_P^{(1)}$ contains both S_P and T_P. Actually $S_P = T_P$ must hold by virtue of Lemma 3.5 applied to a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X})$ containing $G_P^{(1)}$. Assume on the contrary the existence of a point $Q \in \Omega_2$ fixed by a non-trivial element of T. As before this yields $S_Q = T_Q$. Hence $\langle S_P, S_Q\rangle = \langle T_P, T_Q\rangle$. By (v) of Proposition 3.12, $S = \langle S_P, S_Q\rangle$. Therefore, $S \le T$. Since S and T are Sylow p-subgroups of $\mathrm{Aut}(\mathcal{X})$, this yields $S = T$. □

Lemma 7.4. *If a Sylow p-subgroup T of* $\mathrm{Aut}(\mathcal{X})$ *preserves $\Omega_1 \cup \Omega_2$ then it does both Ω_1 and Ω_2.*

Proof. We may assume that $T \ne S$. The assertion follows from Lemma 7.3. □

Lemma 7.5. *Assume that S is not a normal subgroup of* $\mathrm{Aut}(\mathcal{X})$*. If Ω_1 is preserved by all Sylow p-subgroups of* $\mathrm{Aut}(\mathcal{X})$ *then M_1 is a normal subgroup of* $\mathrm{Aut}(\mathcal{X})$*.*

Proof. Let T be any Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X})$ other than S. From the proof of Lemma 7.3, $S_P = T_P$ for every point $P \in \Omega_1$. Since M_1 is generated by all stabilizers S_P with P ranging over Ω_1, this shows that M_1 is a subgroup of T. Therefore, all the Sylow p-subgroups share M_1. Since M_1 has index p in S, M_1 is their complete intersection. From this the assertion follows. □

Lemma 7.6. *Let N be a normal subgroup of* $\mathrm{Aut}(\mathcal{X})$*. Let Π be the set of all points of $\mathcal{X}$ which are fixed by some non-trivial element of N. Assume that S is not a normal subgroup of* $\mathrm{Aut}(\mathcal{X})$*. If $0 < |\Pi| < p^n$ then $\Pi = \Omega_1$ (or $\Pi = \Omega_2$) and M_1 (or M_2) is a normal subgroup of* $\mathrm{Aut}(\mathcal{X})$*.*

Proof. Since N is normal, Π is partitioned in orbits of $\mathrm{Aut}(\mathcal{X})$. In particular, the orbit of $P \in \Pi$ under the action of any Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X})$ is contained in Π. If $|\Pi| \le p^{n-1}$ then $\Pi = \Omega_1$ (or $\Pi = \Omega_2$), and all Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X})$ preserve Ω_1 (or Ω_2). Therefore, the assertion follows from Lemma 7.5. If $p^{n-1} < |\Pi| < p^n$, then $\Pi = \Omega_1 \cup \Omega_2$, and both M_1 and M_2 are normal subgroups of $\mathrm{Aut}(\mathcal{X})$ by Lemmas 7.4 and 7.5. But then $S = \langle M_1, M_2\rangle$ would be normal in $\mathrm{Aut}(\mathcal{X})$, a contradiction. □

Lemma 7.7. *Let N be a normal subgroup of* $\mathrm{Aut}(\mathcal{X})$ *such that the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$ is elliptic. Assume that S is not a normal subgroup of* $\mathrm{Aut}(\mathcal{X})$*. If the order of N is prime to p then M_1 (or M_2) is a normal subgroup of* $\mathrm{Aut}(\mathcal{X})$*.*

Proof. Since $|N|$ is prime to p, S can be regarded as a $\mathbb{K}$-automorphism group of $\bar{\mathcal{X}}$. For $P \in \Omega_1 \cup \Omega_2$, let $\bar{P}$ be the point of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$ lying under P. Since S_P has order p by Lemma 3.5, the point $\bar{P}$ is fixed by a $\mathbb{K}$-automorphism of order p. As p is odd and $\bar{\mathcal{X}}$ is elliptic, we have $p = 3$; see [21, Theorem 11.84]. From the Hurwitz genus formula applied to N,

$$\mathfrak{g} - 1 = 3^{n-1} = 3^{n-1}\tfrac{1}{2}(d_P + d_Q) + \tfrac{\tau}{2}\,3^n$$

with $P \in \Omega_1$, $Q \in \Omega_2$ and τ a non-negative integer. This is only possible when $\tau = 0$ and $d_P + d_Q = 2$. Therefore, either Ω_1, or Ω_2, or $\Omega_1 \cup \Omega_2$ coincide with the set of all points of $\mathcal{X}$ which are fixed by some non-trivial element of N. Now, the assertion follows from Lemma 7.6. □

Lemma 7.8. *For an odd prime d other than p, let U be a d-subgroup of* $\mathrm{Aut}(\mathcal{X})$ *of order d^u and exponent d^e. Then d^{u-e} divides $p-2$.*

Proof. If U has no short orbit, then d^u divides $\mathfrak{g}-1$ by the Hurwitz genus formula applied to U, and the assertion follows. We may assume that U has $m \geq 1$ short orbits and let $\ell_1, \dots, \ell_m$ be their lengths. From the Hurwitz genus formula applied to U,

$$2\mathfrak{g}-2 = 2(p-2)p^{n-1} = d^u(2\bar{\mathfrak{g}}-2) + \sum_{i=1}^{m}(d^u - \ell_i) \tag{25}$$

where $\bar{\mathfrak{g}}$ is the genus of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/U$. Let P be a point from a short orbit of length ℓ_i. Then $d^u = |U_P|\ell_i$. Since U_P is a cyclic subgroup of U, we also have that $|U_P| = p^{u_i} \leq p^e$. Therefore, $\ell_i = d^{u-u_i}$ with $u_i \leq e$. From (25),

$$2(p-2)p^{n-1} = d^{u-e}(d^e(2\bar{\mathfrak{g}}-2) + \sum_{i=1}^{m}(d^e - d^{e-u_i}))$$

whence the assertion follows. □

Lemma 7.9. *For $|S| = p^2$, one of the following cases occurs.*

(i) *$\mathcal{X}$ is an Artin–Mumford curve with affine equation (9), and* $\mathrm{Aut}(\mathcal{X})$ *is the semidirect product of S by a dihedral group of order* $2(p-1)$.
(ii) *M_1 (and M_2) is a normal subgroup of* $\mathrm{Aut}(\mathcal{X})$*, and* $\mathrm{Aut}(\mathcal{X})$ *is the semidirect product of S by a subgroup of a cyclic group of order $p-1$.*

Proof. Let $\bar{\mathcal{X}} = \mathcal{X}/M_1$. By Proposition 3.14, $\mathbb{K}(\mathcal{X})|\mathbb{K}(\bar{\mathcal{X}})$ is an Artin–Schreier extension. Therefore, since $|M_1| = p$, M_1 is a normal subgroup $\mathrm{Aut}(\mathcal{X})$ with four exceptions by a result of Madan and Valentini [40]; see also [21, Theorem 11.93]. One exception is given in case (i). Two of the other three exceptions have zero p-rank, while the forth has genus 2, and hence they cannot actually occur in our case.

The above argument holds true for M_2, and hence we may assume that both M_1 and M_2 are normal subgroups of $\mathrm{Aut}(\mathcal{X})$. Since S is generated by M_1 and M_2, it turns out that S is also a normal subgroup of $\mathrm{Aut}(\mathcal{X})$. By Proposition 3.14, the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/M_1$ is rational. Therefore $\mathrm{Aut}(\mathcal{X})/M_1$ is isomorphic to a subgroup Λ of $PGL(2,\mathbb{K})$. Furthermore, S/M_1 is isomorphic to a normal subgroup of Λ of order p. Also, $p^2 \nmid |\Lambda|$, since S is a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X})$. From the classification of subgroups of $PGL(2,\mathbb{K})$, see [22, Chapter II. Hauptsatz 8.27] and [40], $|\Lambda| = pm$ with $m|(p-1)$ and hence Λ is a semidirect product of S/M_1 by a cyclic group L of order m. Therefore, $\mathrm{Aut}(\mathcal{X})/S$ is isomorphic to L and the assertion is proven. □

Remark 6. The property of $\mathrm{Aut}(\mathcal{X})$ given in (i) of Lemma 7.9 characterizes the Artin–Mumford curve; see [1].

Lemma 7.10. *Any* 2*-subgroup of* $\mathrm{Aut}(\mathcal{X})$ *has a cyclic subgroup of index* 2*.*

Proof. Let U be a subgroup of $\mathrm{Aut}(\mathcal{X})$ of order $d = 2^u \geq 2$. From the Hurwitz genus formula applied to U,

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

where $\bar{\mathfrak{g}}$ is the genus of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/U$ and $\ell_1, \ldots, \ell_m$ are the short orbits of U on $\mathcal{X}$. Since $2(p-2)p^{n-1} \equiv 2 \pmod 4$ while $2^u(2\bar{\mathfrak{g}} - 2) \equiv 0 \pmod 4$, 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 $\mathcal{X}$ and hence is cyclic. □

Remark 7. From Lemma 7.10 and [22, Chapter I, Satz 14.9], any 2-subgroup of $\mathrm{Aut}(\mathcal{X})$ is either cyclic, or abelian with a cyclic subgroup of index 2, or generalized quaternion, or dihedral, or semidihedral, or type (3) with Huppert's notation [22]. This together with deep results from Group theory, see [2,17,18,41] yields that if G is a non-abelian simple subgroup of $\mathrm{Aut}(\mathcal{X})$, then a Sylow 2-subgroup of G is either dihedral, or semidihedral. In the former case, $G \cong PSL(2,q)$, with $q \geq 5$ or $G \cong \mathrm{Alt}_7$ (the Gorenstein–Walter theorem); in the latter case, $G \cong PSL(3,q)$ with $q \equiv 3 \pmod 4$, or $G \cong PSU(3,q)$ with $q \equiv 1 \pmod 4$, or $G = M_{11}$, where q is an odd prime power (the Alperin–Brauer–Gorenstein theorem).

We are going to investigate the possibilities of the existence of a simple normal subgroup N in $\mathrm{Aut}(\mathcal{X})$, as described in Remark 7. For our purpose, it will be sufficient to consider the cases when the quotient curve $\mathcal{X}/N$ is rational. Under this hypothesis, p divides $|N|$. In fact, otherwise S is an abelian p-subgroup of $PGL(2,\mathbb{K})$, and hence $n = 2$ by Proposition 3.6, while $\mathrm{Aut}(\mathcal{X})$ is solvable for $n = 2$ by Lemma 7.9.

Lemma 7.11. *Let N be a normal subgroup of* $\mathrm{Aut}(\mathcal{X})$ *such that the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$ is rational. Then N is not isomorphic to $PSU(3,q)$ with $q \equiv 1 \pmod 4$.*

Proof. Let $\mu = 3$ or $\mu = 1$ according as 3 divides $q+1$ or does not, and factorize the order of $PSU(3,q)$ as $q^3(q^2-q+1)(q-1)(q+1)^2/\mu$.

Assume first that p is prime to q. Since a Sylow subgroup M of $PSU(3,q)$ of order q^3 has exponent at most q, Lemma 7.8 applied to M yields $q^2 \mid (p-2)$. On the other hand, as p divides one of the integers $q^2-q+1, q-1, q+1$, we have $p < q^2$. This contradiction proves the claim for $(p,q) = 1$.

Assume that $q = p^m$ for some $m \geq 1$. Take a subgroup in $PSU(3,q)$ that is the direct product of two cyclic groups C and C_1 both of odd order $\frac{1}{2}(q+1)/\mu$. Write

$|C| = p_1^{u_1} \cdots p_t^{u_t}$ with $p_1, \dots, p_t$ pairwise distinct prime numbers. Obviously, the subgroup G_i of G of order $p_i^{2u_i}$ has exponent p^{u_i}. Since $p \nmid (q+1)/\mu$, Lemma 7.8 applied to G_i yields that $p_i^{u_i}$ divides $p-2$. Therefore, $|C|$ itself divides $p-2$ showing that $(\frac{1}{2}(q+1)/\mu) \mid (p-2)$. From this, $\lambda(p^m+1) = 2\mu(p-2)$ for a positive integer λ, whence $p^m \in \{5, 17\}$ follows. We may assume that S contains M.

We show that $S = M$. For $q \in \{5, 17\}$, $|\mathrm{Aut}(PSU(3,q))| = 6|PSU(3,q)|$ holds, and hence no element in $S \setminus M$ is in $\mathrm{Aut}(PSU(3,q))$. Therefore, if we suppose S to be larger than M, the elements of S not in M commute with M. According to (v) of Lemma 3.12, take a pair $\{s_1, s_2\}$ of generators of S, both of order p. Obviously, one of them, say s_1, is not in M. Then s_2 is not M as well, otherwise $|S| = p^2 < p^3 = |M|$. Therefore, every element in M is falls in $Z(S)$ as both s_1 and s_2 commute with M. But then M is contained in $Z(S)$ which is impossible since M is not abelian.

It remains to rule out the possibility that either $|S| = |M| = 5^3$ or $|S| = |M| = 17^3$. Assume first that $|S| = 5^3$. From Propositions 3.8 and 3.9, the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/Z(S)$ is a Nakajima extremal curve of genus $\bar{\mathfrak{g}} = (p-2)p = 15$. By Lemma 7.9, a Sylow 2-subgroup of $\mathrm{Aut}(\mathcal{X})$ is a subgroup of a dihedral group of order $2(p-1) = 8$. On the other hand, the normalizer T of $Z(S)$ in $PSU(3,5)$ has order $1000 = 8 \cdot 125$ and its factor group $\bar{T} = T/Z(S)$ has a cyclic group of order 8. Since $\bar{T}$ is a subgroup of $\mathrm{Aut}(\bar{\mathcal{X}})$, this is impossible. The proof for $|S| = 17^3$ is analogous. In fact, the normalizer T of $Z(S)$ in $PSU(3,17)$ has order $32 \cdot 3 \cdot 17^3$ and the factor group $\bar{T} = T/Z(S)$ has a cyclic group of order 32. $\square$

Lemma 7.12. *Let N be a normal subgroup of* $\mathrm{Aut}(\mathcal{X})$ *such that the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$ is rational. Then N is not isomorphic to $PSL(3,q)$ with $q \equiv 3 \pmod 4$.*

Proof. We argue as in the proof of Lemma 7.11. Let $\mu = 3$ or $\mu = 1$ according as 3 divides $q-1$ or does not, and factorize the order of $PSL(3,q)$ as $q^3(q^2+q+1)(q+1)(q-1)^2/\mu$.

Assume first that p is prime to q. Since a Sylow subgroup M of $PSL(3,q)$ of order q^3 has exponent at most q, Lemma 7.8 applied to M yields $q^2 \mid (p-2)$. On the other hand, as p divides one of the integers $q^2+q+1, q-1, q+1$, we have either $p < q^2$, or $p = q^2+q+1$. Both cases are inconsistent with $q^2 \mid (p-2)$. This contradiction proves the claim for $(p,q) = 1$.

Assume that $q = p^m$ for some $m \geq 1$. Then $p \equiv 3 \pmod 4$. Take a subgroup in $PSL(3,q)$ that is the direct product of two cyclic groups C and C_1 both of odd order $\frac{1}{2}(q-1)/\mu$. Write $|C| = p_1^{u_1} \cdots p_t^{u_t}$ with $p_1, \dots, p_t$ pairwise distinct prime numbers. Obviously, the subgroup G_i of G of order $p_i^{2u_i}$ has exponent p^{u_i}. Since $p \nmid (q-1)/\mu$, Lemma 7.8 applied to G_i yields that $p_i^{u_i}$ divides $p-2$. Therefore, $|C|$ itself divides $p-2$ showing that $(\frac{1}{2}(q-1)/\mu) \mid (p-2)$. From this, $\lambda(p^m-1) = 2\mu(p-2)$ for a positive integer λ, whence either $p^m = 3$, or $p^m = 7$ follow. We may assume that S contains M. As in the proof of Lemma 7.11, this implies $S = M$ since $|\mathrm{Aut}(PSL(3,3))| = 2|PSL(3,3)|$ and $|\mathrm{Aut}(PSL(3,7))| = 6|PSL(3,7)|$.

Assume that $p^m = 7$. Then $N \cong PSL(3,7)$, and $S \cong UT(3,7)$ whose center $Z(S)$ has order 7. The normalizer L of $Z(S)$ in N has order $4116 = 7^3 \cdot 12$, and the factor group $L/Z(S)$ is the semidirect product of a normal subgroup $S/Z(S)$ of order 7^2 by an abelian subgroup of order 12. Such a group $L/Z(S)$ is a subgroup of the $\mathbb{K}$-automorphism group of the Nakajima extremal curve $\mathcal{X}/Z(S)$ of genus $15 = 7 \cdot (7-5) + 1$. Since a dihedral group of order bigger than 4 is not abelian, this contradicts Lemma 7.9.

Assume that $p^m = 3$. Take a subgroup C of $PSL(3,3)$ of order 13. The Hurwitz formula applied to C yields that $9 = 13(\bar{\mathfrak{g}} - 1) + 6\lambda$ where $\bar{\mathfrak{g}}$ is the genus of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/C$ and λ is an integer. Therefore, $\bar{\mathfrak{g}} = 0$ and hence $22 = 6\lambda$ which is impossible. □

Lemma 7.13. *Let N be a normal subgroup of* Aut$(\mathcal{X})$ *such that the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$ is rational. Then N is not isomorphic to $PSL(2,q)$ with $q \geq 5$.*

Proof. Assume on the contrary that $N \cong PSL(2,q)$ with $q \geq 5$, and choose a Sylow p-subgroup T of N. By Lemma 7.2, T is a subgroup of S of index at most p. By Proposition 6.3, T is a non-cyclic group. From the classification of subgroups of $PSL(2,q)$, see [22, Chapter II. Hauptsatz 8.27] and [40], T is an elementary abelian group of order q where q is a power of p. If $S = T$ then S is elementary abelian as well, and hence $|S| = p^2$, by Proposition 3.6. But then, by Lemma 7.9, $\mathrm{Aut}(\mathcal{X})$ is solvable and hence contains no subgroup isomorphic to $PSL(2,q)$ with $q \geq 5$.

Therefore, $[S : T] = p$. We show that $q = p^r$ with r divisible by p. Take an element $s \in S$ not in T. Since s normalizes N, either s induces an automorphism of N, or centralizes N. The latter case cannot actually occur as S is not abelian by Proposition 3.6. Thus $s \in \mathrm{Aut}(N)$. From [22, Chapter II, Aufgabe 15], the automorphism group of $PSL(2,p^r)$ is $P\Gamma L(2,p^r)$. Since $P\Gamma L(2,p^r)$ only contains p-elements other than those in $PSL(2,p^r)$ when $p \mid r$, we have that $r = \lambda p$ for an integer λ.

The normalizer of T in N is a semidirect product $T \rtimes C$ with a cyclic group C of order $\frac{1}{2}(q-1)$. Since T is a normal subgroup of S, the normalizer of T in $\mathrm{Aut}(\mathcal{X})$ also contains S. Actually, S also normalizes $T \rtimes C$. In fact, since S normalizes T, any subgroup $s^{-1}(T \rtimes C)s$ with $s \in S$ is a subgroup of N containing T. Since $p \geq 5$, the classification of subgroups of $PSL(2,q)$, see [22, Chapter II. Hauptsatz 8.27] and [40], yields that N has a unique subgroup of order $\frac{1}{2}q(q-1)$ containing T. Therefore, $s^{-1}(T \rtimes C)s = T \rtimes C$. It turns out that $S(T \rtimes C)$ is a subgroup of the normalizer of T in $\mathrm{Aut}(\mathcal{X})$ whose order is $\frac{1}{2}(q-1)|S|$. Therefore, since $[S : T] = p$, the factor group $S(T \rtimes C)/T$ has order $\frac{1}{2}p(q-1)$, and it may be regarded as a $\mathbb{K}$-automorphism group of the quotient curve $\mathcal{Y} = \mathcal{X}/T$. Observe that $\frac{1}{2}p(q-1) \geq \frac{1}{2}5(5^5 - 1) > 60$.

Two cases arise according as $\mathcal{Y}$ is rational or not.

In the former case, $S(T \rtimes C)/T$ is isomorphic to a subgroup of $PGL(2,\mathbb{K})$. From the classification of subgroups of $PSL(2,\mathbb{K})$, see [22, Chapter II. Hauptsatz 8.27] and [40], $q = p$ must hold. But we have already shown that $r > 1$, a contradiction.

In the latter case, Proposition 3.14 yields that T is one of the subgroups M_i with $3 \leq i \leq p+1$, and hence by Proposition 3.15 the curve $\mathcal{Y}$ satisfies the hypotheses of Proposition 2.1. For $p > 3$, Proposition 2.1 yields that C is isomorphic to a subgroup of a dihedral group of order $2(p-1)$. Therefore $\frac{1}{2}(q-1)$ divides $p-1$. Since $q = p^r$ with $r > 1$ is this is impossible. For $p = 3$, Proposition 2.1 gives some more possibilities namely that C is isomorphic to a cyclic subgroup of $GL(2,3)$. Then $|C| \in \{2,3,4,6,8\}$, but none of these number is equal to $\frac{1}{2}(q-1)$ for $q = 3^r$ with r divisible by 3. $\square$

Lemma 7.14. *Let N be a normal subgroup of* $\mathrm{Aut}(\mathcal{X})$ *such that the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$ is rational. Then N is not isomorphic to $N \cong \mathrm{Alt}_7$ or $N \cong \mathrm{M}_{11}$.*

Proof. Since both Alt_7 and M_{11} have subgroups of odd non-prime order d only for $d = 9$, Lemma 7.2 yields $p = 3$ and $n = 3$. Since the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$ is rational, and neither Alt_7 nor M_{11} has an outer automorphism of order 3, the case $n = 3$ can only occur if each element of $S \setminus N$ centralizes N. But then S would be abelian contradicting Proposition 3.6. $\square$

Proposition 7.15. *Let N be a minimal normal subgroup of* $\mathrm{Aut}(\mathcal{X})$ *such that the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$ is rational. Then N is an elementary abelian group.*

Proof. Assume on the contrary that N is isomorphic to the direct product $R_1 \times \ldots \times R_k$ of pairwise isomorphic non-abelian simple groups. Let U_i be a Sylow 2-subgroup of R_i for $i = 1, \ldots k$. By Remark 7, U_i is either dihedral or semidihedral. Therefore N contains a 2-subgroup which is the direct product of k dihedral, or semidihedral groups. This implies for $k > 1$ that N contains an elementary abelian subgroup of order 8, but this contradicts Lemma 7.10. Therefore $k = 1$. Now, the assertion follows from Remark 7 together with Lemmas 7.11, 7.12, 7.13, and 7.14. $\square$

Lemma 7.16. *Let U be a 2-subgroup of* $\mathrm{Aut}(\mathcal{X})$*. If U normalizes M_1 (or M_2) then U is cyclic.*

Proof. By Proposition 3.14, M_1 has p orbits on Ω_1 each of length p^{n-2}. Since Ω_1 is the set of points which are fixed by some non-trivial elements of M_1, U preserves Ω_1, and induces a permutation group on the set of the p^{n-2} M_1-orbits. As U has order a power of 2, it preserves some of these M_1-orbits. Since the length of such a U-invariant M_1-orbit is odd, some point of it must be fixed by U. Therefore, U fixes a point of $\mathcal{X}$, and hence U is cyclic. $\square$

We are in a position to prove Theorem 1.3.

Our proof is by induction on the order of S. The assertion holds for $|S| = p^2$ by Lemma 7.9. Assume that it holds for all extremal Nakajima curves with Sylow p-subgroup of order p^k with $2 \leq k \leq n-1$. Take a minimal normal subgroup N of $\mathrm{Aut}(\mathcal{X})$. If the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$ is not elliptic then Lemmas 7.1 and 7.2 together with

Proposition 7.15 show that N is a p-group and hence it is a subgroup of S. If $\bar{\mathcal{X}} = \mathcal{X}/N$ is elliptic and N is not a p-group, replace N with $\Phi(S)$ when S is a normal subgroup of $\mathrm{Aut}(\mathcal{X})$, otherwise replace N with or M_1 (or M_2) according to Lemma 7.7. Therefore, N may be assumed to be a p-group.

If N is semiregular on $\mathcal{X}$, then the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$ has positive p-rank, and one of the cases (ii) or (iii) of Theorem 1.1 occurs. Therefore, $\bar{\mathcal{X}}$ is either an extremal Nakajima curve, or a curve of genus $p-1$ given in Proposition 2.1, where S/N is a Sylow p-subgroup of $\mathrm{Aut}(\bar{\mathcal{X}})$. In case (iii), Theorem 1.3 holds for $\bar{\mathcal{X}}$ by induction, and accordingly let $\bar{L} = \bar{S}$ when $\bar{S}$ is a normal subgroup of $\mathrm{Aut}(\bar{\mathcal{X}})$, but let $\bar{L} = \bar{M}$ when the sporadic case $p = 3$ with $GL(2,3)$ occurs. In case (ii), Proposition 2.1 holds for $\bar{\mathcal{X}}$, and let $\bar{L} = \bar{S}$ when $\bar{S}$ is a normal subgroup of $\mathrm{Aut}(\bar{\mathcal{X}})$, but let $\bar{L}$ be the identity subgroup when the sporadic case $p = 3$ with $GL(2,3)$ occurs. Since $\bar{L}$ is contained in S/N, there exists a normal subgroup L of $\mathrm{Aut}(\mathcal{X})$ containing N such that $L/N = \bar{L}$. Then L is a p-group and

$$\frac{\mathrm{Aut}(\mathcal{X})}{L} \cong \frac{\mathrm{Aut}(\mathcal{X})/N}{L/N} \cong \frac{\bar{G}}{\bar{L}}$$

where $\bar{G}$ is a subgroup of $\mathrm{Aut}(\bar{\mathcal{X}})$. If $\bar{S} = \bar{L}$ then $S = L$ and hence $\bar{G}$ has order prime to p. By induction, $\bar{G}$ is a subgroup of a dihedral group of order $2(p-1)$, and hence Theorem 1.3 holds. If $[\bar{S} : \bar{L}] = p$ then $p = 3$, and $3 \mid |G|$. By induction, $\bar{G}$ is isomorphic to a subgroup of $GL(2,3)$, and hence Theorem 1.3 holds.

If N is not semiregular on $\mathcal{X}$, Proposition 3.7 shows that $N = M_1$ (or $N = M_2$). From Proposition 3.14, the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/N$ is rational. Therefore, $\mathrm{Aut}(\mathcal{X})/N$ is isomorphic to a subgroup Γ of $PGL(2,\mathbb{K})$. As S is a Sylow p-subgroup of $\mathrm{Aut}(\mathcal{X})$ containing M_1 and $[S : M_1] = p$, the order of Γ is divisible by p but not by p^2. Also, a Sylow 2-subgroup of Γ is cyclic, by Lemma 7.16. In particular, Γ is not isomorphic to Alt_4, or Sym_4, or Alt_5, or $PSL(2,q)$, or $PGL(2,q)$ with a power q of p. From the classification of finite subgroups of $PGL(2,\mathbb{K})$, see [40] or [21, Theorem A.8], we are left with only one possibility for Γ, namely a subgroup of the semidirect product of S/M_1 by a cyclic group whose order divides $p-1$. Hence Theorem 1.3 holds.

Our proof of Theorem 1.3 also shows that if $\mathbb{K}(\mathcal{X})$ is not an unramified Galois extension of the Artin–Mumford function field then the dihedral subgroup of order $2(p-1)$ may be weakened to the cyclic group of order $p-1$.

8. Nakajima extremal curves with small genera for $p = 3$

Proposition 8.1. *Let $p = 3$. If S has maximal class then $\Phi(S)$ is an abelian metacyclic group.*

Proof. We may assume that $|\Phi(S)| = 3^m$ with $m \geq 3$. From (ii) of Proposition 3.12, $|S| = 3^{m+2} \geq 3^5$. From [3, Theorem 5.2], every subgroup of S can be generated by two elements. Therefore, $d(\Phi(S)) = 2$. Assume on the contrary that $\Phi(S)$ is not abelian. From [24, Theorem 3], $\Phi(S)$ is metacyclic. Since $\Phi(S)$ is supposed to be non-abelian, [24, Theorem 1] shows the existence of a metacyclic subgroup B of S such that $\Phi(B) = \Phi(S)$. By Proposition 6.1, B is a proper subgroup of S containing $\Phi(S)$. Since B is finite, $B \neq \Phi(B)$ and hence $[B : \Phi(S)] = p$. The Burnside fundamental theorem, [22, Chapter III, Satz 3.15] yields that B and hence $\Phi(S)$ is cyclic, a contradiction. □

8.1. 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.

Proposition 8.2. *Let $p = 3$. Up to isomorphisms, the Artin–Mumford curve with affine equation (9) is the unique extremal Nakajima curve of genus 4.*

Proof. See the preliminary version of the paper [16]. □

8.2. Case $|S| = 27$

In this case, the maximal subgroups of S are elementary abelian groups of order 9 and Theorem 4.2 applies. Therefore, the Nakajima extremal curves of genus 10 are the curves $\mathcal{X}_c$ as given in Proposition 5.3. A different presentation of the function field $\mathbb{K}(\mathcal{X}_c)$ of $\mathcal{X}_c$ is $\mathbb{K}(\mathcal{X}_c) = \mathbb{K}(u, v, y, x)$ where

(i) $u(v^3 - v) + u^2 - c = 0$;
(ii) $y^3 - y - u = 0$;
(iii) $(z^3 - z)(v^3 + 1) + v^3 - v^2 - u = 0$.

Here, both $\mathbb{K}(u, v, y)$ and $\mathbb{K}(u, v, z)$ are unramified degree p Galois-extensions of $\mathbb{K}(u, v)$, and $\mathbb{K}(\mathcal{X}_c)$ can be obtained as the special case $p = 3$, $N = 1$ of the construction given in Section 4.

8.3. Case $|S| = 81$

Lemma 8.3. *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) $S \cong S(81, 9) = \langle a, b, c | a^9 = b^3 = c^3 = 1, ab = ba, cac^{-1} = ab^{-1}, cbc^{-1} = a^3 b\rangle$ *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 $i=1,\dots,7$, and each of them has an abelian normal subgroup of index 3. By Proposition 6.5, 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 $UT(3,3)$ and hence it contains all elements of order 3. On the other hand, (iv) of Proposition 3.12 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 3.12 and 3.13. □

We point out that both cases in Lemma 8.3 occur. The curve $\mathcal{X}$ with function field $\mathbb{K}(x,y,u,s,w)$ defined by the equations

(i) $x(y^3-y)-x^2-1=0$;
(ii) $u^3-u-x=0$;
(iii) $(u-y)(w^3-w)-1=0$;
(iv) $(u-(y+1))(s^3-s)-1=0$

has genus $\mathfrak{g}(\mathcal{X})=28$ and it has a $\mathbb{K}$-automorphism group $S \cong S(81,7)$ generated by g_1,g_2,g_3,g_4,g_5 where

$$\begin{aligned}
g_1 &: (x,y,u,w,s) \mapsto (x,y+1,u,s,u-w-s),\\
g_2 &: (x,y,u,w,s) \mapsto (x,y+1,u,s,u-w-s),\\
g_3 &: (x,y,u,w,s) \mapsto (x,y+1,u+1,w,s),\\
g_4 &: (x,y,u,w,s) \mapsto (x,y,u,w+1,s),\\
g_5 &: (x,y,u,w,s) \mapsto (x,y,u,w,s+1).
\end{aligned}$$

To show an example for the other case, we apply Theorem 4.1 for $N=2$ and obtain a Nakajima extremal curve of genus 82 with a $\mathbb{K}$-automorphism group S such that

(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 $M_1 \cong C_9 \times C_9$.

Since $|Z(S)| = 3$, Proposition 3.9 applied to $N = Z(S)$ yields the existence of a Nakajima extremal curve of genus 28 with a $\mathbb{K}$-automorphism group isomorphic to $S/Z(S)$. Here $S/Z(S) \cong S(81, 10)$ and therefore this curve provides an example for Case (b).

8.4. Case $|S| = 243, 729$

Proposition 8.4. *If* $|S| = 243$ *and* S *has a maximal abelian subgroup, then there are only two possibilities for* S*, namely* (i) *and*

(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 8.3 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 8.3 that ruled out possibility (d). Therefore, $S \cong S(243, 25)$ and $S \cong S(243, 28)$ cannot occur in our situation. □

Theorem 4.4 applied to $p = 3$, $N = 1$ provides a Nakajima extremal curve $\mathcal{X}$ of genus $\mathfrak{g} = 244$ and $|S| = 729$ so that $\Phi(S)$ is the direct product of two cyclic groups of order 9. Using this and some other properties of S established before and relying on the database of GAP, it is possible to prove that $S = S(729, 34)$. Therefore, S has nilpotency class 4 and $|Z(S)| = 3$. Moreover, $|\mathrm{Aut}(\Phi(S))| = 2^9 \cdot 3^5 \cdot 5 \cdot 11$ which is equal to $(3^4 - 1)(3^4 - 3)(3^4 - 3^2)(3^4 - 3^3)$. Since $d(\Phi(S)) = 4$, this shows that $\Phi(S)$ hits the Burnside–Hall bound (14) and hence $\mathcal{X}$ is the unique Nakajima extremal curve of genus $\mathfrak{g} = 244$ with $S = S(729, 34)$. The quotient curve $\bar{\mathcal{X}} = \mathcal{X}/Z(S)$ is a Nakajima extremal curve of genus $\mathfrak{g} = 82$ and its $\mathbb{K}$-automorphism group $\bar{S} = S/Z(S)$ is $S(243, 3)$. In particular, $\bar{S}$ has nilpotency class 3 and $Z(\bar{S}) = 9$. Moreover, $Z(\bar{S})$ contains two subgroups, say $\bar{T}_1$ and $\bar{T}_2$, of order 3 so that the arising quotient curves $\bar{\mathcal{X}}/\bar{T}_1$ and $\bar{\mathcal{X}}/\bar{T}_2$ are non-isomorphic Nakajima extremal curves of genus 28. Therefore, they are the curves given in Lemma 8.3.

References

[1] N. Arakelian, G. Korchmáros, A characterization of the Artin–Mumford curve, J. Number Theory 154 (2015) 278–291.

[2] J.L. Alperin, R. Brauer, D. Gorenstein, Finite groups with quasi-dihedral and wreathed Sylow 2-subgroups, Trans. Amer. Math. Soc. 151 (1970) 1–261.

[3] Y. Berkovich, On subgroups and epimorphic images of finite p-groups, J. Algebra 248 (2002) 472–553.
[4] Y. Berkovich, Short proofs of some basic characterization theorems of finite p-group theory, Glas. Mat. 41 (2006) 239–258.
[5] Y. Berkovich, Groups of Prime Power Order. Vol. I, Walter de Gruyter GmbH & Co. KG, Berlin, 2008, xx+512 pp.
[6] Y. Berkovich, Z. Janko, Groups of Prime Power Order. Vol II, Walter de Gruyter GmbH & Co. KG, Berlin, 2008, xvi+596 pp.
[7] Y. Berkovich, Z. Janko, Groups of Prime Power Order. Vol III, Walter de Gruyter GmbH & Co. KG, Berlin, 2011, xxvi+639 pp.
[8] N. Blackburn, On prime-power groups with two generators, Proc. Cambridge Philos. Soc. 54 (1958) 327–337.
[9] I.I. Bouw, The p-rank of ramified covers of covers, Compos. Math. 126 (2001) 209–322.
[10] G. Cardona, On the number of curves of genus 2 over a finite field, Finite Fields Appl. 9 (2003) 505–526.
[11] G. Cardona, 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.
[12] M. Giulietti, G. Korchmáros, Large 2-groups of automorphisms of algebraic curves over a field of characteristic 2, J. Algebra 427 (2015) 264–294.
[13] M. Giulietti, G. Korchmáros, Algebraic curves with a large non-tame automorphism group fixing no point, Trans. Amer. Math. Soc. 362 (2010) 5983–6001.
[14] M. Giulietti, G. Korchmáros, Automorphism groups of algebraic curves with p-rank zero, J. Lond. Math. Soc. 81 (2) (2010) 277–296.
[15] M. Giulietti, G. Korchmáros, Garden of curves with many automorphisms, in: Harald Niederreiter, Alina Ostafe, Daniel Panario, Arne Winterhof (Eds.), Algebraic Curves and Finite Fields, in: Radon Ser. Comput. Appl. Math., vol. 16, De Gruyter, 2014, pp. 93–120.
[16] M. Giulietti, G. Korchmáros, Large p-groups of automorphisms of algebraic curves in characteristic p, arXiv:1507.03737 [math.AG].
[17] D. Gorenstein, J.H. Walter, The characterization of finite groups with dihedral Sylow 2-subgroups. I, J. Algebra 2 (1965) 85–151.
[18] D. Gorenstein, J.H. Walter, The characterization of finite groups with dihedral Sylow 2-subgroups. II, J. Algebra 2 (1965) 218–270.
[19] R. Guralnick, B. Malmskog, R. Pries, The automorphism groups of a family of maximal curves, J. Algebra 361 (2012) 92–106.
[20] M. Hall Jr., The Theory of Groups, Chelsea Publ. Comp., New York, 1976, xiii+434 pp.
[21] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves Over a Finite Field, Princeton Univ. Press, Princeton and Oxford, 2008, xx+696 pp.
[22] B. Huppert, Endliche Gruppen. I, Grundlehren Math. Wiss., vol. 134, Springer, Berlin, 1967, xii+793 pp.
[23] J. Igusa, Arithmetic variety moduli for genus 2, Ann. of Math. (2) 72 (1960) 612–649.
[24] G.L. Lange, Two-generator Frattini subgroups of finite p-groups, Israel J. Math. 29 (1978) 357–360.
[25] C. Lehr, M. Matignon, Automorphism groups for p-cyclic covers of the affine line, Compos. Math. 141 (2005) 1213–1237.
[26] M. Matignon, M. Rocher, On smooth curves endowed with a large automorphism p-group in characteristic $p > 0$, Algebra Number Theory 2 (2008) 887–926.
[27] S. Nakajima, p-ranks and automorphism groups of algebraic curves, Trans. Amer. Math. Soc. 303 (1987) 595–607.
[28] A. Pacheco, Unramified Galois coverings of algebraic curves, J. Number Theory 53 (1995) 211–228.
[29] A. Pacheco, K. Stevenson, Finite quotients of the algebraic fundamental group of projective curves in positive characteristic, Pacific J. Math. 192 (2000) 143–158.
[30] R. Pries, K. Stevenson, A survey of Galois theory of curves in characteristic p, in: Women in Numbers: Research Directions in Number Theory, in: Fields Inst. Commun., vol. 60, Amer. Math. Soc., Providence, RI, 2011, pp. 169–191.
[31] M. Rocher, Large p-groups actions with a p-elementary abelian second ramification group, J. Algebra 321 (2009) 704–740.
[32] M. Rocher, Large p-groups actions with $|G|/g^2 > 4/(p^2-1)^2$, arXiv:0801.3494v1 [math.A.G.].
[33] H.L. Schmid, E. Witt, Unverzweigte abelsche Körper vom Exponenten p^n über einem algebraischen Funktionenkörper der Charakteristik p, J. Reine Angew. Math. 176 (1936) 168–173.

[34] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe, Arch. Math. 24 (1973) 527–544.
[35] J.-P. Serre, Local Fields, Grad. Texts in Math., vol. 67, Springer, New York, 1979, viii+241 pp.
[36] I.R. Shafarevich, On p-extensions, Amer. Math. Soc. Transl. 4 (1954) 59–71.
[37] T. Shaska, L. Beshaj, The arithmetic of genus two curves, in: Information Security, Coding Theory and Related Combinatorics, in: NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 29, IOS, Amsterdam, 2011, pp. 59–98.
[38] H. Stichtenoth, Algebraic Function Fields and Codes, 2nd edition, Springer-Verlag, Berlin Heidelberg, 2009, xiv+360 pp.
[39] D. Subrao, The p-rank of Artin–Schreier curves, Manuscripta Math. 16 (1975) 169–193.
[40] R.C. Valentini, M.L. Madan, A Hauptsatz of L.E. Dickson and Artin–Schreier extensions, J. Reine Angew. Math. 318 (1980) 156–177.
[41] J.H. Walter, The characterization of finite groups with abelian Sylow 2-subgroups, Ann. of Math. 89 (1969) 405–514.
[42] G. van der Geer, M. van der Vlugt, Kloosterman sums and the p-torsion of certain Jacobians, Math. Ann. 290 (1991) 549–563.
[43] Mingyao Xu, Lijian An, Qinhai Zhang, Finite p-groups all of whose non-abelian proper subgroups are generated by two elements, J. Algebra 319 (2008) 3603–3620.