Automorphism groups of algebraic curves with p-rank zero

M. GIULIETTI AND G. KORCHMÁROS

Abstract. In positive characteristic, algebraic curves can have many more automorphisms than expected from the classical Hurwitz's bound. There even exist algebraic curves of arbitrary high genus g with more than $16g^4$ automorphisms. It has been observed on many occasions that the most anomalous examples invariably have zero p-rank. In this paper, the $\mathbb{K}$-automorphism group $\mathrm{Aut}(\mathcal{X})$ of a zero 2-rank algebraic curve $\mathcal{X}$ defined over an algebraically closed field $\mathbb{K}$ of characteristic 2 is investigated. The main result is that if the curve has genus $g \geq 2$ and $|\mathrm{Aut}(\mathcal{X})| > 24g^2$, then $\mathrm{Aut}(\mathcal{X})$ has a fixed point on $\mathcal{X}$, apart from few exceptions. In the exceptional cases the possibilities for $\mathrm{Aut}(\mathcal{X})$ and g are determined.

1. Introduction

Let $\mathcal{X}$ be a (projective, geometrically irreducible, non-singular) algebraic curve defined over an algebraically closed groundfield $\mathbb{K}$ of characteristic $p \geq 0$. Let $\mathbb{K}(\mathcal{X})$ be the field of rational functions (the function field of one variable over $\mathbb{K}$) of $\mathcal{X}$. The $\mathbb{K}$–automorphism group $\mathrm{Aut}(\mathcal{X})$ of $\mathcal{X}$ is defined to be the automorphism group $\mathrm{Aut}(\mathbb{K}(\mathcal{X}))$ consisting of those automorphisms of $\mathbb{K}(\mathcal{X})$ which fix each element of $\mathbb{K}$.

By a classical result, $\mathrm{Aut}(\mathcal{X})$ is finite if the genus g of $\mathcal{X}$ is at least two, see [29, 16, 18, 17, 27].

It is known that every finite group occurs in this way, since for any groundfield $\mathbb{K}$ and any finite group G, there exists $\mathcal{X}$ such that $\mathrm{Aut}(\mathcal{X}) \cong G$, see Greenberg [6] for $\mathbb{K} = \mathbb{C}$ and Madden and Valentini [22] for $p \geq 0$, see also Madan and Rosen [21] and Stichtenoth [32].

This raises a general problem for groups and curves: Determine the finite groups that can be realized as the $\mathbb{K}$-automorphism group of some curve with a given invariant, such as genus g, p-rank (for $p > 0$) or number of $\mathbb{F}_q$-rational places (for $\mathbb{K} = \bar{\mathbb{F}}_q$), where $\mathbb{F}_q$ stands for the finite field of order q.

Research supported by the Italian Ministry MURST, Strutture geometriche, combinatoria e loro applicazioni, PRIN 2006-2007.

2000 *Math. Subj. Class.*: 14H37.

In the present paper we deal with zero p-rank curves and their $\mathbb{K}$–automorphism groups. Interestingly, zero p-rank curves with large $\mathbb{K}$–automorphism groups are known to exist, see Roquette [28], Stichtenoth [30, 31], Henn [9], Hansen and Petersen [8], Garcia, Stichtenoth and Xing [2], Çakçak and Özbudak [1], Giulietti, Korchmáros and Torres [5], Lehr and Matignon [20], Giulietti and Korchmáros [4]. Those for $p = 2$ are the non-singular models of the plane curves listed below.

(I) $\mathbf{v}(Y^2 + Y + X^{2^k+1})$, a hyperelliptic curve of genus $g = 2^{k-1}$ with $\mathrm{Aut}(\mathcal{X})$ fixing a point of $\mathcal{X}$ and $|\mathrm{Aut}(\mathcal{X})| = 2^{2k+1}(2^k + 1)$;

(II) $\mathbf{v}(Y^n + Y - X^{n+1})$, the Hermitian curve of degree $n + 1$ with $\mathrm{Aut}(\mathcal{X}) \cong \mathrm{PGU}(3, n)$, n a power of 2;

(III) $\mathbf{v}(X^{n_0}(X^n + X) + Y^n + Y)$, the DLS curve (Deligne-Lusztig curve of Suzuki type) of genus $g = n_0(n - 1)$ with $\mathrm{Aut}(\mathcal{X}) \cong \mathrm{Sz}(n)$ where $\mathrm{Sz}(n)$ is the Suzuki group, $n_0 = 2^r, r \geq 1, n = 2n_0^2$.

(IV) $\mathbf{v}(Y^{n^3+1} + (X^n + X)(\sum_{i=0}^{n}(-1)^{i+1}X^{i(n-1)})^{n+1})$, a curve of genus $g = \frac{1}{2}(n^3 + 1)(n^2 - 2) + 1$ with $\mathrm{Aut}(\mathcal{X})$ containing a subgroup isomorphic to $\mathrm{SU}(3, n)$, n a power of 2.

The essential idea in our investigation is to deduce from the zero p-rank condition the purely group theoretic property that every $\mathbb{K}$–automorphism of $\mathcal{X}$ of order p has exactly one fixed point. Then deeper results from Group Theory can be used to determine the structure and action of $\mathrm{Aut}(\mathcal{X})$ on the set of points of $\mathcal{X}$. This idea works well for $p = 2$ and produces the following result.

Theorem 1.1. *Let $\mathcal{X}$ be a zero 2-rank algebraic curve of genus $g \geq 2$ defined over an algebraically closed groundfield $\mathbb{K}$ of characteristic 2. Let G be a subgroup of $\mathrm{Aut}(\mathcal{X})$ of even order. Let S be the subgroup generated by all elements of G of order a power of 2. If no point of $\mathcal{X}$ is fixed by G, then one of the following holds*:

(a) *S is isomorphic to one of the groups below*:

$$\mathrm{PSL}(2, n),\ \mathrm{PSU}(3, n),\ \mathrm{SU}(3, n),\ \mathrm{Sz}(n) \text{ with } n = 2^r \geq 4; \tag{1}$$

(b) *$S = O(S) \rtimes S_2$, where $O(S)$ is the largest normal subgroup of odd order of S, and S_2 is a Sylow 2-subgroup which is either a cyclic group or a generalised quaternion group.*

If G fixes a point of $\mathcal{X}$ then $G = S_2 \rtimes H$, with a Sylow subgroup S_2 of G.

Theorem 1.1 is the essential tool in the present investigation on the spectrum of the genera of zero 2-rank curves with large automorphism groups. Our results are summarized below.

Let $\mathcal{X}$ be a zero 2-rank curve. If $\mathrm{Aut}(\mathcal{X})$ is a solvable group and has no fixed point on $\mathcal{X}$, then $|\mathrm{Aut}(\mathcal{X})| \leq 24g^2$, see Theorem 4.2.

Assume that $\mathrm{Aut}(\mathcal{X})$ is non-solvable. Then S coincides with the commutator group $\mathrm{Aut}(\mathcal{X})'$ of $\mathrm{Aut}(\mathcal{X})$, see Theorem 5.1. The possible genera of $\mathcal{X}$ can be computed from the order of $\mathrm{Aut}(\mathcal{X})'$ provided that $\mathrm{Aut}(\mathcal{X})$ is big enough, namely whenever both

(2) $|\mathrm{Aut}(\mathcal{X})_P|$ *is even and bigger than* $3g$ *for at least one point* $P \in \mathcal{X}$

and

$$|\mathrm{Aut}(\mathcal{X})'| \geq 6(g-1) \tag{3}$$

hold, see Theorem 6.1. Such possibilities for g are the following:

(i) $\mathrm{Aut}(\mathcal{X})' = \mathrm{PSL}(2,n)$ and $g = \frac{1}{2}(t-1)(n-1)$ with $t|(n+1)$.

(ii) $\mathrm{Aut}(\mathcal{X})' = \mathrm{PSU}(3,n)$ and either

$$g = \tfrac{1}{2}\,(n-1)(t(n+1)^2 - (n^2+n+1))$$

with $t|(n^2-n+1)/\mu$, and $\mu = \gcd(3, n+1)$, or

$$g = \tfrac{1}{2}(n-1)\left(\frac{t(n^3+1)}{\mu} - (n^2+n+1)\right),$$

with $t \mid n+1$; in the former case, $t=1$ only occurs when $\mathcal{X}$ is as in (II).

(iii) $\mathrm{Aut}(\mathcal{X})' = \mathrm{Sz}(n)$ and either

$$g \;= \tfrac{1}{2}\left[(t-1)(n^2-1) - 2tn_0(n-1)\right]$$

with $t|(n+2n_0+1)$, or

$$g \;= \tfrac{1}{2}\left[(t-1)(n^2-1) + 2tn_0(n-1)\right]$$

with $t|(n-2n_0+1)$; in the latter case $t=1$ only occurs when $\mathcal{X}$ is as in (III).

(iv) $\mathrm{Aut}(\mathcal{X})' = \mathrm{SU}(3,n)$ with $3|(n+1)$ and either

$$g = \tfrac{1}{2}(n-1)[3t(n+1)^2 - (n^2+n+1)]$$

with $t|(n^2-n+1)/3$, or

$$g = \tfrac{1}{2}(n-1)\left(t(n^3+1) - (n^2+n+1)\right),$$

with $t \mid (n+1)$; in the former case $t = n^2-n+1$ (equivalently, in latter case $t = n+1$) occurs when $\mathcal{X}$ is as in (IV).

Both technical conditions (2) and (3) are satisfied when $\mathrm{Aut}(\mathcal{X})$ is large enough, see Lemma 6.3. Therefore, the above results have the following corollary.

Theorem 1.2. *Let* $\mathcal{X}$ *be a zero* 2*-rank algebraic curve of genus* $g \geq 2$ *defined over an algebraically closed groundfield* $\mathbb{K}$ *of characteristic* 2*. Assume that* $\mathrm{Aut}(\mathcal{X})$ *fixes no point on* $\mathcal{X}$*. If* $|\mathrm{Aut}(\mathcal{X})| > 24g^2$*, then one of the above four cases* (i)-(iv) *occurs, and* $\mathrm{Aut}(\mathcal{X})$ *contains a cyclic* *normal subgroup N of odd order such that the factor group* $\mathrm{Aut}(\mathcal{X})/N$ *is isomorphic to one of the groups* $\mathrm{PSL}(2,n)$*,* $\mathrm{PSU}(3,n)$*,* $\mathrm{PGU}(3,n)$ *and* $\mathrm{Sz}(n)$*.*

For $\mathrm{PSL}(2,n)$ and $\mathrm{Sz}(n)$, the above central extension is splitting, see Theorem 6.2. In any case, N coincides with the subgroup of $\mathrm{Aut}(\mathcal{X})$ fixing point-wise the unique non-tame orbit of $\mathrm{Aut}(\mathcal{X})$ on $\mathcal{X}$.

It may be asked whether similar results for zero p-rank curves can hold for odd p. Here we limit ourselves to extend the bound $|G| \leq 24g^2$ to solvable $\mathbb{K}$–automorphism groups $|G|$ whose order is divisible for p^2.

Surveys on $\mathbb{K}$-automorphism groups of curves in positive characteristic are found in [26] and [13].

2. Background

$\mathrm{Aut}(\mathcal{X})$ has a faithful permutation representation on the set of all points of $\mathcal{X}$ (equivalently on the set of all places of $\mathbb{K}(\mathcal{X})$). The orbit

$$o(P) = \{Q \mid Q = P^\alpha, \alpha \in G\}$$

is *long* if $|o(P)| = |G|$, otherwise $o(P)$ is *short* and G_P is non-trivial.

If G is a finite subgroup of $\mathrm{Aut}(\mathcal{X})$, the subfield $\mathbb{K}(\mathcal{X})^G$ consisting of all elements of $\mathbb{K}(\mathcal{X})$ fixed by every element in G, is also a function field of one variable over $\mathbb{K}$. Let $\mathcal{Y}$ be a non-singular model of $\mathbb{K}(\mathcal{X})^G$, that is, a (projective, geometrically irreducible, non-singular) algebraic curve defined over $\mathbb{K}$ with function field $\mathbb{K}(\mathcal{X})^G$. Usually, $\mathcal{Y}$ is called the quotient curve of $\mathcal{X}$ by G and denoted by $\mathcal{X}/G$. The covering $\mathcal{X} \mapsto \mathcal{Y}$ has degree $|G|$ and the field extension $\mathbb{K}(\mathcal{X})/\mathbb{K}(\mathcal{X})^G$ is Galois.

If P is a point of $\mathcal{X}$, the stabiliser G_P of P in G is the subgroup of G consisting of all elements fixing P. For $i = 0, 1, \ldots$, the i-th ramification group $G_P^{(i)}$ of $\mathcal{X}$ at P is

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

where t is a uniformizing element of $\mathcal{X}$ at P. Here $G_P^{(0)} = G_P$ and $G_P^{(1)}$ is the unique Sylow p-subgroup of G_P. If $\mathcal{X}/G_P^{(1)}$ is non-rational, then $|G_P^{(1)}| \leq g$, by a result due to Stichtenoth [30]. Also, $G_P = G_P^{(1)} \rtimes H$ with H a cyclic group whose order is prime to p. Furthermore, for $i \geq 1$, $G_P^{(i)}$ is a normal subgroup of G_P and the factor group $G_P^{(i)}/G_P^{(i+1)}$ is an elementary abelian p-group. For i big enough, $G_P^{(i)}$ is trivial.

For any point Q of $\mathcal{X}$, let $e_Q = |G_Q|$ and

$$d_Q = \sum_{i \geq 0} (|G_Q^{(i)}| - 1).$$

Then $d_Q \geq e_Q - 1$ and equality holds if and only if $\gcd(p, |G_Q|) = 1$.

Let g' be the genus of $\mathcal{X}/G$. From the Hurwitz genus formula,

$$2g-2=|G|(2g'-2)+\sum_{Q\in\mathcal{X}} d_Q. \tag{4}$$

If G is tame, that is $p\nmid |G|$, or more generally for G with $p\nmid e_Q$ for every $Q\in\mathcal{X}$, Equation (4) is simpler and may be written as

$$2g-2=|G|(2g'-2)+\sum_{i=1}^{k}(|G|-\ell_i) \tag{5}$$

where $\ell_1,\ldots,\ell_k$ are the sizes of the short orbits of G on $\mathcal{X}$.

Let $G_P=G_P^{(1)}\rtimes H$. The following upper bound on $|H|$ depending on g is due to Stichtenoth [30]:

$$|H|\le 4g+2.$$

For any abelian subgroup G of $\mathrm{Aut}(\mathcal{X})$, Nakajima [25] proved that

$$|G|\le\begin{cases} 4g+4 & \text{for} \quad p\neq 2,\\ 4g+2 & \text{for} \quad p=2.\end{cases}$$

An equation similar to (5) holds for any p-group S of $\mathbb{K}$–automorphisms of $\mathcal{X}$ whenever the genus g is replaced by the p-rank. Recall that the p-rank γ of a curve is its Hasse-Witt invariant and that $0\le\gamma\le g$. The elementary abelian subgroup $\mathrm{Pic}_0(\mathcal{X},p)$ of elements of order p in the zero divisor class group $\mathrm{Pic}_0(\mathcal{X})$ has dimension γ, that is, $\mathrm{Pic}_0(\mathcal{X},p)\cong(\mathbb{Z}_p)^\gamma$. If γ' denotes the p-rank of $\mathcal{X}/S$, the Deuring-Shafarevich formula is

$$\gamma-1=|S|(\gamma'-1)+\sum_{i=1}^{k}(|S|-\ell_i) \tag{6}$$

where $\ell_1,\ldots,\ell_k$ are the short orbits of S on $\mathcal{X}$. Upper bounds on $|S|$ depending on γ are found in [24, 25].

Let m be the smallest non-gap at P, and suppose that $\xi\in\mathbb{K}(\mathcal{X})$ has a pole of order m at P and is regular elsewhere. If $g\in G_P$, then $g(\xi)=c\xi+d$ with $c,d\in\mathbb{K}$ and $c\neq 0$.

Let $\mathcal{L}$ be the projective line over $\mathbb{K}$. Then $\mathrm{Aut}(\mathcal{L})\cong\mathrm{PGL}(2,\mathbb{K})$, and $\mathrm{Aut}(\mathcal{L})$ acts on the set of all points of $\mathcal{L}$ as $\mathrm{PGL}(2,\mathbb{K})$ naturally on $\mathrm{PG}(1,\mathbb{K})$. In particular, the identity of $\mathrm{Aut}(\mathcal{L})$ is the only $\mathbb{K}$–automorphism in $\mathrm{Aut}(\mathcal{L})$ fixing at least three points of $\mathcal{L}$. Every $\mathbb{K}$–automorphism $\alpha\in\mathrm{Aut}(\mathcal{L})$ fixes a point; more precisely, α fixes either one or two points according as its order is p or relatively prime to p. Also, $G_P^{(1)}$ is an infinite elementary abelian p-group. For a classification of subgroups of $\mathrm{PGL}(2,\mathbb{K})$, see [35].

Let $\mathcal{E}$ be an elliptic curve. Then $\mathrm{Aut}(\mathcal{E})$ is infinite; however for any point $P \in \mathcal{E}$ the stabiliser of P is rather small, namely

$$|\mathrm{Aut}(\mathcal{E})_P| = \begin{cases} 2,4,6 & \text{when } p \neq 2,3, \\ 2,4,6,12 & \text{when } p = 3, \\ 2,4,6,8,12,24 & \text{when } p = 2. \end{cases}$$

Let $\mathcal{F}$ be a (hyperelliptic) curve of genus 2 having more than one Weierstrass point. For any solvable subgroup G of $\mathrm{Aut}(\mathcal{F})$, Nakajima's bound together with some elementary facts on finite permutation groups, yield $|G| \leq 48$.

From finite group theory, the following results play a role in the proofs.

Huppert's classification theorem, see [15], Chapter XII, Section 7: Let G be a solvable 2-transitive permutation group of degree n. Then n is a power of some prime p, and G is a subgroup of the affine semi-linear group $\mathrm{A\Gamma L}(1,n)$, except possibly when n is $3^2, 5^2, 7^2, 11^2, 23^2$ or 3^4.

The Kantor-O'Nan-Seitz theorem, see [19]: Let G be a 2-transitive permutation group of odd degree. If the 2-point stabiliser of G is cyclic, then G has either an elementary abelian regular normal subgroup, or G is one of the following groups in its natural 2-transitive permutation representation:

$$\mathrm{PSL}(2,n),\ \mathrm{PSU}(3,n),\ \mathrm{PGU}(3,n), \mathrm{Sz}(n),$$

where $n \geq 4$ is a power of 2.

The natural 2-transitive permutation representations of the above linear groups:

- (A) $G = \mathrm{PSL}(2,n)$, is the $\mathbb{K}$–automorphism group of $\mathrm{PG}(1,n)$; equivalently, G acts on the set Ω of all $\mathbb{F}_n$-rational points of the projective line defined over $\mathbb{F}_n$.
- (B) $G = \mathrm{PGU}(3,n)$ is the linear collineation group preserving the classical unital in the projective plane $\mathrm{PG}(2,n^2)$, see [12]; equivalently G is the $\mathbb{K}$–automorphism group of the Hermitian curve regarded as a plane non-singular curve defined over the finite field $\mathbb{F}_n$ acting on the set Ω of all $\mathbb{F}_{n^2}$-rational points, see (II). For $n \equiv 0,1 \pmod 3$, $\mathrm{PSU}(3,n) = \mathrm{PGU}(3,n)$. For $n \equiv -1 \pmod 3$, $\mathrm{PSU}(3,n)$ is a subgroup of $\mathrm{PGU}(3,n)$ of index 3, and this is the natural 2-transitive representation of $\mathrm{PSU}(3,n)$.
- (C) $G = \mathrm{Sz}(n)$ with $n = 2n_0^2$, $n_0 = 2^r$ and $r \geq 1$, is the linear collineation group of $\mathrm{PG}(3,n)$ preserving the Tits ovoid, see [33, 34, 11]; equivalently G is the $\mathbb{K}$–automorphism group of the DLS curve regarded as a non-singular curve defined over the finite field $\mathbb{F}_n$ acting on the set Ω of all $\mathbb{F}_n$-rational points, see (III).

For each of the above linear groups, the structure of the 1-point stabilizer and its action in the natural 2-transitive permutation representation, as well as its $\mathbb{K}$–automorphism group, are explicitly given in the papers quoted. In this paper, we will need the following corollary.

Lemma 2.1. *Let n be a power of 2 and $n \geq 4$. Let L be any of the groups $\mathrm{PSL}(2,n)$, $\mathrm{PSU}(3,n)$, $\mathrm{Sz}(n)$ given in its natural 2-transitive permutation representation on a set Ω. Let $\bar{G}$ be a subgroup of $\mathrm{Aut}(L)$ containing L properly, and choose a point $P \in \Omega$. If the Sylow 2-subgroup of $\bar{G}_P$ properly contains the Sylow 2-subgroup of L_P, then some non-trivial element of order 2 contained in $\bar{G}_P \setminus L_P$ fixes a point other than P. Otherwise, either $\bar{G}_P$ contains a non-cyclic subgroup of odd order, or $L = \mathrm{PSU}(3,n)$ and $\bar{G} = \mathrm{PGU}(3,n)$ with $3|(n+1)$.*

Cyclic fix-point-free subgroups of some 2-transitive groups. The following lemma is a corollary of the classification of subgroups of $\mathrm{PSU}(3,n)$ and $\mathrm{Sz}(n)$.

Lemma 2.2. *Let G be a 2-transitive permutation group of degree n. Let U be a cyclic subgroup of G which contains no non-trivial element fixing a point.*

- (i) *If $G = \mathrm{PSU}(3,n)$ in its natural 2-transitive permutation representation, then $|U|$ divides either $n+1$ or $(n^2-n+1)/\mu$, with $\mu = \gcd(3, n+1)$.*
- (ii) *If $G = \mathrm{Sz}(n)$ in its natural 2-transitive permutation representation, then $|U|$ divides either $n - 2n_0 + 1$ or $n + 2n_0 + 1$.*

3. $\mathbb{K}$–automorphism groups of curves with p–rank zero

In this section, subgroups of $\mathrm{Aut}(\mathcal{X})$ whose order is divisible by p and in which

(7) *every element of order p has exactly one fixed point*

are investigated. In terms of ramification, (7) means that for every $\alpha \in G$ of order p the covering $\mathcal{X} \mapsto \mathcal{X}/\langle\alpha\rangle$ ramifies at exactly one point.

Remark 3.1. A suitable power β of any non-trivial element α of a p-group has order p. Also, every fixed point of α is fixed by β as well. Since $G_P^{(1)}$ is a p-group, it is a subgroup of a Sylow p-subgroup S_p of G. Choose a non-trivial element ζ from the centre of S_p. Then ζ commutes with a non-trivial element of $G_P^{(1)}$. This together with (7) imply that ζ fixes P. Therefore, $\zeta \in G_P^{(1)}$. In particular, ζ fixes no point of $\mathcal{X}$ distinct from P. Let $\alpha \in S_p$. Then $\zeta\alpha = \alpha\zeta$ implies that

$$(P^\alpha)^\zeta = P^{\alpha\zeta} = P^{\zeta\alpha} = (P^\zeta)^\alpha = P^\alpha$$

whence $P^\alpha = P$. This shows that every element of S_p must fix P, and hence $S_p = G_P^{(1)}$. Since the Sylow p-subgroups of G are conjugate under G, every p-element fixes exactly one point of $\mathcal{X}$.

Therefore, condition (7) is satisfied by a subgroup G of $\mathrm{Aut}(\mathcal{X})$ if and only if every p-element in G has exactly one fixed point. Further, the non-trivial elements of a Sylow p-subgroup S_p of a $\mathbb{K}$-automorphism G of $\mathrm{Aut}(\mathcal{X})$ satisfying (7) have the same fixed point.

Property (7) is known to occur in several circumstances, for instance in [30], Satz 1, see also [20] and [3]. Another such circumstance is described in the following two lemmas.

Lemma 3.2. *If $\mathcal{X}$ has p-rank* 0, *then* (7) *holds in* $\mathrm{Aut}(\mathcal{X})$.

Proof. Let $\alpha \in \mathrm{Aut}(\mathcal{X})$ have order p. Applying the Deuring–Shafarevich formula (6) to the group generated by α gives $-1 = p(\gamma' - 1) + m(p-1)$, where γ' is the p-rank of $\mathbb{K}(\mathcal{X})^\alpha$ and m is the number of fixed points of α. This is only possible when $\gamma' = 0$ and $m = 1$. □

The converse of Lemma 3.2 is not true in general, a counterexample for $p = 2$ being the non-singular model of the irreducible curve

$$\mathcal{F}: \quad \mathbf{v}(Y^6 + Y^5 + Y^4 + Y^3 + Y^2 + Y + 1 + X^3(Y^2 + Y)).$$

The 2-rank of such a curve $\mathcal{X}$ is equal to 4, while the birational transformation $x' = x$, $y' = y + 1$ is a $\mathbb{K}$–automorphism of $\mathbb{K}(\mathcal{X})$ which has only one fixed point, namely that arising from the unique branch of $\mathcal{F}$ tangent to the infinite line. A partial converse of Lemma 3.2 is the following result.

Lemma 3.3. *Assume that* $\mathrm{Aut}(\mathcal{X})$ *contains a p-subgroup G. If $\mathcal{Y} = \mathcal{X}/G$ has p-rank zero, and* (7) *holds, then $\mathcal{X}$ has p-rank zero, as well.*

Proof. Let P be the fixed point of G. Since $\gamma' = 0$, (6) applied to G gives $\gamma - 1 = -|G| + |G| - 1$, whence $\gamma = 0$. □

Suppose that a subgroup G of $\mathrm{Aut}(\mathcal{X})$ has a Sylow p-subgroup with property (7). Then (7) is satisfied by all Sylow p-subgroups of G. Suppose further that G has no normal Sylow p-subgroup. Let S_p and S_p' two distinct Sylow p-subgroups of G. By Remark 3.1, S_p and S_p' each have exactly one fixed point, say P and P'. Also, S_p is the unique Sylow p-subgroup of the stabiliser of P under G, and $G_P = S_p \rtimes H$. Further, $P \neq P'$; for, if $P = P'$, then S_p and S_p' are two distinct Sylow p-subgroups in G_P. However, this is impossible as S_p is a normal subgroup of G_P. Therefore, any two distinct Sylow p-subgroups in G have trivial intersection.

A subgroup V of a group G is a *trivial intersection set* if, for every $g \in G$, either $V = g^{-1}Vg$ or $V \cap g^{-1}Vg = \{1\}$. A Sylow p-subgroup T of G is a trivial intersection set in G if and only if that T meets every other Sylow p-subgroup of G trivially. Hence, Lemma 3.2 has the following corollary.

Theorem 3.4. *If $\mathcal{X}$ has p-rank* 0, *then every Sylow p-subgroup S_p in* $\mathrm{Aut}(\mathcal{X})$ *is a trivial intersection set.*

A classical result on trivial intersection sets is the following.

Theorem 3.5. (Burnside) *If a Sylow p-subgroup S_p of a finite solvable group is a trivial intersection set*, *then either S_p is normal or cyclic*, *or $p = 2$ and S_2 is a generalised quaternion group.*

For a proof, see [7].

Finite groups whose Sylow 2-subgroups are trivial intersection sets have been classified. This has been refined to groups containing a subgroup of even order which intersects each of its distinct conjugates trivially.

Theorem 3.6. (Hering [10]) *Let V be a subgroup of a finite group G with trivial normaliser intersection*; *that is*, *the normaliser $N_G(V)$ of V in G has the following two properties*:

(a) $V \cap x^{-1}Vx = \{1\}$ *for all* $x \in G \setminus N_G(V)$;
(b) $N_G(V) \neq G$.

If $|V|$ is even and S is the normal closure of V in G, then the following hold.

(i) $S = O(S) \rtimes V$, *the semi-direct product of $O(S)$ by V*, *with V a Frobenius complement*, *unless S is isomorphic to one of the groups*,

$$\mathrm{PSL}(2, n),\ \mathrm{Sz}(n),\ \mathrm{PSU}(3, n),\ \mathrm{SU}(3, n), \tag{8}$$

where n is a power of 2.

(ii) *Let $\bar{G}$ be the permutation group induced by G on the set Ω of all conjugates of V under G. Then*

ii(a) *$C_G(S)$ is the kernel of this representation*;
ii(b) *S is transitive on Ω*;
(c) *$|\Omega|$ is odd*;
ii(d) *in the exceptional cases*,
  (1) $|\Omega| = n + 1, n^2 + 1, n^3 + 1, n^3 + 1$;
  (2) $\bar{G} = G/C_G(S)$ *contains a normal subgroup L isomorphic to one of the groups* $\mathrm{PSL}(2, n)$, $\mathrm{Sz}(n)$, $\mathrm{PSU}(3, n)$, *acting in its natural* 2*-transitive permutation representation;*

(3) *$\bar{G}$ is isomorphic to an automorphism group of L containing L.*

Hering's result does not extend to subgroups of odd order with trivial normal intersection. A major result which can be viewed as a generalisation of Theorem 3.5 is found in [36].

Theorem 3.7. *Let S_d, with $d > 11$, be a Sylow d-subgroup of a finite group G that is a trivial intersection set but not a normal subgroup. Then S_d is cyclic if and only if G has no composition factors isomorphic to either* $\mathrm{PSL}(2, d^n)$ *with $n > 1$ or* $\mathrm{PSU}(3, d^m)$ *with $m \geq 1$.*

Now, some consequences of the above results are stated.

Let $p = 2$. If (7) is satisfied by a subgroup G of $\mathrm{Aut}(\mathcal{X})$, then Theorem 3.6 applies to G where V is a Sylow 2-subgroup S_2 of G (or any non-trivial subgroup of S_2). In fact, (a) is true, while (b) holds provided that G is larger than G_P, where P is the fixed point of S_2.

When $G_P = G$, then $G = G_P^{(1)} \rtimes H$ with $p \nmid |H|$. Otherwise, G has no fixed point, and Hering's theorem determines the abstract structure of the normal subgroup S of G generated by all elements whose order is a power of 2. Note that, since S_2 has only one fixed point, $N_G(S_2) = G_P$ holds. If $S = O(S) \rtimes S_2$, then S_2 is a Frobenius complement, and hence it has a unique involutory element. Note that it is not claimed that S is a Frobenius group. In the exceptional cases, if $C_G(S)$ is the centraliser of S in G, then $G/C_G(S)$ is an automorphism group of a group listed in Hering's theorem.

Therefore, the following result is obtained which together with Lemma 3.2 imply Theorem 1.1.

Theorem 3.8. *Let $p = 2$ and assume that* (7) *holds. Let S be the subgroup G of* $\mathrm{Aut}(\mathcal{X})$ *of even order, generated by all elements whose order is a power of* 2*. One of the following holds*:

(a) *S isomorphic to one of the following groups*:

$$\mathrm{PSL}(2, n),\ \mathrm{Sz}(n),\ \mathrm{PSU}(3, n),\ \mathrm{SU}(3, n),\ \text{with } n = 2^r \geq 4; \tag{9}$$

(b) *$S = O(S) \rtimes S_2$ with S_2 a Sylow* 2*-subgroup of G; here, S_2 is either a cyclic group or a generalised quaternion group.*

(c) *S is a Sylow* 2*-subgroup and $G = S \rtimes H$, with H a subgroup of odd order.*

Using Theorem 3.6, the action of S on the set Ω of all points of $\mathcal{X}$ fixed by some involution or, equivalently, on the set consisting of all involutions in G can be investigated. Let $\bar{S}$ be the permutation group induced by S on Ω. If M is the kernel of the permutation representation of S, then

$|M|$ is odd, $\bar{S} = S/M$, and $\bar{S}_2 = S_2M/M$ is a Sylow 2-subgroup of $\bar{S}$. Here, $\bar{S}$ is transitive on Ω; also, $\bar{S}_2$ fixes P and acts on $\Omega \setminus \{P\}$ as a semi-regular permutation group. Further, the kernel of the permutation representation of G on Ω is $N = C_G(S)$. If S is isomorphic to one of the groups in (9), then $\bar{S}$ is 2-transitive on Ω, and $|\Omega| = n+1,\ n^2+1, n^3+1$ according as $\bar{S} \cong \mathrm{PSL}(2,n)$, $\mathrm{Sz}(n)$, $\mathrm{PSU}(3,n)$.

4. Upper bound on the orders of solvable subgroups of $\mathbb{K}$–automorphism groups of p–rank zero curves

Theorem 4.1. *Suppose $p > 2$ and let G be a solvable subgroup of* $\mathrm{Aut}(\mathcal{X})$ *satisfying condition* (7)*. Assume that G fixes no point, and that*

$$|G| \text{ is divisible by } p^2. \tag{10}$$

If $\mathcal{X}$ has genus $g \geq 2$, then $|G| \leq 24g(g-1)$.

Proof. Since p is odd, $\mathcal{X}$ has more than one Weierstrass points. So, if $g = 2$, then $|G| \leq 48$ and hence Theorem 4.1 is true.

Let N be a minimal normal subgroup of G. Since G is solvable, N is an elementary abelian group of order d^r with a prime d. If $d = p$, then (7) implies that N fixes a unique point P. But then G itself must fix P, contradicting one of the hypotheses. So, $p \neq d$. Theorem 3.5 yields that the Sylow p-subgroups of G are cyclic. As $d \neq p$, the Sylow p-subgroups of G and G/N are isomorphic, while (10) remains valid for G/N.

This suggests that $\bar{G} = G/N$, viewed as a subgroup of $\mathrm{Aut}(\mathcal{Y})$ with $\mathcal{Y} = \mathcal{X}/G$, should be investigated. The aim is to show that $\bar{G}$ also satisfies (7).

The point $\bar{P} \in \mathcal{Y}$ lying below P is fixed by a Sylow p-subgroup of $\bar{G}$. Since G/N can be viewed as a subgroup $\mathrm{Aut}(\mathcal{Y})$, this and (10) rule out the possibility that $\mathcal{Y}$ is elliptic. Similarly, $\mathcal{Y}$ cannot be rational. In fact, if $\mathcal{Y}$ were rational, then no p-subgroup of G/N and hence of G would be a cyclic group of order p^i with $i \geq 2$, contradicting Theorem 3.5.

Therefore, $\mathcal{Y}$ has genus $\bar{g} \geq 2$. Assume that Theorem 4.1 does not hold, and choose a minimal counterexample with genus g as small as possible. Then $|G| > 24g(g-1)$, but Theorem 4.1 holds for all genera g' with $2 \leq g' < g$. (4) applied to N gives $2g-2 \geq |N|(2\bar{g}-2)$, whence

$$|G| > 12g(2g-2) \geq |N|\, 12g(2\bar{g}-2).$$

Therefore $|G/N| > 24\bar{g}(\bar{g}-1)$. By the divisibility condition (10) on $|G|$, the order of $\bar{G} = G/N$ is not a prime. Hence $\bar{G}$ is a solvable group. Since $d \neq p$, so $\bar{G}$ satisfies (10). On the other hand, $\bar{G}$ can be regarded as a subgroup of $\mathrm{Aut}(\mathcal{Y})$.

To show that $\bar{G}$ also satisfies condition (7), let $\bar{\alpha}$ be any element of $\bar{G}$ of order p. Choose an element α in G whose image is $\bar{\alpha}$ under the natural homomorphism $G \mapsto G/N$. By (7), $\mathcal{X}$ has a unique point P fixed by α. Then, $\bar{\alpha}$ fixes the point $\bar{P}$ lying under P in the covering $\mathcal{X} \to \mathcal{Y}$.

Assume on the contrary that $\bar{\alpha}$ fixes another point of $\mathcal{Y}$, say $\bar{Q}$. Then the set of points of $\mathcal{Y}$ lying over $\bar{Q}$ is preserved by α. The number of such points is prime to p since their number divides $|N|$. But then α must fix one of these points, contradicting (7).

Since G is a minimal counterexample, $\bar{G}$ fixes a point of $\mathcal{Y}$. Equivalently, an orbit of N is preserved by G. Such an orbit consists of points of $\mathcal{X}$ fixed by p-elements of G. Since any Sylow p-subgroup S_p of G has only one fixed point, so $|S_p| \leq |N| - 1$. This together with (10) implies that $|N| \geq 10$. As $g - 1 \geq |N|(\bar{g} - 1)$, it follows that $g \geq 11$.

Note that $|\bar{G}| = |\bar{G}_{\bar{P}}| = |\bar{G}_{\bar{P}}^{(1)}|\,|\bar{H}|$, with $\bar{H}$ a cyclic group of order prime to p. By Stichtenoth's bound, $|\bar{H}| \leq 4\bar{g} + 2$. Let $\bar{S}_p$ be the Sylow p-subgroup of $\bar{G}$; then $\bar{S}_p = \bar{G}_{\bar{P}}^{(1)}$. Since $p \nmid |N|$, so $\bar{S}_p$ is isomorphic to S_p.

By Theorem 3.5, S_p is cyclic. By Nakajima's bound, $|\bar{G}_{\bar{P}}^{(1)}| \leq 4\bar{g} + 4$. Therefore,

$$|\bar{G}| \leq (4\bar{g} + 4)(4\bar{g} + 2),$$

whence $|G| \leq (4\bar{g} + 4)(4\bar{g} + 2)|N|$. Since $g - 1 \geq |N|(\bar{g} - 1)$, $\bar{g} \geq 2$ and $|N| \geq 10$, it follows that

$$\begin{aligned} |G| &\leq 16(\bar{g} + 1)(\bar{g} + \tfrac{1}{2})|N| \\ &\leq \frac{16}{10} \cdot \frac{\bar{g} + 1}{\bar{g} - 1}(\bar{g} - 1)|N| \cdot \frac{\bar{g} + \frac{1}{2}}{\bar{g} - 1}(\bar{g} - 1)|N| \\ &\leq \frac{8}{5} \cdot \frac{2\bar{g}^2 + 3\bar{g} + 1}{2(\bar{g} - 1)^2}(g - 1)^2 \\ &\leq 12(g - 1)^2 < 24g(g - 1). \end{aligned}$$

But then G is not a counterexample. □

Under the hypothesis that 16 divides $|G|$, the above proof with some modifications also works for $p = 2$. Here an alternative proof is given for $p = 2$ which does not require that hypothesis.

Theorem 4.2. *Let $p = 2$, $g \geq 2$, and assume that* (7) *holds. If G is a solvable subgroup of* $\mathrm{Aut}(\mathcal{X})$ *fixing no point of $\mathcal{X}$ then $|G| \leq 24g^2$.*

Proof. Since $84(g-1) < 24g^2$, the group G may be supposed to be one of the exceptions in [30], Satz 3. Since G has no fixed point, from Theorem 3.8, $S = O(S) \rtimes S_2$, and $O(S)$ acts transitively on the set Ω consisting of all points fixed by involutory elements in G. In particular, Ω is the unique non-tame orbit of G. Let $P \in \Omega$. By assumption (7), $G_P^{(1)}$ is a

Sylow 2-subgroup S_2 of G. From $|O(S)| = |\Omega||O(S)_P|$, it follows

$$|G| = \frac{|G_P||O(S)|}{|O(S)_P|}. \tag{11}$$

In particular, Ω has odd size. As $O(S)$ is transitive on Ω and $N_G(S_2) = G_P$, each element in G is the product of an element fixing P and an element from $O(S)$, that is, $G = G_P O(S)$. Also, as $O(S)$ is a characteristic subgroup of S and $S \trianglelefteq G$, so $O(S) \trianglelefteq G$. Hence $\bar{G} = G/O(S)$ is a factor group which can be viewed as a subgroup of Aut $(\mathcal{Y})$ where $\mathcal{Y} = \mathcal{X}/O(S)$.

Assume that $\mathcal{Y}$ is rational. Then every 2-subgroup of $\bar{G}$ is elementary abelian. On the other hand, as $S_2 \cong S_2O(S)/O(S)$, from Theorem 3.5 the factor group $S_2O(S)/O(S)$ has only one involutory element. Thus, $|S_2O(S)/O(S)| = 2$, whence $|S_2| = 2$. This implies that $G = O(G) \rtimes S_2$. Hence

$$|G| = 2|O(G)| \leq 168(g-1) \leq 24g^2$$

for $g \geq 6$.

To show that this holds true for $2 \leq g \leq 5$, some results from [30] are needed, see the proof of Theorem 3: If G has more than three short orbits, then $|G| \leq 12(g-1) < 24g^2$. Since S_2 has exactly one fixed point, it preserves only one orbit of $O(G)$. Therefore, either $O(G)$ (and hence G) has only one short orbit, or G has 2 tame orbits and 1 wild orbit. Since $p = 2$, in the latter case $|G| \leq 84(g-1)$ as it follows from another result shown in the proof of the above mentioned Theorem 3. Therefore, $|G| < 24g^2$.

Assume that Ω is the unique short orbit of G. Then $|\Omega|$ divides $2g-2$. Therefore,

$$|G| \leq |\Omega||G_P| \leq (2g-2)|S_2||H| \leq (4g-4)|H|,$$

where H is the complement of S_2 in G_P. Then Stichtenoth's bound $|H| \leq 4g+2$ yields $|G| < 24g^2$.

Assume that $\mathcal{Y}$ is elliptic. From (5),

$$2g-2 = |O(S)| \sum_{i=1}^{k} \left(\frac{|O(S)_{P_i}| - 1}{|O(S)_{P_i}|} \right),$$

where $P_1, \ldots, P_k$ are representatives of the short orbits of $O(S)$. Note that $k \geq 1$, as otherwise $g = 1$. Hence, $|O(S)| < 4(g-1)$. As $G_PO(S)/O(S)$ fixes a point of $\mathcal{Y}$, it follows that $|G| = |G_PO(S)| \leq 24|O(S)| \leq 96(g-1) \leq 24g^2$.

We are left with the case that the genus of the quotient curve $\mathcal{Y} = \mathcal{X}/O(S)$ is greater than 1. From (5), $|O(S)| \leq g-1$. Hence, by (11),

$$|G| \leq (g-1)|G_P|.$$

Assume that the quotient curve $\mathcal{Z} = \mathcal{X}/S_2$ has genus $g' > 1$. Then $|S_2|(g'-1) < g-1$ by (4). Since G_P/S_2 is a tame subgroup of $\mathrm{Aut}(\mathcal{Z})$ fixing the point of $\mathcal{Z}$ lying under P, from Stichtenoth's bound, $|G_P/S_2| \leq 4g'+2$. Hence,

$$|G_P| < \frac{4g'+2}{g'-1}(g'-1)|S_2| \leq 10(g-1).$$

Since $|\Omega| \leq |O(S)| \leq g-1$, this implies that $|G| < 10(g-1)^2 < 24g^2$.

If $\mathcal{Z}$ is elliptic, then $|G_P/S_2| \leq 24$, while $|S_2| \leq g$ by Stichtenoth's bound. Therefore, $|G| \leq 24g(g-1) < 24g^2$.

So, take $\mathcal{Z}$ to be rational. Let $R \in \Omega$ be a point distinct from P. If the stabiliser $G_{P,R}$ of R in G_P is trivial, then $|G_P| < |\Omega|$, and hence

$$|G| = |G_P||\Omega| < |\Omega|^2 \leq |O(S)|^2 \leq (g-1)^2.$$

Therefore, let $|G_{P,R}| > 1$ for every $R \in \Omega$. We show that G acts on Ω as a 2-transitive permutation group $\bar{G}$.

Let $\Omega_0 = \{P\}, \Omega_1, \ldots \Omega_r$ with $r \geq 1$ denote the orbits of S_2 contained in Ω. Then, $\Omega = \bigcup_{i=0}^{r} \Omega_i$. To prove that G acts 2-transitively on Ω, it suffices to show that $r = 1$. For any i with $1 \leq i \leq r$, take a point $R \in \Omega_i$. By hypothesis, R is fixed by an element $\alpha \in G_P$ whose order m is a prime different from p. Since $|G_P| = |S_2||H|$ and m divides $|G_P|$, this implies that m must divide $|H|$. By the Sylow theorem, there is a subgroup H' conjugate to H in G_P which contains α; here, α preserves Ω_i. Since the quotient curve $\mathcal{Z}$ is rational, α fixes at most two orbits of S_2. Therefore, Ω_0 and Ω_i are the orbits preserved by α. As H' is abelian and $\alpha \in H'$, this yields that H' either preserves both Ω_0 and Ω_i or interchanges them. The latter case cannot actually occur as H' preserves Ω_0. So, the orbits Ω_0 and Ω_i are also the only orbits of S_2 which are fixed by H'. Since $G_P = S_2 \rtimes H'$, this implies that the whole group G_P fixes Ω_i. As i can be any integer between 1 and r, it follows that G_P fixes each of the orbits $\Omega_0, \Omega_1, \ldots, \Omega_r$. Hence, either $r = 1$ or G_P preserves at least three orbits of S_2. The latter case cannot actually occur, as the quotient curve $\mathcal{Z}$ is rational. Therefore $r = 1$. Also, the size of Ω is of the form $q+1$ with $q = S_2$; in particular, q is a power of 2, and Ω comprises P together with all points in the unique non-trivial orbit of S_2.

The latter assertion implies that $|\Omega| = |S_2| + 1 = q+1$, $q = 2^r$. Let $\bar{G}$ denote the 2-transitive permutation group induced by G on Ω. As G is solvable, $\bar{G}$ admits an elementary abelian w-group acting on Ω as a sharply transitive permutation group. Hence, $|\Omega| = w^k$ with an odd prime w. From $q+1 = w^k$, either $k = 1$, or $k = 2$, $q = 8$, $w = 3$, see [23]. Let M be the kernel of the permutation representation of G on Ω.

It may be that M is trivial, that is $G = \bar{G}$, and this possibility is investigated first. Assume that $k = 1$. Then $G = \mathrm{AGL}(1, w)$ and G is sharply 2-transitive on Ω. Let N be the normal subgroup of G of order w. If the quotient curve $\mathcal{U} = \mathcal{X}/N$ has genus $g' \geq 2$, then

$$2g - 2 \geq w(2g' - 2) \geq 2w,$$

and hence

$$|G| = |\Omega|(|\Omega| - 1) = w(w - 1) \leq (g - 1)(g - 2) < 24g^2.$$

If $\mathcal{U}$ is elliptic, then $|S_2|$ is either 2, or 4, or 8. The last case cannot occur because 9 is not a prime number. If $|S_2| = 2$, then $w = 3$, and hence $|G| = 6$, while $|S_2| = 4$ occurs when $w = 5$ and hence $|G| = 20$.

If $\mathcal{U}$ is rational, then S_2, viewed as a subgroup of $\mathrm{Aut}(\mathcal{U})$ must be an elementary abelian group. On the other hand, S_2 is the 1-point stabiliser of $\mathrm{AGL}(1, w)$ which is cyclic. It follows that $|S_2| = 2$. Therefore, $|o| = 3$, whence $|G| = 6$.

If $k = 2, w = 3, q = 8$, then G has an elementary abelian normal subgroup N of order 9. Since G is a subgroup of the normalizer of N, it follows that G_P is a subgroup of $\mathrm{GL}(2, 3)$ whose order is divisible by eight but not by sixteen. Since $|\mathrm{GL}(2, 3)| = 48$, either $|G_P| = 8$, or $|G_P| = 24$. In the former case, $|G| = 72$ and hence $|G| < 24g^2$. In the latter case, $|G| = 216$, which is greater than $24g^2$ only for $g = 2$. But this does not actually occur, as $\mathcal{X}$ has more than one Weierstrass -point and hence the assertion holds for $g = 2$.

Suppose M is non-trivial. Then M is cyclic of odd order. Let $\mathcal{U}$ be the quotient curve $\mathcal{X}/M$. Then $\bar{G} = G/M$ can be viewed as a subgroup of $\mathrm{Aut}(\mathcal{U})$. The Sylow 2-subgroup $\bar{S}_2 = S_2M/M$ of $\bar{G}$ is isomorphic to S_2. Arguing as in the proof of Theorem 4.1 shows that $\bar{G}$ has property (7).

From above, if the genus $\bar{g}$ of $\mathcal{U}$ is at least 2, then $|\bar{G}| \leq 24\bar{g}^2$; in consequence, $|G| \leq 24|M|\bar{g}^2$. Since $|\Omega| \geq 3$, from (5),

$$2g - 2 \geq |M|(2\bar{g} - 2) + 3(|M| - 1) \geq 2|M|\bar{g} - 2.$$

This shows that $|G| \leq 24g\bar{g} < 24g^2$.

If $\mathcal{U}$ is elliptic, then G/M has order at most 24 and the assertion holds for $|M| = 3$. Furthermore, $S_2 \cong S_2M/M$ consists of at most 8 elements. Assume that $|M| > 3$. Then $|S_2| \leq 2(|M| - 1)$. From $2g - 2 \geq (|M| - 1)|\Omega|$,

$$| G |= |G_P||\Omega| \leq |S_2|(4g+2)|\Omega| = 2(4g+2)(|M|-1)|\Omega| \leq 4(g-1)(4g+2)$$

which is smaller than $24g^2$.

Finally, if $\mathcal{U}$ is rational, then $|S_2| = 2$, and the argument above gives

$$|G| \leq |S_2|(4g+2)(|S_2|+1) \leq 6(4g+2) < 24g^2.$$

$\square$

5. Large simple $\mathbb{K}$–automorphism groups of p–rank zero curves

Throughout this and the next sections, the hypotheses of Theorem 1.1 are assumed, and notation as used in Sections 1, 2 and 3 is maintained. Our purpose is to prove the following result.

Theorem 5.1. *The possibilities in Theorem 1.1 are the following.*

(a) *S fixes a point of $\mathcal{X}$.*

(b) *S is solvable and $|S| \leq 24g^2$.*

(c) *$S \cong \mathrm{PSL}(2,n)$ and if both $|S| > 6(g-1)$ and (2) hold, then $g = \frac{1}{2}(t-1)(n-1)$ with $t|(n+1)$.*

(d) *$S \cong \mathrm{PSU}(3,n)$ and if both $|S| > 6(g-1)$ and (2) hold, then either*

$$g = \tfrac{1}{2}\,(n-1)(t(n+1)^2 - (n^2+n+1))$$

with $t|(n^2-n+1)/\mu$, or

$$g = \tfrac{1}{2}(n-1)\left(\frac{t(n^3+1)}{\mu} - (n^2+n+1)\right),$$

with $t \mid (n+1)$. In the former case, if $t=1$ then $\mathcal{X}$ is as in (II).

(e) *$S \cong \mathrm{SU}(3,n)$ with $3|(n+1)$ and if both $|S| > 6(g-1)$ and (2) hold, then either*

$$g = \tfrac{1}{2}\,(n-1)[3t(n+1)^2 - (n^2+n+1)]$$

with $t|(n^2-n+1)/3$, or

$$g = \tfrac{1}{2}(n-1)\left(t(n^3+1) - (n^2+n+1)\right),$$

with $t \mid (n+1)$.

(f) *$S \cong \mathrm{Sz}(n)$ and if both $|S| > 6(g-1)$ and (2) hold, then either*

$$g = \tfrac{1}{2}\left[(t-1)(n^2-1) - 2tn_0(n-1)\right]$$

with $t|(n+2n_0+1)$, or

$$g = \tfrac{1}{2}\left[(t-1)(n^2-1) + 2tn_0(n-1)\right]$$

with $t|(n-2n_0+1)$; if $t=1$ in the latter case then $\mathcal{X}$ is as in (III).

For the purpose of the proof, S may be assumed to be one of the four groups in (1). From the discussion at the end of Section 3, S has exactly one non-tame orbit, namely Ω, on which S acts as one of the groups $\mathrm{PSL}(2,q)$, $\mathrm{PSU}(3,n)$ and $\mathrm{Sz}(n)$ in its natural 2-transitive permutation representation. In particular, every complement H of $S_P^{(1)}$ in S_P has just one more fixed point in Ω.

Before investigating such cases separately, we prove a few lemmas.

Lemma 5.2. *Let $P\in\Omega$. Assume that $|S|>6(g-1)$. If $\mathcal{X}_1=\mathcal{X}/S_P^{(1)}$ is rational, then S has exactly two short orbits, namely Ω and a tame orbit Δ.*

Proof. By an argument going back to Hurwitz and adapted for any groundfield by Stichtenoth [30], the hypothesis $|S|>6(g-1)$ implies that S has at most one tame orbit. On the other hand, assume that Ω is the unique short orbit of S. Since $\mathcal{X}_1$ is rational, from (4) and (7),

$$2g-2+2|S_P^{(1)}|=2|S_P^{(1)}|-2+|S_P^{(2)}|-1+\ldots=d_P-|S_P|+|S_P^{(1)}|. \tag{12}$$

Therefore,

$$d_P=2g-2+|S_P^{(1)}|+|S_P|. \tag{13}$$

Also, from (4),

$$2g-2=-2|S|+\deg D(\mathcal{X}/S)=|\Omega|\,(d_P-2|S_P|). \tag{14}$$

Hence $|\Omega|(|S_P|-|S_P^{(1)}|)=(|\Omega|-1)(2g-2)$. Since S acts on Ω as one of the groups $\mathrm{PSL}(2,q)$, $\mathrm{PSU}(3,n)$ and $\mathrm{Sz}(n)$ in its natural 2-transitive permutation representation, $|\Omega|=|S_P^{(1)}|+1$ holds. Thus, $|\Omega|(|H|-1)=2g-2$ for a complement H of $S_P^{(1)}$ in S_P. From this $|\Omega|^2|H|^2<16g^2$. Therefore,

$$|S|=|S_P^{(1)}||H||\Omega|=(|\Omega|-1)|H||\Omega|<16g^2,$$

a contradiction. $\square$

Lemma 5.3. *If (2) holds then $\mathcal{X}_1=\mathcal{X}/S_P^{(1)}$ is rational.*

Proof. Assume on the contrary that the genus g' of $\mathcal{X}_1$ is positive. From (4) applied to $S_P^{(1)}$,

$$g\geq g'\,|S_P^{(1)}|. \tag{15}$$

Take a complement D of $S_P^{(1)}$ in $\mathrm{Aut}(\mathcal{X})_P$. D acts faithfully on $\mathcal{X}_1$ as a subgroup of $\mathrm{Aut}(\mathcal{X}_1)$. Furthermore, D has at least two fixed points, as S is one of the groups in (1), namely the points $\bar{P}$ and $\bar{Q}$ lying under P and a point $Q\in\Omega\setminus\{P\}$ in the covering $\mathcal{X}\mapsto\mathcal{X}_1$. Let g'' be the genus of the quotient curve $\mathcal{Z} = \mathcal{X}_1/D$ of $\mathcal{X}_1$ with respect to D. From (5) applied to D,

$$2g' - 2 \geq |D|(2g'' - 2) + 2(|D| - 1).$$

If $g'' \geq 1$, this yields $g' \geq |D|$ whence $g \geq |\mathrm{Aut}(\mathcal{X})_P|$ by (15). Assume that $g'' = 0$. From (5),

$$2g' = \sum_{i=1}^{k}(|D| - \ell_i)$$

with $\ell_1, \ldots, \ell_k$ being the sizes of the short orbits of D on $\mathcal{X}_1$, other than the two trivial ones $\{\bar{P}\}$ and $\{\bar{Q}\}$. Since $|D|$ is odd, because $p = 2$, each such short orbit has length at most $\frac{1}{3}|D|$. From this, $g' \geq \frac{1}{3}|D|$ whence $g \geq \frac{1}{3}|\mathrm{Aut}(\mathcal{X})_P|$ by (15). But this contradicts (2). □

Lemma 5.4. *Assume that $|S| > 6(g-1)$ and that $\mathcal{X}_1 = \mathcal{X}/S_P^{(1)}$ is rational. Let $Q \in \Delta$. Then the subgroups S_P and S_Q have trivial intersection, and S_Q is a cyclic group whose order divides $q+1$. Also,*

$$2g - 2 = \frac{|S|\,(|S_P| - |S_P^{(1)}|\,|S_Q|)}{|S_Q|(|S| - |S_P|)} \tag{16}$$

Proof. Let $\alpha \in S_P \cap S_Q$ be non-trivial. Then $p \nmid \mathrm{ord}\,\alpha$, and hence α is in a complement H of $S_P^{(1)}$. Therefore, α fixes not only P but another point in Ω, say R. Since $Q \notin \Omega$, this shows that α has at least three fixed points. These points are in three different orbits of $S_P^{(1)}$. Since the quotient curve $\mathcal{X}_1 = \mathcal{X}/S_P^{(1)}$ is rational, this implies that α is trivial, a contradiction. Hence $|S_P \cap S_Q| = 1$. Therefore, no non-trivial element of S_Q fixes a point in Ω. Since $|\Omega| = q+1$, the second assertion follows. Let

$$\eta = |S_Q|(d_P - |S_P|) - |S_P|. \tag{17}$$

Then

$$|S| = 2(g-1)\frac{|S_P^{(1)}||H||S_Q|}{\eta}, \tag{18}$$

where H is a complement of $S_P^{(1)}$ in S_P. Substituting d_P from (13) into (17) and then this into (18) gives (16). □

5.1. **Case** $S \cong \mathrm{PSL}(2,q)$**.** In this case $n = q$ and

$$|S| = q^3 - q,\ |S_P| = q(q-1),\ |S_P^{(1)}| = q.$$

By Lemma 5.3, if (2) holds then $\mathcal{X}_1$ is rational. Lemma 5.4 implies that $|S_Q|$ divides $q+1$. Let $|S_Q| = (q+1)/t$ with $t|(q+1)$. Equation (16) gives $2g = (t-1)(q-1)$.

5.2. **Case $S \cong \mathrm{PSU}(3,n)$.** In this case, $q = n^3$ and

$$|S| = (n^3+1)n^3(n^2-1)/\mu, \ |S_P| = n^3(n^2-1)/\mu, \ |S_P^{(1)}| = n^3,$$

Also, by Lemma 5.3, (2) implies that $\mathcal{X}_1$ is rational. By Lemmas 2.2 and 5.4, two cases are to be discussed, according as $|S_Q|$ divides either $(n^2-n+1)/\mu$, or $n+1$. By (16),

$$2g = \frac{(n^3+1)(n^2-1)}{\mu|S_Q|} - (n^3-1).$$

If $|S_Q| = (n^2-n+1)/(t\mu)$, then

$$2g = (n-1)(t(n+1)^2 - (n^2+n+1)). \tag{19}$$

If $t=1$, then $g = \frac{1}{2}n(n-1)$. Therefore, $t=1$ only occurs when (II) holds.

If $|S_Q| = (n+1)/t$, then

$$2g = (n-1)\left[\frac{(n^3+1)t}{\mu} - (n^2+n+1)\right].$$

5.3. **Case $S \cong \mathrm{SU}(3,n)$ with $3|(n{+}1)$.** Let $\mathcal{Y} = \mathcal{X}/Z(S)$ be the quotient curve of $\mathcal{X}$ with respect to the centre $Z(S)$ of S. By Lemma 5.4, the points in Ω are the fixed points of the non-trivial elements in $Z(S)$. The group $\bar{S} = S/Z(S) \cong \mathrm{PSU}(3,n)$ can be viewed as a subgroup of $\mathrm{Aut}(\mathcal{Y})$. Since $|Z(S)| = 3$, from (5)

$$2g-2 = 3(2\bar{g}-2) + 2(n^3+1)$$

where $\bar{g}$ is the genus of $\mathcal{Y}$. From this, if (2) holds, then $|\mathrm{Aut}(\mathcal{Y})_{\bar{P}}|$ is even and bigger than $3\bar{g}$ for the point $\bar{P}$ lying under P in the covering $\mathcal{X} \to \mathcal{Y}$. Also, $|\bar{S}| > 6(\bar{g}-1)$ holds. Hence, the preceding case applies to $\mathcal{Y}$ whence the assertion follows for $\mathcal{X}$.

5.4. **Case $S = \mathrm{Sz}(n)$.** In this case, $n = 2n_0^2$, $n_0 = 2^r$, $r \geq 1$, and

$$|S| = (n^2+1)n^2(n-1), \ |S_P| = n^2(n-1), \ |S_P^{(1)}| = n^2.$$

Also, by Lemma 5.3, if (2) holds then $\mathcal{X}_1$ is rational. From Lemmas 2.2 and 5.4, there is an odd integer t such that either (A) or (B) holds, where

$$\text{(A)} \qquad 2g = (t-1)(n^2-1) - 2tn_0(n-1), \quad |S_Q| = (n+2n_0+1)/t;$$

$$\text{(B)} \qquad 2g = (t-1)(n^2-1) + 2tn_0(n-1), \quad |S_Q| = (n-2n_0+1)/t.$$

In case (B), if $t=1$ then (III) holds.

6. Non-solvable $\mathbb{K}$–automorphism groups of p–rank zero curves

Theorem 6.1. *Let $\mathcal{X}$ be a zero 2-rank algebraic curve of genus $g \geq 2$ defined over an algebraically closed groundfield $\mathbb{K}$ of characteristic 2. If $\mathrm{Aut}(\mathcal{X})$ is non-solvable then its commutator group $\mathrm{Aut}(\mathcal{X})'$ coincides with S and hence is one of the groups in (1).*

Proof. Since groups of odd order, as well as subgroups of $\mathrm{Aut}(\mathcal{X})$ fixing a point of $\mathcal{X}$, are solvable, case (a) in Theorem 1.1 holds. In particular, S is a perfect group, that is, S coincides with its commutator group. Then S is a subgroup of the commutator subgroup $\mathrm{Aut}(\mathcal{X})'$ of $\mathrm{Aut}(\mathcal{X})$.

On the other hand, since S is a normal subgroup of $\mathrm{Aut}(\mathcal{X})$, the factor group $\mathrm{Aut}(\mathcal{X})/S$ can be viewed as a $\mathbb{K}$-automorphism group of the quotient curve $\mathcal{Z} = \mathcal{X}/S$. For a point P in Ω, let $\bar{P}$ be the point of $\mathcal{Z}$ lying under P. Since Ω an S-orbit on $\mathcal{X}$, the set of points lying over $\bar{P}$ coincides with Ω. As Ω is also an $\mathrm{Aut}(\mathcal{X})$-orbit, this implies that the factor group $\mathrm{Aut}(\mathcal{X})/S$ fixes $\bar{P}$. Furthermore, $\mathrm{Aut}(\mathcal{X})/S$ is tame as $\mathrm{Aut}(\mathcal{X})/S$ has odd order. Hence, $\mathrm{Aut}(\mathcal{X})/S$ is cyclic. Therefore, S contains $\mathrm{Aut}(\mathcal{X})'$. $\square$

For a non-solvable group $\mathrm{Aut}(\mathcal{X})$, the following theorem describes the structure of $\mathrm{Aut}(\mathcal{X})$ in terms of $\mathrm{Aut}(\mathcal{X})'$ and the kernel N of the permutation representation of $\mathrm{Aut}(\mathcal{X})$ on Ω.

Theorem 6.2. *Let $\mathcal{X}$ be a zero 2-rank algebraic curve of genus $g \geq 2$ defined over an algebraically closed groundfield $\mathbb{K}$ of characteristic 2. If $\mathrm{Aut}(\mathcal{X})$ is non-solvable then $\mathrm{Aut}(\mathcal{X})' = S$ and one of the following cases occur for a cyclic group of odd order N:*

- (i) $\mathrm{Aut}(\mathcal{X})' = \mathrm{PSL}(2,n)$ *and* $\mathrm{Aut}(\mathcal{X}) = \mathrm{PSL}(2,n) \times N$*;*
- (ii) $\mathrm{Aut}(\mathcal{X})' = \mathrm{Sz}(n)$ *and* $\mathrm{Aut}(\mathcal{X}) = \mathrm{Sz}(n) \times N$*;*
- (iii) $\mathrm{Aut}(\mathcal{X})' = \mathrm{PSU}(3,n)$ *and either*
  - (iii)(a) $\mathrm{Aut}(\mathcal{X})/N = \mathrm{PSU}(3,n)$ *and* $\mathrm{Aut}(\mathcal{X}) = \mathrm{PSU}(3,n) \times N$*, or*
  - (iii)(b) $\mathrm{Aut}(\mathcal{X})/N = \mathrm{PGU}(3,n)$ *and* $\mathrm{PSU}(3,n) \times N$ *is a subgroup of index* 3 *of* $\mathrm{Aut}(\mathcal{X})$.
- (iv) $\mathrm{Aut}(\mathcal{X})' = \mathrm{SU}(3,n)$ *and either*
  - (iv)(a) $\mathrm{Aut}(\mathcal{X})/N = \mathrm{PSU}(3,n)$ *and* $\mathrm{Aut}(\mathcal{X}) = \mathrm{SU}(3,n)N$*, or*
  - (iv)(b) $\mathrm{Aut}(\mathcal{X})/N = \mathrm{PGU}(3,n)$ *and* $\mathrm{SU}(3,n)N$ *is a subgroup of index* 3 *of* $\mathrm{Aut}(\mathcal{X})$*;*

where $n \geq 4$ is a power of 2.

Proof. Consider the quotient curve $\mathcal{Z} = \mathcal{X}/N$ where N is the subgroup of $\mathrm{Aut}(\mathcal{X})$ fixing Ω pointwise. Then $\mathrm{Aut}(\mathcal{X})/N$ can be viewed as an automorphism group of the quotient curve $\mathcal{X}/N$. From Lemma 2.1 applied to $L = SN/N$, it follows that

$$\mathrm{Aut}(\mathcal{X})/N \cong \begin{cases} \mathrm{PSL}(2,n), \\ \mathrm{PSU}(3,n), \\ \mathrm{PGU}(3,n), \quad \gcd(3,n+1)=3, \\ \mathrm{Sz}(n). \end{cases}$$

Furthermore,

$$SN/N \cong \begin{cases} \mathrm{PSL}(2,n), \\ \mathrm{PSU}(3,n), \\ \mathrm{Sz}(n). \end{cases}$$

From the third isomorphism theorem,

$$\mathrm{Aut}(\mathcal{X})/SN \cong (\mathrm{Aut}(X)/N)/(SN/N).$$

This implies that either $\mathrm{Aut}(\mathcal{X}) = SN$ or $\mathrm{Aut}(\mathcal{X})/N \cong \mathrm{PGU}(3,n)$ and $SN/N \cong \mathrm{PSU}(3,n)$ with $\gcd(3,n+1)=3$. Note that S and N have non-trivial intersection only for $S = \mathrm{SU}(3,n)$ when $|S \cap N| = 3$. Hence, if $\mathrm{Aut}(\mathcal{X}) = SN$ holds, then one of the cases (i), (ii), (iiia), (iva) occurs. Furthermore, if $\mathrm{Aut}(\mathcal{X})/N \cong \mathrm{PGU}(3,n)$ then SN has index 3 in $\mathrm{Aut}(\mathcal{X})$, and either (iiib) or (ivb) holds. □

Finally, Theorem 1.2 is a consequence of Theorems 5.1, 6.1 and 6.2 together with the following lemma.

Lemma 6.3. *Assume that* $|\mathrm{Aut}(\mathcal{X})| > 24g^2$. *If* $\mathrm{Aut}(\mathcal{X})$ *is non-solvable, then both conditions* (2) *and* (3) *are satisfied.*

Proof. Take a point $P \in \Omega$, and assume on the contrary that (2) does not hold. Since $|\mathrm{Aut}(\mathcal{X})_P|$ is even, this only occurs when $|\mathrm{Aut}(\mathcal{X})_P| \leq 3g$. Then clearly $|S_P^{(1)}| \leq 3g$ holds. This and $|\Omega| = |S_P^{(1)}| + 1$ imply that $|\Omega| \leq (3g+1)$. Therefore,

$$|\mathrm{Aut}(\mathcal{X})| = |\mathrm{Aut}(\mathcal{X})_P|\,|\Omega| \leq 3g(3g+1),$$

a contradiction with $\mathrm{Aut}(\mathcal{X})| \geq 24g^2$.

To prove that (3) holds, note that by Theorem 6.2

$$|S| \geq \frac{|\mathrm{Aut}(\mathcal{X})|}{3|N|} > \frac{8g^2}{|N|}, \tag{20}$$

with N a cyclic group of odd order fixing $|\Omega| = |S_P^{(1)}| + 1 \geq 3$ points of $\mathcal{X}$. Then, by (5),

$$2g-2 \geq -2|N| + |\Omega|(|N|-1) \geq (|N|-1)(|\Omega|-2) - 2.$$

Since $|N| \geq 3$ and $|\Omega| \geq 5$, this yields that $2g \geq \frac{2}{3}|N|(|\Omega|-2) \geq 2|N|$. From this and (20), we obtain that $|S| > 8g > 6(g-1)$. □

7. Some examples

As pointed out in Introduction, each case in Theorem 1.1 (a) occurs, examples being the four curves (I)-(IV). To complete the discussion after Theorem 1.1, we exhibit further examples for (i) and for the first case in both (ii) and (iv). As far as we know, no more examples exist.

In case (i), Stichtenoth's result, see [31], Satz 7, determines all examples of curves $\mathcal{X}$ with an absolutely irreducible plane model $\mathcal{C}$

$$\mathbf{v}(A(Y)+B(X)), \tag{21}$$

where

(I) $\deg \mathcal{C} \geq 4$;
(II) $A(Y) = a_nY^{2^n} + a_{n-1}Y^{2^{n-1}} + \ldots + a_0Y, \quad a_j \in K,\ a_0,\ a_n \neq 0$;
(III) $B(X) = b_mX^m + b_{m-1}X^{m-1} + \ldots + b_1X + b_0, \quad b_j \in K,\ b_m \neq 0$;
(IV) m is odd;
(V) $n \geq 1,\ m \geq 3$.

Such a curve $\mathcal{X}$ has genus $g = \frac{1}{2}(m-1)(p^n-1)$, and Stichtenoth's result for $p = 2$ is as follows.

Proposition 7.1. *If $\mathcal{C}$ is a curve of type* (21), *then* $\mathrm{Aut}(\mathcal{X})$ *fixes a point, except in the following two cases:*

(i) (a) $\mathcal{C} = \mathbf{v}(Y^{2^n} + Y + X^m)$, *with* $m < 2^n$, $2^n \equiv -1 \pmod m$;
(b) $\mathrm{Aut}(\mathcal{X})$ *contains a cyclic subgroup* C_m *of order* m *such that* $\mathrm{Aut}(\mathcal{X}) \cong \mathrm{PSL}(2, 2^n) \times C_m$.
(ii) (a) $\mathcal{X} = \mathcal{C} = \mathbf{v}(Y^{2^n} + Y + X^{2^n+1})$, *the Hermitian curve;*
(b) $\mathrm{Aut}(\mathcal{X}) \cong \mathrm{PGU}(3, 2^n)$.

Proposition 7.2. *Let* $3|(n+1)$. *For every divisor* t *of* $(n^2-n+1)/3$, *the non-singular model of the plane curve*

$$\mathbf{v}(Y^{(n^2-n+1)/t} - X^{n^3} - X + (X^n+X)^{n^2-n+1}) \tag{22}$$

of genus $g = \frac{1}{2}(n-1)(3t(n+1)^2 - (n^2+n+1))$ *has a* $\mathbb{K}$*-automorphism group isomorphic to* $\mathrm{SU}(3, n)$. *Furthermore, the non-singular model of the plane curve*

$$\mathbf{v}(Y^{(n^2-n+1)/(3t)} - X^{n^3} - X + (X^n+X)^{n^2-n+1}) \tag{23}$$

of genus $g = \frac{1}{2}(n-1)(t(n+1)^2 - (n^2+n+1))$ *has a* $\mathbb{K}$*-automorphism group isomorphic to* $\mathrm{PSU}(3, n)$.

Proof. To show the first part, let $\mathcal{Y}$ be a non-singular model of the curve (22). Note that $\mathcal{Y}$ can be regarded as the quotient curve of the curve $\mathcal{X}$ given in (IV) with respect to the subgroup H of $\mathrm{Aut}(\mathcal{X})$ generated by the automorphism of equation $x' = x$, $y' = \lambda y$ where $\lambda \in \mathbb{K}$ is a primitive t-root of unity. The fixed points of the non-trivial automorphisms in H

are the n^3+1 points of $\mathcal{X}$ arising from the n^3+1 branches of the plane curve (22) centred at points on the X-axis. Since t is odd and $\mathcal{X}$ has genus $\frac{1}{2}(n^3+1)(n^2-2)$, from (5) $g=\frac{1}{2}(n-1)(3t(n+1)^2-(n^2+n+1))$ follows. The normalizer of H in $\mathrm{Aut}(\mathcal{X})$ contains a subgroup isomorphic to $\mathrm{SU}(3,n)$ with intersects H trivially. This completes the proof of the first part.

To show the second part, let $\mathcal{Z}$ be a a non-singular model of the curve (23). This time, $\mathcal{Z}$ is regarded as the quotient curve of the curve $\mathcal{Y}$ with respect to the subgroup H of $\mathrm{Aut}(\mathcal{Y})$ generated by the automorphism of equation $x'=x$, $y'=\epsilon y$ where $\epsilon\in\mathbb{K}$ is a primitive third root of unity. As before, the fixed points of the non-trivial automorphisms in H are the n^3+1 points of $\mathcal{Y}$ arising from the n^3+1 branches of the plane curve (22) centred at points on the X-axis. From (5) applied to $\mathcal{Y}$ and G, we get $g=\frac{1}{2}(n-1)(t(n+1)^2-(n^2+n+1))$. The centralizer of H in $\mathrm{Aut}(\mathcal{Y})$ is a subgroup T isomorphic to $\mathrm{SU}(3,n)$. Since $\mathrm{SU}(3,n)/Z(\mathrm{SU}(3,n))\cong\mathrm{PSU}(3,n)$, this shows that $\mathrm{Aut}(\mathcal{Z})$ has a subgroup isomorphic to $\mathrm{PSU}(3,n)$. □

Proposition 7.3. *Let $3|(n-1)$. For every divisor t of n^2-n+1, the non-singular model $\mathcal{X}$ of the plane curve*

$$\mathbf{v}(Y^{(n^2-n+1)/t}-X^{n^3}-X+(X^n+X)^{n^2-n+1}) \tag{24}$$

of genus $g=\frac{1}{2}(n-1)(3t(n+1)^2-(n^2+n+1))$ has a $\mathbb{K}$-automorphism group isomorphic to $\mathrm{PSU}(3,n)$.

Proof. For $3|(n-1)$, $\mathrm{SU}(3,n)=\mathrm{PSU}(3,n)$ holds, and the proof can be carried out following the first part in the proof of Proposition 7.2. □

Our final remark is that the curves discussed in the last two propositions are investigated in [4].

References

[1] E. Çakçak and F. Özbudak, Subfields of the function field of the Deligne–Lusztig curve of Ree type. Acta Arith. **115** (2004), 133–180.

[2] A. Garcia, H. Stichtenoth and C.P. Xing, On subfields of the Hermitian function field. Compositio Math. **120** (2000), 137–170.

[3] M. Giulietti and G. Korchmáros, On large automorphism groups of algebraic curves in positive characteristic. Available at http://arxiv.org/abs/0706.2320.

[4] M. Giulietti and G. Korchmáros, A new family of maximal curves over a finite field. Available at http://arxiv.org/abs/0711.0445.

[5] M. Giulietti, G. Korchmáros and F. Torres, Quotient curves of the Deligne–Lusztig curve of Suzuki type. Acta Arith. **122** (2006), 245–274.

[6] L. Greenberg, Maximal groups and signatures. Ann. of Math. Studies **79** (1974), 207-226.

[7] R. Gow, Some TI subgroups of solvable groups. J. London Math. Soc. **12** (1976), 285–286.
[8] J.P. Hansen and J.P. Pedersen, Automorphism group of Ree type, Deligne-Lusztig curves and function fields. J. Reine Angew. Math. **440** (1993), 99–109.
[9] H.W. Henn, Funktionenkörper mit groβer Automorphismengruppe. J. Reine Angew. Math. **302** (1978), 96–115.
[10] C. Hering, On subgroups with trivial normalizer intersection. J. Algebra **20** (1972), 622–629.
[11] J.W.P. Hirschfeld, *Finite Projective Spaces of Three Dimensions*, Oxford Univ. Press, Oxford, 1985, x+316 pp.
[12] J.W.P. Hirschfeld, *Projective Geometries Over Finite Fields*, Second edition, Oxford University Press, Oxford, 1998, xiv+555 pp.
[13] J.W.P. Hirschfeld, G. Korchmáros and F. Torres *Algebraic Curves Over a Finite Field*, Princeton Univ. Press, Princeton and Oxford, 2008, xx+696 pp.
[14] B. Huppert, *Endliche Gruppen. I*, Grundlehren der Mathematischen Wissenschaften **134**, Springer, Berlin, 1967, xii+793 pp.
[15] B. Huppert and B.N. Blackburn, *Finite groups. III*, Grundlehren der Mathematischen Wissenschaften **243**, Springer, Berlin, 1982, ix+454 pp.
[16] K. Iwasawa and T. Tamagawa, On the group of automorphisms of a function field. J. Math. Soc. Japan **3** (1951), 137–147.
[17] K. Iwasawa and T. Tamagawa, Correction: On the group of automorphisms of a function field. J. Math. Soc. Japan **4** (1952), 100–101.
[18] K. Iwasawa and T. Tamagawa, Correction: On the paper "On the group of automorphisms of a function field". J. Math. Soc. Japan **4** (1952), 203–204.
[19] W.M. Kantor, M. O'Nan and G.M. Seitz, 2-transitive groups in which the stabilizer of two points is cyclic. J. Algebra **21** (1972), 17–50.
[20] C. Lehr and M. Matignon, Automorphism groups for p-cyclic covers of the affine line. Compositio Math. **141** (2005), 1213–1237.
[21] M. Madan and M. Rosen, The automorphism group of a function field. Proc. Amer. Math. Soc. **115** (1992), 923-929.
[22] D.J. Madden and R.C. Valentini, The group of automorphisms of algebraic function fields. J. Reine Angew. Math. **343** (1983), 162–168.
[23] P. Mihauilescu, Primary cyclotomic units and a proof of Catalan's conjecture. J. Reine Angew. Math. **572** (2004), 167–195.
[24] S. Nakajima, p-ranks and automorphism groups of algebraic curves. Trans. Amer. Math. Soc. **303** (1987), 595–607.
[25] S. Nakajima, On abelian automorphism groups of algebraic curves. J. London Math. Soc. **36** (1987), 23–32.
[26] S. Nakajima, On automorphism groups of algebraic curves, *Current Trends in Number Theory*, Hindustan Book Agency, New Delhi, 2002, 129–134.
[27] P. Roquette, Über die Automorphismengruppe eines algebraischen Funktionenkörpers. Arch. Math. **3** (1952), 343–350.
[28] P. Roquette, Abschätzung der Automorphismenanzahl von Funktionenkörpern bei Primzahlcharakteristik. Math. Z. **117** (1970), 157–163.
[29] H.I. Schmid, Über Automorphismen eines algebraische Funktionenkörpern von Primzahlcharakteristic. J. Reine Angew. Math. **179** (1938), 5-15.

[30] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I. Eine Abschätzung der Ordnung der Automorphismengruppe. Arch. Math. **24** (1973), 527–544.
[31] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. II. Ein spezieller Typ von Funktionenkörpern. Arch. Math. **24** (1973), 615–631.
[32] H. Stichtenoth, Zur Realisierbarkeit endlicher Gruppen als Automorphismengruppen algebraischer Funktionenkörper. Math. Z. **187** (1984), 221–225.
[33] J. Tits, Les groupes simples de Suzuki et de Ree. Séminaire Bourbaki **6**, Soc. Math. France, Paris, 1995, 65–82.
[34] J. Tits, Ovoides et groupes de Suzuki. Arch. Math. **13** (1962), 187–198.
[35] R.C. Valentini and M.L. Madan, A Hauptsatz of L.E. Dickson and Artin–Schreier extensions. J. Reine Angew. Math. **318** (1980), 156–177.
[36] J.P. Zhang, On the finite group with a TI Sylow p-subgroup. Chinese Ann. Math. Ser. B **12** (1991), 147–151.

Authors' addresses:

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

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