ALGEBRAIC CURVES WITH A LARGE NON-TAME AUTOMORPHISM GROUP FIXING NO POINT

M. GIULIETTI AND G. KORCHMÁROS

Abstract. Let \( K \) be an algebraically closed field of characteristic \( p > 0 \), and let \( X \) be a curve over \( K \) of genus \( g \geq 2 \). Assume that the automorphism group \( \text{Aut}(X) \) of \( X \) over \( K \) fixes no point of \( X \). The following result is proven. If there is a point \( P \) on \( X \) whose stabilizer in \( \text{Aut}(X) \) contains a \( p \)-subgroup of order greater than \( gp/(p-1) \), then \( X \) is birationally equivalent over \( K \) to one of the irreducible plane curves (II), (III), (IV), (V) listed in the Introduction.

1. Introduction

In this paper, \( K \) denotes an algebraically closed field of positive characteristic \( p > 0 \). Let \( \text{Aut}(X) \) be the \( K \)-automorphism group of a projective, non-singular, geometrically irreducible, algebraic curve \( X \) of genus \( g \geq 2 \). It is well known that \( \text{Aut}(X) \) is finite and that the classical Hurwitz bound

\[
|\text{Aut}(X)| \leq 84(g-1)
\]

holds provided that \( p \nmid |\text{Aut}(X)| \). If \( p \) divides \( |\text{Aut}(X)| \), then the curve \( X \) may happen to have a much larger \( K \)-automorphism group compared to its genus.

The curves \( X \) with \( |\text{Aut}(X)| \geq 8g^2 \) are listed below, up to a birational equivalence over \( K \) to an irreducible plane curve \( v(F) \) with \( F \in K[X,Y] \), where \( F = 0 \) stands for an affine equation of the curve; see [12] and Remark [24] and also [13, Theorem 11.127].

(1) The hyperelliptic curve \( v(Y^2 + Y + X^{2^k+1}) \) with \( p = 2 \), \( g = 2k-1 \), \( k \geq 2 \), \( |\text{Aut}(X)| = 2^{2k+1}k^2+1 \), \( \text{Aut}(X) \) fixes a point \( P \in X \).

(II) The hyperelliptic curve \( v(Y^2 - (X^n - X)) \) with \( p > 2 \), \( n = p^k > 3 \), \( g = \frac{1}{2}(n-1)\), \( |\text{Aut}(X)/M| = \text{PGL}(2,n) \), \( |M| = 2 \), \( |\text{Aut}(X)| = 2(n+1)n(n-1) \).

(III) The Hermitian curve \( v(Y^n + Y - X^{n+1}) \) with \( n = p^k \geq 3 \), \( g = \frac{1}{2}(n^2 - n) \), \( |\text{Aut}(X)| = \text{PGU}(3,n) \), \( |\text{Aut}(X)| = (n^3 + 1)n^3(n^2 - 1) \).

(IV) The DLS curve (the Deligne-Lusztig curve arising from the Suzuki group) \( v(X^{n_0}(X^n + X) - (Y^n + Y)) \) with \( p = 2 \), \( n_0 = 2^r \), \( r \geq 1 \), \( n = 2n_0^2 \), \( g = n_0(n-1) \), \( |\text{Aut}(X)| = \text{Sz}(n) \), where \( \text{Sz}(n) \) is the Suzuki group, \( |\text{Aut}(X)| = (n^2 + 1)n^2(n-1) \).

Another relevant example in this direction is the following.
(V) The DLR curve (the Deligne-Lusztig curve arising from the Ree group) $v(Y^n - 1 + (X^n - X)^{n-1})Y^n + (X^n - X)^{n-1}Y - X^n(Y^n - X)^{n+n_0}$, with $p = 3, n_0 = 3^r, n = 3n_0^2, g = \frac{3}{2}n_0(n-1)(n+n_0+1)$, $\text{Aut}(X) \cong \text{Ree}(n)$, where $\text{Ree}(n)$ is the Ree group, $|\text{Aut}(X)| = (n^3 + 1)n^3(n-1)$.

Each of these curves has a large $p$-subgroup in $\text{Aut}(X)$ compared to its genus. Therefore, they are of interest in an on-going project aimed at obtaining a classification of curves $X$ having a $p$-subgroup $S$ in $\text{Aut}(X)$ with a “big action”, that is,

$$|S| \geq \frac{2p}{p - 1},$$  

The term of big action was introduced by Lehr and Matignon [19] and found its motivation in earlier work by Stichtenoth [27] and Nakajima [22]. As a consequence of Nakajima’s results, (1.2) implies that $S$ fixes a point of $X$. This was observed by Lehr and Matignon [19]. In their investigation on big actions satisfying the condition

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

they proved that (1.2) and (1.3) only occur simultaneously when the curve is birationally equivalent over $K$ to an Artin-Schreier curve $v(Y^n - Y - f(X))$ such that $f(X) = XP(X) + cX$, where $P(X)$ is an additive polynomial of $K[X]$; see [19]. Matignon and Rocher [20, 23, 24] continued the work of Lehr and Matignon, especially in order to classify big actions in which

$$|S| \geq 2g + 1$$

In this paper the following result is obtained.

**Theorem 1.1.** Let $X$ be a projective, geometrically irreducible, non-singular curve of genus $g \geq 2$. If $\text{Aut}(X)$ has no fixed point on $X$ and contains a $p$-subgroup $S$ fixing a point of $X$ such that

$$|S| \geq \frac{p}{p - 1},$$

then $X$ is birationally equivalent over $K$ to one of the irreducible plane curves (II),(III),(IV),(V).

The curves (II),(III),(IV),(V) have indeed the required properties in Theorem 1.1 when $S$ is a Sylow $p$-subgroup of $\text{Aut}(X)$. Furthermore, if (1.4) is replaced by the stronger big-action hypothesis (1.2), then the condition on $S$ to have a fixed point is satisfied and it can be dropped from the hypotheses of Theorem 1.1. Also, if (1.3) is replaced by the stronger condition $|S| > 2g + 1$ in Theorem 1.1 then one of the three cases (III),(IV),(V) holds, up to birational equivalence over $K$. This weaker form of Theorem 1.1 was our preliminary result, and it appears as Theorem 11.140 in [13].

An essential idea in our proof of Theorem 1.1 is to use deeper group theory by exploiting the following purely group-theoretic property which is a consequence of the hypotheses: Every element of $\text{Aut}(X)$ of order a power of $p$ has exactly one
fixed point; see Theorem 3.1. Let \( \Omega \) be the set of all points of \( X \) which are fixed by some element of \( G \) of order \( p \). Looking into Henn’s paper [12] with that property in mind, one may realize that a thorough investigation of the action of \( \text{Aut}(X) \) on \( \Omega \) is possible with methods building on those of Henn. The goal is that such an action is 2-transitive with non-trivial cyclic two-point stabilizer, as in Section 5 of Henn’s paper. This is achieved in Lemma 4.2 when \( \Omega \) is the unique short orbit of \( \text{Aut}(X) \) on \( X \), and in Proposition 5.3 when there is another short orbit. Therefore, the Kantor-O’Nan-Seitz theorem provides all possibilities arising for \( \text{Aut}(X) \) in such a way. Besides those appearing in (II),(III),(IV) and (V), they are solvable groups. To determine which curves comply with these groups under the hypothesis (1.4), and in particular to rule out solvable groups from our context, we continue relying mostly on group theory and geometry rather than on function field theory, unlike Henn did in the rest of his paper using only elementary facts from group theory regarding the one- and two-point stabilizers of the groups in (II),(III),(IV) and (V). Nevertheless, another result from Henn’s paper enters in our proof; see Lemma 5.4, which corresponds to (8) of [12]. New ingredients in our case-by-case analysis of the groups admitted by the Kantor-O’Nan-Seitz theorem to be candidates for \( \text{Aut}(X) \) include a few results on the actions of cyclic subgroups of 2-transitive groups together with some consequences of classical results, such as Huppert’s classification of solvable 2-transitive permutation groups, Griess’ results on Schur multipliers of simple groups, and Zassenhaus’ classification of 2-transitive permutation groups with trivial 3-point stabilizer. More precisely, Huppert’s classification together with Catalan’s conjecture from Number Theory play an important role when we deal with solvable groups, while Griess’ results together with Zassenhaus’ classification are the main ingredients in our investigation when the action of \( \text{Aut}(X) \) on \( \Omega \) is not faithful. All these results are independent of the classification of finite simple groups and are outlined in Section 2.

We point out that a similar classification under a bit weakened hypothesis than (1.4) may involve more curves, as suggested by the following example.

For an odd prime \( p \), with \( p \equiv 2 \pmod{3} \), let \( X \) be the non-singular model of the irreducible plane curve

\[
v(Y^{3(p^2-p+1)} - (X^{p^3} + X - (X^p + X)^{p^2-p+1})).
\]

From [4], see also [5], \( X \) has genus \( g = \frac{1}{2} (2p^3 + 3p^2 - 3p - 2) \), and \( \text{Aut}(X) \) has a subgroup \( G \) isomorphic to \( \text{SU}(3,p) \). Further, \( G \) fixes no point of \( X \). Also, every Sylow \( p \)-subgroup \( S \) of \( G \) has order \( p^3 \) and fixes a point \( P \in X \). Then

\[
\frac{|S|}{g} = \frac{p}{p-1} - \frac{5}{2(p-1)} \left( 1 - \frac{p + 2}{2p^2 + 5p + 10} \right).
\]

2. Background and some preliminary results

Let \( X \) be a projective, non-singular, geometrically irreducible, algebraic curve of genus \( g \geq 2 \) embedded in the \( r \)-dimensional projective space \( PG(r,K) \) over an algebraically closed field \( K \) of positive characteristic \( p > 0 \). Let \( \Sigma \) be the function field of \( X \) which is an algebraic function field of transcendence degree one over \( K \). The automorphism group \( \text{Aut}(X) \) of \( X \) is defined to be the automorphism group of \( \Sigma \) fixing every element of \( K \). It has a faithful permutation representation on the set of all points \( X \) (equivalently on the set of all places of \( \Sigma \)).
Let $G$ be a finite subgroup of $\text{Aut}(X)$. The orbit

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

is long if $|o(P)| = |G|$; otherwise $o(P)$ is short.

The subfield $\Sigma^G$ consisting of all elements of $\Sigma$ fixed by every element in $G$ also has transcendency degree one over $K$. Let $\mathcal{Y}$ be a non-singular model of $\Sigma^G$, that is, a projective, non-singular, geometrically irreducible, algebraic curve with function field $\Sigma^G$. Sometimes, $\mathcal{Y}$ is called the quotient curve of $X$ by $G$ and denoted by $X/G$. The covering $X \to \mathcal{Y}$ has degree $|G|$ and the field extension $\Sigma/\Sigma^G$ is Galois.

If $P$ is a point of $X$, the stabiliser $G_P$ of $P$ in $G$ is the subgroup of $G$ consisting of all elements fixing $P$. For a non-negative integer $i$, the $i$-th ramification group of $X$ at $P$ is denoted by $G_P^{(i)}$ (or $G_i(P)$ as in [26 Chapter IV]) and defined to be

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

where $t$ is a uniformizing element (local parameter) at $P$. Here $G_P^{(0)} = G_P$ and $G_P^{(1)}$ is the unique Sylow $p$-subgroup of $G_P$. Moreover, $G_P^{(1)}$ has a cyclic complement $H$ in $G_P$, that is, $G_P = G_P^{(1)} \rtimes H$ with a cyclic group $H$ of order coprime with $p$. In particular, $G_P$ is a solvable group. 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 $X$, let $e_Q = |G_Q|$ and

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

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 the quotient curve $X/G$. The Hurwitz genus formula gives the following equation:

$$2g - 2 = |G|/(2g' - 2) + \sum_{Q \in X} d_Q. \tag{2.1}$$

Assume that $G_P^{(1)}$ only ramifies at $P$. Then (2.1) applied to $G_P^{(1)}$ gives

$$2g - 2 = |G_P^{(1)}|/(2g' - 2) + 2(|G_P^{(1)}| - 1) + \sum_{i \geq 2} \left( |G_P^{(i)}| - 1 \right), \tag{2.2}$$

where $g'$ denotes the genus of the quotient curve $X/G_P^{(1)}$.

If $G$ is tame, that is, $p \nmid |G|$, or more generally if $p \nmid e_Q$ for every $Q \in X$, Equation (2.1) is simpler and may be written as

$$2g - 2 = |G|(2g' - 2) + \sum_{i=1}^k (|G| - \ell_i), \tag{2.3}$$

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

The following upper bounds depending on $g$ are due to Stichtenoth [27]; see also [13 Theorems 11.60 and 11.78].

**Theorem 2.1.** Let $g \geq 1$. If $G_P = G_P^{(1)} \rtimes H$ with $P \in X$ and $p \nmid |H|$, then $|H| \leq 4g + 2$. 

Theorem 2.2. Let $g \geq 1$. If $P \in \mathcal{X}$, then

$$|G_p^{(1)}| \leq \frac{4p}{p-1}g^2.$$  

More precisely, if $X_i$ is the quotient curve $X/G_p^{(i)}$, then one of the following cases occurs:

(i) $X_1$ is not rational, and $|G_p^{(1)}| \leq g$;

(ii) $X_1$ is rational, the covering $X \to X_1$ ramifies not only at $P$ but at some other point of $X$, and (1.4) does not hold for $S = G_p^{(1)}$, that is,  

$$|G_p^{(1)}| \leq \frac{p}{p-1}g;$$

(iii) $X_1$ and $X_2$ are rational, the covering $X \to X_1$ ramifies only at $P$, and

$$|G_p^{(1)}| \leq \frac{4|G_p^{(2)}|}{(|G_p^{(2)}| - 1)^2}g^2 \leq \frac{4p}{(p-1)^2}g^2.$$  

It may be noted that the non-singular model of the irreducible plane curve $v(Y^p + Y - X^{p+1})$ provides an example with $|G_p^{(1)}| = 4pg^2/(p-1)^2$, showing that the bound $|G_p^{(1)}| \leq 4pg^2/(p-1)^2$ in (2.4) is sharp; see [27], p. 533, Remark 1, [28] Satz 5], and [13] Theorem 12.9. The curves attaining this bound are determined by Lehr and Matignon [19]; see the Introduction. It may be noted that for $g \geq 2$, Theorem [13] gives a complete classification for case (iii) under the hypothesis that Aut($X$) fixes no point of $X$.

Lemma 2.3. Up to birational equivalence over $\mathbb{K}$, each of the irreducible plane curves (II), (III), (IV), (V) is uniquely determined by its genus and its automorphism group over $\mathbb{K}$. In case (III), this even holds true when Aut($X$) is only assumed to contain a subgroup isomorphic to PSU(3, n).


Remark 2.4. As mentioned in the Introduction, Henn’s paper [12] contains a classification of curves with $|\text{Aut}(X)| \geq 8p^3$ showing that such curves are those listed in (I), (II), (III), (IV). Nakajima [22] claimed that Henn’s proof contained a gap. That gap was filled up in [11]. For a revised version of Henn’s proof, see [13] Chapter 11.12.

In the rest of this section, $\mathcal{X}$ stands for a non-hyperelliptic curve of genus $g \geq 3$, and it is assumed to be the canonical curve of $\mathbb{K}(\mathcal{X})$. So, $\mathcal{X}$ is a non-singular curve of degree $2g - 2$ embedded in PG$(g - 1, \mathbb{K})$, and the canonical series of $\mathbb{K}(\mathcal{X})$ is cut out on $\mathcal{X}$ by hyperplanes. Let $1, x_1, \ldots, x_{g-1}$ denote the coordinate functions of this embedding with respect to a homogeneous coordinate frame $(X_0, X_1, \ldots, X_{g-1})$ in PG$(g - 1, \mathbb{K})$.

For a point $P \in \mathcal{X}$, the order sequence of $\mathcal{X}$ at $P$ is the strictly increasing sequence

$$j_0(P) = 0 < j_1(P) = 1 < j_2(P) < \ldots < j_{g-1}(P)$$

such that each $j_i(P)$ is the intersection number $I(P, \mathcal{X} \cap H_i)$ of $\mathcal{X}$ and some hyperplane $H_i$ at $P$; see [29] and [13] Chapter 7.6. For $i = g - 1$, such a hyperplane $H_{g-1}$ is uniquely determined, being the osculating hyperplane to $\mathcal{X}$ at $P$. Another
characterisation of the integers \( j(P) \), called \( P \)-orders or Hermitian \( P \)-invariants, appearing in (2.5) is that \( j \) is a \( P \)-order if and only if \( j + 1 \) is a Weierstrass gap; that is, no element in \( \mathbb{K}(X) \) regular outside \( P \) has a pole of order \( j + 1 \). Now, assume that \( j_{g-1}(P) = 2g - 2 \), that is, that \( P \) is the unique common point of \( H_{g-1} \) with \( X \). Then the hyperplanes of \( \text{PG}(g-1, \mathbb{K}) \) whose intersection number with \( X \) at \( P \) is at least \( j_{g-2}(P) \) cut out on \( X \) a linear series \( g_n^j \) of degree \( n = 2g - 2 - j_{g-2}(P) \) and projective dimension 1. Let \( \mathcal{L} \) be the projective line over \( \mathbb{K} \). Then \( g_n^j \) gives rise to a covering \( X \to \mathcal{L} \) of degree \( n \) which completely ramifies at \( P \). If it also completely ramifies at the points \( P_1, \ldots, P_k \) of \( X \) other than \( P \), then by Hurwitz’s Theorem \[ \text{(2.6)} \] \[ 2g - 2 \geq -2n + (k + 1)(n - 1). \]

Note that \( n \) must be at least 3 as \( X \) is neither rational nor elliptic nor hyperelliptic.

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

Huppert’s classification theorem; see [17, Chapter XII, Section 7] and [13, Theorem A.18]: Let \( \mathcal{G} \) be a solvable 2-transitive permutation group of degree \( n \). Then \( n \) is a power of some prime \( p \), and \( \mathcal{G} \) is a subgroup of the affine semi-linear group \( \mathsf{AGL}(1, n) \), 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 [18] and [13, Theorem A.17]: Let \( \mathcal{G} \) be a finite 2-transitive permutation group whose 2-point stabiliser is cyclic. Then \( \mathcal{G} \) has either an elementary abelian regular normal subgroup, or \( \mathcal{G} \) is one of the following groups in their natural 2-transitive permutation representations: \( \text{PSL}(2, n), n \geq 4 \), \( \text{PGL}(2, n), n \geq 4 \), \( \text{PSU}(3, n), n \geq 3 \), \( \text{PGU}(3, n), n \geq 3 \), \( \text{Sz}(n) \), \( \text{Ree}(n) \).

Zassenhaus’ classification theorem; see [17, Chapter XI, Section 11] and [13, Theorem A.16]: Let \( \mathcal{G} \) be a 2-transitive permutation group whose 3-point stabiliser is trivial, and suppose that \( \mathcal{G} \) has no regular normal subgroup. If \( \mathcal{G} \) has degree \( n + 1 \), order \( (n + 1)nd \) with \( d \) even and \( d \leq \frac{1}{2}(n - 1) \), then \( n \) is odd and \( \mathcal{G} \) is \( \text{PSL}(2, n) \) in its natural 2-transitive permutation representation.

The natural 2-transitive permutation representations of the above linear groups on a finite set \( \Omega \):

(i) The projective linear group \( \mathcal{G} = \text{PGL}(2, n) \) has order \( n(n-1)(n+1) \). It is the automorphism group of \( \text{PG}(1, n) \); equivalently, \( \mathcal{G} \) acts on the set \( \Omega \) of size \( n + 1 \) consisting of all \( \mathbb{F}_n \)-rational points of the projective line defined over \( \mathbb{F}_n \). For every point \( P \in \Omega \), the stabilizer \( \mathcal{G}_P \) has size \( n(n-1) \). The natural 2-transitive representation of \( \text{PSL}(2, n) \) is obtained when \( \text{PSL}(2, n) \) is viewed as a subgroup of \( \text{PGL}(2, n) \); see [16, Chapters II.7 and II.8] and [13, Appendix A, Example A.7]. For even, \( \text{PGL}(2, n) = \text{PSL}(2, n) \). For odd, \( \text{PSL}(2, n) \) has order \( \frac{1}{2}n(n-1)(n+1) \). For \( n \geq 4 \), \( \text{PSL}(2, n) \) is a simple group and \( \text{PGL}(2, n) \) is a non-solvable group.

(ii) The projective unitary group \( \mathcal{G} = \text{PGU}(3, n) \) has order \( (n^3+1)n^3(n^2-1) \). It is the linear collineation group in the projective plane \( \text{PG}(2, n^2) \) preserving the classical unital \( \Omega \) of size \( n^3 + 1 \) consisting of all absolute points of a non-degenerate unitary polarity of \( \text{PG}(2, n^2) \); see [15, Chapter II.8] and [13, Appendix A, Example A.9]. For every point \( P \in \Omega \), the stabilizer \( \mathcal{G}_P \) has size \( n^3(n^2-1) \). Furthermore, \( \mathcal{G} \) is the automorphism group of the Hermitian curve, regarded as a non-singular plane curve defined over the finite field \( \mathbb{F}_n \), acting on the set \( \Omega \) of all its \( \mathbb{F}_{n^2} \)-rational points. The special projective
unitary group $\text{PSU}(3, n)$ either coincides with $\text{PGU}(3, n)$ or is a subgroup of $\text{PGU}(3, n)$ of index 3 according as $\mu = 1$ or $\mu = 3$ with $\mu = \gcd(3, n+1)$. In its action on $\Omega$, $\text{PSU}(3, n)$ is still 2-transitive and this is the natural 2-transitive representation of $\text{PSU}(3, n)$; see [15] Chapter II.8 and [14]. For $n \geq 4$, $\text{PSU}(3, n)$ is a simple group and $\text{PGU}(3, n)$ is a non-solvable group.

(iii) The Suzuki group $\mathcal{G} = \text{Sz}(n)$ with $n = 2q_0^2$, $n_0 = 2^r$ and $r \geq 1$ has order $(n^2 + 1)n^2(n - 1)$. It is the linear collineation group of $\text{PG}(3, n)$ preserving the Tits ovoid $\Omega$ of size $n^2 + 1$; see [17] Chapter XI.3 and [13] Appendix A, Example A.11. For every point $P \in \Omega$, the stabilizer $\mathcal{G}_P$ has size $n^2(n - 1)$. Furthermore, $\mathcal{G}$ is the automorphism group of the DLS curve, regarded as a non-singular curve defined over the finite field $\mathbb{F}_n$, acting on the set $\Omega$ of all its $\mathbb{F}_n$-rational points; see [8]. $\text{Sz}(n)$ is a simple group.

(iv) The Ree group $\mathcal{G} = \text{Ree}(n)$ with $n = 3q_0^2$, $n_0 = 3^r$ has order $(n^3 + 1)n^2(n - 1)$. It is the linear collineation group of $\text{PG}(6, n)$ preserving the Ree ovoid $\Omega$ of size $n^3 + 1$; see [17] Chapter XI.3 and [13] Appendix A, Example A.13. For every point $P \in \Omega$, the stabilizer $\mathcal{G}_P$ has size $n^3(n - 1)$. Furthermore, $\mathcal{G}$ is the automorphism group of the DLS curve, regarded as a non-singular curve defined over the finite field $\mathbb{F}_n$, acting on the set $\Omega$ of all its $\mathbb{F}_n$-rational points; see [11] and [2]. For $n > 3$, $\text{Ree}(n)$ is simple, while $\text{Ree}(3) \cong \text{PGL}(2, 3)$.

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 automorphism group, are explicitly given in the papers quoted.

Cyclic subgroups of some 2-transitive groups. The following technical lemmas are corollaries of the classifications of subgroups of $\text{PSL}(2, n)$, $\text{PSU}(3, n)$, $\text{Sz}(n)$ and $\text{Ree}(n)$. For a proof, see [6].

**Lemma 2.5.** Let $n \geq 5$ be odd. Any two distinct cyclic maximal subgroups of $\text{PSL}(2, n)$ have trivial intersection.

**Lemma 2.6.** Let $\mathcal{G}$ be a 2-transitive permutation group on a set $\Omega$. Let $U$ be a cyclic subgroup of $\mathcal{G}$ which contains no non-trivial element fixing a point.

(i) If $\mathcal{G} = \text{PSU}(3, n)$, $n \geq 3$, in its natural 2-transitive permutation representation, then $|U|$ divides either $n + 1$ or $(n^2 - n + 1)/\mu$, where $\mu = \gcd(3, n+1)$.

(ii) If $\mathcal{G} = \text{Sz}(n)$ in its natural 2-transitive permutation representation, then $|U|$ divides either $n - 2n_0 + 1$ or $n + 2n_0 + 1$.

(iii) If $\mathcal{G} = \text{Ree}(n)$, $n > 3$, in its natural 2-transitive permutation representation, then $|U|$ divides either $n + 1$, or $n - 3n_0 + 1$, or $n + 3n_0 + 1$.

Schur multiplier of some simple groups. For a finite group $\mathcal{G}$, a group $\Gamma$ is said to be a covering of $\mathcal{G}$ if $\Gamma$ has a central subgroup $U$, i.e. $U \subseteq Z(\Gamma)$, such that $\mathcal{G} \cong \Gamma/U$. If, in addition, $\Gamma$ is perfect, that is, $\Gamma$ coincides with its commutator subgroup, then the covering is called proper. For a non-abelian simple group $\mathcal{G}$, a proper covering is also called a semisimple group. From Schur’s work, see [14] Chapter 33 and [16] V.23,24,25, if $\mathcal{G}$ is a non-abelian simple group, then it possesses a “universal” proper covering group $\tilde{\Gamma}$ with the property that every proper covering group of $\mathcal{G}$ is a homomorphic image of $\tilde{\Gamma}$. The center $Z(\tilde{\Gamma})$ is called the Schur multiplier of $\mathcal{G}$. The Schur multipliers of simple groups are known; see Griess [9, 10]. In particular, the Schur multiplier of $\text{PSL}(2, n)$ with $n \geq 5$ odd has order 2; $\text{PSU}(3, n)$ with $n \geq 3$ has non-trivial Schur multiplier only for $3|q+1$, and if this occurs the Schur multiplier
has order 3. Therefore, if \( G \cong \text{PSU}(3, n) \) with \( n \geq 3 \) has a proper covering \( \Gamma \), then \( 3(n+1) \) and \( |Z(\Gamma)| = 3 \). \( \text{Ree}(n) \) with \( n > 3 \) has trivial Schur multiplier, and hence it admits no proper covering.

**Lemma 2.7.** Let \( G \) be a simple group isomorphic to either \( \text{PSU}(3, n) \) with \( n \geq 3 \), or \( \text{Ree}(n) \) with \( n > 3 \). If the center \( Z(\Gamma) \) of a group \( \Gamma \) has order 2 and \( G \cong \Gamma/Z(\Gamma) \), then \( \Gamma \) has a subgroup isomorphic to \( G \) and \( \Gamma = G \times Z(\Gamma) \).

**Proof.** The condition \( |Z(\Gamma)| = 2 \) implies that the commutator subgroup \( \Gamma' \) is a proper subgroup of \( \Gamma \). If \( \Gamma' \) contained \( Z(\Gamma) \), then \( \Gamma'/Z(\Gamma) \) would be isomorphic to a proper subgroup \( D \) of \( G \). Since \( \Gamma' \) is a normal subgroup of \( \Gamma \), this would yield that \( D \) is a proper normal subgroup of \( G \), contradicting the hypothesis. So, \( \Gamma' \cap Z(\Gamma) = \{id\} \), and hence \( \Gamma' \times Z(\Gamma) \) is a subgroup of \( \Gamma \). In particular,

\[
\Gamma' \cong (\Gamma' \times Z(\Gamma))/Z(\Gamma).
\]

Therefore, \( \Gamma' \) is isomorphic to a subgroup of \( G \). Since \( G \) is simple, this yields that \( \Gamma' \cong G \). From this, \( \Gamma = \Gamma' \times Z(\Gamma) \) with \( \Gamma' \cong G \).

\( \square \)

3. Short orbits of large automorphism groups

The first step in our proof of Theorem 1.1 is the following result.

**Theorem 3.1.** Let \( \mathcal{X} \) be a projective, geometrically irreducible, non-singular curve of genus \( g \geq 2 \), and let \( G \) be a subgroup of \( \text{Aut}(\mathcal{X}) \) which has no fixed point on \( \mathcal{X} \). Assume that \( G \) has a \( p \)-subgroup \( S \) fixing a point \( P \in \mathcal{X} \) such that (1.4) holds. Then every \( p \)-element of \( \text{Aut}(\mathcal{X}) \) fixes exactly one point. Let \( \Omega \) be the set of all points \( R \in \mathcal{X} \) which are fixed by some element of \( G \) order \( p \). Then one of the following cases occurs:

(A) \( \Omega \) is the unique short orbit of \( G \).

(B) \( G \) has two short orbits, namely \( \Omega \) and a tame \( G \)-orbit.

**Proof.** Since \( S \leq G_{p}^{(1)} \) we have that \( |G_{p}^{(1)}| > gp/(p-1) \). In terms of the action of \( G \) on \( \mathcal{X} \), Theorem 2.2 implies that

(*) no non-trivial \( p \)-element in \( G_{p} \) fixes a point distinct from \( P \).

Since \( P \in \Omega \) and \( G \neq G_{p} \), \( \Omega \) contains at least two points. It may be noted that the 2-point stabilizer of \( G \) is tame and hence cyclic.

As \( G_{p}^{(1)} \) is a \( p \)-group, it is a subgroup of a Sylow \( p \)-subgroup \( S_{p} \) of \( G \). Choose a non-trivial element \( z \) from the centre of \( S_{p} \). Then \( z \) commutes with a non-trivial element \( u \) of \( G_{p}^{(1)} \). From \( uz = zu \), we have

\[
(Pz)^u = P^zu = P^{uz} = (Pu)^z = P^z.
\]

Since \( P \) is the unique fixed point of \( u \), this implies that \( P^z = P \). Therefore, \( z \in G_{p}^{(1)} \).

In particular, \( z \) fixes no point of \( \mathcal{X} \) distinct from \( P \). Let \( g \in S_{p} \). Then \( zg = gz \) implies that

\[
(Pg)^z = Pg^z = P^{gz} = (Pz)^g = Pg,
\]

whence \( Pg = P \). 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 \( \mathcal{X} \). From Gleason’s Lemma, see [3, Theorem 4.14], \( \Omega \) is a \( G \)-orbit, and hence the unique non-tame \( G \)-orbit. Since case (iii) in
Theorem 2.2 holds, the quotient curve $\mathcal{X} = \mathcal{X}/G_p^{(1)}$ is rational. This implies that $\mathcal{Y} = \mathcal{X}/G$ is also rational.

If there are at least two more short $G$-orbits, say $\Omega_1$ and $\Omega_2$, from (2.1),

$$2g - 2 \geq -2|G| + (|G_p| + |G_p^{(1)}| + |G_p^{(2)}| - 3)|\Omega| + (|G_{Q_1}| - 1)|\Omega_1| + (|G_{Q_2}| - 1)|\Omega_2|,$$

where $Q_i \in \Omega_i$ for $i = 1, 2$. Note that

$$|\Omega_i| \geq |G|$$

since $|G_{Q_i}| - 1 \geq \frac{1}{2}|G_{Q_i}|$, and $|G| = |G_{Q_i}| |\Omega_i|$. Also, $|G| = |G_p| |\Omega|$, and $|G_p^{(2)}| > 1$ as (iii) in Theorem 2.2 holds. Therefore,

$$2g - 2 \geq (|G_p^{(1)}| - 1)|\Omega|.$$

Since $|\Omega| \geq 2$, this implies that $g \geq |G_p^{(1)}|$, a contradiction. □

Before investigating the above cases separately, a useful equation is established.

Since $\mathcal{X}_1$ is rational and $G_p^{(1)}$ only ramifies at $P$, from (2.1) and (2.2),

$$(3.1) \quad 2g - 2 + 2|G_p^{(1)}| = 2|G_p^{(1)}| - 2 + |G_p^{(2)}| - 1 + \ldots = d_P - |G_p| + |G_p^{(1)}|,$$

Therefore,

$$(3.2) \quad d_P = 2g - 2 + |G_p^{(1)}| + |G_p|.$$

4. CASE (A) IN THEOREM 3.1

We prove that only one example occurs, namely the DLR curve for $n = 3$.

**Lemma 4.1.** Let $G_p = G_p^{(1)} \times H$ with $p \nmid |H|$. Then $|H| = 2$ and $p \neq 2$.

**Proof.** Let $R \in \Omega \setminus \{P\}$. From (*), the identity is the unique element in $G_p^{(1)}$ fixing $R$. Hence the orbit of $R$ in $G_p^{(1)}$ has size $|G_p^{(1)}|$ and is contained in $\Omega \setminus \{P\}$.

Therefore,

$$|\Omega| \geq |G_p^{(1)}| + 1,$$

whence

$$(4.1) \quad |\Omega| > g - 1$$

by (1.4). On the other hand, since $P \in \Omega$ and $\Omega$ is the unique short orbit of $G$, (2.1) gives

$$(4.2) \quad 2g - 2 = -2|G| + |\Omega|d_P = -2|\Omega||G_p| + |\Omega|d_P = |\Omega|(d_P - 2|G_p|).$$

Hence $|\Omega|$ is a divisor of $2g - 2$. This and (4.1) imply that $|\Omega| = 2g - 2$. Thus $d_P = 2|G_p| + 1$. This and (4.2) give

$$(4.3) \quad 2g - 2 + |G_p^{(1)}| - |G_p| = 1.$$ 

Since $G_p = G_p^{(1)} \times H$, it follows that $2g - 2 = (|H| - 1)|G_p^{(1)}| + 1$. This and (1.4) imply that $|H| = 2$. Since $p$ does not divide $H$, $p \neq 2$ must hold. □

**Lemma 4.2.** $G$ acts on $\Omega$ as a 2-transitive permutation group of degree $2g - 2$.

**Proof.** From the proof of Lemma 4.1, $|G_p^{(1)}| = 2g - 3$. As $|\Omega| = 2g - 2$, this and (*) imply that $G_p^{(1)}$ acts on $\Omega \setminus \{P\}$ as a sharply transitive permutation group. Hence, $|\Omega| = q + 1$ with $q = |G_p^{(1)}|$. Since $\Omega$ is a $G$-orbit, the assertion follows. □
Let \( q \) stand for \( G_p^{(1)} \). With this notation, \( |\Omega| = q + 1 \).

Let \( \bar{G} \) be the 2-transitive permutation group induced by \( G \) on \( \Omega \). As \( |H| = 2 \), the 1-point stabiliser of \( \bar{G} \) has order either \( q \) or \( 2q \), and this occurs according as \( |G| = 2|\bar{G}| \) or \( |G| = 2|\bar{G}| \). In the latter case, \( G \cong \bar{G} \) and we may assume without loss of generality that \( G = \bar{G} \).

**Lemma 4.3.** The case \( |G| = 2|\bar{G}| \) does not occur.

*Proof.* If \( |G| = 2|\bar{G}| \), the subgroup \( H \) is the kernel of the permutation representation of \( G \) on \( \Omega \); that is, \( H \) fixes every point in \( \Omega \). In particular, \( H \) is a normal subgroup of \( G \). Therefore, \( \bar{G} \) can be viewed as a \( K \)-automorphism group of the quotient curve \( Z = X/H \). Let \( g' \) be the genus of \( Z \). Since \( |\Omega| = 2g - 2 \), and \( |H| = 2 \), \( g' \) applied to \( H \) implies that \( g' = 1 \). Let \( P' \) be the point of \( Z \) lying under \( P \). Since \( |G_p^{(1)}| \) is odd, \( G_p^{(1)} \cong \bar{G}_p^{(1)} \). Let \( P' \) be the point of \( Z \) lying under \( P \). Since \( |G_p^{(1)}| \) is odd, \( G_p^{(1)} \cong \bar{G}_p^{(1)} \) holds. As \( p \neq 2 \) and \( g' = 1 \) we have that \( \bar{G}_p^{(1)} = 3 \); see [13] Theorem 11.94. But then \( |G_p^{(1)}| = 3 \), contradicting [14].

As a consequence of Lemma 4.3, \( G = \bar{G} \).

**Lemma 4.4.** \( G \) is not solvable.

*Proof.* Assume that \( G \) is solvable. From Huppert’s classification theorem, \( q + 1 = d^k \) with \( d \) prime. Since \( |\Omega| = 2g - 2 \) is even, so \( d = 2 \). From Huppert’s classification for \( d = 2 \) it also follows that \( G_p \) is a subgroup of the 1-point stabiliser of \( \Delta \), and hence \( |G_p| \) divides \( kq \). On the other hand, \( g' = 2^k \) only occur when \( k \) and \( q \) are both primes. Since \( |G_p| = 2q \), this implies that \( k = 2 \). Hence \( q = g = 3 \); that is, \( p = 3 \) and \( |G_p^{(1)}| = g = 3 \), which contradicts [14].

**Lemma 4.5.** \( X \) is birationally equivalent over \( K \) to the DLR-curve with \( n = 3 \).

*Proof.* From Lemma 4.4, \( G \) is not solvable. If \( G \) has an elementary abelian regular normal subgroup \( M \), then \( G/M \cong G_p \), but this is impossible as \( G_p \) is solvable. Therefore, \( G \) does not have a regular normal subgroup, and we apply the Kantor-O’Nan-Seitz theorem. Since \( |G_p| = 2q \), this shows that either \( |\Omega| = 6 \) and \( G \cong \text{PSL}(2,5) \), or \( |\Omega| = 28 \) and \( G \cong \text{Ree}(3) \). In the former case, \( |G_p^{(1)}| = 5 \) and \( g = 4 \); hence [13] does not hold. In the latter case, \( |G_p^{(1)}| = 27 \) and \( g = 15 \). This is consistent with [13], and \( X \) is the DLR curve with \( n = 3 \). By Lemma 2.3 (V) holds for \( q = n^3 \) with \( n = 3 \).

5. Case (B) in Theorem 3.1

In Case (B), \( G \) has a unique tame orbit, say \( \Delta \), and \( Q \) will always denote a point from \( \Delta \).

Two possibilities arise, namely

(B1) *there is a point \( R \in \Omega \) such that the stabiliser of \( R \) in \( G \) is trivial;*
(B2) *no point \( R \in \Omega \) with the property as in (B1) exists.*

Before investigating (B1) and (B2) separately, we prove a result originally stated in Henn’s paper [12]; see also [13, p. 516]. For this purpose, let \( N = |Q||d_p - |G_p|| - |G_p| \).

**Lemma 5.1.** Let \( G_p = G_p^{(1)} \times H \) with \( p \nmid |H| \). Then

\[
|G| = 2(g - 1) \frac{|G_p^{(1)}||H||G_Q|}{N}.
\]
Proof. Since $\Omega$ and $\Delta$ are the unique short orbits of $G$ and $P \in \Omega$, $Q \in \Delta$, (2.1) gives
\[ 2g - 2 = -2|G| + d_P|\Omega| + d_Q|\Delta| = -2|G| + d_P\frac{|G|}{|G_P|} + |G| - \frac{|G|}{|G_Q|}, \]
whence the assertion follows. \hfill \Box

5.1. Case (B1). We prove that no example exists.

Lemma 5.2. Case (B1) does not occur.

Proof. Assume on the contrary that there exists a point $R \in \Omega$ such that the orbit $\sigma'(R)$ of $R$ under $G_P$ is long. Since $P$ and $R$ lie in the same orbit $\Omega$ of $G$, so $G_R \cong G_P$ and $|G| = |\Omega| \cdot |G_R|$. Also, $\sigma'(R)$ is contained in $\Omega$. This, together with Lemma 5.1 gives
\begin{equation}
|G_P| = |G_R| = \frac{|G|}{|\Omega|} \leq \frac{|G|}{|\sigma'(R)|} = \frac{|G|}{|G_P|} = 2(g - 1) \cdot \frac{|G_Q|}{N} \leq 2(g - 1)|G_Q|.
\end{equation}

Now, a lower bound on $N$ is given. As
\[ N \geq d_P|G_Q| - |G_P||G_Q| - 2(g - 1)|G_Q|, \]
so
\begin{equation}
N \geq |G_Q|(d_P - |G_P| - 2(g - 1)).
\end{equation}
This and (5.2) imply that $N \geq |G_P^{(1)}||G_Q|$. From (5.1),
\[ N \leq 2(g - 1)|G_Q|/|G_P|. \]

Hence $|G_P||G_P^{(1)}| \leq 2(g - 1)$. Since $|G_P| > 1$, this contradicts (1.4). \hfill \Box

5.2. Case (B2). We prove that $X$ is birationally equivalent over $\mathbb{K}$ to one of the curves (II),(III),(IV) and (V) for $n > 3$. First the possible structure of $G$ and its action on $\Omega$ are investigated.

Proposition 5.3. $G$ acts on $\Omega$ as a 2-transitive permutation group. In particular, $|\Omega| = q + 1$ with $q = p^t$, $t \geq 1$, and the possibilities for the permutation group $G$ induced by $G$ on $\Omega$ are as follows:
\begin{enumerate}
\item[(1a)] $G \cong \text{PGL}(2, q)$, $q \geq 4$;
\item[(1b)] $G \cong \text{PSL}(2, q)$, $q$ odd, $q > 4$;
\item[(2a)] $G \cong \text{PSU}(3, n)$, with $q = n^3$, $n \geq 3$;
\item[(2b)] $G \cong \text{PGU}(3, n)$, with $\gcd(3, n + 1) > 1$, $q = n^3$, $n \geq 3$;
\item[(3)] $G \cong \text{Sz}(n)$, with $p = 2$, $n = 2n_0^2$, $n_0 = 2^r$, $r \geq 1$ and $q = n^2$;
\item[(4)] $G \cong \text{Rec}(n)$ with $p = 3$, $n = 3n_0^2$, $n_0 = 3^r$, $r \geq 0$ and $q = n^3$;
\item[(5)] $G$ has an elementary abelian regular normal subgroup and the size of $\Omega$ is a prime power.
\end{enumerate}

In each of the first six cases, $G$ acts with its natural 2-transitive permutation representation.

Proof. For a point $P \in \Omega$, let $\Omega_0 = \{P\}$, $\Omega_1, \ldots, \Omega_k$ with $k \geq 1$ denote the orbits of $G_P^{(1)}$ contained in $\Omega$. Then, $\Omega = \bigcup_{i=0}^k \Omega_i$. To prove that $G$ acts 2-transitively on $\Omega$, it suffices to show that $k = 1$.

For any $i$ with $1 \leq i \leq k$, 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 $|G_P| = |G_P^{(1)}||H|$
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 $\alpha$. Note that $\alpha$ preserves $\Omega_i$ as $G_P^{(i)}$ is a normal subgroup of $G_P$.

Since the quotient curve $X_1 = \mathcal{X}/G_P^{(1)}$ is rational, $\alpha$ viewed as an automorphism of $X_1$ has at most two fixed points on $X_1$; see [13 Theorem 11.14]. Hence, $\alpha$ fixes at most two orbits of $G_P^{(1)}$. Therefore, $\Omega_0$ and $\Omega_i$ are the orbits preserved by $\alpha$. As $H'$ is abelian and $\alpha \in H'$, this yields that $H'$ either preserves both $\Omega_0$ and $\Omega_i$ or interchanges them. The latter case cannot actually occur as $H'$ preserves $\Omega_0$. So, the orbits $\Omega_0$ and $\Omega_i$ are also the only orbits of $G_P^{(1)}$ which are fixed by $H'$. Since $G_P = G_P^{(1)} \rtimes H'$, this implies that the whole group $G_P$ fixes $\Omega_i$. As $i$ can be any integer between 1 and $k$, it follows that $G_P$ fixes each of the orbits $\Omega_0, \Omega_1, \ldots, \Omega_k$. Hence, either $k = 1$ or $G_P$ preserves at least three orbits of $G_P^{(1)}$. The latter case cannot actually occur, as the quotient curve $X_1 = \mathcal{X}/G_P^{(1)}$ is rational.

Therefore $k = 1$. Also, the size of $\Omega$ is of the form $q + 1$ with $q = |G_P^{(1)}|$; in particular, $q$ is a power of $p$.

Let $\bar{G}$ denote the 2-transitive permutation group induced by $G$ on $\Omega$. We apply the Kantor-O’Nan-Seitz theorem to $\bar{G}$. Up to isomorphism, $\bar{G}$ is one of the groups on the list, with $\bar{G}$ acting as in its natural 2-transitive permutation representation.

\[ \square \]

**Lemma 5.4.** The subgroups $G_P$ and $G_Q$ have trivial intersection, and $G_Q$ is a cyclic group whose order divides $q + 1$. Also,

\[ (5.3) \quad 2g - 2 = \frac{|G|(|G_P| - |G_P^{(1)}| |G_Q|)}{|G_Q||G - G_P|}. \]

**Proof.** Let $\alpha \in G_P \cap G_Q$ be non-trivial. As $G_P^{(1)}$ is normal in $G_P$, $\alpha$ belongs to the normalizer of $G_P^{(1)}$ in $G$. Also, $\alpha$ fixes three orbits under the action of $G_P^{(1)}$, namely $\{P\}, \Omega \setminus \{P\}$ and the orbit containing $Q$. Since the quotient curve $X_1 = \mathcal{X}/G_P^{(1)}$ is rational, this implies that $\alpha$ fixes every orbit of $G_P^{(1)}$, a contradiction. Hence $|G_P \cap G_Q| = 1$. Therefore, no non-trivial element of $G_Q$ fixes a point in $\Omega$. Since $|\Omega| = q + 1$, the second assertion follows. Substituting $d_P$ from (3.2) into the equation of Lemma 5.1 gives (5.3).

First the case when the action of $G$ is faithful on $\Omega$ is considered.

**Lemma 5.5.** If $G$ acts faithfully on $\Omega$, then case (1a) in Proposition 5.3 does not occur.

**Proof.** For $G \cong \operatorname{PGL}(2, q)$,

\[ |G| = q^3 - q, \quad |G_P| = q^2 - q, \quad |G_P^{(1)}| = q. \]

Since case (iii) in Theorem 2.2 holds, the second ramification group $G_P^{(2)}$ is non-trivial. As $G \cong \operatorname{PGL}(2, q)$, $G_P$ has a unique conjugacy class of elements of order $p$. Since $G_P^{(i)}$ is a normal subgroup of $G_P$, if $g \in G_P^{(i)}$ with $i \geq 1$, then every conjugate
of \( g \) in \( G \) also belongs to \( G_p^{(i)} \). Therefore,
\[
G_p^{(1)} = G_p^{(2)} = \ldots = G_p^{(k)}, \quad |G_p^{(k)}| = 1.
\]
Since the quotient curve \( X_1 = X/G_p^{(1)} \) is rational, from (2.2),
\[
2g = (q - 1)(k - 1).
\]
By (1.4), this is only possible for \( k = 2 \). Therefore \( g = \frac{1}{2}(q - 1) \) with \( q \geq 5 \) odd, and \( |G_Q| = \frac{1}{2}(q + 1) \) follows by (5.3).

For the rest of the proof, some elementary facts on the involutions of \( \text{PGL}(2, q) \) are useful; for the proofs, the reader is referred to [6, Prop. 2.3].

Let \( q \equiv 1 \pmod{4} \). Then \( 2g - 2 \equiv 2 \pmod{4} \), and an involutory element in \( \text{PGL}(2, q) \setminus \text{PSL}(2, q) \) has no fixed point on \( \Omega \). Since \( G_Q \) has odd order, such an involutory element in \( \text{PGL}(2, q) \setminus \text{PSL}(2, q) \) has no fixed point in \( \Delta \), either. Therefore, an involutory element in \( \text{PGL}(2, q) \setminus \text{PSL}(2, q) \) fixes no point of \( \mathcal{X} \). From (2.3) applied to such an involutory element, \( 2g - 2 \equiv 0 \pmod{4} \), a contradiction.

Let \( q \equiv 3 \pmod{4} \). Then \( 2g - 2 \equiv 0 \pmod{4} \) and an involutory element in \( \text{PGL}(2, q) \setminus \text{PSL}(2, q) \) has exactly two fixed points in \( \Omega \). Lemma 5.5 implies that such an involutory element has no fixed point in \( \Delta \). Therefore, an involutory element in \( \text{PGL}(2, q) \setminus \text{PSL}(2, q) \) fixes exactly two points of \( \mathcal{X} \). From (2.3) applied to such an involutory element, \( 2g - 2 \equiv 2 \pmod{4} \), a contradiction. This completes the proof. \( \square \)

**Lemma 5.6.** If \( G \) acts faithfully on \( \Omega \), then case (1b) in Proposition 2.3 does not occur.

**Proof.** For \( G \cong \text{PSL}(2, q) \),
\[
|G| = \frac{1}{2}(q^3 - q), \quad |G_p| = \frac{1}{2}(q^2 - q), \quad |G_p^{(1)}| = q.
\]
The argument of Lemma 5.5 depending on the higher ramification groups at \( P \) still works as \( G_p \) has two conjugacy classes of elements of order \( p \), and each of them generates \( G_p^{(1)} \); see [6, Prop. 2.4]. Therefore, \( k = 2 \) and hence \( g = \frac{1}{2}(q - 1) \). But to show that this case cannot actually occur, more is needed. From (5.3), \( |G_Q| = \frac{1}{4}(q + 1) \); in particular, \( q \equiv 3 \pmod{4} \). We first show that \( \mathcal{X} \) is not hyperelliptic. This depends on the fact that the automorphism group of a hyperelliptic curve contains a central involution, say \( \alpha \); see [13, Theorem 11.98]. Since \( \alpha \) commutes with every \( p \)-element of \( G \), from (*) it follows that \( \alpha \) must fix \( \Omega \) pointwise. In particular, \( \alpha \not\in G \). This shows that the subgroup \( U \) generated by \( G \) and \( \alpha \) also falls in case (B2). From (5.3) applied to \( U \), \( |U_Q| = \frac{1}{2}(q + 1) \). Since no generator of \( U_Q \) belongs to \( G_Q \), there exists \( \beta \in G \) such that \( \alpha \beta \) is a generator of \( U_Q \). Then \( \beta^2 \) fixes \( Q \), as \( \beta^2 = (\alpha \beta)^2 \in U_Q \).

The groups \( G_Q \) and \( \langle \beta \rangle \) share a non-trivial element. By Lemma 2.5, this yields \( \beta \in G_Q \). Since \( |U_Q| = \frac{1}{2}(q + 1) \), \( (\alpha \beta)^{(q+1)/4} \) has order 2. As
\[
(\alpha \beta)^{(q+1)/4} = \alpha^{(q+1)/4} \beta^{(q+1)/4} = \alpha^{(q+1)/4},
\]
this yields \( \frac{1}{2}(q + 1) \) is odd and hence \( \alpha = (\alpha \beta)^{(q+1)/4} \). Then \( \alpha \in U_Q \); that is, \( \alpha \) must fix \( Q \). But this contradicts Lemma 5.4.

Therefore, \( \mathcal{X} \) is not hyperelliptic. So, \( \mathcal{X} \) may be assumed to be the canonical curve of \( \mathbb{K}(\mathcal{X}) \) embedded in \( \text{PG}(g - 1, \mathbb{K}) \). Then \( G \) is isomorphic to a linear collineation group \( \Gamma \) of \( \text{PG}(g - 1, \mathbb{K}) \) preserving \( \mathcal{X} \) such that the restriction of the
action of $\Gamma$ on $\mathcal{X}$ is $G$. To simplify notation, the symbol $G$ is used to indicate $\Gamma$, too. We need the following results.

(R1) $j_{g-1}(P) = 2g - 2$.
(R2) Let $H_{g-2}$ be a hyperplane of $\text{PG}(g-1, \mathbb{K})$ such that

$$I(P, \mathcal{X} \cap H_{g-2}) = j_{g-2}(P).$$

If $H_{g-2}$ contains a point $R \in \Omega$ distinct from $P$, then $P$ and $R$ are the only common points of $\mathcal{X}$ and $H_{g-2}$, and hence

$$I(R, \mathcal{X} \cap H_{g-2}) = 2g - 2 - j_{g-2}(P).$$

To show (R1) assume on the contrary that the osculating hyperplane $H_{g-1}$ to $\mathcal{X}$ at $P$ contains a point $S \in \mathcal{X}$ distinct from $P$. Since $G_{(1)}^P$ preserves $H_{g-1}$, the $G_{(1)}^P$-orbit of $S$ lies in $H_{g-1}$. Since such a $G_{(1)}^P$-orbit is long, this implies that $H_{g-1}$ contains from $\mathcal{X}$ at least $q$ points other than $P$. Hence, $\deg \mathcal{X} \geq j_{g-1}(P) + q$. On the other hand, $j_{g-1}(P) \geq g - 1$. Therefore,

$$\deg \mathcal{X} \geq g - 1 + q > g - 1 + pg/(p - 1) > 2g - 2,$$

contradicting $\deg \mathcal{X} = 2g - 2$.

A similar argument may be used to show (R2). Again, assume on the contrary that $H_{g-2}$ contains a point $T \in \mathcal{X}$ other than $P$ and $R$. As $H_{g-1}$ does not contain $R$, $H_{g-2}$ is the unique hyperplane through $R$ whose intersection number with $\mathcal{X}$ at $P$ is $j_{g-2}(P)$. In particular, the stabiliser $F$ of $R$ in $G_P$ preserves $H_{g-2}$. Since $|F| = \frac{1}{2}(q - 1)$ and the $F$-orbit of $T$ is long, $H_{g-2}$ contains from $\mathcal{X}$ at least $\frac{1}{2}(q - 1)$ points other than $P$ and $R$. On the other hand, $j_{g-2}(P) \geq g - 2$. Therefore,

$$2g - 2 = \deg \mathcal{X} \geq g - 2 + 1 + \frac{1}{2}(q - 1),$$

whence $g \geq \frac{1}{2}(q + 1)$, a contradiction which proves (R2).

Since $\Omega$ is a $G_{(1)}^P$-orbit, (R2) shows that for every $R \in \Omega \setminus \{P\}$ there exists a hyperplane $H_{g-2}(R)$ such that

$$I(P, \mathcal{X} \cap H_{g-2}(R)) = j_{g-2}(P), \quad I(R, \mathcal{X} \cap H_{g-2}(R)) = n = 2g - 2 - j_{g-2}(P).$$

Since such hyperplanes are distinct for distinct points $R$, from (2.6) it follows that $2g - 2 \geq -(n + 1) + q(n - 1)$. By $g = \frac{1}{2}(q - 1)$, this yields that $n = 2$. But then $\mathcal{X}$ would be hyperelliptic, a contradiction. This completes the proof of Lemma 5.6.

**Lemma 5.7.** If $G$ acts faithfully on $\Omega$ and case (2a) of Proposition 5.3 holds, then $\mathcal{X}$ is isomorphic over $\mathbb{K}$ to the irreducible plane curve (III).

**Proof.** For $G \cong \text{PSU}(3, n)$,

$$|G| = (n^3 + 1)n^3(n^2 - 1)/\mu, \quad |G_P| = n^3(n^2 - 1)/\mu, \quad |G_{(1)}^P| = n^3,$$

where $\mu = \gcd(3, n + 1)$. By (5.3),

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

By Lemmas 5.4 and 2.6(i), two possibilities for $|G_Q|$ occur.
Assume that $|G_Q|$ divides $n + 1$. If $n$ is odd, then the order of $G_Q$ must be odd as every involutory element in $G$ has a fixed point in $\Omega$. In particular, $|G_Q| \leq \frac{1}{2} (n + 1)$. Then

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

But this is not consistent with (1.4). If $n$ is even, then (1.4) reads $n^3 > 2g$, and hence

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

giving $|G_Q| > (n^2 - 1)/(2\mu)$. Comparing this to $|G_Q| \leq n + 1$ implies that $n = 2$, $|G_Q| = 3$. For these values, $g$ is not positive, a contradiction.

So, we may assume that $|G_Q|$ divides $(n^2 - n + 1)/\mu$. Then there is a divisor $t \geq 1$ of $(n^2 - n + 1)/\mu$ such that $|G_Q| = (n^2 - n + 1)/(4\mu)$. Hence

$$2g = (n - 1)(t(n + 1)^2 - (n^2 + n + 1)).$$

Since $t$ is odd, this and (1.4) imply that $t = 1$. Then $g = \frac{1}{2} n(n - 1)$. By Lemma 2.3, $\mathcal{X}$ is isomorphic over $k$ to the irreducible plane curve (III). \hfill $\square$

Lemma 5.8. If $G$ acts faithfully on $\Omega$ and case (2b) of Proposition 5.3 holds, then $\mathcal{X}$ is isomorphic over $k$ to the irreducible plane curve (III).

Proof. Since in this case $PSU(3, n)$ is a subgroup of $G \cong PGU(3, n)$ of index 3, the argument of Lemma 5.7 works here as well. \hfill $\square$

Lemma 5.9. If $G$ acts faithfully on $\Omega$ and case (3) in Proposition 5.3 holds, then $\mathcal{X}$ is birationally equivalent over $k$ to the irreducible plane curve (IV).

Proof. For $G \cong Sz(n)$,

$$|G| = (n^2 + 1)n^2(n - 1), \quad |G_P| = n^2(n - 1), \quad |G_P^{(1)}| = n^2.$$ 

From (5.3),

$$2g = \frac{(n + 2n_0 + 1)(n - 2n_0 + 1)(n - 1)}{|G_Q|} - (n^2 - 1).$$

By Lemma 2.6(ii), there is an odd integer $t$ such that either (a) or (b) holds, where

(a) $2g = (t - 1)(n - 1) - 2tn_0(n - 1), \quad |G_Q| = (n + 2n_0 + 1)/t$;

(b) $2g = (t - 1)(n^2 - 1) + 2tn_0(n - 1), \quad |G_Q| = (n - 2n_0 + 1)/t$.

In case (a), $t \geq 3$ is odd and $n_0 > 2$. But then (1.4) does not hold. In case (b), (1.4) implies that $t = 1$. Then $g = n_0(n - 1)$. By Lemma 2.3, $\mathcal{X}$ is birationally equivalent over $k$ to the irreducible plane curve (IV). \hfill $\square$

Lemma 5.10. If $G$ acts faithfully on $\Omega$, and case (4) of Proposition 5.3 holds, then $\mathcal{X}$ is birationally equivalent over $k$ to the irreducible plane curve (V) with $n > 3$.

Proof. For $G \cong Ree(n)$,

$$|G| = (n^3 + 1)n^3(n - 1), \quad |G_P| = n^3(n - 1), \quad |G_P^{(1)}| = n^3.$$ 

By (5.3), $|G_P| > |G_P^{(1)}| \cdot |G_Q|$, and hence for $n = 3$ this reads $|G_Q| < 2$, a contradiction. So $n > 3$. Again by (5.3),

$$2g = \frac{(n^3 + 1)(n + 1)}{|G_Q|} - (n^3 - 1).$$
Again the argument of Lemma 5.9 based on (1.4) and Lemmas 2.6 and 5.4 works, showing this time the existence of an integer \( t \geq 1 \) such that either (a) or (b), or (c) holds, where

\[
\begin{align*}
(a) \quad 2g &= (n - 1)[(t - 1)(n^2 + 1) - (t + 1)n], \quad |G_Q| = (n + 1)/t; \\
(b) \quad 2g &= (n - 1)[(t - 1)n^2 - 3tn_0 + n(2t - 1) - 3tn_0 + t - 1], \quad |G_Q| = (n + 3n_0 + 1)/t; \\
(c) \quad 2g &= (n - 1)[(t - 1)n^2 + 3tn_0 + n(2t - 1) + 3tn_0 + t - 1], \quad |G_Q| = (n - 3n_0 + 1)/t.
\end{align*}
\]

In case (a), (1.4) yields \( t = 2 \). Then \( |G_Q| = \frac{1}{2}(n + 1) \); hence \( |G_Q| \) is even. But this is impossible as every involution in \( \text{Ree}(n) \) has a fixed point in \( \Omega \). If case (b) occurs, then \( t \geq 2 \). Since \( t \) is odd and \( t \neq 3 \), \( t \) must be at least 5. But then (1.4) does not hold.

If case (c) holds for \( t = 1 \), then (c) reads \( 2g = 3n_0(n - 1)(n + n_0 + 1) \), and from Lemma 2.6 it follows that \( X \) is birationally equivalent over \( \mathbb{K} \) to the irreducible plane curve \( (V) \). Otherwise, \( t \geq 5 \), contradicting (1.4).

**Lemma 5.11.** If \( G \) acts faithfully on \( \Omega \), then case (5) in Proposition 5.3 does not occur.

**Proof.** In this case, \( G \) is a solvable 2-transitive group on \( \Omega \). In fact, \( G = G_P \rtimes M \)
the semidirect product of \( M \) by \( G_P \), where \( M \) is the elementary abelian regular normal subgroup on \( \Omega \), and both \( G_P \) and \( N \) are solvable. Furthermore, \( |\Omega| = |M| \)
is a power of a prime \( w \). Therefore, \( q + 1 = w^k \). Also, \( G \) is not sharply 2-transitive on \( \Omega \) as condition (B2) holds.

The diophantine equation \( q + 1 = w^k \) has solutions only in three cases; see [21]:

\[
\begin{align*}
(x) \quad q &= 2^m, \quad k = 1, \text{ that is, } w \text{ is a Mersenne prime; } \\
(xx) \quad w &= 2, \quad q = p \text{ and } k \text{ prime; } \\
(xxx) \quad q &= 8, \quad w = 3, \quad k = 2.
\end{align*}
\]

By Huppert’s classification, if (x) holds, then \( G \) must be sharply 2-transitive on \( \Omega \). So, case (x) does not occur.

In case (xx), \( p \) is prime, and [21] applied to \( G_P^{(1)} \) reads \( 2g - 2 = -2p + \lambda(p - 1) \) with a positive integer \( \lambda \). Since \( g \geq 2 \), \( \lambda \geq 3 \) holds. By (1.4), this implies that \( \lambda = 3 \). Therefore \( g = \frac{1}{2}(p - 1) \). In particular, \( p > 3 \). As PSL(2, \( p \)) is simple for \( p > 3 \), from Roquette’s theorem [25], see also [13] p. 545, we have that \( |G| \leq 84(g - 1) = 42(p - 3) \). On the other hand, since \( k \) is prime and \( G \) is not sharply 2-transitive on \( \Omega \), Huppert’s classification yields \( |G| = (p + 1)pk \). Hence, \( 2^kpk \leq 42(p - 3) \), which leaves only one case, namely \( q = p = 7, \quad g = 3, \quad G \cong \text{ATL}(1, 8) \). By (5.3), \( |G_Q| = 2 \). In particular, the tame orbit \( \Delta \) of \( G \) has size 84. Since \( G \) has exactly seven involutory elements and they are pairwise conjugate under \( G \), an involutory element \( \alpha \in G \) has exactly 12 fixed points on \( \Delta \). But then [21] applied to \( \alpha \) gives \( 4 \geq -2 + 12 \), a contradiction.

In case (xxx), we have \( q + 1 = 9 \), so Huppert’s classification does not apply. Since in our case \( G \) has an elementary abelian regular normal subgroup \( M \) of order 9, we may find \( G \) as a subgroup of the normalizer \( N(M) \) of \( M \) in the symmetric group \( \text{Sym}(9) \) on \( \Omega \). Since \( N(M) \) has order 432, this number is divisible by \( |G| \). On the other hand, since \( G \) is 2-transitive (but not sharply 2-transitive) on \( \Omega \), \( |G_P^{(1)}| = 8k \) with \( k > 1 \). Here \( k \neq 2 \), since \( |G_P^{(1)}| = 8 \). Therefore, \( k = 3 \), and \( |G| = 216 = 27 \cdot 8 \).
Furthermore, either $|G_Q| = 9$ or $|G_Q| = 3$. Taking (5.3) into account, the former case is impossible while the latter gives $g = 1$. This completes the proof. \hfill $\square$

It remains to investigate the possibility that the permutation representation $\bar{G}$ of $G$ on $\Omega$ has a non-trivial kernel.

**Lemma 5.12.** If $G$ does not act faithfully on $\Omega$, then $\chi$ is birationally equivalent over $\mathbb{K}$ to the irreducible plane curve (II).

**Proof.** The kernel $T$ of the action of $G$ on $\Omega$ is a cyclic normal subgroup of $G$ whose order is relatively prime to $p$. By Lemma 5.4, no point outside $\Omega$ is fixed by a non-trivial element in $T$. Let $\tilde{\gamma}$ be the genus of the quotient curve $\mathcal{Y} = \chi/T$. From (II) applied to $T$, 

$$2g - 2 = |T|(2\tilde{\gamma} - 2) + (|T| - 1)(q + 1).$$

By (1.4), this implies that either $|T| = 2$, or $|T| = 3$ and $\tilde{\gamma} = 0$.

Suppose first that $|T| = 2$, $\tilde{\gamma} = 0$. Then, $\chi$ is hyperelliptic of genus $g = 1/2(q - 1)$ and $\mathcal{Y}$ may be assumed to be the projective line $\mathcal{L}$ over $\mathbb{K}$. Let $\Omega'$ be the set of all points of $\mathcal{L}$ which lie under the points of $\Omega$. Then $|\Omega'| = |\Omega|$ and $\bar{G}$ acts on $\Omega'$ and $\Omega$ in the same way. So, $\bar{G}$ may be viewed as a subgroup of $PGL(1, \mathbb{K})$ acting on a subset $\Omega'$ of $\mathcal{L}$. This shows that no non-trivial element of $\bar{G}$ fixes three distinct points; that is, $\bar{G}$ is a Zassenhaus group.

In case (5) of Proposition 5.3, $G$ is solvable. In fact, $\bar{G} = \bar{G}_P \ltimes \tilde{M}$, where $\tilde{M}$ is the elementary abelian regular normal subgroup $\tilde{G}$, and $G_P = G_P/T$ is solvable, as both $G_P$ and $T$ are solvable. Let $|\tilde{M}| = |\Omega| = w^k$; that is, $q + 1 = w^k$, where $w$ is a prime. Since $|T| = 2$, arguing as in the proof of Lemma 5.11, the case (xx) can only occur; that is, $q = p$ and $k$ is prime. Furthermore, $g = 1/2(p - 1)$. From Roquette's theorem [25], see also [13, p. 545], $|G| < 84(g - 1) = 42(p - 3)$. On the other hand, $2(p + 1)p$ divides $|G|$ as $\bar{G}$ is 2-transitive on $\Omega$. This together with $p + 1 = 2k$ leaves only one possibility, namely $p = 7$, $k = 3$, $g = 3$, $|\tilde{M}| = 112$ and $\bar{G}$ is sharply 2-transitive on $\Omega$. In particular, $|G_P| = 14$, $|G_P^{(1)}| = 7$. But this is inconsistent with 5.3.

If $\bar{G}$ has no elementary abelian regular normal subgroup, from the classification of Zassenhaus groups, $\bar{G}$ contains a subgroup isomorphic to $PSL(2, q)$ acting on $\Omega'$ as $PSL(2, q)$ in its natural 2-transitive representations. By [13, Proposition 101], $\chi$ is birationally equivalent over $\mathbb{K}$ to the irreducible plane curve (II). In particular, $Z(G) = T$ and the covering $G$ of $PSL(2, q)$ is proper.

Suppose next that $|T| = 2$ and $\tilde{\gamma} = 1$. Since $G_P^{(1)}$ may be viewed as a subgroup of $Aut(\mathcal{Y})$ of the elliptic curve $\mathcal{Y} = \chi/T$, the order of $G_P^{(1)}$ does not exceed 24; see [13, Theorem 11.94]. Thus, $q$ is one of the integers 2, 3, 4, 8. This leaves just one case, namely $q = p = g = 3$, but then (1.4) fails.

Suppose now that $|T| = 2$, $\tilde{\gamma} \geq 2$. Then (1.4) holds for $\mathcal{Y} = \chi/T$ with $\bar{G}$ acting faithfully on $\Omega$. Therefore, Proposition 5.3 holds true for $\mathcal{Y}$ and $\bar{G}$. So we may apply Lemmas 5.5, 5.6, 5.7, 5.10 and 5.11. It turns out that either $\tilde{G}$ contains a subgroup $\tilde{G}^* \cong PSU(3, n)$ of index $\mu = \gcd(3, n + 1)$, or $\tilde{G} \cong \text{Ree}(n)$ with $n > 3$.

In the former case, let $G^*$ be the subgroup of $G$ containing $T$ for which $G^*/T = \tilde{G}^*$. Since $|T| = 2$ and $T$ is a normal subgroup of $G^*$, we have that $T \subset Z(G^*)$. On the other hand, if $z \in Z(G^*)$, then $z$ fixes $\Omega$ point-wise, and hence $z \in T$. Thus $T = Z(G^*)$. From Lemma 2.7, $G^* = T \times U$ with $U \cong PSU(3, n)$. Also, $U$ acts on $\Omega$ as $PSU(3, n)$ in its natural 2-transitive permutation representation. Since the
1-point stabiliser $U_p$ of $U$ contains a non-trivial cyclic 2-subgroup $V$, it turns out that the subgroup $W$ of $G$ generated by $V$ and $T$ must be a non-cyclic 2-subgroup fixing $P$. But this contradicts the fact that $W$ is a tame subgroup of $X$ fixing a point on $X$.

In the latter case, the same argument works, the only difference being $G^* = T \times U$ with $U \cong \text{Ree}(n)$.

Finally, suppose that $|T| = 3$, $g = 0$. Then $g = q - 1$. This together with (1.3) implies that $p > q$, a contradiction. 

Acknowledgements

The authors are grateful to the anonymous referee for a careful reading of the paper and valuable comments and remarks.

References

18. 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. MR0357561 (50:10029)
20. M. Matignon and M. Rocher, Smooth curves having a large automorphism $p$-group in characteristic $p > 0$, Algebra Number Theory 2 (2008), 887-926. MR2457356


DIPARTIMENTO DI MATematica E INFORMatica, Università deglI studi di perugia, Via Vanvitelli, 1, 06123 PERUGIA, ITALY

E-mail address: giuliet@dipmat.unipg.it

DIPARTIMENTO DI Matematica, Università della Basilicata, contrada Macchia Ro-

mana, 85100 Potenza, Italy

E-mail address: gabor.korchmaros@unibas.it