Journal of Algebra 566 (2021) 374–404

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Curves with more than one inner Galois point

Gábor Korchmáros, Stefano Lia, Marco Timpanella *

Dipartimento di Matematica, Informatica ed Economia, Università degli Studi della Basilicata, Contrada Macchia Romana, 85100 Potenza, Italy

A R T I C L E   I N F O

Article history:
Received 15 March 2019
Available online 15 September 2020
Communicated by Gunter Malle

MSC:
14H37
14H05

Keywords:
Algebraic curves
Algebraic function fields
Positive characteristic
Automorphism groups

A B S T R A C T

Let $\mathcal{C}$ be an irreducible plane curve of $\mathrm{PG}(2, \mathbb{K})$ where $\mathbb{K}$ is an algebraically closed field of characteristic $p \geq 0$. A point $Q \in \mathcal{C}$ is an inner Galois point for $\mathcal{C}$ if the projection π_Q from Q is Galois. Assume that $\mathcal{C}$ has two different inner Galois points Q_1 and Q_2, both simple. Let G_1 and G_2 be the respective Galois groups. Under the assumption that G_i fixes Q_i, for $i = 1, 2$, we provide a complete classification of $G = \langle G_1, G_2 \rangle$ and we exhibit a curve for each such G. Our proof relies on deeper results from group theory.

1. Introduction

In this paper, $\mathcal{X}$ stands for a (projective, geometrically irreducible, non-singular) algebraic curve defined over an algebraically closed field $\mathbb{K}$ of characteristic $p \geq 0$. Also, $\mathcal{C}$ stands for a plane model of $\mathcal{X}$, that is, for a plane curve $\mathcal{C}$ defined over $\mathbb{K}$ and birationally equivalent to $\mathcal{X}$. Let φ be a morphism $\mathcal{X} \mapsto \mathrm{PG}(2, \mathbb{K})$ which realizes it, so that φ is birational onto its image $\mathcal{C}$. Further, $\mathbb{K}(\mathcal{X})$ denotes the function field of $\mathcal{X}$, and $\mathrm{Aut}(\mathcal{X})$ stands for the automorphism group of $\mathcal{X}$ which fixes $\mathbb{K}$ element-wise. A point Q in

* Corresponding author.
E-mail addresses: gabor.korchmaros@unibas.it (G. Korchmáros), stefano.lia@unibas.it (S. Lia), marco.timpanella@unibas.it (M. Timpanella).

https://doi.org/10.1016/j.jalgebra.2020.08.024
0021-8693/

$PG(2, \mathbb{K})$ is a *Galois point* for $\mathcal{C}$ if the projection π_Q from Q is Galois; more precisely, if the field extension $\mathbb{K}(\mathcal{X})/\pi_Q^*(\mathbb{K}(\mathrm{PG}(1, \mathbb{K}))$ is Galois. In this case, if G is the Galois group which realizes π_Q, then Q *is a Galois point with Galois group* G. A Galois point Q is either *inner* or *outer* according as $Q \in \mathcal{C}$ or $Q \in PG(2, \mathbb{K}) \setminus \mathcal{C}$. An inner Galois point may be a singular point of $\mathcal{C}$.

The concept of a Galois point is due to H. Yoshihara and dates back to late 1990s; see [36]. Ever since, several papers have been dedicated to studies on Galois points, especially on the number of Galois points of a given plane curve. For non-singular plane curves, that number is already known [3,36]. Nevertheless, for plane models with singularities the picture is much more involved, as it emerges from several recent papers [3–6,9,11,14, 21,25,37] where the authors focused on the problem of determining plane curves with at least two Galois points.

In this context, our paper is about plane models $\mathcal{C}$ of $\mathcal{X}$ with two different inner Galois points $\varphi(P_1)$ and $\varphi(P_2)$ both simple, or more generally unibranch. Here $\mathcal{C}$ is *unibranch* at its point Q if $\varphi(P) = \varphi(R) = Q$ implies $P = R$.

Let $\varphi(P_1), \varphi(P_2) \in \mathcal{C}$ be two different inner Galois points with Galois groups G_1 and G_2 respectively. Then

(I) The quotient curves $\mathcal{X}/G_1$ and $\mathcal{X}/G_2$ are rational.

From now on we assume that G_i fixes P_i, for $i = 1, 2$. By Lemma 2.14 (see also [5]), $\varphi(P_1)$ and $\varphi(P_2)$ are simple if the following two properties hold.

(II) G_1 and G_2 have trivial intersection.
(III) In the divisor group of $\mathcal{X}$, $P_1 + \sum_{\sigma \in G_1} \sigma(P_2) = P_2 + \sum_{\tau \in G_2} \tau(P_1)$.

Since (I), (II), (III) are independent of the model $\mathcal{C}$, general properties of inner Galois points can be obtained by investigating curves $\mathcal{X}$ with two subgroups G_1, G_2 of $\mathrm{Aut}(\mathcal{X})$ satisfying (I), (II), (III) and such that $|\Omega| > 2$, where Ω is the support of the divisor in (III). In this paper we go in that direction pursuing the strategy of using not only function field theory but also deeper results from group theory. Our starting point is to look inside the action of $G = \langle G_1, G_2 \rangle$ on Ω. Lemma 2.14 shows that the action of G_i on $\Omega \setminus \{P_i\}$ is sharply transitive, and hence G induces on Ω a doubly transitively permutation group. Furthermore, a 1-point stabilizer of G is solvable. It should be noticed that some non-trivial element of G may fix Ω pointwise. In other words, the kernel K of the permutation representation $\bar{G}$ of G on Ω may be non-trivial so that $\bar{G} = G/K$ is the doubly transitive permutation group induced by G on Ω. Since all doubly transitive permutation groups with solvable 1-point stabilizer have been classified in 1970's by Holt [20] and O'Nan [27], this gives a chance to determine the possibilities for $\bar{G}$ and then recover G from $\bar{G}$ using Schur multipliers. In this strategy, an important simplification is that G_1 is a normal subgroup of the stabilizer of P_1 in G. Also, a natural idea is to regard G as a doubly transitive group space on Ω where G_1 is a normal subgroup of a

1-point stabilizer of G and G_1 is sharply transitive on the remaining points of Ω. Such doubly transitive group spaces were completely determined by Hering [18]. It turns out that Hering's result provides a complete list of possibilities for G and its action on Ω. The question of which of these possibilities actually occur for some curve $\mathcal{X}$ is completely answered in our main theorem.

Theorem 1.1. *Let $\mathcal{C}$ be a plane model of $\mathcal{X}$ associated with the morphism $\varphi : \mathcal{X} \mapsto PG(2,\mathbb{K})$. Let $P_1, P_2 \in \mathcal{X}$ be two distinct points together with two distinct subgroups G_1, G_2 of $\mathrm{Aut}(\mathcal{X})$ such that $\varphi(P_1)$ and $\varphi(P_2)$ are simple Galois points of $\mathcal{C}$ with Galois groups G_1 and G_2, respectively. If G_i fixes P_i for $i = 1, 2$ then $G = \langle G_1, G_2\rangle$ is isomorphic to one of the following groups:*

(i) $\mathrm{PSL}(2, q), \mathrm{SL}(2, q), Sz(q), \mathrm{PSU}(3, q), \mathrm{SU}(3, q), Ree(q)$ *where q is a power of p, and $\deg(\mathcal{C})$ equals $q + 1$ in the linear case, $q^2 + 1$ in the Suzuki case and $q^3 + 1$ in the unitary and Ree case. Here G is supposed to be non-solvable.*
(ii) $\mathrm{P\Gamma L}(2, 8)$, *$p = 3$, and* $\deg(\mathcal{C}) = 28$.
(iiia) $\mathrm{AGL}(1, m)$ *for a prime power m of p,* $\deg(\mathcal{C}) = m$, *and $\mathcal{X}$ is rational.*
(iiib) $\mathrm{AGL}(1, 3)$, *$p \neq 3$,* $\deg(\mathcal{C}) = 3$, *and $\mathcal{X}$ is rational.*
(iiic) $\mathrm{AGL}(1, 4)$, *$p \neq 2$,* $\deg(\mathcal{C}) = 4$, *and $\mathcal{X}$ is rational.*
(iva) $\mathrm{AGL}(1, m)$, *for $m = 3, 4, 5, 7$, $p \neq 2, 3$,* $\deg(\mathcal{C}) = m$ *and $\mathcal{X}$ is elliptic.*
(ivb) $\mathrm{AGL}(1, m)$, *for $m = 3, 4, 5, 7$, $p = 3$,* $\deg(\mathcal{C}) = m$, *and $\mathcal{X}$ is elliptic.*
(ivc) $\mathrm{PSU}(3, 2)$, *$p = 2$, $|\Omega| = 9$, and $\mathcal{X}$ is elliptic.*
(ivd) $\mathrm{AGL}(1, m)$, *for $m = 3, 5, 7$, $p = 2$,* $\deg(\mathcal{C}) = m$, *and $\mathcal{X}$ is elliptic.*
(ive) $(C_5 \times C_5) \times \mathrm{SL}(2, 3)$, *for $p = 2$,* $\deg(\mathcal{C}) = 25$, *and $\mathcal{X}$ is elliptic.*
(va) $\mathrm{SU}(3, 2)$, *$p = 2$, and* $\mathfrak{g}(\mathcal{X}) = 10$.
(vb) $\mathrm{SL}(2, 3)$, *$p \neq 2, 3$ and* $\mathfrak{g}(\mathcal{X}) = 3$.

All the above cases occur, see Section 8. A corollary of Theorem 1.1 is the following result.

Theorem 1.2. *Under the hypotheses of Theorem 1.1, if $p \nmid |G_1|$, in particular if $p = 0$ or $p > 2\mathfrak{g}(\mathcal{X}) + 1$, then $\mathcal{X}$ is either rational or elliptic, or it has genus* 3.

Remark 1.3. If the order of the 1-point stabilizer of any point in G is coprime with p (that is G is tame), then the hypothesis that $\varphi(P_1)$ and $\varphi(P_2)$ are simple Galois points can be relaxed to unibranch Galois points, with just one exception, namely

(via) $G = G_1 \times G_2$ is cyclic, $\deg(C) = |G_1| + |G_2|$, and $\mathfrak{g}(\mathcal{X}) = 0$.

For an example; see Remark 2.13.

Remark 1.4. For a Galois point $\varphi(Q)$ with Galois group G it may happen that G does not fix any point $P \in \mathcal{X}$ such that $\varphi(P) = Q$; an example is given in Remark 2.11.

Our notation and terminology are standard; see [2,19,22,23,32]. In particular, $\mathrm{AGL}(1, m)$ denotes the automorphism group of the affine line over $\mathbb{F}_m$. Here, $\mathrm{AGL}(1, 3) \cong \mathbf{S}_3$, $\mathrm{AGL}(1, 4) \cong \mathbf{A}_4$.

2. Background from function field theory and some preliminary results

For a subgroup G of $\mathrm{Aut}(\mathcal{X})$, let $\bar{\mathcal{X}}$ denote a non-singular model of $\mathbb{K}(\mathcal{X})^G$, that is, a projective non-singular geometrically irreducible algebraic curve with function field $\mathbb{K}(\mathcal{X})^G$, where $\mathbb{K}(\mathcal{X})^G$ consists of all elements of $\mathbb{K}(\mathcal{X})$ fixed by every element in G. Usually, $\bar{\mathcal{X}}$ is called the quotient curve of $\mathcal{X}$ by G and denoted by $\mathcal{X}/G$. The field extension $\mathbb{K}(\mathcal{X})|\mathbb{K}(\mathcal{X})^G$ is Galois of degree $|G|$.

Since our approach is mostly group theoretical, we often use notation and terminology from finite group theory rather than from function field theory.

Let Φ be the cover of $\mathcal{X} \mapsto \bar{\mathcal{X}}$ where $\bar{\mathcal{X}} = \mathcal{X}/G$ is a quotient curve of $\mathcal{X}$ with respect to G. A point $P \in \mathcal{X}$ is a ramification point of G if the stabilizer G_P of P in G is nontrivial; the ramification index e_P is $|G_P|$; a point $\bar{Q} \in \bar{\mathcal{X}}$ is a branch point of G if there is a ramification point $P \in \mathcal{X}$ such that $\Phi(P) = \bar{Q}$; the ramification (branch) locus of G is the set of all ramification (branch) points. The G-orbit of $P \in \mathcal{X}$ is the subset $o = \{R \in \mathcal{X} \mid R = g(P),\, g \in G\}$, and it is *regular* (or long) if $|o| = |G|$, otherwise $o(P)$ is *short*. For a point $\bar{Q}$, the G-orbit o lying over $\bar{Q}$ consists of all points $P \in \mathcal{X}$ such that $\Phi(P) = \bar{Q}$. If $P \in o$ then $|o| = |G|/|G_P|$ and hence $\bar{\mathcal{Q}}$ is a branch point if and only if o is a short G-orbit. It may be that G has no short orbits. This is the case if and only if every non-trivial element in G is fixed–point-free on $\mathcal{X}$, that is, the cover Φ is unramified. On the other hand, G has a finite number of short orbits. For a non-negative integer i, the i-th ramification group of $\mathcal{X}$ at P is denoted by $G_P^{(i)}$ (or $G_i(P)$ as in [28, Chapter IV]) and defined to be

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

where t is a uniformizing element (local parameter) at P. Here $G_P^{(0)} = G_P$. The structure of G_P is well known; see for instance [28, Chapter IV, Corollary 4] or [19, Theorem 11.49].

Result 2.1. *The stabilizer G_P of a point $P \in \mathcal{X}$ in G has the following properties.*

(i) $G_P^{(1)}$ *is the unique normal p-subgroup of G_P;*
(ii) *For $i \geq 1$, $G_P^{(i)}$ is a normal subgroup of G_P and the quotient group $G_P^{(i)}/G_P^{(i+1)}$ is an elementary abelian p-group.*
(iii) $G_P = G_P^{(1)} \rtimes U$ *where the complement U is a cyclic group whose order is prime to p.*

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

$$2\mathfrak{g} - 2 = |G|(2\bar{\mathfrak{g}} - 2) + \sum_{P \in \mathcal{X}} d_P, \tag{1}$$

where

$$d_P = \sum_{i \geq 0} (|G_P^{(i)}| - 1). \tag{2}$$

Here $D(\mathcal{X}|\bar{\mathcal{X}}) = \sum_{P \in \mathcal{X}} d_P$ is the *different*. For a tame subgroup G of $\mathrm{Aut}(\mathcal{X})$, that is for $p \nmid |G_P|$,

$$\sum_{P \in \mathcal{X}} d_P = \sum_{i=1}^{m} (|G| - \ell_i)$$

where $\ell_1, \ldots, \ell_m$ are the sizes of the short orbits of G.

A group is a p'-group (or a prime to p group) if its order is prime to p. A subgroup G of $\mathrm{Aut}(\mathcal{X})$ is *tame* if the 1-point stabilizer of any point in G is p'-group. Otherwise, G is *non-tame* (or *wild*). Obviously, every p'-subgroup of $\mathrm{Aut}(\mathcal{X})$ is tame, but the converse is not always true. From the classical Hurwitz's bound, if $|G| > 84(\mathfrak{g}(\mathcal{X}) - 1)$ then G is non-tame; see [30,31] or [19, Theorems 11.56]. An orbit o of G is *tame* if G_P is a p'-group for $P \in o$, otherwise o is a *non-tame orbit* of G.

Let γ be the p-rank of $\mathcal{X}$, and let $\bar{\gamma}$ be the p-rank of the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/G$. The Deuring-Shafarevich formula, see [34] or [19, Theorem 11,62], states for a p-subgroup G of $\mathrm{Aut}(\mathcal{X})$ that

$$\gamma - 1 = |G|(\bar{\gamma} - 1) + \sum_{i=1}^{k} (|G| - \ell_i) \tag{3}$$

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

Result 2.2. *If $\mathcal{X}$ has zero p-rank then* $\mathrm{Aut}(\mathcal{X})$ *has the following properties:*

(i) *A Sylow p-subgroup of* $\mathrm{Aut}(\mathcal{X})$ *fixes a point $P \in \mathcal{X}$ but its nontrivial elements have no fixed point other than P.*
(ii) *The normalizer of a Sylow p-subgroup fixes a point of $\mathcal{X}$.*
(iii) *Any two distinct Sylow p-subgroups have trivial intersection.*

Claim (i) is [19, Theorem 11.129]. Claim (ii) follows from Claim (i). Claim (iii) is [19, Theorem 11.133].

For the following results, see [19, Lemmas 11.129, 11.75, 11.60]

Result 2.3. *Assume that* $\mathrm{Aut}(\mathcal{X})$ *contains a p-subgroup* G *of order* p^r*. If the quotient curve* $\mathcal{X}/G$ *has p-rank zero, and every non-trivial element in* G *has exactly one fixed point, then* $\mathcal{X}$ *has p-rank zero.*

Result 2.4 *(Serre). Let* $\alpha \in G_P$ *and* $\beta \in G_P^{(k)}$, $k \geq 1$*. If* $\alpha \notin G_P^{(1)}$*, then the commutator* $[\alpha, \beta] = \alpha\beta\alpha^{-1}\beta^{-1}$ *belongs to* $G_P^{(k+1)}$ *if and only if either* $\alpha^k \in G_P^{(1)}$ *or* $\beta \in G_P^{(k+1)}$*.*

Result 2.5. *If the order* n *of* G_P *is prime to* p*, then* $n \leq 4\mathfrak{g}(\mathcal{X}) + 2$*.*

Let $\mathcal{E}$ be a non-singular plane cubic curve viewed as a birational model of an elliptic curve $\mathcal{X}$. For an inflection point O of $\mathcal{E}$, the set of points of $\mathcal{E}$ can be equipped by an operation $\bigoplus$ to form an abelian group G_O with zero-element O, which is isomorphic to the zero Picard group of $\mathcal{E}$; see for instance [19, Theorem 6.107]. The translation τ_a associated with $a \in \mathcal{E}$ is the permutation on the points of $\mathcal{E}$ with equation $\tau_a : x \mapsto x \bigoplus a$. Since there exists an automorphism in $\mathrm{Aut}(\mathcal{E})$ which acts on $\mathcal{E}$ as τ_a does, translations of $\mathcal{E}$ can be viewed as elements of $\mathrm{Aut}(\mathcal{E})$. They form the translation group $J(\mathcal{E})$ of $\mathcal{E}$ which acts faithfully on $\mathcal{E}$ as a sharply transitive permutation group. For every prime r, the elements of order r in $J(\mathcal{E})$ are called r-torsion points. They together with the identity form an elementary abelian r-group of rank h. Here $h = 2$ for $r \neq p$ while h equals the p-rank of $\mathcal{E}$ for $r = p$, that is, $h = 0, 1$ according as $\mathcal{E}$ is supersingular or not.

Result 2.6. *The translation group* $J(\mathcal{E})$ *is a normal subgroup of* $\mathrm{Aut}(\mathcal{E})$*, and* $\mathrm{Aut}(\mathcal{E}) = J(\mathcal{E}) \rtimes \mathrm{Aut}(\mathcal{E})_P$ *for every* $P \in \mathcal{E}$*.*

Proof. For complex cubic curves the claim is known. Here we provide a characteristic free proof based on [29, Theorem 4.8]. Let O be the neutral element of the group structure of $\mathcal{E}$. Then $\mathrm{Aut}(\mathcal{E})_O$ is additive on $\mathcal{E}$; see [29, Theorem 4.8]. Therefore $\mathrm{Aut}(\mathcal{E})_O$ normalizes the group of translations $J(\mathcal{E})$. By transitivity of $J(\mathcal{E})$, $\mathrm{Aut}(\mathcal{E}) = J(\mathcal{E})\mathrm{Aut}(\mathcal{E})_O$, and $J(\mathcal{E}) \cap J(\mathcal{E})_O = \{\mathrm{id}\}$ by regularity of $J(\mathcal{E})$ on $\mathcal{E}$. Furthermore, again by transitivity of $J(\mathcal{E})$, O may be replaced by any $P \in \mathcal{E}$. $\square$

The following result comes from [29, Theorem 10.1] and [19, Theorem 11.94].

Result 2.7. *Let* $\mathcal{E}$ *be an elliptic curve, and* $P \in \mathcal{E}$*. If the stabilizer* H *of* P *in* $\mathrm{Aut}(\mathcal{E})$ *has order at least* 3 *then*

$$\begin{array}{ll} H \cong C_4, \text{ or } H \cong C_6 & \text{when } p \neq 2,3; \\ H \cong C_3 \rtimes C_4, \text{ and } j(\mathcal{E}) = 0 & \text{when } p = 3; \\ H \cong \mathrm{SL}(2,3) \text{ and } j(\mathcal{E}) = 0 & \text{when } p = 2. \end{array} \tag{4}$$

If $j(\mathcal{E}) = 0$ then $\mathcal{E}$ is birationally equivalent to either the cubic of affine equation $y^2 = x^3 + 1$, $y^2 = x^3 - x$ or $y^2 + y = x^3$, according as $p \neq 2, 3$, $p = 3$ or $p = 2$. Result 2.7 has the following corollary, see [19, Theorem 11.94].

Result 2.8. *Let $\mathcal{E}$ be an elliptic curve. If G is a subgroup of $\mathrm{Aut}(\mathcal{E})$ and $P \in \mathcal{E}$ then*

$$|G_P| = \begin{cases} 1,2,4,6 & \text{when } p \neq 2,3, \\ 1,2,4,6,12 & \text{when } p = 3, \\ 1,2,4,6,8,24 & \text{when } p = 2. \end{cases} \tag{5}$$

Moreover, if $G_{\mathcal{P}}$ is non-trivial then the quotient curve $\mathcal{E}/G$ is rational. For $p = 2$, the stabilizer $G_{\mathcal{P}}$ is cyclic when $|G_{\mathcal{P}}| \leq 4$, and it is the quaternion group when $|G_{\mathcal{P}}| = 8$, and the linear group $\mathrm{SL}(2,3)$ when $|G_{\mathcal{P}}| = 24$. All cases occur.

For a prime r, let R be the group of r-torsion points. Since R is the unique elementary abelian r-subgroup of $J(\mathcal{E})$, and $J(\mathcal{E})$ is a normal subgroup of $\mathrm{Aut}(\mathcal{E})$, R is also a normal subgroup of $\mathrm{Aut}(\mathcal{E})$.

Lemma 2.9. *Let $\mathcal{E}$ be an elliptic curve, and $\alpha \in \mathrm{Aut}(\mathcal{E})$ a non-trivial automorphism of prime order $t \neq p$. If α has at least two fixed points, then either $t = 2$ and α has exactly 4 fixed points, or $t = 3$ and α has exactly 3 fixed points. Furthermore,*

(i) *if $t = 3$, no non-trivial translation of $J(\mathcal{E})$ preserving the set of fixed points of α has order 3;*
(ii) *if $t = 2$ and, in addition, 4 divides the stabilizer of a fixed point of α then no non-trivial translation of $J(\mathcal{E})$ preserving the set of fixed points of α has order 2.*

Proof. The Hurwitz genus formula applied to the subgroup generated by α gives

$$0 = 2\mathfrak{g}(\mathcal{E}) - 2 = -2t + \lambda(t-1)$$

where λ counts the fixed points of α. From this, the first claim follows. Let $t = 3$. Since the 3-torsion group R of $\mathcal{E}$ has order 9, α together with R generate a subgroup M of $\mathrm{Aut}(\mathcal{E})$ of order 27. For a fixed point $P \in \mathcal{E}$ of α, let Δ be the R-orbit of P. As R is a normal subgroup of M, Δ is left invariant by M. Furthermore, since $|\Delta| = 9$, the stabilizer M_P of P in M has order 3 and its three fixed points are in Δ. Therefore, $M_P = \langle \alpha \rangle$ and the fixed points of α are in Δ. Since $J(\mathcal{E})$ is sharply transitive on $\mathcal{E}$, this yields that no non-trivial element of order prime to 3 may take P to another fixed point of α whence (i) follows for $t = 3$. Let $t = 2$. This time R is an elementary abelian group of order 4 which together with α generate a subgroup of $\mathrm{Aut}(\mathcal{E})$ of order eight. Also, M_P has order two and hence again $M_P = \langle \alpha \rangle$, and α fixes either two points in Δ, or all its 4 fixed points are in Δ. In the latter case, (ii) follows as for $t = 3$. To investigate the former case, suppose that $\alpha = \gamma^2$ with $\gamma \in \mathrm{Aut}(\mathcal{E})$ fixing P. The subgroup T generated by R together with γ has order 16 and preserves Δ. The kernel of the representation of T on Δ is not faithful, as $|\mathbf{S}_4|$ is not divisible by 16. Therefore, T contains an involution τ fixing Δ pointwise. Since $P \in \Delta$ and the stabilizer of P in $\mathrm{Aut}(\mathcal{E})$ is cyclic, τ coincides with α whence (ii) follows. $\square$

For a plane model $\mathcal{C}$ of $\mathcal{X}$ associated with the morphism $\varphi : \mathcal{X} \mapsto PG(2, \mathbb{K})$, there exists a one-to-one correspondence between points of $\mathcal{X}$ and branches of $\mathcal{C}$. For any point $P \in \mathcal{X}$ the associated branch γ of $\mathcal{C}$ is centered at $\varphi(P)$. Furthermore, the order of γ is the positive integer j_1 such that the intersection number $I(\varphi(P), \gamma \cap \ell) = j_1$ for all but just one line through $\varphi(P)$. For the exceptional line t, called the tangent to γ at $\varphi(P)$, we have $I(\varphi(P), \gamma \cap t) = j_2$ with $j_2 > j_1$; see [19, Section 4.2].

Let ω be the quadratic transformation with fundamental points $A_1A_2A_3$ and exceptional lines A_1A_2, A_2A_3, A_3A_1, where $A_1 = \varphi(P_1), A_2 = \varphi(P_2), A_3 = t_1 \cap t_2$, with t_i the tangent line at P_i; see [19, Sections 3.3, 3.4]. For any non-exceptional line ℓ through a fundamental point A_i, the image of ℓ by ω is a line ℓ' through A_i; more precisely the points of ℓ distinct from A_i are taken to the points of ℓ' distinct from A_i. For a branch δ of $\mathcal{C}$ centered at a point C of an exceptional line A_iA_j with $C \neq \{A_i, A_j\}$, its image $\omega(\delta)$ is a branch centered at the opposite vertex A_k, and the tangent of $\omega(\delta)$ is a non-exceptional line through A_k. The converse also holds. If $C = A_i$ and A_iA_j is the tangent of δ, then $\omega(\delta)$ is a branch centered at A_k and A_kA_j is its tangent.

Remark 2.10. Let P_1 be an inner Galois point of $\mathcal{X}$ with Galois group G_1. Up to a change of coordinates, $\mathcal{C}$ has affine equation $f(X, Y) = 0$, and $Y_\infty = \varphi(P_1)$. Furthermore, the G_1-fibers are represented by lines through Y_∞. For a G_1-fiber Λ, let ℓ be such a line. Then a point $P \in \mathcal{X}$ is in Λ if and only if the associated branch γ of $\mathcal{C}$ has one of the following properties: either $\varphi(P) \neq \varphi(P_1)$ and $\varphi(P) \in \ell$, or $\varphi(P) = \varphi(P_1)$ and the tangent to γ at $\varphi(P)$ coincides with the line ℓ. Furthermore, if G_1 fixes P_1 then the fiber of P_1 contains no more point. Therefore, if t is the tangent to $\mathcal{C}$ at $\varphi(P_1)$, then γ is the unique branch of $\mathcal{C}$ whose center lies on t and whose tangent coincides with t.

Remark 2.11. The following example shows that G_1 may not fix any branch centered at Y_∞. For $p \neq 2$, let $\mathcal{X}$ be a non-singular model of the singular plane curve with affine equation $Y^2 = g(X)$ with a separable polynomial $g(X) \in \mathbb{K}[X]$ of degree 4. From [19, Example 5.59], $\mathfrak{g}(\mathcal{X}) = 1$ and Y_∞ is the unique singular point of $\mathcal{C}$. More precisely, two branches of $\mathcal{C}$, say γ and γ', are centered at Y_∞, both tangent to the line ℓ_∞ at infinite. The linear map $u : (X, Y) \to (X, -Y)$ is in $\mathrm{Aut}(\mathcal{X})$, and $G_1 = \langle u \rangle$ preserves every line ℓ through Y_∞, acting transitively on its points distinct from Y_∞. Therefore, $P_1 = Y_\infty$ is an inner Galois point of $\mathcal{X}$ with Galois group G_1 of order 2, and the points $P_1, P_1' \in \mathcal{X}$ associated with γ, γ' respectively, form a G_1-fiber. We show that G_1 fixes no P_1 (and P_1'). Obviously, G_1 fixes each of the four points of $\mathcal{C}$ lying on the X-axis. From the Hurwitz genus formula applied to G_1, $0 = 2\mathfrak{g}(\mathcal{X}) - 2 = 2(2\mathfrak{g}(\bar{\mathcal{X}}) - 2)) + n$ where $\bar{\mathcal{X}} = \mathcal{X}/G_1$ and n is the number of fixed points of G_1 on $\mathcal{X}$. Since $n \geq 4$, this is only possible for $\mathfrak{g}(\bar{\mathcal{X}}) = 0$ and $n = 4$. In particular, neither Q_1 nor Q_2 is fixed by G_1. Now suppose $p \neq 2, 3$, and let $g(X) = \epsilon X(X-1)(X-\epsilon)(X-\epsilon^2)$ for a primitive third root of unity ϵ. A straightforward computation shows that $\mathcal{X}$ has another inner Galois point, namely the origin $O = (0, 0)$, with Galois group G_2 of order 3 generated by the linear map $v : (x, y) \to (\epsilon x, \epsilon y)$. Since O is not an inflection point with tangent OY_∞, and G_2 fixes both γ and γ', the singletons

$\{P_1\}$ and $\{P_2\}$ are G_2-fibers. In particular, the line OY_∞ contains no point from $\mathcal{C}$ other than P_1 and P_2. A generalization is obtained for $p \nmid d$ taking for $\mathcal{C}$ the plane curve of affine equation $Y^d = g(X)$ with $g(X) = \epsilon X(X-1)(X-\epsilon)\cdots(X-\epsilon^{2d-2})$ where ϵ is a primitive $(2d-1)$th root of unity

From previous works on Galois points, we need a very recent result due to Fukasawa; see [5, Theorem 1]. We state it for the case of two inner Galois points $\varphi(P_1), \varphi(P_2)$. We also add some properties in case where the corresponding Galois group G_i fixes P_i for $i = 1, 2$.

Lemma 2.12. *Let $\mathcal{C}$ be a plane model of $\mathcal{X}$ associated with the morphism $\varphi : \mathcal{X} \mapsto PG(2, \mathbb{K})$. Let $P_1, P_2 \in \mathcal{X}$ be two distinct points together with two distinct subgroups G_1, G_2 of $\mathrm{Aut}(\mathcal{X})$ such that $\varphi(P_1)$ and $\varphi(P_2)$ are unibranch Galois points of $\mathcal{C}$ with Galois groups G_1 and G_2, respectively. Then the following properties hold:*

- (I) *The quotient curves $\mathcal{X}/G_1$ and $\mathcal{X}/G_2$ are rational;*
- (II) *G_1 and G_2 have trivial intersection.*

Assume in addition that G_i fixes P_i for $i = 1, 2$ and let $G = \langle G_1, G_2\rangle$. If

$$\text{the line through } \varphi(P_1) \text{ and } \varphi(P_2) \text{ contains a further point of } \mathcal{C} \tag{6}$$

then the stabilizer $(G_1)_{P_2}$ of P_2 in G_1 and the stabilizer $(G_2)_{P_1}$ of P_1 have the same order and that number equals the multiplicity of both $\varphi(P_1)$ and $\varphi(P_2)$. Also, (6) implies that the following conditions are equivalent:

- (III) *In the divisor group of $\mathcal{X}$, $P_1 + \sum_{\sigma \in G_1} \sigma(P_2) = P_2 + \sum_{\tau \in G_2} \tau(P_1)$.*
- (i) *Both $\varphi(P_1)$ and $\varphi(P_2)$ are simple points.*
- (ii) *Both $(G_1)_{P_2}$ and $(G_2)_{P_1}$ are trivial.*

For tame G, (6) implies (ii).

If (6) does not hold then either $\varphi(P_1)$ or $\varphi(P_2)$ is a singular point of $\mathcal{C}$, both P_1 and P_2 are fixed by G, and, for tame G, G is cyclic.

Proof. By definition, (I) holds. Since both G_1 and G_2 are finite groups, and $\mathcal{C}$ has a finite number of singular points, there exists a simple point $\varphi(P) \in \mathcal{C}$ not on the line $\varphi(P_1)\varphi(P_2)$ which is not fixed by any non-trivial element from either G_1 or G_2. To show (II), assume by way of a contradiction that $g \in G_1 \cap G_2$ with $g \neq 1$. Let r be the line through $\varphi(P)$ and $\varphi(g(P))$ in $\mathrm{PG}(2, \mathbb{K})$. Then the points $\varphi(P_1), \varphi(P), \varphi(g(P))$ are three distinct points on the line r, and similarly, $\varphi(P_2), \varphi(P), \varphi(g(P))$ are three distinct points on the same line r. This yields that P lies on the line through $\varphi(P_1)$ and $\varphi(P_2)$, a contradiction. Up to a change of the projective frame, $\varphi(P_1) = Y_\infty$ and

$\varphi(P_2) = X_\infty$. Let $\mathcal{P}_1$ the set of all points of $\mathcal{X}$ which are taken by φ to points of $\mathcal{C}$ lying on the line ℓ_∞ at infinity. Obviously, $P_2 \in \mathcal{P}_1$, and hence the G_1-orbit Δ_1 of P_2 is also contained in $\mathcal{P}_1$. Furthermore, every point $P \in \mathcal{X}$ with $\varphi(P) \neq \varphi(P_1)$ and $\varphi(P) \in \ell_\infty$ is in Δ_1. However, a point $P \in \mathcal{X}$ with $\varphi(P) = \varphi(P_1)$ is in Δ_1 if and only if $\varphi(P)$, viewed as a branch of $\mathcal{C}$ centered at $\varphi(P_1)$, is tangent to ℓ_∞. Let $\mathcal{Q}_1 = \mathcal{P}_1 \setminus \Delta_1$. In the divisor group of $\mathbb{K}(\mathcal{X})$, let $B_1 = \sum_{P\in\mathcal{Q}_1} P$, $D_1 = \sum_{P\in\Delta_1} P$, and $m_1 = |(G_1)_{P_2}| = |(G_1)_P|$ for every $P \in \Delta_1$. Now, since $\varphi(P_1)$ is unibranch, we have $B_1 = P_1$, and hence $m_1(P_1 + D_1) = m_1P_1 + \sum_{\sigma\in G_1} \sigma(P_2)$. On the other hand, since P_1 is a Galois point with Galois group G_1, in the intersection divisor $\mathcal{C} \circ \ell_\infty$ the coefficient of $P \in \Delta_1$ is $|(G_1)_P| = m_1$. In particular, m_1 is equal to the multiplicity of $\varphi(P_2)$.

The analog pointsets $\mathcal{P}_2, \Delta_2, \mathcal{Q}_2$ and divisors B_2, D_2 and m_2 are defined interchanging P_1 with P_2 and replacing G_1 by G_2.

Since (6) implies that $|\Delta_1| > 1$ and $|\Delta_2| > 1$, their intersection contains a point P. Therefore, $m_1 = m_2$. Let $m = m_1$. Then both points $\varphi(P_1)$ and $\varphi(P_2)$ have multiplicity m, and $|G_1| = |G_2| = (\deg(\mathcal{C}) - m)/m$. Therefore,

$$mP_1 + \sum_{\sigma\in G_1} \sigma(P_2) = mP_2 + \sum_{\tau\in G_2} \sigma(P_1).$$

Now, (III) holds if and only if $m = 1$, that is, both points $\varphi(P_1)$ and $\varphi(P_2)$ are simple. The latter condition is equivalent to $|(G_1)_{P_2}| = |(G_2)_{P_1}| = 1$.

Since $|\Omega| > 2$, G is finite, otherwise $\mathcal{X}$ would be either rational, or elliptic, and an infinite number of elements in G would fix Ω pointwise which contradicts Result 2.7 and the fact that no non-trivial automorphism of a rational curve may fix more than two points. To show the final claim in Lemma 2.12, assume on the contrary that $m > 1$, and take a point $Q \in \Delta_1 \cap \Delta_2$. Then both $(G_1)_Q$ and $(G_2)_Q$ are subgroups of G_Q of order m. Since G is supposed to be tame, (iii) of Result 2.1 yields that G_Q is cyclic whence $(G_1)_Q = (G_2)_Q$ follows. This contradicts (II).

Suppose that (6) does not hold. Then Bézout's theorem, see [19, Theorems 3.14, 4.36], applied to the line $\ell_\infty = \varphi(P_1)\varphi(P_2)$ yields $\deg(\mathcal{C}) = \deg(\mathcal{C} \circ \ell_\infty) = I(\varphi(P_1), \mathcal{C} \cap \ell_\infty) + I(\varphi(P_2), \mathcal{C} \cap \ell_\infty)$. Since $\varphi(P_i)$ is unibranch and ℓ_∞ is not the tangent to $\mathcal{C}$ at P_i, the multiplicity μ_i of $\varphi(P_i)$ equals $I(\varphi(P_i), \mathcal{C} \cap \ell)$. Therefore, $\deg(\mathcal{C}) = \mu_1 + \mu_2$. From $\deg(\mathcal{C}) > 2$, either μ_1 or μ_2 exceeds 1, and hence one of the points $\varphi(P_1), \varphi(P_2)$ is singular. To show that G_1 fixes P_2, it is enough to observe that P_2 is the unique pole of y where $\mathbb{K}(y) = \mathcal{X}^{G_1}$. Therefore, both G_1 and G_2 fix P_2, and this holds true for P_1 as P_1 is the unique pole of x with $\mathbb{K}(x) = \mathcal{X}^{G_2}$. Therefore G fixes both P_1 and P_2. If G is tame then (ii) Result 2.1 implies that G is cyclic. $\square$

Remark 2.13. An example for the case where (6) does not hold is the curve $f(X, Y) = X^uY^v - 1$ with $u > v > 1$ and g.c.d$(u, v) = 1$ where $u = |G_2|$ and $v = |G_1|$. The automorphisms in G_1 are induced on $\mathcal{C}$ by the homology $(X, Y) \mapsto (X, \lambda Y)$ with λ ranging in the multiplicative subgroup of $\mathbb{K}$ of order $|G_1|$. The fixed points of such a homology in the plane are Y_∞ and the points on the line $Y = 0$. Therefore, a non-trivial automorphism in G_1 fixes exactly two points of $\mathcal{X}$, namely P_1 and P_2. Now, the Hurwitz genus formula applied to G_1 gives $\mathfrak{g}(\mathcal{X}) = 0$. The same holds for G_2 and the group G generated by G_1 and G_2 is the cyclic group of order $|G_1||G_2|$. This gives case (via) in Remark 1.3. Earlier references for this example are [13] and [17].

Lemma 2.14. *Let P_1, P_2 be two distinct points of $\mathcal{X}$ together with two distinct subgroups G_1, G_2 of* $\mathrm{Aut}(\mathcal{X})$ *such that* (I), (II), (III) *hold. Assume that G_i fixes P_i for $i = 1, 2$. Let D be the divisor defined in* (III). *If* $|\mathrm{Supp}(D)| > 2$ *then*

(i) *for $i = 1, 2$, the group G_i is a sharply transitive group on* $\mathrm{Supp}(D) \setminus \{P_i\}$*;*
(ii) *the group G generated by G_1 and G_2 acts on* $\mathrm{Supp}(D)$ *as a doubly transitive permutation group;*

Furthermore, there exists a birational model $\mathcal{C}$ of $\mathcal{X}$ such that $\varphi(P_1)$ and $\varphi_(P_2)$ are Galois points with Galois groups G_1 and G_2 respectively, and the equation $f(X, Y) = 0$ of $\mathcal{C}$ can be chosen in such way that

(iii) $|\mathrm{Supp}(D)| = \deg(\mathcal{C})$ *and both $\varphi(P_1)$ and $\varphi(P_2)$ are simple points.*
(iv) $\mathcal{X}^{G_1} = \mathbb{K}(x)$ *and* $\mathcal{X}^{G_2} = \mathbb{K}(y)$*,*
(v) $\varphi(P_1) = Y_\infty$ *and* $\varphi(P_2) = X_\infty$*,*
(vi) *the poles of x are the points in* $\mathrm{Supp}(D) \setminus \{P_1\}$*, each of multiplicity* 1*, and the poles of y are the points in* $\mathrm{Supp}(D) \setminus \{P_2\}$*, each of multiplicity* 1*.*

Proof. Take $u, v \in \mathbb{K}(\mathcal{X})$ with $\mathcal{X}^{G_1} = \mathbb{K}(u)$ and $\mathcal{X}^{G_2} = \mathbb{K}(v)$. Let $g(X, Y) \in \mathbb{K}[X, Y]$ be an irreducible polynomial such that $g(u, v) = 0$. From [5, Proposition 1], the plane curve $\mathcal{D}$ with affine equation $g(X, Y) = 0$ is a birational model of $\mathcal{X}$. Then $X_\infty = (1:0:0), Y_\infty = (0, 1, 0)$ are Galois points of $\mathcal{D}$ with Galois groups G_1 and G_2, respectively. Let $\psi : \mathcal{X} \mapsto \mathcal{D} \subset \mathrm{PG}(2, \mathbb{K})$ be the associated morphism. For $i = 1, 2$, let γ_i be the branch of $\mathcal{D}$ associated with P_i. From Remark 2.10, the tangent t_i of γ_i is different from the line $\psi(P_1)\psi(P_2)$. Let $\varphi = \omega \circ \psi$ where ω is a quadratic transformation with fundamental points $U_1 = \psi(P_1), U_2 = \psi(P_2), U_0 = t_1 \cap t_2$, and look at the birationally plane model $\mathcal{C}$ associated to φ. An equation of $\mathcal{C}$ is $f(X, Y) = 0$ with $f(\omega(u), \omega(v)) = 0$. From the properties of ω quoted before Remark 2.10, both U_2 and U_1 are inner Galois points of $\mathcal{C}$ with Galois group G_2 and G_1, respectively; see also [24]. Furthermore, from Remark 2.10, both these points of $\mathcal{C}$ are unibranch as $\omega(\gamma_1), \omega(\gamma_2)$ are the unique branches of $\mathcal{C}$ centered at U_2 and U_1 respectively. Also, the tangents of $\omega(\gamma_i)$ and $\omega(\gamma_2)$ are the lines U_0U_2 and U_0U_1 respectively.

Up to a change of x by $x - a$ with $a \in \mathbb{F}^*$, P_1 is a pole of x of multiplicity 1. A similar change in y ensures that P_2 is a pole of y of multiplicity 1. Thus (iv) and (v) hold. Note that for $\sigma \in G_1$, each point $\sigma(P_2)$ is also a pole of x.

Now, Lemma 2.12 applies. Since $|\mathrm{Supp}(D)| > 2$, (III) yields that Condition (6) is satisfied. Therefore, $\varphi(P_1)$ and $\varphi(P_2)$ are simple points.

We point out that $\sigma(P_2) = P_2$ with $\sigma \in G_1$ only occurs when $\sigma = 1$. (III) reads

$$P_1 + \sum_{\sigma \in G_1^*} \sigma(P_2) = \sum_{\tau \in G_2} \tau(P_1)$$

where G_1^* denotes the set of non-trivial elements of G_1. Now, if $\sigma(P_2) = P_2$ with $\sigma \in G_1^*$ then P_2 would be in the support of the divisor on the left hand side, but not on the right hand side as $\tau(P_2) = P_2$ for every $\tau \in G_2$; a contradiction. Similarly $\tau(P_1) = P_1$ never holds for $\tau \in G_2^*$. Therefore (i) and hence (ii) follow from (III). Also, $|\mathrm{Supp}(D)| - 1 = |G_1| = |G_2|$. A further consequence is that the poles of x are exactly the points $\mathrm{Supp}(D) \setminus \{P_1\}$ each with multiplicity 1. The same holds for y when P_1 is replaced by P_2. From this (vi) follows.

Finally, since $\varphi(P_1)$ is a simple point of $\mathcal{C}$, $|\mathrm{Supp}(D)| = \deg(\mathcal{C})$ follows from (III). $\square$

Assume that P is a pole of $v \in \mathbb{K}(\mathcal{X})$ with multiplicity 1. For a local parameter t of P, we have $v = t^{-1} + w$ with $v_P(w) \geq 0$. If $\alpha \in \mathrm{Aut}(\mathcal{X})$ fixes P choose the smallest integer m such that $\alpha^m(v) = v$. Assume that m is a power of p then $\alpha(v) = (t + \bar{w})^{-1} + w_1$ with $v_P(\bar{w}) \geq 2$ and $v_P(w_1) \geq 0$. Since $(t + \bar{w})^{-1} = t^{-1}(1 + w_2)$ with $v_P(w_2) \geq 1$ this yields $v_P(\alpha(v) - v) \geq 0$, that is, P is not a pole of $\alpha(v) - v$. For $p \nmid m$, the above argument can be adapted, as $(ut + w)^{-1} = u^{-1}t^{-1}(1 + w_3)$ with $v_P(w_3) \geq 0$. It turns out that P is not a pole of $\alpha(v) - u^{-1}v$. This holds true for α^k when u^{-1} is replaced by u^{-k}. Therefore, P is not a pole of $\alpha(v) - u^{-1}v$ for any m-th root of unity. This gives the following result.

Lemma 2.15. *For a pole P of $v \in \mathbb{K}(\mathcal{X})$, let $\alpha \in \mathrm{Aut}(\mathcal{X})$ be a non-trivial automorphism fixing P. Let m be the smallest integer such that $\alpha^m(v) = v$. If m is a power of p then P is not a pole of $\alpha(v) - v$. If $p \nmid m$ then P is not a pole of $\alpha(v) - uv$ for all m-th roots of unity $u \in \mathbb{K}$.*

The following result is well known for complex curves; see [1, Theorem 5.9]. It remains valid in any characteristic; see [19, Theorem 11.114].

Result 2.16. *Let S be a subgroup of $\mathrm{Aut}(\mathcal{X})$ of order n which has a partition with components $S_1, \ldots, S_k$, with $n_i = |S_i|$ for $i = 1, \ldots, k$, and let $\mathfrak{g}'$, $\mathfrak{g}'_i$ be the genera of the quotient curves $\mathcal{X}/S$ and $\mathcal{X}/S_i$, for $i = 1, \ldots, k$. Then*

$$(k-1)\mathfrak{g}(\mathcal{X}) + n\mathfrak{g}' = \sum_{i=1}^{k} n_i \mathfrak{g}'_i. \tag{7}$$

3. Background from group theory

From group theory we need properties of Lie type simple groups, namely the projective special group, the projective special unitary group, the Suzuki group $Sz(q)$, and the Ree Group $Ree(q)$. The main reference is [35, Section 3]; see also [19, Appendix A]. Our notation and terminology are standard. In particular, $Z(G)$ stands for the center of a group G. The normal closure S of subgroup H of a group G is the subgroup generated by all conjugates of H in G. By definition, S is the smallest normal subgroup of G containing H.

For $q = r^h$ with r prime, the projective special group $\mathrm{PSL}(2,q)$ has order $(q+1)q(q-1)/\tau$ with $\tau = \text{g.c.d.}(2, q+1)$. $\mathrm{PSL}(2,q)$ is simple for $q \geq 4$, isomorphic to a subgroup of the automorphism group of the projective line $\mathrm{PG}(1,q)$ over $\mathbb{F}_q$ and doubly-transitive on the set Ω of points of $\mathrm{PG}(1,q)$. If $r = 2$ then $\mathrm{PGL}(2,q) = \mathrm{PSL}(2,q)$ whereas, for r odd, $x \to (ax+b)/(cx+d) \in \mathrm{PSL}(2,q)$ if and only if $ad - bc$ is a non-zero square element of $\mathbb{F}_q$.

Result 3.1. *([Dickson's classification; see [33, Theorem 3]) The finite subgroups of the group* $\mathrm{PGL}(2,\mathbb{K})$ *are isomorphic to one of the following groups:*

(i) *prime to p cyclic groups;*
(ii) *elementary abelian p-groups;*
(iii) *prime to p dihedral groups;*
(iv) *Alternating group* $\mathbf{A}_4$*;*
(v) *Symmetric group* $\mathbf{S}_4$*; and* $p > 2$
(vi) *Alternating group* $\mathbf{A}_5$*;*
(vii) *Semidirect product of an elementary abelian p-group of order* p^h *by a cyclic group of order* $n > 1$ *with* $n \mid (p^h - 1)$*;*
(viii) $\mathrm{PSL}(2,p^f)$ *for* $f \mid m$*;*
(ix) $\mathrm{PGL}(2,p^f)$ *for* $f \mid m$*.*

Here, $\mathbf{A}_4 \cong \mathrm{AGL}(1,4)$, and $\mathbf{A}_5 \cong \mathrm{PSL}(2,5)$.

The special linear group $\mathrm{SL}(2,q)$ has center of order 2, and $\mathrm{SL}(2,q)/Z(\mathrm{SL}(2,q)) \cong \mathrm{PSL}(2,q)$. Moreover, the automorphism group of $\mathrm{PSL}(2,q)$ is the semilinear group $\mathrm{P\Gamma L}(2,\mathrm{q})$. Since $Z(\mathrm{PSL}(2,q))$ is trivial, $\mathrm{PSL}(2,q)$ can be viewed as a (normal) subgroup of $\mathrm{P\Gamma L}(2,\mathrm{q})$ consisting of all semilinear maps $x \to (ax^\sigma + b)/(cx^\sigma + d)$ where $a,b,c,d \in \mathbb{F}_q$ with $ad - bc \neq 0$, and $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$. The quotient group $\mathrm{P\Gamma L}(2,\mathrm{q})/\mathrm{PSL}(2,\mathrm{q})$ is either C_h, or $C_h \times C_2$, according as $r = 2$, or r is odd. The "linear subgroup" of $\mathrm{P\Gamma L}(2,\mathrm{q})$ is $\mathrm{PGL}(2,q)$ which is isomorphic to $\mathrm{Aut}(\mathrm{PG}(1,q))$, and consists of all linear maps $x \to (ax+b)/(cx+d)$ where $a,b,c,d \in \mathbb{F}_q$ with $ad - bc \neq 0$. Either $\mathrm{PGL}(2,q) = \mathrm{PSL}(2,q)$ or $[\mathrm{PGL}(2,q) : \mathrm{PSL}(2,q) = 2]$ according as $r = 2$ or r is odd.

Lemma 3.2. *Let* S_r *be a Sylow* r*-subgroup of the* 1*-point stabilizer* M *of a subgroup* L *of* $\mathrm{P\Gamma L}(2,\mathrm{q})$ *containing* $\mathrm{PSL}(2,q)$*. If* S_r *contains a Sylow* r*-subgroup* T_r *of* $\mathrm{PSL}(2,q)$ *then either* $S_r = T_r$*, or* $r|h$ *and* S_r *is not a normal subgroup of* M*. Furthermore, if* $S_r = T_r$ *and* M/S_r *is cyclic then* $G \leq \mathrm{PGL}(2,q)$*.*

Proof. If $r \nmid h$ then the Sylow r-subgroups of $\mathrm{PSL}(2,q)$ are also the Sylow r-groups of $\mathrm{P\Gamma L(2,q)}$. Therefore, we may assume that $h = r^u v$ with $u \geq 1, r \nmid v$. Any Sylow r-subgroup S_r of $\mathrm{P\Gamma L(2,q)}$ has order qr^u. Up to conjugacy, the 1-point stabilizer is the subgroup of $\mathrm{P\Gamma L(2,q)}$ fixing the point at infinity ∞ of $\mathrm{PG}(1,q)$. Then T_r consists of all transformations $x \to x + b$ with $b \in \mathbb{F}_q$. Furthermore, the transformations $x \to x^\sigma + b$ with $\sigma \in \mathrm{Aut}(GF(q))$, $\sigma^{r^u} = 1$, and $b \in GF(q)$, form a group of order qr^u which is a Sylow r-subgroup F of $\mathrm{P\Gamma L(2,q)}$. By Sylow's theorem, S_r may be assumed to be a subgroup of F. Let $w \in S_r$ be the semilinear transformation $w : x \to x^\sigma + a$ with a non-trivial automorphism σ of order p^k with $1 \leq k \leq u$, and $a \in \mathbb{F}_q$. Take an element $\lambda \in \mathbb{F}_q$ of order $q-1$ for q even and of order $\frac{1}{2}(q-1)$ for q odd. Let $l(x) = \lambda x$. Then $l \in \mathrm{PSL}(2,q)$ and l fixes ∞. Also, $(l^{-1}wl)(x) = \lambda^{\sigma-1}x^\sigma + \lambda^{-1}a$. By way of contradiction, assume that S_r is a normal subgroup of M. Then $l^{-1}wl \in S_r$ which yields $\lambda^\sigma = \lambda$, that is, λ lies in a proper subfield $\mathbb{F}_{r^k}$ of $\mathbb{F}_q$. But this contradicts the choice of λ. Finally, if $S_r = T_r$ and M/S_r is cyclic but $G \lneqq \mathrm{PGL}(2,q)$, let $M = S_r \rtimes U$ and take a semilinear transformation $u : x \to \lambda x^\sigma$ in U together with a linear transformation $v : x \to \mu x$ such that $\mu^\sigma \neq \mu$. Then $uv \neq vu$, and hence U cannot be cyclic. $\square$

For $q = r^h$ with r prime, the projective special unitary group $\mathrm{PSU}(3,q)$ has order $(q^3+1)q^3(q^2-1)/\mu$ with $\mu = \text{g.c.d.}(3, q+1)$. $\mathrm{PSU}(3,q)$ is simple for $q \geq 3$, isomorphic to a subgroup of $\mathrm{Aut}(\mathcal{H}_q)$ and doubly-transitive on the set Ω of all $\mathbb{F}_{q^2}$-rational points of $\mathcal{H}_q$. Furthermore, its automorphism group is the semilinear group $\mathrm{P\Gamma U(3,q)}$. Since $Z(\mathrm{PSU}(3,q))$ is trivial, $PSU(3,q)$ can be viewed as a (normal) subgroup of $\mathrm{P\Gamma U(3,q)}$. The "linear subgroup" of $\mathrm{P\Gamma U(3,q)}$ is $\mathrm{PGU}(3,q)$ which is isomorphic to $\mathrm{Aut}(\mathcal{H}_q)$. Let ∞ denote the (unique) point at infinity ∞ of $\mathcal{H}_q$. Then the stabilizer of ∞ in $\mathrm{P\Gamma U(3,q)}$ consists of all transformations t where $t(x) = ax^\sigma + c, t(y) = by^\sigma + \bar{a}^\sigma x + d$ with $a, b, c, d \in \mathbb{F}_{q^2}$, $\bar{a} = a^q, b \in \mathbb{F}_q^*, d^q + d = c^{q+1}$, and $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^2})$. Here $t \in PSU(3,q)$ for $\sigma = 1$ and $a^m = 1$ where either $m = \frac{1}{3}(q+1)$ or $m = q+1$, according as 3 divides $q+1$ or does not.

The special unitary group $\mathrm{SU}(3,q)$ has center of order $\mu = \text{g.c.d.}(3, q+1)$, and $\mathrm{SU}(3,q)/Z(\mathrm{SU}(3,q)) \cong \mathrm{PSU}(3,q)$.

Lemma 3.3. *Let S_r be a Sylow r-subgroup S_r of a 1-point stabilizer M of a subgroup L of $\mathrm{P\Gamma U(3,q)}$ containing $\mathrm{PSU}(3,q)$. If S_r contains a Sylow r-subgroup T_r of $\mathrm{PSU}(3,q)$. Then either $S_r = T_r$, or $r|h$ and S_r is not a normal subgroup of M. Furthermore, if $S_r = T_r$ and M/S_r is cyclic then $G \leq \mathrm{PGU}(3,q)$.*

Proof. We argue as in the proof of Lemma 3.2. By way of contradiction, S_r may be assumed to contain a transformation w where $w(x) = x^\sigma + a, w(y) = y^\sigma + x^\sigma + b$ with $b = a^q + a$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^2})$ of order r^k with $1 \leq k \leq u$. Let l be a transformation with $l(x) = \lambda x, l(y) = y$ where $\lambda \in \mathbb{F}_{q^2}$ has order $q+1$ for $3 \nmid (q+1)$ and $\frac{1}{3}(q+1)$ for $3 \mid (q+1)$. Then $l \in PSU(3,q)$ and ℓ fixes ∞. Moreover, $(l^{-1}wl)(x) = \lambda^{\sigma-1}x^\sigma + \lambda^{-1}a$.

As in the proof of Lemma 3.2, this leads to a contradiction. For the proof of the final claim the argument in the proof of Lemma 3.2 can be used. □

For $q = 2^h$ with $h \geq 3$ odd, the Suzuki group $Sz(q)$ has order $(q^2+1)q^2(q-1)$. It is a simple group, isomorphic to $\mathrm{Aut}(\mathcal{S}_q)$ where $\mathcal{S}_q$ stands for the Suzuki curve, see [19, Section 12.2]. $Sz(q)$ acts faithfully as a doubly transitive permutation group on the set Ω of all $\mathbb{F}_q$-rational points of $\mathcal{S}_q$. As $Z(Sz(q))$ is trivial, $Sz(q)$ can be viewed as a normal subgroup of its automorphism group $\mathrm{Aut}(Sz(q))$. Furthermore, the quotient group $\mathrm{Aut}(Sz(q))/Sz(q)$ is C_h. Therefore, the first claim of Lemma 3.2 trivially holds for $r = 2$ when $\mathrm{PSL}(2,q)$ and $\mathrm{P\Gamma L}(2,\mathrm{q})$ are replaced by $Sz(q)$ and $\mathrm{Aut}(Sz(q))$, respectively. A direct computation similar to that carried out at the end of the proof of Lemma 3.2 shows that if $S_r = T_r$ and M/S_r is cyclic then $G \leq Sz(q)$.

Lemma 3.4. *Let S_2 be a Sylow 2-subgroup of the 1-point stabilizer M of a subgroup L of $\mathrm{Aut}(Sz(q))$ containing $Sz(q)$. Then $S_r = T_r$. Furthermore, if M/S_r is cyclic then $G \leq Sz(q)$.*

For $q = 3^h$ with $h \geq 3$ odd, the Ree group $Ree(q)$ has order $(q^3+1)q^3(q-1)$. It is simple, isomorphic to $\mathrm{Aut}(\mathcal{R}_q)$ and doubly-transitive on the set Ω of all $\mathbb{F}_q$-rational points of the Ree curve $\mathcal{R}_q$. As $Z(Ree(q))$ is trivial, $Ree(q)$ can be viewed as a normal subgroup of its automorphism group $\mathrm{Aut}(Ree(q))$. Furthermore, the quotient group $\mathrm{Aut}(Ree(q))/Ree(q)$ is C_h. Furthermore, $Ree(q)$ has a faithful representation in the six-dimensional projective space $\mathrm{PG}(6,q)$ as a subgroup of $\mathrm{PGL}(7,\mathbb{F}_q)$ which preserves the Ree-Tits ovoid Q. The action of $Ree(q)$ on Q is doubly transitive, and it is the same as on Ω. We refer to an explicit presentation of Q in a projective frame $(X_0, X_1, \ldots, X_6)$ of $\mathrm{PG}(6,\mathbb{F}_q)$ as given in [19, Appendix A, Example A.13]. Then $Z_\infty = (0,0,0,0,0,1) \in Q$. Moreover, a Sylow 3-subgroup T_3 of $Ree(q)$ fixes Z_∞ and consists of all projectivities $\alpha_{a,b,c}$ associated to the matrices

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ a & 1 & 0 & 0 & 0 & 0 & 0 \\ b & a^\varphi & 1 & 0 & 0 & 0 & 0 \\ c & b - a^{\varphi+1} & -a & 1 & 0 & 0 & 0 \\ v_1(a,b,c) & w_1(a,b,c) & -a^2 & -a & 1 & 0 & 0 \\ v_2(a,b,c) & w_2(a,b,c) & ab+c & b & -a^\varphi & 1 & 0 \\ v_3(a,b,c) & w_3(a,b,c) & w_4(a,b,c) & c & -b+a^{\varphi+1} & -a & 1 \end{bmatrix}$$

for $a, b, c \in \mathbb{F}_q$. Also, the stabilizer $Ree(q)_{Z_\infty, O}$ with $O = (1,0,0,0,0,0,0) \in Q$ is the cyclic group C_{q-1} consisting of projectivities β_d associated to the diagonal matrices,

$$\mathrm{diag}(1, d, d^{\varphi+1}, d^{\varphi+2}, d^{\varphi+3}, d^{2\varphi+3}, d^{2\varphi+4})$$

for $d \in \mathbb{F}_q$. The stabilizer of Z_∞ in $Ree(q)$ is the semidirect product of $T_3 \rtimes C_{q-1}$. Moreover, the stabilizer of Z_∞ in $\mathrm{Aut}(Ree(q))$ consists of all semilinear transformations which are products uv where $u \in S_3$ and v is a σ-Frobenius map of $\mathrm{PG}(6, \mathbb{F}_q)$ where, for every $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$, the associated σ-Frobenius map is defined by $(X_0, \ldots, X_6) \to (X_0^\sigma, \ldots, X_6^\sigma)$. A direct computation similar to that carried out at the end of the proof of Lemma 3.2 shows that if $S_r = T_r$ and M/S_r is cyclic then $G \le Ree(q)$.

Lemma 3.5. *Let S_3 be a Sylow 3-subgroup of the 1-point stabilizer M of a subgroup L of $\mathrm{Aut}(Ree(q))$ containing $Ree(q)$. If S_3 contains a Sylow 3-subgroup T_3 of $Ree(q)$ then either $S_3 = T_3$, or $3|h$ and S_3 is not a normal subgroup of M. Furthermore, if $S_r = T_r$ and M/S_r is cyclic then $G \le Ree(q)$.*

Proof. We argue as in the proofs of Lemmas 3.2 and 3.3. We may assume $h = 3^u v$ with $3 \nmid v$. Let H_∞ be the hyperplane at infinity of equation $X_0 = 0$ so that the arising affine space $AG(6, \mathbb{F}_q)$ has coordinates $x_1 = X_1/X_0, \ldots, x_6 = X_6/X_0$. Look at the 1-point stabilizer of Z_∞. Up to an isomorphism, S_3 consists of products $\alpha\beta$ where $\alpha \in T_3$ and β is a Frobenius map $(x_1, \ldots, x_6) \to (x_1^\sigma, \ldots, x_6^\sigma)$ with $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$. In particular, S_3 contains a transformation w such that $w(x) = x^\sigma + a$, and σ of order 3^k with $1 \le k \le u$. For a primitive element $\lambda \in \mathbb{F}_q$, let l denote a transformation associated with the diagonal matrix $\mathrm{diag}(1, \lambda, \lambda^{\varphi+1}, \lambda^{\varphi+2}, \lambda^{\varphi+3}, \lambda^{2\varphi+3}, \lambda^{2\varphi+4})$. Computing $l^{-1}wl(x)$ shows again that $l^{-1}wl \notin S_3$, a contradiction as in the proof of Lemma 3.2 where ∞ is replaced with Z_∞. $\square$

Essential tools in our work are the classification of finite 2-transitive permutation groups whose 1-point stabilizer has a solvable normal subgroup due to Holt and O'Nan, and its generalization to group spaces, due to Hering.

Result 3.6. *(Holt, [20, Main Theorem]) Let G be a finite 2-transitive permutation group of even degree, and suppose that the 1-point stabilizer of G is solvable. Then either G has a regular normal subgroup, or G has a normal 2-transitive subgroup W isomorphic to $\mathrm{PSL}(2, q)$, $\mathrm{PSU}(3, q)$ (for some odd prime power q), or to $Ree(q)$. In the latter case, the action of W is the natural 2-transitive permutation representation of $\mathrm{PSL}(2, q)$, $\mathrm{PSU}(3, q)$ and $Ree(q)$ respectively, with only one exception: $G \cong \mathrm{P\Gamma L}(2, 8)$ and $W \cong \mathrm{PSL}(3, 2) \cong \mathrm{PSL}(2, 7)$ with degree 28.*

Result 3.7. *(O'Nan, [27, Theorem B]) Let G be a finite 2-transitive group of odd degree, and suppose that the 1-point stabilizer G has an abelian normal subgroup of order > 1. Then G has either a regular normal subgroup, or a normal 2-transitive subgroup W isomorphic to*

(i) $\mathrm{PSL}(r + 1, q)$, *with* $1 + q + \ldots + q^r$ *odd and* $r \ge 1$, *or*
(ii) $\mathrm{PSU}(3, 2^k)$, *or*

(iii) $\mathrm{Sz}(2^{2k+1})$,

and the action of W *is the natural* 2*-transitive representation of* $\mathrm{PSL}(r+1,q)$*,* $\mathrm{PSU}(3,2^k)$ *and* $\mathrm{Sz}(2^{2k+1})$*, respectively.*

A *group space* consists of a pair (Ω, G) where Ω is a set and G is generated, as an abstract group, by a set of permutations on Ω. Clearly, G induces a permutation group $\bar{G}$ on Ω so that $\bar{G} \cong G/K$ where the subgroup K is the kernel consisting of elements in G which fix Ω element-wise. A group space is *transitive*, if $\bar{G}$ is transitive on Ω. A transitive group space whose 1-point stabilizer has a subgroup transitive on the remaining points is 2-transitive.

Result 3.8. *(Hering, [18, Theorem 2.4]) Let* (Ω, G) *be a finite transitive group space with* $|\Omega| > 2$*. Assume that for some* $P \in \Omega$ *the stabilizer* G_P *contains a normal subgroup* Q *which is sharply transitive on* $\Omega \setminus \{P\}$*. If* S *is the normal closure of* Q *in* G*, then one of the following holds:*

(i) $S \cong \mathrm{PSL}(2,q), \mathrm{SL}(2,q), Sz(q), \mathrm{PSU}(3,q), \mathrm{SU}(3,q), Ree(q)$*, where* q *is a prime power, and* $|\Omega|$ *is* $q+1$ *in the linear case,* q^2+1 *in the Suzuki case and* q^3+1 *in the unitary and Ree case.*
(ii) $S \cong \mathrm{P\Gamma L}(2,8)$ *and* $|\Omega| = 28$*.*
(iii) S *is a sharply doubly transitive permutation group on* Ω*.*
(iv) $|\Omega| = d^2$ *for* $d \in \{3,5,7,11,23,29,59\}$*,* $S = O_d(S) \rtimes Q$*,* $O_d(S)$ *is extraspecial of order* d^3 *and exponent* d*,* $Z(O_d(S)) = Z(S)$ *is the kernel of* (Ω, S) *and* S *induces a sharply 2-transitive group on* Ω*.*

To deal with Case (iii), we need a corollary to Zassenhaus' classification of finite sharply doubly transitive groups.

Result 3.9. *(Zassenhaus [23, XII Theorem 9.8]) Let* G *be a sharply doubly transitive permutation group on a finite set* Ω*. Then* $|\Omega|$ *is a prime power* m*, and the elements in* G *which have no fixed point in* Ω *together with the identity permutation form an elementary abelian group* M *of order* m*. An example is the group* $\mathrm{AGL}(1,m)$ *which acts on the points of the affine line over the finite field* $\mathbb{F}_m$ *as a sharply doubly transitive permutation group. For* m *prime, there exists no other examples. For* $m = r^2$ *with* $r > 2$ *prime there exists further examples arising from nearfields of degree* r^2*.*

The group $\mathrm{A}\gamma\mathrm{L}(2,r^2)$ arises from the regular nearfield of degree r^2 and consists of all permutations on the elements of the finite field $\mathbb{F}_{r^2}$ which are of the form $x \mapsto a \circ x + b$ where $a, b \in \mathbb{F}_{r^2}$ and $a \circ x = ax$ for a a square in $\mathbb{F}_{r^2}$ while $a \circ x = ax^r$ for non-square a in $\mathbb{F}_{r^2}$. For $r \in \{5,7,11,23,20,59\}$, there exist irregular nearfields each of them gives rise to a sharply doubly transitive group as the regular nearfield does; see [23, Section 9].

For smaller values of m, the following holds. For $m = 9$ there exist exactly two sharply doubly transitive permutation groups, namely $\mathrm{AGL}(1,9)$ and $\mathrm{A\gamma L}(1,9)$, whereas for $m = 25$ three, namely $\mathrm{AGL}(1,25)$, $\mathrm{A\gamma L}(1,25)$, and $\mathcal{N}(5) \cong (C_5 \times C_5) \rtimes \mathrm{SL}(2,3)$ arising from the unique irregular nearfield of degree 25. In particular, $\mathrm{A\gamma L}(1,9) \cong \mathrm{PSU}(3,2)$. Furthermore, the 1-point stabilizer of $\mathrm{A\gamma L}(1,25)$ contains a subgroup of order 12 while that of $\mathcal{N}(5)$, isomorphic to $\mathrm{SL}(2,3)$, does not.

4. Doubly transitive groups on curves with simple minimal normal subgroup

Theorem 4.1. *Let G be a group acting on a finite set Ω with $|\Omega| > 2$ such that*

(i) *G acts on Ω as a 2-transitive permutation group,*
(ii) *the action of G on Ω is faithful,*
(iii) *the 1-point stabilizer has a normal Sylow p-subgroup with cyclic complement.*

If G has a simple non-abelian normal minimal subgroup W then either $G \cong \mathrm{P\Gamma L}(2,8)$ and $W \cong \mathrm{PSL}(2,8)$ with $|\Omega| = 28$ and $p = 3$, or one of the following cases occurs: $W \cong \mathrm{PSL}(2,q), Sz(q), \mathrm{PSU}(3,q)$, $Ree(q)$, where q is a power of p, and $|\Omega|$ is $q+1$ in the linear case, q^2+1 in the Suzuki case, q^3+1 in the unitary and Ree case.

Proof. The 1-point stabilizer of G is solvable. In particular, since G is not solvable, it does not contain any regular normal subgroup.

First the case where Ω has odd size is investigated. As a minimal normal subgroup of a solvable group is abelian, Result 3.7 applies. In case (i) of Result 3.7, since W acts on Ω as $\mathrm{PSL}(r+1,q)$ on the points of the projective space $\mathrm{PG}(r,q)$, the 1-point stabilizer of $\mathrm{PSL}(r+1,q)$ contains the linear group $\mathrm{SL}(r,q)$ which is solvable only when either $r = 1$, or $r = 2$ and $q = 2,3$. If $r = 1$, (iii) of Result 2.1 yields $p = 2$ as the unique maximal normal subgroup of the 1-point stabilizer has order q, and $q+1$ is odd. If $r = q = 2$ then $|\Omega| = 7$ and hence the 1-point stabilizer is isomorphic to $\mathbf{S_4}$, but the Sylow 2-subgroup of $\mathbf{S}_4$ is not a normal subgroup of $\mathbf{S}_4$, and Condition (iii) yields that this case cannot actually occur. If $r = 2, q = 3$ then $|\Omega| = 13$ and the 1-point stabilizer contains a subgroup isomorphic to $\mathrm{SL}(2,3)$ that contains no normal 3-subgroup. But, by Condition (iii), this is impossible.

If the size of Ω is even, Result 3.6 applies. Apart from the exceptional cases, the 1-point stabilizer has a unique normal subgroup of order q, and hence Condition (iii) yields that q is a power of p. If $G \cong \mathrm{P\Gamma}L(2,8)$, $W \cong \mathrm{PSL}(2,8)$ and $|\Omega| = 28$ then the 1-point stabilizer contains a non-cyclic normal subgroup of order 27, and Condition (iii) yields $p = 3$. □

Proposition 4.2. *Let G be a group acting on a finite set Ω with $|\Omega| > 2$ such that Conditions (i), (ii) and (iii) of Theorem 4.1 are satisfied. Assume that G has a simple non-abelian minimal normal subgroup W. If the 1-point stabilizer T of G has a subgroup*

H of order $|\Omega|-1$ that acts (sharply) transitively on the remaining $|\Omega|-1$ points then H is a normal subgroup of T.

Proof. Theorem 4.1 applies.

If $G \cong \mathrm{P\Gamma L}(2,8)$ and $|\Omega| = 28$ then the 1-point stabilizer T has order 54 and contains only one subgroup of order 27. Hence, the latter one is H, and it is normal in T.

If $W \cong \mathrm{PSL}(2,q)$ with $q \geq 4$ (and $|\Omega| = q+1$ with $q = p^h$) then $\mathrm{PSL}(2,q) \leq G \leq \mathrm{P\Gamma L}(2,q)$. Assume that H is not contained in $\mathrm{PSL}(2,q)$, and look at the subgroup L generated by $\mathrm{PSL}(2,q)$ and H. The subgroup $\mathrm{PSL}(2,q) \cap H$ is a p-subgroup of $\mathrm{PSL}(2,q)$ which fixes P. The stabilizer W_P of P in W has a Sylow p-subgroup R of $\mathrm{PSL}(2,q)$, and $\mathrm{PSL}(2,q) \cap H$ is contained in R. Since W_P is a normal subgroup of G_P, RH is a p-subgroup of L whose order equals $|R||H|/|R \cap H|$. Thus, RH is a Sylow p-subgroup of L. From Condition (iii) of Theorem 4.1 applied to L_P, RH is a normal subgroup of L_P. From Lemma 3.2, $R = H$.

If $W \cong \mathrm{PSU}(3,q)$ with $q \geq 3$ (and $|\Omega| = q^3+1$ with $q = p^h$) then $\mathrm{PSU}(3,q) \leq G \leq \mathrm{P\Gamma U}(3,q)$. The above argument used for $\mathrm{PSL}(2,q)$ still works with $|H| = q^3$ and Lemma 3.3.

If $W \cong Sz(q)$ (and $|\Omega| = q^2+1$ with $q = 2^h, h \geq 3$ odd) then $|H| = 2^{2h}$ but $[\mathrm{Aut}(Sz(q)) : Sz(q)] = h$ is odd. Therefore, up to conjugacy, $H = Sz(q)$. The 1-point stabilizer of $Sz(q)$ has a unique (Sylow) 2-subgroup of order q^2 which acts transitively on the set of the remaining $|\Omega|-1$ points. In particular, that Sylow 2-subgroup is normal and coincides with H.

If $W \cong Ree(q)$ (and $|\Omega| = q^3+1$ with $q = 3^h, h \geq 1$ odd) then $|H| = 3^{3h}$ and $[\mathrm{Aut}(Ree(q)) : Ree(q)] = h$. The above argument used for $\mathrm{PSL}(2,q)$ still works with $|H| = q^3$ and Lemma 3.5. □

Remark 4.3. By (iii) of Result 2.1, both Theorem 4.1 and Proposition 4.2 are valid for $\mathrm{Aut}(\mathcal{X})$ provided that Conditions (i) and (ii) in Theorem 4.1 are satisfied.

5. Doubly transitive groups on curves with solvable minimal normal subgroup

Theorem 5.1. *Let G be a subgroup of $\mathrm{Aut}(\mathcal{X})$ which has an orbit Ω with $|\Omega| > 2$ such that both (i) and (ii) in Theorem 4.1 hold. If, in addition,*

(iii) *G has a solvable minimal normal subgroup N,*
(iv) *the 1-point stabilizer of G has a subgroup T that is sharply transitive on the remaining points of Ω,*
(v) *the quotient curve $\mathcal{X}/T$ is rational,*

then $\mathcal{X}$ is either rational, or elliptic.

Proof. Let $d = |\Omega|$. Since N is faithful and sharply transitive on Ω, $T \cap N$ is trivial, the subgroup $S = TN$ has order $d(d-1)$ and hence it is a sharply doubly transitive group on Ω. Therefore, S has a partition whose components are the subgroup N of order d together with the stabilizers S_U in S with U ranging over Ω. Result 2.16 applies to S with $k = 1 + d$, where $S_1 = N$, and, for $i = 2, \dots k$, S_i are the conjugates of T in S. In particular, the quotient curves $\mathcal{X}/S_i$ for $i \geq 2$ are isomorphic. Since one of them, namely $\mathcal{X}/T$ is rational, we have $\mathfrak{g}(\mathcal{X}/S_i) = 0$ for $i = 2, \dots k$. Also $\mathfrak{g}(\mathcal{X}/S) = 0$, as T is a subgroup of S. Now, (7) reads $m\mathfrak{g}(\mathcal{X}) = m\mathfrak{g}(\mathcal{X}/N)$ whence $\mathfrak{g}(\mathcal{X}) = \mathfrak{g}(\mathcal{X}/N)$. This is only possible when either $\mathfrak{g}(\mathcal{X}) = 0$ or $\mathfrak{g}(\mathcal{X}) = 1$. $\square$

Remark 5.2. Theorem 5.1 is special case of a more general result of Guralnick; see [16, Corollary 3.2].

Proposition 5.3. *Let $\mathcal{X}$ be a rational curve. If G is a subgroup of* $\mathrm{Aut}(\mathcal{X})$ *such that both (i) and (ii) in Theorem 4.1 hold, and, in addition, G has a solvable minimal normal subgroup then one of the following cases occurs.*

(i) *G is sharply doubly transitive on Ω, $G \cong \mathrm{AGL}(1, m)$ with $|\Omega| = m$ where either m is a power of p, or $m = 3$ and $p \neq 3$, or $m = 4$ and $p \neq 2$.*
(ii) *$|\Omega| = 4$, $G \cong \mathbf{S}_4$, $p \neq 2$, and $\mathrm{AGL}(1, 4) \cong \mathbf{A}_4$ is the unique subgroup of G which is sharply doubly transitive on Ω.*

Proof. From the proof of Theorem 5.1, $S = TN$ is a sharply doubly transitive group on Ω. In particular, the order of S is the product of two consecutive integers. From Result 3.1 applied to S, we have $S \cong \mathrm{AGL}(1, m)$ where either m is a power of p, or $m = 3$ and $p \neq 3$, or $m = 4$ and $p \neq 2$. Moreover, if m is a power of p then any solvable subgroup of $\mathrm{PGL}(2, \mathbb{K})$ containing $\mathrm{AGL}(1, \mathrm{m})$ has an abelian subgroup of order $m' = mp^r$ with $r > 1$. Therefore, G cannot contain S properly. Also, $\mathrm{AGL}(1, 3)$ is the only doubly transitive permutation group of degree 3, and hence $G = S$ for $m = 3$ and $p \neq 3$. Finally, there are two doubly transitive permutation groups of degree 4, one is $\mathrm{AGL}(1, 4) \cong \mathbf{A}_4$ the other $\mathbf{S}_4$, and in the former case $G = S$ but $[G : S] = 2$ in the latter. $\square$

Proposition 5.4. *Let $\mathcal{E}$ be an elliptic curve. If G is a subgroup of* $\mathrm{Aut}(\mathcal{E})$ *such that both (i) and (ii) in Theorem 4.1 hold then one of the following occurs.*

(i) *G is sharply doubly transitive on Ω, $G \cong \mathrm{AGL}(1, m)$ with $m = |\Omega|$ where $m = 3, 4, 5, 7$ for $p \neq 2, 3$, and $m = 3, 4, 5, 7$ for $p = 3$, and $m = 3, 5, 7$ for $p = 2$,*
(ii) *G is sharply doubly transitive on Ω, $G \cong \mathrm{PSU}(3, 2)$ where $|\Omega| = 9$ and $p = 2$.*
(iii) *G is sharply doubly transitive on Ω, $G \cong (C_5 \times C_5) \rtimes \mathrm{SL}(2, 3)$ where $|\Omega| = 25$ and $p = 2$.*
(iv) *G is not sharply doubly transitive on Ω, $G \cong \mathbf{S}_4$ where $|\Omega| = 4$, $p \neq 2$.*
(v) *G is not sharply doubly transitive on Ω, $G \cong \mathrm{A\Gamma L}(1, 9)$ where $|\Omega| = 9$ and $p = 2$.*

Proof. Since a 1-point stabilizer G_P of G has order at least $|\Omega|-1$, Result 2.8 gives the possibilities for $|\Omega|$, namely $|\Omega|=3,5,7$ for $p \neq 2,3$, and $|\Omega|=3,5,7,13$ for $p=3$, and $3,4,5,9,25$ for $p=2$. Comparison of the cases listed in (i), . . . , (v) with Result 3.9 (and the subsequent remark) shows that only two cases have to be ruled out, namely $|\Omega|=13$ for $p=3$, and $|\Omega|=4$ for $p=2$. In the former case, G is sharply doubly transitive, and since 13 is a prime $G \cong \mathrm{AGL}(1,13)$ and its 1-point stabilizer G_P is cyclic; see Result 3.9. On the other hand, G_P is not abelian in this case by Result 2.7, a contradiction. In the latter case, $G \cong \mathrm{AGL}(1,4)$, and $p=2$. Since $j(\mathcal{E})=0$, $\mathcal{E}$ has zero 2-rank and hence it has no translation of order 2. On the other hand the only non-trivial normal subgroup of $\mathrm{AGL}(1,4)$ has order 4. But this contradicts Result 2.6. This contradiction ends the proof. $\square$

Proposition 5.5. *Let G be a subgroup of* $\mathrm{Aut}(\mathcal{X})$ *which has an orbit Ω such that both (i) and (ii) in Theorem 4.1 hold. If, in addition,*

(iii) *G has a solvable minimal normal subgroup N,*
(iv) *the* 1*-point stabilizer of G has a subgroup T that is sharply transitive on the remaining points of Ω,*
(v) *the quotient curve $\mathcal{X}/T$ is rational,*

then T is a normal subgroup of the 1*-point stabilizer of G.*

Proof. In Propositions 5.3 and 5.4, either T coincides with the 1-point stabilizer of G, or T is an index 2 subgroup of it. $\square$

6. Auxiliary results for the proof of Theorem 1.1

In this section, P_1, P_2 are distinct points of $\mathcal{X}$, and G_1, G_2 are distinct subgroups of $\mathrm{Aut}(\mathcal{X})$ where G_1 fixes P_1 and G_2 fixes P_2. Moreover, $|\mathrm{Supp}(D)|>2$, and G_1, G_2 have properties (I), (II), (III). By Lemmas 2.12 and 2.14, properties (i), (ii) and (vi) of Lemma 2.14 also hold.

As before, let Ω denote $\mathrm{Supp}(D)$ of the divisor D of $\mathcal{X}$ defined in (III). Then (ii) of Lemma 2.14 states that G acts on Ω as a doubly transitive permutation group. Actually, the normal closure S of G_1 in G still acts doubly transitively on Ω. In fact, there exists $g \in G$ which takes P_1 to P_2 and the subgroup $H_2 = g^{-1}G_1 g$ of G fixes P_2 and acts (sharply) transitively on $\Omega \setminus \{P_2\}$. Hence G_1, H_2 also have properties (I), (II), (III).

Our aim is to determine all possibilities for S. Since S may happen to be not faithful on Ω, we begin by investigating the subgroup K of G consisting of all elements which fix Ω pointwise.

Lemma 6.1. *K is a cyclic group whose order is prime to p and divides* $\deg(\mathcal{C})$*. Furthermore, $K=Z(G)=Z(S)$.*

Proof. From (vi) of Lemma 2.14, the poles of x are the points of Ω different from P_1, each with multiplicity 1. Take a non-trivial element $\alpha \in K$ of order s. For any $v \in \mathbb{K}(\mathcal{C})$, α takes a pole of v with multiplicity m to a pole of $\alpha(v)$ with the same multiplicity m. Therefore, $\alpha(x)$ has the same poles of x.

We show that p does not divide $|K|$. By way of a contradiction, assume $s = p$. From Lemma 2.15, no point $P \in \Omega$ is a pole of $\alpha(x) - x$. Also, no branch of $\mathcal{C}$ centered at an affine point is a pole of $\alpha(x) - x$. Thus $\alpha(x) - x \in \mathbb{K}$. Similarly, $\alpha(y) - y \in \mathbb{K}$. Therefore, α is a translation, that is, $\alpha(x) = x + a, \alpha(y) = y + b$ for $a, b \in \mathbb{K}$, and it has order p. Assume that $\alpha\beta \neq \beta\alpha$ for some $\alpha \in K$ and $\beta \in G_1$. Then $\beta^{-1}\alpha\beta(x) = \beta^{-1}(\alpha(x)) = \beta^{-1}(x+a) = \beta^{-1}(x)+\beta^{-1}(a) = x+a$. Therefore $\alpha^{-1}\beta^{-1}\alpha\beta(x) = x$. Since $\mathbb{K}(x) = \mathcal{X}^{G_1}$ this yields $\alpha^{-1}\beta^{-1}\alpha\beta \in G_1$. On the other hand $\alpha^{-1}\beta^{-1}\alpha\beta$ fixes Ω pointwise. Therefore $\alpha^{-1}\beta^{-1}\alpha\beta$ is the identity but this contradicts $\alpha\beta \neq \beta\alpha$. Therefore α centralizes G_1. As the same holds for G_2, $\alpha \in Z(G)$ follows. For a translation $\alpha \in K$, let T denote its center. Take a point $P \in \mathrm{Supp}(D)$ such that $\varphi(P)$ is different from T. Let γ be the branch of $\mathcal{C}$ associated with P. Then γ is centered at $\varphi(P)$, and its tangent t is different from the line at infinity by (vi) of Lemma 2.14. Then α does not leave invariant t and hence α does not fix P, a contradiction which shows that K contains no translation. Therefore, $p \nmid |K|$.

For $p \nmid s$, the same argument may be used. In fact, Lemma 2.15 shows that no point $P \in \Omega$ is a pole of $\alpha(x) - ux$ where u is a non-trivial m-th root of unity and m is the smallest integer for which $\alpha^m(x) = x$. Thus $\alpha(x) = ux + b$ with $b \in \mathbb{K}$, and similarly $\alpha(y) = ry + c$ with some $r \in \mathbb{K}$. Since α fixes a point $\varphi(Q) \in \ell_\infty$ other than $\varphi(P_1)$ and $\varphi(P_2)$, α is a homology. Therefore $u = r$ and the center of α is in the point $(-b/(u-1), -c/(u-1))$. From this, $\alpha\beta = \beta\alpha$, and hence $K \leq Z(G)$ follows. As before, for a point $P \in \mathrm{Supp}(D)$, let γ be the branch of $\mathcal{C}$ associated with P, centered at $\varphi(P)$, and with tangent t different from the line at infinity. Then the homology α leaves t invariant, and hence t passes through the center of α. This shows that the tangents to the branches of $\mathcal{C}$ arising from the points in $\mathrm{Supp}(D)$ are concurrent at the center of α. Furthermore, since any group generated by two homologies with different centers contains a translation, it turns out that K consists of homologies with the same center C. In particular, K is isomorphic to a finite multiplicative subgroup of $\mathbb{K}$. Therefore, K is cyclic and $p \nmid |K|$. Since G_1 fixes $\varphi(P_1) = Y_\infty$ and Y_∞ is a simple point of $\mathcal{C}$, the tangent to $\mathcal{C}$ at Y_∞ contains no point of $\mathcal{C}$ other than Y_∞. Therefore C is not a point of $\mathcal{C}$. Take a line ℓ through C and disjoint from Ω such that ℓ intersects $\mathcal{C}$ in non-singular points. From every K-orbit Δ_j in $\ell \cap \mathcal{C}$, take a unique point R_j. Then for the intersection divisor $\mathcal{C} \circ \ell$, Bézout's theorem gives $\deg(\mathcal{C}) = \deg(\mathcal{C} \circ \ell) = \sum_j |\Delta_j| I(R_j, \mathcal{C} \cap \ell)$. Also, $|\Delta_j| = |K|$ as no non-trivial element in K fixes a point in $\ell \cap \mathcal{C}$. From this $|K|$ divides $\deg(\mathcal{C})$.

Finally, since any point in Ω is the only fixed point of a conjugate of G_1 in G, $Z(S)$ fixes Ω pointwise. Therefore $Z(G) \leq Z(S) \leq K \leq Z(G)$ whence $K = Z(G) = Z(S)$. □

A useful ingredient in the proof of Theorem 1.1 is the following result.

Theorem 6.2. *G_1 is a normal subgroup of the stabilizer of P_1 in G.*

Proof. By Propositions 4.2 and 5.5, K may be assumed to be non-trivial. Let $\bar{G}$ be the doubly transitive permutation group induced by G on Ω. Then $\bar{G}$ acts on Ω as G does, and no nontrivial element in $\bar{G}$ fixes Ω pointwise. Propositions 4.2 and 5.5 apply to the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/K$. Therefore, $\bar{G_1} = G_1K/K$ is a normal subgroup of the stabilizer of $\bar{P}_1$ in $\bar{G}$ where $\bar{P}_1$ is the point lying under P_1 in the cover $\mathcal{X}|\bar{\mathcal{X}}$. Therefore, G_1K is a normal subgroup of the stabilizer of P_1 in G. From Proposition 6.1, $|K|$ divides $\deg(\mathcal{C}) = |\Omega|$ and $K = Z(G)$ whereas $|G_1| = |\Omega| - 1$ by (iii) of Lemma 2.14. Thus $G_1K = G_1 \times K$ with $\mathrm{g.c.d.}(|\mathrm{G}_1|, |\mathrm{K}|) = 1$. Therefore, G_1 is a characteristic subgroup of $G_1 \times K$, and hence G_1 is a normal subgroup of G_{P_1}. □

Remark 6.3. An alternative proof for Theorem 6.2 can be carried out by using Results 3.6 and 3.7.

7. Proof of Theorem 1.1

Let ℓ denote the line through $\varphi(P_1)$ and $\varphi(P_2)$.

The case where $\varphi(P)$ with $P \in \mathcal{X}$ lies on ℓ only for $P = P_1$ or $P = P_2$ cannot occur since in this case (6) does not hold and hence at least one of the points $\varphi(P_1)$ and $\varphi(P_2)$ of $\mathcal{C}$ is singular.

From now on we assume that $\varphi(P) \in \ell$ for some $P \in \mathcal{X}$ other than P_1 and P_2. Then $|\Omega| > 2$ where $\Omega = \mathrm{Supp}(D)$. Theorem 6.2 allows us to apply Result 3.8 to the group space (Ω, G) with $Q = G_1$ where S is the normal closure of G_1 in G.

7.1. S is of type (i) in Result 3.8

S is simple for $S = \mathrm{PSL}(2,q), q > 3, Sz(q), \mathrm{PSU}(3,q), q > 2, Ree(q)$ and Theorem 6.2 applies showing that q is a power of p. In the other non-solvable case we have either $S = \mathrm{SL}(2,q), q > 3$ or $\mathrm{SU}(3,q), q > 2$, and S acts on Ω as $\mathrm{PSL}(2,q)$, or $\mathrm{PSU}(3,q)$ in their natural 2-transitive representation. This permutation representation has non-trivial kernel z. Thus Theorem 6.2 applies to the quotient curve $\mathcal{X}/Z$, and it shows that q is a power of p. In the remaining cases, S is one of the solvable groups $\mathrm{PSL}(2,2), \mathrm{PSL}(2,3), \mathrm{SL}(2,2), \mathrm{SL}(2,3), \mathrm{PSU}(3,2), \mathrm{SU}(3,2)$. If either $S = \mathrm{PSL}(2,2) \cong \mathrm{AGL}(1,3)$, or $S = \mathrm{PSL}(2,3) \cong \mathrm{AGL}(1,4)$, or $S = \mathrm{PSU}(3,2)$, the permutation representation of S on Ω is faithful and sharply doubly transitive. These cases are also of type (iii) in Result 3.8 and are treated below; see Subsection 7.3. Also, $S = \mathrm{SU}(3,2)$ falls in case (iv) of Result 3.8 and it is investigated later; see Subsection 7.4.

We are left with the case $S = \mathrm{SL}(2,3)$ (and $|\Omega| = 4$). From (iii) of Lemma 2.14, $\deg(C) = 4$, and hence $\mathfrak{g}(\mathcal{X}) \leq 3$. We show that $\mathfrak{g}(\mathcal{X}) = 3$.

Since $\mathrm{SL}(2,3)$ is not a subgroup of $\mathrm{PGL}(2,\mathbb{K})$ by Result 3.1, $\mathcal{X}$ is not rational.

Assume that $\mathcal{X}$ is an elliptic curve $\mathcal{E}$. We show that $|G \cap J(\mathcal{E})| = 4$. For any point $Q \in \Omega$, there exists $h \in G$ which takes P_1 to Q. On the other hand, $J(\mathcal{E})$ has a translation τ taking Q to P_1. Then τh fixes P_1. Since the stabilizer of P_1 in $\mathrm{Aut}(\mathcal{E})$ has order ≤ 6 whereas the stabilizer of P_1 in $S = \mathrm{SL}(2,3)$ has order 6, it turns out that every automorphism in $\mathrm{Aut}(\mathcal{E})$ fixing P_1 is in S. Therefore, τh and hence τ itself is in S whence $|S \cap J(\mathcal{E})| \ge 4$ follows. As no non-trivial translation fixes a point of $\mathcal{E}$, this yields $|S \cap J(\mathcal{E})| = 4$. From Result 2.6, $S \cap J(\mathcal{E})$ is a normal subgroup of S. This contradicts the fact that $\mathrm{SL}(2,3)$ has no normal subgroup of order 4.

Assume that $\mathfrak{g}(\mathcal{X}) = 2$. The Hurwitz genus formula applied to G yields that G has exactly three short orbits, of length $4, 6$ and 12, respectively. In particular, each point in the orbit of length 12 is fixed by an involution. Since $\mathrm{SL}(2,3)$ has only one involution h, this yields that h has at least 12 fixed points. This contradicts the fact that no non-trivial automorphism of a genus $\mathfrak{g}$ curve may have more than $2\mathfrak{g}+2$ fixed points; see [19, Lemma 11.12].

Therefore, $\mathfrak{g}(\mathcal{X}) = 3$ and hence it $\mathcal{C}$ is a non-singular curve of degree four.

All cases occur as shown by the examples exhibited in Section 8. Here we observe that $\mathfrak{g}(\mathcal{X}) \ge 2$ apart from the possibilities where $S \cong \mathrm{PSL}(2,q)$ and $|\Omega| = q+1$, or $S \cong \mathbf{A}_5$ and $|\Omega| = 5$. This follows by comparison of the list in (i) of Result 3.8 with Result 3.1 (for $\mathfrak{g}(\mathcal{X}) = 0$) and with Result 2.8 (for $\mathfrak{g}(\mathcal{X}) = 1$).

7.2. S is of type (ii) in Result 3.8

An example is the smallest Ree curve; see Section 8.

7.3. S is of type (iii) in Result 3.8

Proposition 5.3 applies to S, and the possibilities come from Propositions 5.3 and 5.4. All cases occur; see Section 8.

7.4. S is of type (iv) in Result 3.8

Our goal is to show that $S \cong \mathrm{SU}(3,2)$ and $\mathfrak{g}(\mathcal{X}) = 10$. In case (iv) of Result 3.8, $|Z(S)| = d$ with $|\Omega| = d^2$. Furthermore, the quotient curve $\tilde{\mathcal{X}} = \mathcal{X}/G_1$ is rational and the quotient group $\tilde{Z} = (Z(S) \times G_1)/G_1$ is a subgroup of $\mathrm{Aut}(\tilde{\mathcal{X}})$ isomorphic to $Z(S)$. Since $Z(S)$ fixes Ω pointwise whereas G_1 has two orbits on Ω, we have that $\tilde{Z}$ has at least two fixed points in $\tilde{\mathcal{X}}$. Therefore, p is prime to the order of $\tilde{Z}$, that is, $p \ne d$. Also, $\tilde{Z}$ has no further fixed point. This shows that Ω coincides with the set of all fixed points of $Z(S)$. Now, look at the quotient curve $\bar{\mathcal{X}} = \mathcal{X}/Z(S)$. From the Hurwitz genus formula, $2\mathfrak{g}(\mathcal{X}) - 2 = d(2\mathfrak{g}(\bar{\mathcal{X}}) - 2) + d^2(d-1)$. Since $\bar{S} = S/Z(S)$ is sharply doubly transitive on Ω, Theorem 5.1 applies to $\bar{\mathcal{X}}$. Thus, $\bar{\mathcal{X}}$ is either rational, or elliptic. In the former case, as $d \ne p$, Result 3.1 yields $\bar{S} \cong \mathbf{A}_4$. This implies $d = 2$, a contradiction.

Therefore, $\bar{\mathcal{X}}$ is elliptic, and $\mathfrak{g}(\mathcal{X}) = \frac{1}{2}(d^2(d-1)+2)$. Also, the quotient group $\bar{G}_1 = (G_1 \times Z(S))/Z(S)$ is a subgroup of $\mathrm{Aut}(\bar{\mathcal{X}})$ fixing the point $\bar{P}_1$ of $\bar{\mathcal{X}}$ lying under P_1 in the cover $\mathcal{X}|\bar{\mathcal{X}}$. Since $\bar{G}_1 \cong G_1$ and $|G_1| = d^2-1$ with $d \geq 3$, Result 2.8 yields $p = 2$ and $d = 3, 5$. For $d = 3$, we have $|S| = 216$. More precisely, a MAGMA computation shows that either $S \cong \mathrm{SU}(3,2) = \mathit{SmallGroup}(216, 88)$, or $S \cong \mathit{SmallGroup}(216, 160)$. The latter case cannot actually occur since the 3-Sylow subgroup of $\mathit{SmallGroup}(216, 160)$ is abelian, and hence is not extra-special.

We are left with the possibility that $p = 2$, $d = 5$, $\mathfrak{g}(\mathcal{X}) = 51$, and $|S| = 3000$. Since $16 \nmid 3000$, a Sylow 2-subgroup S_2 of G_1 is also a Sylow 2-subgroup of S. Obviously, S_2 fixes P_1. We show that no non-trivial element in S_2 fixes a point other than P_1. The quotient group $\bar{S}_2 = (Z(S) \times S_2)/Z(S)$ is isomorphic to S_2 and it is a subgroup of $\mathrm{Aut}(\bar{\mathcal{X}})$ which fixes $\bar{P}_1$. From Result 2.8, $\bar{S}_2$ (and hence S_2) is isomorphic to the quaternion group Q_8 of order 8. The quotient curve $\hat{\mathcal{X}} = \bar{\mathcal{X}}/\bar{S}_2$ is rational, and it has zero 2-rank. From Result 2.3, $\bar{\mathcal{X}}$ has also zero 2-rank. Therefore, no non-trivial element in $\bar{S}_2$ fixes a point of $\mathcal{X}$ other than $\bar{P}_1$. This yields that S_2 fixes P_1 but its non-trivial elements fix no point other than P_1. To apply the Hurwitz genus formula to S_2, compute the ramification groups of S_2 at P_1. By definition, $S_2 = S_2^{(0)} = S_2^{(1)}$. From Result 2.4 applied to a generator α of $Z(S)$, we have $S_2^{(1)} = \ldots = S_2^{(5)}$. Since S_2 is not an elementary abelian group, (ii) of Result 2.1 yields that $S^{(6)}$ is non-trivial. Therefore, $S^{(6)}$ contains the (unique) subgroup T of S_2 of order 2. Since T is in G_1 and G_1 contains a (cyclic) subgroup C_{15} of order 15, Result 2.4 applies to a generator α of C_{15} whence $S_2^{(i)}$ for contains T for $i = 6, \ldots 15$. Let $\mathcal{X}' = \mathcal{X}/S_2$. From the Hurwitz genus formula applied to S_2,

$$100 = 2(\mathfrak{g}(\mathcal{X}) - 1) \geq 16(\mathfrak{g}(\mathcal{X}') - 1) + 42 + 10 \tag{8}$$

whence $\mathfrak{g}(\mathcal{X}') \leq 4$. Moreover, $(C_{15} \times S_2)/S_2 \cong C_{15}$ is a subgroup of $\mathrm{Aut}(\mathcal{X}')$ which fixes the point P_1' lying under P_1 in the cover $\mathcal{X}|\mathcal{X}'$.

If $\mathcal{X}'$ is rational, then the subgroup $(Z(S) \times S_2)/S_2 \cong C_5$ of $\mathrm{Aut}(\mathcal{X}')$ fixes exactly two points, namely P_1' and U'. Therefore, the fixed points of C_5 are P_1 and some (or all) of the points in the S_2-orbit lying over U'. This shows that C_5 has at most $9 < 25$ fixed points, a contradiction.

We may assume that $\mathfrak{g}(\mathcal{X}') \geq 1$. Result 2.5 yields $15 \leq 4\mathfrak{g}(\mathcal{X}') + 2$ whence $\mathfrak{g}(\mathcal{X}') = 4$. This shows that equality holds in (8). In particular, $S_2 = S_2^{(i)}$, for $i = 0, 1, \ldots, 5$, and $T = S_2^{(i)}$ for $i = 6, \ldots 15$, and $S_2^{(16)} = \{1\}$. From (2) applied to G_1, we have then $d_{P_1} = 23 + 5 \cdot 7 + 10 = 68$. Let C_3 be the subgroup of C_{15} of order 3. Then the quotient group $C_3' = (S_2 \rtimes C_3)/S_2 \cong C_3$ is a subgroup of $\mathrm{Aut}(\mathcal{X}')$. Let $\check{\mathcal{X}}$ be the quotient curve $\mathcal{X}'/C_3'$. The Hurwitz genus formula applied to C_3' reads $6 = 2(\mathfrak{g}(\mathcal{X}')-1) = 6(\mathfrak{g}(\check{\mathcal{X}})-1)+2r$ where r counts the fixed points of C_3'. Here $r \geq 1$ as C_3' fixes P_1'. From this, $\mathfrak{g}(\check{\mathcal{X}}) \leq 1$, and $r = 3$ or $r = 6$ according as $\check{\mathcal{X}}$ is elliptic or rational. The former case cannot actually occur by Result 2.8, since $(Z(S) \times (S_2 \rtimes C_3))/(S_2 \rtimes C_3) \cong C_5$ is a subgroup of $\mathrm{Aut}(\check{\mathcal{X}})$ fixing the point lying under the point P_1 in the cover $\mathcal{X}|\check{\mathcal{X}}$. Therefore, $\check{\mathcal{X}}$ is rational, and $r = 6$. Take a fixed point U' of C_3' other than P_1' and consider the S_2-orbit Δ lying over U'. Since C_3 leaves Δ invariant, and $|\Delta| = 8$, C_3 has at least two fixed points in Δ. Therefore, C_3 has at least 12 fixed points. Moreover, G_1 has four (pairwise conjugate) subgroups of order 3. Now, the Hurwitz genus formula applied to G_1 reads, $100 = 2(\mathfrak{g}(\mathcal{X}) - 1) \geq -48 + 68 + 4 \cdot 24 = 116$ a contradiction.

7.5. *S coincides with G*

By way of a contradiction, assume that some non-trivial element $g \in G_2$ does not belong to S. Since S is a normal subgroup of G, g is in the normalizer of $Z(S)$. Let $\bar{S} = S/Z(S)$ and $\bar{g} = gZ(S)/Z(S)$. We show that $\bar{g} \notin Z(\bar{S})$. Assume on the contrary that $gsg^{-1}s^{-1} \in Z(S)$ for every $s \in S$. Since $Z(S)$ fixes Ω pointwise, this yields $gs(P_2) = sg(P_2) = s(P_2)$. As P_2 is the unique fixed point of g, it follows $s(P_2) = P_2$, a contradiction S being transitive on Ω. Therefore, $\bar{g}$ induces by conjugation a non-trivial automorphism of $\bar{S}$.

If S is of type (i) in Result 3.8 then $d - 1$ a power of p and $\bar{S}$ is isomorphic to one of the groups $L = \mathrm{PSL}(2, q)$, $\mathrm{PSU}(3, q)$, $Sz(q)$, $Ree(q)$, and the action of $\bar{S}$ on Ω is the natural doubly transitive permutation representation of L. If $L = \mathrm{PSL}(2, q)$ then L together with $\bar{g}$ generate a subgroup D of $\mathrm{P\Gamma}L(2, q)$ strictly containing $\mathrm{PSL}(2, q)$. From (iii) of Result 2.1, the stabilizer M of P_2 in D is the semidirect product of the Sylow q-subgroup of D fixing P_2 by a cyclic complement. Now the second claim in Lemma 3.2 yields that $D \leqq L$, a contradiction. Similar arguments can be used to investigate the other possibilities for L where Lemma 3.2 by Lemmas 3.3, 3.4, and 3.5, respectively.

If S is of type (ii) in Result 3.8 then $S \cong \mathrm{P\Gamma L}(2, 8) = \mathrm{Aut}(\mathrm{P\Gamma L}(2, 8)) \cong \mathrm{Aut}(S)$, and hence $\bar{g} \in \bar{S}$, a contradiction.

If S is of type (iii) in Result 3.8 then $\mathcal{X}$ is either rational, or elliptic and one of the cases in Propositions 5.3 and 5.4 occurs. Let N be the (unique) minimal normal subgroup of S. Then N is a characteristic subgroup of S, and hence it is a minimal normal subgroup of G. Furthermore, $G_1N \leq S$ is a sharply doubly transitive group on Ω. Thus $S = G_1N$. Since $S \leq G$, either $G = S$, or $G > S$ and Lemma 5.4 shows that G_1N is the unique sharply doubly transitive subgroup of G on Ω. Since G_2N is another sharply doubly transitive subgroup of G on Ω, this yields $G_2 \leq S$, that is $G = S$.

If S is of type (iv) in Result 3.8 then $S \cong \mathrm{SU}(3, 2)$ and hence $\bar{S} \cong \mathrm{PSU}(3, 2)$. Also, $\mathrm{Aut}(\mathrm{PSU}(3, 2)) \cong \mathrm{P\Gamma U}(3, 2)$, and every involution in $\mathrm{P\Gamma U}(3, 2) \setminus \mathrm{PSU}(3, 2)$ has more than one fixed points. Again, $\bar{g}$ cannot be one of them, a contradiction.

8. Examples for Theorem 1.1

For each group G listed in Theorem 1.1 we exhibit an example of a plane curve with two different internal Galois points P_1 and P_2 both simple. These examples arise from automorphism groups satisfying (I), (II), (III) via Lemma 2.14. We keep our notation used in Theorem 1.1.

8.1. Case (i)

We show that the curves on which G acts naturally provide examples. All but the second examples on the Hermitian curve are known and they can be found in some recent papers of Fukasawa and his coauthors; see [7,10,12]. We refer to those papers for the proofs of (I), (II), (III).

8.1.1. Hermitian curve

Let $q = p^h$. The Hermitian curve (also called the Deligne-Lusztig curve of unitary type) $\mathcal{X}$ is the non-singular plane curve $\mathcal{C}$ of genus $\frac{1}{2}q(q-1)$ given by the affine equation $x^{q+1} + y^{q+1} + 1 = 0$; see [19, Section 12.3]. Furthermore, $\mathrm{PSU}(3, q)$ is isomorphic to a subgroup G of $\mathrm{Aut}(\mathcal{X}) \cong \mathrm{PGU}(3, q)$ which acts on the set Ω of all $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$ as doubly transitive permutation group. Here $|\Omega| = q^3 + 1 > 2$, and the stabilizer of $P \in \Omega$ in G contains a normal subgroup N_P which acts on $\Omega \setminus \{P\}$ as a sharply transitive permutation group, and P is a Galois point of $\mathcal{C}$ with Galois group N_P. For any two distinct points $P_1, P_2 \in \Omega$, define $G_1 = N_{P_1}$ and $G_2 = N_{P_2}$. The subgroup $G = \langle G_1, G_2\rangle$ is isomorphic $\mathrm{PSU}(3, q)$, and G is in turn the normal closure of G_1 in G.

Another example arises from the Hermitian curve if G is taken as the centralizer of an involution of $\mathrm{Aut}(\mathcal{X})$ which is the subgroup of $\mathrm{Aut}(\mathcal{X})$ preserving a chord ℓ of Ω. Here $G \cong \mathrm{SL}(2, q)$ (and $\mathrm{PSL}(2, q)$ for even q). For any two distinct points $P_1, P_2 \in \Omega \cap \ell$, define G_i to be the subgroup fixing P_i. Then Conditions (II), (III) are satisfied. To show (I) the sequence of the ramification groups $G_1^{(i)}$ at P_1 is useful. From [19, Lemma 12.1(e)], $G_1 = G_1^{(0)} = G_1^{(1)} = \ldots = G_1^{(q)}$ whereas $G_1^{(q+1)} = \{1\}$. From the Hurwitz genus formula applied to G_1, $(q + 1)(q - 2) = 2\mathfrak{g}(\mathcal{X}) - 2 = q(2\mathfrak{g}(\mathcal{X}/G_1) - 2) + (q + 1)(q - 1)$, whence $\mathfrak{g}(\mathcal{X}/G_1) = 0$. Similarly, for G_2. Moreover, $G = \langle G_1, G_2\rangle$, and G is the normal closure of G_1 in G.

8.1.2. Roquette curve

Let $q = p^h > 3$ with odd prime p. The Roquette curve $\mathcal{X}$ is the non-singular model of the irreducible (hyperelliptic) plane curve $\mathcal{C}$ of genus $\frac{1}{2}(q - 1)$ given by the affine equation $x^q - x = y^2$. Then either $\mathrm{PSL}(2, q)$ or $\mathrm{SL}(2, q)$ (according as $q \equiv 1 \pmod 4$ or $q \equiv -1 \pmod 4$) is isomorphic to a subgroup of $\mathrm{Aut}(\mathcal{X})$ which acts on the set Ω of all $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$ as a doubly transitive permutation group isomorphic to $\mathrm{PSL}(2, q)$.

8.1.3. Suzuki curve

Let $p = 2$, $q_0 = 2^s$, with $s \geq 0$ and $q = 2q_0^2 = 2^{2s+1}$. The Suzuki curve (also called the Deligne-Lusztig curve of Suzuki type) $\mathcal{X}$ is the non-singular model of the irreducible plane curve $\mathcal{C}$ of genus $q_0(q - 1)$ given by the affine equation $x^{2q_0}(x^q + x) = y^q + y$; see [19, Section 12.2]. The Suzuki group $Sz(q)$ is isomorphic to a subgroup G of $\mathrm{Aut}(\mathcal{X})$ which acts on the set Ω of all $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$. Here $|\Omega| = q^2 + 1 > 2$.

8.1.4. Ree curve

Let $p = 3$, $q = 3q_0^2$, with $q_0 = 3^s$, $s \geq 2$. The Ree curve (also called the Deligne-Lusztig curve of Ree type) $\mathcal{X}$ is the non-singular model of the irreducible plane curve $\mathcal{C}$ of genus $\frac{3}{2}q_0(q-1)(q+q_0+1)$ given by the affine equation $y^{q^2} - [1+(x^q-x)^{q-1}]y^q + (x^q - x)^{q-1}y - x^q(x^q-x)^{q+3q_0} = 0$; see [19, Section 12.4] Let $s \geq 2$. The Ree group $Ree(q)$ is isomorphic to a subgroup G of $\mathrm{Aut}(\mathcal{X})$ which acts on the set Ω of all $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$ as a doubly transitive permutation group.

8.1.5. GK curve

Let $q = p^{3r}$, with $r \geq 1$. The GK curve is the non-singular model of the irreducible plane curve $\mathcal{C}$ of genus $\frac{1}{2}(n^3+1)(n^2-2)+1$ given by the affine equation $y^{q+1} - (x^q + x) + (x^n+x)^{n^2-n+1} = 0$ where $n = p^r$, see [15]. Moreover, $\mathrm{SU}(3,n)$ is isomorphic to a subgroup of $\mathrm{Aut}(\mathcal{X})$ which acts on the set Ω of the n^3+1 $\mathbb{F}_q$-rational points of $\mathcal{X}$ as a doubly transitive permutation group.

8.2. Case (ii)

Let $p = 3$. The Ree curve $\mathcal{X}$ with $s = 1$ provides an example. Indeed, $\mathrm{P\Gamma L}(2,8)$ is isomorphic to a subgroup G of $\mathrm{Aut}(\mathcal{X})$ which acts on the set Ω of the 28 $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$ as a doubly transitive permutation group.

8.3. Cases (iii)

The basic tool is Result 3.1.

8.3.1. Case (iiia)

Let $m = p^h$. The rational curve $\mathcal{C}$ with homogeneous equation $yz^{m-1} = x^m - xz^{m-1}$ is an example with $G \cong \mathrm{AGL}(1,m)$. To show this, observe that the non-singular points of $\mathcal{C}$ defined over $\mathbb{F}_m$ are those lying on the X-axis, and they coincide with the points $P_u = (u,0,1)$ with $u \in \mathbb{F}_m$. For every non-zero $\lambda \in \mathbb{F}_m$ the transformation w with $w(x) = \lambda x$, $w(y) = \lambda y$ is in $\mathrm{Aut}(\mathcal{X})$ and preserves every line through P_0. They form a subgroup G_1 of order $m-1$ fixing P_0. Therefore, P_0 is a Galois point with Galois group G_1. The transformation τ with $\tau(x) = x - z$, $\tau(y) = y$ is in $\mathrm{Aut}(\mathcal{X})$, and $G_2 = \tau^{-1}G_1\tau$ is a subgroup of order $m-1$ fixing P_1. Therefore, P_1 is also a Galois point with Galois group G_2. Furthermore, $G_1 \cap G_2 = \{1\}$ and $G = \langle G_1, G_2 \rangle \cong \mathrm{AGL}(1,m)$. Earlier reference for this example is [9].

8.3.2. Case (iiib)

Let $p \neq 3$. The rational curve $\mathcal{C}$ with equation of degree 3 provides an example with $G \cong \mathrm{AGL}(1,3)$. To show this, for a subgroup $G \cong \mathrm{AGL}(1,3)$, take an involution $\alpha \in G$. Let $P \in \mathcal{X}$ be one of the fixed points of α. Then the orbit Ω of P in G has size 3. In G, take two distinct subgroups G_1 and G_2 of order 2. Let P_i with $i = 1,2$ be the fixed point of G_i. Then conditions (I), (II) and (III) are satisfied. Therefore P_i is an inner Galois point of $\mathcal{X}$ with Galois group G_i.

8.3.3. Case (iiic)

Let $p \neq 2$. The quartic curve $\mathcal{C}$ with homogeneous equation $x^2y^2 + y^2z^2 + z^2x^2 = 0$ is rational. For a primitive third root of unity $\varepsilon \in \mathbb{K}$, the cubic transformation α_1 with $\alpha_1(x) = y$, $\alpha_1(y) = z$, $\alpha_1(z) = x$ is in $\mathrm{Aut}(\mathcal{C})$ and fixes the point $P_1 = (1 : \varepsilon : \varepsilon^2)$. Also, the involution β with $\beta(x) = x$, $\beta(y) = -y$, $\beta(z) = z$ is in $\mathrm{Aut}(\mathcal{C})$, and takes P_1 to the point $P_2 = (1 : -\varepsilon : \varepsilon^2)$. Therefore, $\alpha_2 = \beta\alpha_1\beta \in \mathrm{Aut}(\mathcal{C})$ is a cubic transformation such that $\alpha_2(x) = -y$, $\alpha_2(y) = -z$, $\alpha_2(z) = x$ and $\alpha_2(P_2) = P_2$. Let $G_i = \langle \alpha_i \rangle$ for $i = 1, 2$. Then $G = \langle G_1, G_2 \rangle \cong \mathrm{AGL}(1, 4)$, and Condition (I), (II), (III) are satisfied, and $|\Omega| = 4 > 2$. Therefore, P_1 and P_2 are Galois points with Galois groups G_1 and G_2, respectively. Plane quartic curves with two Galois points are investigated in [8], where examples for Case (iiic) are also found.

8.4. Cases (iv)

We show a general procedure relying on Lemma 2.9 which provides examples for $p \nmid m$. Let $\mathcal{E}$ be an elliptic curve. For a prime r different from p, the translations in $\mathrm{Aut}(\mathcal{E})$ associated to the r-torsion points together with the identity transformation form an elementary abelian subgroup R of $\mathrm{Aut}(\mathcal{E})$ of order r^2. In $\mathrm{Aut}(\mathcal{E})$, the Jacobian subgroup $J(\mathcal{E})$ of $\mathrm{Aut}(\mathcal{X})$ consisting of all translations of $\mathcal{E}$ is abelian, and hence R is the unique elementary abelian subgroup of $J(\mathcal{E})$. Since $J(\mathcal{E})$ is a normal subgroup of $\mathrm{Aut}(\mathcal{E})$, this shows that R is also a normal subgroup of $\mathrm{Aut}(\mathcal{X})$. For a point $P_1 \in \mathcal{E}$ let Ω be the R-orbit of P_1, and G_1 the stabilizer of P_1 in $\mathrm{Aut}(\mathcal{E})$. For a non-trivial element $\alpha \in R$, the point $P_2 = \alpha(P_1)$ is fixed by $G_2 = \alpha^{-1}G_1\alpha$. Therefore, conditions (I) and (II) are satisfied. Moreover, Lemma 2.9 shows that no non-trivial element in G_1 fixes a point of Ω other than P_1. Therefore, (III) holds with $\mathrm{Supp}(D) = \Omega$ if and only if $|G_1| = r^2 - 1$. If this is the case then $G = \langle G_1, G_2 \rangle$ is sharply doubly transitive on $\mathrm{Supp}(D)$, and, from Result 3.9 and subsequent discussion, either $G \cong \mathrm{AGL}(1, r^2)$, or $G \cong \mathrm{A\gamma L}(1, r^2)$, or G arises from an irregular nearfield. This together with Result 2.8 provide an example with $m = 4, 9, 25$; more precisely $\mathrm{AGL}(1, 4)$ for $p \neq 2$, and $\mathrm{A\gamma L}(1, 9)$, and $(C_5 \times C_5) \rtimes \mathrm{SL}(2, 3)$ for $p = 2$. Therefore, Conditions (I), (II) and (III) are satisfied, and examples for (iva), (ivb), (ivc), (ivd), (ive) are obtained from (i), (ii) and of Proposition 5.4, respectively.

8.5. Case (va)

Let $p = 2$. The GK curve $\mathcal{C}$ has genus 10 and defined over $\mathbb{F}_8$ with homogeneous equation $z^9 + x^8y + xy^8 + (x^2y + xy^2)^3 = 0$. $\mathcal{C}$ has two Galois points $P_1 = (0 : 1 : 0)$ and $P_2 = (1 : 0 : 0)$ with Galois groups $G_1 \cong G_2$. Here $G = \langle G_1, G_2 \rangle \cong \mathrm{SU}(3, 2)$ and G_1 is the Sylow 2-subgroup of P_1 isomorphic to the quaternion group. Earlier reference of this example is [12].

8.6. Case (vb)

Let $p \neq 2, 3$. The non-singular plane quartic $\mathcal{C}$ of equation $X^4 + Y^4 + YZ^3 = 0$ has four internal Galois points, two of them are $P_1 = (0 : 0 : 1)$ and $P_2 = (0 : -1 : 1)$. The group G generated by the respective Galois groups is isomorphic to $\mathrm{SL}(2, 3)$. Earlier reference of this example is [26].

References

[1] R.D.M. Accola, Topics in Theory of Riemann Surfaces, Lecture Notes in Math., vol. 1595, Springer Verlag, 1994.

[2] P.J. Cameron, Finite permutation groups and finite simple groups, Bull. Lond. Math. Soc. 13 (1981) 1–22.

[3] S. Fukasawa, Complete determination of the number of Galois points for a smooth plane curve, Rend. Semin. Mat. Univ. Padova 129 (2013) 93–113.

[4] S. Fukasawa, Galois points for a non-reflexive plane curve of low degree, Finite Fields Appl. 23 (2013) 69–79.

[5] S. Fukasawa, A birational embedding of an algebraic curve into a projective plane with two Galois points, J. Algebra 511 (2018) 95–101.

[6] S. Fukasawa, An upper bound for the number of Galois points for a plane curve, in: Topics in Finite Fields, in: Contemp. Math., vol. 632, Amer. Math. Soc., 2015, pp. 111–119.

[7] S. Fukasawa, Birational embeddings of the Hermitian, Suzuki and Ree curves with two Galois points, Finite Fields Appl. 57 (2019) 60–67.

[8] S. Fukasawa, Rational curves of degree four with two inner Galois points, arXiv:1511.02598.

[9] S. Fukasawa, T. Hasegawa, Singular plane curves with infinitely many Galois points, J. Algebra 323 (2010) 10–13.

[10] S. Fukasawa, K. Higashine, A birational embedding with two Galois points for certain Artin-Schreier curves, Finite Fields Appl. 52 (2018) 281–288.

[11] S. Fukasawa, K. Higashine, A birational embedding with two Galois points for quotient curves, arXiv:1809.01777.

[12] S. Fukasawa, K. Higashine, Galois lines for the Giulietti-Korchmáros curve, Finite Fields Appl. 57 (2019) 268–275.

[13] S. Fukasawa, K. Miura, Galois points for a plane curve and its dual curve, Rend. Semin. Mat. Univ. Padova 132 (2014) 61–74.

[14] S. Fukasawa, P. Speziali, Plane curves possessing two outer Galois points, arXiv:1801.03198.

[15] M. Giulietti, G. Korchmáros, A new family of maximal curves, Math. Ann. 343 (2009) 229–245.

[16] R.M. Guralnick, Frobenius groups as monodromy groups, J. Aust. Math. Soc. 85 (2008) 191–196, 14H30 (14D05 14H05).

[17] H. Hayashi, H. Yoshihara, Galois Group at Each Point for Some Self-Dual Curves, Hindawi Publishing Corporation Geometry, 2013.

[18] C. Hering, A theorem on group spaces, Hokkaido Math. J. 8 (1979) 115–120.

[19] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field, Princeton Series in Applied Mathematics, Princeton University Press, Princeton, NJ, 2008, xx+696 pp.

[20] D.F. Holt, Doubly transitive groups with a solvable one point stabilizer, J. Algebra 44 (1977) 29–92.

[21] M. Homma, Galois points for a Hermitian curve, Commun. Algebra 34 (2006) 4503–4511.

[22] B. Huppert, Endliche Gruppen. I, Grundlehren der Mathematischen Wissenschaften, vol. 134, Springer, Berlin, 1967, xii+793 pp.

[23] B. Huppert, B.N. Blackburn, Finite Groups. III, Grundlehren der Mathematischen Wissenschaften, vol. 243, Springer, Berlin, 1982, ix+454 pp.

[24] K. Miura, Galois points for plane curves and Cremona transformations, J. Algebra 320 (2008) 987–995.

[25] K. Miura, Galois points on singular plane quartic curves, J. Algebra 287 (2005) 283–293.

[26] K. Miura, H. Yoshihara, Field theory for function fields of plane quartic curves, J. Algebra 226 (2000) 283–294.

[27] M. O'Nan, Doubly transitive groups of odd degree whose one point stabilizers are local, J. Algebra 39 (1976) 440–482.

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

[29] J.H. Silverman, The Arithmetic of Elliptic Curves, second edition, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009, xx+513 pp.

[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 Primzahl- charakteristik. II. Ein spezieller Typ von Funktionenkörpern, Arch. Math. 24 (1973) 615–631.

[32] H. Stichtenoth, Algebraic Function Fields and Codes, Springer Verlag, 2009.

[33] R.C. Valentini, M.L. Madan, A Hauptsatz of L.E. Dickson and Artin–Schreier extensions, J. Reine Angew. Math. 318 (1980) 156–177.

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

[35] R.A. Wilson, The Finite Simple Groups, Springer Verlag, 2009.

[36] H. Yoshihara, Function field theory of plane curves by dual curves, J. Algebra 239 (2001) 340–355.

[37] H. Yoshihara, Rational curve with Galois point and extendable Galois automorphism, J. Algebra 321 (2009) 1463–1472.