学　位　論　文

Criteria for the existence of a plane model with two Galois points for algebraic curves

(代数曲線に対するガロア点を 2 つもつ平面モデル存在の判定法)

March, 2021

Graduate School of Science and Engineering
Yamagata University

Kazuki Higashine

Acknowledgments

I would like to express my deepest gratitude to my supervisor Professor Satoru Fukasawa for all his advice and continued encouragement. I learned many things about what I should be as a mathematician from him. I think that he has spent countless hours for me. Without his many comments, suggestions, and proper guidance, I would never have been able to write this dissertation. Also, the paper co-authored with him is part of this dissertation.

I also would like to thank everyone involved in this dissertation. In particular, I would like to thank the sub-chief examiner Professors Masato Arai, Tomohiro Okuma, and Daisuke Shiomi.

Finally, I would like to express my gratitude to my family for their continuous support and encouragement. Without the support of my family, I would not have been able to keep learning mathematics.

Kazuki HIGASHINE
Graduate School of Science and Engineering
Yamagata University
Kojirakawa-machi 1-4-12
Yamagata 990-8560
Japan
E-mail: s182102d@st.yamagata-u.ac.jp

Contents

Chapter 1

Introduction

Let k be an algebraically closed field of characteristic $p \geq 0$. We fix k as the ground field of our discussion in this dissertation. In 1996, Hisao Yoshihara introduced the notion of Galois points in algebraic geometry. Let C be an irreducible (possibly singular) plane (algebraic) curve over k. We consider the projection

$$\pi_P : C \dashrightarrow \mathbb{P}^1; Q \mapsto \overline{PQ}$$

with the center $P \in \mathbb{P}^2$, where $\overline{PQ}$ represents the line passing through points P, $Q \in \mathbb{P}^2$ if $P \neq Q$. If the field extension $k(C)/\pi_P^* k(\mathbb{P}^1)$ of function fields induced by π_P is Galois, then P is called a Galois point for C (see [9, 41, 47]). Assume that P is a Galois point. If P is a smooth point of C (resp. a singular point of C, a point contained in C, a point not contained in C), then P is called a smooth Galois point (resp. a non-smooth Galois point, an inner Galois point, an outer Galois point), after [39, 40, 45]. The associated Galois group

$$G_P = \mathrm{Gal}(k(C)/\pi_P^* k(\mathbb{P}^1))$$

is called a Galois group at P.

In the theory of Galois points, plane curves with two or more Galois points are important. In 2013, with the contribution of four researchers Yoshihara, Kei Miura, Masaaki Homma, and Satoru Fukasawa, a complete classification of smooth plane curves with two or more Galois points was obtained ([41, 47, 36, 6, 8, 7, 10, 15, 12]). A classification of plane curves with infinitely many inner Galois points was obtained by Fukasawa and Takehiro Hasegawa [21]. In the case of infinitely many outer Galois points, a classification was

obtained by Fukasawa [11]. It is known that a plane curve with two or more Galois points may have a very large automorphism group ([14]). The relation between the set of rational points and the set of Galois points has been pointed out ([36, 13, 16]). In [25], using the set of Galois points, Fukasawa, Homma and Seon Jeong Kim constructed algebraic geometry codes.

In 2016, Fukasawa [17] presented a criterion for the existence of a birational embedding of a smooth projective curve into a projective plane with two smooth Galois points. Let X be a (reduced, irreducible) smooth projective curve over k. Then the following theorem is Fukasawa's criterion (for smooth Galois points).

Theorem ([17], Theorem 1)**.** *Let G_1, G_2 be finite subgroups of* $\mathrm{Aut}(X)$ *and let P_1, P_2 be different points of X. Then the three conditions*

(a) $X/G_1 \cong \mathbb{P}^1$, $X/G_2 \cong \mathbb{P}^1$,

(b) $G_1 \cap G_2 = \{1\}$, *and*

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

are satisfied, if and only if there exists a birational embedding $\varphi : X \to \mathbb{P}^2$ of degree $|G_1| + 1$ such that $\varphi(P_1)$ and $\varphi(P_2)$ are different smooth Galois points for $\varphi(X)$ and $G_{\varphi(P_i)} = G_i$ for $i = 1, 2$.

This criterion completely describes the conditions for the existence of a plane model with two smooth Galois points from the viewpoint of an automorphism group and its action. Using this criterion, Fukasawa, Katsushi Waki, and the author obtained new examples of plane curves with two smooth Galois points (see [17, 22, 26]). Before this criterion was obtained, only seven types of examples of plane curves with two smooth Galois points were known.

In this dissertation, we focus mainly on two generalizations of Fukasawa's criterion. These results are dealt with in Chapters 3 and 4. We also discuss the related results for the Giulietti–Korchmáros curve in Chapter 5. First, we recall the basic notation and facts about algebraic curves and their function fields in Chapter 2. We start with a review of the correspondence between the linear systems on a curve X and morphisms from X into projective spaces. For a morphism between smooth projective curves, we also recall the Riemann–Hurwitz formula and basic properties of a Galois covering. At the end of Chapter 2, Fukasawa's criteria are described. These results are used to prove the main theorems.

In Chapter 3, we generalize Fukasawa's criteria by focusing on a quotient curve of (a smooth model of) a plane curve with two Galois points. In Fukasawa's criteria, a finite set on which an automorphism group acts is important. In [18], new examples of plane curves with two Galois points were obtained using the set of rational points. In [22], the set of Weierstrass points were used. However, in general, it is difficult to assume a suitable finite set. On the other hand, some known examples of plane curves with two Galois points are regarded as quotient curves X/H of curves X with a finite subgroup $H \subset \mathrm{Aut}(X)$ such that X admits a birational embedding with two Galois points. By focusing on such examples, the main theorem in Chapter 3 is obtained.

Theorem 1.0.1. *Let H, G_1, $G_2 \subset \mathrm{Aut}(X)$ be finite subgroups with $H \lhd G_i$ for $i = 1, 2$, and let P_1, $P_2 \in X$. Then the four conditions*

(a') $X/G_1 \cong \mathbb{P}^1$, $X/G_2 \cong \mathbb{P}^1$,

(b') $G_1 \cap G_2 = H$,

(c') $\sum_{h \in H} h(P_1) + \sum_{\sigma \in G_1} \sigma(P_2) = \sum_{h \in H} h(P_2) + \sum_{\tau \in G_2} \tau(P_1)$, *and*

(d') $H \cdot P_1 \neq H \cdot P_2$, *where $H \cdot P_i$ represents the orbit of P_i for $i = 1, 2$,*

are satisfied, if and only if there exists a birational embedding $\varphi : X/H \to \mathbb{P}^2$ of degree $|G_1/H| + 1$ such that $\varphi(\overline{P_1})$ and $\varphi(\overline{P_2})$ are different smooth Galois points for $\varphi(X/H)$ and $G_{\varphi(\overline{P_i})} = \overline{G_i}$ for $i = 1, 2$.

Note that the image of the natural homomorphism $G_i \to \mathrm{Aut}(X/H)$ is denoted by $\overline{G_i}$ for $i = 1, 2$ in Theorem 1.0.1. As an application of this theorem, for the case where X admits a plane model with two smooth Galois points, we present sufficient conditions for the existence of a plane model of a quotient curve X/H with two Galois points.

Corollary 1.0.2. *Let G_1, G_2, H be finite subgroups of $\mathrm{Aut}(X)$, and let P_1, P_2 be different points of X. Assume that the three conditions*

(a) $X/G_1 \cong \mathbb{P}^1$, $X/G_2 \cong \mathbb{P}^1$,

(b) $G_1 \cap G_2 = \{1\}$, *and*

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

are satisfied. If the three conditions

(d) $H \cap G_1G_2 = \{1\}$,

(e) $HG_1 = H \rtimes G_1$, $HG_2 = H \rtimes G_2$, *and*

(f) $H \cdot P_1 \neq H \cdot P_2$

are satisfied, then there exists a birational embedding $\psi : X/H \to \mathbb{P}^2$ *of degree* $|G_1| + 1$ *such that* $\psi(\overline{P_1})$ *and* $\psi(\overline{P_2})$ *are different smooth Galois points for* $\psi(X/H)$ *and* $G_{\psi(\overline{P_i})} \cong G_i$ *for* $i = 1, 2$.

Note that similar statements hold for outer Galois points. Owing to this generalization, we can construct new examples of plane curves with two Galois points from known examples of plane curves with two Galois points. In fact, we apply our criterion to some maximal curves. A smooth projective curve defined over a finite field, for which the number of rational points attains the Hasse–Weil upper bound, is called a maximal curve. We focus on the Giulietti–Korchmáros curve [28] and the curves constructed by Skabelund [42]. Using these maximal curves, we present new examples of plane curves with two smooth Galois points.

In Chapter 4, we extend Fukasawa's criterion to all cases with two (possibly non-smooth) Galois points. There have been some known examples of plane curves with two or more non-smooth Galois points. For example, the Ballico–Hefez curve ([13, Theorem 1]), some self-dual curves ([33, Theorem 17]), the (plane model of) Giulietti–Korchmáros curve ([23, Theorem 2]), the (q^3, q^2)-Frobenius nonclassical curve ([2, Theorem 1]), and the Artin–Schreier–Mumford curve (proof of [19, Theorem 1]) are such curves. However, these examples are not intended to actively focus on non-smooth Galois points. Only few research studies have focused on non-smooth Galois points. Takeshi Takahashi [45] studied plane quintic curves with a double point P and determined defining equations when P is a Galois point. As far as the author knows, this is the only study that focused on a non-smooth Galois point so far. To study non-smooth Galois points systematically, it is good to have a criterion for non-smooth Galois points. The following theorem is one of the main theorems in Chapter 4.

Theorem 1.0.3. *Let* G_1, G_2 *be finite subgroups of* $\mathrm{Aut}(X)$ *and let* P_1, P_2 *be different points of* X. *Then there exists a birational embedding* $\varphi : X \to \mathbb{P}^2$ *such that* $\varphi(P_1)$, $\varphi(P_2)$ *are different inner Galois points, that* $G_{\varphi(P_i)} = G_i$ *for*

$i = 1, 2$, and that $L = \overline{\varphi(P_1)\varphi(P_2)}$ is not a tangent line at $\varphi(P_1)$, if and only if the following conditions are satisfied:

(a) $X/G_1 \cong \mathbb{P}^1, X/G_2 \cong \mathbb{P}^1$,

(b) $G_1 \cap G_2 = \{1\}$, *and*

(c) *one of the following holds:*

(c-i) $P_1 \notin G_1 \cdot P_2$, $P_2 \notin G_2 \cdot P_1$, $G_1 \cdot P_2 \cap G_2 \cdot P_1 \neq \emptyset$, *and* $|G_1(P_2)| = |G_2(P_1)|$.

(c-ii) $G_1 \cdot P_2 \cap G_2 \cdot P_1 = \emptyset$.

(c-iii) $P_1 \notin G_1 \cdot P_2$, $G_1 \cdot P_2 \cap G_2 \cdot P_1 \neq \emptyset$ *and* $|G_1(P_2)| > |G_2(P_1)|$.

Furthermore, for any φ as in the above, the following hold:

(i) *L is not a tangent line at $\varphi(P_2)$ with $L \cap \varphi(X) \supsetneq \{\varphi(P_1), \varphi(P_2)\}$ if and only if condition* (c-i) *is satisfied.*

(ii) *L is not a tangent line at $\varphi(P_2)$ with $L \cap \varphi(X) = \{\varphi(P_1), \varphi(P_2)\}$ if and only if condition* (c-ii) *is satisfied.*

(iii) *L is a tangent line at $\varphi(P_2)$ if and only if condition* (c-iii) *is satisfied.*

For a birational embedding φ in Theorem 1.0.3, multiplicities and order sequences at Galois points are also described in detail.

Theorem 1.0.4. *Let φ be as in Theorem 1.0.3, and let Λ be the linear system on X corresponding to the morphism φ. Let $(0, \alpha_P, \beta_P)$ denote the (Λ, P)-order sequence at a point $P \in X$. Then the following hold.*

(1) *The multiplicity $m_{\varphi(P_1)}$ of $\varphi(X)$ at $\varphi(P_1)$ is equal to*

$$|G_2(P_1)| \cdot |G_2 \cdot P_1 \setminus (G_1 \cdot P_2 \cap G_2 \cdot P_1)|.$$

(2) *The divisor $\sum_{P \in \varphi^{-1}(\varphi(P_1))} \alpha_P P$ is equal to*

$$\sum_{Q \in G_2 \cdot P_1 \setminus (G_1 \cdot P_2 \cap G_2 \cdot P_1)} |G_2(P_1)| Q.$$

(3) *The multiplicity* $m_{\varphi(P_2)}$ *of* $\varphi(X)$ *at* $\varphi(P_2)$ *is equal to*

$$|G_1(P_2)|\cdot|G_1\cdot P_2\setminus(G_1\cdot P_2\cap G_2\cdot P_1)|+(|G_1(P_2)|-|G_2(P_1|)\cdot|G_1\cdot P_2\cap G_2\cdot P_1|.$$

(4) *The divisor* $\sum_{P\in\varphi^{-1}(\varphi(P_2))}\alpha_P P$ *is equal to*

$$\sum_{R\in G_1\cdot P_2\setminus(G_1\cdot P_2\cap G_2\cdot P_1)}|G_1(P_2)|R+\sum_{S\in G_1\cdot P_2\cap G_2\cdot P_1}(|G_1(P_2)|-|G_2(P_1)|)S.$$

(5) *In the case* (iii) *of Theorem 1.0.3, the equality* $\beta_P=|G_1(P_2)|$ *holds at each point* $P\in G_1\cdot P_2\cap G_2\cdot P_1$.

(6) *The divisor* φ^*L *is equal to*

$$\sum_{Q\in G_2\cdot P_1\setminus(G_1\cdot P_2\cap G_2\cdot P_1)}|G_2(P_1)|Q+\sum_{R\in G_1\cdot P_2}|G_1(P_2)|R.$$

To explain the usefulness of these theorems, we apply them to rational curves. We present three examples of plane rational curves with two non-smooth Galois points, and calculate the second or third order at each point contained in the line passing through these two Galois points.

In Chapter 5, we determine the arrangement of all Galois lines for the Giulietti–Korchmáros curve and the number of Galois points for a plane model of this curve. These results are applied in Chapters 3 and 4. In more detail, as a quotient curve of the Giulietti–Korchmáros curve, new examples of plane curves with two smooth Galois points are obtained in Chapter 3. The plane model of the Giulietti–Korchmáros curve is an example of a plane curve with two or more non-smooth Galois points, as observed in Chapter 4. A line $\ell\subset\mathbb{P}^3$ is called a Galois line for a space curve $C\subset\mathbb{P}^3$ if the field extension $k(C)/\pi_\ell^*k(\mathbb{P}^1)$ induced by the projection $\pi_\ell : C \dashrightarrow \mathbb{P}^1$ with the center ℓ is Galois. This notion was introduced by Yoshihara as a generalization of the notion of Galois points (see [4, 48]).

Chapter 2

Preliminaries

We recall some basic notation and facts about algebraic curves and their function fields (see, for example, [43, 46]). At the end of this chapter, Fukasawa's criteria [17] are described. Let X be a (reduced, irreducible) smooth projective curve over k, and let $k(X)$ be its function field. The group of all k-automorphisms of X (resp. $k(X)$) is denoted by $\mathrm{Aut}(X)$ (resp. $\mathrm{Aut}_k(k(X))$). Note that there exists a natural isomorphism

$$\mathrm{Aut}(X) \cong \mathrm{Aut}_k(k(X)); \varphi \mapsto \varphi^*,$$

where φ^* represents the pullback of φ. In this dissertation, we always identify $\mathrm{Aut}(X)$ with $\mathrm{Aut}_k(k(X))$ by this isomorphism. For projective space $\mathbb{P}^n$ over k, we also identify $\mathrm{Aut}(\mathbb{P}^n)$ with the projective linear group $\mathrm{PGL}(n+1, k)$.

2.1 Linear system

In this section, we recall the notion of linear systems on a curve. The group of all divisors on X, that is, the free abelian group which is generated by the points of X, is denoted by $\mathrm{Div}(X)$. Let $D = \sum n_P P \in \mathrm{Div}(X)$. For a point $P \in X$, we write $\mathrm{ord}_P(D) := n_P$. The degree of D is defined by

$$\deg(D) = \sum \mathrm{ord}_P(D).$$

The set

$$\mathrm{supp}(D) = \{P \in X \mid \mathrm{ord}_P(D) \neq 0\}$$

is called the support of D. If $\mathrm{ord}_P(D) \geq 0$ at each point $P \in X$, we write $D \geq 0$. For any two divisors E, $G \in \mathrm{Div}(X)$, we write $E \geq G$ if $E - G \geq 0$.

For a point $P \in X$, the local ring of X at P is denoted by $\mathcal{O}_P(X)$. A generator of the unique maximal ideal of $\mathcal{O}_P(X)$ is called a local parameter at P. If t_P is a local parameter at P, then each $f \in k(X)^\times$ has a representation of the form $f = ut_P^n$ for some $n \in \mathbb{Z}$ and $u \in \mathcal{O}_P(X)^\times$. We write $\mathrm{ord}_P(f) := n$ and call $\mathrm{ord}_P(f)$ the order of f at P. We define the divisor

$$\mathrm{div}(f) := \sum \mathrm{ord}_P(f)P.$$

We also define the divisors

$$(f)_0 := \sum_{\mathrm{ord}_P(f)>0} \mathrm{ord}_P(f)P,$$

$$(f)_\infty := \sum_{\mathrm{ord}_P(f)<0} -\mathrm{ord}_P(f)P.$$

Note that the equality

$$\mathrm{div}(f) = (f)_0 - (f)_\infty$$

of divisors holds. Two divisors E, $G \in \mathrm{Div}(X)$ are called linearly equivalent if there exists $f \in k(X)^\times$ such that $E - G = \mathrm{div}(f)$. We write $E \sim G$ if two divisors E, G are linearly equivalent.

For a divisor $D \in \mathrm{Div}(X)$, we define the k-linear space

$$\mathcal{L}(D) = \{f \in k(X)^\times \mid D + \mathrm{div}(f) \geq 0\} \cup \{0\}$$

and we put $\ell(D) := \dim_k(\mathcal{L}(D))$. For two divisors E, $G \in \mathrm{Div}(X)$ such that $E \geq G$, $\mathcal{L}(E) \supset \mathcal{L}(G)$ holds and we have

$$\ell(E) - \ell(G) \leq \deg(E) - \deg(G).$$

If $E \sim G$, then $\deg(D) = \deg(E)$ and $\mathcal{L}(D) \cong \mathcal{L}(E)$.

The complete linear system $|D|$ associated to $D \in \mathrm{Div}(X)$ is defined by

$$|D| = \{E \in \mathrm{Div}(X) \mid E \geq 0, D \sim E\}.$$

Note that $|D|$ is equal to

$$\{D + \mathrm{div}(f) \mid f \in \mathcal{L}(D) \setminus \{0\}\}.$$

Since, for f, $g \in k(X)^\times$, $\mathrm{div}(f) = \mathrm{div}(g)$ if and only if there exists $c \in k^\times$ such that $f = cg$, there exists a bijection

$$|D| \to \mathbb{P}(\mathcal{L}(D)); D + \mathrm{div}(f) \mapsto [f].$$

A linear system Λ on X is a subset of some complete linear system $|D|$ such that

$$\Lambda = \{D + \mathrm{div}(f) \mid f \in V \setminus \{0\}\},$$

where V is a k-linear subspace of $\mathcal{L}(D)$. The integers $\deg(\Lambda) := \deg(D)$ and $\dim(\Lambda) := \dim_k(V) - 1$ are called the degree and (projective) dimension of Λ respectively. A point $P \in X$ is called the base point of Λ if $P \in \bigcap_{E \in \Lambda} \mathrm{supp}(E)$. A linear system is called base-point-free if there is no base point.

Let $\varphi : X \to \mathbb{P}^n$ be a morphism. Assume that φ is non-degenerate, that is, $\varphi(X) \not\subset H$ for each hyperplane $H \subset \mathbb{P}^n$. For a hyperplane $H \subset \mathbb{P}^n$, the divisor on X induced by the intersection of $\varphi(X)$ and H is denoted by $\varphi^* H$. Then

$$\Lambda_\varphi = \{\varphi^* H \mid H \text{ is a hyperplane contained in } \mathbb{P}^n\}$$

is a base-point-free linear system. We consider

$$\mathcal{L} = \{\Lambda \mid \Lambda \text{ is a base-point-free linear system on } X\},$$

$$\mathcal{M} = \{[\varphi] \mid \varphi : X \to \mathbb{P}^n \text{ is a non-degenerate morphism for some } 0 \leq n \in \mathbb{Z}\},$$

where $[\varphi] := \{T \circ \varphi \mid T \in \mathrm{Aut}(\mathbb{P}^n)\}$ represents the projective equivalence class of φ. Then there exists a bijection

$$\mathcal{M} \to \mathcal{L}; [\varphi] \mapsto \Lambda_\varphi.$$

2.2 The Riemann–Hurwitz formula

Let $\varphi : X \to Y$ be a surjective separable morphism of smooth projective curves. We consider $k(Y) \subset k(X)$ by $\varphi^* : k(Y) \to k(X)$. The degree of φ is defined by $\deg(\varphi) = [k(X) : k(Y)]$, where $[k(X) : k(Y)]$ represents the degree of $k(X)/k(Y)$. Let P be a point of X. We put $Q = \varphi(P)$. The ramification index of P over Q is defined by

$$e_P = e_P(\varphi) = e(P|Q) := \mathrm{ord}_P(\varphi^*(t_Q)),$$

where t_Q represents a local parameter at Q. The complementary module over $\mathcal{O}_Q(Y)$ is defined by

$$\mathcal{C}_Q = \{f \in k(X) \mid \mathrm{Tr}_{k(X)/k(Y)}(f \cdot \overline{\mathcal{O}_Q(Y)}) \subset \mathcal{O}_Q(Y)\},$$

where $\overline{\mathcal{O}_Q(Y)}$ is the integral closure of $\mathcal{O}_Q(Y)$ in $k(X)$. The complementary module $\mathcal{C}_Q$ is generated by an element as a $\overline{\mathcal{O}_Q(Y)}$-module. Let t be a generator of $\mathcal{C}_Q$ as a $\overline{\mathcal{O}_Q(Y)}$-module. For a point $P' \in \varphi^{-1}(Q)$, the different exponent of P' over Q is defined by

$$d(P'|Q) = -\mathrm{ord}_{P'}(t).$$

Note that $d(P'|Q) = 0$ holds for all most all $Q \in Y$ and $P' \in \varphi^{-1}(Q)$. In general, $d(P'|Q) \geq e(P'|Q) - 1$ holds, and the equality holds if and only if $e(P'|Q)$ is not divisible by the characteristic p.

Theorem 2.2.1 (Riemann–Hurwitz formula)**.** *If $\varphi : X \to Y$ is a surjective separable morphism of smooth projective curves, then*

$$2g_X - 2 = \deg(\varphi) \cdot (2g_Y - 2) + \sum_{Q \in Y} \sum_{P \in \varphi^{-1}(Q)} d(P|Q),$$

where g_X (resp. g_Y) is the genus of X (resp. Y).

2.3 Galois covering

For a finite subgroup $G \subset \mathrm{Aut}(X)$ and a point $P \in X$, the stabilizer of P in G (resp. the orbit of P under G) is denoted by $G(P)$ (resp. $G \cdot P$). Let $\varphi : X \to Y$ be a Galois covering, that is, φ is a surjective morphism of smooth projective curves and the extension $k(X)/\varphi^* k(Y)$ is a Galois extension. Then the following hold.

Theorem 2.3.1. *Let G be the associated Galois group of φ.*

(1) *If P, $Q \in X$, $\varphi(P) = \varphi(Q)$, then there exists an element $\sigma \in G$ such that $\sigma(P) = Q$. In particular, $G \cdot P = G \cdot Q$.*

(2) *If P, $Q \in X$, $\varphi(P) = \varphi(Q)$, then $e_P(\varphi) = e_Q(\varphi)$.*

(3) *If $P \in X$, then $e_P(\varphi)$ divides $[k(X) : \varphi^* k(Y)]$.*

(4) *If $P \in X$, then the order $|G(P)|$ is equal to $e_P(\varphi)$.*

2.4 Fukasawa's criteria

In 2016, a criterion for the existence of a birational embedding with two Galois points was presented by Fukasawa ([17]). We recall this criterion. For a finite subgroup $G \subset \mathrm{Aut}(X)$, the quotient curve of X by G, that is, the smooth projective curve corresponding to the fixed field of $k(X)$ by G, is denoted by X/G. A morphism $\varphi : X \to \mathbb{P}^2$, which is birational onto $\varphi(X)$, is called a birational embedding of X to $\mathbb{P}^2$. The cardinality of a set S is denoted by $|S|$.

Theorem 2.4.1 ([17], Theorem 1)**.** *Let G_1, G_2 be finite subgroups of* $\mathrm{Aut}(X)$ *and let P_1, P_2 be different points of X. Then the three conditions*

(a) $X/G_1 \cong \mathbb{P}^1$, $X/G_2 \cong \mathbb{P}^1$,

(b) $G_1 \cap G_2 = \{1\}$, *and*

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

are satisfied, if and only if there exists a birational embedding $\varphi : X \to \mathbb{P}^2$ of degree $|G_1| + 1$ such that $\varphi(P_1)$ and $\varphi(P_2)$ are different smooth Galois points for $\varphi(X)$ and $G_{\varphi(P_i)} = G_i$ for $i = 1, 2$.

Theorem 2.4.2 ([17], Theorem 1 and Remark 1)**.** *Let G_1, G_2 be finite subgroups of* $\mathrm{Aut}(X)$ *and let $Q \in X$. Then the three conditions*

(a) $X/G_1 \cong \mathbb{P}^1$, $X/G_2 \cong \mathbb{P}^1$,

(b) $G_1 \cap G_2 = \{1\}$, *and*

(c) $\sum_{\sigma \in G_1} \sigma(Q) = \sum_{\tau \in G_2} \tau(Q)$

are satisfied, if and only if there exists a birational embedding $\varphi : X \to \mathbb{P}^2$ of degree $|G_1|$ and different outer Galois points P_1, $P_2 \in \mathbb{P}^2 \setminus \varphi(X)$ exist for $\varphi(X)$ such that $G_{P_i} = G_i$ for $i = 1, 2$ and points $\varphi(Q)$, P_1, and P_2 are collinear.

Chapter 3

A birational embedding with two Galois points for quotient curves

Some known examples of plane curves with two Galois points are regarded as quotient curves X/H of curves X with a subgroup $H \subset \mathrm{Aut}(X)$ such that X admits a birational embedding with two Galois points. Typical examples are quotient curves of the Hermitian curve ([22, 36]), and the Hermitian curve as a Galois subcover of the Giulietti–Korchmáros curve ([18, 23]). Quotient curves are important in the study of maximal curves with respect to the Hasse–Weil bound (see, for example, [27, 28, 29, 30, 31]). Motivated by this observation, the aim of this chapter is to present a criterion for the existence of a plane model with two Galois points for quotient curves.

3.1 Main theorems

Let X be a (reduced, irreducible) smooth projective curve over k. For a finite subgroup H of $\mathrm{Aut}(X)$ and a point $Q \in X$, the quotient map is denoted by $f_H : X \to X/H$ and the image $f_H(Q)$ is denoted by $\overline{Q}$. Assume that H is a normal subgroup of a subgroup $G \subset \mathrm{Aut}(X)$. Then it follows that for each $\sigma \in G$, the pullback $\sigma^* : k(X) \to k(X)$ satisfies $\sigma^*(k(X)^H) = k(X)^H$. Therefore, there exists a natural homomorphism

$$G \to \mathrm{Aut}(X/H); \sigma \mapsto \overline{\sigma},$$

where $\overline{\sigma}$ corresponds to the restriction $\sigma^* \mid_{k(X)^H}$. The image is denoted by $\overline{G}$, which is isomorphic to G/H. The following two theorems are our main results.

Theorem 3.1.1. *Let H, G_1, $G_2 \subset \mathrm{Aut}(X)$ be finite subgroups with $H \lhd G_i$ for $i = 1, 2$, and let P_1, $P_2 \in X$. Then the four conditions*

(a') $X/G_1 \cong \mathbb{P}^1$, $X/G_2 \cong \mathbb{P}^1$,

(b') $G_1 \cap G_2 = H$,

(c') $\sum_{h \in H} h(P_1) + \sum_{\sigma \in G_1} \sigma(P_2) = \sum_{h \in H} h(P_2) + \sum_{\tau \in G_2} \tau(P_1)$, *and*

(d') $H \cdot P_1 \neq H \cdot P_2$

are satisfied, if and only if there exists a birational embedding $\varphi : X/H \to \mathbb{P}^2$ of degree $|G_1/H| + 1$ such that $\varphi(\overline{P_1})$ and $\varphi(\overline{P_2})$ are different smooth Galois points for $\varphi(X/H)$ and $G_{\varphi(\overline{P_i})} = \overline{G_i}$ for $i = 1, 2$.

Theorem 3.1.2. *Let H, G_1, $G_2 \subset \mathrm{Aut}(X)$ be finite subgroups with $H \lhd G_i$ for $i = 1, 2$, and let $Q \in X$. Then the three conditions*

(a') $X/G_1 \cong \mathbb{P}^1$, $X/G_2 \cong \mathbb{P}^1$,

(b') $G_1 \cap G_2 = H$, *and*

(c') $\sum_{\sigma \in G_1} \sigma(Q) = \sum_{\tau \in G_2} \tau(Q)$

are satisfied, if and only if there exists a birational embedding $\varphi : X/H \to \mathbb{P}^2$ of degree $|G_1/H|$ and different outer Galois points P_1, $P_2 \in \mathbb{P}^2 \setminus \varphi(X/H)$ exist for $\varphi(X/H)$ such that $G_{P_i} = \overline{G_i}$ for $i = 1, 2$ and points $\varphi(\overline{Q})$, P_1, and P_2 are collinear.

As an application, for the case where X admits a birational embedding with two Galois points, the following two results hold.

Corollary 3.1.3. *Let G_1, G_2, H be finite subgroups of $\mathrm{Aut}(X)$, and let P_1, P_2 be different points of X. Assume that the three conditions*

(a) $X/G_1 \cong \mathbb{P}^1$, $X/G_2 \cong \mathbb{P}^1$,

(b) $G_1 \cap G_2 = \{1\}$, *and*

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

are satisfied. If the three conditions

(d) $H \cap G_1 G_2 = \{1\}$,

(e) $HG_1 = H \rtimes G_1$, $HG_2 = H \rtimes G_2$, *and*

(f) $H \cdot P_1 \neq H \cdot P_2$

are satisfied, then there exists a birational embedding $\psi : X/H \to \mathbb{P}^2$ *of degree* $|G_1| + 1$ *such that* $\psi(\overline{P_1})$ *and* $\psi(\overline{P_2})$ *are different smooth Galois points for* $\psi(X/H)$ *and* $G_{\psi(\overline{P_i})} \cong G_i$ *for* $i = 1, 2$.

Corollary 3.1.4. *Let* G_1, G_2, H *be finite subgroups of* $\mathrm{Aut}(X)$, *and let* $Q \in X$. *Assume that three conditions*

(a) $X/G_1 \cong \mathbb{P}^1$, $X/G_2 \cong \mathbb{P}^1$,

(b) $G_1 \cap G_2 = \{1\}$, *and*

(c) $\sum_{\sigma \in G_1} \sigma(Q) = \sum_{\tau \in G_2} \tau(Q)$

are satisfied. If the two conditions

(d) $H \cap G_1 G_2 = \{1\}$, *and*

(e) $HG_1 = H \rtimes G_1$, $HG_2 = H \rtimes G_2$

are satisfied, then there exists a birational embedding $\psi : X/H \to \mathbb{P}^2$ *of degree* $|G_1|$ *and different outer Galois points* P_1, $P_2 \in \mathbb{P}^2 \setminus \psi(X/H)$ *exist for* $\psi(X/H)$ *such that* $G_{P_i} \cong G_i$ *for* $i = 1, 2$ *and points* $\psi(\overline{Q})$, P_1, *and* P_2 *are collinear.*

3.2 Proofs of the main theorems

Proof of Theorem 3.1.1. We consider the 'only if' part. Assume that conditions (a'), (b'), (c'), and (d') of Theorem 3.1.1 are satisfied. By condition (d'), $\overline{P_1} \neq \overline{P_2}$. We would like to prove that conditions (a), (b), and (c) of Theorem 2.4.1 are satisfied for the 4-tuple $(\overline{G_1}, \overline{G_2}, \overline{P_1}, \overline{P_2})$. Since

$$k(X/H)^{\overline{G_i}} = k(X)^{G_i},$$

by condition (a'), the fixed field $k(X/H)^{\overline{G_i}}$ is rational. It follows from condition (b') that $\overline{G_1} \cap \overline{G_2} = \{1\}$. Therefore, conditions (a) and (b) for the 4-tuple $(\overline{G_1}, \overline{G_2}, \overline{P_1}, \overline{P_2})$ are satisfied. Since

$$\sum_{\sigma \in G_1} \sigma(P_2) = \sum_{H\sigma \in G_1/H} \sum_{h \in H} h\sigma(P_2),$$

it follows that

$$(f_H)_* \left(\sum_{\sigma \in G_1} \sigma(P_2) \right) = \sum_{H\sigma \in G_1/H} |H| \cdot \overline{\sigma(P_2)} = |H| \sum_{\overline{\sigma} \in \overline{G_1}} \overline{\sigma}(\overline{P_2}),$$

where $(f_H)_* : \mathrm{Div}(X) \to \mathrm{Div}(X/H)$ is a homomorphism such that

$$(f_H)_* \left(\sum n_i P_i \right) = \sum n_i f_H(P_i)$$

for any divisor $\sum n_i P_i$ on X ([32, IV, Exercise 2.6]). On the other hand,

$$(f_H)_* \left(\sum_{h \in H} h(P_1) \right) = |H| \overline{P_1}.$$

It follows from condition (c') that

$$|H| \left(\overline{P_1} + \sum_{\overline{\sigma} \in \overline{G_1}} \overline{\sigma}(\overline{P_2}) \right) = |H| \left(\overline{P_2} + \sum_{\overline{\tau} \in \overline{G_2}} \overline{\tau}(\overline{P_1}) \right).$$

Since $|H| \cdot D = 0$ implies $D = 0$ for any divisor D, we are able to cut the multiplier $|H|$. Condition (c) for the 4-tuple $(\overline{G_1}, \overline{G_2}, \overline{P_1}, \overline{P_2})$ is satisfied.

We consider the 'if' part. By Theorem 2.4.1, we have that conditions (a), (b), and (c) of Theorem 2.4.1 are satisfied for the 4-tuple $(\overline{G_1}, \overline{G_2}, \overline{P_1}, \overline{P_2})$. Since $k(X)^{G_i} = k(X/H)^{\overline{G_i}}$, by condition (a), the fixed field $k(X)^{G_i}$ is rational. Condition (a') is satisfied. Since $\overline{G_1} \cap \overline{G_2} = \{1\}$, condition (b') is satisfied. Since $\varphi(\overline{P_1}) \neq \varphi(\overline{P_2})$, condition (d') is satisfied. By condition (c),

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

Since $(f_H)^*(\overline{Q}) = \sum_{h\in H} h(Q)$ for each $Q \in X$, where $(f_H)^*$ denotes the pullback, by Theorem 2.3.1,

$$\begin{aligned}(f_H)^*\left(\overline{P_1} + \sum_{\overline{\sigma}\in\overline{G_1}} \overline{\sigma}(\overline{P_2})\right) &= (f_H)^*(\overline{P_1}) + \sum_{\overline{\sigma}\in\overline{G_1}} (f_H)^*(\overline{\sigma}(\overline{P_2})) \\ &= \sum_{h\in H} h(P_1) + \sum_{H\sigma\in G_1/H} \sum_{h\in H} h\sigma(P_2) \\ &= \sum_{h\in H} h(P_1) + \sum_{\sigma\in G_1} \sigma(P_2).\end{aligned}$$

Similarly,

$$(f_H)^*\left(\overline{P_2} + \sum_{\overline{\tau}\in\overline{G_2}} \overline{\tau}(\overline{P_1})\right) = \sum_{h\in H} h(P_2) + \sum_{\tau\in G_2} \tau(P_1).$$

Condition (c') is satisfied. □

Proof of Theorem 3.1.2. We consider the 'only if' part. Assume that conditions (a'), (b'), and (c') of Theorem 3.1.2 are satisfied. We would like to prove that conditions (a), (b), and (c) of Theorem 2.4.2 are satisfied for the triple $(\overline{G_1}, \overline{G_2}, \overline{Q})$. Since

$$k(X/H)^{\overline{G_i}} = k(X)^{G_i},$$

by condition (a'), the fixed field $k(X/H)^{\overline{G_i}}$ is rational. It follows from condition (b') that $\overline{G_1} \cap \overline{G_2} = \{1\}$. Therefore, conditions (a) and (b) for the triple $(\overline{G_1}, \overline{G_2}, \overline{Q})$ are satisfied. Since

$$\sum_{\sigma\in G_1} \sigma(Q) = \sum_{H\sigma\in G_1/H} \sum_{h\in H} h\sigma(Q),$$

it follows that

$$(f_H)_*\left(\sum_{\sigma\in G_1} \sigma(Q)\right) = \sum_{H\sigma\in G_1/H} |H| \cdot \overline{\sigma(Q)} = |H| \sum_{\overline{\sigma}\in\overline{G_1}} \overline{\sigma}(\overline{Q}).$$

It follows from condition (c') that

$$|H|\left(\sum_{\overline{\sigma}\in\overline{G_1}} \overline{\sigma}(\overline{Q})\right) = |H|\left(\sum_{\overline{\tau}\in\overline{G_2}} \overline{\tau}(\overline{Q})\right).$$

Since $|H| \cdot D = 0$ implies $D = 0$ for any divisor D, we are able to cut the multiplier $|H|$. Condition (c) for the triple $(\overline{G_1}, \overline{G_2}, \overline{Q})$ is satisfied.

We consider the 'if' part. By Theorem 2.4.2, we have that conditions (a), (b), and (c) of Theorem 2.4.2 are satisfied for the triple $(\overline{G_1}, \overline{G_2}, \overline{Q})$. Since $k(X)^{G_i} = k(X/H)^{\overline{G_i}}$, by condition (a), the fixed field $k(X)^{G_i}$ is rational. Condition (a') is satisfied. Since $\overline{G_1} \cap \overline{G_2} = \{1\}$, condition (b') is satisfied. By condition (c),

$$\sum_{\overline{\sigma} \in \overline{G_1}} \overline{\sigma}(\overline{Q}) = \sum_{\overline{\tau} \in \overline{G_2}} \overline{\tau}(\overline{Q}).$$

Since $(f_H)^*(\overline{Q}) = \sum_{h \in H} h(Q)$ for each $Q \in X$ by Theorem 2.3.1,

$$\begin{aligned} (f_H)^* \left(\sum_{\overline{\sigma} \in \overline{G_1}} \overline{\sigma}(\overline{Q}) \right) &= \sum_{\overline{\sigma} \in \overline{G_1}} (f_H)^*(\overline{\sigma}(\overline{Q})) \\ &= \sum_{H\sigma \in G_1/H} \sum_{h \in H} h\sigma(Q) \\ &= \sum_{\sigma \in G_1} \sigma(Q). \end{aligned}$$

Similarly,

$$(f_H)^* \left(\sum_{\overline{\tau} \in \overline{G_2}} \overline{\tau}(\overline{Q}) \right) = \sum_{\tau \in G_2} \tau(Q).$$

Condition (c') is satisfied. □

Proof of Corollary 3.1.3. By condition (d), $H \cap G_i = \{1\}$ for $i = 1, 2$. By condition (e), $HG_i = H \rtimes G_i$. Let $\hat{G}_i = H \rtimes G_i$ for $i = 1, 2$. Note that $H \triangleleft \hat{G}_i$ for $i = 1, 2$. We would like to prove that conditions (a'), (b'), (c'), and (d') of Theorem 3.1.1 are satisfied for the 5-tuple $(\hat{G}_1, \hat{G}_2, H, P_1, P_2)$. Condition (f) is the same as condition (d'). Since $k(X)^{\hat{G}_i} \subset k(X)^{G_i}$, by condition (a) and Lüroth's theorem, it follows that $X/\hat{G}_i \cong \mathbb{P}^1$. Condition (a') is satisfied.

Let $\eta \in \hat{G}_1 \cap \hat{G}_2$. Then there exist $h_1, h_2 \in H$, $\sigma \in G_1$, and $\tau \in G_2$ such that $\eta = h_1\sigma = h_2\tau$. Then $\sigma\tau^{-1} = h_1^{-1}h_2 \in H$. By condition (d), $\sigma\tau^1 = 1$ and hence, $\sigma = \tau \in G_1 \cap G_2$. By condition (b), $\sigma = \tau = 1$. This implies that $\eta \in H$. It follows that $\hat{G}_1 \cap \hat{G}_2 = H$. Condition (b') is satisfied.

By condition (c), it follows that

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

For each $h \in H$,

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

Therefore,

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

Since each element of $\hat{G}_1$ (resp. of $\hat{G}_2$) is represented uniquely as $h\sigma$ (resp. $h\tau$) for some $h \in H$ and $\sigma \in G_1$ (resp. $\tau \in G_2$), condition (c') is satisfied. □

Proof of Corollary 3.1.4. Similarly to the proof of Corollary 3.1.3, we prove that conditions (a'), (b'), and (c') of Theorem 3.1.2 are satisfied for the 4-tuple $(\hat{G}_1, \hat{G}_2, H, Q)$, where $\hat{G}_i = H \rtimes G_i$ for $i = 1, 2$. The proof for conditions (a') and (b') is the same as the proof of Corollary 3.1.3. By condition (c), it follows that

$$\sum_{\sigma \in G_1} \sigma(Q) = \sum_{\tau \in G_2} \tau(Q).$$

For each $h \in H$,

$$\sum_{\sigma \in G_1} h\sigma(Q) = \sum_{\tau \in G_2} h\tau(Q).$$

Therefore,

$$\sum_{h \in H} \sum_{\sigma \in G_1} h\sigma(Q) = \sum_{h \in H} \sum_{\tau \in G_2} h\tau(Q).$$

Since each element of $\hat{G}_1$ (resp. of $\hat{G}_2$) is represented uniquely as $h\sigma$ (resp. $h\tau$) for some $h \in H$ and $\sigma \in G_1$ (resp. $\tau \in G_2$), condition (c') is satisfied. □

3.3 An application to cyclic subcovers of the GK curve

In this section, we apply Corollary 3.1.3 to the Giulietti–Korchmáros curve. Theorem 3.3.1 provide new examples of plane curves with two Galois points (see the Table in [50]).

Let $p > 0$ and let q be a power of p. We consider the Giulietti–Korchmáros curve $\widetilde{\mathcal{H}} \subset \mathbb{P}^3$, which is defined by

$$x^q + x - y^{q+1} = 0 \quad \text{and} \quad y((x^q + x)^{q-1} - 1) - z^{q^2-q+1} = 0$$

(see [28]). The group

$$G_1 := \left\{ \left[\begin{array}{cccc} 1 & b^q & 0 & a \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right] \;\middle|\; a, b \in \mathbb{F}_{q^2}, a^q + a - b^{q+1} = 0 \right\} \subset \mathrm{PGL}(4, k)$$

of order q^3 acts on $\widetilde{\mathcal{H}}$ (see [28, Lemma 7]). This group acts on the set

$$\widetilde{\mathcal{H}} \cap \{Z = 0\} = \widetilde{\mathcal{H}}(\mathbb{F}_{q^2})$$

of all $\mathbb{F}_{q^2}$-rational points of $\widetilde{\mathcal{H}}$, and fixes a point $P_1 := (1 : 0 : 0 : 0) \in \widetilde{\mathcal{H}}$. Let

$$\xi(x, y, z) = \left(\frac{1}{x}, -\frac{y}{x}, \frac{z}{x} \right).$$

Then ξ acts on $\widetilde{\mathcal{H}}$ ([28, Lemma 7])). This automorphism acts on $\widetilde{\mathcal{H}}(\mathbb{F}_{q^2})$, and $P_2 := \xi(P_1) = (0 : 0 : 0 : 1)$. Let $G_2 := \xi G_1 \xi^{-1}$, which fixes P_2. According to Theorem 5.1.2 in Chapter 5 (or [23, Theorem 2]), conditions (a), (b), and (c) of Theorem 2.4.1 are satisfied for the 4-tuple (G_1, G_2, P_1, P_2).

It follows from [28, Equation (9)] that the cyclic group

$$C_{q^2-q+1} := \{(x, y, z) \mapsto (x, y, \zeta z) \mid \zeta^{q^2-q+1} = 1\}$$

acts on $\widetilde{\mathcal{H}}$. We prove the following.

Theorem 3.3.1. *Let H be a subgroup of C_{q^2-q+1}. Then there exists a birational embedding $\psi : \widetilde{\mathcal{H}}/H \to \mathbb{P}^2$ of degree $q^3 + 1$ with two smooth Galois points.*

Proof. Note that H fixes all points of $\widetilde{\mathcal{H}}(\mathbb{F}_{q^2})$ $(= \widetilde{\mathcal{H}} \cap \{Z = 0\})$. Therefore, $H \cdot P_1 = \{P_1\} \neq \{P_2\} = H \cdot P_2$. Since $\sigma \mid_{\widetilde{\mathcal{H}}(\mathbb{F}_{q^2})} \neq \tau \mid_{\widetilde{\mathcal{H}}(\mathbb{F}_{q^2})}$ for any $\sigma \in G_1 \setminus \{1\}$ and $\tau \in G_2 \setminus \{1\}$, $H \cap G_1 G_2 = \{1\}$ follows. It is easily verified that $HG_1 = H \times G_1$. Since $\xi h = h \xi$ for each element $h \in H$, $HG_2 = H \times G_2$ follows. Therefore, conditions (d), (e), and (f) of Corollary 3.1.3 are satisfied for the 5-tuple (G_1, G_2, P_1, P_2, H). By Corollary 3.1.3, the assertion follows. $\square$

3.4 The curves constructed by Skabelund and their quotient curves

In this section, we apply Corollary 3.1.3 to the curves constructed by Skabelund. Theorems 3.4.1, 3.4.2, and 3.4.3 also provide new examples of plane curves with two Galois points (see the Table in [50]).

We consider the cyclic cover $\widetilde{\mathcal{S}}$ of the Suzuki curve $\mathcal{S}$, constructed by Skabelund ([42]). Let $p = 2$, let q_0 be a power of 2, and let $q = 2q_0^2$. The curve $\widetilde{\mathcal{S}}$ is the smooth model of the curve defined by

$$y^q + y = x^{q_0}(x^q + x) \quad \text{and} \quad x^q + x = z^{q-2q_0+1}$$

in $\mathbb{P}^3$. Let $P_1 \in \widetilde{\mathcal{S}}$ be the pole of x. It is known that the group

$$G_1 := \left\{ \left[\begin{array}{cccc} 1 & 0 & 0 & a \\ a^{q_0} & 1 & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right] \middle| \, a, b \in \mathbb{F}_q \right\} \subset \mathrm{PGL}(4, k)$$

of order q^2 acts on $\widetilde{\mathcal{S}}$ (see [42, Lemma 3.3], [29, Section 2]). This group acts on the set $\widetilde{\mathcal{S}}(\mathbb{F}_q)$ of all $\mathbb{F}_q$-rational points of $\widetilde{\mathcal{S}}$, and fixes P_1. Let $\alpha := y^{2^{q_0}} + x^{2q_0+1}$, $\beta := xy^{2q_0} + \alpha^{2q_0}$ and let

$$\xi(x, y, z) = \left(\frac{\alpha}{\beta}, \frac{y}{\beta}, \frac{z}{\beta} \right).$$

Then ξ acts on $\widetilde{\mathcal{S}}$ (see [42, Proofs of Lemma 3.3 and 3.4], [29, Section 2]). This automorphism acts on $\widetilde{\mathcal{S}}(\mathbb{F}_q)$, and $P_2 := \xi(P_1) = (0 : 0 : 0 : 1)$ (see [42, Proofs of Lemma 3.3 and 3.4], [29, Section 2]). Let $G_2 := \xi G_1 \xi^{-1}$, which fixes P_2. Then we have the following.

Theorem 3.4.1. *The curve $\widetilde{\mathcal{S}}$ admits a plane model of degree $q^2 + 1$ with two smooth Galois points.*

Proof. We prove that conditions (a), (b), and (c) of Theorem 2.4.1 are satisfied for the 4-tuple (G_1, G_2, P_1, P_2). It is not difficult to check that $k(\widetilde{\mathcal{S}})^{G_1} = k(z)$ and $k(\widetilde{\mathcal{S}})^{G_2} = k(z/\beta)$. Since no nontrivial element of G_1 fixes

P_2, $G_1 \cap G_2 = \{1\}$. Conditions (a) and (b) are satisfied. Condition (c) is satisfied, since

$$P_1 + \sum_{\sigma \in G_1} \sigma(P_2) = \sum_{Q \in \widetilde{\mathcal{S}}(\mathbb{F}_q)} Q = P_2 + \sum_{\tau \in G_2} \tau(P_1).$$

□

It follows from the shape of the second equation that the cyclic group

$$C_{q-2q_0+1} := \{(x, y, z) \mapsto (x, y, \zeta z) \mid \zeta^{q-2q_0+1} = 1\}$$

acts on $\widetilde{\mathcal{S}}$. Similarly to the proof of Theorem 3.3.1, the following holds.

Theorem 3.4.2. *Let H be a subgroup of C_{q-2q_0+1}. Then there exists a birational embedding $\psi : \widetilde{\mathcal{S}}/H \to \mathbb{P}^2$ of degree q^2+1 with two smooth Galois points.*

We consider the cyclic cover $\widetilde{\mathcal{R}}$ of the Ree curve $\mathcal{R}$, constructed by Skabelund. Let $p = 3$, let q_0 be a power of 3, and let $q = 3q_0^2$. The curve $\widetilde{\mathcal{R}}$ is the smooth model of the curve defined by

$$y^q - y = x^{q_0}(x^q - x),\ z^q - z = x^{2q_0}(x^q - x) \text{ and } x^q - x = t^{q-3q_0+1}.$$

Let $P_1 \in \widetilde{\mathcal{R}}$ be the pole of x. It is known that the group

$$G_1 := \left\{ \left[\begin{array}{ccccc} 1 & 0 & 0 & 0 & a \\ a^{q_0} & 1 & 0 & 0 & b \\ a^{2q_0} & -a^{q_0} & 1 & 0 & c \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array} \right] \middle| \, a, b, c \in \mathbb{F}_q \right\} \subset \mathrm{PGL}(5, k)$$

of order q^3 acts on $\widetilde{\mathcal{R}}$ (see [42, Lemma 4.2], [29, Section 2]). This group acts on the set $\widetilde{\mathcal{R}}(\mathbb{F}_q)$ of all $\mathbb{F}_q$-rational points of $\widetilde{\mathcal{R}}$, and fixes P_1. There exists an involution ξ of $\widetilde{\mathcal{R}}$ such that ξ acts on $\widetilde{\mathcal{R}}(\mathbb{F}_q)$ and $P_2 := \xi(P_1) = (0:0:0:0:1)$ (see [42, Proofs of Lemma 4.2 and 4.3], [29, Section 2]). Let $G_2 := \xi G_1 \xi^{-1}$, which fixes P_2.

It follows from the shape of the third equation that the cyclic group

$$C_{q-3q_0+1} := \{(x, y, z, t) \mapsto (x, y, z, \zeta t) \mid \zeta^{q-3q_0+1} = 1\}$$

acts on $\widetilde{\mathcal{R}}$. Similarly to Theorem 3.4.1 and 3.4.2, the following holds.

Theorem 3.4.3. *Let H be a subgroup of C_{q-3q_0+1}. Then the curves $\widetilde{\mathcal{R}}$ and $\widetilde{\mathcal{R}}/H$ admit plane models of degree q^3+1 with two smooth Galois points.*

3.5 Relations with the previous works

In this section, we discuss the relation between Corollaries 3.1.3, 3.1.4 and the previous works.

We can provide another proof of Theorems 1 and 2 in [22], by Corollaries 3.1.3, 3.1.4 and the analysis of the Hermitian curve $\mathcal{H} \subset \mathbb{P}^2 : x^q + x = y^{q+1}$. We recover Theorem 1(1) in [22] here. Precisely:

Theorem 3.5.1 ([22], Theorem 1(1))**.** *Let a positive integer m divide $q+1$. Then the smooth model of the curve $y^m = x^q + x$ possesses a birational embedding into $\mathbb{P}^2$ of degree $q+1$ with two smooth Galois points.*

Proof. Let $P_1 = (1:0:0)$ and $P_2 = (0:0:1) \in \mathbb{P}^2$. Then P_1 and P_2 are smooth Galois points for the Hermitian curve $\mathcal{H} \subset \mathbb{P}^2$ ([36]). The associated Galois groups at P_1, P_2 are represented by

$$G_1 := \left\{ \begin{bmatrix} 1 & 0 & \alpha \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \;\middle|\; \alpha^q + \alpha = 0 \right\}, G_2 := \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha & 0 & 1 \end{bmatrix} \;\middle|\; \alpha^q + \alpha = 0 \right\}$$

respectively. Then conditions (a), (b), and (c) of Theorem 2.4.1 are satisfied for the 4-tuple (G_1, G_2, P_1, P_2). Let $sm = q+1$ and let C_s be a cyclic group of order s generated by the automorphism $(x, y) \mapsto (x, \zeta y)$, where ζ is a primitive s-th root of unity. Note that C_s fixes all points in the line $Y = 0$. Therefore, $C_s \cdot P_1 = \{P_1\} \neq \{P_2\} = C_s \cdot P_2$. It is easily verified that $C_s \cap G_1 G_2 = \{1\}$ and $C_s G_i = C_s \times G_i$. Conditions (d), (e), and (f) of Corollary 3.1.3 are satisfied. By Corollary 3.1.3, the quotient curve $\mathcal{H}/C_s$ has a birational embedding of degree $q+1$ with two smooth Galois points. On the other hand, the quotient curve $\mathcal{H}/C_s$ has a plane model defined by $y^m = x^q + x$. □

A similar argument is applicable to the curve $C \subset \mathbb{P}^2$ defined by $x^3 + y^4 + 1 = 0$, which has two smooth Galois points $P_1 = (1:0:0)$ and $P_2 = (-1:0:1)$ on the line $Y = 0$ (under the assumption $p \neq 2, 3$), by taking $H = \langle \eta \rangle$ with $\eta(x, y) = (x, -y)$ (see [37, 41, 47]). Here, the associated Galois groups G_1, G_2 at P_1, P_2 are generated by matrices

$$\begin{bmatrix} \omega & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} \frac{-\omega}{-\omega+1} & 0 & \frac{2}{-\omega+1} \\ 0 & 1 & 0 \\ \frac{1}{-\omega+1} & 0 & \frac{\omega^2}{-\omega+1} \end{bmatrix}$$

respectively, where $\omega^2 + \omega + 1 = 0$ (see [37, Lemma 1] for the explicit description of the generators). Then the quotient curve C/H is the elliptic curve $y^2 + x^3 + 1 = 0$. It is well known that this curve is isomorphic to the Fermat curve. (An elliptic curve E admitting a triple Galois covering $E \to \mathbb{P}^1$ is uniquely determined [32, IV, Corollary 4.7]. One proof is given in [17, p.100].) Since the Galois group G_i at P_i fixes P_i, the group $\overline{G_i} := \overline{HG_i}$ fixes $\overline{P_i}$ for $i = 1, 2$. Then the point $\overline{P_i}$ is a ramification point of index $e_{\overline{P_i}} = |\overline{G_i}| = 3$ for the covering $C/H \to (C/H)/\overline{G_i}$ by Theorem 2.3.1. Let ψ be the induced birational embedding, according to Corollary 3.1.3. Then $\psi(\overline{P_i})$ is a smooth Galois point for $\psi(C/H) \subset \mathbb{P}^2$. Since

$$e_{\overline{P_i}} + 1 = I_{\psi(\overline{P_i})}(\psi(C/H), T_{\psi(\overline{P_i})}\psi(C/H))$$

for the projection from $\psi(\overline{P_i})$, where $I_{\psi(\overline{P_i})}(\psi(C/H), T_{\psi(\overline{P_i})}\psi(C/H))$ is the intersection multiplicity of $\psi(C/H)$ and the tangent line $T_{\psi(\overline{P_i})}\psi(C/H)$ of $\psi(C/H)$ at $\psi(\overline{P_i})$, it follows that $\psi(\overline{P_i})$ is a total inflection point. The following result is similar to [17, Theorem 3], but the proofs are different.

Theorem 3.5.2. *Let $p \neq 2, 3$. For the cubic Fermat curve, there exists a plane model of degree four with two smooth Galois points such that they are total inflection points.*

Chapter 4

A criterion for the existence of a plane model with two inner Galois points for algebraic curves

In 2016, Fukasawa [17] presented a criterion for the existence of a birational embedding of a smooth projective curve into a projective plane with two smooth Galois points and obtained new examples of plane curves with two smooth Galois points by using this criterion. On the other hand, there have been some known examples of plane curves with two or more non-smooth Galois points. For example, the Ballico–Hefez curve ([13, Theorem 1]), some self-dual curves ([33, Theorem 17]), the (plane model of) Giulietti–Korchmáros curve ([23, Theorem 2]), the (q^3, q^2)-Frobenius nonclassical curve ([2, Theorem 1]), and the Artin–Schreier–Mumford curve (proof of [19, Theorem 1]) are such curves. However, these examples are not intended to focus actively on non-smooth Galois points. Takahashi [45] studied plane quintic curves with a double point P and determined defining equations when P is a Galois point. As far as the author knows, This is the only study that focused on a non-smooth Galois point so far. To study non-smooth Galois points systematically, it is good to have a criterion for non-smooth Galois points. In this chapter, we extend Fukasawa's criterion [17, Theorem 1] to all cases with two (possibly non-smooth) Galois points.

4.1 Main theorems

Let X be a (reduced, irreducible) smooth projective curve over k. The following are our main theorems.

Theorem 4.1.1. *Let G_1, G_2 be finite subgroups of $\mathrm{Aut}(X)$ and let P_1, P_2 be different points of X. Then there exists a birational embedding $\varphi : X \to \mathbb{P}^2$ such that $\varphi(P_1)$, $\varphi(P_2)$ are different inner Galois points, that $G_{\varphi(P_i)} = G_i$ for $i = 1, 2$, and that $L = \overline{\varphi(P_1)\varphi(P_2)}$ is not a tangent line at $\varphi(P_1)$, if and only if the following conditions are satisfied:*

(a) $X/G_1 \cong \mathbb{P}^1, X/G_2 \cong \mathbb{P}^1$,

(b) $G_1 \cap G_2 = \{1\}$, *and*

(c) *one of the following holds:*

(c-i) $P_1 \notin G_1 \cdot P_2$, $P_2 \notin G_2 \cdot P_1$, $G_1 \cdot P_2 \cap G_2 \cdot P_1 \neq \emptyset$, *and* $|G_1(P_2)| = |G_2(P_1)|$.

(c-ii) $G_1 \cdot P_2 \cap G_2 \cdot P_1 = \emptyset$.

(c-iii) $P_1 \notin G_1 \cdot P_2$, $G_1 \cdot P_2 \cap G_2 \cdot P_1 \neq \emptyset$ *and* $|G_1(P_2)| > |G_2(P_1)|$.

Furthermore, for any φ as in the above, the following hold:

(i) *L is not a tangent line at $\varphi(P_2)$ with $L \cap \varphi(X) \supsetneq \{\varphi(P_1), \varphi(P_2)\}$ if and only if condition* (c-i) *is satisfied.*

(ii) *L is not a tangent line at $\varphi(P_2)$ with $L \cap \varphi(X) = \{\varphi(P_1), \varphi(P_2)\}$ if and only if condition* (c-ii) *is satisfied.*

(iii) *L is a tangent line at $\varphi(P_2)$ if and only if condition* (c-iii) *is satisfied.*

Theorem 4.1.2. *Let φ be as in Theorem 4.1.1, and let Λ be the linear system on X corresponding to the morphism φ. Let $(0, \alpha_P, \beta_P)$ denote the (Λ, P)-order sequence at a point $P \in X$. Then the following hold.*

(1) *The multiplicity $m_{\varphi(P_1)}$ of $\varphi(X)$ at $\varphi(P_1)$ is equal to*

$$|G_2(P_1)| \cdot |G_2 \cdot P_1 \setminus (G_1 \cdot P_2 \cap G_2 \cdot P_1)|.$$

(2) *The divisor* $\sum_{P\in\varphi^{-1}(\varphi(P_1))}\alpha_P P$ *is equal to*

$$\sum_{Q\in G_2\cdot P_1\setminus(G_1\cdot P_2\cap G_2\cdot P_1)}|G_2(P_1)|Q.$$

(3) *The multiplicity* $m_{\varphi(P_2)}$ *of* $\varphi(X)$ *at* $\varphi(P_2)$ *is equal to*

$$|G_1(P_2)|\cdot|G_1\cdot P_2\setminus(G_1\cdot P_2\cap G_2\cdot P_1)|+(|G_1(P_2)|-|G_2(P_1)|)\cdot|G_1\cdot P_2\cap G_2\cdot P_1|.$$

(4) *The divisor* $\sum_{P\in\varphi^{-1}(\varphi(P_2))}\alpha_P P$ *is equal to*

$$\sum_{R\in G_1\cdot P_2\setminus(G_1\cdot P_2\cap G_2\cdot P_1)}|G_1(P_2)|R+\sum_{S\in G_1\cdot P_2\cap G_2\cdot P_1}(|G_1(P_2)|-|G_2(P_1)|)S.$$

(5) *In the case* (iii) *of Theorem 4.1.1, the equality* $\beta_P=|G_1(P_2)|$ *holds at each point* $P\in G_1\cdot P_2\cap G_2\cdot P_1$.

(6) *The divisor* φ^*L *is equal to*

$$\sum_{Q\in G_2\cdot P_1\setminus(G_1\cdot P_2\cap G_2\cdot P_1)}|G_2(P_1)|Q+\sum_{R\in G_1\cdot P_2}|G_1(P_2)|R.$$

To explain the usefulness of Theorems 4.1.1 and 4.1.2, we apply these theorems to rational curves.

Theorem 4.1.3. *For the projective line* $\mathbb{P}^1$*, there exist the following birational embeddings* $\varphi:\mathbb{P}^1\to\mathbb{P}^2$.

(1) $p=3$, $\deg(\varphi(\mathbb{P}^1))=14$ *and there exist two non-smooth Galois points* $\varphi(P_1)$ *and* $\varphi(P_2)\in\varphi(\mathbb{P}^1)$ *such that* $m_{\varphi(P_1)}=4$, $m_{\varphi(P_2)}=8$, $G_{\varphi(P_1)}\cong\mathbf{D}_5$, $G_{\varphi(P_2)}\cong\mathrm{AGL}(1,\mathbb{F}_3)$, *and* $L=\overline{\varphi(P_1)\varphi(P_2)}$ *is not a tangent line at* $\varphi(P_1)$ *and* $\varphi(P_2)$. *The second order is equal to* 2 *at each point contained in* $\mathrm{supp}(\varphi^*L)$.

(2) $p\neq 2,5$, $\deg(\varphi(\mathbb{P}^1))=16$ *and there exist two non-smooth Galois points* $\varphi(P_1)$ *and* $\varphi(P_2)\in\varphi(\mathbb{P}^1)$ *such that* $m_{\varphi(P_1)}=4$, $m_{\varphi(P_2)}=11$, $G_{\varphi(P_1)}\cong\mathbf{A}_4$, $G_{\varphi(P_2)}\cong\mathbb{Z}/5\mathbb{Z}$, $L=\overline{\varphi(P_1)\varphi(P_2)}$ *is not a tangent line at* $\varphi(P_1)$, *and* L *is a tangent line at* $\varphi(P_2)$. *The second order is equal to* 2 (*resp.* 1) *at each point* $Q\in G_1\cdot P_2\setminus\{P_2\}$ (*resp.* $Q\in G_2\cdot P_1$), *and the third order is equal to* 2 *at* P_2.

(3) $p \neq 2, 5$, $\deg(\varphi(\mathbb{P}^1)) = 28$ *and there exist two non-smooth Galois points* $\varphi(P_1)$ *and* $\varphi(P_2) \in \varphi(\mathbb{P}^1)$ *such that* $m_{\varphi(P_1)} = 4$, $m_{\varphi(P_2)} = 23$, $G_{\varphi(P_1)} \cong \mathbf{S}_4$, $G_{\varphi(P_2)} \cong \mathbb{Z}/5\mathbb{Z}$, $L = \overline{\varphi(P_1)\varphi(P_2)}$ *is not a tangent line at* $\varphi(P_1)$, *and* L *is a tangent line at* $\varphi(P_2)$. *The second order is equal to* 4 (*resp.* 3, 1) *at each point* $Q \in G_1 \cdot P_2 \setminus \{P_2\}$ (*resp. at* P_2, *at each point* $Q \in G_2 \cdot P_1 \setminus \{P_2\}$), *and the third order is equal to* 4 *at* P_2.

4.2 Order sequence and the ramification index of the projection

Let $\varphi : X \to \mathbb{P}^2$ be a birational embedding of X to $\mathbb{P}^2$. Assume that $\varphi(X)$ is not a line. We recall the notion of order sequences (see [35, Chapter 7]). Note that

$$\Lambda = \{\varphi^* L \mid L \text{ is a line contained in } \mathbb{P}^2\}$$

is the linear system on X corresponding to the morphism φ. For a point $P \in X$, we put

$$\alpha_P = \min\{\mathrm{ord}_P(\varphi^* L) \mid \varphi^* L \in \Lambda, P \in \mathrm{supp}(\varphi^* L)\}.$$

Then there exists a unique line $\widetilde{L}$ such that $\beta_P = \mathrm{ord}_P(\varphi^* \widetilde{L}) > \alpha_P$. We call the line $\widetilde{L}$ the osculating line at P, and we call the sequence $(0, \alpha_P, \beta_P)$ the (Λ, P)-order sequence at P. A line $\widetilde{L}$ passing through $\varphi(P)$ is called a tangent line at $\varphi(P)$ if $\widetilde{L}$ is the osculating line at a point contained in $\varphi^{-1}(\varphi(P))$. Note that a line $\widetilde{L}$ is a tangent line at $\varphi(P)$ if and only if $m_{\varphi(P)} < I_{\varphi(P)}(\varphi(X), \widetilde{L})$, where $I_{\varphi(P)}(\varphi(X), \widetilde{L})$ is the intersection multiplicity of $\varphi(X)$ and $\widetilde{L}$ at $\varphi(P)$.

Next, We consider the projection $\pi_{\varphi(P)}$, and we put

$$\hat{\pi}_{\varphi(P)} = \pi_{\varphi(P)} \circ \varphi : X \to \mathbb{P}^1.$$

We recall some properties of a ramification index of $\hat{\pi}_{\varphi(P)}$. We put

$$\varphi^{-1}(\varphi(P)) = \{P_1, \ldots, P_n\}.$$

Let $(0, \alpha_{P_i}, \beta_{P_i})$ be the (Λ, P_i)-order sequence for $i = 1, \ldots, n$. Then the following proposition is well-known.

Proposition 4.2.1. *Let* $Q \in X \setminus \{P_1, \ldots, P_n\}$.

(1) *The equality* $e_Q(\hat{\pi}_{\varphi(P)}) = \mathrm{ord}_Q(\varphi^* \overline{\varphi(P)\varphi(Q)})$ *holds.*

(2) *The equality* $e_{P_i}(\hat{\pi}_{\varphi(P)}) = \beta_{P_i} - \alpha_{P_i}$ *holds for* $i = 1, \ldots, n$.

4.3 Proofs of Theorems 4.1.1 and 4.1.2

Let $\varphi : X \to \mathbb{P}^2$ be a birational embedding. The following lemma shows that Theorem 4.1.1 describes all cases with two inner Galois points.

Lemma 4.3.1. *Let $P_1, P_2 \in X$, and assume that $\varphi(P_1), \varphi(P_2)$ are different inner Galois points. We put $L = \overline{\varphi(P_1)\varphi(P_2)}$. Then either $m_{\varphi(P_1)} = I_{\varphi(P_1)}(\varphi(X), L)$ or $m_{\varphi(P_2)} = I_{\varphi(P_2)}(\varphi(X), L)$ holds.*

Proof. We put

$$\varphi^{-1}(\varphi(P_1)) = \{P_{11} = P_1, P_{12}, \ldots, P_{1n_1}\},$$

$$\varphi^{-1}(\varphi(P_2)) = \{P_{21} = P_2, P_{22}, \ldots, P_{2n_2}\}.$$

Let $(0, \alpha_{P_{ij}}, \beta_{P_{ij}})$ be the (Λ, P_{ij})-order sequence for i, j. Assume by contradiction that

$$m_{\varphi(P_1)} < I_{\varphi(P_1)}(\varphi(X), L),\ m_{\varphi(P_2)} < I_{\varphi(P_2)}(\varphi(X), L)$$

hold. By Theorem 2.3.1, the ramification index of $\hat{\pi}_{\varphi(P_1)}$ (resp. $\hat{\pi}_{\varphi(P_2)}$) at each point contained in $\varphi^{-1}(\varphi(P_2))$ (resp. $\varphi^{-1}(\varphi(P_1))$) coincides with $|G_{\varphi(P_1)}(P_2)|$ (resp. $|G_{\varphi(P_2)}(P_1)|$). By Proposition 4.2.1 (1) and Theorem 2.3.1, $|G_{\varphi(P_1)}(P_2)|$ (resp. $|G_{\varphi(P_2)}(P_1)|$) coincides with $\mathrm{ord}_{P_{2j}}(\varphi^* L)$ for each j (resp. $\mathrm{ord}_{P_{1i}}(\varphi^* L)$ for each i). Since L is a tangent line at $\varphi(P_1)$ (resp. $\varphi(P_2)$), there exists i_0 (resp. j_0) such that

$$\beta_{P_{1i_0}} = \mathrm{ord}_{P_{1i_0}}(\varphi^* L) \text{ (resp. } \beta_{P_{2j_0}} = \mathrm{ord}_{P_{2j_0}}(\varphi^* L)).$$

By Proposition 4.2.1 (2) and Theorem 2.3.1,

$$|G_{\varphi(P_1)}(P_2)| = \beta_{P_{1i_0}} - \alpha_{P_{1i_0}} \text{ (resp. } |G_{\varphi(P_2)}(P_1)| = \beta_{P_{2j_0}} - \alpha_{P_{2j_0}})$$

holds. Therefore, we have a contradiction as follows:

$$\begin{aligned} |G_{\varphi(P_2)}(P_1)| &< |G_{\varphi(P_2)}(P_1)| + \alpha_{P_{2j_0}} = \beta_{P_{2j_0}} = \mathrm{ord}_{P_{2j_0}}(\varphi^* L) = |G_{\varphi(P_1)}(P_2)| \\ &< |G_{\varphi(P_1)}(P_2)| + \alpha_{P_{1i_0}} = \beta_{P_{1i_0}} = \mathrm{ord}_{P_{1i_0}}(\varphi^* L) = |G_{\varphi(P_2)}(P_1)|. \end{aligned}$$

□

Proof of Theorem 4.1.1. We consider the 'if' part. Assume that conditions (a), (b), and (c) in Theorem 4.1.1 are satisfied. Let $f, g \in k(X)$ be the generators of $k(X)^{G_1}, k(X)^{G_2}$ such that

$$(f)_\infty = \sum_{\sigma \in G_1} \sigma(P_2),\ (g)_\infty = \sum_{\tau \in G_2} \tau(P_1),$$

which exist by condition (a), where $(f)_\infty$ (resp. $(g)_\infty$) is the pole divisor of f (resp. g). We consider the morphism $\varphi = (f : g : 1) : X \to \mathbb{P}^2$. First, we show that the equality $\varphi(P_1) = (0 : 1 : 0)$ holds. We put $n_g = \mathrm{ord}_{P_1}((g)_\infty)$. Note that n_g is equal to $|G_2(P_1)|$. Let t_{P_1} be a local parameter at P_1. Since $P_1 \notin G_1 \cdot P_2 = \mathrm{supp}((f)_\infty)$ by condition (c),

$$\mathrm{ord}_{P_1}(t_{P_1}^{n_g} f) = n_g + \mathrm{ord}_{P_1}(f) \geq n_g > 0$$

hold. Therefore, we have the equality $\varphi(P_1) = (0 : 1 : 0)$. We also show that the equality $\varphi(P_2) = (1 : 0 : 0)$ holds. We put $n_f = \mathrm{ord}_{P_2}((f)_\infty)$. Note that n_f is equal to $|G_1(P_2)|$. Let t_{P_2} be a local parameter at P_2. If $P_2 \notin G_2 \cdot P_1 = \mathrm{supp}((g)_\infty)$, we have

$$\mathrm{ord}_{P_2}(t_{P_2}^{n_f} g) = n_f + \mathrm{ord}_{P_2}(g) \geq n_f > 0.$$

If $P_2 \in G_2 \cdot P_1$, then condition (c-iii) is satisfied, and we have

$$\mathrm{ord}_{P_2}(t_{P_2}^{n_f} g) = n_f + \mathrm{ord}_{P_2}(g) = |G_1(P_2)| - |G_2(P_1)| > 0.$$

Therefore, the equality $\varphi(P_2) = (1 : 0 : 0)$ holds. By a method similar to the proof of [17, Proposition 1], by condition (b), we can show that the morphism φ is birational onto its image. The morphism $(f : 1)$ (resp. $(g : 1)$) coincides with the projection from the point $\varphi(P_1) = (0 : 1 : 0)$ (resp. $\varphi(P_2) = (1 : 0 : 0)$). Therefore $\varphi(P_1)$, $\varphi(P_2)$ are different inner Galois points, and $G_{\varphi(P_i)} = G_i$ for $i = 1, 2$. We show that $L = \overline{\varphi(P_1)\varphi(P_2)}$ is not a tangent line at $\varphi(P_1)$. Assume by contradiction that L is a tangent line at $\varphi(P_1)$. Then there exists a point $Q \in \varphi^{-1}(\varphi(P_1))$ such that $Q \in G_1 \cdot P_2$. Let Λ be the linear system on X corresponding to the morphism φ, and let $(0, \alpha_Q, \beta_Q)$ be the (Λ, Q)-order sequence at Q. Since L is the osculating line at Q, we have

$$|G_2(P_1)| = \mathrm{ord}_Q(\varphi^* L) = \beta_Q$$

by Proposition 4.2.1 (1) and Theorem 2.3.1. On the other hand, by Proposition 4.2.1 (2) and Theorem 2.3.1, the equality

$$|G_1(P_2)| = \beta_Q - \alpha_Q$$

holds. Therefore, we have $G_1 \cdot P_2 \cap G_2 \cdot P_1 \neq \emptyset$ and $|G_1(P_2)| < |G_2(P_1)|$. This is a contradiction to condition (c). Therefore, L is not a tangent line at $\varphi(P_1)$.

We consider the 'only if' part. Assume that there exists a birational embedding $\varphi : X \to \mathbb{P}^2$ such that $\varphi(P_1)$, $\varphi(P_2)$ are different inner Galois points, $G_{\varphi(P_i)} = G_i$ for $i = 1, 2$, and $L = \overline{\varphi(P_1)\varphi(P_2)}$ is not a tangent line at $\varphi(P_1)$. Since

$$k(X)^{G_i} = (\hat{\pi}_{\varphi(P_i)})^*(k(\mathbb{P}^1)) \cong k(\mathbb{P}^1)$$

for $i = 1, 2$, condition (a) is satisfied. By a method similar to the proof of [17, Theorem 1], condition (b) is satisfied. Since L is not a tangent line at $\varphi(P_1)$, we have $P_1 \notin G_1 \cdot P_2$. We show condition (c) by dividing into the following three cases (I), (II), and (III).

(I) Assume that L is not a tangent line at $\varphi(P_2)$ and $L \cap \varphi(X) \supsetneq \{\varphi(P_1), \varphi(P_2)\}$. We show that condition (c-i) is satisfied. Since L is not a tangent line at $\varphi(P_2)$ and

$$(L \cap \varphi(X)) \setminus \{\varphi(P_1), \varphi(P_2)\} \neq \emptyset,$$

we have $P_2 \notin G_2 \cdot P_1$ and $G_1 \cdot P_2 \cap G_2 \cdot P_1 \neq \emptyset$. We take a point

$$Q \in \varphi^{-1}((L \cap \varphi(X)) \setminus \{\varphi(P_1), \varphi(P_2)\}).$$

By Proposition 4.2.1 (1) and Theorem 2.3.1, we have the equalities

$$|G_1(P_2)| = \mathrm{ord}_Q(\varphi^* L) = |G_2(P_1)|.$$

Therefore, condition (c-i) is satisfied.

(II) Assume that L is not a tangent line at $\varphi(P_2)$ and $L \cap \varphi(X) = \{\varphi(P_1), \varphi(P_2)\}$. Then $G_1 \cdot P_2 = \varphi^{-1}(\varphi(P_2))$ and $G_2 \cdot P_1 = \varphi^{-1}(\varphi(P_1))$ hold, and we have $G_1 \cdot P_2 \cap G_2 \cdot P_1 = \emptyset$. Therefore, condition (c-ii) is satisfied.

(III) Assume that L is a tangent line at $\varphi(P_2)$. We show that condition (c-iii) is satisfied. Since L is a tangent line at $\varphi(P_2)$, there exists a point $Q \in \varphi^{-1}(\varphi(P_2))$ such that $Q \in G_2 \cdot P_1$. Since $G_1 \cdot P_2 \supset \varphi^{-1}(\varphi(P_2))$, we have $G_1 \cdot P_2 \cap G_2 \cdot P_1 \neq \emptyset$. Let Λ be the linear system on X corresponding to the morphism φ, and let $(0, \alpha_Q, \beta_Q)$ be the (Λ, Q)-order sequence at Q. Since L is the osculating line at Q, we have

$$|G_1(P_2)| = \mathrm{ord}_Q(\varphi^* L) = \beta_Q$$

by Proposition 4.2.1 (1) and Theorem 2.3.1. On the other hand, by Proposition 4.2.1 (2) and Theorem 2.3.1, the equality

$$|G_2(P_1)| = \beta_Q - \alpha_Q$$

holds, and we have $|G_1(P_2)| > |G_2(P_1)|$. Therefore, condition (c-iii) is satisfied.

Finally, we show (i), (ii), and (iii) in Theorem 4.1.1. Let φ be as in Theorem 4.1.1. Then condition (c-i), (c-ii), or (c-iii) is satisfied. Since these conditions are mutually exclusive, it is enough to show 'only if' part of (i), (ii), and (iii) in Theorem 4.1.1. This task has been already done above. □

Proof of Theorem 4.1.2. Let φ be as in Theorem 4.1.1, and let Λ be the linear system on X corresponding to the morphism φ. We put

$$\varphi^{-1}(\varphi(P_1)) = \{P_{11} = P_1, P_{12}, \ldots, P_{1n_1}\},$$
$$\varphi^{-1}(\varphi(P_2)) = \{P_{21} = P_2, P_{22}, \ldots, P_{2n_2}\}.$$

Let $(0, \alpha_{P_{ij}}, \beta_{P_{ij}})$ be the (Λ, P_{ij})-order sequence for i, j.

First, we show Theorem 4.1.2 (1) and (2). Since the linear system corresponding to the morphism $\hat{\pi}_{\varphi(P_1)}$ is

$$\left\{ E - \sum_{i=1}^{n_1} \alpha_{P_{1i}} P_{1i} \;\middle|\; E \in \Lambda, E \geq \sum_{i=1}^{n_1} \alpha_{P_{1i}} P_{1i} \right\}$$

and $\hat{\pi}_{\varphi(P_1)}$ is a Galois covering, the following equalities of divisors hold:

$$\varphi^* L - \sum_{i=1}^{n_1} \alpha_{P_{1i}} P_{1i} = (\hat{\pi}_{\varphi(P_1)})^*([L]) = \sum_{\sigma \in G_1} \sigma(P_2),$$

where $[L]$ represents the divisor of the point $[L] \in \mathbb{P}^1$ corresponding to the line L. By Proposition 4.2.1 (1) and Theorem 2.3.1, the equality $|G_2(P_1)| = \mathrm{ord}_{P_{1i}}(\varphi^* L)$ holds for all i. Since L is not a tangent line at $\varphi(P_1)$, the equality $\alpha_{P_{1i}} = |G_2(P_1)|$ holds for all i. It is not difficult to check that

$$(\varphi^{-1}(\varphi(P_1))) \cup (G_1 \cdot P_2) = \mathrm{supp}(\varphi^* L) = (G_2 \cdot P_1) \cup (G_1 \cdot P_2)$$

hold. Since the intersection of the two sets $\varphi^{-1}(\varphi(P_1))$ and $G_1 \cdot P_2$ is the empty set, we have

$$\begin{aligned} \varphi^{-1}(\varphi(P_1)) &= ((\varphi^{-1}(\varphi(P_1))) \cup (G_1 \cdot P_2)) \setminus (G_1 \cdot P_2) \\ &= G_2 \cdot P_1 \setminus (G_1 \cdot P_2 \cap G_2 \cdot P_1). \end{aligned}$$

Therefore, the equality

$$\sum_{i=1}^{n_1} \alpha_{P_{1i}} P_{1i} = \sum_{Q \in G_2 \cdot P_1 \setminus (G_1 \cdot P_2 \cap G_2 \cdot P_1)} |G_2(P_1)|Q$$

of divisors holds, and we have Theorem 4.1.2 (2). Since

$$m_{\varphi(P_1)} = \sum_{i=1}^{n_1} \alpha_{P_{1i}},$$

we have Theorem 4.1.2 (1).

Next, we show Theorem 4.1.2 (6). By the above, the equality

$$\varphi^* L = \sum_{Q \in G_2 \cdot P_1 \setminus (G_1 \cdot P_2 \cap G_2 \cdot P_1)} |G_2(P_1)|Q + \sum_{\sigma \in G_1} \sigma(P_2)$$

holds. Since

$$\sum_{\sigma \in G_1} \sigma(P_2) = \sum_{R \in G_1 \cdot P_2} |G_1(P_2)|R,$$

we have Theorem 4.1.2 (6).

Finally, we show Theorem 4.1.2 (3), (4), and (5). Since

$$\sum_{\tau \in G_2} \tau(P_1) = \sum_{S \in G_1 \cdot P_2 \cap G_2 \cdot P_1} |G_2(P_1)|S + \sum_{Q \in G_2 \cdot P_1 \setminus (G_1 \cdot P_2 \cap G_2 \cdot P_1)} |G_2(P_1)|Q,$$

the following equalities of divisors hold:

$$\begin{aligned}
& \sum_{R \in G_1 \cdot P_2 \setminus (G_1 \cdot P_2 \cap G_2 \cdot P_1)} |G_1(P_2)|R \\
& \quad + \sum_{S \in G_1 \cdot P_2 \cap G_2 \cdot P_1} (|G_1(P_2)| - |G_2(P_1)|)S + \sum_{\tau \in G_2} \tau(P_1) \\
= & \left(\sum_{R \in G_1 \cdot P_2 \setminus (G_1 \cdot P_2 \cap G_2 \cdot P_1)} |G_1(P_2)|R + \sum_{S \in G_1 \cdot P_2 \cap G_2 \cdot P_1} |G_1(P_2)|S \right) \\
& \quad + \sum_{Q \in G_2 \cdot P_1 \setminus (G_1 \cdot P_2 \cap G_2 \cdot P_1)} |G_2(P_1)|Q \\
= & \sum_{Q \in G_2 \cdot P_1 \setminus (G_1 \cdot P_2 \cap G_2 \cdot P_1)} |G_2(P_1)|Q + \sum_{R \in G_1 \cdot P_2} |G_1(P_2)|R \\
= & \varphi^* L,
\end{aligned}$$

where the last equality comes from Theorem 4.1.2 (6). Therefore, the equality

$$\begin{aligned}\varphi^*L - \sum_{\tau\in G_2}\tau(P_1) &= \sum_{R\in G_1\cdot P_2\setminus(G_1\cdot P_2\cap G_2\cdot P_1)}|G_1(P_2)|R \\ &\quad + \sum_{S\in G_1\cdot P_2\cap G_2\cdot P_1}(|G_1(P_2)|-|G_2(P_1)|)S\end{aligned}$$

of divisors holds. On the other hand, since the linear system corresponding to the morphism $\hat{\pi}_{\varphi(P_2)}$ is

$$\left\{E - \sum_{j=1}^{n_2}\alpha_{P_{2j}}P_{2j} \;\middle|\; E\in\Lambda, E\geq\sum_{j=1}^{n_2}\alpha_{P_{2j}}P_{2j}\right\}$$

and $\hat{\pi}_{\varphi(P_2)}$ is a Galois covering, the following equalities of divisors hold:

$$\varphi^*L - \sum_{j=1}^{n_2}\alpha_{P_{2j}}P_{2j} = (\hat{\pi}_{\varphi(P_2)})^*([L]) = \sum_{\tau\in G_2}\tau(P_1).$$

Therefore, the equalities

$$\begin{aligned}\sum_{j=1}^{n_2}\alpha_{P_{2j}}P_{2j} &= \varphi^*L - \sum_{\tau\in G_2}\tau(P_1) \\ &= \sum_{R\in G_1\cdot P_2\setminus(G_1\cdot P_2\cap G_2\cdot P_1)}|G_1(P_2)|R \\ &\quad + \sum_{S\in G_1\cdot P_2\cap G_2\cdot P_1}(|G_1(P_2)|-|G_2(P_1)|)S\end{aligned}$$

of divisors hold, and we have Theorem 4.1.2 (4). Since

$$m_{\varphi(P_2)} = \sum_{j=1}^{n_2}\alpha_{P_{2j}},$$

we have Theorem 4.1.2 (3). Assume that the condition (c-iii) in Theorem 4.1.1 is satisfied. Then

$$0 < |G_1(P_2)| - |G_2(P_1)| < |G_1(P_2)|$$

hold. By Theorem 4.1.2 (6), the equality $|G_1(P_2)| = \mathrm{ord}_P(\varphi^*L)$ holds at each point $P\in G_1\cdot P_2$. By Theorem 4.1.2 (4), the second (Λ, P)-order coincides

with $|G_1(P_2)| - |G_2(P_1)|$ at each point $P \in G_1 \cdot P_2 \cap G_2 \cdot P_1$. Therefore, the third (Λ, P)-order coincides with $|G_1(P_2)|$ at each point $P \in G_1 \cdot P_2 \cap G_2 \cdot P_1$, and Theorem 4.1.2 (5) holds. □

Remark 4.3.2. In [20], Fukasawa presented a criterion for the existence of a birational embedding with a pair of Galois points consisting of a smooth Galois point and an outer Galois point. By a method similar to the proof of Theorems 4.1.1 and 4.1.2, we can extend the criterion to non-smooth and outer Galois points. The necessary and sufficient conditions for the existence of a birational embedding with inner and outer Galois points are that $X/G_i \cong \mathbb{P}^1$ for $i = 1, 2$, $G_1 \cap G_2 = \{1\}$, and there exist $\eta \in G_2$ and $P \in X$ such that

$$|G_2(P)| \sum_{Q \in (G_2 \cdot P) - (G_1 \cdot \eta(P))} Q + (|G_2(P)| - |G_1(\eta(P))|) \sum_{R \in G_1 \cdot \eta(P)} R \geq P.$$

4.4 Proof of Theorem 4.1.3

We apply Theorems 4.1.1 and 4.1.2 to rational curves. In this case, condition (a) in Theorem 4.1.1 is always satisfied, by Lüroth's theorem. We put $Q_\infty = (1:0), Q_a = (a:1) \in \mathbb{P}^1$ for any $a \in k$.

Proof of Theorem 4.1.3. Let $p \neq 2, 5$, let $i \in k$ be a root of the polynomial $T^2 + 1 \in k[T]$, and let ξ be a primitive fifth root of unity.

(1) Let $p = 3$, and let $P_1 = Q_0$, $P_2 = Q_\xi$. We consider two sets:

$$G_1 = \left\langle \begin{bmatrix} \xi & 0 \\ 0 & 1 \end{bmatrix} \right\rangle \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle, G_2 = \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle \left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle.$$

It is known that

$$G_1 = \left\langle \begin{bmatrix} \xi & 0 \\ 0 & 1 \end{bmatrix} \right\rangle \rtimes \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle \cong \mathbf{D}_5,$$

where $\mathbf{D}_5$ is the dihedral group of degree 5 (see [5, Theorem C]). It is not difficult to check that

$$G_2 = \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle \rtimes \left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\rangle \cong \mathrm{AGL}(1, \mathbb{F}_3),$$

where $\mathrm{AGL}(1, \mathbb{F}_3)$ is the general affine group of degree 1 over $\mathbb{F}_3$. By direct computations, we have the equalities

$$G_1 \cap G_2 = \{1\},$$

$$G_1 \cdot P_2 = \{Q_1, Q_\xi, Q_{\xi^2}, Q_{\xi^3}, Q_{\xi^4}\},$$

$$G_2 \cdot P_1 = \{Q_{-1}, Q_0, Q_1\},$$

$$G_1 \cdot P_2 \cap G_2 \cdot P_1 = \{Q_1\},$$

$$G_1(P_2) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & \xi^2 \\ 1 & 0 \end{bmatrix} \right\},$$

$$G_2(P_1) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \right\}.$$

Therefore, conditions (b) and (c- i) in Theorem 4.1.1 are satisfied, and there exists a birational embedding $\varphi : \mathbb{P}^1 \to \mathbb{P}^2$ such that $\varphi(P_1)$, $\varphi(P_2)$ are different inner Galois points, $G_{\varphi(P_1)} \cong \mathbf{D}_5$, $G_{\varphi(P_2)} \cong \mathrm{AGL}(1, \mathbb{F}_3)$, and $L = \overline{\varphi(P_1)\varphi(P_2)}$ is not a tangent line at $\varphi(P_1)$, $\varphi(P_2)$. By Theorem 4.1.2 (1), (3) and (6), $m_{\varphi(P_1)} = 4$, $m_{\varphi(P_2)} = 8$ and $\deg(\varphi(\mathbb{P}^1)) = 14$. By Theorem 4.1.2 (6), the second order is equal to 2 at each point contained in $\mathrm{supp}(\varphi^* L)$.

(2) Let $P_1 = Q_\xi$, $P_2 = Q_1$. We consider

$$G_1 = \left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle \left\langle \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix} \right\rangle, G_2 = \left\langle \begin{bmatrix} \xi & 0 \\ 0 & 1 \end{bmatrix} \right\rangle.$$

Obviously, $G_2 \cong \mathbb{Z}/5\mathbb{Z}$, and the following fact is known.

$$G_1 = \left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle \rtimes \left\langle \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix} \right\rangle \cong \mathbf{A}_4,$$

where $\mathbf{A}_4$ is the alternating group of degree 4 (see [5, Theorem C]). Since 5 and 12 are coprime, condition (b) in Theorem 4.1.1 is satisfied. By direct computations, we have the following equalities:

$$G_1 \cdot P_2 = \{Q_{-i}, Q_{-1}, Q_0, Q_1, Q_i, Q_\infty\},$$

$$G_2 \cdot P_1 = \{Q_1, Q_\xi, Q_{\xi^2}, Q_{\xi^3}, Q_{\xi^4}\},$$

$$G_1 \cdot P_2 \cap G_2 \cdot P_1 = \{Q_1 = P_2\},$$

$$G_1(P_2) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\},$$

$$G_2(P_1) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}.$$

Therefore, condition (c-iii) in Theorem 4.1.1 is satisfied, and there exists a birational embedding $\varphi : \mathbb{P}^1 \to \mathbb{P}^2$ such that $\varphi(P_1)$, $\varphi(P_2)$ are different inner Galois points, $G_{\varphi(P_1)} \cong \mathbf{A}_4$, $G_{\varphi(P_2)} \cong \mathbb{Z}/5\mathbb{Z}$, $L = \overline{\varphi(P_1)\varphi(P_2)}$ is not a tangent line at $\varphi(P_1)$, and L is a tangent line at $\varphi(P_2)$. By Theorem 4.1.2 (1), (3) and (6), $m_{\varphi(P_1)} = 4$, $m_{\varphi(P_2)} = 11$ and $\deg(\varphi(\mathbb{P}^1)) = 16$. By Theorem 4.1.2 (2), (4), and (5), the second order is equal to 2 (resp. 1) at each point $Q \in G_1 \cdot P_2 \setminus \{P_2\}$ (resp. $Q \in G_2 \cdot P_1$), and the third order is equal to 2 at P_2.

(3) Let $P_1 = Q_\xi$, $P_2 = Q_1$. We consider two groups:

$$G_1 = \left\langle \left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle \rtimes \left\langle \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix} \right\rangle, \left\langle \begin{bmatrix} i & 0 \\ 0 & 1 \end{bmatrix} \right\rangle \right\rangle,$$

$$G_2 = \left\langle \begin{bmatrix} \xi & 0 \\ 0 & 1 \end{bmatrix} \right\rangle.$$

Obviously, $G_2 \cong \mathbb{Z}/5\mathbb{Z}$, and the following fact is known:

$$\left\langle \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle \rtimes \left\langle \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix} \right\rangle \lhd G_1 \cong \mathbf{S}_4,$$

where $\mathbf{S}_4$ is the symmetric group of degree 4 (see [5, Theorem C]). Since 5 and 24 are coprime, condition (b) in Theorem 4.1.1 is satisfied. By direct computations, we have the following equalities:

$$G_1 \cdot P_2 = \{Q_{-i}, Q_{-1}, Q_0, Q_1, Q_i, Q_\infty\},$$

$$G_2 \cdot P_1 = \{Q_1, Q_\xi, Q_{\xi^2}, Q_{\xi^3}, Q_{\xi^4}\},$$

$$G_1 \cdot P_2 \cap G_2 \cdot P_1 = \{Q_1 = P_2\},$$

$$G_1(P_2) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} i & 1 \\ 1 & i \end{bmatrix}, \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \right\},$$

$$G_2(P_1) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}.$$

Therefore, condition (c-iii) in Theorem 4.1.1 is satisfied, and there exists a birational embedding $\varphi : \mathbb{P}^1 \to \mathbb{P}^2$ such that $\varphi(P_1)$, $\varphi(P_2)$ are different inner Galois points, $G_{\varphi(P_1)} \cong \mathbf{S}_4$, $G_{\varphi(P_2)} \cong \mathbb{Z}/5\mathbb{Z}$, $L = \overline{\varphi(P_1)\varphi(P_2)}$ is not a tangent line at $\varphi(P_1)$, and L is a tangent line at $\varphi(P_2)$. By Theorem 4.1.2 (1), (3) and (6), $m_{\varphi(P_1)} = 4$, $m_{\varphi(P_2)} = 23$ and $\deg(\varphi(\mathbb{P}^1)) = 28$. By Theorem 4.1.2 (2), (4), and (5) the second order is equal to 4 (resp. 3, 1) at each point $Q \in G_1 \cdot P_2 \setminus \{P_2\}$ (resp. at P_2, at each point $Q \in G_2 \cdot P_1 \setminus \{P_2\}$), and the third order is equal to 4 at P_2. □

Chapter 5

Galois lines for the Giulietti–Korchmáros curve

Let $C \subset \mathbb{P}^3$ be an irreducible (possibly singular) space curve over k. We take a line $\ell \subset \mathbb{P}^3$ and consider the projection

$$\pi_\ell : C \dashrightarrow \mathbb{P}^1; P \mapsto \langle \ell, P \rangle$$

with the center ℓ, where $\langle \ell, P \rangle$ represents the hyperplane spanned by ℓ and P. If the field extension $k(C)/\pi_\ell^* k(\mathbb{P}^1)$ of function fields induced by π_ℓ is Galois, then ℓ is called a Galois line for C. This notion was introduced by Yoshihara (see [4, 48]). For a Galois line ℓ, the associated Galois group $\mathrm{Gal}(k(C)/\pi_\ell^*(\mathbb{P}^1))$ is denoted by G_ℓ. The degree of a Galois line ℓ is defined as $\deg(\pi_\ell) = [k(C) : \pi_\ell^* k(\mathbb{P}^1)]$. The following problems are raised in [50].

(a) Find new examples of plane curves having many Galois points.

(b) Find Galois lines ℓ for C in two cases where $\ell \cap C = \emptyset$ and $\ell \cap C \neq \emptyset$.

In Algebraic Geometry, the Hermitian curve

$$\mathcal{H} : x^q + x - y^{q+1} = 0$$

in $\mathbb{P}^2$ over a field of characteristic $p > 0$ has many interesting and important properties, where q is a power of p. The following beautiful theorem presented by Homma in the theory of Galois points represents one of them:

Theorem ([36])**.** *For the Hermitian curve $\mathcal{H}$, the set of all Galois points coincides with the set of all $\mathbb{F}_{q^2}$-rational points of $\mathbb{P}^2$.*

In 2007, Giulietti and Korchmáros discovered the curve $\widetilde{\mathcal{H}} \subset \mathbb{P}^3$ defined by

$$x^q + x - y^{q+1} = 0 \text{ and } y((x^q + x)^{q-1} - 1) - z^{q^2-q+1} = 0,$$

as the first example of maximal curve not covered by the Hermitian curve ([28]). This curve is called the Giulietti–Korchmáros (GK) curve. The full automorphism group $\mathrm{Aut}(\widetilde{\mathcal{H}})$ of $\widetilde{\mathcal{H}}$ was also determined in [28]. Recently, Beelen and Montanucci described the Weierstrass semigroups on $\widetilde{\mathcal{H}}$ completely ([1]).

It would be good to obtain a result for Galois lines similar to the theorem of Homma. In this chapter, we determine the arrangement of all Galois lines in $\mathbb{P}^3$ for the GK curve $\widetilde{\mathcal{H}}$. As an application, the arrangement of all Galois points for a plane model of the GK curve is also determined.

5.1 Main theorems

In Theorem 5.1.1, the arrangement of Galois lines for $\widetilde{\mathcal{H}}$ is described.

Theorem 5.1.1. *The set of all Galois lines for $\widetilde{\mathcal{H}}$ coincides with the set of all $\mathbb{F}_{q^2}$-lines ℓ with $\ell \ni (0:0:1:0)$ or $\ell \subset \{Z = 0\}$.*

Giulietti and Korchmáros introduced a plane model

$$x^{q^3} + x - (x^q + x)^{q^2-q+1} - z^{q^3+1} = 0$$

([28, Theorem 4]). The projective closure $(\widetilde{\mathcal{H}})'$ of this curve is the same as the image $\pi_R(\widetilde{\mathcal{H}})$ under the projection $\pi_R : \mathbb{P}^3 \dashrightarrow \mathbb{P}^2$ from the point $R := (0:1:0:0)$. As an application of Theorem 5.1.1, we will describe the arrangement of all Galois points for $(\widetilde{\mathcal{H}})'$.

Theorem 5.1.2. *The set of all Galois points for $(\widetilde{\mathcal{H}})'$ coincides with the set*

$$\{(0:1:0)\} \cup ((\widetilde{\mathcal{H}})' \cap \{Z = 0\}).$$

According to Theorem 5.1.2, the number $\delta((\widetilde{\mathcal{H}})')$ of Galois points contained in $(\widetilde{\mathcal{H}})' \setminus \mathrm{Sing}((\widetilde{\mathcal{H}})')$ is equal to $q+1$, where $\mathrm{Sing}((\widetilde{\mathcal{H}})')$ is the set of all singular points of $(\widetilde{\mathcal{H}})'$. This is a new family of plane curves C of degree d such that $\delta(C) \to \infty$ as $d \to \infty$.

5.2 Properties of the GK curve

We consider the Giulietti–Korchmáros curve $\widetilde{\mathcal{H}} \subset \mathbb{P}^3$ over an algebraically closed field k of characteristic $p > 0$. Let $(X : Y : Z : W)$ and $(X : Z : W)$ be systems of homogeneous coordinates of $\mathbb{P}^3$ and of $\mathbb{P}^2$ respectively. An affine open set of $\mathbb{P}^3$ defined by $W \neq 0$ is denoted by U_W, and

$$(x, y, z) = \left(\frac{X}{W}, \frac{Y}{W}, \frac{Z}{W}\right)$$

is a system of affine coordinates of U_W. For points P, $Q \in \mathbb{P}^3$ with $P \neq Q$, the line passing through P, Q is denoted by $\overline{PQ}$.

Let $\mathcal{H}$ be the Hermitian curve given by $Z = X^q W + X W^q - Y^{q+1} = 0$, and let $\mathcal{H}(\mathbb{F}_{q^2})$ be the set of all $\mathbb{F}_{q^2}$-rational points on $\mathcal{H}$. Note that

$$\mathcal{H}(\mathbb{F}_{q^2}) = \widetilde{\mathcal{H}} \cap \{Z = 0\} = \widetilde{\mathcal{H}}(\mathbb{F}_{q^2}).$$

The following result is well known (see, for example, [36, Corollary 3.4]).

Proposition 5.2.1. *Let ℓ be a line contained in $\mathbb{P}^3$. If $\ell \subset \{Z = 0\}$, then $|\ell \cap \mathcal{H}(\mathbb{F}_{q^2})| = 0$, 1, or $q + 1$.*

Note that the projection from $R' = (0 : 0 : 1 : 0)$ induces a cyclic covering $\widetilde{\mathcal{H}} \to \mathcal{H}$ of degree $q^2 - q + 1$ (see [28, p.234]). Using the property of this covering, Giulietti and Korchmáros computed the genus of $\widetilde{\mathcal{H}}$.

Proposition 5.2.2 ([28], Theorem 2)**.** *The set of all ramification points of the cyclic covering $\pi_{R'} : \widetilde{\mathcal{H}} \to \mathcal{H}$ coincides with $\widetilde{\mathcal{H}} \cap \{Z = 0\}$. Furthermore, the genus of the Giulietti-Korchmáros curve $\widetilde{\mathcal{H}}$ is $\frac{1}{2}(q^3 + 1)(q^2 - 2) + 1$.*

To determine the arrangement of Galois lines, the exact values of orders of hyperplanes in $\mathbb{P}^3$ are important. Let $i : \widetilde{\mathcal{H}} \to \mathbb{P}^3$ be the inclusion. In the following proposition, the second assertion is a result of Duursma [3], Beelen and Montanucci [1].

Proposition 5.2.3 (see [1], p.13)**.** *Let $P \in \widetilde{\mathcal{H}}$ and let $H \subset \mathbb{P}^3$ be a hyperplane with $H \ni P$.*

(1) *If $P \in \widetilde{\mathcal{H}} \cap \{Z = 0\}$, then $\mathrm{ord}_P(i^*H) = 1$, $q^2 - q + 1$, or $q^3 + 1$.*

(2) *If $P \notin \widetilde{\mathcal{H}} \cap \{Z = 0\}$, then $\mathrm{ord}_P(i^*H) = 1$, q, q^3, or $q^3 + 1$.*

Furthermore, we will need the following theorem of Giulietti and Korchmáros on the automorphism group of $\widetilde{\mathcal{H}}$.

Proposition 5.2.4 (A weak version of Theorem 7 in [28]). *The full automorphism group* $\mathrm{Aut}(\widetilde{\mathcal{H}})$ *acts on* $\widetilde{\mathcal{H}} \cap \{Z = 0\}$*, and the action of the subgroup* $\mathrm{Aut}(\widetilde{\mathcal{H}}) \cap \mathrm{PGL}(4, k)$ *on this set is doubly transitive.*

5.3 Galois lines with degree q^3

Let $P_\infty := (1 : 0 : 0 : 0) \in \widetilde{\mathcal{H}}$, and let $\ell_\infty \subset \mathbb{P}^3$ be the line defined by $Z = W = 0$. Then $P_\infty \in \ell_\infty$, and $\ell_\infty = \overline{RP_\infty}$. First, we show that ℓ_∞ is a Galois line. Note that the affine part $\widetilde{\mathcal{H}}_W$ of $\widetilde{\mathcal{H}}$ given by $W \neq 0$ is the same as the curve defined by

$$x^q + x - y^{q+1} = y^{q^2} - y - z^{q^2-q+1} = 0.$$

The subgroup

$$G_1 := \left\{ \begin{bmatrix} 1 & b^q & 0 & a \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \;\middle|\; a, b \in \mathbb{F}_{q^2}, a^q + a - b^{q+1} = 0 \right\} \subset \mathrm{PGL}(4, k)$$

of order q^3 acts on $\widetilde{\mathcal{H}}$ ([28, p.238]). It is not difficult to check that $k(\widetilde{\mathcal{H}})^{G_1} = k(z)$. The extension $k(\widetilde{\mathcal{H}})/k(\widetilde{\mathcal{H}})^{G_1}$ coincides with the extension $k(\widetilde{\mathcal{H}})/k(z)$ induced by the projection

$$\pi_{\ell_\infty} : \mathbb{P}^3 \dashrightarrow \mathbb{P}^1; (X : Y : Z : W) \mapsto (Z : W)$$

from ℓ_∞. Therefore, ℓ_∞ is a Galois line with $\ell_\infty \cap \widetilde{\mathcal{H}} = \{P_\infty\}$. Note that ℓ_∞ coincides with the tangent line of the Hermitian curve

$$Z = X^q W + X W^q - Y^{q+1} = 0$$

at P_∞. By Proposition 5.2.4, there exist $q^3 + 1$ Galois lines for $\widetilde{\mathcal{H}}$.

We would like to show that the number of Galois lines with degree q^3 is at most q^3+1. Assume that $\ell \subset \mathbb{P}^3$ is a Galois line with degree q^3. Note that the Galois group G_ℓ of order q^3 acts on the set $\widetilde{\mathcal{H}} \cap \{Z = 0\}$ of cardinality q^3+1, by Proposition 5.2.4. By a fact of group theory (see [44, Chapter 2, Section

1 (1.3)]), there exists a point $P \in \widetilde{\mathcal{H}} \cap \{Z = 0\}$ fixed by any element of G_ℓ. It follows from Theorem 2.3.1 (4) that the ramification index at P is equal to q^3 for the projection π_ℓ from ℓ. We can assume that $P = P_\infty$. Assume by contradiction that $P_\infty \notin \ell$. Then there exists a hyperplane H such that $\mathrm{ord}_{P_\infty}(i^*H) = q^3$, where $i : \widetilde{\mathcal{H}} \to \mathbb{P}^3$ is the inclusion. This is a contradiction to Proposition 5.2.3. Therefore, $P_\infty \in \ell$. Since $\pi_\ell^{-1}(\pi_\ell(P_\infty)) = \{P_\infty\}$, the hyperplane $W = 0$ includes ℓ. Assume by contradiction that $\ell \not\subset \{Z = 0\}$. Then $\ell \cap \{Z = 0\} = \{P_\infty\}$ and

$$|\widetilde{\mathcal{H}} \cap \{Z = 0\} \cap H| = 1 \text{ or } q + 1$$

for each hyperplane $H \supset \ell$, by Proposition 5.2.1. By Theorem 2.3.1 (1), (3), and Proposition 5.2.4, there exists a ramification point different from P_∞ with index a power of p. This is a contradiction to Proposition 5.2.3. Therefore, ℓ is defined by $Z = W = 0$. The proof of the assertion for Galois lines with degree q^3 in Theorem 5.1.1 is completed.

We consider Galois points in $(\widetilde{\mathcal{H}})' \setminus \mathrm{Sing}((\widetilde{\mathcal{H}})')$. Note that Galois lines ℓ for $\widetilde{\mathcal{H}}$ passing through R correspond to Galois points $P \in \mathbb{P}^2$ for $(\widetilde{\mathcal{H}})'$, by $\ell \mapsto \pi_R(\ell)$, since the projection $\pi_R : \widetilde{\mathcal{H}} \to (\widetilde{\mathcal{H}})'$ is birational. Since all Galois lines with degree q^3 are included in the plane $\{Z = 0\}$, all Galois points with degree q^3 on $(\widetilde{\mathcal{H}})'$ are contained in the line $\{Z = 0\}$ in $\mathbb{P}^2$. Note that if a line ℓ with $R \in \ell \subset \{Z = 0\}$ intersects $\widetilde{\mathcal{H}}$ at $q + 1$ points, then $\pi_R(\ell) \in \mathrm{Sing}((\widetilde{\mathcal{H}})')$. Considering $\mathbb{F}_{q^2}$-lines passing through R, it is inferred that there exists exactly $q + 1$ Galois points on $(\widetilde{\mathcal{H}})'$ with degree q^3, which points are $(\alpha : 0 : \beta) \in \mathbb{P}^2$ with $\alpha^q\beta + \alpha\beta^q = 0$. The assertion in Theorem 5.1.2 for Galois points with degree q^3 follows.

5.4 Galois lines with degree $q^3 + 1$

We consider Galois line $\ell \subset \mathbb{P}^3$ with $\ell \cap \widetilde{\mathcal{H}} = \emptyset$. Let $R' = (0 : 0 : 1 : 0)$ and ℓ_0 be the line defined by $X = W = 0$. Then $\ell_0 \cap \widetilde{\mathcal{H}} = \emptyset$, and ℓ_0 coincides with the line passing through R' and $R = (0 : 1 : 0 : 0)$. The subgroup

$$G_2 := \left\{ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \zeta^{q^2-q+1} & 0 & 0 \\ 0 & 0 & \zeta & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \middle| \, \zeta \in k, \zeta^{q^3+1} = 1 \right\} \subset \mathrm{PGL}(4, k)$$

of order q^3+1 acts on $\widetilde{\mathcal{H}}$. It is not difficult to check that $k(\widetilde{\mathcal{H}})^{G_2} = k(x)$. The extension $k(\widetilde{\mathcal{H}})/k(\widetilde{\mathcal{H}})^{G_2}$ coincides with the extension $k(\widetilde{\mathcal{H}})/k(x)$ induced by the projection

$$\pi_{\ell_0} : \mathbb{P}^3 \dashrightarrow \mathbb{P}^1; (X : Y : Z : W) \mapsto (X : W)$$

from ℓ_0. Therefore, ℓ_0 is a Galois line with $\ell_0 \cap \widetilde{\mathcal{H}} = \emptyset$.

By Proposition 5.2.4, for each $\mathbb{F}_{q^2}$-rational point $Q \in \{Z = 0\} - \widetilde{\mathcal{H}} \subset \mathbb{P}^3$, there exists a line $\ell \subset \mathbb{P}^3$ with $Q \in \ell \not\subset \{Z = 0\}$ such that π_ℓ induces a Galois extension of degree q^3+1. Therefore, the number of Galois lines with degree q^3+1 is at least $q^4+q^2+1-(q^3+1) = q^4-q^3+q^2$.

We consider the case where a Galois line ℓ is included in the plane $Z = 0$. Note that the projection π_ℓ is not ramified at each point in $\widetilde{\mathcal{H}} \cap \{Z = 0\}$. By Theorem 2.3.1 (3) and Proposition 5.2.3, the ramification index at all ramification points for π_ℓ is equal to q^3+1. By the Riemann–Hurwitz formula, the integer $2g_{\widetilde{\mathcal{H}}} - 2 + 2(q^3+1)$ is divisible by q^3. This is a contradiction to Proposition 5.2.2 (this integer is equal to $(q^3+1)q^2$). Therefore, $\ell \not\subset \{Z = 0\}$ holds for all Galois lines ℓ with $\ell \cap \widetilde{\mathcal{H}} = \emptyset$.

Let $\ell \subset \mathbb{P}^3$ be a line with $\ell \cap \{Z = 0\} = \{Q\} \not\subset \widetilde{\mathcal{H}}$ which induces a Galois extension of degree q^3+1. It follows from Proposition 5.2.1 that

$$|\widetilde{\mathcal{H}} \cap \{Z = 0\} \cap H| = 0, 1, \text{ or } q+1,$$

for each hyperplane $H \supset \ell$. By Theorem 2.3.1 (1), (3), and Proposition 5.2.4, π_ℓ is ramified at points in $\widetilde{\mathcal{H}} \cap \{Z = 0\}$ with index q^3+1 or q^2-q+1. Note that if the index at $P \in \widetilde{\mathcal{H}} \cap \{Z = 0\}$ is q^3+1, then the line $\overline{QP}$ is $\mathbb{F}_{q^2}$-rational. Considering lines in the plane $Z = 0$ passing through Q, there exist at least two lines over $\mathbb{F}_{q^2}$ containing Q. Therefore, the point Q is an $\mathbb{F}_{q^2}$-rational point. By Proposition 5.2.4, we can assume that $Q = R = (0 : 1 : 0 : 0)$.

We would like to show the uniqueness of the Galois line $\ell \ni R$ with $\ell \cap \widetilde{\mathcal{H}} = \emptyset$. We consider the projection $\pi_R : \mathbb{P}^3 \dashrightarrow \mathbb{P}^2$. Since all points of $\widetilde{\mathcal{H}} \cap \{Z = 0\}$ are ramification points for π_ℓ, all tangent lines at smooth points in $(\widetilde{\mathcal{H}})' \cap \{Z = 0\}$ contain the point $\pi_R(\ell)$. This implies that $\pi_R(\ell) = (0 : 1 : 0)$. The uniqueness follows. This observation also implies that the number of outer Galois points for $(\widetilde{\mathcal{H}})'$ is exactly one.

Remark 5.4.1. The tangent line at each point of $\widetilde{\mathcal{H}} \cap \{Z = 0\}$ passes through $R' = (0 : 0 : 1 : 0)$, by Proposition 5.2.2. Furthermore, $R' \in \ell$ for all Galois

lines ℓ with $\ell \cap \widetilde{\mathcal{H}} = \emptyset$. Therefore, a Galois line ℓ with $\ell \cap \widetilde{\mathcal{H}} = \emptyset$ coincides with the line passing through R' and an $\mathbb{F}_{q^2}$-rational point in the plane $Z = 0$ but not on $\widetilde{\mathcal{H}}$.

Remark 5.4.2. For each Galois line ℓ with $\ell \cap \widetilde{\mathcal{H}} = \emptyset$, the Galois group G_ℓ includes the subgroup

$$\left\{ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \eta & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \middle| \, \eta \in k, \eta^{q^2-q+1} = 1 \right\} \subset \mathrm{PGL}(4, k).$$

Therefore, $G_\ell \cap G_{\ell'} \neq \{1\}$ for each two Galois lines ℓ and ℓ' not intersecting $\widetilde{\mathcal{H}}$. According to [17, Theorem 1], there exist no plane model of $\widetilde{\mathcal{H}}$ realizing G_ℓ and $G_{\ell'}$ as Galois groups at two outer Galois points.

5.5 Galois lines with degree at most $q^3 - 1$

The tangent line at each point of $\widetilde{\mathcal{H}} \cap \{Z = 0\}$ is a Galois line. In fact, the projection from the line $Y = W = 0$ induces the extension $k(x, y, z)/k(y)$, and y is fixed by automorphisms $(x, y, z) \mapsto (x + \alpha, y, \eta z)$, where $\alpha^q + \alpha = 0$ and $\eta^{q^2-q+1} = 1$.

We show that any line $\ell \subset \{Z = 0\}$ such that $\ell \cap \widetilde{\mathcal{H}}$ contains at least two points is a Galois line. It follows from Proposition 5.2.1 that ℓ is $\mathbb{F}_{q^2}$-rational and contains exactly $q + 1$ points of $\widetilde{\mathcal{H}}$. We consider the line $Y = Z = 0$. Then the extension is $k(x, y, z)/k(y/z)$. The automorphisms

$$\sigma_\alpha : (x, y, z) \mapsto (x + \alpha, y, z) \quad \text{and} \quad \tau : (x, y, z) \mapsto (\xi^{q+1} x, \xi y, \xi z)$$

act on $\widetilde{\mathcal{H}}$, where $\alpha^q + \alpha = 0$ and ξ is a primitive $(q - 1)$-th root of unity, and fix y/z. Note that the group generated by such automorphisms contains $q(q - 1)$ elements and fixes P_∞. We consider the linear transformation φ on $\mathbb{P}^3$ represented by

$$A = \begin{bmatrix} 1 & 0 & 0 & \rho^q \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & -\rho \end{bmatrix},$$

where $\rho^q + \rho = 1$ (see [31]). Then $\varphi(\widetilde{\mathcal{H}})$ is given by

$$x^{q+1} - 1 = y^{q+1} \text{ and } y\frac{x^{q^2} - x}{x^{q+1} - 1} = z^{q^2-q+1}.$$

The linear transformation ψ given by

$$\begin{bmatrix} \beta^2 & 0 & 0 & 0 \\ 0 & \beta & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

where β is a primitive $(q+1)$-th root of unity, acts on $\varphi(\widetilde{\mathcal{H}})$. Since

$$\varphi^*\left(\frac{y}{z}\right) = -\frac{y}{z} \text{ and } \psi^*\left(\frac{y}{z}\right) = \frac{y}{z},$$

$\mu^* := (\varphi^{-1} \circ \psi \circ \varphi)^*$ fixes y/z. Let $G_3 \subset \mathrm{Aut}(\widetilde{\mathcal{H}})$ be the group generated by τ, μ, and all σ_α. Since $\beta^2 \neq 1$, $\mu(P_\infty) = (\beta^2\rho + \rho^q : 0 : 0 : \beta^2 - 1) \neq P_\infty$. It follows that G_3 acts on $\widetilde{\mathcal{H}} \cap \{Y = Z = 0\}$ transitively. Therefore, there exist at least $q(q-1)$ elements of G_3 fixing P, for each point $P \in \widetilde{\mathcal{H}} \cap \{Y = Z = 0\}$. It follows that

$$|G_3| \geq q(q-1)(q+1)$$

and hence, the line $Y = Z = 0$ is a Galois line whose Galois group is equal to G_3. By Proposition 5.2.4, the claim follows. Furthermore, for each line ℓ such that $R = (0 : 1 : 0 : 0) \in \ell \subset \{Z = 0\}$ and $\ell \cap \widetilde{\mathcal{H}}$ contains $q+1$ points, $\pi_R(\ell) \in \mathrm{Sing}((\widetilde{\mathcal{H}})')$ and this is also a Galois point.

Remark 5.5.1. The automorphism $\varphi^{-1} \circ \psi \circ \varphi$ is represented by

$$\begin{bmatrix} \beta^2\rho + \rho^q & 0 & 0 & (\beta^2 - 1)\rho^{q+1} \\ 0 & \beta & 0 & 0 \\ 0 & 0 & \beta & 0 \\ \beta^2 - 1 & 0 & 0 & \beta^2\rho^q + \rho \end{bmatrix}.$$

Assume that a line $\ell \subset \mathbb{P}^3$ induces a Galois extension of degree $d \leq q^3 - 1$. By Proposition 5.2.1 and the previous paragraph, we can assume that $\ell \not\subset \{Z = 0\}$.

We consider the case where $\ell \cap \{Z = 0\} = \{Q\} \subset \widetilde{\mathcal{H}}$. We can assume that $Q = P_\infty$ and ℓ is not the tangent line at P_∞. Note that $\pi_{P_\infty}(\widetilde{\mathcal{H}}) \subset \mathbb{P}^2$ is defined by

$$y^{q^2} - y = z^{q^2-q+1},$$

and the projection from each point of $\mathbb{P}^2$ is not birational onto $\mathbb{P}^1$ for this curve. Since π_ℓ factors through the projection π_{P_∞}, it follows that $d > q$. By Proposition 5.2.1, for each hyperplane $H \supset \ell$,

$$|(\widetilde{\mathcal{H}} \cap \{Z = 0\} \cap H) \setminus \{P_\infty\}| = 0 \ \text{ or } \ q.$$

Then, by Theorem 2.3.1 (1), (2), and Proposition 5.2.4, there exists a ramification point different from P_∞ with index d/q. It follows from Proposition 5.2.3 that $d = q(q^2 - q + 1)$ or q. Therefore, $d = q(q^2 - q + 1)$. Let P_1 and $P_2 \in \widetilde{\mathcal{H}} \cap \{Z = 0\} \setminus \{P_\infty\}$ with $\overline{P_\infty P_1} \neq \overline{P_\infty P_2}$. Then ℓ is given by the intersection of planes spanned by $\overline{P_\infty P_1}$ and R', $\overline{P_\infty P_2}$ and R'. This implies that ℓ is the tangent line at P_∞. This is a contradiction.

We consider the case where $\ell \cap \{Z = 0\} = \{Q\} \not\subset \widetilde{\mathcal{H}}$. By Theorem 2.3.1 (1), (2), Proposition 5.2.1, and Proposition 5.2.4, ramification indices for each point of $\widetilde{\mathcal{H}} \cap \{Z = 0\}$ are d or $d/(q+1)$. It follows from Proposition 5.2.3 that $d = q^2 - q + 1$ or $d = q + 1$. Assume that $d = q^2 - q + 1$ and $q > 2$. Then, for each $P \in \widetilde{\mathcal{H}} \cap \{Z = 0\}$, the line $\overline{QP}$ intersects $\widetilde{\mathcal{H}}$ at a unique point P. Then π_ℓ ramified at each point $P \in \widetilde{\mathcal{H}} \cap \{Z = 0\}$ and hence, the tangent line at P intersects ℓ. If $\ell \not\ni R'$, then the tangent lines are included in the plane spanned by ℓ and R'. This is a contradiction. Therefore, $\ell \ni R'$ and $\ell = \overline{R'Q}$. Using Proposition 5.2.2, we can assume that Q is not $\mathbb{F}_{q^2}$-rational and $\overline{R'Q} \cap \widetilde{\mathcal{H}}$ consists of $q^2 - q + 1$ points. Then

$$d = (q^3 + 1) - (q^2 - q + 1) = q^2 - q + 1.$$

This is a contradiction. Assume that $q = 2$ and $d = q^2 - q + 1 = 3$. If there exist two lines in $\{Z = 0\}$ containing Q and $q + 1$ points of $\widetilde{\mathcal{H}}$, then Q is $\mathbb{F}_{q^2}$-rational, since such lines are $\mathbb{F}_{q^2}$-rational. We can assume that $Q = R$. Then $\pi_R(\ell) \in \mathrm{Sing}((\widetilde{\mathcal{H}})') \setminus \{Z = 0\}$. This is a contradiction. Therefore, there exist points P_1 and $P_2 \in \widetilde{\mathcal{H}} \cap \{Z = 0\}$ with $\overline{QP_1} \neq \overline{QP_2}$ such that the tangent lines at P_1 and P_2 intersect ℓ. If $R' \notin \ell$, then P_1 and P_2 are included in the plane spanned by ℓ and R'. This is a contradiction to that points Q, P_1, and P_2 are not collinear in the plane $\{Z = 0\}$. Therefore, $\ell \ni R'$ and $\ell = \overline{R'Q}$.

We can assume that Q is not $\mathbb{F}_{q^2}$-rational and $\overline{R'Q} \cap \widetilde{\mathcal{H}}$ consists of $q^2 - q + 1$ points. Then

$$d = (q^3 + 1) - (q^2 - q + 1) = q^2 - q + 1.$$

This is a contradiction.

Assume that $d = q + 1$. If $q = 2$, then

$$d = q + 1 = q^2 - q + 1.$$

We can assume that $q > 2$. It follows from Proposition 5.2.3 that, for each $P \in \widetilde{\mathcal{H}} \cap \{Z = 0\}$, the line $\overline{QP}$ contains exactly $q + 1$ points of $\widetilde{\mathcal{H}}$. This implies that $\overline{QP}$ is $\mathbb{F}_{q^2}$-rational and hence, Q is $\mathbb{F}_{q^2}$-rational. We can assume that $Q = R$. Then $\pi_R(\ell) \in \mathrm{Sing}((\widetilde{\mathcal{H}})') \setminus \{Z = 0\}$. This is a contradiction.

Bibliography

[1] P. Beelen and M. Montanucci, Weierstrass semigroups on the Giulietti–Korchmáros curve, Finite Fields Appl. **52** (2018), 10–29.

[2] H. Borges and S. Fukasawa, Galois points for double-Frobenius non-classical curves, Finite Fields Appl. **61** (2020), 101579, 8 pages.

[3] I. Duursma, Two-point coordinate rings for GK-curves, IEEE Trans. Inf. Theory **57** (2011), 593–600.

[4] C. Duyaguit and H. Yoshihara, Galois lines for normal elliptic space curves, Algebra Colloq. **12** (2005), 205–212.

[5] X. Faber, Finite p-irregular subgroups of $\mathrm{PGL}_2(k)$, preprint, arXiv:1112.1999.

[6] S. Fukasawa, Galois points on quartic curves in characteristic 3, Nihonkai Math. J. **17** (2006), 103–110.

[7] S. Fukasawa, On the number of Galois points for a plane curve in positive characteristic, II, Geom. Dedicata **127** (2007), 131–137.

[8] S. Fukasawa, On the number of Galois points for a plane curve in positive characteristic, Comm. Algebra **36** (2008), 29–36.

[9] S. Fukasawa, Galois points for a plane curve in arbitrary characteristic, Geom. Dedicata **139** (2009), 211–218.

[10] S. Fukasawa, On the number of Galois points for a plane curve in positive characteristic, Ⅲ, Geom. Dedicata **146** (2010), 9–20.

[11] S. Fukasawa, Classification of plane curves with infinitely many Galois points, J. Math. Soc. Japan **63** (2011), 195–209.

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

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

[14] S. Fukasawa, Automorphism groups of smooth plane curves with many Galois points, Nihonkai Math. J. **25** (2014), 69–75.

[15] S. Fukasawa, Galois points for a plane curve in characteristic two, J. Pure Appl. Algebra **218** (2014), 343–353.

[16] S. Fukasawa, Rational points and Galois points for a plane curve over a finite field, Finite Fields Appl. **39** (2016), 36–42.

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

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

[19] S. Fukasawa, Galois lines for the Artin–Schreier–Mumford curve, preprint, arXiv:2005.10073.

[20] S. Fukasawa, Algebraic curves admitting inner and outer Galois points, preprint, arXiv:2010.00815.

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

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

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

[24] S. Fukasawa and K. Higashine, A birational embedding with two Galois points for quotient curves, J. Pure Appl. Algebra **225** (2021), 106525, 10 pages.

[25] S. Fukasawa, M. Homma and S. J. Kim, Rational curves with many rational points over a finite field, Arithmetic, Geometry, Cryptography and Coding theory, pp.37–48, Contemp. Math. **574**, Amer. Math. Soc., Providence, RI, 2012.

[26] S. Fukasawa and K. Waki, Examples of plane rational curves with two Galois points in positive characteristic, Finite Fields and their Applications: Proceedings of the 14th International Conference on Finite Fields and their Applications, Vancouver, June 3-7, 2019, pp.181–188, De Gruyter, 2020.

[27] A. Garcia and H. Stichtenoth, A maximal curve which is not a Galois subcover of the Hermitian curve, Bull. Braz. Math. Soc. **37** (2006), 139–152.

[28] M. Giulietti and G. Korchmáros, A new family of maximal curves over a finite field, Math. Ann. **343** (2009), 229–245.

[29] M. Giulietti, M. Montanucci, L. Quoos and G. Zini, On some Galois covers of the Suzuki and Ree curves, J. Number theory **189** (2018), 220–254.

[30] M. Giulietti, M. Montanucci and G. Zini, On maximal curves that are not quotients of the Hermitian curve, Finite Fields Appl. **41** (2016), 72–88.

[31] M. Giulietti, L. Quoos and G. Zini, Maximal curves from subcovers of the GK-curve, J. Pure Appl. Algebra **220** (2016), 3372–3383.

[32] R. Hartshorne, Algebraic Geometry, Graduate Texts in Mathematics, vol. **52**, Springer-Verlag, New York, 1977.

[33] H. Hayashi and H. Yoshihara, Galois group at each point for some self-dual curves, Geometry **2013** (2013), Article ID 369420, 6 pages.

[34] K. Higashine, A criterion for the existence of a plane model with two inner Galois points for algebraic curves, Hiroshima Math. J., to appear.

[35] J. W. P. Hirschfeld, G. Korchmáros and F. Torres, Algebraic curves over a finite field, Princeton Univ. Press, Princeton, 2008.

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

[37] M. Kanazawa, T. Takahashi and H. Yoshihara, The group generated by automorphisms belonging to Galois points of the quartic surface, Nihonkai Math. J. **12** (2001), 89–99.

[38] M. Kanazawa and H. Yoshihara, Galois lines for space elliptic curve with $j = 12^3$, Beitr. Algebra Geom. **59** (2018), 431–444.

[39] K. Miura, Field theory for function fields of singular plane quartic curves, Bull. Austral. Math. Soc. **62** (2000), 193–204.

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

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

[42] D. C. Skabelund, New maximal curves as ray class fields over Deligne–Lusztig curves, Proc. Am. Math. Soc. **146** (2018), 525–540.

[43] H. Stichtenoth, Algebraic function fields and codes, Universitext, Springer-Verlag, Berlin, 1993.

[44] M. Suzuki, Group Theory I, Grundlehren der Mathematischen Wissenschaften, vol. **247**, Springer-Verlag, Berlin-New York, 1982.

[45] T. Takahashi, Non-smooth Galois points on a quintic curve with one singular point, Nihonkai Math. J. **16** (2005), 57–66.

[46] F. Torres, The approach of Stöhr–Voloch to the Hasse–Weil bound with applications to optimal curves and plane arcs, 2000.

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

[48] H. Yoshihara, Galois lines for space curves, Algebra Colloq. **13** (2006), 455–469.

[49] H. Yoshihara, Galois lines for normal elliptic space curves, II, Algebra Colloquium **19** (2012), No. spec01, 867–876.

[50] H. Yoshihara and S. Fukasawa, List of problems, available at:
http://hyoshihara.web.fc2.com/openquestion.html.