Rend. Sem. Mat. Univ. Padova, Vol. 129 (2013)
DOI 10.4171/RSMUP/129-7

Complete Determination of the Number of Galois Points for a Smooth Plane Curve

Satoru Fukasawa (*)

Dedicated to my son Atsumu and my wife Kaori

Abstract - Let C be a smooth plane curve. A point P in the projective plane is said to be Galois with respect to C if the function field extension induced by the projection from P is Galois. We denote by $\delta(C)$ (resp. $\delta'(C)$) the number of Galois points contained in C (resp. in $\mathbb{P}^2 \setminus C$). In this article, we determine the numbers $\delta(C)$ and $\delta'(C)$ in any remaining open cases. Summarizing results obtained by now, we will present a complete classification theorem of smooth plane curves by the number $\delta(C)$ or $\delta'(C)$. In particular, we give new characterizations of Fermat curve and Klein quartic curve by the number $\delta'(C)$.

Mathematics Subject Classification (2010). 14H50, 12F10, 14H05.

Keywords. Galois point, plane curve, positive characteristic, Galois group.

1. Introduction

Let the base field K be an algebraically closed field of characteristic $p \geq 0$ and let $C \subset \mathbb{P}^2$ be a smooth plane curve of degree $d \geq 4$. In 1996, H. Yoshihara introduced the notion of *Galois point* (see [14, 17] or survey paper [5]). If the function field extension $K(C)/K(\mathbb{P}^1)$, induced by the projection $\pi_P : C \to \mathbb{P}^1$ from a point $P \in \mathbb{P}^2$, is Galois, then the point P is said to be Galois with respect to C. When a Galois point P is contained in C (resp. $\mathbb{P}^2 \setminus C$), we call P an inner (resp. outer) Galois point. We denote by $\delta(C)$ (resp. $\delta'(C)$) the number of inner (resp. outer) Galois points for C. It is

(*) Indirizzo dell'A.: Department of Mathematical Sciences, Faculty of Science, Yamagata University, Kojirakawa-machi 1-4-12, Yamagata 990-8560, Japan.
E-mail: s.fukasawa@sci.kj.yamagata-u.ac.jp

remarkable that many classification results of algebraic varieties have been given in the theory of Galois point.

Yoshihara and K. Miura determined $\delta(C)$ and $\delta'(C)$ in characteristic $p=0$ ([14, 17]). In characteristic $p>0$, M. Homma [13] settled $\delta(H)$ and $\delta'(H)$ for the Fermat curve H of degree p^e+1. Recently, the present author determined $\delta(C)$ when $p>2$ or $d-1$ is not a power of 2 ([3, 4]), and $\delta'(C)$ when d is not divisible by p, $d=p$, or $d=2^e$ in $p=2$ ([3, 4, 7]). The following problems remain open ([4, Part III, Problem], [5, Problem 2]).

Problem. (1) *Let $p=2$ and let $e \geq 2$. Find and classify smooth plane curves of degree $d=2^e+1$ with $\delta(C)=d$.*

(2) *Let $p>0$, $e\geq 1$ and let $d=p^e l$, where l is not divisible by p. Assume that $(p^e, l) \neq (p,1), (2^e,1)$. Then, determine $\delta'(C)$.*

In this article, we give a complete answer to these problems.

Theorem 1. *Let $p=2$, let $e\geq 2$ and let C be a smooth plane curve of degree $d=2^e+1$. Then, $\delta(C)=d$ if and only if C is projectively equivalent to the curve given by*

$$\prod_{\alpha\in\mathbb{F}_{2^e}}(x+\alpha y+\alpha^2)+cy^{2^e+1}=0, \tag{1c}$$

where $c\in K\setminus\{0,1\}$.

Theorem 2. *Let the characteristic $p>0$, let $e\geq 1$, let l be not divisible by p, and let C be a smooth plane curve of degree $d=p^e l\geq 4$. If $(p^e,l)\neq(2^e,1)$, then $\delta'(C)\leq 1$.*

Summarizing Theorems 1 and 2 and the results of Yoshihara, Miura, Homma and the present author, we obtain the following classification theorem of smooth plane curves by the number $\delta(C)$ or $\delta'(C)$.

Theorem 3 (Yoshihara, Miura, Homma, Fukasawa). *Let C be a smooth plane curve of degree $d\geq 4$ in characteristic $p\geq 0$. Then:*

- (I) *$\delta(C)=0,1,d$ or $(d-1)^3+1$. Furthermore, we have the following.*
  - (i) *$\delta(C)=(d-1)^3+1$ if and only if $p>0$, $d=p^e+1$ and C is projectively equivalent to the Fermat curve.*
  - (ii) *$\delta(C)=d\geq 5$ if and only if $p=2$, $d=2^e+1$ and C is projectively equivalent to the curve defined by $\prod_{\alpha\in\mathbb{F}_{2^e}}(x+\alpha y+\alpha^2)+cy^{2^e+1}=0$, where $c\in K\setminus\{0,1\}$.*

(iii) $\delta(C) = d = 4$ *if and only if* $p \neq 2, 3$ *and* C *is projectively equivalent to the curve defined by* $x^3 + y^4 + 1 = 0$.

(II) $\delta'(C) = 0, 1, 3, 7$ *or* $(d-1)^4 - (d-1)^3 + (d-1)^2$. *Furthermore, we have the following.*

(i) $\delta'(C) = (d-1)^4 - (d-1)^3 + (d-1)^2$ *if and only if* $p > 0$, $d - 1$ *is a power of* p *and* C *is projectively equivalent to the Fermat curve.*

(ii) $\delta'(C) = 7$ *if and only if* $p = 2$, $d = 4$ *and* C *is projectively equivalent to Klein quartic curve.*

(iii) $\delta'(C) = 3$ *and three Galois points are not contained in a common line if and only if* d *is not divisible by* p, $d - 1$ *is not a power of* p, *and* C *is projectively equivalent to the Fermat curve.*

(iv) $\delta'(C) = 3$ *and three Galois points are contained in a common line if and only if* $p = 2$, $d = 4$ *and* C *is projectively equivalent to the curve defined by*

$$(x^2 + x)^2 + (x^2 + x)(y^2 + y) + (y^2 + y)^2 + c = 0,$$

where $c \in K \setminus \{0, 1\}$.

This is a modified and extended version of the paper [4, Part IV] (which will have been published only in arXiv).

2. Preliminaries

Let $C \subset \mathbb{P}^2$ be a smooth plane curve of degree $d \geq 4$ in characteristic $p > 0$. For a point $P \in C$, we denote by $T_PC \subset \mathbb{P}^2$ the (projective) tangent line at P. For a projective line $l \subset \mathbb{P}^2$ and a point $P \in C \cap l$, we denote by $I_P(C, l)$ the intersection multiplicity of C and l at P. We denote by $\overline{PR}$ the line passing through points P and R when $P \neq R$, and by $\pi_P : C \to \mathbb{P}^1; R \mapsto \overline{PR}$ the projection from a point $P \in \mathbb{P}^2$. If $R \in C$, we denote by e_R the ramification index of π_P at R. It is not difficult to check the following.

Lemma 1. *Let* $P \in \mathbb{P}^2$ *and let* $R \in C$. *Then for* π_P *we have the following.*

(1) *If* $R = P$, *then* $e_R = I_R(C, T_RC) - 1$.

(2) *If* $R \neq P$, *then* $e_R = I_R(C, \overline{PR})$.

Let P be a Galois point. We denote by G_P the group of birational maps from C to itself corresponding to the Galois group $\mathrm{Gal}(K(C)/\pi_P^*K(\mathbb{P}^1))$. We find easily that the group G_P is isomorphic to a subgroup of the automorphism group $\mathrm{Aut}(C)$ of C. We identify G_P with the subgroup. When we use the symbol γ for an automorphism of the curve C, we use the symbol γ^* for the automorphism of the function field $K(C)$ corresponding to γ.

If a Galois covering $\theta : C \to C'$ between smooth curves is given, then the Galois group G acts on C naturally. We denote by $G(R)$ the stabilizer subgroup of R. The following fact is useful to find Galois points (see [15, III. 7.1, 7.2 and 8.2]).

Fact 1. *Let $\theta : C \to C'$ be a Galois covering of degree d with Galois group G and let $R, R' \in C$. Then we have the following.*

(1) *For any $\sigma \in G$, we have $\theta(\sigma(R)) = \theta(R)$.*
(2) *If $\theta(R) = \theta(R')$, then there exists an element $\sigma \in G$ such that $\sigma(R) = R'$.*
(3) *The order of $G(R)$ is equal to e_R at R for any point $R \in C$.*
(4) *If $\theta(R) = \theta(R')$, then $e_R = e_{R'}$.*
(5) *The index e_R divides the degree d.*

We recall a theorem on the structure of the Galois group at a Galois point (see [4, Part II]). Let $d - 1 = p^e l$ (resp. $d = p^e l$), where l is not divisible by p, let ζ be a primitive l-th root of unity, and let $k = [\mathbb{F}_p(\zeta) : \mathbb{F}_p]$. Let $P = (1 : 0 : 0)$ be an inner (resp. outer) Galois point for C. The projection $\pi_P : C \to \mathbb{P}^1$ is given by $(x : y : 1) \mapsto (y : 1)$. We have a field extension $K(x, y)/K(y)$ via π_P. Let $\gamma \in G_P$. Then, the automorphism $\gamma \in G_P$ can be extended to a linear transformation of $\mathbb{P}^2$ (see [1, Appendix A, 17 and 18] or [2]). Let $A_\gamma = (a_{ij})$ be a 3×3 matrix representing γ. Since $\gamma \in G_P$, $\gamma^*(y) = y$. Then, $(a_{21}x + a_{22}y + a_{23}) - (a_{31}x + a_{32}y + a_{33})y = 0$ in $K(x, y)$. Since $d \geq 4$, we have $a_{21} = a_{23} = a_{31} = a_{32} = 0$ and $a_{22} = a_{33}$. We may assume that $a_{22} = a_{33} = 1$. Since $\gamma^{p^e l} = 1$, we have $a_{11}^l = 1$. We take a group homomorphism $G_P \to K \setminus 0; \gamma \mapsto a_{11}(\gamma)$, where $a_{11}(\gamma)$ is the $(1, 1)$-element of A_γ. Then, we have the splitting exact sequence of groups

$$0 \to (\mathbb{Z}/p\mathbb{Z})^{\oplus e} \to G_P \to \langle \zeta \rangle \to 1,$$

and the following theorem.

Theorem 4. *Let $C \subset \mathbb{P}^2$ be a smooth curve and let P be an inner (resp. outer) Galois point. Then, k divides e and $G_P \cong (\mathbb{Z}/p\mathbb{Z})^{\oplus e} \rtimes \langle \zeta \rangle$.*

Remark 1. The condition that k divides e is equivalent to that l divides $p^e - 1$. We give a proof here. If k divides e, $\mathbb{F}_p(\zeta) = \mathbb{F}_{p^k}$ is a subfield of $\mathbb{F}_{p^e}$.

Since $\zeta \in \mathbb{F}_{p^e}$, $\zeta^{p^e-1} = 1$. Since the order of ζ in the multiplicative group $\mathbb{F}_{p^e} \setminus 0$ is l, l divides $p^e - 1$. The converse also holds.

We denote the kernel (resp. quotient) by $\mathcal{K}_P$ (resp. by $\mathcal{Q}_P$). An element $\sigma \in \mathcal{K}_P$ (resp. a generator $\tau \in \mathcal{Q}_P$) is represented by a matrix

$$A_\sigma = \begin{pmatrix} 1 & a_{12}(\sigma) & a_{13}(\sigma) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \left(\text{resp. } A_\tau = \begin{pmatrix} \zeta & a_{12}(\tau) & a_{13}(\tau) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right),$$

where $a_{12}(\sigma), a_{13}(\sigma), a_{12}(\tau), a_{13}(\tau) \in K$. For each non-identity element $\gamma \in G_P$, there exist $\sigma \in \mathcal{K}_P$ and i such that $\gamma = \sigma\tau^i$. Then, there exists a unique line L_γ, which is defined by $(\zeta^i - 1)X + (a_{12}(\sigma) + a_{12}(\tau^i))Y + (a_{13}(\sigma) + a_{13}(\tau^i))Z = 0$, such that $\gamma(R) = R$ for any $R \in L_\gamma$. Note that $P \in L_\gamma$ if and only if $\gamma \in \mathcal{K}_P$. Furthermore, for $\sigma \in \mathcal{K}_P$ and $R \neq P$, $L_\sigma = \overline{RP}$ if and only if $\sigma(R) = R$. For a suitable system of coordinates, we can take $a_{12}(\tau) = a_{13}(\tau) = 0$.

Finally in this section, we note the following facts on automorphisms of $\mathbb{P}^1$.

Lemma 2. *We denote by* $\mathrm{Aut}(\mathbb{P}^1)$ *the automorphism group of* $\mathbb{P}^1$.

(1) *Let* $P_1, P_2, P_3 \in \mathbb{P}^1$ *be three distinct points and let* $\gamma_1, \gamma_2 \in \mathrm{Aut}(\mathbb{P}^1)$. *If* $\gamma_1(P_i) = \gamma_2(P_i)$ *for* $i = 1, 2, 3$, *then* $\gamma_1 = \gamma_2$.
(2) *Let* $P_1, P_2 \in \mathbb{P}^1$ *be distinct points and let* $G \subset \mathrm{Aut}(\mathbb{P}^1)$ *be a finite subgroup. If* $\gamma(P_1) = P_1$ *and* $\gamma(P_2) = P_2$ *for any* $\gamma \in G$, *then* G *is a cyclic group whose order is not divisible by* p *if* $p > 0$.
(3) *Let* l *be not divisible by* p, *let* $P \in \mathbb{P}^1$, *and let* $G \subset \mathrm{Aut}(\mathbb{P}^1)$ *be a subgroup of order* l. *Assume that* G *is cyclic and* $\tau(P) = P$ *for any* $\tau \in G$. *Then, there exists a unique point* Q *such that* $Q \neq P$ *and* $\tau(Q) = Q$ *for any* $\tau \in G$.

Proof. The fact (1) is easily proved, if we use the classical fact that any automorphism of $\mathbb{P}^1$ is a linear transformation. We prove (2). We may assume that $P_1 = (1 : 0)$ and $P_2 = (0 : 1)$. Let $\gamma \in G$. Since $\gamma(P_1) = P_1$ and $\gamma(P_2) = P_2$, γ is represented by a matrix

$$A_\gamma = \begin{pmatrix} a(\gamma) & 0 \\ 0 & 1 \end{pmatrix},$$

where $a(\gamma) \in K$. Then, the homomorphism $\psi : G \to K \setminus 0 : \gamma \mapsto a(\gamma)$ is injective and $\psi(G)$ is cyclic. Let m be the order of $\psi(G)$. Then, $\psi(G)$ is contained in the set $\{x \in K \setminus 0 | x^m - 1 = 0\}$. If m is divisible by p, the set consists of at most m/p elements. Therefore, m is not divisible by p. We have the conclusion.

We prove (3). We may assume that $P = (1 : 0)$. Let τ be a generator of G. Since $\tau(P) = P$ and τ is an automorphism of order l not divisible by p, τ is represented by a matrix

$$A_\tau = \begin{pmatrix} \zeta & b \\ 0 & 1 \end{pmatrix},$$

where ζ is a primitive l-th root of unity and $b \in K$. Then, τ^i is represented by the matrix

$$A_{\tau^i} = \begin{pmatrix} \zeta^i & \dfrac{\zeta^i - 1}{\zeta - 1} b \\ 0 & 1 \end{pmatrix}.$$

Let $Q = (x : 1)$. Then, $\tau^i(Q) = Q$ if and only if $(\zeta - 1)x + b = 0$. We have the conclusion. □

3. Only-if-part of the proof of Theorem 1

Let $p = 2$, let $q = 2^e \geq 4$ and let C be a plane curve of degree $d = q + 1$. Assume that $\delta(C) = d$. Let $P_1, \ldots, P_d$ be inner Galois points for C. By the results of the previous paper [4, Part III, Lemma 1, Propositions 1, 3 and 4], we have the following.

PROPOSITION 1. *Assume that $\delta(C) = d$. Then, we have the following.*

(1) *Galois points $P_1, \ldots, P_d$ are contained in a common line.*
(2) *For any i and any element $\sigma \in G_{P_i} \setminus \{1\}$, the order of σ is two.*
(3) *For any i and any elements $\sigma, \tau \in G_{P_i} \setminus \{1\}$ with $\sigma \neq \tau$, $L_\sigma \neq T_{P_i}C$ and $L_\sigma \neq L_\tau$. In particular, the set $\{T_{P_1}C \cap T_{P_i}C | 2 \leq i \leq d\}$ consists of exactly $d - 1$ points.*

By the condition (1) *and Fact* 1(2), *for each i with $3 \leq i \leq d$, there exists $\tau_i \in G_{P_i}$ such that $\tau_i(P_1) = P_2$. Let $\{Q\} = T_{P_1}C \cap T_{P_2}C$. In addition, we have the following by the condition* (2).

(4) *For any i with $3 \leq i \leq d$, $\tau_i(P_2) = P_1$ and $\tau_i(Q) = Q$.*
(5) *For any i,j with $3 \leq i,j \leq d$, $\tau_i\tau_j(P_1) = P_1$, $\tau_i\tau_j(P_2) = P_2$ and $\tau_i\tau_j(Q) = Q$.*

LEMMA 3. *For a suitable system of coordinates, we may assume that* $P_1 = (1:0:0)$, $P_2 = (0:0:1)$ *and* $Q = (0:1:0)$.

By Lemma 3 and Proposition 1(2)(4), τ_i is given by a matrix

$$A_{\tau_i} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & a_i & 0 \\ a_i^2 & 0 & 0 \end{pmatrix},$$

for some $a_i \in K$. Then, $\tau_i\tau_j$ is given by the matrix

$$A_{\tau_i\tau_j} = \begin{pmatrix} a_j^2 & 0 & 0 \\ 0 & a_i a_j & 0 \\ 0 & 0 & a_i^2 \end{pmatrix}.$$

Let $H(C)$ be the subgroup of $\mathrm{Aut}(\mathbb{P}^2)$ consisting of any $\gamma \in \mathrm{Aut}(\mathbb{P}^2)$ satisfying

(h1) $\gamma(P_1) = P_1$, $\gamma(P_2) = P_2$ and $\gamma(Q) = Q$,
(h2) $\{\gamma(P_i) | 3 \le i \le d\} = \{P_i | 3 \le i \le d\}$, and
(h3) $\gamma(C) = C$.

LEMMA 4. *The group $H(C)$ is a cyclic group whose order is at most $d - 2 = q - 1$.*

PROOF. By the condition (h1) of $H(C)$, for any $\gamma \in H(C)$, γ is represented by a matrix

$$A_\gamma = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

for some $a, b \in K$. We prove that γ depends only on the image of P_3. Precisely, we show that for $\gamma_1, \gamma_2 \in H(C)$, if $\gamma_1(P_3) = \gamma_2(P_3)$, then $\gamma_1 = \gamma_2$. To prove this, it suffices to show that $\gamma = 1$ if $\gamma(P_3) = P_3$. Assume that $\gamma(P_3) = P_3$. Since γ fixes three distinct points P_1, P_2, P_3 on the line $\overline{P_1P_2}$, γ is identity on the line $\overline{P_1P_2}$, by Lemma 2(1) in Section 2. We have $a = 1$, since $\overline{P_1P_2}$ is given by $Y = 0$. On the other hand, by the condition (h3), $\gamma(T_{P_3}C) = T_{P_3}C$. Then, the point Q_0 given by $T_{P_1}C \cap T_{P_3}C$ is fixed by γ. Note that $Q_0 \ne Q, P_1$ by Proposition 1(3)(1) and Fact 1(3). Since γ fixes three distinct points P_1, Q, Q_0 on the line $\overline{P_1Q}$ and $\overline{P_1Q}$ is given by $Z = 0$, we have $b = 1$.

By the above discussion and the condition (h2), the order of $H(C)$ is at most $d - 2 = q - 1$. We consider the group homomorphism $H(C) \to \overline{P_1P_2} \cong \mathbb{P}^1$ given by restrictions, which is well-defined by the condition (h1) of $H(C)$. Then, this is injective by the above discussion. It follows from Lemma 2(2) that $H(C)$ is cyclic. $\square$

We consider the set $S = \{\tau_3\tau_i | 3 \le i \le d\}$. Then, $S \subset H(C)$ by Proposition 1(5)(1). Since the cardinality of S is $q-1$, $S = H(C)$ by Lemma 4. Since $H(C)$ is cyclic, there exists i such that $\tau_3\tau_i$ is a generator of $H(C)$. Therefore, $\tau_3\tau_i$ is given by the matrix

$$A_{\tau_3\tau_i} = \begin{pmatrix} \zeta^2 & 0 & 0 \\ 0 & \zeta & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

where ζ is a primitive $(q-1)$-th root of unity. We denote $\tau_3\tau_i$ by γ.

By Proposition 1(3), there exists an element $\sigma \in G_{P_1} \setminus \{1\}$ such that the $(1,2)$-element $a_{12}(\sigma)$ and $(1,3)$-element $a_{13}(\sigma)$ of a matrix A_σ representing σ are not zero (see also Section 2). If we take a linear transformation ϕ with $Y \mapsto (1/a_{12}(\sigma))Y$ and $Z \mapsto (1/a_{13}(\sigma))Z$, then $\phi(P_i) = P_i$ for $i = 1, 2$, $\phi(Q) = Q$, $\phi \circ \gamma \circ \phi^{-1} = \gamma$ and $\phi \circ \sigma \circ \phi^{-1}$ is represented by the matrix

$$A_0 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Therefore, we may assume that σ is represented by the matrix $A_\sigma = A_0$. The automorphism $\gamma^j\sigma\gamma^{-j}$ is represented by the matrix

$$\begin{pmatrix} 1 & \zeta^j & \zeta^{2j} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

In particular, $\gamma^j\sigma\gamma^{-j} \in G_{P_1}$ for any j with $1 \le j \le q-1$. Since the cardinality of the set $\{\gamma^j\sigma\gamma^{-j} | 1 \le j \le q-1\} \subset G_{P_1}$ is $q-1$, $G_{P_1} = \{\gamma^j\sigma\gamma^{-j} | 1 \le j \le q-1\} \cup \{1\}$. Then, the rational function $g(x, y) := \prod_{\alpha \in \mathbb{F}_q} (x + \alpha y + \alpha^2) \in K(x, y)$ is fixed by any element of G_{P_1}. Therefore, $g(x, y) \in K(y)$. There exists $h(y) \in K(y)$ such that $g(x, y) + h(y) = 0$ in $K(x, y)$. Let $h(y) = h_1(y)/h_2(y)$, where $h_1, h_2 \in K[y]$. Then, $g(x, y)h_2(y) +$

$h_1(y) = 0$ on C. Let $f(x, y)$ be a defining polynomial. Then, there exists $v(x, y) \in K[x, y]$ such that $f(x, y)v(x, y) = g(x, y)h_2(y) + h_1(y)$ as polynomials. Since $P_1 \in C$ is smooth and the tangent line $T_{P_1}C = \overline{P_1Q}$ is given by $Z = 0$, the coefficient of x^{2^e} for $f(x, y)$ as in $(K[y])[x]$ is a constant. Comparing the coefficient of degree 2^e in variable x, we have $v(x, y) \in K[y]$ and $v(x, y) = h_2(y)$ up to a constant. Then, $h_2(y)$ divides $h_1(y)$ and we have $h(y) \in K[y]$. Therefore, we may assume that $f(x, y) = g(x, y) + h(y)$, where $h(y) \in K[y]$. By the condition that the tangent line $T_{P_2}C = \overline{P_2Q}$ is given by $X = 0$, $g(x, y) + cy^{q+1} = 0$ for some $c \in K \setminus 0$. Therefore, we have a defining equation $f(x, y) = g(x, y) + cy^{q+1} = 0$.

Finally in this section, we investigate conditions for the smoothness of C. Let $G(X, Y, Z) := Z^{q+1}g(X/Z, Y/Z)$ and let $F(X, Y, Z) := Z^{q+1}f(X/Z, Y/Z)$. Then, by direct computations, we have $F(Z, Y, X) = F(X, Y, Z)$. Since there exist exactly d points contained in C and the line defined by $Y = 0$, such points are smooth. Therefore, singular points should lie on $Y \neq 0$. Let $h(x, z) = G(x, 1, z)$. We consider h as an element of $K(z)[x]$. Then, the set $\{\alpha + \alpha^2 z | \alpha \in \mathbb{F}_q\} \subset K(z)$, which consists of all roots of $h(x, z) = 0$, forms an additive subgroup of $K(z)$. According to [8, Proposition 1.1.5 and Theorem 1.2.1], we have the following.

Lemma 5. *The polynomial $h(x, z) \in K(z)[x]$ has only terms of degree equal to some power of p. In particular, $h_x(x, z) = z^q + z$, where h_x is a partial derivative by x.*

Assume that $(x, z) \in C$ is a singular point, i.e. $h_x(x, z) = h_z(x, z) = 0$. Then, (x, z) is $\mathbb{F}_q$-rational by Lemma 5. We have $c \neq 1$ by the following.

Lemma 6. *The equality $\{h(x, z) | x, z \in \mathbb{F}_q\} = \{0, 1\}$ holds.*

Proof. If $z = 0$, then $h(x, z) = 0$. We fix $z_0 \in \mathbb{F}_q \setminus 0$. We consider $h(x, z_0) = z_0 \prod_{\alpha \in \mathbb{F}_q} (x + \alpha + \alpha^2 z_0) \in \mathbb{F}_q[x]$. For each $\alpha \in \mathbb{F}_q$, there exists a unique $\beta \in \mathbb{F}_q$ with $\beta \neq \alpha$ such that $\alpha + \alpha^2 z_0 = \beta + \beta^2 z_0$. Therefore, the cardinality of the set $S_0 := \{\alpha + \alpha^2 z_0 | \alpha \in \mathbb{F}_q\}$ is $q/2 = 2^{e-1}$. By direct computations, we find that any element of S_0 is a root of the separable polynomial $h_0(x) = \sum_{i=0}^{e-1} z_0^{2^i} x^{2^i}$, which is of degree $q/2$. Then, $h(x, z_0) = h_0(x)^2$ as elements of $\mathbb{F}_q[x]$. Then, by direct computations, we have $h_0(x)(h_0(x) + 1) = z_0(x^q + x)$

as elements of $\mathbb{F}_q[x]$. Assume $x \in \mathbb{F}_q$. Then, $h_0(x)(h_0(x)+1) = 0$. Therefore, $h(x, z_0) = 0$ or 1. If we take $x \in \mathbb{F}_q \setminus S_0$, then $h_0(x) \neq 0$ and hence, $h(x, z_0) = 1$. □

4. If-part of the proof of Theorem 1

We use the same notation as in the previous section, g, f, F, and so on. Let C be the plane curve given by Equation (1c) with $c \in K \setminus \{0, 1\}$. As in the previous section, C is smooth. We prove $\delta(C) = d$. We consider the projection π_{P_1} from $P_1 = (1:0:0)$. Then, we have the field extension $K(x, y)/K(y)$ with $f(x, y) = g(x, y) + cy^{q+1} = 0$. Since $(x + \alpha y + \alpha^2) + \beta y + \beta^2 = x + (\alpha + \beta)y + (\alpha + \beta)^2$, we have $f(x + \alpha y + \alpha^2, y) = f(x, y)$ for any $\alpha \in \mathbb{F}_q$. Therefore, P_1 is Galois. By the symmetric property of $F(X, Y, Z)$ for X, Z, we find that a point $(0:0:1)$ is also inner Galois for C. We also find that there exist a tangent line T such that $I_Q(C, T) = 2$ for some $Q \in C \cap T$. Therefore, C is not projectively equivalent to the Fermat curve of degree $q+1$ (see, for example, [13]). According to [4, Part III, Lemma 1 and Proposition 1], we have $\delta(C) = d$.

Remark 2. The projective equivalence class of the plane curve given by Equation (1c) is uniquely determined by a constant $c \in K \setminus 0$. Therefore, infinitely many classes exist. Precisely, we have Lemma 7 below.

Lemma 7. *Let $a, b \in K \setminus 0$ and let C_a (resp. C_b) be the plane curve given by Equation* (1c) *with $c = a$ (resp. $c = b$). If there exists a projective transformation ϕ such that $\phi(C_a) = C_b$, then $a = b$.*

Proof. Let $P_1, \ldots, P_d$ be inner Galois points for C_a, which are contained in the line defined by $Y = 0$. Then, $P_1, \ldots P_d$ are also inner Galois for C_b. Since the tangent lines $T_P C_a$ and $T_P C_b$ at $P = (\alpha^2 : 0 : 1)$ with $\alpha \in \mathbb{F}_q$ are given by the same equation $X + \alpha Y + \alpha^2 Z = 0$, $T_{P_i} C_a = T_{P_i} C_b$ for $i = 1, \ldots, d$. We may assume that $P_1 = (1:0:0)$, $P_2 = (0:0:1)$ and $P_3 = (1:0:1)$. Let $Q_2 = (0:1:0)$ and let $Q_3 = (1:1:0)$. Then, $T_{P_1} C_a \cap T_{P_2} C_a = T_{P_1} C_b \cap T_{P_2} C_b = \{Q_2\}$ and $T_{P_1} C_a \cap T_{P_3} C_a = T_{P_1} C_b \cap T_{P_3} C_b = \{Q_3\}$. Let ϕ be a linear transformation such that $\phi(C_a) = C_b$.

If $\phi(P_1) = P_i$ for some $i \neq 1$, then we take $\sigma \in G_{P_j}(C_b)$ for some j such that $\sigma(P_i) = P_1$, by Fact 1(2). Then, $\sigma \circ \phi(P_1) = P_1$. Therefore, there exists a linear transformation ϕ such that $\phi(C_a) = C_b$ and $\phi(P_1) = P_1$. If $\phi(P_2) = P_i$ for some $3 \leq i \leq d$, then we take $\tau \in G_{P_1}(C_b)$ such that

$\tau(P_3) = P_2$, by Fact 1(2). Then, $\tau \circ \phi(P_2) = P_2$. Therefore, there exists a linear transformation ϕ such that $\phi(C_a) = C_b$, $\phi(P_1) = P_1$ and $\phi(P_2) = P_2$. If $\phi(P_3) = P_i$ for some $4 \le i \le d$, then we take $\gamma \in H(C_b)$ such that $\gamma(P_i) = P_3$, where $H(C_b)$ is the group for C_b discussed in the previous section. Then, $\gamma \circ \phi(P_3) = P_3$. Therefore, there exists a linear transformation ϕ such that $\phi(C_a) = C_b$, $\phi(P_i) = P_i$ for $i = 1, 2, 3$ and $\phi(Q_j) = Q_j$ for $j = 2, 3$. Since $\phi(P_1) = P_1, \phi(P_2) = P_2$ and $\phi(Q_2) = Q_2$, ϕ is represented a matrix

$$A_\phi = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}$$

for some $\lambda_1, \lambda_2, \lambda_3 \in K \setminus 0$. Since $\phi(P_3) = P_3$ and $\phi(Q_3) = Q_3$, we have $\lambda_1 = \lambda_3$ and $\lambda_1 = \lambda_2$. Then, ϕ is identity. Therefore, by considering the defining equations of C_a and C_b, we should have $a = b$. □

REMARK 3. If $c = 1$, then the plane curve C defined by Equation (1c) is parameterized as $\mathbb{P}^1 \to \mathbb{P}^2 : (s : 1) \mapsto (s^{q+1} : s^q + s : 1)$. The distribution of Galois points for this curve has been settled in [6].

5. Proof of Theorem 2 (The case where $l \ge 3$)

If we have two outer Galois points, then we note the following (see Section 2).

LEMMA 8. *Let P, P_2 be outer Galois points for C. Then, any element $\gamma \in G_P$ can be extended to a linear transformation of $\mathbb{P}^2$, and hence $\gamma(P_2) \in \mathbb{P}^2$ is also outer Galois for C.*

Let $d = p^e l$, where $e \ge 1$, $l \ge 3$ and l divides $p^e - 1$, and let $P = (1 : 0 : 0)$ be an outer Galois point. It follows from a generalization of Pardini's theorem by Hefez [9, (5.10) and (5.16)] and Homma [12] that the generic order of contact for C is equal to 2, i.e. $I_R(C, T_R C) = 2$ for a general point $R \in C$ (see also [10, 11]).

Let $M \subset \mathbb{P}^2$ be a projective line with $P \in M$. Note that $\gamma(M) = M$ for any $\gamma \in G_P$, by the forms of the matrices A_σ and A_τ as in Section 2. The homomorphism $r_P[M] : G_P \to \mathrm{Aut}(M)$, which is induced by the restriction, is well-defined. Then, the kernel Ker $r_P[M]$ is a subgroup of $\mathcal{K}_P$ and the cardinality of Ker $r_P[M]$ is a power of p, since $\gamma \in$ Ker $r_P[M]$ if and only if

$L_\gamma = M$. We denote it by $p^{v[M]}$. Since the kernel Ker $r_P[M]$ is a subspace of G_P as $\mathbb{F}_p$-vector spaces, we have the following diagram.

$$\begin{array}{ccccccccc} & & (\mathbb{Z}/p\mathbb{Z})^{\oplus v[M]} & \cong & \text{Ker } r_P[M] & & & & \\ & & \downarrow & & \downarrow & & & & \\ 0 & \rightarrow & (\mathbb{Z}/p\mathbb{Z})^{\oplus e} & \rightarrow & G_P & \rightarrow & \langle\zeta\rangle & \rightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \rightarrow & (\mathbb{Z}/p\mathbb{Z})^{\oplus e-v[M]} & \rightarrow & \text{Im } r_P[M] & \rightarrow & \langle\zeta\rangle & \rightarrow & 1 \end{array}$$

Using lower splitting exact sequence as groups, we have the following.

Lemma 9. *The integer l divides $p^{e-v[M]} - 1$ for any line M with $P \in M$.*

Hereafter in this section, we assume that $P_2 \in \mathbb{P}^2 \setminus \{P\}$ is an outer Galois point for C.

Proposition 2. *Assume that $l \geq 3$. Then:*

(1) *$v[\overline{PP_2}] = e$, and there exists a unique point $Q \in \mathbb{P}^2$ with $Q \neq P$ such that $\gamma(Q) = Q$ for any $\gamma \in G_P$.*

Let Q be the point as in (1). *Furthermore, we have the following.*

(2) *If $l \geq 5$, then $P_2 = Q$.*
(3) *If $l = 4$ and $P_2 \neq Q$, then $Q \in C$ or there exist two outer Galois point P_3, P_4 such that $\gamma(P_4) = P_4$ for any $\gamma \in G_{P_3}$.*
(4) *If $l = 3$ and $P_2 \neq Q$, then $Q \in C$.*

Proof. Let $\gamma \in G_P \setminus \mathcal{K}_P$ and let L_γ be the line, which is a fixed locus, defined as in Section 2. The set $C \cap L_\gamma$ consists of d points, because $T_R C = \overline{PR} \neq L_\gamma$ if $R \in C \cap L_\gamma$ by Fact 1(3) and Lemma 1(2). Let $\tau \in \mathcal{Q}_P$ be a generator and let L_τ be the line, defined as in Section 2. We denote $v[\overline{PP_2}]$ by v and assume that $v < e$.

We consider the case where $\gamma(P_2) = P_2$ for some $\gamma \in G_P \setminus \mathcal{K}_P$. Let $\sigma \in \mathcal{K}_{P_2}$. Then, $\sigma(R) \in L_\gamma$ and $\sigma(R) \neq R$ if $R \in C \cap L_\gamma$, by Fact 1(1)(3) and that L_γ consists of exactly d points. Furthermore, $\sigma(P) \in T_{\sigma(R_1)}C \cap T_{\sigma(R_2)}C = \{P\}$, if $R_1, R_2 \in C \cap L_\gamma$ with $R_1 \neq R_2$. Therefore, we should have $\sigma(P) = P$. This is a contradiction to $v < e$.

We consider the case where $\gamma(P_2) \neq P_2$ for any $\gamma \in G_P \setminus \mathcal{K}_P$. Assume that $\gamma_1(P_2) = \gamma_2(P_2)$ for $\gamma_1, \gamma_2 \in G_P$. Note that any element $\gamma \in G_P$ is represented as $\gamma = \sigma\tau^i$ for some $\sigma \in \mathcal{K}_P$ and some i (see Section 2). Let

$\gamma_1 = \sigma_1 \tau^i$ and $\gamma_2 = \sigma_2 \tau^j$, where $\sigma_1, \sigma_2 \in \mathcal{K}_P$. Since $(\tau^{-j} \sigma_2^{-1} \sigma_1 \tau^j)\tau^{i-j}(P_2) = P_2$ and $\tau^{-j}\sigma_2^{-1}\sigma_1\tau^j \in \mathcal{K}_P$, we have $i = j$ and $\gamma_2^{-1}\gamma_1 \in \mathcal{K}_P$ by the assumption. Furthermore, we have $\gamma_2^{-1}\gamma_1 \in \mathrm{Ker}\, r_P[\overline{PP_2}]$, since $\gamma_2^{-1}\gamma_1(P) = P$ and $\gamma_2^{-1}\gamma_1(P_2) = P_2$. Therefore, we have $p^{e-v}l + 1$ outer Galois points on the line $\overline{PP_2}$, by Lemma 8 and that the group $\mathrm{Im}\, r_P[\overline{PP_2}]$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{\oplus e-v} \rtimes \langle \zeta \rangle$.

Let $R \in C \cap L_\tau$. We consider points on the line $\overline{PR}$. Let $\sharp G_P(R) = p^b l$, where $G_P(R)$ is the stabilizer subgroup at R. Then we have p^{e-b} flexes of order $(\sharp G_P(R) - 2)$ by Fact 1(3). We note that $(p^b l - 2)p^{e-b} \geq p^e(l-2)$. Furthermore, for each outer Galois points, we spent at least degree $(d-1)(p^e(l-2))$ as the degree of the Wronskian divisor. Therefore, it follows from the degree of Wronskian divisor ([16, Theorem 1.5]) that

$$(p^{e-v}l + 1)(d-1)p^e(l-2) \leq 3d(d-2).$$

Then, we have

$$(p^{e-v}l + 1)p^e(l-2) < 3d = 3p^e l.$$

Therefore, $(p^{e-v}l + 1)(l-2) - 3l < 0$. Note that $p^{e-v} - 1 \geq l$ by Lemma 9. Then, $(l^2 + l + 1)(l-2) - 3l < 0$. This is a contradiction. Therefore, $v = e$.

In particular, the group $\mathrm{Im}\, r_P[\overline{PP_2}]$ is a cyclic group of order l. By Lemma 2(3) in Section 2, a fixed point by the group $\mathrm{Im}\, r_P[\overline{PP_2}]$ which is different from P is uniquely determined. We denote it by Q. Then, $\gamma(Q) = Q$ for any $\gamma \in G_P$, since $\gamma = \sigma\tau^i$ for some $\sigma \in \mathcal{K}_P$ and some i. We have (1).

We prove (2). Assume that $P_2 \neq Q$. Since the group $\mathrm{Im}\, r_P[\overline{PP_2}]$ is a cyclic group of order l, we have $l + 1$ outer Galois points on the line $\overline{PP_2}$, by Lemma 8. Furthermore, for each outer Galois point, we spent at least degree $(d-1)p^e(l-2)$ as the degree of the Wronskian divisor, similarly to the proof of (1). Therefore, it follows from the degree of Wronskian divisor ([16, Theorem 1.5]) that

$$(l+1)(d-1)p^e(l-2) \leq 3d(d-2).$$

Then, we have

$$(l+1)p^e(l-2) < 3d = 3p^e l.$$

Therefore, $(l+1)(l-2) - 3l < 0$. Then, $l^2 - 4l - 2 < 0$. We have $l \leq 4$.

We prove (3). Assume that $P_2 \neq Q$ and $Q \notin C$. Since $\mathrm{Im}\, r_P[\overline{PP_2}]$ is a cyclic group of order l, the cardinality of $C \cap \overline{PP_2}$ is equal to l and there exists $l + 1$ outer Galois points on $\overline{PP_2}$, by Fact 1(3), Lemma 8 and the assumption. Let $C \cap \overline{PP_2} = \{R_1, \ldots, R_l\}$ and let $P, P_2, \ldots, P_{l+1}$ be outer Galois points.

Let $l=4$. The restriction $r_P[\overline{PP_2}](\tau)$ of the generator $\tau \in \mathcal{Q}_P$ is a generator of Im $r_P[\overline{PP_2}]$. We may assume that $\tau(R_i)=R_{i+1}$ for $i=1,2,3,4$, where $R_5=R_1$. We can take $\eta_j \in$ Im $r_{P_j}[\overline{PP_2}]$ such that $\eta_j(R_1)=R_2$ for $j=2,3,4,5$ by Fact 1(2). We consider the case where at least three elements of $\{\eta_j\}$ are of order 4. We may assume that η_2, η_3, η_4 are of order 4. Assume that $\eta_j(R_2)=R_4$ for any j with $2 \le j \le 4$. Then, we have $\eta_j(R_4)=R_3$. Since three points on the line $\overline{PP_2}$ has the same images under η_2, η_3, η_4, these are the same automorphism of the line $\overline{PP_2}$ by Lemma 2(1). Then, η_j fixes P_2, P_3, P_4 for $j=2,3,4$, because $\eta_j(P_j)=P_j$. This implies that η_j is identity on $\overline{PP_2}$, by Lemma 2(1). This is a contradiction. Therefore, there exists j such that $\eta_j(R_2)=R_3$. Then, we have $\eta_j(R_3)=R_4$. Therefore, τ coincides with η_j on the line $\overline{PP_2}$. Then, $\tau(P_j)=\eta_j(P_j)=P_j \ne Q$. This implies that τ fixes P_1, P_j and Q. This is a contradiction.

We consider the case where there exist distinct j,k such that η_j and η_k is of order 2. Then, $\eta_j(R_2)=R_1$, $\eta_j(R_3)=R_4$ and $\eta_j(R_4)=R_3$. This holds also for η_k. Then $\eta_j=\eta_k$ on the line $\overline{PP_2}$ by Lemma 2(1). Then, $\eta_j(P_k)=\eta_k(P_k)=P_k$. Since the group Im $r_{P_j}[\overline{PP_2}]$ is cyclic, $\eta(P_k)=P_k$ for any $\eta \in$ Im $r_{P_j}[\overline{PP_2}]$, by Lemma 2(3). If we take $j=3$ and $k=4$, then we have the conclusion, since any element of G_{P_j} is a product of elements of $\mathcal{K}_{P_j}$ and of $\mathcal{Q}_{P_j}$.

We prove (4). Let $l=3$. Assume that $P_2 \ne Q$ and $Q \notin C$. We may assume that $\tau \in G_P$ satisfies that $\tau(R_i)=R_{i+1}$ for $i=1,2,3$, where $R_4=R_1$. We can take $\eta \in G_{P_2}$ such that $\eta(R_1)=R_2$, by Fact 1(2). Then, we have $\eta(R_2)=R_3$ and $\eta(R_3)=R_1$. This implies that τ coincides with η on $\overline{PP_2}$, by Lemma 2(1). Therefore, $\tau(P_2)=\eta(P_2)=P_2 \ne Q$. This is a contradiction. □

Let $Q \in \mathbb{P}^2 \setminus \{P\}$ be the point such that $\gamma(Q)=Q$ for any $\gamma \in G_P$, as in Proposition 2. We may assume that $Q=(0:1:0)$ for a suitable system of coordinates. Then, the line $\overline{PQ}=\overline{PP_2}$ is defined by $Z=0$. Using Proposition 2(1), we can determine the defining equation of C, as follows.

Proposition 3. *The curve C is projectively equivalent to a plane curve whose defining equation is of the form* $f(x,y)=\left(\sum_{0\le m\le e} \alpha_m x^{p^m}\right)^l + h(y)=0$, *where $\alpha_e, \ldots, \alpha_0 \in K$ and $h(y) \in K[y]$ is a polynomial. Furthermore, $\alpha_e\alpha_0 \ne 0$, the derivative $h'(y)$ is of degree $d-2$, and polynomials $h(y)$ and $h'(y)$ do not have a common root.*

Proof. Let $\sigma \in \mathcal{K}_P$ and let $\tau \in \mathcal{Q}_P$ be a generator, as in Section 2. We may assume that $\tau^*(x)=\zeta x$ and $\tau^* y = y$ for $\tau^*: K(C) \to K(C)$, where ζ is a primitive l-th root of unity. Let A_σ be a matrix representing $\sigma \in \mathcal{K}_P$ as in Section 2. Since L_σ is defined by $Z = 0$, the $(1,2)$-element of A_σ is zero. Since the group $\mathcal{K}_P$ is a $\mathbb{F}_p(\zeta)$-vector space, we have a system of basis $b_1, \dots, b_m$, where $km = e$. For any $\sigma \in \mathcal{K}_P$, the $(1,3)$-element of A_σ is given by $\alpha_1 b_1 + \cdots + \alpha_m b_m$ for some $(\alpha_1, \dots, \alpha_m) \in \oplus^m \mathbb{F}_p(\zeta)$. We define $g_0(x) = \prod_{(\alpha_1,\dots,\alpha_m)} (x + \Sigma_i \alpha_i b_i)$, where the subscript $(\alpha_1, \dots, \alpha_m) \in \oplus^m \mathbb{F}_p(\zeta)$ is taken over all elements. Let $g = g_0^l$. Then, we find easily that $\gamma g(x) = g(x)$ for any element $\gamma \in G_P$. Therefore, there exists an element $h(y) \in K(y)$ such that $g(x) + h(y) = 0$ in $K(C)$. Then, $h(y)$ is a polynomial of degree at most d by considering the degree of C. On the other hand, the set $\left\{ \sum_i \alpha_i b_i | \alpha_i \in \mathbb{F}_p(\zeta) \right\} \subset K$, which consists of all roots of $g_0(x) = 0$, forms an additive subgroup of K. According to [8, Proposition 1.1.5 and Theorem 1.2.1], the polynomial g_0 has only terms of degree equal to some power of p, i.e. $g_0 = \alpha_e x^{p^e} + \cdots + \alpha_1 x^p + \alpha_0 x$ for some $\alpha_e, \dots, \alpha_0 \in K$. Since g_0 is separable and has p^e roots, we have $\alpha_e \alpha_0 \neq 0$.

Finally, we prove that the degree of $h'(y)$ is $d-2$, and $h(y)$ and $h'(y)$ do not have a common root. Since $h(y)$ is of degree at most $d = p^e l$, $h'(y)$ is of degree at most $d-2$. Let $F(X,Y,Z) = f(X/Z, Y/Z)Z^d$, $G_0(X,Z) = g_0(X/Z)Z^{p^e}$ and $H(Y,Z) = h(Y/Z)Z^d$. Then, $F_X = lG_0^{l-1}(\alpha_0 Z^{p^e-1})$, $F_Y = H_Y$ and $F_Z = lG_0^{l-1}(\alpha_0 X Z^{p^e-2}) + H_Z$. We have $F_X(X,Y,0) = 0$. Since $d = p^e l$, $F_Y(X,Y,0) = H_Y(Y,0) = 0$. Assume that $h'(y)$ is of degree at most $d-3$. Then, $F_Z(X,Y,0) = 0 + H_Z(Y,0) = 0$. Therefore, C has singular points on the line defined by $Z = 0$. This is a contradiction to the smoothness of C. On the other hand, if there exist $b \in K$ such that $h(b) = h'(b) = 0$, then a point $(a : b : 1)$ with $g_0(a) = 0$ is a singular point. □

LEMMA 10. *Let C be the plane curve given by the equation as in Proposition 3. Then, $Q \in \mathbb{P}^2 \setminus C$ and $Q \neq P_2$.*

PROOF. It follows from Lemma 2(1) and Fact 1(4) that $L_\sigma = \overline{PP_2}$ for any $\sigma \in \mathcal{K}_{P_2}$. Therefore, any ramified point $R \in C$ of π_{P_2} with $Z \neq 0$ is tame. Let π_Q be the projection from Q. Note that $\pi_Q(x : y : 1) = (x : 1)$. By the form of π_Q, if $x - x_0$ is a local parameter at $(x_0, y_0) \in C$, then (x_0, y_0) is not a ramification point. For a point (x_0, y_0) with $f_x(x_0, y_0) = lg_0(x_0)^{l-1} \neq 0$, $y - y_0$ is a local parameter. Therefore, ramification points of π_Q in $Z \neq 0$ is contained in the locus $\dfrac{dx}{dy} = -\dfrac{h'(y)}{f_x} = 0$, which is equivalent to $h'(y) = 0$. Therefore, there exist $d-2$ lines $l_1, \dots, l_{d-2}$ which contain P and d ramification points of π_Q, by Proposition 3. Since $P_2 \neq P$, for any ramification point R of π_Q, the cardinality of the set $\overline{P_2R} \cap \{R' \in C | Q \in T_{R'}C\} \subset \overline{P_2R} \cap \bigcup_{i=1}^{d-2} l_i$ is at most $d-2$.

Assume that $Q \in C$. It follows from Fact 1(3) that $I_Q(C, \overline{PQ}) = d$. By Fact 1(3) again, $\gamma(Q) = Q$ for any $\gamma \in G_{P_2}$. Let $R \in C$ be a ramification point of π_Q in $Z \neq 0$. It follows from Lemma 1(2) that $Q \in T_RC$. Since $\gamma(Q) = Q$ for any $\gamma \in G_{P_2}$, $Q \in T_{\gamma(R)}C$ for any $\gamma \in G_{P_2}$. Then, the cardinality of $C \cap \overline{P_2R}$ is d and $Q \in T_{R'}C$ for any $R' \in C \cap \overline{P_2R}$. This is a contradiction to that the cardinality of $\overline{P_2R} \cap \{R' \in C | Q \in T_{R'}C\}$ is at most $d-2$. Therefore, $Q \in \mathbb{P}^2 \setminus C$.

Assume that $Q \in \mathbb{P}^2 \setminus C$ and $Q = P_2$. Then, the set $C \cap \overline{PP_2}$ contains l points, since the group Im $r_P[\overline{PP_2}]$ is cyclic of order l. Let $\tau_2 \in \mathcal{Q}_{P_2}$ be a generator and let L_{τ_2} be the line defined as in Section 2. Then, the locus $\Sigma = \bigcup_{\sigma \in \mathcal{K}_{P_2}} \sigma(L_{\tau_2})$ consists of p^e lines. By considering the order of G_{P_2}, the ramification locus of π_Q in the affine plane $Z \neq 0$ is contained in the locus Σ. Note that the set $\bigcap_{\sigma \in \mathcal{K}_{P_2}} \sigma(L_{\tau_2})$ consists of a unique point, which is not contained in C, by Fact 1(3) and that the set $C \cap \overline{PP_2}$ contains two or more distinct points. Since the set $C \cap \sigma(L_{\tau_2})$ consists of exactly d points for any $\sigma \in \mathcal{K}_{P_2}$, the number of ramification points in $Z \neq 0$ is exactly $p^e \times d$. On the other hand, for each $b \in K$ with $h'(b) = 0$, there exist exactly d points (a, b) such that $f(a, b) = 0$, since $\alpha_e\alpha_0 \neq 0$ and $h(b) \neq 0$ by Proposition 3. Therefore, $h'(y)$ has exactly p^e roots. Let R be a ramification point of π_Q which is contained in $Z \neq 0$. Since R is tame (stated above), e_R is computed as the order of $\dfrac{dx}{dy} = -\dfrac{h'(y)}{f_x}$ at R plus one. Since $e_R = l$ for any ramification point $R \in C$ with $Z \neq 0$, the polynomial $h'(y)$ is divisible by $(y-b)^{l-1}$ if $h'(b) = 0$. Therefore, $h'(y)$ should be of the form $c(y-b_1)^{l-1} \cdots (y-b_{p^e})^{l-1}$, which is of degree $p^e(l-1)$. Since $h'(y)$ is of degree p^el-2, by Proposition 3, we have $p^e = 2$. Since $l \geq 3$ divides $p^e - 1 = 1$, this is a contradiction. □

Proof of Theorem 2 (when $l \geq 3$). It follows from Lemma 10 that $P_2 \neq Q$ and $Q \notin C$. If $l \geq 5$ or $l = 3$, then this is a contradiction to Proposition 2(2)(4). Assume that $l = 4$. Then, by Proposition 2(3), there exists two distinct outer Galois points P_3, P_4 such that $\gamma(P_4) = P_4$ for any $\gamma \in G_{P_3}$. Then, the point P_4 satisfies the condition of "Q" as in Proposition 2(1) for P_3. Then, this is a contradiction to Lemma 10. □

6. Proof of Theorem 2 (The case where $l \leq 2$)

Let $p \geq 3$, let $e \geq 1$, let $l \leq 2$ and let C be a smooth plane curve of degree $d = p^e l \geq 4$. We denote by $L_\infty \subset \mathbb{P}^2$ the line defined by $Z = 0$. Let $P \in \mathbb{P}^2 \setminus C$ be Galois with respect to C. Assume that $P = (1 : 0 : 0)$. Let $\gamma \in G_P$ and let A_γ be a 3×3 matrix representing γ. Then,

$$A_\gamma = \begin{pmatrix} a_{11}(\gamma) & a_{12}(\gamma) & a_{13}(\gamma) \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

where $a_{11}(\gamma) = \pm 1$ and $a_{12}(\gamma), a_{13}(\gamma) \in K$. Then, $\gamma^*(x) = a_{11}(\gamma)x + a_{12}(\gamma)y + a_{13}(\gamma)$. Note that $\mathcal{K}_P = \{\gamma \in G_P | a_{11}(\gamma) = 1\}$. Let $g(x, y) := \prod_{\sigma \in \mathcal{K}_P} (x + a_{12}(\sigma)y + a_{13}(\sigma))$. Note that the set of roots $\{a_{12}(\sigma)y + a_{13}(\sigma) | \sigma \in \mathcal{K}_P\} \subset K(y)$ forms an additive subgroup of $K(y)$. According to [8, Proposition 1.1.5 and Theorem 1.2.1], $g(x, y) \in K[y][x]$ has only terms of degree equal to some power of p in variable x. Therefore, $g(x, y) = \alpha_e(y)x^{p^e} + \alpha_{e-1}(y)x^{p^{e-1}} + \cdots + \alpha_1(y)x^p + \alpha_0(y)x$ for some $\alpha_e(y), \ldots, \alpha_0(y) \in K[y]$ with $\deg \alpha_i(y) \leq p^e - p^i$ for $i = 0, \ldots, e$. Then, $\alpha_e(y) = 1$ and $\alpha_0(y) = \prod_{\sigma \in \mathcal{K}_P \setminus 0} (a_{12}(\sigma)y + a_{13}(\sigma))$.

Assume that $l = 1$. Then, $\mathcal{K}_P = G_P$ and $g \in K(y)$, since $\sigma^* g = g$ for any $\sigma \in G_P$. There exists $h(y) \in K(y)$ such that $g(x, y) + h(y) = 0$ in $K(x, y)$. Let $h(y) = h_1(y)/h_2(y)$, where $h_1, h_2 \in K[y]$. Then, $g(x, y)h_2(y) + h_1(y) = 0$ on C. Let $f(x, y)$ be a defining polynomial. Then, there exists $v(x, y) \in K[x, y]$ such that $f(x, y)v(x, y) = g(x, y)h_2(y) + h_1(y)$ as polynomials. Since $(1 : 0 : 0) \notin C$, $f(x, y)$ has the term of degree p^e in variable x. Comparing the coefficient of degree p^e in variable x, we have $v(x, y) \in K[y]$ and $v(x, y) = h_2(y)$ up to a constant. Then, $h_2(y)$ divides $h_1(y)$ and we have $h(y) \in K[y]$. Therefore, $g(x, y) + h(y)$ is a defining polynomial.

Lemma 11. *Assume that $l = 1$. Then, the defining equation of C is of the form $g(x, y) + h(y) = 0$, where $g(x, y) \in K[y][x]$ has only terms of degree equal to some power of p in variable x.*

Assume that $\delta'(C) \geq 2$. Let $P_2 \in \mathbb{P}^2 \setminus (C \cup \{P\})$ be Galois with respect to C. By taking a suitable system of coordinates, we may assume that $P_2 = (0 : 1 : 0)$. Then, $\overline{PP_2} = L_\infty$. Similar to the previous section, we consider the group homomorphism $r_P : G_P \to \mathrm{Aut}(\overline{PP_2})$, which is induced by the restriction. The cardinality of the kernel Ker r_P is a power of p. We denote it by p^v. Obviously, $0 \leq v \leq e$. Then, Ker $r_P = \{\sigma \in G_P | \sigma(P_2) = P_2\}$, since $P_2 \in L_\sigma$ if and only if $\sigma(P_2) = P_2$ for $\sigma \in \mathcal{K}_P$. Since $a_{12}(\sigma) = 0$ if and only if $\sigma \in \mathcal{K}_P$, $\alpha_0(y)$ is of degree $p^e - p^v$ in variable y.

Lemma 12. *If $l = 1$, then $v = e$.*

Proof. We assume that $v < e$. Then, the defining polynomial $g(x, y) + h(y)$ has the term $\alpha_0(y)x$, which is of degree $p^e - p^v > 0$ in variable y. Since $P_2 = (0 : 1 : 0)$ is Galois, the defining polynomial $g(x, y) + h(y)$ has only terms of degree equal to some power of p in variable y, by Lemma 11. Therefore, $p^e - p^v = p^v(p^{e-v} - 1)$ is a power of p. Then, $p^{e-v} - 1 = p^b$ for some integer b. This implies $b = 0$ and $p = 2$. This is a contradiction. □

By Lemmas 11 and 12, we have a defining equation $g(x) + h(y) = 0$, where g, h have only terms of degree equal to some power of p. It is not difficult to check that C is singular. This is a contradiction.

Assume that $l = 2$. Let $\tau \in G_P \setminus \mathcal{K}_P$. Then, $\tau(x, y) = (-x + a_{12}(\tau)y + a_{13}(\tau), y)$ for some $a_{12}(\tau), a_{13}(\tau) \in K$. Then, $G_P = \{\sigma\tau^i | \sigma \in \mathcal{K}_P, i = 0, 1\}$. Note that $\sigma\tau(x, y) = (-x + (a_{12}(\sigma) + a_{12}(\tau))y + (a_{13}(\sigma) + a_{13}(\tau)), y)$. Therefore, $\hat{g}(x, y) := \prod_{\gamma \in G_P} \gamma^*(x) = g(x, y) \times g(-x + a_{12}(\tau)y + a_{13}(\tau), y) = -g^2(x, y) - g(x, y)g(-a_{12}(\tau)y - a_{13}(\tau), y)$, since $g(x, y)$ is linear in variable x. Since $\gamma^*\hat{g}(x, y) = \hat{g}(x, y)$ for any $\gamma \in G_P$, there exists $h(y) \in K(y)$ such that $f(x, y) := \hat{g}(x, y) + h(y) = 0$ in $K(x, y)$. Then, $h(y)$ is a polynomial and $f(x, y)$ is a defining polynomial (similarly to the case $l = 1$).

Lemma 13. *Assume that $l = 2$. Then, the defining equation of C is of the form $g^2(x, y) + g(x, y)g(ay + b, y) + h(y) = 0$, where $a, b \in K$ and $g \in K[y][x]$ has only terms of degree equal to some power of p in variable x.*

We consider $P_2 = (0 : 1 : 0)$. It follows from Lemma 13 that there exist polynomials $g_1(x, y) \in K[x][y]$ and $h_1(x) \in K[x]$ such that $g_1(x, y)$ has only terms of degree equal to some power of p in variable y and $f_1(x, y) := g_1^2(x, y) + g_1(x, y)g_1(x, cx + d) + h_1(x)$ is a defining polynomial of C for some $c, d \in K$. Let $g_1(x, y) = \beta_e(x)y^{p^e} + \beta_{e-1}(x)y^{p^e - 1} + \cdots + \beta_0(x)y$, where $\beta_e(x) = 1$ and $\beta_{e-1}(x), \ldots, \beta_0(x) \in K[x]$. Since $f(x, y)$ and $f_1(x, y)$ are defining polynomials of C, we have $cf(x, y) = f_1(x, y)$ for some $c \in K$.

LEMMA 14. *If $l = 2$, then $v = e$.*

PROOF. Assume that $v < e$. Firstly we prove that $p = 3$ and $v = e - 1$. Now, $\alpha_0(y)$ is of degree $p^e - p^v > 0$. Considering the polynomials $g^2(x, y)$, $g(x, y)g(ay + b, y)$ and $h(y), f(x, y)$ has the term $\alpha_0^2(y)x^2$, which is of degree $2(p^e - p^v)$ in variable y. We consider this term for $f_1(x, y)$. Since $g_1(x, y)g_1(x, cx + d) = \sum_i \beta_i(x)g_1(x, cx + d)y^{p^i}$ has only terms of degree equal to some power of p in variable y and $2(p^e - p^v)$ is not a power of p in $p > 2$, the term of the highest degree of $\alpha_0^2(y)x^2$ does not appear here. Therefore, this term should appear in $g_1^2(x, y)$ (up to a constant). Since the polynomial $g_1^2(x, y) = \sum_{i,j} \beta_i(x)\beta_j(x)y^{p^i + p^j}$ has only terms of degree $p^i + p^j = p^i(1 + p^{j-i})$ with $i \le j$ and $0 \le i, j \le e$ in variable y, we have $2p^v(p^{e-v} - 1) = p^i(1 + p^{j-i})$ for some i, j with $i \le j$. Then, we should have $i = v$ and $2(p^{e-v} - 1) = 1 + p^{j-i}$. This implies that $2p^{e-v} - p^{j-i} = 3$. If $j = i$, then $p = 2$. This is a contradiction. If $j \ne i$, then $p^{j-i}(2p^{e-v-j+i} - 1) = 3$. We should have $p = 3, j - i = 1$ and $p^{e-v-1} = 1$. Since $i = v$ and $i < j$ as above, $i = v = e - 1$ and $j = e$.

Secondly we prove that $p = 3$, $e = 1$ and $v = 0$. Note that $p^e - p^{e-1} = 2p^{e-1}$ in $p = 3$. Since the polynomial $g^2(x, y) = \sum_{i,j} \alpha_i(y)\alpha_j(y)x^{p^i + p^j}$ has the term $2\alpha_0(y)x^{p^e + 1}$, which is of degree $2p^{e-1}$ in variable y, and the polynomial $g_1(x, y)g_1(x, cx + d)$ has only terms of degree equal to some power of p in variable y, the term of the highest degree $2p^{e-1} + p^e + 1$ of $2\alpha_0(y)x^{p^e + 1}$ appears in $g_1^2(x, y)$ (up to a constant). Since $g_1^2(x, y) = \sum_{i,j} \beta_i(x)\beta_j(x)y^{p^i + p^j}$, and $p^i + p^j = 2p^{e-1}$ implies that $i = j = e - 1$, $\beta_{e-1}^2(x)y^{2p^{e-1}}$ has the term of the highest degree $2p^{e-1} + p^e + 1$ of $2\alpha_0(y)x^{p^e + 1}$. Let k be the degree of $\beta_{e-1}(x)$. Since $\beta_{e-1}(x)$ has the term of degree at least $(p^e + 1)/2$, we have $(p^e + 1)/2 \le k \le p^e - p^{e-1} = 2p^{e-1}$. Then, $\beta_{e-1}(x)\beta_0(x)y^{p^{e-1} + 1}$ is of degree $k + (p^e - p^{e-1}) = k + 2p^{e-1}$ in variable x. Since $(p^e + 1)/2 + (p^e - p^{e-1}) = p^e + (p^e - 2p^{e-1} + 1)/2 = p^e + (p^{e-1} + 1)/2$, the term of the highest degree of $\beta_{e-1}(x)\beta_0(x)y^{p^{e-1} + 1}$ appears in $g^2(x, y)$. Since $g^2(x, y) = \sum_{i,j} \alpha_i(y)\alpha_j(y)x^{p^i + p^j}$, $k + (p^e - p^{e-1}) = p^{i_1} + p^{j_1}$ for some $i_1 \le j_1$. Since $p^e + (p^{e-1} + 1)/2 \le k + (p^e - p^{e-1}) = p^{i_1} + p^{j_1}$, we have $j_1 = e$ and $i_1 = e - 1$. Therefore, $k = 2p^{e-1} = p^e - p^{e-1} = p^e - p^v$. We have $e - 1 = 0$, since $\deg \beta_i(x) = p^e - p^v$ if and only if $i = 0$.

Finally, we consider the remaining case where $p = 3$, $e = 1$ and $v = 0$. Then, $g(x, y) = x^3 - (\alpha y + \beta)^2 x$ and $g_1(x, y) = y^3 - (\alpha_1 x + \beta_1)^2 y$ for some $\alpha, \beta, \alpha_1, \beta_1 \in K$ with $\alpha, \alpha_1 \ne 0$. Note that $g(ay + b) = (ay + b)((a + \alpha)y + (b + \beta))((a - \alpha)y + (b - \beta))$. Since $f(x, y) = g^2(x, y) +$

$g(ay+b,x)g(x,y)+h(y)$, the coefficient of xy^5 of $f(x,y)$ is equal to the one of $g(ay+b,y)$, which is equal to $\alpha^2 a(a+\alpha)(a-\alpha)$. If $a(a+\alpha)(a-\alpha)\neq 0$, then the coefficient of xy^5 of $f_1(x,y)$ is not zero. However, by considering $g_1^2(x,y)+g_1(x,cx+d)g_1(x,y)$, that is zero. Therefore, we should have $a(a+\alpha)(a-\alpha)=0$. Then, $g(ay+b)$ is of degree at most two. If $g(ay+b,y)$ is of degree at most one, then two of the three conditions $a=0$, $a+\alpha=0$ and $a-\alpha=0$ hold. Then, we have $a=\alpha=0$. This is a contradiction to $\alpha\neq 0$. Therefore $g(ay+b)$ is of degree two. Then the coefficient of x^3y^2 of $f(x,y)$ is not zero. Since y^2 appears only in $g_1^2(x,y)$ or $h_1(y)$ for $f_1(x,y)$ and $g_1^2(x,y)=y^6-2(\alpha_1 x+\beta_1)y^4+(\alpha_1 x+\beta_1)^2y^2$, the coefficient of x^3y^2 of $f_1(x,y)$ is zero. This is a contradiction. □

By Lemma 14, we have $p^v=p^e$. Then, $g(x,y)\in K[x]$ and $g_1(x,y)\in K[y]$. We denote $g(x,y)$ by $g(x)$ and $g_1(x,y)$ by $g_1(y)$. We have $f(x,y)=g^2(x)+\ g(x)(g(ay)+g(b))+\lambda_1 g_1^2(y)+\lambda_2$ for some $\lambda_1,\lambda_2\in K$. Let $G(X,Z)=Z^{p^e}g(X/Z)$ and let $G_1(Y,Z)=Z^{p^e}g_1(Y/Z)$. Then, $F(X,Y,Z)=Z^{2p^e}f(X/Z,Y/Z)=G^2(X,Z)+G(X,Z)(G(aY,Z)+g(b)Z^{p^e})+\lambda_1 G_1^2(Y,Z)+\lambda_2 Z^{2p^e}$. Let α (resp. β) be the coefficient of XZ^{p^e-1} (resp. YZ^{p^e-1}) for $G(X,Z)$ (resp. $G_1(Y,Z)$). Then, $F_X=2G(X,Z)\alpha Z^{p^e-1}+\alpha Z^{p^e-1}(G(aY,Z)+g(b)Z^{p^e})$, $F_Y=a\alpha Z^{p^e-1}G(X,Z)+2\lambda_1 G_1(Y,Z)\beta Z^{p^e-1}$ and $F_Z=-2G(X,Z)\cdot\alpha XZ^{p^e-2}\ -\alpha XZ^{p^e-2}(G(aY,Z)+g(b)Z^{p^e})+G(X,Z)(-a\beta YZ^{p^e-2})-\ 2\lambda_1 G_1(Y,Z)\beta YZ^{p^e-2}$. Therefore, $F_X(X,Y,0)=F_Y(X,Y,0)=F_Z(X,Y,0)=0$ and we have singular points on the line L_∞.

We have the assertion of Theorem 2.

Acknowledgements. The author is grateful to Professor Masaaki Homma for helpful discussions. The parameterization as in Remark 3 appeared during discussions with Homma. The author thanks Professor Hisao Yoshihara for helpful comments. The author also thanks the referee for helpful comments, by which the author could improve several proofs. The author was partially supported by Grant-in-Aid for Young Scientists (B) (22740001), MEXT and JSPS, Japan.

REFERENCES

[1] E. Arbarello - M. Cornalba - P. A. Griffiths - J. Harris, *Geometry of algebraic curves*, Vol. I. Grundlehren der Mathematischen Wissenschaften **267**, Springer-Verlag, New York, 1985.

[2] H. C. Chang, *On plane algebraic curves*, Chinese J. Math. **6** (1978), pp. 185–189.

[3] S. FUKASAWA, *Galois points on quartic curves in characteristic* 3, Nihonkai Math. J. **17** (2006), pp. 103–110.
[4] S. FUKASAWA, *On the number of Galois points for a plane curve in positive characteristic*, Comm. Algebra **36** (2008), pp. 29–36; II, Geom. Dedicata **127** (2007), pp. 131–137; III, ibid. **146** (2010), pp. 9–20; IV, preprint, arXiv:1011.3648.
[5] S. FUKASAWA, *Galois points for a plane curve in arbitrary characteristic*, Proceedings of the IV Iberoamerican conference on complex geometry, Geom. Dedicata **139** (2009), pp. 211–218.
[6] S. FUKASAWA, *Galois points for a non-reflexive plane curve of low degree*, preprint.
[7] S. FUKASAWA, *Galois points for a plane curve in characteristic two*, preprint.
[8] D. GOSS, *Basic structures of function field arithmetic*, Springer-Verlag, Berlin (1996).
[9] A. HEFEZ, *Non-reflexive curves*, Compositio Math. **69** (1989), pp. 3–35.
[10] A. HEFEZ - S. KLEIMAN, *Notes on the duality of projective varieties*, "Geometry Today", Prog. Math. vol **60**, Birkhäuser, Boston, 1985, pp. 143–183.
[11] M. HOMMA, *Funny plane curves in characteristic* $p > 0$, Comm. Algebra, **15** (1987), pp. 1469–1501.
[12] M. HOMMA, *A souped-up version of Pardini's theorem and its application to funny curves*, Compositio Math. **71** (1989), pp. 295–302.
[13] M. HOMMA, *Galois points for a Hermitian curve*, Comm. Algebra **34** (2006), pp. 4503–4511.
[14] K. MIURA - H. YOSHIHARA, *Field theory for function fields of plane quartic curves*, J. Algebra, **226** (2000), pp. 283–294.
[15] H. STICHTENOTH, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin (1993).
[16] K. O. STÖHR - J. F. VOLOCH, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3), **52** (1986), pp. 1–19.
[17] H. YOSHIHARA, *Function field theory of plane curves by dual curves*, J. Algebra, **239** (2001), pp. 340–355.

Manoscritto pervenuto in redazione il 26 Ottobre 2011.