Research Article

Galois Group at Each Point for Some Self-Dual Curves

Hiroyuki Hayashi,¹ and Hisao Yoshihara²

¹Graduate School of Science and Technology, Niigata University, Niigata 950-2181, Japan
²Department of Mathematics, Faculty of Science, Niigata University, Niigata 950-2181, Japan

Correspondence should be addressed to Hisao Yoshihara; yoshihara@math.sc.niigata-u.ac.jp

Received 10 October 2012; Accepted 21 December 2012

Copyright © 2013 H. Hayashi and H. Yoshihara. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We study the Galois group defined by a point projection for plane curve. First, we present a sufficient condition that the group is primitive and then determine the structure at each point for some self-dual curves.

1. Introduction

This study is a continuation of [1–4], and so forth. In general, it is not easy to determine the Galois group $G_p$ at every point $P$ for plane curve, in particular for curve with singular point. When we determine the structure of $G_p$, it is important to know whether it is primitive or not. However, there are not so many results which are useful for our purpose (cf. [5]). In this paper we give a geometrical criterion and then determine the group at each point for some self-dual curves.

Let $k$ be an algebraically closed field of characteristic zero. We fix it as the ground field of our discussions. Let $C$ be an irreducible plane curve of degree $d$ ($\geq 2$) and $K = k(C)$ the rational function field of $C$. Let $(X : Y : Z)$ be a set of homogeneous coordinates on $\mathbb{P}^2$ and put $P_1 = (0 : 0 : 1), P_2 = (0 : 1 : 0), \text{ and } P_3 = (1 : 0 : 0).$ Let $F(X, Y, Z)$ be the defining equation of $C$ and put $f(x, y) = F(X, Y, Z)/Z^d$, where $x = X/Z, y = Y/Z.$

1.1. Galois Group. Let $r : \overline{C} \to C$ be the resolution of singularities of $C$. For a point $P \in \mathbb{P}^2$, let $\tilde{P}$ be the dual line in the dual space $\tilde{\mathbb{P}}^2$ of $\mathbb{P}^2$ corresponding to $P$. We define the morphism $\pi_p$ by

$$\pi_p : \overline{C} \ni Q \mapsto \ell_{PR} \in \tilde{P} \equiv \mathbb{P}^1,$$

where $\ell_{PR}$ is the point in $\tilde{\mathbb{P}}^2$ corresponding to the line $\ell_{PR}$, which passes through $P$ and $R = r(Q)$ if $P \neq R$. In case $P = R$, the line $\ell_{PR}$ is the tangent line to the branch of $C$ at $R$. Clearly, we have $\deg \pi_p = d - m_p(C)$ and a field extension $\pi_p : k(\mathbb{P}^1) \hookrightarrow K = k(\overline{C})$, where $m_p(C)$ denotes the multiplicity of $C$ at $P$. In case $P \notin C$, we understand $m_p(C) = 0$. We put $n(P) = d - m_p(C)$; if there is no fear of confusion, we simply denote it by $n$. Since the extension depends only on $P$, we denote $k(\mathbb{P}^1)$ by $K_p$, that is, we have $\pi_p : K_p \hookrightarrow K$. Let $L_p$ be the Galois closure of $K/K_p$ and $G_p$ the Galois group $\text{Gal}(L_p/K_p)$.

Definition 1. We call $G_p$ the Galois group at $P$ for $C$. In case $K/K_p$ is a Galois extension, the point $P$ is said to be a Galois point.

In case $k$ is the field of complex numbers, $G_p$ is isomorphic to the monodromy group of the covering $\pi_p : \overline{C} \to \mathbb{P}^1$ [6, 7].

1.2. Self-Dual Curve

Definition 2. A point $Q \in C$ is said to be a cusp of $C$ if it is a singular point and $r^{-1}(Q)$ consists of a single point. Furthermore, if $\mu : B_Q(\mathbb{P}^2) \to \mathbb{P}^2$ is a blow-up and $\mu^{-1}(Q)$ is a nonsingular point of the proper transform of $\mu^{-1}(C)$, the point $Q$ is said to be a simple cusp.

Denote by $\overline{C}$ the dual curve of $C$.

Definition 3. If $\overline{C}$ is projectively equivalent to $C$, then $C$ is said to be a self-dual curve.
Suppose $C$ is smooth. Then, $C$ is self-dual if and only if $d = 2$. However, if $C$ has a singular point, the condition that $C$ is self-dual becomes complicated. The following proposition has been known (cf. [8]).

**Proposition 4.** Suppose $C$ is one of the following curves:

1. $C$ has just one singular point;
2. $C$ is rational and has only simple cusps as singular points.

Then, $C$ is a self-dual curve if and only if $d$ is a prime number, which we call a nonsingular projective algebraic curve. Let $C$ be such a curve. A line $ℓ_{PQ}$ is said to be a simple $e$-tangent line to $C$ if the following conditions are satisfied:

- The curve defined by $Y = X^d$, $gcd(e,d) = 1$, $1 \leq e \leq d - 1$;
- The curve defined by $(YZ - X^3)^2 = X^3Y$ (cf. [9]);
- The curve defined by $(XY - XZ + YZ)^3 + 54X^3Y^2Z^2 = 0$ (cf. [10]).

For the curve $C_{(e,d)}$, if $1 < e < d - 1$, then $P_1 = (0 : 0 : 1)$ and $P_2 = (0 : 1 : 0)$ are not simple cusps and $C_{(e,d)}$ has no flex. The curve $C_{(e,d)}$ has two cusps $P_1$ and $P_2$, where $P_1$ is not a simple cusp. The curve $C_{34}$ has three cusps $P_1, P_2,$ and $P_3$ and the normalization is an elliptic curve. It is easy to find the dual curve of $C_{(e,d)}$; however, in the other curves we need some consideration, for the details, see [9, 10].

**Remark 6.** Let $Φ_C$ be the rational map $\mathbb{P}^2 \to \mathbb{P}^2$ giving the dual of $C$, that is,

$$Φ_C(X : Y : Z) = (\partial_X F : \partial_Y F : \partial_Z F),$$

where $F$ is the defining equation of $C$. In the case where $C = C_{(e,d)}$, the map $Φ_C$ turns out to be a quadratic transformation of $\mathbb{P}^2$:

$$Φ_C(X : Y : Z) = (-dYZ : eZX : (d - e) XY).$$

We use the following notation:

1. $Z_m$: the cyclic group of order $m$;
2. $S_d$: the symmetric group of degree $d$;
3. $i(X_1, X_2; Q)$: the intersection number of two curves $X_1$ and $X_2$ at $Q$;
4. $ℓ_{PQ}$: the line passing through $P$ and $Q$;
5. $ℓ_P$: a line passing through $P$;
6. $T_{PQ} = T_{QP}(C)$: the tangent line to $C$ at $Q$.

### 2. Statement of Results

We need some preparations before stating the results. A curve means a nonsingular projective algebraic curve. Let $X_1$ and $X_2$ be curves and $f : X_1 \to X_2$ a surjective morphism, which we call a covering for short. We denote by $e(R, f)$ the ramification index of $f$ at $R \in X_1$. If there is no fear of confusion, we simply denote it by $e(R)$.

**Definition 7.** Let $f : X_1 \to X_2$ be the covering above. If there exists a curve $X_3$ and coverings $α : X_1 \to X_3$ and $β : X_3 \to X_2$ such that $f = βα$, $deg α ≥ 2$ and $deg β ≥ 2$, then $f$ is said to be decomposable and $X_3$ an intermediate covering. If such a curve $X_3$ does not exist, then $f$ is said to be indecomposable (cf. [11]).

**Definition 8.** Let $f : X_1 \to X_2$ be the covering above and $R_1, ..., R_r$ all the ramification points for $f$. Put $e(R_i) = e_i (1 ≤ i ≤ r)$. The covering $f$ is said to be an $s$-covering over $f(R_i)$ if there exists no ramification point in $f^{-1}(f(R_i))$ except $R_i$. The $f$ is said to be an $s$-covering if it is an $s$-covering over each $f(R_i)$ ($1 ≤ i ≤ r$).

**Definition 9.** With the same notation as in Definition 8, we call $\{R_1, ..., R_r\}, (e_1, ..., e_r\}$ (or, simply, $(e_1, ..., e_r)$) the ramification data for $f$.

We give several sufficient conditions that $f$ is indecomposable. Some of them will not be used later in this paper.

**Proposition 10.** Let $f : X_1 \to X_2$ be the covering above and $m = deg f$. If one of the following conditions is satisfied, then $f$ is indecomposable.

1. For some $i (1 ≤ i ≤ r)$, $e_i$ is prime and $n < 2e_i$.
2. $e_i = n - 1$.
3. $X_2$ is a rational curve, $f$ is an $s$-covering except over $f(R_i)$ and $e_i$ is prime for each $i ≥ s + 1$, where $f^{-1}(f(R_i)) = \{R_1, ..., R_r\}$.

**Proposition 11.** With the same notation as in Proposition 10, if $f$ is an $s$-covering and satisfies one of the following conditions, then $f$ is indecomposable.

1. $X_1$ is a rational curve, $e_1 ≥ e_2, n - 1 ≥ e_2$, and $e_i$ is prime for each $i ≥ 3$.
2. $X_1$ is a rational curve and $e_i$ is prime for each $i ≥ 2$.
3. $X_2$ is a rational curve and $e_i$ is prime for each $i$.

Hereafter, we follow the notation in Section 1. By taking a suitable projective change of coordinates, we can assume the projection center is $P_1$ without changing the structure of $G_p$. Putting $y = tx$, we have $K_0 = k(t)$ and $K = k(x, y) = k(t, x)$. Put $g(x) = f(x, tx)/x^n \in k(t)[x]$, where $m = mp(C)$ and let $\{x_1, ..., x_n\}$ be the roots of $g(x) = 0$. Then, we can consider $G_p$ as a permutation subgroup of $S_n$.

**Theorem 12.** The group $G_p$ is primitive if and only if $π_p$ is indecomposable. In particular, if $n(P)$ is a prime number, then $G_p$ is primitive for $P \in \mathbb{P}^2$.

**Definition 13.** Assume $Q \in C$ is a smooth point or a cusp. A line $ℓ = ℓ_{PQ}$ is said to be a simple $e$-tangent line to $C$ if the following conditions are satisfied:
Table 1

| P   | P₁, P₂, P₃ | P ∈ C \ [P₁, P₂] | P ∈ P¹ \ C |
|-----|-------------|----------------|------------|
| Gₚ  | Zₐ, e       | Sₐ⁻¹           | S₁         |

Table 2

| P   | P₁, P₂, P₃ | P ∈ C \ [P₁, P₂] | P ∈ P¹ \ C |
|-----|-------------|----------------|------------|
| Gₚ  | Z₂          | S₁             | S₃         |

(1) if Q ≠ P (resp., Q = P), then if(C, ℓ; Q) = e (resp., e + m), where e ≥ 2 and m = mₚ(C);
(2) the curves C and ℓ have normal crossings except at Q.

Sometimes we call ℓ a simple e-tangent for short.

Note that a simple e-tangent ℓₑₚᵧ produces a s-covering over πₚ(Q).

Lemma 14. We have the following assertions for Gₚ.

1. If each line ℓₑₚ has normal crossings with C or is a simple e-tangent line to C such that e is a prime number, then Gₚ is primitive (cf. [5, Lemma 4.4.4]).
2. If there exists a simple 2-tangent line ℓₑₚ, then Gₚ contains a transposition.

The following lemma is well known.

Lemma 15. If a permutation group G ⊂ Sₙ is primitive and contains a transposition, then it is a full symmetric group.

Combining the above results, we get the following corollary.

Corollary 16. If the covering πₑₚ : Č → P¹ is one of the coverings in Propositions 10 and 11 and πₑₚ is an s-covering over πₑₚ(Rᵢ) with ei = 2 for some i (1 ≤ i ≤ r), then Gₑₚ is a full symmetric group. In particular, if each line ℓₑₚ has normal crossings with C or is a simple 2-tangent, then Gₑₚ is a full symmetric group.

Corollary 16 implies [2, Theorem 1 and 1¹]. Now we can state the structure of Gₑₚ as follows.

Theorem 17. For the curves C in Example 5, the Galois groups Gₑₚ are as follows, where Z₁ indicates the trivial group

(I) the case C = Cₑₚ(ε, d) (see Table 1);
(II) the case C = Cₑₚ(d) (see Table 2);
(III) the case C = CₑₚS₄ (see Table 3).

Remark 18. For the curves in Theorem 17, P is a Galois point if and only if Gₑₚ is a cyclic group. However, the same assertion does not hold true in general, see, for example, [3].

3. Proofs

First, we prove Propositions 10 and 11.

Claim 1. Suppose f and a ramification point R ∈ X₁ satisfy the following conditions:

1. f is an s-covering over f(R).
2. e(R) is prime.

If there exists an intermediate covering β : X₃ → X₂, then β is unramified at R' = α(R).

Proof. Suppose β is ramified at R'. Then, since e(R) is prime, we have e(R', β) = e(R, f), hence R' is not a branch point for α. Then, there will appear another ramification point for f in f⁻¹(f(R)). This is a contradiction.

The proof of Proposition 10 is as follows. Suppose f is decomposable and there exists a covering β : X₁ → X₂ as in Definition 7. First, we prove the assertion (1). Since e₁ is prime, β is unramified at R₁ by Claim 1. Hence, we have e(R₁, α) = e(R₁, f). Since there exists at least two points in β⁻¹(f(R₁)), we have n = deg f ≥ 2e₁, which contradicts the assumption. Next we prove (2). Clearly α and β are ramified at R₁ and R₁, respectively. Put B₁ = f(R₁). Then, since e₁ = 1, β⁻¹(B₁) consists of one or two points. In the former case, α⁻¹(β⁻¹(B₁)) consists of two points, on the other hand in the latter case α⁻¹(B₁) (i = 1, 2) consists of one point, where β⁻¹(B₁) = {B₁₁, B₁₂}. In each case we infer the inequality n = deg f ≥ (n₁ - 1) + 2, which is a contradiction. We go to the proof of (3). Then, by Claim 1, B₁ (i ≥ 2) is not a branch point for β. Thus, B₁ is the only branch point for β. Then, by Hurwitz's formula, we have 2g(X₁) = -2b + c, where g(X₁) is the genus of X₁, b is the degree of β, and c ≤ b - 1. Since g(X₁) ≥ 0, this inequality implies b = 1, which is a contradiction.

Next we prove Proposition 11. In each case we use the reduction to absurdity, that is, suppose f is decomposable. So we use the notation Rᵢ = α(Rᵢ) (1 ≤ i ≤ r). In the case (I), by Claim 3, β is unramified at Rᵢ (i ≥ 3). Since X₂ and X₃ are rational, from Hurwitz's formula, we infer that β is ramified with the index e(Rᵢ, β) = e(R₂, β) = deg β. Then, since there exists no ramification points in f⁻¹(f(Rᵢ)) except Rᵢ (i = 1, 2), α must branch at Rᵢ and R₂. However, there exists an unramified point in f⁻¹(f(Rᵢ)), this is a contradiction. Therefore, f is indecomposable. In the case (II), by Claim 1, β is unramified at Rᵢ for i ≥ 2. Since X₂ is rational, by Hurwitz's formula, we have a contradiction. In the case (III) similarly, by Claim 1, β is unramified at every point; however, since X₂ is rational, β must be an identity, which is a contradiction. This completes the proof of Proposition 11.

The proof of Theorem 12 is as follows: suppose Gₑₚ is not primitive and let Gₓ be the isotropy group of x = x₁ in Gₑₚ. Then, there exists a subgroup H of Gₑₚ such that Gₓ ⊆ H ⊆
Let $C_H$ be the nonsingular model of the intermediate field which corresponds to $H$ by the Galois correspondence. Then, there exist the coverings $\alpha : \tilde{C} \to C_H$ and $\beta : C_H \to \mathbb{P}^1$ such that $\pi_{c} = \beta \alpha$. Thus, $\pi_P$ is decomposable. The converse assertion is clear from the Galois correspondence.

The proof of Lemma 14 is simple. In view of Definition 13, we see that the assertion (1) is another expression of (3) in Proposition 11. The assertion (2) may be well known (cf. [7]).

Now we proceed to the proof of Theorem 17. The structure of $G_P$ depends on the covering $\pi_P$ and $\pi_{P}$ depends on the position of $P$. We prove by examining the cases where $P$ lies on the tangent line to $C$ at the cusp or at the flex. Hereafter, we assume $C$ is the curve in Theorem 17. Since $C$ is a self-dual curve and has only cusps as the singularity, the following remark is clear.

Remark 19. Suppose a line $\ell$ satisfies the following conditions:

(1) $\ell$ does not pass through any cusp;
(2) $\ell$ is not the tangent line to $C$ at the flex.

Then, $\ell$ is a simple 2-tangent line to $C$ or $\ell$ and $C$ have normal crossings.

Proof of the Case (I). Assume $C = C_{(e,d)}$. It has the following property.

Claim 2. The tangent line $T_{P_{1}}$ (resp., $T_{P_{2}}$) is $Y = 0$ (resp., $Z = 0$) and $T_{P_{1}} \cap T_{P_{2}} = \{P_{3}\}$, which does not lie on $C$. In case $e = 1$ (resp., $d - 1$), $C$ has one flex at $P_{1}$ (resp., $P_{2}$). On the other hand, in case $1 < e < d - 1$, $C$ has no flex.

Proof. Calculating the Hessian of $X^{d} - Y^{e}Z^{d-e}$ (cf. [12]), we infer readily the assertions.

If $P = P_{1}, P_{2},$ or $P_{3}$, then $G_{P}$ can be determined explicitly. In fact, if $P = P_{1}$, then consider the affine part $Z \neq 0$ of $C$, that is, the affine defining equation is $Y^{e} - X^{d-e} = 0$. Then, putting $z = x$, we get $Y^{e} - X^{d-e} = 0$, hence $G_{P} \equiv Z_{d-e}$. The other case $P = P_{2}$ is similarly determined. If $P = P_{3}$, then consider the affine part $X \neq 0$, we get $Z^{d-e} = 1$. Putting $z = x$, we get $Z^{d-e} = 1$, hence $G_{P} \equiv Z_{d-e}$. As we have seen above, these points are Galois ones.

Next, we treat the case $P \in C \setminus \{P_{1}, P_{2}\}$. First, we prove the subcase $1 < e < d - 1$. Since $C$ is a self-dual curve and has no flex, we see that, if a line $\ell_{P}$ passes through neither $P_{1}$ nor $P_{2}$, then it always has normal crossings with $C$ or it is a simple 2-tangent line to $C$. Furthermore, by Hurwitz’s formula, we see there exists a simple 2-tangent. Then, by (1) in Proposition 11 and Lemma 15, we have $G_{P} \equiv S_{d-1}$. Next, we prove the subcase $e = 1$. Then, $P_{1}$ (resp., $P_{2}$) is a flex (resp., cusp) and the tangent line at $P_{1}$ (resp., $P_{2}$) does not meet $C$ except at $P_{1}$ (resp., $P_{2}$). If a line $\ell_{P}$ does not pass through $P_{2}$, then it always has normal crossings with $C$ or it is a simple 2-tangent line to $C$. Then, by (2) in Proposition 11 and Lemma 15, we have $G_{P} \equiv S_{d-1}$. The proof of the case $e = d - 1$ is the same.

Now we prove the case where $P \in \mathbb{P}^2 \setminus C$ and $P \neq P_{3}$. If $P \in \ell_{P_{1}P_{2}}$, and $1 < e < d - 1$, then $\pi_{P}$ has two ramification points $R_{1}$ and $R_{2}$ such that $\pi_{P}(R_{1}) = e, e(R_{2}) = d - e$ and $\pi_{P}(R_{1}) = \pi_{P}(R_{2})$. Thus, $\pi_{P}$ is not an $s$-covering. If $\ell_{P}$ passes through neither $P_{1}$ nor $P_{2}$, then $\ell_{P}$ is a simple 2-tangent to $C$ or has normal crossings with $C$. By (3) in Proposition 10, $\pi_{P}$ is indecomposable. Since there exists a simple 2-tangent $\ell_{P}$, we conclude $G_{P} \equiv S_{d}$. In case $P \in \ell_{P_{1}P_{2}}$, and $e = 1$ or $d - 1$, $\pi_{P}$ is an $s$-covering and $e_{1} = d - 1$ and $e_{2} = 2$, hence by (2) in Proposition 10, $G_{P}$ is primitive and there exists a simple 2-tangent line $\ell_{P}$, thus we conclude $G_{P} \equiv S_{d}$. In view of Remark 19, we conclude easily from the similar argument that $G_{P} \equiv S_{2}$ when $P \in \mathbb{P}^2 \setminus \{C \cup \ell_{P_{1}P_{2}}\}$.

Proof of the Case (II). Assume $C = C_{(4)}$. It has the following property.

Claim 3. The $T_{P_{1}}$ (resp., $T_{P_{2}}$) is $Y = 0$ (resp., $Z = 0$) and $T_{P_{1}} \cap T_{P_{2}} = \{P_{3}\}$, which does not lie on $C$. Furthermore, $T_{P_{1}} \cap C = \{P_{1}\}$ and $T_{P_{2}} \cap C = \{P_{2}, (1 : 1 : 0)\}$. The $C$ has one flex $F$ of order 1, that is, if $C, T_{F}; F = 3$ and $T_{F}$ does not pass through $P_{3}$.

Proof. The last assertion is checked by Hurwitz’s formula and the others are simple.

Remark 20. The coordinates of the flex $F$ are computed as $(-576 : -4096 : 135)$.

Clearly, if $P = P_{1}$ or $P_{2}$, then $C = Z_{2}$. If $P \in C \setminus \{P_{1}, P_{2}\}$, then $n = 3$, hence $G_{P}$ is primitive. We divide the proof into three cases:

(1) $P = F$;
(2) $P = (1 : 1 : 0)$;
(3) $P$ is the other point.

In any case, by Hurwitz’s formula, we infer that there exists at least one simple 2-tangent line passing through $P$, hence $G_{P} \equiv S_{3}$. Then consider the case $P \in \mathbb{P}^2 \setminus C$. If $P \in \ell_{P_{1}P_{2}}$, then $\pi_{P}$ has ramification points $R_{1}$ and $R_{2}$ such that $e(R_{1}) = e(R_{2}) = 2$ and $\pi_{P}(R_{1}) = \pi_{P}(R_{2})$. Thus, $\pi_{P}$ is not an $s$-covering. Consider $\pi_{P}$ for the most special case $\ell_{P_{1}P_{2}} \cap T_{F} = \{P\}$. We infer from Hurwitz’s formula that the ramification data is $(3, 2^{4}) := (3, 2, 2, 2, 2)$. By (3) in Proposition 10, we have $G_{P} \equiv S_{4}$. There are several cases of position of $P$ which yield different ramification data; however, it is easy to see that there exists $i$ such that $e_{i} = 2$. Then from Propositions 10 or 11, we conclude $G_{P} \equiv S_{4}$.

Proof of the Case (III). Assume $C = C_{5g}$. It has the following property. There exists a projective transformation $\sigma$ such that $\sigma(C) = C$ and $\sigma(X, Y, Z) = (Y, X, -Z), (-X, Z, Y)$ or $(Z, Y, X)$ so that $\sigma$ interchanges $P_{1}$ ($i = 1, 2, 3$).

Claim 4. The flexes of $C$ are $F_{1} = (4 : -1 : 4), F_{2} = (1 : -4 : 4), F_{3} = (4 : -4 : 1)$, hence the tangent lines to $C$ at them are $L_{1} : X + 8Y + Z = 0, L_{2} : 8X + Y - Z = 0, and L_{3} : -X + Y + 8Z = 0$, respectively. On the other hand, the
tangent lines to $C$ at $P_1, P_2,$ and $P_3$ are $L_4 : X = Y, L_5 : X = Z,$ and $L_6 : Y = Z,$ respectively. There exist just three points $Q_i$ ($i = 1, 2, 3$) satisfying the following conditions:

1. $Q_i \notin C$;
2. if $i = \ell_{Q_i}$ does not pass through any cusp, then $\ell$ and $C$ have normal crossings or there exist two points $Q' \in C$ satisfying the condition

$$
\ell(\ell, \ell; Q') \geq 3.
$$

Such $Q_i$ is an intersection $L_i \cap L_k$, where $\{i, j, k\} = \{1, 2, 3\}$, indeed $Q_1 = (1 : -7 : 1i), Q_2 = (7 : -1 : 1i)$, and $Q_3 = (1 : -1 : 7i)$. Therefore, if $P \in \mathbb{P}^2 \setminus \{C, Q_1, Q_2, Q_3\}$, then there exists a line $\ell$ passing through $P$ such that $\ell$ is a simple 2-tangent line to $C$.

**Proof.** Making use of the results in [10] and observing the self-duality of $C$, we can check the assertions by direct computations.

Now let us begin the proof. If $P = P_1$, then $n = 3$, hence $G_{P_1}$ is primitive. The lines $\ell_{P_1P_2}$ and $\ell_{P_1P_3}$ yield the ramification points of order three of $\pi_P$, hence we infer from Hurwitz's formula that there exists $i$ such that $e_i = 2$. Thus, we get $G_{P_1} \cong S_3$. For $P = P_2$ or $P_3$, using the projective transformation $\sigma$ above, we see $G_{P_2} \cong S_3$ ($i = 2, 3$).

Next consider the case $P \in C \setminus \{P_1, P_2, P_3\}$. Then we have $n = 5$, hence $G_{P}$ is primitive. Using Hurwitz's formula or the self-duality of $C$, we see that there exists a simple 2-tangent line to $C$, thus we have $G_{P} \cong S_5$.

Finally, we consider the remaining case $P \in \mathbb{P}^2 \setminus C$.

**Claim 5.** Let $n_i$ be the number of ramification points with index $i$. Then we have $n_2 + 2n_3 + 3n_4 = 12$, where $n_4 \leq 3$. In particular, if $n_4 = 3$ (resp., 2), then $P = (1 : 1 : 1)$ (resp., $Q_i$), furthermore; $n_5 = 0$ (resp., 3) and $n_2 = 3$ (resp., 0).

**Proof.** The former assertion is clear from Claim 4 and Hurwitz's formula. The proof of the latter assertion is as follows: observing Claim 4, we infer that, if $n_4 = 3$, then $P$ is unique ($1 : 1 : 1$), which is the intersections of the three lines $L_4, L_5, L_6$ (Figure 1). Similarly observing Claim 4, we infer that if $n_4 = 2$, then $P = Q_1, Q_2$ or $Q_3$. In this case, we have $i(C, \ell_{pp}) (P_i) = 3$, hence $n_3 = 3$.

**Claim 6.** If $\pi_P$ is an $s$-covering, then $\pi_P$ is indecomposable.

**Proof.** By Claim 5 the ramification index is $2, 3, 4$. Suppose $\pi_P$ is decomposable. Then, $\deg \beta = 2$ or $3$. By Claim 1, $\beta$ cannot be unramified at $R_i = \alpha(R_i)$, where $e_i = 2$ or $3$. By Claim 5, we have $n_4 \leq 3$. As we have seen in the proof of Proposition 11, $\beta$ cannot be ramified at only one point. Thus, we have $n_4 \neq 1$.

If $n_4 = 0$, then the proof is clear by (3) in Proposition 11. If $n_4 = 2$, then $P = Q_i$ ($i = 1, 2, 3$). In case $\deg \beta = 2$, $\beta$ is ramified at $R_1$ and $R_2$. Since $\deg \alpha = 3$, this cannot occur. In case $\deg \beta = 3$, $\beta$ is ramified at $R_1$ and $R_2$ with $e(R_1, \beta) = e(R_2, \beta) = 2$; however, these do not satisfy Hurwitz's formula. If $n_4 = 3$, then $P = (1 : 1 : 1)$ and from Claim 4 and Hurwitz's formula we infer that the ramification data is $(4, 3, 2)$. Thus we conclude $G_P \cong S_5$.

The proofs of the other two cases $Q_2$ and $Q_3$ are almost the same.
The proof of the case (iii) is as follows: here we notice
that if \( P \in T_{F_i} \), \( i \neq j \), \( (i, j = 1, 2, 3) \), then \( \pi_P \) is not a
covering. First we consider the special case where \( P \) is in some
\( T_{F_i} \), for example, \( T_{F_1} \cap T_{F_2} = \{ P \} \). Then the ramification
data is \( \{(F_1, P_1, P_2, P_3, R_5, R_6, R_7), (4, 3^5, 2^3)\} \) and \( \pi_P(P_1) = \pi_P(P_2) \). Suppose \( \pi_P \) is decomposable. Then, by Claim 1, \( \beta : X_3 \rightarrow \mathbb{P}^1 \) is unramified at \( \alpha(P_i) \) and \( R_i \), \( (i \geq 5) \). Namely, \( \beta \) is ramified at just two points. Then, the ramification data
of \( \beta \) is \( \{(\alpha(F_1), \alpha(P_1)), (2, 2)\} \) or \( \{(\alpha(F_1), \alpha(P_1)), (3, 3)\} \), where \( \deg \beta = 2 \) or 3, respectively. However, it is easy to see that this
is impossible considering \( \alpha \) and \( \pi_P \), so \( \pi_P \) is indecomposable.
Since there exist \( e_i = 2 \) \( (i = 5, 6, 7) \), we conclude \( G_p \cong S_6 \). On
the other hand, if \( P \) is not in \( T_{F_i} \) for each \( i \) \( (i = 1, 2, 3) \), then,
by (3) in Proposition 10, \( f \) is indecomposable. Since there
exists a simple 2-tangent, we have \( G_p \cong S_6 \).

Thus, we complete all the proofs.

Remark 21. In the list of Theorem 17 only two kinds of group
appear. Of course, other kinds will appear in other examples,
for example, let us take the Fermat quartic \( X^4 + Y^4 + Z^4 = 0 \).
Then, there exist 12 points such that \( G_p \) is the dihedral group
of order 8 (cf. [13]).

Problem. Concerning the Galois groups for \( C_{e,d}(1 < e < d - 1) \), full symmetric group \( S_d \) degenerates into the cyclic
group. How does the symmetric group degenerate for various
curves?

Acknowledgments

The authors would like to express their thanks to Oka for
teaching the example of self-dual curve \( C_{54} \). They thank also
the referee(s) for carefully reading the paper and giving the
suitable suggestions for improvements.

References

[1] K. Miura, ”Field theory for function fields of singular plane
quartic curves,” Bulletin of the Australian Mathematical Society,
vol. 62, no. 2, pp. 193–204, 2000.
[2] H. Yoshihara, ”Function field theory of plane curves by dual
curves,” Journal of Algebra, vol. 239, no. 1, pp. 340–355, 2001.
[3] H. Yoshihara, ”Galois points for plane rational curves,” Far East
Journal of Mathematical Sciences, vol. 25, no. 2, pp. 273–284,
2007.
[4] H. Yoshihara, ”Rational curve with Galois point and extendable
Galois automorphism,” Journal of Algebra, vol. 321, no. 5, pp.
1463–1472, 2009.
[5] J.-P. Serre, Topics in Galois Theory, vol. 1 of Research Notes in
Mathematics, Jones & Bartlett, Boston, Mass, USA, 1992.
[6] F. Cukierman, ”Monodromy of projections,” Matemáticas Con-
temporáneas, vol. 16, pp. 9–30, 1999 (Portuguese), 15th School
of Algebra.
[7] J. Harris, ”Galois groups of enumerative problems,” Duke
Mathematical Journal, vol. 46, no. 4, pp. 685–724, 1979.
[8] H. Yoshihara, ”Applications of Plücker’s formula,” Sūgaku,
vol. 32, no. 4, pp. 367–369, 1980 (Japanese).
[9] S. Iitaka, K. Ueno, and Y. Namikawa, Descartes No Seishin To
Daisikika, NipponHyoron Sha, Tokyo, Japan, 1980.
