Hindawi Publishing Corporation
Geometry
Volume 2013, Article ID 369420, 6 pages
http://dx.doi.org/10.1155/2013/369420

Research Article

Galois Group at Each Point for Some Self-Dual Curves

Hiroyuki Hayashi,[1] and Hisao Yoshihara[2]

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

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

Received 10 October 2012; Accepted 21 December 2012

Academic Editor: Michel Planat

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 (≥ 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 $P_1 = (0 : 0 : 1)$, $P_2 = (0 : 1 : 0)$, 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 $r : \widetilde{C} \to C$ be the resolution of singularities of C. For a point $P \in \mathbb{P}^2$, let $\widehat{P}$ be the dual line in the dual space $\widehat{\mathbb{P}^2}$ of $\mathbb{P}^2$ corresponding to P. We define the morphism π_P by

$$\pi_P : \widetilde{C} \ni Q \longmapsto \widehat{\ell_{PR}} \in \widehat{P} \cong \mathbb{P}^1, \tag{1}$$

where $\widehat{\ell_{PR}}$ is the point in $\widehat{\mathbb{P}^2}$ corresponding to the line ℓ_{PR}, which passes through P and $R = r(Q)$ if $P \neq R$. In case $P = R$, the line ℓ_{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 $\pi_P^* : k(\mathbb{P}^1) \hookrightarrow K = k(\widetilde{C})$, 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 $\mathrm{Gal}(L_P/K_P)$.

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 $\pi_P : \widetilde{C} \to \mathbb{P}^1$ [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 $\widehat{C}$ the dual curve of C.

Definition 3. If $\widehat{C}$ 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 C is projectively equivalent to the curve defined by $y = x^d$.

Example 5. It seems that only a few self-dual curves have been known. Here, we present some of them

(I) $C_{(e,d)}$: the curve defined by $Y^e Z^{d-e} = X^d$, $\gcd(e, d) = 1$, $1 \le e \le d - 1$;

(II) $C_{(4)}$: the curve defined by $(YZ - X^2)^2 = X^3 Y$ (cf. [9]);

(III) C_{54}: the curve defined by $(XY - XZ + YZ)^3 + 54X^2Y^2Z^2 = 0$ (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 $C_{(4)}$ has two cusps P_1 and P_2, where P_1 is not a simple cusp. The curve C_{54} 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 $\mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ giving the dual of C, that is,

$$\Phi_C (X : Y : Z) = \left(\partial_X F : \partial_Y F : \partial_Z F\right), \tag{2}$$

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 $\mathbb{P}^2$:

$$\Phi_C (X : Y : Z) = (-dYZ : eZX : (d - e) XY). \tag{3}$$

We use the following notation:

(i) Z_m: the cyclic group of order m;

(ii) S_d: the symmetric group of degree d;

(iii) $i(X_1, X_2; Q)$: the intersection number of two curves X_1 and X_2 at Q;

(iv) ℓ_{PQ}: the line passing through P and Q;

(v) ℓ_P: a line passing through P;

(vi) $T_Q = T_Q(C)$: 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 $\alpha : X_1 \to X_3$ and $\beta : X_3 \to X_2$ such that $f = \beta\alpha$, $\deg \alpha \ge 2$ and $\deg \beta \ge 2$, 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 $R_1, \dots, R_r$ all the ramification points for f. Put $e(R_i) = e_i$ $(1 \le i \le r)$. 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 $f(R_i)$ $(1 \le i \le r)$.

Definition 9. With the same notation as in Definition 8, we call $\{(R_1, \dots, R_r), (e_1, \dots, e_r)\}$ (or, simply $(e_1,\dots,e_r)$) 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 $n = \deg f$. If one of the following conditions is satisfied, then f is indecomposable.*

(1) *For some i $(1 \le i \le r)$, e_i is prime and $n < 2e_i$.*

(2) *$e_1 = n - 1$.*

(3) *X_2 is a rational curve, f is an s-covering except over $f(R_1)$ and e_i is prime for each $i \ge s + 1$, where $f^{-1} f(R_1) = \{R_1, \dots, R_s\}$.*

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, $e_1 \ge e_2$, $n - 1 \ge e_2$, and e_i is prime for each $i \ge 3$.*

(2) *X_1 is a rational curve and e_i is prime for each $i \ge 2$.*

(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 $K_P = k(t)$ and $K = k(x, y) = k(t, x)$. Put $g(x) = f(x, tx)/x^m \in k(t)[x]$, where $m = m_P(C)$ and let $\{x_1, \dots, x_n\}$ $(n = n(P))$ be the roots of $g(x) = 0$. Then, we can consider G_P as a permutation subgroup of S_n. Note that G_P is a transitive subgroup of S_n. Hence, G_P is a primitive group if and only if the isotropy subgroup of an element of $\{x_1, \dots, x_n\}$ is a maximal 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 $\ell = \ell_{PQ}$ is said to be a simple e-tangent line to C if the following conditions are satisfied:

Table 1

P	P_1	P_2	P_3	$P \in C \setminus \{P_1, P_2\}$	$P \in \mathbb{P}^2 \setminus C \cup \{P_3\}$
G_P	Z_{d-e}	Z_e	Z_d	S_{d-1}	S_d

Table 2

P	P_1, P_2	$P \in C \setminus \{P_1, P_2\}$	$P \in \mathbb{P}^2 \setminus C$
G_P	Z_2	S_3	S_4

(1) if $Q \neq P$ (resp., $Q = P$), then $i(C, \ell; Q) = e$ (resp., $e + m$), where $e \geq 2$ and $m = m_P(C)$;

(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 ℓ_{PQ} yields an s-covering over $\pi_P(Q)$.

Lemma 14. *We have the following assertions for G_P.*

(1) *If each line ℓ_P has normal crossings with C or is a simple e-tangent line to C such that e is a prime number, then G_P is primitive (cf. [5, Lemma 4.4.4]).*

(2) *If there exists a simple 2-tangent line ℓ_P, then G_P contains a transposition.*

The following lemma is well known.

Lemma 15. *If a permutation group $G \subset S_n$ is primitive and contains a transposition, then it is a full symmetric group.*

Combining the results above, we get the following corollary.

Corollary 16. *If the covering $\pi_P : \widetilde{C} \to \mathbb{P}^1$ is one of the coverings in Propositions 10 or 11 and π_P is an s-covering over $\pi_P(R_i)$ with $e_i = 2$ for some i $(1 \leq i \leq r)$, then G_P is a full symmetric group. In particular, if each line ℓ_P has normal crossings with C or is a simple 2-tangent, then G_P is a full symmetric group.*

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

Theorem 17. *For the curves C in Example 5, the Galois groups G_P are as follows, where Z_1 indicates the trivial group*

(I) *the case $C = C_{(e,d)}$ (see Table 1);*

(II) *the case $C = C_{(4)}$ (see Table 2);*

(III) *the case $C = C_{54}$ (see Table 3).*

Remark 18. For the curves in Theorem 17, P is a Galois point if and only if G_P 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.

Table 3

P	P_1, P_2, P_3	$P \in C \setminus \{P_1, P_2, P_3\}$	$P \in \mathbb{P}^2 \setminus C$
G_P	S_3	S_5	S_6

Claim 1. Suppose f and a ramification point $R \in X_1$ satisfy the following conditions:

(1) f is an s-covering over $f(R)$.

(2) $e(R)$ is prime.

If there exists an intermediate covering $\beta : X_3 \to X_2$, then β is unramified at $R' = \alpha(R)$.

Proof. Suppose β is ramified at R'. Then, since $e(R)$ is prime, we have $e(R', \beta) = e(R, f)$, 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 $\beta : X_3 \to X_2$ as in Definition 7. First, we prove the assertion (1). Since e_i is prime, β is unramified at $R_i^{'}$ by Claim 1. Hence, we have $e(R_i, \alpha) = e(R_i, f)$. Since there exists at least two points in $\beta^{-1}(f(R_i))$, we have $n = \deg f \geq 2e(R_i, f)$, which contradicts the assumption. Next we prove (2). Clearly α and β are ramified at R_1 and $R_1^{'}$, respectively. Put $B_1 = f(R_1)$. Then, since $e_1 = n - 1$, $\beta^{-1}(B_1)$ consists of one or two points. In the former case, $\alpha^{-1}(\beta^{-1}(B_1))$ consists of two points, on the other hand in the latter case $\alpha^{-1}(B_{1i})$ $(i = 1, 2)$ consists of one point, where $\beta^{-1}(B_1) = \{B_{11}, B_{12}\}$. In each case we infer the inequality $n = \deg f \geq (n - 1) + 2$, which is a contradiction. We go to the proof of (3). Then, by Claim 1, B_i $(i \geq 2)$ is not a branch point for β. Thus, B_1 is the only branch point for β. Then, by Hurwitz's formula, we have $2g(X_3) - 2 = -2b + c$, where $g(X_3)$ is the genus of X_3, b is the degree of β, and $c \leq b - 1$. Since $g(X_3) \geq 0$, 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 $R_i^{'} = \alpha(R_i)$ $(1 \leq i \leq r)$. In the case (I), by Claim 3, β is unramified at $R_i^{'}$ $(i \geq 3)$. Since X_2 and X_3 are rational, from Hurwitz's formula, we infer that β is ramified with the index $e(R_1^{'}, \beta) = e(R_2^{'}, \beta) = \deg \beta$. Then, since there exists no ramification points in $f^{-1}(f(R_i))$ except R_i $(i = 1, 2)$, α must branch at $R_1^{'}$ and $R_2^{'}$. However, there exists an unramified point in $f^{-1}(f(R_2))$, this is a contradiction. Therefore, f is indecomposable. In the case (II), by Claim 1, β is unramified at $R_i^{'}$ for $i \geq 2$. Since X_3 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 X_2 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 G_P is not primitive and let G_x be the isotropy group of $x = x_1$ in G_P. Then, there exists a subgroup H of G_P such that $G_x \subsetneq H \subsetneq$

G_P. Let C_H be the nonsingular model of the intermediate field which corresponds to H by the Galois correspondence. Then, there exist the coverings $\alpha : \widetilde{C} \to C_H$ and $\beta : C_H \to \mathbb{P}^1$ such that $\pi_P = \beta\alpha$. Thus, π_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 π_P and π_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 ℓ satisfies the following conditions:

(1) ℓ does not pass through any cusp;

(2) ℓ is not the tangent line to C at the flex.

Then, ℓ is a simple 2-tangent line to C or ℓ 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 directly. In fact, if $P = P_1$, then consider the affine part $Z \neq 0$ of C, that is, the affine defining equation is $y^e - x^d = 0$. Then, putting $y = tx$, we get $t^e - x^{d-e} = 0$, hence $G_P \cong Z_{d-e}$. The other case $P = P_2$ is similarly determined. If $P = P_3$, then consider the affine part $X \neq 0$, we get $y^e z^{d-e} = 1$. Putting $z = ty$, we get $t^{d-e} y^d = 1$, hence $G_P \cong Z_d$. 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 ℓ_P passes through neither P_1 nor P_2, then it 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 $G_P \cong S_{d-1}$. 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 ℓ_P does not pass through P_2, then it has normal crossings with C or it is a simple 2-tangent line to C. By (2) in Proposition 11 and Lemma 15, we have $G_P \cong S_{d-1}$. 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 $P \in \ell_{P_1P_2}$ and $1 < e < d-1$, then π_P has two ramification points R_1 and R_2 such that $e(R_1) = e$, $e(R_2) = d-e$ and $\pi_P(R_1) = \pi_P(R_2)$. Thus, π_P is not an s-covering. If ℓ_P passes through neither P_1 nor P_2, then ℓ_P is a simple 2-tangent to C or has normal crossings with C. By (3) in Proposition 10, π_P is indecomposable. Since there exists a simple 2-tangent ℓ_P, we conclude $G_P \cong S_d$. In case $P \in \ell_{P_1P_2}$ and $e = 1$ or $d-1$, π_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 ℓ_P, thus we conclude $G_P \cong S_d$. In view of Remark 19, we conclude easily from the similar argument that $G_P \cong S_d$ when $P \in \mathbb{P}^2 \setminus \{C \cup \ell_{P_1P_2}\}$.

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, $i(C, T_F; F) = 3$ and T_F does not pass though 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 $G_P \cong Z_2$. 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 $G_P \cong S_3$. Then consider the case $P \in \mathbb{P}^2 \setminus C$. If $P \in \ell_{P_1P_2}$, then π_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, π_P is not an s-covering. Consider π_P for the most special case $\ell_{P_1P_2} \cap T_F = \{P\}$. 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 $G_P \cong S_4$. 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 $G_P \cong S_4$.

Proof of the Case (III). Assume $C = C_{54}$. It has the following property. There exists a projective transformation σ such that $\sigma(C) = C$ and $\sigma(X, Y, Z) = (Y, X, -Z)$, $(-X, Z, Y)$ or (Z, Y, X) so that σ interchanges P_i $(i = 1, 2, 3)$.

Claim 4. The flexes of C are $F_1 = (4 : -1 : 4)$, $F_2 = (1 : -4 : 4)$, and $F_3 = (4 : -4 : 1)$, 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 $\ell = \ell_{Q_i}$ does not pass through any cusp, then ℓ and C have normal crossings or there exist two points $Q' \in C$ satisfying $i(C, \ell; Q') \geq 3$.

Such Q_i is an intersection $L_j \cap L_k$, where $\{i, j, k\} = \{1, 2, 3\}$, indeed $Q_1 = (1 : -7 : 1)$, $Q_2 = (7 : -1 : 1)$, and $Q_3 = (1 : -1 : 7)$. Therefore, if $P \in \mathbb{P}^2 \setminus \{C, Q_1, Q_2, Q_3\}$, then there exists a line ℓ passing through P such that ℓ 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 is primitive. The lines $\ell_{P_1P_2}$ and $\ell_{P_1P_3}$ yield the ramification points of order three of π_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 σ above, we see $G_{P_i} \cong S_3$ $(i = 2, 3)$.

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; $n_3 = 0$ (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, and 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 $i(C, \ell_{PP_i}; P_i) = 3$, hence $n_3 = 3$. □

Claim 6. If π_P is an s-covering, then π_P is indecomposable.

Proof. By Claim 5 the ramification index is 2, 3, or 4. Suppose π_P is decomposable. Then, $\deg \beta = 2$ or 3. By Claim 1, β is 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 10, β 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 $\deg \beta = 2$, β is ramified at R_1' and R_2'. Since $\deg \alpha = 3$, this cannot occur. In case $\deg \beta = 3$, β 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 $(4^3, 2^3) := (4, 4, 4, 2, 2, 2)$. Suppose π_P is decomposable. Then, $\deg \beta = 2$ or 3. If $\deg \beta = 2$, then β is ramified at R_i', $(i = 1, 2, 3)$. However, since $\deg \alpha = 3$, this case cannot occur. Then, we have $\deg \beta = 3$. We see easily that β is ramified at R_i' with $e(R_i', \beta) = 2$ $(i = 1, 2, 3)$. However, this does not satisfy Hurwitz's formula. Therefore, π_P is indecomposable. □

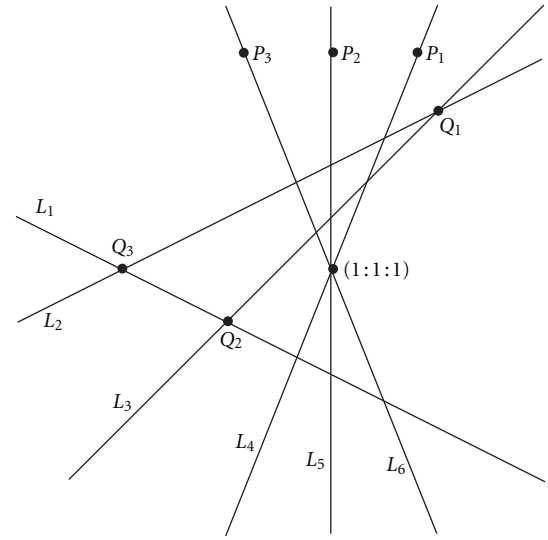

Figure 1

Now we resume the proof. We prove by examining the cases:

(i) $P = (1 : 1 : 1)$;

(ii) $P = Q_i$ $(i = 1, 2, 3)$;

(iii) $P \in \ell_{P_iP_j}$ $(1 \leq i, j \leq 3)$, $P \neq (1 : 1 : 1)$, and $P \neq Q_i$ $(i = 1, 2, 3)$;

(iv) P is the point not appearing in the above case.

By Claims 5 and 6, the proof is complete for (i) and (iv). So let us treat the case (ii). By Claim 6, G_P is primitive. However, there exists no simple 2-tangent line. Take $Q_1 = (1 : -7 : 1)$ and consider the affine part $Z \neq 0$. The defining equation is $(xy - x + y)^3 + 54x^2y^2 = 0$. Putting $u = x - 1$, $v = y + 7$ and $v = tu$, we get $h(t, u) := (tu^2 - 8u + 2tu - 15)^3 + 54(u + 1)(tu - 7)^2 = 0$. Here, we consider the Galois group obtained by the special value $t = 2$. By the aid of a software, for example, PARI, we see that the polynomial $h(2, u) = (2u^2 - 4u - 15)^3 + 54(u + 1)(2u - 7)^2$ in $\mathbb{Q}[u]$ is irreducible and the Galois group of this polynomial is S_6. Let $u_1(t), \ldots, u_6(t)$ be the roots of $h(t, u) = 0$ with respect to u. Note that $u_i(t)$ $(1 \leq i \leq 6)$ is regular near $t = 2$ and $\{u_1(2), \ldots, u_6(2)\}$ are the roots of $h(2, u) = 0$. We can find $c_i \in \mathbb{Q}(1 \leq i \leq 6)$ satisfying the conditions: $\widetilde{u}(t) = c_1u_1(t) + \cdots + c_6u_6(t)$ (resp., $\widetilde{u}(2) = c_1u_1(2) + \cdots + c_6u_6(2)$) is a generator of the minimal splitting field of $h(t, u)$ (resp., $h(2, u)$) over $k(t)$ (resp., $\mathbb{Q}$). Suppose the degree of $\widetilde{u}(t)$ is less than 6!. Then, so is $\widetilde{u}(2)$, which is a contradiction. Hence we have $[k(t, u) : k(t)] = 6!$, thus we conclude $G_P \cong S_6$. 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 $P \in \ell_{P_iP_j}$, $i \neq j$, $(i, j = 1, 2, 3)$, then π_P is not an s-covering. First we consider the special case where P is in some T_{F_i}, for example, $\ell_{P_1P_2} \cap T_{F_1} = \{P\}$. Then the ramification data is $\{(F_1, P_1, P_2, P_3, R_5, R_6, R_7), (4, 3^3, 2^3)\}$ and $\pi_P(P_1) = \pi_P(P_2)$. Suppose π_P is decomposable. Then, by Claim 1, $\beta : X_3 \to \mathbb{P}^1$ is unramified at $\alpha(P_3)$ and $R_i^{'}, (i \geq 5)$. Namely, β is ramified at just two points. Then, the ramification data of β 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 α and π_P, so π_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," *Matemática Contemporânea*, 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," *Sûgaku*, vol. 32, no. 4, pp. 367–369, 1980 (Japanese).

[9] S. Iitaka, K. Ueno, and Y. Namikawa, *Descartes No Seishin To Daisûkika*, NipponHyoron Sha, Tokyo, Japan, 1980.

[10] M. Oka, "Elliptic curves from sextics," *Journal of the Mathematical Society of Japan*, vol. 54, no. 2, pp. 349–371, 2002.

[11] G. P. Pirola and E. Schlesinger, "Monodromy of projective curves," *Journal of Algebraic Geometry*, vol. 14, no. 4, pp. 623–642, 2005.

[12] W. Fulton, *Algebraic Curves*, Mathematics Lecture Notes Series, Benjamin, New York, NY, USA, 1969.

[13] K. Miura and H. Yoshihara, "Field theory for function fields of plane quartic curves," *Journal of Algebra*, vol. 226, no. 1, pp. 283–294, 2000.