# GALOIS GROUP AT EACH POINT FOR SOME SELF-DUAL CURVES

HIROYUKI HAYASHI

Doctoral Program in Information Science and Engineering
Graduate School of Science and Technology
Niigata University

The purpose of the present thesis is to determine the Galois groups at each point for some self-dual curves. This thesis is divided into four sections. Sections 1-3 are devoted to preliminaries of Section 4.

In Section 1 we begin by defining an analytic subset in a complex manifold. We introduce affine algebraic sets and projective algebraic sets as examples of analytic subsets. Section 2 treats Riemann surfaces and covering spaces. And we state the connection between Galois covering maps and Galois extensions of the fields of meromorphic functions. We also note the Riemann-Hurwitz formula for a compact Riemann surface. Section 3 is concerned with algebraic curves in a projective plane. For an algebraic curve we define the dual curve and give an example. In Section 4 we proceed to the main subject of the present thesis. First, for an irreducible algebraic curve and a point on a projective plane we define the Galois group at the point and give the definition of self-dual curves. We rewrite a condition being primitive represented by group theory in theory of covering spaces in our case.

The author wishes to express his sincere thanks to Professor Yoshihara for valuable suggestions given during the period of the preparation of this thesis.

## 1. Complex Manifolds

### 1.1. **Analytic Subsets.** Let $X$ be an $n$-dimensional complex manifold.

**Definition 1.1.** A subset $A \subset X$ is said to be *analytic* if for each point $q \in X$ there are a (connected) open neighborhood $U(q)$ of $q$ and finitely many holomorphic functions $f^1(p), \dots, f^\nu(p)$ on $U(q)$ such that

$$A \cap U(q) = \{p \in U(q) \mid f^1(p) = \cdots = f^\nu(p) = 0\}.$$

We call $A$ an *analytic hypersurface* if we can always take $\nu = 1$.

Examples. (1) A subset $A = \{1/m \mid m \in \boldsymbol{N}\}$ of a complex plane $\boldsymbol{C}$ is an analytic subset of $\boldsymbol{C}$, but $A \cup \{0\} = \{1, 1/2, \dots, 1/m, \dots\} \cup \{0\}$ is not an analytic subset of $\boldsymbol{C}$.

(2) We consider the domain $G = G_1 \cup G_2$ with

$$G_1 = \{(z_1, z_2) \in \boldsymbol{C}^2 \mid |z_1| < \frac{1}{2} \text{ and } |z_2| < 1\},$$

$$G_2 = \{(z_1, z_2) \in \boldsymbol{C}^2 \mid |z_1| < 1 \text{ and } \frac{1}{2} < |z_2| < 1\}.$$

For the analytic subset we take $A = \{(z_1, z_2) \in G_2 \mid z_1 = z_2\}$. The sets $G_1, G_2$ give an open covering of $G$ with $A \cap G_1 = \emptyset$ and $A \cap G_2 = \{(z_1, z_2) \in G_2 \mid z_1 - z_2 = 0\}$. So $A$ is an analytic subset of $G$.

**Definition 1.2.** Let $A \subset X$ be an analytic subset. Then $A$ is said to be *reducible* if there exist analytic subsets $A_1, A_2 \subset X$ such that $A = A_1 \cup A_2, A \neq A_1, A \neq A_2$. Otherwise, $A$ is said to be *irreducible*.

Let $f^1(p), \dots, f^\nu(p)$ be holomorphic functions that are defined on an open subset $U \subset X$. Let $q \in U$ be a point and $z : p \longrightarrow z(p) = (z^1(p), \dots, z^n(p))$ be a

complex local coordinates of $q$. The mapping $f : p \longrightarrow f(p) = (f^1(p), \ldots, f^\nu(p))$ is holomorphic, and we consider

$$\frac{\partial(f^1(z(p)), \ldots, f^\nu(z(p)))}{\partial(z^1(p), \ldots, z^n(p))} = \left(\frac{\partial f^j(z(p))}{\partial z^k(p)}\right)_{\substack{j=1,\ldots,\nu \\ k=1,\ldots,n}}.$$

This is something like a Jacobian matrix of $f$ at $p$, but it depends on the local coordinates $(z^1, \ldots, z^n)$. Let $w : p \longrightarrow w(p) = (w^1(p), \ldots, w^n(p))$ be other local complex coordinates of $q$. Since

$$\frac{\partial f^j(z(p))}{\partial z^k(p)} = \sum_{l=1}^{n} \frac{\partial f^j(w(p))}{\partial w^l(p)} \cdot \frac{\partial w^l(p)}{\partial z^k(p)}, \quad w^l(p) = w^l(z(p)),$$

we have

$$\frac{\partial(f^1(z(p)), \ldots, f^\nu(z(p)))}{\partial(z^1(p), \ldots, z^n(p))} = \frac{\partial(f^1(w(p)), \ldots, f^\nu(w(p)))}{\partial(w^1(p), \ldots, w^n(p))} \cdot \frac{\partial(w^1(p), \ldots, w^n(p))}{\partial(z^1(p), \ldots, z^n(p))}.$$

This shows that

$$\operatorname{rank} \frac{\partial(f^1(z(p)), \ldots, f^\nu(z(p)))}{\partial(z^1(p), \ldots, z^n(p))}$$

is independent of the chosen local complex coordinates $(z^1, \ldots, z^n)$.

**DEFINITION 1.3.** An analytic subset $A \subset X$ is said to be *regular* (or *smooth* or *nonsingular*) *of codimension* $\nu$ at a point $q \in A$ if there are open neighborhood $U(q) \subset X$ of $q$ and holomorphic functions $f^1(p), \ldots, f^\nu(p)$, $\nu = \nu(q)$, on $U(q)$ such that:

(i) $A \cap U(q) = \{p \in U(q) \mid f^1(p) = \cdots = f^\nu(p) = 0\}$.

(ii) $\operatorname{rank} \dfrac{\partial(f^1(z(q)), \ldots, f^\nu(z(q)))}{\partial(z^1(q), \ldots, z^n(q))} = \nu$.

The number $n - \nu$ is called the *dimension* of $A$ at $q$.

1.2. **Projective Algebraic Manifolds.** Denote by $\boldsymbol{P}^n$ a complex projective space of dimension $n$.

**DEFINITION 1.4.** An analytic subset $X \subset \boldsymbol{P}^n$ that is the zero set of finitely many homogeneous polynomials is called a (*projective*) *algebraic set*. The subsets

$$X \cap \{(\zeta_0, \ldots, \zeta_n) \in \boldsymbol{P}^n \mid \zeta_j \neq 0\}$$

are called (*affine*) *algebraic set*.

A complex manifold $X$ is called *projective algebraic manifold* if there are a positive integer $N$ and a holomorphic embedding $j : X \longrightarrow \boldsymbol{P}^N$ such that $j(X)$ is a regular algebraic set.

Example. We consider $\boldsymbol{C} - 0$. Using a mapping $t \longrightarrow (z_1, z_2) = (t, 1/t), t \in \boldsymbol{C} - 0$, we find that $\boldsymbol{C} - 0$ is mapped biholomorphically onto an affine algebraic hypersurface $\{z \in \boldsymbol{C}^2 \mid P(z_1, z_2) = 0\}$, where $P(z_1, z_2) = z_1 z_2 - 1$. Then

$$\bar{P}(\zeta_0, \zeta_1, \zeta_2) = \zeta_1 \zeta_2 - \zeta_0^2$$

is a homogeneous polynomial of degree 2. The projective algebraic subset $\{\zeta \in \boldsymbol{P}^2 \mid \bar{P}(\zeta_0, \zeta_1, \zeta_2) = 0\}$ is such that

$$\{\zeta \in \boldsymbol{P}^2 \mid \bar{P}(\zeta_0, \zeta_1, \zeta_2) = 0\} - \{\zeta \in \boldsymbol{P}^2 \mid \zeta_0 = 0\} \cong \{z \in \boldsymbol{C}^2 \mid P(z_1, z_2) = 0\}.$$

Let $\pi : \boldsymbol{C}^{n+1} - 0 \longrightarrow \boldsymbol{P}^n$ be the canonical projection.

**THEOREM 1.1** (Chow)**.** *Every analytic subset $X$ in the projective space $\boldsymbol{P}^n$ is the zero set of finitely many homogeneous polynomials $F_1, \ldots, F_s$ such that if $x \in X$ is a regular point of codimension $\nu$, then*

$$\operatorname{rank} \frac{\partial(F_1(z), \ldots, F_s(z))}{\partial(z_0, \ldots, z_n)} = \nu$$

*for every $z \in \pi^{-1}(x)$.*

Let $V \subset \boldsymbol{C}^{n+1}$ be a complex linear subspace of codimension $\nu$. Then there are linear forms $f_1, \ldots, f_\nu$ on $\boldsymbol{C}^{n+1}$ such that

$$V = \{z \in \boldsymbol{C}^{n+1} \mid f_j(z) = 0, \quad j = 1, \ldots, \nu\}.$$

Since the linear forms are homogeneous polynomials of degree 1,

$$\boldsymbol{P}(V) = \{(\zeta_0, \ldots, \zeta_n) \in \boldsymbol{P}^n \mid f_j(\zeta_0, \ldots, \zeta_n) = 0, \quad j = 1, \ldots, \nu\}$$

is a regular algebraic set. We call $\boldsymbol{P}(V)$ a (*projective*) *linear subspace*. It is complex analytically homeomorphic to $\boldsymbol{P}^{n-\nu}$.

The dimension of a linear subspace $\boldsymbol{P}(V) \subset \boldsymbol{P}^n$ is one less than the dimension of the vector subspace $V$:

$$\dim \boldsymbol{P}(V) = \dim V - 1.$$

By definition, the empty set has dimension $-1$.

Linear subspaces of dimension zero are the points; a linear subspace of dimension one is called a line. In general, a linear subspace of dimension $k$ is called a *$k$-plane*.

Suppose that $Z \subset \boldsymbol{P}^n$ is any subset. We define the *span of* $Z$, denoted by $\langle Z \rangle$, to be the intersection of all linear subspaces containing $Z$. If $\boldsymbol{P}(V) = \langle Z \rangle$, we might also say that $Z$ spans $\boldsymbol{P}(V)$. We say that $Z$ is *nondegenerate* if $Z$ spans all of $\boldsymbol{P}^n$.

We have the following dimension formula, which follows easily from the corresponding formula for vector subspaces of a vector space:

**LEMMA 1.1.** *If $L$ and $M$ are two linear subspaces of $\boldsymbol{P}^n$, then*

$$\dim\langle L \cup M \rangle = \dim L + \dim M - \dim(L \cup M).$$

Two disjoint linear subspaces $L \subset \boldsymbol{P}^n$ and $M \subset \boldsymbol{P}^n$, $\dim L + \dim M = n$, are called *complementary* linear subspaces.

Let $L \subset \boldsymbol{P}^n$ be a $k$-plane and $M \subset \boldsymbol{P}^n$ be an $(n - k - 1)$-plane which are disjoint subspaces. Note that $L$ and $M$ together span all of $\boldsymbol{P}^n$.

Suppose $p$ is a point not on $L$. Then the span of $L \cup p$ is a linear subspace $L_1$ which has dimension one more than that of $L$, i.e., $L_1$ is a $(k+1)$-plane. Hence by the dimension formula, we see that

$$\begin{aligned}\dim(L \cap M) &= \dim L_1 + \dim M - \dim\langle L_1 \cup M\rangle \\ &= (k+1) + (n-k+1) - n \\ &= 0,\end{aligned}$$

so that $L_1 \cap M$ is a single point, in $M$ of course.

**DEFINITION 1.5.** The *projection* from $L$ to $M$ is the mapping

$$\pi : \boldsymbol{P}^n - L \longrightarrow M$$

defined by sending a point $p \in \boldsymbol{P}^n - L$ to the intersection point of $\langle L \cup p\rangle$ with $M$:

$$\pi(p) = \langle L \cup p\rangle \cap M.$$

The subspace $L$ is called the *center of projection*.

It is easy to see that if $L$ is defined by $\zeta_{k+1} = \zeta_{k+2} = \cdots = \zeta_n = 0$ and $M$ is described by $\zeta_0 = \zeta_1 = \cdots = \zeta_k = 0$, then

$$\pi(\zeta_0, \zeta_1, \ldots, \zeta_n) = (0, 0, \ldots, 0, \zeta_{k+1}, \zeta_{k+2}, \ldots, \zeta_n).$$

One often suppresses the choice of the target subspace $M$ in the language, and refers to $\pi$ simply as "the projection from $L$". The reason for this is that if $M_1$ and $M_2$ are two complementary subspaces to $L$, with projections $\pi_1$ from $L$ to $M_1$ and $\pi_2$ from $L$ to $M_2$, then the restriction of $\pi_2$ to $M_1$ is a projective transformation $\varphi : M_1 \longrightarrow M_2$, and

$$\varphi \circ \pi_1 = \pi_2.$$

So for most purposes it does not matter which subspace one is projecting to.

**DEFINITION 1.6.** Let $V$ be a complex vector space. The *dual projective space* $\boldsymbol{P}(V)^*$ is the set of codimension one subspaces of $V$.

Note that any codimension one subspace $W$ of $V$ induces a hyperplane $\boldsymbol{P}(W) \subset \boldsymbol{P}(V)$; indeed, the dual space $\boldsymbol{P}(V)^*$ may be identified with the set of hyperplanes in $\boldsymbol{P}(V)$.

**THEOREM 1.2.** *There is a natural bijection between $\boldsymbol{P}(V^*)$ and $\boldsymbol{P}(V)^*$ given by associating to the span of nonzero functional $f : V \longrightarrow \boldsymbol{C}$ the codimension one subspace which is the kernel of $f$.*

We consider some connections with complex algebraic geometry.

A meromorphic function $f$ on $\boldsymbol{P}^n$ is called *rational* if $f = 0$, or if there are homogeneous polynomials $F$ and $G$ of the same degree such that $F \neq 0$ and

$$f(\zeta_0, \ldots, \zeta_n) = \frac{F(\zeta_0, \ldots, \zeta_n)}{G(\zeta_0, \ldots, \zeta_n)}.$$

**THEOREM 1.3.** *Every meromorphic function on $\boldsymbol{P}^n$ is rational.*

## 1.3. **Modifications.**

**DEFINITION 1.7.** Let $f : X \longrightarrow Y$ be a proper surjective holomorphic mapping between two $n$-dimensional connected complex manifolds. The mapping $f$ is called a (*proper*) *modification* of $Y$ if there are nowhere dense analytic subsets $E \subset X$ and $S \subset Y$ such that the following hold:

(i) $f(E) \subset S$.
(ii) $f$ maps $X - E$ biholomorphically onto $Y - S$.
(iii) Every fiber $f^{-1}(y), y \in S$, consists of more than one point.

The set $S$ is called the *center* of the modification and $E = f^{-1}(S)$ the *exceptional set*.

Let $U$ be a small neighborhood around the origin in $\boldsymbol{C}^{n+1}$. We want to replace the origin in $U$ by an $n$-dimensional complex projective space $\boldsymbol{P}^n = \{(\zeta_1, \ldots, \zeta_{n+1}) \in \boldsymbol{P}^n\}$. If $\pi : \boldsymbol{C}^{n+1} - 0 \longrightarrow \boldsymbol{P}^n$ is the canonical projection, then every line $\boldsymbol{C}v$ through the origin determines an element $\zeta = \pi(v)$ in $\boldsymbol{P}^n$, and $\zeta$ determines the line $l(\zeta) = \pi^{-1}(\zeta) \cup 0$ such that $\boldsymbol{C}v = l(\pi(v))$. Now we insert $\boldsymbol{P}^n$ in such a way that we reach the point $\zeta$ by approaching the origin along $l(\zeta)$.

We define

$$X = \{(z, \zeta) \in U \times \boldsymbol{P}^n \mid z \in l(\zeta)\}$$

and this can be rewritten in the form

$$X = \{(z, \zeta) \in U \times \boldsymbol{P}^n \mid \zeta_j z_k - \zeta_k z_j = 0, \quad j, k = 1, \ldots, n+1\}.$$

This is so-called *incidence set*. We first show that it is an $(n+1)$-dimensional complex manifold. Set $U_j = \{\zeta \in \boldsymbol{P}^n \mid \zeta_j \neq 0\}, j = 1, \ldots, n+1$. Then $X$ is an analytic subset of $U \times \boldsymbol{P}^n$, with

$$X \cap (U \times U_1) \cong \{(z, w) \in U \times \boldsymbol{C}^n \mid z_k = w_k z_1, \quad k = 2, 3, \ldots, n+1\}, \quad w_k = \zeta_k/\zeta_1.$$

In $U \times U_j, j = 2, \ldots, n+1$, there is a similar representations. It follows that $X$ is a submanifold of codimension $n$ in the $(2n+1)$-dimensional manifold $U \times \boldsymbol{P}^n$. We have a holomorphic mapping $q : (z, \zeta) \longrightarrow z$ of $X$ onto $U$ which maps $X - q^{-1}(0)$ biholomorphically onto $U - 0$ and $q^{-1} : z \longrightarrow (z, \pi(z))$. Obviously, $q$ is a proper mapping.

The preimage $q^{-1}(0)$ is the exceptional set $\{(0, \zeta) \in X \mid 0 \in l(\zeta)\} = 0 \times \boldsymbol{P}^n$. So $q : X \longrightarrow U$ is a proper modification. It is called *Hopf's $\sigma$-process* or the *blowing up* of $U$ at the origin.

If $z \neq 0$ is a point of $U$ and $\{\lambda_\nu\}$ a sequence of nonzero complex numbers converging to 0, then $q^{-1}(\lambda_\nu z) = (\lambda_\nu z, \pi(z))$ converges to $(0, \pi(z))$. This is the desired property.

We consider the case $n = 1$. Let $M$ be a 2-dimensional connected complex manifold and $p \in M$ a point. Let $U \subset M$ be a small neighborhood with complex coordinates $z, w$ such that $(z(p), w(p)) = (0, 0)$. Let $X \subset U \times \boldsymbol{P}^1$ be the blowing up of $U$ at the origin. Then

$$Q_p(M) = (M - U) \cup X = (M - p) \cup \boldsymbol{P}^1$$

is again a 2-dimensional complex manifold. We call $Q_p(M)$ the *qudratic transformation* of $M$ at $p$.

Let $F : M_1 \longrightarrow M_2$ be a holomorphic mapping between 2-dimensional complex manifolds and $F(p_1) = p_2$. Let $q_1 : Q_{p_1}(M_1) \longrightarrow M_1$ and $q_2 : Q_{p_2}(M_2) \longrightarrow M_2$ be the quadratic transformations. Then there exists a biholomorphic mapping $\hat{F} : Q_{p_1}(M_1) \longrightarrow Q_{p_2}(M_2)$ such that $q_2 \circ \hat{F} = F \circ q_1$. This follows directly from the construction, and it shows that the quadratic transformation is a canonical process.

## 2. Covering Spaces and Compact Riemann Surfaces

Riemann surfaces, i.e., connected 1-dimensional complex manifolds, originated in function theory as a means of dealing with the problem of multi-valued functions. Such multi-valued functions occur because the analytic continuation of a given holomorphic function element along different paths leads in general to different branches of that function. It was the idea of Riemann to replace the domain of the function with a many sheeted covering of the complex plane. If the covering is constructed so that it has as many points lying over any given point in the plane as there are function elements at that point, then on this "covering surface" the analytic function becomes single-valued.

### 2.1. **Elementary Properties of Holomorphic Mappings.**

We note some of the elementary topological properties of holomorphic mappings between Riemann surfaces.

**Theorem 2.1.** *Let $X$ and $Y$ be Riemann surfaces and $f : X \longrightarrow Y$ be a non-constant holomorphic mapping and $a \in X$ and $b = f(a)$. Then there exists a positive integer $k$ and coordinate systems $\varphi : U \longrightarrow V$ on $X$ and $\psi : U' \longrightarrow V'$ on $Y$ with the following properties:*

(i) $a \in U, \varphi(a) = 0, \quad b \in U', \psi(b) = 0.$

(ii) $f(U) \subset U'$.

(iii) *The mapping $F = \psi \circ f \circ \varphi^{-1} : V \longrightarrow V'$ is given by*

$$F : z \longrightarrow F(z) = z^k, \quad z \in V.$$

The number $k$ in Theorem 2.1 can be characterized in the following way. For every neighborhood $U_0$ of $a$ there exist neighborhoods $U \subset U_0$ of $a$ and $W$ of $b = f(a)$ such that the set $f^{-1}(y) \cap U$ contains exactly $k$ elements for every point $y \in W, y \neq b$. We call $k$ the *multiplicity* with which the mapping $f$ takes the value $b$ at the point $a$ or we just say that $f$ has *multiplicity* $k$ at the point $a$.

### 2.2. **Branched and Unbranched Coverings.**

Nonconstant holomorphic mappings between Riemann surfaces are "covering mappings", possibly having "branch points". For this reason we now gather together the most important ideas and results from the theory of covering spaces.

**Definition 2.1.** Let $X$ and $Y$ be Riemann surfaces and $p : Y \longrightarrow X$ be a non-constant holomorphic mapping. A point $y \in Y$ is called a *branch point* of $p$ if there is no neighborhood $V$ of $y$ such that $p|V$ is injective. The mapping $p$ is called an *unbranched holomorphic mapping* if it has no branch points.

**THEOREM 2.2.** *Let $X$ and $Y$ be Riemann surfaces. A non-constant holomorphic mapping $p : Y \longrightarrow X$ has no branch points if and only if $p$ is a local homeomorphism.*

Examples. (1) Let $k$ be a natural number $\geqq 2$ and $p_k : \boldsymbol{C} \longrightarrow \boldsymbol{C}$ be the mapping defined by $p_k : z \longrightarrow p_k(z) = z^k$. Then $0 \in \boldsymbol{C}$ is a branch point of $p_k$ and the mapping $p_k|(\boldsymbol{C} - 0) : \boldsymbol{C} - 0 \longrightarrow \boldsymbol{C}$ is unbranched.
(2) Let $p : Y \longrightarrow X$ be a nonconstant holomorphic mapping and $y \in Y$, $x = p(y)$. Then $y$ is a branch point if and only if the mapping $p$ takes the value $x$ at the point $y$ with multiplicity $\geqq 2$. By Theorem 2.1 the local behavior of $p$ near $y$ is just the same as the local behavior of the mapping $p_k$ in Example (1) near the origin.

**DEFINITION 2.2.** Let $X$ and $Y$ be topological spaces. A mapping $p : Y \longrightarrow X$ is called a *covering map* if the following hold:

Every point $x \in X$ has an open neighborhood $U$ such that its preimage $p^{-1}(U)$ can be represented as

$$p^{-1}(U) = \bigcup_j V_j,$$

where the $V_j$ are disjoint open subsets of $Y$, and all the mappings $p|V_j : V_j \longrightarrow U$ are homeomorphisms. In particular, $p$ is a local homeomorphism.

Examples. (1) Let $D = \{z \in \boldsymbol{C} \mid |z| < 1\}$ be the unit disk in the complex plane and let $p : D \longrightarrow \boldsymbol{C}$ be the canonical injection. Then $p$ is a local homeomorphism, but not a covering map. For, no point $a \in \boldsymbol{C}$ with $|a| = 1$ has a neighborhood $U$ with the property required in the definition.

(2) Let $k$ be a natural number $\geqq 2$ and let

$$p_k : z \longrightarrow p_k(z) = z^k, \quad z \in \boldsymbol{C} - 0.$$

Then $p_k$ is a covering map. *Proof*: Suppose $a \in \boldsymbol{C} - 0$ is arbitrary and choose $b \in \boldsymbol{C} - 0$ with $p_k(b) = a$. Since $p_k$ is a local homeomorphism, there are open neighborhoods $V_0$ of $b$ and $U$ of $a$ such that $p_k|V_0 : V_0 \longrightarrow U$ is a homeomorphism. Then

$$p_k^{-1}(U) = V_0 \cup \omega V_0 \cup \cdots \cup \omega^{k-1} V_0,$$

where $\omega$ is a $k$th primitive root of unity, say $\omega = \exp(2\pi i/k)$. It is clear that the sets $V_j = \omega^j V_0, j = 0, \ldots, k-1,$ are pairwise disjoint and each $p_k|V_j : V_j \longrightarrow U$ is a homeomorphism.

(3) The mapping $\exp : \boldsymbol{C} \longrightarrow \boldsymbol{C} - 0$ is a covering map. *Proof*: Suppose $a \in \boldsymbol{C} - 0$ and $b \in \boldsymbol{C}$ with $\exp(b) = a$. Since $\exp$ is a local homeomorphism, there exist open neighborhoods $V_0$ of $b$ and $U$ of $a$ such that $\exp|V_0 : V_0 \longrightarrow U$ is a homeomorphism. Then

$$\exp^{-1}(U) = \bigcup_{n \in \boldsymbol{Z}} V_n,$$

where $V_n = V_0 + 2\pi i n$. Clearly the $V_n$ are pairwise disjoint and each mapping $\exp|V_n : V_n \longrightarrow U$ is a homeomorphism.

**THEOREM 2.3.** *Let $X$ and $Y$ be Hausdorff spaces with $X$ pathwise connected and $p : Y \longrightarrow X$ be a covering map. Then for any two points $x_0, x_1 \in X$ the sets $p^{-1}(x_0), p^{-1}(x_1)$ have the same cardinality.*

The cardinality of $p^{-1}(x)$ for $x \in X$ is called the *number of sheets* of the covering and may be either finite or infinite.

Let $X$ and $Y$ be Riemann surfaces and $f : X \longrightarrow Y$ be a proper nonconstant holomorphic mapping. It follows from Theorem 2.1 that the set $A$ of branch points of $f$ is closed and discrete. Since $f$ is proper, $B = f(A)$ is also closed and discrete. We call $B$ the set of *critical values* of $f$.

Let $Y' = Y - B$ and $X' = X - f^{-1}(B) \subset X - A$. Then $f|X' : X' \longrightarrow Y'$ is a proper unbranched holomorphic covering and it has a well-defined finite number of sheets $n$. This means that every value $c \in Y'$ is taken exactly $n$ times. In order to be able to extend this statement to the critical values $b \in B$ as well, we have to consider the multiplicities.

For $x \in X$ denote by $v(f, x)$ the multiplicity with which $f$ takes the values $f(x)$ at the point $x$. Then we shall say that $f$ takes the value $c \in Y$, counting multiplicities, $m$ times on $X$, if

$$m = \sum_{x \in f^{-1}(c)} v(f, x).$$

**THEOREM 2.4.** *Let $X$ and $Y$ be Riemann surfaces and $f : X \longrightarrow Y$ be a proper nonconstant holomorphic mapping. Then there exists a natural number $n$ such that $f$ takes every value $c \in Y$, counting multiplicities, $n$ times.*

A proper nonconstant holomorphic map will be called an *$n$-sheeted holomorphic covering map*, where $n$ is the integer found in the previous theorem. Note that holomorphic covering maps are allowed to have branch points. If we wish to emphasize that there are none, then we shall specifically say that the map is *unbranched*. If we speak of a topological covering map or if there is no complex structure, then we mean a covering map in the sense of Definition 2.2.

**DEFINITION 2.3.** Let $X$ and $Y$ be topological spaces and $p : Y \longrightarrow X$ be a covering map. By a *covering transformation* or *deck transformation* of this covering we shall mean a fiber-preserving homeomorphism $f : Y \longrightarrow Y$. With operation the composition of mappings, the set of all covering transformation of $p : Y \longrightarrow X$ forms a group which we denote by $\mathrm{Deck}(Y/X)$. If there is any chance of confusion, then we will write $\mathrm{Deck}(Y \xrightarrow{p} X)$ instead of $\mathrm{Deck}(Y/X)$.

**DEFINITION 2.4.** Let $X$ and $Y$ be connected Hausdorff spaces and $p : Y \longrightarrow X$ be a covering map. The covering map is said to be *Galois* (the terms *normal* and *regular* are also in common usage) if for every pair of points $y_0, y_1 \in Y$ with $p(y_0) = p(y_1)$ there exists a covering transformation $f : Y \longrightarrow Y$ such that $f(y_0) = y_1$.

Example. The mapping $p_k : z \longrightarrow p_k(z) = z^k, z \in \boldsymbol{C} - 0,$ is a covering map. It is Galois since for any $z_1, z_2 \in \boldsymbol{C} - 0$ with $p_k(z_1) = p_k(z_2)$, we have $z_2 = \omega z_1$, where $\omega$ is a $k$th root of unity and the mapping $z \longrightarrow \omega z$ is a covering transformation.

Let $X$ be a Riemann surface and $U$ be an open subset of $X$. We denote by $\mathscr{M}(U)$ the set of all meromorphic functions on $U$.

If $\pi : Y \longrightarrow X$ is a nonconstant holomorphic mapping between Riemann surfaces $X$ and $Y$, then for any meromorphic function $f$ on $X$ the function $\pi^* f = f \circ \pi$ is a meromorphic function on $Y$. Thus there is a map

$$\pi^* : \mathscr{M}(X) \longrightarrow \mathscr{M}(Y)$$

which is a monomorphism of fields.

The following theorem shows that the continuation of the covering is uniquely determined up to isomorphism.

**THEOREM 2.5.** *Let $X, Y$ and $Z$ be Riemann surfaces and $\pi : Y \longrightarrow X, \tau : Z \longrightarrow X$ be proper holomorphic covering maps. Let $A \subset X$ be a closed discrete subset and let $X' = X - A, Y' = \pi^{-1}(X')$ and $Z' = \tau^{-1}(X')$. Then every fiber-preserving biholomorphic mapping $\sigma' : Y' \longrightarrow Z'$ can be extended to a fiber-preserving biholomorphic mapping $\sigma : Y \longrightarrow Z$. In particular every covering transformation $\sigma' \in \mathrm{Deck}(Y'/X')$ can be extended to a covering transformation $\sigma \in \mathrm{Deck}(Y/X)$.*

Theorem 2.5 makes the following definition meaningful.

**DEFINITION 2.5.** Let $X$ and $Y$ be Riemann surfaces and $\pi : Y \longrightarrow X$ be a branched holomorphic covering. Let $A \subset X$ be the set of critical values of $\pi$ and let $X' = X - A$ and $Y' = \pi^{-1}(X')$. Then the covering $Y \longrightarrow X$ is said to be *Galois* if the covering $Y' \longrightarrow X'$ is Galois.

**THEOREM 2.6.** *Let $X$ be a Riemann surface and*

$$P(T) = T^n + c_1 T^{n-1} + \cdots + c_n \in \mathscr{M}(X)[T]$$

*be an irreducible polynomial of degree $n$. Then there exist a Riemann surface $Y$, a branched holomorphic $n$-sheeted covering $\pi : Y \longrightarrow X$ and a meromorphic function $F \in \mathscr{M}(Y)$ such that $(\pi^* P)(F) = 0$. The triple $(Y, \pi, F)$ is uniquely determined in the following sense. If $(Z, \tau, G)$ has the corresponding properties, then there exists exactly one fiber-preserving biholomorphic mapping $\sigma : Z \longrightarrow Y$ such that $G = \sigma^* F$.*

To simplify the terminology $(Y, \pi, F)$ is called the *algebraic function* defined by the polynomial $P(T)$.

If $X$ and $Y$ are Riemann surfaces and $\pi : Y \longrightarrow X$ is a branched holomorphic covering map, then $\mathrm{Deck}(Y/X)$ has a representation into the automorphism group of the field $\mathscr{M}(Y)$ defined in the following way. For $\sigma \in \mathrm{Deck}(Y/X)$ let

$\sigma f = f \circ \sigma^{-1}$. Clearly the correspondence $f \longrightarrow \sigma f$ is an automorphism of $\mathscr{M}(Y)$. The mapping

$$\mathrm{Deck}(Y/X) \longrightarrow \mathrm{Aut}(\mathscr{M}(Y))$$

is a group homomorphism. For suppose $\sigma, \tau \in \mathrm{Deck(Y/X)}$. Then for every $f \in \mathscr{M}(Y)$

$$(\sigma\tau)f = f \circ (\sigma\tau)^{-1} = f \circ \tau^{-1} \circ \sigma^{-1} = \sigma(f \circ \tau^{-1}) = \sigma(\tau f).$$

Obviously every such automorphism $f \longrightarrow \sigma f$ leaves invariant the functions of the subfield $\pi^*\mathscr{M}(X) \subset Y$ and thus is an element of the Galois group $\mathrm{Aut}(\mathscr{M}(Y)/\pi^*\mathscr{M}(X))$.

**THEOREM 2.7.** *Let $X$ be a Riemann surface, $K = \mathscr{M}(X)$ be the field of meromorphic functions on $X$ and $P(T) \in K[T]$ be an irreducible monic polynomial of degree $n$. Let $(Y, \pi, F)$ be the algebraic function defined by $P(T)$ and $L = \mathscr{M}(Y)$. By means of the monomorphism $\pi^* : K \longrightarrow L$ consider $K$ as a subfield of $L$. Then $L/K$ is a field extension of degree $n$ and $L \cong K[T]/P(T)$. Every covering transformation $\sigma : Y \longrightarrow Y$ of $Y$ over $X$ induces an automorphism $f \longrightarrow \sigma f = f \circ \sigma^{-1}$ of $L$ leaving $K$ fixed and the mapping*

$$\mathrm{Deck}(Y/X) \longrightarrow \mathrm{Aut}(L/K)$$

*which is so defined, is a group isomorphism. The covering map $Y \longrightarrow X$ is Galois if and only if the field extension $L/K$ is Galois.*

2.3. **Compact Riemann Surfaces.** Among all Riemann surfaces the compact ones are especially important. They arise, for example, as those covering surfaces of the Riemann sphere defined by algebraic functions.

**THEOREM 2.8.** *If $X$ is a compact Riemann surface, then*

$$\dim H^1(X, \mathscr{O}) < +\infty.$$

**DEFINITION 2.6.** Let $X$ be a compact Riemann surface. Then

$$g = \dim H^1(X, \mathscr{O})$$

is called the *genus* of $X$.

Let $X$ and $Y$ be compact Riemann surfaces and $f : X \longrightarrow Y$ be a nonconstant holomorphic mapping. For $x \in X$ let $v(f, x)$ be the multiplicity with which $f$ takes the value $f(x)$ at the point $x$. The number

$$b(f, x) = v(f, x) - 1$$

is called the *branching order* of $f$ at the point $x$. Note that $b(f, x) = 0$ if and only if $f$ is unbranched at $x$. Since $X$ is compact, there are only finitely many points $x \in X$ such that $b(f, x) \neq 0$. Thus

$$b(f) = \sum_{x \in X} b(f, x),$$

the *total branching order* of $f$, is well-defined.

**THEOREM 2.9** (Riemann-Hurwitz formula)**.** *Let $f : X \longrightarrow Y$ be an $n$-sheeted holomorphic covering mapping between compact Riemann surfaces $X$ and $Y$ with total branching order $b = b(f)$. Let $g$ be the genus of $X$ and $g'$ be the genus of $Y$. Then we have*

$$2g - 2 = n(2g' - 2) + b.$$

## 3. ALGEBRAIC CURVES

### 3.1. **Affine Algebraic Curves and Projective Algebraic Curves.**

**DEFINITION 3.1.** A subset $C \subset \boldsymbol{C}^2$ is called an *affine algebraic curve* if there exists a polynomial $f \in \boldsymbol{C}[X_1, X_2]$ such that $\deg f \geqq 1$ and

$$C = V(f) = \{(x_1, x_2) \in \boldsymbol{C}^2 \mid f(x_1, x_2) = 0\}.$$

Every polynomial $f \in \boldsymbol{C}[X_1, X_2], \deg f \geqq 1,$ has an associated curve $V(f) \subset \boldsymbol{C}^2$. If $f$ is a divisor of $g \in \boldsymbol{C}[X_1, X_2]$, i.e., if $g = fh$ for some $h \in \boldsymbol{C}[X_1, X_2]$, then $V(f) \subset V(g)$. Since the ring of polynomials is a unique factorization domain, we have a good general idea of the divisibility properties of polynomials. We would like to use these to draw conclusions about the possibles subcurves of a given curve. The following will help us find our way back from the loci of the curves to the polynomials.

**THEOREM 3.1** (Study's lemma)**.** *Let $f, g \in \boldsymbol{C}[X_1, X_2]$. If $f$ is irreducible of degree $\geqq 1$ and $V(f) \subset V(g)$, then $f$ is a divisor of $g$.*

Of the numerous consequences of Study's lemma, the first one we discuss is the decomposition of an algebraic curve into "components". Since rings of polynomials over fields are unique factorization domains, every nonconstant polynomial $f \in \boldsymbol{C}[X_1, X_2]$ admits a factorization

$$f = f_1^{k_1} \cdots f_\rho^{k_\rho} \cdots f_r^{k_r},$$

where the $f_\rho$ are irreducible and no two of them are associates. This factorization is unique up to units and the order in which the $f_\rho$ occur. Hence we have

$$V(f) = V(f_1) \cup \cdots \cup V(f_\rho) \cup \cdots \cup V(f_r).$$

In other words, the curve defined by $f$ can be decomposed into *components* $V(f_\rho)$.

If $C = V(f) = V(g)$ for some other polynomial $g$, then we obtain

$$g = a f_1^{l_1} \cdots f_\rho^{l_\rho} \cdots f_r^{l_r},$$

where $a \in \boldsymbol{C} - 0$ and $l_\rho \in \boldsymbol{N}$.

We shall say

$$\tilde{f} = f_1 \cdots f_r$$

a *minimal polynomial* for the curve $C$.

**DEFINITION 3.2.** If $C = V(f) \subset \boldsymbol{C}^2$ is an affine algebraic curve and $f$ a minimal polynomial, then

$$\deg C = \deg f$$

is called the *degree* of the curve $C$.

**DEFINITION 3.3.** A subset $C \subset \boldsymbol{P}^2$ is called a *projective algebraic curve* if there exists a homogeneous polynomial $F \in \boldsymbol{C}[X_0, X_1, X_2]$ such that $\deg F \geqq 1$ and $C = V(F) = \{(x_0, x_1, x_2) \in \boldsymbol{P}^2 \mid F(x_0, x_1, x_2) = 0\}$.

**LEMMA 3.1.** *Let $f \in \boldsymbol{C}[X_1, X_2]$ be a nonconstant polynomial, and let $F \in \boldsymbol{C}[X_0, X_1, X_2]$ be its homogenization. Then $f$ is irreducible if and only if $F$ is irreducible.*

For nonconstant homogeneous polynomial $F \in \boldsymbol{C}[X_0, X_1, X_2]$ let

$$F = F_1^{k_1} \cdots F_\rho^{k_\rho} \cdots F_r^{k_r}$$

be a prime factorization, where $F_\rho^{k_\rho}$ is homogeneous polynomial. If $C = V(F) = V(G)$ for some other homogeneous polynomial $G$, then we obtain

$$G = aF_1^{l_1} \cdots F_r^{l_r},$$

where $a \in \boldsymbol{C} - 0, l_\rho \in \boldsymbol{N}$.

We shall say

$$\tilde{F} = F_1 \cdots F_r$$

a *minimal polynomial* for the curve $C$.

**DEFINITION 3.4.** If $C = V(f) \subset \boldsymbol{P}^2$ is a projective algebraic curve and $F$ a minimal polynomial, then

$$\deg C = \deg F$$

is called the *degree* of the curve $C$. If $F$ is not necessarily a minimal polynomial, one speaks of the *degree* of the divisor.

To get a first measure of the nastiness of a singularity, we consider higher derivative of the defining polynomial. Let $f \in \boldsymbol{C}[X_1, X_2]$ and $p = (c_1, c_2) \in \boldsymbol{C}^2$ be a fixed point. The substitution

$$X_j = (X_j - c_j) + c_j$$

gives the power series expansion of $f$ about $p$:

$$f(X_1, X_2) = \sum_\nu f_\nu(X_1, X_2),$$

where $f_\nu(X_1, X_2) = \sum_{m_1+m_2=\nu} a_{m_1 m_2}(X_1 - c_1)^{m_1}(X_2 - c_2)^{m_2}, a_{m_1 m_2} = \dfrac{1}{m_1! m_2!} \dfrac{\partial^{m_1+m_2} f(c_1, c_2)}{\partial X_1^{m_1} \partial X_2^{m_2}}$.

Thus the *order* of $f$ at $p$ can be defined as

$$\mathrm{ord}_p(f) = \min\{\nu \mid f_\nu \neq 0\}.$$

If $f$ is a minimal polynomial of a curve $C \subset \boldsymbol{C}^2$, then

$$k_p = \mathrm{ord}_p(C) = \mathrm{ord}_p(f)$$

is called the *order* of $C$ at $p$. It is clear that
(1) $0 \leqq \mathrm{ord}_p(C) \leqq \deg C$,
(2) $p \in C$ if and only if $\mathrm{ord}_p(C) = 1$,
(3) $C$ is singular at $p$ if and only if $\mathrm{ord}_p(C) > 1$.

The extreme case $\mathrm{ord}_p(C) = \deg C$ occurs if and only if $f = f_n$, where $n = \deg C$.

**THEOREM 3.2.** *If $C \subset \boldsymbol{C}^2$ is an affine algebraic curve and $L$ is a line through a point $p \in C$, then*

$$\mathrm{ord}_p(C) \leqq (C.L)_p,$$

*and the inequality is strict for at most $\mathrm{ord}_p(C)$ lines through $p$, where $(C.L)_p$ denotes the intersection multiplicity of $C$ and $L$ at $p$.*

To avoid splitting the definition into cases, we set $(C.L)_p = +\infty$ if $p \in L \subset C$. This allows us to define tangents of an algebraic curve at singular points as well.

**DEFINITION 3.5.** Let $C \subset \boldsymbol{C}^2$ be an algebraic curve and $L$ be a line through a point $p \in C$. The line $L$ is called a *tangent line* of $C$ at $p$ if

$$\mathrm{ord}_p(C) < (C.L)_p.$$

**DEFINITION 3.6.** Let $T$ be the tangent line of $C$ at a smooth point $p$. If $(C.T)_p = 2$ then $T$ is called a *simple tangent*. If $(C.T)_p \geqq 3$ then $T$ is called an *inflectional tangent* and $p$ is called an *inflection point*.

**DEFINITION 3.7.** Let $F \in \boldsymbol{C}[X_0, X_1, X_2]$ be a homogeneous polynomial of degree $\geqq 2$. Then the symmetric $3 \times 3$ matrix

$$H_F = \left( \frac{\partial^2 F}{\partial X_j \partial X_k} \right)_{j,k=0,1,2}$$

is called the *Hessian matrix* of $F$. If $F$ is a minimal polynomial of a curve $C = V(F) \subset \boldsymbol{P}^2$ and $\deg(\det H_F) \geqq 1$, then $H(C) = V(\det H_F)$ is called the *Hessian curve* of $C$.

**THEOREM 3.3.** (1) *The Hessian curve is independent of the coordinates.*
(2) $\deg(\det H_F) = 3(n-2)$ *if* $\det H_F \neq 0$.
(3) $\mathrm{Sing}(C) \subset H(C)$, *where* $\mathrm{Sing}(C)$ *denotes the set of singular points of* $C$.

The following theorem shows that the significance of the Hessian curve.

**THEOREM 3.4.** *Let $C = V(F) \subset \boldsymbol{P}^2$ be a curve that contains no lines. Then*
(1) $\det H_F \neq \emptyset$;
(2) *a smooth point $p \in C$ is an inflection point if and only if $p \in H(C)$*;
(3) *$C$ and $H(C)$ have no common component*;

(4) *if $p \in C$ is a simple inflection point, then*

$$(C.H(C))_p = 1,$$

*where $(C.H(C))_p$ denotes the intersection multiplicity of $C$ and $H(C)$ at $p$.*

Let $C \subset \boldsymbol{P}^2$ be an algebraic curve, and $S$ a Riemann surface. Then a mapping

$$\varphi : S \longrightarrow C$$

is said to be *holomorphic* if it is holomorphic as a mapping to $\boldsymbol{P}^2$. With these preliminaries out of the way, we can state the theorem.

**THEOREM 3.5.** *For every irreducible algebraic curve $C \subset \boldsymbol{P}^2$, there exists a compact Riemann surface $S$ and a holomorphic mapping $\varphi : S \longrightarrow C$ with the following properties:*

(i) *Let $C' = C - \mathrm{Sing}(C)$ be the smooth part of $C$, and let $S' = \varphi^{-1}(C') \subset S$. Then*

$$\varphi | S' : S' \longrightarrow C'$$

*is biholomorphic.*

(ii) *For every point $p \in C$ there is a bijection mapping*

$$\varphi^{-1}(p) \longrightarrow \{\textit{branches of } C \textit{ at } p\}.$$

*In particular, $\varphi^{-1}(p)$ is finite for every $p \in C$.*

For any irreducible algebraic curve $C \subset \boldsymbol{P}^2$, we define the genus of $C$ as the genus of $S$.

## 3.2. **Dual Curves.**

**DEFINITION 3.8.** Let $C \subset \boldsymbol{P}^2$ be an algebraic curve. Then

$$C^* = \{L \in (\boldsymbol{P}^2)^* \mid L \textit{ is a tangent line of } C \textit{ at some } p \in C\}$$

is called the *dual curve* of $C$.

By the definition, the condition on $L$ means that $\mathrm{ord}_p(C) < (C.L)_p$. For each point $p \in C$ there are only finitely many such lines. If $C$ itself is a line, then $C^*$ consists of a single point.

**THEOREM 3.6.** *Let $C \subset \boldsymbol{P}^2$ be an algebraic curve that has no lines as components. Then*

(1) *$C^* \subset (\boldsymbol{P}^2)^*$ is an algebraic curve;*
(2) *if $C$ is irreducible then $C^*$ is irreducible and $\deg C^* \geqq 2$;*
(3) *$C^{**} = C$.*

Example. Let $C \subset \boldsymbol{P}^2$ be a smooth quadric and $p = (c^0, c^1, c^2)$ be a point of $C$. $C$ has a corresponding symmetric matrix $A = (a_{jk}) \in \mathrm{GL}(3, \boldsymbol{C})$. Denoting by $(X^0, X^1, X^2)$ the homogeneous coordinates on $\boldsymbol{P}^2$,

$$F(X) = \sum_{j,k=0}^{2} a_{jk} X^j X^k$$

is a minimal polynomial of $C$. Since

$$\frac{\partial F(X)}{\partial X^j} = 2 \sum_{k=0}^{2} a_{jk} X^k,$$

the coordinates of $T_p(C)$ in $(\boldsymbol{P}^2)^*$ are given by

$$\left( \sum_{j=0}^{2} a_{j0} c^j, \sum_{j=0}^{2} a_{j1} c^j, \sum_{j=0}^{2} a_{j2} c^j \right).$$

Consider the map $\sigma$ of $\boldsymbol{P}^2$ into $(\boldsymbol{P}^2)^*$ defined by

$$\sigma : x = (x^0, x^1, x^2) \longrightarrow y = (y_0, y_1, y_2) = \sigma(x) = \left( \sum_{k=0}^{2} a_{0k} x^k, \sum_{k=0}^{2} a_{1k} x^k, \sum_{k=0}^{2} a_{2k} x^k \right).$$

Then we obtain $\sigma(C) = C^*$. Hence $y \in C^*$ if and only if $x \in C$, provided that $y_j = \sum_{k=0}^{2} a_{jk} x^k, j = 0, 1, 2$. We set $A^{-1} = \left(a^{jk}\right)$ and if $y_j = \sum_{k=0}^{2} a_{jk} x^k, j = 0, 1, 2$, then the computation

$$\begin{aligned} \sum_{j,k=0}^{2} a^{jk} y_j y_k &= \sum_{j,k=0}^{2} a^{jk} \left( \sum_{\alpha=0}^{2} a_{j\alpha} x^\alpha \right) \left( \sum_{\beta=0}^{2} a_{k\beta} x^\beta \right) \\ &= \sum_{k,\alpha,\beta=0}^{2} \delta^k_\alpha a_{k\beta} x^\alpha x^\beta \\ &= \sum_{\alpha,\beta=0}^{2} a_{\alpha\beta} x^\alpha x^\beta \end{aligned}$$

shows that the condition $x \in C$ can be rewritten in the form

$$\sum_{j,k=0}^{2} a^{jk} y_j y_k = 0.$$

Therefore, $C^*$ is the quadric described by $A^{-1}$.

## 4. MAIN RESULTS

# Galois group at each point for some self-dual curves

HIROYUKI HAYASHI AND HISAO YOSHIHARA

ABSTRACT. 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.

4.1. **Introduction.** This is a continuation of [M], [Y2, Y3, Y4] and etc. 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. [S]). In this article 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 $P_1 = (0 : 0 : 1),\ P_2 = (0 : 1 : 0),\ P_3 = (1 : 0 : 0)$. Let $F(X, Y, Z)$ be the defining equation of $C$ and put $f(x, y) = F(X, Y, Z)/Z^d$ where $x = X/Z,\ y = Y/Z$.

4.1.1. *Galois group.* Let $r : \widetilde{C} \longrightarrow C$ 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 $\pi_P$ by

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

where $\widehat{\ell_{PR}}$ is the point in $\widehat{\mathbb{P}^2}$ 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 ${\pi_P}^* : k(\mathbb{P}^1) \hookrightarrow K = k(\widetilde{C})$, 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 $K_P$, i.e., 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 $\pi_P : \widetilde{C} \longrightarrow \mathbb{P}^1$ [C, H].

4.1.2. *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 $\mu : B_Q(\mathbb{P}^2) \longrightarrow \mathbb{P}^2$ 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. [Y1]).

**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 $Y^eZ^{d-e} = X^d,\ \gcd(e,d) = 1,\ 1 \le e \le d-1$
(II) $C_{(4)}$ : the curve defined by $(YZ - X^2)^2 = X^3Y$ (cf. [I-U-N])
(III) $C_{54}$ : the curve defined by $(XY - XZ + YZ)^3 + 54X^2Y^2Z^2 = 0$ (cf. [O])

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 [I-U-N, O].

**Remark 1.** Let $\Phi_C$ be the rational map $\mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ giving the dual of $C$, i.e.,

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

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

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

We use the following notation:

- $Z_m$ : the cyclic group of order $m$
- $S_d$ : the symmetric group of degree $d$
- $i(X_1, X_2\,; Q)$ : the intersection number of two curves $X_1$ and $X_2$ at $Q$
- $\ell_{PQ}$ : the line passing through $P$ and $Q$, $\quad P \neq Q$
- $\ell_P$ : a line passing through $P$
- $T_Q = T_Q(C)$ : the tangent line to $C$ at $Q$

4.2. **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 $f : X_1 \longrightarrow X_2$ a surjective morphism, which we call a covering for short. We denote by $e(R, f)$ be 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 6.** Let $f : X_1 \longrightarrow X_2$ be the covering above. If there exists a curve $X_3$ and coverings $\alpha : X_1 \longrightarrow X_3$ and $\beta : X_3 \longrightarrow X_2$ 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. [P-S]).

**Definition 7.** Let $f : X_1 \longrightarrow X_2$ be the covering above and $R_1, \ldots, R_r$ all the ramification points for $f$. Put $e(R_i) = e_i$ $(1 \leq i \leq r)$. 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 $f(R_i)$ $(1 \leq i \leq r)$.

**Definition 8.** With the same notation as in Definition 7 we call $\{(R_1, \ldots, R_r),\ (e_1, \ldots, e_r)\}$ (or, simply $(e_1, \ldots, e_r)$) the ramification data for $f$.

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

**Proposition 9.** *Let $f : X_1 \longrightarrow X_2$ be the covering above and $n = \deg f$. If one of the following conditions are satisfied, then $f$ is indecomposable.*

(1) *For some $i$ $(1 \leq i \leq r)$, $e_i$ 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 $i \geq s + 1$, where $f^{-1}f(R_1) = \{R_1, \ldots, R_s\}$.*

**Proposition 10.** *With the same notation as in Proposition 9, if $f$ is an s-covering and satisfies one of the following conditions, then $f$ is indecomposable.*

(1) *$X_1$ is a rational curve, $e_1 \geq e_2$, $n - 1 \geq e_2$ and $e_i$ is prime for each $i \geq 3$.*
(2) *$X_1$ is a rational curve and $e_i$ is prime for each $i \geq 2$.*
(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 $\{x_1, \ldots, x_n\}$ $(n = n(P))$ 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 $\{x_1, \ldots, x_n\}$ is a maximal subgroup of $S_n$.

**Theorem 11.** *The group $G_P$ is primitive if and only if $\pi_P$ is indecomposable. In particular, if $n(P)$ is a prime number, then $G_P$ is primitive for $P \in \mathbb{P}^2$.*

**Definition 12.** 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:

(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 $\ell$ have normal crossings except at $Q$.

Sometimes we call $\ell$ a simple $e$-tangent for short.

Note that a simple $e$-tangent $\ell_{PQ}$ yields an s-covering over $\pi_P(Q)$.

**Lemma 13.** *We have the following assertions for $G_P$.*

(1) *If each line $\ell_P$ 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. [S, Lemma 4.4.4]).*
(2) *If there exists a simple 2-tangent line $\ell_P$, then $G_P$ contains a transposition.*

The following lemma is well-known.

**Lemma 14.** *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 15.** *If the covering $\pi_P : \widetilde{C} \longrightarrow \mathbb{P}^1$ is one of the coverings in Propositions 9 or 10 and $\pi_P$ 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 $\ell_P$ has normal crossings with $C$ or is a simple 2-tangent, then $G_P$ is a full symmetric group.*

Corollary 15 implies [Y2, Theorem 1 and 1′]. Now we can state the structure of $G_P$ as follows:

**Theorem 16.** *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 $C = C_{(e,d)}$*

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

(II) *the case $C = C_{(4)}$*

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

(III) *the case $C = C_{54}$*

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

**Remark 2.** For the curves in Theorem 16, $P$ 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 [Y3].

4.3. **Proofs.** First we prove Propositions 9 and 10.

**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 $\beta : X_3 \longrightarrow X_2$, then $\beta$ is unramified at $R' = \alpha(R)$.*

*Proof.* Suppose $\beta$ 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 $\alpha$. Then, there will appear another ramification point for $f$ in $f^{-1}(f(R))$. This is a contradiction. □

The proof of Proposition 9 is as follows. Suppose $f$ is decomposable and there exists a covering $\beta : X_3 \longrightarrow X_2$ as in Definition 6. First we prove the assertion (1). Since $e_i$ is prime, $\beta$ 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 $\alpha$ and $\beta$ 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, $B_i$ $(i \geq s+1)$ is not a branch point for $\beta$. Thus $B_1$ is the only branch point for $\beta$. 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 $\beta$ and $c \leq b-1$. Since $g(X_3) \geq 0$, this inequality implies $b \leq 1$, which is a contradiction.

Next we prove Proposition 10. In each case we use the reduction to absurdity, i.e., suppose $f$ is decomposable. So we use the notation $R_i' = \alpha(R_i)$ $(1 \leq i \leq r)$. In the case (1), by Claim 1, $\beta$ is unramified at $R_i'$ $(i \geq 3)$. Since $X_2$ and $X_3$ are rational, from Hurwitz's Formula, we infer that $\beta$ 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 $R_i$ $(i = 1, 2)$, $\alpha$ 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 (2), by Claim 1, $\beta$ 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 (3) similarly, by Claim 1, $\beta$ is unramified at every point $R_i'$, however, since $X_2$ is rational, $\beta$ must be an identity, which is a contradiction. This completes the proof of Proposition 10.

The proof of Theorem 11 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 $\alpha : \widetilde{C} \longrightarrow C_H$ and $\beta : C_H \longrightarrow \mathbb{P}^1$ such that $\pi_P = \beta\alpha$. Thus $\pi_P$ is decomposable. The converse assertion is clear from the Galois corresponding.

The proof of Lemma 13 is simple. In view of Definition 12 we see that the assertion (1) is another expression of (3) in Proposition 10. The assertion (2) may be well-known (cf. [H]).

Now we proceed to the proof of Theorem 16. 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 16. Since $C$ is a self-dual curve and has only cusps as the singularity, the following remark is clear.

**Remark 3.** 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. [F]), 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 $C$, i.e., 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 sub-case $1 < e < d-1$. 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 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 10 and Lemma 14, we have $G_P \cong S_{d-1}$. Next we prove the sub-case $e = 1$. 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 has normal crossings with $C$ or it is a simple 2-tangent line to $C$. By (2) in Proposition 10 and Lemma 14, 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 $\pi_P$ 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 $\pi_P$ 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 9, $\pi_P$ is indecomposable. Since there exists a simple 2-tangent $\ell_P$, we conclude $G_P \cong S_d$. In case $P \in \ell_{P_1P_2}$ 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 9, $G_P$ is primitive and there exists a simple 2-tangent line $\ell_P$, thus we conclude $G_P \cong S_d$. In view of Remark 3 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, i.e., $i(C, T_F; F) = 3$ 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 4.** The coordinates of the flex $F$ is 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 $\pi_P$ 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 $\ell_{P_1P_2} \cap T_F = \{P\}$. We infer from Hurwitz's Formula that the ramification data is $(3, 2^4) := (3, 2, 2, 2, 2)$. By

(3) in Proposition 9 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 Proposition 9 or 10 we conclude $G_P \cong S_4$.

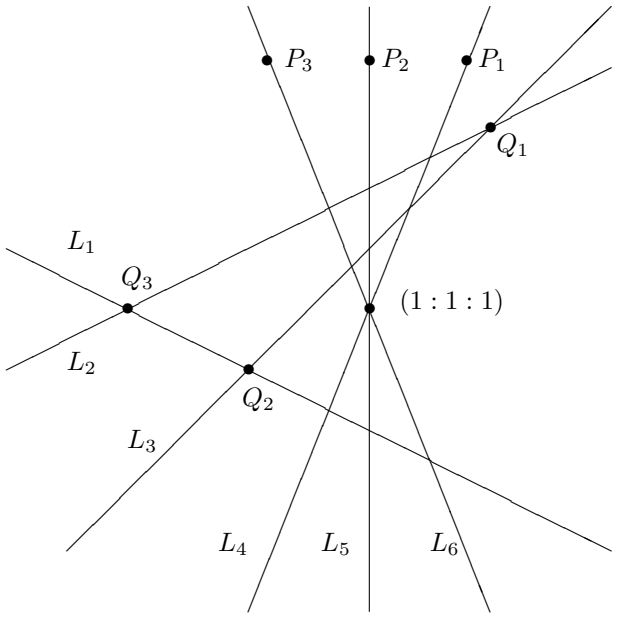
Proof of the case (III)

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

**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 line 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 $\ell$ 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 $P \in \mathbb{P}^2 \setminus (C \cup \{Q_1, Q_2, Q_3\})$, 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 [O] 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 $\pi_P$, 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 $G_{P_i} \cong S_3$ $(i = 2, 3)$.

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 $L_6$. 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 $\pi_P$ is an s-covering, then $\pi_P$ is indecomposable.*

*Proof.* By Claim 5 the ramification index is $2,\ 3$ or $4$. Suppose $\pi_P$ is decomposable. Then, $\deg \beta = 2$ or 3. By Claim 1 $\beta$ 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 9, $\beta$ 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 10. 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 $(4^3, 2^3) := (4, 4, 4, 2, 2, 2)$. If $\deg \beta = 2$, then $\beta$ 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 that easily that $\beta$ is ramified at $R'_i$ with $e(R'_i, \beta) = 2$ $(i = 1, 2, 3)$. However, this does not satisfy Hurwitz's Formula. Therefore $\pi_P$ is indecomposable. □

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 polynomialis $S_6$. 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 proof 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 $\pi_P$ 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 $\pi_P$ is decomposable. Then, by Claim 1, $\beta : X_3 \longrightarrow \mathbb{P}^1$ is unramified at $\alpha(P_3)$ 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 9, $\pi_P$ is indecomposable. Since there exists a simple 2-tangent, we have $G_P \cong S_6$.

Thus we complete all the proofs.

**Remark 5.** In the list of Theorem 16 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. [M-Y]).

**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 reviewers for carefully reading the manuscript and giving the suitable suggestions for improvements.

## REFERENCES OF SECTION 4

[C ] F. Cukierman, Monodromy of projections, *Mat. Contemp.*, **16** 15th School of Algebra (Portuguese) (1999), 9–30.

[F ] W. Fulton, Algebraic Curves, *Math. Lecture Note Series*, Benjamin, New York (1969).

[H ] J. Harris, Galois groups of enumerative problems, *Duke Math. J.*, **46** (1979), 685–724.

[I-U-N ] S. Iitaka, K. Ueno and Y. Namikawa, Descartes no Seishin to Daisûkika, *Nippon Hyoron Sha*, 1980 (in Japanese).

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

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

[O ] M. Oka, Elliptic curves from sextics, *J. Math. Soc. Japan*, **54** (2002), 349–371.

[P-S] G.-P. Pirola and E. Schlesinger, Monodromy of projective curves, *J. Algebraic Geometry*, **14** (2005), 623–642.

[S] J.-P. Serre, Topics in Galois Theory, *Res. Notes in Math.*, Jones & Bartlett (1992).

[Y1] H. Yoshihara, An application of Plüker's relations (in Japanese), *Sugaku*, **32** (1980), 367–369.

[Y2] ———, Function field theory of plane curves by dual curves, *J. Algebra*, **239** (2001), 340–355.

[Y3] ———, Galois points for plane rational curves, *Far east J. Math.*, **25** (2007), 273–284

[Y4] ———, Rational curve with Galois point and extendable Galois automorphism, *J. Algebra*, **321** (2009), 1463–1472.

## REFERENCES

[1] M. Field, Several Complex Variables and Complex Manifolds I. Cambridge University Press, 1982.
[2] G. Fischer, Plane Algebraic Curves. American Mathematical Society, 2001.
[3] O. Forster, Lectures on Riemann Surfaces. Springer-Verlag, 1981.
[4] K. Fritzsche and H. Grauert, From Holomorphic Functions to Complex Manifolds. Springer-Verlag, 2002.
[5] P. Griffiths, Introduction to Algebraic Curves. Princeton University Press, 1989.
[6] H. Hayashi and H. Yoshihara, Galois Group at Each Point for Some Self-Dual Curves. Hindawai Publishig Corporation, Geometry, vol. 2013 (2013), pp. 1-6.
[7] L. Kaup and B. Kaup, Holomorphic Functions of Several Variables. Walter de Gruyter, 1983.
[8] F. Kirwan, Complex Algebraic Curves. Cambridge University Press, 1992.
[9] R. Miranda, Algebraic Curves and Riemann Surfaces. American Mathematical Society, 1995.
[10] M. Namba, GEOMETRY OF PROJECTIVE ALGEBRAIC CURVES. MARCEL DEKKER, INC., 1984.
[11] R. Walker, Algebraic Curves. Springer-Verlag, 1978.
[12] H. Whitney, COMPLEX ANALYTIC VARIETIES. Addison-Wesley Publishing Company, 1972.