GALOIS POINTS FOR SMOOTH HYPERSURFACES

Hisao Yoshihara

Department of Mathematics, Faculty of Science, Niigata University, Niigata 950-2181, Japan

E-mail:yosihara@math.sc.niigata-u.ac.jp

Abstract. Let V be a smooth hypersurface in $\mathbb{P}^{n+1}$. We consider a projection of V from $P \in \mathbb{P}^{n+1}$ to a hyperplane H. This projection induces an extension of fields $k(V)/k(H)$, which does not depend on the choice of H. We study the structures of this extension and the hypersurfaces together. The point P is called a Galois point if the extension is Galois. We show estimates of the number of the Galois points and some rules of their distributions. Especially we give the defining equation of V with maximal number of Galois points.

Key words: hypersurface; Galois group; Galois point.

1. Introduction

Let k be the field of complex numbers. We fix it as the ground field of our discussions. Let V be a smooth hypersurface of degree d in the projective $(n+1)$-space $\mathbb{P}^{n+1}$ and $K = k(V)$ the function field of V. Let P be a point in $\mathbb{P}^{n+1}$ and $\pi_P : V \cdots \to H$ a projection with center P, where H is a hyperplane not containing P. When we do not mention otherwise, we always assume that $d \geq 4$. Then we have an extension of function fields $\pi_P{}^* : k(H) \hookrightarrow K$. It is not difficult to see that the structure of this extension does not depend on the choice of H but on the point P. So that we use the notation K_P instead of $k(H)$. Clearly we have $[K : K_P] = d - 1$ [resp. d] if $P \in V$ [resp. $P \notin V$].

Definition 1. The point $P \in \mathbb{P}^{n+1}$ is called a Galois point for V if the extension K/K_P is Galois. If, moreover, $P \in V$ [resp. $P \notin V$], then we call P an inner [resp. outer] Galois point. We denote by $\delta(V)$ [resp. $\delta(V^c)$] the number of inner [resp. outer] Galois points.

If $P \notin V$, then π_P is a finite morphism, however if $P \in V$ and $n \geq 2$, then it is not even a morphism. The restriction $\pi'_P := \pi_P|_{V \setminus P}$:

$V \setminus P \longrightarrow H$ becomes a morphism. Let L be the union of linear varieties contained in V and passing through P. Then, $\pi''_P := \pi_P|_{V \setminus L} : V \setminus L \longrightarrow H \setminus L$ becomes a quasi-finite morphism.

By Lemma 1 in Section 2, we can say that a point $P \in V$ [resp. P $\notin V$] is a Galois point if and only if π''_P [resp. π_P] is a Galois covering in the sense of Namba [8].

Definition 2. We denote by L_P the Galois closure of K/K_P and put $G_P = \mathrm{Gal}(L_P/K_P)$. We call it a Galois group at P.

We study the extension K/K_P from geometrical points of view, especially we consider the following problems:

(A) *Find all the Galois points. Do there exist any rules for the distribution of the points* (*like quartic surfaces* [13]) ?
(B) *Find the structure of the Galois group G_P at each point $P \in \mathbb{P}^{n+1}$.*
(C) *Find the structure of a nonsingular projective model of L_P.*

We have studied these problems in detail when $n = 1$ (see, [7] and [12]) and $n = 2, d = 4$ (see, [10] and [13]). Note that the definitions and assertions above do not depend on projective changes of coordinates. We will consider several objects up to projective equivalence.

Remark 1. For the motivation of our research, see [12].

Remark 2. In the case where $n = 1$, the field K_P is always a maximal rational subfield of K. Similarly in the case where $n = 2$, it is maximal rational except the case where $d = 4$, $P \notin V$ and P is a Galois point. In fact, if $d \geq 5$ or $d = 4$ and $P \in V$, then K_P is maximal rational by [1] and [11].

We use the following notation and convention throughout this paper:

- $(X_0, \ldots, X_{n+1})$: homogeneous coordinates on $\mathbb{P}^{n+1}$
- $F(X_0, \ldots, X_{n+1}) = 0$: the defining equation of V
- $\mathfrak{S}_n$: the symmetric group on n letters
- $\mathrm{e}_n := \exp(2\pi\sqrt{-1}/n)$
- $F(n, d)$: the Fermat variety of degree d, which is defined by $X_0^d + X_1^d + \cdots + X_{n+1}^d = 0$
- $\sigma[Y]$: the proper transform of Y by a birational map σ
- $i(Y, Z; P)$: the intersection number of Y and Z at P
- Let M_i be square matrices of size m_i $(1 \leq i \leq r)$ and

$$M = \begin{pmatrix} M_1 & & & & \mathbf{0} \\ & M_2 & & & \\ & & \ddots & & \\ & & & \ddots & \\ \mathbf{0} & & & & M_r \end{pmatrix}.$$

Then we denote M by $M_1 \oplus M_2 \oplus \cdots \oplus M_r$.

- $diag[\alpha_1, \cdots, \alpha_n]$: the diagonal matrix $(\alpha_1) \oplus \cdots \oplus (\alpha_n)$
- l_{PQ} : the line passing through two points P and Q

2. Statement of results

Suppose that P is a Galois point. Then $\sigma \in \mathrm{Gal}(K/K_P)$ induces a birational transformation of V over H, we denote it by the same letter σ.

Lemma 1. *The transformation σ becomes an automorphism of V, in fact it turns out to be a restriction of a projective transformation $M(\sigma) \in PGL(n+1, k)$. Hence we have a representation of G_P in $PGL(n+1, k)$.*

When there is no fear of confusion, we will use the notation σ instead of $M(\sigma)$. We will show that $\sigma(P) = P$ and $\sigma(l) = l$ for any line l passing through P. From Lemma 1 we infer the following.

Theorem 1. *If V is general in the class of hypersurfaces with $d \geq 4$, then it has no Galois point.*

Next we consider G_P for a given hypersurface V. If P is a general point among the ones for $P \in V$ [resp. $P \notin V$], then we will show that $G_P \cong \mathfrak{S}_{d-1}$ [resp. $\mathfrak{S}_d$]. We now state this fact in more definite form.

Let $\mu : \widetilde{V} \longrightarrow V$ be a blowing-up of V at P. Then $\widetilde{\pi} := \pi_P \cdot \mu$ becomes a morphism $\widetilde{V} \longrightarrow H$. Let Δ_P be the discriminant divisor of this covering $\widetilde{\pi}$. Δ_P is a divisor in H and is defined locally as follows: we can take homogeneous coordinates on $\mathbb{P}^{n+1}$ satisfying the following conditions (1), (2) and (3):

(1) $P = (1, 0, \ldots, 0)$.
(2) The hyperplane $X_1 = 0$ is not tangent to V at any points.
(3) For each irreducible component W of $\{X_0 = 0\} \cap V$, there exists a point $Q \in W$ satisfying that the line l_{PQ} does not touch V at Q.

Under these conditions we put $x_i = X_i/X_0$ $(i = 1, \dots, n+1)$ and $f(x_1, \dots, x_{n+1}) = F(X_0, X_1, \dots, X_{n+1})/X_0^d$.

Moreover, we put $x = x_1$, $x_i = t_{i-1}x_1$ $(i = 2, \dots, n+1)$ and

$$f^\star(t_1, \dots, t_n, x) = \begin{cases} f(x, xt_1, \dots, xt_n)/x & \text{if } P \in V \\ f(x, xt_1, \dots, xt_n) & \text{if } P \notin V. \end{cases}$$

Note that $f^\star = 0$ is the defining equation of the affine part of the blowing-up of V at P. The affine part of Δ_P is the divisor defined by the discriminant of $f^\star$ with respect to x.

Theorem 2. *Suppose that each component of Δ_P is reduced. Then $G_P \cong \mathfrak{S}_{d-1}$ [resp. $\mathfrak{S}_d$] if $P \in V$ [resp. $P \notin V$].*

As an application we have the following.

Theorem 3. *There exists a divisor $D \subset \mathbb{P}^{n+1}$ satisfying the following conditions*:

(1) *If $P \in V \setminus D$, then $G_P \cong \mathfrak{S}_{d-1}$.*

(2) *If $P \in \mathbb{P}^{n+1} \setminus (V \cup D)$, then $G_P \cong \mathfrak{S}_d$.*

We obtain the following readily.

Corollary 4. *If P is a general point, then there exists no field between K and K_P.*

Note that, in the case where $n = 1$, we have that $\deg D \le d(d-1)(d^2-3)/2$ (cf. [12]). It seems interesting to study the structure of G_P when P belongs to D. We have also an interest to find the structure of a nonsingular projective model of L_P. For lower dimensional cases we have some results, see [7], [10] and [12].

Next, we investigate several structures in the most special case, i.e., the case of Galois points.

Theorem 5. *If P is a Galois point, then G_P is a cyclic group of order $d-1$ [resp. d] for $P \in V$ [resp. $P \notin V$].*

From this theorem we infer the following useful corollary.

Corollary 6. *If $P = (1, 0, \dots, 0)$ is an inner [resp.outer] Galois point, then the defining equation of V can be given by $F = X_1X_0^{d-1} + G = 0$ [resp. $X_0^d + G = 0$], where G is a form of degree d in $k[X_1, \dots, X_{n+1}]$.*

To find inner Galois points we can use the folllowing.

Corollary 7. *Let $H(F)$ be the Hessian of F. If P is an inner Galois point, then $H(F)(P) = 0$*

Definition 3. For a Galois point P an automorphism induced from an element of G_P is said to be an automorphism associated with P.

Assumption. *When we consider several Galois points at the same time, we assume that all of them are inner or outer simultaneously.*

Here we present a simple but useful lemma.

Lemma 2. *If P and Q are distinct Galois points, and σ and τ are generators of G_P and G_Q respectively. Then $\sigma(Q)$ and $\tau(P)$ are also Galois points. If, moreover, there exists no other Galois points on the line l_{PQ}, then σ and τ commute in $PGL(n+1,k)$.*

Note 8. *Under the assumption of Lemma 2, suppose that $\sigma|_l$ is not identity, where $l = l_{PQ}$. Then Q is the only other fixed point of the automorphism $\sigma|_l$ on l.*

Now, we study the cardinality of Galois points.

Definition 4. A set of Galois points $\{P_0, \dots, P_r\}$ is said to be independent, if for any two points P_i and P_j $(0 \le i, j \le r)$ all the Galois points for V lying on $l_{P_iP_j}$ are just P_i and P_j.

Lemma 3. *If $P_0, \dots, P_r$ are independent Galois points, then we can choose coordinates $(X_0, \dots, X_{n+1})$ satisfying that $X_j(P_i) = \delta_{ji}$ $(0 \le i \le r,\ 0 \le j \le n+1)$ and a generator σ_i of G_{P_i} $(0 \le i \le r)$ has a representation as diag$[\zeta, \cdots, \zeta, 1, \zeta, \cdots, \zeta]$, where 1 is in i-th position and $\zeta = \mathrm{e}_{d-1}$ [resp. e_d]. Especially we have $r \le n+1$, i.e., the cardinality of a set of independent Galois points is at most $n+2$.*

First we consider inner Galois points in detail. Hereafter we denote by $m = [n/2]$ the integral part of $n/2$.

Lemma 4. *The cardinality of a set of independent inner Galois points is at most $m+1$.*

Theorem 9. *We have the following assertions for inner Galois points.*

(1) *If $d = 4$, then we have $\delta(V) \le 4(m+1)$. The equality holds true if and only if V is projectively equivalent to the hypersurface defined by the equation*

$$F = X_{m+1}X_0^3 + \cdots + X_{2m+1}X_m^3 + X_{m+1}^4 + \cdots + X_{n+1}^4 = 0.$$

(2) *If $d \ge 5$, then the set of Galois points is independent, hence we have $\delta(V) \le m+1$. The equality holds true if and only if V is projectively equivalent to the hypersurface defined by the equation*

$$F = X_{m+1}{X_0}^{d-1} + \cdots + X_{2m+1}{X_m}^{d-1} + G = 0,$$

where G is a form in $k[X_{m+1}, \dots, X_{n+1}]$ and has $\deg G = d$.

On the other hand, for outer Galois points, we have the following simple assertion.

Theorem 10. *We have $\delta(V^c) \le n+2$. The equality holds true if and only if V is projectively equivalent to the Fermat variety $F(n,d)$.*

For a more detailed result, see Proposition 11 in Section 3. We have a characterization of a Fermat variety, i.e., "a smooth hypersurface V is a Fermat variety if and only if it has the maximal number of outer Galois points."

Remark 3. In the case where V is not smooth, the assertions of Lemma 1 and Theorem 5 do not hold true. In fact, we have the following example.

Let W be the hypersurface defined by

$$X_{n+1}(X_1^2+\cdots+X_{n+1}^2)^d+(X_1^{d+1}+\cdots+X_{n+1}^{d+1})X_0^d+X_{n+1}X_0^{2d}=0.$$

Then $Q=(1:0:\cdots:0)\in W$ is a Galois point and the Galois group at Q is isomorphic to the dihedral group of order $2d$. Indeed, let σ be a quadratic transformation of $\mathbb{P}^{n+1}$ defined by

$$\sigma(X_0,X_1,\ldots,X_{n+1})=(X_1^2+\cdots+X_{n+1}^2, X_0X_1,\ldots,X_0X_{n+1}),$$

and let τ be a projective transformation of $\mathbb{P}^{n+1}$ defined by

$$\tau(X_0,X_1,\ldots,X_{n+1})=(\mathrm{e}_dX_0,X_1,\ldots,X_{n+1}).$$

Then $\sigma^2=\tau^d=1$ and $\sigma\tau\sigma=\tau^{-1}$. Clearly σ and τ induce birational transformations on W, and G_Q is generated by σ and τ. For Galois points on singular varieties, we have only a few results (cf. [6]).

Finally we raise problems.

Problem. (I) Find the Galois group at $P\in D$ and the distribution rule of the points P satisfying that $G_P\cong G$ for a given finite group G.

(II) Study the problems (A), (B) and (C) in Introduction when V has singularities.

(III) Let V and L be an n-dimensional subvariety and an $(N-n-1)$-dimensional linear subvariety of $\mathbb{P}^N$ respectively. Consider a projection $\pi_L:\mathbb{P}^N\cdots\to L_0$ with center L satisfying that $\pi_L|_V: V\cdots\to L_0$ is dominant, where L_0 is an n-dimensional lienar subvariety $L\cap L_0=\emptyset$. Then, study the extension $k(V)/k(L_0)$ similarly as above (cf. [14]).

3. Proofs and some other results

First we prove Lemma 1. In the case where $\dim V=1$, the proof is standard (cf. [12]), so we prove when $\dim V\ge 2$. Let $Q(\ne P)$ be a point in V and $l=l_{PQ}$ be the line passing through P and Q.

Lemma 5. *If l meets V at d distinct points, then σ is regular at Q and $\sigma(Q)$ is one of the points in $l \cap V$.*

Proof. Blow up P. Then we get a morphism $\widetilde{\pi} : \widetilde{V} \longrightarrow V$, where $\widetilde{V}$ is the blowing up at P. So, $\widetilde{V} = V$ if $P \notin V$. Then $\widetilde{\pi}$ is a finite morphism near $\widetilde{\pi}(Q)$ by the hypothesis (actually the line l is not completely contained in V is enough for this). Since $\sigma \in Gal(K/K_P)$, we see that σ induces a birational map from $\widetilde{V}$ to $\widetilde{V}$ over H. But, since $\widetilde{\pi}$ is finite near $\widetilde{\pi}(Q)$ and $\widetilde{V}$ is smooth (normal is enough), by elementary algebra, we see that σ is a morphism (necessarily an isomorphism) from a suitable open set of the form $\widetilde{\pi}^{-1}(U)$ containing Q. □

Let U_Q be a small neighbourhood of Q. Then $Z_Q = U_Q \cap \pi_P^{-1}(\Delta_P)$ is a set of zero points of some holomorphic function in U_Q, where Δ_P is the discriminant. Let $\sigma = (\sigma_1, \dots, \sigma_n)$ be an expression of σ on U_Q. Then each σ_i is regular and bounded on $U_Q \setminus Z_Q$ by Lemma 5. Then, by Riemann's Extension Theorem ([2, p. 9]), σ is regular at Q. Thus σ is regular in $V \setminus \{P\}$. Then, by Hartogs' Theorem (cf. [2, p. 7]), we see that σ is regular at P. Hence it becomes an automorphism of V. By the definition of σ it preserves hyperplane sections passing through P, i.e., letting H be a hyperplane passing through P and $V' = H \cdot V$, which is the intersection divisor on V, then by definition we have $\sigma(V') = V'$. Since $\mathrm{H}^0(\mathbb{P}^{n+1}, \mathcal{O}(H)) \cong \mathrm{H}^0(V, \mathcal{O}(V'))$, σ is a restriction of a projective transformation.

Now the proof of Theorem 1 is simple. If P is a Galois point, then there exists a monomorphism $G_P \hookrightarrow \mathrm{Aut}(V)$ by Lemma 1. It may be well known that $\mathrm{Aut}(V)$ ={id} if V is general and $d \geq 4$ (cf. [5]). Hence the assertion is clear.

We prove Theorem 2 by induction on the dimension of V. In the case where $n = 1$, the assertion holds true by [12]. We assume that $n \geq 2$.

We can take a hyperplane H_P satisfying the following conditions (i), (ii) and (iii):

(i) H_P passes through P.

(ii) The intersection of H_P and Δ_P is reduced.

(iii) $V' := V \cap H_P$ is irreducible and smooth.

Then V' is a smooth hypersurface of H_P. Put $\pi' := \pi_P|_{V'} : V' \cdots \rightarrow H' := H \cap H_P$. Let $\mu : \widetilde{V} \longrightarrow V$ be a blowing-up of V at P. Then $\widetilde{\pi} := \pi_P \cdot \mu : \widetilde{V} \longrightarrow H$ is a morphism. Let W be a nonsingular projective model of L_P satifying that there exists a surjective morphism $\rho : W \longrightarrow \widetilde{V}$. Put $W' := \rho^{-1}(\mu^{-1}[V'])$, where $\mu^{-1}[V']$ denotes the proper transform of V'. Each element $\sigma \in G_P$ induces a birational transformation of W over H. Take an irreducible component W'_0 of W' and put

$$G'_P = \{\sigma \in G_P \mid \sigma[W'_0] = W'_0\},$$

which is a subgroup of G_P. Since $\rho^{-1}\widetilde{\pi}^{-1}(H') = W'$, we have $\sigma[W'] = W'$. Since G_P acts transitively on each fiber in an open dense subset of W', we infer that W'_0/G'_P is birational to H', i.e., for some open dense subset W_* of W'_0 each element of G'_P acts as an automorphism and W_*/G'_P is isomorphic to some dense subset of H'. Therefore $k(W'_0)$ is a Galois extension of $k(H')$. Applying the induction hypothesis to the covering $\pi' : V' \cdots \to H'$, we have that the Galois group of V' at P is the full symmetric group. Hence we infer that $\deg((\widetilde{\pi}\cdot\rho)|_{W'_0}) = (d-1)!$ [resp. $d!$]. (Especially, W'_0 is irrducible.) Hence we conclude G_P is also the full symmetric group.

Next we prove Theorem 3. Let f be the defining equation of V in the affine part $X_0 \neq 0$ as in Section 2. Put

$$g(u_1, \ldots, u_{n+1}, t_0, \ldots, t_n, x) := f(u_1 + xt_0, \ldots, u_{n+1} + xt_n),$$

where $(t_0, \ldots, t_n) \in \mathbb{P}^n$. Let $\Sigma = \Sigma(u_1, \ldots, u_{n+1}, t_0, \ldots, t_n)$ be the discriminant of g with respect to x. Consider a hyperplane H_Q of $\mathbb{P}^{n+1}_{X_0} = \mathbb{A}^{n+1}$ satisfying that H_Q passes through $Q = (u_1, \ldots, u_{n+1})$ and $V \cap H_Q$ is smooth. Let

$$h(x_1, \ldots, x_{n+1}) = a_0 + \sum_{i=1}^{n+1} a_i x_i$$

be the defining equation of H_Q and let L_Q be the linear variety in $\mathbb{A}^{n+1} \times \mathbb{P}^n$ defined by the simultaneous equations:

$$\begin{cases} a_0 + a_1u_1 + \cdots + a_{n+1}u_{n+1} & = & 0 \\ a_1t_0 + \cdots + a_{n+1}t_n & = & 0. \end{cases}$$

Let $\bar{g}$ be the polynomial which is a restriction of g to $a_0 + \sum_{i=1}^{n+1} a_i u_i = \sum_{j=0}^{n} a_{j+1}t_j = 0$. Let $\overline{\Sigma}$ be the discriminant of $\bar{g}$ with respect to x. Since discriminants can be given by resultants, we infer easily that $\overline{\Sigma}$ is the restriction of Σ to L_Q.

Claim 1. *Each component of* Σ *is reduced.*

Proof. We prove by induction on the dimension of V. In the case where $n = 1$, let $\mathcal{M}$ be the set of multitangent lines to the curve $C(= V)$, where the definition is as follows:

A line l is said to be a multitangent line to a plane curve C if it satisfies the following condition (1) or (2):

(1) There exists a point $P \in C \cap l$ satisfying that $i(C, l\,; P) \geq 3$.

(2) There exist at least two points $P_i \in C \cap l$ satisfying that $i(C, l\,; P_i) = 2$ for $i = 1, 2$.

Since the cardinality of $\mathcal{M}$ is finite, we infer that each component of Σ is reduced. In fact, Σ is reduced and irreducible (cf. [12]).

Let H_Q be a general hyperplane passing through $Q = (u_1, \dots, u_{n+1})$. Then $(V \cap \mathbb{A}^{n+1}) \cap H_Q$ is smooth, and by induction hypothesis $\overline{\Sigma}$ is reduced. Since H_Q is general, from the consideration before this claim we conclude that Σ is also reduced. □

Let p be the first projection $\mathbb{A}^{n+1} \times \mathbb{P}^n \longrightarrow \mathbb{A}^{n+1}$, i.e., $p(u_1, \dots, u_{n+1}, t_0, \dots, t_n) = (u_1, \dots, u_{n+1})$. Since each component of Σ is reduced, there exists a divisor D_a in $\mathbb{A}^{n+1}$ satisfying that each component of $p^{-1}(Q)$ is reduced if $Q \notin D_a$. Therefore, taking D as the divisor $\overline{D_a} \cup \{X_0 = 0\}$, where $\overline{D_a}$ is the closure of D_a in $\mathbb{P}^{n+1}$, we see the assertions of Theorem 3 hold true.

If P is a general point among the ones in V [resp. $\mathbb{P}^{n+1}$], then $G_P \cong \mathfrak{S}_{d-1}$ [resp. $\mathfrak{S}_d$]. As we have seen above, we have $K = K_P(x_0)$, where $f^\star(t_1, \dots, t_n, x_0) = 0$. Hence the group corresponding to $K = k(V)$ is the symmetric group $\mathfrak{S}_{d-2}$ [resp. $\mathfrak{S}_{d-1}$], which is primitive, hence it is a maximal subgroup of $\mathfrak{S}_{d-1}$ [resp. $\mathfrak{S}_d$].

Next we prove Theorem 5. Let P be a Galois point and let σ be any element of G_P. Take coordinates as $P = (1, 0, \dots, 0)$. By Lemma 1, σ has a projective representation, which satisfies $\sigma(P) = P$ and $\sigma(l) = l$ for each line passing through P. Hence we infer that it has a representation as

$$M(\sigma) = \begin{pmatrix} a & \overrightarrow{a} \\ \overrightarrow{0} & \lambda E_{n+1} \end{pmatrix},$$

where the entries are as follows: $a \in k^\times$, $\overrightarrow{a}$ and $\overrightarrow{0}$ are row and column vectors of size $n+1$ respectively, and E_{n+1} is a unit matrix of size $n+1$. Moreover σ^r is identity if $r = d-1$ [resp. d], hence we have $a^r = \lambda^r$. Thus we can express $\lambda = a\zeta$, where $\zeta^r = 1$. Note that, if $\zeta = 1$, then $\overrightarrow{a}$ must be a zero vector. Whence we get a homomorphism $\rho : G_P \longrightarrow k^\times$, defined by $\rho(\sigma) = \zeta$. By the note above ρ is injective, hence we conclude G_P is a cyclic group of order $d-1$ [resp. d] if $P \in V$ [resp. $P \notin V$].

Now the proof of Corollary 6 is simple. Indeed, if P is a Galois point, then by Theorem 5 we have the representation $M(\sigma) = 1 \oplus \zeta E_{n+1}$, where $\zeta = \mathrm{e}_{d-1}$ [resp. e_d]. Since F is invariant up to constants by the action of σ, the assertion is easy to see.

The proof of Corollary 7 is clear from the following lemma, which may be well known (cf. [9]).

Lemma 6. *Let f be the defining equation of an affine part of V and $\bar{f}$ be the restriction of f to the affine tangent plane of V at P. Then the Taylor expansion of $\bar{f}$ at P starts with a nondegenerate quadratic form if and only if $H(F)(P) \neq 0$.*

Let us prove Lemma 2. Put $\sigma(Q) = Q'$ and consider the projective transformation $\tau' = \sigma\tau\sigma^{-1}$. Then we have $\tau'(Q') = Q'$ and $\tau'(l') = l'$ for any line l' passing through Q'. From this we infer that Q' is a Galois point and $G_{Q'} = \langle \tau' \rangle$, and similarly so is $\tau(P)$. Let l be the line passing through P and Q, if there exists no other Galois points on l, then $\sigma(Q) = Q$ and $\tau(P) = P$. Therefore we infer that $\tau' \in G_Q$. By Theorem 5 we have that $\tau' = \tau^r$ for some $r \in \mathbb{N}$. Comparing eigenvalues of τ and τ', we obtain that $r = 1$.

We go to the proof of Lemma 3. Let σ_i be an automorphism associated with P_i. Taking a suitable coordinates, we can assume that $P_0 = (1, 0, \ldots, 0)$ and $\sigma_0 = 1 \oplus \zeta E_{n+1}$, where $\zeta = e_{d-1}$ [resp. e_d]. Since the Galois points are independent, by Lemma 2, the points P_i ($i \geq 1$) are fixed by σ_0. Thus we infer that P_i ($i \geq 1$) are in the hyperplane $X_0 = 0$. Next we take coordinates on $X_0 = 0$ satisfying that $P_1 = (0, 1, 0, \ldots, 0)$ and (i, j)-th entry of σ_1 is 0 if $i \neq j$ or $i \neq 2$. Since $\sigma_0\sigma_1 = \sigma_1\sigma_0$ by Lemma 2, we have that $(2, 1)$-th entry of σ_1 is zero. Then it is not hard to see that we can assume that $\sigma_2 = diag[\zeta, 1, \zeta, \cdots, \zeta]$. Thus $P_j (j \geq 2)$ lie in the intersection of hyperplanes $X_0 = X_1 = 0$. In this way we can take such coordinates as is stated in this lemma.

Making use of Lemma 3, we can prove Lemma 4 as follows. Suppose that $r = \delta(V) \geq m + 2$. Then take a system of coordinates $(X_0, \ldots, X_{n+1})$ satisfying that $X_j(P_i) = \delta_{ji}$, where $0 \leq i \leq m + 1$ and $0 \leq j \leq n + 1$. By Lemma 3, we can assume that σ_i is a diagonal matrix $diag[\zeta, \ldots, \zeta, 1, \zeta, \ldots, \zeta]$, where $\zeta = \mathrm{e}_{d-1}$. Since $F^{\sigma_i} = \lambda_i F$ for $\lambda_i \in k^\times$, we infer that F has the expression as

$$F = A_0 X_0^{d-1} + \cdots + A_{m+1} X_{m+1}^{d-1} + G,$$

where A_i and G are forms in $k[X_{m+2}, \ldots, X_{n+1}]$, and deg $A_i = 1$ and deg $G = d$. Putting $A_i = \sum_{j=m+2}^{n+1} a_{ij} X_j$, we consider the simultaneous equations $\partial F / \partial X_i = 0$ ($i = 0, \ldots, n + 1$). Then the following simultaneous linear equations

$$\left\{\begin{array}{ccccccc} a_{0m+2}y_0 & + & \cdots & + & a_{m+1m+2}y_{m+1} & = & 0 \\ \cdots & & \cdots & & \cdots & & \\ a_{0n+1}y_0 & + & \cdots & + & a_{m+1n+1}y_{m+1} & = & 0 \end{array}\right.$$

have non-trivial solutions. We infer from this that the hypersurface defined by $F = 0$ has a singular point, which is a contradiction. Therefore we conclude that $\delta(V) \leq m + 1$.

Before the proof of Theorem 9 we prepare several lemmas. Let l be a line in $\mathbb{P}^{n+1}$ and Λ_l be the linear system on V defined by

$$\{\ V \cdot H \mid H \text{ is a hyperplane } \supset l\},$$

where $V \cdot H$ denotes the intersection divisor on V.

Lemma 7. *A general member V_g in Λ_l is smooth and irreducible if one of the following conditions is satisfied*:

(1) $\dim V \geq 2$ *and* $l \not\subset V$
(2) $\dim V \geq 3$

Proof. By Bertini's Theorem (cf. [3, pp. 274–275]), general member of Λ_l is irreducible and smooth except at the points in $l \cap V$. In the case (1), $l \cap V$ consists of finitely many points. Since (projective) $\dim \Lambda_l \geq 1$, we can find in general members an element given by a hyperplane not tangent to at any points in $l \cap V$. Hence we can take a smooth irreducible member. In the case (2), we have $\dim(l \cap V) \leq 1$ and $\dim \Lambda_l \geq 2$. By the same reasoning as above, we have the same conclusion. □

Claim 2. *Suppose that $d = 4$. Then the following assertions holds true*:

(1) *If a line l is contained in V, then the number of Galois points on l is at most two.*

(2) *If a line l is not contained in V, then the number of Galois points on $V \cap l$ is zero, one or four.*

Proof. We prove by induction on n. If $n = 1$ or $n = 2$, then the assertions hold true by [12] and [13]. Suppose that $n \geq 3$. Then, consider the linear system Λ_l given by the hyperplanes as above. By Lemma 7 a general member V_g is irreducible and smooth. Since the Galois points for V become the ones for V_g, the assertion is true by induction hypothesis. □

Here we state two lemmas from plane curve theory. Let Γ be an irreducible (possibly singular) plane curve of degree d and Γ_0 be the smooth part. Put

$$W(\Gamma) = \sum_{P \in \Gamma_0} \{i(\Gamma, T_P; P) - 2\},$$

where T_P is the tangent line to Γ at $P \in \Gamma_0$. Let P_j be a place of a singular point and $x = t^{\nu_j}, y = a_1 t^{\lambda_j} + \cdots$ is a local equation of Γ at P_j. Then we have the following lemma (cf. [4]), where g is the genus of the normalization of Γ.

Lemma 8. *$W(\Gamma) = 3d + 6(g-1) - \sum_{P_j} (\lambda_j + \nu_j - 3)$.*

If P is a smooth point on Γ and the projection with center $\pi_P : \Gamma \longrightarrow \mathbb{P}^1$ induces a Galois extension of fields $\pi_P{}^* : k(\mathbb{P}^1) \hookrightarrow k(\Gamma)$, then we call P a (smooth) Galois point. Under this situation we have the following lemma, which is due to Miura.

Lemma 9. *The number $\delta' = \delta'(\Gamma)$ of (smooth) Galois points on a quartic curve Γ is at most four.*

Proof. Let C be the normalization of Γ and P a Galois point. We have a triple Galois covering $\widetilde{\pi_P} : C \longrightarrow \mathbb{P}^1$. Let r be the number of ramification points for this covering. Then we have that $r = 2 + g$ by Hurwitz's theorem. If Γ is smooth, then this lemma is true (cf. [12]). So we assume that Γ has singular points and prove by considering several kinds of singularities separately (cf. [6]).

(i) Γ has a cusp Q with multiplicity three. Then $\delta'(\Gamma) \leq 2$.

Because, in this case we have $g = 0$ and Γ has no other singular point. Hence we have $r = 2$ and $W(\Gamma) = 3 \cdot 4 - 6 - 4 = 2$. Therefore we infer that $\delta'(\Gamma) \leq 2$.

(ii) Γ has no cusp of multiplicity three. Then $\delta'(\Gamma) \leq 4$.

We divide this case into two subcases (ii-1) and (ii-2):

(ii-1) Γ has a cusp of multiplicity two. Then $\delta' \leq 1$.

Because, the cusp Q will be a ramification point for $\widetilde{\pi_P}$ with order 3 [resp. 2] if l_{PQ} is the tangent [resp. not tangent] line to Γ at Q. Since $\widetilde{\pi_P}$ is a triple Galois covering, l_{PQ} must be the tangent line, from this fact we infer that $\delta'(\Gamma) \leq 1$.

(ii-2) Γ has no cusp of multiplicity two. Then $\delta' \leq 4$.

Because, the singular points do not become the ramification points for $\widetilde{\pi_P}$, we have that $r\delta' \leq W(\Gamma)$. This implies that $\delta'(\Gamma) \leq 4$. □

Claim 3. *If $d = 4$, then there does not exist seven Galois points $P_0, P_1, P_1', P_2, P_2', P_3, P_3'$ such that P_0, P_1, P_2, P_3 are collinear and P_0, P_1', P_2', P_3' are collinear.*

Proof. Suppose the contrary. Then let L be the two dimensional linear variety containing all the points. Then by Claim 2 we have $L \not\subset V$ and hence $\Gamma = V \cap L$ is a quartic curve in $L \cong \mathbb{P}^2$. Note that, if σ is an automorphism associated with one of the Galois points, then $\sigma|_L$ is a projective transformation of L satisfying $\sigma(\Gamma) = \Gamma$. Since the order of σ is three and it acts on the covering $\pi_P|_\Gamma : \Gamma \longrightarrow \mathbb{P}^1$ transitively, Γ must be irreducible. Indeed, Γ is reduced. Otherwise, Γ can be written as $2\Gamma_0$, where Γ_0 is a conic. Since the Galois point lies on Γ_0, this is absurd. Hence Γ is reduced. Suppose that it is reducible. Then, it can be written as $\Gamma_1 + \Gamma_2$, where $\deg \Gamma_1 = 1$, $\deg \Gamma_2 = 3$ or $\deg \Gamma_1 = \deg \Gamma_2 = 2$. Since σ acts on Γ transitively, $\sigma(\Gamma_1) = \Gamma_2$. Hence the first case cannot occur. In the second case we have that $\sigma(\Gamma_1) = \Gamma_2$ and $\sigma^3 = id$. This implies $\sigma(\Gamma_1) = \Gamma_1$, which contradicts the transitivity. Therefore Γ is irreducible. Since the degree of Γ is four, it is smooth at the Galois points. By Lemma 9 a quartic curve has at most four smooth Galois points. Then we have a contradiction. □

Now let us proceed with the proof of Theorem 9. First we treat the case (1) $d = 4$. Let $P_1, \dots, P_r$ be independent inner Galois points such that the number r is the maximal one. We have $r \le m + 1$ by Lemma 4. If there exists another Galois point Q, then by definition and Claim 2 there exists $P_{i(1)}$ $(1 \le i(1) \le r)$ satisfying that on the line $l_{QP_{i(1)}}$ there exist four inner Galois points $P_{i(1)}, Q = Q_1, Q_2, Q_3$. Of course, on the line $l_{P_jQ_i}$, where $j \ne i(1), i = 1, 2, 3$, there exist no Galois points except P_j and Q_i by Claim 3. If moreover there exists another Galois point Q_4, then by the same reasoning as above there exists $P_{i(2)}$ $(1 \le i(2) \le r)$ satisfying that on the line $l_{Q_4P_{i(2)}}$ there exist four Galois points $P_{i(2)}, Q_4, Q_5, Q_6$. Here we notice that $i(1) \ne i(2)$ by Claim 3. In this way we conclude the former assertion of (1). For the latter one, the "if part" is checked by direct computation. Indeed, we can make use of Corollary 7. By rather tedious computations of the Hessian of F, we can show that $\delta(V) \ge 4(m + 1)$. Then, the equality follows from the first assertion. So we prove the "only if part". If the equality holds, then by Lemma 4 and Claim 3, V has $(m + 1)$ independent Galois points $P_0, \dots, P_m$. Then by Lemma 3 we can assume the following:

(i) $X_j(P_i) = \delta_{ji}$, where $0 \le i \le m$, $0 \le j \le n + 1$,

(ii) $\sigma_i = diag[\omega, \dots, \omega, 1, \omega, \dots, \omega]$, where σ_i is a generator of G_{P_i} and $\omega = \mathrm{e}_3$.

(iii) $F = A_0X_0^3 + \cdots + A_mX_m^3 + G$, where A_i and G are linear and quartic forms in $k[X_{m+1}, \dots, X_{n+1}]$ respectively.

Since $\delta(V) = 4(m+1)$, by the same reasoning as in the proof of the former assertion of (1), there exists a Galois point P_i' satisfying that $P_i, P_i', \sigma_i(P_i'), {\sigma_i}^2(P_i')$ are collinear, where σ_i is an automorphism associated with P_i $(0 \le i \le m)$. Then the line $l_{P_i P_i'}$ is not contained in V and $\sigma_j(P_i') = P_i'$ if $i \ne j$. Therefore we have that $X_j(P_i') = 0$ if $0 \le j \le m$ and $j \ne i$. Consequently, we can take coordinates satisfying the following conditions:

(i′) $X_j(P_i) = \delta_{ji}$, where $0 \le i \le m$, $0 \le j \le n+1$. $X_j(P_i') = \delta_{ji}$, where $0 \le i, j \le m$.

(ii′) $\sigma_i = diag[\omega, \dots, \omega, 1, \omega, \dots, \omega]$, where σ_i is a generator of G_{P_i} and $\omega = \mathrm{e}_3$.

(iii′) $F = X_{m+1}X_0^3 + \cdots + X_{2m+1}X_m^3 + G$, where G is a quartic form in $k[X_{m+1}, \dots, X_{n+1}]$.

Since the line $l_{P_i' P_j}$ is contained in V $(j \ne i)$, we see that $P_i' \in T_0 \cap \cdots \cap T_{i-1} \cap T_{i+1} \cap \cdots \cap T_m$, where T_j is the tangent plane to V at P_j. Hence we have that $X_j(P_i') = 0$ for $i \ne j$ and $j \ne m+i+1$, i.e., $P_i' = (0, \dots, 0, 1, 0, \dots, 0, \alpha_i, 0, \dots, 0)$, where 1 and α_i $(\ne 0)$ are in i-th and $(m+i+1)$-th positions respectively.

Here we mention a criterion that a point on a quartic hypersurface to be a Galois point. Let the origin $P = (0, \dots, 0)$ be an inner Galois point for a quartic hypersurface V in $\mathbb{A}^{n+1}$ defined by $f = f_1 + f_2 + f_3 + f_4$, where f_i is the homogeneous part of f with degree i. Then we have shown the following in [12, Lemma 11].

Lemma 10. *Under the condition above, P is a Galois point of V if and only if $f_2 = 3f_1f_3$.*

Let us continue the proof. Apply this lemma to find the condition that P_i' $(0 \le i \le m)$ becomes a Galois point. Consider the affine part $X_i \ne 0$ of V. Then the defining equation is

$$f = x_{m+1}x_0^3 + \cdots + x_{m+i} + \cdots + x_{2m+1}x_m^3 + g(x_{m+1}, \cdots, x_{n+1}),$$

where $x_j = X_j/X_i$ and $P_i' = (0, \dots, 0, \alpha_i, 0, \cdots, 0)$. Putting $x_{m+i+1} - \alpha_i = x$, we get

$$\begin{aligned} f &= x + \alpha_i + h(x_o, \cdots, x_{i-1}, x_{i+1}, \cdots, x_{n+1}) \\ &+ \lambda(x+\alpha_i)^4 + g_1 \cdot (x+\alpha_i)^3 + g_2 \cdot (x+\alpha_i)^2 + g_3 \cdot (x+\alpha_i) + g_4, \end{aligned}$$

where g_i is a form with degree i in $k[x_{m+1}, \dots, x_{m+i}, x_{m+i+2}, \dots, x_{n+1}]$. Making use of Lemma 10, we conclude that $g_1 = g_2 = g_3 = 0$ by simple calculations. In this way we will obtain that G has an expression as $\sum_{i=1}^{n-m+1} \lambda_i X_{m+i}^4$, where $\lambda_i \in k^\times$. Taking new coordinates, we obtain the latter assertion of (1).

Before proceeding with the proof of (2) we prepare some lemmas.

Lemma 11. *Suppose that $d \geq 5$. Then the following assertions holds true.*

(1) *If a line l is contained in V, then the number of Galois points on l is at most two.*

(2) *If a line l is not contained in V, then the number of Galois points on $V \cap l$ is zero or one.*

Proof. First we prove (1). Of course, in this case we have $n \geq 2$. In the case where $n = 2$, suppose that there exist at least three Galois points on l. Then, let H be a hyperplane containing l and put $V \cap H = l \cup C$. If H is general, then C is smooth and irreducible by Bertini's Theorem [3, pp. 274–275]. The Galois points become the outer Galois points for C in the plane $H \cong \mathbb{P}^2$. However such collinear outer Galois points cannot exist, see [12]. This is a contradiction. In the case where $n \geq 3$, we prove by induction using the linear system Λ_l defined before Lemma 7. Second we prove (2). In the case where $n = 1$ this is true by [12, Theorem 4]. So we assume that this holds true in the case where $\dim V = n - 1 \geq 1$. Suppose that there exist at least two Galois points on a line l. Then let H be a hyperplane containing l. By Lemma 7 we have a smooth irreducible subvariety $V \cap H$. From this we get a contradiction, hence the number is zero or one. □

As a direct consequence of this lemma we have the following.

Lemma 12. *If $d \geq 5$, then inner Galois points are independent. Especially we have $\delta(V) \leq m + 1$.*

Thus the former assertion of (2) is proved. For the latter one, "if part" is clear. Indeed, the points P_i satisfying that $X_j(P_i) = \delta_{ji}$, where $0 \leq i \leq m$, $0 \leq j \leq n + 1$, are Galois points. Hence we have $\delta(V) \geq m + 1$. By the inequality in the former assertion we have $\delta(V) = m + 1$. The "only if part" may also be clear. By Lemma 12, V has $(m + 1)$ independent Galois points. Then by Lemma 3 we can assume that $F = A_0 X_0^{d-1} + \cdots + A_m^{d-1} + G$, where A_i and G are forms in $k[X_{m+1}, \ldots, X_{n+1}]$ and $\deg A_i = 1$ and $\deg G = d$. Since V is smooth, the matrix obtained from the coefficients of A_i has rank $m+1$. Therefore we can take such coordinates as F has the representation as in the theorem. Thus we complete the proof of Theorem 9.

Finally we consider outer Galois points and prove Theorem 10.

Lemma 13. *Outer Galois points are independent if $d \geq 3$.*

Proof. This holds true when $n = 1$ (cf. [12]). We prove this by induction on n. Suppose that this assertion does not hold true. Then, there exist at least three outer Galois points $\{P_i\}$ for V which lie on a line l. Of course, l is not contained in V. By Lemma 7 if H is a general hyperplane containing l, then $V' = V \cap H$ is smooth and irreducible. Hence $\{P_i\}$ are also outer Galois points for V', which are collinear. This is a contradiction by induction hypothesis. □

Proposition 11. *We have $\delta(V^c) = 0, 1, 2, \dots, n, n+2$. If $\delta(V^c) = r+1$, then the defining equation of V can be expressed as $F = X_0^d + \cdots + X_r^d + G$, where G is a form of degree d in $k[X_{r+1}, \dots, X_{n+1}]$. Especially, if $\delta(V^c) = n+2$, then F is the Fermat variety.*

Proof. By Lemmas 3 and 13 the proof is straightforward. □

Thus we complete all the proofs.

ACKNOWLEDGEMENT

The author expresses his sincere thanks to the referee for giving him invaluable suggestions, especially the proof of Lemma 1 is the revised one suggested by the referee.

References

1. R. Cortini, *Degree of irrationality of smooth surface of* $\mathbb{P}^3$, to appear.
2. P. Griffiths and J. Harris, *Principles of Algebraic Geometry*, Pure and Applied Mathematics, A Wiley-Interscience Publication, New York, 1978.
3. R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, **52** Springer-Verlag, New York, Heidelberg, Berlin, 1977.
4. S. Iitaka, *Algebraic Geometry*, Graduate Texts in Mathematics, **76** Springer-Verlag, New York, Heidelberg, Berlin, 1982.
5. H. Matsumura and P. Monsky, *On the automorphisms of hypersurfaces*, J. Math. Kyoto Univ., **3** (1964), 347–361.
6. K. Miura, *Field theory for function fields of singular plane quartic curves*, Bull. Austral. Math. Soc., **62** (2000), 193–204.
7. K. Miura and H. Yoshihara, *Field theory for function fields of plane quartic curves*, J. Algebra, **226** (2000), 283–294; doi:10.1006/jabr.1999.8173.
8. M. Namba, *Branched coverings and algebraic functions*, Pitman Research Notes in Math. Series, **161**.
9. M. Reid, *Undergraduate Algebraic Geometry*, London Math. Soc. Student Texts **12** Cambridge University Press, Cambridge, 1990.
10. T. Takahashi, *Minimal splitting surface determined by a projection of a smooth quartic surface*, Algebra Colloquium, **9**(2002), 107–115.
11. H. Yoshihara, *Degree of irrationality of an algebraic surface*, J. Algebra, **167** (1994), 634–640.
12. ———, *Function field theory of plane curves by dual curves*, J. Algebra, **239** (2001), 340–355; doi:10.1006/jabr.2000.8675.
13. ———, *Galois points on quartic surfaces*, J. Math. Soc. Japan, **53** (2001), 731–743.
14. ———, *Galois lines for space curves*, to appear.