Algebraic curves admitting non-collinear Galois points

SATORU FUKASAWA*

ABSTRACT – This paper presents a criterion for the existence of a birational embedding into a projective plane with non-collinear Galois points for algebraic curves and describes its application via a novel example of a plane curve with non-collinear Galois points. In addition, this paper presents a new characterisation of the Fermat curve in terms of non-collinear Galois points.

MATHEMATICS SUBJECT CLASSIFICATION (2010). 14H50, 14H05, 14H37.

KEYWORDS. Galois point, plane curve, Galois group, automorphism group.

1. Introduction

The theory of Galois points was formulated by Hisao Yoshihara in 1996 and was developed by him and several other authors ([1, 13, 15, 16]), resulting in many interesting studies. One such study was on the number of Galois points, and it contained several characterisation results of algebraic varieties according to the number. The relation between Galois point theory and other research subjects, such as automorphism groups of algebraic curves, the theory of maximal curves with respect to the Hasse–Weil bound, coding theory and others, was also elucidated. The automorphism group generated by the Galois groups of Galois points is large in many cases ([3, 11, 12]). A class of curves characterised as smooth plane curves of degree $d \geq 5$ possessing exactly $d$ inner Galois points has interesting properties, more precisely, they are ordinary and admit many automorphisms ([3]). All curves with many automorphisms appearing in the classification list by Stichtenoth and Henn ([9, Theorem 11.127]) have a plane model with two Galois points ([5, 6, 10]). Many important maximal curves and their quotient curves also admit a plane model with two Galois points ([5, 6, 7, 10]). For the Ballico–Hefez

*The author was partially supported by JSPS KAKENHI Grant Number 19K03438.

Satoru Fukasawa, Department of Mathematical Sciences, Yamagata University, Kojirakawamachi 1-4-12, Yamagata 990-8560, Japan
E-mail: s.fukasawa@sci.kj.yamagata-u.ac.jp
curve, the set of Galois points coincides with the set of rational points ([2]), and 
algebraic-geometric codes from this curve have good parameters ([8]).

Let $X$ be a (reduced, irreducible) smooth projective curve over an algebraically 
closed field $k$ of characteristic $p \geq 0$, and let $k(X)$ be its function field. We consider 
a morphism $\varphi : X \to \mathbb{P}^2$, which is birational, onto its image. Fixing a point $P \in \mathbb{P}^2$ 
and a line $\ell \subset \mathbb{P}^2$ with $\ell \neq P$, we consider the projection $\pi_P : \varphi(X) \dashrightarrow \ell \cong \mathbb{P}^1$ 
from $P$ to $\ell$. Note that the subfield $\pi_P^*k(\ell) \subset k(\varphi(X))$ does not depend on 
the choice of the line $\ell$. The point $P$ is called a Galois point if the extension 
$k(\varphi(X))/\pi_P^*k(\ell)$ is Galois ([13, 15]). The associated Galois group is then denoted 
by $G_P$. Furthermore, a Galois point $P$ is said to be inner (resp. outer) if $P \in 
\varphi(X) \setminus \text{Sing}(\varphi(X))$ (resp. if $P \in \mathbb{P}^2 \setminus \varphi(X)$).

To obtain a general result regarding the number of Galois points for plane 
curves, it would avail us to gather numerous examples of plane curves with two 
Galois points. Until recently, it has been difficult to construct a pair 
$(X, \varphi)$ such that $\varphi(X)$ admits two Galois points. In 2016, a criterion for the 
existence of birational embedding with two Galois points was described by the 
present author ([4]) whereby many new examples of plane curves with two Galois 
points were obtained ([4, 5, 6, 7, 12, 16]). This criterion is described hereunder.

**FACT 1.1.** Fix two finite subgroups $G_1$ and $G_2$ of $\text{Aut}(X)$ and two different 
points $P_1$ and $P_2$ of $X$. Then the conditions (1) and (2) below are equivalent.

1. The following three conditions are satisfied:
   - (a) $X/G_i \cong \mathbb{P}^1$ for $i = 1, 2$;
   - (b) $G_1 \cap G_2 = \{1\}$;
   - (c) $P_1 + \sum_{\sigma \in G_1} \sigma(P_2) = P_2 + \sum_{\tau \in G_2} \tau(P_1)$ in $\text{Div}(X)$.

2. There exists a birational embedding $\varphi : X \to \mathbb{P}^2$ of degree $|G_1| + 1$ such that 
   $\varphi(P_1)$ and $\varphi(P_2)$ are different inner Galois points for $\varphi(X)$ and $G_{\varphi(P_i)} = G_i$ 
   for $i = 1, 2$.

Obtaining three Galois points, however, would greatly aid further development. 
For non-collinear Galois points, we obtained the following theorems.

**THEOREM 1.2.** Fix three finite subgroups $G_1, G_2$ and $G_3$ of $\text{Aut}(X)$ and three 
different points $P_1$, $P_2$ and $P_3$ of $X$. Then the conditions (1) and (2) below are 
equivalent.

1. The following four conditions are satisfied:
   - (a) $X/G_i \cong \mathbb{P}^1$ for $i = 1, 2, 3$;
   - (b) $G_i \cap G_j = \{1\}$ for any $i, j$ with $i \neq j$;
   - (c) $P_i + \sum_{\sigma \in G_j} \sigma(P_j) = P_j + \sum_{\tau \in G_j} \tau(P_i)$ for any $i, j$ with $i \neq j$;
   - (d) $G_i P_j \neq G_k P_k$ for any $i, j, k$ with $\{i, j, k\} = \{1, 2, 3\}$.
There exists a birational embedding \( \varphi : X \to \mathbb{P}^2 \) of degree \( |G_1| + 1 \) such that 
\( \varphi(P_1), \varphi(P_2) \) and \( \varphi(P_3) \) are non-collinear inner Galois points for \( \varphi(X) \) and 
\( G_{\varphi(P_i)} = G_i \) for \( i = 1, 2, 3 \).

**Theorem 1.3.** Fix three finite subgroups \( G_1, G_2 \) and \( G_3 \) of \( \text{Aut}(X) \) and three different points \( Q_1, Q_2 \) and \( Q_3 \) of \( X \). Then the conditions (1) and (2) below are equivalent.

1. The following four conditions are satisfied:
   - (a) \( X/G_i \cong \mathbb{P}^1 \) for \( i = 1, 2, 3 \);
   - (b) \( G_i \cap G_j = \{1\} \) for any \( i, j \) with \( i \neq j \);
   - (c') \( \sum_{\sigma \in G_i} \sigma(Q_k) = \sum_{\tau \in G_j} \tau(Q_k) \) for any \( i, j, k \) with \( \{i, j, k\} = \{1, 2, 3\} \);
   - (d') \( G_i Q_j \neq G_i Q_k \) for any \( i, j, k \) with \( \{i, j, k\} = \{1, 2, 3\} \).

2. There exists a birational embedding \( \varphi : X \to \mathbb{P}^2 \) of degree \( |G_1| \) and non-collinear outer Galois points \( P_1, P_2 \) and \( P_3 \) exist for \( \varphi(X) \) such that \( G_{P_i} = G_i \) and \( P_i P_j \ni \varphi(Q_k) \) for any \( i, j, k \) with \( \{i, j, k\} = \{1, 2, 3\} \), where \( P_i P_j \) is the line passing through \( P_i \) and \( P_j \).

A new example of a plane curve with non-collinear outer Galois points was constructed as follows for the purposes of application.

**Theorem 1.4.** Let the characteristic \( p \) be positive, \( q \) be a power of \( p \), and let \( X \subset \mathbb{P}^2 \) be the Hermitian curve, which is (the projective closure of) the curve given by
\[
x^q + x = y^{q+1}.
\]
If a positive integer \( s \) divides \( q - 1 \), then a plane model of \( X \) of degree \( s(q + 1) \) admitting non-collinear outer Galois points \( P_1, P_2 \) and \( P_3 \) is derived.

The next task was to classify plane curves with non-collinear Galois points. We considered the group \( G := \langle G_{P_1}, G_{P_2}, G_{P_3} \rangle \subset \text{Aut}(X) \) for non-collinear outer Galois points \( P_1, P_2 \) and \( P_3 \). The following result provides a criterion to establish when for all points \( Q \in \varphi^{-1}(\bigcup_{i \neq j} P_i P_j) \) the orbit \( GQ \) of \( Q \) is contained in 
\( \varphi^{-1}(\bigcup_{i \neq j} P_i P_j) \).

**Theorem 1.5.** Let \( \varphi : X \to \mathbb{P}^2 \) be a birational embedding of degree \( d \geq 3 \), and let \( C = \varphi(X) \). Then the following conditions are equivalent.

(a) There exist non-collinear Galois points \( P_1, P_2 \) and \( P_3 \in \mathbb{P}^2 \setminus C \) such that 
\( GQ \subset \varphi^{-1}(\bigcup_{i \neq j} P_i P_j) \) for any \( Q \in \varphi^{-1}(\bigcup_{i \neq j} P_i P_j) \), where \( G = \langle G_{P_1}, G_{P_2}, G_{P_3} \rangle \).

(b) \( p = 0 \) or \( d \) is prime to \( p \), and \( C \) is projectively equivalent to the Fermat curve 
\( X^d + Y^d + Z^d = 0 \).
2. Proofs of Theorems 1.2 and 1.3

Proof of Theorem 1.2. First, we must consider (2) \(\Rightarrow\) (1). According to Fact 1.1, conditions (a), (b) and (c) are satisfied. Since the points \(\varphi(P_1), \varphi(P_2)\) and \(\varphi(P_3)\) are not collinear, the lines \(\varphi(P_i)\varphi(P_j)\) and \(\varphi(P_i)\varphi(P_k)\) are different for any \(i, j, k\) with \(\{i, j, k\} = \{1, 2, 3\}\). According to the definition of the Galois points and a property of a Galois extension ([14, III.7.1]), it follows that \(G_{\varphi(P_i)}P_j \subset \varphi^{-1}(\varphi(P_i)\varphi(P_j))\), and that if the line \(\varphi(P_i)\varphi(P_j)\) is not a tangent line at \(\varphi(P_t)\), then \(G_{\varphi(P_i)}P_j = \varphi^{-1}(\varphi(P_i)\varphi(P_j)) \setminus \{P_t\}\). Since both \(\varphi(P_i)\varphi(P_j)\) and \(\varphi(P_i)\varphi(P_k)\) are not tangent lines at \(\varphi(P_t)\), it follows that \(G_iP_j = G_{\varphi(P_i)}P_j \neq G_{\varphi(P_i)}P_k = G_iP_k\). Condition (d) is satisfied.

Then, we must consider (1) \(\Rightarrow\) (2). According to condition (d),

\[
\supp\left( \sum_{\sigma \in G_1} \sigma(P_2) \right) \cap \supp\left( \sum_{\sigma \in G_1} \sigma(P_3) \right) = \emptyset.
\]

Then, by condition (a), there exists a function \(f \in k(X) \setminus k\) such that

\[
k(X)^{G_1} = k(f), \quad (f) = \sum_{\sigma \in G_1} \sigma(P_3) - \sum_{\sigma \in G_1} \sigma(P_2)
\]

(see also [14, III.7.1, III.7.2, III.8.2]). Similarly, there exists \(g \in k(X) \setminus k\) such that

\[
k(X)^{G_2} = k(g), \quad (g) = \sum_{\tau \in G_2} \tau(P_3) - \sum_{\tau \in G_2} \tau(P_1).
\]

Considering condition (c), we take a divisor

\[
D := P_1 + \sum_{\sigma \in G_1} \sigma(P_2) = P_2 + \sum_{\tau \in G_2} \tau(P_1).
\]

Then \(f, g \in \mathcal{L}(D)\). It follows that the sublinear system of \(|D|\) corresponding to a linear space \((f, g, 1)\) is base-point-free. Under condition (b), the induced morphism

\[
\varphi : X \to \mathbb{P}^2; \quad (f : g : 1)
\]

is birational onto its image, and points \(\varphi(P_1) = (0 : 1 : 0)\) and \(\varphi(P_2) = (1 : 0 : 0)\) are inner Galois points for \(\varphi(X)\) such that \(G_{\varphi(P_1)} = G_1\) and \(G_{\varphi(P_2)} = G_2\) (see [4, Proofs of Proposition 1 and of Theorem 1]). Furthermore, \(\varphi(P_3) = (0 : 0 : 1)\).
Under condition (c), we have

\[
(g/f) = \sum_{\tau \in G_2} \tau(P_3) - \sum_{\tau \in G_2} \tau(P_1) - \sum_{\sigma \in G_1} \sigma(P_3) + \sum_{\sigma \in G_1} \sigma(P_2)
\]

\[
= (P_2 + \sum_{\tau \in G_2} \tau(P_3)) - (P_2 + \sum_{\tau \in G_2} \tau(P_1))
\]

\[
- (P_1 + \sum_{\sigma \in G_1} \sigma(P_3)) + (P_1 + \sum_{\sigma \in G_1} \sigma(P_2))
\]

\[
= (P_3 + \sum_{\gamma \in G_3} \gamma(P_2)) - (P_3 + \sum_{\gamma \in G_3} \gamma(P_1))
\]

\[
= \sum_{\gamma \in G_3} \gamma(P_2) - \sum_{\gamma \in G_3} \gamma(P_1).
\]

Then, the subfield \(k(g/f)\) induced via projection from \(P_3\) coincides with \(k(X)^{G_3}\). Therefore, this point \(\varphi(P_3)\) is an inner Galois point with \(G_{\varphi(P_3)} = G_3\). □

The proof for Theorem 1.3 is similar to the preceding.

3. A new example

Let \(X \subseteq \mathbb{P}^2\) be the Hermitian curve of degree \(q + 1\). The set of all \(\mathbb{F}_q^2\)-rational points of \(X\) is denoted by \(X(\mathbb{F}_q^2)\); see [9] for the properties of the Hermitian curve.

**Proof of Theorem 1.4.** Let \(Q_1 = (1 : 0 : 0)\) and \(Q_2 = (0 : 0 : 1)\), and let \(Q_3 = (\alpha : \beta : 1) \in X(\mathbb{F}_q^2)\) with \(Q_3 \notin Q_1Q_2 = \{Y = 0\}\). The matrix

\[
A_a := \begin{pmatrix}
a^{q+1} & 0 & 0 \\
0 & a & 0 \\
0 & 0 & 1
\end{pmatrix}
\]

then acts on \(X\) and fixes \(Q_1\) and \(Q_2\), where \(a \in \mathbb{F}_q^2 \setminus \{0\}\). Let \(sm = q - 1\) and let \(G_3 \subseteq \text{Aut}(X)\) be the cyclic group of order \(s(q + 1)\) whose elements are the matrices \(A_{\alpha^m}\). Note that each element of \(G_3 \setminus \{1\}\) does not fix \(Q_4\). There exists an automorphism \(\Phi \in \text{Aut}(X)\) represented by

\[
\begin{pmatrix}
0 & 0 & a^{q+1} \\
0 & -\alpha^q & a^q\beta \\
1 & -\beta^q & a^q
\end{pmatrix}
\]

such that \(\Phi(Q_1) = Q_2, \Phi(Q_2) = Q_3\) and \(\Phi(Q_3) = Q_1\). In such a case, the group \(\Phi G_3 \Phi^{-1}\) fixes points \(Q_2\) and \(Q_3\), and each element of this group that differs from identity does not fix \(Q_1\). Therefore, for each pair \((Q_i, Q_j)\), there exists a cyclic group \(G_k\) of order \(s(q + 1)\) such that \(G_k\) fixes points \(Q_i\) and \(Q_j\), and each element of \(G_k \setminus \{1\}\) does not fix \(Q_k\). Therefore, we would like to show that conditions (a), (b), (c') and (d') in Theorem 1.3 are satisfied for groups \(G_1, G_2\) and \(G_3\).
Note that 

\[(A^m)^\ast = A_{m-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a^{q-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}.
\]

Let \(G'_3 \subset G_3\) be a subgroup consisting entirely of \(A_{q-1}\). Since \(k(X)^{G_3} \subset k(X)^{G'_3} = k(x)\), by Lüroth’s theorem, \(X/G_3\) is rational. Condition (a) is thus satisfied. Since \(G_1\) fixes \(Q_2\) and the set \(G_2 \setminus \{1\}\) does not contain an element fixing \(Q_2\), \(G_1 \cap G_2 = \{1\}\). Condition (b) is thus satisfied. For any \(i, j, k\) with \(\{i, j, k\} = \{1, 2, 3\}\),

\[
\sum_{\sigma \in G_i} \sigma(Q_k) = s(q + 1)Q_k = \sum_{\tau \in G_j} \tau(Q_k).
\]

Therefore, condition (c’) is satisfied. Since \(G_iQ_j = \{Q_j\} \neq \{Q_k\} = G_iQ_k\), condition (d’) is also satisfied. \(\blacksquare\)

4. A characterisation of the Fermat curve

**Proof of Theorem 1.5.** (a) \(\Rightarrow\) (b). Let \(Q \in \varphi^{-1}(P_1P_2)\). By the definition of the outer Galois points, \(G_{P_1}Q \subset \varphi^{-1}(P_1P_2)\), \(G_{P_2}Q \subset \varphi^{-1}(P_1P_2)\) and \(G_{P_3}Q \subset \varphi^{-1}(P_3\varphi(Q))\). If \(\gamma(Q) \in \varphi^{-1}(P_2P_3)\) for some \(\gamma \in G_{P_3}\), then \(\varphi(\gamma(Q)) \in P_3\varphi(Q) \cap P_2P_3 = \{P_3\}\). This is a contradiction. Therefore, condition (a) implies that \(G_{P_i}Q \subset \varphi^{-1}(P_1P_2)\), and it follows that \(\gamma \in G_{P_i}\) induces a bijection of \(\text{supp}(\varphi^*P_1P_2)\). Since \(G_{P_1}\) acts on \(\text{supp}(\varphi^*P_1P_2)\) transitively,

\[
\varphi^*P_1P_2 = \sum_{Q \in \text{supp}(\varphi^*P_1P_2)} mQ
\]

for some integer \(m \geq 1\). Therefore, for any \(\gamma \in G_{P_3}\),

\[
\gamma^*\varphi^*P_1P_2 = \varphi^*(P_1P_2).
\]

Let \(D := \varphi^*P_3P_1\). We take a function \(f \in k(X)\) with \(k(f) = k(X)^{G_3}\) such that

\[
(f) = \varphi^*P_3P_2 - \varphi^*P_3P_1.
\]

Similarly, we can take a function \(g \in k(X)^{G_1}\) such that

\[
(g) = \varphi^*P_1P_2 - \varphi^*P_1P_3.
\]

Since \(P_1P_2\) does not pass through \(P_3\), it follows that \(g \notin (1, f) \subset \mathcal{L}(D)\). It follows from the condition \(\gamma^*\varphi^*(P_1P_2) = \varphi^*(P_1P_2)\) that \(\gamma^*g = a(\gamma)g\) for some \(a(\gamma) \in k\). Therefore, a linear subspace \((1, f, g) \subset \mathcal{L}(D)\) is invariant under the action of any \(\gamma \in G_{P_3}\). Since \(\varphi\) is represented by \((1 : f : g)\), there exists an injective homomorphism

\[
G_{P_3} \twoheadrightarrow \text{PGL}(3, k); \quad \gamma \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a(\gamma) \end{pmatrix}.
\]
It follows that $d$ is prime to $p$, and the map $G_{P_3} \to k \setminus \{0\}; \gamma \mapsto a(\gamma)$ is an injective homomorphism. This implies that $G_{P_3}$ is a cyclic group and that $C$ is invariant under the linear transformation $(X : Y : Z) \mapsto (X : \zeta Y : Z)$, where $\zeta$ is a primitive $d$-th root of unity. Similarly, $G_{P_1}$ is generated by the automorphism given by the linear transformation $(X : Y : Z) \mapsto (X : \zeta Y : Z)$. Let $F(X, Y, Z) = \sum_{i=0}^{d} F_i(X, Y)Z^i$ be a defining polynomial of $C$. Since $F(X, Y, Z) = F(X, Y, Z)$ up to a constant, it follows that $F_1 = \cdots = F_{d-1} = 0$. Let $F_0 = \sum_{i=0}^{d} G_i(X)Y^i$. Similarly, it follows that $G_1 = \cdots = G_{d-1} = 0$. Therefore, $F = aX^d + bY^d + cZ^d$ for some $a, b, c \in k \setminus \{0\}$. It follows that $C$ is projectively equivalent to the Fermat curve $X^d + Y^d + Z^d = 0$.

(b) $\Rightarrow$ (a). This is derived from the fact that groups $G_{P_1}, G_{P_2}$ and $G_{P_3}$ fix all points on the lines $\{X = 0\}, \{Y = 0\}$ and $\{Z = 0\}$, respectively, for the Fermat curve, where $P_1 = (1 : 0 : 0)$, $P_2 = (0 : 1 : 0)$ and $P_3 = (0 : 0 : 1)$.

\[\square\]

Acknowledgements

The author is grateful to Doctor Kazuki Higashine for helpful discussions. The author also thanks the referee for useful comments, by which the author can improve some explanation in the previous version of this paper.

References


Received submission date; revised revision date