Rend. Sem. Mat. Univ. Padova 149 (2023), 183–190
DOI 10.4171/RSMUP/114

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 (2020) – Primary 14H50; Secondary 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, 14, 16, 17], 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, or coding theory, was also elucidated. The automorphism group generated by the Galois groups of Galois points is large in many cases [3, 11–13]. 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

(*) *Indirizzo dell'A.*: Department of Mathematical Sciences, Yamagata University, Kojirakawa-machi 1-4-12, Yamagata 990-8560, Japan; s.fukasawa@sci.kj.yamagata-u.ac.jp

curves also admit a plane model with two Galois points [5–7, 10]. For the Ballico–Hefez 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 $\ell \not\ni P$, we consider the projection $\pi_P : \varphi(X) \dashrightarrow \ell \cong \mathbb{P}^1$ from P to ℓ. Note that the subfield $\pi_P^* k(\ell) \subset k(\varphi(X))$ does not depend on the choice of the line ℓ. The point P is called a *Galois point* if the extension $k(\varphi(X))/\pi_P^* k(\ell)$ is Galois [14, 16]. The associated Galois group is then denoted by G_P. Furthermore, a Galois point P is said to be inner (resp. outer) if $P \in \varphi(X) \setminus \mathrm{Sing}(\varphi(X))$ (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 (or more) Galois points. Until recently, it has been difficult to construct a pair (X, φ) 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 [4–7, 12, 17]. This criterion is described hereunder.

Fact 1.1. *Fix two finite subgroups G_1 and G_2 of* 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* $\mathrm{Div}(X)$.

(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* 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) $P_i + \sum_{\sigma \in G_i} \sigma(P_j) = P_j + \sum_{\tau \in G_j} \tau(P_i)$ *for any* i, j *with* $i \neq j$*;*

 (d) $G_i P_j \neq G_i P_k$ *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* $|G_1| + 1$ *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* 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* $\overline{P_i P_j} \ni \varphi(Q_k)$ *for any* i, j, k *with* $\{i, j, k\} = \{1, 2, 3\}$*, where* $\overline{P_i P_j}$ *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 $Q \in \varphi^{-1}(\bigcup_{i \neq j} \overline{P_i P_j})$ the orbit GQ of Q is contained in $\varphi^{-1}(\bigcup_{i \neq j} \overline{P_i P_j})$.

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 $GQ \subset \varphi^{-1}(\bigcup_{i \neq j} \overline{P_i P_j})$ for any $Q \in \varphi^{-1}(\bigcup_{i \neq j} \overline{P_i P_j})$, 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 $\overline{\varphi(P_i)\varphi(P_j)}$ and $\overline{\varphi(P_i)\varphi(P_k)}$ 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 [15, III.7.1 Theorem], it follows that $G_{\varphi(P_i)} P_j \subset \varphi^{-1}(\overline{\varphi(P_i)\varphi(P_j)})$, and that if the line $\overline{\varphi(P_i)\varphi(P_j)}$ is not a tangent line at $\varphi(P_i)$, then $G_{\varphi(P_i)} P_j = \varphi^{-1}(\overline{\varphi(P_i)\varphi(P_j)}) \setminus \{P_i\}$. Since one of the lines $\overline{\varphi(P_i)\varphi(P_j)}$ and $\overline{\varphi(P_i)\varphi(P_k)}$ is not a tangent line at $\varphi(P_i)$, it follows that $G_i P_j = G_{\varphi(P_i)} P_j \neq G_{\varphi(P_i)} P_k = G_i P_k$. Condition (d) is satisfied.

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

$$\operatorname{supp}\Big(\sum_{\sigma \in G_1} \sigma(P_2)\Big) \cap \operatorname{supp}\Big(\sum_{\sigma \in G_1} \sigma(P_3)\Big) = \emptyset.$$

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 [15, III.7.1 Theorem, III.7.2 Corollary, III.8.2 Theorem]). 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 $\langle f, g, 1\rangle$ 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 Theorem 1]). Furthermore, $\varphi(P_3) = (0:0:1)$. Under condition (c), we have

$$\begin{aligned}(g/f) &= \sum_{\tau\in G_2}\tau(P_3) - \sum_{\tau\in G_2}\tau(P_1) - \sum_{\sigma\in G_1}\sigma(P_3) + \sum_{\sigma\in G_1}\sigma(P_2)\\ &= \Big(P_2 + \sum_{\tau\in G_2}\tau(P_3)\Big) - \Big(P_2 + \sum_{\tau\in G_2}\tau(P_1)\Big)\\ &\qquad - \Big(P_1 + \sum_{\sigma\in G_1}\sigma(P_3)\Big) + \Big(P_1 + \sum_{\sigma\in G_1}\sigma(P_2)\Big)\\ &= \Big(P_3 + \sum_{\gamma\in G_3}\gamma(P_2)\Big) - \Big(P_3 + \sum_{\gamma\in G_3}\gamma(P_1)\Big)\\ &= \sum_{\gamma\in G_3}\gamma(P_2) - \sum_{\gamma\in G_3}\gamma(P_1).\end{aligned}$$

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 of Theorem 1.3 is similar to the preceding one.

3. A new example

Let $X \subset \mathbb{P}^2$ 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 $Q_3 \notin \overline{Q_1Q_2} = \{Y = 0\}$. 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 $G_3 \subset \mathrm{Aut}(X)$ be the cyclic group of order $s(q+1)$ whose elements are the matrices A_{a^m}. Note that each element of $G_3 \setminus \{1\}$ does not fix Q_3. There exists an automorphism $\Phi \in \mathrm{Aut}(X)$ represented by

$$\begin{pmatrix} 0 & 0 & \alpha^{q+1}\\ 0 & -\alpha^q & \alpha^q\beta\\ 1 & -\beta^q & \alpha^q\end{pmatrix}$$

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

$$(A_{a^m})^s = A_{a^{q-1}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a^{q-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Let $G_3' \subset G_3$ be a subgroup consisting entirely of $A_{a^{q-1}}$. 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, we have $G_1 \cap G_2 = \{1\}$. 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 $G_i Q_j = \{Q_j\} \neq \{Q_k\} = G_i Q_k$, condition (d′) is also satisfied. ∎

4. A characterisation of the Fermat curve

Proof of Theorem 1.5. (a) ⇒ (b). Let $Q \in \varphi^{-1}(\overline{P_1P_2})$. By the definition of the outer Galois points,

$$G_{P_1}Q \subset \varphi^{-1}(\overline{P_1P_2}), \quad G_{P_2}Q \subset \varphi^{-1}(\overline{P_1P_2}), \quad G_{P_3}Q \subset \varphi^{-1}(\overline{P_3\varphi(Q)}).$$

If $\gamma(Q) \in \varphi^{-1}(\overline{P_2P_3})$ for some $\gamma \in G_{P_3}$, then $\varphi(\gamma(Q)) \in \overline{P_3\varphi(Q)} \cap \overline{P_2P_3} = \{P_3\}$. This is a contradiction. Therefore, condition (a) implies that $G_{P_3}Q \subset \varphi^{-1}(\overline{P_1P_2})$, and it follows that $\gamma \in G_{P_3}$ induces a bijection of $\mathrm{supp}(\varphi^*\overline{P_1P_2})$. Since G_{P_1} acts on $\mathrm{supp}(\varphi^*\overline{P_1P_2})$ transitively,

$$\varphi^*\overline{P_1P_2} = \sum_{Q \in \mathrm{supp}(\varphi^*\overline{P_1P_2})} mQ$$

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

$$\gamma^*\varphi^*(\overline{P_1P_2}) = \varphi^*(\overline{P_1P_2}).$$

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

$$(f) = \varphi^*\overline{P_3P_2} - \varphi^*\overline{P_3P_1}.$$

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

$$(g) = \varphi^* \overline{P_1 P_2} - \varphi^* \overline{P_1 P_3}.$$

Since $\overline{P_1 P_2}$ does not pass through P_3, it follows that $g \not\in \langle 1, f \rangle \subset \mathcal{L}(D)$. It follows from the condition $\gamma^* \varphi^*(\overline{P_1 P_2}) = \varphi^*(\overline{P_1 P_2})$ that $\gamma^* g = a(\gamma) g$ for some $a(\gamma) \in k$. Therefore, a linear subspace $\langle 1, f, g \rangle \subset \mathcal{L}(D)$ is invariant under the action of any $\gamma \in G_{P_3}$. Since φ is represented by $(1 : f : g)$, there exists an injective homomorphism

$$G_{P_3} \hookrightarrow \mathrm{PGL}(3, k); \quad \gamma \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a(\gamma) \end{pmatrix}.$$

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 $(X : Y : Z) \mapsto (X : Y : \zeta Z)$, where ζ 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 $F(X, Y, \zeta Z) = F(X, Y, Z)$ 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 $P_3 = (0 : 0 : 1)$. ∎

Acknowledgements – The author is grateful to Doctor Kazuki Higashine for helpful discussions. The author also thanks the referee for useful comments that allowed the author to improve some explanations in the previous version of this paper.

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

References

[1] S. Fukasawa, Galois points for a plane curve in arbitrary characteristic. *Geom. Dedicata* **139** (2009), 211–218. Zbl 1160.14304 MR 2481846

[2] S. Fukasawa, Galois points for a non-reflexive plane curve of low degree. *Finite Fields Appl.* **23** (2013), 69–79. Zbl 1314.14054 MR 3061085

[3] S. Fukasawa, Automorphism groups of smooth plane curves with many Galois points. *Nihonkai Math. J.* **25** (2014), no. 1, 69–75. Zbl 1307.14040 MR 3270973

[4] S. Fukasawa, A birational embedding of an algebraic curve into a projective plane with two Galois points. *J. Algebra* **511** (2018), 95–101. Zbl 1400.14084 MR 3834764

[5] S. Fukasawa, Birational embeddings of the Hermitian, Suzuki and Ree curves with two Galois points. *Finite Fields Appl.* **57** (2019), 60–67. Zbl 1423.14212 MR 3913757

[6] S. Fukasawa – K. Higashine, A birational embedding with two Galois points for certain Artin-Schreier curves. *Finite Fields Appl.* **52** (2018), 281–288. Zbl 1397.14042 MR 3807853

[7] S. Fukasawa – K. Higashine, A birational embedding with two Galois points for quotient curves. *J. Pure Appl. Algebra* **225** (2021), no. 3, Paper No. 106525. Zbl 1443.14037 MR 4137715

[8] S. Fukasawa – M. Homma – S. J. Kim, Rational curves with many rational points over a finite field. In *Arithmetic, geometry, cryptography and coding theory*, pp. 37–48, Contemp. Math. 574, American Mathematical Society, Providence, RI, 2012. Zbl 1317.11059 MR 2961398

[9] J. W. P. Hirschfeld – G. Korchmáros – F. Torres, *Algebraic curves over a finite field*. Princeton Ser. Appl. Math., Princeton University Press, Princeton, NJ, 2008. Zbl 1200.11042 MR 2386879

[10] M. Homma, Galois points for a Hermitian curve. *Comm. Algebra* **34** (2006), no. 12, 4503–4511. Zbl 1111.14023 MR 2273720

[11] M. Kanazawa – T. Takahashi – H. Yoshihara, The group generated by automorphisms belonging to Galois points of the quartic surface. *Nihonkai Math. J.* **12** (2001), no. 1, 89–99. Zbl 1077.14548 MR 1833745

[12] G. Korchmáros – S. Lia – M. Timpanella, Curves with more than one inner Galois point. *J. Algebra* **566** (2021), 374–404. Zbl 1457.14072 MR 4152768

[13] K. Miura – A. Ohbuchi, Automorphism group of plane curve computed by Galois points. *Beitr. Algebra Geom.* **56** (2015), no. 2, 695–702. Zbl 1327.14145 MR 3391197

[14] K. Miura – H. Yoshihara, Field theory for function fields of plane quartic curves. *J. Algebra* **226** (2000), no. 1, 283–294. Zbl 0983.11067 MR 1749889

[15] H. Stichtenoth, *Algebraic function fields and codes*. Universitext, Springer, Berlin, 1993. Zbl 0816.14011 MR 1251961

[16] H. Yoshihara, Function field theory of plane curves by dual curves. *J. Algebra* **239** (2001), no. 1, 340–355. Zbl 1064.14023 MR 1827887

[17] H. Yoshihara – S. Fukasawa, List of problems, https://sites.google.com/sci.kj.yamagata-u.ac.jp/fukasawa-lab/open-questions-english.

Manoscritto pervenuto in redazione il 2 dicembre 2020.