Journal of Algebra 511 (2018) 95–101

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

A birational embedding of an algebraic curve into a projective plane with two Galois points

Satoru Fukasawa [1]

Department of Mathematical Sciences, Faculty of Science, Yamagata University, Kojirakawa-machi 1-4-12, Yamagata 990-8560, Japan

ARTICLE INFO

Article history:
Received 23 October 2017
Available online 30 June 2018
Communicated by Kazuhiko Kurano

MSC:
14H50
14H05
14H37

Keywords:
Galois point
Plane curve
Galois group
Automorphism group

ABSTRACT

A criterion for the existence of a birational embedding of an algebraic curve into a projective plane with two Galois points is presented. Several novel examples of plane curves with two inner Galois points as an application are described.

1. Introduction

The notion of *Galois point* was introduced by Hisao Yoshihara in 1996, to investigate the function fields of algebraic curves ([5,9]). For about twenty years, many interesting results have been obtained by several authors (Yoshihara, Miura, Takahashi, Fukasawa, et al., see also [11]). One of the most interesting problems in the theory of Galois point is

E-mail address: s.fukasawa@sci.kj.yamagata-u.ac.jp.

[1] The author was partially supported by JSPS KAKENHI Grant Number 16K05088.

https://doi.org/10.1016/j.jalgebra.2018.06.020

to determine the number of Galois points for any plane curve. For smooth plane curves, the number of Galois points is completely determined ([3,9]). On the other hand, there are not so many known examples of (singular) plane curves with two Galois points (see the Tables in [11]). It is important to find a condition for the existence of two Galois points.

Let C be a (reduced, irreducible) smooth projective curve over an algebraically closed field k of characteristic $p \geq 0$ with $k(C)$ as its function field. We consider a rational map φ from C to $\mathbb{P}^2$, which is birational onto its image. For a point $P \in \mathbb{P}^2$, if the function field extension $k(\varphi(C))/\pi_P^* k(\mathbb{P}^1)$ induced by the projection π_P is Galois, then P is called a Galois point for $\varphi(C)$. Furthermore, if a Galois point P is a smooth point of $\varphi(C)$ (resp. is contained in $\mathbb{P}^2 \setminus \varphi(C)$), then P is said to be inner (resp. outer). The associated Galois group at P is denoted by G_P.

The following proposition is presented after discussions with Takahashi [7], Terasoma [8] and Yoshihara [10].

Proposition 1. *Let C be a smooth projective curve. Assume that there exist two finite subgroups, G_1 and G_2, of the full automorphism group* $\mathrm{Aut}(C)$ *such that $G_1 \cap G_2 = \{1\}$ and $C/G_i \cong \mathbb{P}^1$ for $i = 1, 2$. Let f and g be generators of function fields of C/G_1 and C/G_2, respectively. Then, the rational map*

$$\varphi : C \dashrightarrow \mathbb{P}^2; \ (f : g : 1)$$

is birational onto its image, and two points $P_1 = (0 : 1 : 0)$ and $P_2 = (1 : 0 : 0)$ are Galois points for $\varphi(C)$.

For both points P_1 and P_2 to be inner, or outer, we need additional conditions. In this article, we present the following criterion.

Theorem 1. *Let C be a smooth projective curve and let G_1 and G_2 be different finite subgroups of* $\mathrm{Aut}(C)$. *Then, there exist a morphism $\varphi : C \to \mathbb{P}^2$ and different inner Galois points $\varphi(P_1)$ and $\varphi(P_2) \in \varphi(C)$ such that φ is birational onto its image and $G_{\varphi(P_i)} = G_i$ for $i = 1, 2$, if and only if the following conditions are satisfied.*

(a) *$C/G_1 \cong \mathbb{P}^1$ and $C/G_2 \cong \mathbb{P}^1$.*
(b) *$G_1 \cap G_2 = \{1\}$.*
(c) *There exist two different points P_1 and $P_2 \in C$ such that*

$$P_1 + \sum_{\sigma \in G_1} \sigma(P_2) = P_2 + \sum_{\tau \in G_2} \tau(P_1)$$

as divisors.

Remark 1. For outer Galois points, we have to replace (c) by

(c') There exists a point $Q \in C$ such that $\sum_{\sigma \in G_1} \sigma(Q) = \sum_{\tau \in G_2} \tau(Q)$ as divisors.

We present the following application for rational or elliptic curves.

Theorem 2. *Let $p \neq 2$. Then, there exist the following morphisms $\varphi : \mathbb{P}^1 \to \mathbb{P}^2$, which are birational onto their images.*

(1) $\deg \varphi(C) = 5$ *and there exist two Galois points $\varphi(P_1)$ and $\varphi(P_2) \in \varphi(C)$ such that $G_{\varphi(P_i)} \cong \mathbb{Z}/4\mathbb{Z}$ for $i = 1, 2$, if $p \neq 3$.*
(2) $\deg \varphi(C) = 5$ *and there exist two Galois points $\varphi(P_1)$ and $\varphi(P_2) \in \varphi(C)$ such that $G_{\varphi(P_i)} \cong (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$ for $i = 1, 2$.*
(3) $\deg \varphi(C) = 5$ *and there exist two Galois points $\varphi(P_1)$ and $\varphi(P_2) \in \varphi(C)$ such that $G_{\varphi(P_1)} \cong \mathbb{Z}/4\mathbb{Z}$ and $G_{\varphi(P_2)} \cong (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$.*
(4) $\deg \varphi(C) = 6$ *and there exist two Galois points $\varphi(P_1)$ and $\varphi(P_2) \in \varphi(C)$ such that $G_{\varphi(P_i)} \cong \mathbb{Z}/5\mathbb{Z}$ for $i = 1, 2$.*

Theorem 3. *Let $p \neq 3$ and let $E \subset \mathbb{P}^2$ be the curve defined by $X^3 + Y^3 + Z^3 = 0$. Then, there exists a morphism $\varphi : E \to \mathbb{P}^2$ such that φ is birational onto its image,* $\deg \varphi(E) = 4$, *and there exist two inner Galois points for $\varphi(E)$.*

2. Proof of the main theorem

Proof of Proposition 1. Let $P_1 = (0 : 1 : 0)$ and $P_2 = (1 : 0 : 0)$. Then, the projection π_{P_1} (resp. π_{P_2}) is given by $(x : y : 1) \mapsto (x : 1)$ (resp. $(x : y : 1) \mapsto (y : 1)$), and hence, $\pi_{P_1} \circ \varphi = (f : 1)$ (resp. $\pi_{P_2} \circ \varphi = (g : 1)$). We have to only show that $k(C) = k(f, g)$. Since $k(C)/k(f)$ is Galois, there exists a subgroup H_1 of G_1 such that $H_1 = \mathrm{Gal}(k(C)/k(f, g))$. Similarly, there exists a subgroup H_2 of G_2 such that $H_2 = \mathrm{Gal}(k(C)/k(f, g))$. Since $G_1 \cap G_2 = \{1\}$, $H_1 = H_2 = \{1\}$. Therefore, $k(C) = k(f, g)$. □

Proof of Theorem 1. We consider the only-if part. Let $\varphi(P_1)$ and $\varphi(P_2) \in \varphi(C)$ be inner Galois points such that $G_{\varphi(P_i)} = G_i$ for $i = 1, 2$. Assertion (a) is obvious. To prove (b), we take a suitable system of coordinates so that $\varphi(P_1) = (0 : 1 : 0)$ and $\varphi(P_2) = (1 : 0 : 0)$. Then, $k(C)^{G_1} = k(x)$ and $k(C)^{G_2} = k(y)$. For $\sigma \in G_1 \cap G_2$, $\sigma^*(x) = x$ and $\sigma^*(y) = y$. Since $k(C) = k(x, y)$, $\sigma = 1$. Assertion (b) follows (see also [1, Lema 3.2] and [2, Lemma 7]). Let D be the divisor induced by the intersection of $\varphi(C)$ and the line $\overline{\varphi(P_1)\varphi(P_2)}$, where $\overline{\varphi(P_1)\varphi(P_2)}$ is the line passing through $\varphi(P_1)$ and $\varphi(P_2)$. We can consider the line $\overline{\varphi(P_1)\varphi(P_2)}$ as a point in the images of $\pi_{P_1} \circ \varphi$ and $\pi_{P_2} \circ \varphi$. Since $\pi_{P_1} \circ \varphi$ (resp. $\pi_2 \circ \varphi$) is a Galois covering and $P_2 \in \varphi^{-1}(\varphi(C) \cap \overline{\varphi(P_1)\varphi(P_2)})$ (resp. $P_1 \in \varphi^{-1}(\varphi(C) \cap \overline{\varphi(P_1)\varphi(P_2)})$),

$$(\pi_{P_1} \circ \varphi)^*(\overline{\varphi(P_1)\varphi(P_2)}) = \sum_{\sigma \in G_1} \sigma(P_2) \quad \left(\text{resp. } (\pi_{P_2} \circ \varphi)^*(\overline{\varphi(P_1)\varphi(P_2)}) = \sum_{\tau \in G_2} \tau(P_1)\right)$$

as divisors (see, for example, [6, III.7.1, III.7.2, III.8.2]). On the other hand, it follows that $(\pi_{P_1} \circ \varphi)^*(\overline{\varphi(P_1)\varphi(P_2)}) = D - P_1$ (resp. $(\pi_{P_2} \circ \varphi)^*(\overline{\varphi(P_1)\varphi(P_2)}) = D - P_2$). Therefore,

$$D = P_1 + \sum_{\sigma \in G_1} \sigma(P_2) = P_2 + \sum_{\tau \in G_2} \tau(P_1),$$

which is nothing but assertion (c).

We then consider the if-part. Let D be the divisor

$$D = P_1 + \sum_{\sigma \in G_1} \sigma(P_2) = P_2 + \sum_{\tau \in G_2} \tau(P_1),$$

by (c). Let f and $g \in k(C)$ be generators of $k(C/G_1)$ and $k(C/G_2)$ such that $(f)_\infty = D - P_1$ and $(g)_\infty = D - P_2$, by (a), where $(f)_\infty$ is the pole divisor of f. Then, $f, g \in \mathcal{L}(D)$. Let $\varphi : C \to \mathbb{P}^2$ be given by $(f : g : 1)$. Similar to Proposition 1, by (b), φ is birational onto its image. The sublinear system of $|D|$ corresponding to $\langle f, g, 1\rangle$ is base-point-free, since $\mathrm{supp}(D) \cap \mathrm{supp}((f) + D) = \{P_1\}$ and $\mathrm{supp}(D) \cap \mathrm{supp}((g) + D) = \{P_2\}$. Therefore, $\deg \varphi(C) = \deg D$, and the morphism $(f : 1)$ (resp. $(g : 1)$) coincides with the projection from the smooth point $\varphi(P_1) \in \varphi(C)$ (resp. $\varphi(P_2) \in \varphi(C)$). $\square$

3. Applications

First, we consider rational curves. In this case, condition (a) in Theorem 1 is always satisfied, by Lüroth's theorem.

Proof of Theorem 2. (1). Let $\sigma, \tau \in \mathrm{Aut}(\mathbb{P}^1)$ be represented by

$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -\frac{1}{2} & 1 \end{pmatrix}$$

respectively, by assuming $p \neq 2$. Let $G_1 = \langle \sigma \rangle$, $G_2 = \langle \tau \rangle$, $P_1 = (2 : 1)$ and $P_2 = (-1 : 1)$. If $p \neq 3$, then $P_1 \neq P_2$. Note that

$$\{\sigma^i(P_2) | i = 1, 2, 3\} = \{(1 : 0), (1 : 1), (0 : 1)\} = \{\tau^i(P_1) | i = 1, 2, 3\}.$$

Condition (c) in Theorem 1 is satisfied. Furthermore, $\sigma^4 = 1$ and $\tau^4 = 1$. We prove condition (b) in Theorem 1. Assume by contradiction that $\sigma^i = \tau^j$ for some i, j. If $i = 1$ or 3, then there exists an integer l such that $(\sigma^i)^l = \sigma$. Then, $\tau^{jl}(0 : 1) = \sigma(0 : 1) = (-1 : 1)$. However, there exists no integer i such that $\tau^i(0 : 1) = (-1 : 1)$. This is a contradiction. Therefore, $i = 2$ and $j = 2$. However, $\sigma^2(1 : 0) = (0 : 1) \neq (1 : 1) = \tau^2(1 : 0)$.

(2). Let $\alpha \neq 0, 1, -1$ and let $\sigma_\alpha, \tau_\alpha \in \mathrm{Aut}(\mathbb{P}^1)$ be represented by

$$\begin{pmatrix} 0 & 1 \\ \alpha & 0 \end{pmatrix}, \begin{pmatrix} 1 & -\frac{1}{\alpha} \\ 1 & -1 \end{pmatrix},$$

respectively. Let $G_\alpha = \langle \sigma_\alpha, \tau_\alpha \rangle$. Since $\sigma_\alpha \tau_\alpha = \tau_\alpha \sigma_\alpha$, $G_\alpha \cong (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$. We take $\alpha' \neq 0, 1, -1, \alpha$. Let $G_1 = G_\alpha$, $G_2 = G_{\alpha'}$, $P_1 = (1 : \alpha')$ and $P_2 = (1 : \alpha)$. Note that

$$\{\sigma_\alpha(P_2), \tau_\alpha(P_2), \sigma_\alpha\tau_\alpha(P_2)\} = \{(1:1), (0:1), (1:0)\} = \{\sigma_{\alpha'}(P_1), \tau_{\alpha'}(P_1), \sigma_{\alpha'}\tau_{\alpha'}(P_1)\}.$$

Condition (c) in Theorem 1 is satisfied. Condition (b) is obviously satisfied in this case.

(3). We take σ as in (1) and $\sigma_\alpha, \tau_\alpha$ as in (2). Let $P_1 = (1 : \alpha)$ and $P_2 = (1 : -1)$. Note that

$$\{\sigma^i(P_2) | i = 1, 2, 3\} = \{(1:0), (1:1), (0:1)\} = \{\sigma_\alpha(P_1), \tau_\alpha(P_1), \sigma_\alpha\tau_\alpha(P_1)\}.$$

Furthermore, $\sigma^2 \notin \langle \sigma_\alpha, \tau_\alpha \rangle$. Similar to the proof of (2), the assertion follows by Theorem 1.

(4). Let $\alpha^2 + \alpha - 1 = 0$ and let $\sigma, \tau \in \mathrm{Aut}(\mathbb{P}^1)$ be represented by

$$\begin{pmatrix} 1 & -1 \\ 1 & -\alpha \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ \alpha - 1 & 1 \end{pmatrix}$$

respectively. Let $G_1 = \langle \sigma \rangle$, $G_2 = \langle \tau \rangle$, $P_1 = (\alpha : 2\alpha - 1)$ and $P_2 = (1 : 1 + \alpha)$. If $p \neq 2$, then $P_1 \neq P_2$. Note that

$$\{\sigma^i(P_2) | 1 \le i \le 4\} = \{(1:0), (0:1), (1:1), (1:\alpha)\} = \{\tau^i(P_1) | 1 \le i \le 4\}.$$

Condition (c) in Theorem 1 is satisfied. Furthermore, $\sigma^5 = 1$ and $\tau^5 = 1$. Condition (b) is obviously satisfied. □

Remark 2. Let σ and $\tau \in \mathrm{Aut}(\mathbb{P}^1)$ be as in the proof of Theorem 2(1). Let $f := \sum_{i=0}^{3} \sigma^*(t) \in k(\mathbb{P}^1) = k(t)$ and let $g := \sum_{i=0}^{3} \tau^*(t) \in k(t)$. Then, $f \in k(\mathbb{P}^1/\langle\sigma\rangle)$, $g \in k(\mathbb{P}^1/\langle\tau\rangle)$, and

$$f = t - \frac{t+1}{t-1} - \frac{1}{t} + \frac{t-1}{t+1} = \frac{t^4 - 6t^2 + 1}{t(t-1)(t+1)},$$
$$g = t + \frac{2t-1}{2t} + \frac{t-1}{2t-1} - \frac{1}{2t-2} = \frac{4t^4 - 12t^2 + 8t - 1}{2t(t-1)(2t-1)}.$$

The birational embedding $\varphi = (f : g : 1) : \mathbb{P}^1 \to \mathbb{P}^2$ is represented by

$$(2(t^4 - 6t^2 + 1)(2t - 1) : (4t^4 - 12t^2 + 8t - 1)(t + 1) : 2t(t + 1)(t - 1)(2t - 1)).$$

For Theorem 2(2),

$$f = t + \sigma_\alpha^*(t) + \tau_\alpha^*(t) + (\sigma_\alpha\tau_\alpha)^*(t) = t + \frac{\alpha}{t} + \frac{\alpha(t-1)}{t-\alpha} + \frac{t-\alpha}{t-1} = \frac{(t^2-\alpha)^2}{t(t-1)(t-\alpha)}$$

and we have a birational embedding

$$((t^2-\alpha)^2(t-\alpha') : (t^2-\alpha')^2(t-\alpha) : t(t-1)(t-\alpha)(t-\alpha')).$$

Remark 3. According to [4, Theorem 1], if $p = 0$, $C = \mathbb{P}^1$ and $\deg\varphi(C) = 6$, then the number of inner Galois points is bounded by two. Our curve in Theorem 2(4) attains this bound.

Next, we consider elliptic curves. Let $p \neq 3$. Note that if an elliptic curve E admits a Galois covering ψ over $\mathbb{P}^1$ of degree three, then E has an embedding $\varphi : E \to \mathbb{P}^2$ such that the image is the Fermat cubic.

We prove it here. Let Q be a (total) ramification point of ψ. Then, $\psi^*(\psi(Q)) = 3Q$, the complete linear system $|3Q|$ is of dimension 2, and the induced morphism $\varphi_{|3Q|} : E \to \mathbb{P}^2$ is an embedding. Since ψ corresponds to some (base-point-free) sublinear system of $|3Q|$, ψ is considered as the projection from some point $P \in \mathbb{P}^2 \setminus \varphi_{|3Q|}(E)$. (This implies that P is an outer Galois point for $\varphi_{|3Q|}(E)$.) For a suitable system of coordinates, we can assume that $P = (1 : 0 : 0)$. Let $\sigma \in \mathrm{Aut}(E)$ be an automorphism of order three induced by ψ. Since $\sigma^*(3Q) = 3Q$, there exists a linear transformation η of $\mathbb{P}^2$ such that $\sigma = \varphi_{|3Q|}^{-1}\eta\varphi_{|3Q|}$. Note that $\varphi_{|3Q|}^*\eta^*(y) = \varphi_{|3Q|}^*(y)$. For a suitable system of coordinates, η is given by $(X : Y : Z) \mapsto (\omega X : Y : Z)$, where $w^2 + w + 1 = 0$ (see [9]). Then, $\varphi_{|3Q|}(E)$ is defined by $X^3 + G(Y, Z) = 0$ for some homogeneous polynomial $G \in k[Y, Z]$ of degree three. Since the action of $\mathrm{Aut}(\mathbb{P}^1) \cong \mathrm{PGL}(2, k)$ on the projective line defined by $X = 0$ is 3-transitive, we have the defining equation $X^3 + c(Y^3 + Z^3) = 0$ for some $c \in k \setminus \{0\}$. Therefore, $\varphi_{|3Q|}(E)$ coincides with the Fermat curve, up to a projective equivalence.

To consider the case where $\deg\varphi(E) = 4$, we assume that $E \subset \mathbb{P}^2$ is the curve defined by $X^3 + Y^3 + Z^3 = 0$.

Proof of Theorem 3. Let σ be the automorphism of E given by $(X : Y : Z) \mapsto (\omega X : Y : Z)$, where $\omega^2 + \omega + 1 = 0$. Then, σ is of order three and $E/\langle\sigma\rangle \cong \mathbb{P}^1$. We take a point $Q \in E \setminus \{XYZ = 0\}$ such that $\sigma(Q) \neq Q$ and $\sigma^2(Q) \neq Q$. Note that there exists an involution η such that $\eta(Q) = \sigma(Q)$, by the linear system $|Q + \sigma(Q)|$. We take $\tau := \eta\sigma^2\eta$. Then, $\tau(Q) = \sigma(Q)$, τ is of order three and $E/\langle\tau\rangle \cong \mathbb{P}^1$. Let $G_1 = \langle\sigma\rangle$ and $G_2 = \langle\tau\rangle$. Then, condition (a) in Theorem 1 is satisfied for G_1 and G_2. Furthermore, we take $P_1 = \tau^2(Q)$ and $P_2 = \sigma^2(Q)$. To prove (b) and (c) in Theorem 1, we have to only show that $\sigma^2(Q) \neq \tau^2(Q)$.

Assume by contradiction that $\tau^2(Q) = \sigma^2(Q)$. Then, $\eta(\sigma^2(Q)) = \sigma^2(Q)$, and hence, $\sigma^2(Q)$ is a ramification point of the double covering induced by $|Q + \sigma(Q)|$. It follows that $2\sigma^2(Q) \sim Q + \sigma(Q)$, and hence, $3\sigma^2(Q) \sim Q + \sigma(Q) + \sigma^2(Q) =: D$. Since D is given by $E \cap \overline{Q\sigma(Q)}$ and the linear system $|D|$ is complete, where $\overline{Q\sigma(Q)}$ is the line passing through Q and $\sigma(Q)$, $\sigma^2(Q)$ is a total inflection point. Then, Q is also a total inflection point, because σ is a linear transformation of $\mathbb{P}^2$. It is impossible because all total inflection points of this curve lie on the locus defined by $XYZ = 0$.

By Theorem 1, the assertion follows. □

Remark 4. According to [4, Theorem 1], if $p = 0$ and $\deg \varphi(C) = 4$, then the number of inner Galois points is bounded by four. When C is an elliptic curve, it is not known whether or not the bound is sharp.

Acknowledgments

The author is grateful to Professor Takeshi Takahashi, Professor Tomohide Terasoma and Professor Hisao Yoshihara for helpful conversations. The author thanks the referee for helpful comments, by which the latter half of the proof of Theorem 3 became simpler.

References

[1] C. Chacca, Classificação de curvas planas com infinitos pontos de Galois externos, Master thesis, Universidade Federal Fluminense, 2010 (in Portuguese).
[2] S. Fukasawa, Classification of plane curves with infinitely many Galois points, J. Math. Soc. Japan 63 (2011) 195–209.
[3] S. Fukasawa, Complete determination of the number of Galois points for a smooth plane curve, Rend. Semin. Mat. Univ. Padova 129 (2013) 93–113.
[4] K. Miura, Galois points on singular plane quartic curves, J. Algebra 287 (2005) 283–293.
[5] K. Miura, H. Yoshihara, Field theory for function fields of plane quartic curves, J. Algebra 226 (2000) 283–294.
[6] H. Stichtenoth, Algebraic Function Fields and Codes, Universitext, Springer-Verlag, Berlin, 1993.
[7] T. Takahashi, Private communications, July 2012 and September 2015.
[8] T. Terasoma, Private communications, September 2015.
[9] H. Yoshihara, Function field theory of plane curves by dual curves, J. Algebra 239 (2001) 340–355.
[10] H. Yoshihara, Rational Galois subfields, May 2008, unpublished.
[11] H. Yoshihara, S. Fukasawa, List of problems, available at: http://hyoshihara.web.fc2.com/openquestion.html.