Nihonkai Math. J.
Vol.17(2006), 103-110

GALOIS POINTS ON QUARTIC CURVES IN CHARACTERISTIC 3

SATORU FUKASAWA

ABSTRACT. We study Galois points for a smooth quartic curve $C \subset \mathbf{P}^2$ in characteristic 3. If C has the separable dual map onto its dual, then we have $\delta(C)+\delta'(C)\le 1$, where $\delta(C)$ (resp. $\delta'(C)$) is the number of inner (resp. outer) Galois points for C. On the other hand, the condition $\delta(C)+\delta'(C)>1$ gives a characterization of the Fermat curve $X^4+Y^4+Z^4=0$.

1. INTRODUCTION

A *Galois point* $P \in \mathbf{P}^2$ for a plane smooth curve $C \subset \mathbf{P}^2$ of degree ≥ 4 is a point at which the point projection $\pi_P : C \to \mathbf{P}^1$ induces a Galois extension $k(\mathbf{P}^1) \subset k(C)$ of function fields. We call the Galois point $P \in \mathbf{P}^2$ an inner (resp. outer) Galois point for C if $P \in C$ (resp. $P \notin C$). These concepts were introduced by K. Miura and H. Yoshihara ([3], [6]). Galois points have been studied mainly in characteristic 0. If we denote by $\delta(C)$ (resp. $\delta'(C)$) the number of inner (resp. outer) Galois points for C, then it is known that $\delta(C)=0,1$ or 4 and $\delta'(C)=0,1$ or 3 in characteristic 0 ([3], [6]). Recently, the first result on Galois points in positive characteristic p case was given by M. Homma ([1]). He studied Galois points on Hermitian curves (of degree $q+1$) over the algebraic closure of the finite field $\mathbf{F}_{q^2}$, where q is a power of p, and found that such curves have many inner and outer Galois points, hence $\delta(C)\le 4$ and $\delta'(C)\le 3$ fail for Hermitian curves (of degree ≥ 4). Let $(X:Y:Z)$ be a set of homogeneous coordinates on $\mathbf{P}^2$. Then we note that the Hermitian curve over $\mathbf{F}_{q^2}$ is projectively equivalent to the Fermat curve $X^{q+1}+Y^{q+1}+Z^{q+1}=0$ (over the algebraic closure of $\mathbf{F}_{q^2}$) and has the inseparable dual map onto its dual ([2], [4]). (A plane curve is called reflexive if the dual map is separable onto its dual ([2]).)

2000 *Mathematics Subject Classification.* 12F10, 14H50.
Key words and phrases. Galois point, quartic curve, positive characteristic.

In this paper we study Galois points on smooth quartic curves in characteristic 3, and clarify the distribution of Galois points. The separable case of dual map is contained. Our results are as follows.

Theorem 1. *Let $C \subset \mathbf{P}^2$ be a smooth curve of degree 4 over an algebraically closed field of characteristic 3. If the dual map of C is separable onto its dual curve, then we have*

$$\delta(C) + \delta'(C) \leq 1.$$

Theorem 2. *Under the same assumption as in Theorem 1 we have that $\delta(C) + \delta'(C) > 1$ if and only if C is projectively equivalent to the Fermat curve $X^4 + Y^4 + Z^4 = 0$.*

Under the same assumption as above, if we use Pardini's theorem ([4, Proposition 3.7]) and Homma's result, then we infer readily Theorem 2. However, our proof does not depend on their results.

2. Preliminaries

We will use only classical methods of plane algebraic curves and Galois theory. We recall some basic notions.

Let $C \subset \mathbf{P}^2$ be a smooth projective plane curve over an algebraically closed field k of characteristic $p \geq 0$ and let $k(C)$ be its function field. The *dual map* (or Gauss map) $\gamma : C \to \mathbf{P}^{2*}$ is a morphism which assigns to a point $P \in C$ its (projective) tangent line T_PC, hence if F is the defining polynomial then $\gamma = (\partial F/\partial X : \partial F/\partial Y : \partial F/\partial Z)$. We call $\gamma(C) \subset \mathbf{P}^{2*}$ the *dual curve*, denoted by C^*. If x is a local coordinate on C with coordinates (x, y), then the dual map is given by $\gamma = (-dy/dx : 1 : -y + xdy/dx)$ and, hence the dual map is separable if and only if $\dfrac{d}{dx}\left(\dfrac{dy}{dx}\right)$ is not 0 as an element of $k(C)$. For a point $P \in C$, if the intersection multiplicity of C and T_PC at P is ≥ 3, we call P a *flex*, and if the multiplicity $= 3$ (resp. 4), we call P a 1-flex (resp. 2-flex) ([3], [5]).

We have a well-known criterion that a point to be a flex in characteristic $p \neq 2$. If $f(x, y)$ is the defining polynomial of an affine part of C, then $P \in C$ is a flex if and only if the rank of the matrix

$$h(f) = \begin{pmatrix} f_{xx} & f_{xy} & f_x \\ f_{xy} & f_{yy} & f_y \\ f_x & f_y & 0 \end{pmatrix}$$

is not 3 at P ([5]). If $f_y \neq 0$ at some smooth point, then x is a local coordinate. By the calculation of differentials, we have $\dfrac{d}{dx}\left(\dfrac{dy}{dx}\right) = \dfrac{\det h(f)}{f_y^3}$. Therefore, the dual map is inseparable if and only if $\det h(f)$ is identically zero.

3. Quartic curves with Galois points

In this section, let a curve $C \subset \mathbf{P}^2$ mean a smooth curve (of degree 4) over an algebraically closed field of characteristic 3. For inner Galois points, we have the following proposition.

Proposition 1. *A quartic curve C has an inner Galois point if and only if C is projectively equivalent to the curve defined by either of the following two forms:*

(a) $X^3Z - XZ^3 + Y^4 + a_3Y^3Z + a_2Y^2Z^2 + a_1YZ^3$,
(b) $X^3Y - XYZ^2 + a_3Y^3Z + a_2Y^2Z^2 + a_1YZ^3 + Z^4$,

where a_i $(i = 1, 2, 3)$ are constants and in the case (b), $a_3 \neq 0$. Furthermore, the dual map of C is inseparable onto its dual if and only if C is in the case (a) with $a_2 = 0$.

Proof. Let $P = (1 : 0 : 0) \in C$. Since the point projection π_P is expressed as $\pi_P(X, Y, Z) = (Y : Z)$, $\pi_P(x, y, 1) = (y : 1)$ in the affine part $Z \neq 0$, where $x = X/Z$ and $y = Y/Z$. Then we have the field extension $k(x, y)/k(y)$ where x is algebraic over $k(y)$. We assume that P is an inner Galois point. Let G_P be the Galois group of the Galois extension $k(x, y)/k(y)$. Now G_P is a cyclic group of order 3. For an automorphism $\sigma \in G_P$, we have the automorphism $\phi : C \to C$ such that $\phi = (\sigma(x) : \sigma(y) : 1)$. The embedding of a smooth curve of degree 4 in $\mathbf{P}^2$ is canonical, hence any automorphism on C is a linear transformation. Hence ϕ is a linear transformation. Let $A_\sigma = (a_{ij})$ be a matrix which represents ϕ. Now $\sigma(y) = y$, hence $f := (a_{21}x + a_{22}y + a_{23}) - (a_{31}x + a_{32}y + a_{33})y$ is zero on C. By considering the degree of f, f must be 0 as a polynomial. This implies that $a_{21} = a_{23} = a_{31} = a_{32} = 0$

and $a_{22} = a_{33}$. We may assume $a_{22} = a_{33} = 1$. Since A_σ^3 is the unit matrix, we have $a_{11} = 1$. Let $a_{12} = a$ and $a_{13} = b$. Now we have a linear transform ψ such that $\psi(X, Y, Z) = (X : Z : aY + bZ)$ if $a \neq 0$ or $\psi = (X : Y : aY + bZ)$ if $b \neq 0$. Then $\psi(P) = P$ and $\psi\sigma\psi^{-1}$ is expressed as the following matrix:

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence we may assume $\sigma(x) = x + 1$. Then, $x^3 - x = x(x+1)(x+2) \in k(y)$. We can write $x^3 - x = g/h$ where $g(y), h(y)$ are polynomials. Because the degree of C is 4, g has the degree ≤ 4 and h has the degree 0 or 1. If h has the degree 0, then we have the form (a). If h has the degree 1, then we may assume $h = y$, hence we have the form (b).

We prove the second assertion. In the case (a), we have the equation $f_1(x, y) = x^3 - x + y^4 + a_3y^3 + a_2y^2 + a_1y$ if $Z \neq 0$. Then we have

$$h(f_1) = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 2a_2 & y^3 + 2a_2y + a_1 \\ -1 & y^3 + 2a_2y + a_1 & 0 \end{pmatrix}$$

and $\det h(f_1) = a_2$. In the case (b), we have the equation $f_2(x, z) = x^3 - xz^2 + a_3z + a_2z^2 + a_1z^3 + z^4 = 0$ if $Y \neq 0$. Then we have

$$h(f_2) = \begin{pmatrix} 0 & z & -z^2 \\ z & x + 2a_2 & xz + a_3 + 2a_2z + z^3 \\ -z^2 & xz + a_3 + 2a_2z + z^3 & 0 \end{pmatrix}$$

and $\det h(f_2) = z^3(a_3 + z^3)$. We have that $\det h(f_1)$ is identically zero if and only if $a_2 = 0$, and $\det h(f_2)$ is always a nonzero polynomial. We complete the proof. $\square$

We have determined the defining polynomial. As an application, we have the following:

Corollary 1. *An inner Galois point on a quartic curve C is a 2-flex. Furthermore, if C has the separable dual map onto its dual and an inner Galois point, then $\delta(C) = 1$ and the number of the flexes on C is 1 or 5.*

Proof. The first assertion is easy, because the tangent line of C given in the case (a) (resp. (b)) at $P = (1:0:0)$ is $Z = 0$ (resp. $Y = 0$), hence the tangent line at P intersects C only at P.

Now, we find flexes and Galois points on C given in the case (a). Since the line $Z = 0$ and C intersect only at P, if $Z \neq 0$, then C has the defining polynomial $f_1(x, y) = x^3 - x + y^4 + a_3y^3 + a_2y^2 + a_1y$ (same as in the proof of Proposition 1). As in the proof of Proposition 1, we have $\det h(f_1) = a_2 \neq 0$, owing to the assumption. This implies that there do not exist flexes on C with $Z \neq 0$, hence C has only one inner Galois point.

Next we find flexes and Galois points on C given in the case (b). Let $Y \neq 0$, we have $f_2(x, z) = x^3 - xz^2 + a_3z + a_2z^2 + a_1z^3 + z^4$. As we saw the proof of Proposition 1, we have $\det h(f_2) = z^3(a_3 + z^3)$. If $z = 0$, then we have $x = 0$. If $z = \sqrt[3]{-a_3}$, then we have $x^3 - (\sqrt[3]{-a_3})^2x + a_2(\sqrt[3]{-a_3})^2 - a_1a_3 = 0$ and this has three roots. Hence we have just five flexes on C. We note that the point $Q = (0:1:0)$ is a 1-flex and the tangent line at Q is $Z = 0$ which contains P. The three points given by $z = \sqrt[3]{-a_3}$ can not be Galois points, because for each of such a point P' there does not exist a flex at which the tangent line contains P'. Hence a curve C with (b) has only one Galois point. $\square$

Example. *We consider the curves given by* $F = X^3Y - XYZ^2 + Y^3Z + Z^4$ *and* $G = X^3Y - XYZ^2 + (Y + Z)^4$. *These are of the form (b). We can easily check that the curve given by F (resp. G) has only one Galois point and four* 1*-flexes (resp.* 2*-flexes). The* 2*-flexes, which are not the point* $(1:0:0)$, *on the curve given by G are not Galois points.*

Concerning outer Galois points we have the following proposition:

Proposition 2. *A quartic curve C has an outer Galois point if and only if C is projectively equivalent to the curve given by*

(c) $X^4 + Y^3Z + a_2Y^2Z^2 + YZ^3$,

where $a_2 \in k \setminus \{-1, 1\}$. Furthermore, the dual map of C is inseparable onto its dual if and only if $a_2 = 0$.

Proof. Let $P = (1:0:0) \in \mathbf{P}^2 \setminus C$. $\pi_P(x, y, 1) = (y : 1)$ in the affine part $Z \neq 0$, where $x = X/Z$ and $y = Y/Z$. We assume that P is an outer Galois point. Let G_P be the Galois group of the Galois extension $k(x, y)/k(y)$, which has the order 4. For an automorphism $\sigma \in G_P$, we have the automorphism $\phi : C \to C$, this is a linear transformation because the embedding of C in $\mathbf{P}^2$ is canonical. Let $A_\sigma = (a_{ij})$ be a 3×3 matrix representing ϕ. As in the proof of Proposition 1, $a_{21} = a_{23} = a_{31} = a_{32} = 0$ and $a_{22} = a_{33}$. Let $a_{22} = a_{33} = 1$. If $a_{11} = 1$ then $a_{12} = a_{13} = 0$ because the $(1, 2)$-element of A_σ^4 is $4a_{12} = a_{12}$. Therefore we can take an injective group homomorphism $\det : G_P \to k \setminus 0$, hence G_P is a cyclic group of order 4. We assume $\sigma \in G_P$ is a generator, then we have $a_{11} = \zeta$ which is a primitive fourth root of unity. Now A_σ has eigenvalues ζ and 1, and is diagonalizable. Therefore, there exists a linear transformation ψ, expressed as a matrix Q, such that $\psi(P) = P$ and

$$QA_\sigma Q^{-1} = \begin{pmatrix} \zeta & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence we may assume $\sigma(x) = \zeta x$. Then $x^4 \in k(y)$, hence we write $x^4 + g = 0$ where g is a polynomial of degree ≤ 4. We have the projective form $X^4 + a_4Y^4 + a_3Y^3Z + a_2Y^2Z^2 + a_1YZ^3 + a_0Z^4$ as the defining polynomial of C. For a suitable coordinate, we have $X^4 + a_3Y^3Z + a_2Y^2Z^2 + a_1YZ^3$. By the smoothness of C we have the condition $a_3, a_1 \neq 0$, which implies that the polynomial is projectively equivalent to $X^4 + Y^3Z + a_2Y^2Z^2 + YZ^3$.

We prove that the condition $a_2 = 0$ in (c) is equivalent to the inseparability of the dual map onto its dual. Let $f_3(x, y) = x^4 + y^3 + a_2y^2 + y$. By easy computations, we have $\det h(f_3) = a_2x^6$, hence $\det h(f_3)$ is zero polynomial if and only if $a_2 = 0$. We get the assertion. □

Remark 1. *The result that the Galois group induced from an outer Galois point for a smooth curve of degree* 4 *is a cyclic group of order* 4 *is also true for the case of characteristic* $p > 2$. *In our proof, the assumption that the characteristic* p *is* 3 *is used only for that the Galois group* G_P *has an injective homomorphism to* $k \setminus 0$, *which is derived from that the characteristic* p *does not divide* 4.

Corollary 2. *If a quartic curve C has the separable dual map onto its dual and an outer Galois point P, then we have just four flexes on C, and the tangent line of C at each flex contains P. Therefore the number of outer Galois points is at most one.*

Proof. We investigate the flexes of $f_3(x, y) = x^4 + y^3 + a_2y^2 + y = 0$ and $f_4(x, z) = x^4 + z + a_2z^2 + z^3 = 0$. By easy computations, we have $\det h(f_3) = \det h(f_4) = a_2x^6$. Therefore we have just four flexes which lie in $X = 0$. We return to the homogeneous equation $F = X^4 + Y^3Z + a_2Y^2Z^2 + YZ^3$. For each flex Q, the tangent line at Q is given by $\frac{\partial F}{\partial Y}(Q)Y + \frac{\partial F}{\partial Z}(Q)Z = 0$ because $\frac{\partial F}{\partial X}(Q) = X^3(Q) = 0$. The tangent line contains $P = (1 : 0 : 0)$. We complete the proof. □

Proof of Theorem 1. We note the number of flexes on C with Galois points. By the Corollaries 1 and 2, we have the assertion. □

Proof of Theorem 2. First, we prove that the forms given in the cases (a) with $a_2 = 0$ and (c) with $a_2 = 0$ are projectively equivalent to the curve defined by $X^4+Y^4+Z^4$.

We consider the case (a). If $a_3 = a_1 = 0$ then we have $X^3Z - XZ^3 + Y^4$, which is projectively equivalent to the Fermat curve. If not, we have $X^3Z-XZ^3+Y^4+a_3Y^3Z$ for a suitable coordinate. Let $\alpha \in k$ be an element such that $\alpha^9 + \alpha + a_3^3 = 0$, let c be the cubic root of α, and let β be an element such that $\beta^3 - \beta - c^4 = 0$. Let $\hat{X} = X - (\alpha Y + \beta Z)$ and $\hat{Y} = Y - cZ$. Then we have $\hat{X}^3Z - \hat{X}Z^3 + \hat{Y}^4 = 0$, which is projectively equivalent to the Fermat curve. In the case (b), it is easy.

By the above discussion, the Fermat curve $X^4 + Y^4 + Z^4 = 0$ has both inner and outer Galois points, hence $\delta(C) + \delta'(C) > 1$. Conversely, if $\delta(C) + \delta'(C) > 1$ then the dual map is inseparable by Theorem 1, hence Propositions 1, 2 and the above consideration imply that C is the Fermat curve. □

Remark 2. *The converse assertion of Theorem 1 is also true by Pardini's theorem (*[4, Proposition 3.7]*).*

Acknowledgements

The author expresses gratitude to Professor Kei Miura for helpful advice, one of which improved Theorem 1. The author thanks Professor Masaaki Homma for giving him the forthcoming paper [1]. The author is grateful to Professor Nobuyoshi Takahashi for telling him the gap of the proof of Proposition 1 in the first draft of this paper.

References

[1] Homma, M. Galois points for a Hermitian curve, Comm. Algebra (to appear).

[2] Kleiman, S. L. Tangency and duality, In: Proceedings of the 1984 Vancouver conference in algebraic geometry, CMS Conference Proceedings, **6**, Amer. Math. Soc., Providence, RI, 1986, pp.163–226.

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

[4] Pardini, R. Some remarks on plane curves over fields of finite characteristic, Compositio Math. **60** (1986), 3–17.

[5] Shafarevich, I. R. Basic algebraic geometry. 1. Varieties in projective space. Second edition. Springer-Verlag, Berlin, 1994.

[6] Yoshihara, H. Function field theory of plane curves by dual curves, J. Algebra **239**, 340-355 (2001).

Department of Mathematics, Graduate School of Science, Hiroshima University, Kagamiyama 1-3-1, Higashi-Hiroshima, 739-8526, Japan.

E-mail address: `sfuka@hiroshima-u.ac.jp`

Received June 5, 2006
Revised June 19, 2006