Nihonkai Math. J.
Vol.25(2014), 69–75

AUTOMORPHISM GROUPS OF SMOOTH PLANE CURVES WITH MANY GALOIS POINTS

SATORU FUKASAWA

ABSTRACT. We describe the automorphism groups of curves appearing in a classification list of smooth plane curves with at least two Galois points. One of them is an ordinary curve whose automorphism group exceeds the Hurwitz bound.

1. Introduction

Let the base field K be an algebraically closed field of characteristic $p = 2$ and let $q = 2^e \geq 4$. We consider smooth plane curves given by

$$Z \prod_{\alpha \in \mathbb{F}_q} (X + \alpha Y + \alpha^2 Z) + \lambda Y^{q+1} = 0, \qquad (*)$$

or

$$(X^2 + XZ)^2 + (X^2 + XZ)(Y^2 + YZ) + (Y^2 + YZ)^2 + \lambda Z^4 = 0, \qquad (**)$$

where $\lambda \in K \setminus \{0, 1\}$. These curves appear in the classification list of smooth plane curves with at least two Galois points ([4, Theorem 3], see [12, 17] for definition of Galois point). The automorphism groups of other curves (Fermat, Klein quartic and the curve $x^3 + y^4 + 1 = 0$) in the list were studied by many authors (see, for example, [6, 8, 10, 14]). In this paper, we describe the automorphism groups of these curves, as follows.

Theorem 1.1. *Let C be the plane curve given by $(*)$ of degree $q + 1$ and genus $g_C = q(q-1)/2$. Then,* $\mathrm{Aut}(C) \cong \mathrm{PGL}(2, \mathbb{F}_q)$. *In particular,* $|\mathrm{Aut}(C)| = q^3 - q$ *and* $> 84(g_C - 1)$ *if* $q \geq 64$.

Theorem 1.2. *Let C be the plane curve given by $(**)$ of degree four. Then,* $\mathrm{Aut}(C)$ *is isomorphic to the symmetric group S_4 of degree four. In particular,* $|\mathrm{Aut}(C)| = 24$.

2010 *Mathematics Subject Classification.* Primary 14H37, 14H50; Secondary 12F10.
Key words and phrases. smooth plane curve, automorphism group, positive characteristic, ordinary curve, Galois point.
The author was partially supported by JSPS KAKENHI Grant Number 25800002.

It is well known that the order of the automorphism group of any curve with genus $g_C > 1$ is bounded by $84(g_C - 1)$ in characteristic zero, by Hurwitz. Our curve given by $(*)$ is an ordinary curve whose automorphism group exceeds the Hurwitz bound (see Remark 2.1). This is different from the examples of Subrao [16] and of Nakajima [13] by the genera.

Our theorems are proved by considering the Galois groups at Galois points. Therefore, our study is related to the results of Kanazawa, Takahashi and Yoshihara [9], Miura and Ohbuchi [11].

2. Proof of Theorem 1.1

According to [1, Appendix A, 17 and 18] or [2], any automorphism of smooth plane curves of degree at least four is the restriction of a linear transformation. Therefore, we have an injection

$$\mathrm{Aut}(C) \hookrightarrow \mathrm{PGL}(3, K).$$

Let L_Y be the line given by $Y = 0$, and let $P_1 = (1 : 0 : 0)$ and $P_2 = (0 : 0 : 1)$. A point $P \in \mathbb{P}^2$ is said to be Galois, if the field extension induced by the projection π_P from P is Galois. If P is a Galois point, then we denote by G_P the Galois group. For $\gamma \in \mathrm{Aut}(C)$, we denote the set $\{Q \in \mathbb{P}^2 \mid \gamma(Q) = Q\}$ by L_γ. We have the following properties for curves with $(*)$ (see also [4]).

Proposition 2.1. *Let C be the plane curve given by $(*)$. Then, we have the following.*

(a) *$C \cap L_Y = L_Y(\mathbb{F}_q)$, where $L_Y(\mathbb{F}_q)$ is the set of $\mathbb{F}_q$-rational points of L_Y. We denote by $L_Y(\mathbb{F}_q) = \{P_1, \ldots, P_{q+1}\}$.*

(b) *The set of Galois points on C coincides with $L_Y(\mathbb{F}_q)$.*

(c) *For the projection π_{P_1} from P_1, the ramification index at P_1 is q and there exist exactly $(q-1)$ lines ℓ such that the ramification index at each point of $C \cap \ell$ is equal to two. Furthermore, $\sigma(P_1) = P_1$ for any $\sigma \in G_{P_1}$.*

(d) *If i, j, k are different, then there exists $\sigma \in G_{P_i}$ such that $\sigma(P_j) = P_k$.*

Proof. Since the set $C \cap L_Y$ is given by $Y = Z \prod_{\alpha \in \mathbb{F}_q}(X + \alpha^2 Z) = 0$, we have (a). See [3, Section 3], [4, Section 4] for (b). An automorphism $\sigma \in G_{P_1}$ is given by $(x, y) \mapsto (x + \alpha y + \alpha^2, y)$ for some $\alpha \in \mathbb{F}_q$ (see [4, Section 4]). If $\alpha \neq 0$, then the set L_σ coincides with the line defined by $Y + \alpha Z = 0$. Therefore, $G_{P_1}(P_1) := \{\tau \in G_{P_1} \mid \tau(P_1) = P_1\} = G_{P_1}$, and $G_{P_1}(Q) := \{\tau \in G_{P_1} \mid \tau(Q) = Q\}$ is of order two for any $\sigma \in G_{P_1} \setminus \{1\}$ and any $Q \in C \cap L_\sigma \setminus \{P_1\}$. It follows from [15, III.8.2] that the ramification index at P (resp. at Q) is equal to the order $|G_{P_1}(P_1)|$ (resp. $|G_{P_1}(Q)|$). We have (c). Since G_{P_i} acts on $C \cap \ell \setminus \{P_i\}$ transitively if ℓ is a line passing through P_i by a natural property of Galois extension ([15, III.7.1]), we have (d). □

We determine $\mathrm{Aut}(C)$.

Lemma 2.1. *The restriction map $\gamma \mapsto \gamma|_{L_Y}$ gives an injection*

$$r : \mathrm{Aut}(C) \hookrightarrow \mathrm{PGL}(L_Y(\mathbb{F}_q)) \cong \mathrm{PGL}(2, \mathbb{F}_q).$$

Proof. Let $\gamma \in \mathrm{Aut}(C)$. Since the set of Galois points is invariant under a linear transformation, $\gamma(L_Y(\mathbb{F}_q)) = L_Y(\mathbb{F}_q)$, by Proposition 2.1(a)(b). Therefore, r is well-defined. Note also that $\gamma(T_{P_i}C) = T_{\gamma(P_i)}C$, since a tangent line is invariant under a linear transformation.

Assume that $\gamma|_{L_Y}$ is identity. Then, $\gamma(T_{P_i}C) = T_{\gamma(P_i)}C = T_{P_i}C$ and the point given by $T_{P_1}C \cap T_{P_i}C$ is fixed by γ for any i. If $P_i = (\beta : 0 : 1) \in L_Y(\mathbb{F}_q)$, then $T_{P_i}C$ is given by $X + \sqrt{\beta}Y + \beta Z = 0$. Since $\gamma|_{T_{P_1}C}$ is an automorphism of $T_{P_1}C \cong \mathbb{P}^1$ and there exist q (≥ 4) points fixed by γ, $\gamma|_{T_{P_1}C}$ is identity. Since $\gamma|_{L_Y} = 1$ and $\gamma|_{T_{P_1}C} = 1$, γ is identity on $\mathbb{P}^2$. □

Lemma 2.2. *Let $H(C) := \{\gamma \in \mathrm{Aut}(C) \mid \gamma(P_1) = P_1, \gamma(P_2) = P_2\}$ and let $H_0 := \{\tau \in \mathrm{PGL}(L_Y(\mathbb{F}_q)) \mid \tau(P_1) = P_1, \tau(P_2) = P_2\}$. Then, $r(H(C)) = H_0$. In particular, $H_0 \subset r(\mathrm{Aut}(C))$.*

Proof. We have $r(H(C)) \subset H_0$. According to [4, Lemma 4 and Page 100], $H(C)$ is a cyclic group of order $q-1$. We can also prove that H_0 is a cyclic group of order at most $q-1$ (see, for example, [4, Lemma 2(2)]). Therefore, we have $r(H(C)) = H_0$. □

Lemma 2.3. *The restriction map r is surjective.*

Proof. Let $\tau \in \mathrm{PGL}(L_Y(\mathbb{F}_q))$ and let $\tau(P_1) = P_i$, $\tau(P_2) = P_j$. We take $k \neq 1, i$. By Proposition 2.1(d), there exists $\gamma_1 \in r(G_{P_k})$ such that $\gamma_1\tau(P_1) = P_1$. Further, by Proposition 2.1(c)(d), there exists $\gamma_2 \in r(G_{P_1})$ such that $\gamma_2\gamma_1\tau(P_1) = P_1$ and $\gamma_2\gamma_1\tau(P_2) = P_2$. Then, $\gamma_2\gamma_1\tau \in H_0$. By Lemma 2.2, $\gamma_2\gamma_1\tau \in r(\mathrm{Aut}(C))$. This implies $\tau \in r(\mathrm{Aut}(C))$. □

We have $\mathrm{Aut(C)} \cong \mathrm{PGL}(2, \mathbb{F}_q)$ by Lemmas 2.1 and 2.3.

Remark 2.1. According to Deuring-Šafarevič formula ([16, Theorem 4.2]), the p-rank γ_C of the curve C is computed by ramification indices for the Galois covering π_{P_1}. Using Proposition 2.1(c), we have

$$\frac{\gamma_C - 1}{q} = (-1) + \left(1 - \frac{1}{q}\right) + (q-1)\left(1 - \frac{1}{2}\right).$$

This implies $\gamma_C = q(q-1)/2 = g_C$, i.e. C is ordinary.

Remark 2.2. We also have the following for $\mathrm{Aut}(C)$.

(a) $|\mathrm{Aut}(C)| = g_C \times (3 + \sqrt{8g_C + 1})$.

(b) $\mathrm{Aut}(C) = \langle G_{P_1}, \ldots, G_{P_{q+1}} \rangle = \langle G_{P_1}, G_{P_2} \rangle$.

Remark 2.3. When $\lambda = 1$, we can check that the curve C with $(*)$ is parameterized as $\mathbb{P}^1 \to \mathbb{P}^2; (s:1) \mapsto (s^{q+1} : s^q + s : 1)$ by direct computation ([4, Remark 3]). Therefore, C is rational and singular. The similar result $\mathrm{Aut}_0(C) \cong \mathrm{PGL}(2, \mathbb{F}_q)$ has been obtained by Hoai and Shimada [7, Proposition 1.3], where $\mathrm{Aut}_0(C) := \{\phi \in \mathrm{PGL}(3, K) \mid \phi(C) = C\}$.

3. Proof of Theorem 1.2

Similarly to the previous section, we have an injection

$$\mathrm{Aut}(C) \hookrightarrow \mathrm{PGL}(3, K).$$

Let L_Z be the line given by $Z = 0$, and let $P_1 = (1:0:0)$, $P_2 = (1:1:0)$ and $P_3 = (0:1:0)$. If P is a Galois point, then we denote by G_P the Galois group. For $\gamma \in \mathrm{Aut}(C)$, we denote the set $\{Q \in \mathbb{P}^2 \mid \gamma(Q) = Q\}$ by L_γ. We have the following properties for curves with $(**)$ (see [5, Sections 3 and 4]).

Proposition 3.1. *Let C be the plane curve given by $(**)$. Then, we have the following.*

(a) *The set of Galois points in $\mathbb{P}^2 \setminus C$ coincides with $L_Z(\mathbb{F}_2) = \{P_1, P_2, P_3\}$.*

(b) *For each i, there exists a unique element $\sigma_i \in G_{P_i} \setminus \{1\}$ such that $L_{\sigma_i} = L_Z$.*

(c) *For each i, there exist exactly two lines ℓ such that $\ell \ni P_i$, $\ell \neq L_Z$ and ℓ is the tangent line at two points in $C \cap \ell$. Conversely, if ℓ is such a line, then there exists $\tau \in G_{P_i} \setminus \langle \sigma_i \rangle$ such that $L_\tau = \ell$.*

(d) *There exist exactly four non-Galois points $Q_1, Q_2, Q_3, Q_4 \in \mathbb{P}^2$ such that the line $\overline{Q_iQ_j}$ which passes through Q_i, Q_j is a tangent line of C for each i, j with $i \neq j$ and $\overline{Q_iQ_j} \ni P_k$ for some k. Such points are $(0:0:1)$, $(1:0:1)$, $(0:1:1)$ and $(1:1:1)$.*

Proof. For (a)(d), see [5, Section 4] (we need $\lambda \neq 1$). We explain (b)(c) for $i = 1$. Let σ, τ be linear transformations given by

$$\sigma(X:Y:Z) = (X+Z:Y:Z),\ \tau(X:Y:Z) = (X+Y:Y:Z).$$

Then, $G_{P_1} = \{1, \sigma, \tau, \sigma\tau\}$. Since $\sigma|_{L_Z} = 1$ and $\tau|_{L_Z} \neq 1$, we have (b). Note that the line L_τ is given by $Y = 0$ and the line $L_{\sigma\tau}$ is given by $Y + Z = 0$. Referring [15, III. 8.2], we have (c). For $i = 2, 3$, we consider the linear transformations $\phi_2 : (X, Y, Z) \mapsto (X, Y + X, Z)$ and $\phi_3 : (X, Y, Z) \mapsto (Y, X, Z)$. Then, $\phi_i(C) = C$, $\phi_i(P_1) = P_i$ and $G_{P_i} = \phi_i G_{P_1} \phi_i^{-1}$. We also have (b)(c) for $i = 2, 3$. $\square$

First we prove the following.

Lemma 3.1. *Let $X = \{Q_1, Q_2, Q_3, Q_4\}$ and let $S(X)$ be the group of all permutations on X. Then, there exists an injection $\mathrm{Aut}(C) \hookrightarrow S(X) \cong S_4$.*

Proof. By Proposition 3.1(d), we have a well-defined homomorphism $\mathrm{Aut}(C) \to S(X)$ by $\gamma \mapsto \gamma|_X$. If $\gamma \in \mathrm{Aut}(C)$ fixes Q_1, Q_2, Q_3, Q_4, then γ fixes P_1, P_2, P_3 also. Note that $X \cup \{P_1, P_2, P_3\} = \mathbb{P}^2(\mathbb{F}_2)$. Then, γ is identity on the projective plane. $\square$

We prove that $|\mathrm{Aut}(C)| \geq 24$. Let $H := \langle \sigma_1, \sigma_2 \rangle$.

Lemma 3.2. *The restriction map*

$$r : \mathrm{Aut}(C) \to \mathrm{PGL}(L_Z(\mathbb{F}_2)) \cong S_3;\ \gamma \mapsto \gamma|_{L_Z}$$

is surjective and its kernel coincides with H. In particular, $|\mathrm{Aut}(C)| \geq 24$.

Proof. Let $\gamma \in \mathrm{Aut}(C)$. Since the set of Galois points is invariant under a linear transformation, $\gamma(\{P_1, P_2, P_3\}) = \{P_1, P_2, P_3\}$, by Proposition 3.1(a). Therefore, r is well-defined.

We consider the kernel. Assume that $\gamma|_{L_Z}$ is identity. Let $\sigma_i \in G_{P_i}$ be an automorphism as in Proposition 3.1(b) for $i = 1, 2$ and let $\tau, \eta \in G_{P_1} \setminus \langle \sigma_1 \rangle$ with $\tau \neq \eta$. By Proposition 3.1(c), L_τ and L_η are tangent lines of C containing P_1. Since $\gamma(P_1) = P_1$, $\gamma(L_\tau)$ is a tangent line with $P_1 \in \gamma(L_\tau)$. We have $\gamma(L_\tau) = L_\tau$ or L_η by Proposition 3.1(c). Assume that $\gamma(L_\tau) = L_\tau$. Since σ_1 acts on $C \cap L_\tau$ ([15, III.7.1]), $\sigma_1^l \gamma$ fixes P_1 and two points of $C \cap L_\tau$ for $l = 0$ or 1. Then $\sigma_1^l \gamma$ is identity on L_τ by a property of an automorphism of $L_\tau \cong \mathbb{P}^1$. We have $\sigma_1^l \gamma = 1$ on $\mathbb{P}^2$, because $\sigma_1^l \gamma|_{L_Z} = 1$ and $\sigma_1^l \gamma|_{L_\tau} = 1$. Then, $\gamma \in H$. Assume that $\gamma(L_\tau) = L_\eta$. Now, $\sigma_2(L_\eta)$ is a tangent line containing P_1. By Proposition 3.1(c), $\sigma_2(L_\eta) = L_\eta$ or L_τ. Let $Q \in C \cap L_\eta$ and let $\overline{P_2 Q}$ be the line passing through P_2, Q. Since $Q \notin L_Z = L_{\sigma_2}$ and σ_2 acts on $C \cap \overline{P_2 Q}$ ([15, III.7.1]), $\sigma_2(Q) \neq Q$ and $\sigma_2(Q) \in \overline{P_2 Q}$. We have $\sigma_2(L_\eta) \neq L_\eta$, because $\sigma_2(Q) \notin L_\eta$. Therefore, $\sigma_2(L_\eta) = L_\tau$ and $\sigma_2 \gamma(L_\tau) = L_\tau$. Similarly to the case $\gamma(L_\tau) = L_\tau$, $\sigma_1^l \sigma_2 \gamma$ is identity on $\mathbb{P}^2$ for $l = 0$ or 1. We have $\gamma \in H$.

We prove that r is surjective. We have an injection $\mathrm{Aut}(C)/H \hookrightarrow S_3$. Let $\tau_i \in G_{P_i} \setminus \langle \sigma_i \rangle$ for each i. Since $\tau_1 \tau_2(P_1) = P_2$, $\tau_1 \tau_2(P_2) = P_3$ and $\tau_1 \tau_2(P_3) = P_1$, the order of $\tau_1 \tau_2 H \in \mathrm{Aut}(C)/H$ is three. Since the group $\mathrm{Aut}(C)/H$ has elements of order two and three, we have $\mathrm{Aut}(C)/H = S_3$. $\square$

We have the conclusion, by these two lemmas.

Remark 3.1. We also have $\mathrm{Aut}(C) = \langle G_{P_1}, G_{P_2}, G_{P_3} \rangle = \langle G_{P_1}, G_{P_2} \rangle$.

References

[1] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of algebraic curves*, Vol. I. Grundlehren der Mathematischen Wissenschaften **267**, Springer-Verlag, New York, 1985.

[2] H. C. Chang, *On plane algebraic curves*, Chinese J. Math. **6** (1978), 185–189.

[3] S. Fukasawa, *On the number of Galois points for a plane curve in positive characteristic, III*, Geom. Dedicata **146** (2010), 9–20.

[4] S. Fukasawa, *Complete determination of the number of Galois points for a smooth plane curve*, Rend. Sem. Mat. Univ. Padova **129** (2013), 93–113.

[5] S. Fukasawa, *Galois points for a plane curve in characteristic two*, J. Pure Appl. Algebra **218** (2014), 343–353.

[6] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*, Princeton Ser. Appl. Math., Princeton Univ. Press, Princeton, 2008.

[7] H. T. Hoai and I. Shimada, *On Ballico-Hefez curves and associated supersingular surfaces*, preprint, arXiv:1402.3372.

[8] N. Hurt, *Many rational points*, Kluwer Academic Publishers, Dordrecht, 2003.

[9] M. Kanazawa, T. Takahashi, and H. Yoshihara, *The group generated by automorphisms belonging to Galois points of the quartic surface*, Nihonkai Math. J. **12** (2001), 89–99.

[10] M. J. Klassen and E. F. Schaefer, *Arithmetic and geometry of the curve $y^3+1=x^4$*, Acta Arith. **74** (1996), 241–257.

[11] K. Miura and A. Ohbuchi, *Automorphism group of plane curve computed by Galois points*, Beitr. Algebra Geom., to appear.

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

[13] S. Nakajima, *p-ranks and automorphism groups of algebraic curves*, Trans. Amer. Math. Soc. **303** (1987), 595–607.

[14] C. Ritzenthaler, *Automorphism group of $C : y^3 + x^4 + 1 = 0$ in characteristic p*, JP J. Algebra Number Theory Appl. **4** (2004), 621–623.

[15] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.

[16] D. Subrao, *The p-rank of Artin-Schreier curves*, Manuscripta Math. **16** (1975), 169–193.

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

(Satoru Fukasawa) Department of Mathematical Sciences, Faculty of Science, Yamagata University, Kojirakawa-machi 1-4-12, Yamagata 990-8560, Japan.

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

Received April 24, 2014
Revised July 8, 2014