International Journal of Algebra, Vol. 1, 2007, no. 12, 563 - 585

The Galois Group of a Projection of a Hermitian Curve

Masaaki Homma[1]

Department of Mathematics, Kanagawa University
Yokohama 221-8686, Japan
homma@n.kanagawa-u.ac.jp

Abstract

For a Hermitian curve H in projective plane $\mathbb{P}^2$ and an arbitrary point P of $\mathbb{P}^2$, we find out the Galois group of the projection $H \to \mathbb{P}^1$ with center P. To achieve this aim, we discuss the Galois group of an equation and that of a finite separable morphism between curves in slightly more general context. Moreover, we compute the genus of the so-called Galois-closure curve $\widetilde{H_P}$.

Mathematics Subject Classification: 14H45, 14H50, 14H25

Keywords: Plane curve, Positive characteristic, Galois group, Hermitian curve

1 Introduction

The Galois group of a linear projection of a curve has been studied for the past decade by Miura and Yoshihara (e.g. [9, 10, 11, 15, 16]). They are mainly concerned with the characteristic 0 case. If we consider the Galois group in positive characteristic, unusual phenomena may occur even if the center of the projection is a point. In fact, we saw it by an example when the projection is a Galois covering, which is explained in Theorem 1 below. Recently, Fukasawa studied the matter of Galois points in positive characteristic in general [3, 4, 5, 6].

Let C be a nonsingular plane curve of degree $d \geq 4$ over an algebraic closed field k. For an assigned point P of $\mathbb{P}^2$, the projection $\pi_P : C \to \mathbb{P}^1$ with center P gives rise to the field extension $k(C)/k(\mathbb{P}^1)$, where $k(C)$ and $k(\mathbb{P}^1)$ are the function fields over k of C and $\mathbb{P}^1$ respectively. We know the extension

[1]Partially supported by Grants-in-Aid for Scientific Research (17540045 and 19540058), JSPS.

$k(C)/k(\mathbb{P}^1)$ is separable by [8]. The Galois group G_P of the Galois closure of $k(C) \overset{\pi_P^*}{\hookleftarrow} k(\mathbb{P}^1)$ is the object of our study. When the extension $k(C)/k(\mathbb{P}^1)$ via π_P^* is Galois, the center P of the projection is called a Galois point for C. Since the automorphism group of C is finite and each automorphism, which gives rise to a linear transformation of $\mathbb{P}^2$, has finitely many fixed points, the number of Galois points for C is finite. When P is not Galois, $\widetilde{C_P}$ denotes the nonsingular projective curve corresponding to the Galois closure of $k(C)/k(\mathbb{P}^1)$ via π_P^*.

Before stating our results, we explain what we already know in characteristic 0. In [15, 16], Yoshihara showed that *the number of Galois points on C is 0 or 1 or 4 if $d = 4$ and it is 0 or 1 if $d \geq 5$; and the number of Galois points outside C is 0 or 1 or 3.* Moreover, he showed that *if P is a general point of C, then G_P is the symmetric group S_{d-1} of degree $d-1$ and the genus of $\widetilde{C_P}$ is $(d-1)!(d+2)(d-3)/4+1$; and if P is a general point of $\mathbb{P}^2 \setminus C$, then G_P is the symmetric group S_d of degree d and the genus of $\widetilde{C_P}$ is $(d-1)!(d^2-d-4)/4+1$.*

Our purpose is to observe the behavior of a Hermitian curve in the framework of Yoshihara's theory, which may suggest the difference between the phenomena in characteristic 0 and those in characteristic $p > 0$.

Let p be a prime number and $q = p^e$ with $q \geq 4$. We denote by $\mathbb{F}_{q^2}$ the field of q^2 elements, and by k the algebraic closure of $\mathbb{F}_{q^2}$. We consider a plane curve H given by

$$y^q + y = x^{q+1}, \tag{1}$$

where x and y are inhomogeneous coordinates of the ambient projective plane $\mathbb{P}^2$ over k. When we choose $\mathbb{F}_{q^2}$ as a field of definition of H, the curve is called a Hermitian curve.

In the previous paper [7], we proved the following fact.

Theorem 1 *The field extension $k(H)/k(\mathbb{P}^1)$ by means of π_P is Galois if and only if P is $\mathbb{F}_{q^2}$-rational. Moreover we have*

(a) $G_P \overset{\sim}{=} \overset{e}{\oplus} \mathbb{Z}/p\mathbb{Z}$ *if* $P \in H(\mathbb{F}_{q^2})$;

(b) $G_P \overset{\sim}{=} \mathbb{Z}/(q+1)\mathbb{Z}$ *if* $P \in \mathbb{P}^2(\mathbb{F}_{q^2}) \setminus H(\mathbb{F}_{q^2})$,

where $\mathbb{P}^2(\mathbb{F}_{q^2})$ and $H(\mathbb{F}_{q^2})$ denote the set of $\mathbb{F}_{q^2}$-rational points of $\mathbb{P}^2$ and H respectively.

In this paper, we show the following theorem.

Theorem 2 (a) *If $P \in H \setminus H(\mathbb{F}_{q^2})$, then G_P is isomorphic to*

$$AGL(1, \mathbb{F}_q) = \{\sigma : \mathbb{F}_q \to \mathbb{F}_q \mid \sigma(z) = \alpha z + \beta,\ \alpha \in \mathbb{F}_q^\times, \beta \in \mathbb{F}_q\}$$

and the genus of $\widetilde{H_P}$ is $(q-1)^2 q/2$.

(b) *If* $P \in \mathbb{P}^2 \setminus (H \cup \mathbb{P}^2(\mathbb{F}_{q^2}))$*, then* G_P *is isomorphic to the projective general linear group* $PGL(2, \mathbb{F}_q)$ *of* $\mathbb{P}^1(\mathbb{F}_q)$*, and the genus of* $\widetilde{H_P}$ *is* $q(q^3-q-2)/2$.

In order to prove Theorem 2, we prepare two properties of a Galois group in slightly more general setting than our original one. The first property is algebraic, which is discussed in Section 2, the second one is geometric, discussed in Section 3. Both of the properties are modification of what Ballico and Hefez [2] or Rathmann [13] proved. In Section 2, we use Abhyankar's method of throwing away roots [1] to find the Galois group of an equation coming from π_P, which is an important step for computing the genus of $\widetilde{H_P}$. Sections 4 and 5 are devoted to the proof of Theorem 2.

2 Galois group of an algebraic equation

In the first half of this section, we consider a polynomial $f(X)$ of degree $d > 0$ over a field K which has no multiple roots but is possibly reducible. Let $\{\alpha_1, \dots, \alpha_d\}$ be the set of roots of $f(X)$ in the algebraic closure $\bar{K}$ of K, and $G(f/K)$ the Galois group of $K(\alpha_1, \dots, \alpha_d)/K$. The Galois group $G(f/K)$ acts on $\{\alpha_1, \dots, \alpha_d\}$ transitively if $f(X)$ is irreducible over K.

We introduce a non-common terminology.

Definition 2.1 For $f(X) \in K[X]$, we construct successive pairs

$$\{(K_i, f_i(X))\}_{i=0,1,\dots,\mu}$$

each of which consists of a field K_i and a polynomial $f_i(X)$ with $f_i(X) \in K_i[X]$ inductively as follows.
(0) Put $K_0 = K$ and $f_0(X) = f(X)$;
(1) After we constructed pairs $\{(K_i, f_i(X))\}_{i=0,1,\dots,\rho}$ up to the $\rho + 1$st step,

(1a) the construction terminates, if either $f_\rho(X)$ is reducible over K_ρ or $\deg f_\rho = 0$.

(1b) If $f_\rho(X)$ is irreducible, put $K_{\rho+1} = K_\rho[Y]/(f_\rho(Y))$ and $\bar{Y} = Y \mod f_\rho(Y)$ in $K_{\rho+1}$. Then $X - \bar{Y}$ divides $f_\rho(X)$ in $K_{\rho+1}[X]$, that is, there is a polynomial $g(X) \in K_{\rho+1}[X]$ such that $f_\rho(X) = (X - \bar{Y})g(X)$. We put $f_{\rho+1}(X) = g(X)$.

The number μ is called the *splitting height* of $f(X)$ over K.

It is obvious that the splitting height of $f(X)$ is at most the degree of $f(X)$, and it is 0 if and only if $f(X)$ is reducible.

Lemma 2.2 *Let $f(X)$ be the polynomial of $K[X]$ considered in Definition* 2.1. *Let ρ be a nonnegative integer with $\rho \leq \mu$, where μ is the splitting height of $f(X)$ over K. Then for any ρ roots $\{\alpha_{i_1}, \ldots, \alpha_{i_\rho}\}$ of $f(X)$ we have $K_\rho \cong K(\alpha_{i_1}, \ldots, \alpha_{i_\rho})$ over K and $\dim_K K_\rho = d!/(d-\rho)!$.*

Proof. We prove this by induction on ρ. Suppose that $K_{\rho-1} \cong K(\alpha_{i_1}, \ldots, \alpha_{i_{\rho-1}})$ and $\dim_K K_{\rho-1} = d!/(d-\rho+1)!$. By the construction of successive pairs,

$$f(X) = (X - \alpha_{i_1}) \cdots (X - \alpha_{i_{\rho-1}}) f_{\rho-1}(X)$$

in $K_{\rho-1}[X]$ via the isomorphism $K_{\rho-1} \cong K(\alpha_{i_1}, \ldots, \alpha_{i_{\rho-1}})$. Since $f(X)$ has no multiple root, $f_{\rho-1}(\alpha_{i_\rho}) = 0$, which means $f_{\rho-1}$ is a minimal polynomial of α_{i_ρ} over $K_{\rho-1}$ because $f_{\rho-1}(X)$ is irreducible over $K_{\rho-1}$. Therefore

$$K_\rho \cong K_{\rho-1}[X]/(f_{\rho-1}(X)) \cong K_{\rho-1}(\alpha_{i_\rho}) \cong K(\alpha_{i_1}, \ldots, \alpha_{i_\rho})$$

and

$$[K_\rho : K_{\rho-1}] = \deg f_{\rho-1}(X) = d - \rho + 1.$$

Hence $\dim_K K_\rho = (d-\rho+1)\frac{d!}{(d-\rho+1)!} = d!/(d-\rho)!$. □

The following proposition is a polynomial version of [13, Prop. 1.5].

Proposition 2.3 (Abhyankar's MTR) *Let $f(X) \in K[X]$ be an irreducible polynomial of degree d and $\{\alpha_1, \ldots, \alpha_d\}$ the set of roots of $f(X)$ in $\bar{K}$, which are distinct elements. For $\nu \in \mathbb{Z}$ with $0 \leq \nu \leq d$, the following conditions are equivalent*:

(i) $\dim_K K[\alpha_1, \ldots, \alpha_\nu] = \frac{d!}{(d-\nu)!}$;

(ii) $\dim_K K[\alpha_{i_1}, \ldots, \alpha_{i_\nu}] = \frac{d!}{(d-\nu)!}$ *for an arbitrary ν roots $\{\alpha_{i_1}, \ldots, \alpha_{i_\nu}\} \subset \{\alpha_1, \ldots, \alpha_d\}$*;

(iii) *the splitting height of f over K is at least ν*;

(iv) *$G(f/K)$ acts ν-fold transitively on $\{\alpha_1, \ldots, \alpha_d\}$.*

Proof. When $\nu = 0$, there is nothing to do. (ii)⇒(i) is obvious, and (iii)⇒(ii) follows from Lemma 2.2.

(i)⇒(iii). Put $K_\rho = K[\alpha_1, \ldots, \alpha_\rho]$ for $\rho \leq \nu$. Since the roots $\alpha_1, \ldots, \alpha_\nu$ of $f(X)$ are in K_ν, we have the decomposition $f(X) = (X-\alpha_1) \cdots (X-\alpha_\nu) g(X)$ in $K_\nu[X]$. Put

$$f_\rho(X) = \begin{cases} (X - \alpha_{\rho+1}) \cdots (X - \alpha_\nu) g(X) & \text{if } \rho < \nu \\ g(X) & \text{if } \rho = \nu. \end{cases}$$

We prove that if $\rho < \nu$, then $f_\rho(X)$ is an irreducible polynomial over K_ρ. For $\rho = 0$, it is obvious because $f_0(X) = f(X) \in K[X]$. Since $\alpha_1, \dots, \alpha_\rho \in K_\rho$ are roots of $f(X)$, we have a polynomial in $K_\rho[X]$ of degree $d - \rho$ that is the quotient of $f(X)$ by $(X-\alpha_1)\cdots(X-\alpha_\rho)$, which is just $f_\rho(X)$. Since $\alpha_{\rho+1}$ is a root of $f(X)$, it is a root of $f_\rho(X)$. On the other hand, since $K_{\rho+1} = K_\rho[\alpha_{\rho+1}]$ and

$$[K_{\rho+1} : K_\rho] = \frac{d!}{(d-(\rho+1))!} \Big/ \frac{d!}{(d-\rho)!} = d - \rho$$

by the assumption (ii), $f_\rho(X)$ is a minimal polynomial of $\alpha_{\rho+1}$ over K_ρ, and irreducible particularly.

(iii)⇒(iv). Let $\{\alpha_{i_1}, \dots \alpha_{i_\nu}\}$ and $\{\alpha_{j_1}, \dots \alpha_{j_\nu}\}$ be two sets of ν roots of $f(X)$. By construction of the successive pairs $\{(K_i, f_i(X))\}_{i=0,1,\dots,\nu}$ in the proof of Lemma 2.2, we have a commutative diagram

$$\begin{array}{ccccc} K[\alpha_{i_1}, \dots \alpha_{i_{\rho-1}}][\alpha_{i_\rho}] & \cong & K_\rho = K_{\rho-1}[X]/f_{\rho-1}(X) & \cong & K[\alpha_{j_1}, \dots \alpha_{j_{\rho-1}}][\alpha_{j_\rho}] \\ \uparrow & & \uparrow & & \uparrow \\ K[\alpha_{i_1}, \dots \alpha_{i_{\rho-1}}] & \cong & K_{\rho-1} & \cong & K[\alpha_{j_1}, \dots \alpha_{j_{\rho-1}}] \end{array}$$

for any $\rho \le \nu$. Note that α_{i_ρ} is a root of $f_{\rho-1}(X)$ if we regard $f_{\rho-1}(X)$ as a polynomial over $K[\alpha_{i_1}, \dots \alpha_{i_{\rho-1}}]$ via the isomorphism at the lower left in the diagram; and so is α_{j_ρ} if we regard $f_{\rho-1}(X)$ as a polynomial over $K[\alpha_{j_1}, \dots \alpha_{j_{\rho-1}}]$ via the isomorphism at the lower right. Hence there is an isomorphism $\sigma : K[\alpha_{i_1}, \dots \alpha_{i_\rho}] \to K[\alpha_{j_1}, \dots \alpha_{j_\rho}]$ over K so that $\sigma(\alpha_{i_\rho}) = \alpha_{j_\rho}$ $(\rho = 1, 2, \dots, \nu)$. This σ can be extended to an element of $G(f/K)$.

(iv)⇒(i). Since

$$\dim_K K[\alpha_{i_1}, \dots \alpha_{i_\nu}] = {}^{\#}\{\sigma : K[\alpha_{i_1}, \dots \alpha_{i_\nu}] \hookrightarrow \bar{K} \mid \sigma \text{ is an embedding over } K\},$$

and $\sigma(\alpha_i)$ is a root of $f(X)$, we have

$$\dim_K K[\alpha_{i_1}, \dots, \alpha_{i_\nu}] \le \nu! \binom{d}{\nu} \tag{2}$$

in general. The ν-fold transitivity of the action $G(f/K)$ on $\{\alpha_1, \dots \alpha_d\}$ implies that the equality in (2) is attained. □

As applications of Proposition 2.3, we handle two concrete polynomials, which are already discussed in [13, the proofs of 2.15 and 2.17].

Lemma 2.4 *Let K be a field containing $\mathbb{F}_q$, and*

$$f(X) = X^{q+1} + AX^q + BX + C \in K[X].$$

Suppose $f(X)$ is irreducible. Then $f(X)$ is separable and the Galois group $G(f/K)$ of $f(X)$ over K is a subgroup of the projective general linear group $PGL(2, \mathbb{F}_q)$ of $\mathbb{P}^1(\mathbb{F}_q)$. Moreover the action $G(f/K)$ onto the roots of $f(X)$ is 3-fold transitive if and only if $G(f/K) = PGL(2, \mathbb{F}_q)$.

Proof. Since $f'(X) = X^q + B$, $f(X)$ is separable. Let x be a root of $f(X)$. Putting $U = X - x$, we have

$$f(X) = U(U^q + (x + A)U^{q-1} + (x^q + B)).$$

Put $V = 1/U$. Then the equation $U^q + (x+A)U^{q-1} + (x^q+B) = 0$ is equivalent to

$$(x^q + B)V^q + (x + A)V + 1 = 0. \tag{3}$$

In fact, $x^q + B = f'(x) \neq 0$ as we saw. Choose a root of (3), say v, and put $W = V - v$. Then the polynomial in V is equal to

$$W((x^q + B)W^{q-1} + (x + A)).$$

Choose a root of the equation

$$(x^q + B)W^{q-1} + (x + A) = 0 \tag{4}$$

on W, say w. Hence the set of roots of (4) is $\{zw \mid z \in \mathbb{F}_q \setminus \{0\}\}$, and those of (3) is $\{v + zw \mid z \in \mathbb{F}_q\}$. Therefore the set of roots of $f(X)$ is

$$\{x\} \cup \{x + \frac{1}{zw + v} \mid z \in \mathbb{F}_q\} = \{x + \frac{z_2}{z_1 w + z_2 v} \mid (z_1, z_2) \in \mathbb{P}^1(\mathbb{F}_q)\}. \tag{5}$$

Now we describe the action of $G(f/K)$ to the set (5). Let $\sigma \in G(f/K)$. Since $\sigma(x)$, $\sigma(x + \frac{1}{v})$ and $\sigma(x + \frac{1}{w+v})$ are also in the set (5) and distinct, we can find $\alpha', \gamma', \beta', \delta', \varepsilon', \zeta' \in \mathbb{F}_q$ so that

$$\begin{aligned} \sigma(x) &= x + \frac{\gamma'}{\alpha' w + \gamma' v} \\ \sigma(x + \frac{1}{v}) &= x + \frac{\delta'}{\beta' w + \delta' v} \\ \sigma(x + \frac{1}{w + v}) &= x + \frac{\zeta'}{\varepsilon' w + \zeta' v}. \end{aligned}$$

Since $(\alpha', \gamma') \neq (\beta', \delta')$ as elements of $\mathbb{P}^1$, there are $k, l \in \mathbb{F}_q$ with

$$\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix} \begin{pmatrix} k \\ l \end{pmatrix} = \begin{pmatrix} \varepsilon' \\ \zeta' \end{pmatrix},$$

where both the solutions k and l are nonzero because $(\alpha', \gamma') \neq (\varepsilon', \zeta')$ and $(\beta', \delta') \neq (\varepsilon', \zeta')$ as elements of $\mathbb{P}^1$. Put $\alpha = k\alpha', \beta = l\beta', \gamma = k\gamma'$ and $\delta = l\delta'$. Then

$$\sigma(x) = x + \frac{\gamma}{\alpha w + \gamma v}$$

$$\begin{aligned}\sigma(x+\frac{1}{v}) &= x+\frac{\delta}{\beta w+\delta v}\\ \sigma(x+\frac{1}{w+v}) &= x+\frac{\gamma+\delta}{(\alpha+\beta)w+(\gamma+\delta)v}.\end{aligned}$$

Hence we have

$$\begin{aligned}\sigma(v) &= \frac{1}{\sigma(x+\frac{1}{v})-\sigma(x)} = \frac{(\alpha w+\gamma v)(\beta w+\delta v)}{(\alpha\delta-\beta\gamma)w}\\ \sigma(w) &= \frac{1}{\sigma(x+\frac{1}{w+v})-\sigma(x)}-\sigma(v) = \frac{(\alpha w+\gamma v)^2}{(\alpha\delta-\beta\gamma)w}.\end{aligned}$$

Then, by direct computation, we have

$$\begin{aligned}\sigma(x+\frac{z_2}{z_1w+z_2v}) &= \sigma(x)+\frac{z_2}{z_1\sigma(w)+z_2\sigma(v)}\\ &= x+\frac{\gamma z_1+\delta z_2}{(\alpha z_1+\beta z_2)w+(\gamma z_1+\delta z_2)v},\end{aligned}$$

in other words, σ gives rise to the projective transormation

$$\mathbb{P}^1(\mathbb{F}_q)\ni\begin{pmatrix}z_1\\ z_2\end{pmatrix}\mapsto\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}z_1\\ z_2\end{pmatrix}\in\mathbb{P}^1(\mathbb{F}_q)$$

via the identification (5) of the set of roots of $f(X)$ with $\mathbb{P}^1(\mathbb{F}_q)$. It is obvious that this correspondence $G(f/K)\to PGL(2,\mathbb{F}_q)$ is an injective group homomorphism. If this homomorphism is surjective, $G(f/K)$ acts on the set of roots of $f(X)$ 3-fold transitively because the action of $PGL(2,\mathbb{F}_q)$ to $\mathbb{P}^1(\mathbb{F}_q)$ is 3-fold transitive. Conversely if $G(f/K)$ does so, then

$$\dim_K K[x,v,w]=(q+1)!/(q+1-3)!=(q+1)q(q-1)$$

by Proposition 2.3. Since the order of $PGL(2,\mathbb{F}_q)$ is also $(q+1)q(q-1)$, the injective homomorphism is an isomorphism. □

By argument similar to the proof of the above lemma, we can show the following fact.

Lemma 2.5 *Let K be a field containing $\mathbb{F}_q$, and*

$$f(X)=X^q+AX^{q-1}+B\in K[X].$$

Suppose $f(X)$ is irreducible. Then $f(X)$ is separable and the Galois group $G(f/K)$ of $f(X)$ over K is a subgroup of

$$AGL(1,\mathbb{F}_q):=\{\sigma:\mathbb{A}^1(\mathbb{F}_q)\to\mathbb{A}^1(\mathbb{F}_q)\mid\sigma(z)=\alpha z+\beta,\ \alpha\in\mathbb{F}_q^\times,\ \beta\in\mathbb{F}_q\}.$$

Moreover the action $G(f/K)$ onto the roots of $f(X)$ is 2-fold transitive if and only if $G(f/K)=AGL(1,\mathbb{F}_q)$.

Proof. Since $f(X)$ is irreducible, $B \neq 0$. Hence $f(X)$ has no multiple roots, and the equation $f(X) = 0$ is equivalent to the equation

$$BY^q + AY + 1 = 0 \tag{6}$$

under the condition $Y = 1/X$. Choose a root of (6), say y, and put $V = Y - y$. Then we have

$$V(BV^{q-1} + A) = 0.$$

Choose a root of the equation

$$BV^{q-1} + A = 0, \tag{7}$$

say v. Then the set of roots of (7) is $\{zv \mid z \in \mathbb{F}_q \setminus \{0\}\}$. So the set of roots of $f(X)$ is

$$\left\{ \frac{1}{zv + y} \mid z \in \mathbb{F}_q \right\}. \tag{8}$$

Hence the splitting field of $f(X)$ over K is $K[y, v]$. Let $\sigma \in G(f/K)$. Since σ acts on the set (8), we can find α and $\beta \in \mathbb{F}_q$ so that

$$\begin{aligned} \sigma\left(\frac{1}{y}\right) &= \frac{1}{\beta v + y} \\ \sigma\left(\frac{1}{v + y}\right) &= \frac{1}{(\alpha + \beta)v + y}. \end{aligned}$$

Hence $\sigma(y) = \beta v + y$ and $\sigma(v) = \alpha v$. Hence for $z \in \mathbb{F}_q$,

$$\sigma\left(\frac{1}{zv + y}\right) = \frac{1}{(\alpha z + \beta)v + y},$$

in other words, we have a map

$$G(f/K) \ni \sigma \mapsto \alpha z + \beta \in AGL(1, \mathbb{F}_q).$$

It is easy to see that this map is an injective group homomorphism.

If this group homomorphism is an isomorphism, $G(f/K)$ acts on the set (8) 2-fold transitively because $AGL(1, \mathbb{F}_q)$ acts on $\mathbb{F}_q$ 2-fold transitively. Conversely if $G(f/K)$ does so,

$$\dim_K K[y, v] = q!/(q-2)! = q(q-1)$$

by Proposition 2.3. Since ${}^{\#}AGL(1, \mathbb{F}_q) = q(q-1)$, the injective group homomorphism $G(f/K) \to AGL(1, \mathbb{F}_q)$ is an isomorphism. □

3 Galois group of a separable morphism of curves

Throughout this section, we fix the following situation.

Setup 3.1 Let X and Y be irreducible curves over an algebraically closed field k. We consider a finite separable morphism $\pi : X \to Y$ of degree d. The morphism gives rise to the field extension $k(X) \overset{\pi^*}{\hookleftarrow} k(Y)$, which is separabele of degree d. The Galois group of the Galois closure of $k(X)$ over $k(Y)$ is denoted by G. Let $y \in Y$ in general position, and $\pi^{-1}(y) = \{x_1, \ldots, x_d\}$. Then π is unramified at each x_i. Hence the natural morphism

$$\pi_{x_i}^* : \text{f.f.}(\widehat{\mathcal{O}}_{Y,y}) \ \xrightarrow{\sim}\ \text{f.f.}(\widehat{\mathcal{O}}_{X,x_i}).$$

is an isomorphism. Here $\widehat{R}$ denotes the completion of a local ring R with respect to the maximal ideal, and f.f.(R) the field of fractions of an integral domain R. We denote by $\tau_{x_i} = (\pi_{x_i}^*)^{-1}$. Then we have a commutative diagram

$$\begin{array}{ccccc} k(X) & \to & \text{f.f.}(\widehat{\mathcal{O}}_{X,x_i}) & \overset{\tau_{x_i}}{\to} & \text{f.f.}(\widehat{\mathcal{O}}_{Y,y}) \\ & {\scriptstyle \pi^*}\nwarrow & & \nearrow & \\ & & k(Y) & & \end{array} \quad , \tag{9}$$

where all morphisms are natural inclusions. Let L be the composite field of $\tau_{x_i}(k(X))$ $(i = 1, \ldots, d)$ in f.f.$(\widehat{\mathcal{O}}_{Y,y})$. Hence L is the Galois closure of $\tau_{x_i}(k(X))/k(Y)$ for any i. We denote by τ_{x_i} again the embedding of $k(X)$ into L coming from (9). It is obvious that the set of embeddings $k(X)$ into L over $k(Y)$ is $\{\tau_{x_i} \mid i = 1, \ldots, d\}$. On the other hand, since G acts on L by definition, the composition $\sigma\tau_{x_i}$ of τ_{x_i} and $\sigma \in G$ is also an embedding of $k(X)$ into L. So we can find $x_{\sigma(i)}$ such that $\sigma\tau_{x_i} = \tau_{x_{\sigma(i)}}$. This gives a represntation of G as a subgroup of the permutation group $\text{Per}(x_1, \ldots, x_d)$ of $\{x_1, \ldots, x_d\}$:

$$G \ \hookrightarrow\ \text{Per}(x_1, \ldots, x_d). \tag{10}$$

If we choose an element $\alpha \in k(X)$ such that $k(X) = k(Y)[\alpha]$, then (10) is equivalent to the representation using the roots of the minimal polynomial of α.

The following property of G is a modification of [2, Prop. 3]. In the proposition, $\text{Reg}\, X$ denotes the open subset of a curve X consisting of nonsingular points.

Proposition 3.2 *Under Setup* 3.1*, assume that there is a point* $\eta \in \text{Reg}\, Y$ *and an integer* l *with* $0 < l < d$ *such that*

(1) $\pi^{-1}(\eta) = \{\xi_0, \xi_1, \dots, \xi_{d-l}\} \subset \operatorname{Reg} X$

(2) *π is unramified at ξ_i for $1 \leq i \leq d-l$.*

Then there is a subgroup G' of G such that under suitable re-numbering $\{x_1, \dots, x_d\}$ appeared in Setup 3.1*,*

(a) *G' acts on $\{x_1, \dots, x_l\}$ transitively, and*

(b) *an arbitrary element of G' fixes x_j for any $j > l$.*

Proof. The proof is the essentially same with that of [13, Prop. 1.11]. Choose an affine open subset $\operatorname{Spec} B \subset \operatorname{Reg} Y$ such that $\eta \in \operatorname{Spec} B$ and $\pi^{-1}(\operatorname{Spec} B) \subset \operatorname{Reg} X$. Since $\pi^{-1}(\operatorname{Spec} B)$ is affine, we denote it by $\operatorname{Spec} A$. Since A is integral over B, we can choose $\alpha \in A$ such that $A = B[\alpha]$ and the minimal polynomial $f(T)$ of α over $k(Y) = \text{f.f.}(B)$ belongs $B[T]$. Let B_η be the local ring at $\eta \in \operatorname{Spec} B$ with maximal ideal $\mathfrak{m}_\eta$, and $\widehat{B}_\eta$ the $\mathfrak{m}_\eta$-adic completion of B_η. Let $f(T) = f_0(T) \cdots f_s(T)$ be the irreducible decomposition of $f(T)$ in $\text{f.f.}(\widehat{B}_\eta)[T]$. So we have

$$\text{f.f.}(\widehat{B}_\eta) \otimes_B A = \text{f.f.}(\widehat{B}_\eta)[T]/f(T) = \bigoplus_{i=0}^{s} \text{f.f.}(\widehat{B}_\eta)[T]/f_i(T) \tag{11}$$

by the Chinese remainder theorem.

On the other hand, it is not hard to see that

$$\text{f.f.}(\widehat{B}_\eta) \otimes_B A \cong \bigoplus_{i=0}^{d-l} \text{f.f.}(\widehat{A}_{\xi_i}), \tag{12}$$

where $\widehat{A}_{\xi_i}$ is the completion of the local ring A_{ξ_i} at $\xi_i \in X$. For details, consult [12, Sections 16 and 17]. Since $\text{f.f.}(\widehat{B}_\eta) \otimes_B A$ is Artinian, two decompositions (11) and (12) into fields must coincide. Hence $s = d - l$, and

$$\text{f.f.}(\widehat{B}_\eta)[T]/f_i(T) \cong \text{f.f.}(\widehat{A}_{\xi_i}) \ (i = 0, 1, \dots, d-l)$$

after renumbering the polynomials. Since π is unramified at ξ_i for $i = 1, \dots, d-l$, $\text{f.f.}(\widehat{B}_\eta) = \text{f.f.}(\widehat{A}_{\xi_i})$, which means $\deg f_i(T) = 1$. Hence there is an element $\alpha_i \in \text{f.f.}(\widehat{B}_\eta)$ so that $f_i(T) = T - \alpha_i$. Since $f_0(T) = \frac{f(T)}{(T-\alpha_1)\cdots(T-\alpha_{d-l})}$ is a polynomial in

$$\text{f.f.}(B)[\alpha_1, \dots, \alpha_{d-l}][T] = k(Y)[\alpha_1, \dots, \alpha_{d-l}][T]$$

and irreducible over $\text{f.f.}(\widehat{B}_\eta)$, it is also irreducible over $k(Y)[\alpha_1, \dots, \alpha_{d-l}]$. Let G' be the Galois group of the extension $L/k(Y)[\alpha_1, \dots, \alpha_{d-l}]$, which is, needless to say, Galois. Then G' can be regard as a subgroup of G and has required properties. □

4 Projection from a point on the Hermitian curve

First we give a lemma on a permutation group.

Lemma 4.1 *Let G be a group acting the d-symbols $\{x_1, \dots, x_d\}$ transitively. If there is a subgroup G' of G such that*

(1) *$\sigma'(x_d) = x_d$ for any $\sigma' \in G'$, and*

(2) *G' acts on $\{x_1, \dots, x_{d-1}\}$ transitively,*

then the action of G to $\{x_1, \dots, x_d\}$ is 2-fold transitive.

Proof. For arbitrary two symbols x_i and x_j, we can find an element $\sigma \in G$ so that $\sigma(x_i) = x_1$ and $\sigma(x_j) = x_d$. In fact, if $x_j = x_d$, then we can find $\sigma' \in G'$ so that $\sigma'(x_i) = x_1$ from the assumption (2). When $x_j \neq x_d$, first choose $\sigma \in G$ so that $\sigma(x_j) = x_d$. Then choose $\sigma' \in G'$ so that $\sigma'(\sigma(x_i)) = x_1$. Hence $\sigma'\sigma$ has the required property. □

Now we go back to the original situation described in Introduction. In this section, we prove the first part of Theorem 2. We handle the Hermitian curve in more concrete way. So we prepare some additional notation. The line at infinity with respect to the inhomogeneous coordinates x, y in (1) meets H at only one point, which is denoted by P_∞. For a point $P \in H \setminus \{P_\infty\}$, we denote by $P = P_{a,b}$ when $x(P) = a$ anf $y(P) = b$. Then $b^q + b = a^{q+1}$ holds. It is easy to see that the tangent line at $P_{a,b}$ to H is given by

$$a^q x - y - b^q = 0. \tag{13}$$

Moreover if we consider $a^q x - y - b^q$ as a function on H, we have

$$\mathrm{div}\,(a^q x - y - b^q) = qP_{a,b} + P_{a^{q^2},b^{q^2}} - (q+1)P_\infty \tag{14}$$

where div is an abbreviation for 'divisor of'.

Theorem 4.2 *Let $P \in H \setminus H(\mathbb{F}_{q^2})$. Then the projection $\pi_P : H \to \mathbb{P}^1$ with center P is separable, and $G_P \cong AGL(1, \mathbb{F}_q)$.*

Proof. Since P_∞ is an $\mathbb{F}_{q^2}$-rational point, we may assume that $P = P_{a,b}$ with $b^q + b = a^{q+1}$. Since the family of lines passing through P is $\{y - b = t(x - a) \mid t \in \mathbb{P}^1\}$, we can regard t as a coordinate of the target $\mathbb{P}^1$ of π_P. Substitute $y - b = t(x - a)$ in (1), and put $u = x - a$. Then we have

$$\begin{aligned} & x^{q+1} - t^q x^q - tx + a^q t^q + at - (b^q + b) \\ = \;& (u^q + (a - t^q)u^{q-1} + a^q - t)u = 0. \end{aligned}$$

Hence the extension $k(H)/k(t)$ via π_P^* is obtained by adding a root u of the polynomial

$$U^q + (a - t^q)U^{q-1} + a^q - t \tag{15}$$

in U over $k(t)$, which has no multiple root. Since $\deg \pi_P = q$, the polynomial is irreducible. So the Galois group G_P of π_P is that of (15). Since P is not $\mathbb{F}_{q^2}$-rational, $\pi_P^{-1}(\pi_P(P)) = \{P, P'\}$ with $P' \neq P$ and π_P is unramified at P' (see, for example [7, Lem. 3.1]). Therefore G_P acts on the q roots of (15) 2-fold transitively by Proposition 3.2 and Lemma 4.1. So we have $G_P \cong AGL(1, \mathbb{F}_q)$ by Lemma 2.5. □

Theorem 4.3 *Let $P \in H \setminus H(\mathbb{F}_{q^2})$, and $\widetilde{H_P}$ the Galois closure curve for $\pi_P : H \to \mathbb{P}^1$ explained in Introduction. Then the genus of $\widetilde{H_P}$ is $(q-1)^2 q/2$.*

Proof. We follow the notation used in the proof of Theorem 4.2. Moreover, let v be a root of $(a^q - t)V^{q-1} + a - t^q$, which corresponds Eq. (7) in the proof of Lemma 2.5. Then, from the proof, we have the field extension

$$k(\widetilde{H_P}) = k(t, u, v) \supset k(H) = k(t, u) = k(x, y)$$

with equations

$$\begin{aligned} &y^q + y = x^{q+1} \\ &y - b = t(x - a) \qquad (16) \\ &u^q + (a - t^q)u^{q-1} + a^q - t = 0 \\ &(a^q - t)v^{q-1} + a - t^q = 0. \qquad (17) \end{aligned}$$

Put $w = (x - a)v$. Then $k(\widetilde{H_P}) = k(H)[w]$. We find the minimal polynomial of w over $k(H) = k(x, y)$. Using (16), eliminate t from (17). Then

$$(x - a)^{q-1}(a^q x - y - b^q)v^{q-1} + (a^{1/q}x - y - b^{1/q})^q = 0.$$

So the extension $k(\widetilde{H_P}) = k(H)[w]/k(H)$ is given by

$$w^{q-1} + \frac{(a^{1/q}x - y - b^{1/q})^q}{a^q x - y - b^q} = 0,$$

which is a Kummer extension. From (14), we have

$$\operatorname{div} \frac{(a^{1/q}x - y - b^{1/q})^q}{a^q x - y - b^q} = q^2 P_{a^{1/q^2}, b^{1/q^2}} - P_{a^{q^2}, b^{q^2}} - (q^2 - 1)P_\infty.$$

Applying [14, III 7.3] to our situation, we know that π_P is ramified at exactly two points $P_{a^{1/q^2}, b^{1/q^2}}$, $P_{a^{q^2}, b^{q^2}}$, and the ramification index is $q-1$ at each point. Hence the genus of $\widetilde{H_P}$ is $(q-1)^2 q/2$ by Riemann-Hurwitz formula. □

5 Projection from a point outside the Hermitian curve

Next we consider the case where the center P of the projection is outside $(\mathbb{P}^2(\mathbb{F}_{q^2}) \cup H)$. We may assume that P is in the affine plane with respect to the affine coordinates x, y. In fact, *if P is on the line at infinity, we can find an automorphism τ of $\mathbb{P}^2$ over $\mathbb{F}_{q^2}$ such that $\tau(H) = H$ and $\tau(P)$ is in the affine plane* (see Remark 5.1 below).

Remark 5.1 The italicized statement above follows from the following two facts.

(i) The line at infinity is the tangent line at P_∞ to H;

(ii) Any automorphism of H is defined over $\mathbb{F}_{q^2}$, and the group of automorphisms acts on the set of $\mathbb{F}_{q^2}$-rational points $H(\mathbb{F}_{q^2})$ transitively (see [7, Sec. 3]).

Proof of the italicized statement: Choose an automorphism τ of H such that $\tau(P_\infty) = P_{0,0}$. Then $\tau(P)$ lies on the tangent line at $P_{0,0}$ to H. The only one point of the tangent line lies on the line at infinity, which is the intersection of two tangent lines at P_∞ and $P_{0,0}$ to H. Since both of the tangent lines are defined over $\mathbb{F}_{q^2}$, so is the intersection point. Since P is not $\mathbb{F}_{q^2}$-rational, neither is $\tau(P)$. Hence $\tau(P)$ is in the affine plane.

Lemma 5.2 *Let P be a point of $\mathbb{P}^2 \setminus H$. If P is not $\mathbb{F}_{q^2}$-rational, then there is a line L passing through P such that $L.H = qQ + Q'$ with $Q \neq Q'$.*

Proof. We may assume that P is in the affine plane with respect to the affine coordinates x, y, say $P = (a, b)$. Consider the tangent line T_Q at $Q = P_{\alpha,\beta} \in H$, which is given by $\alpha^q x - y - \beta^q = 0$. The system of equations in two variables α, β

$$\begin{cases} \alpha^q a - b - \beta^q = 0 \\ \beta^q + \beta = \alpha^{q+1} \end{cases}$$

is equivalent to

$$\begin{cases} \alpha a^{1/q} - b^{1/q} - \beta = 0 \\ \beta^q + \beta = \alpha^{q+1}. \end{cases} \tag{18}$$

For any solution (α, β) of (18), we have

$$T_{P_{\alpha,\beta}}.H = qP_{\alpha,\beta} + P_{\alpha^{q^2},\beta^{q^2}} \tag{19}$$

(see [7, Lem. 3.1]), and $T_{P_{\alpha,\beta}} \ni P$. We want to show $P_{\alpha,\beta} \neq P_{\alpha^{q^2},\beta^{q^2}}$ for some solution (α, β). From (18), we have

$$\alpha^{q+1} - a\alpha^q - a^{1/q}\alpha + b + b^{1/q} = 0, \tag{20}$$

which has $q+1$ distinct roots because $b^q + b \neq a^{q+1}$. If α is an element of $\mathbb{F}_{q^2}$, then so is β. Hence if the two roots of Eq. (20) are elements of $\mathbb{F}_{q^2}$, then P is $\mathbb{F}_{q^2}$-rational because P is the intersection of two tangent lines defined over $\mathbb{F}_{q^2}$. Therefore we can find a solution of (18) which is not $\mathbb{F}_{q^2}$-rational. So $P_{\alpha,\beta} \neq P_{\alpha^{q^2},\beta^{q^2}}$. □

Theorem 5.3 *Let $P \in \mathbb{P}^2 \setminus (\mathbb{P}^2(\mathbb{F}_{q^2}) \cup H)$. Then the projection $\pi_P : H \to \mathbb{P}^1$ with center P is separable, and $G_P \cong PGL(2, \mathbb{F}_q)$.*

Proof. As already explained, we may assume that $P = (a, b)$ with respect to the affine coordinates x, y. Hence the family of lines passing through P is $\{y - b = t(x - a) \mid t \in \mathbb{P}^1\}$. Substituting $y - b = t(x - a)$ into (1), we know the minimal polynomial of x over $k(t)$ via π_P^* is

$$f(X) = X^{q+1} - t^q X^q - tX + a^q t^q + at - (b^q + b).$$

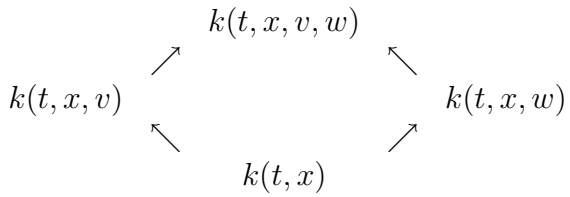
Since $k(\widetilde{H_P})$ is the field obtained by adding all the roots of $f(X)$ to $k(t)$, we wish to find them. Put $V = 1/(X - x)$. Then the roots of $f(X)$ other than x come from the roots of the polynomial

$$(x^q - t)V^q + (x - t^q)V + 1 \tag{21}$$

in V (see (3) in the proof of Lemma 2.4). From Lemma 5.2 with Proposition 3.2 and Lemma 4.1, G_P acts on the set of roots of $f(X)$ 2-fold transitively. Hence (21) is irreducible over $k(t, x)$ by Proposition 2.3. Let v be a root of (21), and put $W = V - v$. Then the roots of (21) other than v come from the roots of the polynomaial

$$(x^q - t)W^{q-1} + x - t^q. \tag{22}$$

If this polynomial is irreducible over $k(t, x, v)$, then the splitting height of $f(X)$ over $k(t)$ is at least 3. Hence the action of G_P is 3-fold transitive, and hence we can conclude that $G_P = PGL(2, \mathbb{F}_q)$ by Lemma 2.4. So our claim is that the polynomial (22) is irreducible over $k(t, x, v)$. Suppose that the polynomial (22) is irreducible as an element of $k(t, x)[W]$, and choose a root of the polynomial, say w. Look at the commutative diagram of field extensions



Since $[k(t,x,v) : k(t,x)] = q$ and $[k(t,x,w) : k(t,x)] = q-1$, we have $[k(t,x,v,w), k(t,x,v)] = q-1$, which means that the polynomial (22) is irreducible over $k(t,x,v)$.

We devote the rest of the proof to showing the polynomial (22) to be irreducible over $k(t,x)$. It is enough to show the polynomial is irreducible over $k[t,x]$, which can be regarded as the ring of the affine curve H' defined by

$$f(x,t) = x^{q+1} - t^q x^q - tx + a^q t^q + at - (b^q + b)$$

in $\mathbb{A}^2_{(x,t)}$. It is easy to see that H' is nonsingular. Consider the solution of the system of equations

$$\begin{cases} f(x,t) = 0 \\ x - t^q = 0. \end{cases}$$

Then

$$f(t^q, t) = -(t^{q+1} - a^q t^q - at + b^q + b) = 0. \tag{23}$$

Since $(a,b) \notin \mathbb{P}^2(\mathbb{F}_{q^2})$, there is a root ζ of (23) with $\zeta \notin \mathbb{F}_{q^2}$. Consider a point $R = (\zeta^q, \zeta) \in H'$, and the local ring $\mathcal{O}_{H',R}$ at R, which is regular local because H' is nonsingular. Since $\mathcal{O}_{H',R} \supset k[t,x]$, it is sufficient to see that the polynomial (22) is irreducible as an element of $\mathcal{O}_{H',R}[W]$. Put $x' = x - \zeta^q$ and $t' = t - \zeta$. Then the maximal ideal $\mathbf{m}$ of $\mathcal{O}_{H',R}$ is generated by these two elements, and $(\zeta^{q^2} - \zeta)x' + (a - \zeta^q)t'$ is an element of $\mathbf{m}$ corresponding the tangent line to H' at R. Note that $a - \zeta^q \neq 0$. In fact, if $a = \zeta^q$, then $a^{q+1} = a^q \zeta^q = b^q + b$ because ζ is a root of (23), which contradicts with our starting point. Hence x' is a local parameter at R, and hence a prime element of $\mathcal{O}_{H',R}$. The polynomial (22) can be written as

$$(x'^q - t' + \zeta^{q^2} - \zeta)W^{q-1} + (x' - t'^q). \tag{24}$$

Since $\zeta \notin \mathbb{F}_{q^2}$ and x' is a local parameter, we have

$$\begin{array}{ccc} x' & \not| & x'^q - t' + \zeta^{q^2} - \zeta \\ x' & | & x' - t'^q \\ x'^2 & \not| & x' - t'^q. \end{array}$$

Therefore the polynomial (24) is irreducible by Eisenstein's criterion. □

The last task is to compute the genus of $\widetilde{H_P}$, which involves tedious calculation. We use the same notations as those in the proof of Theorem 5.3. Let H_1 be the nonsingular projective curve whose function field is $k(t,x,v)$. Recall that $\widetilde{H_P}$ is the nonsingular curve whose function field is the Galois closure of

$k(H) = k(x, y)$ over $k(t)$, namely, $k(\widetilde{H_P}) = k(t, x, v, w)$. Hence the natural morphism $\widetilde{H_P} \to H$ splits into

$$\widetilde{H_P} \overset{\Theta}{\to} H_1 \overset{\Phi}{\to} H$$

via the field extensions

$$k(t, x, v, w) \overset{\Theta^*}{\hookleftarrow} k(t, x, v) \overset{\Phi^*}{\hookleftarrow} k(t, x) = k(x, y).$$

Theorem 5.4 (a) *The genus of H is $q(q-1)/2$.*

(b) *The genus of H_1 is $(q+2)q(q-1)/2$.*

(c) *The genus of $\widetilde{H_P}$ is $q(q^3-q-2)/2$.*

Proof. (a) Obvious.

(b) From (21) with $t = \frac{y-b}{x-a}$, the field extension $k(H_1) = k(H)[v]/k(H) = k(x, y)$ is given by

$$(x-a)^{q-1}(y - a^{1/q}x + b^{1/q})^q v^q + (y - a^q x + b^q)v + (x-a)^q = 0. \tag{25}$$

For simplification, we denote by $l = y - a^{1/q}x + b^{1/q}$ and $m = y - a^q x + b^q$. Put $v_1 = (x-a)lv$. Then $k(H_1) = k(H)[v_1]$ with equation

$$v_1^q + \frac{m}{l}v_1 + (x-a)^{q+1} = 0. \tag{26}$$

For the latter use, suspending the proof, we investigate the configuration of points on H that lie on the line $l = 0$ or $m = 0$.

Lemma 5.5 *We regard x, y as coordinates of the affine plane $\mathbb{A}^2 = \mathbb{A}^2_{(x,y)}$. Then there are $2q+2$ points $Q_1, \ldots, Q_{q+1}; Q'_1, \ldots, Q'_{q+1}$ of $\mathbb{A}^2$ such that*

$$H \cap \{l = 0\} = \{Q_1, \ldots, Q_{q+1}\}$$
$$H \cap \{m = 0\} = \{Q'_1, \ldots, Q'_{q+1}\},$$

and the line joining Q_i and Q'_i passes through $P = (a, b)$ and is tangent to H at Q_i.

Proof. Since each of the two lines is not defined over $\mathbb{F}_{q^2}$, it meets with H at $q+1$ distinct points. Let $P_{\alpha,\beta} \in l \cap H$. Then the tangent line $T_{P_{\alpha,\beta}}$ to H at $P_{\alpha,\beta}$ is given by $y - \alpha^q x + \beta^q = 0$. On the other hand, since $P_{\alpha,\beta} \in l$,

$$\beta - a^{1/q}\alpha + b^{1/q} = 0.$$

Hence we have

$$\beta^q - a\alpha^q + b = 0$$

and

$$\beta^{q^2} - a^q \alpha^{q^2} + b^q = 0.$$

The former equality means $(a, b) \in T_{P_{(\alpha,\beta)}}$, and the latter one $P_{(\alpha^{q^2},\beta^{q^2})} \in m$. Since $T_{P_{(\alpha,\beta)}}.H = qP_{(\alpha,\beta)} + P_{(\alpha^{q^2},\beta^{q^2})}$ [7, Lem. 3], we have completed the proof. □

Continuation of the proof of Theorem 5.4. We consider x and y to be functions on H. Then

$$\begin{aligned} \operatorname{div} l &= Q_1 + \cdots + Q_{q+1} - (q+1)P_\infty \\ \operatorname{div} m &= Q'_1 + \cdots + Q'_{q+1} - (q+1)P_\infty \end{aligned}$$

by Lemma 5.5. Moreover, it is easy to see that

$$\operatorname{div}(x-a) = \sum_{\delta \text{ with } \operatorname{Tr}\delta=0} P_{a,c+\delta} - qP_\infty,$$

where Tr is the trace map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$ and $c \in k$ with $c^q + c = a^{q+1}$.

In order to find the genus of H_1, we compute the length of $\left(\Omega_{H_1/H}\right)_{\tilde{P}}$ for $\tilde{P} \in H_1$, where $\Omega_{H_1/H}$ is the sheaf of relative differentials of H_1 over H. The computation is divided into 4 cases according to where $P = \Phi(\tilde{P})$ is.
Case b-1. If $P = \Phi(\tilde{P}) \notin (l)_0 \cup (m)_0 \cup \{P_\infty\}$, then

$$v_1^q + \frac{m(P)}{l(P)} v_1 + (x(P) - a)^{q+1} = 0$$

has q distinct roots as a polynomial in v_1. Hence $\Phi^{-1}(P)$ consists of q points by Kummer's theorem [14, III 3.7]. So length $\left(\Omega_{H_1/H}\right)_{\tilde{P}} = 0$.
Case b-2. Next we consider the case $P = Q' = \Phi(\tilde{P}) \in (m)_0$. Put $\alpha = x(Q')$, $\beta = y(Q')$ and $\gamma = v_1(\tilde{P})$. Hence $\beta^q + \beta = \alpha$ and $\gamma^q + (\alpha - a)^{q+1} = 0$ hold. Furthermore, put

$$\begin{cases} r = v_1 - \gamma \\ s_1 = x - \alpha \\ s_2 = y - \beta. \end{cases}$$

We denote by $e_{\tilde{P}}$ the ramification index at $\tilde{P}$ for Φ, and by $f = v_{\tilde{P}}(r)$, where $v_{\tilde{P}}$ is the valuation at $\tilde{P} \in H_1$. A local equation of H around Q' is given by

$$s_2^q + s_2 = s_1^{q+1} + \alpha s_1^q + \alpha^q s_1 \tag{27}$$

and the extension

$$k(H_1) = k(v_1, x, y) = k(r, s_1, s_2) \big/ k(H) = k(x, y) = k(s_1, s_2)$$

is given by

$$r^q + \frac{m}{l}r + \frac{m}{l}\gamma + s_1^{q+1} + (\alpha - a)s_1^q + (\alpha - a)^q s_1 = 0 \tag{28}$$

because of (26). Note that l and m can be represented by using s_1 and s_2 as

$$l = s_2 - a^{1/q}s_1 + (\beta - a^{1/q}\alpha + b^{1/q}) \tag{29}$$

$$m = s_2 - a^q s_1. \tag{30}$$

The constant term $\beta - a^{1/q}\alpha + b^{1/q}$ of l is nonzero because $Q' \notin (l)_0$. Hence $v_{Q'}(l) = 0$. Since $v_{Q'}(m) = 1$ by Lemma 5.5, $v_{\tilde{P}}(m) = e_{\tilde{P}}$. Therefore the values of $v_{\tilde{P}}$ at each term in (28) are as in Table 1.

term	r^q	$\frac{m}{l}r$	$\frac{m}{l}\gamma$	s_1^{q+1}	$(\alpha - a)s_1^q$	$(\alpha - a)^q s_1$
$v_{\tilde{P}}$	qf	$e_{\tilde{P}} + f$	$e_{\tilde{P}}$	$e_{\tilde{P}}(q+1)$	$e_{\tilde{P}}q$	$e_{\tilde{P}}$

Table 1: Values of $v_{\tilde{P}}$

We prove that $e_{\tilde{P}} = q$ and $f = 1$. Obviously $e_{\tilde{P}} < \min\{e_{\tilde{P}} + f, e_{\tilde{P}}(q+1), e_{\tilde{P}}q\}$ holds, and $e_{\tilde{P}} \leq qf$ because $e_{\tilde{P}} \leq \deg \Phi = q$.

Suppose $e_{\tilde{P}} < q$. Then

$$\frac{m}{l}\gamma + (\alpha - a)^q s_1 \equiv 0 \mod \mathbf{m}_{\tilde{P}}^{e_{\tilde{P}}+1}$$

by (28) and Table 1, where $\mathbf{m}_{\tilde{P}}$ is the maximal ideal at $\tilde{P}$. In other words, by (29) and (30),

$$\{(s_2 - a^q s_1)\gamma + (\alpha - a)^q(s_2 - a^{1/q}s_1)s_1 + (\beta - a^{1/q}\alpha + b^{1/q})(\alpha - a)^q s_1\}/l \equiv 0 \mod \mathbf{m}_{\tilde{P}}^{e_{\tilde{P}}+1}. \tag{31}$$

Since the denominator l of (31) is a unit of $\mathcal{O}_{\tilde{P}}$ and $(\alpha - a)^q(s_2 - a^{1/q}s_1)s_1 \in \mathbf{m}_{\tilde{P}}^{2e_{\tilde{P}}}$, we have

$$(s_2 - a^q s_1)\gamma + (\beta - a^{1/q}\alpha + b^{1/q})(\alpha - a)^q s_1 \equiv 0 \mod \mathbf{m}_{\tilde{P}}^{e_{\tilde{P}}+1}. \tag{32}$$

On the other hand, we know that

$$\begin{aligned}&(s_2 - a^q s_1)\gamma + (\beta - a^{1/q}\alpha + b^{1/q})(\alpha - a)^q s_1 \\ &\equiv (\alpha - a)^q(b^q + b - a^{q+1})^{1/q}s_1 \mod \mathbf{m}_{\tilde{P}}^{e_{\tilde{P}}+1},\end{aligned}$$

because

$$\begin{aligned}&(s_2 - a^q s_1)\gamma + (\beta - a^{1/q}\alpha + b^{1/q})(\alpha - a)^q s_1 = \\ &\quad (s_1^{q+1} + \alpha s_1^q - s_2^q + (\alpha - a)^q s_1)\gamma + (\beta - a^{1/q}\alpha + b^{1/q})(\alpha - a)^q s_1 \quad \text{(by (27))} \\ &\quad \equiv (\alpha - a)^q(\gamma + \beta - a^{1/q}\alpha + b^{1/q}) \mod \mathbf{m}_{\tilde{P}}^{e_{\tilde{P}}+1}\end{aligned}$$

and

$$\begin{aligned} & \gamma+\beta-a^{1/q}\alpha+b^{1/q} \\ = \; & -(\alpha-a)^{1+1/q}+\beta-a^{1/q}\alpha+b^{1/q} \\ = \; & (b^q+b-a^{q+1})^{1/q} \end{aligned}$$

by $\gamma^q+(\alpha-a)^{q+1}=0$, $\beta^q+\beta=\alpha$ and $\beta-a^q\alpha+b^q=0$. The last condition comes from the assumption $Q'=(\alpha,\beta)\in(m)_0$. Here $\alpha-a\neq 0$. In fact, if $\alpha-a=0$, then the line $x=a$ is tangent to H at Q', which is absurd because the line passes through P_∞. Since $(a,b)\notin H$, b^q+b-a^{q+1} is not zero either. So

$$\begin{aligned} & v_{\tilde{P}}((s_2-a^qs_1)\gamma+(\beta-a^{1/q}\alpha+b^{1/q})(\alpha-a)^qs_1) \\ = \; & v_{\tilde{P}}((\alpha-a)^q(b^q+b-a^{q+1})^{1/q}s_1) \\ = \; & v_{\tilde{P}}(s_1)=e_{\tilde{P}}, \end{aligned}$$

which contradicts to (32). Hence we have $e_{\tilde{P}}=qf$. Since $e_{\tilde{P}}\leq q$, we can conclude that $e_{\tilde{P}}=q$ and $f=1$.

Now we compute the length of $(\Omega_{H_1/H})_{\tilde{P}}$. Since $v_{\tilde{P}}(r)=f=1$, r is a local parameter at $\tilde{P}\in H_1$. Since s_1 is a local parameter at $Q'=\Phi(\tilde{P})\in H$, $\mathrm{length}(\Omega_{H_1/H})_{\tilde{P}}=v_{\tilde{P}}(\frac{ds_1}{dr})$. From (27),

$$\frac{ds_2}{dr}=(s_1^q+\alpha^q)\frac{ds_1}{dr}. \tag{33}$$

From (28),

$$(r+\gamma)\frac{d(\frac{m}{l})}{dr}+\frac{m}{l}+(s_1^q+(\alpha-a)^q)\frac{ds_1}{dr}=0. \tag{34}$$

On the other hand, using the relation (33), we have

$$\begin{aligned} \frac{dl}{dr} &= (s_1^q+\alpha^q-a^{1/q})\frac{ds_1}{dr} \\ \frac{dm}{dr} &= (s_1^q+\alpha^q-a^q)\frac{ds_1}{dr} \end{aligned}$$

from Eq. (29) and Eq. (30) respectively. Hence

$$\frac{d(\frac{m}{l})}{dr}=\frac{\frac{dm}{dr}l-\frac{dl}{dr}m}{l^2}=\frac{(s_1^q+\alpha^q-a^q)l-(s_1^q+\alpha^q-a^{1/q})m}{l^2}\cdot\frac{ds_1}{dr}. \tag{35}$$

Substituting (35) for $\frac{d(\frac{m}{l})}{dr}$ in Eq. (34), we have

$$\{(r+\gamma)\frac{(s_1^q+\alpha^q-a^q)l-(s_1^q+\alpha^q-a^{1/q})m}{l^2}+s_1^q+(\alpha-a)^q\}\frac{ds_1}{dr}=-\frac{m}{l}. \tag{36}$$

Looking at the coefficient of $\frac{ds_1}{dr}$ modulo $\mathbf{m}_{\tilde{P}}$ carefully, we know the coefficient is a unit of $\mathcal{O}_{\tilde{P}}$. From (29), (30) and (27), $v_{\tilde{P}}(-\frac{m}{l}) = v_{\tilde{P}}(s_1) = e_{\tilde{P}} = q$. Therefore $v_{\tilde{P}}(\frac{ds_1}{dr}) = q$.
Case b-3. We prove that if $P = Q \in (l)_0$, then

$$\Phi^*(Q) = (q-1)\tilde{P} + \tilde{P}' \text{ with } \tilde{P} \neq \tilde{P}'.$$

We start from Eq. (25), namely

$$(x-a)^{q-1} l^q v^q + mv + (x-a)^q = 0.$$

Put $v_2 = 1/v$. Then

$$v_2^q + \frac{m}{(x-a)^q} v_2^{q-1} + \frac{l^q}{x-a} = 0. \tag{37}$$

Let $\alpha = x(Q)$ and $\beta = y(Q)$. Then $\alpha - a \neq 0$ by argument similar to the previous one, and $m(Q) \neq 0$ because $(m)_0 \cap (l)_0 = \emptyset$. So Eq. (37) is an integral equation over $\mathcal{O}_{H,Q}$. Hence $v_2 \in \mathcal{O}_{H_1,\tilde{P}}$ for any point $\tilde{P}$ lying over Q. Considering Eq. (37) modulo the maximal ideal $\mathbf{m}_Q$ of $\mathcal{O}_{H,Q}$, we have

$$v_2^{q-1} \left(v_2 + \frac{m(Q)}{(\alpha - a)^q} \right) = 0. \tag{38}$$

So there are at least two points lying over Q, say $\tilde{P}$ and $\tilde{P}'$. We may assume that $\tilde{P}$ corresponds the solution $v_2 = 0$ of (38) and $\tilde{P}'$ the solution $v_2 = -m(Q)/(\alpha - a)^q$. It is not hard to see that the ramification index at $\tilde{P}$ is $q-1$ and that at $\tilde{P}'$ is 1.
Case b-4. We consider the case $P \in (x-a)_0$. Considering Eq. (26) modulo the maximal ideal of $\mathcal{O}_{H,P}$, we know $\Phi^{-1}(P)$ consists of q distinct points by Kummer's theorem [14].
Case b-5. Finally we consider the ramification over P_∞. Put $\rho = 1/y$ and $\tau = x/y$. Then $\rho^q + \rho = \tau^{q+1}$ holds because $y^q + y = x^{q+1}$. Rewrite (26) by using ρ and τ:

$$v_1^q + \frac{1 - a^q\tau + b^q\rho}{1 - a^{1/q}\tau + b^{1/q}\rho} v_1 + \frac{(\tau - a\rho)^{q+1}}{\rho^{q+1}} = 0. \tag{39}$$

Put $v_2 = \rho v_1$. Then we have

$$v_2^q + \rho^{q-1} \frac{1 - a^q\tau + b^q\rho}{1 - a^{1/q}\tau + b^{1/q}\rho} v_2 + \frac{(\tau - a\rho)^{q+1}}{\rho} = 0.$$

Furthermore, put $v_3 = v_2 + 1$, $v_4 = v_3/\tau$, $v_5 = v_4 - a^{1/q}$ and $v_6 = v_5/\left(\frac{\rho}{\tau}\right)$ continuously. Then we get

$$v_6^q + \frac{1 - a^q\tau + b^q\rho}{1 - a^{\frac{1}{q}}\tau + b^{\frac{1}{q}}\rho} v_6 + \frac{(a^{q+1} + b^{\frac{1}{q}} - b^q) - (a^{q+1+\frac{1}{q}} - a^{\frac{1}{q}}b^q + a^q b^{\frac{1}{q}})\tau + a^{q+1}b^{\frac{1}{q}}\rho}{1 - a^{\frac{1}{q}}\tau + b^{\frac{1}{q}}\rho} = 0. \quad (40)$$

Looking at Eq. (40) modulo the maximal ideal of $\mathcal{O}_{H,P_\infty}$, we have

$$v_6^q + v_6 + (a^{q+1} + b^{\frac{1}{q}} - b^q) = 0.$$

So $\Phi^{-1}(P_\infty)$ consists of q distinct points.

Summing up, we can compute the genus g_1 of H_1 as

$$2g_1 - 2 = q\left(2\frac{q(q-1)}{2} - 2\right) + (q+1)q + (q+1)(q-2)$$

by Hurwitz's formula. Hence we have

$$g_1 = \frac{(q-1)q(q+2)}{2}.$$

(c) From (22) with $t = \frac{y-b}{x-a}$, the field extension $k(\widetilde{H_P}) = k(H_1)[w]/k(H_1)$ is given by

$$(x-a)^{q-1}l^q w^{q-1} + m = 0.$$

Put $w_1 = (x-a)lw$. Then $k(H_1)[w] = k(H_1)[w_1]$ and $w_1^{q-1} + \frac{m}{l}$. We already saw

$$\begin{aligned} \mathrm{div}_H l &= Q_1 + \cdots + Q_{q+1} - (q+1)P_\infty \\ \mathrm{div}_H m &= Q'_1 + \cdots + Q'_{q+1} - (q+1)P_\infty \end{aligned}$$

on H. Furthermore, $\Phi^{-1}(Q_i)$ consists of two points, one of which, say P_i is of ramification index $q-1$ and the other, say P'_i, is of ramification index 1, and $\Phi^{-1}(Q'_i)$ consists of a unique point, say R_i, with ramification index q. Therefore

$$\mathrm{div}_{H_1}\frac{m}{l} = \sum_{i=1}^{q+1} qR_i - \sum_{i=1}^{q+1}\left((q-1)P_i + P'_i\right).$$

By [14, III, 7.3], we know the behavior of the ramification of Θ:

(i) $\Theta^{-1}(R_i)$ consists of one point, say $\tilde{R}_i$, and $e_{\tilde{R}_i} = q-1$;

(ii) $\Theta^{-1}(P_i)$ consists of $q-1$ points, and each of the $q-1$ points is of ramification index 1;

(iii) $\Theta^{-1}(P_i')$ consists of one point, say $\tilde{P'}_i$, and $e_{\tilde{P'}_i} = q-1$;

(iv) For a point $P \in H_1$ other than the above points, $\Theta^{-1}(P)$ consists of $q-1$ points, and each of them is of ramification index 1.

Hence by Hurwitz's formula, we have

$$2\tilde{g} - 2 = (q-1)(2g_1 - 2) + 2(q+1)(q-2),$$

where $\tilde{g}$ is the genus of $\widetilde{H_P}$. So we have $\tilde{g} = q(q^3 - q - 2)/2$ □

References

[1] S. S. Abhyankar, Galois theory on the line in nonzero characteristic, Bull. Amer. Math. Soc. (N.S.) 27 (1992) 68–133.

[2] E. Ballico and A. Hefez, On the Galois group associated to a generically étale morphism, Comm. Algebra 14 (1986) 899–909.

[3] S. Fukasawa, Galois points on quartic curves in characteristic 3, Nihonkai Math. J. 17 (2006) 103–110.

[4] S. Fukasawa, On the number of Galois points for a plane curve in positive characteristic, to appear in Comm. Algebra.

[5] S. Fukasawa, Galois point with the nonabelian group, preprint, July 2006.

[6] S. Fukasawa, On the number of Galois points for a plane curve in positive characteristic II, preprint, Dec. 2006.

[7] M. Homma, Galois points for a Hermitian curve, Comm. Algebra 34 (2006) 4503–4511.

[8] E. Lluis, Variedades Algebraicas con Ciertas Condiciones en sus Tangentes, Bol. Soc. Mat. Mexicana 7 (1962) 47–56.

[9] K. Miura, Galois points on singular plane quartic curves, J. Algebra 287 (2005) 283–293.

[10] K. Miura and H. Yoshihara, Field theory for the function field of the quintic Fermat curve, Comm. Algebra 28 (2000) 1979–1988.

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

[12] M. Nagata, Local ring, Wiley, New York 1962.

[13] J. Rathmann, The uniform position principle for curves in characteristic p, Math. Ann. 276 (1987) 565–579.

[14] H. Stichtenoth, Algebraic function fields and codes, Springer-Verlag, Berlin, Heidelberg, New York 1993.

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

[16] H. Yoshihara, Galois lines for space curves, Algebra Colloquium 13 (2006) 455–469.

Received: July 16, 2007