Journal of Number Theory **89**, 14–30 (2001)
doi:10.1006/jnth.2000.2609, available online at http://www.idealibrary.com on IDEAL®

Rational Points on Picard Groups of Some Genus-Changing Curves of Genus at Least 2

Sangtae Jeong

Department of Mathematics, University of Texas, Austin, Texas 78712; and
[1]*Department of Mathematics, Seoul National University, Seoul, Korea 151-747*
E-mail: stj@math.snu.ac.kr

Communicated by D. Goss

Received December 28, 1998; published online April 17, 2001

For an algebraic curve C/K defined by $y^2 = x^p + a$ ($a \notin K^p$) with relative genus

$gal(K^{sep}/K)$ has a finite number of K-rational points as a variety, where K is a function field in one variable with a finite constant field of characteristic $p \geqslant 5$ and K^{sep} is the separable closure of K.

1. INTRODUCTION

It is well known that the Jacobian variety, denoted Jac(C), of a nonsingular projective curve C of genus $g \geqslant 2$ over an algebraically closed field is an abelian variety of dimension g. In fact, it is naturally isomorphic to the Picard group of divisors of degree 0 modulo linearly equivalence of the given curve. As a variety, little is known about the defining equations for Jacobians of curves. But we are interested in points on the Jacobian of a curve via the Albanese map defined by sending $P \in C$ to the class of $P - P_\infty$ in Jac(C), where P_∞ is the point at infinity. Here we will consider an algebraic curve C defined by $y^2 = x^p + a$ ($a \notin K^p$) over a function field K in one variable with a finite constant field of characteristic $p \geqslant 5$. It turns out that the given curve C is a typical example of algebraic curves that change genus under base field extensions. Indeed it is a singular curve of relative genus $g = (p-1)/2$ and absolute genus 0. It is shown in [V, J1, J2] that a class of such curves over K has a finite number of rational points.

For this curve C we will construct the Picard group of divisors of degree 0, denoted $\text{Pic}_K^0(C)$, of C/K fixed by the action of the Galois group $G = gal(K^{sep}/K)$, where K^{sep} is the separable closure of K. As we will see,

[1] Current address.

0022-314X/01 $35.00

it turns out that $\mathrm{Pic}_K^0(C)$ is an algebraic variety over K of dimension $g=(p-1)/2$, which corresponds to the relative genus of C. Without knowing the defining equations of this Picard group, it will be interesting to study the set of rational points on $\mathrm{Pic}_K^0(C)$ defined over K.

The purpose of the paper is to prove that for the algebraic curve C/K given above, the Picard group $\mathrm{Pic}_K^0(C)$ has finitely many K-rational points (Theorem 2) as a variety. As an easy corollary one sees then that the curve C has finitely many rational points by pointing out the above Albanese map is injective. On the other hand it is shown in [J1] that the explicit upper bound for the number of rational points of C is given in terms of the height of a and the genus g of the base field K: $\sharp C(K) \leqslant 2p^{6h(a)+3g-2}$.

Toward the proof of Theorem 2, the paper is organized as follows. To better understand the definition of $\mathrm{Pic}_K^0(C)$, in Section 2 we will summarize the definitions of divisors groups and the Galois group action both on divisors groups and on the function field of a curve. Section 3 is devoted to proving that the variety over K defined by $x-x^{p^r}=a_1\, {y_1}^{p^r}+a_2\, {y_2}^{p^r} + \cdots + a_n\, {y_n}^{p^r}$ has finitely many K-rational points under certain assumptions. By using computations of derivations on function fields, Section 4 is concerned with finding an equation of a variety associated to the Picard group and then with the proof of Theorem 2. Finally, in Section 5, we give an example of a surface whose rational points consists only of p points by explicitly bounding valuations of rational points on the surface and then prove that $\mathrm{Pic}_K^0(C)$ has only 5 rational points when C is defined by $y^2=x^5+a$ for infinitely many squares $a\notin K^5$, where K is a rational function field of characteristic 5.

2. PICARD GROUPS

Throughout this paper, we restrict K to a function field of one variable over a finite field of characteristic $p\geqslant 5$ and denote the separable closure of K by K^{sep}. And we will consider the algebraic curve C/K defined by $y^2=x^p+a$ ($a\notin K^p$). We see that it is of absolute genus 0 as it is parameterizable over any extension fields of K containing a pth root of a. Under the assumption $a\notin K^p$, we can apply the Riemann–Roch Theorem to show that the genus of C relative to K is $(p-1)/2$. For example, we refer to [Sil, Exercise 2.14] for explicit computations of genus of hyper-elliptic curves. By extending a base field K we assume that the a is a square in K so that the point at infinity $P_\infty=[0:a^{1/2}:0]$ is a rational point of C.

We shall construct the Picard group of divisors of degree 0, denoted $\mathrm{Pic}_K^0(C)$, of C/K fixed by the Galois group $G=gal(K^{sep}/K)$, which is analogous to the construction of the Jacobian of a smooth curve of higher genus. We refer to [M] for a more extensive exposition of Jacobians of smooth curves of genus at least 2. We now summarize the definitions of the Picard group of divisors of degree 0, $\mathrm{Pic}^0_K(C)$, of C/K fixed by the Galois group $G = gal(K^{sep}/K)$ that we shall use here.

The divisor group of a curve C, denoted $\mathrm{Div}(C)$, is the free abelian group generated by the points of C. By points we here mean that they have coordinates over K^{sep}. Then a divisor $D \in \mathrm{Div}(C)$ is expressed as a finite formal sum of the form $D = \sum_{P \in C} n_P(P)$, where the $n_P \in \mathbf{Z}$ and the P are points of C. The degree of D is defined by $\deg(D) = \sum_{P \in C} n_P$. Since C is defined over K, we let the Galois group G act on $\mathrm{Div}(C)$ in such a way that $D^\sigma = \sum_{P \in C} n_P(P^\sigma)$. We say that D is fixed by the group G if $D = D^\sigma$ for all $\sigma \in G$. We denote by $\mathrm{Div}_K(C)$ the group of divisors fixed by the Galois group G and by $\mathrm{Div}^0_K(C)$ the subgroup of divisors of degree 0 in $\mathrm{Div}_K(C)$. The Galois group G also acts on $f \in K^{sep}(C)$, which is the function field of C/K^{sep}, by acting on its coefficients. Then we can associate to f the divisor $\mathrm{div}(f)$ given by $\mathrm{div}(f) = \sum_{P \in C} v_P(f)(P)$. Now if $\sigma \in G$, then one easily sees that $\mathrm{div}(f^\sigma) = \mathrm{div}(f)^\sigma$. In particular, if $f \in K(C)$, then $\mathrm{div}(f) \in \mathrm{Div}_K(C)$. A divisor $D \in \mathrm{Div}(C)$ is principal if it is of the form $D = \mathrm{div}(f)$ for some non-zero function $f \in K^{sep}(C)$. By $\mathrm{Prin}(C)$ we now denote the group of principal divisors, which in fact a subgroup of $\mathrm{Div}^0(C)$, because $\mathrm{div}(f)$ has degree 0 for any non-zero function $f \in K^{sep}(C)$. Two divisors D_1, D_2 are linearly equivalent, denoted $D_1 \sim D_2$, if $D_1 - D_2$ belongs to $\mathrm{Prin}(C)$. The Picard group of degree 0 of C, denoted $\mathrm{Pic}^0(C)$, is defined as the quotient of $\mathrm{Div}^0(C)$ by the subgroup of principal divisors, i.e., $\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{Prin}(C)$. Finally $\mathrm{Pic}^0_K(C)$ is well-defined as the subgroup of $\mathrm{Pic}^0(C)$ fixed by the Galois group G as justified in Proposition 1 below.

PROPOSITION 1. *Let C, K, G be the same before. Then*

$$\mathrm{Pic}^0_K(C) = \mathrm{Div}^0_K(C)/\mathrm{Prin}_K(C).$$

Proof. We consider the following exact sequence:

$$1 \to K^{sep}(C)^*/K^{sep\,*} \to \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0.$$

Since $\mathrm{Prin}(C) = K^{sep}(C)^*/K^{sep\,*}$, from the long exact sequence it is enough to show that $H^1(G, K^{sep}(C)^*/K^{sep\,*}) = 0$. Consider another exact sequence:

$$1 \to K^{sep\,*} \to K^{sep}(C)^* \to K^{sep}(C)^*/K^{sep\,*} \to 0. \qquad (*)$$

From the long exact sequence of $(*)$ we see easily that $H^1(G, K^{sep}(C)^*/K^{sep*}) = 0$ if and only if $H^2(G, K^{sep})$ injects into $H^2(G, K^{sep}(C)^*)$. Here $H^2(G, K^{sep})$ is nothing but the Brauer group of K, denoted $\mathrm{Br}(K)$. Now the result follows from the well-known fact that $\mathrm{Br}(K)$ injects into $\mathrm{Br}(K(C))$ if the curve C/K has a K-rational point. ▌

Let $\mathscr{A}$ denote the category of separable extensions of K in K^{sep}. Let F be an object of $\mathscr{A}$, then $G_F = gal(K^{sep}/F)$ is a subgroup of $G = gal(K^{sep}/K)$. Denoting by $\mathrm{Div}_F(C)$ the F-rational members of $\mathrm{Div}(C)$, i.e., the group of divisors fixed by G_F, we also set $\mathrm{Div}_F^0(C) = \mathrm{Div}^0(C) \cap \mathrm{Div}_F(C)$, $\mathrm{Prin}_F(C) = \mathrm{Prin}(C) \cap \mathrm{Div}_F^0(C)$, $\mathrm{Pic}_F^0(C) = \mathrm{Dic}_F^0(C) + \mathrm{Prin}(C)/\mathrm{Prin}(C)$. Then we show that $\mathrm{Pic}_F^0(C)$ is isomorphic to $\mathrm{Div}_F^0(C)/\mathrm{Prin}_F(C)$ and in particular, if $F = K$, then $\mathrm{Pic}_K^0(C) = \mathrm{Div}_K^0(C)/\mathrm{Prin}_K(C)$, which also shows Proposition 1.

We will close this section by showing a useful lemma on $\mathrm{Div}_K^0(C)$, which we will use in Section 4.

LEMMA 1. *Let $f \in K^{sep}(C)$ be a non-zero rational function on C and* $\mathrm{div}(f) \in \mathrm{Div}_K^0(C)$. *Then there is a non-zero $\lambda \in K^{sep}$ such that $\lambda f \in K(C)$.*

Proof. If $\mathrm{div}(f) \in \mathrm{Div}_K^0(C)$, then $\mathrm{div}(f) = \mathrm{div}(f^\sigma)$ for all $\sigma \in G$, hence $\mathrm{div}(f^\sigma/f) = 0$. This implies that $f^\sigma/f = c_\sigma$, a constant depending on σ. From the relation we see that c defines a 1-cocycle from G to $K^{sep\,*}$. That is, $c_{\sigma\tau} = c_\sigma{}^\tau c_\tau$. By Hilbert Theorem 90, there is $\lambda \in K^{sep\,*}$ such that $c_\sigma = \lambda/\lambda^\sigma$. Therefore we have $f^\sigma/f = \lambda/\lambda^\sigma$ for all $\sigma \in G$, completing the proof. ▮

3. FINITENESS OF RATIONAL POINTS ON A VARIETY

Let K be a function field of one variable over a finite field of characteristic $p > 0$. We denote by M_K the set of normalized discrete valuations v of K, and by K_v the completion of K at the place $v \in M_K$. Indeed K_v is isomorphic to the field of formal power series with coefficients in $\mathbf{F}_q$, that is, $K_v = \mathbf{F}_q((t_v))$ where t_v is a local parameter at v. Note that the constant field $\mathbf{F}_q$ of K_v depends only on v. If $x \in K_v$ has a pole at v of order $n > 0$ then x is uniquely written as the Laurent series with coefficients in $\mathbf{F}_q$ in terms of a local parameter: $x = \sum_{i=-n}^{\infty} x_i t_v{}^i$. We can define the Hasse derivations $D_{t_v}^{(j)}$, $j \geqslant 0$ on K_v by

$$D_{t_v}^{(j)}\left(\sum_{i=-n}^{\infty} x_i t_v{}^i\right) = \sum_{i=-n}^{\infty} \binom{i}{j} x_i t_v{}^{i-j}.$$

Then we see that Hasse derivations depends only on the local parameter but we will drop the subscript for the local parameter from the notation of Hasse deviations if it causes no confusion. It is well known in [Sch] that $\{D^{(j)}, j \geqslant 0\}$ is a sequence of additive operators on K_v such that

(1) $D^{(0)}$ is the identity operator.

(2) $D^{(j)}(xy) = \sum_{i=0}^{j} D^{(i)}(x)\, D^{(j-i)}(y)$,

(3) $D^{(j)}(D^{(i)}(x)) = \binom{j+i}{i}\, D^{(j+i)}(x)$ for all $x, y \in K_v$.

We call such a sequence $\{D^{(j)}, j \geqslant 0\}$ iterative derivation on K_v. Since $K \subset \mathbf{F}_q((t_v))$ it is known in [HS] that $\{D^{(j)}, j \geqslant 0\}$ is also an iterative derivation on K with the property that $\{x \in K \mid D^{(j)}(x) = 0 \text{ for } 1 \leqslant j \leqslant p^r - 1\} = K^{p^r}$ for each $r \geqslant 1$. Note that K is a purely inseparable extension of K^{p^r} of degree p^r (see [Sti, III9.2]).

We will now consider a variety V/K defined by $x - x^{p^r} = a_1 {y_1}^{p^r} + a_2 {y_2}^{p^r} + \cdots + a_n {y_n}^{p^r}$, where $1, a_1, a_2, ..., a_n \in K$ are linearly independent over K^{p^r}. In what follows, whenever we refer to the variety V/K, we always assume that the coefficients $1, a_1, a_2, ..., a_n$ are linearly independent over K^{p^r}. Equivalently, by the generalized Wronskian property (see [GV, Theorem 1]) the matrix $A = (D^{(\varepsilon_j)} a_i)_{i,\, j=1, ..., n}$ is non-singular for some sequence of exponents $(\varepsilon_i)_{i=1}^n$ such that $0 < \varepsilon_1 < \varepsilon_2 < \cdots < \varepsilon_n < p^r$. In this section, by computing valuations of iterative derivations $D^{(j)}$ we aim to show that the variety V/K has finitely many rational points under the assumption $\varepsilon_n < p^r - 1$ (Theorem 1).

LEMMA 2. *For each place $v \in M_K$, there exists a constant c_v depending on v such that $c_v = 0$ for almost all places $v \in M_K$, so that for every $x \in K^*$, we have $v(D^{(j)} x) \geqslant v(x) - j + c_v$ for each $j \geqslant 1$.*

Proof. Fix an element $t \notin K^p$. We first consider the places $v \in M_K$ with $v(t) \geqslant 0$. If $t - t(v)$ is a local parameter at the chosen place v, then we claim $D_t^{(j)} = D_{t-t(v)}^{(j)}$. Since t is a separable element, for given $x \in K^*$ there is an algebraic relation $f(x, t) = 0$ depending on x. From the implicit function theorem this relation gives $D_t^{(j)}(x) = \sum_{i=0}^{j} f_{ij} D_{t-t(v)}^{(i)}(x)$ for some f_{ij}. Now by substituting $(t - t(v))^j$ for x in the equation above we can use induction on $j \geqslant 1$ to show that $f_{jj} = 1$, $f_{ij} = 0$ if $i < j$. Hence we calculate $v(D_t^{(j)} x) = v(D_{t-t(v)}^{(j)} x) \geqslant v(x) - j$ for every $x \in K^*$ and $j \geqslant 1$. So $c_v = 0$ for such a place v.

Let v be a place with a local parameter u for which $v(t) < 0$. Then we use the chain rule of Hasse derivations [Ha] to calculate $v(D_t^{(j)} x)$ for every $x \in K^*$ and $j \geqslant 1$ as follows:

$$\begin{aligned} v(D_t^{(j)} x) &= v\Bigg(\sum_{\substack{i_1, i_2, ..., i_j \geqslant 0 \\ i_1 + 2i_2 + \cdots + ji_j = j}} (D_u^{(i_1 + i_2 + \cdots + i_j)} x) \binom{i_1 + i_2 + \cdots + i_j}{i_1, ..., i_j} \\ &\qquad \times (D_t^{(1)} u)^{i_1} \cdots (D_t^{(j)} u)^{i_j} \Bigg) \\ &\geqslant \min_{\substack{i_1, i_2, ..., i_j \geqslant 0 \\ i_1 + 2i_2 + \cdots + ji_j = j}} \{ v(D_u^{(i_1 + i_2 + \cdots + i_j)} x) + v(*) \} \\ &\geqslant \min_{\substack{i_1, i_2, ..., i_j \geqslant 0 \\ i_1 + 2i_2 + \cdots + ji_j = j}} \{ v(x) - (i_1 + i_2 + \cdots + i_j) + v(*) \} \end{aligned}$$

$$\begin{aligned} &\geqslant \min_{\substack{i_1, i_2, ..., i_j \geqslant 0 \\ i_1 + 2i_2 + \cdots + ji_j = j}} \{v(x) - j + v(*)\} \\ &= v(x) - j + c_v, \end{aligned}$$

where $c_v = \min\{v(*)\}$ and $(*)$ means the remaining part of the term in the first equality, which is independent of x. Note also that $c_v = 0$ for all but only finitely many places. The result now follows. ▮

Lemma 3. *Let V/K be a variety defined by $x - x^{p^r} = a_1 y_1{}^{p^r} + a_2 y_2{}^{p^r} + \cdots + a_n y_n{}^{p^r}$. If $\varepsilon_n < p^r - 1$, then there exists a finite set S of places of K such that every x-component of rational points of V has no poles at every place v not in S.*

Proof. Since $1, a_1, a_2, ..., a_n$ are linearly independent over K^{p^r}, from the generalized Wronskian property [GV] the matrix $A = (D^{(\varepsilon_j)} a_i)_{i,\, j = 1, ..., n}$ is non-singular for some sequence of exponents such that $0 < \varepsilon_1 < \varepsilon_2 < \cdots < \varepsilon_n < p^r$. Let $B = (b_{ij})$ be the inverse matrix of A, then by characteristic p, we obtain that for each $j = 1, ..., n$,

$$D^{(\varepsilon_j)}(x) = D^{(\varepsilon_j)}(x - x^{p^r}) = \sum_{i=1}^{n} D^{(\varepsilon_j)}(a_i) \cdot y_i^{p^r}.$$

Hence we get $y_i^{p^r} = \sum_{j=1}^{n} b_{ij} D^{(\varepsilon_j)}(x)$ for each $1 \leqslant i \leqslant n$. Taking a valuation v of the equation gives

$$\begin{aligned} p^r v(y_i) &\geqslant \min_{1 \leqslant j \leqslant n} \{v(b_{ij}) + v(D^{(\varepsilon_j)}(x)\} \\ &\geqslant v(x) - \varepsilon_n + c_v{}', \qquad (1) \end{aligned}$$

where the second inequality comes from Lemma 2 and $c_v{}' = c_v + \min_{1 \leqslant j \leqslant n} \{v(b_{ij})\}$. Here we note that $c_v{}' = 0$ for almost all places v. On the other hand, if $v(x) < 0$, then

$$\begin{aligned} p^r v(x) &= v(x - x^{p^r}) \\ &\geqslant \min_{1 \leqslant i \leqslant n} \{v(a_i) + p^r v(y_i)\} \\ &\geqslant v(x) - \varepsilon_n + c_v{}'', \qquad (2) \end{aligned}$$

where $c_v{}'' = c_v{}' + \min_{1 \leqslant i \leqslant n}\{v(a_i)\}$ and the first equality follows from the strict triangle inequality and the third inequality comes from (1).

So from the inequality (2) we have $v(x) \geqslant (-\varepsilon_n + c_v{}'')/(p^r - 1)$. Suppose now that $c_v{}'' = 0$. Then we easily see that $v(x) > -1$ from the hypothesis $\varepsilon_n < p^r - 1$. Hence $v(x) \geqslant 0$ since v is an integer-valued function on K. But this contradicts the hypothesis $v(x)<0$. So the above discussion shows that $\{v\in M_K \mid v(x)<0\}\subseteq\{v\in M_K \mid c_v{''}\neq 0\}$ for every x-coordinate of rational points of V. It then suffices to take $S=\{v\in M_K \mid c_v{''}\neq 0\}$, as $c_v{''}=0$ for all but a finite number of places v. ▌

THEOREM 1. *Let V/K be defined by $x-x^{p^r}=a_1\,{y_1}^{p^r}+a_2\,{y_2}^{p^r}+\cdots+a_n\,{y_n}^{p^r}$. If $\varepsilon_n<p^r-1$, then the set $V(K)$ of K-rational points of V is finite.*

Proof. Let $V(K)$ be the set of K-rational points on the variety V. Then characteristic p clearly guarantees that $V(K)$ has a group structure under addition, which is defined component-wise. From Lemma 3 we see that there is a finite set S of places of K such that every x-coordinate of rational points of V has no poles at every place $v\notin S$. In the case where S is nonempty, viewing every x-coordinate as an element in the completion K_v of K at each place $v\in S$ we can define a map

$$\phi\colon V(K)\to\bigoplus_{v\in S}{\mathbf{F}_q}^{(|v(x)|+1)},$$

$$(x, y_1, y_2, ..., y_n)\mapsto(\mathrm{coeff}(x, t^{v(x)}; t^0))_{v\in S},$$

where $\mathrm{coeff}(x, t^{v(x)}; t^0)$ is a $(|v(x)|+1)$-tuple of the coefficients of terms whose degrees run over from $v(x)$ to 0 in the Laurent series expansion of x. We can then check that the map is well-defined from the observation on S made above. Moreover it is obvious that ϕ is a group homomorphism. To prove the finiteness of $V(K)$, since the codomain is only a finite group, it is enough to show that the kernel of ϕ, denoted $\mathrm{Ker}(\phi)$, is finite, in fact, only trivial. If $(x, y_1, y_2, ..., y_n)\in\mathrm{Ker}(\phi)$, then it follows from the definition of ϕ that $v(x)>0$ for every place $v\in S$. On the other hand, we know that $v(x)\geqslant 0$ for every place $\notin S$. Hence we observe that x has no poles at all, but x has zeros at finitely many places in S. This fact forces x to be 0. Thus, $y_1=y_2=\cdots=y_n=0$ follow from hypothesis that $1, a_1, a_2, ..., a_n$ are linearly independent over K^{p^r}. In the case where S is empty, we shall show that $V(K)$ is a group of order at most p^r. For any element $(x, y_1, y_2, ..., y_n)\in V(K)$, we note that x has no poles at all places, that is, $v(x)\geqslant 0$ for all $v\in M_K$. By a result of [Sil] II Proposition 1.2, x must be in the constant field $\mathbf{F}_q$ of K, in particular, $x=u^{p^r}$ for some $u\in\mathbf{F}_q$. Hence $x-x^{p^r}=(u-u^{p^r})^{p^r}$ is a p^rth power. Again the linearly independence of $1, a_1, a_2, ..., a_n$ over K^{p^r} implies that $x=u=u^{p^r}$ and $y_1, y_2, ..., y_n$ are all 0. ▌

Remark. As in the proof, can we give an explicit example of a variety V whose rational points consist only of p points, in the case where the set S is just empty and $r=1$? In Section 5 we will give a variety given by $x-x^p=2b^3y^p+bz^p$ that has only p rational points for infinitely many

$b \notin K^p$. Using the result, we show that $\mathrm{Pic}_K^0(C)(K)$ is a cyclic group of order 5 for infinitely many b when C is given by $y^2 = x^5 + b^2$ over a rational function field K of one variable with a finite field of characteristic $p = 5$.

4. FINDING AN EQUATION OF A VARIETY

Consider the equation of a curve $C/K: y^2 = x^p + a$ $(a \notin K^p)$ with relative genus $g = (p-1)/2$ and absolute genus 0. In this section, via computations of derivations on function fields of C we will derive an equation of a variety associated with the Picard group $\mathrm{Pic}_K^0(K)$. As we will see, the assumption that a is a square in K leads us to show that the equation we will obtain is K-isomorphic to the equation which we have already dealt with in the previous section.

Let $a = \xi^p$ and let $K' = K(\xi)$, then we see that K' is a purely inseparable extension of degree p over K. We choose a derivation δ: $K' \to K'$ such that $\mathrm{Ker}(\delta) = \{u \in K' : \delta u = 0\} = K$. Since K' is a purely inseparable extension over K, for simplicity of computations we can select δ so that $\delta(\xi) = 2$ (see [La, p. 360]). Let $K(C)$, $K'(C)$ be the function field of C over K and K', respectively. By assigning $\delta x = 0$, $\delta y = 0$, δ can be extended to $K'(C)$. We note that $\mathrm{Ker}(\delta) = K(C)$ and it turns out that the curve C is rational over K' and $K'(C) = K'(t)$ for a variable t:

$$x = t^2 - \xi \tag{3}$$

$$y = t^p. \tag{4}$$

One can easily express t in terms of x, y as

$$t = \frac{y}{(x+\xi)^g}. \tag{5}$$

Taking the δ of Eq. (3), we obtain $\delta t = \frac{1}{t}$ and then $\delta(\frac{1}{t}) = -1/t^3$.

Let us fix P_∞ the point at infinity on the curve C, for example $P_\infty = [0 : a^{1/2} : 0]$. For $D_1, D_2, D_3 \in \mathrm{Div}_K^0(C)$ it follows from the Riemann–Roch Theorem that $D_1 \sim (P_1) + (P_2) + \cdots + (P_g) - g(P_\infty)$, $D_2 \sim (P_{g+1}) + (P_{g+2}) + \cdots + (P_{2g}) - g(P_\infty)$, $D_3 \sim (P_{2g+1}) + (P_{2g+2}) + \cdots + (P_{3g}) - g(P_\infty)$, where $P_i = (x_i, y_i)$ $i = 1, ..., 3g$ are points on C. Let $f_1 := (t - t_{P_1})(t - t_{P_2}) \cdots (t - t_{P_g})$, $f_2 := (t - t_{P_{g+1}})(t - t_{P_{g+2}}) \cdots (t - t_{P_{2g}})$, $f_3 := (t - t_{P_{2g+1}})(t - t_{P_{2g+2}}) \cdots (t - t_{P_{3\,g}})$ be the function of degree g in $(K')^{sep}\,(C)$ associated with D_1, D_2, D_3 respectively, where $t_{P_i} = t_i$ is given by (5) for each $i = 1, ..., 3g$. Note that for each $i = 1, ..., 3g$ and $k = 1, ..., g$, the functions t_i, $1/y_i$, and $x_i^{\,k}/y_i$ are well-defined at P_∞. Now we have the following.

LEMMA 4. *Let $D_1, D_2, D_3, f_1, f_2, f_3$ be as above. Then the following are equivalent:*

(a) $D_1 + D_2 \sim D_3$.

(b) $f_1 f_2 / f_3 \in K(C)$.

(c) $\delta(f_1 f_2 / f_3) = 0$.

Proof. (a) ⇒ (b). If $D_1 + D_2 \sim D_3$, then $D_1 + D_2 = D_3 + \operatorname{div}(g)$ for some non-zero function $g \in K^{sep}(C)$. Since D_1, D_2 and D_3 are in $\operatorname{Div}_K^0(C)$, by Lemma 1 we may assume that g is in $K(C)^*$. We also have $D_i = \operatorname{div}(f_i) + \operatorname{div}(g_i)$ for $g_i \in K(C)^*$, $i = 1, 2, 3$. Hence we get $\operatorname{div}(f_1) + \operatorname{div}(g_1) + \operatorname{div}(f_2) + \operatorname{div}(g_2) = \operatorname{div}(f_3) + \operatorname{div}(g_3) + \operatorname{div}(g)$. Now we have $\operatorname{div}(f_1 f_2 / f_3) = \operatorname{div}(g_3 g / g_1 g_2)$. Lemma 1 again leads to $f_1 f_2 / f_3 \in \lambda \cdot K(C)$ for some $\lambda \in K^{sep*}$. It is easy to see from Eqs. (3) and (4) that $\lambda \cdot K(C) \cap K'(C) \neq \emptyset$ implies $\lambda \in K^*$.

(b) ⇒ (a). It follows from the relations of D_i and f_i.

The equivalence of (b) and (c) follows from the observation that $\operatorname{Ker}(\delta) = K(C)$. ▮

We retain notations for $D_1, D_2, D_3, f_1, f_2, f_3$ as before. If $D_1 + D_2$ and D_3 are linearly equivalent, then we need to explicitly compute $\delta(f_1 f_2 / f_3) = 0$ in terms of polynomials in t, from Lemma 4(c). The quotient formula of δ yields

$$\frac{f_3 \delta(f_1 f_2) - f_1 f_2 \delta(f_3)}{f_3{}^2} = 0. \tag{6}$$

Clearing the denominator of (6) and applying the derivation δ we get

$$\begin{aligned} &\prod_{i=1}^{g} (t - t_{2g+i}) \sum_{i=1}^{2g} (t - t_1) \cdots (\widehat{t - t_i}) \cdots (t - t_{2g}) \left(\frac{1}{t} - \frac{1}{t_i} \right) \\ &\quad = \prod_{i=1}^{2g} (t - t_i) \sum_{i=1}^{g} (t - t_{2g+1}) \cdots (\widehat{t - t_{2g+i}}) \cdots (t - t_{3g}) \left(\frac{1}{t} - \frac{1}{t_{2g+i}} \right), \end{aligned} \tag{7}$$

where $\widehat{t_i}$ means the term with $\widehat{t_i}$ is omitted in the summation. The equation obtained is an identity in t, so equating the coefficients of the term $\frac{1}{t}$ on both sides of (7) we get

$$\begin{aligned} &(-1)^g t_{2g+1} \cdots t_{3g} \sum_{i=1}^{2g} (-1)^{2g-1} t_1 t_2 \cdots \widehat{t_i} \cdots t_{2g} \\ &\quad = (-1)^{2g} t_1 \cdots t_{2g} \sum_{i=1}^{g} (-1)^{g-1} t_{2g+1} t_{2g+2} \cdots \widehat{t_{2g+i}} \cdots t_{2g}. \end{aligned} \tag{8}$$

Hence from (8) we obtain a crucial identity in terms of the t_i's;

$$\sum_{i=1}^{g} \frac{1}{t_{2g+i}} = \sum_{i=1}^{2g} \frac{1}{t_i}. \tag{9}$$

Applying iterated derivations δ^j to (9) and canceling the coefficient yields, for each $1 \leqslant j \leqslant g-1$,

$$\sum_{i=1}^{g} \frac{1}{t_{2g+i}{}^{2j+1}} = \sum_{i=1}^{2g} \frac{1}{t_i{}^{2j+1}}. \tag{10}$$

We summarize the above discussion to get the following lemma.

LEMMA 5. *Let $D_1, D_2, D_3, f_1, f_2, f_3$ be as before. Assume that $D_1 + D_2 \sim D_3$, then we have, for each $0 \leqslant j \leqslant g-1$,*

$$\sum_{i=1}^{g} \frac{1}{y_{2g+i}{}^{2j+1}} = \sum_{i=1}^{2g} \frac{1}{y_i{}^{2j+1}}. \tag{11}$$

Proof. It follows from taking pth power of (9) and (10), respectively, and then using (4). ▮

These g identities in Lemma 5 allow us to define homomorphisms, denoted X_j: $\mathrm{Pic}_K^0(C) \to K^{sep+}$, $[D] \mapsto X_j(D) := \sum_{i=1}^{g} (1/y_i{}^{2j+1})$ for each $0 \leqslant j \leqslant g-1$, where $D \sim (x_1, y_1) + (x_2, y_2) + \cdots + (x_g, y_g) - g(P_\infty)$. We note that $X_j(D)$ lies in K. Indeed, if $[D]$ is in $\mathrm{Pic}_K^0(C)$, then the divisor $(P_1) + (P_2) + \cdots + (P_g) - g(P_\infty)$ is in $\mathrm{Div}_K^0(C)$. Since P_∞ is fixed by the Galois group G, $(P_1) + (P_2) + \cdots + (P_g) = (P_1{}^\sigma) + (P_2{}^\sigma) + \cdots + (P_g{}^\sigma)$ for all $\sigma \in G$. In other words, G permutes the P's in an appropriate fashion. Hence $(\sum_{i=1}^{g} (1/y_i{}^{2j+1}))^\sigma = \sum_{i=1}^{g} (1/(y_i{}^\sigma)^{2j+1}) = \sum_{i=1}^{g} (1/y_i{}^{2j+1})$ for all $\sigma \in G$. So $X_j(D)$ lies in K.

We now return to the equation of $C/K: y^2 = x^p + a$. With a slight change of the equation of C, one can obtain, for each $1 \leqslant k \leqslant g$,

$$\left(\frac{x^k}{y}\right)^p = \frac{(y^2-a)^k}{y^p} = \frac{\sum_{l=0}^{k} \binom{k}{l} (-a)^l \, y^{2(k-l)}}{y^p}, \tag{12}$$

where $\binom{k}{l}$ means the binomial coefficient. Using these identities in (12) one can also construct maps, denoted Y_k: $\mathrm{Pic}_K^0(C) \to K^{sep+}$, $[D] \mapsto Y_k(D) := \sum_{i=1}^{g} (x_i{}^k / y_i)$ for each $1 \leqslant k \leqslant g-1$, where D is as before. It turns out that they are group homomorphisms because of the relations between the X_i and Y_j listed in Eqs. (13) below. From Eqs. (12) we now look for the relations between them and list the relations below keeping in mind that $2g = p-1$:

$$
\begin{aligned}
&{Y_1}^p = X_{g-1} - a{X_0}^p \\
&{Y_2}^p = X_{g-2} - 2aX_{g-1} + a^2{X_0}^p \\
&\qquad \cdots \\
&{Y_k}^p = X_{g-k} - kaX_{g-k-1} + \cdots + \binom{k}{l}(-a)^l X_{g-k-l} + \cdots + (-a)^k {X_0}^p \\
&\qquad \cdots \\
&{Y_g}^p = X_0 - gaX_1 + \cdots + \binom{g}{l}(-a)^l X_{g-l} + \cdots + (-a)^g {X_0}^p.
\end{aligned}
\tag{13}
$$

Getting rid of terms running X_1 through X_{g-1} from g Eqs. (13) we finally obtain

$$X_0 = a^g {X_0}^p + ga^{g-1}{Y_1}^p + \cdots + \binom{g}{l} a^{g-l}{Y_{g-l}}^p + \cdots + {Y_g}^p. \tag{14}$$

Note that the variety given by (14) is defined over K and has a group structure under addition, due to characteristic p. Here let us recall the assumption that a is a square in K. For $a = b^2 \in K$, since $2g = p-1$ we see by substituting $X = bX_0$ that the variety given by Eq. (14) is K-isomorphic to

$$X = X^p + gb^{2(g-1)+1}{Y_1}^p + \cdots + \binom{g}{l} b^{2(g-l)+1}{Y_{g-l}}^p + \cdots + b{Y_g}^p. \tag{15}$$

Now we use the Wronskian criterian to easily check that all the coefficients of Eq. (15) are linearly independent over K^p. Hence we see from Theorem 1 that the variety (15) has only finitely many K-rational points, so the variety (14) also has only a finite number of K-rational points.

THEOREM 2. *Let K be a function field of one variable over a finite field of characteristic $p \geqslant 5$ and let $C/K: y^2 = x^p + a$ $(a \notin K^p)$, then* $\mathrm{Pic}_K^0(C)$ *has only finitely many K-rational points.*

Proof. We define a map from $\mathrm{Pic}_K^0(C)$ to the variety given by Eq. (14) defined by $[D] \mapsto (X_0(D), Y_1(D), Y_2(D), \ldots, Y_g(D))$. It is obvious that the map is a well-defined group homomorphism. Since the variety in question has only finitely many rational points it is enough to show that the map has only trivial kernel. Suppose $[D]$ is in the kernel of the homomorphism.

Then any divisor of the form $(x_1, y_1)+(x_2, y_2)+\cdots+(x_g, y_g)-g(P_\infty)$ which is linearly equivalent to D satisfies the equations

$$\begin{aligned}
&\frac{1}{y_1}+\frac{1}{y_2}+\cdots+\frac{1}{y_g}=0\\
&\frac{x_1}{y_1}+\frac{x_2}{y_2}+\cdots+\frac{x_g}{y_g}=0\\
&\frac{x_1^2}{y_1}+\frac{x_2{}^2}{y_2}+\cdots+\frac{x_g{}^2}{y_g}=0 \qquad (16)\\
&\cdots\\
&\frac{x_1{}^g}{y_1}+\frac{x_2{}^g}{y_2}+\cdots+\frac{x_g{}^g}{y_g}=0.
\end{aligned}$$

We may assume that not all $P_i=(x_i, y_i)$ $i=1, ..., g$ are the point at infinity. From Eqs. (16) we can view $1/y_i$ as a variable and consider the first equation as a constraint and then form a matrix equation:

$$\begin{bmatrix} x_1 & x_2 & \cdots & x_g \\ x_1{}^2 & x_2{}^2 & \cdots & x_g{}^2 \\ x_1{}^3 & x_2{}^3 & \cdots & x_g{}^3 \\ \vdots & \vdots & \ddots & \vdots \\ x_1{}^g & x_2{}^g & \cdots & x_g{}^g \end{bmatrix} \begin{bmatrix} \frac{1}{y_1} \\ \frac{1}{y_2} \\ \frac{1}{y_3} \\ \vdots \\ \frac{1}{y_g} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \qquad (17)$$

From the assumption that not all P_i are the point at infinity, the matrix associated with Eq. (17) is singular, so we deduce that $x_i=x_j$ for some $i\neq j$, because the determinant of the matrix is $x_1x_2\cdots x_g\prod_{i<j}(x_i-x_j)$. After renumbering, we may assume that $i=1$, $j=2$. From the equation of C we know that either $y_1=y_2$ or $y_1=-y_2$, that is, $P_1=P_2$ or $P_2=\overline{P_1}=(x_1, -y_1)$. Hence $D\sim(P_3)+(P_4)+\cdots+(P_g)-(g-2)(P_\infty)$ or $2(P_1)+(P_3)+(P_4)+\cdots+(P_g)-g(P_\infty)$ since $(P_1)+(\overline{P_1})-2(P_\infty)$ is principal. This implies that we can get rid of one or two terms from each equation (16) and keep on applying the process to the remaining divisor $(P_3)+(P_4)+\cdots+(P_g)-(g-2)(P_\infty)$ or $2(P_1)+(P_3)+(P_4)+\cdots+(P_g)-g(P_\infty)$ to reduce that the divisor $[D]$ in the kernel is principal. This completes the proof. ▮

Corollary 1. *Let K be the same as before and $C/K: y^2 = x^p + a$ $(a \notin K^p)$. Then $C(K)$ is at most finite.*

Proof. Define a map $C(K) \to \mathrm{Pic}^0_K(C)(K)$, $P \mapsto [(P) - (P_\infty)]$. Since C is not rational over K it is easy to see that the map is injective. It follows then from Theorem 2 that $C(K)$ is at most finite. ▌

5. AN EXPLICIT EXAMPLE

Let K be a function field of one variable over a finite field of characteristic $p \geqslant 5$. Let $\mathscr{S}/K$ be a surface defined by $x - x^p = 2b^3y^p + bz^p$ $(b \notin K^p)$, which is obtained from Eq. (15) in the case of genus $g = 2$. Since $b \notin K^p$ it is easy to see that $1, b, 2b^3$ are linearly independent over K^p. By Theorem 1 we already know the surface $\mathscr{S}$ has finitely many rational points. We here show that $\mathscr{S}(K)$ consists of p elements for infinitely many choices of b. We retain all notations from Section 4.

First of all, we will consider any place $v \in M_K$ such that $v(b) = 0$. Then $b = b_0 + b_1 t_v + b_2 {t_v}^2 + b_3 {t_v}^3 + \cdots \in K_v$ is written as a power series in terms of t_v, where t_v is a local parameter at such a place v. We notice that $b_0 \neq 0$, as $v(b) = 0$. From the assumption on $b \notin K^p$, we can put $j := \min\{i \geqslant 1 \mid b_i \neq 0, (p, i) = 1\}$. It follows then from the definition of j that $v(db) = j - 1 \geqslant 0$, where db is a differential form of b. Set $j_v := \lceil \frac{-2j}{p-1} \rceil \leqslant 0$, where $\lceil d \rceil$ is the least integer $\geqslant d$. In what follows, we always denote by $(l, m, n) \in \mathbf{Z}^3$ a triple of values that every element $(x, y, z) \in \mathscr{S}(K)$ takes at the place v.

Lemma 6. *Let $v \in M_K$ be any place such that $v(b) = 0$, then for every element $(x, y, z) \in \mathscr{S}(K)$, we have $v(x) \geqslant j_v$, $v(y) \geqslant j_v$, $v(z) \geqslant j_v$.*

Proof. For such a place v, suppose that there exists an element $(x, y, z) \in \mathscr{S}(K_v)$ for which at least one of $v(x), v(y), v(z)$ is less than j_v. Then we can observe that either y or z has valuation $< j_v$ at v. Otherwise, taking the valuation v of the equation of $\mathscr{S}$ gives

$$v(x - x^p) = v(2b^3y^p + bz^p) \geqslant \min\{pv(y), pv(z)\} \geqslant pj_v.$$

From the hypothesis we have that $v(x) < j_v \leqslant 0$, hence $v(x - x^p) = pv(x) \geqslant pj_v$, which is a contradiction.

The proof will be then broken up into three cases for the possible choices of $v(y) = m$, $v(z) = n$ as follows:

(I) If $m < j_v$ and $m < n$, then $l = m$.

(II) If $n < j_v$ and $n < m$, then $l = n$.

(III) If $m = n < j_v$, then $l \geqslant m = n$.

For each case, from the property of a place it is not hard to determine what l is, as it is written above. Taking the derivation δ of the equation of $\mathcal{S}$ yields

$$\delta x = (6b^2y^p + z^p)\,\delta b. \tag{$*$}$$

Now we claim that $v(6b^2y^p + z^p) \leqslant pm + j$ in case (III).

To prove the claim, it suffices to show that coeff$(6b^2y^p + z^p, t^{pm+j})$ is not equal to 0, where coeff(E, t^i) means the coefficient of the term of which t-exponent is i, in the Laurent series expansion of E. Squaring the power series expansion of b, we note from the definition of j that all non-vanishing terms in b^2 whose t-exponents are less than j have exponent of p-multiple. Hence we can easily find out

$$\text{coeff}(6b^2y^p + z^p, t^{pm+j}) = 12b_0b_j\,{y_m}^p \neq 0.$$

By taking the valuation of Eq. $(*)$ we obtain

$$v(dx) = v(6b^2y^p + z^p) + v(db) = \begin{cases} pm + j - 1 & \text{for (I)} \\ pn + j - 1 & \text{for (II)} \\ \leqslant pm + 2j - 1 & \text{for (III)} \end{cases}$$

On the other hand, we get

$$v(dx) \geqslant v(x) - 1 = \begin{cases} m - 1 & \text{for (I)} \\ n - 1 & \text{for (II)} \\ l - 1 \geqslant m - 1 & \text{for (III)} \end{cases}$$

Simple computations of the above two arrays give that in each case all $l, m, n \geqslant j_v$, which contradicts the hypothesis. ∎

Next let us consider any place $v \in M_K$ such that $v(b) = j \neq 0$.

LEMMA 7. *For each $v \in M_K$ such that $v(b) = j \neq 0$, there is an integer j_v, depending on v such that every solution $(x, y, z) \in \mathcal{S}(K)$ has valuations $\geqslant j_v$.*

Proof. We shall consider two cases depending on whether $(p, j) = 1$ or not. Suppose $(p, j) = 1$. Then it is obvious that $v(db) = j - 1$. The assumption on j follows that $v(2b^3y^p) \neq v(bz^p)$. Hence we have either $3j + pm < j + pn$ or $3j + pm > j + pn$.

If $3j + pm < j + pn$, then taking the valuation v of the equation of $\mathscr{S}$, we have

$$v(x - x^p) = 3j + pm.$$

We claim that $v(x) = l \geqslant 0$. Otherwise $v(x - x^p) = pl = 3j + pm$ from the preceding equation, contradicting the fact that $(p, j) = 1$. Hence we obtain that $l \geqslant 0$, $m \geqslant -3j/p$, $n > -2j/p + m \geqslant -5j/p$. Put $j_{v-} := \min\{0, \ulcorner -3j/p \urcorner, \ulcorner -5j/p \urcorner\}$.

If $3j + pm > j + pn$, then the same argument yields that $l \geqslant 0$, $n \geqslant -j/p$, $m > -2j/p + n \geqslant -3j/p$. Set $j_{v+} := \min\{0, \ulcorner -j/p \urcorner, \ulcorner -3j/p \urcorner\}$. In either case it is enough to take $j_v = \min\{j_{v-}, j_{v+}\}$.

Suppose $p \mid j$. Then we can rewrite $b = u^p b'$, where $u = t^{j/p}$, $v(b') = 0$, $b' \notin K^p$. Here we can employ a change of variables in the equation of $\mathscr{S}$: $(x, y, z) \to (x', y', z') = (x, u^3 y, uz)$ to get $x' - x'^p = 2b'^3 y'^p + b' z'^p$. Hence this case can be reduced to that of Lemma 6. Thus we complete the proof. ▮

Fix the set $S' := \{v \in M_K \mid v(b) \neq 0 \text{ or } v(db) \neq 0\}$. Then it is obvious that S' is a finite set of places of K. For every place v outside of S', we get $v(b) = 0$ and $v(db) = 0$. Hence we know from Lemma 6 that every element $(x, y, z) \in \mathscr{S}(K)$ has no poles at every place $v \notin S'$, because $j = 1$, hence $j_v = 0$. In addition, we see that for even a place $v \in S'$ every element $(x, y, z) \in \mathscr{S}(K)$ may not have a pole there, so we here eliminate such places. So we assume that the set S consists of finite places at which every $(x, y, z) \in \mathscr{S}(K)$ has no poles. In other words, $S = \{v \in S' \mid j_v < 0\}$ where j_v is as Lemmata 6 and 7.

PROPOSITION 2. *Let $\mathscr{S}$ be a surface defined by $x - x^p = 2b^3 y^p + bz^p$ over a rational function field $K = \mathbf{F}_q(T)$ of characteristic $p \geqslant 5$. Then $\mathscr{S}(K) = \{(0, 0, 0), (1, 0, 0), \ldots, (p-1, 0, 0)\}$ for infinitely many $b \notin K^p$.*

Proof. Take $b = T$, then we can easily check that T has only a zero place v_0 and an infinite place v_∞ on K. In other words, $v_0(T) = 1$, $v_\infty(T) = -1$. So, the set S' given above consists only of two places v_0 and v_∞. From the proof of Lemma 7 we know that $j_v \geqslant 0$ in each case. Hence it follows from the proof of Theorem 1 that the emptiness of S completes the proof of the case where $b = T$. For $b = T^{pk+1}$, where k is any non-negative integer, we can use a change of variables to reduce this case to the previous one. ▮

As an application of Proposition 2 we consider a curve C: $y^2 = x^5 + T^{2(5k+1)}$ defined over a rational function field $K = \mathbf{F}_q(T)$ of characteristic 5, where k is any non-negative integer and q is a power of 5. Then we know that the (relative) genus of C is 2 and that $(0, T^{5k+1})$, $(0, -T^{5k+1})$ are rational points of C. We denote $(0, T^{5k+1})$, $(0, -T^{5k+1})$ and the point at infinity by P_+, P_-, P_∞, respectively.

Corollary 2. *Let C: $y^2 = x^5 + T^{2(5k+1)}$ be a curve defined over a rational function field $K = \mathbf{F}_q(T)$ of characteristic* 5. *Then* $\mathrm{Pic}^0_K(C)$ *consists only of* 5 *rational points.*

Proof. Let $\mathscr{S}$ a surface defined by $x - T^{4(5k+1)}x^5 = 2T^{2(5k+1)}y^5 + z^5$, which is isomorphic to $x - x^5 = 2T^{3(5k+1)}y^5 + T^{(5k+1)}z^5$. Then we know from Proposition 2 that $\mathscr{S}(K)$ contains 5 points. We consider a map $\mathrm{Pic}^0_K(C)(K) \to \mathscr{S}(K)$, $[D] \mapsto (X_0(D), Y_1(D), Y_2(D))$ as defined in the proof of Theorem 2, where D is linearly equivalent to $(x_1, y_1) + (x_2, y_2) - 2(P_\infty)$. It is shown there that the map is injective. Moreover it is a group homomorphism, so $\mathrm{Pic}^0_K(C)(K)$ is a group of order 5 since it contains at least two rational points. ▮

Corollary 3. *Let $C: y^2 = x^5 + T^{2(5k+1)}$ be a curve defined over a rational function field $K = \mathbf{F}_q(T)$ of characteristic* 5. *Then* $C(K) = \{(0, T^{5k+1}), (0, -T^{5k+1})\}$.

Proof. Define $C(K) \to \mathrm{Pic}^0_K(C)(K)$, $Q \mapsto [(Q) - (P_\infty)]$. Then we already know that the map is a well-defined injective map since C is not rational over K. From Corollary 2 we see that $\mathrm{Pic}^0_K(C)(K)$ is a cyclic group of order 5. Suppose that there exists another rational point $P = (x, y)$ different from P_+, P_-, P_∞ on C. Then $\bar{P} = (x, -y)$ is also a rational point on C and notice that the map above is bijective. Let now $[(P_+) - (P_\infty)]$ be a generator of $\mathrm{Pic}^0_K(C)(K)$. We then get $[(P) - (P_\infty)] = [2(P_+) - 2(P_\infty)]$ and $[(\bar{P}) - (P_\infty)] = [3(P_+) - 3(P_\infty)]$. From two identities we deduce two rational functions f, $g \in K(C)^*$ such that

$$(P) + (P_\infty) = 2(P_+) + \mathrm{div}(f)$$

$$(P) + 2(P_\infty) = 3(P_+) + \mathrm{div}(g).$$

We note that f has zeros at P and P_∞ but a pole of order 2 at P_+ and that $f \in L(2P_+)$. Hence $L(2P_+)$ is a vector space of dimension at least 2 over K. On the other hand, from the Riemann–Roch Theorem it follows that $l(3P_+) = 2$. Since $L(2P_+) \subset L(3P_+)$, $L(2P_+)$ is exactly a two-dimensional vector space over K. So we take $\{1, f\}$ as a basis for $L(2P_+)$, so $g = \lambda + \mu f$ is written for some λ, $\mu \in K$ as $g \in L(3P_+)$. Since both f and g have a zero at P we get $\lambda = 0$, so $g = \mu f$, which is impossible because f and g have a pole of order 2 and 3 at P_+, respectively. ▮

ACKNOWLEDGMENTS

This paper is part of the results of the author's Ph.D. thesis at The University of Texas at Austin. The author thanks his advisor, José Felipe Voloch, for suggesting this interesting problem and for his encouragement and guidance, and thanks David Saltman for clarification of Proposition 1.

REFERENCES

[GV] A. Garcia and J. F. Voloch, Wronskians and linear independence in fields of prime characteristic, *Manuscripta Math.* **59** (1989), 457–469.

[Ha] H. Hasse, Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit volkommenem Konstantenkörper bei beliebiger Charakteristik, *J. Reine Angew. Math.* **175** (1936), 50–54.

[HS] H. Hasse and F. K. Schmidt, Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten, *J. Reine Angew. Math.* **177** (1937), 215–237.

[J1] S. Jeong, Rational points on algebraic curves that change genus, *J. Number Theory* **67** (1998), 170–181.

[J2] S. Jeong, "Diophantine Problems in Function Fields of Positive Characteristic," Ph.D. thesis, University of Texas at Austin, 1999.

[La] S. Lang, "Algebra," 3rd ed., Addison–Wesley, Menlo Park, CA, 1993.

[M] D. Mumford, "Curves and Their Jacobians," Univ. of Michigan Press, Ann Arbor, MI, 1975.

[Sch] F. K. Schmidt, Die Wronskische Determinante in beliebigen differenzierbaren Funktionenkörpern, *Math. Z.* **45** (1939), 62–74.

[Sil] J. H. Silverman, "The Arithmetic of Elliptic Curves," Springer-Verlag, New York, 1986.

[Sti] H. Stichtenoth, "Algebraic Function Fields and Codes," Springer-Verlag, Berlin/Heidelberg, 1993.

[V] J. F. Voloch, A Diophantine problem on algebraic curves over function fields of positive characteristic, *Bull. Soc. Math. France* **119** (1991), 121–126.