158. *On Fields of Division Points of Algebraic Function Fields of One Variable*

By Makoto ISHIDA

Department of Mathematics, Tsuda College, Tokyo

(Comm. by Zyoiti SUETUNA, M.J.A., Dec. 12, 1963)

Let K be a field of algebraic functions of one variable over an algebraically closed constant field k. Let $D_0(K)$ be the group of all the divisors of degree 0 of K and $C(K)$ the divisor class group of K, i.e. the factor group of $D_0(K)$ by the subgroup consisting of all the divisors which are linearly equivalent to 0 (in notation: ~ 0). We use the additive notation for the group laws of $D_0(K)$ and $C(K)$. Let g be the genus of K. Then, for a natural number n prime to the characteristic of k, it is known that there exist exactly n^{2g} elements $c_1,\cdots,c_N$ ($N=n^{2g}$) of $C(K)$ such that $nc_i=0$. We call these c_i the *n-division points* of $C(K)$.

Let $D_1,\cdots,D_N$ be an *arbitrary* system of representative divisors of the classes $c_1,\cdots,c_N$ (c_i is the divisor class containing D_i). Then nD_i is linearly equivalent to 0 and so there exist N elements $x_1,\cdots,x_N$ of K such that the divisor (x_i) of x_i is equal to nD_i. We consider the subfield $K_n=k(x_1,\cdots,x_N)$ of K generated by $x_1,\cdots,x_N$ over k. We shall call such a field K_n a *field of n-division points of K*. Since there are infinitely many choices of systems of representative divisors of the classes c_i, there are also, for a fixed given n, infinitely many fields of n-division points of K. We note that if $n>1$, K_n has the transcendental degree 1 over k and so the degree $[K:K_n]$ is finite. In fact, for $n>1$, some c_i is not equal to 0 and so x_i is not a constant.

Now we shall prove the following

Theorem. *Suppose $g\geqq 2$. Let $l\geqq 3$ be a prime number different from the characteristic of k. Then, for any field K_l of l-division points of K, K is purely inseparable over K_l. In particular, if the characteristic of k is 0, we have $K=K_l$.*

The case where $l=2$ (and the characteristic $=0$) was considered by Arima in [1]. We shall prove our theorem in the separable case by the same idea.

The proof of the theorem is divided into two cases.

1) First we consider the case where K is separable over K_l. We assume that $K\neq K_l$ and deduce a contradiction. Let g_0 be the genus of K_l. Then, as $g\geqq 2$ and $K\neq K_l$, we have $g>g_0$ by the formula of Hurwitz. We denote by $(x_i)_K$ and $(x_i)_{K_l}$ the divisors of the function

x_i in K and K_l respectively. We also denote by f^{-1} the conorm mapping of divisors for the extension K/K_l (cf. Chevalley [2]). If $(x_i)_{K_l}=le_i$ and $(x_j)_{K_l}=le_j$ with divisors e_i and e_j of K_l, then, as in [1], e_i and e_j $(i\neq j)$ determines distinct l-division points of $C(K_l)$. In order to prove this statement, we use the fact that f^{-1} is a homomorphism and $f^{-1}((x_i)_{K_l})=(x_i)_K$. Hence at most l^{2g_0} divisors $(x_i)_{K_l}$ are of the form le_i and so there exist at least $l^{2g}-l^{2g_0}$ (>0) functions x_j such that the divisors $(x_j)_{K_l}$ have the form

$$(*)\qquad (x_j)_{K_l}=\cdots+tp+\cdots,\quad t\not\equiv 0 \pmod{l},$$

where p is a prime divisor of K_l and the right hand side is the reduced expression. Such x_j and $(x_j)_{K_l}$ will be called an element and a divisor *of $(*)$-type*. Let $M=\{p_1,\cdots,p_m\}$ be the set of all the prime divisors p_i of K which appear in the reduced expression of some $(x_j)_{K_l}$ of $(*)$-type with the coefficient $\not\equiv 0 \pmod{l}$. We write all the divisors $(x_j)_{K_l}$ of $(*)$-type as follows:

$$(x_j)_{K_l}=a_j+lb_j,$$

where a_j is of the form $t_{j1}p_1+\cdots+t_{jm}p_m$ with $0\leqq t_{ji}\leqq l-1$ and $(t_{j1},\cdots,t_{jm})\neq(0,\cdots,0)$. If we have $a_j=a_h$ $(j\neq h)$, then we have $lf^{-1}(b_j-b_h)=f^{-1}((x_j)_{K_l}-(x_h)_{K_l})=(x_j)_K-(x_h)_K=lD_j-lD_h$ and so $f^{-1}(b_j-b_h)=D_i-D_h$. So we have $b_j-b_h\not\sim 0$ (not linearly equivalent to 0) but $l(b_j-b_h)=(x_j)_{K_l}-(x_h)_{K_l}\sim 0$. Hence we see that, for a given a_j, the number of $(x_h)_{K_l}$ with $a_h=a_j$ is at most equal to the number of the l-division points of $C(K_l)$ i.e. l^{2g_0}. On the other hand, the number of such a_j is at most equal to $l^{m-1}-1$. In fact, since $\deg(a_j)=t_{j1}+\cdots+t_{jm}=\deg((x_j)_{K_l})-\deg(lb_j)\equiv 0 \pmod{l}$, t_{jm} is uniquely determined as the least non-negative residue of $-(t_{j1}+\cdots+t_{j,m-1})$ modulo l; and so the number of a_j does not exceed the number of $(t_{j1},\cdots,t_{j,m-1})\neq(0,\cdots,0)$ with $0\leqq t_{ji}\leqq l-1$ i.e. $l^{m-1}-1$. Therefore we have

$$l^{2g}-l^{2g_0}\leqq(\text{the number of } x_j \text{ of } (*)\text{-type})\leqq(l^{m-1}-1)\cdot l^{2g_0}$$

and so

$$(1)\qquad m\geqq 2(g-g_0)+1.$$

Let p be a prime divisor in M. Then there exists an element x_j of $(*)$-type such that $(x_j)_{K_l}=\cdots+tp+\cdots$ with $t\not\equiv 0 \pmod{l}$. Let $f^{-1}(p)=t_1P_1+\cdots+t_hP_h$ be the reduced expression, where P_i is a prime divisor of K; then we have $lD_j=(x_j)_K=\cdots+tt_1P_1+\cdots+tt_hP_h+\cdots$. Hence l divides t_j and so the degree $n=t_1+\cdots+t_h$ of K over K_l and we have

$$(2)\qquad \frac{t_i}{l}\geqq 1,\ \frac{n}{l}\geqq 1.$$

Moreover, denoting by $m(P_i)$ the differential exponent of P_i for the extension K/K_l (cf. [2]), we have

$$(3)\qquad \sum_{i=1}^{h} m(P_i)\geqq n\left(1-\frac{1}{l}\right).$$

In fact, we have $\sum_i m(P_i) \geqq \sum_i (t_i - 1) = n - h$ and, by (2), $h \leqq \sum_i \frac{t_i}{l} = \frac{n}{l}$. Therefore we have, by the formula of Hurwitz and by (1) and (3),

$$2g-2 \geqq n(2g_0-2) + \{2(g-g_0)+1\} n\left(1-\frac{1}{l}\right)$$
$$= \frac{n}{l}\{2(l-1)g + 2g_0 - (l+1)\}.^{*)}$$

Since $\frac{n}{l} \geqq 1$, $g_0 \geqq 0$ and $2(l-1)g > l+1$, we have

$$2g-2 \geqq 2(l-1)g - (l+1)$$

and so
$$4g-1 \geqq (2g-1)l.$$

Consequently we have

$$l \leqq \frac{4g-1}{2g-1} = 2 + \frac{1}{2g-1} < 3,$$

which is a contradiction.

2) Next we consider the case where K is not separable over K_l. Let K' be the maximal separable extension of K_l in K. Then K is purely inseparable over K' and the genus of K' is also g. Let $(x_i)_K$ be the divisor of x_i in K' and f'^{-1} the conorm mapping for the extension K/K'. We have $f'^{-1}((x_i)_{K'}) = lD_i$ and so, taking the norm mapping f', we have $[K: K'](x_i)_{K'} = lf'(D_i)$. Since $[K: K']$ is a power of the characteristic of k and is prime to l, we have $(x_i)_{K'} = lD'_i$ with some divisors D'_i in K'. Then, by a similar argument as above, we can show that $D'_1, \cdots, D'_N (N = l^{2g})$ represent all the l-division points of $C(K')$. Hence $K_l = k(x_1, \cdots, x_N)$ is also one of the fields of l-division points of K'. Since K' is separable over K_l, we have, by the first part of the proof, $K' = K_l$ and so K is purely inseparable over K_l.

Thus the proof is completed.

Finally we shall give three remarks.

REMARK 1. Let K_n be a field of n-division points of K and m a natural number dividing n. Then we can easily prove that there exists a field K_m of m-division points of K such that we have $K_n \supset K_m$. On the other hand, as in the first part of the proof, we can prove that if $K \neq K_{l^n}$ and K is separable over K_{l^n} (l is a prime number $\neq$ the characteristic p of k) then l^n divides the degree $[K: K_{l^n}]$. Hence, combining with the result of Arima for $l=2$, we see that K is purely inseparable over any field K_n of n-division points of K, provided n is divisible by a prime number $l(\neq p) \geqq 3$ or by 2^3 (in the case $2 \neq p$).

REMARK 2. When the characteristic p of k is positive, there occur, for the same prime number l, actually two cases: 1) $K = K_l$ and 2) $K \neq K_l$ (K/K_l is purely inseparable). We fix a divisor $A = P_1 + \cdots + P_g$ with $P_i \neq P_j$ $(i \neq j)$ and take the divisors $D_i = B_i - A$ as the

*) For $l=2$, we have $2+1/(g-3/2) \geqq n$, from which Arima proved his theorem.

representative divisors of l-division points c_i, where B_i is a positive divisor of degree g. Then the field K_l of l-division points of K obtained by the choice of such representative divisors coincides with K. In fact, for a non-constant x_i, each coefficient of a prime divisor in the pole of x_i is not divisible by p and so $x_i^{\frac{1}{p}}$ is not in K. Hence x_i is a separating element over k of K and so, as $K \supset K_l \supset k(x_i)$, K is separable over K_l, i.e. we have $K=K_l$. On the other hand, we consider $K'=K^p$ and a field $K_l'=k(y_1,\cdots,y_N)$ of l-division points of K' $(N=l^{2g})$. Then, denoting $(y_i)_{K'}=lD_i'$, we have $(y_i)_K=lf'^{-1}(D_i')$, where f'^{-1} is the conorm mapping for the extension K/K'. If $f'^{-1}(D_i') \sim f'^{-1}(D_j')$, then $f'^{-1}(D_i'-D_j')=(z)$ with some element z in K. Then, taking the norm mapping f', we have $q(D_i'-D_j')=(N_{K/K'}z)$, where q is a power of p. Hence we have $q(D_i'-D_j')\sim 0$ and, as $l(D_i'-D_j') =(y_i)_{K'}-(y_j)_{K'}\sim 0$, we have $D_i'-D_j'\sim 0$, which is a contradiction. Hence $K_l'=k(y_1,\cdots,y_N)$ is also one of the fields of l-division points of K and we have $K \supsetneqq K' \supset K_l'$.

REMARK 3. From the results obtained above, we can show that K has two systems of generators over k, which have the following properties: We fix a prime number l which is $\geqq 3$ and different from the characteristic and we put $N=l^{2g}$. 1) For given g distinct prime divisors $P_1,\cdots,P_g$, there exist N elements $x_1,\cdots,x_N$ of K such that $K=k(x_1,\cdots,x_N)$ and the pole of x_j has the form $lP_{j1}+\cdots+lP_{js}$, $P_{ji}\in\{P_1,\cdots,P_g\}$. 2) For a given prime divisor P_0, there exist N elements $y_1,\cdots,y_N$ of K such that $K=k(y_1,\cdots,y_N)$ and the pole of y_j has the form lt_jP_0.

References

[1] S. Arima: Certain generators of non-hyperelliptic fields of algebraic functions of genus $\geqq 3$, Proc. Japan Acad., **36**, 6-9 (1960).

[2] C. Chevalley: Introduction to the Theory of Algebraic Functions of One Variable, New York (1951).