3. Certain Generators of Non-hyperelliptic Fields of Algebraic Functions of Genus$\geqq 3$

By Satoshi ARIMA

Department of Mathematics, Musashi Institute of Technology, Tokyo

(Comm. by Z. SUETUNA, M.J.A., Jan. 12, 1960)

Let Ω be an algebraically closed field of characteristic 0, and K a field of algebraic functions of one variable over Ω whose genus will be denoted by G. We shall denote the elements of K by letters like x_i, x, y, u, u', v; the divisors by E_i, prime divisors by P, the divisor classes of E_i by $\bar{E}_i$. The divisor classes of degree 0 form a group, which becomes the Jacobian variety of K when Ω is the field $\boldsymbol{C}$ of complex numbers. We shall consider the elements of this group whose orders are finite and divide 2. They will be called *two-division points* of K. They form a group $\mathfrak{g}$ isomorphic to the direct sum of $2G$ cyclic groups of order 2, so that there are 2^{2G} two-division points $\bar{E}_i$, $1\leqq i\leqq 2^{2G}$, of K (cf. [1, p. 176, Th. 16 and Cor. to Th. 16] and [2, p. 79]). Let E_i be *arbitrary* representatives of $\bar{E}_i$, $1\leqq i\leqq 2^{2G}$, and x_i an element of K such that $(x_i)=E_i^2$. Now we consider the subfield

$$k=\Omega(x_1,\cdots,x_{2^{2G}})$$

of K. We shall show in Theorem 1 that $K=k$ (i.e. that K is generated by the functions x_i determined by two-division points $\bar{E}_i$ if K is not hyperelliptic and $G\geqq 3$, and in Theorem 2 that $[K:k]=1$, 2 or 4 if K is hyperelliptic.

The above notations will be used throughout the paper. The genus of k will be denoted by g. We put $[K:k]=n$.

LEMMA. *If $n>1$ and $G\geqq 2$, then $g=0$ and $n\leqq 2+\dfrac{1}{G-3/2}$.*

PROOF. We use Riemann-Hurwitz's formula:

$$2G-2=n(2g-2)+\sum_P(e_P-1), \tag{1}$$

where P runs over the prime divisors of K and e_P is the ramification index of P. We recall first, that $G>g$ since $G\geqq 2$, and that the number of 2-division points of k is 2^{2g}. Denote by $(x_i)_K$ and $(x_i)_k$ the divisors of x_i in K and k respectively. We have

$$(x_i)_K=E_i^2=\mathrm{Con}_{k/K}(x_i)_k.$$

Now every divisor $(x_i)_k$ is either a square of another divisor: $(x_i)_k=e_i^2$ or not a square of any divisor: $(x_i)_k=e_i$; but we can show here that at most 2^{2g} divisors $(x_i)_k$ are squares of other divisors; in fact, if $(x_i)_k=e_i^2$, then e_i represents a 2-division point of k, and it follows from

$E_i^2=\mathrm{Con}_{k/K}(e_i^2)$ and $E_i=\mathrm{Con}_{k/K}(e_i)$ that*)

$$i \neq h \Rightarrow E_i \nsim E_h \text{ in } K \Rightarrow e_i \nsim e_h \text{ in } k,$$

so that these e_i represent distinct 2-division points of k and hence the number of divisors $(x_i)_k$ which are squares of other divisors, is at most 2^{2g}.

This being so, we see that at least $2^{2G}-2^{2g}$ divisors $(x_i)_k$ are not squares of any divisors of k; we use, from now on, suffix j and h to denote these x_i, e_i and E_i:

(2) $$(x_j)_k=e_j, \quad E_j^2=\mathrm{Con}_{k/K}(e_j).$$

Call b the least common multiple of the denominators of the e_j's, and put

(3) $$e_j=\frac{a_j}{b}, \quad \deg b=\deg a_j=m.$$

If $j \neq h$, we have $a_j \neq a_h$ but $a_j \sim a_h$. Denote by M the totality of prime divisors of k which appear in some a_j with odd exponents, and let l be the number of divisors belonging to M. Then we have

(4) $$l \geqq 2(G-g)+1.$$

In fact, suppose that a_j and a_h $(j \neq h)$ have the same factors up to their square factors:

$$a_j=(p_{j_1}\cdots p_{j_r})\ (q_{j_{r+1}}\cdots q_{j_s})^2,$$
$$a_h=(p_{j_1}\cdots p_{j_r})\ (q_{h_{r+1}}\cdots q_{h_s})^2, \ r+2s=m,$$

then we have

$$\left(\frac{q_{j_{r+1}}\cdots q_{j_s}}{q_{h_{r+1}}\cdots q_{h_s}}\right)^2=\frac{a_j}{a_h}=\frac{e_j}{e_h}\sim 1.$$

On the other hand, we see that

$$j \neq h \Rightarrow \mathrm{Con}_{k/K}(e_j/e_h)^{\frac{1}{2}}=E_j/E_h \nsim 1 \Rightarrow \frac{q_{j_{r+1}}\cdots q_{j_s}}{q_{h_{r+1}}\cdots q_{h_s}}=\frac{e_j}{e_h} \nsim 1 \text{ in } k,$$

so that, if we fix a_j, these $q_{j_{r+1}}\cdots q_{j_s}/q_{h_{r+1}}\cdots q_{h_s}$ represent distinct 2-division points of k and the number of these 2-division points does not exceed 2^{2g}. Thus we see that, for a given a_j, the number of a_h's which coincide with a_j up to their square factors is at most 2^{2g}. Therefore, if we classify all the a_j's by bringing those a_j's which have the same factors up to their square factors into the same class, then the number of the classes is at least $(2^{2G}-2^{2g})/2^{2g}=2^{2(G-g)}-1$. Now from the meanings of l and m, we have clearly $2^{2(G-g)}-1 \leqq \binom{l}{m}+\binom{l}{m+2}+\cdots \leqq 2^{l-1}$. So we get $2^{2(G-g)} \leqq 2^{l-1}$. The formula (4) is thereby proved.

Now if a prime divisor $p \in M$ appears in b with an even exponent, then it follows clearly from (2) and (3) that p is ramified in K; if p occurs in a_j and b both with odd exponents, then p occurs in the denominator of the reduced expression of another e_h with an odd exponent

*) $\sim$ denotes the linear equivalence relation between two divisors.

(since b is the common multiple of the denominators of the reduced expressions of e_j's), and so p is also ramified in K. Every $p \in M$ is therefore ramified in K.

We shall now show that

$$(5) \qquad \sum_{P|p} (e_P - 1) \geqq n/2$$

for l prime divisors $p \in M$. To show this, write $\mathrm{Con}_{k/K}(p) = (P_1^{u_1} \cdots P_h^{u_h})^2$, $e_{P_i} = 2u_i$, then we have $n = [K:k] = 2u_1 + \cdots + 2u_h \geqq 2h$ since the constant field Ω is algebraically closed, and so we have $n/2 \leqq n - h \leqq (2u_1 - 1) + \cdots + (2u_h - 1) = \sum_{P|p} (e_P - 1)$, which proves (5).

We have from (1), (4) and (5) that

$$(6) \qquad 2G-2 \geqq n(2g-2) + n/2\{2(G-g)+1\}.$$

If $g \geqq 1$, then it follows from (6) that $2G-2 \geqq 2(2g-2) + 2(G-g) + 1$ and $g=0$ which is a contradiction. Hence we must have $g=0$. By (6), we get therefore $2(G-1) \geqq n(G-3/2)$; as $G \geqq 2$, we have $n \leqq 2 + \dfrac{1}{G-3/2}$.

q.e.d.

THEOREM 1. *If K is not hyperelliptic and $G \geqq 3$, then $n=1$.*

PROOF. If $n>1$, from $G \geqq 3$ follows by Lemma that $g=0$ and $n=2$, which implies that K is hyperelliptic; we must have therefore $n=1$.

COROLLARY. *Let $\bar{E}_1, \cdots, \bar{E}_{2G}$ be generators of $\mathfrak{g}$. Then we have*

$$K = \Omega(x_1, \cdots, x_{2G}).$$

PROOF. In Theorem 1, take $E = E_1^{\varepsilon_1} \cdots E_{2G}^{\varepsilon_{2G}}$ as representative divisors of 2-division points $\bar{E} \neq \bar{E}_i$ $(1 \leqq i \leqq 2G)$ of K, where ε_i are 1 or 0; let x be a function determined by E; it follows that

$$x = \text{constant} \cdot x_1^{\varepsilon_1} \cdots x_{2G}^{\varepsilon_{2G}} \in \Omega(x_1, \cdots, x_{2G}),$$

which shows that $\Omega(x_1, \cdots, x_{2^{2G}}) = \Omega(x_1, \cdots, x_{2G})$ and proves our assertion.

THEOREM 2. *Let K be hyperelliptic.* 1) *If $G \geqq 3$, then $n=1$ or 2 and in the latter case we have $g=0$.* 2) *If $G=2$, then $n=1$ or 2 or 4, and in case $n=2$ or 4, we have $g=0$.*

PROOF. Assume that $n>1$. If $G \geqq 3$, we have $n=2$ from Lemma; if $G=2$, we have $n=2$ or $n=4$. And from $n>1$ follows $g=0$ also by Lemma.

REMARK. We shall show that cases $n=1$ and 2 for hyperelliptic K really take place. Let

$$K = \boldsymbol{C}(x, y), \quad y^2 = (x-\alpha_1)\ (x-\alpha_2) \cdots (x-\alpha_{2G+1}),$$

where $\alpha_i \in \boldsymbol{C}(1 \leqq i \leqq 2G+1)$. Then K is hyperelliptic and of genus G. Denoting by Q_i and Q_∞ the zeros and the poles of $x-\alpha_i$ $(1 \leqq i \leqq 2G+1)$, we have $(x-\alpha_i) = Q_i^2/Q_\infty^2$ and $(y) = Q_1 \cdots Q_{2G+1}/Q_\infty^{2G+1}$. The divisors Q_1/Q_∞, $\cdots, Q_{2G}/Q_\infty$ determine clearly a system of generators of 2-division points of K, and 2-division points of K are represented by the divisors E of the form $E = (Q_1/Q_\infty)^{\varepsilon_1} \cdots (Q_{2G}/Q_\infty)^{\varepsilon_{2G}}$ where $\varepsilon_1, \cdots, \varepsilon_{2G}$ are 1 or 0. The elements u of K determined by $(u)=E^2=(x-\alpha_1)^{\varepsilon_1}\cdots(x-\alpha_{2G})^{\varepsilon_{2G}}$ *generate the subfield* $\boldsymbol{C}(x)$ *of* K *over which* K *is of degree* 2. Next, take an element v of K such that $\boldsymbol{C}(x, v^2)=K$ (for this, it is sufficient to set $v=y-1$). The divisor $(v)Q_1/Q_\infty$ determine the same 2-division points of K as that of Q_1/Q_∞, and 2-division points of K are also represented by the divisors E' of the form $E'=((v)Q_1/Q_\infty)^{\varepsilon_1}(Q_2/Q_\infty)^{\varepsilon_2}\cdots(Q_{2G}/Q_\infty)^{\varepsilon_{2G}}$ where $\varepsilon_1,\cdots,\varepsilon_{2G}$ are 1 or 0. The elements u' of K determined by $(u')=E'^2=v^{2\varepsilon_1}(x-\alpha_1)^{\varepsilon_1}\cdots(x-\alpha_{2G})^{\varepsilon_{2G}}$ *generate the field* $\boldsymbol{C}(x, v^2)=K$.

We have however not succeeded in constructing an example for $n=4$. The author is inclined to believe that this would not take place, which could be proved in making use of more precise inequalities than (4).

References

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

[2] S. Schilling: Foundations of an abstract theory of abelian functions, Amer. J. Math., **61** (1939).