A Note on Transcendental Elements of an
Algebraic Function Field of
One Variable

Tadashi WASHIO

The Department of the Mathematics, Faculty of Education.
Nagasaki University, Nagasaki

(Received October 31, 1971)

§ 1. Abstract

Let \( K \) be an algebraic function field of one variable with a constant field \( k \). We shall assume that \( K \) is separably generated over \( k \) and then we shall denote by \( x \) a separating element of \( K \) over \( k \).

The purpose of this note is to discuss the problem whether we can find the elements \( a, b, c, d \), in \( k \) satisfying \( ad - bc \neq 0 \) such that every prime divisor of \( K \) that divides the denominator divisor or the numerator divisor of the element of the form \( \frac{ax + b}{cx + d} \) is unramified over the rational function field \( k(x) \), or not.

It is obvious that we can find such elements if \( k \) is not finite. But it is impossible in general if \( k \) is finite. In § 2, we shall prove that there exist such elements in \( k \) under some condition, and we shall show that this is the best condition in a sense in § 3.

§ 2. Sufficient condition

Let \( k \) be a finite field and let \( K \) be an algebraic function field of one variable over \( k \). We shall denote by \( l \) the exact constant field, i.e., \( l \) is the algebraic closure of \( k \) in \( K \). So \( l \) is a finite extension of \( k \). Let \( x \) be a separating element of \( K \) over \( k \), i.e., \( K \) is a separable extension over \( k(x) \). Then we have the following lemma.

**Lemma.** \( g \) denotes the genus of \( K \) and \( N \) denotes the number of all prime divisors of \( K \) that are ramified over \( k(x) \). Then \( N \leq 2[K : l(x)] + 2g - 2 \) holds. Especially, if \( k \) is of characteristic 2, \( N \leq [K : l(x)] + g - 1 \) holds where
\([K : l(x)]\) means the degree of \(K\) over \(l(x)\).

**Proof.** Since \(x\) is a separating element of \(K\) over \(k\), the different \(b(K/k(x))\) of \(k\) over \(K(x)\), the different \(b(K/l(x))\) of \(K\) over \(l(x)\) and the different \(b(l(x)/k(x))\) of \(l(x)\) over \(k(x)\) exist. As well known,
\[
b(K/k(x)) = b(K/l(x)) \text{Con}_{l(x)/k} b(l(x)/k(x))
\]
holds, where \(\text{Con}_{l(x)/k}\) means the conorm of \(l(x)\) to \(K\). (e.g., C. Chevalley [1]; p. 75, Theorem 8).

\(l(x)\) is a separable constant field extension of \(k(x)\) and \(k\) is finite. Thus \(b(l(x)/k(x))\) is the unit divisor of \(K\), whence \(\text{Con}_{l(x)/k} b(l(x)/k(x))\) is so. (e.g., C. Chevalley [1]; pp. 69–72 and M. Deuring [2]; p. 124).

Therefore, we obtain the equality
\[
(1) \quad b(K/k(x)) = b(K/l(x)).
\]

Since \(k\) is finite, all and only prime divisors that are ramified over \(k(x)\) are the prime divisors of \(K\) which divide \(b(K/k(x))\). So the equality \((1)\) means that only these prime divisors appear in \(b(K/l(x))\).

Therefore \(N\) is at most the degree of \(b(K/l(x))\); i.e., \(N \leq 2[K : l(x)] + 2g - 2\). Especially, if \(k\) is of characteristic 2, then all prime divisors of \(K\) that are ramified over \(k(x)\) appear in \(b(K/l(x))\) at least with order 2. (e.g., C. Chevalley [1]; p. 69, Theorem 7).

This implies that \(N\) is at most the half degree of \(b(K/l(x))\); i.e., \(N \leq [K : l(x)] + g - 1\). The lemma is thereby proved.

We shall denote by \(|k|\) the number of the elements in \(k\). Moreover, for a non-zero element \(y\) of \(K\), \(\mathfrak{z}(y)\) denotes the numerator divisor of \(y\) and \(\mathfrak{n}(y)\) denotes the denominator divisor of \(y\). Then we shall prove the following theorem.

**Theorem.** If \(|k| \geq 2[K : l(x)] + 2g - 2\) holds, there exist elements \(a, b, c, d\) in \(k\) satisfying \(ad - bc \neq 0\) such that, for an element \(x\), of the form \(x = \frac{ax + b}{cx + d}\), all prime divisors of \(K\) that appear in the product \(\mathfrak{z}(x_i) \mathfrak{n}(x_i)\) are unramified over \(k(x)\). Especially, in the case that \(k\) is of characteristic 2, we can replace the above inequality by \(|k| \geq [K : l(x)] + g - 1\).

**Proof.** If all prime divisors of \(K\) are not ramified, the theorem is trivial. So we may assume that there exist ramified prime divisors. We shall denote by \(\{p_1, \ldots, p_t\}\) the set of all prime divisors of \(K\) that are ramified over \(k(x)\).

Then, by making use of the lemma and the assumption of the theorem, \(N \leq |k|\) holds. If each \(p_i\) does not appear in \(\mathfrak{z}(x) \mathfrak{n}(x)\), the theorem is obvious. So, we shall investigate only the three cases.
Case 1. Each $p_i (i=1,\ldots,N)$ does not divide $n(x)$ and some $p_i$ divides $\delta(x)$.

We shall denote by $x_{p_i}$ the residue class of $x$ mod. $p_i$. Then, in this case, each $x_{p_i}(i=1,\ldots,N)$ is finite; i.e., each $x_{p_i}$ is algebraic over $I$, whence it is algebraic over $k$.

From $|k|>N$, there exists an element $a$ in $k$ such that $x_{p_i} \neq a (i=1,\ldots,N)$. We shall take such an element $a$ in $k$. Then $\text{ord}_{p_i}(x-a)=0 (i=1,\ldots,N)$ holds, where $\text{ord}_{p_i}$ denotes the order at $p_i$. Therefore $p_i (i=1,\ldots,N)$ does not appear in $\delta(x-a)n(x-a)$.

Case 2. Each $p_i (i=1,\ldots,N)$ does not divide $\delta(x)$ and some $p_i$ appears in $n(x)$.

In this case, $\delta(x)=n(\frac{1}{x})$ and $n(x)=\delta(\frac{1}{x})$. So this is reduced in the case 1. Thus there exists an element $a$ in $k$ such that each $p_i (i=1,\ldots,N)$ does not appear in $\delta(\frac{1}{x}-a)n(\frac{1}{x}-a)$.

Case 3. Some $p_i$ divides $\delta(x)$ and another $p_j$ divides $n(x)$.

We shall denote by $\{q_1,\ldots,q_s\}$ the set of all prime divisors $p_i$ such that $p_i$ does not divide $n(x)$. Then $x_{q_i} (i=1,\ldots,s)$ is finite. In this case, from $|k|>N$ $|k|>s$ hold, and $x_{q_i} (i=1,\ldots,s)$ is finite.

This implies that there exist at least two elements $a, b$ in $k$ which differ from $x_{q_i} (i=1,\ldots,s)$. We shall take such elements $a, b$ in $k$. Then we have the equalities
\[
\text{ord}_{q_i}(x-a)=0 \quad (i=1,\ldots,s) \quad \text{and}
\]
\[
\text{ord}_{q_i}(x-b)=0 \quad (i=1,\ldots,s).
\]

So
\[
(2) \quad \text{ord}_{q_i}(\frac{x-a}{x-b})=0 \quad (i=1,\ldots,s) \quad \text{holds}.
\]

While, for any other $p_j$ that differs from $q_i (i=1,\ldots,s)$,
\[
\text{ord}_{p_j}x=\text{ord}_{p_j}(x-a)=\text{ord}_{p_j}(x-b) \quad \text{holds; namely}
\]
\[
(3) \quad \text{ord}_{p_j}(\frac{x-a}{x-b})=0.
\]

Whence the equalities (2) and (3) follow
\[
\text{ord}_{p_i}(\frac{x-a}{x-b})=0 \quad (i=1,\ldots,N).
\]

Thus there exist $a, b$ in $k$ such that each $p_i (i=1,\ldots,N)$ does not appear in $\delta(\frac{x-a}{x-b})n(\frac{x-a}{x-b})$. In the above three cases, the elements which we got are of the form $\frac{ax+b}{cx+d}$ satisfying $ad-bc \neq 0$. Therefore the theorem is completely proved.
§3. Consideration for the conditions.

The assumptions \(|k| > 2[K : l(x)] + 2g - 2\) and \(|k| > [K : l(x)] + g - 1\) in the theorem are the best conditions for \(k\) in a sense. In fact, if the characteristic of \(k\) is an odd prime, then it happens to exist a function field satisfying \(|k| = 2[K : l(x)] + 2g - 3\) such that the theorem does not hold.

If \(k\) is of characteristic 2, then it happens to exist one satisfying \(|k| = [K : l(x)] + g - 1\) such that the theorem does not hold. So we shall show such examples.

Example 1. We shall put \(k = GF(q), q = p^n\) where \(p\) is an odd prime integer, \(y^a = \Pi(x-a)\) and \(K = k(x, y)\). Then we get \(|k| = q, l = k\) and \(g = \frac{q-1}{2}\), whence \(|k| = 2[K : l(x)] + 2g - 3 = q\) holds. Now we shall denote by \(p_a, (a \in k)\), the prime divisor in \(n(x-a)\) and denote by \(p\) the prime divisor in \(n(x)\).

Then we obtain obviously that \(p_a, (a \in k), p\) are all prime divisors that are ramified over \(k(x)\). In order to investigate \(g\left(\frac{ax+b}{cx+d}\right)\) and \(n\left(\frac{ax+b}{cx+d}\right)\) for the elements of the form \(\frac{ax+b}{cx+d}, (ad-bc \neq 0, k \ni a, b, c, d)\), it is enough to consider the three cases \(x-a, \frac{1}{x-a}\) and \(\frac{x-a}{x-b}, (a \neq b, k \ni a, b)\). For the principal divisor of \(z\) equals to the principal divisor of \(hz\) for any non-zero element \(z\) in \(K\) and any non-zero element \(h\) in \(k\), in general.

\(p\) divides \(n(x)\) and \(p_a\) divides \(g(x-a), g\left(\frac{x-a}{x-b}\right)\) and \(n\left(\frac{1}{x-a}\right)\) for \(a \in k\). Therefore every prime divisor that is ramified over \(k(x)\) divides always some \(g\left(\frac{ax+b}{cx+d}\right)n\left(\frac{ax+b}{cx+d}\right)\).

Example 2. We shall put \(k = GF(2), y^a + xy = x\) and \(K = k(x, y)\). Then we get \(|k| = 2, l = k\) and \(g = 0\), whence \(|k| = [K : l(x)] + g - 1 = 2\) holds.

We shall denote by \(p_a\) the numerator divisor of \(y\) and by \(p\) the denominator divisor of \(y\). Then we have easily that \(p_a\) and \(p\) are prime divisors of \(K\) and they are all prime divisors that are ramified over \(k(x)\).

In this case, the set of all elements of the form \(\frac{ax+b}{cx+d}, (ad-bc \neq 0, k \ni a, b, c, d)\) is \(\{x, \frac{1}{x}, x-1, \frac{x-1}{x}, \frac{x}{x-1}, \frac{x-1}{x}\}\). Obviously, \(p_a\) divides \(g(x), g\left(\frac{x}{x-1}\right), g\left(\frac{x-1}{x}\right)\) and \(n(x-1)\) and \(p\) divides \(n(x-1)\). Therefore we can not choose \(a, b, c\) and \(d\) in \(k\) such that every prime divisor that is ramified over \(k(x)\) does not appear in \(g\left(\frac{ax+b}{cx+d}\right)n\left(\frac{ax+b}{cx+d}\right)\).
Bibliography
