
University of New Mexico

ON EXTENSIONS OF THE FIELD OF CONSTANTS OF AN ALGEBRAIC FUNCTION FIELD

EVAR D. NERING

1. The purpose of this paper is to discuss the applications of a previous paper, Reduction of an algebraic function field modulo a prime in the constant field, [3], to cases where the constant field is extended. For completeness, we shall restate the principal results of that paper.

Let $K$ be an algebraic function field of one variable with constant field $k$, and let $k$ have a discrete non-Archimedean valuation $h$. Let $x$ be a fixed arbitrary element in $K$ transcendental over $k$. Let $h$ be extended to a valuation, also denoted by $h$, of $k(x) = F$ by the Gaussian definition. Then extend $h$ to valuations $H_i$, $i = 1, 2, \ldots, s$, on $K$. Let $K_i$ be the residue class field of $K$ modulo $H_i$. Let $\bar{k}$ and $\bar{F}$ denote the residue class fields of $k$ and $F$ modulo $h$. Properly interpreted, $K_i$ is finite algebraic over $\bar{k}(x) = \bar{F}$, i.e., $K_i$ is an algebraic function field. If $k_i$ is the constant field of $K_i$, then $k_i$ is of finite degree $r_i$ over $\bar{k}$. Let $g$ be the genus of $K$ and $g_i$ the genus of $K_i$. Let $e(H_i)$ be the ramification index of $H_i$. If the radical degree of each $H_i$ is 1, then

Presented to the Society, August 28, 1957 under the title, An application of results on the reduction of an algebraic function field to extensions of the field of constants of an algebraic function field; received by the editors August 21, 1958.
(1) \[ g - 1 = \sum_{i=1}^{r} r_i \cdot e(H_i) (g_i - 1) + \rho, \]

where \( \rho \geq 0. \)

\( \rho \) is one-half the degree of the norm of a conductor. The conductor is a divisor which may have a component of positive order at any valuation, including the infinite primes. However, this conductor is best described in terms of ideals, and to simplify its interpretation we shall assume that the ideals we mention take into account all valuations at which the conductor may be of positive order.

If \( \mathfrak{A} \) is any set of elements in \( K \), we shall denote by \( \mathfrak{A}^* \) the set of those elements of \( \mathfrak{A} \) integral at all extensions of \( h \). There is an element in \( k \) of order one at \( h \), and we shall denote it by \( h \) also. Then \( hK^* \) is an ideal of \( K^* \), and we may construct the residue class ring \( \overline{K} = K^*/hK^* \). For any \( \mathfrak{A} \subset K \), we denote by \( \overline{\mathfrak{A}} \) the image of \( \mathfrak{A}^* \) under the homomorphism of \( K^* \) onto \( \overline{K} \). We see that \( \overline{K} \) contains \( k \) and \( \overline{F} \).

Let \( \mathcal{O}_K \) be the ring of elements in \( K \) integral over \( k[x] \), and let \( \mathcal{O}_{\overline{K}} \) be the ring of elements in \( \overline{K} \) integral over \( \overline{k}[\overline{x}] \). It is easily shown that \( \mathcal{O}_K \subset \overline{\mathcal{O}_K} \). Let \( f \) be the conductor of \( \overline{\mathcal{O}_K} \) with respect to \( \overline{\mathcal{O}_{\overline{K}}} \); \( f = \overline{\mathcal{O}_K} : \overline{\mathcal{O}_{\overline{K}}} \). The norm of \( f \) in \( \overline{F} \) has a divisor of order \( 2\rho \). Since \( \overline{\mathcal{O}_K} \subset \overline{\mathcal{O}_{\overline{K}}} \), \( f \) is integral and \( \rho \geq 0. \)

2. Transcendental extensions. It is well known that the genus of an algebraic function field is unchanged when a transcendental element is adjoined to the constant field (e.g., see E. Artin [1, p. 296], or C. Chevalley [2, p. 99]), but as we need this construction as an intermediate step for the algebraic extensions, we shall include the discussion here.

**Theorem 2.1.** Let \( K \) be an algebraic function field of genus \( g \) with constant field \( k \). If \( \Lambda \) is transcendental over \( K \), then \( K(\Lambda) \) is an algebraic function field of genus \( g \) over \( k(\Lambda) \).

**Proof.** Let \( x \in K \) be transcendental over \( k \) so that \( K \) is finite algebraic over \( F = k(x) \). Define \( \overline{k} = k(\Lambda) \), \( \overline{F} = \overline{k}(x) = \overline{F}(\Lambda) \), and \( \overline{K} = K(\Lambda) = \overline{F}(K) \). Let \( \mathfrak{o} = k[x] \) be a ring of integers in \( F \) and \( \mathcal{O} \) the elements in \( K \) integral over \( \mathfrak{o} \). Let \( \overline{\mathfrak{o}} = \overline{k}[x] \) and \( \overline{\mathcal{O}} \) be defined similarly in \( \overline{F} \) and \( \overline{k} \). It is clear that \( \mathfrak{o} \subset \overline{\mathfrak{o}} \) and \( \mathcal{O} \subset \overline{\mathcal{O}} \).

Now take the valuation \( h \) on \( k \) which is trivial on \( k \) and assigns a value less than 1 to \( \Lambda \). Reduce the field \( \overline{K} \) modulo this prime. The resulting residue class field is actually \( K \) itself. Since \( \mathcal{O} = \overline{\mathcal{O}} \subset \overline{\mathcal{O}} \subset \mathcal{O} \) we see that \( \overline{\mathcal{O}} = \mathcal{O} \). Thus the conductor \( f = \mathcal{O} \). This may also be done for the rings \( \mathfrak{o} = k[1/x] \), \( \overline{\mathfrak{o}} = \overline{k}[1/x] \), and their extensions with similar results. Thus the conductor of \( \overline{K} \) to \( K \) must be the unit divisor and
Furthermore, \( p = 0 \). Furthermore, \( h \) remains prime in \( \overline{K} \) so that \( s = 1 \), \( e(H_1) = 1 \), \( r_1 = 1 \), and, by formula (1), the genus of \( \overline{K} \) is equal to the genus of \( \overline{K}^* = K \).

3. **Algebraic extensions.** A simple algebraic extension can be constructed by making a transcendental extension and then reducing this field modulo the irreducible polynomial for the algebraic element. Let \( K \) be an algebraic function field with constant field \( k \), and let \( \lambda \) be algebraic over \( k \). Let \( \Lambda \) be transcendental over \( K \). Then \( K(\Lambda) = \overline{K} \) is an algebraic function field with constant field \( k(\Delta) = \overline{k} \). The genus of \( \overline{K} \) is the same as the genus of \( K \). Let \( h(\Lambda) \in k[\Lambda] \) be an irreducible polynomial for \( \lambda \). Then \( h(\Lambda) \) defines a discrete non-Archimedean valuation \( h \) on \( k \). Let \( x \) be an arbitrary, but fixed, element in \( K \) transcendental over \( k \), and extend \( h \) to a valuation of \( k(x) = \overline{F} \) by the Gaussian definition. Since \( \overline{K} \) is algebraic over \( \overline{F} \), we can extend \( h \) to \( \overline{K} \). The first step is to determine the nature of this extension.

**Theorem 3.1.** There is but one extension \( H \) of \( h \) to a valuation of \( \overline{K} \).

**Proof.** Since \( k \) is relatively algebraically closed in \( K \) and \( h(\Lambda) \) is irreducible in \( k[\Lambda] \), \( h(\Lambda) \) is also irreducible in \( K[\Lambda] \). Since \( h(\Delta) \) is of positive order at any extension of \( h \) to \( \overline{K} \) and irreducible, there is but one extension \( H \) of \( h \) to a valuation of \( \overline{K} \).

**Theorem 3.2.** \( e(H) = 1 \).

**Proof.** Since \( h(\Delta) \) is irreducible in \( K[\Lambda] \), it is also irreducible in \( F[\Lambda] \). The ring of integers of \( h \) in \( \overline{F} \) is

\[
F^* = \{f(\Lambda)/g(\Lambda); \text{where } f(\Lambda), g(\Lambda) \in F[\Lambda] \text{ and } h(\Lambda) \not| g(\Lambda)\}.
\]

Then the residue class field of \( h \) in \( \overline{K} \) is \( F(\lambda) \). The ring of integers of \( H \) in \( \overline{K} \) is \( \overline{K}^* = \{f(\Lambda)/g(\Lambda); \text{where } f(\Lambda), g(\Lambda) \in K[\Lambda] \text{ and } h(\Lambda) \not| g(\Lambda)\} \).

The residue class field of \( H \) in \( \overline{K} \) is \( K(\lambda) \). Thus the residue class-field degree of \( H \) is \([K(\lambda): F(\lambda)] = [K: F] = [\overline{K}: \overline{F}] \). Since \([\overline{K}: \overline{F}] = e(H)[K(\lambda): F(\lambda)] \), we see that \( e(H) = 1 \).

Now \( \overline{K} = \overline{K}^*/(h) \) is a ring which has a radical \( \Gamma \neq \{0\} \) only if \( H \) is ramified over \( h \). Thus \( \overline{K} = K(\lambda) \) is the residue class field of \( H \) in \( \overline{K} \). \( \overline{F} = F^*/(h) \cap \overline{F}^* \) and \( \overline{k} = k^*/(h) \cap k^* \) are subfields of \( \overline{K} \). Since \( \overline{F} \) is transcendental over \( k \) and \( \overline{K} \) is algebraic over \( \overline{F} \), \( \overline{K} \) is an algebraic function field of genus \( g_1 \). Let \( k_1 \supset k \) be the constant field of \( \overline{K} \), and let \( r_1 \) be the degree of \( k_1 \) over \( k \). In this case, formula (1) reduces to

\[
g - 1 = r_1(g_1 - 1) + \rho.
\]

The terms \( r_1 \) and \( \rho \) have been identified, but we wish to examine them in more detail.
Theorem 3.3. If either \( K \) is separable over \( F \) or \( k = k(\lambda) \) is separable over \( k \), then \( k(\lambda) \) is the field of constants of \( K \), i.e., \( k(\lambda) \) is relatively algebraically closed in \( K \).

A proof of this theorem is given by Chevalley, [2, p. 91]. In the same place, Chevalley gives an example in which \( r_1 \neq 1 \). In this example, \( P \) is a field of characteristic \( p \); \( a, b \), and \( x \) are algebraically free over \( P \). \( k = P(a, b) \), \( F = k(x) \), and \( K = F(y) \) where \( y^p = ax^p + b \). Upon adjoining \( \lambda = a^{1/p} \) to \( K \), the field of constants becomes \( k = P(\lambda, y - \lambda x) \), which is algebraic of degree \( p \) over \( k = P(\lambda, b) \). In formula (2), the terms are \( g = (p - 1)(p - 2)/2 \), \( r_1 = p \), \( g_1 = 0 \), and \( \rho = p(p - 1)/2 \).

Theorem 3.4. If \( h(\Lambda) \) is separable, then \( \Omega_K = \Omega_K \).

Proof. Let \( m \) be the degree of \( h(\Lambda) \) and let \( \lambda \) be the image of \( \Lambda \) in \( K \), i.e., \( h(\lambda) = 0 \). Then \( \{1, \lambda, \ldots, \lambda^{m-1}\} \) is a basis of \( K \) over \( K \). It is also a basis of \( \Omega_K \) over \( \Omega_K \). Since \( K \) is separable over \( K \), the trace \( S_{K/K} \) of \( K \) into \( K \) is a nontrivial linear map of \( K \) into \( K \).

Since \( h(\Lambda) \in k[\Lambda] \), \( S_{K/K}(\lambda^i) \in k \) for all \( i \geq 0 \). Thus the complementary module \( \Omega_K \) of \( \Omega_K \) with respect to \( S_{K/K} \) is \( \Omega_K \) itself, i.e., \( \Omega_K = \Omega_K \). This is easily seen by computing a basis of \( \Omega_K \). For each \( i = 0, 1, \ldots, m-1 \), solve the system of equations

\[
\sum_{j=0}^{m-1} a_{ij}S_{K/K}(\lambda^j\lambda^i) = \delta_{il} \quad (l = 0, 1, \ldots, m - 1)
\]

for the \( a_{ij} \). The determinant of the system of equations is \( \neq 0 \) and in \( k \). Thus the \( a_{ij} \in k \), and hence

\[
\Lambda_i = \sum_{j=0}^{m-1} a_{ij}\lambda^j \in k.
\]

Since \( \Lambda_i \in k \subseteq \Omega_K \), \( \alpha \in \Omega_K \) implies that \( S_{K/K}(\alpha \Lambda_i) \in \Omega_K \). Let \( \alpha = \sum_{j=0}^{m-1} a_j\lambda^j \). Then \( S_{K/K}(\alpha \Lambda_i) = \sum_{j=0}^{m-1} a_jS_{K/K}(\lambda^j\Lambda_i) = a_i \) so that \( a_i \in \Omega_K \) and \( \alpha \in \Omega_K \). This shows that \( \Omega_K \subseteq \Omega_K \). But since \( S_{K/K}(\Omega_K) \subseteq \Omega_K \), \( \Omega_K \subseteq \Omega_K \), and hence \( \Omega_K = \Omega_K \).

Since \( \Omega_K \) is integral over \( \Omega \) and algebraic over \( K \), \( \Omega_K \) is also integral over \( \Omega_K \). Thus \( S_{K/K}(\Omega_K) \subseteq \Omega_K \). But then \( S_{K/K}(\Omega_K \Omega_K) = S_{K/K}(\Omega_K) \subseteq \Omega_K \) so that \( \Omega_K \subseteq \Omega_K = \Omega_K \). But since \( \Omega_K \subseteq \Omega_K \), we see that \( \Omega_K = \Omega_K \).

Corollary 3.5. If \( h(\Lambda) \) is separable, \( \rho = 0 \).

Proof. Since \( \Omega_K = \Omega_K \), \( f \) is the unit ideal, \( f = \Omega_K \), and hence \( \rho = 0 \).

Theorem 3.6. If \( h(\Lambda) \) is separable, then the genus of \( K \) is equal to the genus of \( K \).
Proof. Of the terms in formula (2), \( r_1 = 1 \) and \( \rho = 0 \). Thus \( g - 1 = g_1 - 1 \), or \( g = g_1 \).

There remains the question of what happens when \( h(\Lambda) \) is inseparable. This question has already been treated by Tate in \([4]\). His result is the assertion that \( g - g_i \) is divisible by \((p - 1)/2\). To establish this result Tate shows that the degree of the divisor of a different is divisible by \( p - 1 \). In our notation the different occurring in Tate's work is \( \Delta'_K : \Delta_K \). To make use of Tate's work we shall establish the following theorem.

**Theorem 3.7.** \( \Delta'_K : \Delta_K = \Delta_K : \Delta'_K = \mathfrak{f} \).

**Proof.** Let \( \mathfrak{L} \) be any nontrivial linear mapping of \( \overline{K} \) into \( K \). Let \( \Delta'_K = \{ \gamma : \mathfrak{L}(\gamma \Delta_K) \subseteq \Delta_K \} \), \( \Delta'_K = \{ \gamma : \mathfrak{L}(\gamma \Delta_K) \subseteq \Delta_K \} \), and \( \mathfrak{f} = \Delta_K : \Delta_K \).

For any \( \beta \in \mathfrak{f} \), \( \mathfrak{L}(\beta \Delta'_K \Delta_K) \subseteq \mathfrak{L}(\Delta'_K \Delta_K) \subseteq \Delta_K \) so that \( \beta \Delta_K \subseteq \Delta_K \). Thus \( \mathfrak{f} \subseteq \Delta'_K : \Delta_K \). On the other hand, let \( \beta \in \Delta'_K : \Delta_K \). Then \( \mathfrak{L}(\beta \Delta'_K \Delta_K) \subseteq \mathfrak{L}(\Delta'_K \Delta_K) \subseteq \Delta_K \) so that \( \beta \Delta_K \subseteq (\Delta'_K)' = \Delta_K \). Thus \( \Delta'_K : \Delta_K \subseteq \Delta_K : \mathfrak{f} = \mathfrak{f} \). This shows that \( \mathfrak{f} = \Delta'_K : \Delta_K \).

**Corollary 3.8.** \( \rho \) is divisible by \((p - 1)/2\).

**Proof.** In view of Theorem 3.7, any statement about the conductor is equivalent to a corresponding statement about the different. Lemma 3 by Tate in \([4]\) implies the statement of the corollary.

The conductor which plays a role here and the different used by Tate are essentially dual. Tate starts with a differential \( \omega \) mapping \( K \) into \( k \) and defines linear mappings \( S_0 \) of \( k_1 \) into \( k \) and \( S_\alpha \) of \( \overline{K} \) into \( K \). He then shows the existence of a differential \( \Omega \) mapping \( \overline{K} \) into \( k_1 \) such that \( \omega S_\alpha = S_0 \Omega \). The different in Tate's result is related to the mapping \( S_\alpha \). In our construction, it is the differential \( \Omega \) which is given by the linear mapping \( \mathfrak{L} \) of \( \overline{K} \) into \( \overline{k} \). We then define a corresponding linear mapping of \( \overline{K} \) into \( \overline{k} \), also denoted by \( \mathfrak{L} \). We then fill out the picture by constructing the conductor to relate these two linear mappings. Theorem 3.7 shows that the two methods, though starting at different points, are entirely analogous.

**Bibliography**


University of Arizona