GENUS CHANGE IN INSEPAREABLE EXTENSIONS
OF FUNCTION FIELDS

JOHN TATE

1. A substitute for the trace in inseparable extensions of degree $p$.
Let $k$ be any field of characteristic $p > 0$, and suppose that $K$ is an inseparable extension of $k$ of degree $p$. If we select any fixed generator $\alpha$ of $K$ over $k$ and express the generic element $\xi \in K$ in terms of $\alpha$:

$$\xi = x_0 + x_1\alpha + \cdots + x_p\alpha^{p-1}, \quad x_i \in k,$$

we can define a nontrivial $k$-linear map $S_\alpha$ of $K$ onto $k$ by putting

$$S_\alpha(\xi) = x_{p-1}.$$

Since $\alpha$ satisfies an equation of the form $X^p - a$ over $k$, we have, for $0 \leq r \leq p-1$,

$$\xi \alpha^{p-1-r} = x_0\alpha^{p-1-r} + \cdots + x_r\alpha^{p-1} + x_{r+1}a + \cdots + x_{p-1}\alpha^{p-1-r-1}.$$

Therefore $x_r = S_\alpha(\xi\alpha^{p-1-r})$ and the formula

$$\xi = \sum_{r=0}^{p-1} S_\alpha(\xi\alpha^{p-1-r})\alpha^r$$

holds for all $\xi \in K$.

$S_\alpha$ is a particularly convenient substitute for the trace from $K$ to $k$, which is identically 0. Of course $S_\alpha$, although not completely arbitrary, is nevertheless noninvariant, and the question arises as to how $S_\alpha$ transforms if we replace $\alpha$ by another generator $\beta$. This question can be more precisely stated if we recall that since $K$ is a field and $S_\alpha$ is nontrivial, any $k$-linear map $S$ of $K$ into $k$ can be expressed in the form $S(\xi) = S_\alpha(\xi \gamma)$, where $\gamma$ is some element of $K$ uniquely determined by $S$. Our question is therefore: How does one compute, in terms of $\alpha$ and $\beta$, the element $\gamma$ for which $S_\beta(\xi) = S_\alpha(\xi \gamma)$?

The answer is most conveniently expressed in terms of derivations. A derivation in a ring is a map $x \mapsto Dx$ of the ring into itself with the properties $D(x+y) = D(x) + D(y)$ and $D(xy) = x(Dy) + (Dx)y$. The rule $D(x^r) = r\alpha^{p-1}Dx$ follows by induction if the ring is commutative. The ordinary formal differentiation $F(X) \mapsto F'(X)$ is a derivation in the ring $k[X]$ of polynomials in one letter $X$ over our field $k$. It maps a principal ideal generated by a polynomial of the form $X^p - a$ into itself because $((X^p - a)F(X))' = (X^p - a)F'(X)$. The
kernel of the homomorphism $F(X) \rightarrow F(\alpha)$ of $k[X]$ onto $K$ is an ideal of this type. Therefore, the formal differentiation in $k[X]$ induces a well-defined derivation in $K$ which we can denote by $D_\alpha$. Namely, if $\xi = F(\alpha)$ is any expression of an element $\xi \in K$ as a polynomial in $\alpha$ with coefficients in $k$, then $D_\alpha \xi = F'(\alpha)$. Especially, if $\xi$ is the element in (1), then

$$D_\alpha \xi = x_1 + 2x_2 \alpha + \cdots + (p - 1)x_{p-1} \alpha^{p-2}.$$  

It is clear that $D_\alpha \xi = 0$ if and only if $\xi \in k$, and that $D_\alpha$ is $k$-linear.

One relationship between $D_\alpha$ and $S_\alpha$ is

$$S_\alpha(D_\alpha(\xi)) = 0$$

for all $\xi \in K$, as one sees from a glance at (1), (2), and (4). Somewhat more interesting is the following lemma.

**Lemma 1.** $S_\alpha(\xi^{p-1}D_\alpha \xi) = (D_\alpha \xi)^p$ for all $\xi \in K$.

**Remark.** Since $\xi^p \in k$, an equivalent statement is:

$$S_\alpha \left( \frac{D_\alpha \xi}{\xi} \right) = \left( \frac{D_\alpha \xi}{\xi} \right)^p \text{ for all } \xi \neq 0 \text{ in } K.$$  

In other words the function $S_\alpha$ of a "logarithmic derivative" equals the $p$th power of the logarithmic derivative.\(^1\)

**Proof.** Let $R$ be the set of those $\xi \in K$ for which the statement is true. The nonzero elements of $R$ form a multiplicative group because, according to the remark above, they comprise the kernel of the homomorphism $\xi \rightarrow S_\alpha((D_\alpha \xi)/\xi) - ((D_\alpha \xi)/\xi)^p$ of the multiplicative group of $K$ into the additive group of $k$.

If $\xi \in R$, then $\xi + 1 \in R$. Indeed, since $D_\alpha(\xi + 1) = D_\alpha \xi$ we have only to show that $S_\alpha((\xi + 1)^{p-1}D_\alpha \xi) = S_\alpha(\xi^{p-1}D_\alpha \xi)$. This is true according to rule (5) because $((\xi + 1)^{p-1} - \xi^{p-1})D_\alpha \xi$ is a sum of terms of the form $\xi^rD_\alpha \xi$ with $0 \leq \xi \leq p - 2$, which can be "integrated": $\xi^rD_\alpha \xi = D_\alpha(\xi^{r+1}/r + 1)$. Therefore $R$ is closed under addition, because if $\xi \in R$, and $\eta \neq 0, \eta \in R$, then $\xi + \eta = \eta(\eta^{-1}\xi + 1) \in R$.

It is obvious that $k \subset R$ and $\alpha \in R$. We have proved that $R$ is a subfield of $K$ which contains $k$ and $\alpha$. Therefore $R = K$ as contended.

Our question can now be answered.

---

\(^1\) Since $D_\alpha^{-1}(\xi) = (p - 1)x_{p-1} - x_{p-1} = -S_\alpha(\xi)$, our lemma can be viewed as a special case of Theorem 15 of N. Jacobson's paper *Abstract derivations and Lie algebras* (Trans. Amer. Math. Soc. vol. 42 (1937)), where the converse statement—that the above-mentioned property characterizes the elements which are logarithmic derivatives—is also proved.
THEOREM 1. If α and β are two generators of K over k, then \( S_\beta(\xi) = S_\alpha(\xi(D_\alpha \beta)^{1-p}) \) for all \( \xi \in K \).

PROOF. Since both sides are \( k \)-linear functions of \( \xi \), it suffices to prove the statement for the special cases \( \xi = \beta^\nu, 0 \leq \nu \leq p-1 \). Multiplying through by \( (D_\alpha \beta)^\nu \in k \), we must show
\[
(D_\alpha \beta)^\nu S_\beta(\beta^\nu) = S_\alpha(\beta^\nu D_\alpha \beta), \quad 0 \leq \nu \leq p - 1.
\]
For \( \nu = p-1 \), \( \beta^\nu D_\alpha \beta = D_\alpha(\beta^{p+1}/p + 1) \). Hence, by (5), the right side is 0, as is the left. For \( \nu = p-1 \) the left side is \( (D_\alpha \beta)^\nu \), as is the right side according to Lemma 1.

2. Application to the genus change in function fields. There is an interesting application of Theorem 1 to the case in which \( k \) is an algebraic function field in one variable with constant field \( k_0 \). Then \( K \) is also an algebraic function field of one variable over a certain constant field \( K_0 \) which is a finite extension of \( k_0 \). We shall derive an analogue of Zeuthen's formula relating the genus \( G \) of \( K \) to the genus \( g \) of \( k \), the most interesting aspect of which is that it shows that the genus change \( G-g \) is divisible by \( (p-1)/2 \). The general facts about function fields which we presuppose are explained in [1] and [2].

If \( \alpha \) is a generator of \( K \) over \( k \), then any repartition (valuation vector) \( \mathfrak{v} \) of \( K \) can be written uniquely in the form
\[
\mathfrak{v} = \mathfrak{v}_0 + \mathfrak{v}_1 \alpha + \cdots + \mathfrak{v}_{p-1} \alpha^{p-1}
\]
where the coefficients \( \mathfrak{v}_i \) are repartitions of \( k \). The \( k \)-linear map \( S_\alpha \) of \( K \) onto \( k \) which we have discussed in §1 can therefore be extended to a \( k \)-linear map of the space of repartitions of \( K \) onto the space of repartitions of \( k \) by defining
\[
S_\alpha(\mathfrak{v}) = \mathfrak{v}_{p-1}.
\]
This extended map \( S_\alpha \) is continuous in the sense that to any divisor \( a \) of \( k \) there exists a divisor \( \mathfrak{A} \) of \( K \) such that \( \mathfrak{A}|\mathfrak{v} \) implies \( a|S_\alpha(\mathfrak{v}) \).

Therefore, if \( \omega \) is a nontrivial differential of \( k \) and we define \( \Phi(\mathfrak{v}) = \omega(S_\alpha(\mathfrak{v})) \), then \( \Phi \) is a nontrivial \( k_0 \)-linear map of the space of repartitions of \( K \) onto \( k_0 \) which vanishes on elements of \( K \), and on all repartitions of \( K \) which are divisible by a certain fixed divisor of \( K \). Such a map \( \Phi \) is a differential of \( K \) in case \( K_0 = k_0 \); in any case we can easily replace \( \Phi \) by a true differential \( \Omega \) of \( K \). The formula we are looking for will then result from a comparison of the divisors of \( \Omega \) and \( \omega \).

To define \( \Omega \) we need the following abstract lemma.

LEMMA 2. Let \( k_0 \) be a field, \( K_0 \) a finite extension of \( k_0 \), and let \( S_0 \) be a
fixed nontrivial \( k_0 \)-linear map of \( K_0 \) into \( k_0 \). Then if \( X \) is any vector space over \( K_0 \) (therefore also over \( k_0 \)) and \( \Phi \) is any \( k_0 \)-linear map of \( X \) into \( k_0 \), there exists a uniquely determined \( K_0 \)-linear map \( \Omega \) of \( X \) into \( K_0 \) such that \( \Phi = S_0 \Omega \); i.e. \( \Phi(\vec{x}) = S_0(\Omega(\vec{x})) \) for all \( \vec{x} \in X \).

**Proof.** If such a map \( \Omega \) did exist, we would have, for each \( \vec{x} \in X \),

\[
S_0(\Omega(\vec{x})) = S_0(S_0(\vec{x})) = \Phi(\vec{x})
\]

for all \( \vec{x} \in K_0 \). The right-hand side, viewed as a function of \( \vec{x} \), is a \( k_0 \)-linear map of \( K_0 \) into \( k_0 \). Therefore, since \( S_0 \) is nontrivial, there does exist a unique element \( \Omega(\vec{x}) \in K_0 \) which makes the left-hand side of (8) equal to the right. Thus, (8) defines a function \( \Omega(\vec{x}) \). This function has the property \( \Phi = S_0 \Omega \), as we see by putting \( \vec{x} = 1 \) in (8). It is \( K_0 \)-linear because we can prove readily from the definition that

\[
S_0(\Omega(\alpha \vec{x} + \beta \vec{y})) = S_0(\alpha \Omega(\vec{x}) + \beta \Omega(\vec{y}))
\]

for all \( \vec{x} \in K_0 \), for any \( \alpha, \beta \in K_0 \), and any \( \vec{x}, \vec{y} \in X \). This proves the lemma.

Returning to the function fields, let \( S_0 \) be an arbitrary but fixed nontrivial \( k_0 \)-linear map of \( K_0 \) into \( k_0 \), and define \( \Omega \) to be the \( K_0 \)-linear map of the space of repartitions of \( K \) into \( K_0 \) for which

\[
S_0(\Omega(\vec{x})) = \Phi(\vec{x}) = \omega(S_\alpha(\vec{x})).
\]

Then \( \Omega \) is a nontrivial differential of \( K \) which we can use as a substitute for the cotrace of \( \omega \) from \( k \) to \( K \). The corresponding substitute for the different of \( K \) over \( k \) is the divisor \( D_\alpha \) of \( K \) such that

\[
(\Omega) = (\text{Con}_{k/K}(\omega))D_\alpha
\]

where \( (\Omega) \) and \( (\omega) \) are the divisors of \( \Omega \) and \( \omega \) in \( k \) and \( K \).

The computation of \( D_\alpha \) is a purely local problem. Above each place \( \mathfrak{p} \) of \( k \) there lies only one place \( \mathfrak{p} \) of \( K \). This follows for example from the fact that since \( K_\mathfrak{p} \subset k \), the ordinal number function at any \( \mathfrak{p} \) above \( \mathfrak{p} \) is determined up to a constant factor by the ordinal number function at \( \mathfrak{p} \). If \( K_\mathfrak{p} \) and \( k_\mathfrak{p} \) are the respective completions, then \( (K_\mathfrak{p}/k_\mathfrak{p}) = \mathfrak{p} \) since the global degree \( p \) is the sum of the local degrees above each \( \mathfrak{p} \) of \( k \). Viewing our generator \( \alpha \) of \( K \) over \( k \) as an element of \( K_\mathfrak{p} \), we have \( K_\mathfrak{p} = k_\mathfrak{p}(\alpha) \). If \( S_\alpha^\mathfrak{p} \) is the corresponding \( k_\mathfrak{p} \)-linear map of \( K_\mathfrak{p} \) onto \( k_\mathfrak{p} \), then the local description of the repartition map \( S_\alpha \) is

\[
(S_\alpha(\vec{x}))_\mathfrak{p} = S_\alpha^\mathfrak{p}(\vec{x}_\mathfrak{p})
\]

for all repartitions \( \vec{x} = (\vec{x}_\mathfrak{p}) \) of \( K \). It follows, just as in the case of the ordinary different, that \( \rho_\mathfrak{p}(D_\alpha) \) is the greatest rational integer such that:
If e and f are the ramification index and residue class field degree of \( \mathfrak{B} \) over \( p \), then \( ef = (K_{\mathfrak{B}}/K_0) = p \). Thus there are only two possibilities: \( e = 1 \), \( f = p \), and \( e = p \), \( f = 1 \). In both cases, the ring of integers \( \mathfrak{O} \) of \( K_{\mathfrak{B}} \) has an integral basis \( (\text{minimal basis}) \) over the ring of integers \( \mathfrak{O} \) of \( k_p \) consisting of the powers of one element \( \tau \in K_{\mathfrak{B}} \):

\[
\mathfrak{O} = \mathfrak{O} + \mathfrak{O} \tau + \cdots + \mathfrak{O} \tau^{p-1}.
\]

For example, in the first case we can take \( \tau \) to be any unit in \( K_{\mathfrak{B}} \), the residue class which generates the residue class field extension; in the second case we can take \( \tau \) to be any local uniformizing parameter in \( K_{\mathfrak{B}} \). Let \( \tau \) be any such element of \( K_{\mathfrak{B}} \), and let \( D_\tau \) be the derivation with respect to \( \tau \) in the \( p \)-extension \( K_{\mathfrak{B}}/K_0 \).

**Lemma 3.** \( \nu_{\mathfrak{B}}(\mathfrak{D}_\alpha) = \nu_{\mathfrak{B}}((D_\tau \alpha)^{1-p}) \).

**Proof.** By formula (3) and Theorem 1 we have for \( \xi \in K_{\mathfrak{B}} \):

\[
\xi(D_\tau \alpha)^{1-p} = \sum_{r=0}^{p-1} S_r(\xi(D_\tau \alpha)^{1-p} \tau^{p-1-r}) \tau^r = \sum_{r=0}^{p-1} S_\alpha^{\mathfrak{B}}(\xi \tau^{p-1-r}) \tau^r.
\]

If \( \nu_{\mathfrak{B}}(\xi) \geq -\nu_{\mathfrak{B}}((D_\tau \alpha)^{1-p}) \), then the left side is integral and consequently so are all the coefficients on the right, in particular the last, which is \( S_\alpha^{\mathfrak{B}}(\xi) \). On the other hand, if \( \xi \) is some element with \( \nu_{\mathfrak{B}}(\xi) = -\nu_{\mathfrak{B}}((D_\tau \alpha)^{1-p}) - 1 \), then the left side is not integral and consequently one of the coefficients \( S_\alpha^{\mathfrak{B}}(\xi \tau^{p-1-r}) \) is not integral. Therefore \( \xi \tau^{p-1-i} \) is an element of order not less than \( -\nu_{\mathfrak{B}}((D_\tau \alpha)^{1-p}) - 1 \), the \( S_\alpha^{\mathfrak{B}} \) of which is not integral. Thus we have shown that \( \nu_{\mathfrak{B}}((D_\tau \alpha)^{1-p}) \) has the property characterizing \( \nu_{\mathfrak{B}}(\mathfrak{D}_\alpha) \) stated above.

**Theorem 2.** The genera \( G \) and \( g \) of \( K = k(\alpha) \) and \( k \) are related by the formula

\[
2G - 2 = \rho^{1-n}(2g - 2) + (1 - \rho) \sum_\mathfrak{B} \nu_{\mathfrak{B}}(D_\tau \mathfrak{B}) \deg \mathfrak{B}
\]

where \( \tau_\mathfrak{B} \) is the \( \tau \) of the preceding paragraphs, and \( n \) is defined by \( (K_0/k_0) = p^n \).

**Proof.** The term on the left equals \( \deg (\Omega) \). The first term on the right equals \( \deg (\text{Con}_{k(\omega)}(\alpha)) \). The sum on the right equals \( \deg \mathfrak{D}_\alpha \) according to Lemma 3. Therefore our theorem simply states the equality of the degrees in formula (10).

**Corollary 1.** If \( k \) is a field of algebraic functions of one variable of
characteristic \( p > 0 \) and genus \( g \), and \( K \) is a totally inseparable finite extension of \( k \) of genus \( G \), then \( G - g \) is divisible by \( (p - 1)/2 \).

**Proof.** Since the extension \( K/k \) can be broken into steps of degree \( p \), it is enough to prove the statement in case \( (K/k) = p \). In this case, upon multiplying the formula of the preceding theorem through by \( p^n \) and reading it modulo \( (p - 1) \), we obtain

\[
2G - 2 = 2g - 2 \pmod{(p - 1)}.
\]

**Remark.** A simple example of the situation we are discussing is the case where \( f_e = f_{e0}(x, y) \) is a hyperelliptic field generated by an equation of the form \( y^2 = x^p - a \ (p \neq 2) \), of genus \( (p - 1)/2 \). Upon adjunction of \( a^{1/p} \) we obtain a rational field of genus 0. Corollary 1 shows that this genus drop is typical.

**Corollary 2.** If \( k \) is a field of algebraic functions of one variable of characteristic \( p > 0 \) and genus \( g < (p - 1)/2 \), then \( k \) is what Artin [2] has called a "conservative" field. That is, the genus of \( k \) is invariant under all constant field extensions.

**Proof.** This follows immediately from Corollary 1 and the well known facts: (a) that if the genus changes under any constant field extension, the change occurs already in a finite purely inseparable constant extension; (b) that in the latter case the genus can only decrease, never increase; (c) the genus is always \( \geq 0 \).

**Remark.** Fact (b) above follows at once from Theorem 2 because in the case of a constant field extension we have \( n \geq 1 \) and can take \( \alpha \in K_\beta \), so that \( v_\beta(D_{\beta\alpha}) \geq 0 \) for all \( \beta \).

It is perhaps of some interest to see how the numbers \( v_\beta(D_{\beta\alpha}) \) in the formula of Theorem 2 may be computed in the ground field \( k \) in terms of the element \( a = a^p \in k \), the \( p \)th root of which is extracted to obtain \( K \). This is easily done.

**Proposition.** Let \( \mathfrak{p} \) be the place of \( k \) below \( \mathfrak{P} \). Let

\[
r_\mathfrak{p} = \max_{x \in \mathfrak{p}} \{ v_\mathfrak{p}(a - x^p) \}.
\]

Then

\[
p^n v_\mathfrak{p}(D_{\beta\alpha}) \deg \mathfrak{P} = \begin{cases} r_\mathfrak{p} \deg \mathfrak{p}, & \text{if } p \mid r_\mathfrak{p}, \\ (r_\mathfrak{p} - 1) \deg \mathfrak{p}, & \text{if } p \nmid r_\mathfrak{p}.
\end{cases}
\]

**Proof.** Since \( K_\mathfrak{P} = k_\mathfrak{P}(\alpha) = k_\mathfrak{P}(a^{1/p}) \), and \( (K_\mathfrak{P}/k_\mathfrak{P}) = p \), \( a \) is not a \( p \)th power in \( k_\mathfrak{P} \). Therefore \( r_\mathfrak{p} < \infty \). Let \( b \) be an element of \( k_\mathfrak{P} \) such that \( r_\mathfrak{p} = r_\mathfrak{P}(a - b^p) \).

Case 1. If \( p \mid r_\mathfrak{p} \), let \( r_\mathfrak{p} = sp \). Let \( t \) be a local uniformizing parameter
in $k_p$, and put $\tau = (\alpha - b)t^{-s} \in K_\mathfrak{p}$. Then $\tau^p = (a - b^p)t^{-sp}$ is a unit in $k_p$. The residue class of this unit is not a $p$th power of a residue class in $k_p$. Otherwise, if $c \in k_p$, such that $c^p \equiv (a - b^p)t^{-sp} \pmod{p}$, then the $p$th power, $b^p + t^{sp}c^p$, would be a better approximation to $a$ than $b^p$. Therefore we have $f = p$, $e = 1$ in this case, and the powers of $\tau$ are an integral basis for $\mathcal{O}$ over $\mathfrak{o}$. $D, \alpha = (D_\alpha \tau)^{-1} = t^s$ shows that $\nu_\mathfrak{p}(D, \alpha) = s$ and therefore $\nu_\mathfrak{p}(D, \alpha)p^n \deg \mathfrak{B} = sp \deg p = r_\mathfrak{p} \deg p$.

Case 2. If $p \nmid r_\mathfrak{p}$, solve the diophantine equation $r_\mathfrak{p}l - pm = 1$. Let $l$ be a local uniformizing parameter in $k_p$, and put $r = (\alpha - b)t^{-m} \in K_\mathfrak{p}$. Then $\tau^p = (\alpha - b^p)t^{-mp}$ has ordinal number $r_\mathfrak{p}l - mp = 1$ in $k_p$. Therefore $e = p$, $f = 1$, $\tau$ is a local uniformizing parameter in $K_\mathfrak{p}$, and the powers of $\tau$ are an integral basis. $D_\alpha \tau = l(\alpha - b)t^{-l} - m = l(\alpha - b)^{-1}r$ shows that $D, \alpha = (D_\alpha \tau)^{-1} = l^{-1}(\alpha - b)^{-1}r^{-1}$ has ordinal number $r_\mathfrak{p} - 1$ in $K_\mathfrak{p}$, because $l$ is prime to $p$ and $\alpha - b$ has ordinal number $r_\mathfrak{p}$ in $K_\mathfrak{p}$. Therefore $\nu_\mathfrak{B}(D, \alpha)p^n \deg \mathfrak{B} = (r_\mathfrak{p} - 1) \deg p$.

References

1. C. Chevalley, Introduction to the theory of algebraic functions of one variable, Mathematical Surveys, no. 6, American Mathematical Society, 1951. (Especially chapters I, III, IV, and VI.)
2. E. Artin, Algebraic numbers and algebraic functions. I, Notes, New York University, Summer 1951. (Especially chapters 13, 15, and 17.)

Princeton University