GENUS CHANGE IN INSEPARABLE 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 α of K over k and express the generic element $\xi \in K$ in terms of α:

$$\xi = x_0 + x_1\alpha + \cdots + x_{p-1}\alpha^{p-1}, \qquad x_i \in k, \tag{1}$$

we can define a nontrivial k-linear map S_α of K onto k by putting

$$S_\alpha(\xi) = x_{p-1}. \tag{2}$$

Since α satisfies an equation of the form $X^p - a$ over k, we have, for $0 \leqq \nu \leqq p-1$,

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

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

$$\xi = \sum_{\nu=0}^{p-1} S_\alpha\ (\xi\alpha^{p-1-\nu})\alpha^\nu \tag{3}$$

holds for all $\xi \in K$.

S_α is a particularly convenient substitute for the trace from K to k, which is identically 0. Of course S_α, although not completely arbitrary, is nevertheless noninvariant, and the question arises as to how S_α transforms if we replace α by another generator β. This question can be more precisely stated if we recall that since K is a field and S_α is nontrivial, any k-linear map S of K into k can be expressed in the form $S(\xi) = S_\alpha(\xi\gamma)$, where γ is some element of K uniquely determined by S. Our question is therefore: How does one compute, in terms of α and β, the element γ 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 $x \rightarrow Dx$ of the ring into itself with the properties $D(x+y) = D(x) + D(y)$ and $D(xy) = x(Dy) + (Dx)y$. The rule $D(x^\nu) = \nu x^{\nu-1}Dx$ follows by induction if the ring is commutative. The ordinary formal differentiation $F(X) \rightarrow F'(X)$ 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

Received by the editors July 23, 1951.

kernel of the homomorphism $F(X) \to F(\alpha)$ 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_α. Namely, if $\xi = F(\alpha)$ is any expression of an element $\xi \in K$ as a polynomial in α with coefficients in k, then $D_\alpha \xi = F'(\alpha)$. Especially, if ξ is the element in (1), then

$$D_\alpha \xi = x_1 + 2x_2\alpha + \cdots + (p-1)x_{p-1}\alpha^{p-2}. \tag{4}$$

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

One relationship between D_α and S_α is

$$S_\alpha(D_\alpha(\xi)) = 0 \tag{5}$$

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:

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

In other words the function S_α *of a "logarithmic derivative" equals the pth 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 $\xi \to S_\alpha((D_\alpha\xi)/\xi) - ((D_\alpha\xi)/\xi)^p$ 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 $\xi^\nu D_\alpha\xi$ with $0 \leqq \xi \leqq p-2$, which can be "integrated": $\xi^\nu D_\alpha\xi = D_\alpha(\xi^{\nu+1}/\nu+1)$. 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 α. Therefore $R = K$ as contended.

Our question can now be answered.

---

[1] Since $D_\alpha^{p-1}(\xi) = (p-1)!x_{p-1} = -x_{p-1} = -S_\alpha(\xi)$, 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 ξ, it suffices to prove the statement for the special cases $\xi = \beta^\nu$, $0 \leqq \nu \leqq p-1$. Multiplying through by $(D_\alpha\beta)^p \in k$, we must show

$$(D_\alpha\beta)^p S_\beta(\beta^\nu) = S_\alpha(\beta^\nu D_\alpha\beta), \qquad 0 \leqq \nu \leqq p-1.$$

For $\nu < p-1$, $\beta^\nu D_\alpha\beta = D_\alpha(\beta^{\nu+1}/\nu+1)$. Hence, by (5), the right side is 0, as is the left. For $\nu = p-1$ the left side is $(D_\alpha\beta)^p$, 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 α is a generator of K over k, then any repartition (valuation vector) $\mathfrak{X}$ of K can be written uniquely in the form

$$\mathfrak{X} = \mathfrak{x}_0 + \mathfrak{x}_1\alpha + \cdots + \mathfrak{x}_{p-1}\alpha^{p-1} \tag{6}$$

where the coefficients $\mathfrak{x}_i$ are repartitions of k. The k-linear map S_α 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

$$S_\alpha(\mathfrak{X}) = \mathfrak{x}_{p-1}. \tag{7}$$

This extended map S_α is continuous in the sense that to any divisor $\mathfrak{a}$ of k there exists a divisor $\mathfrak{A}$ of K such that $\mathfrak{A} | \mathfrak{X}$ implies $\mathfrak{a} | S_\alpha(\mathfrak{X})$. Therefore, if ω is a nontrivial differential of k and we define $\Phi(\mathfrak{X}) = \omega(S_\alpha(\mathfrak{X}))$, then Φ 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 Φ is a differential of K in case $K_0 = k_0$; in any case we can easily replace Φ by a true differential Ω of K. The formula we are looking for will then result from a comparison of the divisors of Ω and ω.

To define Ω 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 Φ is any k_0-linear map of X into k_0, there exists a uniquely determined K_0-linear map Ω of X into K_0 such that $\Phi = S_0\Omega$; i.e. $\Phi(\mathfrak{X}) = S_0(\Omega(\mathfrak{X}))$ for all $\mathfrak{X} \in X$.*

PROOF. If such a map Ω did exist, we would have, for each $\mathfrak{X} \in X$,

$$S_0(\xi\Omega(\mathfrak{X})) = S_0(\Omega(\xi\mathfrak{X})) = \Phi(\xi\mathfrak{X}) \tag{8}$$

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

$$S_0(\xi\Omega(\alpha\mathfrak{X} + \beta\mathfrak{Y})) = S_0(\xi(\alpha\Omega(\mathfrak{X}) + \beta\Omega(\mathfrak{Y})))$$

for all $\xi \in K_0$, for any $\alpha, \beta \in K_0$, and any $\mathfrak{X}, \mathfrak{Y} \in X$. 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 Ω to be the K_0-linear map of the space of repartitions of K into K_0 for which

$$S_0(\Omega(\mathfrak{X})) = \Phi(\mathfrak{X}) = \omega(S_\alpha(\mathfrak{X})). \tag{9}$$

Then Ω is a nontrivial differential of K which we can use as a substitute for the cotrace of ω from k to K. The corresponding substitute for the different of K over k is the divisor $\mathfrak{D}_\alpha$ of K such that

$$(\Omega) = (\mathrm{Con}_{k/K}\,(\omega))\mathfrak{D}_\alpha \tag{10}$$

where (Ω) and (ω) are the divisors of Ω and ω in k and K.

The computation of $\mathfrak{D}_\alpha$ 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 $K^p \subset k$, 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 $(K_\mathfrak{P}/k_\mathfrak{p}) = p$ since the global degree p is the sum of the local degrees above each $\mathfrak{p}$ of k. Viewing our generator α 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_α is

$$(S_\alpha(\mathfrak{X}))_\mathfrak{p} = S_\alpha^\mathfrak{P}\,(\mathfrak{X}_\mathfrak{P}) \tag{11}$$

for all repartitions $\mathfrak{X} = (\mathfrak{X}_\mathfrak{P})$ of K. It follows, just as in the case of the ordinary different, that $\nu_\mathfrak{P}(\mathfrak{D}_\alpha)$ *is the greatest rational integer such that*:

$\xi \in K_{\mathfrak{P}}$, $\nu_{\mathfrak{P}}(\xi) \geqq -\nu_{\mathfrak{P}}(\mathfrak{D}_\alpha)$ *implies* $\nu_{\mathfrak{p}}(S_\alpha^{\mathfrak{P}}(\xi)) \geqq 0$, where ν is the ordinal number function.

If e and f are the ramification index and residue class field degree of $\mathfrak{P}$ over $\mathfrak{p}$, then $ef = (K_{\mathfrak{P}}/k_{\mathfrak{p}}) = p$. 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 $K_{\mathfrak{P}}$ has an integral basis (minimal basis) over the ring of integers $\mathfrak{o}$ of $k_{\mathfrak{p}}$ consisting of the powers of one element $\tau \in K_{\mathfrak{P}}$:

$$\mathfrak{O} = \mathfrak{o} + \mathfrak{o}\tau + \cdots + \mathfrak{o}\tau^{p-1}.$$

For example, in the first case we can take τ to be any unit in $K_{\mathfrak{P}}$, the residue class of which generates the residue class field extension; in the second case we can take τ to be any local uniformizing parameter in $K_{\mathfrak{P}}$. Let τ be any such element of $K_{\mathfrak{P}}$, and let D_τ be the derivation with respect to τ in the p-extension $K_{\mathfrak{P}}/k_{\mathfrak{p}}$.

LEMMA 3. $\nu_{\mathfrak{P}}(\mathfrak{D}_\alpha) = \nu_{\mathfrak{P}}((D_\tau\alpha)^{1-p})$.

PROOF. By formula (3) and Theorem 1 we have for $\xi \in K_{\mathfrak{P}}$:

$$\xi(D_\tau\alpha)^{1-p} = \sum_{\nu=0}^{p-1} S_\tau(\xi(D_\tau\alpha)^{1-p}\tau^{p-1-\nu})\tau^\nu = \sum_{\nu=0}^{p-1} S_\alpha^{\mathfrak{P}}(\xi\tau^{p-1-\nu})\tau^\nu.$$

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

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

$$2G - 2 = p^{1-n}(2g - 2) + (1 - p)\sum_{\mathfrak{P}} \nu_{\mathfrak{P}}(D_{\tau_{\mathfrak{P}}}\alpha) \deg \mathfrak{P}$$

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

PROOF. The term on the left equals deg (Ω). The first term on the right equals deg $(\mathrm{Con}_{k/K}(\omega))$. 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

$$2G-2\equiv 2g-2 \pmod{(p-1)}.$$

REMARK. A simple example of the situation we are discussing is the case where $k=k_0(x, y)$ 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 $\geqq 0$.

REMARK. Fact (b) above follows at once from Theorem 2 because in the case of a constant field extension we have $n\geqq 1$ and can take $\alpha\in K_0$, so that $\nu_{\mathfrak{P}}(D_{\tau_{\mathfrak{P}}}\alpha)\geqq 0$ for all $\mathfrak{P}$.

It is perhaps of some interest to see how the numbers $\nu_{\mathfrak{P}}(D_{\tau_{\mathfrak{P}}}\alpha)\deg\mathfrak{P}$ in the formula of Theorem 2 may be computed in the ground field k in terms of the element $a=\alpha^p\in k$, the pth 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*

$$r_{\mathfrak{p}}=\operatorname*{Max}_{x\in k_{\mathfrak{p}}}\{\nu_{\mathfrak{p}}(a-x^p)\}.$$

Then

$$p^n\nu_{\mathfrak{P}}(D_{\tau_{\mathfrak{P}}}\alpha)\deg\mathfrak{P} = \begin{cases} r_{\mathfrak{p}}\deg\mathfrak{p}, & \text{if } p\mid r_{\mathfrak{p}},\\ (r_{\mathfrak{p}}-1)\deg\mathfrak{p}, & \text{if } p\nmid r_{\mathfrak{p}}.\end{cases}$$

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 pth power in $k_{\mathfrak{p}}$. Therefore $r_{\mathfrak{p}}<\infty$. Let b be an element of $k_{\mathfrak{p}}$ such that $r_{\mathfrak{p}}=\nu_{\mathfrak{p}}(a-b^p)$.

Case 1. If $p\mid r_{\mathfrak{p}}$, let $r_{\mathfrak{p}}=sp$. Let t be a local uniformizing parameter in $k_\mathfrak{p}$, and put $\tau=(\alpha-b)t^{-s}\in K_\mathfrak{P}$. Then $\tau^p=(a-b^p)t^{-sp}$ is a unit in $k_\mathfrak{p}$. The residue class of this unit is not a pth power of a residue class in $k_\mathfrak{p}$. Otherwise, if $c\in k_\mathfrak{p}$, such that $c^p\equiv(a-b^p)t^{-sp}$ (mod $\mathfrak{p}$), then the pth 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 τ are an integral basis for $\mathfrak{O}$ over $\mathfrak{o}$. $D_\tau\alpha=(D_\alpha\tau)^{-1}=t^s$ shows that $\nu_\mathfrak{P}(D_\tau\alpha)=s$ and therefore $\nu_\mathfrak{P}(D_\tau\alpha)p^n \deg \mathfrak{P}=sp \deg \mathfrak{p}=r_\mathfrak{p} \deg \mathfrak{p}$.

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

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