TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 227, 1977

THE FUNDAMENTAL FORM OF AN INSEPARABLE EXTENSION

BY

MURRAY GERSTENHABER[1]

ABSTRACT. If K is a finite purely inseparable extension of a field k, then the symmetric multiderivations of K (symmetric maps f: $K \times \cdots \times K$ (n times) $\to K$ which are derivations as functions of each single variable) form a ring under the symmetrized cup product. This ring contains an element $\Gamma(K/k)$ called the fundamental form of K over k, which is defined up to multiplication by a nonzero element of K and has the property that if B is any intermediate field between K and k, then $\Gamma(K/B)$ divides $\Gamma(K/k)$.

To every finite purely inseparable extension K of a field k of characteristic $p > 0$, there is assoicated in a natural way a "fundamental form", $\Gamma(K/k)$, which is a certain symmetric cochain, expressible as a sum of cup products of derivations, of K with coefficients in itself. This form is an element of a commutative k-algebra with divided powers (in which, therefore, the ordinary pth power of every element vanishes). The purpose of this paper is to prove the foregoing (announced in [5]) together with the following "Main Theorem" originally conjectured by Shatz: If B is an intermediate field, then $\Gamma(K/B)$ divides $\Gamma(K/k)$.

Our goal, toward which this paper hopefully is a first step, is to develop a Galois theory for inseparable extensions K/k which, instead of finding directly all intermediate fields (of which there are generally infinitely many), first finds the algebraic families of these fields, and then examines these families by means of the algebraic deformation theory. It is easy to see that the intermediate fields of any finite extension K/k form an algebraic set (cf. Richardson [12]) which has, then, only finitely many components. Since separable extensions are rigid (cf. [2]), each component in the separable case is reduced to a single element, giving another proof (using powerful tools) of the finiteness of the number of intermediate fields in a finite separable extension. Any effective Galois theory for inseparable extensions will probably

Received by the editors September 26, 1975.

AMS (MOS) subject classifications (1970). Primary 12F15; Secondary 12F10.

Key words and phrases. Inseparable field extensions, high order derivations, Galois theory.

(1) The author gratefully acknowledges the support of the N.S.F. through a grant to the University of Pennsylvania.

have to preserve some analog of this finiteness.

In a finite purely inseparable extension K/k we conjecture that the algebraic set of intermediate fields of a given dimension actually has but a single component which, however, has additional structure (including the marking of certain cycles) induced by the pth power map of K into itself. Some examples at the end of the paper show that this structure is reflected in the fundamental form, $\Gamma(K/k)$, and perhaps could even be determined from it, if we knew how. Unfortunately, all we can show so far is that the structure of the fundamental form is linked to that of the family of intermediate fields by the Main Theorem.

This paper is relatively self-contained and uses no tools from the deformation theory, but it does draw heavily on ideas of Nakai [8] and Nakai, Kosaki, and Ishibashi [9] who first obtained, by other methods, certain basic results; in particular, parts (i) and (iii) of Theorem 2.1, and part (i) of Theorem 4.5. We acknowledge our indebtedness and refer the reader to those papers both for an approach which may be essential in more general contexts and for a particular inseparable Galois theory which is of interest in itself. The method used here derives from the unpublished thesis of Keith [7]. In §4 we briefly recapitulate, for completeness, certain basic work of Pickert [10] and Rasala [11] on the structure of inseparable extensions which seems not to be as well known as it should be.

1. **The Nakai operator and higher order derivations.** Let A be a commutative algebra over a ring k and $C^n = C^n(A,A)$ be the module of n-cochains of A with coefficients in itself, i.e., of multilinear maps (over k) $f: A \times \cdots \times A$ (n times) $\to A$. We define the *Nakai operator* $\Delta^{(n)}: C^n \to C^{n+1}$ by considering such an f as a function of the first variable alone and applying the Hochschild coboundary operator δ. That is,

$$\begin{aligned}\Delta f(a_1,\ldots,a_{n+1}) &= a_1 f(a_2,\ldots,a_{n+1}) - f(a_1a_2,a_3,\ldots,a_{n+1}) \\ &\quad + a_2 f(a_1,a_3,\ldots,a_{n+1}).\end{aligned} \tag{1.1}$$

When there can be no confusion we write Δ for $\Delta^{(n)}$.

Set $Y^1 = C^1 = \mathrm{End}_k A$, and for every $n > 1$ let Y^n be the submodule of C^n consisting of all f which are symmetric and which, when considered as a function of any two variables, is a two-cocycle.

LEMMA 1.1. *For every n, $\Delta Y^n \subset Y^{n+1}$.*

PROOF. From (1.1), $f \in Y^n$ implies that $\Delta f(a_1,a_2,\ldots,a_{n+1})$ is symmetric in a_1 and a_2, and also in a_i and a_j for all $i,j \geqslant 3$, so to prove symmetry we need only show that interchange of a_2 and a_3 leaves f unchanged. Since f is a 2-

cocycle as a function of its first two variables, we have, writing a_I for $(a_4, \ldots, a_{n+1})$,

$$a_1 f(a_2, a_3, a_I) - f(a_1 a_2, a_3, a_I) + f(a_1, a_2 a_3, a_I) - a_3 f(a_1, a_2, a_I) = 0.$$

From this we may solve for $f(a_1 a_2, a_3, a_I)$. Substituting in (1.1) then gives

$$\Delta f(a_1, a_2, a_3, a_I) = a_2 f(a_1, a_3, a_I) - f(a_1, a_2 a_3, a_I) + a_3 f(a_1, a_2, a_I),$$

which is clearly symmetric in a_2 and a_3. The cocycle condition is evident since Δ is the cohomology operator considered as a function of one variable. □

When A is unital we denote by Y_0^n the submodule of Y^n consisting of all f which vanish when any variable is set equal to 1; we also write $(\mathrm{End}_k A)_0$ for Y_0^1. It is then trivial that $\Delta Y_0^n \subset Y_0^{n+1}$. One can check (but we do not need) that for odd n, the restriction of Δ to Y^n coincides with the Hochschild coboundary δ, but not for even n, and generally $\Delta^2 \neq 0$. An element $f \in Y^1 = \mathrm{End}_k A$ with $\Delta^n f = 0$ will be called an *n-derivation* or *high order derivation*; the least n such that $\Delta^n f = 0$ is the *order* of f, denoted $\gamma(f)$. Since $\Delta^n f(1, 1, \ldots, 1) = f(1)$ it follows that $\Delta^n f = 0$ implies $f \in (\mathrm{End}_k A)_0$ whenever A is unital. Denoting the set of n-derivations by $\mathfrak{D}'^n$ we have $\mathfrak{D}'^1 \subset \mathfrak{D}'^2 \subset \cdots$. The union of these submodules of $(\mathrm{End}_k A)_0$ will be denoted by $\mathfrak{D}'$. Setting $\mathfrak{D}'^0 = \{0\}$, and letting $\mathfrak{D}^0$ consist of multiples of the identity morphism, id_A, we set $\mathfrak{D}^n = \mathfrak{D}'^n + \mathfrak{D}^0$ for all $n \geqslant 0$ and set $\mathfrak{D} = \cup \mathfrak{D}^i$. Every $f \in \mathfrak{D}^n$ can be written in the form $f = f' + f(1) \cdot \mathrm{id}_A$ with $f' \in \mathfrak{D}'^n$ (and hence $f'(1) = 0$), and we extend γ to all of $\mathfrak{D}$ by setting $\gamma(f) = \gamma(f')$.

We adopt the following notation: If $a_1, \ldots, a_n \in A$ and $I = \{i_1, \ldots, i_m\}$ is a subset of $\{1, \ldots, m\}$, then a_I denotes $(a_{i_1}, \ldots, a_{i_m})$, $|a_I|$ denotes the product $a_{i_1} a_{i_2} \cdots a_{i_m}$ (or 1, if I is empty), and $\sharp I$ denotes the cardinality of I, namely m. The complement of I is denoted cI. One readily proves

THEOREM 1.2. *If* $f \in \mathrm{End}_k A$ *then*

$$\Delta^n f(a_1, \ldots, a_{n+1}) = -\sum{}' (-1)^{\sharp I} |a_{cI}| f(|a_I|) \tag{1.2}$$

where $\sum'$ *denotes the sum over all nonempty subset* I *of* $\{1, \ldots, n+1\}$. □

Nakai [8] defines an n-derivation to be one such that the right side of (1.2) vanishes. The theorem shows that this is equivalent to our definition. Note that if $\gamma(f) = \gamma$ then trivially $\Delta(\Delta^{\gamma-1} f) = \Delta^\gamma f = 0$, but this says that $\Delta^{\gamma-1} f$ is a derivation as a function of each single variable; we say that $\Delta^{\gamma-1} f$ is a

"symmetric multiderivation". Nakai [8] and Nakai, Kosaki and Ishibashi [9] have shown that if $f \in \mathfrak{D}'^i$ and $g \in \mathfrak{D}'^j$ then the composite $fg \in \mathfrak{D}'^{i+j}$. Hence $\mathfrak{D}'$ and also $\mathfrak{D}$ are rings with ascending filtrations. This is a special consequence of our "Leibniz rule" of the next section.

Here is one of the most important sources of high order derivations: An "*approximate automorphism*" of order n of a k-algebra A (which for the moment need not be commutative) is a formal polynomial $\Phi_t = \mathrm{id}_A + t\varphi_1 + t^2\varphi_2 + \cdots + t^n\varphi_n$ with $\varphi_i \in \mathrm{End}_k A$, all i, and

$$\Phi_t(ab) \equiv \Phi_t a \cdot \Phi_t b \mod t^{n+1} \tag{1.3}$$

for all $a, b \in A$. That is, Φ_t is an automorphism of $A[t]/t^{n+1}$ whose constant term is the identity map of A. The cup product of $f, g \in C^1 = \mathrm{End}_k A$ is the element $f \cup g$ of C^2 defined by $(f \cup g)(a, b) = f(a) \cdot g(b)$. More generally, if $f \in C^m$, $g \in C^n$ then $f \cup g \in C^{m+n}$ is defined by

$$(f \cup g)(a_I, b_J) = f(a_I) \cdot g(b_J)$$

where a_I is an arbitrary m-tuple and b_J an arbitrary n-tuple of elements of A. Then (1.3) is equivalent to

$$\delta\varphi_1 = 0 \tag{1.4$_1$}$$

(i.e., φ_1 is a derivation of A into itself) and

$$\delta\varphi_i = -[\varphi_1 \cup \varphi_{i-1} + \varphi_2 \cup \varphi_{i-2} + \cdots + \varphi_{i-1} \cup \varphi_1] \tag{1.4$_i$}$$

for $i = 2, \ldots, n$ (cf. [2]). A sequence $\varphi_1, \ldots, \varphi_n \in \mathrm{End}_k A$ with either of the equivalent properties (1.3) or (1.4) is called by Jacobson a "higher derivation", cf. [6]; we avoid this usage here because of confusion with "high order derivation". (Since Δ coincides with δ in dimension 1, one can also give an inductive definition of n-derivations meaningful for noncommutative algebras A; cf. [5].)

Suppose that A is a commutative k-algebra and that there exists an n such that $\mathfrak{D}^n = \mathfrak{D}^{n+1} = \cdots = \mathfrak{D}$. We then say that A has bounded order and will denote the least such n by $\gamma(A/k)$ or $\gamma(A)$, calling it the *order of* A (over k). In that case, the A-module $\Delta^{\gamma-1}\mathfrak{D}'$ will be called the module of forms of A. If by good fortune it is a free module of rank 1 then any generator will be called "the" *fundamental form* of A denoted $\Gamma(A/k)$, or $\Gamma(A)$, and we shall say of A that it has such a form. This will be the case for every finite purely inseparable extension of a field k. Note that if A has bounded order γ, then A has a fundamental form if and only if $\mathfrak{D}^\gamma(A)/\mathfrak{D}^{\gamma-1}(A)$ is a free A-module of rank 1. For $\Gamma(A)$, if it exists, is always of the form $\Delta^{\gamma-1}f$ for some $f \in \mathrm{End}_k A$ with $\gamma(f) = \gamma(A)$. If k is a field than we can choose any such f.

2. **Leibniz rule.** If we have symmetric cochains $f \in C^m = C^m(A,A)$ and $g \in C^n$, then we define symmetric cochains $f * g \in C^{m+n}$ and $f \circledast g \in C^{m+n-1}$ so: Let $a_I = (a_1, \ldots, a_{m+n})$. Then

$$f * g(a_I) = \sum_J f(a_J)g(a_{cJ})$$

where J runs over all m element subsets of $\{1, \ldots, m+n\}$. This multiplication is associative. Now let $a_I = (a_1, \ldots, a_{m+n-1})$, and set

$$f \circledast g(a_I) = \sum_J f(g(a_{cJ}), a_J)$$

where J runs over all $m-1$ element subsets of $\{1, \ldots, m+n-1\}$. If A is commutative, which we now assume, then $f * g = g * f$. If $f, g \in C^1 = \mathrm{End}_k A$, then $f \circledast g = fg$, the usual composite.

THEOREM 2.1 (LEIBNIZ' RULE). *If $f, g \in \mathrm{End}_k A$, then*

$$(\mathrm{L_n}) \qquad \begin{aligned} \Delta^n(fg) = {} & \Delta^n f \circledast g + \Delta^{n-1} f \circledast \Delta g + \Delta^{n-2} f \circledast \Delta^2 g + \cdots + f \circledast \Delta^n g \\ & - [\Delta^{n-1} f * g + \Delta^{n-2} f * \Delta g + \cdots + f * \Delta^{n-1} g]. \end{aligned}$$

PROOF. By induction on n. For $n = 1$ we must show that

$$\Delta(fg)(a_1, a_2) = (\Delta f \circledast g)(a_1, a_2) + (f \circledast \Delta g)(a_1, a_2) - (f * g)(a_1, a_2).$$

The left side is

$$a_1 f(g(a_2)) - f(g(a_1 a_2)) + a_2 f(g(a_1)).$$

Using the commutativity and introducing terms that cancel we can rewrite this so:

$$\begin{aligned} & [a_1 f(g(a_2)) - f(a_1 g(a_2)) + f(a_1)g(a_2)] \\ & \quad + [f(a_1 g(a_2)) - f(g(a_1 a_2)) + f(a_2 g(a_1))] \\ & \quad + [a_2 f(g(a_1)) - f(a_2 g(a_1)) + f(a_2)g(a_1)] - [f(a_1)g(a_2) + f(a_2)g(a_1)]. \end{aligned}$$

The third bracketed expression (when read backwards) is $\Delta f(g(a_1), a_2)$, the first (similarly reversed) is $\Delta f(g(a_2), a_1)$, and the second is $f(\Delta g(a_1, a_2))$. Now

$$\Delta f(g(a_1), a_2) + \Delta f(g(a_2), a_1) = (\Delta f \circledast g)(a_1, a_2)$$

and $f(\Delta g(a_1, a_2))$ is identical with $(f \circledast \Delta g)(a_1, a_2)$. Finally, the fourth bracketed expression is just $(f * g)(a_1, a_2)$, so the asserted formula holds for $n = 1$.

Suppose now that it holds for some $n \geqslant 1$. To prove it for $n+1$, we apply Δ to the right side of equation (L_n) and show that, after a rewriting analogous

to that in the case $n = 1$, the terms that appear are precisely those that appear on the right side of equation (L_{n+1}). To this end, suppose that φ is a symmetric l-cochain and ψ a symmetric m-cochain. We separate $\Delta(\varphi \circledast \psi)(a_1, \ldots, a_{l+m})$ into a sum of two sets of terms, those where either a_1, a_2, or $a_1 a_2$ appear as variables inside ψ, and those where they do not. In the sums that follow, I denotes an $(l-1)$-element subset of $\{3, \ldots, l\}$ and I' is its complement in $\{3, \ldots, l\}$ while J denotes an l-element subset and J' is its complement. Then we have

$$\begin{aligned}\Delta(\varphi * \psi)(a_1, \ldots, a_{l+m}) &= \sum_I [a_1 \varphi(\psi(a_2, a_I), a_{I'}) - \varphi(\psi(a_1 a_2, a_I), a_{I'}) + a_2 \varphi(\psi(a_1, a_I), a_{I'})] \\ &\quad + \sum_J [a_1 \varphi(\psi(a_J), a_2, a_{J'}) - \varphi(\psi(a_J), a_1 a_2, a_{J'}) + a_2 \varphi(\psi(a_J), a_1, a_{J'})].\end{aligned}$$

The first sum equals, as one can readily check (cf. the case for $n = 1$),

$$\begin{aligned}&\sum_I [\Delta\varphi(\psi(a_1, a_I), a_2, a_{I'}) + \Delta\varphi(\psi(a_2, a_I), a_1, a_{I'}) \\ &\quad + \varphi(\Delta\psi(a_1, a_2, a_I), a_{I'}) - \varphi(a_1, a_{I'})\psi(a_2, a_I) - \varphi(a_2, a_{I'})\psi(a_1, a_I)].\end{aligned} \tag{2.1}$$

The second sum is simply

$$\sum_J \Delta\varphi(\psi(a_J), a_1, a_2, a_{J'}). \tag{2.2}$$

Now let $\varphi = \Delta^i f$, $\psi = \Delta^j g$ where $i + j = n$. The first two terms in (2.1) together with (2.2) are then all terms of $(\Delta^{i+1} f \circledast \Delta^j g)(a_1, \ldots, a_{n+1})$ except those where a_1 and a_2 both appear as variables inside $\Delta^j g$. Looking at the third term of (2.1), which consists of all terms of $(\Delta^i f \circledast \Delta^{j+1} g)(a_1, \ldots, a_{n+2})$ in which both a_1 and a_2 appear as variables in $\Delta^{j+1} g$, shows that the missing terms of $(\Delta^{i+1} f \circledast \Delta^j g)(a_1, \ldots, a_{n+2})$ will come from the corresponding expression in $\Delta(\Delta^{i+1} f \circledast \Delta^{j-1} g)(a_1, \ldots, a_{n+2})$. The negative terms in (2.1) are the negatives of all terms in $(\Delta^i f * \Delta^j g)(a_1, \ldots, a_{n+1})$ in which a_1 and a_2 do not appear simultaneously as variables of $\Delta^i f$ or as variables of $\Delta^i g$. But now observe that $\Delta(\Delta^i f * \Delta^j g)(a_1, \ldots, a_{n+2})$ consists precisely of those terms of $(\Delta^{i+1} f * \Delta^j g)(a_1, \ldots, a_{n+2})$ in which a_1 and a_2 both appear as variables in $\Delta^{i+1} f$ together with those terms of $\Delta^i f * \Delta^{j+1} g$ in which a_1 and a_2 both appear as variables in $\Delta^{j+1} g$. The missing terms of $\Delta^i f * \Delta^j g$ therefore appear in the expansion of $\Delta(\Delta^{i-1} f * \Delta^j g + \Delta^i f * \Delta^{j-1} g)$. This verifies that every term on the right of (L_{n+1}) appear precisely once in (a suitably rewritten form of) Δ applied to the right side of (L_n), completing the induction. □

COROLLARY. *If* $f, g \in \mathfrak{D}'$ *and* $\gamma(f) = m$, $\gamma(g) = n$, *then*
(i) $fg \in \mathfrak{D}'$ *and* $\gamma(fg) \leqslant m + n$.

(ii) $\Delta^{m+n-1}(fg) = -\Delta^{m-1}f * \Delta^{n-1}g = \Delta^{m+n-1}(gf)$.
(iii) *Setting* $[f,g] = fg - gf$, *we have* $\gamma([f,g]) \leqslant m + n - 1$.

PROOF. Assertion (i) and the first equality in (ii) are evident from Leibniz' rule. The second equality in (ii) follows from the commutativity of the operation $*$, which in turn implies (iii). □

Assertion (i) shows in particular that if A is a commutative algebra over a ring k, then $\mathfrak{D}'^m \cdot \mathfrak{D}'^n \subset \mathfrak{D}'^{m+n}$ and hence also $\mathfrak{D}^m \cdot \mathfrak{D}^n \subset \mathfrak{D}^{m+n}$. Thus both $\mathfrak{D}'$ and $\mathfrak{D}$ are rings with natural ascending filtrations. Assertion (ii) shows that the associated graded ring to this filtration is commutative. It also shows that if we make $\mathfrak{D}'$ into a ring using the Lie or commutator multiplication then it is natural to reduce the degree by 1 letting the derivations have degree 0, and so forth. With this we again have a ring with increasing filtration in which the subring of elements of (reduced) degree 0 is just the usual Lie ring of derivations of A.

3. **High order derivations of tensor products.** If A and B are commutative k-algebras, and f is in $\mathfrak{D}(A)$, g in $\mathfrak{D}(B)$, then $f \otimes g \in \mathrm{End}_k(A \otimes_k B)$ is the composite of $f \otimes 1_B$ and $1_A \otimes g$; since the latter are in $\mathfrak{D}(A \otimes B)$ so is $f \otimes g$ and clearly $\gamma(f \otimes g) \leqslant \gamma(f) + \gamma(g)$. The inequality may be strict since in particular we may have $A \otimes B = 0$. It is easy to check that for every $l \geqslant 0$ we have

$$\Delta^{l-1}(f \otimes g)(a_1 \otimes b_1, \ldots, a_l \otimes b_l) = -\sum{}' (-1)^{\sharp I} |a_{cI}| f(|a_I|) |b_{cI}| g(|b_I|) \tag{3.1}$$

where the sum $\sum'$ runs over all nonempty subsets of $\{1, \ldots, l\}$. Now suppose that A and B are both unital, write $l = m + n$, and suppose that the argument of $\Delta^{m+n-1}(f \otimes g)$ is of the form $(a_1 \otimes 1, \ldots, a_m \otimes 1, 1 \otimes b_1, \ldots, 1 \otimes b_n)$, which we write for simplicity as $(a_{(m)} \otimes 1, 1 \otimes b_{(n)})$. Suppose moreover that $f(1) = g(1) = 0$. Then it follows from (3.1) that

$$\begin{aligned} &\Delta^{m+n-1} f \otimes g(a_{(m)} \otimes 1, 1 \otimes b_{(n)}) \\ &\quad = -\sum_{I', I''} (-1)^{\sharp I' + \sharp I''} |a_{cI'}| f(|a_{I'}|) \otimes |b_{cI''}| g(|b_{I''}|) \\ &\quad = -[\Delta^{m-1} f(a_{(m)}) \otimes \Delta^{n-1} g(a_{(n)})], \end{aligned} \tag{3.2}$$

where in the foregoing, I' runs through the nonempty subsets of $\{1, \ldots, m\}$ and I'' independently runs through the nonempty subsets of $\{2, \ldots, n\}$.

If k is a field, then the bracketed expression in (3.2) cannot vanish unless one of its tensor factors does. Combining this with the foregoing, one has

LEMMA 3.1. *If A, B are commutative k-algebras, then*

$$\mathfrak{D}(A) \otimes \mathfrak{D}(B) \subset \mathfrak{D}(A \otimes B).$$

Moreover, if $f \in \mathfrak{D}(A)$, $g \in \mathfrak{D}(B)$, *then* $\gamma(f \otimes g) \leqslant \gamma(f) + \gamma(g)$, *equality holding when* k *is a field.* □

There is a partial converse:

THEOREM 3.2. *Let* k *be a field,* A, B *be commutative* k*-algebras. Let* $f_1, \ldots, f_m \in \mathrm{End}_k A$ *be linearly independent over* k, *similarly for* $g_1, \ldots, g_m \in \mathrm{End}_k B$, *and suppose that* $h = f_1 \otimes g_1 + \cdots + f_m \otimes g_m$ *lies in* $\mathfrak{D}(A \otimes B)$. *Then* $f_1, \ldots, f_m \in \mathfrak{D}(A)$ *and* $g_1, \ldots, g_m \in \mathfrak{D}(B)$.

PROOF. Write $f = f' + f(1)\,\mathrm{id}_A$, and similarly for g and h. Then

$$h' = \sum_{j=1}^{m} [f'_j \otimes g'_j + f_j(1)1_A \otimes g'_j + f'_j \otimes g_j(1)1_B] \tag{3.3}$$

and $\Delta^{n-1}h' = 0$ for some n. Therefore, in particular $\Delta^{n-1}h'(a_1 \otimes 1, \ldots, a_n \otimes 1) = 0$, so

$$\sum [\Delta^{n-1}f'_j(a_1, \ldots, a_n)] \otimes g_j(1) = 0. \tag{3.4}$$

As this is so for all $a_1, \ldots, a_n \in A$, we have

$$\sum \Delta^{n-1}f'_j \otimes g_j(1)1_B = 0.$$

We also have $\Delta^n h'(a_1 \otimes 1, \ldots, a_n \otimes 1, 1 \otimes b) = 0$. Now $\Delta^n[f'_j \otimes g_j(1)1_B] \cdot (a_1 \otimes 1, \ldots, a_n \otimes 1, 1 \otimes b) = \Delta^n f'_j(a_1, \ldots, a_n, 1) \otimes bg_j(1)1_B = 0$ because 1 appears as an argument in the left tensor factor. Similarly,

$$\Delta^n[f_j(1)1_A \otimes g'_j](a_1 \otimes 1, \ldots, a_n \otimes 1, 1 \otimes b)|a_I| \cdot f_j(1) \otimes \Delta^n g'_j(1, \ldots, 1, b)$$

$$= 0 \qquad (\text{where } I = \{1, \ldots, n\}).$$

It follows, using (3.2) and (3.3), that

$$\Delta^n h'(a_1 \otimes 1, \ldots, a_n \otimes 1, 1 \otimes b) = -\sum \Delta^{n-1}f'_j(a_1, \ldots, a_n) \otimes g'_j(b) = 0.$$

Multiplying (3.4) by $1 \otimes b$ and combining with this shows that

$$-\sum \Delta^{n-1}f'_j(a_1, \ldots, a_n) \otimes g_j(b) = 0.$$

As this is so for all b, and as the g_j are assumed to be linearly independent, it follows that $\Delta^{n-1}f'_j(a_1, \ldots, a_n) = 0$ for all j and all $a_1, \ldots, a_n \in A$, so $\Delta^{n-1}f'_j = 0$. Thus $f_1, \ldots, f_n \in \mathfrak{D}^{n-1}(A) \subset \mathfrak{D}(A)$, as asserted, and similarly for $g_1, \ldots, g_m$. □

If B is finite dimensional over the field k, then every endomorphism of $A \otimes_k B$ can be written in the form $f_1 \otimes g_1 + \cdots + f_m \otimes g_m$ for suitable linearly independent $f_1, \ldots, f_m \in \mathrm{End}_k A$, $g_1, \ldots, g_m \in \mathrm{End}_k B$. In view of the foregoing, we have

THEOREM 3.3. *Let k be a field, and A, B be commutative k-algebras with B finite dimensional over k. Then the natural isomorphism* $(\mathrm{End}_k A) \otimes (\mathrm{End}_k B) \xrightarrow{\sim} \mathrm{End}_k(A \otimes B)$ *induces an isomorphism*

$$\mathfrak{D}(A) \otimes \mathfrak{D}(B) \xrightarrow{\sim} \mathfrak{D}(A \otimes B).$$

This is an isomorphism of filtered rings, i.e., $\mathfrak{D}^n(A \otimes B)$ is the image of (and can be identified with) $\sum_{i+j=n} \mathfrak{D}^i(A) \otimes \mathfrak{D}^j(B)$. □

Keeping the foregoing hypotheses on A, B and k, we have the following.

COROLLARY. (i) *If A and B have bounded orders, then so does $A \otimes_k B$ and*

$$\gamma(A \otimes_k B) = \gamma(A) + \gamma(B).$$

(ii) *If A and B have fundamental forms, then so does $A \otimes_k B$ and* $\Gamma(A \otimes_k B) = (\Gamma(A) \otimes \mathrm{id}_B) * (\mathrm{id}_A \otimes \Gamma(B))$; *identifying* $\mathrm{End}_k A$ *with its image in* $\mathrm{End}_k A \otimes B$ *and similarly for* $\mathrm{End}_k B$, *we can write* $\Gamma(A \otimes B) = \Gamma(A) * \Gamma(B)$.

PROOF. Assertion (i) is immediate from the theorem which also shows that there is an element of highest order in $\mathrm{End}\, A \otimes B$ of the form $f \otimes g$ with $\gamma(f) = \gamma(A)$, $\gamma(g) = \gamma(B)$. Denoting these orders by m and n, respectively, writing $f \otimes g$ as $(f \otimes \mathrm{id}_B)(\mathrm{id}_A \otimes g)$ and applying Leibniz' rule to $\Delta^{m+n-1}(f \otimes g)$ gives (ii). □

4. High order derivations of an inseparable extension and the fundamental form. We recall some basic facts about finite purely inseparable extensions from the work of Pickert [10], Rasala [11]. A truncated polynomial algebra A over a commutative ring k is a quotient $k[x_1, \ldots, x_n]/(x_1^{n_1}, \ldots, x_n^{n_r})$ of the polynomial ring $k[x_1, \ldots, x_r]$ by an ideal generated by various powers $x_1^{n_1}, \ldots, x_r^{n_r}$ of the variables. (Tacitly $n_i \geqslant 2$ for all i.) Both r and the exponents $n_1, \ldots, n_r$ are independent of the representation of A as such a quotient. For if k is a field, set $N = \mathrm{rad}\, A$, and observe that numbers $\dim_k N^j/N^{j+1}$, $j = 1, 2, \ldots$, from which the n_i can be recovered, depend only on A. In fact $\dim_k N^j/N^{j+1}$ is just the number of ways of writing j in the form $j_1 + \cdots + j_r$ with $0 \leqslant j_i \leqslant n_i - 1$, $i = 1, \ldots, r$. That is, it is the coefficient of t^j in $F(t) = \prod_{i=1}^{s} (1 - t^{n_i})/(1 - t)$, and from this the n_i can be computed. If k is not a field, then consider $A/\underline{m}A$ where $\underline{m}$ is any maximal ideal of A.

Now let K be a finite purely inseparable extension of a field k of characteristic $p > 0$. The exponent, denoted $e(\alpha)$, of an element $\alpha \in K$ is the

least integer e such that $\alpha^{p^e} \in k$; the maximum of all $e(\alpha)$ is called the exponent of K. (Rasala calls this the "height" of K.) A *Pickert generating sequence* $\alpha_1, \ldots, \alpha_r$ of K over k is a p-basis which has been so ordered that for every $i = 1, \ldots, r$ the exponent of α_i over $K_{i-1} = k(\alpha_1, \ldots, \alpha_{i-1})$ is identical with the exponent of K over K_{i-1}. Denoting this exponent by e_i, one has $e_1 \geqslant e_2 \geqslant \cdots \geqslant e_r > 0$. We shall call these the *Pickert exponents* of K (over k). They in fact depend only on K and not on the choice of p-basis, as we see next. First, setting $q_i = p^{e_i}$, we claim that

$$\alpha_i^{q_i} \in k(\alpha_1^{q_i}, \ldots, \alpha_{i-1}^{q_i}), \qquad i = 1, \ldots, r. \tag{4.1}$$

The proof is by induction on the number of generators, r, of K over k. Since this is less than r if we view K as an extension of $k(\alpha_1)$ we may assume that $\alpha_i^{q_i} \in k(\alpha_1, \alpha_2^{q_i}, \ldots, \alpha_{i-1}^{q_i})$. Let s be the highest power of p such that $\alpha_i^{q_i} \in k(\alpha_1^s, \alpha_2^{q_i}, \ldots, \alpha_{i-1}^{q_i})$ which field we denote by L. Since the degree of L over $L' = k(\alpha_1^{ps}, \alpha_2^{q_i}, \ldots, \alpha_{i-1}^{q_i})$ is not more than p, and in fact is precisely p since $\alpha_i^{q_i} \notin L'$ it therefore follows that $L'(\alpha_i^{q_i}) = L$, so $\alpha_1^s \in L'(\alpha_i^{q_i}) = k(\alpha_1^{ps}, \alpha_2^{q_i}, \ldots, \alpha_{i-1}^{q_i}, \alpha_i^{q_i}) = L''$. If $s < q_i$ then $ps \leqslant q_i$, so every generator of L'' has exponent over k not greater than q_1/q_i. This is not true of α_1^s, for any $s < q_i$, a contradiction. Therefore $s \geqslant q_i$, proving (4.1). Now write $\alpha_i^{q_i}$ as a polynomial $f_i(\alpha_1^{q_i}, \ldots, \alpha_{i-1}^{q_i})$ with coefficents in k, let g_i be the polynomial obtained from f by replacing its coefficients by their q_ith roots and let $\tilde{k}$ be the field generated over k by all these roots. Then $\tilde{k} \otimes_k K$ is generated over $\tilde{k}$ by the elements $x_i = \alpha_i - g_i(\alpha_1, \ldots, \alpha_{i-1})$ with the property that $x_i^{q_i} = 0$, so $\tilde{k} \otimes_k K$ is a homomorphic image of the truncated polynomial algebra

$$A = \tilde{k}[x_1, \ldots, x_r]/(x_1^{q_1}, \ldots, x_r^{q_r}).$$

Since they have the same dimensions as $\tilde{k}$-algebras they are isomorphic. This shows, in view of what we already know that not only do the Pickert exponents of K depend only on K but that there is a field $\tilde{k}$ such that $\tilde{k} \otimes_k K$ is of the form

$$A = \tilde{k}[x_1, \ldots, x_r]/(x_1^{p^{e_1}}, \ldots, x_r^{p^{e_r}}),$$

where the e_i are the Pickert exponents. One says that $\tilde{k}$ "*splits*" K over k and in fact there is a smallest such *splitting field* which it is not hard to show is the $\tilde{k}$ just constructed.

Note that A is just the tensor product over $\tilde{k}$ of the algebras $k[x_i]/(x^{q_i})$, so the ring of high order derivations of A will be known, by Theorem 3.3 once we have computed that of an algebra of the form $B = k[x]/(x^q)$ where k has characteristic p and q is a power of p, say $q = p^e$. It will be useful and no harder to consider the slightly more general case where $B = k[x]/(x^q - \alpha)$ with $\alpha \in k$. If α has no pth root in k then this is a simple purely inseparable extension of k of exponent e.

The results that follow are largely due to Keith [7]. An inseparable extension $K \supset k$ which is a tensor product of simple extensions is called modular. The necessary and sufficient condition for this is that K have "enough" approximate autormorphisms, i.e., that for every $\beta \in K$ with $\beta \notin k$ there is an approximate automorphism Φ with $\Phi\beta \neq \beta$ (Sweedler [13], cf. also [4]).

Observe that we have $(x + t)^q = x^q + t^q$, so it follows that

$$B = k[x]/(x^q - \alpha)$$

has an approximate automorphism Φ_t of order $q - 1$ uniquely defined by setting $\Phi_t x = x + t$. Write

$$\Phi_t = \mathrm{id} + t\varphi_1 + \cdots + t^{q-1}\varphi_{q-1} \tag{4.2}$$

and observe that for $m < q$ one has

$$\Phi_t x^m = (x + t)^m = x^m + tx^{m-1} + \binom{m}{2} t^2 x^{m-2} + \cdots + t^m. \tag{4.3}$$

Comparing (4.2) and (4.3), it follows that $\varphi_i(x^m) = \binom{m}{i} x^{m-i}$. In particular, we have

$$\varphi_m(x^m) = 1 \quad \text{and} \quad \varphi_n(x^m) = 0 \quad \text{for} \quad n > m.$$

Now $\mathrm{End}_k B$ is a free B-module of rank q and the foregoing shows that $\mathrm{id}, \varphi_1, \ldots, \varphi_{q-1}$ are a basis. Since these endomorphisms lie in $\mathfrak{D}(B)$, it follows that $\mathfrak{D}(B)$ is all of $\mathrm{End}_k B$. One can, moreover, check without difficulty that repeated application of the formula (1.4) gives

$$(-\Delta)^{l-1}\varphi_m = \sum{}'_{i_1+i_2+\cdots+i_l=m} \varphi_{i_1} \cup \varphi_{i_2} \cup \cdots \cup \varphi_{i_l}, \tag{4.4}$$

$1 \leqslant m \leqslant q - 1$, $1 \leqslant l \leqslant m$, where the sum is taken over distinct partitions $\{i_1, \ldots, i_l\}$ of m. In particular, one has

$$(-1)^m \Delta^m \varphi_m = \varphi_1 \cup \cdots \cup \varphi_1 \quad (m \text{ times}) \tag{4.5}$$

which is not zero, since $\varphi_1(x) = 1$, while $\Delta^{m+1}\varphi_m = 0$. This proves, in particular,

THEOREM 4.1. *Let k be a field of characteristic $p > 0$ and set*

$$B = k[x]/(x^q - \alpha)$$

where $q = p^e$ for some $e \geqslant 1$ and $\alpha \in k$. Then

(i) *$\mathfrak{D}^m = \mathfrak{D}^m(B)$ is a free B-module of rank $m + 1$ and $\mathfrak{D}^m(B)/\mathfrak{D}^{m-1}(B)$ is free of rank 1 for $m = 0, 1, \ldots, q - 1$, while $\mathfrak{D}^q = \mathfrak{D}^{q+1} = \cdots = \mathrm{End}_k B$.*

(ii) *B has bounded order equal to q and has a fundamental form $\Gamma(B/k)$ for which one can take $\varphi_1 \cup \varphi_1 \cup \cdots \cup \varphi_1$ (q times) where φ_1 is the derivation of B sending the coset of x to* 1. □

Note that for all $i, j, m < q$ we have

$$\varphi_i \varphi_j x^m = \binom{m}{j} \varphi_i x^{m-j} = \binom{m}{j}\binom{m-j}{i} x^{m-j-i}$$

and

$$\varphi_{i+j} x^m = \binom{m}{i+j} x^{m-j-i},$$

so

$$\varphi_i \varphi_j = \binom{i+m}{i} \varphi_{i+j}. \tag{4.6}$$

We therefore write symbolically $\varphi_i = D^i/i!$ since these symbols formally multiply by the rule

$$(D^i/i!)(D^j/j!) = \binom{i+j}{i} D^{i+j}/(i+j)!.$$

(For $i \geqslant q$ tacitly $\varphi_i = D^i/i! = 0$.) From (4.6) one has $\varphi_i^p = 0$ for all i. Also, as one can check, if $i = i_0 + i_1 p + \cdots + i_{e-1} p^{e-1}$ with $0 \leqslant i_s \leqslant p-1$ is the p-adic expansion of a nonnegative integer $i \leqslant q-1$, then

$$\varphi_i = (\varphi_1^{i_0}/i_0!)(\varphi_p^{i_1}/i_1!) \cdots (\varphi_{p^{e-1}}^{i_{e-1}}/i_{e-1}!).$$

Therefore, the ring generated over k by the φ_i is isomorphic to the truncated polynomial ring $k[z_0, \ldots, z_{e-1}]/(z_0^p, \ldots, z_{e-1}^p)$.

It follows from Theorem 4.1 that any algebra A of the form

$$A = k[x_1, \ldots, x_r]/(x_1^{q_1} - \alpha_1, \ldots, x_r^{q_r} - \alpha_r) \cong B_1 \otimes \cdots \otimes B_r$$

where k is a field of characteristic p and $B_i = k[x]/(x^{q_i} - \alpha_i)$ with $q_i = p^{e_i}$ and α_i in k has bounded degree and a fundamental form. Recall from Theorem 3.3 that $\mathfrak{D}(A) = \mathfrak{D}(B_1) \otimes_k \cdots \otimes_k \mathfrak{D}(B_r)$. For all $m < q_i$, let $D_i^m/m!$ denote the element of $\operatorname{End}_k B_i$ sending x^n to $\binom{n}{m} x^{n-m}$, and view these $D_i^m/m!$, by abuse of notation, as elements of $\mathfrak{D}(A)$. Then we have

THEOREM 4.2. (i) $\mathfrak{D}(A) = \operatorname{End}_k A$.

(ii) *$\mathfrak{D}^m(A)$ is a free A-module with basis consisting of all products $(D_1^{m_1}/m_1!) \cdots (D_r^{m_r}/m_r!)$ with $0 \leqslant m_i \leqslant q_i - 1$ and $m_1 + \cdots + m_r \leqslant m$.* □.

To apply the foregoing to a finite purely inseparable extension K of k we need only observe that if A is an algebra over a field k and $\tilde{k}$ an extension of k, and if we view $\tilde{k} \otimes_k A$ as a $\tilde{k}$-algebra, then $\mathfrak{D}^n(\tilde{k} \otimes_k A) = \tilde{k} \otimes_k \mathfrak{D}^n(A)$ for all n. It follows in particular that A has bounded degree if and only if $\tilde{k} \otimes A$ does and if either has a fundamental form, then so does the other. Taking for $\tilde{k}$ a splitting field of K we have

THEOREM 4.3. *Let K be a finite purely inseparable extension of a field k of characteristic $p > 0$ with Pickert exponents $e_1, \ldots, e_n$ and set $q_i = p^{e_i}$, $i = 1, \ldots, n$. Then*

(i) $\mathfrak{D}(K)$ *is all of* $\mathrm{End}_k K$.

(ii) $\dim_K \mathfrak{D}^m(K)$ *is equal to the number of sequences $(m_1, \ldots, m_r)$ with $0 \leqslant m_i \leqslant q_i - 1$, $i = 1, \ldots, r$, and $m_1 + \cdots + m_r \leqslant m$.*

(iii) *K has bounded degree equal to $\sum_{i=1}^{r} (q_i - 1) = (\sum q_i) - r$.*

(iv) *K has a fundamental form.* □

Assertion (i) of the foregoing is due to Nakai, Kosaki and Ishibashi [9]; our proof essentially follows Keith [7]. (ii) implies as before that $\dim_K \mathfrak{D}^m/\mathfrak{D}^{m-1} = \dim_K \mathfrak{D}^m - \dim_K \mathfrak{D}^{m-1}$ is equal to the number of sequences $(m_1, \ldots, m_r)$ with $0 \leqslant m_i \leqslant q_i - 1$ with $m_1 + \cdots + m_r = m$. That is, it is the coefficient of t^m in $F(t) = \prod (1 - t^{q_i})/(1 - t)$, and from this the q_i and hence the Pickert exponents $e_1, \ldots, e_r$ can be recovered. Moreover, $\dim_K \mathfrak{D}^m = 1 + \dim_K \mathfrak{D}'^m = 1 + \dim_K \ker \Delta^m$, so in particular one can recover the e_i from a knowledge of $\dim_K \ker \Delta^m$ for every m. (It is the case that except where $r = 1$, $\Gamma(K)$ actually is a coboundary.)

5. **The Main Theorem.** The symmetric multiderivations of a commutative k-algebra A form, under the $*$-multiplication, a commutative ring $\mathfrak{S} = \mathfrak{S}(A/k)$. If $f * g = h$ in $\mathfrak{S}$, then we say that f divides h and write $f|h$ even though in general $\mathfrak{S}$ has many nilpotent elements and factorization is not unique. When $A \supset B \supset k$ then a symmetric multiderivation of A over B is a fortiori one over k so $\mathfrak{S}(A/B) \subset \mathfrak{S}(A/k)$ and it is meaningful to speak of an element of the former ring dividing an element of the latter. In this section we prove the Main Theorem that if $K \supset B \supset k$ are finite purely inseparable field extensions, then $\Gamma(K/B)|\Gamma(K/k)$, but first we examine briefly the structure of $\mathfrak{S}(K/k)$.

More generally suppose that A is a commutative unital ring of prime characteristic $p > 0$ over a ring k. We say that $x_1, \ldots, x_r \in A$ form a p-basis for A and in particular that A has a p-basis, if A is a free module over kA^p with basis consisting of the p^r monomials $x_1^{n_1} \cdots x_r^{n_r}$, $0 \leqslant n_1, \ldots, n_r \leqslant p - 1$. In this case every multiderivation of A over k is a sum of cup products of ordinary derivations. For if $D_1, \ldots, D_r$ is the dual basis of derivations to the p-basis $x_1, \ldots, x_r$, then the multiderivation sending $(x_{i_1}, \ldots, x_{i_m})$ to 1 and all other $(x_{j_1}, \ldots, x_{j_m})$ to 0 is $D_{i_1} \cup \cdots \cup D_{i_m}$, and these clearly span. Clearly p-

bases exist for every finite purely inseparable field extension K/k as well as for any algebra of the form

$$A = k[x_1, \ldots, x_r]/(x_1^{q_i} - \alpha_1, \ldots, x_r^{q_i} - \alpha_r),$$

where k is a field of characteristic $p > 0$, $q_i = p^{e_i}$, and the α_i are elements of k.

Let D be a derivation of A over k. Denoting its mth cup power $D \cup \cdots \cup D$ (m times) by $D^{(m)}$, we have

$$D^{(m)} * D^{(n)} = \binom{m+n}{n} D^{(m+n)}.$$

If $f \in \mathfrak{S}(A/k)$, then we write f^{*m} for $f * \cdots * f$ (m times). It is easy to see that in characteristic p, one has $f^{*p} = 0$ for every f. If A has a p-basis, then this is trivial from (5.1). In that case, if $D_1, \ldots, D_n$ is a basis for the module of derivations, then $\mathfrak{S}(A/k)$ is generated over A by the elements $D_i^{(p^j)}$, $i = 1, \cdots, r$, all $j \geqslant 0$, amongst which there are no relations other than those following from the fact that they commute and that each has vanishing pth*-power. There is, however, a natural "divided pth power" endomorphism $\mathfrak{S}$ sending $D_i^{(p^j)}$ to $D_i^{(p^{j+1})}$ for every i and j.

For the rest of this section, unless otherwise noted, we assume that we have a finite purely inseparable field $K \supset k$ and that B denotes an intermediate field.

Suppose that $\xi \in K$ is an element of exponent $e > 0$ over B and that $h \in (\operatorname{End} B/k)_0$. Set $q = p^e$. We extend h to an endomorphism $\overline{h}$ of $B(\xi)$ by setting $\overline{h}(\sum_{i=0}^{q-1} b_i \xi^i) = \sum_{i=0}^{q-1} \xi^i h(b_i)$. Set $\gamma(\overline{h}) = N$. Since $\Delta^{N-1}\overline{h}$ is a nonzero multiderivation, it follows that one may so choose $a_1, \ldots, a_N$ that $\Delta^{N-1}\overline{h}(a_1, \ldots, a_N) \neq 0$ and every a_i is either in B or is equal to ξ. Set $\xi^q = c \in B$.

LEMMA 5.1. (i) *If* $a_1 = \cdots = a_q = \xi$, *then*

$$\Delta^{N-1}\overline{h}(a_1, \ldots, a_N) = \Delta^{N-q}\overline{h}(c, a_{q+1}, \ldots, a_N).$$

(ii) *Suppose that* $\Delta^{N-1}\overline{h}(a_1, \ldots, a_N) \neq 0$ *with every* a_i *either in* B *or equal to* ξ. (*One need not have* $N = \gamma(\overline{h})$.) *Then amongst the* a_i, *the number equal to* ξ *is divisible by* q.

PROOF. (i) Set $\beta = \Delta^{N-1}\overline{h}(\xi\ (q \text{ times}), a_1, \ldots, a_\nu)$ where the a_i are arbitrary and $q + \nu = N$. In the expansion of β, $|a_I|\xi^i \overline{k}(\xi^{q-i}|a_{cI}|)$ will appear $\binom{q}{i}$ times, always with the same sign, and therefore it does not appear at all unless $i = 0$ or $i = q$. The unique terms for $i = 0$ and $i = q$ appear with opposite signs unless $p = 2$ in which case sign is unimportant. Therefore in computing β the q-tuple $(\xi, \ldots, \xi)$ can effectively be replaced by $\xi^q = c$, as asserted.

(ii) Set $\beta = \Delta^{N-1}\bar{h}(\xi, \ldots, \xi\ (i \text{ times}), b_1, \ldots, b_\nu)$ where all b_j are in B and $i + \nu = N$. By (i) we need only show that if $0 < i < q$, then $\beta = 0$. Choose any subset $I \subset \{1, \ldots, \nu\}$ and consider the sum of all those terms in the expansion of β which are of the form $\pm|b_I|\xi^{i'}\bar{h}(\xi^{i''}|b_{cI}|)$ where cI is the complement of I in $\{1, \ldots, \nu\}$, and $0 \leqslant i', i'', i' + i'' = i$. These terms are all equal except for sign, and equal 0 unless $cI \neq \varnothing$ which we henceforth assume. The signs alternate as we take $i' = 0, 1, \ldots, i$, so the sum of these terms is $[\binom{i}{0} - \binom{i}{1} + \binom{i}{2} - \cdots \pm \binom{i}{i}] = 0$. □

Recall that $\gamma(B(\xi)/B) = q - 1$, for letting Φ_t be the approximate automorphism of order $q - 1$ of $B(\xi)$ over B sending ξ to $\xi + t$ and writing $\Phi_t = \mathrm{id} + t\varphi_1 + \cdots + t^{q-1}\varphi_{q-1}$ we have seen that $\mathrm{id}, \varphi_1, \ldots, \varphi_{q-1}$ span $\mathrm{End}_B B(\xi)$ as a B-module and $\gamma(\varphi_i) = i$. Recall further that $\varphi_i \xi^m = \binom{m}{i}\xi^{m-i}$ whence in particular $\varphi_i \xi^i = 1$, $\varphi_i \xi^j = 0$ for $j < i$.

Now let h be as before an element of $(\mathrm{End}_k B)_0$ which we extend to an element $\bar{h}$ of $(\mathrm{End}_k B(\xi))_0$ by setting $\bar{h}(b\xi^i) = \xi^i h(b)$ for $i = 0, 1, \ldots, q - 1$, and let φ_i be as before. With these notations we have

LEMMA 5.2. $\gamma(\varphi_i \bar{h}) = \gamma(\bar{h}) + i$, $i = 1, \ldots, q - 1$.

PROOF. We have always $\gamma(\varphi_i \bar{h}) \leqslant \gamma(\varphi_i) + \gamma(\bar{h}) = i + \gamma(\bar{h})$, so it is sufficient to show the reverse inequality. Set $\gamma(\bar{h}) = N$. From the foregoing lemma, there exist $n \geqslant 0$ and $b_1, \ldots, b_\nu \in B$ with $nq + \nu = N$ such that

$$\Delta^{N-1}\bar{h}(\xi\ (nq \text{ times}), b_1, \ldots, b_\nu) \neq 0.$$

It will be sufficient to show that

$$\theta = \Delta^{N+i-1}\varphi_i \bar{h}(\xi\ (nq + i \text{ times}), b_1, \ldots, b_\nu) \neq 0.$$

By Leibniz' rule,

$$-\Delta^{N+i-1}(\varphi_i \bar{h}) = \Delta^{i-1}\varphi_i * \Delta^{N-1}\bar{h}.$$

Evaluating this at $(\xi\ (nq + i \text{ times}), b_1, \ldots, b_\nu)$, the only nonzero terms in the expansion will all be of the form

$$\Delta^{i-1}\varphi_i(\xi\ (i \text{ times})) \cdot \Delta^{N-1}\bar{h}(\xi\ (nq \text{ times}), b_1, \ldots, b_\nu)$$

(cf. (3.2)). The first factor in the foregoing is $(-1)^i$ and the number of terms is $\binom{nq+i}{i} \equiv 1 \bmod p$. Therefore in fact $\theta = (-1)^i$ times the second factor, which is not zero. □

We shall say of an $\bar{h} \in \mathrm{End}_k B(\xi)$ obtained from $h \in \mathrm{End}_k B$ by setting $\bar{h}(\sum b_i \xi^i) = \sum \xi^i h(b_i)$ that it is an "*almost linear*" extension of h. The foregoing immediately gives the

COROLLARY. *Let* $\bar{h} \in \mathrm{End}_k B(\xi)$ *be an almost linear extension of some* $h \neq 0$ *in* $\mathrm{End}_k B$ *and* g *be a nonzero element of* $\mathrm{End}_B B(\xi)$. *Then* $\gamma(g\bar{h}) = \gamma(g) + \gamma(\bar{h})$. □

Choose now a Pickert generating sequence $\xi_1, \ldots, \xi_N$ for K over B, and set $B_i = B(\xi_1, \ldots, \xi_i)$, $i = 0, \ldots, N$. Any $h \in \mathrm{End}_k B_i$ can, by this choice of generators, be extended "almost linearly" to an element of $\mathrm{End}_k B_{i+1}$ and so on until we have an element $\bar{h} \in \mathrm{End}_k K$. Let the Pickert exponents of K over B be $e_1, \ldots, e_r$, set $q_i = p^{e_i}$ for $i = 1, \ldots, r$, and for any sequence $M = (m_1, \ldots, m_r)$ of nonnegative integers with $m_i \leqslant q_i - 1$, all i, set $\eta^M = \xi^{m_1} \cdots \xi^{m_r}$. Then these η^M form a basis for K over B and $\bar{h}$ is in effect defined by setting $\bar{h}(\sum b_M \xi^M) = \sum \xi^M h(b_M)$. We call $\bar{h}$ a "normal extension" of h. Notice that almost linear extension of any $h \in \mathrm{End}_k B_i$ to $h' \in \mathrm{End}_k B_{i+1}$ does not decrease its degree, that is $\gamma(h') \geqslant \gamma(h)$.

Define $f_M \in \mathrm{End}_B K$ by setting $f_M(\eta^M) = 1, f_M(\eta^{M'}) = 0$ for $M' \neq M$. These f_M form a K-basis for $\mathrm{End}_B K$, namely the dual basis to the η^M. Each f_M can be written as a composite in the following way: For every $i = 1, \ldots, r$ and every $j = 1, \ldots, q_{i-1}$, let f_{ij} be the element of $\mathrm{End}_{B_{i-1}} B_i$ sending η_i^j to 1 and $\eta_i^{j'}$ to 0 for all $j' \neq j$. If $M = (m_1, \ldots, m_r)$, then

$$f_M = f_{r,m_r} f_{r-1,m_{r-1}} \cdots f_{1,m_1} \tag{5.1}$$

where on the right each f_{ij} is tacitly extended normally by means of the Pickert generating sequence $\xi_1, \ldots, \xi_N$ to an element of $\mathrm{End}_B K$. Another way to read the right side of (5.1) is, starting from the right, to extend f_{1,m_1} to B_2, then extend $f_{2,m_2} f_{1,m_1}$ to B_3, and so forth. Either interpretation gives the same result, namely f_M, but the latter, together with repeated application of the foregoing corollary and the remark that these extensions do not decrease the degree, gives the following:

THEOREM 5.3. *Suppose that we have finite purely inseparable field extensions* $K \supset B \supset k$ *and an element* $h \in \mathrm{End}_k B$. *Let* $\bar{h}$ *be a normal extension of* h *to* $\mathrm{End}_k K$, *relative to some Pickert generating sequence* $\xi_1, \ldots, \xi_r$ *of* K *over* k, *let* $e_1, \ldots, e_r$ *be the Pickert exponents of* K *over* B, *and set* $q_i = p^{e_i}$, $i = 1, \ldots, r$. *Then for every* $M = (m_1, \ldots, m_r)$ *with* $0 \leqslant m_i \leqslant q_s - 1$ *and* $h \in \mathrm{End}_k B$ *with normal extension* $\bar{h}$ *to* $\mathrm{End}_k K$ *we have*

$$\gamma(f_M \bar{h}) \geqslant \gamma(\bar{h}) + \sum m_i. \quad \square$$

Consider now the case where $M = (q_1 - 1, \ldots, q_r - 1)$. Then $\sum m_i = \sum q_i - r = \gamma(K/B)$, since $\gamma(K/k) \geqslant \gamma(f_M \bar{h})$. This yields the result from which the Main Theorem will follow immediately:

COROLLARY. *For every* $h \in \mathrm{End}_k B$ *we have* $\gamma(\bar{h}) \leqslant \gamma(K/k) - \gamma(K/B)$. □

Now observe that if $h_1, \ldots, h_\mu$ are a basis for $\mathrm{End}_k B$ over B with corresponding normal extensions $\bar{h}_1, \ldots, \bar{h}_\mu$ to $\mathrm{End}_k K$ (relative to a Pickert generating sequence $\xi_1, \ldots, \xi_r$), then with the foregoing notations, the set of all $f_M \bar{h}_i$ forms a basis for $\mathrm{End}_k K$ over K. Therefore, amongst these there must exist one, which we assume $f_M \bar{h}_i$ denotes, with $\gamma(f_M \bar{h}) = \gamma(K/k)$. In particular, there is an $f \in \mathrm{End}_B K$ and an $h \in \mathrm{End}_k B$ such that $\gamma(f\bar{h}) = \gamma(K/k)$. Now $\gamma(f\bar{h}) \leqslant \gamma(f) + \gamma(\bar{h})$ and $\gamma(f) \leqslant \gamma(K/B)$ so applying the foregoing corollary we have

$$\gamma(K/k) = \gamma(f\bar{h}) \leqslant \gamma(f) + \gamma(\bar{h}) \leqslant \gamma(K/B) + [\gamma(K/k) - \gamma(K/B)].$$

Therefore equality holds throughout, and we have $\gamma(f) = \gamma(K/B)$, $\gamma(\bar{h}) = \gamma(K/k) - \gamma(K/B)$. This proves the Main Theorem, for setting $\gamma(K/k) = \gamma$, $\gamma(K/B) = \gamma'$, we have, by Leibniz' rule,

$$\Gamma(K/k) = \Delta^{\gamma-1}(f\bar{h}) = -\Delta^{\gamma'-1} f * \Delta^{\gamma-\gamma'-1}\bar{h}.$$

But $\Delta^{\gamma'-1} f = \Gamma(K/B)$. Thus, we have

MAIN THEOREM. *Let* $K \supset B \supset k$ *be finite purely inseparable extensions. Then* $\Gamma(K/k) = \Gamma(K/B) * \Delta^n \bar{h}$ *where* $\bar{h}$ *is the normal extension (relative to some Pickert generating sequence of* K *over* B*) of some* $h \in \mathrm{End}_k B$, *and* $n = \gamma(\bar{h}) - 1$. *In particular,* $\Gamma(K/B)$ *divides* $\Gamma(K/k)$. □

Some of the auxiliary results of this section can be strengthened. We reserve that for another place and close with some simple examples showing how the structure of an inseparable extension is reflected in its fundamental form. First, suppose that K has exponent 1 over k and two generators, x and y with $x^p, y^p \in k$. Let D_x be the derivation sending x to 1 and y to 0, and similarly for D_y. We write $D_x^{(m)}$ for $D_x \cup \cdots \cup D_x$ (m times) and denote the *-multiplication simply by juxtaposition. Then $\Gamma(K/k) = D_x^{(p-1)} D_y^{(p-1)}$.

The only intermediate fields of interest are those B of degree p over k and we now examine the relationship between these and factors of $\Gamma(K/k)$. Every such B is the "fixed field", i.e., kernel of a derivation D of K over k; D is of the form $a_1 D_x + a_2 D_y$ for some $a_1, a_2 \in K$ and is determined up to multiplication by an element of K^*, the multiplicative group of K. One has $\Gamma(K/B) = D^{(p-1)}$. If, say, $a_1 \neq 0$, then since $D_y D_y^{(p-1)} = 0$ we have

$$(a_1 D_x + a_2 D_y)^{(p-1)} D_y^{(p-1)} = a_1^{p-1} D_x^{(p-1)} D_y^{(p-1)} = a_1^{p-1} \Gamma(K/k)$$

exhibiting explicitly that $\Gamma(K/B) | \Gamma(K/k)$. Since these forms are defined only up to multiplication by an element of K^* it is convenient to view $a_1 D_x + a_2 D_y$

also as only so defined, and therefore as being determined by the point (a_1, a_2) of the projective line $P_1(K)$ over K. Thus to every intermediate field B of degree p over k there is assigned a unique point of this line. On the other hand, the fixed field of a derivation $D = a_1 D_x + a_2 D_y$ may be reduced to k, and is larger than k if and only if D^p (the pth composite of D with itself) $= bD$ for some $b \in K$. If $a_1 \neq 0$, then replacing D by $a_1^{-1} D$ we have $D_x = 1$ whence $D^p x = 0$ so $b = 0$. Setting $a_1^{-1} a_2 = a$, the condition that $D_x + aD_y$ have fixed field larger than k is easily seen to be a set of algebraic conditions on the coefficients of a when the latter is expressed in terms of a linear basis of K over k. With this one can verify that the intermediate fields B of degree p are parametrized by the points of a projective variety V contained in $P^1(K)$, which may also be viewed as a k-variety. Thus, while there is a natural assignment of the family of intermediate fields B to a family of factors $(a_1 D_x + a_2 D_y)^{(p-1)}$ of $\Gamma(K/k)$, the members of these families are not in natural correspondence. (Here distinct fields correspond to distinct factors, but the next example will show that that need not be the case.) As a special case of the general conjecture in the introduction, we conjecture that V is irreducible.

As our second example let K again have two generators, x and y, but now suppose that x has exponent 2 over k and y exponent 1. Since $K = k(x) \otimes_k k(y)$ one immediately has that $\Gamma(K/k) = D_x^{(p^2-1)} D_y^{(p-1)}$. Let us consider as before intermediate fields B of degree p over k; such a B is of the form $k(z)$ with $z^p \in k$. If $B \neq k(x^p)$ then K is generated over B by x which still has exponent two relative to B, so $\Gamma(K/B) = D_x^{(p^2-1)}$. Thus, to all such B correspond the same factor of $\Gamma(K/k)$. On the other hand, if $B = k(x^p)$, then $K = k(x) \otimes_B k(y)$ and $\Gamma(K/B) = D_x^{(p-1)} D_y^{(p-1)}$; since $D_x^{(p-1)} D_x^{(p^2-p)} = D_x^{(p^2-1)}$, one again sees explicitly that $\Gamma(K/B) | \Gamma(K/k)$.

Observe in this case that every one of our intermediate fields B is contained in $k(x^p, y) \cong k(x^p) \otimes_k k(y)$, a field like that of the first example. There one had but a single family of factors of the fundamental form corresponding to the family of intermediate fields, and the latter fields were, in some loose sense, indistinguishable within the structure of the larger field. Here the intermediate fields B of degree p are of two readily distinguishable kinds–those over which K has exponent 2 (which are again, in a loose sense, indistinguishable)–to all of which corresponds the same factor of $\Gamma(K/k)$, and the unique $B = k(x^p)$ over which K has exponent 1–to which corresponds a different factor of $\Gamma(K/k)$.

One can see, incidentally, from the factorization of $\Gamma(K/k)$ in this second example, that $k(x^p)$ cannot be a tensor factor of K over k. For were it such then $D_x^{(p^2-p)}$ would have to be the form of the complementary factor, but this cannot be the fundamental form of anything.

As our final example let $K = k(x,y)$ where x and y both have exponent two over k with $y^p = ax^p + b$ where a, b are elements of k having no pth roots there. To compute $\Gamma(K/k)$, set $k' = k(a^{1/p})$, $z = y - a^{1/p}x$, and observe that $k'(x,y) = k'(x) \otimes_{k'} k'(z)$ where $x^{p^2}, z^p \in k'$. Therefore, if φ, ψ are derivations of $K' = K \otimes_k k'$ defined by setting $\varphi x = 1$, $\varphi z = 0$, $\psi x = 0$, $\psi z = 1$ then we have $\Gamma(K'/k') = \varphi^{(p^2-1)}\psi^{(p-1)}$. But $\varphi = D_x + a^{1/p}D_y$ and $\psi = D_y$. Therefore, since $D_y^{(i)} D_y^{(p-1)} = 0$ unless i is a multiple of p, while $D_y^{(np)} D_y^{(p-1)} = D_y^{(np+p-1)}$, and since, for $0 \leqslant n < p$, $\binom{p^2-1}{np} \equiv \binom{p-1}{n} \equiv (-1)^n \bmod p$, we have

$$\Gamma(K'/k') = (D_x^{(p^2-1)} - aD_x^{(p^2-1-p)} D_y^{(p)} + a^2 D_x^{(p^2-1-2p)} D_y^{(2p)} - \cdots) D_y^{(p-1)}$$

$$= (D_x^{(p^2-p)} - aD_x^{(p^2-2p)} D_y^{(p)} + \cdots + a^{p-1} D_y^{(p^2-p)}) D_x^{(p-1)} D_y^{(p-1)}.$$

Since this expression is defined over K it must be identical with $\Gamma(K/k)$. Setting $a = 0$ would bring us back to the preceding example, as would adjoining the pth root of a. There is a unique intermediate field of degree p, namely $B = k(x^p) = k(y^p)$ and $\Gamma(K/B) = D_x^{(p-1)} D_y^{(p-1)}$.

The results of this paper are only partial, leaving open important questions. For example, when is a factor Γ' of $\Gamma(K/k)$ equal to $\Gamma(K/B)$ for some intermediate field B? There are some easily proven necessary conditions: Any factor of Γ must annihilate Γ' and any element of the ring $\mathfrak{S}$ whose pth divided power divides Γ' must itself divide Γ'. The first example shows that this is not sufficient but suggests that any Γ' with these properties must be a member of a family of factors of $\Gamma(K/k)$ corresponding to some family of intermediate fields B. Another open question is to determine when a factorization $\Gamma(K/k) = \Gamma'\Gamma''$ corresponds to a factorization of K into a tensor product of two intermediate fields. A necessary condition is that Γ' and Γ'' each satisfy the preceding conditions and moreover have no common factors. It is tempting to conjecture that this also is sufficient.

References

1. M. Gerstenhaber, *The cohomology structure of an associative ring*, Ann. of Math. (2) **78** (1963), 267–288. MR **28** #5102.
2. ———, *On the deformation of rings and algebras*, Ann. of Math. (2), **79** (1964), 59–103. MR **30** #2034.
3. ———, *On the deformation of rings and algebras*. III, Ann. of Math. (2) **88** (1968), 1–34. MR **39** #1521.
4. ———, *On modular field extensions*, J. Algebra **10** (1968), 478–484. MR **38** #142.
5. ———, *The fundamental form of a finite purely inseparable field extension*, Bull. Amer. Math. Soc. **78** (1972), 717–720. MR **46** #156.
6. N. Jacobson, *Lectures in abstract algebra*, Vol. III, Van Nostrand, Princeton, N. J., 1964, pp. 191–197. MR **30** #3087.
7. Sandra Z. Keith, *High derivations of fields*, Dissertation, Univ. of Pennsylvania, Philadelphia, Pa., 1971.

8. Y. Nakai, *High order derivations.* I, Osaka J. Math. **7** (1970), 1–27. MR **41** #8404.

9. Y. Nakai, K. Kosaki and Y. Ishibashi, *High order derivations.* II, J. Sci. Hiroshima Univ. Ser. A-I Math. **34** (1970), 17–27. MR **42** #1807.

10. G. Pickert, *Eine Normalform für endliche rein-inseparable Körpererweiterungen*, Math. Z. **53** (1950), 133–135. MR **12**, 316.

11. R. Rasala, *Inseparable splitting theory*, Trans. Amer. Math. Soc. **162** (1971), 411–448. MR **44** #1648.

12. R. W. Richardson, Jr., *A rigidity theorem for subalgebras of Lie and associative algebras*, Illinois, J. Math. **11** (1967), 92–110. MR **34** #5992.

13. M. E. Sweedler, *Structure of inseparable extensions*, Ann. of Math. (2) **87** (1968), 401–410; corrigendum, ibid. (2) **89** (1969), 206–207. MR **36** #6391; **38** #4451.

Department of Mathematics, University of Pennsylvania, Philadelphia, Pennsylvania 19174