CLEAVAGE OF INSEPARABLE FIELD PRODUCTS

by

William Duane Montgomery

A Dissertation Submitted to the
Graduate Faculty in Partial Fulfillment of
The Requirements for the Degree of
DOCTOR OF PHILOSOPHY

Major Subject: Mathematics

Approved:

Signature was redacted for privacy.

In Charge of Major Work

Signature was redacted for privacy.

Head of Major Department

Signature was redacted for privacy.

Dean of Graduate College

Iowa State College
Ames, Iowa
1958

TABLE OF CONTENTS

I. INTRODUCTION

In the study of the structure of a finite dimensional associative algebra A with radical $N \neq 0$ (i.e. the ideal of all properly nilpotent elements), the Wedderburn Principal Theorem (1) is a high point. It gives separability of the quotient algebra A/N as a sufficient condition for each element of A to be written uniquely as the sum of an element in N plus one in a semisimple (i.e. one having zero radical) subalgebra S of A. In such a case A is written as S + N. This property of decomposition of each element is termed "cleavage" and has been studied in the more general context of rings by Vinograde (2) and others (3).

The present problem will be to find conditions for the cleavage of a special class of direct product algebras. The direct product of two finite dimensional associative algebras B and C over a field F is defined as follows. All linear combinations of formal products $\{b\ c\}$, $b \in B$, $c \in C$ with coefficients in F, where $f(b\ c) = (f\ b)\ c = b\ (f\ c) = f(c\ b)$ for $f \in F$, form a direct product algebra written as $B \times_F C$. If $\{b_i\}_1^m$ and $\{c_j\}_1^n$ are bases of B and C respectively over F, then one possible basis for $B \times_F C$ is the set $\{b_i\ c_j\}$ of mn formal products. In case C is itself a field extension of F, then the ring $B \times_F C$ may be considered as an algebra over the extended field C with dimension that of B over F.

The algebra A to be considered will be the direct product $L \times_K M$ of two field extensions L and M of K (having prime characteristic p). L will always be finite pure inseparable over K (i.e. L is finite dimensional over K and there exists a single smallest natural number e such that $h \in L$ implies $h^{p^e} \in K$; p^e will be called the exponent of L over K) while M (to be identified with $1 \times_K M$) will be arbitrary over K when A is taken as an algebra over M. When A is taken as an algebra over K or $L = L \times_K 1$ then M will also be considered as finite pure inseparable over K. The conditions for cleavage will be sought in terms of the structural properties of L, M, and the composite L M.

II. PRELIMINARY CONSIDERATIONS

It is appropriate at this point to first give a theorem concerning the nature of the present composite L M. If L | K (read as L over K) and M|K are given with L and M not necessarily contained in a common overfield, then a composite of L and M is defined as follows: let Q be any field containing M and containing also an $L_1 \geq K$ such that $L \underset{K}{\cong} L_1$ ($\underset{K}{\cong}$ denotes an isomorphic mapping which leaves elements of K unchanged) and such that Q is generated by L_1 and M. Then Q is called a composite of L and M. If L and M are contained in a common overfield, then an obvious composite is the field generated by them. Two composites Q_1 and Q_2 are called equivalent if $Q_1 \underset{M}{\cong} Q_2$. The uniqueness, in the sense of equivalence, of the present composite is essentially proven on page 6 and will be assumed here.

Theorem 1. If L|K is pure inseparable and M | K is arbitrary, then there exists a unique pair of subfields (L', M') such that $L \geq L' \geq K$, $M \geq M' \geq K$ and $L' \underset{K}{\cong} M'$. Also the pair is maximal in the sense that for $M \geq M'' \geq M'$, $L \geq L'' \geq L'$, and $L'' \underset{K}{\cong} M''$, then $M'' = M'$ and $L'' = L'$. In addition the composite L M, generated by L_1 and M such that $L \underset{K}{\cong} L_1$, has $\varphi(L') = M' = L_1 \cap M$.

Proof. Define $M' = L_1 \cap M$ and $L' = \varphi^{-1}(M')$ so that $L \geq L' \geq K$ and $M \geq M' \geq K$. The pair (L', M') is uniquely defined

such that $\varphi(L') = M' = L_1 \cap M$ so it only remains to prove the pair maximal. If the pair (L', M') is not maximal then there exists a pair (L'', M'') such that $L'' \overset{\psi}{\underset{K}{\cong}} M''$ and either $L \supseteq L'' \supsetneq L'$ or $M \supseteq M'' \supsetneq M'$. In case $L \supseteq L'' \supsetneq L'$ there exists a non zero $h \in L'' - L'$ with image $\psi(h) = m \in M''$ such that $h^{p^e} = m^{p^e} = k \in K$ for some smallest natural number e (p is the prime characteristic of K). Now $\varphi(h) \neq m$ since $\varphi(h) \notin M'$ so there exists a nilpotent element $\varphi(h) - m$ in L M of index p^e. Similarly in case $M \supseteq M'' \supsetneq M'$ there exists a non zero $m' \in M'' - M'$ with image $\psi^{-1}(m') = h' \in L''$ such that $m'^{p^f} = h'^{p^f} = k' \in K$. Since $\varphi(h') \neq m'$ there exists a nilpotent element $\varphi(h') - m'$ in L M of index p^f. Thus the pair (L', M') is maximal. In all that follows the above M' will be denoted by E.

Next consider a field F of prime characteristic p such that $[F \mid F^p]$, the degree of F over F^p, is finite. Thus F is finite pure inseparable over F^p and there exists a minimum set of elements $\{a_i\}_1^n$ that will generate $F \mid F^p$. Each a_i will satisfy a pure inseparable and irreducible equation $x^p - r_i = 0$ for $r_i \in F^p$ and $i = 1, 2, \ldots, n$. That is r_i has no pth root in F^p. Thus $[F \mid F^p] = p^n$ and n will be called the "degree of imperfection" of F.

Becker and Mac Lane (4) have shown that n is the maximum of the minimum number of generators required for any finite algebraic extension of F. This minimum number of generators

in any case is called the multiplicity of the extension over F. They have also shown that if $[F \mid F^p]$ is infinite, then for every natural number m there exists a finite algebraic extension of F requiring m generators. It is known that every finite algebraic extension of a perfect field is simple (i.e. has multiplicity one), and from the above it is seen that this is also true of a field having degree of imperfection one. Any field of prime characteristic which is of either of the two previously mentioned types is called "almost perfect".

The following notation will be used throughout. For L finite pure inseparable over K and M arbitrary over K define $A = L \times_K M$ as an algebra over M, where $L \times_K 1 \subseteq A$ will be denoted by L_o. In the composite L M the original L will be identified and $E = L \cap M$. Also identifying M with $1 \times_K M \subseteq A$, the structure is as pictured with descending lines used to denote inclusion.

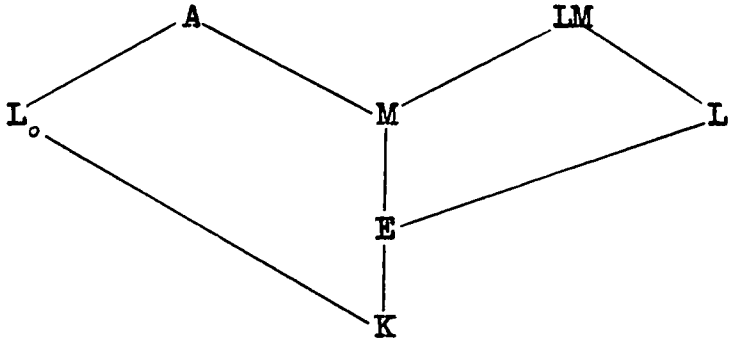

Figure 1. Structure of algebra and composite

Let $\{a_i\}_1^n$ be a basis for L | K and $\{b_j\}_1^n$ the corresponding one for L_o | K. Then $A = \sum M \cdot b_j$ and $L\,M = \sum M \cdot a_i$ suggesting the homomorphism $\sum m_i\, b_i \longrightarrow \sum m_i\, a_i$ of A onto L M. For N the kernel, $A/N \cong L\,M$, with $\overline{L}_o$, $\overline{M}$, and $\overline{K}$ the images in $\overline{A} = A/N$ of L, M, and K in L M (the bar will always denote the homomorphic image of a subset of A in $\overline{A}$). The above isomorphism may be considered as an algebra isomorphism over L, M, or K according as the scalar field is treated in $\overline{A}$ as $\overline{L}_o$, $\overline{M}$, or K respectively. $\overline{L}_o$, $\overline{M}$, or $\overline{K}$ is just the collection of equivalence classes in $\overline{A}$ each of which contains exactly one element of L_o, M, or K. If p^e is the exponent of L | K and d a nilpotent element of A, then for $d = \sum m_i\, b_i$, $m_i \in M$, $d^{p^e} = \sum m_i^{p^e}\, b_i^{p^e} = \sum m_i^{p^e}\, a_i^{p^e} = (\sum m_i\, a_i)^{p^e} = 0$ so $\sum m_i\, a_i \in L\,M$ is zero and $d \in N$. Thus N contains the radical. Also for $d' \in N$, $d' = \sum m_i'\, b_i \rightarrow \sum m_i'\, a_i = 0$ so $d'^{p^e} = \sum m_i'^{p^e}\, b_i^{p^e} = \sum m_i'^{p^e}\, a_i^{p^e} = 0$ and d' is nilpotent. Hence N is the radical of A.

If A cleaves over any of the aforementioned three fields, then A = S + N where S is a semisimple subalgebra of A over the respective field. A maps homomorphically onto S with kernel N so $A/N \cong S$ as algebras over the respective field. Since $A/N \cong L\,M$, then $S \cong L\,M$ as algebras over L, M, or K with L treated in S as L_o. Let $u = 1\, X_K\, 1$, the unity element of A. be written as s + n for $s \in S$ and $n \in N$. Now $u^{p^e} = u = s^{p^e} + n^{p^e} = s^{p^e} \in S$. Thus S has the same unity element as A

which means S contains L_o, M, or K when A cleaves over L_o, M, or K respectively. Conversely if there exists a field S in A containing L_o, M, or K and isomorphic to L M over L, M, or K respectively, the dimension of the vector space sum $S + N \subseteq A$ is that of A over the respective field so $A = S + N$. Thus A cleaves over that field. It is clear that when M is finite pure inseparable over K that cleavage over M implies such over K. The above results are summarized in the following theorem.

Theorem 2. $A = L X_K M$ cleaves over L_o, M, or K is and only if there exists in A a field S containing L_o, M, or K and isomorphic to the composite L M as algebras over L, M, or K respectively.

One more useful result is given by Pickert (5) in the canonical construction of a field L which is finite pure inseparable over a base field K. Let p be the prime characteristic of K, then there exists a minimum set of generators $\{a_i\}_1^m$ for $L \mid K$ such that $a_i^{q_i} = f_i(a_1^{q_i}, a_2^{q_i}, \ldots, a_{i-1}^{q_i})$ for $i = 1, 2, \ldots, m$. Here $q_i = p^{e_i}$, $e_i \geq e_{i+1}$, and $f_i(x_1, x_2, \ldots, x_{i-1})$ are polynomials with coefficients in K such that the power of x_j is $< (q_j/q_i)$ for $j = 1, 2, \ldots, i-1$. Also for any other minimum set of m generators there is an ordering of them which will satisfy polynomials (possibly different) having the same specifications as the f_i and using

exactly the same q_i.

For M arbitrary over K there exists a canonical set of generators $\{a_i\}_1^m$ of L | K such that an initial segment ($\{a_i\}_1^{m'}$, $m' \leqslant m$) of them canonically generate L M | M as follows: $a_i^{q_i'} = g_i(a_i^{q_i'}, a_2^{q_i'}, \ldots, a_{i-1}^{q_i'})$ for $q_i' = p^{e_i'}$, $e_i' \geqslant e_{i+1}'$, $e_i' \leqslant e_i$, $i = 1, 2, \ldots, m$ with $q_i' = 1$ for $i = m' + 1, m' + 2, \ldots, m$. If the algebra $A = L X_K M$ (over M) is considered with $\{b_i\}_1^m$ generating L_o | K exactly as the above set $\{a_i\}_1^m$ generates L | K and L M | M, then Pickert gives a basis for the radical N of A. Define $w_i' = b_i^{q_i'} - g_i(b_1^{q_i'}, b_2^{q_i'}, \ldots, b_{i-1}^{q_i'})$ for $i = 1, 2, \ldots, m$. If $\{w_i\}_1^n$ is the set of all non zero w_i' then a basis of N over M consists of the power products $\left\{\prod_{i=1}^{m'} b_i^{\sigma_i} \prod_{j=1}^{n} w_j^{\tau_j}\right\}$, where $0 \leqslant \sigma_i < q_i'$, $0 \leqslant \tau_j < r_j$, $\sum_{j=1}^{n} \tau_j > 0$, and r_j is the index of the radical element w_j. It is clear that the index of the radical N is $\leqslant$ the exponent of L | K.

III. SOME CASES FOR K = E

Theorem 1. If $A = L X_E M$ and $L \mid E$ is simple then A is a field and hence cleaves over M.

Proof. $L \mid E$ simple implies $L M \mid M$ is also simple so if b generates $L_o \mid E$ just as a generates $L \mid E$, then $b^{p^e} = a^{p^e} = k \in (E - M^p)$ for some e. Since $L_o \cap M = E$, this implies that b satisfies an irreducible equation over M so $A = M(b)$ is a field isomorphic to $L M = M(a)$.

Corollary. For $A = L X_E M$ and E almost perfect, A is a field.

Proof: If E is almost perfect and $L \mid E$ finite, then $L \mid E$ is simple and by Theorem 1 A is a field.

Theorem 2. If $A = L X_E M$ and $L M \mid M$ is simple, then $A \mid M$ cleaves.

Proof. The canonical set $\{a_i\}_1^m$ of Pickert generating $L \mid E$ may be chosen so a_1 will generate $L M \mid M$. Let $\{b_j\}_1^m$ be the corresponding set generating $L_o \mid E$. Now $a_1^{q_1'} = k' \in (M - M^p)$ and $a_1^{q_1} = k \in (E - E^p)$, so since $L \cap M = E$ then $q_1 = q_1'$. Thus $b_1^{q_1} = k \in (M - M^p)$ and $M(b_1) \cong L M = M(a_1)$ as algebras over M, so $A \mid M$ cleaves by Theorem 2, Chapter II. It is interesting to note that in this case A need not be a field. (See the example of Pickert (5) on

pages 95, 96.)

Corollary. For $A = L\ X_E\ M$ and M almost perfect, $A \mid M$ cleaves.

Proof. Since M is almost perfect and $L\ M \mid M$ finite, then $L\ M \mid M$ is simple and by Theorem 2 $A \mid M$ cleaves.

A special case for cleavage is for $A = L\ X_K\ M$ to be a field. A criterion for this is given by the following theorem.

Theorem 3. $A = L\ X_K\ M$ is a field if and only if $K = E$ and $q_i = q_i'$ for $i = 1, 2, \ldots, m$.

Proof. Since $q_i \geqslant p$ for $i = 1, 2, \ldots, m$ the second part of the theorem implies in particular that $m = m'$. The existence of the case $m = m'$ for general m can be easily seen by considering in the composite L M the field $L' = K(a_1, a_2, \ldots, a_{m'})$. Then clearly $L'\ M = L\ M$ and the multiplicity of $L' \mid K$ equals that of $L'\ M \mid M$.

Let $m = 1$, $q_1 = q_1'$, and $K = E$, then by Theorem 1 A is a field. Using an induction on m, assume all algebras $L\ X_K\ M$ are fields for which $m = s$, $K = E$, and $q_i = q_i'$ for $i = 1, 2, \ldots, s$. Consider an algebra $A = L\ X_E\ M$ for which $q_i = q_i'$ for $i = 1, 2, \ldots, s+1$ and $m = s+1$. The subalgebra $L'\ X_E\ M$ for $L' = E(a_1, a_2, \ldots, a_s)$ is such that $L_o' \cap M = E = L' \cap M$, where $L_o' = L'\ X_E\ 1$. Also $q_i = q_i'$ for $i = 1, 2, \ldots, s$ so

by hypothesis $A' = L' X_E M$ is a field. Now $A = A'[b_{s+1}]$ so if b_{s+1} can be shown to satisfy an irreducible equation over A', the induction will be complete. Since $q_{s+1} = q'_{s+1}$, $a_{s+1}^{q_{s+1}}$ is an element of L' with no pth root in $L' M$. The homomorphism of A' onto $L' M$ is an isomorphism, and if g in A' corresponds to $a_{s+1}^{q_{s+1}}$ in $L' M$ then $b_{s+1}^{q_{s+1}} = g \in (A' - A'^p)$ so b_{s+1} satisfies an irreducible equation over A' and A is a field.

Conversely if $L X_K M$ is a field then K must equal E for otherwise there exists an element $h \in (E - K)$ with image h' in L_o, using the isomorphism $L_o \underset{K}{\sim} L$ which leaves the elements of K invariant. Since $L_o \cap M = K$, $h \neq h'$ but $h^{p^e} = h'^{p^e}$ for p^e the exponent of $L \mid K$. Thus there exists a nilpotent element in $L X_K M$ contrary to the field assumption. The usual homomorphism of $L X_K M$ onto $L M$ now becomes an isomorphism, and for the present L_o will be identified with L so $L X_E M = L M$. For $L' = E(a_1, a_2, \ldots, a_n)$, $n < m$, no element in $L - L'$ can be represented in $L' X_E M$ since it would then have two distinct representations in $L X_E M$ as an algebra over M. Thus $m = m'$ and since $a_{n+1}^{q'_{n+1}} \in L' X_E M$ and $a_{n+1}^{q_{n+1}} \in L$, then $a_{n+1}^{q_{n+1}} = a_{n+1}^{q'_{n+1}}$ so $q_{n+1} = q'_{n+1}$ for $n = 0, 1, \ldots, m - 1$.

IV. M AN INBETWEEN FIELD OF L AND K

It should be noted that for $L \geq M \geq K$, $M \mid K$ is finite pure inseparable with $L\,M = L$ and thus $L \underset{K}{X} M$ will always cleave over L_o and K. The image of M in L_o will be denoted by M_o. The structure is pictured below with $M_o \underset{K}{\cong} M$ and $L \cap M = E = M$.

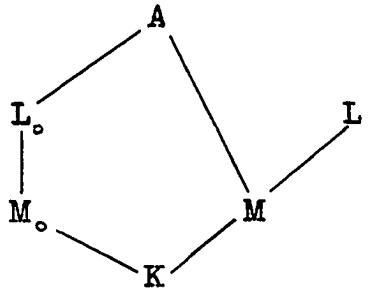

Figure 2. Modified structure

Considering A as an algebra over L_o the subring $M \underset{K}{X} M = B$ is taken as an algebra over $M_o = M \underset{K}{X} 1$. Since $B \mid M_o$ cleaves, with N_1 as the radical of B, it can be written as $B = M_o + N_1$. In going to $A \mid L_o$ any basis of $B \mid M_o$ (such as the basis of $M \mid K$) will remain the basis of $A \mid L_o$ since $[B \mid M_o] = [A \mid L_o] = [M \mid K]$. Thus the basis of $N_1 \mid M_o$ can be used over L_o to obtain the new radical N of $A \mid L_o$.

If in addition $M \mid K$ is simple, generated by a, with b similarly generating $M_o \mid K$, then the radical N of A has a particularly simple form. Since b may be considered as a canonical generator of Pickert, a basis for the radical of B

is formed as follows. Let $a^{q_1} = b^{q_1} = k \in K$ with $q_1' = 1$. Now $w_1' = b - g_1$ for $g_1 \in M$ (for notation see Chapter II), and since $a^{q_1'} = g_1$, $a = g_1$ so $w_1' = b - a = w_1 \neq 0$. Thus the radical N_1 of B will have a basis consisting of powers of $(b - a)$ from one up to one less than the index r of $(b - a)$. Now $(b - a)^{q_1} = k - k = 0$ so $r \leqslant q_1$. But $B = M_\circ + N_1$ as algebras over $M_\circ$ so $[N_1 \mid M_\circ] = [B \mid M_\circ] - [M_\circ / M_\circ] = q_1 - 1$ and thus all powers of $(b - a)$ from one to $q_1 - 1$ must be used as a basis. This implies that $N_1 = \sum_{\circ < i < q_1} M_\circ \cdot (b - a)^i$, and from the previous discussion the radical $N = \sum_{\circ < i < q_1} L_\circ \cdot (b-a)^i$.

One result of the above is that the index of N is q_1, and this fact is used in the following theorem.

Theorem 1. If $L \supseteq M \supseteq K$ and $L \mid K$ is simple, then $A = L \times_K M$ cleaves over M if and only if $M = K$ or $M = L$.

Proof. If $M = K$ then $L \times_K M$ is the field L, while if $M = L$ it is clear by Theorem 2, Chapter II that cleavage occurs. So assume $L \supsetneq M \supsetneq K$. Pickert (5) proves that for $L_\circ \mid K$ simple with $L_\circ = K(b)$, every inbetween field can be written as $K(b^{p^{e-f}})$, where $b^{p^e} = k \in K$ for smallest e and $0 \leqslant f \leqslant e$. For $L_\circ \supseteq M_\circ \supseteq K$, $M_\circ$ can be written as $K(b^{p^{e-f}})$ for $0 < f < e$. If $A \mid M$ cleaves there exists a field $S \supseteq M$ such that $S \cong L$ as algebras over M which means in particular that the elements of K are invariant. Under this isomorphism

let a in S correspond to b in L_o, and thus $a^{p^e} = b^{p^e} = k \in K$. Consider the element $\alpha = (b - a)$; since $\alpha^{p^e} = k - k = 0$ then $\alpha \in N$ so let r be the index of α. Now $\alpha^{p^{e-1}} = b^{p^{e-1}} - a^{p^{e-1}} \neq 0$ since $b^{p^{e-1}} \in (M_o - K)$, $a^{p^{e-1}} \in (M - K)$ and $M_o \cap M = K$. Thus $p^{e-1} < r \leqslant p^f$ since $p^f = q_1$ is the index of N and this implies $e - 1 < f$ or $e \leqslant f$. But $f < e$ by a previous consideration so a contradiction results and A | M does not cleave. This proves the theorem.

A next case in the order of difficulty is to consider $L \supseteq M \supseteq K$ with L | K having a multiplicity of two. Here it is convenient to have M | K of multiplicity one with M a canonical inbetween field of Pickert's form. With M there will be associated a unique set $q_1 = p^{e_1}$, $q_2 = p^{e_2}$ of integers as well as a canonical polynomial (not necessarily unique) $f(x) = \sum_{o \leqslant i \leqslant N} k_i x^i$ with $k_i \in K$ and $N < (q_1/q_2)$. For $M_o = K(b_1)$, $L_o = M(b_2)$ such that $b_1^{q_1} = k \in K$ and $b_2^{q_2} = f(b_1^{q_2})$, the following theorem will give a criterion for the cleavage of $L X_K M$.

Theorem 2. If $L \supseteq M \supseteq K$, L | K has multiplicity two, M | K has multiplicity one with M canonical inbetween L and K with canonical polynomial $f(x) = \sum_{o \leqslant i \leqslant N} k_i x^i$, then $A = L X_K M$ cleaves over M if and only if k_i^{1/q_2} exist in L for i = 0, 1, ..., N.

Proof. If A | M cleaves then there exists an $a_2 \in A$ such that $a_2^{q_2} = f(a_1^{q_2})$, where a_1 in M corresponds to b_1 in $M_o \subseteq L_o$. Considering A as an algebra over L_o, $A = \sum_{o \le i < q_1} L_o \cdot a_1^i$ so $a_2 = \sum_{o \le i < q_1} h_i a_1^i$ for $h_i \in L_o$. Then $a_2^{q_2} = \sum_{o \le i < q_1} h_i^{q_2} a_1^{iq_2} = \sum_{o \le i \le N} k_j a_1^{jp^2}$. Using the well known algorithm $i q_2 = q_1 s_i + r_i$ for $0 \le r_i < q_1$ and for $i = 1, 2, \ldots, N$. So $a_1^{iq_2} = a_1^{r_i} a_1^{q_1 s_i} = k^{s_i} a_1^{r_i} = b_1^{q_1 s_i} a_1^{r_i} = \left[b_1^{s_i \frac{q_1}{q_2}}\right]^{q_2} a_1^{r_i}$, where $\left[b_1^{s_i \frac{q_1}{q_2}}\right] = d_i$ in L_o. Thus $\sum_{o \le i < q_1} h_i^{q_2} a_1^{iq_2} = \sum_{o \le j \le M} d_j a_1^{jq_2}$, with $M < (q_1/q_2)$ since $r_i = iq_2 - q_1 s_i = q_2(i - \frac{q_1}{q_2} s_i) = jq_2$. By uniqueness of the representation of $a_2^{q_2}$ by the basis $\{a_1^i\}_o^{q_1-1}$, $k_j = d_j^{q_2}$ for $j = 0, 1, \ldots, M = N$.

Conversely assume $k_j = d_j^{q_2}$ for $j = 0, 1, \ldots, N$ and $d_j \in L_o$. Construct $\sum_{o \le j \le N} d_j^{q_2} a_1^{jq_2} = \left[\sum_{o \le j \le N} d_j a_1^j\right]^{q_2} = \sum_{o \le j \le N} k_j a_1^{jq_2} = f(a_1^{q_2})$ so there exists an $a_2 = \sum_{o \le j \le N} d_j a_1^j$ such that $a_2^{q_2} = f(a_1^{q_2})$ which implies that there exists an $S \subseteq A$ such that $S \cong L$ as algebras over M, so A | M cleaves and the theorem is proved.

Corollary. If $L \supseteq M \supseteq K$, L | K has multiplicity two, and M | K has multiplicity one with M canonical inbetween L and K, then $L X_K M$ cleaves over M if K has a degree of imperfection of two.

Proof. Pickert's (5) Theorem 19 on page 94 states that if the degree of imperfection of the base field K equals the multiplicity m of the field extension L, then all q_mth roots of elements in K are found in L. In particular each k_j of the canonical polynomial would have a q_2th root in L and so L X_K M cleaves over M by Theorem 2.

The above method of proof can be applied to a slightly more general problem. Let $L \supseteq M \supseteq K$ with L | K having multiplicity m while M is canonical between L and K with M | K of multiplicity m - 1. If in addition $q_1 = q_2 = \cdots = q_{m-1}$ with $L_o = M(b_m)$ such that $b_m^{q_m} = f_m(b_1^{q_m}, b_2^{q_m}, \ldots, b_{m-1}^{q_m})$, then L X_K M cleaves over M if and only if the coefficients of the polynomial $f_m(x_1, x_2, \ldots, x_{m-1})$, which are in K, have q_mth roots in L_o (or equivalently in L).

A corollary similar to the one above can also be stated in this case. That is, a sufficient condition for cleavage is obtained when the multiplicity of L | K is equal to the degree of imperfection of K.

V. THE GENERAL CASE

Returning to the case of M | K arbitrary, a general theorem for cleavage can be obtained using the multiplication tables of L M | M and L | K for any particular pair of bases they may have. The following notation will be used: let $\{a_i\}_i$ be a basis for L | K with $\{b_i\}_i$ the corresponding one for L_o | K, both having the multiplication table $\{\alpha_{ij}^{k}\}_{ijk}$ so that $a_i\, a_j = \sum_K \alpha_{ij}^{k}\, a_k \;|_{ij}$ and $b_i\, b_j = \sum_K \alpha_{ij}^{k}\, b_k \;|_{ij}$. The subscripts $\{\}_i$, $\{\}_{ijk}$, $\sum_K$, $|_{ij}$ all take on values of an index set having as its cardinal number the dimension of L | K. In contradistinction superscripts such as $\{\}^i$, $\sum^K$, $|^{ij}$ will take on values of an index set having as its cardinal number the dimension of L M | M. The symbol $|_j^i$ following an equation will in particular mean that i in the equation takes on values from one index set and j takes on values from the other one. Thus $\{c_i\}^i$ will be a basis for L M | M with multiplication table $\{\beta_{ij}^{k}\}^{ijk}$. It is clear that $\alpha_{ij}^{k} \in K$ and $\beta_{ij}^{k} \in M$. The following theorem will use the above notation.

Theorem 1. $A = L X_K M$ cleaves over M if and only if there exists a set $\{m_{ij}\}_j^i$ of elements in M satisfying the equations $\sum_{st} m_{is}\, m_{jt}\, \alpha_{st}^{v} = \sum^K \beta_{ij}^{k}\, m_{kv} \;|_v^{ij}$.

Proof. The cleavage will depend upon being able to build an algebra $S \subseteq A$ isomorphic over M to L M. This is equivalent

to finding a set $\{c_i'\}^i$ of elements in A such that $c_i' c_j' = \sum^K \beta_{ij}^k c_k' \;|^{ij}$. Supposing that such c_i' exist and considering A as an algebra over M (i.e. $A = \sum_i M \cdot b_i$), $c_i' = \sum_s m_{is} b_s \;|^i$ so $(\sum_s m_{is} b_s)(\sum_t m_{jt} b_t) = \sum_{st} m_{is} m_{jt} b_s b_t = \sum^K \beta_{ij}^k c_k' = \sum_v^K \beta_{ij}^k m_{kv} b_v \;|^{ij}$. Also $\sum_{s+v} m_{is} m_{jt} \alpha_{st}^v b_v = \sum_v^K \beta_{ij}^k m_{kv} b_v \;|^{ij}$ so $\sum_{st} m_{is} m_{jt} \alpha_{st}^v = \sum^K \beta_{ij}^k m_{kv} \;|_v^{ij}$.

Conversely suppose there exist $\{m_{ij}\}_j^i$ satisfying the last above equations, then the steps may be reversed back giving the existence of $c_i' = \sum_s m_{is} b_s$ having $\{\beta_{ij}^k\}^{ijk}$ as multiplication table over M thus proving the theorem. It should be noted that the above criterion is in terms of only the structures of L | K, L M | M and M.

In Chapter IV there are obvious examples of the algebra $A = L X_K M$ which do not cleave over M. Since cleavage over K (it is here assumed that M is also finite pure inseparable over K) is less restrictive it may be asked if there are any cases of A which do not cleave over K. As a preliminary to an example which will show that such cases do exist, the following lemma will be proved.

Lemma 1. In all cases for $A = L X_K M$, $A^p \cap K \subseteq (L M)^p \cap K$, and if A | K cleaves then $A^p \cap K = (L M)^p \cap K$.

Proof. In the usual homomorphism of A onto L M, it is clear that A^p maps onto $(L\,M)^p$. Those elements of A which are in M are invariant under the homomorphism and thus the elements of K are also invariant. These results imply that $A^p \cap K \subseteq (L\,M)^p \cap K$. If now $A \mid K$ cleaves there exists an $S \supseteq K$ such that $S \cong L\,M$ as algebras over K. Since S and L M both have K in common it is clear that an element $k \in K$ which is the pth power of an element in L M will also be a pth power of an element in $S \subseteq A$. Thus $A^p \cap K \supseteq (L\,M)^p \cap K$ and so $A^p \cap K = (L\,M)^p \cap K$.

For the example let P be a prime field of prime characteristic p, and let s and t be independent indeterminates over P. Define $K = P(s, t)$, $L = K(a)$, $M = K(c)$, where $a^{p^2} = s$ and $c^{p^2} = s\,t^p$ so $a^p = s^{1/p}$ and $c^p = s^{1/p}t$. Now $K(a^p) = K(s^{1/p})$ and $K(c^p) = K(s^{1/p}t) = K(s^{1/p})$. Also $L\,M = M(a) = K(a, c) = K(s^{1/p^2}, s^{1/p^2}\,t^{1/p}) = K(s^{1/p^2}, t^{1/p})$. Thus $(L\,M)^p = K^p(s^{1/p}, t) = P^p(s^p, t^p)(s^{1/p}, t)$, where the latter notation means that s^p and t^p give transcendental extensions to P^p while $s^{1/p}$ and t give algebraic ones to the field $P^p(s^p, t^p)$. Now $P^p = P$ as it is a Galois Field and thus perfect. Also $P(s^p, t^p)(s^{1/p}, t)$ contains the integral domain $P[s, t]$ and hence its quotient field $P(s, t) = K$. Thus $(L\,M)^p \supseteq K$ so $(L\,M)^p \cap K = K$.

In the algebra $A = L \times_K M$ let $L_o = K(b)$, where $b^{p^2} = s$

and b^p is one pth root of s in A. The single pth root of s in L M is denoted by $s^{1/p}$. A as an algebra over M can be written $A = \sum_{0 \le i < p^2} M \cdot b^i$ so $A^p = \sum_{0 \le i < p^2} M^p \cdot b^{ip}$, where in the last expression the powers of b indicated are not necessarily a basis for $A^p \mid M^p$. Now $M^p = K^p (c^p) = P (s^p, t^p) (s^{1/p} t)$ so $(t^p)^{-1}$ and $s\, t^p$ are in M^p which implies that $s \in M^p$. Since $b^{p^2} = s \in M^p$ for the smallest power of b, $A^p = \sum_{0 \le i < p} M^p \cdot b^{ip}$, where the powers of b indicated here do form a basis for $A^p \mid M^p$. If t is assumed to be in A^p it must be in M^p for otherwise it would have two distinct representations in A using the basis $\{b^i\}_0^{p^2-1}$. Since $M^p = P (s^p, t^p) (s^{1/p} t)$, the assumption of $t \in M^p$ implies also that $s^{1/p} \in M^p$, and thus $s \in M^p$. This gives $K \subseteq M^p$ and so the pth roots of all elements in K are in M. But by Theorem 19 on page 94 of Pickert (5), only when the multiplicity of the field extension equals the degree of imperfection of the base field does the extension contain all pth roots of the base field. In the present case the multiplicity of $M \mid K$ is one while the degree of imperfection of K is clearly two. This contradiction shows that t cannot be in A^p so $A^p \cap K \subsetneq K$. Thus $A^p \cap K \neq (L\, M)^p \cap K$ and by Lemma 1 A does not cleave over K.

VI. EXTERNAL CRITERIA

It is desirable in the present problem to obtain conditions for the cleavage of $A = L X_K M$ in terms of the properties of L, M, and L M. It is also quite natural in such an investigation that conditions for cleavage will become apparent which are in terms of other properties of the algebra itself. Some of these conditions, which have been termed external, will be brought out in the following theorems.

Theorem 1. If $A = L X_K M$ and $L \supseteq M \supseteq K$, then $A \mid M$ cleaves if and only if there exists a ring endomorphism of A which is an extension of the natural isomorphism $M_o \underset{K}{\overset{-\varphi\rightarrow}{\cong}} M$, where M_o is the image of M in $L_o = L X_K 1$.

Proof. If such an endomorphism exists, the L_o has a homomorphic image L' containing M. Since $M \neq 0$ the homomorphism is an isomorphism and so $L' \cong L M = L$ as algebras over M. Thus $A \mid M$ cleaves.

Conversely if $A \mid M$ cleaves there exists an $L' \supseteq M$ such that $L' \cong L$ as algebras over M. This implies in particular that the elements of K are invariant under the isomorphism so there exists the following isomorphism $L_o \underset{K}{\overset{-\varphi\rightarrow}{\cong}} L'$ which is clearly an extension of $M_o \underset{K}{\overset{-\varphi\rightarrow}{\cong}} M$. In the following notation the conventions of Chapter V regarding subscripts, etc., will be used. Let $\{b_i\}_i$ be a basis for $L_o \mid K$ with the subset $\{b_j\}_j$ a basis

for $M_o \mid K$ having the multiplication table $\{\kappa^{stv}_{st}\}$ such that $b_i\, b_j = \sum^{s} \kappa^{s}_{ij}\, b_s \mid^{ij}$. Similarly let $\{a_i\}^i$ and $\{a_j\}_j$ be the corresponding bases for $L' \mid K$ and $M \mid K$ respectively with the same multiplication table. Considering A as an algebra over K, $A = \sum_i^j K \cdot a_i\, b_j$, which suggests the single valued mapping $x = \sum_i^j k_{ij}\, a_i\, b_j \xrightarrow{\theta} \sum_i^j k_{ij}\, a_j\, b_i$ of A onto $A' = \sum_i^j K \cdot a_j\, b_i$. The procedure is now to show that θ is an endomorphism. Let $x = \sum_i^j k_{ij}\, a_i\, b_j$ and $y = \sum_i^j k'_{ij}\, a_i\, b_j$ be two arbitrary elements in A with images x' and y' respectively under the mapping θ.

$$(x + y)' = \sum_i^j (k_{ij} + k'_{ij})\, a_j\, b_i = x' + y' \ .$$

Also

$$(xy)' = \left[\sum_{is}^{jt} k_{ij}\, k'_{st}\ a_i\, a_s\, b_j\, b_t\right]' =$$

$$\left[\sum_{isu}^{jtv} k_{ij}\, k'_{st}\, \kappa^{u}_{is}\, \kappa^{v}_{jt}\, a_u\, b_v\right]' \ ,$$

while

$$x'\, y' = \sum_{is}^{jt} k_{ij}\, k'_{st}\, a_j\, a_t\, b_i\, b_s \quad =$$

$$\sum_{isu}^{jtv} k_{ij}\, k'_{st}\, \kappa^{u}_{is}\ \kappa^{v}_{jt}\, a_v\, b_u \quad = (x\, y)' \ .$$

To see that the endomorphism θ is an extension of ψ, assume $a_1 = b_1 = 1$ and consider for arbitrary $h \in L_o$, $h = \sum_i k_{1i}\, b_i \xrightarrow{\theta} \sum_i k_{1i}\, a_i = h' \in L'$. Thus the theorem is proved.

There are certain symmetries in the above development, such as $L_o \cap M = K$ and $L' \cap M_o = K$, which suggest that in some cases θ may be an automorphism. This possibility will be pursued a bit further here. Let R be the kernel of θ so $A/R \cong A'$ as algebras over K. If $\sum_i^j k_{ij}\, a_j\, b_i = 0$ is any representation of zero in A' and $a_j = b_j + n_j \; /^j$ for $n_j \in N$, the radical of A, then on substituting $\sum_i^j k_{ij}\, (b_j + n_j)$ $(a_i - n_i) = \sum_i^j k_{ij}\, a_i\, b_j - n = 0$, for $n \in N$ so $\sum_i^j k_{ij}\, a_i\, b_j \in N$ and $R \subseteq N$. R is thus a nilpotent ideal of A which must be properly contained in N (if $N \neq 0$) since $A/N \cong L$, $A/R \cong A'$, and A' contains nilpotent elements (e.g. $b_2 - a_2$). If $R = 0$ then θ is an automorphism, otherwise it is not. In any case, since θ maps M_o onto M and M onto M_o, there exists a sequence of overfields of both M_o and M which are isomorphic to L. This sequence may or may not terminate.

A p-basis for a field F, having prime characteristic p, is constructed by transfinite induction as follows: well order the elements in $F - F^p$ and let the set P contain the first element and each element in turn which cannot be expressed as a polynomial in the previously chosen ones with coefficients in F^p. It is then clear that $F = F^p\,(P)$, and for any finite subset $\{a_i\}_1^n$ of P the relation $\left[F^p\,(a_1, a_2, \ldots, a_n) \mid F^p\right] = p^n$ holds.

Consider a ring R of prime characteristic p having radical

N such that $\overline{R} = R/N$ is a field. Also let $N^{p^e} = 0$ for some natural number e . Narita (6) has shown that R contains a field $S \cong \overline{R}$ such that $\overline{S} = \overline{R}$. The field $S = R^{p^e}(D)$, where $\overline{D}$ is a p-basis for $\overline{R}$. The above results will be used to prove the following theorem.

Theorem 2. Let $A = L \underset{K}{X} M$ and let M be finite pure inseparable over K such that $(L\ M)^{p^e} \subseteq K$, then $A \mid K$ cleaves if and only if $A^{p^i} \cap K = (L\ M)^{p^i} \cap K$ for i = 1, 2, ..., e-1.

Proof. Reasoning exactly as in the proof of Lemma 1, Chapter V the condition is clearly necessary. To prove sufficiency the procedure is as follows. Let F = L M and $G_i = \left\{ x \in (F - F^p) \mid x^{p^i} \in K,\ x^{p^{i-1}} \notin K \right\}$ for i = 0, 1, ..., e. Thus the collection of sets $\{G_i\}_o^e$ is a partitioning of $F - F^p$ into disjoint sets. Any p-basis of F must be chosen from among the elements of $F - F^p = \bigcup_{i=0}^{e} G_i$. These elements may be well ordered such that all elements in G_i precede all those of G_j for $i < j$. Now a set D, algebraically independent over F^{p^e}, may be chosen as before by transfinite induction under the present ordering. D has the natural partitioning into $D_i \subseteq G_i$ so that $D = \bigcup_{i=0}^{e} D_i$. Thus $F = F^{p^e}(D)$ since D contains a p-basis D_o of F. If $D \supsetneq D_o$, then since $F = F^{p^e}(D_o)$, there exists a non zero $d \in (D - D_o)$ which is a polynomial in elements of D with coefficients in F^{p^e}. But this contradicts the algebraic independence of D over F^{p^e}, so $D = D_o$. It is

also clear that $G_i \subseteq F^{p^e}(D_o, D_1, \ldots, D_i)$.

Now since every $k \in (K - F^{p^e})$ equals a^{p^i} for some $a \in (F - F^p)$ with $o \leqslant i < e$, k is in $\left[F^{p^e}(D_o, D_1, \ldots, D_i)\right]^{p^i}$ $\subseteq F^{p^e}(D_o^{p^i}, D_1^{p^i}, \ldots, D_i^{p^i})$. But $D_j^{p^i} \subseteq K$ for $j = 0, 1, \ldots, i$ so that every k in $(K - F^{p^e})$ is expressible as a polynomial in elements of K, as powers of p-basis elements, with coefficients in F^{p^e}. Now let $\overline{D}_A$ be the p-basis of $\overline{A}$ corresponding to the p-basis D of F. D_A will then denote a collection of representatives in A, with exactly one coming from each equivalence class of $\overline{D}_A$. Consider any $k \in (K - F^{p^e})$, so that $k = f^{p^e}(d_o^{p^i}, d_1^{p^i}, \ldots, d_i^{p^i})$ as a polynomial in $d_i \in D_i$ with coefficients in F^{p^e}. In general of course there will be more than one distinct d_i from D_i, but the above notation is sufficient to illustrate the method. Each d_i has an image d_{Ai} in A such that $d_i^{p^i} = d_{Ai}^{p^i} + n_i$ for $n_i \in N$. By the hypothesis, $A^{p^i} \cap K = F^{p^i} \cap K$, so that $d_i^{p^i} = d_{Ai}'^{p^i}$ for $d_{Ai}' \in A$. Thus $d_A'^{p^i}_i = d_{Ai}^{p'} + n_i$, which implies that $d_{Ai}' = d_{Ai} + n_i'$ for $n_i' \in N$. Therefore d_{Ai} can be replaced in D_A by d_{Ai}' such that $d_{Ai}'^{p^i} = d_i^{p^i}$ for all d_i in D. It is then clear that $A^{p^e}(D_A)$ will generate K, so there exists an image $A^{p^e}(D_A)$ of the composite over K. Thus A / K cleaves and this completes the proof of the theorem.

VII. REFERENCES

1. Albert, A. A. Structure of algebras. Amer. Math. Soc. Colloquium Publications 24: 47. 1939.

2. Vinograde, B. Cleft rings. Trans. Amer. Math. Soc. 56: 494-507. 1944.

3. Bryant, S. J. and Zemmer, J. L. A note on completely primary rings. Proc. Amer. Math. Soc. 8: 140-141. 1957.

4. Becker, M. F. and Mac Lane, S. The minimum number of generators for inseparable algebraic extensions. Bull. Amer. Math. Soc. 46: 182-186. 1940.

5. Pickert, G. Inseparable körpererweiterungen. Math. Zeit. 52: 81-136. 1949.

6. Narita, M. On the structure of complete local rings. J. Math. Soc. Japan 7: 435-443. 1955.

VIII. ACKNOWLEDGMENT

I wish to express my gratitude to Dr. Vinograde for introducing me to the present problem as well as for his continuous help and guidance in the preparation of this thesis.