THE FOUNDATIONS FOR AN EXTENSION OF DIFFERENTIAL ALGEBRA(1)

BY
H. F. KREIMER

1. **Introduction.** A differential ring may be regarded as a ring with a self-representation(2), the derivation being derived from the representation. A difference ring and a ring with a higher derivation may also be so regarded. In §2, a class of algebras is defined and an M-system of mappings of a ring R into a ring S is derived from a representation of R into one of these algebras over S. Extensions of M-systems of mappings are considered in §3. M-rings are defined and studied in §4. Among the examples of M-rings are mixed differential-difference rings with operators which need not commute. In §5, the question of compatibility of extensions of M-rings is treated.

2. **A generalization of the notion of a derivation.** In the sequel, ring will mean commutative ring with identity element, subring will mean subring containing the identity element, module will mean unital module, and homomorphism of one ring into another will mean homomorphism mapping the identity element of the one ring onto the identity element of the other. Let C be an associative, commutative coalgebra with identity over a ring W, which is freely generated as a W-module. If M is a basis for C over W, the set of elements of $C \otimes_w C$ of the form $m \otimes n$, m and n in M, is a basis for $C \otimes_W C$ over W. If μ is the coproduct mapping of C into $C \otimes_W C$ and $m \in M$, then $m\mu = \sum_{n,p \in M} z_{mnp}\ n \otimes p$, where $z_{mnp} \in W$, $z_{mnp} = 0$ except for a finite number of elements n and p in M, and z_{mnp} is uniquely determined by the triple (m, n, p) of elements of M. The requirements that C be an associative, commutative coalgebra with identity over W are equivalent to the requirements that $\sum_{n \in M} z_{mnp}\, z_{nqr} = \sum_{n \in M} z_{mqn}\, z_{nrp}$, $z_{mnp} = z_{mpn}$, and there is an element e of $C^* = \mathrm{Hom}_W(C, W)$ such that

$$\sum_{n \in M} z_{mnp} e(n) = \delta_{mp} = \begin{cases} 1, & m = p, \\ 0, & m \neq p. \end{cases}$$

The mapping $C^* \otimes_W C^* \xrightarrow{v} \mathrm{Hom}_W(C \otimes_W C, W) \xrightarrow{\mu^*} \mathrm{Hom}_W(C, W) = C^*$, where μ^* is the transpose of μ and v is the canonical homomorphism of $C^* \otimes_W C^*$ into

Presented to the Society, June 4, 1962; received by the editors January 28, 1963.

(1) Part of a dissertation presented for the degree of Doctor of Philosophy at Yale University.

(2) Cf. N. Jacobson, *An extension of Galois theory to non-normal and non-separable fields*, Amer. J. Math. **66** (1944), 1–29.

$\mathrm{Hom}_W(C \otimes_W C, W)$, determines a multiplication in C^*, with respect to which C^* is an associative, commutative algebra over W and e is an identity element in C^*.

Let a homomorphism $w \to \bar{w}$ of W into a ring S be given. S is a W-module with respect to the operation $w \cdot s = \bar{w}s$; the S-module $C^S = S \otimes_W C$ obtained from the W-module C by inverse transfer of the basic ring to S is an associative, commutative coalgebra with identity over S, with respect to the coproduct mapping $\mu^S = I \otimes \mu$ of $C^S = S \otimes_W C$ into $S \otimes_W C \otimes_W C \cong (S \otimes_W C) \otimes_S (S \otimes_W C) = C^S \otimes_S C^S$; and M is a basis for C^S over S with each element m of M identified with the element $1 \otimes m$ of $C^S = S \otimes_W C$. If ρ is a homomorphism of a ring R into $(C^S)^*$, then for each $m \in M$ there is a mapping $a \to a^\rho(m)$ of R into S, which will also be denoted by m, and the set of these mappings will be called an M-system of mappings of R into S. If a, $b \in R$ and $m \in M$, then $(a + b)m = (a + b)^\rho(m) = (a^\rho + b^\rho)(m) = am + bm$, and $(ab)m = (ab)^\rho(m) = (a^\rho b^\rho)(m) = (a^\rho \otimes b^\rho) \ (\sum_{n,p \in M} \overline{z_{mnp}}\, n \otimes p) = \sum_{n,p \in M} \overline{z_{mnp}} \ (an)(bp)$. The mappings are determined by the representation ρ of R in $(C^S)^*$; the type of the M-system of mappings is determined by the "coefficients" z_{mnp} or, equivalently, by the coalgebra C and its basis M.

(2.1) Example. Let $W = Z$, the ring of integers; let N be a positive integer; let $M = \{D_i \mid i \in Z \text{ and } 0 \leqq i \leqq N\}$; and let $z_{D_i D_j D_k} = \delta_{i,j+k}$. Then an M-system of mappings of R into S consists of a homomorphism D_0 and a higher D_0-derivation of rank N from R into S. Moreover, every higher D_0-derivation of rank N from R into S can be obtained as such an M-system of mappings. If $N = 0$, M consists only of the homomorphism D_0; and if $N = 1$, M consists of the homomorphism D_0 and a D_0-derivation D_1 of R into S. A higher derivation of rank N, in the usual sense, is obtained if R is a subring of S and D_0 is the identity mapping of R into S.

(2.2) Example. Let $W = Z$, let $M = \{D_i \mid i \in Z \text{ and } i \geqq 0\}$, and let $z_{D_i D_j D_k} = \delta_{i,j+k}$. Then an M-system of mappings of R into S consists of a homomorphism D_0 and an infinite higher D_0-derivation of R into S. Moreover, every infinite higher D_0-derivation of R into S can be obtained as such an M-system of mappings. An infinite higher derivation, in the usual sense, is obtained if R is a subring of S and D_0 is the identity mapping of R into S. An infinite higher derivation of R into R is called iterative if $(aD_i)D_j = \binom{i+j}{i}(aD_{i+j})$ for any $a \in R$ and positive $i, j \in Z$.

(2.3) Example. Let $W = Z$, let $M = \{F_1, F_2\}$, and let

$$z_{F_i F_j F_k} = (-1)^i \sin \tfrac{1}{2}(i + j + k)\pi.$$

If Q is the field of rational numbers and $R = Q(\sqrt[3]{2}) = S$, an M-system of mappings of R into S is given by

$$(a + b\sqrt[3]{2} + c\sqrt[3]{4})F_1 = a - c\sqrt[3]{4}$$

and

$$(a + b\sqrt[3]{2} + c\sqrt[3]{4})F_2 = b\sqrt[3]{2} - c\sqrt[3]{4}.$$

Since there are no nontrivial automorphisms, derivations, or higher derivations on $Q(\sqrt[3]{2})$, this M-system of mappings of R into S is not only of different type from the previous examples, but these mappings on $Q(\sqrt[3]{2})$ cannot be algebraic combinations over $Q(\sqrt[3]{2})$ of automorphisms, derivations, and higher derivations.

3. **Extensions of M-systems of mappings.** Let an M-system of mappings of a ring R into a ring S be determined by a representation ρ of R into $(C^S)^*$. Given a homomorphism of S into a ring T, let $C^T = (C^S)^T$ be the coalgebra over T obtained from C^S by inverse transfer of the basic ring to T. The mapping $R \xrightarrow{\rho} (C^S)^* \xrightarrow{\psi} (C^T)^*$, where ψ is the canonical homomorphism of $(C^S)^*$ into $(C^T)^*$, is a homomorphism of R into $(C^T)^*$ and determines an M-system of mappings of R into T, which will be said to be deduced from the M-system of mappings of R into S by inverse transfer of the ring S to T.

Now suppose η is a homomorphism of the ring R onto a ring Q with kernel I. If I is contained in the kernel of the representation ρ, then there is an induced homomorphism $\bar{\rho}$ of Q into $(C^S)^*$. Consequently, an M-system of mappings of Q into S is induced by the M-system of mappings of R into S. Finally, suppose Q is a ring which is an extension of R. If the representation ρ of R into $(C^S)^*$ can be extended to a homomorphism of Q into $(C^S)^*$, then the M-system of mappings of R into S is extended to an M-system of mappings of Q into S.

Let $\{x_\alpha \mid \alpha \in A\}$ be a set of elements algebraically independent over R, let $Q = R[x_\alpha]$ be the ring of polynomials over R in the x_α, $\alpha \in A$, and let $\{s_{\alpha,m} \mid \alpha \in A$ and $m \in M\}$ be a set of elements of S. A homomorphism ρ of R into $(C^S)^*$ can be extended to a homomorphism $\bar{\rho}$ of Q into $(C^S)^*$, such that $x_\alpha^{\bar{\rho}}(m) = s_{\alpha,m}$, $\alpha \in A$ and $m \in M$; thus, an M-system of mappings of R into S can be extended to an M-system of mappings of $Q = R[x_\alpha]$ into S, such that $x_\alpha m = s_{\alpha,m}$, $\alpha \in A$ and $m \in M$.

Let N be a set of elements of R which are not zero divisors in R, and let Q be the ring of quotients of R relative to N. A homomorphism ρ of R into $(C^S)^*$ can be extended to a homomorphism of Q into $(C^S)^*$ and, consequently, an M-system of mappings of R into S can be extended to an M-system of mappings of Q into S if, and only if, a^ρ is a unit in $(C^S)^*$ for every $a \in N$. Furthermore, when such an extension exists, it is unique. An equivalent condition can be obtained. If $f, g \in (C^S)^*$,

$$(f \cdot g)(m) = (f \otimes g) \sum_{n,p \in M} \overline{z_{mnp}}\, n \otimes p = \sum_{n,p \in M} \overline{z_{mnp}} f(n) \cdot g(p) = g\Big(\sum_{n,p \in M} \overline{z_{mnp}} f(n) \cdot p\Big).$$

Therefore, under the regular representation of the algebra $(C^S)^*$, an element f of $(C^S)^*$ is represented by the transpose of the endomorphism of the S-module C^S which is described with respect to the basis M by the row finite $M \times M$

matrix $(\sum_{n\in M}\overline{z_{mnp}}f(n))_{m,p\in M}$. It is readily verified that the mapping $\sigma: f\to(\sum_{n\in M}\overline{z_{mnp}}f(n))_{m,p\in M}$ is an isomorphism of $(C^S)^*$ into the ring S_M of row finite $M\times M$ matrices over S. If f is a unit in $(C^S)^*$, then f^σ is a unit in S_M, and, conversely, if f^σ is a unit in S_M, then f is a unit in $(C^S)^*$ and its inverse is the image of the identity element e of $(C^S)^*$ under the transpose of the endomorphism of C^S described with respect to M by the matrix $(f^\sigma)^{-1}$. Therefore, an M-system of mappings of R into S can be extended to an M-system of mappings of Q into S if, and only if, $a^{\rho\sigma}=(\sum_{n\in M}\overline{z_{mnp}}(an))_{m,p\in M}$ is a unit in S_M for every $a\in N$.

Still letting N, Q, R, and S be as in the preceding paragraph, reconsider Examples (2.1) and (2.2). In Example (2.1), the $M\times M$ matrix $(\sum_{n\in M}\overline{z_{mnp}}(an))_{m,p\in M}$ is a triangular $(N+1)\times(N+1)$ matrix with entries on the main diagonal equal to aD_0, which is a unit in the ring of $(N+1)\times(N+1)$ matrices over S if, and only if, aD_0 is a unit in S. Therefore, this M-system of mappings of R into S can be extended to an M-system of mappings of Q into S if, and only if, aD_0 is a unit in S for every $a\in N$. Moreover any such extension is unique. As a special consequence, if Q is a subring of S, then for any higher derivation of rank N from R into S there is a unique extension to a higher derivation of rank N from Q into S.

For Example (2.2) it will be useful to investigate the algebra $(C^S)^*$ and the representation ρ of R into $(C^S)^*$. Let x be the element of $(C^S)^*$ such that $x(D_i)=\delta_{1,i}$. Then it can be shown that $x^j(D_i)=\delta_{j,i}$. Thus x is transcendental over S, $(C^S)^*$ is isomorphic to the ring of formal power series over S in x, and $a^\rho=\sum_{j=0}^\infty(aD_j)x^j$, $a\in R$. $\sum_{j=0}^\infty s_jx^j$ is a unit in $(C^S)^*$ if, and only if, s_0 is a unit in S. Therefore this M-system of mappings of R into S can be extended to an M-system of mappings of Q into S if, and only if, aD_0 is a unit in S for every $a\in N$. Moreover, any such extension is unique. If Q is a subring of S, then for any infinite higher derivation of R into S there is a unique extension to an infinite higher derivation of Q into S. Let an iterative infinite higher derivation of R into R be given; extend the infinite higher derivation of R into Q, deduced from the higher derivation of R into R by inverse transfer of the ring R to Q, to an infinite higher derivation of Q into Q; and let ρ be the corresponding representation of Q into $(C^Q)^*$. Both of the rules $(q^\rho)D_i=(qD_i)^\rho=\sum_{j=0}^\infty((qD_i)D_j)x^j$ and $(q^\rho)D_i=\sum_{j=0}^\infty\binom{i+j}{i}(qD_{i+j})x^j$, $i=1,2,3,\cdots$, determine infinite higher derivations of Q^ρ into $(C^Q)^*$ which coincide on R^ρ. Since Q^ρ is the ring of quotients of R^ρ with respect to the set N^ρ, both rules must define the same higher derivation of Q^ρ into $(C^Q)^*$. Therefore, $(qD_i)D_j=\binom{i+j}{i}(qD_{i+j})$ for any $q\in Q$ and $i,j=1,2,3,\cdots$, and the extension of an iterative infinite higher derivation of R into R to an infinite higher derivation of Q into Q is again iterative.

4. ***M*-rings.** An M-ring is a system consisting of a ring R and an M-system of mappings of R into R. An M-domain is an M-ring R in which R is an integral domain, and an M-field is an M-ring R in which R is a field.

A partial differential ring R is an M-ring in which the M-system of mappings consists of the identity automorphism and derivations which commute with each other in their action on R. The ordinary differential ring is the special case in which there is just one derivation. The ring of all complex valued functions holomorphic throughout a given region of the complex plane, with ordinary differentiation as the derivation, is a differential ring. Rings with higher derivations of rank greater than one may also be considered, and an M-ring in which the M-system of mappings consists of the identity automorphism and higher derivations will be called a ring of differential type.

A partial difference ring R is an M-ring in which the M-system of mappings consists of homomorphisms of R into R which commute with each other in their action on R. The ordinary difference ring is the special case in which there is just one homomorphism. The ring of all real valued functions defined on the real line, with the transformation $f(x) \to f(x+1)$ as the homomorphism, is a difference ring. An M-ring in which the M-system of mappings consists of homomorphisms will be called a ring of difference type. More generally, rings of mixed difference-differential type may be considered; nor do these exhaust the class of M-rings, as Example (2.3) illustrates.

An M-subring (ideal) of an M-ring R is a subring (ideal) of R which is invariant under operations on R by elements of M. Let S be an M-subring of an M-ring R and let $\{r_\alpha \mid \alpha \in A\}$ be a set of elements of R. The intersection of all M-subrings of R which contain S and the elements r_α, $\alpha \in A$, is the unique smallest M-subring of R which contains S and the elements r_α, $\alpha \in A$, and it will be denoted by $S\{r_\alpha\}$. Analogously, if L is an M-subfield of an M-field K and $\{k_\alpha \mid \alpha \in A\}$ is a set of elements of K; the intersection of all M-subfields of K which contain L and the elements k_α, $\alpha \in A$, is the unique smallest M-subfield of K which contains L and the elements k_α, $\alpha \in A$, and it will be denoted by $L\langle k_\alpha \rangle$.

A homomorphism η of an M-ring R into an M-ring Q is an M-homomorphism if the M-system of mappings of R into Q deduced from the M-system of mappings of R into R by inverse transfer of the ring R to Q induces an M-system of mappings on R^η into Q for which the M-system of mappings of Q into Q is an extension. An M-isomorphism of R into Q is an M-homomorphism of R into Q which is one-to-one, and R and Q are M-isomorphic if there is an M-isomorphism of R onto Q. Finally, an M-extension of an M-ring R is a system (Q, i) consisting of an M-ring Q and an M-isomorphism i of R into Q. The isomorphic image R^i of R will usually be identified with R.

Let I be an M-ideal of an M-ring R and consider the canonical homomorphism of R onto the residue class ring R/I. Since I is an M-ideal of R, the M-system of mappings of R into R/I deduced from the M-system of mappings of R into R by inverse transfer of the ring R to R/I induces an M-system of mappings on R/I into R/I. Thus R/I becomes an M-ring and the canonical homomorphism of R onto R/I is an M-homomorphism. Now suppose η is an M-homomorphism of an M-ring R into an M-ring Q. The kernel of η is an M-ideal I of R, R^{η} is an M-subring of Q, the induced isomorphism $\bar{\eta}$ of R/I onto R^{η} is an M-isomorphism of the M-ring R/I into Q, and $(Q, \bar{\eta})$ is an M-extension of $R/I \cong R^{\eta}$.

Let R be an M-ring, let $\{x_\alpha \mid \alpha \in A\}$ be a set of elements algebraically independent over R, let $R[x_\alpha]$ be the ring of polynomials over R in the x_α, $\alpha \in A$, and let i be the canonical isomorphism of R into $R[x_\alpha]$. If $\{y_{\alpha,m} \mid \alpha \in A \text{ and } m \in M\}$ is a set of elements of $R[x_\alpha]$, then the M-system of mappings of R into $R[x_\alpha]$ deduced from the M-system of mappings of R into R by inverse transfer of the ring R to $R[x_\alpha]$ can be extended to an M-system of mappings of $R[x_\alpha]$ into $R[x_\alpha]$, such that $x_\alpha m = y_{\alpha,m}$, $\alpha \in A$ and $m \in M$. Thus $R[x_\alpha]$ becomes an M-ring and $(R[x_\alpha], i)$ is an M-extension of R.

Let R be an M-ring and let $S'(M)$ be the free semigroup with identity element generated by the set M. Operations on R by elements of $S'(M)$ are defined as follows: the identity element of $S'(M)$ operates on R as the identity automorphism of R, and any other element of $S'(M)$ operates on R as the resultant of the operations on R by its factors. Thus, if $m, n, p \in M$, then $a(mnp) = ((am)n)p$ for any $a \in R$. Let B be any set, let A be the product set $B \times S'(M)$, let $\{x_{\beta,s} \mid (\beta, s) \in B \times S'(M)\}$ be a set of elements algebraically independent over R, let $R[x_{\beta,s}]$ be the ring of polynomials over R in the $x_{\beta,s}$, $(\beta, s) \in B \times S'(M)$; and let i be the canonical isomorphism of R into $R[x_{\beta,s}]$. Setting $y_{(\beta,s),m} = x_{\beta,sm}$ and repeating the construction of the preceding paragraph, $R[x_{\beta,s}]$ becomes an M-ring, such that $x_{\beta,s}m = x_{\beta,sm}$, $(\beta, s) \in B \times S'(M)$ and $m \in M$; and $(R[x_{\beta,s}],i)$ is an M-extension of R. If 1 is the identity element of $S'(M)$ and $x_{\beta,1}$ is denoted simply by x_β, $\beta \in B$; then $R[x_{\beta,s}] = R\{x_\beta\}$. $R\{x_\beta\}$ will be called the M-extension of R by a set $\{x_\beta \mid \beta \in B\}$ of M-indeterminates.

Finally, let N be a set of elements of an M-ring R which are not zero divisors in R, let Q be the ring of quotients of R relative to the set N, and let i be the canonical isomorphism of R into Q. The M-system of mappings of R into Q deduced from the M-system of mappings of R into R by inverse transfer of the ring R to Q can be extended to an M-system of mappings of Q into Q and, consequently, Q becomes an M-ring such that (Q, i) is an M-extension of R, if, and only if, the $M \times M$ matrix $(\sum_{n\in M} \overline{z_{mnp}}(an))_{m,p\in M}$ is a unit in Q_M for every $a \in N$. Furthermore, when such a structure of an M-ring on Q exists, it is unique.

(4.1) PROPOSITION. *Let ϕ be an M-isomorphism of an M-domain R into an M-field K, and let Q be the field of fractions of R. There is a unique structure of an M-field on Q such that Q is an M-extension of R, and there is a unique extension of ϕ to an M-isomorphism of Q into K.*

Proof. Q is the ring of quotients of R relative to the set N of nonzero elements of R, and there is a unique extension of the isomorphism ϕ of R into the field K to an isomorphism $\bar{\phi}$ of Q into K. Identifying Q with its isomorphic image $Q^{\bar{\phi}}$, R is identified with its M-isomorphic image R^{ϕ}. The M-system of mappings of K

into K restricts to an M-system of mappings of Q into K which extends the M-system of mappings of R into $R \subseteq K$. Such an extension is unique and the $M \times M$ matrix $(\sum_{n\in M} \overline{z_{mnp}}(an))_{m,p\in M}$ is a unit in K_M for every $a \in N$. But then $(\sum_{n\in M} \overline{z_{mnp}}(an))_{m,p\in M}$ must already be a unit in Q_M for every $a \in N$, and the M-system of mappings of R into $R \subseteq Q \subseteq K$ can be extended to an M-system of mappings of Q into $Q \subseteq K$. Therefore, the M-system of mappings of K into K must restrict to an M-system of mappings of Q into Q; and, thus, Q becomes an M-field which is an M-extension of R. Such a structure of an M-field on Q must be unique, and the canonical embedding of Q in K is the unique extension of ϕ to an M-isomorphism of Q into K.

(4.2) COROLLARY. *If K is an M-field which is an M-extension of an M-ring R, then the field of fractions of R in K is the unique smallest M-subfield of K which contains R.*

5. **Compatibility of M-extensions and admissible M-isomorphisms.** Let (S, i) and (T, j) be M-extensions of an M-ring R. A common M-extension of S and T over R is a system (U, g, h) consisting of an M-ring U, and M-isomorphism g of S into U, and an M-isomorphism h of T into U, such that $ig = jh$. (S, i) and (T, j) are compatible M-extensions of an M-ring R if there exists a common M-extension (U, g, h) of S and T over R, such that U is an M-domain.

If (S, i) and (T, j) are M-extensions of an M-ring R, then, as extensions of the ring R, S and T are algebras over R, and the algebra $S \otimes_R T$ over R is again a ring. The mapping $g : s \to s \otimes 1$ is a homomorphism of S into $S \otimes_R T$, and the mapping $h : t \to 1 \otimes t$ is a homomorphism of T into $S \otimes_R T$. Consider the M-system of mappings of S into $S \otimes_R T$ deduced from the M-system of mappings of S into S by inverse transfer of the ring S to $S \otimes_R T$, and let ρ be the corresponding representation of S into $(C^{S\otimes_R T})^*$. Similarly, consider the M-system of mappings of T into $S \otimes_R T$ deduced from the M-system of mappings of T into T by inverse transfer of the ring T to $S \otimes_R T$, and let σ be the corresponding representation of T into $(C^{S\otimes_R T})^*$. There is a homomorphism τ of $S \otimes_R T$ into $(C^{S\otimes_R T})^*$ such that $(s \otimes t)^\tau = s^\rho t^\sigma$, $s \in S$ and $t \in T$, and, thus an M-system of mappings of $S \otimes_R T$ into $S \otimes_R T$ is determined and $S \otimes_R T$ becomes an M-ring. Furthermore, the restriction of τ to S^g yields an M-system of mappings of S^g into $S \otimes_R T$ induced by the M-system of mappings of S into $S \otimes_R T$, and the restriction of τ to T^h yields an M-system of T^h into $S \otimes_R T$ induced by the M-system of mappings of T into $S \otimes_R T$. Therefore, g is an M-homomorphism of S into $S \otimes_R T$ and h is an M-homomorphism of T into $S \otimes_R T$.

If S and T are M-domains, then g is an isomorphism of S into $S \otimes_R T$, h is an isomorphism of T into $S \otimes_R T$, and $(S \otimes_R T, g, h)$ is a common M-extension of S and T over R. Furthermore, if R is a field and S is a regular extension of R, then $S \otimes_R T$ is again an integral domain and (S, i) and (T, j) are compatible M-extensions of R.

An admissible M-isomorphism of an M-ring R is an M-isomorphism of R into an M-domain which is an M-extension of R.

(5.1) THEOREM. *If S is an M-domain which is an M-extension of an M-field R, such that S is a regular extension of R, then S is compatible with any M-domain which is an M-extension of R, an M-isomorphism of R into S is extendable to an admissible M-isomorphism of S, and there exists an admissible M-isomorphism of S over R which moves any element of S which is not also an element of R.*

Proof. Let i be the canonical M-isomorphism of R into the M-extension S. If T is an M-domain and j is an M-isomorphism of R into T, then the construction of the preceding paragraphs yields a common M-extension $(S \otimes_R T, g, h)$ of (S, i) and (T, j) over R and $S \otimes_R T$ is an M-domain.

Suppose f is an M-isomorphism of R into S. Letting $T = S$ and $j = f$, $(S \otimes_R T, h)$ is an M-extension of $T = S$ and g is an admissible M-isomorphism of S which extends the M-isomorphism $j = f$. Furthermore, if $f = i$, then g is an admissible M-isomorphism of S over R which moves any element of S which is not also an element of R.

Contrasting relaxations of the hypothesis of this theorem can be obtained in special cases. First let K and L be integral domains of characteristic $p \neq 0$, and let f be a homomorphism of K into L. If $K^{p^{-\infty}}$ and $L^{p^{-\infty}}$ are the perfect closures of K and L, respectively, then there is a unique extension of f to a homomorphism $\bar{f}$ of $K^{p^{-\infty}}$ into $L^{p^{-\infty}}$. Indeed, if $a \in K^{p^{-\infty}}$, then for some positive integer n, $a^{p^n} \in K$, and $a\bar{f}$ is the unique p^nth root of $(a^{p^n})f$. Furthermore if f is an isomorphism, so is $\bar{f}$.

(5.2) THEOREM. *If S is an M-domain of difference type which is an M-extension of an M-field R, such that every element of S algebraic over R is purely inseparable over R; then S is compatible with any M-domain which is an M-extension of R, an M-isomorphism of R into S is extendable to an admissible M-isomorphism of S and there exists an admissible M-isomorphism of S over R which moves any element of S not purely inseparable over R.*

Proof. If R is a field of characteristic zero, then S is a regular extension and Theorem (5.1) applies. Suppose R is a field of characteristic $p \neq 0$. If i is the canonical M-isomorphism of R into S, there is a unique extension of i to an isomorphism $\bar{i}$ of $R^{p^{-\infty}}$ into $S^{p^{-\infty}}$. Identifying $R^{p^{-\infty}}$ with its isomorphic image $(R^{p^{-\infty}})^{\bar{i}}$, R is identified with its M-isomorphic image R^i. The M-system of mappings of S into S consists of homomorphisms of S into S and there exist unique extensions of these homomorphisms to homomorphisms of $S^{p^{-\infty}}$ into $S^{p^{-\infty}}$. In turn, these homomorphisms of $S^{p^{-\infty}}$ into $S^{p^{-\infty}}$ restrict to homomorphisms of $R^{p^{-\infty}}$ into $S^{p^{-\infty}}$, which must be the unique extensions of the homomorphisms in the M-system of mappings of R into R to homomorphisms of $R^{p^{-\infty}}$ into

$R^{p^{-\infty}} \subseteq S^{p^{-\infty}}$. Thus $S^{p^{-\infty}}$ and $R^{p^{-\infty}}$ become M-domains which are M-extensions of S and R, respectively, and the canonical embedding $\bar{i}$ of $R^{p^{-\infty}}$ into $S^{p^{-\infty}}$ is an M-isomorphism.

Similarly, if T is an M-domain and j is an M-isomorphism of R into T, then there is a unique structure of an M-domain on $T^{p^{-\infty}}$ and there is a unique extension of j to an M-isomorphism $\bar{j}$ of $R^{p^{-\infty}}$ into $T^{p^{-\infty}}$. $S^{p^{-\infty}}$ is a regular extension of $R^{p^{-\infty}}$; therefore $(S^{p^{-\infty}}, \bar{i})$ and $(T^{p^{-\infty}}, \bar{j})$ are compatible M-extensions of $R^{p^{-\infty}}$, and (S, i) and (T, j) must be compatible M-extensions of R. If $T = S$, then $T^{p^{-\infty}} = S^{p^{-\infty}}$, $\bar{j}$ can be extended to an admissible M-isomorphism of $S^{p^{-\infty}}$, and the restriction of this admissible M-isomorphism to S is an admissible M-isomorphism of S which extends j. Finally, there is an admissible M-isomorphism of $S^{p^{-\infty}}$ over $R^{p^{-\infty}}$ which moves any element of $S^{p^{-\infty}}$ which is not also an element of $R^{p^{-\infty}}$, and the restriction of this admissible M-isomorphism to S is an admissible M-isomorphism of S over R which moves any element of S not purely inseparable over R.

It is worthwhile to observe that if any two homomorphisms in the M-system of mappings on S and T commute on S and on T, then they commute on $S \otimes_R T$, $S^{p^{-\infty}}$, $T^{p^{-\infty}}$, and $S^{p^{-\infty}} \otimes_{R_{p^{-\infty}}} T^{p^{-\infty}}$. Thus any such commutativity is preserved in the preceding constructions. The importance of the assumption that every element of S algebraic over R be purely inseparable over R can be illustrated as follows: Let R be the difference field consisting of the field of real numbers and the identity automorphism, let S be the difference field consisting of the field of complex numbers and the identity automorphism, and let T be the difference field consisting of the field of complex numbers and the automorphism which maps each complex number onto its conjugate. S and T are M-extensions of R, but they are not compatible, since in any commutative integral domain which is an extension of the field of real numbers there can be at most one subring isomorphic over the field of real numbers to the field of complex numbers.

(5.3) Lemma. *Let L be a ring which is an extension of a field K, and let ζ be an element of L which is separably algebraic over K. For any higher derivation of K into L there is a unique extension to a higher derivation of $K(\zeta)$ into L.*

Proof. Let x be an element transcendental over K and let

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

be an irreducible polynomial over K for which ζ is a root. A higher derivation of K into L together with the identity isomorphism of K into L is an M-system of mappings of K into L [Examples (2.1) and (2.2)]; let ρ be the corresponding representation of K into $(C^L)^*$. Any extension of ρ to a homomorphism of $K(\zeta)$ into $(C^L)^*$ is induced by a homomorphism of $K[x]$ into $(C^L)^*$ which also extends ρ and vanishes on $p(x)$. ρ can be extended to a homomorphism of $K[x]$ into

$(C^L)^*$ which vanishes on $p(x)$ if, and only if, the M-system of mappings of K into L can be extended to an M-system of mappings of $K[x]$ into L such that $(p(x))D_i = 0$ for every non-negative integer i which does not exceed the rank of the higher derivation of K into L. The induced homomorphism of $K(\zeta)$ into $(C^L)^*$ determines a higher derivation of $K(\zeta)$ into L which extends the higher derivation of K into L if, and only if, $xD_0 = \zeta$. Set $xD_0 = \zeta$ and assume that xD_j has already been defined for all positive integers j less than a given positive integer i, which does not exceed the rank of the higher derivation of K into L. Let $p'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$ and let

$$q_i(x) = \sum_{k=1}^{n} \sum_{\substack{j_0+j_1+\cdots+j_k=i \\ j_1,\ldots,j_k<i}} (a_kD_{j_0})(xD_{j_1}) \cdot \cdots \cdot (xD_{j_k}).$$

xD_i must be defined so that $0 = (p(x))D_i = (p'(\zeta))(xD_i) + q_i(x)$. Since ζ is separably algebraic over K, $p'(\zeta) \neq 0$; therefore set $xD_i = -(q_i(x))(p'(\zeta))^{-1}$. Proceeding inductively, the M-system of mappings of K into L is uniquely extended to the desired M-system of mappings of $K[x]$ into L and the theorem is proved.

With suitable modification, the technique used in the last paragraph of §3 may be re-employed to show that the extension of an iterative infinite higher derivation of K into K to an infinite higher derivation of $K(\zeta)$ into $K(\zeta)$ is again iterative.

(5.4) THEOREM. *If S is an M-domain of differential type which is an M-extension of an M-field R, such that S is a separable extension of R, then S is compatible with any M-domain of differential type which is an M-extension of R. An M-isomorphism of R into S is extendable to an admissible M-isomorphism of S, and given any element s_0 of S which is not also an element of R there exists an admissible M-isomorphism of S over R which moves s_0.*

Proof. Let $\bar{R}$ and $\bar{S}$ denote the separable algebraic closures of R and S, respectively. If i is the canonical M-isomorphism of R into S, let $\bar{i}$ be an extension of i to an isomorphism of $\bar{R}$ into $\bar{S}$. Identifying $\bar{R}$ with its isomorphic image $\bar{R}^{\bar{i}}$, R is identified with its M-isomorphic image R^i. The M-system of mappings of S into S consists of the identity automorphism of S and higher derivations of S into S. As a consequence of Lemma (5.3), there exist unique extensions of these higher derivations to higher derivations of $\bar{S}$ into $\bar{S}$, which restrict to higher derivations of $\bar{R}$ into $\bar{S}$. These higher derivations of $\bar{R}$ into $\bar{S}$ must be the unique extensions of the higher derivations in the M-system of mappings of R into R to higher derivations of $\bar{R}$ into $\bar{R} \subseteq \bar{S}$. Thus $\bar{R}$ and $\bar{S}$ become M-domains of differential type which are M-extensions of S and R, respectively, and the canonical embedding $\bar{i}$ of $\bar{R}$ into $\bar{S}$ is an M-isomorphism.

Similarly, if T is an M-domain of differential type and j is an M-isomorphism of R into T, then there is a unique structure of an M-domain of differential type on the separable algebraic closure $\bar{T}$ of T and any extension of j to an isomorphism $\bar{j}$ of $\bar{R}$ into $\bar{T}$ is an M-isomorphism. $\bar{S}$ is a regular extension of $\bar{R}$; therefore $(\bar{S}, \bar{i})$ and $(\bar{T}, \bar{j})$ are compatible M-extensions of $\bar{R}$, and (S, i) and (T, j) must be compatible M-extensions of R. If $T = S$, then $\bar{T} = \bar{S}$, $\bar{j}$ can be extended to an admissible M-isomorphism of $\bar{S}$, and the restriction of this admissible M-isomorphism to S is an admissible M-isomorphism of S which extends j. Furthermore, there is an admissible M-isomorphism of $\bar{S}$ over $\bar{R}$ which moves any element of $\bar{S}$ which is not also an element of $\bar{R}$. The restriction of this admissible M-isomorphism to S is an admissible M-isomorphism of S over R which moves any element of S which is not separably algebraic over R. Suppose s_0 is an element of S which is separably algebraic over R, but $s_0 \notin R$. Let $T = S$, let $j = i$, and let $\bar{j}$ be any extension of j to an isomorphism of $\bar{R}$ into $\bar{T} = \bar{S}$ such that $s_0\bar{j} \neq s_0\bar{i}$. There is an admissible M-isomorphism of $\bar{S}$ which extends $\bar{j}$, and the restriction of this admissible M-isomorphism to S is an admissible M-isomorphism of S over R which moves s_0.

Observe that $\bar{S} \otimes_{\bar{R}} \bar{T}$ is an M-domain of differential type, so the differential type of the M-rings can be preserved throughout the preceding constructions. If any two higher derivations in the M-system of mappings on S and T commute on S and on T, then they commute on $\bar{S}$, $\bar{T}$, and $\bar{S} \otimes_{\bar{R}} \bar{T}$; thus any such commutativity is preserved in the preceding constructions. Finally, if there is an infinite higher derivation in the M-system of mappings on S and T which is iterative on S and on T; then it is iterative on $\bar{S}$, $\bar{T}$, and $\bar{S} \otimes_{\bar{R}} \bar{T}$ and the iterative character is preserved in the preceding constructions. The importance of the assumption that S is a separable extension of R can be illustrated as follows: Let F be a field of characteristic $p \neq 0$, let $\{x_1, x_2, x_3, x_4\}$ be a set of elements algebraically independent over F, and let $F(x_1, x_2, x_3, x_4)$ be the field of rational expressions over F in x_1, x_2, x_3, and x_4. Let R be the differential field consisting of $F(x_1^p, x_2^p)$ and the derivation which maps every element onto zero, let S be the differential field consisting of $F(x_1^p, x_2^p, x_3, x_4, x_1x_3 + x_2x_4)$ and the derivation which maps every element onto zero, and let T be the differential field consisting of $F(x_1, x_2)$ and the derivation which maps x_1 and every element of F onto zero but maps x_2 onto 1. S and T are M-extensions of R; but they are not compatible even though R is algebraically closed in S, since in any M-domain which were a common M-extension of S and T over R, the equation $0 = (x_1x_3 + x_2x_4)D_1 = (x_2D_1)x_4 = x_4$ would be obtained.

FLORIDA STATE UNIVERSITY,
TALLAHASSEE, FLORIDA