

# AN EXTENSION OF DIFFERENTIAL GALOIS THEORY <sup>(1)</sup>

BY

H. F. KREIMER

**1. Introduction.** The terminology and notation of this paper are taken from the author's paper *The foundation for an extension of differential algebra* [1]. Let  $C$  be an associative, commutative coalgebra with identity over a ring  $W$ , which is freely generated as a  $W$ -module by a set  $M$ . If  $w \rightarrow \bar{w}$  is a homomorphism of  $W$  into a ring  $S$ , let  $C^S$  be the  $S$ -module obtained from the  $W$ -module  $C$  by inverse transfer of the basic ring to  $S$ . If  $\rho$  is a homomorphism of a ring  $R$  into the algebra  $(C^S)^* = \text{Hom}_S(C^S, S)$ , then for each  $m \in M$  there is a mapping  $a \rightarrow a^\rho(m)$  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  $S$ . Let  $m \rightarrow \sum_{n, p \in M} z_{mnp} n \otimes p$ , where  $m \in M$ ,  $z_{mnp} \in W$ , and  $z_{mnp} = 0$  except for a finite number of elements  $n$  and  $p$  in  $M$ , be the coproduct mapping of  $C$  into  $C \otimes_W C$ ; if  $a, b \in R$  and  $m \in M$ ,  $(a + b)m = am + bm$  and  $(ab)m = \sum_{n, p \in M} \overline{z_{mnp}} (an)(bp)$ . An  $M$ -ring is a ring together with an  $M$ -system of mappings of the ring into itself.

In §2, the constants of an  $M$ -ring are defined, criteria for the linear independence of elements of an  $M$ -domain over its subring of constants are established, and the structure of an  $M$ -ring is shown to extend to the field of fractions of certain  $M$ -domains. Solution fields and Picard-Vessiot extensions are defined in §3, and connection with the differential Picard-Vessiot theory are made. In §4, strongly normal extensions are defined, and connections with the differential Galois theory of strongly normal extensions are made. For use in this paper, a result from [1] needs to be stated in a stronger form and is stated and proved below.

(1.1.) LEMMA. *Let  $N$  be a set of elements of a ring  $R$  which are not zero-divisors in  $R$ , and let  $Q$  be the ring of quotients of  $R$  relative to  $N$ . An  $M$ -system of mappings of  $R$  into a field  $S$  can be extended to an  $M$ -system of mappings of  $Q$  into  $S$  if, and only if, the  $(M \times M)$ -matrix  $(\sum_{n \in M} \overline{z_{mnp}}(an))_{m, p \in M}$  represents a one-to-one endomorphism of the  $S$ -module  $C^S$  for every  $a \in N$ . Furthermore, when such an extension exists, it is unique.*

**Proof.** Let  $\rho$  be a representation of  $R$  in  $(C^S)^*$ .  $\rho$  can be extended to a homomorphism of  $Q$  into  $(C^S)^*$  if, and only if,  $a^\rho$  is a unit in  $(C^S)^*$  for every  $a \in N$ ; and when such an extension exists, it is unique. Let  $f, g \in (C^S)^*$ ;

---

Presented to the Society, June 4, 1962 under the title *An extension of the Picard-Vessiot theory*; received by the editors February 18, 1963 and, in revised form, January 29, 1964.

<sup>(1)</sup> Part of a dissertation presented for the degree of Doctor of Philosophy in Yale University.

$$\begin{aligned}(f \cdot g)(m) &= (f \otimes g) \left( \sum_{n, p \in M} \overline{z_{mnp}} n \otimes p \right) = \sum_{n, p \in M} \overline{z_{mnp}} f(n) \cdot g(p) \\ &= g \left( \sum_{n, p \in M} \overline{z_{mnp}} f(n) \cdot p \right).\end{aligned}$$

Therefore, under the regular representation of  $(C^S)^*$ , 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  $(\sum_{n \in M} \overline{z_{mnp}} f(n))_{m, p \in M}$ . The mapping  $\sigma: f \rightarrow (\sum_{n \in M} \overline{z_{mnp}} f(n))_{m, p \in M}$  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  $f^\sigma$  is a unit in  $S_M$  and represents a one-to-one endomorphism of  $C^S$ . Conversely if  $f^\sigma$  represents a one-to-one endomorphism of  $C^S$ , the transpose of this endomorphism of  $C^S$  is an endomorphism of the  $S$ -module  $(C^S)^*$  onto itself. Therefore there is an element  $g$  of  $(C^S)^*$  such that  $f \cdot g = e$ , the identity element of  $(C^S)^*$ , and  $f$  is a unit in  $(C^S)^*$ . The lemma now follows at once.

**2. The constants of an  $M$ -ring.** Let  $R$  be an  $M$ -ring and let  $\rho$  be the associated representation of  $R$  in  $(C^R)^*$ . An element  $c$  of  $R$  is a constant if  $(ca)^\rho = c \cdot a^\rho$  for every  $a \in R$ . The constants of  $R$  form a subring which contains the identity element of  $R$ . The subring of constants of  $R$  will be denoted by  $R_c$ . Suppose  $b, d \in R$  and  $d$  is a unit in  $R$ . If  $bd^{-1} \in R_c$ , then  $d \cdot b^\rho = d \cdot (bd^{-1}d)^\rho = b \cdot d^\rho$ ; and, conversely, if  $d \cdot b^\rho = b \cdot d^\rho$ , then  $(bd^{-1}a)^\rho = b^\rho(d^\rho)^{-1}a^\rho = bd^{-1} \cdot a^\rho$  for every  $a \in R$  and  $bd^{-1} \in R_c$ . Taking  $d = 1$ ,  $b \in R_c$  if, and only if,  $b^\rho = 1 \cdot b^\rho = b \cdot 1^\rho$ . This characterization of the constants of an  $M$ -ring implies that if  $S$  is an  $M$ -extension of  $R$ ,  $R_c \subseteq S_c$ . If  $b = 1$  and  $d \in R_c$ , then  $d \cdot 1^\rho = d^\rho = 1 \cdot d^\rho$  and  $d^{-1} \in R_c$ . Consequently, if  $R$  is a field, so is  $R_c$ .

Two elements  $f$  and  $g$  of  $(C^R)^*$  are equal if, and only if,  $f(m) = g(m)$  for every  $m \in M$ . Therefore an element  $c$  of  $R$  is a constant if, and only if,  $(ca)m = c(am)$  for every  $a \in R$  and  $m \in M$ . If  $b, d \in R$  and  $d$  is a unit in  $R$ , then  $bd^{-1} \in R_c$  if, and only if,  $d(bm) = b(dm)$  for every  $m \in M$ . Also  $b \in R_c$  if, and only if,  $bm = b(1m)$  for every  $m \in M$ .

Let  $S'(M)$  be the free semi-group with identity generated by the set  $M$ . Operations by elements of  $S'(M)$  on the  $M$ -ring  $R$  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. Let  $h$  be a positive integer, let  $r_1, r_2, \dots, r_h$  be  $h$  elements of  $R$ , and let  $s_1, s_2, \dots, s_h$  be  $h$  elements of  $S'(M)$ . Denote by  $W(r_1, r_2, \dots, r_h; s_1, s_2, \dots, s_h)$  the determinant:

$$\begin{vmatrix} r_1 s_1 & r_1 s_2 & \cdots & r_1 s_h \\ r_2 s_1 & r_2 s_2 & \cdots & r_2 s_h \\ \vdots & \vdots & \ddots & \vdots \\ r_h s_1 & r_h s_2 & \cdots & r_h s_h \end{vmatrix}.$$

(2.1) THEOREM. Let  $h$  be a positive integer, and let  $r_1, r_2, \dots, r_h$  be  $h$  elements of an  $M$ -domain  $R$ . If  $r_1, r_2, \dots, r_h$  are linearly dependent over  $R_c$ , then  $W(r_1, r_2, \dots, r_h; s_1, s_2, \dots, s_h) = 0$  for every choice of  $h$  elements  $s_1, s_2, \dots, s_h$  in  $S'(M)$ . If  $h \geq 2$ ,  $W(r_1, r_2, \dots, r_h; s_1, s_2, \dots, s_h) = 0$  for every choice of  $h$  elements  $s_1, s_2, \dots, s_h$  in  $S'(M)$ , but for some choice of  $h-1$  elements  $t_1, t_2, \dots, t_{h-1}$  in  $S'(M)$ ,  $W(r_1, r_2, \dots, r_{h-1}; t_1, t_2, \dots, t_{h-1})$  is a unit in  $R$ , then  $r_h$  is equal to a unique linear combination of  $r_1, r_2, \dots, r_{h-1}$  over  $R_c$ .

**Proof.** If  $r_1, r_2, \dots, r_h$  are linearly dependent over  $R_c$ , then there exist  $h$  elements  $c_1, c_2, \dots, c_h$  of  $R_c$ , not all zero, such that  $\sum_{\alpha=1}^h c_\alpha r_\alpha = 0$ . For any  $s \in S'(M)$ ,  $\sum_{\alpha=1}^h c_\alpha (r_\alpha s) = (\sum_{\alpha=1}^h c_\alpha r_\alpha) s = 0$ . Therefore  $W(r_1, r_2, \dots, r_h; s_1, s_2, \dots, s_h)$  is the determinant of a matrix with rows linearly dependent over  $R_c$  and must vanish for every choice of  $h$  elements  $s_1, s_2, \dots, s_h$  in  $S'(M)$ .

Suppose  $h \geq 2$ ,  $W(r_1, r_2, \dots, r_h; s_1, s_2, \dots, s_h) = 0$  for every choice of  $h$  elements  $s_1, s_2, \dots, s_h$  in  $S'(M)$ , but for some choice of  $h-1$  elements  $t_1, t_2, \dots, t_{h-1}$  in  $S'(M)$ ,  $W(r_1, r_2, \dots, r_{h-1}; t_1, t_2, \dots, t_{h-1})$  is a unit in  $R$ . Let  $t_h$  be any given element of  $S'(M)$ . Then  $W(r_1, r_2, \dots, r_h; t_1, t_2, \dots, t_h) = 0$ ; and, if  $A_\alpha$  is the cofactor of  $r_\alpha t_h$  in this determinant,  $\sum_{\alpha=1}^h A_\alpha (r_\alpha t_\beta) = 0$  for  $1 \leq \beta \leq h$ . Therefore  $(A_h \cdot A_1^\rho, A_h \cdot A_2^\rho, \dots, A_h \cdot A_h^\rho)$  is a solution in  $(C^R)^*$  of the system of equations  $\sum_{\alpha=1}^h (r_\alpha t_\beta)^\rho x_\alpha = 0$ ,  $1 \leq \beta \leq h$ . Replacing  $t_h$  by any one of the elements  $t_\beta m$ ,  $m \in M$  and  $1 \leq \beta \leq h$ , yields  $\sum_{\alpha=1}^h A_\alpha (r_\alpha t_\beta)^\rho(m) = \sum_{\alpha=1}^h A_\alpha ((r_\alpha t_\beta)m) = 0$ . Therefore  $\sum_{\alpha=1}^h A_\alpha \cdot (r_\alpha t_\beta)^\rho = 0$  for  $1 \leq \beta \leq h$ ; and  $(A_1 \cdot A_h^\rho, A_2 \cdot A_h^\rho, \dots, A_h \cdot A_h^\rho)$  is another solution in  $(C^R)^*$  of the equations  $\sum_{\alpha=1}^h (r_\alpha t_\beta)^\rho x_\alpha = 0$ ,  $1 \leq \beta \leq h$ . Then

$$(A_h \cdot A_1^\rho - A_1 \cdot A_h^\rho, A_h \cdot A_2^\rho - A_2 \cdot A_h^\rho, \dots, A_h \cdot A_{h-1}^\rho - A_{h-1} \cdot A_h^\rho)$$

is a solution of the system of equations  $\sum_{\alpha=1}^{h-1} (r_\alpha t_\beta)^\rho x_\alpha = 0$ ,  $1 \leq \beta \leq h-1$ . But the determinant of this system of equations is  $(W(r_1, r_2, \dots, r_{h-1}; t_1, t_2, \dots, t_{h-1}))^\rho$ , which is a unit in  $(C^R)^*$ ; therefore, this system of equations can have no non-trivial solution in  $(C^R)^*$  and  $A_h \cdot A_\alpha^\rho = A_\alpha \cdot A_h^\rho$  for  $1 \leq \alpha \leq h-1$ . Since  $A_h = W(r_1, r_2, \dots, r_{h-1}; t_1, t_2, \dots, t_{h-1})$  is a unit in  $R$ ,  $A_\alpha \cdot A_h^{-1} \in R_c$  for  $1 \leq \alpha \leq h-1$ . If  $t_h$  is chosen to be the identity element of  $S'(M)$ , then the equation  $\sum_{\alpha=1}^h A_\alpha (r_\alpha t_h) = 0$  yields

$$r_h = \sum_{\alpha=1}^{h-1} -A_\alpha A_h^{-1} r_\alpha.$$

Since  $W(r_1, r_2, \dots, r_{h-1}; t_1, t_2, \dots, t_{h-1}) \neq 0$ ,  $r_1, r_2, \dots, r_{h-1}$  are linearly independent over  $R_c$  and the expression for  $r_h$  as a linear combination of  $r_1, r_2, \dots, r_{h-1}$  over  $R_c$  is unique.

(2.2) COROLLARY. Let  $h$  be a positive integer, and let  $k_1, k_2, \dots, k_h$  be  $h$  elements of an  $M$ -field  $K$ .  $k_1, k_2, \dots, k_h$  are linearly dependent over  $K_c$  if, and only if,  $W(k_1, k_2, \dots, k_h; s_1, s_2, \dots, s_h) = 0$  for every choice of  $h$  elements  $s_1, s_2, \dots, s_h$  in  $S'(M)$ .

**Proof.** Suppose that  $W(k_1, k_2, \dots, k_h; s_1, s_2, \dots, s_h) = 0$  for every choice of  $h$  elements  $s_1, s_2, \dots, s_h$  in  $S'(M)$ . If  $k_1 = 0$ , then  $k_1, k_2, \dots, k_h$  are linearly dependent over  $K_c$ . If  $k_1 \neq 0$ , there is a positive integer  $i$ ,  $1 < i \leq h$ , such that  $W(k_1, k_2, \dots, k_i; s_1, s_2, \dots, s_i) = 0$  for every choice of  $i$  elements  $s_1, s_2, \dots, s_i$  in  $S'(M)$ , but for some choice of  $i-1$  elements  $t_1, t_2, \dots, t_{i-1}$  in  $S'(M)$ ,  $W(k_1, k_2, \dots, k_{i-1}; t_1, t_2, \dots, t_{i-1}) \neq 0$  and, consequently, is a unit in  $K$ . The corollary now follows from Theorem (2.1).

(2.3) COROLLARY. *If  $R$  is an  $M$ -domain which is an  $M$ -extension of an  $M$ -field  $K$ , then  $K$  and  $R_c$  are linearly disjoint over  $K_c$ .*

**Proof.** Theorem (2.1) and Corollary (2.2) imply that elements of  $K$  which are linearly dependent over  $R_c$  must be linearly dependent over  $K_c$ , whence the corollary.

(2.4) THEOREM. *Let  $R$  be an  $M$ -domain which is an  $M$ -extension of an  $M$ -field  $K$ , and let  $Q$  be the field of fractions of  $R$ . If  $R$  is generated by its subrings  $K$  and  $R_c$  and  $K_c$  is algebraically closed, then there is a unique structure of an  $M$ -field on  $Q$  such that  $Q$  is an  $M$ -extension of  $R$ .*

**Proof.** By Lemma (1.1), 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 uniquely to an  $M$ -system of mappings of  $Q$  into  $Q$ , making  $Q$  an  $M$ -field which is an  $M$ -extension of  $R$ ; if the  $(M \times M)$ -matrix  $(\sum_{n \in M} z_{mnp}(an))_{m, p \in M}$  represents a one-to-one linear transformation on  $C^Q$  for every  $a \neq 0$  in  $R$ . Suppose there were an  $a \neq 0$  in  $R$  such that  $(\sum_{n \in M} \overline{z_{mnp}(an)})_{m, p \in M}$  did not represent a one-to-one linear transformation on  $C^Q$ , or, equivalently, the rows of this matrix were linearly dependent over  $R$ . Let  $b_1, b_2, \dots, b_i$  be the nonzero coefficients in a nontrivial linear relation over  $R$  among the rows of this matrix. If  $\eta$  were an  $M$ -homomorphism of  $K\{a, b_1, b_2, \dots, b_i\}$  over  $K$  into  $K$  such that  $(ab_1)^\eta \neq 0$ , then  $a^\eta$  would be a nonzero element of  $K$  such that  $(\sum_{n \in M} \overline{z_{mnp}(a^\eta n)})_{m, p \in M}$  does not represent a one-to-one linear transformation on  $C^K$ , contradicting the existence of an  $M$ -system of mappings of  $K$  into  $K$ .

$R$  is generated as an abstract ring by  $K$  and  $R_c$ , and  $K$  and  $R_c$  are linearly disjoint over  $K_c$  by Corollary (2.3). Therefore, given a basis for  $K$  over  $K_c$ , every element of  $R$  has a unique representation as a linear combination of the elements of this basis over  $R_c$ . Let  $c_1, c_2, \dots, c_j$  be the nonzero coefficients out of  $R_c$  appearing in the expressions for  $a, b_1, b_2, \dots, b_i, ab_1$  in terms of such a basis, with  $c_1$  appearing in the expression for  $ab_1$ . A specialization of  $c_1, c_2, \dots, c_j$  over  $K_c$  into  $K_c$ , with  $c_1$  being specialized to a nonzero element, can be extended to a specialization over  $K$  which yields an  $M$ -homomorphism  $\eta$  as above. Since  $K_c$  is algebraically closed, such a specialization can be obtained as follows: Select a transcendence basis  $d_1, d_2, \dots, d_v$  for  $K_c(c_1, c_2, \dots, c_j)$  over  $K_c$  which includes  $c_1$  if  $c_1 \notin K_c$ . For  $1 \leq \alpha \leq j$ , there exists a monic polynomial  $f_\alpha(x)$  over  $K_c(d_1, d_2, \dots, d_v)$

for which  $c_\alpha$  is a root. Express the coefficients of the  $f_\alpha(x)$ ,  $1 \leq \alpha \leq j$ , as rational forms over  $K_c$  in  $d_1, d_2, \dots, d_v$  with common denominator  $g(d_1, d_2, \dots, d_v)$ . Choose a specialization of  $d_1, d_2, \dots, d_v$  over  $K_c$  into  $K_c$  for which  $c_1 \cdot g(d_1, d_2, \dots, d_v)$  does not vanish. This specialization can be extended to the coefficients of the  $f_\alpha(x)$  and thence to all the  $c_\alpha$ ,  $1 \leq \alpha \leq j$ , with values in  $K_c$ ; and  $c_1$  is specialized to a nonzero element. Therefore, there is a unique structure of an  $M$ -field on  $Q$ , such that  $Q$  is an  $M$ -extension of  $R$ .

### 3. Picard-Vessiot extensions.

(3.1) Definition. An  $M$ -field  $K$  which is an  $M$ -extension of an  $M$ -field  $L$  is a solution field over  $L$  if there exists a positive integer  $h$  and  $h$  elements  $k_1, k_2, \dots, k_h$  of  $K$ , such that  $K = L \langle k_1, k_2, \dots, k_h \rangle$  and, for some choice of  $h$  elements  $t_1, t_2, \dots, t_h$  in  $S'(M)$ ,  $W(k_1, k_2, \dots, k_h; t_1, t_2, \dots, t_h) = W_0 \neq 0$  while  $W_0^{-1}W(k_1, k_2, \dots, k_h; t_1, \dots, t_{\alpha-1}, t_{\alpha+1}, \dots, t_h, t) \in L$  for  $1 \leq \alpha \leq h$  and  $t = 1$  or  $t = t_\beta m$ ,  $m \in M$  and  $1 \leq \beta \leq h$ . The set of elements  $k_1, k_2, \dots, k_h$  is a fundamental set for  $K$  over  $L$ .

(3.2) THEOREM. Let  $K$  be a solution field over an  $M$ -field  $L$ , and let the notation be as in Definition (3.1). For any  $s \in S'(M)$  and  $1 \leq \beta \leq n$ ,  $k_\beta s = \sum_{\alpha=1}^n A_\alpha(s) \cdot k_\beta t_\alpha$ , where  $A_\alpha(s) \in L$  for  $1 \leq \alpha \leq h$ ;  $L\{k_1, k_2, \dots, k_h\}$  is generated as an abstract ring over  $L$  by the elements  $k_\beta t_\alpha$ ,  $1 \leq \alpha, \beta \leq h$ ; and for any choice of  $h$  elements  $s_1, s_2, \dots, s_h$  in  $S'(M)$ ,  $W_0^{-1}W(k_1, k_2, \dots, k_h; s_1, s_2, \dots, s_h) \in L$ . If  $\phi$  is an  $M$ -homomorphism of  $L\{k_1, k_2, \dots, k_h\}$  over  $L$  into an  $M$ -domain  $R$  which is an  $M$ -extension of  $K$ , then  $k_\alpha \phi$  has a unique expression

$$k_\alpha \phi = \sum_{\beta=1}^n c_{\alpha\beta} k_\beta, \quad 1 \leq \alpha \leq h,$$

where  $(c_{\alpha\beta})_{1 \leq \alpha, \beta \leq h}$  is a matrix over  $R_c$ ; moreover, if  $K_c$  is algebraically closed and  $Q$  denotes the field of fractions of  $K\{k_1 \phi, k_2 \phi, \dots, k_h \phi\}$ , there is a unique structure of an  $M$ -field on  $Q$  such that  $Q$  is an  $M$ -extension of  $K\{k_1 \phi, k_2 \phi, \dots, k_h \phi\}$ .

**Proof.** Let  $t = 1$  or  $t = t_\beta m$ ,  $m \in M$  and  $1 \leq \beta \leq h$ ; and let

$$B_\gamma(t) = (-1)^{h+\gamma+1} W_0^{-1}W(k_1, k_2, \dots, k_h; t_1, t_2, \dots, t_{\gamma-1}, t_{\gamma+1}, \dots, t_h, t), \quad 1 \leq \gamma \leq h.$$

Then  $B_\gamma(t) \in L$  for  $1 \leq \gamma \leq h$ ; and

$$k_\beta t + \sum_{\gamma=1}^h B_\gamma(t) \cdot k_\beta t_\gamma = W_0^{-1}W(k_1, k_2, \dots, k_h, k_\beta; t_1, t_2, \dots, t_h, t) = 0$$

for  $1 \leq \beta \leq h$ . If  $m \in M$  and  $1 \leq \beta \leq h$ , then

$$\begin{aligned} k_\beta t m &= - \sum_{\gamma=1}^h (B_\gamma(t) \cdot k_\beta t_\gamma) m = - \sum_{\gamma=1}^h \sum_{n, p \in M} \overline{z_{mnp}}((B_\gamma(t))n) (k_\beta t_\gamma p) \\ &= - \sum_{\gamma=1}^h \sum_{n, p \in M} \sum_{\alpha=1}^h \overline{z_{mnp}}((B_\gamma(t))n) B_\alpha(t_\beta p) \cdot k_\beta t_\alpha = \sum_{\alpha=1}^h A_\alpha(tm) \cdot k_\beta t_\alpha, \end{aligned}$$

where  $A_\alpha(tm) = - \sum_{\gamma=1}^h \sum_{n,p \in M} \overline{z_{mnp}} ((B_\gamma(t))n) B_\alpha(t_\gamma p) \in L$  for  $1 \leq \alpha \leq h$ . By repetition of this type of argument, it follows that for any  $s \in S'(M)$  and  $1 \leq \beta \leq h$ ,

$$k_\beta s = \sum_{\alpha=1}^h A_\alpha(s) \cdot k_\beta t_\alpha, \quad \text{where } A_\alpha(s) \in L \text{ for } 1 \leq \alpha \leq h.$$

Consequently,  $L\{k_1, k_2, \dots, k_h\}$  is generated as an abstract ring over  $L$  by the elements  $k_\beta t_\alpha$ ,  $1 \leq \alpha, \beta \leq h$ ; and  $W_0^{-1}W(k_1, k_2, \dots, k_h; s_1, s_2, \dots, s_h) = W_0^{-1} \cdot W_0 \cdot \det(A_\alpha(s_\beta))_{1 \leq \alpha, \beta \leq h} = \det(A_\alpha(s_\beta))_{1 \leq \alpha, \beta \leq h} \in L$  for any choice of  $h$  elements  $s_1, s_2, \dots, s_h$  in  $S'(M)$ .

Now let  $s_1, s_2, \dots, s_h, s_{h+1}$  be any  $h+1$  elements of  $S'(M)$ .  $W_0^{-1}W(k_1, k_2, \dots, k_h, k_\alpha; s_1, s_2, \dots, s_h, s_{h+1}) = 0$  for  $1 \leq \alpha \leq h$ ; and expansion of the determinant  $W(k_1, k_2, \dots, k_h, k_\alpha; s_1, s_2, \dots, s_h, s_{h+1})$  in this equation by cofactors of the elements of its last row yields a linear homogeneous equation in  $k_\alpha s_\beta$ ,  $1 \leq \beta \leq h+1$ , over  $L$ . If  $\phi$  is an  $M$ -homomorphism of  $L\{k_1, k_2, \dots, k_h\}$  over  $L$  into an  $M$ -domain  $R$  which is an  $M$ -extension of  $K$ , then

$$\begin{aligned} W_0^{-1}W(k_1, k_2, \dots, k_h, k_\alpha \phi; s_1, s_2, \dots, s_h, s_{h+1}) \\ = (W_0^{-1}W(k_1, k_2, \dots, k_h, k_\alpha; s_1, s_2, \dots, s_h, s_{h+1}))\phi = 0, \quad 1 \leq \alpha \leq h. \end{aligned}$$

Therefore  $W(k_1, k_2, \dots, k_h, k_\alpha \phi; s_1, s_2, \dots, s_h, s_{h+1}) = 0$ , while  $W(k_1, k_2, \dots, k_h; t_1, t_2, \dots, t_h) = W_0$  is a unit in  $R$ ; hence  $k_\alpha \phi$  has a unique expression as  $k_\alpha \phi = \sum_{\beta=1}^h c_{\alpha\beta} k_\beta$ ,  $1 \leq \alpha \leq h$ , where  $(c_{\alpha\beta})_{1 \leq \alpha, \beta \leq h}$  is a matrix over  $R_c$ . Assume  $R = K\{k_1 \phi, k_2 \phi, \dots, k_h \phi\}$ . Then  $R$  is generated by its subrings  $K$  and  $R_c$ ;  $Q$  is the field of fractions of  $R$ ; and, if  $R_c$  is algebraically closed, there is a unique structure of an  $M$ -field on  $Q$  such that  $Q$  is an  $M$ -extension of  $R$  by Theorem 2.4).

(3.3) DEFINITION. A solution field  $K$  over an  $M$ -field  $L$  is a Picard-Vessiot extension of  $L$  if  $K_c = L_c$  and  $L_c$  is algebraically closed.

With Theorem (3.2) and the results on admissible  $M$ -isomorphisms contained in [1], it is possible to develop a Galois theory for P-V extensions. The development can be made analogous to the presentation of the differential Galois theory of P-V extensions of ordinary differential fields in Kaplansky's *An introduction to differential algebra* [2]. The details, which were worked out in the author's doctoral dissertation, will be omitted here and the principal results merely summarized.

The  $M$ -Galois group of an  $M$ -field  $K$  over an  $M$ -subfield  $L$  is the group  $G$  of all  $M$ -automorphisms of  $K$  over  $L$ . If  $K'$  is an intermediate  $M$ -subfield of  $K$ ,  $L \subseteq K' \subseteq K$ , denote by  $A(K')$  the  $M$ -Galois group of  $K$  over  $K'$ , which is a subgroup of  $G$ . If  $H$  is a subgroup of  $G$ , denote by  $I(H)$  the set of all elements of  $K$  left fixed by the automorphisms in  $H$ ;  $I(H)$  is an  $M$ -subfield of  $K$  and  $L \subseteq I(H) \subseteq K$ . An intermediate  $M$ -subfield  $K'$  of  $K$  is Galois closed in  $K$  if  $K' = I(A(K'))$ , a subgroup  $H$  of  $G$  is Galois closed in  $G$  if  $H = A(I(H))$ , and there is the usual

one-to-one correspondence between the intermediate  $M$ -subfields of  $K$  which are Galois closed in  $K$  and the subgroups of  $G$  which are Galois closed in  $G$ .

(3.4) THEOREM. *Let  $K$  be a  $P$ - $V$  extension of an  $M$ -field  $L$  and let  $G$  be the  $M$ -Galois group of  $K$  over  $L$ .  $G$  is an algebraic matrix group over  $L_c$  and the Galois theory implements a one-to-one correspondence between the connected, algebraic subgroups of  $G$  and those intermediate  $M$ -subfields of  $K$  over which  $K$  is a regular extension. Furthermore, let  $K$  be a regular extension of  $L$ ; a connected algebraic subgroup  $H$  of  $G$  is invariant if, and only if,  $L$  is Galois closed in  $I(H)$ ; and, if  $H$  is invariant,  $G/H$  is isomorphic to the  $M$ -Galois group of  $I(H)$  over  $L$ .*

(3.5) THEOREM. *Let  $K$  be an  $M$ -field of differential type which is a  $P$ - $V$  extension of an  $M$ -field  $L$  and let  $G$  be the  $M$ -Galois group of  $K$  over  $L$ . The Galois theory implements a one-to-one correspondence between the algebraic subgroups of  $G$  and those intermediate  $M$ -subfields of  $K$  over which  $K$  is a separable extension. Furthermore, let  $K$  be separable over  $L$ ; an algebraic subgroup  $H$  of  $G$  is invariant if, and only if,  $L$  is Galois closed in  $I(H)$ ; and, if  $H$  is invariant,  $G/H$  is isomorphic to the  $M$ -Galois group of  $I(H)$  over  $L$ .*

**4. Strongly normal extensions.** Let  $S$  and  $T$  be  $M$ -extensions of an  $M$ -ring  $R$ . In §5 of [1], a structure of an  $M$ -ring on  $S \otimes_R T$  is given such that the canonical homomorphisms of  $S$  and  $T$  into  $S \otimes_R T$  are  $M$ -homomorphisms. The structure is unique; and, in the sequel,  $S \otimes_R T$  will always be considered an  $M$ -ring in this way.

(4.1) DEFINITION. An  $M$ -field  $K$  which is an  $M$ -extension of an  $M$ -field  $L$  is a strongly normal extension of  $L$  if:

- (i)  $K$  is a regular extension of  $L$ .
- (ii)  $K$  is finitely generated over  $L$  (as a field).
- (iii)  $K_c = L_c$  and  $L_c$  is algebraically closed.
- (iv) If  $I$  is a prime  $M$ -ideal in  $K \otimes_L K$  and  $Q$  is the field of fractions of  $(K \otimes_L K)/I$ , then there is a unique structure of an  $M$ -field on  $Q$  such that  $Q$  is an  $M$ -extension of  $(K \otimes_L K)/I$ . This  $M$ -field  $Q$  will be denoted by  $\langle (K \otimes_L K)/I \rangle$ . (Since  $K$  is a regular extension of  $L$ ,  $(0)$  is a prime  $M$ -ideal in  $K \otimes_L K$  and  $\langle (K \otimes_L K)/(0) \rangle = \langle K \otimes_L K \rangle$  is the field of fractions of  $(K \otimes_L K)/(0) = K \otimes_L K$ .)
- (v) The field  $\langle K \otimes_L K \rangle$  is generated by its subfields  $K \otimes 1$  and  $\langle K \otimes_L K \rangle_c$ .

If  $K$  is a regular  $P$ - $V$  extension of an  $M$ -field  $L$ , then properties (i) and (iii) are immediate. If  $I$  is a prime  $M$ -ideal in  $K \otimes_L K$ , then  $(K \otimes_L K)/I$  is an  $M$ -extension of  $K$  with respect to the embedding  $K \rightarrow K \otimes 1 \rightarrow (K \otimes_L K)/I$  and  $K \rightarrow 1 \otimes K \rightarrow (K \otimes_L K)/I$  is an  $M$ -homomorphism of  $K$  over  $L$ . Properties (ii), (iv) and (v) now follow from Theorem (3.2).

(4.2) LEMMA. *If  $K$  is a strongly normal extension of an  $M$ -field  $L$  and  $Q$  is the*

field of fractions of  $K \otimes_L K \otimes_L K$ , there is a unique structure of an  $M$ -field on  $Q$  such that  $Q$  is an  $M$ -extension of  $K \otimes_L K \otimes_L K$ .

**Proof.**  $\langle K \otimes_L K \rangle \otimes_K \langle K \otimes_L K \rangle$  is an  $M$ -extension of  $(K \otimes_L K) \otimes_K (K \otimes_L K)$ ; and the canonical isomorphism  $\phi$  of  $(K \otimes_L K) \otimes_K (K \otimes_L K)$  onto  $K \otimes_L K \otimes_L K$ , mapping  $(k_1 \otimes k_2) \otimes (k_3 \otimes k_4)$  onto  $k_1 \otimes k_2 k_3 \otimes k_4$ , is an  $M$ -isomorphism. There is a unique extension of  $\phi$  to an isomorphism  $\bar{\phi}$  of  $\langle K \otimes_L K \rangle \otimes_K \langle K \otimes_L K \rangle$  into  $Q$ ; and, identifying  $\langle K \otimes_L K \rangle \otimes_K \langle K \otimes_L K \rangle$  with its isomorphic image  $(\langle K \otimes_L K \rangle \otimes_K \langle K \otimes_L K \rangle)^{\bar{\phi}}$ ,  $(K \otimes_L K) \otimes_K (K \otimes_L K)$  is identified with its  $M$ -isomorphic image  $K \otimes_L K \otimes_L K$ . Let  $R$  be the  $M$ -subring of  $\langle K \otimes_L K \rangle \otimes_K \langle K \otimes_L K \rangle$  generated by  $\langle K \otimes_L K \rangle_c \otimes 1$ ,  $1 \otimes K \otimes 1$ , and  $1 \otimes \langle K \otimes_L K \rangle_c$ .  $R$  is an  $M$ -extension of  $K$  with respect to the embedding  $K \rightarrow 1 \otimes K \otimes 1$ ;  $R$  is generated by its subrings  $1 \otimes K \otimes 1$  and  $R_c$  which contains  $\langle K \otimes_L K \rangle_c \otimes 1$  and  $1 \otimes \langle K \otimes_L K \rangle_c$ ; and  $Q$  is the field of fractions of  $R$ . By Theorem (2.4) there is a unique structure of an  $M$ -field on  $Q$  such that  $Q$  is an  $M$ -extension of  $R$ . The  $M$ -system of mappings of  $Q$  into  $Q$  restricts to an  $M$ -system of mappings of  $\langle K \otimes_L K \rangle \otimes_K \langle K \otimes_L K \rangle$  into  $Q$  which coincides on  $R$  with the  $M$ -system of mappings of  $\langle K \otimes_L K \rangle \otimes_K \langle K \otimes_L K \rangle$  into  $Q$  deduced from the  $M$ -system of mappings of  $\langle K \otimes_L K \rangle \otimes_K \langle K \otimes_L K \rangle$  into  $\langle K \otimes_L K \rangle \otimes_K \langle K \otimes_L K \rangle$  by inverse transfer of the ring  $\langle K \otimes_L K \rangle \otimes_K \langle K \otimes_L K \rangle$  to  $Q$ . Since any extension of an  $M$ -system of mappings of  $R$  into  $Q$  to an  $M$ -system of mappings of  $\langle K \otimes_L K \rangle \otimes_K \langle K \otimes_L K \rangle$  into  $Q$  is unique, the above two  $M$ -systems of mappings coincide on  $\langle K \otimes_L K \rangle \otimes_K \langle K \otimes_L K \rangle$  and the  $M$ -field  $Q$  is an  $M$ -extension of  $\langle K \otimes_L K \rangle \otimes_K \langle K \otimes_L K \rangle$ . Therefore this  $M$ -field  $Q$  is an  $M$ -extension of  $K \otimes_L K \otimes_L K$ , and the structure of an  $M$ -field on  $Q$  such that  $Q$  is an  $M$ -extension of  $K \otimes_L K \otimes_L K$  must be unique.

It is now possible to develop a Galois theory for strongly normal extensions of  $M$ -fields and this development can be made analogous to the presentation of a Galois theory for strongly normal extensions of a special class of  $M$ -fields by A. Bialynicki-Birula in his paper, *On Galois theory of fields with operators* [3]. Again, the principal results will be merely summarized here.

Let  $G$  be a connected algebraic group defined over  $L_c$  and let  $V$  be a principal homogeneous space with respect to  $G$  defined over  $L$ . If  $g$  is a point of  $G$  rational over  $L_c$ , the action of  $g$  on  $V$  induces an automorphism  $\bar{g}$  of  $L(V)$  over  $L$ . Let  $\bar{G}(L_c)$  denote the group of automorphisms of  $L(V)$  over  $L$  of the form  $\bar{g}$ , where  $g$  is a point of  $G$  rational over  $L_c$ .

(4.3) THEOREM. Let  $K$  be an  $M$ -field which is an  $M$ -extension of an  $M$ -field  $L$ , with properties (iii) and (iv) of Definition (4.1). Then  $K$  is a strongly normal extension of  $L$  if, and only if, there exists a connected algebraic group  $G$  defined over  $L_c$  and a principal homogeneous space  $V$  for  $G$  defined over  $L$ , having the following properties:

- (i)  $V$  is a model for  $K$  over  $L$ .
- (ii) The  $M$ -Galois group of  $K$  over  $L$  contains  $\bar{G}(L_c)$ .

Conditions (i) and (ii) determine  $G$  and  $V$  uniquely up to an isomorphism. Moreover,  $\bar{G}(L_c)$  is the  $M$ -Galois group of  $K$  over  $L$  and  $G$  is a model of  $\langle K \otimes_L K \rangle_c$  over  $L_c$  for every such  $G$ .

(4.4) THEOREM. Let  $K$  be a strongly normal extension of an  $M$ -field  $L$ . The Galois theory implements a one-to-one correspondence between the connected algebraic subgroups of  $\bar{G}(L_c)$  which are defined over  $L_c$  and those intermediate  $M$ -subfields of  $K$  over which  $K$  is a regular extension.

(4.5) THEOREM. Let  $K$  be an  $M$ -field of differential type which is a strongly normal extension of an  $M$ -field  $L$ . The Galois theory implements a one-to-one correspondence between the algebraic subgroups of  $\bar{G}(L_c)$  which are defined over  $L_c$  and those intermediate  $M$ -subfields of  $K$  over which  $K$  is a separable extension.

In [3], Theorem (4.5) is stated only for an  $M$ -field  $K$  of characteristic zero in which the  $M$ -system of mappings consists of the identity automorphism and derivations. Using the separability of  $K$  over the  $M$ -subfields being considered to replace the assumption of zero characteristic, the above generalization follows readily. If  $K$  is an  $M$ -field of characteristic  $p \neq 0$  in which the  $M$ -system of mappings consists of the identity automorphism and derivations, then  $K^p \subseteq K_c = L_c$  and  $K = L = L_c$ , since  $L_c$  is algebraically closed. But if the  $M$ -system of mappings of  $K$  into  $K$  contains higher derivations of arbitrarily large rank or infinite rank,  $K$  may be a nontrivial strongly normal extension of  $L$ .

(4.6) DEFINITION. An element  $a$  of an  $M$ -field  $K$  is a Picard-Vessiot element over an  $M$ -subfield  $L$  of  $K$ , if the vector space over  $L$  spanned by the elements  $as$ ,  $s \in S'(M)$  is finite-dimensional. The dimension of the vector space is the degree of  $a$  over  $L$ .

(4.7) LEMMA. Let  $K$  be a strongly normal extension of an  $M$ -field  $L$  and let  $a \in K$ .  $a$  is a P-V element over  $L$  if, and only if, the vector space over  $L_c$  spanned by the images of  $a$  under  $M$ -automorphisms of  $K$  over  $L$  is finite-dimensional.

(4.8) THEOREM. Let  $K$  be a strongly normal extension of an  $M$ -field  $L$ .  $K$  is a P-V extension of  $L$  if, and only if,  $K$  is generated over  $L$  by its P-V elements over  $L$ .

**Proof.** If  $K$  is a P-V extension of  $L$ , let the notation be as in Definition (3.1).  $K = L\langle k_1, k_2, \dots, k_h \rangle$  and  $k_1, k_2, \dots, k_h$  are P-V elements over  $L$  by Theorem (3.2). Conversely, suppose  $K$  is generated over  $L$  by its P-V elements over  $L$ . Since  $K$  is finitely generated over  $L$ , there exists a finite number of P-V elements of  $K$  over  $L$ , say  $a_1, a_2, \dots, a_i$ , which generate  $K$  over  $L$ . The vector space over  $L_c$  spanned

by the images of  $a_1, a_2, \dots, a_i$  under  $M$ -automorphisms of  $K$  over  $L$  is finite-dimensional by Lemma (4.7). Let  $k_1, k_2, \dots, k_h$  be a basis for this vector space over  $L_c$ . Then  $K = L \langle k_1, k_2, \dots, k_h \rangle$  and, since  $k_1, k_2, \dots, k_h$  are linearly independent over  $L_c = K_c$ , there exist  $h$  elements  $t_1, t_2, \dots, t_h$  in  $S'(M)$  such that  $W(k_1, k_2, \dots, k_h; t_1, t_2, \dots, t_h) = W_0 \neq 0$ . If  $\phi$  is an  $M$ -automorphism of  $K$  over  $L$ ,  $(k_\alpha s)^\phi = k_\alpha^\phi s = \sum_{\beta=1}^h c_{\alpha\beta}(\phi) \cdot (k_\beta s)$ ,  $s \in S'(M)$  and  $1 \leq \alpha \leq h$ , where  $(c_{\alpha\beta}(\phi))_{1 \leq \alpha, \beta \leq h}$  is a matrix over  $L_c$ . For any choice of  $h$  elements  $s_1, s_2, \dots, s_h$  in  $S'(M)$ ,

$$\begin{aligned} & (W_0^{-1} W(k_1, k_2, \dots, k_h; s_1, s_2, \dots, s_h))^\phi \\ &= (\det(c_{\alpha\beta}(\phi))_{1 \leq \alpha, \beta \leq h} \cdot W_0)^{-1} (\det(c_{\alpha\beta}(\phi))_{1 \leq \alpha, \beta \leq h} \cdot W(k_1, k_2, \dots, k_h; s_1, s_2, \dots, s_h)) \\ &= W_0^{-1} W(k_1, k_2, \dots, k_h; s_1, s_2, \dots, s_h). \end{aligned}$$

Since  $L$  is Galois closed in  $K$  by Theorem (4.4),  $W_0^{-1} W(k_1, k_2, \dots, k_h; s_1, s_2, \dots, s_h) \in L$  for every choice of  $h$  elements  $s_1, s_2, \dots, s_h$  in  $S'(M)$  and  $K$  is a P-V extension of  $L$ .

(4.9) THEOREM. *Let  $K$  be a strongly normal extension of an  $M$ -field  $L$ . Then  $K$  is a P-V extension of  $L$  if, and only if, the  $M$ -Galois group of  $K$  over  $L$  is affine.*

#### REFERENCES

1. H. F. Kreimer, *The foundations for an extension of differential algebra*, Trans. Amer. Math. Soc. **111** (1964), 482-492.
2. Irving Kaplansky, *An introduction to differential algebra*, Hermann, Paris, 1957.
3. A. Bialynicki-Birula, *On Galois theory of fields with operators*, Amer. J. Math. **84** (1962), 89-109.
4. E. R. Kolchin, *Algebraic matrix groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations*, Ann. of Math. **49** (1948), 1-42.
5. ———, *Picard-Vessiot theory of partial differential fields*, Proc. Amer. Math. Soc. **3** (1952), 596-603.
6. ———, *Galois theory of differential fields*, Amer. J. Math. **75** (1953), 753-824.

FLORIDA STATE UNIVERSITY,  
TALLAHASSEE, FLORIDA