1972

Differential Rings: Embedding Theorems And Related Ideals

Jay Ladd Delkin

DIFFERENTIAL RINGS:
EMBEDDING THEOREMS AND RELATED IDEALS

by

Jay Ladd Delkin

Department of Mathematics

Submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy

Faculty of Graduate Studies
The University of Western Ontario
London, Canada

July 1972

ABSTRACT

The concept of a <u>differential ring</u>, as a system for which one has operations of addition, multiplication, and derivation, is defined and discussed. For some differential rings this derivation is <u>inner</u> and is consequently definable in terms of the other operations of the system. Given an associative differential ring K, Ore has shown that there exists a ring K(w), the ring of the "noncommutative polynomials" in w over K, which extends the ring K and for which the derivation initially given in K has been extended to an inner derivation in the larger ring.

The construction of analogous extensions K(w) is carried out for rings K which are not (necessarily) associative, and, even considering only associative K, in a more detailed manner than has been done before. One proceeds by stipulating which properties one would like such an embedding ring to satisfy and the realization of this ring K(w) is then shown in terms of operators acting on a (nonassociative) module.

It is next shown that, if K satisfies certain basic conditions, K(w) admits of no proper ideals. Relaxing the conditions on K renders possible the existence of ideals of K; along these lines, a result on the existence of ideals given by Amitsur is generalized and proved.

If K is a division ring, then K(w) may be extended to a division ring $K(w,w^{-1})$, which, for associative K, includes, as a proper subring, a division ring extension defined by Ore. The construction of $K(w,w^{-1})$ is quite similar to the construction of K(w), in terms of operators on a module.

The divisibility conditions on $K(w,w^{-1})$ correlate with certain conditions on the module. By introducing an operation of multiplication in the module, one forms a ring extension of K in which extension all linear differential equations in K have solutions. Continuing along these lines, one constructs a ring T which is closed with respect to linear differential equations (as, analogously, an algebraically closed field is closed with respect to algebraic equations).

ACKNOWLEDGEMENT

I should like to express my deep appreciation to my supervisor, Doctor John T. Moore, and to Doctor Donald O. McKay and Doctor Richard L. Biggs, for their generous help and support in this effort.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION TO DIFFERENTIAL ALGEBRA

1.1 Its Genesis.

The subject of differential algebra is a branch of algebra which arises from sources both in analysis and in algebra. The central idea of differential algebra is to develop an algebraic theory of differentiation and to study systems in which such an algebraic differentiation has been defined. The concept of the derivative, as the result of a differentiation operation, arises in elementary calculus. It is this fundamental concept of the derivative which, from the point of view of differential algebra, is to be considered in an algebraic context.

Analysis may be considered to contain two principal ingredients: topology and algebra. In studies of the concept of differentiation as it is usually defined (whether involved with the simple derivative or with the related concepts of differential, partial derivative, left and right derivatives, etc.), one finds both the topological and the algebraic aspects interwoven. The idea of the limit of the ratio of finite differences is topological; the sum and product laws for derivatives (as given precisely in Section 1.2 below) are algebraic. If one now abstracts from all considerations of a topological nature, the operation of differentiation becomes a purely algebraic mapping subject to certain algebraic laws. The sum and product laws in particular require no topology for their formulation and may be formulated (as will be seen) in a more general context than is usually done. From such considerations as here suggested, one is led to the subject of differential algebra which then has its most natural genesis in analysis. Thus differential algebra arises from the attempt to treat the process of differentiation in analysis in a purely algebraic manner. It may be remarked that a considerable amount of elementary calculus can be developed without explicit reference to limits or other topological notions, but with the sole use of algebraic laws (which could be postulated initially, rather than derived from topological considerations). In differential algebra one merely proceeds further along these lines.

However, in spite of what has just been stated, it is not necessary to approach the subject of differential algebra through the medium of analysis. Differential algebra also arises quite naturally in algebra itself, quite apart from any reference to analysis, and one has simply to recognize this fact. In the theory of associative rings, the commutator or Lie product cb-bc of arbitrary elements b and c of such a ring may be considered to denote a departure (if any) from commutativity, this commutator being zero when c and b commute. Holding either b fixed or c fixed, the commutator defines on the elements of the ring a unary operation which may be shown by routine computations to satisfy the sum and product laws for derivatives; this example is that in (5) of Section 1.2 below. It is then only natural to regard this type of mapping as a differentiation or, as one generally says in algebra, a derivation. This particular type of derivation is called an inner derivation. However one approaches the subject of differential algebra, it is inevitable that the sum and product laws must play an essential role in the central concept of a derivation. Precise definitions are given in Section 1.2 below. In line with the terminology of analysis, the image of an element under a derivation mapping is called its derivative.

As has already been stated, differential algebra is a branch of algebra; and algebra is the study of algebraic systems. An algebraic system $\{S;0_1,\ldots,0_n\}$ is an abstract set of elements on which certain operations, $0_1,\ldots,0_n$, have been defined.

In order to pursue differential algebra in a profitable way, it is desirable to fix one's attention on a particular type of algebraic system in which one can perform two binary operations called addition and multiplication, and one unary operation called derivation, in accordance with the appropriate rules pertaining to such operations. The type of algebraic system selected for this purpose is defined in Section 1.2 below.

1.2 Basic Definition and Examples.

Although the subject of differential algebra is sometimes studied in a more general context as discussed in Section 1.4 below, for the purpose of this thesis differential algebra is restricted to a study of differential rings. A differential ring may be regarded as an ordinary ring to which a derivation has been added as an operator, as will be seen in the formal definition below. While rings with an "involution" - also a unary operator - have been studied extensively, insofar as the writer is aware this is the first time that differential rings - as rings with the unary differential operator - have been studied in a way that is at all comparable. Other studies of differential rings or algebras have studied more general types of systems, of which differential rings are but a special case, or else have involved themselves with matters somewhat "tangent" to the central core of the subject.

The term "ring" invariably means, throughout this thesis, either an ordinary ring or a differential ring (as the context may dictate) <u>for which multiplication need not necessarily be associative</u>.

<u>Definition</u>: A differential ring $\{K;+,\cdot,'\}$ is a set K in which are defined the two binary operations of addition (+) and multiplication ($\cdot$) and the unary operation of derivation ('), subject to the following conditions:

(1) $\{K;+\}$ is an abelian group.

(2) Multiplication is (left and right) distributive with respect to addition. Thus the mapping of b to cb or b to bc, for fixed c and with b ranging over K, is an endomorphism of the group $\{K;+\}$.

(3) For arbitrary $b,c \in K$

(i) $(b+c)' = b'+c'$. This property is called the <u>Sum Law</u> and shows that the derivation is an endomorphism of $\{K;+\}$.

(ii) $(bc)' = bc'+b'c$. This property is called the Product Law.

Upon deleting or ignoring the derivation operator, the differential ring becomes an ordinary ring, defined by conditions (1) and (2). It is convenient to use the symbol K to denote either the ring $\{K;+,\cdot\}$, the differential ring $\{K;+,\cdot,'\}$, or, on occasion, just the set K of the ring, as the context may dictate.

Powers of an element $b \varepsilon K$ are defined inductively: $b^0 = 1$ (if K contains 1), $b^1 = b, \ldots, b^{i+1} = (b^i)b$, this definition being meaningful even if the multiplication of K is nonassociative. The symbol b' denotes the derivative of $b \varepsilon K$ (the result of differentiating b or applying the derivation mapping to b); more generally, $b^{(i)}$ denotes the ith derivative of b in accordance with the inductive definition: $b^{(0)} = b$ and $b^{(i+1)} = (b^{(i)})'$. It may be observed that this definition implies that $b^{(1)} = b'$. Notations b'', b''', ... may also be used, as in elementary calculus, to indicate these higher derivatives of b. On occasion, the derivation ' will also be denoted by the lower case letter d, with $d^i(b) = b^{(i)}$ for $b \varepsilon K$.

Many of the familiar concepts of ring theory carry over with appropriate modifications to the theory of differential rings. In place of ideals and homomorphisms, one now has differential ideals and differential homomorphisms. A differential homomorphism of a differential ring $\{K;+,\cdot,'\}$ is a homomorphism of the underlying ring $\{K;+,,\}$ which commutes with the derivation; the special property of an ideal which is the kernel of a differential homomorphism (i.e., a differential ideal) is that it is closed with respect to the derivation (as shown by Kaplansky [7]). It is natural to pursue differential ring theory along lines which parallel those of ordinary ring theory, asking the analogous questions about differential rings that one asks about ordinary rings. Thus one might try to find structure theorems and study extensions, radicals, and related concepts. There is a discussion of some of these matters in Kaplansky [7], including the Galois theory of differential field extensions and matrix representation of Galois groups. This thesis, however, does not concern itself directly with topics of the kind discussed by Kaplansky.

Some examples of differential rings follow. In the first three examples, the derivation is the usual differentiation operator of analysis.

1. The ring of all polynomials in one variable over the real or complex numbers.

2. The ring of all infinitely differentiable real-valued functions on the real numbers.

3. The ring of all analytic functions on the complex plane.

4. An arbitrary ring K, in which the derivation is defined by $c' = 0$ for all $c \in K$.

5. An arbitrary associative ring K, in which the (inner) derivation is defined by $c' = tc-ct$ for some fixed element $t \in K$. This type of ring, as well as those of (4), (7), and

(9), includes cases when the differential ring K is finite. If K is commutative, then tc-ct = 0, and this example reduces to that of (4) above.

6. An arbitrary Lie ring K, in which the derivation is defined by c' = tc (or c' = ct) for some fixed element $t \in K$. This type of derivation is also called an inner derivation because of the genesis of the Lie product as a product commutator in an associative ring. Routine computations (using the Jacobi and antisymmetric Lie ring laws) show that the sum and product laws are satisfied, as required for a derivation.

7. The algebra K over a field F with basis elements 1, i, and j where $i^2 = j^2 = -1$, ij = ji = 0, i' = j, j' = -i, and, for all $c \in F$, c' = 0. These rules suffice to define K as a differential ring. Moreover, K is nonassociative because (ii)j = -j whereas i(ij) = 0. It may be shown in this case that the underlying ring K is actually a Jordan algebra. It may be observed that types (4), (8), and (9) also include examples of nonassociative differential rings.

8. The ring R defined from an arbitrary ring K in the manner described below. Let the elements of R be the ordered pairs (a,b) of elements $a,b \in K$. Equality is defined by: (a,b) = (c,d) if a = c and b = d. Addition and Multiplication are defined respectively by: (a,b)+(c,d) = (a+c,b+d) and (a,b)(c,d) = (ac,ad+bc). Derivation is defined by: (a,b)' = (0,b). Routine computations show that the sum and product laws for the derivation are satisfied as well as the usual ring properties, and so R is a differential ring. If K is the field of real numbers, then R is the well-known

system of the Clifford numbers. If K is an arbitrary field, then R is an algebra over K with basis elements 1 = (1,0) and v = (0,1) where $v^2 = 0$.

9. The ring R defined from a differential ring K as in (8), except that derivation is defined by: (a,b)' = (0,a'). Again, routine computations show that the necessary conditions for a differential ring are satisfied by R. This example is that of Jacobson [6].

10. The differential ring of polynomials over a field F in a single indeterminate, as given by Kurosh [15].

1.3 Historical Prelude.

The literature on derivations in algebra tends to divide itself into three main classes: the work of Ritt, Kolchin, and others in differential algebra with its origin in analysis; miscellaneous material on derivations in an algebraic context; and the work initiated by Oysten Ore. There is also additional material in the literature further removed from the subject of differential algebra as conceived in this thesis, but still within the broad general context of the subject.

Differential algebra first developed from the works of Ritt [20-21] and Kolchin [8-14], and this in turn arose from the classical theory of differential equations. Typical of these early papers is Ritt's paper on differential equations from the algebraic standpoint [20], although in this paper differential algebra had barely emerged from analysis as a subject in its own right.

Ritt, Kolchin, and others with similar motivations and background noticed that much of classical differential equations theory, especially the theory of linear homogeneous differential equations, is algebraic in nature. It was then a relatively easy step to a consideration of formal differential equations defined in differential rings from which all topological considerations have been omitted; these differential rings were originally taken to be commutative and associative so as to be interpretable as rings of functions. Seidenberg [25] and others used these formal differential equations to define algebraic differential manifolds. Such writers have generally studied in the context of the classical differential theories of analysis but with the omission of all topological considerations.

From the point of view of algebraic analysts such as Ritt and Kolchin, the elements of a differential ring are (implicitly) functions. Abraham Robinson, in two papers on what he calls local differential algebra [22-23], proceeds further along the lines indicated by Ritt and Kolchin and considers certain types of homomorphisms which have the same effect as the classical substitution of particular values into the argument of a function. From a consideration of such homomorphisms, Robinson can, in effect, perform these substitutions without having to postulate explicitly that the elements of the differential ring be functions. Robinson applies these methods and considerations to the boundary value problems of differential equations.

Many writers discuss derivation algebras on arbitrary rings, or on special classes of rings, and others discuss certain classes of derivations. But such matters are not a part of what is considered here to constitute differential algebra. Derivation algebras are algebras whose elements are themselves ring derivations, with the operations of addition and Lie multiplication defined on the derivations. Differential algebra, however, concerns itself with differential rings of abstract elements where a unary operation of derivation has been postulated as one of the operations of the ring. It has already been noted that in differential ring theory as opposed to ring theory in general, all homomorphisms must be <u>differential</u> homomorphisms (with the understanding, however, that there are important examples of differential rings for which every ordinary homomorphism is also a differential homomorphism). Much of the material that has appeared in the last thirty years on derivations in algebra has little direct bearing on the subject of differential algebra as conceived in this thesis; this is especially true of a large amount of material that properly belongs to Lie theory.

1.4 Noncommutative Polynomials and other Algebraic Approaches.

The work of Oysten Ore is considered here. As indicated in his paper [16], Ore's original motivations were those of Ritt and Kolchin; however, his later work proceeds in a new direction and is developed from strictly algebraic premises.

In his paper [17] on this subject, Ore constructs a ring of noncommutative polynomials as generalized polynomials over an arbitrary associative division ring. It is here that

Ore first develops his theory from a strictly algebraic point of view. In this paper, certain types of generalized polynomials in one indeterminate are constructed, subject to certain initially postulated conditions. These include the possibility that every polynomial can be put into a "canonical" form with the coefficients from the division ring on the left (or right) as well as the postulated existence of a well-behaved degree function. Involved in his construction is a "conjugacy" mapping and a generalized derivation mapping (this generalized derivation not always satisfying the product law). Ore observed that, if his conjugacy mapping is taken to be the identity mapping, then his generalized derivation is indeed an ordinary derivation (as defined in Section 1.2 above).

Amitsur, Cohn, and Smits assume a generally nontrivial conjugacy mapping in discussing Ore's construction or generalizations thereof. However, unless the contrary is explicitly stated, in any reference here to Ore's conjugacy mapping the identity mapping will be understood. With this assumption of a trivial conjugacy mapping, Ore's polynomials are then polynomials in an indeterminate or element w, over an associative division ring K, with the important rule $wb-bw = b'$ holding for all $b \in K$.

From the point of view of differential algebra and of this thesis, a ring K is initially given as a differential ring on which a derivation has been postulated. Ore's point of view, however, was that b' is a convenient name given to the difference wb-bw as a function of b, and this function is discovered to satisfy the requirements for a derivation. Ore's paper is primarily devoted to the Division and Euclidean algorithms, factorization, and other related matters in his ring of noncommutative polynomials. One of the points of contact of Ore's work with this thesis, however, is that the derivation defined in the basic ring K is extended to an inner derivation given by wu-uw = u' for all u in the polynomial ring. This ring of noncommutative polynomials is denoted by the symbol K(w), the notation indicating that K(w) is the ring extension of K defined, with the appropriate rules of operation, by the adjunction of w.

Most recent writers dropped the condition of divisibility, requiring principally that K be associative. Naturally one does not obtain all of Ore's particular results with the use of these more general rings K.

Jacobson and Amitsur investigated the problem of finding ideals in K(w) for associative K, all ideals in K(w) being also differential ideals. Jacobson showed [4] that if K is an associative division ring of characteristic zero, then either K(w) is simple or there must be an element $t \varepsilon K$ such that t behaves like the w of K(w): that is, tb-bt = b' for all $b \varepsilon K$. Amitsur showed [1] that Jacobson's result holds also for simple associative rings of characteristic zero (simple in the ordinary rather than in the differential sense). It was further shown by Amitsur that the proper ideals of K(w), for the case of a simple associative ring K, are generated by the monic elements in the center of K(w) and of degree greater than zero. Amitsur also characterized these ideals in terms of what he calls universal differential equations in K, these being equations satisfied by all elements of K; and, conversely, he showed that these ideals determine all universal differential equations. For an arbitrary associative differential ring K with identity, Amitsur and others observed that K(w) may be constructed as the ring of endomorphisms of {K;+} generated by the left multiplications (the mappings c to bc for fixed b and arbitrary c in K) and the derivation mapping. In this construction each element $b \in K$ is identified with the left multiplication that maps each c to bc, whereas w is the derivation mapping itself.

Cohn [2] showed that any associative ring with a degree function that satisfies certain basic properties must be a (generalized) Ore ring K(w) for some ring K. It is important to note here, however, that this result depends on the assumption of a (generally) nontrivial conjugacy mapping.

Smits, in his two papers [26-27], generalizes the Ore construction for rings with a derivation which is nilpotent (a derivation such that, for some n, $c^{(n)} = 0$ for all c in the ring), by adjoining an element w^{-1} to the Ore polynomials. This element w^{-1} serves as the multiplicative inverse of w in the generalized system.

Finally, Qureshi [19] constructs a generalized ring extension for generally nonassociative K, which includes the constructions of Ore and Smits as special cases. Qureshi, in [18], also postulates linear independence and a generalized derivation and shows that these assumptions lead to the Ore polynomials.

Whereas the writers noted in the preceding discussions used the Ore construction of K(w) only with K understood to be associative (with the exception of Qureshi's generalized construction which includes the Ore polynomials), Schafer [24] (without relating to the work of Ore) specifically set out to define a more general concept of *inner derivation* which would reduce to the usual notion in the important special cases of the associative and Lie rings (the examples of (5) and (6) in Section 1.2 above). His inner derivation concept is discussed at length in Section 1.5 below.

A parallel subject of difference algebra has been developed by certain mathematicians, though this subject has no connection with the material of this thesis. Difference algebra and differential algebra can be related by means of exponential mappings and other methods which properly belong to Lie theory.

Other people have studied generalizations of differential algebra: with types of generalized derivations that are not closed with respect to the given ring (as suggested by the differential of a function in analysis); or which satisfy a more general form of the product law (such as the generalized derivations of Ore's polynomials or the exterior derivative of Exterior Algebra); or with differential rings with more than one derivation given (as suggested by the partial and directional derivatives of analysis). Further removed from the subject of this thesis, but still within the general context of the broader subject, are various differential operators; these operators include the differential mapping of a differential group (as applied mainly in algebraic topology, where it is a boundary operator in homology theory).

1.5 Embedding Problems and Nonassociative Inner Derivations.

An inner derivation for an associative or Lie ring is an operation that is easily described because it is definable in terms of the usual operations one already has in the ring. If the derivation operator of an associative differential ring is inner, then (as has already been noted in the case of Ore's work) every ideal of the ring must be closed under the derivation, and hence is a differential ideal (as remarked above in Section 1.2). Moreover, every formal differential equation in a ring of this kind is simply an ordinary algebraic equation; this fact is of theoretical interest despite its apparent uselessness in the actual solution of these equations. Because of the simplifications inherent in the inner derivation concept, it is appropriate to consider the possibility of extending derivations to inner derivations (in the sense made precise below).

For an associative ring K, the following question is answered in the affirmative by the noncommutative polynomial construction of Ore: Is it possible to extend K to a differential ring S in which the derivation is inner and such that this derivation induces (as its restriction to K) the given derivation in K? Specifically, is it possible to find a differential ring S subject to the conditions:

(1) K is a differential subring of S (i.e., K is a subring of S and the value of a derivative b' of b ε K is independent of whether b is regarded as an element of K or of S);

(2) The derivation in S is inner, so that x' = wx-xw for some fixed w ε S and all x ε S?

The answer to this question provides a solution for an <u>embedding problem</u> for the associative ring K. To ask the analogous question of rings which are not assumed to be associative, one must first define a more general concept of "inner derivation" for rings. For a general ring K, it is not appropriate to define an inner derivation as a simple mapping of x to wx-xw: because, unless K is associative, the product law for derivatives may not be valid. The product law requires that

$$w(xy)-(xy)w = (wx-xw)y+x(wy-yw), \quad \text{for } x,y,w \in K,$$

and equality is clear only in those cases where w, x, and y comprise an associating triplet.

Schafer was the first person to consider a general concept of "inner derivation" to apply to rings that are not necessarily either associative or of the Lie type. His motivating interests are clear from his paper [24]. In both the associative and the Lie cases, the set E of all the inner derivations in a ring T is closed with respect to the operations of addition and Lie multiplication. This is equivalent to stating that this set E of endomorphisms is a Lie ring. Schafer endeavored to have these closure properties of E preserved under a more general concept of "inner derivation" in T and at the same time to have his definition reduce (as much as possible) to the usual one in the associative and Lie cases.

In order to include the Lie inner derivations in a comprehensive definition, it was necessary to involve, in an essential way, the left and right multiplications (the mappings of x to bx and of x to xb) in the ring. Accordingly, Schafer's central idea was to consider the left and right multiplications of an arbitrary (generally nonassociative) ring T and to consider further the Lie ring E of endomorphisms of {T;+} generated by these left and right multiplications, i.e., the smallest Lie ring containing all left and right multiplications. A derivation of T is then said to be "inner" in Schafer's sense if it is contained in this Lie ring E of endomorphisms, the inner derivations constituting a Lie subring of E. Schafer shows in his paper that his definition agrees precisely with the usual definition of a derivation given for Lie rings, and that it <u>almost</u> agrees with that given for associative rings. Unfortunately, his definition renders as inner some associative ring derivations which are not inner by the usual commutator definition. Jacobson [5] and others obtain some results pertaining to Schafer's inner derivation concept.

There is, however, no need in this thesis to be bound by Schafer's desire to leave the usual Lie ring concept of inner derivation intact. Moreover, by making the concept more refined, one may hope to obtain more results in the way of structure. It is very desirable, however, to have an inner derivation reduce to the commutator type mapping in the associative cases without any exceptions for which this is not true.

As the term "inner derivation" is already used by Schafer and others in connection with rings that may not be either associative or Lie, the term "strong inner derivation" is adopted for the analogous concept that is defined and used in this thesis. It will be seen that a "strong inner derivation" is <u>formally</u> identical with the ordinary (associative) concept.

<u>Definition</u>: Let T be a ring with an element w that associates with all pairs of elements of T in the following sense:

$w(xy) = (wx)y$, $x(wy) = (xw)y$, $x(yw) = (xy)w$ for all $x,y \in T$.

Then the mapping x' to $wx-xw$ defines a <u>strong inner derivation</u> in T.

It is not obvious, of course, that such mappings exist for a given nonassociative ring T, but, if they exist, strong inner derivations are indeed derivations that satisfy the sum and product laws as given in Section 1.2. It may further be shown that these derivations are also inner in the sense of Schafer, although the converse is not generally true.

If T is associative, it is clear that the concepts of inner derivation (as usually defined for associative rings) and strong inner derivations coincide. A simple computation shows that the set of strong inner derivations on a ring is a Lie ring with respect to the usual Lie ring operations (i.e., a derivation algebra as discussed in Section 1.3). However, while such Lie ring closure is of great importance in the work of Schafer and others, it is of no special relevance to this thesis.

Amitsur [1] and others define the concept of "inner derivation" in still different ways (even in the case of associative rings), but these definitions are not used here.

1.6 Basic Goals.

A major task is to solve an embedding problem for a differential ring K by extending K to a larger ring S, where K is no longer assumed to be necessarily associative, where the derivation in K is thereby extended to a strong inner derivation in S, and where S and K belong to the same general class of rings. To illustrate this third matter, one may point out (for example), that if K is associative, it is desirable that S also be associative. As it is generally the case in mathematics that one constructs the smallest possible system that solves the given problem under consideration, it is further desired that S be minimal, in the sense that no proper subring of S also suffices to solve this embedding problem.

If K is associative but has no other special proper ties (such as being a division ring) that one would wish to preserve in the embedding ring, this embedding ring S may be taken to be the ring K(w) of the noncommutative polynomials of Ore. However, if K is a division ring, whether associative or nonassociative, it is desirable that the embedding ring S also be a division ring. Ore, in his paper [17], extended the ring K(w) to a larger division ring in the case where K is itself an associative division ring. A more general construction of an embedding division ring (which, in the case of associative K, will be shown to include Ore's division ring as a subring) will be carried out in this thesis.

Under the assumption that K satisfies certain minimal conditions, the possibility of nontrivial ideals in the embedding ring K(w) will be investigated. This investigation will relate to the work of Amitsur and Jacobson, as discussed in Section 1.3 above.

A (nonassociative) module construction will afford an actual realization of these embedding rings. It will be shown that, in the case where K is a division ring with identity and characteristic zero, the related divisibility of the embedding ring directly entails results concerning the solvability of (algebraic) differential equations in K, or in extensions of K that one naturally defines. This transition from divisibility in the embedding ring to the solvability of differential equations is effected in terms of this module construction.

Theorems are numbered consecutively throughout the thesis without reference to chapter or section. Lemmas are considered to be preliminary to theorems and so are labeled consecutively, in groupings leading up to each theorem. In making reference to a lemma, the section that contains the lemma is generally included only if it is in an earlier grouping.

CHAPTER 2

THE BASIC EMBEDDING PROBLEM

2.1 Preliminary Ring Concepts.

A differential ring K may conveniently be regarded as a module over the ring of integers, where an expression of the form nb, for $b \in K$ and n an arbitrary integer, has its usual meaning. If, further, K is of characteristic zero and $\{K;+\}$ is a divisible group, then K may also be regarded as a module over the field of rational numbers, an expression of the form $(m/n)b$ for m and n integers $(n \neq 0)$ being well-defined. If K contains an identity, a product $(m/n)b$ may also be interpreted as a product within the ring K rather than as a module product. To obtain this latter interpretation, the rational number m/n is identified with the element $(m/n)\cdot 1 \in K$. It can be easily shown from linearity properties of the derivative, that if $rb \in K$ for a rational number r, then $(rb)' = rb'$.

Any differential ring K may be embedded in a ring K(1) which contains an identity 1. The procedure is the same as for an ordinary ring but with a definition given for derivation in the ring extension. One then lets K(1) consist of the ordered pairs (a,m) for $a \in K$ and m an integer, subject to the following rules:

$(a,m) = (b,n)$ if and only if $a = b$ and $m = n$.

$(a,m)+(b,n) = (a+b,m+n)$.

$(a,m)(b,n) = (ab+na+mb,mn)$.

$(a,m)' = (a',0)$.

The identity of K(1) is (0,1) and K is effectively embedded in K(1) by the identification of (a,0) with a.

Inasmuch as the assumption of an identity in K is a considerable simplifying factor in our discussion and any ring without an identity can so readily be extended to a ring with an identity, it is henceforth assumed that the basic ring K does contain the identity 1.

In a differential ring K the elements whose derivatives are zero are of notable importance. They are called the <u>constants</u> of the ring. It can easily be shown that the elements of the form $r \cdot 1$ for rational r (where these are defined) are constants.

An element $b \varepsilon K$ <u>commutes</u> with $x \varepsilon K$ if $bx = xb$, and the subset of K whose elements commute with all elements of K is (as usual) called the <u>center</u> of K. It will also be said that an element b <u>associates</u> with elements x and y in K if each of the following holds: $x(yb) = (xy)b$, $x(by) = (xb)y$, $b(xy) = (bx)y$, $y(xb) = (yx)b$, $y(bx) = (yb)x$, $b(yx) = (by)x$. The set of all elements b which associate with all pairs x,y of elements of K is called the <u>nucleus</u> of K. The intersection of the center and the nucleus is called the <u>hub</u> of K.

The nucleus, center, and hub of K are each closed under the operation of derivation. For example, if b belongs to the center, then $bx = xb$ for all $x \in K$. Differentiating each side of this equality and using the product law for derivatives, one obtains $b'x+bx' = x'b+xb'$. In particular, b commutes with x', so that $bx' = x'b$, whence $b'x = xb'$. This means that b' is in the center as desired, showing closure of the center under derivation. The nucleus is also closed under derivation, as one differentiates each equality of association and proceeds (as with the center above) to obtain the corresponding equality for b'. Thus, to show that $b'(xy) = (b'x)y$, one differentiates $b(xy) = (bx)y$ to obtain $b'(xy)+b(x'y)+b(xy')$ $= (b'x)y+(bx')y+(bx)y'$; the conclusion then follows from $b(x'y) = (bx')y$ and $b(xy') = (bx)y'$. It now easily follows that the hub is also closed under derivation.

The usual definition of simplicity is that a ring is simple if it admits of no nontrivial factor ring. Since by "ring" may be meant either an ordinary ring or a differential ring, it is important to note that K may be simple either as the ordinary ring $\{K;+,\cdot\}$ or as the differential ring $\{K;+,\cdot,'\}$. (Neither type of simplicity should be confused with that of "differentiably simple" used by some writers.)

For nonassociative rings, there are two types of "division ring", depending on whether equations of the type $ax = b$ and $ya = b$ (for $a \neq 0$ and unknowns x and y) are required to have unique solutions or merely to have solutions. By <u>division ring</u> in this thesis is meant the stronger concept: given any elements a and b of the ring with $a \neq 0$, there is exactly one x such that $ax = b$ and exactly one y such that ya = b.

For future reference the Leibniz formula for the nth derivative of a product is given here. This formula is valid in any abstract differential ring as well as in the familiar rings of analysis, and its proof by induction is analogous to the usual one found in analysis texts.

$$(ab)^{(n)} = \sum_{i=0}^{n} \binom{n}{i} a^{(i)} b^{(n-i)}.$$

When n = 1, the Leibniz formula reduces to the usual product law for derivatives.

2.2 Evolution of the Embedding Ring.

It has been observed earlier that the ring of Ore polynomials provides a solution of the embedding problem for an associative differential ring K. This polynomial embedding ring has an inner derivation which induces the given derivation on the elements of K. In the absence of associativity in the ring K, it is not immediately clear that the related embedding problem can be solved in an analogous manner.

It will be of interest, however, tentatively to suppose the existence of a ring R with a special element w which behaves like the w of the Ore polynomial construction for associative K. Specifically, this would assume that a derivation exists in R such that u' = wu-uw for all $u \in R$ where, for $a \in K$, a' = wa-aw gives the derivative of a already defined in K. The immediate plan, therefore, is to assume the existence of such a ring R, and to explore elementary consequences of this assumption.

In line with the above remarks, it is now assumed that K is embedded in a differential ring R (the identity of R being that of K), and that there exists an element w in R, but not in K, such that:

(1) w is contained in the nucleus of R.

(2) $wu-uw = u'$ for each $u \in R$.

Property (1) above, as will be recalled, implies that w associates with every pair of elements of R. This associative property ensures that $wu-uw = u'$ defines a strong inner derivation in R. Another consequence of Property (1) is that, for non-negative integers m and n, $(w^m)(w^n) = w^{m+n}$.

The existence of a ring R satisfying the above two properties will be shown in the sequel. The following results are relative to the assumption that there does exist such a ring R.

The following lemma shows that powers of w are also contained in the nucleus of R, thus expanding on Property (1) above.

Lemma 1: For all integers $n \geq 0$, w^n is contained in the nucleus of R.

Proof: It must be shown that, for all $u,v \in R$:

(a) $(uw^n)v = u(w^n v)$.

(b) $(uv)w^n = u(vw^n)$.

(c) $(w^n u)v = w^n(uv)$.

The proof of (c) is analogous to that of (b), so only the proofs of (a) and (b) are given.

(a) One proceeds by induction on n.

If $n = 0$, then $w^n = w^0 = 1$, and the conclusion is clear.

As an <u>induction hypothesis</u>, one assumes $u(w^i v) = (uw^i)v$ for all $u,v \in R$ and arbitrary fixed $i \geq 0$.

It must be shown that $u(w^{i+1}v) = (uw^{i+1})v$. One knows that $u(w^{i+1}v) = u((ww^i)v) = u(w(w^i v)) = (uw)(w^i v) = ((uw)w^i)v$ by the associative property of w and an application of the induction hypothesis to uw, w^i, and v. But $((uw)w^i)v = (u(ww^i))v = (uw^{i+1})v$, and so $u(w^{i+1}v) = (uw^{i+1})v$ as asserted.

(b) This proof is also by induction on n.

If $n = 0$ then the conclusion is clear.

As an <u>induction hypothesis</u>, one assumes $u(vw^i) = (uv)w^i$ for all $u,v \in R$ and arbitrary fixed $i \geq 0$.

It must be shown that $u(vw^{i+1}) = (uv)w^{i+1}$. One knows that $u(vw^{i+1}) = u(v(w^i w)) = u((vw^i)w) = (u(vw^i))w = ((uv)w^i)w$ by the associative property of w and an application of the induction hypothesis. But $((uv)w^i)w = (uv)(w^i w) = (uv)w^{i+1}$, and so $u(vw^{i+1}) = (uv)w^{i+1}$ as asserted.

Henceforth, one may write $w^n uv$, $uw^n v$, and uvw^n unambiguously without parentheses.

The principal goal of this section is Theorem 1 below which formalizes the computation of certain basic products in the assumed embedding ring R. But first some preliminary lemmas are needed.

<u>Lemma 2</u>: For all $a,b \in K$ and integers $m,n \geq 0$:

(a) $(a(bw^n) = (ab)w^n$.

(b) $(aw^{m+1})(bw^n) = (aw^m)(bw^{n+1})+(aw^m)(b'w^n)$.

<u>Proof</u>: Part (a) is an immediate consequence of Lemma 1. The proof of (b) is given.

$(aw^{m+1})(bw^n) = ((aw^m)w)(bw^n) = (aw^m)(w(bw^n)) = (aw^m)((wb)w^n)$

$= (aw^m)((bw+b')w^n) = (aw^m)((bw)w^n)+(aw^m)(b'w^n)$

$= (aw^m)(b(ww^n))+(aw^m)(b'w^n) = (aw^m)(bw^{n+1})+(aw^m)(b'w^n)$,

as asserted.

Lemma 2 is a special case of the following lemma, which gives the formal analogue of the product of (single term) associative Ore polynomials (ref. Ore [17]). A symbol $\binom{m}{i}$ has its usual combinatorial meaning, and by convention, $\binom{0}{0} = 1$. If $i > m$, then, by convention, $\binom{m}{i} = 0$.

<u>Lemma 3</u>: For arbitrary $a,b \in K$ and integers $m,n \geq 0$:

$$(aw^m)(bw^n) = \sum_{i=0}^{m} \binom{m}{i} ab^{(i)} w^{m+n-i}.$$

<u>Proof</u>: One proceeds by induction on m, with n arbitrary but assumed fixed.

The case $m = 0$ is that of Lemma 2 (a).

As an <u>induction hypothesis</u>, one assumes that the theorem holds for $m = t \geq 0$, so that $(aw^t)(bw^n)$ $= \sum_{i=0}^{t} \binom{t}{i} ab^{(i)} w^{t+n-i}$.

It must be shown that $(aw^{t+1})(bw^n)$ $= \sum_{i=0}^{t+1} \binom{t+1}{i} ab^{(i)} w^{t+1+n-i}$. One knows that $(aw^{t+1})(bw^n)$ $= (aw^t)(bw^{n+1})+(aw^t)(b'w^n)$ $= \sum_{i=0}^{t} \binom{t}{i} ab^{(i)} w^{t+n+1-i} + \sum_{i=0}^{t} \binom{t}{i} ab^{(i+1)} w^{t+n-i}$, by Lemma 2 (b) and the induction hypothesis. Now replace i by i-1 in the second summation and recall that $\binom{t}{i-1}+\binom{t}{i} = \binom{t+1}{i}$. Then $(aw^{t+1})(bw^n)$

$$= \sum_{i=0}^{t} \binom{t}{i} ab^{(i)} w^{t+n+1-i} + \sum_{i=1}^{t+1} \binom{t}{i-1} ab^{(i)} w^{t+n+1-i}$$

$$= \sum_{i=1}^{t} \binom{t+1}{i} ab^{(i)} w^{t+n+1-i} + \binom{t}{0} ab^{(0)} w^{t+n+1} + \binom{t}{t} ab^{(t+1)} w^{n}$$

$$= \sum_{i=1}^{t} \binom{t+1}{i} ab^{(i)} w^{t+n+1-i} + \binom{t+1}{0} ab^{(0)} w^{t+n+1} + \binom{t+1}{t+1} ab^{(t+1)} w^{n}$$

$$= \sum_{i=0}^{t+1} \binom{t+1}{i} ab^{(i)} w^{t+n+1-i}, \text{ as asserted.}$$

Corollary: For any $b \in K$ and any integer $m \geq 0$:

$$w^m b = \sum_{i=0}^{m} \binom{m}{i} b^{(i)} w^{m-i}.$$

It is useful to note that this corollary implies that $w^m b = bw^m + \ldots$ terms in lower powers of w.

Definition: A canonical polynomial is an element $\sum_{i=0}^{n} c_i w^i \in R$ for $c_i \in K$ and $n \geq 0$. To "put an element u of R into canonical polynomial form" means (if possible) to express u in the equivalent form of a canonical polynomial.

Theorem 1: If an embedding ring R of the type under discussion exists, the canonical polynomials of R must multiply according to the rule:

$$\sum_{i=0}^{m} a_i w^i \cdot \sum_{j=0}^{n} b_j w^j = \sum_{h=0}^{m+n} \sum_{\substack{i=h-n \\ i\geq 0}}^{m} \sum_{\substack{j=h-i \\ 0\leq j\leq n}}^{h} \binom{i}{i+j-h} a_i b_j^{(i+j-h)} w^h.$$

Proof: Multiplying each $a_i w^i$ by each $b_j w^j$, for $0 \leq i \leq m$ and $0 \leq j \leq n$, one obtains (by Lemma 3) a sum of terms of the form $\binom{i}{k} a_i b_j^{(k)} w^{i+j-k}$. By Lemma 3, the product of the two canonical polynomials will contain terms in w^h for $0 \leq h \leq m+n$. To obtain the term in w^h for any fixed h in this range, one must have $i+j-k = h$ or $k = i+j-h$, and so the total term in w^h is $\sum \binom{i}{i+j-h} a_i b_j^{(i+j-h)} w^h$. The inequality $i+j \geq h$ follows from the inequality $k \geq 0$, from which inequality the indicated ranges of summation follow.

2.3 Definition of the Minimal Embedding Ring.

In this section a differential ring $\{K(w),+,\cdot,'\}$ is defined. It will be shown that this ring is indeed a minimal extension of K such that $R = K(w)$ contains an element w that satisfies conditions (1) and (2) of Section 2.2 above. The canonical polynomials of Section 2.2 provide the motivation for the following definitions, although it should be understood that the assumption of the existence of the embedding ring R has now been abandoned.

The elements of the set K(w) are defined to be the polynomials $\sum_{i=0}^{n} a_i w^i$ in a symbol w with $a_i \in K$. The relation of equality, and the operations of addition and multiplication in K(w), are defined by the following rules:

$$\sum_{i=0}^{n} a_i w^i = \sum_{i=0}^{n} b_i w^i \text{ if and only if } a_i = b_i \text{ for } 0 \leq i \leq n.$$

The identity $1 \in K$ is identified with the polynomial $1 \cdot w^0 = w^0$.

$$\sum_{i=0}^{n} a_i w^i + \sum_{i=0}^{n} b_i w^i = \sum_{i=0}^{n} (a_i + b_i) w^i.$$

$$\sum_{i=0}^{m} a_i w^i \cdot \sum_{j=0}^{n} b_j w^j = \sum_{h=0}^{m+n} \sum_{\substack{i=h-n \\ i \geq 0}}^{m} \sum_{\substack{j=h-i \\ 0 \leq j \leq n}}^{h} \binom{i}{i+j-h} a_i b_j^{(i+j-h)} w^h.$$

It is clear that K is a subsystem of K(w) under the identification $c = cw^0$ for any $c \in K$, and that the above rules are in accord with the operations already defined in K.

The rule of multiplication is that of Theorem 1 and was in fact motivated by that result (which assumed the existence of an embedding ring R). For the special case where $a_i = 0$ for $i \neq m$ and $b_j = 0$ for $j \neq n$ (and writing a for a_m and b for b_n), one has the rule of Lemma 3 above. In particular, $wb = bw+b'$ for $b \in K$. It will also be noted that $1 \in K$ is the identity of K(w), and that w itself is the polynomial $0 \cdot w^0 + 1 \cdot w^1$ and hence included in the set K(w) - but not in the basic ring K.

An operation of derivation in K(w) is also required, but it will be defined later. The following theorem shows that K(w), with the structure imposed above, is a ring.

Theorem 2: $\{K(w),+,\cdot\}$ is a ring.

Proof: It is clear that the rule of addition makes the system an abelian group and that the rule of multiplication exhibits multiplicative closure. Hence if it is shown that the distributive laws are valid, the conclusion that K(w) is a ring will be valid.

Let $u = \sum_{i=0}^{n} a_i w^i$, $v = \sum_{j=0}^{n} b_j w^j$, and $t = \sum_{j=0}^{n} c_j w^j$, including zero terms if necessary to ensure identity of ranges of summation. It is required to show that $u(v+t) = uv+ut$ and $(u+v)t = uv+ut$. Using the above definition of multiplication, and simplifying the notation by the omission of some of the limits of summation, one obtains:

$$u(v+t) = \sum_{i=0}^{n} a_i w^i (\sum_{j=0}^{n} b_j w^j + \sum_{j=0}^{n} c_j w^j) = \sum_{i=0}^{n} a_i w^i \cdot \sum_{j=0}^{n} (b_j + c_j) w^j$$

$$= \sum\sum\sum \binom{i}{i+j-h} a_i (b_j + c_j)^{(i+j-h)} w^h$$

$$= \sum\sum\sum \binom{i}{i+j-h} a_i b_j^{(i+j-h)} w^h + \sum\sum\sum \binom{i}{i+j-h} a_i c_j^{(i+j-h)} w^h$$

$$= \sum_{i=0}^{n} a_i w^i \cdot \sum_{j=0}^{n} b_j w^j + \sum_{i=0}^{n} a_i w^i \cdot \sum_{j=0}^{n} c_j w^j = uv+ut \text{ as asserted.}$$

Now write $v = \sum_{i=0}^{n} b_i w^i$, using the symbol i in place of j.

$$(u+v)t = (\sum_{i=0}^{n} a_i w^i + \sum_{i=0}^{n} b_i w^i) \sum_{j=0}^{n} c_j w^j = \sum_{i=0}^{n} (a_i + b_i) w^i \cdot \sum_{j=0}^{n} c_j w^j$$

$$= \sum\sum\sum \binom{i}{i+j-h} (a_i + b_i) c_j^{(i+j-h)} w^h$$

$$= \sum\sum\sum \binom{i}{i+j-h} a_i c_j^{(i+j-h)} w^h + \sum\sum\sum \binom{i}{i+j-h} b_i c_j^{(i+j-h)} w^h$$

$$= \sum_{i=0}^{n} a_i w^i \cdot \sum_{j=0}^{n} c_j w^j + \sum_{i=0}^{n} b_i w^i \cdot \sum_{j=0}^{n} c_j w^j = ut+vt \text{ as asserted.}$$

Theorem 3: The element w is contained in the nucleus of the ring K(w).

Proof: Specifically, one shows that, for all $x,y \in K(w)$: (1) $(wx)y = w(xy)$; (2) $(xw)y = x(wy)$; (3) $(xy)w = x(yw)$. Because the distributive laws are valid in the ring K(w), it will suffice to let $x = aw^m$ and $y = bw^n$ for $a,b \in K$.

(1) <u>To show that $(wx)y = w(xy)$</u>:

$$(wx)y = (w\cdot aw^m)bw^n = (aw^{m+1}+a'w^m)bw^n$$

$$= \sum_{i=0}^{m+1}\binom{m+1}{i}ab^{(i)}w^{m+n+1-i} + \sum_{i=0}^{m}\binom{m}{i}a'b^{(i)}w^{m+n-i}$$

$$= [\binom{m+1}{m+1}ab^{(m+1)}w^n + \binom{m+1}{0}ab^{(0)}w^{m+n+1} + \sum_{i=1}^{m}\binom{m+1}{i}ab^{(i)}w^{m+n+1-i}]$$

$$+ \sum_{i=0}^{m}\binom{m}{i}a'b^{(i)}w^{m+n-i} = [\binom{m}{m}ab^{(m+1)}w^n + \binom{m}{0}ab^{(0)}w^{m+n+1}$$

$$+ \sum_{i=1}^{m}\binom{m+1}{i}ab^{(i)}w^{m+n+1-i}] + \sum_{i=0}^{m}\binom{m}{i}a'b^{(i)}w^{m+n-i}$$

$$= [\binom{m}{m}ab^{(m+1)}w^n + \binom{m}{0}ab^{(0)}w^{m+n+1} + \sum_{i=1}^{m}\binom{m}{i}ab^{(i)}w^{m+n+1-i}$$

$$+ \sum_{i=1}^{m}\binom{m}{i-1}ab^{(i)}w^{m+n+1-i}] + \sum_{i=0}^{m}\binom{m}{i}a'b^{(i)}w^{m+n-i}$$

$$= [\sum_{i=1}^{m+1}\binom{m}{i-1}ab^{(i)}w^{m+n+1-i} + \sum_{i=0}^{m}\binom{m}{i}ab^{(i)}w^{m+n+1-i}]$$

$$+ \sum_{i=0}^{m}\binom{m}{i}a'b^{(i)}w^{m+n-i}.$$

Now replace i by i+1 in the first summation of the above,

obtaining: $\sum_{i=0}^{m}\binom{m}{i}ab^{(i+1)}w^{m+n-i} + \sum_{i=0}^{m}\binom{m}{i}ab^{(i)}w^{m+n+1-i}$

$$+ \sum_{i=0}^{m}\binom{m}{i}a'b^{(i)}w^{m+n-i} = \sum_{i=0}^{m}\binom{m}{i}(ab^{(i)})'w^{m+n-i} + \sum_{i=0}^{m}\binom{m}{i}ab^{(i)}w^{m+n+1-i}$$

$$= w\cdot\sum_{i=0}^{m}\binom{m}{i}ab^{(i)}w^{m+n-i} = w(aw^m\cdot bw^n) = w(xy)$$ as asserted.

(2) <u>To show that $(xw)y = x(wy)$</u>:

$$(xw)y = (aw^m \cdot w)bw^n = (aw^{m+1})(bw^n) = \sum_{i=0}^{m+1} \binom{m+1}{i} ab^{(i)} w^{m+n+1-i}$$

$$= \binom{m+1}{m+1} ab^{(m+1)} w^n + \binom{m+1}{0} ab^{(0)} w^{m+n+1} + \sum_{i=1}^{m} \binom{m+1}{i} ab^{(i)} w^{m+n+1-i}$$

$$= \binom{m}{m} ab^{(m+1)} w^n + \binom{m}{0} ab^{(0)} w^{m+n+1} + \sum_{i=1}^{m} \binom{m}{i} ab^{(i)} w^{m+n+1-i}$$

$$+ \sum_{i=1}^{m} \binom{m}{i-1} ab^{(i)} w^{m+n+1-i}$$

$$= \sum_{i=0}^{m} \binom{m}{i} ab^{(i)} w^{m+n+1-i} + \sum_{i=1}^{m+1} \binom{m}{i-1} ab^{(i)} w^{m+n+1-i}.$$ Now replace i by i+1 in the second summation of the above, obtaining:

$$\sum_{i=0}^{m} \binom{m}{i} ab^{(i)} w^{m+n+1-i} + \sum_{i=0}^{m} \binom{m}{i} ab^{(i+1)} w^{m+n-i}$$

$= aw^m(bw^{n+1} + b'w^n) = aw^m(w \cdot bw^n) = x(wy)$ as asserted.

(3) <u>To show that $(xy)w = x(yw)$</u>:

$$(xy)w = (aw^m \cdot bw^n)w = \left(\sum_{i=0}^{m} \binom{m}{i} ab^{(i)} w^{m+n-i}\right)w$$

$$= \sum_{i=0}^{m} \binom{m}{i} ab^{(i)} w^{m+n+1-i} = (aw^m)(bw^{n+1}) = (aw^m)(bw^n \cdot w)$$

$= x(yw)$ as asserted. This completes the proof of Theorem 3.

The operation of <u>derivation</u> in $K(w)$ is now defined.

<u>Definition</u>: $wu - uw = u'$ for each $u \in K(w)$.

Theorem 3 ensures that $wu - uw = u'$ defines a strong inner derivation in $K(w)$. As noted above, $wa - aw = a'$ for $a \in K$, a' being the derivative of a already defined in K. Thus the derivation defined in $K(w)$ extends the original derivation given in the basic ring K.

It is now possible to sum up the above material in the following theorem.

Theorem 4: There exists a differential ring R which provides a solution of the basic embedding problem for a given differential ring K. Moreover, the unique minimal such ring R may be characterized as a ring of polynomials over K in an element w such that:

(1) w is in the nucleus of R.

(2) $wu - uw = u'$ for any $u \in R$.

Proof: Let R = K(w). The (1) and (2) follow from Theorem 3 and the definition of derivation. By the development of Section 2.2, any subring of K(w) which satisfies these two properties must contain the canonical polynomials and hence all of K(w), thus establishing minimality. The uniqueness of R follows primarily from Theorem 1.

It is clear, of course, that the results in Section 2.2 shown to be valid for the assumed embedding ring R are valid for the ring K(w). In particular, powers of w are contained in the nucleus of K(w).

Finally, it should be noted that K(w) is formally the ring of Ore polynomials, as generalized to a basic ring K no longer assumed to be associative. In the sequel, this ring K(w) is referred to as the ring of the Ore polynomials based on the given differential ring K.

This section is concluded with a brief note to the effect that the ring K(w) is a special case of a more general construction of Qureshi [19]. Qureshi's ring S will be expressed in terms of the notation used in this thesis. One starts with a basic ring K for which k+1 endomorphisms, $f_0, f_1, \ldots, f_k$, of {K;+} are defined.

The crux of Qureshi's rule of multiplication is:

$$w^n b = \sum_{i=0}^{nk} S_n^i(b)w^i \text{ for } b \in K \text{ and}$$

$$S_n^i(b) = \sum_{d_1+\cdots+d_n=i} F_{d_1}F_{d_2}\cdots F_{d_n}(b).$$

To obtain the Ore polynomials, one takes k = 1, $f_0(b) = b'$, and $f_1(b) = b$, for all $b \in K$. Routine computations show that, in this case, $S_n^i(b) = \binom{n}{i}b^{(n-i)}$, and the corollary to Lemma 3 above easily follows.

It may be noted, however, that Qureshi is not concerned with differential rings as such; any derivations that appear as special instances of his construction are incidental to his primary goals.

2.4 The K-module M.

A "left K-module" M is constructed in this section, with K the basic differential ring as described in Chapter 1. This module M will lead to a realization or representation of the polynomial ring K(w). Unless K is itself an associative ring, M will not be a module of the usual kind because the associativity requirements will not be met; the remaining properties of a left unital (or unitary) module, however, will be evident from the definition given below. It may also be noted that the representation of K(w) as a ring of endomorphisms of {K;+}, as was briefly described in Section 1.4 of Chapter 1 above, will not be valid if the basic ring

K is nonassociative.

The underlying set of M is the set of all functions defined on the rational integers, assuming values in K, and subject to the condition that the values of any function are zero for all sufficiently large integers. Thus each element of M may be represented by a symbol $(\ldots,a_{-2},a_{-1},a_0,a_1,a_2,\ldots)$, more simply written in terms of its typical element as $(\ldots,a_i,\ldots)$, where each component $a_i \in K$ and where there exists an n (depending upon the element of M under consideration) such that $a_i = 0$ for all $i > n$. The basic algebraic structure of the system is determined by the following properties which constitute the definition used in this thesis of the system known as a <u>left K-module</u>.

<u>Equality</u>: $(\ldots,a_i,\ldots) = (\ldots,b_i,\ldots)$ if $a_i = b_i$ for all i.

<u>Addition</u>: $(\ldots,a_i,\ldots)+(\ldots,b_i,\ldots) = (\ldots,a_i+b_i,\ldots)$, while subtraction is defined in the analogous componentwise manner.

<u>Left Multiplication</u>: For arbitrary $b \in K$, $b(\ldots,a_i,\ldots) = (\ldots,ba_i,\ldots)$.
Note that $bc(\ldots,a_i,\ldots) = (\ldots,(bc)a_i,\ldots)$, whereas $(b(c(\ldots,a_i,\ldots)) = (\ldots,b(ca_i),\ldots)$; these products are equal only if, for each i, $(bc)a_i = b(ca_i)$.

In addition to the above properties, which make the set comprising M into a K-module for a generally nonassociative ring K, the following unary operation is defined on M:

<u>M-Derivation</u>: $(\ldots,a_i,\ldots)' = (\ldots,a_{i-1}+a_i', \ldots)$.

This M-derivation mapping is not a derivation because M is not a ring. In the sequel, however, formal analogues of the sum and product laws for derivatives are established for this unary operation, and so the notations and terminology of derivatives will be used without special comment. In particular, one may speak of M-derivatives and, for $n \geq 0$, of nth M-derivatives (the results of applying this M-derivation n times) where, for any $m \in M$, $m^{(0)} = m$.

Given an arbitrary $(\ldots,a_i,\ldots) \in M$, it is sometimes convenient to refer to a_i as being in the "ith position". If t is an element of M such that $a_j = 1$ for some fixed j and $a_i = 0$ for all $i \neq j$, this element can be most easily described by saying that it has 1 in the jth position and zeros elsewhere. It is clear from the definition of M-derivation that the nth M-derivative $t^{(n)}$ of t, for $n \geq 0$, is that element of M which has 1 in the (j+n)th position and zeros elsewhere. Each operation of M-differentiation shifts the 1 component one position to the right.

In particular, it is useful to identify a special element to be labelled z. The element z is defined as that element of M which has 1 in the zero-th position and zeros elsewhere. From the above remarks, $z^{(n)}$ is that element with 1 in the nth position and zeros elsewhere (for any $n \geq 0$). The symbol $z^{(-n)}$, for $n > 0$, is defined to be the element with 1 in the (-n)th position and zeros elsewhere. This notation $z^{(-n)}$ for positive n suggests that z is being "M-integrated" n times, a suggestion that is not inappropriate in view of the fact that the nth M-derivative of

$z^{(-n)}$ is z itself. It now follows that, for <u>any</u> integer $n, z^{(n)}$ is that element which has 1 in the nth position and zeros elsewhere. Note, in particular, that $z^{(0)} = z$.

For each element of M that has only a finite number of nonzero components, a canonical form is easily obtained. Thus let $m = (\ldots, a_i, \ldots)$ where, for integers k and n, $a_i = 0$ for all $i < k$ and all $i > n$. Then m can be expressed as the canonical sum $\sum_{i=k}^{n} a_i z^{(i)}$ where $a_i z^{(i)}$ is the element of M with a_i in the ith position and zeros elsewhere.

It is possible to extend the above symbolism in a purely formal way to include arbitrary elements of M. Thus if $m = (\ldots, a_i, \ldots)$ is any element of M (where, for all $i > n$, $a_i = 0$), one has:

$$m = (\ldots, a_i, \ldots) = \sum_{i=-\infty}^{n} a_i z^{(i)}.$$

This indicated sum is, of course, purely formal, with no implication of convergence in any sense of the word.

The above defining properties of M may be restated in terms of these formal infinite sums as follows:

<u>Equality</u>: $\sum_{i=-\infty}^{n} a_i z^{(i)} = \sum_{i=-\infty}^{n} b_i z^{(i)}$ if $a_i = b_i$ for all i.

<u>Addition</u>: $\sum_{i=-\infty}^{n} a_i z^{(i)} + \sum_{i=-\infty}^{n} b_i z^{(i)} = \sum_{i=-\infty}^{n} (a_i + b_i) z^{(i)}$.

<u>Left Multiplication</u>: $b\left(\sum_{i=-\infty}^{n} a_i z^{(i)}\right) = \sum_{i=-\infty}^{n} (ba_i) z^{(i)}$.

<u>M-Derivation</u>: $(\sum_{i=-\infty}^{n} a_i z^{(i)})' = \sum_{i=-\infty}^{n+1} (a_{i-1}+a_i')z^{(i)}$ with $a'_{n+1} = 0$.

The rule of M-derivation just given is essentially that given by Jacobson [4] for what he terms a "differential transformation", with an associative division ring K acting on a finite dimensional K-module.

It will now be shown that the operation of M-derivation in M satisfies the formal sum and product laws for derivatives.

It may be noted that, for any $a,b \in K$ and any integer n, $a(bz^{(n)}) = (ab)z^{(n)}$. This follows from the definition of z and the obvious equality $a(b\cdot 1) = (ab)\cdot 1$. Henceforth one may write $abz^{(n)}$ without ambiguity.

It may also be noted that, for $a \in K$ and any integer n, $(az^{(n)})' = a'z^{(n)}+az^{(n+1)}$. For $az^{(n)} = \sum_{i=-\infty}^{n} a_i z^{(i)}$, where $a_n = a$ and $a_i = 0$ for $i \neq n$. Then $(az^{(n)})' = (\sum_{i=-\infty}^{n} a_i z^{(i)})'$ $= \sum_{i=-\infty}^{n+1} (a_{i-1}+a_i')z^{(i)} = a_n'z^{(n)}+a_n z^{(n+1)} = a'z^{(n)}+az^{(n+1)}$ as asserted.

The formal sum and product laws for M-derivation assume the following forms, for all $x,y \in M$ and $c \in K$:

(1) $(x+y)' = x'+y'$.

(2) $(cx)' = c'x+cx'$.

Since any element of M is expressible as an infinite formal sum of terms where additions and left multiplications are performed termwise, in order to show the validity of these laws it will suffice to let x and y be single terms. Thus let $x = az^{(n)}$ and $y = bz^{(n)}$ for $a,b \in K$. Then

$x'+y' = (az^{(n)})'+(bz^{(n)})' = (a'z^{(n)}+az^{(n+1)})+(b'z^{(n)}+bz^{(n+1)})$

$= (a'+b')z^{(n)}+(a+b)z^{(n+1)} = (a+b)'z^{(n)}+(a+b)z^{(n+1)}$

$= ((a+b)z^{(n)})' = (x+y)'$. And $(cx)' = (c(az^{(n)})'$

$= (caz^{(n)})' = (ca)'z^{(n)}+caz^{(n+1)} = (c'a+ca')z^{(n)}+caz^{(n+1)}$

$= c'az^{(n)}+c(a'z^{(n)}+az^{(n+1)}) = c'(az^{(n)})+c(az^{(n)})' = c'x+cx'$

as asserted.

2.5 Realization of the Ring K(w).

The realization of the embedding ring K(w) is now begun.

First a set S is identified. The elements of S are the functions f, on M into M, of the following type:

$$\text{For } n \geq 0 \text{ and } a_i \in K,\ f(m) = \sum_{i=0}^{n} a_i m^{(i)} \text{ for } m \in M.$$

Thus an element $f \in S$ is determined by the value of n and the choice of elements $a_i \in K$. Note that here n must be non-negative.

The usual functional definitions of equality and addition are applied, so that, for all $f,g \in S$:

$f = g$ only when $f(m) = g(m)$ for all $m \in M$;

$(f+g)(m) = f(m)+g(m)$ for all $m \in M$.

It is clear that S is closed under the operation of addition.

It will be useful to formulate a canonical form for a given $f \in S$. Accordingly, let $f(m) = \sum_{i=0}^{n} a_i m^{(i)}$, and let

$f_i(m) = a_i m^{(i)}$ $(0 \leq i \leq n)$. Then, from the definition of addition, $f = \sum_{i=0}^{n} f_i$, which is now a sum in S. The function f_i will be denoted by the convenient symbol $a_i t^i$; accordingly, $f = \sum_{i=0}^{n} a_i t^i$, and this expression is regarded as the <u>canonical form</u> of f.

Thus $\sum_{i=0}^{n} (a_i t^i)(m) = \sum_{i=0}^{n} a_i m^{(i)}$ for all $m \in M$.

If $n = 0$, a function $f \in S$ is such that $f(m) = a_0 m^{(0)} = a_0 m$, where f is the left multiplication by $a_0 \in K$. In this case, $f = a_0 t^0$, which may be written simply as a_0. Accordingly, $f(m) = a_0(m) = a_0 m$. A left multiplication f is clearly an endomorphism of the group $\{M;+\}$. It will also be noted that t^1 may be written simply as t, and $1 \cdot t^i$ simply as t^i.

If $n = 1$, $a_0 = 0$, and $a_1 = 1$, then $f = 0 \cdot t^0 + 1 \cdot t^1 = t$, and $f(m) = t(m) = m'$, with m' the M-derivative of m. In this case, $f = t$ is the M-derivation mapping. This element t is also, by Section 2.4 above, an endomorphism of $\{M;+\}$. Because $t^i(m) = m^{(i)}$, t^i is really the composite of i applications of the M-derivation t; it is clear, therefore, that each t^i is also an endomorphism of $\{M;+\}$. It is further clear that $a_i t^i$, for $a_i \in K$, is a composite of the left multiplication by a_i and the mapping t^i, and thus an endomorphism of $\{M;+\}$. Thus the elements of S, as finite sums of the functions $a_i t^i$ for $0 \leq i$ and $a_i \in K$, are endomorphisms of $\{M;+\}$.

In view of the basic role played by t in this description, the set S will henceforth be denoted by the symbol K(t). Further operations of multiplication and derivation will be defined on this set to obtain a differential ring, and it will be found that this ring will be an embedding ring for K isomorphic to the ring K(w) of the Ore polynomials.

Setting m = z in the definition of equality in K(t), one finds that $\sum_{i=0}^{n} a_i t^i = \sum_{i=0}^{n} b_i t^i$ if and only if, for each i, $a_i = b_i$. This is because $\sum_{i=0}^{n} (a_i t^i)(z) = \sum_{i=0}^{n} a_i z^{(i)}$,

$\sum_{i=0}^{n} (b_i t^i)(z) = \sum_{i=0}^{n} b_i z^{(i)}$, and equality is termwise in M. From the definition of addition given above, it is clear that $\sum_{i=0}^{n} a_i t^i + \sum_{i=0}^{n} b_i t^i = \sum_{i=0}^{n} (a_i + b_i) t^i$. (Of course, given two elements of S in canonical form, zero terms may be included in either of them to ensure identity of ranges of summation.)

It can easily be shown that {K(t);+} is an <u>abelian group</u> with zero, $0 = \sum_{i=0}^{n} 0 \cdot t^i$ (for any $n \geq 0$), and inverses,

$- \sum_{i=0}^{n} a_i t^i = \sum_{i=0}^{n} (-a_i) t^i$.

It is not possible to define multiplication in K(t) simply as the equivalent of the usual composition of functions: (fg)(m) = f(g(m)) for all m ε M. This is due to the fact that composition of the functions is an associative operation, whereas multiplication in the basic ring K is not assumed to be associative. Thus let a,b,c ε K with

$m = cz \in M$. One finds that $a(b(m)) = (a(bc))z$, whereas applying the product ab to m, one obtains $(ab)(m) = ((ab)c)z$; equality of $(a(bc))z$ and $((ab)c)z$ follows only when $a(bc) = (ab)c$, which equality would not generally hold in a non-associative ring. Hence, for nonassociative K, K(t) would not be a ring extension of K as required for an embedding ring. Therefore it is necessary to give a modified definition for the "product" of functions in K(t).

The following lemma will ensure uniqueness of products.

Lemma 1: If $h,k \in K(t)$ and $h(z) = k(z)$ then $h = k$.

Proof: Let $h = \sum_{i=0}^{n} a_i t^i$, $k = \sum_{i=0}^{n} b_i t^i$. Then $h(z) = k(z)$ entails $\sum_{i=0}^{n} a_i z^{(i)} = \sum_{i=0}^{n} b_i z^{(i)}$, whereupon, for each i, $a_i = b_i$. The conclusion $h = k$ then follows.

Now let f, g, and h be elements of K(t). Then:

The element h is the product fg if $f(g(z)) = h(z)$.

It is important to note in this definition that g and h are applied, not to an arbitrary $m \in M$, but to the special element z. Also, it has not yet been established that this product fg always exists. However, if f is the left multiplication by $a \in K$ and g is the function t^i, then, as an immediate consequence of this definition, the function at^i is indeed the product of a and t^i, as one would naturally expect.

The distributive laws for K(t) are given by the next lemma.

<u>Lemma 2</u>: Let $f,g,h \in K(t)$. Then, if the indicated products are defined, $f(g+h) = fg+fh$ and $(g+h)f = gf+hf$.

<u>Proof</u>: The conclusion follows from applying both sides of each asserted equality to z, using the definition of addition and the fact that these functions f, g, and h are endomorphisms of $\{M,+\}$.

The <u>existence</u> of the product fg for arbitrary elements f and g of $K(t)$ is shown by the following lemma.

<u>Lemma 3</u>: Given any $f,g \in K(t)$ there is an $h \in K(t)$ such that $h = fg$.

<u>Proof</u>: In view of the distributive laws, it will suffice to let $f = at^m$ and $g = bt^n$ for $a,b \in K$. But, applying the Leibniz formula of Section 2.1 above, $(at^m)(bt^n(z))$

$$= (at^m)(bz^{(n)}) = a(bz^{(n)})^{(m)} = a\sum_{i=0}^{m}\binom{m}{i}b^{(i)}(z^{(n)})^{(m-i)}$$

$= \sum_{i=0}^{m}\binom{m}{i}ab^{(i)}z^{(m+n-i)} = \sum_{i=0}^{m}\binom{m}{i}ab^{(i)}t^{m+n-i}(z)$, and hence, by the definition of product, $(at^m)(bt^n) = \sum_{i=0}^{m}\binom{m}{i}ab^{(i)}t^{m+n-i}$.

Thus $\sum_{i=0}^{m}\binom{m}{i}ab^{(i)}t^{m+n-i}$ is the desired element $h = fg$ as asserted.

<u>Theorem 5</u>: $\{K(t);+,\cdot\}$ is a ring isomorphic to the ring $\{K(w);+,\cdot\}$ of the Ore polynomials of Section 2.3 above. The left multiplications by $a \in K$ constitute a subring of $K(t)$ isomorphic to the basic ring K, under the natural correspondence of the element $a \in K$ with the left multiplication by a.

Proof: That $K(t)$ is a ring follows from the preceding lemmas. The asserted isomorphism is naturally given by

$$\sum_{i=0}^{n} a_i w^i \leftrightarrow \sum_{i=0}^{n} a_i t^i$$

for $a_i \varepsilon K$. Clearly the correspondence is one-to-one. The rules of addition are formally the same in the two rings and the isomorphism now follows from the fact that the rules of multiplication, as given in Lemma 3 of Section 2.2 and at the end of proof of Lemma 3 above, are also formally identical.

Henceforth, the left multiplications will be identified with the corresponding elements of K, so that the basic ring K will be embedded in $K(t)$, or, equivalently, $K(t)$ will be a ring extension of K.

It remains to define a strong inner derivation in $K(t)$.

Definition: For all $u \varepsilon K(t)$, $u' = tu-ut$.

The following is an easy corollary to Theorem 5.

Corollary: $\{K(t);+,\cdot,'\}$ is isomorphic to $\{K(w);+,\cdot,'\}$, under the natural correspondence $\sum_{i=0}^{n} a_i t^i \leftrightarrow \sum_{i=0}^{n} a_i w^i$.

Henceforth, the differential rings $K(t)$ and $K(w)$ are identified, so that, in particular, the element $t \varepsilon K(t)$ is equated to the element $w \varepsilon K(w)$ and, in general, $\sum_{i=0}^{n} a_i t^i$ is equated to $\sum_{i=0}^{n} a_i w^i$. Thus this section has effected a realization of the ring $K(w)$ of the Ore polynomials.

CHAPTER 3

IDEALS OF K(w)

3.1 D-Ideals.

The purpose of this chapter is to study ideals in the embedding ring K(w) of the Ore polynomials based on a given ring K. Henceforth, it is assumed that the ring K, and hence also the ring K(w), is of characteristic zero (with identity 1).

It will be useful to consider a mapping D of K(w) into K(w) defined as follows:

$D(\sum_{i=0}^{n} a_i w^i) = \sum_{i=0}^{n} i a_i w^{i-1}$ for $a_i \in K$, where, for $i = 0$, the symbol $i a_i w^{i-1}$ is equated to 0.

In particular, if the mapped element consists of a single term aw^n, then $D(aw^n) = naw^{n-1}$.

It is clear that, for all $u,v \in K(w)$, $D(u+v) = D(u)+D(v)$. This additive property is the Sum Law for derivatives. The following lemma, showing the Product Law to be valid for this mapping D, will ensure that D is a derivation.

Lemma 1: For all $u,v \in K(w)$, $D(uv) = u \cdot D(v)+D(u) \cdot v$.

Proof: Inasmuch as D is additive, it will suffice to consider single term elements. Accordingly, let $u = aw^m$ and $v = bw^n$ for $m,n \geq 0$ and $a,b \in K$.

One uses the identity $\binom{m}{i}n+\binom{m-1}{i}m = \binom{m}{i}(m+n-i)$.

$$D(uv) = D(aw^m \cdot bw^n) = D(\sum_{i=0}^{n} \binom{m}{i} ab^{(i)} w^{m+n-i})$$

$$= \sum_{i=0}^{m} \binom{m}{i}(m+n-i)ab^{(i)}w^{m+n-i-1}$$

$$= nab^{(m)}w^{n-1} + \sum_{i=0}^{m-1} \binom{m}{i}(m+n-i)ab^{(i)}w^{m+n-i-1}$$

$$= nab^{(m)}w^{n-1} + \sum_{i=0}^{m-1} [\binom{m}{i}n+\binom{m-1}{i}m]ab^{(i)}w^{m+n-i-1}$$

$$= nab^{(m)}w^{n-1} + \sum_{i=0}^{m-1} \binom{m}{i}nab^{(i)}w^{m+n-i-1} + \sum_{i=0}^{m-1} \binom{m-1}{i}mab^{(i)}w^{m+n-i-1}$$

$$= \sum_{i=0}^{m} \binom{m}{i}nab^{(i)}w^{m+n-i-1} + \sum_{i=0}^{m-1} \binom{m-1}{i}mab^{(i)}w^{m+n-i-1}$$

$$= (aw^m)(nbw^{n-1})+(maw^{m-1})(bw^n)$$

$= u\cdot D(v)+D(u)\cdot v$ as asserted.

It is clear that D is <u>formal</u> polynomial differentiation of ordinary calculus applied to the elements of K(w).

As suggested in Section 1.2 of Chapter 1, the letter d may be used as an alternative symbol for the derivation ' in either K or K(w). Accordingly:

$$d(\sum_{i=0}^{n} a_i w^i) = \sum_{i=0}^{n} d(a_i)w^i = \sum_{i=0}^{n} a_i' w^i,$$ recalling that

$d(w^i) = (w^i)' = 0$.

A <u>D-constant</u> is an element $u \in K(w)$ such that $D(u) = 0$. It is clear that every element $a \in K$ is a D-constant. Conversely, inasmuch as K is of characteristic zero, $D(aw^n) = naw^{n-1} = 0$ only when $a = 0$ or $n = 0$;

hence every D-constant is an element of K. On the other hand, a <u>d-constant</u> is an element $u \in K(w)$ such that $d(u) = u' = 0$. Since $d(w) = 0$ and $D(w) = 1$, w is a d-constant but not a D-constant.

A <u>D-ideal</u> of K(w) is a differential ideal of the ring $\{K(w);+,\cdot,D\}$, or, equivalently, an ideal of $\{K(w);+,\cdot\}$ which is closed with respect to the derivation D. If K(w) has no D-ideals other than itself and the zero ideal, it is <u>D-simple</u>. One similarly defines the concepts of <u>d-ideal</u> and <u>d-simple</u> in terms of closure with respect to the derivation d.

Trivially, every ideal of the basic ring K is closed with respect to D. Every ideal of K(w) is similarly closed with respect to d because $d(u) = wu-uw$ for any $u \in K(w)$. However, it is a nontrivial matter to consider d-ideals of K and D-ideals of K(w). The words <u>ideal</u> and <u>simple ring</u> without further qualification will be used relative to ideals of either K or K(w) which are not necessarily closed with respect to either derivation (except for d in K(w)).

It is of interest to find conditions for the D-simplicity of K(w). To this end, some preliminary definitions and lemmas are needed.

Let $u = \sum_{i=0}^{n} a_i w^i$ for $a_i \in K$ and $a_n \neq 0$, where it should be recalled that this canonical representation of $u \in K(w)$ is unique. The <u>degree</u> of u is n, the largest index i for which $a_i \neq 0$, and one writes $n = \text{Deg } u$. The degree of the one exceptional element zero is not defined. It is clear that Deg u = 0 if and only if $u \in K$ and $u \neq 0$. If $a_n = 1$, so that $u = w^n + \sum_{i=0}^{n-1} a_i w^i$, or $u = 1 \cdot w^0 = 1$ if n is zero, then u is monic.

The following lemma was proved by Amitsur [1] for a simple, associative ring K. The simplicity of Amitsur is here replaced by d-simplicity while K, as usual, is not assumed to be associative.

Lemma 2: If K is d-simple with I an ideal of K(w) and u any nonzero element of I, then there exists a monic $v \in I$ where Deg u = Deg v.

Proof: Let $u = \sum_{i=0}^{n} a_i w^i$ for $a_i \in K$, $a_n \neq 0$, and let J be the d-ideal generated by a_n in the basic ring K. Since K is d-simple, J = K, and so J contains the identity 1.

Hence there exists a finite sequence of elements $a_n = s_1, s_2, s_3, \ldots, s_m = 1$, where each $s_i \in J$ $(i > 1)$ is derived from the preceding elements of the sequence by means of either subtraction ($s_i = s_j - s_k$, where $j,k < i$), left multiplication by an arbitrary element of K, right multiplication by an arbitrary element of K, or the derivation d.

One then constructs another finite sequence of elements of K(w), $u = x_1, x_2, x_3, \ldots, x_m$, where each x_i is derived from previous elements of this sequence in precisely the same way (by means of the same operations) as s_i was so derived in the corresponding sequence in J. For example, if $s_i = s_j - s_k$, then $x_i = x_j - x_k$; if $s_i = as_j$, then $x_i = ax_j$; if $s_i = s_j a$, then $x_i = x_j a$; and if

$s_i = s_j'$, then $x_i = x_j'$. Then the following three properties hold:

(1) Each $x_i \in I$ (in particular, $x_1 = u \in I$).

(2) Each $x_i = s_i w^n + \ldots$ terms in lower powers of w. For $i = 1$, $x_1 = u = a_n w^n + \ldots = s_1 w^n + \ldots = s_i w^n + \ldots$ terms in lower powers of w. If now $s_i = s_j a$ (for $i > 1$) and it has already been established for s_j that the corresponding x_j is equal to $s_j w^n + \ldots$ terms in lower powers of w, then $x_i = x_j a = (s_j w^n + \ldots)a = s_j a w^n + \ldots = s_i w^n + \ldots$ ...terms in lower powers of w as asserted. A similar remark applies if s_i is obtained from one or more previous elements in the sequence by means of other operations in the ideal.

(3) x_m is monic, because $x_m = s_m w^n + \ldots$ terms in lower powers of w and $s_m = 1$. This element $x_m \in I$ is then the desired v of the lemma, completing proof of Lemma 2.

<u>Lemma 3</u>: If J is a d-ideal of K, then the set I consisting of the elements $\sum_{i=0}^{n} a_i w^i \in K(w)$ for $a_i \in J$ and with n ranging over the non-negative integers is a D-ideal of K(w).

<u>Proof</u>: Let $u = \sum_{i=0}^{n} a_i w^i \in I$, $v = \sum_{i=0}^{n} b_i w^i \in I$,

$t = \sum_{i=0}^{n} c_i w^i \in K(w)$ (including zero terms if necessary to ensure identity of ranges of summation). Then

$u-v = \sum_{i=0}^{n} (a_i - b_i) w^i \in I$ because each $a_i - b_i \in J$. Moreover, $tu \in I$ because tu is (by Theorem 1) a sum of terms of the form $\binom{i}{i+j-h} c_i a_j^{(i+j-h)} w^h$, each $a_j^{(i+j-h)} \in J$ (using the d-closure of J), and hence each $\binom{i}{i+j-h} c_i a_j^{(i+j-h)} \in J$.

Similarly, $ut \in I$. Finally, $D(u) = \sum_{i=0}^{n} ia_i w^{i-1} \in I$ because each $ia_i \in J$, and the proof of the lemma is complete.

The following theorem gives a necessary and sufficient condition for $K(w)$ to be D-simple.

Theorem 6: $K(w)$ is D-simple if and only if K is d-simple.

Proof: Let K be d-simple and let I be a nonzero D-ideal of $K(w)$. Then there exists a nonzero element $u \in I$ of least degree, so that $\text{Deg } u \leq \text{Deg } t$ for all nonzero $t \in I$. By Lemma 2, there is a monic element $v \in I$ where $\text{Deg } v = \text{Deg } u$, and hence v is also of least degree in I. Then $v = w^n + \ldots$ terms in lower powers of w, where $n = \deg v$. Since I is a D-ideal and hence closed under the derivation D, $D(v) = nw^{n-1} + \ldots$ terms in lower powers of w and is an element of I. If v were not 1, $D(v)$ would be an element of I of lower degree than v, contradicting the above definition of v. Therefore, $v = 1$, $I = K(w)$, and hence $K(w)$ is D-simple.

Conversely, let $K(w)$ be D-simple and let J be a nonzero d-ideal of K. Let I be the set of the elements $\sum_{i=0}^{n} a_i w^i$ for $a_i \in J$ and n ranging over the non-negative integers. By Lemma 3, I is a D-ideal of $K(w)$, and, since $K(w)$ is D-simple, $I = K(w)$. Hence $1 = 1 \cdot w^0 \in I$. By the way I is defined, $1 \in J$ and so $J = K$. Hence K is d-simple.

In the following special case, D-simplicity in $K(w)$ reduces to ordinary simplicity.

Corollary: If there exists an element x in the center of K such that $x' = 1$, then

$$D(v) = vx-xv \text{ for all } v \in K(w),$$

and K(w) is simple if and only if K is d-simple.

Proof: Let $v = aw^n$ for $a \in K$ and $n \geq 0$, where it clearly suffices to consider v as a single-term element of K(w). Then $vx-xv = (aw^n)x-x(aw^n) = a(xw^n+nx'w^{n-1})-xaw^n$ $= (ax-xa)w^n+nax'w^{n-1} = naw^{n-1} = D(v)$ as asserted.

Since it is clear that every ideal of K(w) is also a D-ideal, by (1), K(w) is simple if and only if it is D-simple. It then follows from the theorem that K(w) is simple if and only if K is d-simple.

3.2 Preliminary Lemmas.

In the sequel, a study will be made of ideals in K(w). In particular, the possibility of ideals in K(w) for a d-simple ring K will be investigated. The D mapping will be used to prove some results which will be needed in the following section.

Lemma 4: If $a,b,c \in K$, $m,n,t \geq 0$, and $a^{(i)}(b^{(j)}c^{(k)}) = (a^{(i)}b^{(j)})c^{(k)}$ for all integers $i,j,k \geq 0$, then $(aw^m)(bw^n \cdot cw^t) = (aw^m \cdot bw^n)(cw^t)$.

Proof: It is first shown that the term in w^0 of $(aw^m)(bw^n \cdot cw^t)$ is equal to the term in w^0 of $(aw^m \cdot bw^n)(cw^t)$.

$$(aw^m)(bw^n \cdot cw^t) = aw^m \sum_{i=0}^{n} \binom{n}{i} bc^{(i)} w^{n+t-i}$$

$$= \sum_{j=0}^{m} \sum_{i=0}^{n} \binom{m}{j}\binom{n}{i} a(bc^{(i)})^{(j)} w^{m+n+t-i-j}.$$

For the term in w^0, $m+n+t-i-j$ must be 0, and because $i \leq n$ and $j \leq m$, $m+n+t-i-j$ can only be zero if $i = n$, $j = m$, and $t = 0$. Thus the term in w^0 must be $\binom{m}{m}\binom{n}{n}a(bc^{(n)})^{(m)}w^0$ $= a(bc^{(n)})^{(m)}$. One now obtains, with the aid of the Leibniz formula:

$$a(bc^{(n)})^{(m)} = a\cdot\sum_{i=0}^{m}\binom{m}{i}b^{(i)}c^{(m+n-i)} = \sum_{i=0}^{m}\binom{m}{i}a(b^{(i)}c^{(m+n-i)}).$$

Similarly, $(aw^m\cdot bw^n)(cw^t) = (\sum_{i=0}^{m}\binom{m}{i}ab^{(i)}w^{m+n-i})(cw^t)$

$$= \sum_{i=0}^{m}\sum_{j=0}^{m+n-i}\binom{m+n-i}{j}\binom{m}{i}(ab^{(i)})(c^{(j)})w^{m+n+t-i-j}.$$

For the term in w^0, $m+n+t-i-j$ must be 0; and because $i \leq m$ and $j \leq m+n-i$, $m+n+t-i-j$ can only be zero if $i+j = m+n$ (i.e., $j = m+n-i$) and $t = 0$. Thus the term in w^0 must be

$$\sum_{i=0}^{m}\binom{m+n-i}{m+n-i}\binom{m}{i}(ab^{(i)})(c^{(m+n-i)})w^0 = \sum_{i=0}^{m}\binom{m}{i}(ab^{(i)})(c^{m+n-i)}).$$

Since, by the hypothesis of the lemma, $a(b^{(i)}c^{(m+n-i)})$ $= (ab^{(i)})(c^{(m+n-i)})$, these two terms in w^0 are equal as asserted.

The proof of the equality $(aw^m)(bw^n\cdot cw^t)$ $= (aw^m\cdot bw^n)(cw^t)$ is now proved by induction on the sum $m+n+t$.

If $m+n+t = 0$ the $m = n = t = 0$, $w^0 = 1$, and the conclusion follows because $a(bc) = (ab)c$.

As an <u>induction hypothesis</u>, one assumes the lemma is true for all m,n,t such that $m+n+t < s$ for some fixed $s \geq 0$.

It must be shown that the lemma is true for $m+n+t = s$. Accordingly, let $(aw^m)(bw^n\cdot cw^t) = (aw^m\cdot bw^n)(cw^t)+r$, where the lemma is true if $r = 0$. Applying the derivation D to each side of this equality, one obtains:

$$(maw^{m-1})(bw^n \cdot cw^t)+(aw^m)(nbw^{n-1} \cdot cw^t)+(aw^m)(bw^n \cdot tcw^{t-1})$$

$$= (maw^{m-1} \cdot bw^n)(cw^t)+aw^m \cdot nbw^{n-1})(cw^t)+aw^m \cdot bw^n)(tcw^{t-1})+D(r).$$

By the induction hypothesis, noting in each case that the sum of the exponents is less than s, $(aw^{m-1})(bw^n \cdot cw^t)$ $= (aw^{m-1} \cdot bw^n)(cw^t)$, $(aw^m)(bw^{n-1} \cdot cw^t) = (aw^m \cdot bw^{n-1})(cw^t)$, and $(aw^m)(bw^n \cdot cw^{t-1}) = (aw^m \cdot bw^n)(cw^{t-1})$. Hence $D(r) = 0$ and r is an element of the ring K.

Inasmuch as the term in w^0 of $(aw^m)(bw^n \cdot cw^t)$ is the same as the term in w^0 of $(aw^m \cdot bw^n)(cw^t)$ and $r \in K$, it must be that $r = 0$. This completes the proof of the lemma.

Corollary: With a, b, c, and m, n, t as in the lemma,

$$(a^{(i)}w^m)(b^{(j)}w^n \cdot c^{(k)}w^t) = (a^{(i)}w^m \cdot b^{(j)}w^n)(c^{(k)}w^t)$$

for all $i,j,k \geq 0$.

Lemma 5: If c is in the nucleus of K then, for all $n \geq 0$, cw^n is in the nucleus of K(w).

Proof: This follows from Lemma 4, the distributive laws of the ring, and the fact that the nucleus is closed under the derivation d.

Lemma 6: If $v \in K(w)$ associates with all pairs of elements of K, then so does D(v).

Proof: The assumption is that, for all $a,b \in K$, $(va)b = v(ab)$, $(av)b = a(vb)$, and $(ab)v = a(bv)$. The corresponding equalities for D(v) follow by differentiating each of these three equalities of association and then using the fact that $D(c) = 0$ for any $c \in K$. For example, in the case of the first equality of association: $(va)b = v(ab)$, and on applying D to both sides,

$(D(v)\cdot a)b+(v\cdot D(a))b+(va)(D(b))$

$= (D(v))(ab)+v(D(a)\cdot b)+v(a\cdot D(b))$, whereupon, because a and b are D-constants, $(D(v)\cdot a)b = (D(v))(ab)$, as asserted.

<u>Lemma 7</u>: An element $v \in K(w)$ associates with the pair $u,y \in K(w)$ if and only if nv associates with this pair of elements for each nonzero integer n.

<u>Proof</u>: If v associates with u and y, then $v(uy) = (vu)y$, $u(vy) = (uv)y$, and $u(yv) = (uy)v$. The corresponding equalities for nv follow from multiplying each of these three equalities of association by the integer n, recalling that K(w) is a vector space over the integers.

Conversely, let one of these equalities of association fail to hold; without loss of generality, suppose that $v(uy) \neq (vu)y$. The $v(uy) = (vu)y+t$ for $t \neq 0$. Multiplying by n, one obtains $n(v(uy)) = n((vu)y+t)$, and hence $(nv)(uy) = ((nv)u)y+nt$. Since $t \neq 0$ and the ring has zero characteristic, it is clear that $nt = 0$. Hence $(nv)(uy) \neq ((nv)u)y$, so that nv fails to associate with u and y.

<u>Lemma 8</u>: If v associates with all pairs of elements of K, then v is in the nucleus of K(w).

<u>Proof</u>: Let $v = \sum_{i=0}^{n} a_i w^i$ for $a_i \in K$. One applies the operator D^n to v and obtains $D^n(\sum_{i=0}^{n} a_i w^i) = D^n(a_n w^n + \ldots$ terms in lower powers of $w) = n!a_n$. By Lemmas 6 and 7, a_n

associates with all pairs of elements of K. By Lemma 5, $a_n w^n$ must also associate with all pairs of these elements. It is then clear that $v=a_n w^n + \sum_{i=0}^{n-1} a_i w^i$ must associate with all pairs of elements of K.

An application of D^{n-1} to $\sum_{i=0}^{n-1} a_i w^i$ leads to the conclusion that the coefficient a_{n-1} also associates with all pairs of elements of K. In this manner, one successively finds that each of the coefficients, a_n, a_{n-1}, $a_{n-2}, \ldots, a_0$, associates with all pairs of elements of K. By Lemma 5, each $a_i w^i$ is contained in the nucleus of K(w). The conclusion that v is in the nucleus of K(w) follows from taking the finite sum of the $a_i w^i$.

Note: Example 7 of Section 1.2, illustrates the fact that even a nonassociative ring K may have a nontrivial hub, namely the field F, which field may be arbitrarily chosen. It follows easily from Lemma 5 that the hub of K(w) will include all the polynomials in w with coefficients in the hub of K. These remarks indicate that Lemmas 4 through 8 above may apply in nontrivial circumstances.

3.3 Generators of Ideals.

Amitsur [1] obtained the result that, if K is a simple associative ring, then:

(1) Every nonzero ideal I of K(w) is generated by a monic element v in the center of K(w) which is of least degree in I.

(2) Conversely, if v is a monic element in the center of K(w), then v generates an ideal I of K(w) of which it

is an element of <u>least degree</u>.

Theorem 7 below is the analogous statement for a <u>d-simple</u> ring K with identity and of characteristic zero which need not be associative. It will be noted that a ring K may be d-simple or even simple, and yet admit of zero divisors. Example 7 of Section 1.2, is an example of such a ring.

<u>Lemma 1</u>: If a d-constant $v \in K(w)$ commutes with all $a \in K$, then v is in the center of K(w).

<u>Proof</u>: It will suffice to let $v = bw^n$ and to show that $(aw^m)v = v(aw^m)$ for all $a \in K$ and integers m. Since $v' = 0$, it follows that $b' = 0$, and the commutativity of a with v says that $a(bw^n) = av = va = (bw^n)a$.

$$\text{Then } (aw^m)v = (aw^m)(bw^n) = \sum_{i=0}^{m} \binom{m}{i} ab^{(i)} w^{m+n-i}$$

$$= \binom{m}{0} ab^{(0)} w^{m+n} = abw^{m+n} = (a(bw^n))w^m = ((bw^n)a)w^m$$

$= (bw^n)(aw^m) = v(aw^m)$ as asserted.

<u>Lemma 2</u>: If I is any nonzero ideal of K(w) and v is a monic element of I such that $\text{Deg } v \leq \text{Deg } u$ for all nonzero $u \in I$, then v is in the hub of K(w). Conversely, any monic v in the hub of K(w) belongs to an ideal I such that $\text{Deg } v \leq \text{Deg } u$ for all nonzero $u \in I$.

<u>Proof</u>: Let $v = w^n + \sum_{i=0}^{n-1} c_i w^i \in I$ for $c_i \in K$, where I is a nonzero ideal of K(w) and where v is of least degree in I. (If $n = 0$, then v is just 1.)

(1) <u>v commutes with each $a \in K$</u>.

The properties of I as a two-sided ideal require that

$va-av \in I$. Then $va-av = w^n a - aw^n + \ldots$terms in lower powers of w, where $w^n a = aw^n + \ldots$terms in lower powers of w; hence $va-av = aw^n - aw^n + \ldots$terms in lower powers of w. From this it follows that Deg $(va-av) < n$ or $va-av = 0$. But v is of least degree in I, requiring $va-av = 0$, and hence $va = av$ as desired for commutativity.

(2) $v' = 0$.

For $v' = wv-vw$ I, and $v' = (w^n + \sum_{i=0}^{n-1} c_i w^i)' = \sum_{i=0}^{n-1} c_i' w^i$ which must be zero because v' would otherwise be an element of I of lower degree than v.

From Lemma 1, one concludes that v is in the center of $K(w)$. It remains to show that v is contained in the nucleus of $K(w)$. By Lemma 8 of Section 3.2, it will suffice to show that v associates with all pairs of elements of K. Specifically, it will be shown that $(ab)v = a(bv)$ for $a,b \in K$, while analogous calculations establish the other two laws of association: $(av)b = a(vb)$ and $(va)b = v(ab)$. It is clear that $(ab)v-a(bv) \in I$. Recalling that w^n is in the nucleus of $K(w)$, and using the definition of multiplication of canonical polynomials, $(ab)v-a(bv) = abw^n - abw^n + \ldots$terms in lower powers of w. But, as in the proofs of (1) and (2) above, the minimal degree of v requires $(ab)v-a(bv) = 0$, and hence that $(ab)v = a(bv)$ as asserted.

Conversely, let $v = w^n + \sum_{i=0}^{n-1} c_i w^i$ be in the hub of $K(w)$. Let $I = \{u | u = xv \text{ for } x \in K(w)\}$, the set of all left $K(w)$-multiples of v. To show that I is an ideal, it suffices to show closure with respect to subtraction and left and right multiplication by elements of $K(w)$.

If $xv, yv \in I$ and $x,y \in K(w)$, then $xv-yv = (x-y)v \in I$. This shows closure with respect to subtraction.

If $xv \in I$ and $x,y \in K(w)$, then $(xv)y = x(vy) = x(yv) = (xy)v \in I$, as v is in the hub of $K(w)$. This shows closure with respect to right multiplication. And $y(xv) = (yx)v \in I$ establishes closure with respect to left multiplication.

These calculations show that I is an ideal. Let $x = \sum_{i=0}^{m} b_i w^i$ for $b_i \in K$, $b_m \neq 0$, be any nonzero element of $K(w)$. Then the left multiple $xv = b_m w^{m+n} + \ldots$terms in lower powers of w, and hence will be of degree greater than or equal to n (the degree of v). Hence v is an element of least degree as asserted. This completes the proof of the lemma.

The proof just completed entails a result of some interest in itself; if $v = w^n + \sum_{i=0}^{n-1} c_i w^i$ is a monic element of least degree in an ideal I of $K(w)$, then the coefficients c_i are d-constants and lie in the nucleus of $K(w)$.

<u>Lemma 3</u>: If I is any nonzero ideal in $K(w)$ for a <u>d-simple</u> ring K, then I is principal and is generated by its unique monic element of least degree.

<u>Proof</u>: The existence of a monic element v of least degree in I is an immediate consequence of Lemma 2 of Section 3.1 above. If v were not unique, the difference $v-v_0$ of two such monic elements of least degree would yield an element of the ideal of smaller degree.

It will be shown that any element $u \in I$ is a left multiple of v. The proof parallels that for the polynomials of elementary algebra.

Let $v = w^n + \sum_{i=0}^{n-1} c_i w^i$ and $u = \sum_{i=0}^{t} b_i w^i$ where $t \geq n$, $b_t \neq 0$. If $y = b_t w^{t-n} v$, then $y = (b_t w^{t-n})(w^n)+\ldots$terms in lower powers of w. Since $u \in I$ and $y \in I$, it follows that $u-y \in I$. But $u-y = b_t w^t - b_t w^t + \ldots$terms in lower powers of w, requiring Deg $(u-y) <$ Deg u. Now let $r_0 = u$, $q_1 = b_t w^{t-n}$, and $r_1 = u-y$, so that $r_0 = q_1 v + r_1$ where Deg $r_1 <$ Deg r_0 or $r_1 = 0$.

Algorithmically, one gets $r_1 = q_2 v + r_2$, $r_2 = q_3 v + r_3$, ..., and, after a finite number of steps, a remainder $r_k = 0$ is obtained. Then $u = (q_1 + q_2 + \ldots + q_k)v$ and the lemma has now been established.

The above two lemmas now lead to the following composite results.

Theorem 7: If K is d-simple, then:

(1) Every nonzero ideal I of K(w) is generated by a monic element v in the hub of K(w) which is of least degree in I.

(2) Conversely, if v is a monic element in the hub of K(w), then v generates an ideal I of K(w) of which it is an element of least degree.

Definition: If $r, s \in K(w)$ and s is contained in the ideal generated by r, then r divides s. If r divides elements s and t, then r is a common divisor of s and t. If r is a common divisor of s and t and is divisible by any common divisor of s and t, then r is a <u>greatest common divisor</u> of s and t.

(Ore [17] defines a concept of greatest common right divisor, but this is not the same concept as that used here.)

As a corollary to Theorem 7, one has:

<u>Corollary</u>: Let I be the ideal generated by elements s and t of K(w). Then the unique monic element v which also generates I is a greatest common divisor of s and t.

<u>Proof</u>: Since v divides each element of I, in particular v divides s and t. Hence v is a common divisor of s and t. Let r be any common divisor of s and t. Then s and t are contained in the ideal J generated by r. Since s and t generate I, it is clear that $I \subset J$. Hence the element $v \in I$ is also contained in J, and hence r divides v. Thus it has been established that v is a greatest common divisor of s and t.

If r divides s, it need not be the case that s is a multiple of r, in the sense of being of the form s = xr or s = rx for some $x \in K(w)$. All one can say is that s is contained in the ideal generated by r or, equivalently, that every ideal which contains r also contains s. But let I be the ideal generated by r. Then I is also generated by a monic v in the hub of K(w), and it is clear that (1) v divides r and r divides v, and (2) v divides $s \in K(w)$ if and only if r divides s. From the proof of Lemma 2 above, it is clear that v divides s if and only if s is a left multiple sv of v.

It is shown in Section 3.4 below that there exist nontrivial ideals of embedding rings K(w) for certain d-simple rings K.

3.4 Existence of Ideals.

Theorem 8 below asserts a necessary and sufficient condition for the existence of nontrivial ideals in the embedding ring K(w), for a d-simple ring K with identity and of characteristic zero.

The associative version of the following lemma was proved by Jacobson [4]. The omission of the associativity requirement for K renders necessary an additional clause in the statement of the lemma.

It will first be noted that, if K is d-simple, then any nonzero integer n has an inverse $n^{-1} \varepsilon K$; this inverse exists because n is a d-constant in the hub of K and generates the entire ring. Thus for d-simple K, the rings K and K(w) are vector spaces over the rational numbers.

Lemma 4: If K is d-simple and K(w) is not simple, then there exists an element t in the nucleus of K where $a' = ta-at$ for all $a \varepsilon K$.

Proof: Let I be a proper, nonzero ideal in K(w). Then I is generated by a monic element v of least degree.

Then $v = w^n + \sum_{i=0}^{n-1} c_i w^i$ for $c_i \varepsilon K$ and $n \geq 1$.

For all $a \varepsilon K$, $va-av \varepsilon I$. Expanding av and va, one obtains:

$av = aw^n + ac_{n-1}w^{n-1} + \ldots$ terms in lower powers of w, and

$va = w^n a + c_{n-1}w^{n-1}a + \ldots = aw^n + na'w^{n-1} + c_{n-1}aw^{n-1} + \ldots$ terms in lower powers of w.

Subtracting: $va-av = na'w^{n-1}+c_{n-1}aw^{n-1}-ac_{n-1}w^{n-1}+\ldots$ $= (na'+c_{n-1}a-ac_{n-1})w^{n-1}+\ldots$terms in lower powers of w. Hence va-av is either zero or of degree less than n. But $va-av \in I$, v is of least degree in I, and Deg v = n. It follows that va-av can only be zero and, therefore, each coefficient of the canonical form of va-av must be zero. In particular, $na'+c_{n-1}a-ac_{n-1} = 0$.

One concludes that, for all $a \in K$, $a' = ta-at$ where $t = -n^{-1}c_{n-1}$.

As noted in Section 3.3 above, each c_i of the canonical form of such a monic generator v is contained in the nucleus of K. Hence $t = -n^{-1}c_{n-1}$ is contained in the nucleus of K as asserted. This completes the proof the lemma.

The significance of this lemma is that, if K(w) admits of a nontrivial ideal I for a d-simple ring K, then the construction of the embedding ring K(w) is redundant. Because K(w) is constructed for the purpose of extending the derivation in the basic ring to a strong inner derivation in a larger embedding ring. If now K(w) has a nontrivial ideal I and K is d-simple, then, by the lemma just proved, the derivation in K is already a strong inner derivation and there is no embedding problem to be solved.

The monic generator v of a nontrivial ideal I of K(w) need not be of degree one. But if it is, then $v = w+c_0$, and $t = -1^{-1}c_0 = -c_0$, so that $c_0 = -t$ and $v = w-t$ generates the ideal I. However, it is easy to show that v^2, for example, will generate an ideal I in which no element is of degree one. These remarks suggest the following lemma as a converse to Lemma 4.

Lemma 5: If K is d-simple and if there is an element t in the nucleus of K such that $a' = ta-at$ for all $a \in K$, then w-t generates a proper ideal in K(w).

Proof: By Theorem 7, it suffices to show that w-t is in the hub of K(w).

To show that w-t is in the nucleus of K(w) it suffices (since w is contained in this nucleus) to show that t is in the nucleus of K(w). Specifically, it must be shown that, for all $x,y \in K(w)$: $x(yt) = (xy)t$, $x(ty) = (xt)y$, and $t(xy) = (tx)y$. It will suffice to let $x = aw^m$ and $y = bw^n$ for $a,b \in K$. Each of these laws of association now follows directly from Lemma 4 of Section 3.2 together with the fact that $t' = tt-tt = 0$ and hence that all higher derivatives of t are also zero.

It remains to show that w-t is in the center of K(w): for all $x \in K(w)$, $x(w-t) = (w-t)x$. Let $x = aw^m$ for $a \in K$. By the rule of multiplication, $w^m t = tw^m + mt'w^{m-1} + \ldots = tw^m$, because $t' = 0$.

Then $x(w-t) = aw^m(w-t) = aw^{m+1} - aw^m t = aw^{m+1} - atw^m$
$= aw^{m+1} + (ta-at)w^m - taw^m = aw^{m+1} + a'w^m - taw^m = (aw+a')w^m - taw^m$
$= waw^m - taw^m = (w-t)aw^m = (w-t)x$ as asserted.

Two examples of this lemma may be given:

1. Let the basic ring be any arbitrary ring L (of characteristic zero and with identity), and let L(t) be the embedding ring as constructed above with t playing the role of w. Write K = L(t), and let K(w) be, as usual, the

embedding ring of K. Then a' = ta-at for all a ε K, and w-t generates a proper ideal in K(w). If L is d-simple, K will also be d-simple.

2. Let the basic ring K be that of Example 7 of Section 1.2, except that here F is a noncommutative field (for example, the ring of quaternions). Any t ε F will be in the nucleus of K, and a' = ta-at defines a strong inner derivation in K. Then w-t generates a proper ideal in K(w). It can be shown that K is d-simple.

Of course, in each of these examples, the derivation in K is already a strong inner derivation, so that there was no embedding problem to be solved.

Lemmas 4 and 5 are combined in the following theorem:

Theorem 8: If K is d-simple, then either:

1. K(w) is simple, or
2. There exists t in the nucleus of K where a' = ta-at for all a ε K and w-t generates a proper ideal of K(w).

CHAPTER 4

EMBEDDING IN A DIVISION RING

4.1 The Operator $\sum_{i=-\infty}^{m} a_i w^i$.

Throughout this chapter, the basic ring K is a division ring. This means that, for any b ε K and nonzero a ε K, there is exactly one x ε K such that ax = b and exactly one y ε K such that ya = b. As in the preceding chapter, it is assumed that K has an identity and is of characteristic zero (though, in general, a nonassociative division ring need not have an identity). Because K is a division ring, it must now also be an algebra over the rational numbers and admit of no proper zero divisors.

A primary task is to solve an embedding problem for the division ring K by means of an embedding ring which is also a division ring. As discussed in Section 1.6, it has been seen to be desirable to have certain basic properties of the ring K (here the property of divisibility) preserved in an embedding ring. Specifically, one wants to find an embedding ring L such that:

(1) K is a subring of L. In particular, the derivation of the ring K is the derivation of the ring L as restricted to the subset K.

(2) L is itself a division ring.

This embedding problem will be solved by extending the Ore polynomial ring K(w) to a division ring L.

Ore [17] extended K(w) to a division ring for an associative division ring K. His construction is based on the model of the usual quotient field construction from a given integral domain.

The construction of a division ring given in this thesis involves infinite sums and therefore yields a division ring of greater cardinality than that one based on the Ore construction. However, the present construction will be seen to involve a natural extension of the material of the preceding sections, especially of the rule of multiplication of canonical polynomials given in Chapter 2 above. The division ring thus obtained will also be of interest in its own right, being basically a generalization of the classical field of formal power series. In the special case of the derivation in K being nilpotent (though involving a "generalized derivation" rather than a derivation in the sense of this thesis), the construction in this thesis coincides with that of Smits [26], the assumption of nil-potency eliminating the need for infinite sums. However, it is not difficult to show that (using the word "derivation" in the strict sense defined in Chapter 1), there do not exist any division rings of characteristic zero with nilpotent derivation.

In the sequel it will be shown that, in the case of associative K, Ore's division ring is a subring of the division ring constructed in this thesis.

To initiate the task set out above, one must define an element w^{-1} as the inverse of the element $w \in K(w)$. Lemma 1 below will lead the way to such a definition.

The left K-module M of Chapter 2 should be recalled at this time. Each element of M is of the form $\sum_{i=-\infty}^{n} c_i z^{(i)}$ where $c_i \in K$ and n is any integer. The element w of the ring K(w) is the M-derivation mapping. Let $u = \sum_{i=-\infty}^{n-1} b_i z^{(i)}$. Then $w(u) = u' = (\sum_{i=-\infty}^{n-1} b_i z^{(i)})' = \sum_{i=-\infty}^{n} a_i z^{(i)}$ where $a_i = b_{i-1}+b_i'$ for $i < n$ and $a_n = b_{n-1}$. In particular, $w(z^{(n)}) = (z^{(n)})' = z^{(n+1)}$ for any integer n.

Lemma 1: For each $v \in M$, there is exactly one $u \in M$ such that $u' = v$.

Proof: Let $v = \sum_{i=-\infty}^{n} a_i z^{(i)}$ with $a_i \in K$. To show the existence of the desired element, consider $u = \sum_{i=-\infty}^{n-1} b_i z^{(i)}$ where the b_i are defined inductively as follows, b_{i-1} being defined in terms of b_i:

$$b_{n-1} = a_n.$$

$$b_{i-1} = a_i - b_i', \text{ or, equivalently, } b_{i-1}+b_i' = a_i,\ i < n.$$

It is clear from the definition of M-derivation that $u' = v$.

To show the uniqueness of this element u, let $u' = k' = v$ for some $k \in M$. If $m = u-k$, then $m' = (u-k)' = u'-k' = 0$. The argument will be complete if one shows that m can only be zero.

If m is not zero, then $m = \sum_{i=-\infty}^{n-1} c_i z^{(i)}$ for $c_i \in K$, where, without loss of generality, the coefficient c_{n-1} of the highest term can be assumed to be nonzero. Then

$m' = \sum_{i=-\infty}^{n} d_i z^{(i)}$ where $d_i = c_{i-1}+c_i'$ for each $i < n$ and $d_n = c_{n-1}$. But since m' is zero, it follows that $d_n = 0 = c_{n-1}$, contradicting the assumption that $c_{n-1} \neq 0$.

Definition of w^{-1}: w^{-1} is the mapping of M such that $w^{-1}(v) = u$ where $u' = v$. Clearly, $w(w^{-1}(v)) = w^{-1}(w(v)) = v$ for all $v \in M$, so that w^{-1} is the mapping that is inverse to w. This operator w^{-1} may appropriately be referred to as M-integration.

Lemma 1 is now seen as asserting that each element of M has a unique M-integral.

As was seen to be the case for the M-derivation mapping w, the following lemma shows that w^{-1} is also an endomorphism of $\{M;+\}$.

Lemma 2: For all $u,v \in M$, $w^{-1}(u+v) = w^{-1}(u)+w^{-1}(v)$.

Proof: Let $k = w^{-1}(u+v)-w^{-1}(u)-w^{-1}(v)$, so that $w^{-1}(u+v) = w^{-1}(u)+w^{-1}(v)+k$. Applying w to each side of this equality and using the fact that w is an endomorphism, one obtains $u+v = u+v+w(k)$ and hence $w(k) = 0$. Then $w^{-1}(w(k)) = w^{-1}(0)$, whereupon $k = 0$ by Lemma 1 (uniqueness of the M-integral) and the lemma has been established.

The symbolism $z^{(n)}$ was introduced in Chapter 2 to denote that element of M with 1 as its nth component and zeros elsewhere. It was observed that, if n is positive, $z^{(n)}$ is the nth M-derivative of z. It may now be observed that, if n is negative, $z^{(n)}$ is the (-n)th M-integral of z, the result of -n applications of w^{-1} to z. Such symbolism may now be extended to arbitrary elements of M. One may write $v^{(n)}$ where $v \varepsilon M$ and n is any integer. If $n = 0$, then $v^{(n)} = v^{(0)} = v$. If n is positive, then $v^{(n)}$ is the nth M-derivative of v, the result of n applications of w to v. If n is negative, then $v^{(n)}$ is the (-n)th M-integral of v, the result of -n applications of w^{-1} to v. It is Lemma 1 which makes this symbol $v^{(n)}$ meaningful for arbitrary $n < 0$.

As was done in Section 2.5, one can now form finite linear combinations $\sum_{i=k}^{n} a_i w^i$, the summation permissible between <u>arbitrary</u> integers k and n. Thus, for each $v \varepsilon M$, $\sum_{i=k}^{n} a_i w^i(v) = \sum_{i=k}^{n} a_i v^{(i)}$. One makes the analogous definitions of <u>equality</u> and <u>addition</u> as in Section 2.5 for these more general functions, these definitions being the usual ones for mappings. It is easily seen that two such sums are equal as functions only if their corresponding terms are equal, and that they add termwise. As a corollary to Lemma 2, each mapping of the form $\sum_{i=k}^{n} a_i w^i$ is an endomorphism of $\{M;+\}$.

The following lemma will be useful in the sequel.

<u>Lemma 3</u>: If $v = \sum_{i=-\infty}^{n} c_i z^{(i)}$ for $c_i \varepsilon K$, then, for any integer t, there exist $d_i \varepsilon K$ such that $v^{(t)} = \sum_{i=-\infty}^{n+t} d_i z^{(i)}$ (where any of the coefficients c_i or d_i may possibly be zero).

This lemma may alternatively be stated as follows:

For any integer t, if v has no nonzero terms in $z^{(s)}$ for $s > n$, then $v^{(t)}$ has no nonzero terms in $z^{(s)}$ for $s > n+t$.

Proof: If $t = 0$, the lemma is clear. If $t > 0$, then $v^{(t)} = w^t(v)$, where each application of the operator w is an M-differentiation. From the rule for M-differentiation, $w(v) = \sum_{i=-\infty}^{n+1} e_i z^{(i)}$ for $e_i \in K$ where $e_{n+1} = c_n$, as stated (for $t = 1$) in the lemma; the general case ($t > 0$) follows by induction. Similarly, if $t < 0$, then it sufficies to look at a simple application of the inverse operator w^{-1}, and the proof for this case ($t = -1$) is analogous. An inspection of the leading coefficients of v and $v^{(t)}$ show them to be identical, and from this one concludes that the effect of applying w^t to v is to shift the leading coefficient of v by t places.

Definition: The mapping $\sum_{i=-\infty}^{m} a_i w^i$, on M into M, with $a_i \in K$ and m an arbitrary integer, is described as follows:

For any $\sum_{i=-\infty}^{n} b_i z^{(i)} \in M$ with $b_i \in K$,

$\sum_{i=-\infty}^{m} a_i w^i(\sum_{i=-\infty}^{n} b_i z^{(i)}) = \sum_{h=-\infty}^{m+n} c_h z^{(h)}$, where, for each h, c_h is the coefficient of $z^{(h)}$ in $\sum_{i=h-n}^{m} a_i w^i(\sum_{i=h-m}^{n} b_i z^{(i)})$. The set of these mappings will be denoted by $K(w,w^{-1})$.

To see how this definition applies, the computation of the special case $\sum_{i=-\infty}^{m} a_i w^i(z)$ is now carried out. One must compute the term in $z^{(h)}$ for each $h \leq m$. By the definition just given, the term in $z^{(h)}$ of $\sum_{i=-\infty}^{m} a_i w^i(z)$ is the same as the term in $z^{(h)}$ of $\sum_{i=h-0}^{m} a_i w^i(\sum_{i=h-m}^{0} b_i z^{(i)})$, where $b_0 = 1$ and, for $i \neq 0$, $b_i = 0$. But

$\sum_{i=h-0}^{m} a_i w^i(\sum_{i=h-m}^{0} b_i z^{(i)}) = (\sum_{i=h}^{m} a_i w^i)(z) = \sum_{i=h}^{m} a_i z^{(i)}$, and the term in $z^{(h)}$ is $a_h z^{(h)}$. By letting h range from $-\infty$ to m, one finds that $\sum_{i=-\infty}^{m} a_i w^i(z) = \sum_{i=-\infty}^{m} a_i z^{(i)}$, which result extends the corresponding result in Section 2.5. More generally, one finds that $\sum_{i=-\infty}^{m} a_i w^i(z^{(n)}) = \sum_{i=-\infty}^{m} a_i z^{(n+i)}$.

To determine $\sum_{i=-\infty}^{n} a_i w^i(\sum_{i=-\infty}^{m} b_i z^{(i)})$ one must, in effect, find each $(a_j w^j)(b_k z^{(k)})$ for every j and k, and then "add together the results". This is the motivation behind the definition given above. Lemma 3 ensures that there are at most a finite number of terms in each $z^{(h)}$.

If all but a finite number of the a_i are zero, this "infinite sum" operator $\sum_{i=-\infty}^{m} a_i w^i$ reduces to a finite sum operator of the type previously considered, because, as the following lemma shows, in this case the definition given above agrees with the definition previously given for these finite sums. It will suffice to consider the term in $z^{(h)}$ for arbitrary h.

Lemma 4: Let $s \leq m$, $t \leq n$, $a_i, b_i \in K$, $a_i = 0$ for all $i < s$ and $b_i = 0$ for all $i < t$. Then $\sum_{i=-\infty}^{m} a_i w^i (\sum_{i=-\infty}^{m} b_i z^{(i)})$

$= \sum_{i=s}^{m} a_i w^i (\sum_{i=t}^{n} b_i z^{(i)})$.

Proof: It will be shown that, for all $h \leq m+n$, the term in $z^{(h)}$ of $\sum_{i=-\infty}^{m} a_i w^i (\sum_{i=-\infty}^{n} b_i z^{(i)})$ is equal to the term in $z^{(h)}$ of $\sum_{i=s}^{m} a_i w^i (\sum_{i=t}^{n} b_i z^{(i)})$.

By the definition given above, the term in $z^{(h)}$ of $\sum_{i=-\infty}^{m} a_i w^i (\sum_{i=-\infty}^{n} b_i z^{(i)})$ is the term in $z^{(h)}$ of $\sum_{i=h-n}^{m} a_i w^i (\sum_{i=h-m}^{n} b_i z^{(i)})$. By including zero terms if necessary in the given finite summations, one may write $\sum_{i=s}^{m} a_i w^i = \sum_{i=s*}^{m} a_i w^i$ and $\sum_{i=t}^{n} b_i z^{(i)} = \sum_{i=t*}^{n} b_i z^{(i)}$ where $s* \leq s$, $t* \leq t$, $s* \leq h-n$, and $t* < h-m$. Then $\sum_{i=s}^{m} a_i w^i (\sum_{i=t}^{n} b_i z^{(i)})$

$= \sum_{i=s*}^{m} a_i w^i (\sum_{i=t*}^{n} b_i z^{(i)}) = \sum_{i=h-n}^{m} a_i w^i (\sum_{i=h-m}^{n} b_i z^{(i)}) + S$, where S is a sum of terms of the form $a_i w^i (b_j z^{(j)})$ and either $i < h-n$ or $j < h-m$ (or both). In either case (since also $i \leq m$ and $j \leq n$), $h > i+j$. The lemma will be established if it can be shown that S has no nonzero terms in $z^{(h)}$. But since w is the M-derivation operator, each $a_i w^i (b_j z^{(j)}) = a_i (b_j z^{(j)})^{(i)}$. By Lemma 3, this element has no nonzero terms in $z^{(k)}$ for any $k > i+j$; it follows (choosing $k = h$) that S has no nonzero terms in $z^{(h)}$ as asserted.

Definition: The degree of $\sum_{i=-\infty}^{m} a_i w^i$ for $a_i \in K$ and $a_m \neq 0$ is m. It will also be convenient to refer to the degree of an element of M; accordingly, the degree of $\sum_{i=-\infty}^{n} c_i z^{(i)}$ for $c_i \in K$ and $c_n \neq 0$ is n. As in Chapter 3 above, one writes Deg u or Deg v for $u \in K(w,w^{-1})$ or $v \in M$.

4.2 The Ring $K(w,w^{-1})$.

The elements of the system $K(w,w^{-1})$ are the operators $\sum_{i=-\infty}^{m} a_i w^i$ defined in the preceding section, for arbitrary $a_i \in K$ and integer m. An operation of addition is defined below. In order to complete the construction of this system as a ring, the operation of multiplication must also be defined, but this will be deferred until later.

Since $\sum_{i=-\infty}^{m} a_i w^i(z) = \sum_{i=-\infty}^{m} a_i z^{(i)}$ and $\sum_{i=-\infty}^{m} b_i w^i(z) = \sum_{i=-\infty}^{m} b_i z^{(i)}$ for $a_i, b_i \in K$, it is clear from the component-wise definition of equality in M that $\sum_{i=-\infty}^{m} a_i w^i(z) = \sum_{i=-\infty}^{m} b_i w^i(z)$ if and only if, for each i, $a_i = b_i$. It follows easily that $\sum_{i=-\infty}^{m} a_i w^i(v) = \sum_{i=-\infty}^{m} b_i w^i(v)$ for all $v \in M$ if and only if, for each i, $a_i = b_i$. It is therefore natural to define: $\sum_{i=-\infty}^{m} a_i w^i = \sum_{i=-\infty}^{m} b_i w^i$ if, for each i, $a_i = b_i$. (It is also understood that zero terms can be added to an operator without altering its value.)

The following lemma will serve as the basis for a definition of addition in $K(w,w^{-1})$.

Lemma 1: For all $v \varepsilon M$, $a_i, b_i \varepsilon K$:

$$\sum_{i=-\infty}^{m} a_i w^i(v) + \sum_{i=-\infty}^{m} b_i w^i(v) = \sum_{i=-\infty}^{m} (a_i+b_i) w^i(v).$$

Proof: Let $v = \sum_{i=-\infty}^{n} c_i z^{(i)}$ for $c_i \varepsilon K$. The term in $z^{(h)}$ of the left side of the asserted equality is the term in $z^{(h)}$ of $\sum_{i=h-m}^{n} a_i w^i\left(\sum_{i=h-n}^{m} c_i z^{(i)}\right) + \sum_{i=h-m}^{n} b_i w^i\left(\sum_{i=h-n}^{m} c_i z^{(i)}\right)$, and the term in $z^{(h)}$ of the right side is the term in $z^{(h)}$ of $\sum_{i=h-m}^{n} (a_i+b_i) w^i\left(\sum_{i=h-n}^{m} c_i z^{(i)}\right)$. The conclusion now follows from the known equality of these finite sums, letting h range from $-\infty$ to m+n.

Definition: $\sum_{i=-\infty}^{m} a_i w^i + \sum_{i=-\infty}^{m} b_i w^i = \sum_{i=-\infty}^{m} (a_i+b_i) w^i$ for $a_i, b_i \varepsilon K$. It is clear that the definitions of equality and addition given for these operators are the usual functional definitions and thus extend the definitions given earlier for finite sum operators. It is also clear from the above definitions and the obvious existence of the zero element and negatives that $\{K(w,w^{-1});+\}$ is an abelian group.

The following lemma shows that the elements of $K(w,w^{-1})$ satisfy linearity conditions, i.e., are endomorphisms of $\{M;+\}$.

Lemma 2: $\sum_{i=-\infty}^{m} a_i w^i(u) + \sum_{i=-\infty}^{m} a_i w^i(v) = \sum_{i=-\infty}^{m} a_i w^i(u+v)$ for arbitrary $u, v \in M$, $a_i \in K$.

Proof: Let $u = \sum_{i=-\infty}^{n} b_i z^{(i)}$ and $v = \sum_{i=-\infty}^{n} c_i z^{(i)}$, with $b_i, c_i \in K$, adding zero terms if necessary to ensure identity of ranges of summation. Then the term in $z^{(h)}$ of the left side of the asserted equality is the term in $z^{(h)}$ of

$\sum_{i=h-n}^{m} a_i w^i(\sum_{i=h-m}^{n} b_i z^{(i)}) + \sum_{i=h-n}^{m} a_i w^i(\sum_{i=h-m}^{n} c_i z^{(i)})$ and the term in $z^{(h)}$ of the right side is the term in $z^{(h)}$ of $\sum_{i=h-n}^{m} a_i w^i(\sum_{i=h-m}^{n} (b_i + c_i) z^{(i)})$. The conclusion now follows from the known equality of these finite sums, letting h range from $-\infty$ to m+n.

To extend the material of Section 2.5 of Chapter 2 to these more general mappings, it is necessary to state and prove a variation of the Leibniz formula; this is done in Lemma 4 below (see Section 2.1).

Definition: Let n be any integer (possibly zero or negative) while i is a non-negative integer. Then the symbol $\binom{n}{i}$ denotes the number $n(n-1)\dots(n-i+1)/i!$ if $i > 0$, and the number 1 if $i = 0$.

This is an extension of the usual definition for positive n, though in the present usage only the i need be non-negative.

Lemma 3: For all integers n and all positive integers i, $\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}$.

Proof: If $i = 1$, the conclusion is clear, so let $i > 1$.
Then $\binom{n}{i}+\binom{n}{i-1} = n(n-1)\ldots(n-i+1)/i!+n(n-1)\ldots(n-i+2)/(i-1)!$
$= n(n-1)\ldots(n-i+2)((n-i+1)+i)/i!$
$= (n+1)n(n-1)\ldots(n-i+2)/i! = \binom{n+1}{i}$.

Lemma 4: For all $a \in K$ and arbitrary integer n,
$(az)^{(n)} = \sum_{i=0}^{\infty} \binom{n}{i} a^{(i)} z^{(n-i)}$.

Proof: This formula is known to be true for $n \geq 0$; it will be shown, by induction, to be true also for $n < 0$.

If $n = 0$, then the result is trivial in this case.

As an induction hypothesis, one assumes that, for a fixed $n < 0$, $(az)^{(n+1)} = \sum_{i=0}^{\infty} \binom{n+1}{i} a^{(i)} z^{(n-i+1)}$, this being the assertion of the lemma for $n+1$.

It must be shown that the lemma is valid for n, on the assumption that it is valid for $n+1$: effectively that the M-integral of $(az)^{(n+1)}$ is $\sum_{i=0}^{\infty} \binom{n}{i} a^{(i)} z^{(n-i)}$, or,

equivalently, that $w(\sum_{i=0}^{\infty} \binom{n}{i} a^{(i)} z^{(n-i)})$
$= \sum_{i=0}^{\infty} \binom{n+1}{i} a^{(i)} z^{(n-i+1)}$.

By either Section 2.5 of Chapter 2 (or directly from the definition given in Section 4.1 above),
$$w(\sum_{i=0}^{\infty} \binom{n}{i} a^{(i)} z^{(n-i)}) = \sum_{i=0}^{\infty} \binom{n}{i} a^{(i+1)} z^{(n-i)} + \sum_{i=0}^{\infty} \binom{n}{i} a^{(i)} z^{(n-i+1)}.$$

Replacing i by $i-1$ in the first summation, the two infinite sums become:

$$\sum_{i=1}^{\infty} \binom{n}{i-1} a^{(i)} z^{(n-i+1)} + \sum_{i=0}^{\infty} \binom{n}{i} a^{(i)} z^{(n-i+1)}$$

$$= \sum_{i=1}^{\infty} \left[\binom{n}{i-1}+\binom{n}{i}\right] a^{(i)} z^{(n-i+1)} + \binom{n}{0} a^{(0)} z^{(n-0+1)}$$

$$= \sum_{i=1}^{\infty} \binom{n+1}{i} a^{(i)} z^{(n-i+1)} + a^{(0)} z^{(n+1)} = \sum_{i=0}^{\infty} \binom{n+1}{i} a^{(i)} z^{(n-i+1)},$$

whereupon $w\left(\sum_{i=0}^{\infty} \binom{n}{i} a^{(i)} z^{(n-i)}\right) = \sum_{i=0}^{\infty} \binom{n+1}{i} a^{(i)} z^{(n-i+1)}$

as asserted.

The generalization of Section 2.5 of Chapter 2 is now carried out for the more general infinite mapping. In order to regard the system $K(w,w^{-1})$ as a ring which extendes the rings K and K(w), it is necessary to define products in $K(w,w^{-1})$. The definition given here extends that given in Section 2.5.

Definition: Let f, g, and h be elements of $K(w,w^{-1})$. Then h is the product of f and g if $f(g(z)) = h(z)$.

As shown for the finite sum operators in Section 2.5, it is true here as well that this product, where defined, must be unique. Henceforth, the usual multiplicative notations will be used.

Lemma 5: For $a,b \in K$ and m and n arbitrary integers (possibly negative), the product $(aw^m)(bw^n)$ is defined, and equal to $\sum_{i=0}^{\infty} \binom{m}{i} ab^{(i)} w^{m+n-i}$.

Proof: The proof is similar to Lemma 3 of Section 2.5, but using Lemma 4 in place of the (usual) Leibniz formula.

The following lemma shows that the operation of multiplication is closed in $K(w,w^{-1})$, that for <u>all</u> pairs of elements, $f,g \in K(w,w^{-1})$, the product fg exists (uniquely).

<u>Lemma 6</u>: For any $f,g \in K(w,w^{-1})$ there is a (unique) $h \in K(w,w^{-1})$ such that $fg = h$.

<u>Proof</u>: By Section 4.1 above, the element $g(z) \in M$ is determined. Moreover, by applying the mapping f to g(z), the element $f(g(z)) \in M$ is determined. As an element of M, $f(g(z)) = \sum_{i=-\infty}^{n} c_i z^{(i)}$ for some integer n and $c_i \in K$. Thus, if $h = \sum_{i=-\infty}^{n} c_i w^i \in K(w,w^{-1})$, $h(z) = f(g(z))$. By the definition of a product, h is <u>a</u> product of the pair (f,g) and hence (because, as noted above, products are unique) h is <u>the</u> product of this pair.

The following lemma elaborates and clarifies the infinite sum mapping as defined in Section 4.1.

<u>Lemma 7</u>: For $a_i, b_i \in K$ and m and n integers,

$$\sum_{i=-\infty}^{m} a_i w^i \left(\sum_{i=-\infty}^{n} b_i z^{(i)} \right) = \sum_{h=-\infty}^{m+n} \sum_{i=h-n}^{m} \sum_{\substack{j=h-i \\ h-m \le j \le n}}^{h} \binom{i}{i+j-h} a_i b_j^{(i+j-h)} z^{(h)}.$$

<u>Proof</u>: One shows that the term in $z^{(h)}$ of $\sum_{i=-\infty}^{m} a_i w^i \left(\sum_{i=-\infty}^{n} b_i z^{(i)} \right)$ is $\sum \binom{i}{i+j-h} a_i b_j^{(i+j-h)} z^{(h)}$, summing i and j over the ranges indicated above.

By the definition given in Section 4.1 the term in $z^{(h)}$ of

$\sum_{i=-\infty}^{m} a_i w^i (\sum_{i=-\infty}^{n} b_i z^{(i)})$ is identical to the term in $z^{(h)}$ of

$\sum_{i=h-n}^{m} a_i w^i (\sum_{i=h-m}^{n} b_i z^{(i)})$. For each i ($h-n \leq i \leq m$) and each

j ($h-m \leq j \leq n$), it follows from Lemma 5 that

$a_i w^i (b_j z^{(j)}) = (a_i w^i)(b_j w^j)(z) = \sum_{t=0}^{\infty} \binom{i}{t} a_i b_j^{(t)} w^{i+j-t}(z)$

$= \sum_{t=0}^{\infty} \binom{i}{t} a_i b_j^{(t)} z^{(i+j-t)}$. For the terms in $z^{(h)}$ of the one general summand, one considers values of t for which $i+j-t = h$, or, equivalently, $t = i+j-h$, so that the terms in $z^{(h)}$ are of the form $\binom{i}{i+j-h} a_i b_j^{(i+j-h)} z^{(h)}$. Since $t \geq 0$, one sees that $i+j \geq h$. The total term in $z^{(h)}$ for the given expression is then the finite sum

$\sum \binom{i}{i+j-h} a_i b_j^{(i+j-h)} z^{(h)}$ for $h-n \leq i \leq m$, $h-m \leq j \leq n$, and $i+j \geq h$, from which inequalities the indicated ranges of summation follow.

With this result at hand, it is now easy to see how products must be computed for elements of $K(w,w^{-1})$.

<u>Theorem 9</u>: The system $\{K(w,w^{-1});+,\cdot\}$ is a ring which extends K, with multiplication in the ring given by:

$$\left(\sum_{i=-\infty}^{m} a_i w^i\right)\left(\sum_{i=-\infty}^{n} b_i w^i\right) = \sum_{h=-\infty}^{m+n} \sum_{i=h-n}^{m} \sum_{\substack{j=h-i \\ h-m\leq j\leq n}}^{h} \binom{i}{i+j-h} a_i b_j^{(i+j-h)} w^h,$$

for $a_i, b_i \in K$ and m and n arbitrary integers.

<u>Proof</u>: With i and j ranging over the indicated values, one sees that

$$\left(\sum_{i=-\infty}^{m} a_i w^i\right)\left(\sum_{i=-\infty}^{n} b_i w^i\right)(z) = \sum_{i=-\infty}^{m} a_i w^i\left(\sum_{i=-\infty}^{n} b_i w^i(z)\right)$$

$$= \sum_{i=-\infty}^{m} a_i w^i\left(\sum_{i=-\infty}^{n} b_i z^{(i)}\right) = \sum_{h=-\infty}^{m+n} \sum_{i=h-n}^{m} \sum_{\substack{j=h-i \\ h-m\leq j\leq n}}^{h} \binom{i}{i+j-h} a_i b_j (i+j-h)_z (h)$$

$$= \sum_{h=-\infty}^{m+n} \sum_{i=h-n}^{m} \sum_{\substack{j=h-i \\ h-m\leq j\leq n}}^{h} \binom{i}{i+j-h} a_i b_j^{(i+j-h)} w^h(z). \quad \text{Hence}$$

$$\left(\sum_{i=-\infty}^{m} a_i w^i\right)\left(\sum_{i=-\infty}^{n} b_i w^i\right) = \sum_{h=-\infty}^{m+n} \sum_{i=h-n}^{m} \sum_{\substack{j=h-i \\ h-m\leq j\leq n}}^{h} \binom{i}{i+j-h} a_i b_j^{(i+j-h)} w^h$$

as asserted.

To complete the proof that $K(w,w^{-1})$ is a ring, it must be verified that the distributive laws are valid: $f(g+h) = fg+fh$ and $(g+h)f = gf+hf$ for any $f,g,h \in K(w,w^{-1})$. But this follows from Lemma 2 above and an argument which parallels that of Lemma 2 of Section 2.5.

4.3 The Differential Ring $K(w,w^{-1})$.

In order to regard $K(w,w^{-1})$ as a differential ring, one must define an operation of derivation in $K(w,w^{-1})$. For this purpose, it is shown in Lemma 4 below that w is contained in the nucleus of $K(w,w^{-1})$.

Lemma 1: For $a_i, b_i \in K$, m, n, and h integers, and $h \leq m+n$, the term in w^h of $\left(\sum_{i=-\infty}^{m} a_i w^i\right)\left(\sum_{i=-\infty}^{n} b_i w^i\right)$ is equal to the term in w^h of $\left(\sum_{i=h-n}^{m} a_i w^i\right)\left(\sum_{i=h-m}^{n} b_i w^i\right)$.

Proof: This follows from the definition given in Section 4.1 above, and a proof analogous to that of Theorem 9.

It may be noted that

$(\sum_{i=-\infty}^{m} a_i w^i)(\sum_{i=-\infty}^{n} b_i w^i) = \binom{n}{0} a_m b_n^{(0)} w^{m+n} + B = a_m b_n w^{m+n} + B$, where $B \in K(w,w^{-1})$ is zero or of degree less than m+n.

Lemma 2: Let $u,v \in K(w,w^{-1})$, $u \neq 0$, $v \neq 0$. Then Deg uv = Deg u + Deg v.

Proof: Let $u = \sum_{i=-\infty}^{m} a_i w^i$, $v = \sum_{i=-\infty}^{n} b_i w^i$, $a_m \neq 0$, $b_n \neq 0$.

Then $uv = a_m b_n w^{m+n} + B$ for B zero or of degree less than m+n. But K, as a division ring, contains no zero divisors, whereupon $a_m \neq 0$ and $b_n \neq 0$ imply $a_m b_n \neq 0$. Hence $a_m b_n \neq 0$ and Deg uv = Deg u + deg v.

Lemma 3: For $x = aw^m$, $y = bw^n$, and $a,b \in K$, $(wx)y = w(xy)$, $(xw)y = x(wy)$, and $(xy)w = x(yw)$.

Proof: The proof is similar to that of Theorem 3 above, with Lemma 5 of Section 4.2 in place of Lemma 3 of Section 2.5 in the earlier proof.

Lemma 4: The element w is contained in the nucleus of $K(w,w^{-1})$.

Proof: It is shown that $(wu)v = w(uv)$ for $u,v \in K(w,w^{-1})$, while analogous proofs establish the other two laws of association.

Let $u = \sum_{i=-\infty}^{m} a_i w^i$ and $v = \sum_{j=-\infty}^{n} b_j w^j$ for $a_i, b_j \in K$, $a_m \neq 0$, and $b_n \neq 0$. It is to be shown that, for $h \leq m+n+1$, the term in w^h of $(wu)v$ is equal to the term in w^h of $w(uv)$.

Let $Q = \sum_{i=h-n-1}^{m} a_i w^i$, $R = \sum_{i=-\infty}^{h-n-2} a_i w^i$, $S = \sum_{j=h-m-1}^{n} b_j w^j$, and $T = \sum_{j=-\infty}^{h-m-2} b_j w^j$, where Deg Q = m, either Deg R < h-n-1 or R = 0, Deg S = n, and either Deg T < h-m-1 or T = 0. Then u = Q+R, v = S+T, and (wu)v = (wQ)S+(wQ)T+(wR)S+(wR)T.

It follows from Lemma 2 (recalling that Deg w = 1) that:

Either (wQ)T = 0 or Deg (wQ)T < 1+m+(h-m-1) = h.

Either (wR)S = 0 or Deg (wR)S < 1+(h-n-1)+n = h.

Either (wR)T = 0 or Deg (wR)T < 1+(h-n-1)+(h-m-1) < h.

Hence only the summand (wQ)S of (wu)v can contribute to terms in w^h. It follows that the term in w^h of (wu)v is equal to the term in w^h of (wQ)S where one notes that

$$(1) \qquad (wQ)S = \sum_{i=h-n-1}^{m} \sum_{j=h-m-1}^{n} ((w)(a_i w^i))(b_j w^j).$$

Similarly, w(uv) = w(QS)+w(QT)+w(RS)+w(RT), where only the summand w(QS) can contribute to terms in w^h. Hence the term in w^h of w(uv) is equal to the term in w^h of w(QS) where

$$(2) \qquad w(QS) = \sum_{i=h-n-1}^{m} \sum_{j=h-m-1}^{n} (w)((a_i w^i)(b_j w^j)).$$

The conclusion now follows from (1) and (2) and Lemma 3.

Definition For all $v \in K(w,w^{-1})$, the derivative v' = wv-vw.

Since w is contained in the nucleus of $K(w,w^{-1})$, the mapping of v to v' is a strong inner derivation. This definition clearly extends the definitions previously given for the rings K and K(w).

Lemma 5: The element w^{-1} is contained in the nucleus of $K(w,w^{-1})$.

Proof: Let $u,v \in K(w,w^{-1})$. It is shown that $(uv)w^{-1} = u(vw^{-1})$. $(uw^{-1})v = u(w^{-1}v)$, and $(w^{-1}u)v = w^{-1}(uv)$.

(1) To show that $(uv)w^{-1} = u(vw^{-1})$.

Let $v = \sum_{i=-\infty}^{n} a_i w^i$, $v^* = \sum_{i=-\infty}^{n} a_i w^{i-1}$. Then $v^*w = v$, $v^* = vw^{-1}$, and $(uv)w^{-1} = (u(v^*w))w^{-1} = ((uv^*)w)w^{-1} = (uv^*)(ww^{-1}) = uv^*$ $= u(vw^{-1})$ as asserted.

(2) To show that $(uw^{-1})v = u(w^{-1}v)$.

Let $u = \sum_{i=-\infty}^{m} b_i w^i$, $u^* = \sum_{i=-\infty}^{m} b_i w^{i-1}$. The $u^*w = u$, and

$(uw^{-1})v = ((u^*w)w^{-1})v = (u^*(ww^{-1}))v = u^*v = u^*((ww^{-1})v)$
$= u^*(w(w^{-1}v)) = (u^*w)(w^{-1}v) = u(w^{-1}v)$ as asserted.

(3) To show that $(w^{-1}u)v = w^{-1}(uv)$.

The proof of this is analogous to that of (1).

The following lemma states that not only w but arbitrary integral powers of w are contained in the nucleus of $K(w,w^{-1})$. This lemma, together with Lemmas 7 and 8 below, will establish that, if K is associative, $K(w,w^{-1})$ is also associative; this result is stated and proved below as Theorem 10.

Lemma 6: For any integer n, w^n is contained in the nucleus of $K(w,w^{-1})$.

Proof: This follows from Lemmas 4 and 5 by induction arguments analogous to that of Lemma 1 of Section 2.2.

Lemma 7: Let K be associative. Then, for $u,v \in K(w,w^{-1})$, $a \in K$, $(au)v = a(uv)$.

Proof: Let $u = \sum_{i=-\infty}^{m} b_i w^i$ and $v = \sum_{i=-\infty}^{n} c_i w^i$ for $b_i, c_i \in K$.

It is shown that, for $h \le m+n$, the term in w^h of $(au)v$ is equal to the term in w^h of $a(uv)$.

But, by Lemma 1, the term in w^h of $(au)v$ is equal to the term in w^h of (1) $(\sum_{i=h-n}^{m} ab_i w^i)(\sum_{i=h-m}^{n} c_i w^i)$, and the term in w^h of $a(uv)$ is equal to the term in w^h of

(2) $a((\sum_{i=h-n}^{m} b_i w^i)(\sum_{i=h-m}^{n} c_i w^i))$. It will suffice to show that (1) = (2).

However, (1) is a finite sum of terms of the form $(ab_i w^i)(c_j w^j) = \sum_{k=0}^{\infty} \binom{i}{k} (ab_i) c_j^{(k)} w^{i+j-k}$, (2) is a finite sum of terms of the form $a((b_i w^i)(c_j w^j)) = a \sum_{k=0}^{\infty} \binom{i}{k} b_i c_j^{(k)} w^{i+j-k}$, and equality follows by $(ab_i)c_j^{(k)} = a(b_i c_j^{(k)})$ for each choice of i,j,k because K is assumed to be associative and these are products in K.

Lemma 8: Let K be associative. Then $(aw^m \cdot bw^n)cw^t = aw^m(bw^n \cdot cw^t)$ for arbitrary integers m,n,t and $a,b,c \in K$.

Proof: The fact that powers of w are contained in the nucleus of $K(w,w^{-1})$ is used throughout.

Let the symbol d_i denote the element $\binom{n}{i} c^{(i)}$. Then, directly from the rule of multiplication, it follows that $w^n c = \sum_{i=0}^{\infty} d_i w^{n-i}$. This equality will be assumed in what follows.

$(aw^m \cdot bw^n)cw^t = ((aw^m \cdot bw^n)c)w^t = (((aw^m b)(w^n))c)w^t$

$= ((aw^m b)(w^n c))w^t = (\sum((aw^m b)(d_i w^{n-i})))w^t$

$= \sum(aw^m b)(d_i w^{n+t-i})$, omitting the limits of the summation.

Applying Lemma 7 twice, one obtains:

$\sum(aw^m b)(d_i w^{n+t-i}) = a \sum(w^m b)(d_i w^{n+t-i}))$

$= a \sum((w^m)(bd_i w^{n+t-i})) = \sum(aw^m)(bd_i w^{n+t-i})$

$= (\sum(aw^m)(bd_i w^{n-i}))w^t = (\sum(aw^m)((b)(d_i w^{n-i})))w^t$

$= ((aw^m)((b)(w^n c)))w^t = ((aw^m)((bw^n)(c)))w^t$

$= aw^m((bw^n \cdot c)w^t) = aw^m(bw^n \cdot cw^t)$ as asserted.

<u>Theorem 10</u>: If K is associative, then $K(w,w^{-1})$ is associative.

<u>Proof</u>: Let $A,B,C \in K(w,w^{-1})$, and $D = A(BC)-(AB)C$. It is required to show that $D = 0$.

It may be assumed that $A = \sum_{i=-\infty}^{n} a_i w^i$, $B = \sum_{i=-\infty}^{n} b_i w^i$, and $C = \sum_{i=-\infty}^{n} c_i w^i$, for $a_i, b_i, c_i \in K$, where one can without loss of generality assume identity of ranges of summation (by including zero terms if necessary).

Let k be a variable integer less than n. In terms of any given value of k, let:

$A_0 = \sum_{i=-\infty}^{k-1} a_i w^i$, $B_0 = \sum_{i=-\infty}^{k-1} b_i w^i$, $C_0 = \sum_{i=-\infty}^{k-1} c_i w^i$,

$A_1 = \sum_{i=k}^{n} a_i w^i$, $B_1 = \sum_{i=k}^{n} b_i w^i$, and $C_1 = \sum_{i=k}^{n} c_i w^i$.

Then $A = A_0+A_1$, $B = B_0+B_1$, and $C = C_0+C_1$.

It follows that $D = A(BC)-(AB)C$

$= (A_0+A_1)((B_0+B_1)(C_0+C_1)) - ((A_0+A_1)(B_0+B_1))(C_0+C_1)$.

By Lemma 2 (that degrees add), it follows that

$D = A_1(B_1C_1)-(A_1B_1)C_1+\ldots$terms in degrees less than $2n+k$.

But since A_1, B_1, and C_1 are finite sums, it follows from Lemma 8 that $A_1(B_1C_1) = (A_1B_1)C_1$. Hence Deg $D < 2n+k$, or $d = 0$.

As k approaches $-\infty$, $2n+k$ approaches $-\infty$. Hence D, if not zero, is of degree less than any integer. Since this is impossible, one can only conclude that $D = 0$ and hence that $A(BC) = (AB)C$.

4.4 Divisibility in $K(w,w^{-1})$.

The following theorem shows that $K(w,w^{-1})$ is a division ring, and thus satisfies the conditions for an embedding ring as stated in Section 4.1. It will be noted that, with the exception to be noted below, it is henceforth assumed that K is (generally) nonassociative.

Theorem 11: For any nonzero $u \in K(w,w^{-1})$ and arbitrary $v \in K(w,w^{-1})$, there is exactly one $x \in K(w,w^{-1})$ such that $ux = v$, and exactly one $y \in K(w,w^{-1})$ such that $yu = v$.

Proof: The equation $ux = v$ is considered here; the equation $yu = v$ and the corresponding proof of the existence and uniqueness of the element y are analogous. Let

$u = \sum_{i=-\infty}^{m} a_i w^i$ with $a_m \neq 0$ and $v = \sum_{i=-\infty}^{n} b_i w^i$ $(a_i, b_i \in K)$.
Because K is a division ring and $a_m \neq 0$, there is an element $c_{n-m} \in K$ such that $a_m c_{n-m} = b_n$. Let $Q_0 = c_{n-m} w^{n-m}$.
Then $uQ_0 = (a_m w^m)(c_{n-m} w^{n-m}) + B$ and $(a_m w^m)(c_{n-m} w^{n-m}) = b_n w^n + C$ where B and C are either zero or of degrees less than m.

If $v = v_0$, one now sees that $v_0 - uQ_0 = v_1$, where $v_1 = \sum_{i=-\infty}^{n-1} s_i w^i$ for appropriate $s_i \in K$ (some or all of the s_i possibly zero).

In general, however, by defining analogous quantities $Q_1, Q_2, \ldots,$ and $v_2, v_3, \ldots,$ one obtains successively:

$$v_0 = uQ_0 + v_1.$$

$$v_1 = uQ_1 + v_2.$$

$$v_2 = uQ_2 + v_3.$$

....

$$v_i = uQ_i + v_{i+1}$$

....

where, if the (n-i)th term of v_i be denoted by $t_{n-i} w^{n-i}$ (all the terms in higher powers of w being zero), $Q_i = c_{n-m-i} w^{n-m-i}$ and $a_m c_{m-n-i} = t_{n-i}$. (Each $v_i = \sum_{j=-\infty}^{n-i} t_j w^j$ for appropriate $t_j \in K$ where t_{n-i} may be zero.)

Let $x = \sum_{i=0}^{\infty} c_{n-m-i} w^{n-m-i} = \sum_{j=-\infty}^{n-m} c_j w^j$ where $j = n-m-i$.
One now shows that $ux = v$ by showing that, for all $h \leq n$, the term in w^h of ux is equal to the term in w^h of v.

The term in w^h of ux is equal, by Lemma 1, Section 4.3, to the term in w^h of $u(\sum_{j=h-m}^{n-m} c_j w^j) = u\sum_{i=0}^{n-h} c_{n-m-i} w^{n-m-i})$

$= u(\sum_{i=0}^{n-h} Q_i) = u(Q_0+\ldots+Q_{n-h}) = uQ_0+\ldots+uQ_{n-h}$

$= (v_0-v_1)+(v_1-v_2)+\ldots+(v_{n-h}-v_{n-h+1}) = v-v_{n-h+1}$.

But $v_{n-h+1} = \sum_{k=-\infty}^{n-(n-h+1)} t_k w^k = \sum_{k=-\infty}^{h-1} t_k w^k$ for appropriate $t_k \in K$, and it is clear that this sum does not contribute any term in w^h. Hence the term in w^h of ux is equal to the term in w^h of v as asserted. It remains to show the uniqueness of this right quotient x.

If this right quotient were not unique, then there would exist elements x and y such that $ux = uy$ and $x \neq y$; and hence, because $u(x-y) = 0$, u and $x-y$ would be zero divisors. It suffices, therefore, to show that $K(w,w^{-1})$ can contain no divisors of zero. But this follows from Lemma 2 of Section 4.3 above: if $u,v \in K(w,w^{-1})$, $u \neq 0$, and $v \neq 0$, then Deg uv is defined and hence $uv \neq 0$.

For the remainder of this section, the basic ring K is assumed to be associative. Ore [16] indicates an embedding of certain types of noncommutative integral domains in division rings. As applied in his paper [17] to his ring K(w) of noncommutative polynomials, this results in an embedding division ring R. It will be shown here that R can be isomorphically embedded in the ring $K(w,w^{-1})$ constructed above, as understood for an associative ring K.

In his paper [17], Ore shows that, given any nonzero elements $q,r \in K(w)$, there exist nonzero $s,t \in K(w)$ such that $qs = rt$. As an application of this general principle, and given nonzero $v, v_1 \varepsilon K(w)$ and (possibly zero) $u_1 \varepsilon K(w)$, the existence of nonzero $V, V_1, Y \varepsilon K(w)$ and $X \varepsilon K(w)$ such that $vV_1 = v_1V$ and $vX = u_1Y$ will be assumed throughout the following discussion (X will be zero if $u_1 = 0$).

The <u>elements</u> of R are equivalence classes $[u,v]$ of ordered pairs (u,v) for $u,v \varepsilon K(w)$, $v \neq 0$. As a result of Ore's construction, the following rules apply:

<u>Equality</u>: $[u,v] = [u_1,v_1]$ if and only if $uV_1 = u_1V$.

<u>Addition</u>: $[u,v] + [u_1,v_1] = [uV_1+u_1V, vV_1]$.

<u>Multiplication</u>: $[u,v][u_1,v_1] = [uX, v_1Y]$.

(It is not necessary to treat the operation of derivation separately, the derivation being inner in the case under discussion and therefore expressible in terms of the other operations - as discussed in Chapter 1.)

The basic ring K is isomorphically embedded in R by the correspondence $u \rightarrow [u,1]$.

Let S be the subset of $K(w,w^{-1})$ consisting of all products of the form uv^{-1} for $u,v \varepsilon K(w)$, $v \neq 0$. Then $\{S;+,\cdot\}$ is a ring, isomorphic to the ring R, this isomorphism being given by $[u,v] \leftrightarrow uv^{-1}$.

It is first shown that this correspondence is one to one. That it is also an isomorphism will follow from the homomorphism properties shown below.

Let $[u,v] = [u_1,v_1]$. Then $uV_1 = u_1V$, $uV_1(vV_1)^{-1}$ $= u_1V(vV_1)^{-1} = u_1V(v_1V)^{-1}$, $uV_1V_1v^{-1} = u_1VV^{-1}v_1^{-1}$, and so

$uv^{-1} = u_1v_1^{-1}$. Conversely, let $uv^{-1} = u_1v_1^{-1}$. Then $uV_1V_1^{-1}v^{-1} = u_1VV^{-1}v_1^{-1}$, $uV_1(vV_1)^{-1} = u_1V(vV_1)^{-1}$, $uV_1 = u_1V$, and $[u,v] = [u_1,v_1]$.

It remains to show that:

(1) $uv^{-1}+u_1v_1^{-1} = (uV_1+u_1V)(vV_1)^{-1}$, and

(2) $(uv^{-1})(u_1v_1^{-1}) = (uX)(v_1Y)^{-1}$,

and the isomorphism (and the fact that S is a ring) will be established.

But $uv^{-1}+u_1v_1^{-1} = uV_1V_1^{-1}v^{-1}+u_1VV^{-1}v_1^{-1}$

$= uV_1(vV_1)^{-1}+u_1V(v_1V)^{-1} = uV_1(v_1V)^{-1}+u_1V(v_1V)^{-1}$

$= (uV_1+u_1V)(v_1V)^{-1} = (uV_1+u_1V)(vV_1)^{-1}$ as asserted. Also $(uv^{-1})(u_1v_1^{-1})v_1Y = uv^{-1}u_1Y = uv^{-1}vX = uX$, hence $(uv^{-1})(u_1v_1^{-1}) = (uX)(v_1Y)^{-1}$ as asserted.

It is easy to see, however, that the cardinality of $K(w,w^{-1})$ is larger than that of R. For $K(w,w^{-1})$ consists of infinite sums, whereas R consists only of equivalence classes of ordered pairs of $K(w)$. Therefore, the (to within isomorphism) embedding of R in $K(w,w^{-1})$ is proper.

This same cardinality argument shows that $K(w,w^{-1})$, even in the case of a nonassociative K, is not the smallest division ring extension of K. It is easy to give an inductive definition of this smallest division ring D (basically, one postulates that, for all $u,v \in D$, $u+v$, $u-v$, uv, and left and right quotients of u by v also belong to D), and it is seen that the cardinality of D is that of K.

CHAPTER 5

APPLICATIONS TO LINEAR DIFFERENTIAL EQUATIONS

5.1 Construction of a Factor Module.

The following lemma is, in effect, a translation of Theorem 11 from the language of the ring $K(w,w^{-1})$ and its ring operations to the language of the module M and the mappings defined upon it.

Lemma 1: For any nonzero $v \in K(w,w^{-1})$ and any $t \in M$, there is exactly one $s \in M$ such that $v(s) = t$.

Proof: Let $t = \sum_{i=-\infty}^{n} b_i z^{(i)}$ and $p = \sum_{i=-\infty}^{n} b_i w^i$ for $b_i \in K$. Then $t = p(z)$. By Theorem 11, there exists $k \in K(w,w^{-1})$ such that $vk = p$, and by the definition of multiplication in $K(w,w^{-1})$, $v(k(z)) = p(z)$. Let $s = k(z)$. Then $v(s) = p(z) = t$, and the existence of s has been established. It remains to show that this element is unique.

If now there is also $y \in M$ such that $v(y) = t$, let $y = \sum_{i=-\infty}^{m} a_i z^{(i)}$ and $q = \sum_{i=-\infty}^{m} a_i w^i$ for $a_i \in K$. Then $v(y) = v(q(z)) = t = p(z)$, $vq = p = vk$, and hence, by Theorem 11, $q = k$. Then $y = q(z) = k(z) = s$, and uniqueness has been established.

An application to linear differential equations in K of the above lemma will be made later in this chapter. As a preliminary to this investigation, a factor module M* will be constructed. An operation of multiplication will be defined so that M* will have the structure of a differential ring. It will then be seen that linear differential equations in the basic ring K will have solutions in the extension M*.

One considers M as a K(w) module rather than merely as a K module. As shown in Chapter 2, u(m) is a (unique) element of M for any $m \in M$ and $u \in K(w)$, and M satisfies the conditions for a left (nonassociative) K(w) module.

Let H be the subset of M consisting of the elements $\sum_{i=1}^{n} a_i z^{(i)}$ for arbitrary $n > 0$ and $a_i \in K$. It is clear from the definitions given in Chapter 2 that H is closed under the operation of addition and (since the application of the operator w does not add terms of lower degree) the mappings by K(w), and is thus a sub-K(w)-module of M.

The symbol M* is used to denote the factor module M-H. The elements of M* are the cosets m+H for $m \in M$. The following rules are the usual ones associated with a factor module: For $s,t \in M$, $u \in K(w)$, $(s+H)+(t+H) = (s+t)+H$ and $u(s+H) = u(s)+H$. As for derivation, $w(s+H) = w(s)+H = s'+H$, so that one conveniently extendes the earlier terminology, referring to w(s+H) as the M*-derivative of s+H and writing $w(s+H) = (s+H)'$.

There is a natural homomorphism h which maps each $m \in M$ to the corresponding $h(m) = m+H \in M^*$, where, for all $s,t \in M$ and $u \in K(w)$, it follows (from the above rules) that $h(s+t) = h(s)+h(t)$ and $h(u(s)) = u(h(s))$. The symbol

$r^{(i)}$ is used to denote the coset $z^{(i)}+H = h(z^{(i)})$ for any integer i, where it is clear that $r^{(i)}$ is the zero coset H for all $i > 0$. In particular $h(z) = h(z^{(0)}) = r^{(0)} = r$, $h(z^{(i)}) = r^{(i)}$, and, for finite sums generally,

$$h(\sum_{i=t}^{n} a_i z^{(i)}) = \sum_{i=t}^{n} a_i r^{(i)} \quad (= \sum_{i=t}^{0} a_i r^{(i)} \text{ if } n \geq 0).$$ Now

$$h(\sum_{i=-\infty}^{n} a_i z^{(i)}) = \sum_{i=-\infty}^{n} a_i z^{(i)})+H \quad (= \sum_{i=-\infty}^{0} a_i z^{(i)}+H \text{ if } n \geq 0),$$

and one makes the following formal definition:

$$\sum_{i=-\infty}^{0} (a_i z^{(i)}+H) = (\sum_{i=-\infty}^{0} a_i z^{(i)})+H.$$

Hence, in view of the definition of $r^{(i)}$,

$$h(\sum_{i=-\infty}^{0} a_i z^{(i)}) = \sum_{i=-\infty}^{0} a_i r^{(i)}.$$

The following properties follow readily from the corresponding properties of M (as given in Chapter 2) and the fact that h is a module homomorphism; together, these properties completely characterize the module M*. Let $a_i, b_i, c, e_i \in K$:

1. $\sum_{i=-\infty}^{0} a_i r^{(i)} = \sum_{i=-\infty}^{0} b_i r^{(i)}$ if and only if, for each i, $a_i = b_i$.

   (Elements of M are in the kernel H if and only if their homomorphic images are equal.)

2. $\sum_{i=-\infty}^{0} a_i r^{(i)} + \sum_{i=-\infty}^{0} b_i r^{(i)} = \sum_{i=-\infty}^{0} (a_i+b_i) r^{(i)}$.

3. $c(\sum_{i=-\infty}^{0} a_i r^{(i)}) = \sum_{i=-\infty}^{0} ca_i r^{(i)}$.

4. $w(\sum_{i=-\infty}^{0} e_i r^{(i)}) = \sum_{i=-\infty}^{0} (e_{i-1}+e_i')r^{(i)}$.

In computations, the element $r \varepsilon M^*$ is handled in the same manner as the element $z \varepsilon M$ from which it is mapped, except that $r^{(i)} = 0$ for all $i > 0$.

Lemma 2: For any nonzero $v \varepsilon K(w)$ and arbitrary $m \varepsilon M^*$, there exists $y \varepsilon M^*$ such that $v(y) = m$.

Proof: Let $m = h(t)$ for $t \varepsilon M$. By Lemma 1, there exists an $s \varepsilon M$ such that $v(s) = t$. Let $y = h(s)$. Then $v(y) = v(h(s)) = h(v(s)) = h(t) = m$, and the lemma has been established.

5.2 Differential Extensions of K.

The differential ring $K\{x\}$ is the ring of formal power series in a symbol x over K. The elements of this ring are the series $\sum_{i=0}^{\infty} a_i x^i$ for $a_i \varepsilon K$, and these series obey the following familiar rules for formal power series, together with (4) which defines derivation in the system. (See Kaplansky [7] for a similar, but somewhat different definition.)

1. $\sum_{i=0}^{\infty} a_i x^i = \sum_{i=0}^{\infty} b_i x^i$ if and only if, for each i, $a_i = b_i$.

2. $\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i+b_i)x^i$.

3. $(\sum_{i=0}^{\infty} a_i x^i)(\sum_{i=0}^{\infty} b_i x^i) = \sum_{i=0}^{\infty} \sum_{j+k=i} a_j b_k x^i$.

4. $$d\left(\sum_{i=0}^{\infty} a_i x^i\right) = \left(\sum_{i=0}^{\infty} a_i x^i\right)' = \sum_{i=0}^{\infty} ((i+1)a_{i+1}+a_i')x^i.$$

If all but a finite number of the coefficients a_i are zero, then $\sum_{i=0}^{\infty} a_i x^i$ reduces to a polynomial $\sum_{i=0}^{n} a_i x^i$ for some $n \geq 0$. In particular, $\sum_{i=0}^{0} a_i x^i = a_0 x^0 = a_0 \in K$, and, as a special case of (3), $c\left(\sum_{i=0}^{\infty} a_i x^i\right) = \sum_{i=0}^{\infty} ca_i x^i$ for $c \in K$. It will be noted from (4) that, for any $n \geq 0$ and $a \in K$, $d(x^n) = nx^{n-1}$.

That $\{K\{x\};+,.\}$ is a ring follows from the usual proof given in analysis texts. It must be shown that the mapping d is a derivation, and $K\{x\}$ will then be seen to be a differential ring extension of K. The sum law for derivatives is clear from the definition given, and the product law is derived in the following lemma:

Lemma 3: For all $u,v \in K\{x\}$, $(uv)' = u'v+uv'$.

Proof: Let $u = \sum_{i=0}^{\infty} a_i x^i$ and $v = \sum_{i=0}^{\infty} b_i x^i$ for $a_i, b_i \in K$. Then

$$uv = \sum_{i=0}^{\infty} \sum_{j+k=i} a_j b_k x^i = \sum_{i=0}^{\infty} c_i x^i \text{ where } c_i = \sum_{j+k=i} a_j b_k \text{ and}$$

$$c_{i+1} = \sum_{j+k=i+1} a_j b_k = \sum_{s+t=i+1} a_s b_t.$$

As a result of (4), the term of $(uv)'$ in x^i is

$$(i+1)c_{i+1}x^i + c_i'x^i = \sum_{s+t=i+1} (i+1)a_s b_t x^i + \sum_{j+k=i} (a_j b_k)'x^i$$

$$= \sum_{s+t=i+1} (s+t)a_s b_t x^i + \sum_{j+k=i} (a_j' b_k + a_j b_k')x^i$$

$$= \sum_{s+t=i+1} s a_s b_t x^i + \sum_{s+t=i+1} t a_s b_t x^i + \sum_{j+k=i} (a_j' b_k + a_j b_k')x^i$$

$$= \sum_{\substack{1 \leq s \leq i+1 \\ 0 \leq t \leq i \\ s+t=i+1}} s a_s b_t x^i + \sum_{\substack{1 \leq t \leq i+1 \\ 0 \leq s \leq i \\ s+t=i+1}} t a_s b_t x^i + \sum_{j+k=i} (a_j' b_k + a_j b_k') x^i$$

Now let $s = j+1$, $t = k$ in the first summation, and let $s = j$, $t = k+1$ in the second summation. Then the term in x^i of $(uv)'$ equals (summing over j,k such that $j+k = i$).

$$\sum((j+1)a_{j+1}b_k+(k+1)a_j b_{k+1}+a_j' b_k+a_j b_k')x^i$$

$$= \sum((j+1)a_{j+1}+a_j')b_k x^i+\sum a_j((k+1)b_{k+1}+b_k')x^i.$$

Hence, by (3) and (4) above,

$$(uv)' = (\sum_{i=0}^{\infty}((i+1)a_{i+1}+a_i')x^i)(\sum_{i=0}^{\infty}b_i x^i)$$

$$+ (\sum_{i=0}^{\infty}a_i x^i)(\sum_{i=0}^{\infty}((i+1)b_{i+1}+b_i')x^i) = u'v+uv' \text{ as asserted.}$$

It will be shown in Lemma 3 below that $K\{x\}$ and M^* have the same structure as $K(w)$-modules. For the purpose of exhibiting an isomorphism between $K\{x\}$ and M^*, the following symbolism will be used:

For arbitrary $i \leq 0$, let the symbol y_i denote $(1/(-i)!)x^{-i}$.

It is clear that, for $e_i \in K$, $\sum_{i=-\infty}^{0} e_i y_i$ denotes an arbitrary element of $K\{x\}$. Let $j = -i$, and, for all $k \geq 0$, let $a_k = (1/k!)e_{-k}$. Then $d(\sum_{i=-\infty}^{0} e_i y_i) = d\sum_{i=-\infty}^{0} e_i(1/(-i)!)x^{-i})$

$$= d(\sum_{j=0}^{\infty} e_{-j}(1/j!)x^j) = d(\sum_{j=0}^{\infty} a_j x^j) = \sum_{j=0}^{\infty}((j+1)a_{j+1}+a_j')x^j$$

$$= \sum_{j=0}^{\infty}((j+1)(1/(j+1)!)e_{-j-1}+((1/j!)e_{-j}'))x^j$$

$$= \sum_{j=0}^{\infty} (1/j!)(e_{-j-1}+e'_{-j})x^j = \sum_{i=-\infty}^{0} (e_{i-1}+e_i')(1/(-i)!x^{-i}$$

$$= \sum_{i=-\infty}^{0} (e_{i-1}+e_i')y_i .$$

If one now writes $w(u) = d(u) = u'$ for $u \in K\{x\}$, it is clear that $K\{x\}$ is a $K(w)$-module under the rule:

$$(\sum_{i=0}^{n} a_i w^i)(u) = \sum_{i=0}^{n} a_i u^{(i)} .$$

Lemma 4: M^* and $K\{x\}$ are isomorphic as $K(w)$-modules, where the M^*-derivation w of M^* corresponds to the derivation d of $K\{x\}$. This isomorphism ϕ is given by:

$$\phi(\sum_{i=-\infty}^{0} a_i r^{(i)}) = \sum_{i=-\infty}^{0} a_i y_i \text{ for } a_i \in K.$$

Proof: The defining properties of the two systems M^* and $K\{x\}$, as $K(w)$ modules, are the same. In particular, as the above computation shows,

$$d(\sum_{i=-\infty}^{0} e_i y_i) = \sum_{i=-\infty}^{0} (e_{i-1}+e_i')y_i \longleftrightarrow \sum_{i=-\infty}^{0} (e_{i-1}+e_i')r^{(i)}$$

$$= w(\sum_{i=-\infty}^{0} e_i r^{(i)}, \text{ as required for this isomorphism.}$$

One defines multiplication in M^* by the rule: $km = \phi^{-1}(\phi(k)\phi(m))$ for $k,m \in M^*$. Hence $\phi(uv) = \phi(u)\phi(v)$, and it is clear that this rule of multiplication renders M^* and $K\{x\}$ isomorphic as rings. Henceforth, M^* and $K\{x\}$ are identified, and $r^{(i)} = (1/(-i)!)x^{-i}$ for $i \leq 0$ gives the relation between the derivatives of r and the powers of x. This common system will be denoted by M^*. Since M^* is now a ring and not merely a module, every M^*-derivative is now a general (ring) derivative. In effect, M* has been given the structure of a ring by means of defining an operation of multiplication for which the M*-derivation, already defined in M*, satisfies the product law for derivatives.

It is now possible to give an application (to linear differential equations in the basic ring K) of the corollary to Theorem 11 (in the form given in Lemma 1 above).

<u>Lemma 5</u>: For any integer n and any $a_i, b \in K$ such that $a_n \neq 0$, there exists $y \in M^*$ such that $\sum_{i=0}^{n} a_i y^{(i)} = b$.

<u>Proof</u>: By Lemma 2, there exists $y \in M^*$ such that $\sum_{i=0}^{n} a_i w^i(y) = b$ (recalling that K is a subring of $M^* = K\{x\}$, and hence that $b \in M^*$). Since w is the operation of derivation in M*, $\sum_{i=0}^{n} a_i w^i(y) = \sum_{i=0}^{n} a_i y^{(i)} = b$ as asserted.

Lemma 5 asserts that any linear differential equation in K has a solution in the ring extension M*. Results that have some resemblance to that of this lemma (such as Liouville and Picard-Vessiot extensions of differential fields) have been studied by Kolchin [8, 9, 10] and Ritt [21]. These earlier field extensions, however, are more like classical algebraic extension fields and not as general as the solution ring considered here.

It is now desired to improve on the result of Lemma 5 by extending the division ring K to a division ring T in which <u>every</u> linear differential equation in T has a solution <u>in T</u>, without the necessity of having to extend T to a larger system.

The ring $M^* = K\{x\}$ is extended to the ring $K\{x,x^{-1}\}$, the elements of which are the sums $\sum_{i=n}^{\infty} a_i x^i$ for $a_i \varepsilon K$ and n an arbitrary integer (possibly negative). This ring is the formal analogue of the usual field of formal power series, except that assumptions of commutativity and associativity are no longer made, with the following rules:

1. $\sum_{i=n}^{\infty} a_i x^i = \sum_{i=n}^{\infty} b_i x^i$ if and only if, for each i, $a_i = b_i$.

2. $\sum_{i=n}^{\infty} a_i x^i + \sum_{i=n}^{\infty} b_i x^i = \sum_{i=n}^{\infty} (a_i + b_i) x^i$.

3. $(\sum_{i=n}^{\infty} a_i x^i)(\sum_{i=n}^{\infty} b_i x^i) = \sum_{i=2n}^{\infty} \sum_{j+k=i} a_j b_k x^i$.

4. $d(\sum_{i=n}^{\infty} a_i x^i) = (\sum_{i=n}^{\infty} a_i x^i)' = \sum_{i=n}^{\infty} ((i+1)a_{i+1} + a_i') x^i$.

That d is a derivation follows from the proof of Lemma 3 (as suitably modified for the more general lower limits of summation).

That $K\{x,x^{-1}\}$ is a division ring follows from repeating the proof of Theorem 11 for the ring $K(w,w^{-1})$, with the element x playing the role of the element w^{-1} and the element x^{-1} that of w in the earlier proof. Thus one lets the u of the earlier proof be here the element $\sum_{i=-\infty}^{m} a_i x^{-i}$ and v be the element $\sum_{i=-\infty}^{n} b_i x^{-i}$.

Lemma 6: The basic ring K may be extended to a division ring K_1 in which every linear differential equation in K has a solution in K_1.

Proof: This follows from Lemma 5 and the above construction of $K\{x,x^{-1}\}$, where $K_1 = K\{x,x^{-1}\}$ includes the structure M^* of the lemma.

Let $x_1, x_2, x_3, \ldots$ be an infinite sequence of algebraically independent variables over K. Define the sequence of division rings $K_0, K_1, K_2, \ldots$ by repeated applications of Lemma 6, where $K_{i+1} = K_i\{x_{i+1},x_{i+1}^{-1}\}$. Then every linear differential equation in K_i has a solution in K_{i+1} $(i = 1,2,3,\ldots)$, and $K_0 = K$. Let $T = \bigcup_i K_i$. Then T is a differential ring since it is the "direct limit" of a sequence of differential rings (ref Gratzer [3]).

Theorem 12: The ring T satisfies the following properties:

1. T is a differential division ring.
2. K is a differential subring of T.
3. Every linear differential equation in T (of the form $\sum_{i=0}^{n} a_i y^{(i)} = b$ for $a_i, b \in T$, $a_n \neq 0$) has a solution $y \in T$.

Proof: Any equation of the form $ax = b$ or $ya = b$, with $a,b \in T$, has a solution in T because there exists a division ring $K \subset T$, with minimal j, that contains a,b. Hence T is a division ring and (1) is proved. Since $K = K_0$, it is trivial that K is a (differential) subring of T as asserted in (2). In order to establish (3), consider an arbitrary equation $\sum_{i=0}^{n} a_i y^{(i)} = b$ for $a_i, b \in T$, $a_n \neq 0$. It must be shown that there exists a solution $y \in T$, and for this purpose it will suffice to show that, for some j, this equation has a solution in K_j. Consider the set of the coefficients $\{a_0,\ldots,a_n,b\}$ of this equation. Since the K_i are nested, it is clear that one can find an upper bound t such that $a_0,\ldots,a_n,b \in K_t$. It is now seen that this equation is in the ring K_t, and therefore has a solution $y \in K_{t+1}$. The proof is now completed by letting $j = t+1$.

REFERENCES

1. Amitsur, S.A., Derivations in Simple Algebras, Proc London Math Soc (3) 7 (1957), 87-112.

2. Cohn, P.M., On a Generalization of the Euclidean Algorithm, Proc Cambridge Phil Soc 57 (1961), 18-30.

3. Gratzer, G., Universal Algebra, D. Van Nostrand Co. (1968), 128-139.

4. Jacobson, N., Pseudo-Linear Transformations, Ann of Math 38 (1937), 484-507.

5. Jacobson, N., Derivation Algebras and Multiplication Algebras of Semi-simple Jordan Algebras, Ann of Math (2) 50 (1949), 866-874.

6. Jacobson, N., Lectures in Abstract Algebra, D. Van Nostrand Co. vol 3 (1964), 168.

7. Kaplansky, I., An Introduction to Differential Algebra, Publications de L'Institut de Mathematique de L'Universite de Nancago (1957).

8. Kolchin, E.R., Extensions of Differential Fields, Ann of Math 45 (1942), 724-729.

9. Kolchin, E.R., Algebraic Matrix Groups and the Picard-Vessiot Theory of Homogeneous Linear Ordinary Differential Equations, Ann of Math 49 (1948), 1-42.

10. Kolchin, E.R., Existence Theorems connectdd with the Picard-Vessiot Theory of Homogeneous Linear Ordinary Differential Equations, Bull Amer Math Soc 54 (1948), 927-932.

11. Kolchin, E.R., On Certain Concepts in the Theory of Algebraic Matrix Groups, Ann of Math 49 (1948), 774-789.

12. Kolchin, E.R., Picard-Vessiot Theory of Partial Differential Fields, Proc Amer Math Soc 3 (1952), 596-603.

13. Kolchin, E.R., Galois Theory of Differential Fields, Amer J. of Math 75 (1953), 753-824.

14. Kolchin, E.R., On the Galois Theory of Differential Fields, Amer J. of Math 77 (1955), 868-894.

15. Kurosh. A.G., General Algebra, Chelsea Pub. Co. (1963), 254.

16. Ore, O., Linear Equations in Noncommutative Fields, Ann of Math 32 (1931), 463-477.

17. Ore, O., Theory of Noncommutative Polynomials, Ann of Math 34 (1933), 480-508.

18. Qureshi, R., Extensions of a Ring, J. Natur Sci and Math 7 (1967), 71-83.

19. Qureshi, R., On Noncommutative Polynomial Rings, J. Natur Sci and Math 9 (1969), 249-257.

20. Ritt, J.F., Differential Equations from the Algebraic Standpoint, Amer Math Soc Coll Pub 14 (1932).

21. Ritt, J.F., Differential Algebra, Amer Math Soc Coll Pub 33 (1950).

22. Robinson, A., Local Differential Algebra, Trans Amer Math Soc 97 (1960), 427-456.

23. Robinson A. and Halfin, S., Local Partial Differential Algebra, Trans Amer Math Soc 109 (1963), 165-180.

24. Schafer, R.D., Inner Derivations of Nonassociative Algebras, Bull Amer Math Soc 55 (1949), 769-776.

25. Seidenberg, A., Derivations and Integral Closure, Pacific J. Math 16 (1966), 167-173.

26. Smits, T.H.M., Skew Polynomial Rings and Nilpotent Derivations, Utigerevij Waltman Delft (1967), Chapter 1.

27. Smits, T.H.M., Skew Polynomial Rings, Indag Math 30 (1968), 209-224.