On Properties of Differential Rings

MICHAEL GR. VOSKOGLOU
Mathematical Sciences, School of Technological Applications
Graduate T. E.I. of Western Greece
Meg. Alexandrou 1 – 263 34 Patras
GREUCE
mvosk@hol.gr ; http://eclass.teipat.gr/eclass/courses/523102

Abstract: - Properties are studied in this work of a differential ring R, its ideals and the ideals of iterated skew polynomial rings over R defined with respect to a finite set of commuting derivations of R. In particular, it is shown that, if P is a prime d-ideal of a commutative ring R for some derivation d of R, then the ring $d^{-1}(P)$ is integrally closed in R, while if R is a local ring and its maximal ideal M is not invariant under d, then $M^2 + d(M^2) = M$. Also the concept of the integration of R associated to a given derivation of R is introduced, the conditions under which this integration becomes a derivation of R are obtained and some consequences are derived in the form of two corollaries. The new concept of integration of R generalizes basic features of the indefinite integrals.

Key-Words: - Derivations, Integrations associated to derivations, Differential ideals, Iterated skew polynomial rings (ISPRs).

1 Introduction

All the rings considered in this paper are with identity. A derivation on a ring is a function which generalizes certain features of the traditional derivative operator. A differential ring is understood to be a ring with a non empty set D of derivations attached to it (e.g. see [1, 2, 3]). On the other hand the term integration is connected to the computation of an integral.

In the present work properties are studied of the differential ideals of a ring R and of the iterated skew polynomial rings over R defined with respect to a finite set of commuting derivations of R. The concept of the integration of R associated to a given derivation of R is also introduced and some fundamental properties of it are studied. This new concept generalizes basic features of the indefinite integrals.

The rest of the paper is organized as follows: Section 2 contains information about derivations and the differential simplicity of a ring which is necessary for the good understanding of the article’s contents. The main results are presented in Section 3 and the paper closes with the conclusions and some hints for future research, which are contained in Section 4.

2. Differential Rings

We start by recalling the following definitions:

2.1 Definition: Let R be a ring. Then a map $d: R \rightarrow R$ is called a derivation of R, if and only if, $d(x + y) = d(x) + d(y)$ and $d(xy) = xd(y) + d(x)y$, for all $x, y \in R$.

2.2 Definition: Let R be a ring and let d be a derivation of R. Then an ideal I of R is said to be a d-ideal if $d(I) \subseteq I$. If the only d-ideals of R are 0 and R, then R is called a d-simple ring and d is called a simple derivation of R.

2.3 Proposition: Let d be a simple derivation of a ring R. Then:

(i) $R^2 = R$.

(ii) $F = C(R) \cap \ker(d)$ is a field, where $C(R)$ denotes the centre of R and $\ker(d)$ denotes the kernel of d.

Proof: (i) $R^2 = R$.

(ii) Observe that $d(1) = d(1) + 2d(1)$. Therefore $d(1) = 0$, i.e. 1 is in F. Also, given $s \in F$ is $d(sR) = sd(R) \subseteq sR$. Therefore, sR is a non zero d-ideal of R, which implies that sR = R. Thus, there exists $r \in R$ such that $sr = rs=1$. Then $d(sr) = sd(r) = 0 \implies rsd(r) = 0 \implies d(r) = 0$. Assume now that there exists $t \in R$ such that $tr \neq rt$. Then $s(tr)s \neq s(rt)s$, or...
st ≠ ts, which is absurd since s is in C(R). Therefore r is in F, i.e. s has an inverse in F. The rest of the proof is straightforward.

Due to Proposition 2.3 (i) many authors add the condition R ≠ R in Definition 2.2 of a d- simple ring. Also, as a consequence of Proposition 2.3(ii), every d-simple ring is either of characteristic zero or of a prime number p.

Non commutative d-simple rings exist in abundance; for example every simple ring is d-simple for any derivation d of R.

For the case of a commutative ring of prime characteristic we have the following result:

**2.4 Theorem:** Let R be a ring of prime characteristic p, and let d be a simple derivation of R. Then R is a 0-dimensional ring with a unique maximal ideal (quasi-local ring).

**Proof:** Let M be a maximal ideal of R and let I be the ideal of R generated by the set \{m^p : m ∈ M\}. Then, since R is of characteristic p, I is a proper D-ideal of R, therefore the d-simplicity of R implies that I = (0). Thus M is contained in the nil radical, say N, of R (i.e. the set of all nilpotent elements of R) and therefore M=N. Let now P be a prime ideal of R contained in M. Then, since M is equal to the intersection of all prime ideals of R ([4], Proposition 1.8) and M=N, we get that M=P. Thus N is the unique prime ideal of R and this proves the theorem.

As a consequence of the above theorem, if R is a domain, then R is a field (since M=N=(0)) and therefore the interest is turned mainly to commutative rings of characteristic zero.

In this case there is not known any general criterion under which one can decide whether or not a commutative ring possesses simple derivations, unless if R is a 1-dimensional algebra (Krull dimension) over a field k. Then, if R = k[y_1, y_2, ..., y_n] and d is a derivation of R such that d(c) = 0 of all c in k (k-derivation of R), R is d-simple if, and only if, R = (d(y_1), d(y_2), ..., d(y_n)) ([5], Theorem 2.4).

Typical examples of d-simple rings of characteristic zero are the polynomial rings in finitely many variables over a field [6] and the regular local rings of finitely generated type over a field [7]. More examples of d-simple rings of characteristic zero can be found in [6], while in [8] geometric examples are presented of smooth varieties (algebraic sets) over a field with coordinate rings possessing simple derivations.

In case of characteristic zero it is well known that if a commutative ring R is d-simple then R is an integral domain and also that if R has no non zero prime d-ideals, then R is a d-simple ring ([9], Corollary 1.5)

Definition 2.2 can be generalized for a finite set D of derivations of R as follows:

**2.5 Definition:** Let D be a finite set of derivations of R. Then an ideal I of R is called a D-ideal if d(I) ⊆ I for all d in D and R is called a D-simple ring, if it has no proper non zero D-ideals.

Obviously, if R is a d-simple ring for some d in D, then R is also a D-simple ring, but the converse is not true. For example, let S = R[x, y, z] be a polynomial ring over the field R of the real numbers and let d_1 and d_2 be the R-derivations of S defined by d_1: (x, y, z) → (y+z, z-x, -x-y) and d_2: (x, y, z) → (y+2z, xyz-x, -xy+2x) respectively. Then, since d_i(x^2+y^2+z^2)=0 for i=1, 2, d_i induces an R-derivation of the coordinate ring S = \[ \frac{R[x, y, z]}{(x^2+y^2+z^2)} \]
of the real unit-sphere. Then S is a \{d_1, d_2\}-simple ring ([10], Lemma 3.1). However, it is well known that S admits no simple derivations ([7], Section 3, Remark 3).

Proposition 2.3 holds also for D-simple rings, where D is a non singleton set. In this case the field F = C(R) ∩ Ker (d). The proof is the same.

Next we study skew polynomial rings of derivation type in finitely many variables over a ring R We start with the following definition:

**2.6 Definition:** Let R be a ring and let d be a derivation of R. Define on the set S of all polynomials in one variable x over R addition in the usual way and multiplication by the rule: xr=rx+d(r), for all r in R, and the distributive law. It is well known then that S becomes a non commutative ring denoted by R[x, d] and called a skew polynomial ring (of derivation type) over R (e.g. [11], p.35).

Such rings, which are also known as Ore extensions, have been firstly introduced by O. Ore [12] to be used as counter examples.

**2.7 Example:** Let T[x_1] be a polynomial ring over a ring T, then the skew polynomial ring
\[ T[x_1][x_2, \frac{\partial}{\partial x_1}] \]
over T and it is denoted by A_1(T). It becomes evident that the elements of A_1(T) are polynomials in two variables x_1 and x_2 over T, while multiplication is defined by x_1 t = tx_1,
\[ x_2 t = tx_2 + \frac{\partial t}{\partial x_1} = tx_2 \text{ for all } t \in T, \ x_2 x_1 = x_1 x_2 \]
\[ + \frac{\partial x_i}{\partial x_j} = x_i x_{j+1} + 1 \text{ and by the distributive law.} \]

Note that skew polynomial rings can also be defined over \( R \) with respect to an endomorphism \( f \) of \( R \) and in a more general context with respect to \( f \) and an \( f \)-derivation \( d \) of \( R \) [11], which is a generalization of the concept of the ordinary derivation.

Skew polynomial rings (of derivation type) in finitely many variables over \( R \) can also be defined [11] as follows:

2.8 Definition: Let \( S_1 = R[x_1, d_1] \) be a skew polynomial ring over a ring \( R \), where \( d_1 \) is a derivation of \( R \). Then, if \( d_2 \) is a derivation of \( S_1 \), the skew polynomial ring \( S_2 = S_1[x_2, d_2] \) is called an \( \text{iterated skew polynomial ring (ISP) over } R \) and it is denoted by \( S_2 = R[x_1, d_1][x_2, d_2] \).

Applying induction on \( n \) one defines the ISP ring \( S_n = R[x_1, d_1][x_2, d_2] \ldots[x_n, d_n] \) in \( n \) variables over \( R \). In order to simplify our notation we shall denote this ring by \( S_n = R[x, D] \), with \( D = \{d_1, d_2, \ldots, d_n\} \).

ISP rings have been defined by Kishimoto [13] and others.

2.9 Examples: (i) The first Weyl algebra \( A_1(T) \) over a ring \( T \) (Example 2.7) is an ISP of derivation type in two variables over \( T \) of the form \( T[x_1, d_1] \).

(ii) Set \( R = A_1(T) \). Then the first Weyl algebra \( A_1(R) \) over \( R \) is called the \text{second Weyl algebra over } T \) and it is denoted by \( A_2(T) \). Obviously we have that
\[ A_2(T) = A_1[A_1(T)] = T[x_2, \frac{\partial}{\partial x_1}] \{x_1, \frac{\partial}{\partial x_2} \}. \]

(iii) Consider the set of all polynomials in \( n+1 \) variables, say \( x_1, x_2, \ldots, x_n, x_{n+1} \), over a ring \( T \). Then the \( n \)-th Weyl algebra \( A_n(T) \) over \( T \) is defined by induction on \( n \) as \( A_n(T) = A_1[A_{n-1}(T)] \). Obviously we have that
\[ A_n(T) = T[x_1][x_2, \frac{\partial}{\partial x_1}] \ldots[x_{n+1}, \frac{\partial}{\partial x_n}] = T[x, D], \text{ with } D = \{d, \frac{\partial}{\partial x_1}, \frac{\partial}{\partial x_2}, \ldots, \frac{\partial}{\partial x_n} \}, \text{ where } \]
\( d \) denotes the zero derivation of \( T \).

Next, given a finite set \( D \) of derivations of \( R \) commuting to each other, we shall construct an ISP of derivation type over \( R \) of the form \( R[x; D] \). For this, we need the following lemma:

2.10 Lemma: Let \( R \) be a ring, let \( d \) be a derivation of \( R \) and let \( S = R[x, d] \) be the corresponding skew polynomial ring over \( R \). Let also \( d^* \) be another derivation of \( R \). Then \( d^* \) can be extended to a derivation of \( S \) by \( d^*(x) = 0 \), if, and only if, \( d^* \) commutes with \( d \).

Proof: Obviously \( d^* \) extends to a derivation of \( S \), if, and only if, \( d^*(x) \) can be defined in a way compatible to multiplication in \( S \). In other words, if \( d^*(x) = 0 \), then for all \( r \in R \) we must have \( d^*(rx) = d^*(d(r)) \Rightarrow xd^*(r) + hr = rh + d^*(r)x + d^*(d(r)) \Rightarrow d^*(r)x + d[d^*(r)] + hr = rh + d^*(r)x + d^*(d(r)) \).

Therefore \( d^*(r)x + d[d^*(r)] + hr = rh \), which is true for \( h = 0 \).

Let now \( D = \{d_1, d_2, \ldots, d_n\} \) be a finite set of derivations of \( R \) commuting to each other; i.e. we have that \( d_i \circ d_j = d_j \circ d_i \), \( i, j = 1, 2, \ldots, n \). Consider the set \( S_n \) of all polynomials in \( n \) variables, \( x_1, x_2, \ldots, x_n \), and define addition in \( S_n \) in the usual way and multiplication by the rules \( x_i x_j = r_{ij}x_j + d_i(r) + d_j(r) + d_i o d_j(r) \).

For example, in the first Weyl algebra
A_{i}(T) = T[x_{1}, d][x_{2}, \frac{\partial}{\partial x_{1}}] \quad \text{(Example 2.9(i)) the zero derivation } d \text{ commutes with } \frac{\partial}{\partial x_{1}}, \text{ but } x_{1}x_{2} = x_{2}x_{1} + 1 \quad \text{(Example 2.7)}

The ISPRs, which had been initially defined on a completely theoretical basis, have recently found two important applications resulting to the renewal of the researchers’ interest about them. The former concerns the ascertainment that many Quantum Groups (i.e., Hopf algebras having in addition a structure analogous to that of a Lee group [16]), which are used as a basic tool in Theoretical Physics, can be expressed and studied in the form of an ISPR. The latter concerns the utilization of ISPRs in Cryptography for analyzing the structure of certain codes [17].

Voskoglou has also proved the following result [14]:

2.12 Theorem: Let R be a ring, let D = \{d_{1}, \ldots, d_{n}\} be a finite set of derivations of R commuting to each other and let S_{n}=R[X, D] be the corresponding ISPR over R. Assume further that d_{i} is an outer derivation of S_{i-1}, where S_{0} = R. Then S_{n} is a simple ring, if, and only if, R is a D-simple ring.

As an example, consider the polynomial ring R=k[y_{1}, y_{2}, \ldots, y_{n}] over a field k and the set D=\{\frac{\partial}{\partial y_{1}}, \ldots, \frac{\partial}{\partial y_{n}}\} of partial derivatives of R. Then it is straightforward to check that R is a D-simple ring ([18]; Example 1), therefore by the previous theorem the ISPR R[X, D] is a simple ring.

Theorem 2.12 for n=1 is due to D. Jordan [19].

The following definition generalizes the notion of a prime ideal of a ring:

2.13 Definition: Let R be a ring and let D be a finite set of derivations of R commuting to each other and let S_{n}=R[X, D] be the corresponding ISPR over R. Then:

- If P is a prime ideal of S_{n}, P \cap R is a D-prime ideal of R.

3. Main results

Let R be a commutative ring, let d be a derivation and let I be an ideal of R. Then it is straightforward to check that d^{-1}(I) = \{r \in R : d(r) \in I\} is a subring of R. We shall prove the following result:

3.1 Theorem: Let P be a prime d-ideal of R, then the ring d^{-1}(P) is integrally closed in R.

Proof: It suffices to show that, if r is an element of R integral over d^{-1}(P), then r is in d^{-1}(P).

In fact, since r is integral over d^{-1}(P), there exists a monic polynomial f(x) = x^{n}+a_{n-1}x^{n-1}+ \ldots +a_{1}x+a_{0} of minimal degree n with coefficients in d^{-1}(P), such that f(r) = r^{n}+a_{n-1}r^{n-1}+ \ldots +a_{1}r+a_{0} = 0. Differentiating this equation with respect to d one gets that

\[\frac{\partial}{\partial r}f(r) = n\cdot d(r)+a_{n-1}d(r)^{n-1}+ \ldots +a_{1}d(r) = 0,\]

or r_{0}d(r) = -[d(a_{n-1})r^{n-1}+ \ldots +d(a_{1})r],

with

\[r_{0}=nr^{n-1}+(n-1)a_{n-1}r^{n-2}+ \ldots +a_{1}\] (1).

But, since r_{0}, \ldots, a_{1} are in d^{-1}(P), we get that d(a_{n-1}), \ldots, d(a_{1}) are in P. Therefore r_{0}d(r) is in P, which implies that either r_{0} is in P or d(r) is in P. But, if r_{0} is in P, d(r_{0}) is also in P, therefore r_{0} is in d^{-1}(P). Thus equation (1) contradicts to the minimality of n in f(x). Consequently d(r) is in P, which shows that r is in d^{-1}(P) and this completes the proof of the theorem.

Let now s = a + d(b) be an element of I + d(I), with a, b in the ideal I of R. Then d(rb)=rd(b)+d(rb), therefore rs = ra+rd(b) = ra+[d(rb)-d(r)b]=[ra-d(r)b]+d(rb) is in I+d(I), for all r in R. Consequently I + d(I) is an ideal of R.

Further, let R be a local ring, i.e. a Noetherian ring with a unique maximal ideal M and let d be a derivation of R. Then, if M is not a d-ideal of R, M+d(M) is an ideal of R containing properly M, therefore M+d(M)=R. On the other hand, it becomes clear that the ideal M^{k}+d(M^{k}) \subseteq M, for all integers k, k \geq 2. In particular, for k=2 we shall prove the following result:

3.2 Theorem: Let R be a local ring with maximal ideal M and let d be a derivation of R such that M is not a d-ideal of M. Then

\[M^{2}+d(M^{2})=M\] (2).

Proof: Since R is a Noetherian ring, M is a finitely generated ideal of R. Therefore, we can write M=(m_{1}, m_{2}, \ldots, m_{k}), for some positive integer k.

Since M is not a d-ideal of R, there exists at least one generator m_{i} of M such that d(m_{i}) is not in M. We can write then M=(m_{1}+m_{i}, m_{2}+m_{i}, \ldots, m_{k}+m_{i}). Therefore, without loss of generality we may assume that d(m_{i}) is not in M, for all i=1, 2, \ldots, k.
Consequently $d(m_i)$ is a unit of $R$, because otherwise we should have that $(d(m_i))$ is a proper ideal of $R$, which implies that $d(m_i) \subseteq M$, or $d(m_i) \not\subseteq M$, a contradiction. In other words, there exists $r_i$ in $R$ such that $d(r_i)=1$.

Then $d(m_i^2)=2md(m_i)=2m(r_i)$. Therefore $m_i = \frac{1}{2}[2m(r_i)]$ is also in $M^2+d(M^2)$, which completes the proof.

We now introduce the following concept:

**3.3 Definition:** Let $R$ be a ring and let $d$ be in Der-$R$. Then the *integration* of $R$ associated to $d$ is a map $i: R \to R$ such that $d[i(x)]=x$, for all $x$ in $R$.

Next we shall prove:

**3.4 Theorem:** Let $d$ be an injective derivation of a ring $R$ and let $i$ be the integration of $R$ associated to $d$. Then $i$ is a derivation of $R$, if, and only if,

$$xy = -[i(x)d(y)+d(x)i(y)]$$

This, combined to the fact that $d$ is an injective map, we obtain that $d[i(x)+i(y)]=x+y$. Therefore, since $d$ is an injective map, we obtain that

$$i(x+y)=i(x)+i(y)$$  \hspace{1cm} (3)

On the other hand, we have that $d[i(xy)]=xy$ and $d[xi(y)+di(y)] = d[xi(y)]+d[di(y)] = x[d[i(y)]+d(i(x)i(y))+i(x)d(y)+d(i(y))y = 2xy+d(x)i(y)+i(x)d(y)$.

On comparing the last two equations we obtain that

$$d[i(xy)]=d[xi(y)+di(y)]$$ if, and only if,

$$xy=2xy+d(x)i(y)+i(x)d(y)$$

This, combined to the fact that $d$ is an injective map, it finally shows that $i(xy)=xi(y)+i(x)y$, if, and only if, $xy = -[i(x)d(y)+d(x)i(y)]$  \hspace{1cm} (4).

Equations (3) and (4) complete the proof of the theorem.

Theorem 3.4 has the following two important corollaries:

**3.5 Corollary:** Let $R$ be a ring, let $d$ be an injective outer derivation $R$ and let $i$ be the integration of $R$ associated to $d$. Assume further that $xy = -[i(x)d(y)+d(x)i(y)]$, for all $x, y$ in $R$. Then:

1. The skew polynomial ring $S=R[x, i]$ is simple, if, and only if, $R$ is an i-simple ring.
2. If $P$ is a prime ideal of $S$, $P \cap R$ is an i-prime ideal of $R$ and if $I$ is an i-prime ideal of $R$, $IS$ is a prime ideal of $S$.

**Proof:** 1) By Theorem 3.4 $i$ is a derivation of $R$, therefore the result follows by applying Theorem 2.12 for $n=1$.
2) It turns out by combining Theorem 3.4 and Theorem 2.14 for $n=1$.

Next we need the following lemma:

**3.6 Lemma:** Let $D = \{d_1, d_2, \ldots, d_n\}$ be a finite set of injective derivations of a ring $R$ commuting to each other and let $F = \{f_1, f_2, \ldots, f_n\}$ be the set of integrations of $R$, such that $f_i$ is associated to $d_i$, $i=1,2,\ldots,n$. Then the integrations of $F$ commute to each other.

**Proof:** Given $r$ in $R$, we have that $d_i[d_j[f_i(r)] = d_i[d_j[f_i(r)] = d_i[f_i(r)] = d_i[f_i(r)] = r$. In the same way it turns out that $d_i[d_j[f_i(r)] = r$, therefore $d_i[d_j[f_i(r)] = d_i[d_j[f_i(r)]$.

But the map $d_i$, injective, hence $f_i \circ f_j = f_j \circ f_i$ and the result follows.

**3.7 Corollary:** Let $D = \{d_1, d_2, \ldots, d_n\}$ be a finite set of injective derivations of a ring $R$ commuting to each other and let $F = \{f_1, f_2, \ldots, f_n\}$ be the set of integrations of $R$, such that $f_i$ is associated to $d_i$, $i=1,2,\ldots,n$. Assume further that for the derivation $d_i$ and the associated to it integration $f_i$ the equation (3) holds for all the elements of $S_{i-1}$ (where $S_0=R$). Then one can define the ISPR $S_n = R[x, F]$, where we have:

- If $P$ is a prime ideal of $S_n$, $P \cap R$ is an F-prime ideal of $R$.
- If $I$ is an F-prime ideal of $R$, $IS_n$ is a prime ideal of $S_n$.

**Proof:** By Theorem 3.4 the elements of $F$ are derivations of $R$ and by Lemma 3.6 they commute to each other. Therefore we can define the ISPR $S_n = R[x, F]$ and the result follows by Theorem 2.14.

**4. Conclusion**

In this work we studied properties of the differential ideals of a ring $R$ and of the ISPRs of derivation type over $R$. The notion of an integration of $R$ associated to a given derivation of $R$ was also introduced and some fundamental properties of it were studied. This new concept generalizes basic features of the indefinite integrals and therefore a further research on its properties in connection to corresponding properties of the associated derivations seems to have its own importance.

For example, an open question is if the first case of Corollary 3.5 can be extended to ISPRs in finitely many variables defined as in Corollary 3.7. This could happen if each $f_i$ in $F$ in Corollary 3.7 is an outer derivation of $S_{i-1}$, but the conditions under which this happens are under investigation.

**References:**


Lopez-Permouth, S., Matrix Representations of Skew Polynomial Rings with Semisimple