行政院國家科學委員會專題研究計畫 成果報告

代數斜導算及其常數

計畫類別：個別型計畫
計畫編號：NSC91-2115-M-002-012-
執行期間：91年08月01日至92年12月31日
執行單位：國立臺灣大學數學系暨研究所

計畫主持人：莊正良
共同主持人：蔡援宗

報告類型：精簡報告
處理方式：本計畫可公開查詢

中華民國 93年 0月 0日
Abstract. Let $R$ be a prime ring with $d$ a left $R$–algebraic derivation. All possible left $R$–algebraic relations of $d$ are described by a specific ideal of the skew polynomial ring $R[x; d]$. Moreover, the prime radical and the minimal prime ideals over such ideal are also determined. As an application to the main theorem, the nilpotent case is completely obtained.

1. Results

Throughout this paper, $R$ is always a prime ring with $R_F$ its left Martindale quotient ring and $Q$ its symmetric Martindale quotient ring. The center of $R_F$ (and of $Q$ also), denoted by $C$, is called the extended centroid of $R$. We refer these notation to [2] for details. Also, $d$ is always a derivation of $R$. By this, we mean that $d: R \to R$ is an additive map such that $d(ab) = d(a)b + ad(b)$ for all $a, b \in R$. Given $b \in R$, the map $ad(b): r \in R \mapsto [b, r] \overset{\text{def}}{=} br - rb$ obviously defines a derivation, called the inner derivation defined by $b$. We call a derivation outer if it is not of this form. It is well–known that every derivation $d$ of $R$ can be uniquely extended to a derivation of $Q$ and also to a derivation of $R_F$. For any subset $S$ of $R_F$, we define $S^{(d)} \overset{\text{def}}{=} \{ r \in S \mid d(r) = 0 \}$, the set of constants of $d$ on $S$. To analyze derivations of $R$, as shown in Kharchenko’s theory [9, 10], we have to work in the larger ring $Q$. The derivation $d$ is called X–inner if its extension to $Q$ is inner. Otherwise, it is called X–outer.

We denote $R[x; d]$ the skew polynomial ring endowed with the multiplication rule: $xr = rx + d(r)$ for $r \in R$. Since the derivation $d$ can be uniquely extended to a derivation of $R_F$, we can also construct $R_F[x; d]$ analogously and regard $R[x; d]$ as
a subring of $R_\mathcal{F}[x;d]$ in a natural way. For $a_0x^n + \cdots + a_{n-1}x + a_n \in R[x;d]$ and $r \in R$, we define

$$(a_0x^n + \cdots + a_{n-1}x + a_n) \rightarrow r = a_0d^n(r) + \cdots + a_{n-1}d(r) + a_nr \in R.$$  

It is well–known that $R$ forms a left $R[x;d]$–module under the above action. Our first aim is just to describe:

$$\mathcal{A} \overset{\text{def.}}{=} \{g(x) \in R[x;d] \mid g(x) \rightarrow R = 0\}.$$  

Note that $\mathcal{A}$ is a two–sided ideal of $R[x;d]$. The ideal $\mathcal{A}$ describes all possible left $R$–algebraic relations of $d$ (its precise definition will be given below). Let $\mathcal{P}$ be the ideal of $R[x;d]$ containing $\mathcal{A}$ such that $\mathcal{P} / \mathcal{A}$ is the prime radical of $R[x;d] / \mathcal{A}$. Our next aim is to describe the ideal $\mathcal{P}$ and also the minimal prime ideals over $\mathcal{A}$.

There is a natural interpretation of the ring $R[x;d] / \mathcal{A}$: For $a \in R$, let $a_L : x \in R \mapsto ax \in R$ denote the left multiplication by $a$. All $a_L$ are endomorphisms of the abelian additive group $(R, +)$. In the ring of endomorphisms of $(R, +)$, let $S$ be the subring generated by $d$ and all $a_L$, $a \in R$. Note that $da_L = d(a)_L + a_L d$ for $a \in R$. The map

$$\varphi : a_0x^n + \cdots + a_{n-1}x + a_n \mapsto (a_0)_L d^n + \cdots + (a_{n-1})_L d + (a_n)_L \in S$$  

is a surjective ring homomorphism. We see easily that the kernel of $\varphi$ is $\mathcal{A}$. So $R[x;d] / \mathcal{A} \cong S$. In this sense, our result amounts to describing the prime radical and minimal prime ideals of $S$.

To state our result, we need one more notation. If $f(x)$ is a monic element of $R_\mathcal{F}[x;d]$, we define

$$\langle f(x) \rangle \overset{\text{def.}}{=} (R_\mathcal{F}[x;d]f(x)R_\mathcal{F}[x;d]) \cap R[x;d].$$  

In addition, if $f(x)$ is central, then

$$\langle f(x) \rangle = (f(x)R_\mathcal{F}[x;d]) \cap R[x;d]$$  

$$= \{g(x) \in R[x;d] \mid g(x) \text{ is a multiple of } f(x) \text{ in } R_\mathcal{F}[x;d]\}.$$  

We will describe $\mathcal{A}$, $\mathcal{P}$ in terms of ideals in the above form $\langle f(x) \rangle$, where $f(x)$ is central. For this purpose, we must investigate the center of $R_\mathcal{F}[x;d]$. Fortunately, this has been completely done in [13]:

**Proposition 1.** (Matczuk [13]) (I) Assume $\text{char } R = 0$. If $d = \text{ad}(-b)$ for some $b \in Q$, then the center of $R_\mathcal{F}[x;d]$ equals to $C^{(d)}[\zeta]$, where $\zeta \overset{\text{def.}}{=} x + b$. If $d$ is $X$–outer, then the center of $R_\mathcal{F}[x;d]$ is merely $C^{(d)}$. (II) Assume $\text{char } R = p > 0$. If there exists $b \in Q^{(d)}$ and $\alpha_1, \cdots, \alpha_s \in C^{(d)}$ such that

$$d^{p^s} + \alpha_1 d^{p^{s-1}} + \cdots + \alpha_s d = \text{ad}(-b),$$  

then $d^{(d)}$ can be written in one of the following forms:

$$(d^{(d)})_1 = d^{p^{(d)}(-b)}$$  

or

$$(d^{(d)})_2 = d^{p^{(d)}b} + \text{ad}(-b)$$  

or

$$(d^{(d)})_3 = d^{(d)}b + \text{ad}(-b).$$  

Furthermore, the center of $R_\mathcal{F}[x;d]$ equals to

$$C^{(d)}[\zeta] = \{g(x) \in R_\mathcal{F}[x;d] \mid g(x) \text{ is central in } R_\mathcal{F}[x;d]\}.$$  

Finally, the center of $R_\mathcal{F}[x;d]$ can be written as

$$C^{(d)}[\zeta] = \{g(x) = f(x) + b(x) \mid f(x) \in \mathcal{A}, b(x) \in \mathcal{P}\}.$$  

In particular, if $d = \text{ad}(-b)$ and $b \in Q^{(d)}$, then

$$C^{(d)}[\zeta] = \{g(x) = f(x) + b(x) \mid f(x) \in \mathcal{A}, b(x) \in \mathcal{P}\}.$$  

If $d$ is $X$–outer, then

$$C^{(d)}[\zeta] = \{g(x) = f(x) + b(x) \mid f(x) \in \mathcal{A}, b(x) \in \mathcal{P}\}.$$
then we let (1) be the one with $s$ as minimal as possible and set

$$
\zeta \overset{\text{def.}}{=} x^{p^s} + \alpha_1 x^{p^{s-1}} + \cdots + \alpha_s x + b.
$$

The center of $R[x; d]$ is equal to $C^{(d)}[\zeta]$. If there is no such expression (1), then the center of $R[x; d]$ is merely $C^{(d)}$.

The derivation $d$ is said to be \textit{left $R_F$–algebraic} (left $R$–algebraic) if there exist $b_0 \neq 0, b_1, \cdots, b_{n-1} \in R_F$ (resp. $R$) such that

$$
b_0 d^n(r) + b_1 d^{n-1}(r) + \cdots + b_{n-1} d(r) = 0
$$

for all $r \in R$. We say that $d$ is $C$–algebraic if all $b_i \in C$. It is easy to see that the left $R$–algebraicity, the left $R_F$–algebraicity and the $C$–algebraicity of a derivation $d$ are all equivalent. If $d$ is not left $R$–algebraic, then $A = 0$ and $P = 0$. Since the ring $R[x; d]$ is prime, the only minimal prime ideal is $\{0\}$. So there is nothing to do in this case. We hence assume that our $d$ is left $R$–algebraic or, equivalently, left $R_F$–algebraic. Our main theorem is as follows:

**Theorem 1.** Let $R$ be a prime ring and let $d$ be a left $R_F$–algebraic derivation of $R$. Let $\zeta, b$ be as described in Proposition 1. Let $\mu(\lambda)$ be the minimal polynomial of $b$ over $C^{(d)}$. Then the following hold:

1. $A = \langle \mu(\zeta) \rangle$.

2. We factorize $\mu(\lambda)$ into the product of monic irreducible factors in $C^{(d)}[\lambda]$: $\mu(\lambda) = \pi_1(\lambda)^{n_1} \pi_2(\lambda)^{n_2} \cdots \pi_k(\lambda)^{n_k}$. Then all minimal prime ideals of $R[x; d]$ over $A$ are $\langle \pi_s(\zeta) \rangle$, $s = 1, \cdots, k$, and $P = \langle \pi_1(\zeta) \pi_2(\zeta) \cdots \pi_k(\zeta) \rangle$.

Before proceeding to the proof of Theorem 1, let us compute explicitly the $\zeta$ of Proposition 1 for a left $R_F$–algebraic derivation $d$: We apply Kharchenko’s theorem [10, Theorem 2]. If $\text{char } R = 0$, then $d = ad(-b)$ for some $b \in Q$ and we set $\zeta \overset{\text{def.}}{=} x + b$. If $\text{char } R = p > 0$, then $d, d^p, d^{p^2}, \ldots$ are $C$–dependent modulo $X$–inner derivations. Let $s \geq 0$ be the minimal integer such that

$$
d^{p^s}, d^{p^{s-1}}, \cdots, d^p, d
$$

are $C$–dependent modulo $X$–inner derivations. By the minimality of $s$, there exist $\alpha_i \in C$ and $b \in Q$ such that

$$
d^{p^s} + \alpha_1 d^{p^{s-1}} + \cdots + \alpha_s d = ad(-b),
$$

We see easily that $d(\alpha_i) = 0$ and $d(b) \in C$. We divide our discussion into two cases:
Case 1. \( d(b) \in d(C) \): Say, \( d(b) = d(\alpha) \), where \( \alpha \in C \). Then \( d(b - \alpha) = 0 \). Since \( b \) and \( b - \alpha \) define the same \( X \)-inner derivation, we may replace \( b \) by \( b - \alpha \) and assume that \( d(b) = 0 \). So we have
\[
\zeta = x^{p^r} + \alpha_1 x^{p^{r-1}} + \cdots + \alpha_s x + b.
\]

Case 2. \( d(b) \notin d(C) \): Since \( d(\alpha_i) = 0 \), each \( \alpha_i \) considered as left multiplication commutes with \( d \). Since \( d(b) \in C \), \( d(b) \) also commutes with \( d \). Using the commutativity, we raise both sides of (1) to the \( p \)-th power. This gives the equality:
\[
d^{p+1} + \alpha_1^{p} d^{p^{r-1}} + \cdots + \alpha_s^{p} d = \text{ad}(-b^{p}).
\]
Obviously, \( d(b^{p}) = 0 \). So we have
\[
\zeta = x^{p^r+1} + \alpha_1^{p} x^{p^{r}} + \cdots + \alpha_s^{p} x^{p} + b^{p}.
\]

Moreover, we observe that the \( X \)-inner derivation \( \text{ad}(b) \) is \( R_{X} \)-algebraic if and only if \( b \) is \( C \)-algebraic. Note that a differential identity of \( R \) also vanishes on \( R_{X} \) [11, Theorem 2]. In particular, the restriction of \( d \) to \( C \) is \( C \)-algebraic. In view of [1, Theorem 1], \( C \) is finite–dimensional over \( C^{(d)} \). Thus this is also equivalent to say that \( b \) is \( C^{(d)} \)-algebraic. We summarize what we have shown in the following:

**Lemma 1.** Let \( d \) be a left \( R_{X} \)-algebraic derivation and let \( \zeta \) be as described in Proposition 1. If \( \text{char} \ R = 0 \), then \( d = \text{ad}(-b) \) for some \( b \in Q \) and \( \zeta = x + b \). If \( \text{char} \ R = p \geq 2 \), then there exists the minimal integer \( s \geq 0 \) such that
\[
d^{p^r} + \alpha_1^{p} d^{p^{r-1}} + \cdots + \alpha_s d = \text{ad}(-b)
\]
for some \( \alpha_i \in C^{(d)} \) and \( b \in Q \) with \( d(b) \in C \). In the case of \( d(b) \in d(C) \), we may choose \( b \in Q^{(d)} \) and \( \zeta = x^{p^r} + \alpha_1 x^{p^{r-1}} + \cdots + \alpha_s x + b \). In the case that \( d(b) \notin d(C) \), we have \( b^{p} \in Q^{(d)} \) and \( \zeta = x^{p^r+1} + \alpha_1^{p} x^{p^r} + \cdots + \alpha_s^{p} x^{p} + b^{p} \). Moreover, \( b \) above is always \( C^{(d)} \)-algebraic.

To prove Theorem 1, we need another important proposition from [13], which, unfortunately, is not explicitly formulated in [13]. So we include its proof here. See also [14, Theorem 3.3].

**Proposition 2.** (Matczuk) If \( I \) is an ideal of \( R[x; d] \), then there exists a unique monic \( f(x) \) in the center of \( R_{X}[x; d] \) such that any element of \( I \) is a multiple of \( f(x) \) in \( R_{X}[x; d] \), i.e., \( I \subseteq (f(x)) \). Moreover, there exists a nonzero ideal \( I \) of \( R \) such that \( If(x) \subseteq I \).

**Proof.** If \( R \cap I \neq 0 \), we simply take \( f(x) = 1 \) and set \( I \overset{\text{def.}}{=} R \cap I \). Therefore, we assume that \( R \cap I = 0 \). Let \( n \) be the minimal possible degree for nonzero elements of \( I \). We define
\[
I \overset{\text{def.}}{=} \{ a \in R \mid \exists a_1, \ldots, a_n \in R \text{ such that } ax^n + a_1 x^{n-1} + \cdots + a_n \in I \}.
\]
Note that I is a nonzero ideal of R. Since \( R \cap I = 0 \), it follows from the minimality of \( n \) that \( a_1, \ldots, a_n \) are uniquely determined by \( a \). Write \( a_i = \beta_i(a) \) for \( a \in I \). We have \( \beta_i(ra) = r\beta_i(a) \) for \( r \in R \). Each \( \beta_i : I \to R \) is thus a left \( R \)-module map. So there exist \( q_i \in R_F \) such that \( \beta_i(a) = aq_i \). Set our desired monic polynomial to be

\[
f(x) \overset{\text{def.}}{=} x^n + q_1x^{n-1} + \cdots + q_n \in R_F[x; d].
\]

We show that \( f(x) \) is a center element of \( R_F[x; d] \). Note that \( I^2 x \subseteq xI^2 + d(I^2) \subseteq xI^2 + I \). Thus \( I^2 x f(x) R \subseteq I \). It is also clear that \( I^2 f(x) x R \subseteq I \). We have

\[
I^2(xf(x) - f(x)x)R = I^2(d(q_1)x^{n-1} + \cdots + d(q_{n-1})x + d(q_n))R \subseteq I.
\]

By the minimality of \( n \), this implies \( d(q_1) = \cdots = d(q_{n-1}) = d(q_n) = 0 \). Similarly, for \( r \in R \), \( I(rf(x) - f(x)r) \) falls in \( I \) and has degree \( < n \). So \( I(rf(x) - f(x)r) = 0 \), implying that \( rf(x) = f(x)r \). Given \( a \in R_F \), let \( J \) be a nonzero ideal of \( R \) such that \( Ja \subseteq R \). For \( r \in J \) we have

\[
0 = [ra, f(x)] = [r, f(x)]a + r[a, f(x)] = r[a, f(x)],
\]

and so \( J[a, f(x)] = 0 \). This implies \( af(x) = f(x)a \) for all \( a \in R_F \). All these together say that \( f(x) \) falls in the center of \( R_F[x; d] \), as asserted.

Finally, given any \( g(x) \in I \), we write, using the division algorithm in \( R_F[x; d] \),

\[
g(x) = f(x)q(x) + r(x),
\]

where \( q(x), r(x) \in R_F[x; d] \) and the degree of \( r(x) \) is less than \( n \). Pick a nonzero ideal \( J \) of \( R \) such that \( Jq(x) \cup Jr(x) \subseteq R[x; d] \). Let \( a \in I \) and \( b \in J \); then \( abg(x) = af(x)bq(x) + abr(x) \). Since \( af(x) \in I \), this implies that \( abr(x) \in I \) and has degree less than \( n \). Thus \( abr(x) = 0 \). That is, \( Jr(x) = 0 \) and so \( r(x) = 0 \). So any \( g(x) \in I \) is a multiple of \( f(x) \) in \( R_F[x; d] \). Also, it is clear that \( If(x) \subseteq I \) by the definition of \( I \). This completes the proof.

For convenience, we call \( f(x) \) described above the central generator of the ideal \( I \). Proposition 2 says \( I \subseteq \langle f(x) \rangle \). We say \( I \) is stable if \( I = \langle f(x) \rangle \), that is, the ideal consists exactly of multiples of its central generator. Ideals of \( R[x; d] \) are somewhat decided by their central generators but still can involve complexities of the ideal structure of the ring \( R \). But stable ideals are completely determined by their central generators. We now come to the proof of Theorem 1. We first note a simple but important property of central elements in \( R_F[x; d] \):

**Lemma 2.** If \( a_0 x^n + \cdots + a_{n-1} x + a_n \) lies in the center of \( R_F[x; d] \), then

\[
(a_0 x^n + \cdots + a_{n-1} x + a_n) \rightarrow r = ra_n \text{ for all } r \in R_F.
\]
Proof. Set \( f(x) = a_0x^n + \cdots + a_{n-1}x + a_n \). Let \( r \in \mathbb{F} \). Note that \( a_0d^n(r) + \cdots + a_{n-1}d(r) + a_n r \) is the constant term of \( f(x)r \) and \( r a_n \), the constant term of \( rf(x) \).
Since \( f(x)r \) and \( rf(x) \) are equal, so are their constant terms. Thus \( a_0d^n(r) + \cdots + a_{n-1}d(r) + a_n r = r a_n \), proving the lemma.

**Lemma 3.** If \( \pi(\lambda) \in C^{(d)}[\lambda] \) is monic and irreducible, then \( \langle \pi(\xi) \rangle \) is a prime ideal of \( R[x;d] \), where \( \xi \) is as given in Proposition 1.

**Proof.** Suppose that \( J_1 \) and \( J_2 \) are two ideals of \( R[x;d] \) such that \( J_i \supseteq \langle \pi(\xi) \rangle \) for \( i = 1, 2 \) and such that \( J_1 J_2 \subseteq \langle \pi(\xi) \rangle \). Then, by Proposition 2, there exist central generators \( g_1(\xi) \) and \( g_2(\xi) \) of \( J_1 \) and \( J_2 \), respectively. Choose a nonzero ideal \( J \) of \( R \) such that \( J \pi(\xi) \subseteq R[x;d] \) and \( J g_i(\xi) \subseteq J_i \) for \( i = 1, 2 \). Thus

\[
J^2 g_1(\xi) g_2(\xi) = J g_1(\xi) J g_2(\xi) \subseteq J_1 J_2 \subseteq \langle \pi(\xi) \rangle.
\]

If \( (g_1(\lambda) g_2(\lambda), \pi(\lambda)) = 1 \) in \( C^{(d)}[\lambda] \), then there exist \( A(\lambda), B(\lambda) \in C^{(d)}[\lambda] \) such that \( A(\lambda) g_1(\lambda) g_2(\lambda) + B(\lambda) \pi(\lambda) = 1 \). In particular, we have

\[
A(\xi) g_1(\xi) g_2(\xi) + B(\xi) \pi(\xi) = 1.
\]

Choose a nonzero ideal \( I \) of \( R \) such that \( IA(\xi) \cup IB(\xi) \subseteq R[x;d] \). By (2),

\[
0 \neq IJ^2 \subseteq I A(\xi) (J^2 g_1(\xi) g_2(\xi)) + I B(\xi) J^2 \pi(\xi) \subseteq \langle \pi(\xi) \rangle,
\]
a contradiction. Thus \( (g_1(\lambda) g_2(\lambda), \pi(\lambda)) \neq 1 \). The irreducibility of \( \pi(\lambda) \) implies that either \( \pi(\lambda)|g_1(\lambda) \) or \( \pi(\lambda)|g_2(\lambda) \) in \( C^{(d)}[\lambda] \). Assume, without loss of generality, that \( \pi(\lambda)|g_1(\lambda) \). Therefore, there exists \( h(\lambda) \in C^{(d)}[\lambda] \) such that \( g_1(\xi) = h(\xi) \pi(\xi) \). This implies that \( \langle g_1(\xi) \rangle \subseteq \langle \pi(\xi) \rangle \). But \( J_1 \subseteq \langle g_1(\xi) \rangle \). So \( J_1 \subseteq \langle \pi(\xi) \rangle \), proving the lemma.

We are now ready to give the

**Proof of Theorem 1.** By Proposition 2, there exists the central generator \( f(x) \) of \( A \) and an ideal \( I \neq 0 \) of \( R \) such that \( IF(x) \in A \). Thus \( A \subseteq \langle f(x) \rangle \). Since \( IF(x) \in A \), we have \( 0 = IF(x) \rightarrow R = I(f(x) \rightarrow R) \) and hence \( f(x) \rightarrow R = 0 \). This implies \( \langle f(x) \rangle \rightarrow R = 0 \) and hence \( A = \langle f(x) \rangle \). By assumption, \( d \) is \( R[x]-\text{algebraic} \). Assume that \( d \neq 0 \). Let

\[
\zeta = \begin{cases} 
  x + b, & \text{if char } R = 0 \\
  x^p + \alpha_1 x^{p^2} + \cdots + \alpha_s x + b, & \text{if char } R = p > 0
\end{cases}
\]

be given as in Proposition 1. Applying Proposition 2, we may write

\[
f(x) = \zeta^n + \beta_1 \zeta^{n-1} + \cdots + \beta_n,
\]
where $\beta_i \in C^{(d)}$. We set $\tilde{\mu}(\lambda) = \lambda^n + \beta_1 \lambda^{n-1} + \cdots + \beta_n \in C^{(d)}[\lambda]$. It follow from (3) that $\tilde{\mu}(b)$ is the constant term of $f(x)$. By Lemma 2, we have $0 = f(x) \in R = R \tilde{\mu}(b)$ and so $\tilde{\mu}(b) = 0$. Thus $\mu(\lambda)$ divides $\tilde{\mu}(\lambda)$ in $C^{(d)}[\lambda]$.

On the other hand, $\mu(b)$ is the constant term of $\mu(\zeta)$. Since $\mu(\zeta)$ is central, we have $\mu(\zeta) \in R = R \mu(b) = 0$ by Lemma 2. It follows from the minimality of the degree of $f(x)$ that the degree of $\mu(\lambda)$ is equal to or greater than $n$ and so $\mu(\lambda) = \tilde{\mu}(\lambda)$. Hence, $f(x) = \mu(\zeta)$ follows. We factorize $\mu(\lambda)$ into the product of monic irreducible factors in $C^{(d)}[\lambda]$: $\mu(\lambda) = \pi_1(\lambda)^{n_1} \pi_2(\lambda)^{n_2} \cdots \pi_k(\lambda)^{n_k}$, where $n_i$ are positive integers. To show that $\mathcal{P} = \langle \pi_1(\lambda) \pi_2(\lambda) \cdots \pi_k(\lambda) \rangle$ and that minimal prime ideals of $R[x; d]$ over $A$ are $\langle \pi_s(\zeta) \rangle$, $s = 1, \ldots, k$, we quote the following more general Theorem 2.

**Theorem 2.** Let $\mu(\lambda) \in C^{(d)}[\lambda]$ be monic. We factorize $\mu(\lambda)$ into the product of monic irreducible factors in $C^{(d)}[\lambda]$: $\mu(\lambda) = \pi_1(\lambda)^{n_1} \pi_2(\lambda)^{n_2} \cdots \pi_k(\lambda)^{n_k}$, where $n_i$ are positive integers. Then all minimal prime ideals of $R[x; d]$ over $\langle \mu(\zeta) \rangle$ are $\langle \pi_s(\zeta) \rangle$, $s = 1, \ldots, k$, where $\zeta$ is given as in Proposition 1. Moreover, the prime radical of $R[x; d]/\langle \mu(\zeta) \rangle$ is equal to $\langle \pi_1(\lambda) \pi_2(\lambda) \cdots \pi_k(\lambda) \rangle/\langle \mu(\zeta) \rangle$.

The theorem above describes the prime radical and the minimal prime ideals over a stable ideal. For its proof, we need a lemma.

**Lemma 4.** If $\mu_1(\lambda)$ and $\mu_2(\lambda)$ are monic and coprime in $C^{(d)}[\lambda]$, then $\langle \mu_1(\zeta) \rangle \cap \langle \mu_2(\zeta) \rangle = \langle \mu_1(\zeta) \mu_2(\zeta) \rangle$, where $\zeta$ is given as in Proposition 1.

**Proof.** The inclusion $\langle \mu_1(\zeta) \mu_2(\zeta) \rangle \subseteq \langle \mu_1(\zeta) \rangle \cap \langle \mu_2(\zeta) \rangle$ is obvious. For the reverse inclusion, let $f(x) \in \langle \mu_1(\zeta) \rangle \cap \langle \mu_2(\zeta) \rangle$. Write $f(x) = g_1(x)\mu_1(\zeta) = g_2(x)\mu_2(\zeta)$, where $g_i(x) \in R[x; d]$. Since $\mu_1(\lambda)$ and $\mu_2(\lambda)$ are coprime in $C^{(d)}[\lambda]$, there exist $A(\lambda), B(\lambda) \in C^{(d)}[\lambda]$ such that

$$A(\lambda)\mu_1(\zeta) + B(\zeta)\mu_2(\zeta) = 1.$$ 

Thus

$$g_1(x) = A(\zeta)g_1(x)\mu_1(\zeta) + g_1(x)B(\zeta)\mu_2(\zeta) = A(\zeta)g_2(x)\mu_2(\zeta) + g_1(x)B(\zeta)\mu_2(\zeta) = (A(\zeta)g_2(x) + g_1(x)B(\zeta))\mu_2(\zeta),$$

implying that

$$f(x) = (A(\zeta)g_2(x) + g_1(x)B(\zeta))\mu_1(\zeta)\mu_2(\zeta).$$

So $f(x) \in \langle \mu_1(\zeta) \mu_2(\zeta) \rangle$. Thus $\langle \mu_1(\zeta) \rangle \cap \langle \mu_2(\zeta) \rangle \subseteq \langle \mu_1(\zeta) \mu_2(\zeta) \rangle$, proving the lemma.

**Proof of Theorem 2.** Let $\mathcal{Q}$ is an ideal of $R[x; d]$, which is a minimal prime ideal over $A$. Then

$$\mathcal{Q} \supseteq \langle \pi_1(\zeta) \rangle^{n_1} \cdots \langle \pi_k(\zeta) \rangle^{n_k}.$$
By the primeness of $Q$, we see that $Q$ contains $\langle \pi_i(\zeta) \rangle$ for some $i$. By Lemma 3, $\langle \pi_i(\zeta) \rangle$ is a prime ideal of $R[x;d]$. The minimality of $Q$ implies that $Q = \langle \pi_i(\zeta) \rangle$. This proves that all possible minimal prime ideals of $R[x;d]$ over $\langle \mu(\zeta) \rangle$ are $\langle \pi_s(\zeta) \rangle$, $s = 1, \ldots, k$. Conversely, we show each $\langle \pi_i(\zeta) \rangle$ is a minimal prime ideal over $A$: Let $Q_0$ be a prime ideal of $R[x;d]$ such that $\langle \pi_i(\zeta) \rangle \supseteq Q_0 \supseteq \langle \mu(\zeta) \rangle$. Applying the same argument above yields $Q_0 \supseteq \langle \pi_j(\zeta) \rangle$ for some $j$ and so $\langle \pi_i(\zeta) \rangle \supseteq \langle \pi_j(\zeta) \rangle$. Suppose $i \neq j$. There exist $A(\zeta), B(\zeta) \in C^{(d)}[\zeta]$ such that

$$A(\zeta)\pi_i(\zeta) + B(\zeta)\pi_j(\zeta) = 1.$$ 

Choose a nonzero ideal $I$ of $R$ such that $IA(\zeta) \cup I\pi_i(\zeta) \cup IB(\zeta) \cup I\pi_j(\zeta) \subseteq R[x;d]$. Then

$$0 \neq I^2 \subseteq IA(\zeta)I\pi_i(\zeta) + IB(\zeta)I\pi_j(\zeta) \subseteq IA(\zeta)I\pi_i(\zeta) + \langle \pi_j(\zeta) \rangle \subseteq \langle \pi_i(\zeta) \rangle,$$

a contradiction. Let $H$ be the ideal of $R[x;d]$ such that $H/\langle \mu(\zeta) \rangle$ is the prime radical of $R[x;d]/\langle \mu(\zeta) \rangle$. Choose a positive integer $m \geq n_i$ for all $i$. Then

$$\langle \pi_1(\lambda)\pi_2(\lambda)\cdots\pi_k(\lambda) \rangle^m \subseteq \langle \mu(\zeta) \rangle \subseteq H.$$

But $H$ is a semiprime ideal of $R[x;d]$. So $\langle \pi_1(\lambda)\pi_2(\lambda)\cdots\pi_k(\lambda) \rangle \subseteq H$ follows. On the other hand, by Lemma 3 each $\langle \pi_i(\zeta) \rangle$ is a prime ideal of $R[x;d]$ and so

$$H \subseteq \langle \pi_1(\lambda) \rangle \cap \cdots \cap \langle \pi_1(\lambda) \rangle \subseteq \langle \pi_1(\lambda)\pi_2(\lambda)\cdots\pi_k(\lambda) \rangle,$$

where the second inclusion is implied by Lemma 4. Thus $H = \langle \pi_1(\lambda)\pi_2(\lambda)\cdots\pi_k(\lambda) \rangle$. The proof is now complete.

2. An Application to the Nilpotent Case

Firstly, we need an important notion:

**Definition.** ([4, 3]) Let $d$ be a nilpotent derivation of $R$. The least integer $m$ such that $d^m(R)c = 0$ for some nonzero $c \in R$ is called the annihilating nilpotency of $d$ and is denoted by $m_d(R)$.

For a nilpotent derivation $d$ of a prime ring $R$, there is another interesting construction, which has been employed extensively and fruitfully in the literature [4]–[8]: In the ring $R[x;d]$, we consider the two-sided ideal $\langle x^m \rangle$, where $m = m_d(R)$. For $r \in R$,

$$x^m r = r x^m + \binom{m}{1} d(r) x^{m-1} + \cdots + \binom{m}{m-1} d^{m-1}(r) x + d^m(r).$$
Therefore, if $a_0x^n + a_1x^{n-1} + \cdots + a_n \in \langle x^m \rangle$, then $a_n \in R^d(R)$. This implies $R^d(R)$ contains $\langle x^m \rangle \cap R$, which is an ideal of $R$. Since $R^d(R)$ has nonzero left annihilator, we have $\langle x^m \rangle \cap R = 0$. Extend $\langle x^m \rangle$ to an ideal $M$ of $R[x;d]$ maximal with respect to the property that $M \cap \langle x^m \rangle = 0$. Then we see easily that $M$ is a prime ideal of $R[x;d]$. The quotient ring $r[x;d]/M$ is called the $d$-extension of $R$ [6].

Our aim is to prove that $M$ is equal to the ideal $P$ described in Theorem 1. For this purpose we need a structure result of nilpotent derivations. The following is given in [3, Theorems 1–4].

**Theorem 3.** Let $d$ be a nilpotent derivation of a prime ring $R$.

1. In the case of $\text{char} R = 0$, there exists a nilpotent $b \in Q$ with the nilpotency $l$ such that $d = \text{ad}(-b)$ and $m_d(R) = 1$.

2. In the case of $\text{char} R = p \geq 2$, let $s$ be the least integer $\geq 1$ such that $d^{p^i}$, $0 \leq i \leq s$, are $C$-dependent modulo $X$-inner ones. Then there exists $b \in Q$ such that $d^{p^s} = \text{ad}(-b)$ and such that the minimal polynomial of $b$ over $C$ assumes the form $(b^{p^s} - \alpha)^l = 0$, where $\alpha \in C^{(d)}$, $l, t \geq 0$ and $(l,p) = 1$. Moreover, $m_d(R) = p^{s+1}$. For a nilpotent derivation $d$, we have the following detailed description of $M$ defined above:

**Theorem 4.** For a nilpotent derivation $d$ of a prime ring $R$, let $A, P$ be as described in Theorem 1 and $M$, the ideal described above. In the notation of Theorem 3, we have the following

1. In the case of $\text{char} R = 0$, $A = \langle \zeta^l \rangle$ and $P = M = \langle \zeta \rangle$, where $\zeta = x + b$ and where $l$ is the nilpotency of $b$.

2. In the case of $\text{char} R = p \geq 2$, there are two subcases given as follows:

   (i) Suppose that $b$ is chosen such that $d(b) = 0$. Set $\zeta = x^{p^s} + b$. Then

   $$A = \langle (\zeta^{p^s} - \alpha)^l \rangle \quad \text{and} \quad M = P = \langle \zeta^{p^s} - \alpha^{1/p^s} \rangle,$$

   where $u$ is the largest integer such that $0 \leq u \leq t$ and $\alpha^{1/p^u} \in C^{(d)}$.

   (ii) Suppose that $d(b) \notin d(C)$. Set $\zeta = x^{p^{s+1}} + b^p$. Then

   $$A = \langle (\zeta^{p^{s+1}} - \alpha)^l \rangle \quad \text{and} \quad M = P = \langle \zeta^{p^{s+1}} - \alpha^{1/p^u} \rangle,$$

   where $u$ is the largest integer such that $0 \leq u \leq t - 1$ and $\alpha^{1/p^u} \in C^{(d)}$.

We need the following lemma. See [2, Theorem 2.3.3] for the proof.

**Lemma 5.** Let $v_1, v_2, \ldots, v_n$ be $C$-independent elements in $R_\mathcal{F}$ and let $I$ be a nonzero ideal of $R$. Then there exist finitely many $a_i, b_i \in I$ such that $\sum_i a_i v_j b_i = 0$ for $1 \leq j \leq n - 1$ but $\sum_i a_i v_n b_i \neq 0$. 
Proof of Theorem 4. We will keep the notation of Theorem 3 in the following.

Firstly, assume that char $R = 0$: Then, by Theorem 3, $d = \text{ad}(-b)$ for some nilpotent $b \in Q$ with the nilpotency $l$, that is, $b^l = 0$ but $b^{l-1} \neq 0$. By Proposition 1, the center of $R_{\mathcal{F}}[x;d]$ is equal to $C^{(d)}[\zeta]$, where $\zeta = x + b$. The minimal polynomial of $b$ over $C^{(d)}$ is obviously $\lambda^l$, where $\lambda$ is a commuting indeterminate over $C^{(d)}$.

It follows from Theorem 1 that $\mathcal{A} = \langle \zeta \rangle$ and $\mathcal{P} = \langle \zeta \rangle$. By Lemma 3, $\mathcal{P}$ is prime, as asserted. We compute the ideal $\mathcal{M}$ described above: By Theorem 3, $m_d(R) = l$. Now, we look at the central generator of $\langle x^l \rangle$: Write $x = \zeta + b$. Noting that $b^l = 0$ and $\zeta$ is central, we have

$$x^l = (\zeta + b)^l = \zeta^l + \binom{l}{1} \zeta^{l-1}b + \ldots + \binom{l}{l-1} \zeta b^{l-1},$$

implying that $\langle x^l \rangle \subseteq \langle \zeta \rangle$. Since $1, b, \ldots, b^{l-1}$ are $C$–independent, by Lemma 5 there exist finitely many $r_i, r'_i \in I$ such that $\sum_i r_i b^j r'_i = 0$ for $0 \leq j < l - 1$ but $\sum_i r_i b^{l-1} r'_i \neq 0$. We have

$$\langle x^l \rangle \ni \sum_i r_i x^l r'_i = \left(\frac{l}{l-1}\right) \zeta \left(\sum_i r_i b^{l-1} r'_i\right) \neq 0.$$

This shows that $\zeta$ is the central generator of the ideal $\langle x^l \rangle$. Since $\mathcal{M}$ extends $\langle x^l \rangle$, the central generator of $\mathcal{M}$ divides the central generator $\zeta$ of $\langle x^l \rangle$. Since $\mathcal{M} \cap R = 0$, the central generator of $\mathcal{M}$ cannot be 1 and hence must be $\zeta$. But $\langle \zeta \rangle$ also extends $\langle x^l \rangle$ and intersects $R$ trivially. By the maximality of $\mathcal{M}$, it follows $\mathcal{M} = \langle \zeta \rangle = \mathcal{P}$.

Next, we assume char $R = p \geq 2$. Let $s$ be the least integer $\geq 1$ such that $d^s$, $0 \leq i \leq s$, are $C$–independent modulo $X$–inner derivations. Then, by Theorem 3, there exists $b \in Q$ such that $d^s = \text{ad}(-b)$ and such that the minimal polynomial of $b$ over $C$ assumes the form $(b^s - \alpha)^l = 0$, where $\alpha \in C$, $l, t \geq 0$ and $(l, p) = 1$. By Theorem 3 again, $m_d(R) = p^{s+l}$. Our next step is to find the central generator of the ideal $\langle x^m \rangle$, where $m = m_d(R) = p^{s+l}$. For this purpose, we must first decide $\zeta$ described in Proposition 1. Analogous to Lemma 1, we divide our argument into two cases:

Case 1. $d(b) \in d(C)$: By Lemma 1, we may assume that $d(b) = 0$ and so $\zeta = x^{p^s} + b$. Applying $d$ to $(b^s - \alpha)^l = 0$, we obtain

$$-l(b^s - \alpha)^{l-1} d(\alpha) = 0.$$

Since $l \not\equiv 0$ modulo $p$ and $(b^s - \alpha)^{l-1} \neq 0$, it follows $d(\alpha) = 0$. So $\zeta - \alpha$ is also in
the center of \( R[x; d] \). With this, we compute
\[
x^m = x^{p^{r+1}} = (\zeta - b)^{p^r} = (\zeta^{p^r} - b^{p^r})^l = ((\zeta^{p^r} - \alpha) - (b^{p^r} - \alpha))^l \\
= (\zeta^{p^r} - \alpha)^l - \binom{l}{1}(\zeta^{p^r} - \alpha)^{l-1}(b^{p^r} - \alpha) + \cdots \\
+ (-1)^{l-1}\binom{l}{l-1}(\zeta^{p^r} - \alpha)^{l-1}(b^{p^r} - \alpha)^l.
\]

Since \((b^{p^r} - \alpha) = 0\), we have \(x^m \in \langle \zeta^{p^r} - \alpha \rangle\) and hence \(x^m \subseteq \langle \zeta^{p^r} - \alpha \rangle\). On the other hand, since \(l\) is the nilpotency of \(b^{p^r} - \alpha\), the elements \(1, b^{p^r} - \alpha, \ldots, (b^{p^r} - \alpha)^{l-1}\) are \(C\)-independent. By Lemma 5, there exist \(r_i, r'_i \in I\) such that \(\sum_i r_i(b^{p^r} - \alpha)^j r'_i = 0\) for \(0 \leq j < l - 1\) but \(\sum_i r_i(b^{p^r} - \alpha)^{l-1} r'_i \neq 0\). Multiplying the above displayed expression of \(x^m\) by \(r_i, r'_i\) from the left and right respectively and adding them up, we have
\[
0 \neq \sum_i r_i x^m r'_i = l(\zeta^{p^r} - \alpha)\left(\sum_i r_i(b^{p^r} - \alpha)^{l-1} r'_i\right) \subseteq \langle x^m \rangle.
\]

The central generator of the ideal \(\langle x^m \rangle\) is thus \(\zeta^{p^r} - \alpha\).

Let \(u\) be the largest integer such that \(0 \leq u \leq t\) and \(\alpha^{1/p^u} \in C(d)\). Set \(\beta = \alpha^{1/p^u}\). Then \(\zeta^{p^r} - \alpha = (\zeta^{p^{r-u}} - \beta)^{p^u}\). Note that \(\lambda^{p^{r-u}} - \beta \in C(d)[\lambda]\) is irreducible. Since \(\mathcal{M} \supseteq \langle x^m \rangle\), the central generator of \(\mathcal{M}\) is a divisor of \((\lambda^{p^{r-u}} - \beta)^{p^u}\), say \((\lambda^{p^{r-u}} - \beta)^v\), where \(0 \leq v \leq p^u\). Also, since \(\mathcal{M} \cap R = 0\), \(v\) must be > 0. We have
\[
\mathcal{M} \subseteq \langle (\zeta^{p^{r-u}} - \beta)^v \rangle \subseteq \langle \zeta^{p^{r-u}} - \beta \rangle.
\]

Since \(\langle \zeta^{p^{r-u}} - \beta \rangle \cap R = 0\), it follows that \(\mathcal{M} = \langle \zeta^{p^{r-u}} - \beta \rangle\) by the maximality of \(\mathcal{M}\).

We now compute the ideals \(\mathcal{A}\) and \(\mathcal{P}\) by Theorem 1: Since the minimal polynomial of \(b\) over \(C(d)\) is \((\lambda^{p^r} - \alpha)^l = (\lambda^{p^{r-u}} - \beta)^{p^u l} \in C(d)[\lambda]\), the ideal \(\mathcal{A}\) is thus equal to
\[
\langle (\zeta^{p^{r-u}} - \beta)^{p^u l} \rangle.
\]

The only irreducible factor of \((\lambda^{p^{r-u}} - \beta)^{p^u l}\) is \(\lambda^{p^{r-u}} - \beta\). So the ideal \(\mathcal{P}\) is given by \(\langle \zeta^{p^{r-u}} - \beta \rangle\) and is hence equal to \(\mathcal{M}\), as asserted.

**Case 2.** \(d(b) \notin d(C)\): We have \(\zeta = x^{p^{r+1}} + b^p\) by Lemma 1. We claim \(t > 0\): Assume otherwise \(t = 0\). That is, \((b - \alpha)^l = 0\). Applying \(d\), we obtain
\[
l(b - \alpha)^{l-1}(d(b) - d(\alpha)) = 0.
\]

Since \(d(b) \notin d(C)\), \(d(b) - d(\alpha) \neq 0\). But \(l \neq 0\) modulo \(p\) by our assumption and \((b^{p^r} - \alpha)^{l-1} \neq 0\) by the minimality of \(l\). This contradiction shows \(t > 0\) as claimed.
Applying $d$ to $(b^t - \alpha)^l = 0$ and using $d(b) \in C$ and $t > 0$, we obtain $l(b^t - \alpha)^{l-1}d(\alpha) = 0$. It follows $d(\alpha) = 0$. So $\alpha$ is also in the center of $R[\alpha]$.

We compute analogously

\[
x^m = x^{p^{t+1}} = (\zeta - b^t)(b^t)^{p^{t-1}} = (\zeta^{p^{t-1}} - \alpha)^l = \left( (\zeta^{p^{t-1}} - \alpha) - (b^t - \alpha) \right)^l
\]

\[
= \left( \zeta^{p^{t-1}} - \alpha \right)^l - \binom{l}{1} \left( \zeta^{p^{t-1}} - \alpha \right)^{l-1} (b^t - \alpha) + \cdots
\]

\[
+ (-1)^{l-1} \binom{l}{l-1} \left( \zeta^{p^{t-1}} - \alpha \right) (b^t - \alpha)^{l-1} + (-1)^l \binom{l}{l} (b^t - \alpha)^l.
\]

As in Case 1, the central generator of $\langle x^m \rangle$ is $\zeta^{p^{t-1}} - \alpha$. We let $u$ be the largest integer such that $0 \leq u \leq t - 1$ and $\alpha^{1/p^u} \in C(d)$. Set $\beta = \alpha^{1/p^u}$. Then $\zeta^{p^{t-1}} - \alpha = (\zeta^{p^{t-1-u}} - \beta)^{p^u}$. Arguing as in Case 1, we have

\[
\mathcal{M} = \langle \zeta^{p^{t-1-u}} - \beta \rangle.
\]

The minimal polynomial of $b^t$ over $C(d)$ is $\langle (\lambda^{p^{t-1}} - \alpha)^l = (\lambda^{p^{t-1-u}} - \beta)^{p^u} \rangle \in C(d)[\lambda]$. By Theorem 1, $\mathcal{A}$ is equal to

\[
\langle (\zeta^{p^{t-1-u}} - \beta)^{p^u} \rangle.
\]

Since the only irreducible factor of $(\lambda^{p^{t-1-u}} - \beta)^{p^u}$ is $\lambda^{p^{t-1-u}} - \beta$, the ideal $\mathcal{P}$ is given by $\langle \zeta^{p^{t-1-u}} - \beta \rangle$ and is also equal to $\mathcal{M}$, as asserted.

References


