ABSTRACT DERIVATIONS

A STUDY IN CONNECTION WITH HOMOMORPHISMS, ALGEBRAIC SEPARABILITY, AND PURELY INSEPARABLE ALGEBRAIC FIELD EXTENSIONS OF EXPONENT ONE

by

ALISTER O'BRIEN CAMPBELL

A Thesis presented to the University of Manitoba in partial fulfilment of the requirements for the degree of Master of Science

February, 1968

INTRODUCTION

Throughout our considerations we shall presuppose a knowledge of the basic concepts of modern abstract algebra. In particular, we shall presuppose a knowledge of vector spaces, rings and ideals, elementary Galois theory of field extensions, the construction (intrinsic) of a tensor product of algebras as in, for example, Zariski and Samuel [12]. Unless otherwise stated, we shall assume that rings (subrings) are commutative with identity $1 \neq 0$, and that algebras are associative with identity $1 \neq 0$.

The first section deals with some properties of derivations and gives their connections with extensions of algebra homomorphisms and separable and inseparable algebraic extensions. In the second section we introduce the notion of p-dependence and give further discussions on derivation algebras. In both these sections, there are worked exercises from Jacobson [9], some of which lead to results due to Baer and Hochschild. We also derive an analogue to the normal basis theorem. In the third section we derive a Galois type correspondence between subfields Φ of a given field P which is purely inseparable of exponent one over Φ, $[P:\Phi] < \infty$, and derivation algebras which are finite dimensional over Φ. In the fourth section we introduce the notion of higher derivations (of finite rank) and examine briefly higher derivations of purely inseparable fields P over Φ. We include the case where P is a tensor product of simple extensions.

Finally, and without in any way making him responsible for the contents of this work, I should like to take this opportunity to publicly thank Dr. K. W. Armstrong most of all for the criticisms he made and the encouragement I received during the preparation of this thesis.

SECTION I

Definition 1.1. A non-associative (= not necessarily associative) algebra $\mathfrak{A}$ over a field Φ, usually denoted by $\mathfrak{A}/\Phi$, is a vector space over Φ in which a product $xy \in \mathfrak{A}$ is defined for x, y in $\mathfrak{A}$ such that

(1) $(x_1 + x_2)y = x_1 y + x_2 y, \; x(y_1 + y_2) = xy_1 + xy_2$

(2) $\alpha(xy) = (\alpha x)y = x(\alpha y), \quad \alpha \in \Phi$

An algebra $\mathfrak{A}$ is called associative if its multiplication satisfies the associative law

$$(xy)z = x(yz) , \quad x, y, z \text{ in } \mathfrak{A}.$$

We recall that a sub-algebra of $\mathfrak{A}$ is a subspace of $\mathfrak{A}$ which is also a subring. Observe that $\Phi[x_1 , \ldots , x_n]$, the ring of polynomials in the n indeterminates $x_1 , \ldots , x_n$ with coefficients in Φ is an algebra (commutative) over Φ. For this reason, $\Phi[x_1 , \ldots , x_n]$ and $\Phi(x_1 , \ldots , x_n)$, the field of rational functions of $\Phi[x_1 , \ldots , x_n]$ are frequently referred to as algebras over Φ.

Definition 1.2. A non-associative algebra $\mathfrak{A}$ is called a Lie algebra if its multiplication satisfies the Lie conditions

(3) $x^2 = 0 , \quad (xy)z + (yz)x + (zx)y = 0 .$

The second condition is the so-called Lie-Jacobi identity.

Definition 1.3. If $\mathfrak{A}/\Phi$ is a sub-algebra of an algebra $\mathfrak{B}/\Phi$, a derivation D of $\mathfrak{A}/\Phi$ into $\mathfrak{B}/\Phi$ is a mapping of $\mathfrak{A}/\Phi$ into $\mathfrak{B}/\Phi$ such that for x,y in $\mathfrak{A}$, α in Φ ,

(4) $(x + y)D = xD + yD, \quad (x\alpha)D = (xD)\alpha$

(5) $(xy)D = (xD)y + x(yD)$.

Condition (4) states that D is linear. If $\mathfrak{A} = \mathfrak{B}$, then we speak of a derivation in $\mathfrak{B}$ or a derivation of $\mathfrak{B}$ into itself. The mapping of the polynomial algebra $\Phi[x]$ into itself given by $f(x) \to f'(x)$ the formal derivative of $f(x)$ is clearly an example of a derivation in $\Phi[x]$.

Let $\mathrm{Der}_\Phi(\mathfrak{A},\mathfrak{B})$ denote the set of derivations of $\mathfrak{A}/\Phi$ into $\mathfrak{B}/\Phi$. Then $D \in \mathrm{Der}_\Phi(\mathfrak{A},\mathfrak{B})$ is a linear transformation of $\mathfrak{A}/\Phi$ into $\mathfrak{B}/\Phi$ satisfying the special condition (5). If D, D_1, D_2 are linear transformations of $\mathfrak{A}/\Phi$ into $\mathfrak{B}/\Phi$, $x \in \mathfrak{A}$, $\alpha \in \Phi$, define $D_1 \pm D_2$, $D\alpha$, D_1D_2 respectively by $x(D_1 \pm D_2) = xD_1 \pm xD_2$, $x(D\alpha) = (xD)\alpha$, and $x(D_1D_2) = (xD_1)(D_2)$. Thus $D_1 \pm D_2$, $D\alpha$, and D_1D_2, are linear transformations of $\mathfrak{A}/\Phi$ into $\mathfrak{B}/\Phi$. In particular, if $D_1, D_2 \in \mathrm{Der}_\Phi(\mathfrak{A},\mathfrak{B})$, $x,y \in \mathfrak{A}$, $\alpha \in \Phi$, we then have

$$\begin{aligned}(xy)(D_1 \pm D_2) &= (xy)D_1 \pm (xy)D_2\\ &= (xD_1)y + x(yD_1) \pm (xD_2)y + x(yD_2)\\ &= (xD_1 \pm xD_2)y + x(yD_1 \pm yD_2)\\ &= \{x(D_1 \pm D_2)\}y + x\{y(D_1 \pm D_2)\}\end{aligned}$$

and

$$\begin{aligned}(xy)D\alpha &= \{(xy)D\}\alpha = \{(xD)y + x(yD)\}\alpha\\ &= \{(xD)y\}\alpha + \{x(yD)\}\alpha\\ &= \{(xD)\alpha\}y + x\{(yD)\alpha\}\\ &= \{x(D\alpha)\}y + x\{y(D\alpha)\}\ .\end{aligned}$$

This shows that $D_1 \pm D_2$, $D\alpha$ belong to $\mathrm{Der}_\Phi(\mathfrak{A},\mathfrak{B})$.

Remark 1.1. Take $\mathfrak{A} = \mathfrak{B}$. Then we observe that $D\alpha$, $D_1 \pm D_2$ are derivations in $\mathfrak{B}$. However, it should not be inferred that $D_1 D_2$ is also a derivation in $\mathfrak{B}$. Indeed, it is clear that

$$\begin{aligned} (xy)(D_1 D_2) &= \{(xy)D_1\}D_2 = \{(xD_1)y + x(yD_1)\}D_2 \\ &= \{(xD_1)y\}D_2 + \{x(yD_1)\}D_2 \\ &= x(D_1 D_2)y + (xD_1)(yD_2) + (xD_2)(yD_1) + x\{y(D_1 D_2)\} \end{aligned}$$

Hence $(xy)(D_1 D_2) \neq \{x(D_1 D_2)\}y + x\{y(D_1 D_2)\}$ for all x,y in $\mathfrak{B}$. In view of this remark, we can say no more than Der $(\mathfrak{B},\mathfrak{B})$ = Der $(\mathfrak{B})$ is a subspace of $\mathfrak{L}(\mathfrak{B},\mathfrak{B}) = \mathfrak{L}(\mathfrak{B})$ the space of linear transformations in $\mathfrak{B}$.

Definition 1.4. Let $\mathfrak{A}$ be an associative algebra. If $D, D_1, D_2, \ldots$ belong to Der $\mathfrak{A}$, then the Lie product or additive commutator of D_1 and D_2 is given by $[D_1, D_2] = D_1 D_2 - D_2 D_1$. It is clear that $[D_1, D_2]$ belongs to $\mathfrak{L}(\mathfrak{A})$. We next observe that the following relation is satisfied

$$(6) \qquad [D,D] = 0; \quad \big[[D_1,D_2], D_3\big] + \big[[D_2,D_3], D_1\big] + \big[[D_3,D_1], D_2\big] = 0$$

The first part of the relation (6) is evident. The second part follows immediately since

$$\begin{aligned} \big[[D_1,D_2], D_3\big] &= [(D_1 D_2 - D_2 D_1), D_3] \\ &= (D_1 D_2 - D_2 D_1)D_3 - D_3(D_1 D_2 - D_2 D_1) \\ &= D_1 D_2 D_3 - D_2 D_1 D_3 - D_3 D_1 D_2 + D_3 D_2 D_1 \\ \big[[D_2,D_3], D_1\big] &= (D_2 D_3 - D_3 D_2)D_1 - D_1(D_2 D_3 - D_3 D_2) \\ &= D_2 D_3 D_1 - D_3 D_2 D_1 - D_1 D_2 D_3 + D_1 D_3 D_2 \\ \big[[D_3,D_1], D_2\big] &= (D_3 D_1 - D_1 D_3)D_2 - D_2(D_3 D_1 - D_1 D_3) \\ &= D_3 D_1 D_2 - D_1 D_3 D_2 - D_2 D_3 D_1 + D_2 D_1 D_3 . \end{aligned}$$

We next observe that

$$\begin{aligned}
[D_1 + D_2, D_3] &= (D_1 + D_2)D_3 - D_3(D_1 + D_2) \\
&= D_1D_3 + D_2D_3 - D_3D_1 - D_3D_2 \\
&= D_1D_3 - D_3D_1 + D_2D_3 - D_3D_2 \\
&= [D_1, D_3] + [D_2, D_3] \qquad ,
\end{aligned}$$

$$\begin{aligned}
[D_1, D_2 + D_3] &= D_1(D_2 + D_3) - (D_2 + D_3)D_1 \\
&= D_1D_2 + D_1D_3 - D_2D_1 - D_3D_1 \\
&= [D_1, D_2] + [D_1, D_3]
\end{aligned}$$

and

$$\begin{aligned}
\alpha[D_1, D_2] &= \alpha(D_1D_2) - \alpha(D_2D_1) \\
&= (\alpha D_1)D_2 - D_2(\alpha D_1) = [\alpha D_1, D_2] \ .
\end{aligned}$$

Since $\alpha(D_1D_2) - \alpha(D_2D_1) = D_1(\alpha D_2) - (\alpha D_2)D_1 = [D_1, \alpha D_2]$, we must therefore have

$$\alpha[D_1, D_2] = [\alpha D_1, D_2] = [D_1, \alpha D_2] \text{ for any } \alpha \in \Phi \ .$$

We have already shown (cf. Remark 1.1) that

$$(xy)\, D_1D_2 = \{x(D_1D_2)\}y + (xD_1)(yD_2) + (xD_2)(yD_1) + x\{y(D_1D_2)\}.$$

Since this relation is clearly symmetrical in D_1 and D_2,

$$(xy)D_2D_1 = \{x(D_2D_1)\}y + (xD_2)(yD_1) + (xD_1)(yD_2) + x\{y(D_2D_1)\}.$$

Clearly $x\{y(D_1D_2)\} - x\{y(D_2D_1)\} = x\{y(D_1D_2) - y(D_2D_1)\}$

and $\{x(D_1D_2)\}y - \{x(D_2D_1)\}y = \{x(D_1D_2 - D_2D_1)\}y$.

Therefore $(xy)[D_1, D_2] = (x[D_1, D_2])y + x(y[D_1, D_2])$.

Hence D, D_1, D_2 belong to $\mathrm{Der}_{\Phi}(\mathfrak{A})$ and $\alpha \in \Phi$ together imply that $D_1 \pm D_2$, $D\alpha$, $[D_1, D_2]$ belong to $\mathrm{Der}_{\Phi}(\mathfrak{A})$. These observations lead to the following definition:

Definition 1.5. Der $\mathfrak{A}$ the set of derivations in the algebra $\mathfrak{A}$ is called the <u>Lie algebra of derivations</u> or simply the <u>derivation algebra</u> of $\mathfrak{A}$.

Let D be a derivation in $\mathfrak{A}$ and $x,y \in \mathfrak{A}$. Then induction on k gives the Leibniz rule

$$(7) \qquad (xy)D^k = (xD^k)y + \sum_{i=1}^{k-1} \binom{k}{i}(xD^i)(yD^{k-i}) + x(yD^k)$$

where $\binom{k}{i}$ is the usual binomial coefficient[1] $\dfrac{k(k-1)\ .\ .\ .\ (k-i+1)}{1.2\ .\ .\ .\ .\ i}$

Proof. Take $D^0 = 1$. Then (7) holds for $k = 1$ by definition. We may point out that if $D_1 = D_2$ in Remark 1.1, the formula (7) holds for $k = 2$. Let us now assume that (7) holds for all $k \leq n$. Since $(xy)D^{n+1} = \{(xy)D\}D^n = \{(xD)y + x(yD)\}D^n$, we now have

$$\begin{aligned}(xy)D^{n+1} &= \{(xD)y\}D^n + \{x(yD)\}D^n \\ &= (xD^{n+1})y + \sum_{i=1}^{n-1}\binom{n}{i}(xD^{i+1})(yD^{n-i}) + (xD)(yD^n) \\ &\quad + (xD^n)(yD) + \sum_{j=1}^{n-1}\binom{n}{j}(xD^j)(yD^{n+1-j}) + x(yD^{n+1}) \\ &= (xD^{n+1})y + \sum_{k=1}^{n}(xD^h)(yD^{n+1-h})\left(\binom{n}{h} + \binom{n}{h-1}\right) + x(yD^{n+1})\ .\end{aligned}$$

Since $\binom{n}{h} + \binom{n}{h-1} = \binom{n+1}{h}$, we now have

---

[1]This coefficient will be assumed to be a rational integer.

$$(xy)D^{n+1} = (xD^{n+1})y + \sum_{i=1}^{n} \binom{n+1}{i}(xD^i)(yD^{n+1-i}) + x(yD^{n+1}) .$$

Thus (7) holds for all rational integers $k = 1,2, \ldots .$

If the characteristic of Φ is 0 we can divide (7) by $k!$ and obtain the relation

$$(8) \qquad (xy)\frac{D^k}{k!} = \frac{(xD^k)y}{k!} + \sum_{i=1}^{k-1}\left(\frac{xD^i}{i!}\right)\left(\frac{yD^{k-i}}{(k-i)!}\right) + \frac{x(yD^k)}{k!}$$

$$= \sum_{i=0}^{k}\left(\frac{xD^i}{i!}\right)\left(\frac{yD^{k-i}}{(k-i)!}\right)$$

We shall now give a direct connection between derivations and automorphisms. Let $\mathfrak{A}$ be the polynomial algebra $\Phi[x]$ where Φ is a field of characteristic 0. Let a derivation D in $\mathfrak{A}$ be defined by $f(x)D = f'(x)$ the formal derivative of $f(x) \in \Phi[x]$. Consider the series

$$G = \exp D = 1 + \frac{D}{1!} + \frac{D^2}{2!} + \cdots .$$

If $f(x)$ is of degree n, then $f(x)\, D^{n+1} = 0$. Hence the series $f(x)G$ converges. We assert that $f(x)G = f(x+1)$.

Let us set $f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n$.

$$\begin{aligned}\text{Then } f(x)G = {} & a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n \\ & + a_0\binom{n}{1}x^{n-1} + a_1\binom{n-1}{1}x^{n-2} + a_2\binom{n-2}{1}x^{n-3} + \cdots + a_{n-2}\binom{2}{1}x + a_{n-1} \\ & + a_0\binom{n}{2}x^{n-2} + a_1\binom{n-1}{2}x^{n-3} + a_2\binom{n-2}{2}x^{n-4} + \cdots + a_{n-2} \\ & + a_0\binom{n}{3}x^{n-3} + a_1\binom{n-1}{3}x^{n-4} + \cdots \\ & \cdots\cdots\cdots + a_0\end{aligned}$$

Rearranging the terms, we now have

$$f(x)G = a_0x^n + a_0\binom{n}{1}x^{n-1} + a_0\binom{n}{2}x^{n-2} + \ldots . + a_0$$

$$+ a_1x^{n-1} + a_1\binom{n-1}{1}x^{n-2} + \ldots + a_1 + \ldots$$

$$\ldots\ldots\ldots\ldots + a_n$$

$$= a_0(x+1)^n + a_1(x+1)^{n-1} + \ldots . + a_n = f(x+1) \in \Phi[x]$$

This shows that $f(x-1)G = f(x)$, whence G is onto.

Since the map D is linear, it is clear that the map G is also linear. Consequently, in order to show that $\big(f(x)\ h(x)\big)G = f(x)G \cdot h(x)G$, we need only verify this statement for $f(x) = x^r$ and $h(x) = x^s$, $0 \le r,s$. We have seen that $f(x)G = (x+1)^r$ and $h(x)G = (x+1)^s$. Therefore $\big(f(x)\ h(x)\big)G = x^{r+s}G = (x+1)^{r+s} = f(x)G \cdot h(x)G$. Finally, we assert that the kernel of the map G is the zero polynomial. Let $h(x) = b_mx^m + \ldots + b_1x + b_0$ be an arbitrary non-zero polynomial of degree m. Then $b_m \neq 0$. Hence $h(x-1) = b_m(x-1)^m + \ldots + b_1(x-1) + b_0$ is also a non-zero polynomial of degree m. This shows that the kernel of the map G is the zero polynomial. We have thus shown that exp D is an automorphism of $\Phi[x]$.

Definition 1.6. Let Φ be a field of characteristic p (= 0 or otherwise). A <u>restricted Lie algebra</u> of characteristic p is an algebra $\mathfrak{L}_p$ over Φ in which the multiplication $[x,y]$ satisfies

$$[x,y] = -[y,x]$$

$$\big[[x,y],z\big] + \big[[y,z],x\big] + \big[[z,x],y\big] = 0 \quad ,$$

and for every y in $\mathfrak{R}_p$ there exists an element called y^p such that

$$\underbrace{\left[\cdots\left[[x,y],y\right],\cdots\cdots y\right]}_{p\text{ times}} = [x,y^p] \text{ for any } x \in \mathfrak{R}.$$

A restricted subalgebra $\mathfrak{R}_p'$ of $\mathfrak{R}_p$ is a subalgebra containing y^p for every y in $\mathfrak{R}_p'$. Similarly we define a restricted ideal, etc. It should not be inferred that this element y^p is necessarily an ordinary p-th power since multiplication is not necessarily associative. If $p \neq 2$, $[x,x] = 0$ for all $x \in \mathfrak{R}_p$ and $\mathfrak{R}_p$ is then a Lie algebra.

Exercise 1.1. Let $\mathfrak{A}$ be an (associative) algebra over Φ and $d \in \mathfrak{A}$. Verify that the mapping $I_d : a \to [a,d] = ad - da$ is a derivation in $\mathfrak{A}$. Such a mapping is called an <u>inner derivation</u> in $\mathfrak{A}$. Prove that

$$I_{\alpha_1 d_1 + \alpha_2 d_2} = \alpha_1 I_{d_1} + \alpha_2 I_{d_2}, \quad \alpha_i \in \Phi, \quad \text{and}$$

$$I_{[d_1, d_2]} = [I_{d_1}, I_{d_2}].$$ Show that if Φ is of characteristic $p \neq 0$, then $I_{d^p} = (I_d)^p$.

Proof. Let $a,b \in \mathfrak{A}$, $a \neq 0$. Then we have

$$\begin{aligned}(ab)I_d &= (ab)d - d(ab)\\ &= abd - adb + adb - dab\\ &= a(bd - db) + (ad - da)b\\ &= a(b\,I_d) + (a\,I_d)b\end{aligned}$$

Since I_d is evidently linear, I_d is a derivation in $\mathfrak{A}$.

Now $a\, I_{\alpha_1 d_1 + \alpha_2 d_2} = a(\alpha_1 d_1 + \alpha_2 d_2) - (\alpha_1 d_1 + \alpha_2 d_2)a$

$$= a\,\alpha_1 d_1 - \alpha_1 d_1 a + a\,\alpha_2 d_2 - \alpha_2 d_2 a$$

$$= a(I_{\alpha_1 d_1} + I_{\alpha_2 d_2}) .$$

Since $a\, I_{\alpha d} = a(\alpha d) - (\alpha d)a$

$$= \alpha(ad) - \alpha(da) = \alpha(ad - da)$$

implies that $I_{\alpha d} = \alpha\, I_d$, we must have

$$I_{\alpha_1 d_1 + \alpha_2 d_2} = \alpha_1 I_{d_1} + \alpha_2 I_{d_2} .$$

Next, $a\, I_{[d_1 , d_2]} = a[d_1 , d_2] - [d_1 , d_2]a$

$$= ad_1 d_2 - ad_2 d_1 - d_1 d_2 a + d_2 d_1 a$$

$$= ad_1 d_2 - d_1 ad_2 - d_2 ad_1 + d_2 d_1 a$$

$$+ d_2 ad_1 - ad_2 d_1 + d_1 ad_2 - d_1 d_2 a$$

$$= (ad_1 - d_1 a)d_2 - d_2 (ad_1 - d_1 a)$$

$$- (ad_2 - d_2 a)d_1 + d_1 (ad_2 - d_2 a)$$

$$= (a\, I_{d_1})I_{d_2} - (a\, I_{d_2})I_{d_1}$$

$$= a(I_{d_1} I_{d_2} - I_{d_2} I_{d_1}) = a[I_{d_1} , I_{d_2}] .$$

Hence $I_{[d_1 , d_2]} = [I_{d_1} , I_{d_2}]$

It is clear that $a\, I_{d^p} = [a, d^p]$ and that

$a(I_d)^p = \Big[\, . \, . \, . \, . \, . \, \overbrace{[[a,d],d], \, . \, . \, . \, . \, . \, . \, d}^{p \text{ times}} \Big]$. Let d_R denote the mapping $a \to ad$ and d_L denote the mapping $a \to da$. Clearly $I_d = d_R - d_L$ and $a(d_R d_L) = (ad_R)d_L = d(ad) = (da)d = (ad_L)d_R$. We note that $a(I_d)^2 = [(ad - da), d] = ad^2 - 2dad + d^2 a$.

Let us assume that

$$(8') \qquad a(I_d)^k = ad^k + \sum_{i=1}^{k-1} \binom{k}{i} (-d)^i ad^{k-i} + (-d)^k a \text{ for all } 1 \le k \le n.$$

Then

$$a(I_d)^{n+1} = \left(ad^n + \sum_{i=1}^{n-1} \binom{n}{i} (-d)^i ad^{n-i} + (-d)^n a\right) d$$

$$- d\left(ad^n + \sum_{i=1}^{n-1} \binom{n}{i} (-d)^i ad^{n-i} + (-d)^n a\right)$$

$$= ad^{n+1} + \sum_{j=1}^{n} \left(\binom{n}{j} + \binom{n}{j-1}\right) (-d)^j ad^{n+1-j} + (-d)^{n+1} a$$

$$= ad^{n+1} + \sum_{j=1}^{n} \binom{n+1}{j} (-d)^j ad^{n+1-j} + (-d)^{n+1} a$$

This shows that (8′) holds for all $k = 1,2, \ldots$ In particular, if $k = p$, $\binom{k}{i} = 0$ for each $i = 1, 2, \ldots, p - 1$. Hence $a(I_d)^p = ad^p + (-d)^p a$. We know that $p = 2$ or p is odd. If $p = 2$, $y^2 = -y^2$ for all $y \in \mathfrak{A}$. If p is odd, $(-d)^p = -d^p$. Hence $(I_d)^p = I_{d^p}$ or equivalently

$$\Big[\ldots\ldots \overbrace{\big[[a,d],d\big], \ldots\ldots d}^{p \text{ times}} \Big] = [a,d^p].$$

We may here comment that if D, D_1 are elements of $Der_\Phi(\mathfrak{A})$, $\mathfrak{A}$ an algebra over Φ with characteristic $p \neq 0$, the above method shows that

$$(9) \qquad \Big[\ldots\ldots \overbrace{\big[[D_1,D], D\big], \ldots\ldots D}^{p \text{ times}} \Big] = [D_1, D^p]$$

In this case ($p \neq 0$), Leibniz's rule (7) reduces to

$$(xy)D^p = (xD^p)y + x(yD^p)$$

and so implies that $D^p \in \mathrm{Der}_\Phi(\mathfrak{A})$. Hence $\mathrm{Der}_\Phi(\mathfrak{A})$ is a restricted Lie algebra of characteristic $p \neq 0$.

Remark 1.2. Following upon the results of Exercise 1.1, it can be shown that $\mathcal{J}(\mathfrak{A})$ the set of inner derivations in $\mathfrak{A}$ is a restricted right ideal in Der $(\mathfrak{A})$. It remains to show that $I_{dD} = [I_d, D]$ is in $\mathcal{J}(\mathfrak{A})$, where $D \in$ Der $(\mathfrak{A})$, $d \in \mathfrak{A}$.

Proof. We have seen that $I_d = d_R - d_L$. By definition, $(da)D = (dD)a + d(aD)$. Put otherwise, $(da)D - d(aD) = (dD)a$. This can be written in operator form as $[d_L, D] = (dD)_L$. Similarly, $(ad)D - (aD)d = a(dD)$ can be written as $[d_R, D] = (dD)_R$. Hence we obtain the relation

$$\begin{aligned}(dD)_R - (dD)_L &= (d_R D - Dd_R) - (d_L D - Dd_L) \\ &= (d_R - d_L)D - D(d_R - d_L) = [(d_R - d_L), D]\end{aligned}$$

Since $(dD)_R - (dD)_L = I_{dD}$, we now have $I_{dD} = [I_d, D]$.

Remark 1.3. Let c be an element of the centre of $\mathfrak{B}$ (i.e., $cx = xc$ for all x in $\mathfrak{B}$) and $D \in \mathrm{Der}_\Phi(\mathfrak{A}, \mathfrak{B})$. Let c_R denote the mapping $x \to xc$ in $\mathfrak{B}$. Then $\mathrm{Der}_\Phi(\mathfrak{A}, \mathfrak{B})$ is closed under right multiplication by c_R.

It is clear that

$$\begin{aligned}(x + y)D\, c_R &= \big((x + y)D\big)c_R = (xD + yD)c_R \\ &= x\,D\,c_R + y\,D\,c_R.\end{aligned}$$

If $\alpha \in \Phi$,

$$\begin{aligned}(x\alpha)\,D\,c_R &= \big((x\alpha)D\big)\,c_R = \big((xD)\alpha\big)\,c \\ &= \big((xD)c\big)\,\alpha = (x\,D\,c_R)\,\alpha\end{aligned}$$

Hence $D\,c_R$ is linear. If y is an element of $\mathfrak{A}$, we also have

$$(xy)D\,c_R = \Big((xD)y + x(yD)\Big)c_R = (xD)yc + x(yD)c$$

$$= (xD)cy + x(yD)c = (x\,D\,c_R)y + x(y\,D\,c_R)\ .$$

Therefore $D\,c_R$ is an element of $\mathrm{Der}_\Phi(\mathfrak{A},\mathfrak{B})$.

This result may be specialized for the case $\mathfrak{A} = \mathfrak{B}$ where $\mathfrak{B}$ is a field P over Φ. Moreover, without specifying which field is the base field of P, we observe that Der (P) is closed under right multiplication by elements ρ_R, $\rho \in P$.

In order to give another connection between derivations and homomorphisms, let us construct the so-called algebra of dual numbers. Recall that if (x^2) is the principal ideal generated by x^2 over the base field Φ, then $1 + (x^2)$ and $x + (x^2)$ form a basis for the algebra $\Phi[x]\ /\ (x^2)$ over Φ. Let us denote the coset $x + (x^2)$ in $\Phi[x]\ /\ (x^2)$ by t and set $\mathfrak{C} = \Phi[x]\ /\ (x^2)$. Then $\mathfrak{C}$ is an associative algebra with basis (1,t) over Φ and the multiplication rule $t^2 = 0$. If $\mathfrak{B}$ is an arbitrary (associative) algebra over Φ, form the algebra (= Kronecker or tensor product) $\mathfrak{B} \otimes \mathfrak{C}$ over Φ (see, e.g. Zariski and Samuel [12], pp. 182-183). Here, multiplication is defined by

$$(b_1 \otimes u_1)(b_2 \otimes u_2) = b_1 b_2 \otimes u_1 u_2\ ,\ b_i \in \mathfrak{B},\ u_i \in \mathfrak{C}\ .$$

In particular, $(b \otimes 1)(1 \otimes t) = b \otimes t$ and $(1 \otimes b)(t \otimes 1) = t \otimes b$. Since $b \otimes 1 = 1 \otimes b$ and $1 \otimes t = t \otimes 1$, we must therefore have $b \otimes t = t \otimes b$. If we identify $\mathfrak{B}$ with the subalgebra of the elements $b \otimes 1$, $b \in \mathfrak{B}$ and identify $\mathfrak{C}$ with the subalgebra of the elements $1 \otimes u$, $u \in \mathfrak{C}$, then the elements of $\mathfrak{B} \otimes \mathfrak{C}$ can be uniquely written as $b_1 + b_2 t$, $b_i \in \mathfrak{B}$. This follows readily from the fact that any element of $\mathfrak{C}$ can be uniquely written as $\alpha_1 + \alpha_2 t$, $\alpha_i \in \Phi$. In $\mathfrak{B} \otimes \mathfrak{C}$ we now have $bt = tb$ and the multiplication rule

$$(10) \qquad (b_1 + b_2 t)(b_3 + b_4 t) = b_1 b_3 + (b_1 b_4 + b_2 b_3) t , \qquad b_i \in \mathfrak{B} .$$

The algebra $\mathfrak{B} \otimes \mathfrak{C}$ is called the algebra of dual numbers over $\mathfrak{B}$. This construction shows that if $\mathfrak{B}$ is an arbitrary (associative) algebra, then $\mathfrak{B}$ is indeed a subalgebra of an (associative) algebra $\mathfrak{T}$ in which there is an element t such that $t^2 = 0$, $bt = tb$ for all $b \in \mathfrak{B}$, and every element $u \in \mathfrak{T}$ can be uniquely written as $b_1 + b_2 t$, $b_i \in \mathfrak{B}$.

Let D be a derivation of $\mathfrak{A}$ into $\mathfrak{B}$. Define a mapping $s = s(D)$ of $\mathfrak{A}$ into $\mathfrak{B} \otimes \mathfrak{C}$ by

$$(11) \qquad a \to a^s \equiv a + (aD)t$$

Then
$$\begin{aligned}(a + b)^s &= (a + b) + \big((a + b)D\big)t, \qquad a,b \in \mathfrak{A} \\ &= (a + b) + (aD + bD)t = a + (aD)t + b + (bD)t \\ &= a^s + b^s ,\end{aligned}$$

and
$$\begin{aligned}(a\alpha)^s &= a\alpha + \big((a\alpha)D\big)t \qquad , \quad \alpha \in \Phi , \\ &= a\alpha + \big((aD)\alpha\big)t = a\alpha + (aD)t\alpha \\ &= \big(a + (aD)t\big)\alpha = a^s\alpha .\end{aligned}$$

Hence the mapping s is linear. Furthermore, we have

$$\begin{aligned}a^s b^s &= \big(a + (aD)t\big)\big(b + (bD)t\big) = ab + a(bD)t + (aD)tb \\ &= ab + \big(a(bD) + (aD)b\big)t = ab + \big((ab)D\big)t = (ab)^s .\end{aligned}$$

Hence the mapping s is a homomorphism of $\mathfrak{A}$ into $\mathfrak{B} \otimes \mathfrak{C}$. Let us now consider a mapping π of $\mathfrak{B} \otimes \mathfrak{C}$ into $\mathfrak{B}$ given by

$$(a + bt) \to (a + bt)^\pi = a, \qquad a,b \in \mathfrak{B} .$$

Then $(a + bt)^\pi(c + dt)^\pi = ac = \big((a + bt)(c + dt)\big)^\pi$ by rule (10). It is clear that the mapping π is linear. Hence the mapping π is a homomorphism of $\mathfrak{B} \otimes \mathfrak{C}$ into $\mathfrak{B}$ which is the identity on $\mathfrak{B}$. In particular, if $a \in \mathfrak{A}$ and the mapping s is defined as in (11), then $a^{s\pi} = \left(a + (aD)t\right)^{\pi} = a$. This shows that the mapping s is one-to-one (1 - 1), since $a_1{}^{s} = a_2{}^{s}$ would imply that $a_1{}^{s\pi} = a_2{}^{s\pi}$, that is $a_1 = a_2$.

Conversely, let s be any homomorphism of $\mathfrak{A}$ into $\mathfrak{B} \otimes \mathfrak{C}$ such that $a^{s\pi} = a$, $a \in \mathfrak{A}$. Then we have $a^{s} = a + bt$, $a \in \mathfrak{B}$, $b \in \mathfrak{B}$. The uniqueness of the form a + bt implies that b is uniquely determined by a. Hence, we have the mapping $D: a \to b$ and we may write $a^{s} = a + (aD)t$. We shall now prove that D is a derivation of $\mathfrak{A}$ into $\mathfrak{B}$.

Proof. Since the mapping s is linear, $(a + c)^{s} = a^{s} + c^{s}$.

Therefore $(a + c) + \left((a + c)D\right)t = a^{s} + c^{s} = \left(a + (aD)t\right) + \left(c + (cD)t\right)$

$$= (a + c) + \left((aD) + (cD)\right)t \ .$$

Hence $(a + c)D = aD + cD$. We also have $(a\alpha)^{s} = a^{s}\alpha$.

Therefore $a\alpha + \left((a\alpha)D\right)t \ = \ a^{s}\alpha \ = \ \left(a + (aD)t\right)\alpha \ , \ \alpha \in \Phi$

$$= a\alpha + \left((aD)\alpha\right)t \ .$$

We have therefore shown that D is linear. Since $a^{s}c^{s} = (ac)^{s}$ for all $a, c, \in \mathfrak{A}$,

$$\left(a + (aD)t\right)\left(c + (cD)t\right) = ac + \left((aD)c\right)t + \left(a(cD)\right)t$$

$$= (ac)^{s} = ac + \left((ac)D\right)t \ .$$

Hence $(ac)D = (aD)c + a(cD)$. This completes the proof that D is a derivation of $\mathfrak{A}$ into $\mathfrak{B}$.

We can therefore state the following result (cf. Jacobson [9],

p. 169).

Theorem 1.A. If $\mathfrak{A}$ is a subalgebra of $\mathfrak{B}$ and D is a derivation of $\mathfrak{A}$ into $\mathfrak{B}$, then $s : a \to a + (aD)t$ is an isomorphism of $\mathfrak{A}$ into the algebra of dual numbers $\mathfrak{B} \otimes \mathfrak{C}$ over $\mathfrak{B}$ such that $a^{s\pi} = a$. Conversely, any homomorphism of $\mathfrak{A}$ into $\mathfrak{B} \otimes \mathfrak{C}$ satisfying this condition has the form

$a \to a + (aD)t$ where D is a derivation of $\mathfrak{A}$ into $\mathfrak{B}$.

Here the author [9] gives two consequences of this connection between derivations and isomorphisms. First, if two derivations coincide on a set X of generators of $\mathfrak{A}$, these derivations are identical. Secondly, if s is a homomorphism of $\mathfrak{A}$ into $\mathfrak{B} \otimes \mathfrak{C}$ such that $x^{s\pi} = x$ for $x \in X$, then $a^{s\pi} = a$ for all $a \in \mathfrak{A}$. Hence s defines a derivation D in the manner indicated.

Exercise 1.2. Let $\mathfrak{A}$ be a subalgebra of an algebra $\mathfrak{B}$. Verify that the mapping D of $\mathfrak{A}$ into $\mathfrak{B}$ is a derivation if and only if the mapping

$$s : a \to \begin{bmatrix} a & aD \\ 0 & a \end{bmatrix}$$

of $\mathfrak{A}$ into the matrix algebra $\mathfrak{B}_2$ of 2×2 matrices over $\mathfrak{B}$ is an isomorphism.

Proof. Suppose that D is a derivation of $\mathfrak{A}$ into $\mathfrak{B}$ and $a,b \in \mathfrak{B}$. We then have

$$(a + b)^s = \begin{bmatrix} (a + b) & (a + b)D \\ 0 & a + b \end{bmatrix} = \begin{bmatrix} a + b & aD + bD \\ 0 & a + b \end{bmatrix}$$

$$= \begin{bmatrix} a & aD \\ 0 & a \end{bmatrix} + \begin{bmatrix} b & b_D \\ 0 & b \end{bmatrix} = a^s + b^s ,$$

$$(a\alpha)^s = \begin{bmatrix} a\alpha & (a\alpha)D \\ 0 & a\alpha \end{bmatrix} = \begin{bmatrix} a\alpha & (aD)\alpha \\ 0 & a\alpha \end{bmatrix}$$

$$= \begin{bmatrix} a & aD \\ 0 & a \end{bmatrix} \begin{bmatrix} \alpha\cdot 1 & 0 \\ 0 & \alpha\cdot 1 \end{bmatrix} = a^s\cdot\alpha ,$$

and $$(ab)^s = \begin{bmatrix} ab & (ab)D \\ 0 & ab \end{bmatrix} = \begin{bmatrix} ab & (aD)b + a(bD) \\ 0 & ab \end{bmatrix}$$

$$= \begin{bmatrix} a & aD \\ 0 & a \end{bmatrix} \begin{bmatrix} b & bD \\ 0 & b \end{bmatrix} = a^s b^s$$

We also have

$$\begin{bmatrix} a & aD \\ 0 & a \end{bmatrix} = \begin{bmatrix} b & bD \\ 0 & b \end{bmatrix}$$

if and only if a = b. Hence the mapping s is an isomorphism of $\mathfrak{A}$ into $\mathfrak{B}_2$.

Conversely, suppose that s is an isomorphism. It is clear that the linearity of s implies that D is linear. Since we have

$$(ab)^s = \begin{bmatrix} ab & (ab)D \\ 0 & ab \end{bmatrix} = a^s b^s$$

$$= \begin{bmatrix} a & aD \\ 0 & a \end{bmatrix} \begin{bmatrix} b & bD \\ 0 & b \end{bmatrix} = \begin{bmatrix} ab & (aD)b + a(bD) \\ 0 & ab \end{bmatrix} ,$$

we must therefore have (ab)D = (aD)b + a(bD). We have thus proved that D is a derivation of $\mathfrak{A}$ into $\mathfrak{B}$.

Definition 1.7. An element c of a subalgebra $\mathfrak{A}$ of an algebra $\mathfrak{B}$ whose image under a derivation D of $\mathfrak{A}$ into $\mathfrak{B}$ is zero is called a D-constant.

Remark 1.4. The relation (11) implies that an element $c \in \mathfrak{A}$ is a D-constant if and only if $c^s = c$ for the isomorphism $s = s(D)$.

Remark 1.5. The set of D-constants form a subalgebra of $\mathfrak{A}$ with identity $1 \neq 0$.

Proof. It is clear that $1^2 = 1$ implies that $1^2D = (1D)1 + 1(1D) = 1D$. Hence $1D = 0$ for every derivation D of $\mathfrak{A}$ into $\mathfrak{B}$. Let $a,b \in \mathfrak{A}$ be D-constants and $\alpha \in \Phi$. Then $(a \pm b)D = aD \pm bD = 0$, $(a\alpha)D = (aD)\alpha = 0$ and $(ab)D = (aD)b + a(bD) = 0$.

Remark 1.6. If $\mathfrak{B}$ is commutative and Φ is of characteristic p, then every p-th power in $\mathfrak{A}$ is a D-constant.

Proof. By definition, $a^2 = a(aD) + (aD)a = 2a(aD)$ for all $a \in \mathfrak{A}$. It is clear that $a^3D = (a^2D)a + a^2(aD) = 2a(aD)a + a^2(aD) = 3a^2(aD)$. Let us assume that $a^kD = ka^{k-1}(aD)$ for all $k \leq n$. Then

$$a^{n+1}D = (a^nD)a + a^n(aD) = na^{n-1}(aD)a + a^n(aD)$$
$$= na^n(aD) + a^n(aD) = (n+1)\, a^n(aD).$$

It now follows by induction that

$$(12) \qquad a^kD = k\, a^{k-1}(aD), \qquad k = 1,2, \ldots .$$

Take $k = p$ and conclude that a^p is a D-constant.

Remark 1.7. If $\mathfrak{A} = P$ is a field over Φ, then the set of D-constants of P form a subfield Γ of P which contains Φ. Moreover, the trivial derivation $D = 0$ is the only derivation on Φ.

Proof. Since $\alpha D = (1 \cdot \alpha)D = (1D)\alpha = 0$ for all $\alpha \in \Phi$, $\Phi \subseteq \Gamma$. In view of Remark 1.5, it remains only to show that for all $a \neq 0$ in Γ, a^{-1} is also in Γ. This is clear since

$$0 = 1D = (a\, a^{-1})D = (aD)a^{-1} + a(a^{-1}D)$$

implies that

$$(13) \qquad a^{-1}D = -(aD)a^{-2}, \text{ for all } a \in \mathfrak{A}.$$

Hence $a \in \Gamma$, $a \neq 0$, implies that $a^{-1} \in \Gamma$. Since $\alpha D = 0$ for all $\alpha \in \Phi$ and for all D in $\mathrm{Der}_{\Phi}(P)$, $D = 0$ is the only derivation on Φ.

Exercise 1.3. Let D be a derivation in P/Φ, Γ the subfield of D-constants of P over Φ. Prove that the elements $\rho_1, \rho_2, \ldots, \rho_m$ of P are linearly independent over Γ if and only if the so-called Wronskian determinant

$$\Delta = \begin{vmatrix} \rho_1 & \rho_2 & \cdots & \rho_r & \cdots & \rho_m \\ \rho_1 D & \rho_2 D & \cdots & \rho_r D & \cdots & \rho_m D \\ \vdots & \vdots & & \vdots & & \vdots \\ \rho_1 D^{r-1} & \rho_2 D^{r-1} & \cdots & \rho_r D^{r-1} & \cdots & \rho_m D^{r-1} \\ \vdots & \vdots & & \vdots & & \vdots \\ \rho_1 D^{m-1} & \rho_2 D^{m-1} & \cdots & \rho_r D^{m-1} & \cdots & \rho_m D^{m-1} \end{vmatrix} = 0$$

In order to prove that this condition holds, we shall use the following lemma.[1]

[1] See, e.g., Scott, R. F. and Mathews, G. B., [11], pp. 36, 62-63.

Lemma 1.0. Let a_{tr} denote the element in the t-th row (column) and r-th column (row) of an $m \times m$ determinant (a_{ij}), A_{tr} denote the minor corresponding to a_{tr}, and Δ denote the value of the determinant. If δ_{rs} denotes the Kronecker delta ($\delta_{rs} = 1$, if $r = s$, and $\delta_{rs} = 0$, if $r \neq s$), then

$$(14) \quad \sum_t a_{tr} A_{ts} = \delta_{rs}\Delta .$$

Secondly, if

$$M = \begin{vmatrix} A_{ik} & A_{is} & \cdots & A_{if} \\ A_{rk} & A_{rs} & \cdots & A_{rf} \\ \vdots & \vdots & & \vdots \\ A_{tk} & A_{ts} & \cdots & A_{tf} \end{vmatrix}$$

is an $h \times h$ determinant and Δ^{*} is the complementary $(m - h) \times (m - h)$ determinant of

$$\Delta^{**} = \begin{vmatrix} a_{ik} & a_{is} & \cdots & a_{if} \\ a_{rk} & a_{rs} & \cdots & a_{rf} \\ \vdots & \vdots & & \vdots \\ a_{tk} & a_{ts} & \cdots & a_{tf} \end{vmatrix}$$

formed from Δ by deleting the h rows and h columns which contain the elements Δ^{**}, then we have the identity

$$(15) \quad \Delta^{h} \Delta^{*} = \Delta M$$

We next remark that Δ can be regarded as a polynomial in the m^2 variables a_{ij}, $1 \leq i,\ j \leq m$. Since, for example, the coefficient of

$a_{11} a_{22} \ldots a_{mm}$ is +1, Δ is a polynomial which is not identically zero. Hence the relation (15) is an identity in which each member is a polynomial in the m^2 variables a_{ij}, $1 \le i, j \le m$, with $\Delta \not\equiv 0$. Therefore, we obtain the relation

$$(15') \quad M = \Delta^{h-1}\Delta^* .$$

Proof (Exercise 1.3). We recall that $\rho_1, \rho_2, \ldots \rho_m$ are linearly dependent over Γ if and only if there exist $c_1, c_2, \ldots c_m$ in Γ, not all $c_i = 0$, such that $c_1\rho_1 + c_2\rho_2 + \ldots + c_m\rho_m = 0$. Let us assume that this condition holds. Write Δ briefly as $(1, D, \ldots, D^{m-1})|\rho_1, \rho_2, \ldots \rho_m|$ and denote the minor corresponding to $\rho_r D^{m-1}$ by the Wronskian Δ_r. If each $\rho_i \in \Gamma$, there is nothing to prove since $\rho_i D^k = 0$ for $k = 1, 2, \ldots, m-1$. We shall assume that not all $\rho_i \in \Gamma$. We next observe that $(c_i\rho_i)D = c_i(\rho_i D)$, $(c_i\rho_i)D^2 = \big(c_i(\rho_i D)\big)D = c_i(\rho_i D^2)$. If we assume that $(c_i\rho_i)D^k = c_i(\rho_i D^k)$ for all $k \le n$, then $(c_i\rho_i)D^{n+1} = \big((c_i\rho_i)D^n\big)D = \big(c_i(\rho_i D^n)\big)D = c_i(\rho_i D^{n+1})$ implies that $(c_i\rho_i)D^k = c_i(\rho_i D^k)$ for all $k = 1, 2, \ldots$. Hence

$$\begin{aligned}
c_1\rho_1 + c_2\rho_2 + \ldots + c_m\rho_m &= 0 \\
c_1(\rho_1 D) + c_2(\rho_2 D) + \ldots + c_m(\rho_m D) &= 0 \\
&\vdots \\
c_1(\rho_1 D^{m-1}) + c_2(\rho_2 D^{m-1}) + \ldots + c_m(\rho_m D^{m-1}) &= 0
\end{aligned}$$

is a system of m linear equations which has non-trivial solutions in the c_i. This shows that $\Delta = 0$.

Conversely, assume that $\Delta = 0$ but one of the Wronskians, say Δ_1, does not vanish. Let us write

$$\Delta_r = \begin{vmatrix} \rho_1 & \cdots & \rho_{r-1} & \rho_{r+1} & \cdots & \rho_m \\ \rho_1 D & \cdots & \rho_{r-1}D & \rho_{r+1}D & \cdots & \rho_m D \\ \vdots & & & & & \\ \rho_1 D^{m-2} & \cdots & \rho_{r-1}D^{m-2} & \rho_{r+1}D^{m-2} & \cdots & \rho_m D^{m-2} \end{vmatrix}$$

as $(1, D, \ldots, D^{m-2})|\rho_1\rho_2 \ldots \hat{\rho}_r \ldots \rho_m|$. It follows directly from the rule for differentiating a determinant that $\Delta_r D = (1, D, \ldots, D^{m-3}, D^{m-1})|\rho_1\rho_2 \ldots \hat{\rho}_r \ldots \rho_m|$ which is the minor corresponding to $\rho_r D^{m-2}$. Similarly, $\Delta_s D$ is the minor corresponding to $\rho_s D^{m-2}$. From (15′), we see that $\Delta = 0$ implies that

$$(\Delta_r D)\Delta_s - \Delta_r(\Delta_s D) = \begin{vmatrix} \Delta_r D & \Delta_s D \\ \Delta_r & \Delta_s \end{vmatrix} = 0 \quad , \quad r,s = 1,2, \ldots, m$$

In particular, $(\Delta_r D)\Delta_1 - \Delta_r(\Delta_1 D) = 0$. We now have

$$\begin{aligned} (\Delta_r\Delta_1^{-1})D &= (\Delta_r D)\Delta_1^{-1} + \Delta_r(\Delta_1^{-1} D) \\ &= (\Delta_r D)\Delta_1^{-1} - \Delta_r(\Delta_1 D)\Delta_1^{-2} \qquad \text{, by (13),} \\ &= \Big((\Delta_r D)\Delta_1 - \Delta_r(\Delta_1 D)\Big)\Delta_1^{-2} = 0 \; . \end{aligned}$$

Hence $\Delta_r\Delta_1^{-1} = c_r \in \Gamma$. By (14) above, $\Delta_1\rho_1 + \Delta_2\rho_2 + \ldots + \Delta_m\rho_m = 0$. This proves that $\rho_1 + c_2\rho_2 + \ldots + c_m\rho_m = 0$, which is of the required form.

Finally, we observe that if one of the Wronskians, say $\Delta_1 = 0$, we can start with Δ_1 as the leading Wronskian and arrive at a particular relation of the form $\rho_2' + c_3\rho_3' + \ldots + c_m\rho_m' = 0$, $\rho_i' \in P$.

We now recall two results on extensions of homomorphisms and give reference to corresponding results on extensions of derivations.

(i) Let $\mathfrak{A}$ be a subring (with 1) of a field P, M be a subset of non-zero elements of $\mathfrak{A}$ containing 1 and closed under multiplication, $\mathfrak{A}_M$ the subring of P generated by $\mathfrak{A}$ and the inverses of the elements of M. ($\mathfrak{A}_M = \{ab^{-1}, a \in \mathfrak{A}, b \in M\}$). Let s be a homomorphism of $\mathfrak{A}$ into a field P′ such that $\beta^s \neq 0$ for every $\beta \in M$. Then s has a unique extension to a homomorphism S of $\mathfrak{A}_M$ into P′. Moreover, S is an isomsrphism if and only if s is an isomorphism. (cf. Jacobson [9], pp. 2-3).

The corresponding result on derivations is given by the following theorem (Jacobson [9], p. 170).

Theorem 1.B. Let P be a field over Φ, $\mathfrak{A}$ a subalgebra of P/Φ (containing 1), M a multiplicatively closed subset of non-zero elements of $\mathfrak{A}$ containing 1, and let $\mathfrak{A}_M$ be the subalgebra of P of elements of the form ab^{-1}, $a \in \mathfrak{A}$, $b \in M$. Let D be a derivation of $\mathfrak{A}$ into P. Then D can be extended in one and only one way to a derivation of $\mathfrak{A}_M$ into P.

Remark. Here we observe that the isomorphism $a \to a + (aD)t$ of $\mathfrak{A}$ into $P \otimes \mathfrak{C}$ the algebra of dual numbers over P has a unique extension to an isomorphism s of $\mathfrak{A}_M$ into $P \otimes \mathfrak{C}$ given by

$$(ab^{-1})^s = ab^{-1} + \Big((aD)b^{-1} - ab^{-2}(bD)\Big)t$$

Since $(ab^{-1})D = (aD)b^{-1} - ab^{-2}(bD)$, we can write

$(ab^{-1})^s = ab^{-1} + \Big((ab^{-1})D\Big)t$. It can easily be shown (cf. discussion leading to Theorem 1.A) that the mapping θ associated with