HIGHER DERIVATIONS OF A PLANE ALGEBRAIC CURVE OVER A FIELD OF PRIME CHARACTERISTIC

Dissertation for the Degree of Ph. D.
MICHIGAN STATE UNIVERSITY
ANNE LARIMER LUDINGTON
1975

This is to certify that the

thesis entitled

HIGHER DERIVATIONS OF A PLANE ALGEBRAIC CURVE OVER A FIELD OF PRIME CHARACTERISTIC

presented by

Anne Larimer Ludington

has been accepted towards fulfillment
of the requirements for

Ph.D. degree in Mathematics

Dr. William C. Brown
Major professor

Date 20 June 1975

O-7639

ABSTRACT

HIGHER DERIVATIONS OF A PLANE ALGEBRAIC CURVE OVER A FIELD OF PRIME CHARACTERISTIC

By

Anne Larimer Ludington

Let Γ be a plane irreducible algebraic curve defined over an algebraically closed field k. Let P be a point on the curve and let R be the local ring of Γ at P.

$\mathrm{Der}_k^n(R)$ is the R-module of all n-th order k-derivations of R to R. Thus $\varphi \in \mathrm{Der}_k^n(R)$ if and only if $\varphi \in \mathrm{Hom}_k(R,R)$ and for all $r_0, \cdots, r_n \in R$ we have

$$\varphi(r_0 \cdots r_n) = \sum_{s=1}^{n} (-1)^{s-1} \sum_{i_1 < \cdots < i_s} r_{i_1} \cdots r_{i_s} \varphi(r_0 \cdots \check{r}_{i_1} \cdots \check{r}_{i_s} \cdots r_n).$$

Let $\mathrm{Der}(R) = \bigcup_n \mathrm{Der}_k^n(R)$. If k has characteristic zero, we define $\mathrm{der}(R)$ to be the subalgebra of $\mathrm{Der}(R)$ generated by composites of 1st order derivations. If the characteristic of k is $p \neq 0$, we say $\mathrm{Der}(R)$ is generated by p^i-th order derivations if the following condition is satisfied:

Let $\lambda \in \mathrm{Der}(R)$ and let n be the smallest integer such that $\lambda \in \mathrm{Der}_k^n(R)$. Let the p-adic expansion of n be given by $n = \sum_{i=0}^{N} \alpha_i p^i$. Then there exist

p^i-th order derivations $\tau_{1i}, \cdots, \tau_{mi} \in Der_k^{p^i}(R)$, $i = 0, \cdots, N$, such that $\lambda - (\tau_{1N}^{\alpha_N} \circ \cdots \circ \tau_{10}^{\alpha_0} + \cdots + \tau_{mN}^{\alpha_N} \circ \cdots \circ \tau_{m0}^{\alpha_0}) \in Der_k^{n-1}(R)$.

Here $Der_k^0(R) = 0$. Thus $Der(R)$ is generated by p^i-th order derivations if every n-th order derivation is a sum of composites of p^i-th order derivations. If $Der(R)$ is generated by p^i-th order derivations, we write $Der(R) = der(R)$.

Chapter 1 is devoted to theorems which characterize $Der_k^n(R)$ when it is a free R-module. We show that if it is free, it must be free on n generators. Further, if $Der_k^n(R)$ is free for all n, then there exist derivations $\lambda_1, \cdots, \lambda_n, \cdots$ and elements $x_1, \cdots, x_n, \cdots$ of R such that $\lambda_i \in Der_k^i(R)$; $Der_k^n(R)$ is generated by $\lambda_1, \cdots, \lambda_n$; and $\lambda_i(x_j) = \begin{cases} 0 & j < i \\ 1 & j = i \end{cases}$.

In Chapter 2 we consider the following example: R is the local ring at the origin of Γ: $f(X,Y) = X^2 - Y^3$ over a field of characteristic 2. Since $(0,0)$ is a singular point of Γ, R is not a regular local ring. We show that $Der_k^n(R)$ is a free R-module for all n and that $Der(R) = der(R)$. Thus this example shows that over a field of characteristic $p \neq 0$ the following two conjectures are false:

(I) $Der_k^n(R)$ is a free R-module for all n if and only if R is a regular local ring.

(II) Der(R) = der(R) if and only if R is a regular local ring.

The first conjecture is a generalization of a conjecture by Lipman; the second is Nakai's conjecture.

The main theorem of Chapter 3 is that if Der(R) = der(R) and $\mathrm{Der}_k^n(R)$ is a free R-module for all n, then R is analytically irreducible, that is, $\hat{R}$, the completion of R, is an integral domain. Geometrically this means that Γ has only one branch at P.

HIGHER DERIVATIONS OF A PLANE ALGEBRAIC CURVE OVER A FIELD OF PRIME CHARACTERISTIC

By

Anne Larimer Ludington

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

Department of Mathematics

1975

TO PAUL

ACKNOWLEDGEMENTS

I am grateful to my thesis advisor, Dr. William C. Brown for suggesting this topic and for the guidance and help that he gave me during the last two years. I am particularly appreciative of the time and effort that he spent while I was writing the rough draft. I also wish to thank my husband, Paul, for being a source of inspiration and encouragement.

TABLE OF CONTENTS

INTRODUCTION

Throughout this entire paper we shall assume that Γ is a plane irreducible algebraic curve, defined over an algebraically closed field k. Let P be a point on the curve, and let R be the local ring at P. Without loss of generality, we may assume that P is $(0,0)$. We shall denote the quotient field of R by K. If Γ is given by $f(X,Y) = 0$, then $R = (k[x,y])_{(x,y)}$ where $k[x,y] = k[X,Y]/(f(X,Y))$, $f(X,Y)$ is irreducible over k, and $f(0,0) = 0$.

For each $n = 1,2,\cdots$, we let $Der_k^n(R,M)$ denote the R-module of all n-th order derivations of R to an R-module M which vanish on k. Thus, $\varphi \in Der_k^n(R,M)$ if and only if $\varphi \in Hom_k(R,M)$ and for all $r_0,\cdots, r_n \in R$ we have

(1)

$$\varphi(r_0\cdots r_n) = \sum_{s=1}^{n} (-1)^{s-1} \sum_{i_1<\cdots<i_s} r_{i_1}\cdots r_{i_s}\varphi(r_0\cdots \check{r}_{i_1}\cdots \check{r}_{i_s}\cdots r_n)$$

When $M = R$, we write $Der_k^n(R)$ instead of $Der_k^n(R,R)$.

$\Omega_k^n(R)$ will denote the R-module of all n-th order differentials. $Der_k^n(R)$ is the dual module of $\Omega_k^n(R)$ so $Der_k^n(R) = Hom_R(\Omega_k^n(R),R)$.

Let $\mathrm{Der}(R) = \bigcup_n \mathrm{Der}_k^n(R)$. If k has characteristic zero, we define $\mathrm{der}(R)$ to be the subalgebra of $\mathrm{Der}(R)$ generated by composites of 1st order derivations. If the characteristic of k is $p \neq 0$, we say $\mathrm{Der}(R)$ is generated by p^i-th order derivations if the following condition is satisfied:

Let $\lambda \in \mathrm{Der}(R)$ and let n the smallest integer such that $\lambda \in \mathrm{Der}_k^n(R)$. Let $n = \sum_{i=0}^{N} \alpha_i p^i$ be the p-adic expansion of n. Then there exist p^i-th order derivations $\tau_{1i}, \cdots, \tau_{mi} \in \mathrm{Der}_k^{p^i}(R)$, $i = 0, \cdots, N$, such that

$$\lambda - (\tau_{1N}^{\alpha_N} \circ \cdots \circ \tau_{10}^{\alpha_0} + \cdots + \tau_{mN}^{\alpha_N} \circ \cdots \circ \tau_{m0}^{\alpha_0}) \in \mathrm{Der}_k^{n-1}(R).$$

Here $\mathrm{Der}_k^0(R) = 0$. Thus by induction we see that $\mathrm{Der}(R)$ is generated by p^i-th order derivations if every n-th order derivation is a sum of composites of p^i-th order derivations. If $\mathrm{Der}(R)$ is generated by p^i-th order derivations, we shall write $\mathrm{Der}(R) = \mathrm{der}(R)$. For K, $\mathrm{Der}(K) = \mathrm{der}(K)$, [Prop. 18;7]. Further, if R is a regular local ring, then $\mathrm{Der}(R) = \mathrm{der}(R)$ [Theorem 4.3;4].

Well-known properties of $\mathrm{Der}_k^n(R)$, $\Omega_k^n(R)$, and $\mathrm{Der}(R)$ may be found in Nakai's papers [6 and 7].

The starting point of this thesis concerns two conjectures which are known to hold for plane curves when k has characteristic zero:

(I) Lipman's conjecture: $\mathrm{Der}_k^1(R)$ is a free R-module if and only if R is a regular local ring [Theorem 1; 2].

(II) Nakai's conjecture: $\mathrm{Der}(R) = \mathrm{der}(R)$ if and only if R is regular [3].

It is easily shown that (I) is false when the characteristic of k is $p \neq 0$; in fact, the example given in Chapter 2 is a counterexample. That (I) is false is perhaps to be expected, since when k has characteristic zero, $\mathrm{Der}(K)$ is generated by composities of 1-st order derivations [Prop. 18; 7]. However, when the characteristic is p, $\mathrm{Der}(K)$ is generated by composities of p^i-th order derivations, $i = 0,1,\cdots$ [Prop. 18; 7]. Thus, the following conjecture arises when k has characteristic p:

(III) $\mathrm{Der}_k^n(R)$ is a free R-module for all $n = 1,2,\cdots$ if and only if R is a regular local ring.

It is known that if R is regular and k has characteristic $p \neq 0$, then $\mathrm{Der}_k^n(R)$ is a free R-module for all n [Theorem 16.11.2; 1]. The example which we shall give in Chapter 2 will show that the converses of (II) and (III) are false. That is, we shall construct a ring R over a field k of characteristic p which is not regular, but such that $\mathrm{Der}(R) = \mathrm{der}(R)$ and $\mathrm{Der}_k^n(R)$ is a free R-module for all n.

In order to show (II) and (III) are false, some results about $\mathrm{Der}_k^n(R)$ are needed. Thus, Chapter 1 is devoted to theorems which characterize $\mathrm{Der}_k^n(R)$ when it is a free R-module.

The main result of Chapter 3 is that if $\mathrm{Der}(R) = \mathrm{der}(R)$ and $\mathrm{Der}_k^n(R)$ is a free R-module for all n, then R is analytically irreducible; that is, $\hat{R}$, the completion of R, is an integral domain. Geometrically this means that Γ has only one branch centered at P.

CHAPTER I

CHARACTERIZATION OF $\mathrm{DER}_k^n(R)$ AS A FREE R-MODULE

The first lemma of this chapter shows that we may assume K is a separable algebraic extension over $k(x)$. The remainder of the chapter gives necessary and sufficient conditions for $\mathrm{Der}_k^n(R)$ to be a free R-module. We shall show that if $\mathrm{Der}_k^n(R)$ is free, it must be free on n generators. Moreover, there exists a set of generators $\lambda_1, \cdots, \lambda_n$ of $\mathrm{Der}_k^n(R)$ and monomials $x_1, \cdots, x_n$ of $k[x,y]$ such that $\lambda_i(x_j) = \begin{cases} 0 & j < i \\ 1 & j = 1 \end{cases}$.

<u>Lemma 1.1</u>: K is a separable algebraic extension of either $k(x)$ or $k(y)$.

<u>Proof</u>: The only case requiring proof is when k has characteristic $p \neq 0$. Let f_X and f_Y denote the partial derivatives of $f(X,Y)$ with respect to X and Y respectively. Suppose $f_X(x,y) = 0$ and $f_Y(x,y) = 0$. Pulling back to $k[X,Y]$ gives $f_X(X,Y) = h(X,Y)f(X,Y)$. Viewing these as polynomials in X with coefficients in $k[Y]$ gives $\deg f_X < \deg f \leq \deg fh$, which is a contradiction unless $f_X(X,Y) = 0$. So $f_X(X,Y) = 0$ and $f_Y(X,Y) = 0$. This implies that $f(X,Y) = g(X^p,Y^p) = (h(X,Y))^p$,

contradicting the assumption that f is irreducible. Hence, either $f_X(x,y) \neq 0$ or $f_Y(x,y) \neq 0$. Thus K is a separable algebraic extension of $k(x)$ or $k(y)$. QED

Henceforth, we shall assume $f_Y(x,y) \neq 0$; thus K is a separable algebraic extension of $k(x)$.

<u>Theorem 1.2</u>: $\mathrm{Der}_k^n(K)$ is a free K-module; it is free on n generators. If $\mathrm{Der}_k^n(R)$ is a free R-module, then it is free on n generators.

<u>Proof</u>: Since K is a separable algebraic extension of $k(x)$, $\Omega_k^n(K) \cong \Omega_k^n(k[x]) \otimes_{k[x]} K$ [p.26;7]. Since $\Omega_k^n(k[x])$ is a free $k[x]$-module of rank n [II, Prop. 2; 6], we have that $\Omega_k^n(K)$ is free of rank n over K. Now, $\mathrm{Der}_k^n(K) = \mathrm{Hom}_K(\Omega_k^n(K), K)$, so $[\mathrm{Der}_k^n(K): K] = n$.

Now $\mathrm{Der}_k^n(R) \otimes_R K = \mathrm{Hom}_R(\Omega_k^n(R), R) \otimes_R K \cong \mathrm{Hom}_K(\Omega_k^n(R) \otimes_R K, K)$. Since $\Omega_k^n(R) \otimes_R K \cong \Omega_k^n(K)$ [II, Theorem 9; 6], $\mathrm{Der}_k^n(R) \otimes_R K \cong \mathrm{Der}_k^n(K)$. Thus, if $\mathrm{Der}_k^n(R)$ is a free R-module, it must be free on n generators. QED

Since $f_Y(x,y) \neq 0$, $f(X,Y)$ must have a term involving Y. Further, since $f(X,Y)$ is irreducible, there must be a term of the form αY^N, $\alpha \in k$; otherwise, X would divide $f(X,Y)$. Hence $\mathrm{subdeg}_Y f(0,Y) > 0$.

<u>Lemma 1.3</u>: Let $\mathrm{subdeg}_Y f(0,Y) = N$. Then $y^{N-1}/x \notin R$.

<u>Proof</u>: As shown above, $N > 0$. Write $f(X,Y) = Xh(X,Y) + Y^N g(Y)$, where $g(Y)$ begins with a non-zero constant term.

Suppose $y^{N-1}/x \in R$. Then $y^{N-1}/x = r(x,y)/s(x,y)$, where $r(x,y)$, $s(x,y) \in k[x,y]$ and $s(x,y) \notin (x,y)$. Then $y^{N-1}s(x,y) - xr(x,y) = 0$. Pulling back to $k[X,Y]$ we have

$$(2) \quad Y^{N-1}s(X,Y) - r(X,Y)X = t(X,Y)[Xh(X,Y) + Y^N g(Y)].$$

Evaluating (2) at $X = 0$ gives

$$(3) \qquad Y^{N-1}s(0,Y) = t(0,Y)Y^N g(Y).$$

Thus, $s(0,Y) = t(0,Y)Yg(Y)$. Since $s(X,Y)$ has a constant term, $s(0,Y) \neq 0$. Thus, (3) implies that Y divides $s(0,Y)$, which is a contradiction. Hence, $y^{N-1}/x \notin R$.

QED

In the theorems which follow, we shall often use the fact that an n-th order derivation is also an $(n+1)$-st order derivation [I, Prop. 4; 6]. We shall also use the result that if $\lambda \in \mathrm{Der}_k^n(R)$, then $\lambda \in \mathrm{Der}_k^n(K)$ [I, Theorem 15; 6]. Hence if $\lambda_1, \cdots, \lambda_n$ are a free basis for $\mathrm{Der}_k^n(R)$, these derivations must also be a free basis for $\mathrm{Der}_k^n(K)$.

If $\lambda_1, \cdots, \lambda_n$ are a free basis for $\mathrm{Der}_k^n(R)$, then we shall write $\mathrm{Der}_k^n(R) = \langle \lambda_1, \cdots, \lambda_n \rangle$.

Before $\mathrm{Der}_k^n(R)$ is considered for arbitrary n, $\mathrm{Der}_k^1(R)$ is studied. Special attention should be paid to the method of proof, since the same technique will be used when $n > 1$.

<u>Theorem 1.4</u>: $\mathrm{Der}_k^1(R)$ is a free R-module if and only if there exists $\lambda \in \mathrm{Der}_k^1(R)$ and $z \in R$ such that $\lambda(z) = 1$.

<u>Proof</u>: Let $\mathrm{Der}_k^1(R)$ be generated by γ as a free R-module. Suppose $\gamma(r) \in (x,y)$ for all $r \in R$. Then $\gamma(r)$ may be written as $\gamma(r) = xr_x + yr_y$ with $r_x, r_y \in R$. As in Lemma 1.3, write $f(X,Y) = Xh(X,Y) + Y^N g(Y)$. Now consider $(y^{N-1}/x)\gamma$ which is certainly a derivation from K to K. For $r \in R$,

$$\begin{aligned}(y^{N-1}/x)\gamma(x) &= (y^{N-1}/x)(xr_x + yr_y)\\ &= y^{N-1}r_x + (y^N/x)r_y\\ &= y^{N-1}r_x - (h(x,y)/g(y))r_y.\end{aligned}$$

Since $g(y)$ is a unit in R, $(y^{N-1}/x)\gamma\colon R \to R$. Thus $(y^{N-1}/x)\gamma \in \mathrm{Der}_k^1(R)$ which implies that $(y^{N-1}/x)\gamma = t\gamma$ for some $t \in R$. Thus $(y^{N-1}/x - t)\gamma = 0$ on R, hence on K. Thus $y^{N-1}/x - t = 0$ or $y^{N-1}/x = t \in R$ which is a contradiction. Thus there exists $z \in R$ such that $\gamma(z)$ is a unit in R. Let $\lambda = \gamma/\gamma(z)$. Then $\mathrm{Der}_k^1(R) = \langle \lambda \rangle$ and $\lambda(z) = 1$.

Conversely, suppose such a λ and z exist. $\mathrm{Der}_k^1(R) \subseteq \mathrm{Der}_k^1(K)$ and λ may be regarded as the generator of the K-module, $\mathrm{Der}_k^1(K)$. Now let $\delta \in \mathrm{Der}_k^1(R)$. Then since $\delta \in \mathrm{Der}_k^1(K)$, $\delta = t\lambda$ where $t \in K$. Evaluating at z gives $\delta(z) = t\lambda(z) = t$. Thus $t = \delta(z) \in R$. Hence $\mathrm{Der}_k^1(R)$ is a free R-module. QED

Theorem 1.4 yields an easy proof of (I), Lipman's conjecture, for a plane curve Γ defined over a field of characteristic zero. For if $\mathrm{Der}_k^1(R)$ is free on λ, then by Theorem 1.4 there exists $z \in R$ such that $\lambda(z) = 1$. Thus by Zariski's Lemma [Theorem 2; 2], $\hat{R} \cong B[[z]]$ where z is analytically independent over B. By Chevalley's Theorem [Theorem 31, p. 320;9], $\hat{R}$ has no nilpotent elements. Thus, the dimension of $\hat{R}$ is 1 which implies that B is a reduced, zero-dimensional local ring. Therefore, B is a field and $\hat{R}$ is regular. Hence, R is regular.

<u>Theorem 1.5</u>: $\mathrm{Der}_k^n(R)$ is a free R-module if and only if there exist n-th order derivations $\lambda_1, \cdots, \lambda_n$ and distinct elements $x_1, \cdots, x_n \in R$ such that

$$\lambda_i(x_j) = \begin{cases} 0 & j < i \\ 1 & j = 1 \end{cases}.$$

<u>Proof</u>: Assume $\mathrm{Der}_k^n(R) = \langle \delta_1, \cdots, \delta_n \rangle$. Suppose $\delta_1(r) \in (x,y)$ for all $r \in R$. Then, as is the proof of Theorem 1.4, $(y^{N-1}/x)\,\delta_1 \in \mathrm{Der}_k^n(R)$. So, $(y^{N-1}/x)\,\delta_1 = \sum_{i=1}^{n} t_i \delta_i$ with $t_i \in R$. Thus, $(t_1 - y^{N-1}/x)\,\delta_1 + \sum_{i=2}^{n} t_i \delta_i = 0$ on R, hence, on K. This implies $y^{N-1}/x = t_1 \in R$ which is a contradiction. So, there exists an $x_1 \in R$ such that $\delta_1(x_1)$ is a unit. Let $\lambda_1 = \delta_1/\delta_1(x_1)$. Then $\mathrm{Der}_k^n(R) = \langle \lambda_1, \delta_2, \cdots, \delta_n \rangle$.

We now proceed by induction. Suppose we have found derivations $\lambda_1 \cdots, \lambda_{m-1}$ and elements $x_1, \cdots, x_{m-1} \in R$ such that $\mathrm{Der}_k^n(R) = \langle \lambda_1, \cdots, \lambda_{m-1}, \delta_m, \cdots, \delta_n \rangle$ and $\lambda_i(x_j) = \begin{cases} 0 & j < i \\ 1 & j = i \end{cases}$ for $1 \le i \le m-1$ and $1 \le j \le m-1$. Define $\bar{\lambda}_m$ as follows:

$$\bar{\lambda}_m = \delta_m - \sum_{i=1}^{m-1} r_i \lambda_i \quad \text{where } r_1 = \delta_m(x_1)$$

$$\text{and } r_i = \delta_m(x_i) - \sum_{j=1}^{i-1} r_j \lambda_j(x_i).$$

Computing $\bar{\lambda}_m(x_\ell)$, $\ell = 1, \cdots, m-1$, gives

$$\begin{aligned} \bar{\lambda}_m(x_\ell) &= \delta_m(x_\ell) - \sum_{i=1}^{m-1} r_i \lambda_i(x_\ell) \\ &= \delta_m(x_\ell) - \sum_{i=1}^{\ell-1} r_i \lambda_i(x_\ell) - r_\ell \\ &= 0. \end{aligned}$$

Also, $\mathrm{Der}_k^n(R) = \langle \lambda_1, \cdots, \lambda_{m-1}, \bar{\lambda}_m, \cdots, \delta_n \rangle$. As before, there is an element $x_m \in R$ such that $\bar{\lambda}_m(x_m)$ is a unit in R. Finally, let $\lambda_m = \bar{\lambda}_m / \bar{\lambda}_m(x_m)$. Therefore $\mathrm{Der}_k^n(R) = \langle \lambda_1, \cdots, \lambda_m, \delta_{m+1}, \cdots, \delta_n \rangle$ and $\lambda_i(x_j) = \begin{cases} 0 & j < i \\ 1 & j = i \end{cases}$ for $1 \le i \le m$ and $1 \le j \le m$.

Thus, by induction, $\mathrm{Der}_k^n(R) = \langle \lambda_1, \cdots, \lambda_n \rangle$ and there are elements $x_1, \cdots, x_n$ of R such that $\lambda_i(x_j) = \begin{cases} 0 & j < i \\ 1 & j = i \end{cases}.$

Conversely, suppose such elements and derivations exist. Consider

(4) $a_1\lambda_1 + \cdots + a_n\lambda_n = 0$

with $a_i \in R \subset K$. Evaluating (4) at x_1 gives $a_1 = 0$ since $\lambda_i(x_1) = 0$ for $i > 1$. Suppose a_i equals zero for $1 \leq i \leq m-1$. Then evaluating (4) at x_m gives $a_m = 0$. Hence $a_i = 0$ for $1 \leq i \leq n$.

Thus, $\mathrm{Der}_k^n(K) = < \lambda_1, \cdots, \lambda_n >$. Let $\gamma \in \mathrm{Der}_k^n(R)$. Then γ may be written as $\gamma = \sum_{i=1}^{n} t_i\lambda_i$ with $t_i \in K$. It suffices to show $t_i \in R$. Now $\gamma(x_1) = t_1 \in R$. Inductively assume that $t_1, \cdots, t_{m-1} \in R$. Then $\gamma(x_m) = \sum_{i=1}^{m-1} t_i\lambda_i(x_m) + t_m$ since again $\lambda_i(x_m) = 0$ for $m+1 \leq i \leq n$. So $t_m = \gamma(x_m) - \sum_{i=1}^{m-1} t_i\lambda_i(x_m) \in R$. Hence, $\mathrm{Der}_k^n(R) = < \lambda_1, \cdots, \lambda_n >$. QED

Theorem 1.5 does not require that $\mathrm{Der}_k^i(R)$ be a free R-module for $i < n$. With this added assumption we get a much stronger result.

<u>Theorem 1.6</u>: Suppose $\mathrm{Der}_k^{n-1}(R)$ is a free R-module with generators $\lambda_1, \cdots, \lambda_{n-1}$ where $\lambda_i \in \mathrm{Der}_k^i(R)$ for $1 \leq i \leq n-1$. Further suppose that there exist distinct elements of R, $x_1, \cdots, x_{n-1}$, such that $\lambda_i(x_j) = \begin{cases} 0 & j < i \\ 1 & j = i \end{cases}$. If $\mathrm{Der}_k^n(R)$ is a free R-module, then the following hold:

(a) $\mathrm{Der}_k^n(R) = \mathrm{Der}_k^{n-1}(R) \oplus R\gamma$ where $\gamma \in \mathrm{Der}_k^n(R)$.

(b) There exists an n-th order derivation λ_n and an element $x_n \in R$ such that $x_n \neq x_i$, $i = 1,\cdots,n-1$; $\lambda_n(x_i) = 0$, $i = 1,\cdots, n-1$; and $\lambda_n(x_n) = 1$.

<u>Proof</u>: Suppose $\mathrm{Der}_k^n(R) = <\delta_1,\cdots, \delta_n>$. Since an (n-1)-st order derivation is an n-th order derivation, $\lambda_{n-1} \in \mathrm{Der}_k^n(R)$ and $\lambda_{n-1} = \sum_{i=1}^{n} r_i\delta_i$ where $r_i \in R$. Evaluating λ_{n-1} at x_{n-1} gives $1 = \sum_{i=1}^{n} r_i\delta_i(x_{n-1})$. So, for some I, $1 \leq I \leq n$, r_I and $\delta_I(x_{n-1})$ are units in R. We reorder, if necessary, so that $I = n-1$. Thus,

$$\delta_{n-1} = \frac{1}{r_{n-1}}\lambda_{n-1} - \sum_{i=1}^{n-2}\frac{r_i}{r_{n-1}}\delta_i - \frac{r_n}{r_{n-1}}\delta_n .$$

And so, $\mathrm{Der}_k^n(R) = <\delta_1,\cdots, \delta_{n-2},\lambda_{n-1},\delta_n>$.

Inductively we assume $\mathrm{Der}_k^n(R) = <\delta_1,\cdots, \delta_m,\lambda_{m+1},\cdots, \lambda_{n-1},\delta_n>$, and we show that δ_m may be replaced by λ_m, after relabeling the δ_i's if need be. Since $\lambda_m \in \mathrm{Der}_k^n(R)$, λ_m may be written as

$$(5) \qquad \lambda_m = \sum_{i=1}^{m} t_i\delta_i + \sum_{j=m+1}^{n-1} t_j\lambda_j + t_n\delta_n.$$

Evaluating (5) at x_m gives

$$1 = \sum_{i=1}^{m} t_i\delta_i(x_m) + \sum_{j=m+1}^{n-1} t_j\lambda_j(x_m) + t_n\delta_n(x_m)$$
$$= \sum_{i=1}^{m} t_i\delta_i(x_m) + t_n\delta_n(x_m)$$

since $\lambda_j(x_m) = 0$ for $j = m+1, \cdots, n-1$. For some I, t_I and $\delta_I(x_m)$ are units in R, $I = 1, \cdots, m, n$. Rearrange the δ_i, if necessary, so that $I = m$. Thus,

$$\delta_m = \frac{1}{t_m}\lambda_m - \sum_{i=1}^{m-1}\frac{t_i}{t_m}\delta_i - \sum_{j=m+1}^{n-1}\frac{t_j}{t_m}\lambda_j - \frac{t_n}{t_m}\delta_n .$$

Hence, $\mathrm{Der}_k^n(R) = \langle \delta_1, \cdots, \delta_{m-1}, \lambda_m, \cdots, \lambda_{n-1}, \delta_n \rangle$.

Therefore by induction, $\mathrm{Der}_k^n(R) = \langle \lambda_1, \cdots, \lambda_{n-1}, \delta_n \rangle$. This completes the proof of (a).

To prove (b), we assume by (a) that $\mathrm{Der}_k^n(R) = \langle \lambda_1, \cdots, \lambda_{n-1}, \delta_n \rangle$. We define a new n-th order derivation as follows:

$$(6) \quad \gamma = \delta_n + \sum_{i=1}^{n-1} r_i\lambda_i \quad \text{where } r_1 = -\delta_n(x_1)$$
$$\text{and } r_i = -\delta_n(x_i) - \sum_{j=1}^{i-1} r_j\lambda_j(x_i).$$

Then since $\lambda_i(x_m) = 0$ for $i = m+1, \cdots, n-1$, evaluating (6) at x_m gives

$$\gamma(x_m) = \delta_n(x_m) + \sum_{i=1}^{n-1} r_i\lambda_i(x_m)$$
$$= \delta_n(x_m) + \sum_{i=1}^{m-1} r_i\lambda_i(x_m) + r_m$$
$$= 0.$$

Thus $\gamma(x_m) = 0$ for $1 \leq m \leq n-1$. Moreover, $\mathrm{Der}_k^n(R) = \langle \lambda_1, \cdots, \lambda_{n-1}, \gamma \rangle$.

As in Theorems 1.4 and 1.5, there must exist an element $x_n \in R$ such that $\gamma(x_n)$ is an unit in R. Finally then, let $\lambda_n = \gamma/\gamma(x_n)$. The theorem is now proved. QED

We shall use the following lemma to show that the x_i given in Theorems 1.5 and 1.6 may be assumed to be monomials in $k[x,y] \subseteq R$.

<u>Lemma 1.7</u>: If λ is an n-th order derivation and $\lambda(r) = 1$ for some $r \in R$, then $\lambda(x^i y^j)$ is a unit in R for some $x^i y^j \in k[x,y] \subseteq R$.

<u>**Proof**</u>: Write $r = s(x,y)/t(x,y)$ where $s(x,y), t(x,y) \in k[x,y]$ and $t(x,y) \notin (x,y)$. By [I, Theorem 5;6]

$$\begin{aligned} 1 &= \lambda(r) \\ &= \lambda(s/t) \\ &= (-1)^n \sum_{m=0}^{n} (-1)^m \binom{n+1}{m} t^m \lambda(t^{n-m}s)/t^{n+1}. \end{aligned}$$

For some m, $\lambda(t^{n-m}s)$ is a unit in R. Write $t^{n-m}s = \sum \alpha_{ij} x^i y^j \in k[x,y]$. So, $\lambda(x^i y^j)$ is a unit for some $x^i y^j$. QED

The following theorem summarizes the results of this chapter.

<u>Theorem 1.8</u>: If $\mathrm{Der}_k^n(R)$ is a free R-module for all n, then there exist derivations $\lambda_1, \cdots, \lambda_n$ and monomials $x_1, \cdots, x_n \in k[x,y]$ such that

(a) $\lambda_i \in \mathrm{Der}_k^i(R)$

(b) $\mathrm{Der}_k^n(R) = < \lambda_1, \cdots, \lambda_n >$

(c) $\lambda_i(x_j) = \begin{cases} 0 & j < i \\ 1 & j = i \end{cases}$

<u>Proof</u>: The only part of the theorem that requires proof is that the x_i may be choosen to be monomials. We show this by induction on n. If $n = 1$, then by Theorem 1.4 there exists a derivation λ such that $\mathrm{Der}_k^1(R) = < \lambda >$ and $\lambda(z) = 1$ for some $z \in R$. By Lemma 1.7 there exists a monomial $x_1 \in k[x,y]$ such that $\lambda(x_1)$ is a unit in R. Let $\lambda_1 = \lambda/\lambda(x_1)$. Then $\mathrm{Der}_k^1(R) = < \lambda_1 >$ and $\lambda_1(x_1) = 1$ where x_1 is a monomial in $k[x,y]$.

We now assume that $\mathrm{Der}_k^{n-1}(R) = < \lambda_1, \cdots, \lambda_{n-1} >$ and $\lambda_i(x_j) = \begin{cases} 0 & j < i \\ 1 & j = i \end{cases}$ for monomials $x_i \in k[x,y]$. By Theorem 1.6 there exists a derivation $\bar{\lambda}_n$ and an element $\bar{x}_n \in R$ such that $\mathrm{Der}_k^n(R) = < \lambda_1, \cdots, \lambda_{n-1}, \bar{\lambda}_n >, \bar{\lambda}_n(x_i) = 0$ for $i < n$, and $\bar{\lambda}_n(\bar{x}_n) = 1$. Again by Lemma 1.7, there exists a monomial $x_n \in k[x,y]$ such that $\bar{\lambda}_n(x_n)$ is a unit in R. Now let $\lambda_n = \bar{\lambda}_n/\bar{\lambda}_n(x_n)$. Then $\mathrm{Der}_k^n(R) = < \lambda_1, \cdots, \lambda_n >, \lambda_n(x_i) = 0$ for $i < n$, and $\lambda_n(x_n) = 1$ where x_n is a monomial in $k[x,y]$. QED

CHAPTER II

AN EXAMPLE

In this chapter we give an example of a curve Γ defined over a field of characteristic 2. Γ is given by $f(X,Y) = X^2 - Y^3$. Since $(0,0)$ is a singular point of Γ, the local ring, R, at $(0,0)$ is not regular. By constructing i-th order derivations λ_i and monomials $x_i \in k[x,y]$ which satisfy the conditions of Theorem 1.5, we shall show that $\mathrm{Der}_k^n(R)$ is a free R-module for all n. We shall also show $\mathrm{Der}(R) = \mathrm{der}(R)$. Thus, this example shows that both (II) and (III) are false.

The following lemma will be used repeatedly in the example. The results hold for any characteristic $p \neq 0$. Thus, we shall prove the lemma in this more general setting even though in the example k has characteristic 2.

<u>Lemma 2.1</u>: If $\lambda \in \mathrm{Der}_k^{p^n}(R)$ and $r,s \in R$, then

(a) $\lambda(r^{p^n} s) = r^{p^n}\lambda(s) + s\lambda(r^{p^n})$

(b) $\lambda(r^{p^{n+i}} s) = r^{p^{n+i}}\lambda(s)$ for $i \geq 1$.

<u>Proof</u>: The proof of (a) follows immediately from the definition of a p^n-th order derivation; this is equation (1).

For (b), the previous part gives

$$\lambda(r^{p^{n+i}}s) = \lambda((r^{p^i})^{p^n}s)$$
$$= r^{p^{n+i}}\lambda(s) + s\lambda(r^{p^{n+i}}).$$

Since $\lambda(r^{p^{n+i}}) = 0$ [I, Prop. 10;6], $\lambda(r^{p^{n+i}}s) = r^{p^{n+i}}\lambda(s)$.
QED

Example 2.2: Let R be the local ring at $(0,0)$ of $\Gamma: f(X,Y) = X^2 - Y^3$ over a field k of characteristic 2. $R = (k[x,y])_{(x,y)}$ and $x^2 = y^3$. Then $\mathrm{Der}_k^n(R)$ is a free R-module for all n and $\mathrm{Der}(R) = \mathrm{der}(R)$.

Proof: Let $A = k[x,y] = k[X,Y]/(X^2-Y^3)$. So $R = (A)_{(x,y)}$. For $m = 0,1,\cdots,$ define $\gamma_{2^m} \in \mathrm{Der}_k^{2^m}(k[y])$ as follows:

$$(7) \qquad \gamma_{2^m}(y^i) = \begin{cases} 0 & i < 2^m \\ 1 & i = 2^m \end{cases}$$

Thus, γ_{2^m} is a 2^m-th order derivation of $k[y]$ to $k[y]$. Define $\gamma_i = \gamma_{2^I}^{\alpha_I} \circ \cdots \circ \gamma_1^{\alpha_0}$ where the α_j's are the coefficients in the 2-adic expansion of i; that is $i = \sum_{j=0}^{I} \alpha_j 2^j$. It is easily shown that $\gamma_i(y^j) = \begin{cases} 0 & j < i \\ 1 & j = i \end{cases}$.

We now define a 2^n-th order derivation on $k[x]$ to $k[x,y]$, $n = 0,1,\cdots,$. For $n = 0$, define

$\lambda_{2^n} \in \mathrm{Der}_k^{2^n}(k[x],\ k[x,y])$ as follows:

(8a) $\lambda_{2^n}(x) = 0$

(8b) $\lambda_{2^n}(x^{2j}) = \gamma_{2^{n-1}}(y^{3j}) \qquad j = 1,\cdots,\ 2^{n-1}$

(8c) $\lambda_{2^n}(x^{2j+1}) = x\lambda_{2^n}(x^{2j}) \qquad j = 1,\cdots,\ 2^{n-1}-1.$

For each n, λ_{2^n} extends uniquely to a 2^n-th order derivation of $k(x)$ to $k(x,y)$ [I,Theorem 15;6]. We call this extension λ_{2^n}. Since $k(x,y)$ is separably algebraic over $k(x)$, λ_{2^n} extends in a unique way to a 2^n-th order derivation of $k(x,y)$ to $k(x,y)$ [Theorem 17;7]. This extension is also called λ_{2^n}.

We shall show that $\lambda_{2^n} \in \mathrm{Der}_k^{2^n}(A)$. First however we shall show that (8b) and (8c) hold for all values of j.

From the definition of λ_{2^n}, we have that $\lambda_{2^n}(x^{2^n}) = y^{2^n}$. For, by Lemma 2.1,

$$\lambda_{2^n}(x^{2^n}) = \lambda_{2^n}((x^2)^{2^{n-1}}) = \gamma_{2^{n-1}}((y^3)^{2^{n-1}}) = \gamma_{2^{n-1}}(y^{2^{n-1}+2^n})$$

$$= y^{2^n}\gamma_{2^{n-1}}(y^{2^{n-1}}) = y^{2^n}$$

We now show by induction that for all j we have

(8b) $\lambda_{2^n}(x^{2j}) = \gamma_{2^{n-1}}(y^{3j}).$

First, suppose $2j = 2^n + 2i$ where $i = 1, \cdots, 2^{n-1}$. Evaluating both sides of equation (8b) gives

$$\begin{aligned}
\lambda_{2^n}(x^{2j}) &= \lambda_{2^n}(x^{2^n} x^{2i}) \\
&= x^{2^n} \lambda_{2^n}(x^{2i}) + x^{2i}\, \lambda_{2^n}(x^{2^n}) \\
&= x^{2^n} \gamma_{2^{n-1}}(y^{3i}) + x^{2i} y^{2^n}
\end{aligned}$$

and

$$\begin{aligned}
\gamma_{2^{n-1}}(y^{3j}) &= \gamma_{2^{n-1}}(y^{(2+1)(2^{n-1}+i)}) \\
&= \gamma_{2^{n-1}}(y^{2^n} y^{2^{n-1}} y^{3i}) \\
&= y^{2^n} \gamma_{2^{n-1}}(y^{2^{n-1}} y^{3i}) \\
&= y^{2^n} y^{2^{n-1}} \gamma_{2^{n-1}}(y^{3i}) + y^{2^n} y^{3i} \\
&= x^{2^n} \gamma_{2^{n-1}}(y^{3i}) + y^{2^n} x^{2i}.
\end{aligned}$$

Thus, (8b) is valid for $2j \leq 2^{n+1}$.

Now suppose that (8b) holds for $2j \leq 2^{n+k}$ where $k > 0$. We show (8b) also holds for $2j = 2^{n+k} + 2i$ where $i = 1, \cdots, 2^{n+k-1}$. Again we compute $\lambda_{2^n}(x^{2j})$ and $\gamma_{2^{n-1}}(y^{3j})$:

$$\lambda_{2^n}(x^{2j}) = \lambda_{2^n}(x^{2^{n+k}} x^{2i})$$

$$= x^{2^{n+k}} \lambda_{2^n}(x^{2i})$$

$$= x^{2^{n+k}} \gamma_{2^{n-1}}(y^{3i})$$

$$\gamma_{2^{n-1}}(y^{3j}) = \gamma_{2^{n-1}}(y^{2^{n+k}} y^{2^{n+k-1}} y^{3i})$$

$$= y^{2^{n+k}} y^{2^{n+k-1}} \gamma_{2^{n-1}}(y^{3i})$$

$$= x^{2^{n+k}} \gamma_{2^{n-1}}(y^{3i}) .$$

Thus (8b) holds for $2j \leq 2^{n+k+1}$ and so by induction holds for all values of j.

Now we show that (8c) is valid for all values of j. That is, $\lambda_{2^n}(x^{2j+1}) = x\lambda_{2^n}(x^{2j})$. First suppose $2j + 1 = 2^n + 2i + 1$ where $i = 0, \cdots, 2^{n-1} - 1$. Then

$$\lambda_{2^n}(x^{2j+1}) = \lambda_{2^n}(x^{2^n} x^{2i+1})$$

$$= x^{2^n} \lambda_{2^n}(x^{2i+1}) + x^{2i+1} \lambda_{2^n}(x^{2^n})$$

$$= x^{2^n} x\lambda_{2^n}(x^{2i}) + x^{2i+1} \lambda_{2^n}(x^{2^n})$$

$$= x(x^{2^n} \lambda_{2^n}(x^{2i}) + x^{2i} \lambda_{2^n}(x^{2^n}))$$

$$= x\lambda_{2^n}(x^{2^n} x^{2i})$$

$$= x\lambda_{2^n}(x^{2j}) .$$

Now suppose that (8c) holds for $2j + 1 \leq 2^{n+k} - 1$ where $k > 0$. We show (8c) holds for $2j + 1 = 2^{n+k} + 2i - 1$ where $i = 1, \cdots, 2^{n+k-1} - 1$.

$$\begin{aligned}
\lambda_{2^n}(x^{2j+1}) &= \lambda_{2^n}(x^{2^{n+k}} x^{2i+1}) \\
&= x^{2^{n+k}} \lambda_{2^n}(x^{2i+1}) \\
&= x^{2^{n+k}} x\lambda_{2^n}(x^{2i}) \\
&= x\lambda_{2^n}(x^{2j}) .
\end{aligned}$$

Thus, (8c) is valid for $2j + 1 \leq 2^{n+k+1}$ and hence, by induction (8c) holds for all values of j.

We now show that $\lambda_{2^n} \in \mathrm{Der}_k^{2^n}(A)$. In order to show this, we compute $\lambda_{2^n}(y^i)$ and $\lambda_{2^n}(xy^i)$ and show that

$$\lambda_{2^n}(y^i) = \gamma_{2^{n-1}}(y^i) \tag{9a}$$

$$\lambda_{2^n}(xy^i) = x\gamma_{2^{n-1}}(y^i) \tag{9b}$$

where $i = 1,2,\cdots$ and $n = 1,2,\cdots$.

To show (9a), there are several cases depending on whether $i \equiv 0,1,2 \pmod 3$.

<u>Case 1</u>: $i \equiv 0 \pmod 3$

Let $i = 3\ell$. Then from (8b), $\lambda_{2^n}(y^i) = \lambda_{2^n}(y^{3\ell}) = \lambda_{2^n}(x^{2\ell}) = \gamma_{2^{n-1}}(y^{3\ell}) = \gamma_{2^{n-1}}(y^i)$.

<u>Case 2</u>: $i \equiv 1 \pmod 3$ and $2^n \equiv 1 \pmod 3$.

<u>Case 3</u>: $i \equiv 2 \pmod 3$ and $2^n \equiv 2 \pmod 3$.

These cases are considered together for in both $i + 2^{n+1} \equiv 0 \pmod 3$. Let $i + 2^{n+1} = 3\ell$. Then $\lambda_{2^n}(y^i\, y^{2^{n+1}}) = y^{2^{n+1}} \lambda_{2^n}(y^i)$. On the other hand

$$\begin{aligned}
\lambda_{2^n}(y^{3\ell}) &= \lambda_{2^n}(x^{2\ell}) \\
&= \gamma_{2^{n-1}}(y^{3\ell}) \\
&= \gamma_{2^{n-1}}(y^i y^{2^{n+1}}) \\
&= y^{2^{n+1}} \gamma_{2^{n-1}}(y^i).
\end{aligned}$$

So, $y^{2^{n+1}} \lambda_{2^n}(y^i) = y^{2^{n+1}} \gamma_{2^{n-1}}(y^i)$ or $\lambda_{2^n}(y^i) = \gamma_{2^{n-1}}(y^i)$.

<u>Case 4</u>: $i \equiv 2 \pmod 3$ and $2^n \equiv 1 \pmod 3$.

<u>Case 5</u>: $i \equiv 1 \pmod 3$ and $2^n \equiv 2 \pmod 3$.

In both of these cases, $i + 2^{n+2} \equiv 0 \pmod 3$. Say, $i + 2^{n+2} = 3\ell$. Then, $\lambda_{2^n}(y^i y^{2^{n+2}}) = y^{2^{n+2}} \lambda_{2^n}(y^i)$. On the other hand

$$\begin{aligned}
\lambda_{2^n}(y^{3\ell}) &= \lambda_{2^n}(x^{2\ell}) \\
&= \gamma_{2^{n-1}}(y^{3\ell})
\end{aligned}$$

$$= \gamma_{2^{n-1}}(y^i\, y^{2^{n+2}})$$

$$= y^{2^{n+2}}\, \gamma_{2^{n-1}}(y^i)$$

So, $y^{2^{n+2}}\, \lambda_{2^n}(y^i) = y^{2^{n+2}}\, \gamma_{2^{n-1}}(y^i)$ or $\lambda_{2^n}(y^i) = \gamma_{2^{n-1}}(y^i)$.

Now we show that $\lambda_{2^n}(xy^i) = x\gamma_{2^{n-1}}(y^i)$. The cases are the same as above.

<u>Case 1</u>: $i \equiv 0 \pmod 3$.

Let $i = 3\ell$. The result follows immediately from (8c):

$$\lambda_{2^n}(xy^i) = \lambda_{2^n}(xx^{2\ell})$$

$$= x\lambda_{2^n}(x^{2\ell})$$

$$= x\gamma_{2^{n-1}}(y^{3\ell})$$

$$= x\gamma_{2^{n-1}}(y^i).$$

<u>Case 2</u>: $i \equiv 1 \pmod 3$ and $2^n \equiv 1 \pmod 3$.

<u>Case 3</u>: $i \equiv 2 \pmod 3$ and $2^n \equiv 2 \pmod 3$.

Again $i + 2^{n+1} \equiv 0 \pmod 3$. Say, $i + 2^{n+1} = 3\ell$.
Then, $\lambda_{2^n}(xy^i y^{2^{n+1}}) = y^{2^{n+1}}\, \lambda_{2^n}(xy^i)$.

Also

$$\begin{aligned}\lambda_{2^n}(xy^{3\ell}) &= \lambda_{2^n}(xx^{2\ell})\\ &= x\lambda_{2^n}(x^{2\ell})\\ &= x\gamma_{2^{n-1}}(y^{3\ell})\\ &= x\gamma_{2^{n-1}}(y^i\, y^{2^{n+1}})\\ &= xy^{2^{n+1}}\gamma_{2^{n-1}}(y^i)\,.\end{aligned}$$

Thus, $y^{2^{n+1}}\lambda_{2^n}(xy^i) = xy^{2^{n+1}}\gamma_{2^{n-1}}(y^i)$ or $\lambda_{2^n}(xy^i) = x\gamma_{2^{n-1}}(y^i)$.

<u>Case 4</u>: $i \equiv 2 \pmod 3$ and $2^n \equiv 1 \pmod 3$.

<u>Case 5</u>: $i \equiv 1 \pmod 3$ and $2^n \equiv 2 \pmod 3$.

Here $i + 2^{n+2} \equiv 0 \pmod 3$. Let $i + 2^{n+2} = 3\ell$. Now $\lambda_{2^n}(xy^i\, y^{2^{n+2}}) = y^{2^{n+2}}\lambda_{2^n}(xy^i)$. On the other hand

$$\begin{aligned}\lambda_{2^n}(xy^{3\ell}) &= \lambda_{2^n}(xx^{2\ell})\\ &= x\lambda_{2^n}(x^{2\ell})\\ &= x\gamma_{2^{n-1}}(y^{3\ell})\\ &= x\gamma_{2^{n-1}}(y^i\, y^{2^{n+2}})\\ &= xy^{2^{n+2}}\gamma_{2^{n-1}}(y^i)\,.\end{aligned}$$

So again we have $y^{2^{n+2}} \lambda_{2^n}(xy^i) = xy^{2^{n+2}} \gamma_{2^{n-1}}(y^i)$ or $\lambda_{2^n}(xy^i) = x\gamma_{2^{n-1}}(y^i)$. Thus, we have completed the proofs of (9a) and (9b).

Since every monomial in A can be written as $x^j y^i$ with $j = 0$ or 1 and $0 \leq i$, (9a) and (9b) imply that $\lambda_{2^n}: A \to A$ for $n = 1, 2, \cdots$. To show that $\lambda_1 : A \to A$ we compute $\lambda_1(y)$. Since

$$0 = \lambda_1(x^2) = \lambda_1(y^3) = y^2 \lambda_1(y),$$

$\lambda_1(y) = 0$. Thus, $\lambda_1 \in \mathrm{Der}_k^1(A)$. Hence, $\lambda_{2^n}: A \to A$ for $n = 0, 1, \cdots$.

By taking composites, we define an m-th order derivation for $m = 1, 2, \cdots$. Write m in its 2-adic expansion as $m = \sum_{i=0}^{M} \alpha_i 2^i$ where $\alpha_i = 0$ or 1. Define

$\lambda_m = \lambda_{2^M}^{\alpha_M} \circ \cdots \circ \lambda_1^{\alpha_0}$. Then $\lambda_m \in \mathrm{Der}_k^m(A)$.

We now make some observations about λ_m. We first consider $\lambda_{2\ell} = \lambda_{2^L}^{\alpha_L} \circ \cdots \circ \lambda_2^{\alpha_1}$ where $2\ell = \sum_{i=1}^{L} \alpha_i 2^i$.

Equation (9a) shows that λ_{2^n} when restricted to $k[y]$ equals $\gamma_{2^{n-1}}$. Thus, if $\lambda_{2\ell}$ is restricted to $k[y]$, we have

$$\lambda_{2\ell}|_{k[y]} = \gamma_{2^{L-1}}^{\alpha_L} \circ \cdots \circ \gamma_1^{\alpha_1} = \gamma_\ell.$$

By the definition of γ_i, $\lambda_{2\ell}(y^i) = \gamma_\ell(y^i) = \begin{cases} 0 & i < \ell \\ 1 & i = \ell \end{cases}$.
Also $\lambda_{2\ell}(x) = 0$ since $\lambda_{2^n}(x) = 0$ for $n \geq 1$. And finally, $\lambda_{2\ell}(xy^i) = x\lambda_{2\ell}(y^i)$ by (9b).

Now consider $\lambda_{2\ell+1} = \lambda_{2\ell} \circ \lambda_1$. Since $\lambda_1(x) = 1$, $\lambda_1(y^i) = 0$, and $\lambda_1(xy^i) = y^i$, the following hold:

(11a) $\lambda_{2\ell+1}(x) = 0$

(11b) $\lambda_{2\ell+1}(y^i) = 0 \qquad i = 1,2, \cdots$

(11c) $\lambda_{2\ell+1}(xy^i) = \lambda_{2\ell}(y^i) \qquad i = 1,2, \cdots$

Thus, we have defined derivations λ_n, $n = 1,2, \cdots$, from A to A. Since $R = (A)_{(x,y)}$, it follows that $\lambda_n \in \mathrm{Der}_k^n(R)$ [I, Theorem 15;6].

Summarizing the above, we have that the λ_n satisfy the following:

(12) $\lambda_1(x) = 1$

$\lambda_{2\ell}(y^\ell) = 1$ and $\lambda_{2\ell}(y^i) = 0 \qquad i = 1,\cdots, \ell - 1$

$\lambda_{2\ell}(xy^i) = 0 \qquad i = 0,\cdots, \ell - 1$

$\lambda_{2\ell+1}(xy^\ell) = 1$ and $\lambda_{2\ell+1}(y^i) = 0 \qquad i = 1,\cdots, \ell$

$\lambda_{2\ell+1}(xy^i) = 0 \qquad i = 0,\cdots, \ell - 1$

where $\ell = 1,2,\cdots$.

We now define x_i as follows:

$$(13) \qquad x_{2\ell+1} = xy^{\ell} \qquad \ell = 0,1,\cdots$$

$$x_{2\ell} = y^{\ell} \qquad \ell = 1,2,\cdots .$$

Thus using the notation of (13), equation (12) says that $\lambda_i(x_j) = \begin{cases} 0 & j < i \\ 1 & j = i \end{cases}$. Thus, the conditions of Theorem 1.5 are satisfied and $\mathrm{Der}_k^n(R)$ is a free R-module for all n. And by construction, $\mathrm{Der}(R) = \mathrm{der}(R)$.

Since Γ has a singular point at the origin, R is not regular. Thus, R is an example of a local ring which is not regular but $\mathrm{Der}_k^n(R)$ is a free R-module for all n and $\mathrm{Der}(R) = \mathrm{der}(R)$. Hence, we have shown that (II) and (III) are false.

CHAPTER III

THE COMPLETION $\hat{R}$

In this chapter we shall prove the following theorem:

If $Der_k^n(R)$ is a free R-module for all n and $Der(R) = der(R)$, then $\hat{R}$ is an integral domain.

If the characteristic of k is zero, then $Der_k^1(R)$ being free implies that R is a regular local ring [Theorem 1;2]. Hence $\hat{R}$ is regular and thus an integral domain. Thus, we shall assume throughout this chapter that the characteristic of k is $p \neq 0$. Further, if P is a simple point of Γ, then R is regular. So, $\hat{R}$ is an integral domain and the theorem is trivial in this case. Thus, we also assume P is a singular point of Γ; that is, subdeg $f \geq 2$.

As in Chapter 1, we shall assume in this chapter that $f_y(x,y) \neq 0$. Thus, K is a separable algebraic extension of $k(x)$.

We shall use the following notation in this chapter. Let δ_i denote the i-th order derivation of $k[x]$ to $k[x]$ defined by $\delta_i(x^j) = \begin{cases} 0 & j < i \\ 1 & j = i \end{cases}$. The following results hold for δ_i:

(14) $\mathrm{Der}_k^n(k[x]) = \langle \delta_1, \cdots, \delta_n \rangle$ as a $k[x]$-module.

$\mathrm{Der}_k^n(k(x)) = \langle \delta_1, \cdots, \delta_n \rangle$ as a $k(x)$-module [pp. 26,27; 7].

(15) Since K is a separable algebraic extension of $k(x)$, $\delta_n \in \mathrm{Der}_k^n(K)$ [Theorem 17; 7]. Hence, $\mathrm{Der}_k^n(K) = \langle \delta_1, \cdots, \delta_n \rangle$.

(16) $\delta_n = \dfrac{\delta_{p^N}^{\alpha_N}}{\alpha_N!} \circ \cdots \circ \dfrac{\delta_1^{\alpha_0}}{\alpha_0!}$ where the p-adic expansion of n is given by $n = \sum_{i=0}^{N} \alpha_i p^i$ [Prop. 18; 7].

(17) $\delta_{p^i}^p = 0$.

<u>Proof</u>: $\delta_{p^i}^p$ is a p^{i+1}-order derivation. Hence, $\delta_{p^i}^p = \sum_{j=1}^{p^{i+1}} r_j \delta_j$. It is easily verified that $\delta_{p^i}^p(x^j) = 0$ for $j = 1, \cdots, p^{i+1}$ so, $r_j = 0$, $j = 1, \cdots, p^{i+1}$.

(18) $\delta_{p^n} \circ \delta_{p^m} = \delta_{p^m} \circ \delta_{p^n}$.

<u>Proof</u>: $\delta_{p^n} \circ \delta_{p^m} = \delta_{p^m} \circ \delta_{p^n} + [\delta_{p^n}, \delta_{p^m}]$ where $[\delta_{p^n}, \delta_{p^m}]$ is a derivation of order $p^n + p^m - 1$ [I, Cor. 6.2; 6].

So, $\delta_{p^n} \circ \delta_{p^m} = \delta_{p^m} \circ \delta_{p^n} + \sum_{i=1}^{p^n+p^m-1} r_i \delta_i$. But

$\delta_{p^n} \circ \delta_{p^m}(x^j) = 0$ and $\delta_{p^m} \circ \delta_{p^n}(x^j) = 0$ for $j = 1,\cdots, p^n + p^m - 1$. Hence, $\delta_{p^n} \circ \delta_{p^m} = \delta_{p^m} \circ \delta_{p^n}$.

Now consider the completion of R, denoted by $\hat{R}$, with respect to its maximal ideal $m = (x,y)$. We note that if $\lambda \in \mathrm{Der}_k^N(R)$, then λ extends to an N-th order k-derivation from $\hat{R}$ to $\hat{R}$. Let $\lambda \in \mathrm{Der}_k^N(R)$. Define $\bar{\lambda}: \hat{R} \to \hat{R}$ by $\bar{\lambda}(r) = \lim \lambda(r_n)$ where $r = \lim r_n$ with $\{r_n\}$ a Cauchy sequence in R. We show $\bar{\lambda}$ is continuous. For any n_0 we must find n such that $\lambda((m)^n) \subseteq m^{n_0}$ for the ideal m. Let $n = n_0^{N+1}$. Then it is easily checked using the definition of an N-th order derivation, equation (1), that $\lambda(m^n) \subseteq m^{n_0}$. Hence, $\bar{\lambda}$ is continuous. That $\bar{\lambda}$ is an N-th order derivation on $\hat{R}$ follows from the fact that λ is an N-th order derivation on R. Henceforth, we shall denote $\bar{\lambda}$ by λ.

The next theorem relates derivations and zero divisors.

<u>Theorem 3.1</u>: Let A be a commutative reduced k-algebra where k is a field of characteristic p. Let $D = \{0\} \cup \{\text{zero divisors in } A\}$. Then D is closed under every derivation λ.

<u>Proof</u>: Suppose λ is a derivation of order n. Choose N such that $p^N > n$. Then λ may be viewed as a derivation of order p^N.

Now let $r \in D$, $r \neq 0$, and find $s \neq 0$ such that $rs = 0$. Then $rs^{p^N} = 0$ and $s^{p^N} \neq 0$. Then

$$0 = \lambda(rs^{p^N}) = s^{p^N} \lambda(r) + r\lambda(s^{p^N}) = s^{p^N} \lambda(r)$$

since $\lambda(s^{p^N}) = 0$ [I, Prop. 10:6]. Thus, $\lambda(r) \in D$. So, D is closed under λ. QED

Theorem 3.1 assumes that A is reduced; that is, A has no nilpotent elements. We can apply this theorem to $\hat{R}$ because $\hat{R}$ has no nilpotent elements if k is perfect [Theorem 31, p. 320; 9]. This is our case.

$\hat{R} = k[[x,y]]$; that is, every element in $\hat{R}$ may be written as $\sum \alpha_{ij} x^i y^j$ with $\alpha_{ij} \in k$. This representation, however, is not necessarily unique.

<u>Theorem 3.2</u>: Suppose $\mathrm{Der}_k^n(R)$ is a free R-module for all n and $\mathrm{Der}(R) = \mathrm{der}(R)$. Let $\{\lambda_i\}$ be any set of generators such that $\lambda_i \in \mathrm{Der}_k^i(R)$ and $\mathrm{Der}_k^n(R) = < \lambda_1, \cdots, \lambda_n >$. Define derivations γ_m as follows:

$$(19) \qquad \gamma_m = \frac{\lambda_{p^M}^{\alpha_M}}{\alpha_M!} \circ \cdots \circ \frac{\lambda_1^{\alpha_0}}{\alpha_0!} \quad \text{where} \quad m = \sum_{i=0}^{M} \alpha_i p^i .$$

Then $\mathrm{Der}_k^n(R) = < \gamma_1, \cdots, \gamma_n >$.

Before we prove this theorem we note that Theorem 1.8 implies the existence of such λ_i's.

<u>Proof</u>: We first show that the following three relationships hold:

(20a) $(\lambda_{p^i} \circ r\lambda_{p^j}) - (r\lambda_{p^i} \circ \lambda_{p^j}) \in \mathrm{Der}_k^{p^i+p^j-1}(R)$ for $r \in R$.

(20b) $r_1\lambda_{p^{i_1}} \circ \cdots \circ r_n\lambda_{p^{i_n}} - (\prod_{j=1}^{n} r_j)(\lambda_{p^{i_1}} \circ \cdots \circ \lambda_{p^{i_n}}) \in$

$\mathrm{Der}_k^{m-1}(R)$ where $m = \sum_{j=1}^{n} p^{i_j}$.

(20c) $(\sum_{j=1}^{p^{i_1}} s_{1j}\lambda_j) \circ \cdots \circ (\sum_{j=1}^{p^{i_n}} s_{nj}\lambda_j) - (\prod_{j=1}^{n} s_{jp^{i_j}})\lambda_{p^{i_1}} \circ \cdots \circ \lambda_{p^{i_n}} \in$

$\mathrm{Der}_k^{m-1}(R)$ where $m = \sum_{j=1}^{n} p^{i_j}$.

For (a),

$$\lambda_{p^i} \circ r\lambda_{p^j} = r\lambda_{p^j} \circ \lambda_{p^i} + [\lambda_{p^i}, r\lambda_{p^j}]$$

$$= r(\lambda_{p^i} \circ \lambda_{p^j} + [\lambda_{p^j}, \lambda_{p^i}]) + [\lambda_{p^i}, r\lambda_{p^j}].$$

Since $[\lambda_{p^i}, r\lambda_{p^j}]$ and $[\lambda_{p^j}, \lambda_{p^i}]$ are derivations of order $p^i + p^j - 1$ [I, Cor. 6.2; 6], the result follows.

Result (b) follows from (a) by induction. And (c) follows immediately from (b).

We prove the theorem by induction. For $n = 1$, $\gamma_1 = \lambda_1$ and $\mathrm{Der}_k^1(R) = \langle \lambda_1 \rangle = \langle \gamma_1 \rangle$. Assume that $\mathrm{Der}_k^{n-1}(R) = \langle \gamma_1, \cdots, \gamma_{n-1} \rangle$. To show $\mathrm{Der}_k^n(R) = \langle \gamma_1, \cdots, \gamma_n \rangle$ it suffices to show that $\lambda_n = \sum_{i=1}^{n} r_i\gamma_i$ for some $r_i \in R$. Since $\mathrm{Der}_k^n(R) = \mathrm{Der}_k^{n-1}(R) \oplus R\lambda_n$, we see that n is the smallest integer such that $\lambda_n \in \mathrm{Der}_k^n(R)$. Since $\mathrm{Der}(R) = \mathrm{der}(R)$, we have

$$(21) \qquad \lambda_n = \tau_{1N}^{\alpha_N} \circ \cdots \circ \tau_{10}^{\alpha_0} + \cdots + \tau_{mN}^{\alpha_N} \circ \cdots \circ \tau_{m0}^{\alpha_0} + \sigma$$

where $\sigma \in \mathrm{Der}_k^{n-1}(R)$ and $\tau_{ij} \in \mathrm{Der}_k^{p^j}(R)$. Here $n = \sum_{j=0}^{N} \alpha_j p^j$ is the p-adic expansion of n. By absorbing any bogus terms in with σ, we may assume p^j is the smallest power of p such that $\tau_{ij} \in \mathrm{Der}_k^{p^j}(R)$, $j = 0, \cdots, N$. Thus, $\sum_{j=0}^{N} \mathrm{ord}\, \tau_{ij}^{\alpha_j} = n$ for $i = 1, \cdots, m$.

Now consider one of the summands $\tau_{iN}^{\alpha_N} \circ \cdots \circ \tau_{i0}^{\alpha_0}$ in (21). Since $\mathrm{Der}_k^{p^j}(R) = \langle \lambda_1, \cdots, \lambda_{p^j} \rangle$ we have by (20c)

$$(22) \qquad \tau_{iN}^{\alpha_N} \circ \cdots \circ \tau_{i0}^{\alpha_0} = \left(\sum_{\ell=0}^{p^N} s_{iN\ell}\, \lambda_\ell\right)^{\alpha_N} \circ \cdots \circ (s_{i01}\lambda_1)^{\alpha_0}$$

$$= s(\lambda_{p^N}^{\alpha_N} \circ \cdots \circ \lambda_1^{\alpha_0}) + \sigma'$$

where $\sigma' \in \mathrm{Der}_k^{n-1}(R)$ and $s \in R$.

Thus λ_n has the form $\lambda_n = r(\lambda_{p^N}^{\alpha_N} \circ \cdots \circ \lambda_1^{\alpha_0}) + \sigma''$ where $r \in R$ and $\sigma'' \in \mathrm{Der}_k^{n-1}(R) = \langle \gamma_1, \cdots, \gamma_{n-1} \rangle$. Now $\gamma_n = \alpha \lambda_{p^N}^{\alpha_N} \circ \cdots \circ \lambda_1^{\alpha_0}$ where $\alpha = 1/\prod_{i=0}^{N} \alpha_i!$ is a non-zero constant in k. Thus $\lambda_n = (r/\alpha)\gamma_n + \sigma''$ or $\lambda_n \in \langle \gamma_1, \cdots, \gamma_n \rangle$. QED

<u>Corollary 3.3</u>: Under the assumptions of the previous theorem and using the notation of it, $\lambda_n = r\gamma_n + \sum_{i=1}^{n-1} r_i\gamma_i$ and $\gamma_n = s\lambda_n + \sum_{i=1}^{n-1} s_i\lambda_i$ where r and s are units in R.

<u>Proof</u>: The only part requiring proof is that r and s are units. Substituting for γ_i in $\lambda_n = r\gamma_n + \sum_{i=1}^{n-1} r_i\gamma_i$ gives $\lambda_n = rs\lambda_n + \sum_{i=1}^{n-1} t_i\lambda_i$. Thus, $rs = 1$ and since $r, s \in R$, they must be units. QED

<u>Corollary 3.4</u>: Again assume the conditions and notation of Theorem 3.2. For $\gamma = \gamma_n + \sum_{i=1}^{n-1} r_i\gamma_i \in \mathrm{Der}_k^n(R)$ for some $r_i \in R$, there exists an element $r \in R$ such that $\gamma(r)$ is a unit in R.

<u>Proof</u>: As in Lemma 1.3, write $f(X,Y) = Xh(X,Y) + Y^N g(Y)$. Suppose $\gamma(r) \in (x,y)$ for all $r \in R$. Then $(y^{N-1}/x)\gamma \in \mathrm{Der}_k^n(R)$. Since $\mathrm{Der}_k^n(R) = \langle \gamma_1, \cdots, \gamma_n \rangle$, $(y^{N-1}/x)\gamma = \sum_{i=1}^{n} s_i\gamma_i$ with $s_i \in R$. Also $(y^{N-1}/x)\gamma = (y^{N-1}/x)\gamma_n + \sum_{i=1}^{n-1} (y^{N-1}/x)r_i\gamma_i$. But this implies that $y^{N-1}/x = s_n \in R$; this is a contradiction. Therefore, there exists some $r \in R$ such that $\gamma(r)$ is a unit. QED

<u>Proposition 3.5</u>: Let $S = (k[x,z])_{(x,z)}$ where k has characteristic p, $k[x,z] = k[X,Z]/(h(X,Z))$, and $h(X,Z)$

is an irreducible polynomial such that $h_Z(x,z) \neq 0$ and $h(0,0) = 0$. Suppose $\delta_{p^i}(z) = 0$ for all i less than some fixed N. Then $h(X,Z) = g(X^{p^N},Z)$ and $\delta_{p^i}z = z\delta_{p^i}$ for $i < N$.

<u>Proof</u>: Since $h_Z(x,z) \neq 0$, δ_{p^i} extends uniquely to $k(x,z)$. We shall view all calculations which we make in the proof of this proposition as taking place in $k(x,z)$.

Now $h_X(x,z)\delta_1(x) + h_Z(x,z)\delta_1(z) = 0$. So, $\delta_1(z) = -h_X(x,z)/h_Z(x,z)$ and since $\delta_1(z) = 0$, $h_X(x,z) = 0$. As in Lemma 1.1, this implies that $h_X(X,Z) = 0$. Thus, $h(X,Z) = g_1(X^p,Z)$.

Inductively, we suppose that $h(X,Z) = g_i(X^{p^i},Z)$ with $i < N$. Now δ_{p^i} is a 1st order derivation on $k[x^{p^i}]$ [I, Theorem 14;6]. Since $(g_i)_Z(x^{p^i},z) = h_Z(x,z) \neq 0, \delta_{p^i}$ extends uniquely to a 1st order derivation on $k(x^{p^i},z)$. Thus, $(g_i)_Z(x^{p^i},z)\delta_{p^i}(z) + (g_i)_{X^{p^i}}\delta_{p^i}(x^{p^i}) = 0$. So,

$\delta_{p^i}(z) = -(g_i)_{X^{p^i}}(x^{p^i},z)/(g_i)_Z(x^{p^i},z)$. Since $\delta_{p^i}(z) = 0$, $(g_i)_{X^{p^i}}(x^{p^i},z) = 0$. And therefore $(g_i)_{X^{p^i}}(X^{p^i},Z) = 0$.

Hence, $h(X,Z) = g_{i+1}(X^{p^{i+1}},Z)$. By induction then $h(X,Z) = g(X^{p^n},Z)$.

We now show by induction that $\delta_{p^i}z = z\delta_{p^i}$, $i < N$. For $i = 0$, $\delta_1(zr) = r\delta_1(z) + z\delta_1(r) = z\delta_1(r)$, for any $r \in S$. Thus $\delta_1 z = z\delta_1$.

For $1 < i < N$, consider the polynomials $g, Zg, \cdots, Z^{p^i-1}g$. Write $Z^j g$, $j = 0, \cdots, p^i-1$, as

$$(23) \qquad Z^j g = \sum_{n=1}^{p^i} r_{jn}(X^{p^N}, Z^{p^i}) Z^n + r_j(X^{p^N})$$

where $r_{jn}(X^{p^N}, Z^{p^i}) = \sum_{k,m} \alpha_{jnkm}(X^{p^N})^k (Z^{p^i})^m$. Since $\delta_{p^i}(z^j g) = 0$, evaluating (23) gives

(24)

$$\begin{aligned}
0 &= \delta_{p^i}(z^j g) \\
&= \sum_{n=1}^{p^i} r_{jn}(x^{p^N}, z^{p^i}) \delta_{p^i}(z^n) + \sum_{n=1}^{p^i} z^n \delta_{p^i}(r_{jn}(x^{p^N}, z^{p^i})) + 0 \\
&= \sum_{n=1}^{p^i} r_{jn} \delta_{p^i}(z^n) + \sum_{n=1}^{p^i} z^n \delta_{p^i}\left(\sum_{k,m} \alpha_{jnkm}(x^{p^N})^k (z^{p^i})^m\right) \\
&= \sum_{n=1}^{p^i} r_{jn} \delta_{p^i}(z^n) + \sum_{n=1}^{p^i} z^n \sum_{k,m} \alpha_{jnkm} x^{kp^N} \delta_{p^i}(z^{mp^i}) \\
&= \sum_{n=1}^{p^i} r_{jn} \delta_{p^i}(z^n) + \sum_{n=1}^{p^i} z^n \sum_{k,m} \alpha_{jnkm} x^{kp^N} m (z^{p^i})^{m-1} \delta_{p^i}(z^{p^i}) \\
&= \sum_{n=1}^{p^i} r_{jn} \delta_{p^i}(z^n) + r_j' \delta_{p^i}(z^{p^i}) \\
&= \sum_{n=1}^{p^i} \bar{r}_{jn} \delta_{p^i}(z^n)
\end{aligned}$$

where $\bar{r}_{jn} = r_{jn}$ if $n < p^i$ and $\bar{r}_{jp^i} = r_{jp^i} + r_j'$. The equations in (24) yield the following matrix equation:

$$(\bar{r}_{jn})\begin{pmatrix}\delta_{p^i}(z)\\ \vdots\\ \delta_{p^i}(z^{p^i})\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}$$

Suppose that the determinant of $(\bar{r}_{jn})$ is zero. Then there exists a non-zero solution, say $(t_1,\cdots, t_{p^i})$. Since $(\bar{r}_{jn}) \in \{k(x^{p^N},z)\}_{p^i}$, we have $t_j \in k(x^{p^N},z)$, $j=1,\cdots, p^i$. By replacing the t_j with some multiple, if necessary, we may assume $t_j \in k[x^{p^N},z]$.

Now consider the short exact sequence:

$$0 \to (g(X^{p^N},Z)) \to k[X^{p^i},Z] \xrightarrow{\pi} k[x^{p^i},z] \to 0.$$

Let $T_j \in k[X^{p^i},Z]$ such that $\pi(T_j) = t_j$, $j=1,\cdots, p^i$. We define $\bar{\delta}_{p^i}$: $k[X] \to k[X]$ to be the canonical p^i-th order derivation; that is, $\bar{\delta}_{p^i}(X^j) = \begin{cases} 0 & j<p^i \\ 1 & j=p^i \end{cases}$. Now we define $\bar{\lambda} \in \mathrm{Der}_k^{p^i}(k[X^{p^i},Z])$ as follows:

$$\bar{\lambda}(Z^j) = T_j \qquad j = 1,\cdots, p^i$$

$$\bar{\lambda}((X^{p^i})^{\ell}) = \bar{\delta}_{p^i}((X^{p^i})^{\ell}) \qquad \ell = 1,\cdots, p^i$$

$$\bar{\lambda}((X^{p^i})^{\ell}Z^j) = (X^{p^i})^{\ell}\, T_j + Z^j\bar{\delta}_{p^i}((X^{p^i})^{\ell}) \qquad 0 < \ell + j \leq p^i$$

extend $\bar{\lambda}$ to monomials of $k[X^{p^i},Z]$ using (1).

We first observe that $\bar{\lambda} = \bar{\delta}_{p^i}$ on $k[X^{p^i}]$. This is obvious since both are p^i-th order derivations on $k[X^{p^i}]$ and $\bar{\lambda}((X^{p^i})^{\ell}) = \bar{\delta}_{p^i}((X^{p^i})^{\ell})$ for $\ell = 1,\cdots, p^i$.

We next show

$$(26) \qquad \bar{\lambda}((X^{p^i})^{\ell} Z^j) = (X^{p^i})^{\ell}\, \bar{\lambda}(Z^j) + Z^j\, \bar{\lambda}((X^{p^i})^{\ell})$$

for all ℓ and j. By the definition of $\bar{\lambda}$, (26) holds for $\ell + j \le p^i$. We first prove (26) for ℓ and j when $\ell < p^i$ and $j < p^i$. The proof is by induction. Suppose $\ell + j = p^i + 1$. Using (1) and the fact that $\sum_{m=0}^{\ell} (-1)^m \binom{\ell}{m} = 0$, we get

$$\begin{aligned}
\bar{\lambda}((X^{p^i})^{\ell} Z^j) &= \sum_{\substack{n=0\\ 1\le n+m\le p^i}}^{j} \sum_{m=0}^{\ell} (-1)^{n+m-1} \binom{\ell}{m}\binom{j}{n} (X^{p^i})^m Z^n \bar{\lambda}((X^{p^i})^{\ell-m} Z^{j-n}) \\
&= \sum_{\substack{n=0\\ 1\le n+m\le p^i}}^{j} \sum_{m=0}^{\ell} (-1)^{n+m-1} \binom{\ell}{m}\binom{j}{n} (X^{p^i})^m Z^n \{ (X^{p^i})^{\ell-m} \bar{\lambda}(Z^{j-n}) \\
&\qquad + Z^{j-n}\, \bar{\lambda}((X^{p^i})^{\ell-m}) \} \\
&= \sum_{\substack{n=0\\ 1\le n+m\le p^i}}^{j} \sum_{m=0}^{\ell} (-1)^{n+m-1} \binom{\ell}{m}\binom{j}{n} \{ (X^{p^i})^{\ell}\, Z^n \bar{\lambda}(Z^{j-n}) \\
&\qquad + Z^j\, (X^{p^i})^m\, \bar{\lambda}((X^{p^i})^{\ell-m}) \} \\
&= \sum_{n=0}^{j} \sum_{m=0}^{\ell} (-1)^{n+m-1} \binom{\ell}{m}\binom{j}{n} \{ (X^{p^i})^{\ell}\, Z^n \bar{\lambda}(Z^{j-n}) \\
&\qquad + Z^j (X^{p^i})^m\, \bar{\lambda}((X^{p^i})^{\ell-m}) \}
\end{aligned}$$

$$+ \binom{\ell}{0}\binom{j}{0}[(x^{p^i})^{\ell}\,\bar{\lambda}(z^j) + z^j\,\bar{\lambda}((x^{p^i})^{\ell})]$$

$$= \sum_{n=0}^{j} (-1)^{n-1}\binom{j}{n} z^n\,\bar{\lambda}(z^{j-n})\,(x^{p^i})^{\ell} \sum_{m=0}^{\ell}(-1)^m\binom{\ell}{m}$$

$$+ \sum_{n=0}^{j} (-1)^n\binom{j}{n} \sum_{m=0}^{\ell}(-1)^{m-1}\binom{\ell}{m}(x^{p^i})^m z^j\bar{\lambda}((x^{p^i})^{\ell-m})$$

$$+ (x^{p^i})^{\ell}\,\bar{\lambda}(z^j) + z^j\,\bar{\lambda}((x^{p^i})^{\ell})$$

$$= (x^{p^i})^{\ell}\,\bar{\lambda}(z^j) + z^j\,\bar{\lambda}((x^{p^i})^{\ell})\,.$$

Thus, (26) holds for $\ell + j = p + 1$ when $\ell < p^i$ and $j < p^i$. Suppose (26) holds for $\ell' < p^i$ and $j' < p^i$ whenever $\ell' + j' < \ell + j$, $\ell < p^i$, $j < p^i$. We now show (26) is valid for $\ell + j$. Since $\ell < p^i$ and $\ell + j \geq p^i + 2$, $j \geq 3$. Write $j = j_1 + j_2$ where $j_1 = p^i - \ell$. Then

$$(x^{p^i})^{\ell} z^j = (x^{p^i})^{\ell}\, z^{j_1}(z^{j_2}) = x^{p^i}\cdots x^{p^i} z\cdots z(z^{j_2})\,.$$

Equation (1) gives

$$\bar{\lambda}((x^{p^i})^{\ell} z^j) = \bar{\lambda}((x^{p^i})^{\ell}\, z^{j_1}(z^{j_2}))$$

$$= \sum_{\substack{n=0\\ 1\leq n+m+t\leq p^i}}^{j_1}\ \sum_{m=0}^{\ell}\ \sum_{t=0}^{1} (-1)^{n+m+t-1}\binom{\ell}{m}\binom{j_1}{n}(x^{p^i})^m z^n (z^{j_2})^t$$

$$\bar{\lambda}((x^{p^i})^{\ell-m}\, z^{j_1-n}\,(z^{j_2})^{1-t})$$

$$= \sum_{\substack{n=0\\ 1\leq n+m}}^{j_1}\ \sum_{m=0}^{\ell}(-1)^{n+m-1}\binom{\ell}{m}\binom{j_1}{n}(x^{p^i})^m z^n\bar{\lambda}((x^{p^i})^{\ell-m}\, z^{j_1-n+j_2})$$

$$+ \sum_{\substack{n=0\\ n+m\leq p^i}}^{j_1}\ \sum_{m=0}^{\ell} (-1)^{n+m}\binom{\ell}{m}\binom{j_1}{n}(x^{p^i})^m\, z^{n+j_2}$$

$$\bar{\lambda}((x^{p^i})^{\ell-m} z^{j_1-n})$$

$$= \sum_{\substack{n=0\\1\le n+m}}^{j_1} \sum_{m=0}^{\ell} (-1)^{n+m-1} \binom{\ell}{m} \binom{j_1}{n} (x^{p^i})^m z^n [(x^{p^i})^{\ell-m} \bar{\lambda}(z^{j-n})$$

$$+ z^{j-n} \bar{\lambda}((x^{p^i})^{\ell-m})]$$

$$+ \sum_{\substack{n=0\\n+m\le p^i}}^{j_1} \sum_{m=0}^{\ell} (-1)^{m+n} \binom{\ell}{m} \binom{j_1}{n} (x^{p^i})^m z^{n+j_2} [(x^{p^i})^{\ell-m} \bar{\lambda}(z^{j_1-n})$$

$$+ z^{j_1-n} \bar{\lambda}((x^{p^i})^{\ell-m})]$$

$$= \sum_{n=0}^{j_1} \sum_{m=0}^{\ell} (-1)^{n+m-1} \binom{\ell}{m} \binom{j_1}{n} (x^{p^i})^{\ell} z^n \bar{\lambda}(z^{j-n})$$

$$+ \sum_{n=0}^{j_1} \sum_{m=0}^{\ell} (-1)^{n+m-1} \binom{\ell}{m} \binom{j_1}{n} z^j (x^{p^i})^m \bar{\lambda}((x^{p^i})^{\ell-m})$$

$$+ \binom{\ell}{0} \binom{j_1}{0} [(x^{p^i})^{\ell} \bar{\lambda}(z^j) + z^j \bar{\lambda}((x^{p^i})^{\ell})]$$

$$+ \sum_{n=0}^{j_1} \sum_{m=0}^{\ell} (-1)^{n+m} \binom{\ell}{m} \binom{j_1}{n} (x^{p^i})^{\ell} z^{n+j_2} \bar{\lambda}(z^{j_1-n})$$

$$+ \sum_{n=0}^{j_1} \sum_{m=0}^{\ell} (-1)^{n+m} \binom{\ell}{m} \binom{j_1}{n} (x^{p^i})^m z^j \bar{\lambda}((x^{p^i})^{\ell-m})$$

$$= (x^{p^i})^{\ell} \bar{\lambda}(z^j) + z^j \bar{\lambda}((x^{p^i})^{\ell}).$$

Thus, we have shown that (26) holds for all ℓ and j when $\ell < p^i$ and $j < p^i$. We now prove (26) for arbitrary ℓ and j. Write $\ell = \ell_1 + \ell_2 p^i + \ell_3 p^{i+1}$ with $0 \le \ell_1 < p^i$, $0 \le \ell_2 < p$, $0 \le \ell_3$ and $j = j_1 + j_2 p^i + j_3 p^{i+1}$ with $0 \le j_1 < p^i$, $0 \le j_2 < p$, $0 \le j_3$. Then using Lemma 2.1, we have

$$\bar{\lambda}((X^{p^i})^{\ell} Z^j) = \bar{\lambda}((X^{p^i})^{\ell_1}(X^{p^i})^{\ell_2 p^i}(X^{p^i})^{\ell_3 p^{i+1}} Z^{j_1} Z^{j_2 p^i} Z^{j_3 p^{i+1}})$$

$$= (X^{p^i})^{\ell_3 p^{i+1}} Z^{j_3 p^{i+1}} \bar{\lambda}((X^{p^i})^{\ell_1}(X^{p^i})^{\ell_2 p^i} Z^{j_1} Z^{j_2 p^i})$$

$$= (X^{p^i})^{\ell_3 p^{i+1}} Z^{j_3 p^{i+1}} [(X^{p^i})^{\ell_1} Z^{j_1} \bar{\lambda}((X^{p^i})^{\ell_2 p^i} Z^{j_2 p^i})$$

$$+ (X^{p^i})^{\ell_2 p^i} Z^{j_2 p^i} \bar{\lambda}((X^{p^i})^{\ell_1} Z^{j_1})]$$

$$= (X^{p^i})^{\ell_3 p^{i+1}} Z^{j_3 p^{i+1}} [(X^{p^i})^{\ell_1} Z^{j_1}((X^{p^i})^{\ell_2 p^i} \bar{\lambda}(Z^{j_2 p^i})$$

$$+ Z^{j_2 p^i} \bar{\lambda}(X^{p^i})^{\ell_2 p^i}) + (X^{p^i})^{\ell_2 p^i} Z^{j_2 p^i}((X^{p^i})^{\ell_1} \bar{\lambda}(Z^{j_1})$$

$$+ Z^{j_1} \bar{\lambda}((X^{p^i})^{\ell_1}))]$$

$$= (X^{p^i})^{\ell} Z^{j_3 p^{i+1}} (Z^{j_1} \bar{\lambda}(Z^{j_2 p^i}) + Z^{j_2 p^i} \bar{\lambda}(Z^{j_1}))$$

$$+ (X^{p^i})^{\ell_3 p^{i+1}} Z^j ((X^{p^i})^{\ell_1} \bar{\lambda}((X^{p^i})^{\ell_2 p^i})$$

$$+ (X^{p^i})^{\ell_2 p^i} \bar{\lambda}((X^{p^i})^{\ell_1}))$$

$$= (X^{p^i})^{\ell} Z^{j_3 p^{i+1}} \bar{\lambda}(Z^{j_1 + j_2 p^i})$$

$$+ (X^{p^i})^{\ell_3 p^{i+1}} Z^j \bar{\lambda}((X^{p^i})^{\ell_1 + \ell_2 p^i})$$

$$= (X^{p^i})^{\ell} \bar{\lambda}(Z^j) + Z^j \bar{\lambda}((X^{p^i})^{\ell}).$$

Hence, (26) holds for arbitrary ℓ and j.

We want to show

(27) $\bar{\lambda}(s(X^{p^i}, Z^{p^i})r) = s(X^{p^i}, Z^{p^i})\bar{\lambda}(r) + r\,\bar{\lambda}(s(X^{p^i}, Z^{p^i}))$

for any $r \in k[x^{p^i}, Z]$. To do this we first show

$$\bar{\lambda}((X^{p^i})^n (Z^{p^i})^m (X^{p^i})^{\ell} Z^j) = (X^{p^i})^n (Z^{p^i})^m \bar{\lambda}((X^{p^i})^{\ell} Z^j)$$

$$+ (X^{p^i})^{\ell} Z^j \bar{\lambda}((X^{p^i})^n (Z^{p^i})^m).$$

Using (26) and Lemma 2.1, we have

$$\bar{\lambda}(X^{np^i} Z^{mp^i} X^{\ell p^i} Z^j) = X^{np^i} X^{\ell p^i} \bar{\lambda}(Z^{mp^i} Z^j) + Z^j Z^{mp^i} \bar{\lambda}(X^{np^i} X^{\ell p^i})$$

$$= X^{np^i} X^{\ell p^i} [Z^{mp^i} \bar{\lambda}(Z^j) + Z^j \bar{\lambda}(Z^{mp^i})]$$

$$+ Z^j Z^{mp^i} [\bar{\delta}_{p^i} (X^{np^i} X^{\ell p^i})]$$

$$= X^{np^i} Z^{mp^i} [X^{\ell p^i} \bar{\lambda}(Z^j) + Z^j \bar{\lambda}(X^{\ell p^i})]$$

$$+ X^{\ell p^i} Z^j [X^{np^i} \bar{\lambda}(Z^{mp^i}) + Z^{mp^i} \bar{\lambda}(X^{np^i})]$$

$$= X^{np^i} Z^{mp^i} \bar{\lambda}(X^{\ell p^i} Z^j) + X^{\ell p^i} Z^j \bar{\lambda}(X^{np^i} Z^{mp^i}).$$

Now we consider $\bar{\lambda}((X^{p^i})^n (Z^{p^i})^m r)$ where $r = \sum \alpha_{\ell j} (X^{p^i})^{\ell} Z^j$:

$$\bar{\lambda}(X^{np^i} Z^{mp^i} r) = \bar{\lambda}(X^{np^i} Z^{mp^i} \sum \alpha_{\ell j} (X^{p^i})^{\ell} Z^j)$$

$$= \sum \alpha_{\ell j} [X^{np^i} Z^{mp^i} \bar{\lambda}(X^{\ell p^i} Z^j) + X^{\ell p^i} Z^j \bar{\lambda}(X^{np^i} Z^{mp^i})]$$

$$= X^{np^i} Z^{mp^i} \bar{\lambda}(r) + r \bar{\lambda}(X^{np^i} Z^{mp^i})$$

Now we prove (27) with $s(X^{p^i}, Z^{p^i}) = \sum \alpha_{nm} (X^{p^i})^n (Z^{p^i})^m$:

$$\bar{\lambda}(s(X^{p^i},Z^{p^i})r) = \bar{\lambda}((\Sigma\, \alpha_{nm}(X^{p^i})^n(Z^{p^i})^m)r)$$

$$= \Sigma\, \alpha_{nm}\ \bar{\lambda}(X^{np^i}Z^{mp^i}r)$$

$$= \Sigma\, \alpha_{nm}(X^{np^i}Z^{mp^i}\ \bar{\lambda}(r)\ +\ r\bar{\lambda}(X^{np^i}Z^{mp^i}))$$

$$= \Sigma\, \alpha_{nm}X^{np^i}\ Z^{mp^i}\ \bar{\lambda}(r)\ +\ r\bar{\lambda}(\Sigma\, \alpha_{nm}X^{np^i}Z^{mp^i})$$

$$= s(X^{p^i},Z^{p^i})\bar{\lambda}(r)\ +\ r\bar{\lambda}(s(X^{p^i},Z^{p^i}).$$

Thus, we have proven (27). We use (27) to show

$$(28)\qquad \bar{\lambda}(s(X^{p^{i+1}},Z^{p^{i+1}})r) = s(X^{p^{i+1}},Z^{p^{i+1}})\bar{\lambda}(r)$$

for $r \in k[X^{p^i},Z]$. By (27) we have

$$\bar{\lambda}(s(X^{p^{i+1}},Z^{p^{i+1}})r) = s(X^{p^{i+1}},Z^{p^{i+1}})\bar{\lambda}(r) + r\bar{\lambda}(s(X^{p^{i+1}},Z^{p^{i+1}}).$$

Now

$$\bar{\lambda}(s(X^{p^{i+1}},Z^{p^{i+1}})) = \bar{\lambda}(\Sigma\alpha_{nm}(X^{p^{i+1}})^n(Z^{p^{i+1}})^m)$$

$$= \Sigma\, \alpha_{nm}\ \bar{\lambda}(X^{np^{i+1}}Z^{mp^{i+1}})$$

$$= \Sigma\, \alpha_{nm}\ Z^{mp^{i+1}}\ \bar{\lambda}(X^{np^{i+1}})$$

$$= \Sigma\, \alpha_{nm}\ Z^{mp^{i+1}}\ \bar{\delta}_{p^i}(X^{np^{i+1}})$$

$$= 0.$$

Thus, $\bar{\lambda}(s(X^{p^{i+1}},\ Z^{p^{i+1}})r) = s(X^{p^{i+1}},Z^{p^{i+1}})\ \bar{\lambda}(r)$.

We now use (27) and (28) to show that $\bar{\lambda}((g)) \subseteq (g)$. Suppose $f(X^{p^i},Z) \in (g)$. Then $f(X^{p^i},Z) = k(X^{p^i},Z)g(X^{p^N},Z) = \sum_{m=0}^{p^{i+1}-1} \sum_{\ell=0}^{p-1} s_{\ell m}(X^{p^{i+1}},Z^{p^{i+1}})(X^{p^i})^{\ell} Z^m g(X^{p^N},Z)$. Thus,

$$\begin{aligned}
\bar{\lambda}(f(X^{p^i},Z)) &= \bar{\lambda}\Big(\sum_{m=0}^{p^{i+1}-1} \sum_{\ell=0}^{p-1} s_{\ell m} X^{\ell p^i} Z^m g\Big) \\
&= \sum_{m=0}^{p^{i+1}-1} \sum_{\ell=0}^{p-1} \bar{\lambda}(s_{\ell m} X^{\ell p^i} Z^m g) \\
& \sum_{m=0}^{p^{i+1}-1} \sum_{\ell=0}^{p-1} s_{\ell m}\bar{\lambda}(X^{\ell p^i} Z^m g)
\end{aligned}$$

by(28) since $s_{\ell m} \in k[X^{p^{i+1}},Z^{p^{i+1}}]$. Thus, it suffices to show $\bar{\lambda}(X^{\ell p^i} Z^m g) \in (g)$ where $0 \le \ell < p$, $0 \le m \le p^{i+1}-1$. Let $m = np^i + j$ where $0 \le n < p$ and $j < p^i$. Then $\bar{\lambda}(X^{\ell p^i} Z^m g) = \bar{\lambda}(X^{\ell p^i} Z^{np^i} Z^j g) = X^{\ell p^i} Z^{np^i} \bar{\lambda}(Z^j g) + Z^j g \bar{\lambda}(X^{\ell p^i} Z^{np^i})$ by (27). So, it suffices to show $\bar{\lambda}(Z^j g) \in (g)$ for $0 \le j < p^i$.

Now by (23), $Z^j g = \sum_{n=1}^{p^i} r_{jn}(X^{p^N},Z^{p^i})Z^n + r_j(X^{p^N})$.

Thus,

$$\begin{aligned}
\bar{\lambda}(Z^j g) &= \sum_{n=1}^{p^i} \bar{\lambda}(r_{jn}(X^{p^N},Z^{p^i})Z^n) + \bar{\lambda}(r_j(X^{p^N})) \\
&= \sum_{n=1}^{p^i} r_{jn}\bar{\lambda}(Z^n) + \sum_{n=1}^{p^i} Z^n \bar{\lambda}(r_{jn}) + \bar{\delta}_{p^i}(r_j(X^{p^N}))
\end{aligned}$$

by (27). Using the notation of (24), we have

$$\bar{\lambda}(Z^j g) = \sum_{n=1}^{p^i} r_{jn}\bar{\lambda}(Z^n) + \sum_{n=1}^{p^i} Z^n\bar{\lambda}(\sum_{k,m} \alpha_{jnkm}X^{kp^N}Z^{mp^i}) + 0$$

$$= \sum_{n=1}^{p^i} r_{jn}\bar{\lambda}(Z^n) + \sum_{n=1}^{p^i} Z^n \sum_{k,m} \alpha_{jnkm}X^{kp^N}\bar{\lambda}(Z^{mp^i})$$

$$= \sum_{n=1}^{p^i} r_{jn}\bar{\lambda}(Z^n) + \sum_{n=1}^{p^i} Z^n \sum_{k,m} \alpha_{jnkm}X^{kp^N} m(Z^{p^i})^{m-1}\bar{\lambda}(Z^{p^i})$$

$$= \sum_{n=1}^{p^i} r_{jn}\bar{\lambda}(Z^n) + r_j' \,\bar{\lambda}(Z^{p^i})$$

$$= \sum_{n=1}^{p^i} \bar{r}_{jn}\bar{\lambda}(Z^n)$$

$$= \sum_{n=1}^{p^i} \bar{r}_{jn}\, T_n.$$

Now $\pi(\sum_{n=1}^{p^i} \bar{r}_{jn}T_n) = \sum_{n=1}^{p^i} \bar{r}_{jn}(x^{p^N},z)t_n = 0$. Thus,

$\bar{\lambda}(Z^j g) \in \ker \pi = (g)$. Thus, we have shown that $\bar{\lambda}(g) \subseteq (g)$.

Now $\bar{\lambda}$ induces a p^i-th order derivation λ on the ring $k[x^{p^i},z]$ as follows:

$$\lambda(a) = \pi\bar{\lambda}(A) \quad \text{where} \quad \pi A = a$$

or $\lambda(A + (g)) = \bar{\lambda}(A) + (g)$ where $A \in k[X^{p^i},Z]$. If $A + (g) = B + (g)$ then $A-B \in (g)$; $\bar{\lambda}(A) - \bar{\lambda}(B) = \bar{\lambda}(A-B) \in (g)$ since $\bar{\lambda}(g) \subseteq (g)$. Thus, $\lambda(A + (g)) = \lambda(B + (g))$ and so λ is well defined.

We observe that $\lambda(z^j) = t_j$:

$$\lambda(z^j) = \lambda(Z^j + (g)) = \bar{\lambda}(Z^j) + (g) = T_j + (g) = t_j$$

for $j = 1, \cdots, p^i$. Also, we have $\lambda((x^{p^i})^{\ell}) = \delta_{p^i}((x^{p^i})^{\ell})$ for all ℓ. For, $\lambda((x^{p^i})^{\ell}) = \lambda((x^{p^i})^{\ell} + (g)) = \bar{\lambda}((x^{p^i})^{\ell}) + (g) = \bar{\delta}_{p^i}((x^{p^i})^{\ell}) + (g) = \delta_{p^i}((x^{p^i})^{\ell})$.

Thus, λ is a p^i-th order derivation from $k[x^{p^i}, z]$ to $k[x^{p^i}, z]$. So, $\lambda \in \mathrm{Der}_k^{p^i}(k(x^{p^i}, z))$ and λ agrees with δ_{p^i} on $k(x^{p^i})$. This is a contradiction since δ_{p^i} has a unique extension to $k(x^{p^i}, z)$. Hence, the determinant in (25), $|(\bar{r}_{jn})|$, is non-zero.

Multiplying (23) by x^m, $m = 1, \cdots, p^i - 1$, gives $x^m z^j g = \sum_{n=1}^{p^i} r_{jn}(x^{p^N}, z^{p^i}) x^m z^j + x^m r_j(x^{p^N})$. These give rise to the following equations in $k(x,z)$:

(29)

$$\begin{aligned}
0 &= \delta_{p^i}(x^m z^j g) \\
&= \sum_{n=1}^{p^i} r_{jn}\delta_{p^i}(x^m z^n) + \sum_{n=1}^{p^i} x^m z^n \delta_{p^i}(r_{jn}) + r_j(x^{p^N})\delta_{p^i}(x^m) \\
&= \sum_{n=1}^{p^i} r_{jn}\delta_{p^i}(x^m z^n) + x^m \sum_{n=1}^{p^i} z^n \delta_{p^i}(r_{jn}) + 0 \\
&= \sum_{n=1}^{p^i} r_{jn}\delta_{p^i}(x^m z^n) + x^m r_j' \,\delta_{p^i}(z^{p^i}).
\end{aligned}$$

Now $\delta_{p^i}(x^m z^{p^i}) = x^m \delta_{p^i}(z^{p^i}) + z^{p^i}\delta_{p^i}(x^m) = x^m \delta_{p^i}(z^{p^i})$;

$\delta_{p^i}(x^m) = 0$ since $m < p^i$. So, (29) can be written as

$$0 = \sum_{n=1}^{p^i} r_{jn}\delta_{p^i}(x^m z^n) + r_j'\delta_{p^i}(x^m z^{p^i})$$

$$= \sum_{n=1}^{p^i} \bar{r}_{jn}\delta_{p^i}(x^m z^n).$$

Since $|(\bar{r}_{jn})| \neq 0$, $\delta_{p^i}(x^m z^n) = 0$ for $0 \leq m < p^i$, $1 \leq n \leq p^i$.

Now we consider the p^i-1 order derivation $[\delta_{p^i}, z]$ given by $[\delta_{p^i}, z](r) = \delta_{p^i}(zr) - r\delta_{p^i}(z) - z\delta_{p^i}(r)$ [I,p.3;6]. For $m = 1,\cdots, p^i-1$, $[\delta_{p^i}, z](x^m) = \delta_{p^i}(zx^m) - x^m\delta_{p^i}(z) - z\delta_{p^i}(x^m) = 0$. Now $[\delta_{p^i}, z] \in \mathrm{Der}_k^{p^i-1}(k(x,z))$ so, $[\delta_{p^i}, z] = \sum_{j=1}^{p^i-1} r_j\delta_j$ for some $r_j \in k(x,z)$. Evaluating $[\delta_{p^i}, z]$ at x shows that $r_1 = 0$. Similarly, since $[\delta_{p^i}, z](x^m) = 0$, $r_m = 0$ for $m = 1,\cdots, p^i-1$. Thus, $[\delta_{p^i}, z] = 0$. Hence,

$$0 = [\delta_{p^i}, z](r)$$

$$= \delta_{p^i}(zr) - r\delta_{p^i}(z) - z\delta_{p^i}(r)$$

$$= \delta_{p^i}(zr) - z\delta_{p^i}(r).$$

Thus, $\delta_{p^i}z = z\delta_{p^i}$ for $i < N$. QED

We now prove a special case of the main theorem. Namely, if $\delta_n \in \mathrm{Der}_k^n(R)$ for all n, then $\hat{R}$ is an integral domain. If $\delta_n \in \mathrm{Der}_k^n(R)$ for all n, then

$\mathrm{Der}_k^n(R) = \langle \delta_1, \cdots, \delta_n \rangle$. Also $\mathrm{Der}(R) = \mathrm{der}(R)$ since $\delta_n = \delta_{p^t}^{\alpha_t}/\alpha_t! \circ \cdots \circ \delta_1^{\alpha_0}/\alpha_0!$ where the p-adic expansion of n is given by $n = \sum_{i=0}^{t} \alpha_i p^i$. Thus, $\delta_n \in \mathrm{Der}_k^n(R)$ for all n implies that both hypotheses of the main theorem are satisfied. That is, $\mathrm{Der}_k^n(R)$ is free for all n and $\mathrm{Der}(R) = \mathrm{der}(R)$.

<u>Theorem 3.6</u>: If $\delta_n \in \mathrm{Der}_k^n(R)$ for all n, then $\hat{R}$ is an integral domain.

<u>Proof</u>: We define a sequence of elements in R as follows:

$$(30) \qquad z_1 = y + \sum_{i=1}^{p-1} (-1)^i \frac{\delta_1^i(y)x^i}{i!}$$

$$z_n = z_{n-1} + \sum_{i=1}^{p-1} (-1)^i \frac{\delta^i_{p^{n-1}}(z_{n-1})x^{ip^{n-1}}}{i!}$$

Consider z_n. Since K is a separable algebraic extension of $k(x)$ and since $z_n \in K$, z_n satisfies a minimal polynomial $g(Z)$ with coefficients in $k(x)$ such that $g_Z \neq 0$. By multiplying g by some $d(x) \in k[x]$, g may be assumed to be in $k[x][Z]$. If g factors over $k[X,Z]$ so that $g = g_1g_2$, then either g_1 or g_2 is in $k[X]$ since $\deg_Z g = \deg_Z g_1 + \deg_Z g_2$ and g is the polynomial of minimal Z-degree which z_n satisfies.

Thus, g may be assumed to be irreducible over k. Thus, for each z_n there exists an irreducible polynomial $g(X,Z)$ with $g(x,z_n) = 0$ and $g_Z(x,z_n) \neq 0$.

We shall show that $\delta_{p^j} z_n = z_n \delta_{p^j}$ for $j < n$. We first consider δ_1.

$$\delta_1(z_1) = \delta_1(y) - \delta_1(y) - \delta_1(y)x + \delta_1(y)x + \cdots$$

$$+(-1)^{p-2}\delta_1^{p-1}(y)x^{p-2}/(p-2)! + (-1)^{p-1}\delta_1^{p-1}(y)x^{p-2}/(p-2)!$$

$$+(-1)^{p-1}\delta_1^{p}(y)x^{p-1}/(p-1)!$$

$$=(-1)^{p-1}\delta_1^{p}(y)x^{p-1}/(p-1)!$$

$$= 0$$

since $\delta_1^p(y) = 0$ by (17). Thus, by Proposition 3.5, $\delta_1 z_1 = z_1 \delta_1$.

Now we assume that $\delta_{p^j} z_{n-1} = z_{n-1}\delta_{p^j}$ for $j = 1, \cdots, n-2$. Evaluating $\delta_{p^{n-1}}(z_n)$, as above, gives that $\delta_{p^{n-1}}(z_n) = 0$. Also, since $\delta_{p^j} \circ \delta_{p^{n-1}} = \delta_{p^{n-1}} \circ \delta_{p^j}$ and $\delta_{p^j}(z_{n-1}) = 0$ for $j = 1, \cdots, n-2$, we have

$$\delta_{p^j}(z_n) = \delta_{p^j}(z_{n-1}) + \sum_{i=1}^{p-1}(-1)^i \frac{\delta^i_{p^{n-1}}\delta_{p^j}(z_{n-1})x^{ip^{n-1}}}{i!}$$

$$= 0.$$

Thus, $\delta_{p^j}(z_n) = 0$ for $j < n$. Hence by Proposition 3.5, $\delta_{p^j} z_n = z_n \delta_{p^j}$ for $j < n$.

Now z_n is a Cauchy sequence since $z_{n+1} - z_n \in m^{p^n}$. Let $z = \lim z_n$; $z \in \hat{R}$. Now δ_{p^j} is a continuous function on $\hat{R}$. Thus for $r \in \hat{R}$ with $r = \lim r_n, r_n \in R$, we have

$$\begin{aligned}
\delta_{p^j}(zr) &= \delta_{p^j}(\lim z_n \lim r_n) \\
&= \delta_{p^j}(\lim z_n r_n) \\
&= \lim \delta_{p^j}(z_n r_n) \\
&= \lim (z_n \delta_{p^j}(r_n)) \\
&= \lim z_n \lim \delta_{p^j}(r_n) \\
&= z\, \delta_{p^j}(\lim r_n) \\
&= z \delta_{p^j}(r).
\end{aligned}$$

Thus, $\delta_{p^j} z = z \delta_{p^j}$ for all j and hence, $\delta_i z = z \delta_i$ for all i.

Now $z = z_1 + (z_2 - z_1) + \cdots + (z_n - z_{n-1}) + \cdots$; so, $z = y + \sum_{i>0} \alpha_{ij} x^i y^j$. Hence, $y = z - \sum_{i>0} \alpha_{ij} x^i y^j$. We substitute for y on the right hand side of the equation; thus, $y = z - \sum_{i>0} \alpha_{ij} x^i (z - \sum_{i>0} \alpha_{ij} x^i y^j)^j$. Continue substituting for y. This gives that y may be written as $y = \sum \beta_{ij} x^i z^j$ and from this follows that every element $r \in \hat{R}$ is of the form $r = \sum \mu_{ij} x^i z^j$.

Suppose r is a zero divisor in $\hat{R}$. Then $r = \sum \alpha_{ij} x^i z^j$ with $\alpha_{ij} \in k$ and $\alpha_{00} = 0$. By Theorem 3.1, $\delta_1(r)$ is a zero divisor. Now $\delta_1(r) = \alpha_{10} + \sum \alpha_{ij} \delta_1(x^i z^j)$. $\delta_1(x^i z^j) = z^j \delta_1(x^i) \in (x,y)$ for $i + j \geq 2$, so, $\delta_1(r)$ is a unit unless $\alpha_{10} = 0$. Hence, $\alpha_{10} = 0$. Suppose $\alpha_{i0} = 0$ for $i < n$. Then, $\delta_n(r) = \alpha_{n0} + \sum \alpha_{ij} \delta_n(x^i z^j)$ is a zero divisor. Since $\delta_n(x^i z^j) \in (x,y)$, $\alpha_{n0} = 0$. Hence, we have shown that $\alpha_{i0} = 0$ for all i. Thus, elements of the form $\sum \alpha_{ij} x^i z^j$ with $\alpha_{I0} \neq 0$ for some I are not zero divisors in $\hat{R}$.

Now we suppose that $rs = 0$ with $r = \sum \alpha_{ij} x^i z^j$ and $s = \sum \beta_{ij} x^i z^j$. Then writing $r = z^{\ell} \sum_{j \geq \ell} \alpha_{ij} x^i z^{j-\ell}$ with $\alpha_{I\ell} \neq 0$ for some I, the above shows that $\sum_{j \geq \ell} \alpha_{ij} x^i z^{j-\ell}$ is not a zero divisor. Note that if r is a zero divisor, but not equal to zero, then ℓ must be greater than zero. Likewise $s = z^m \sum_{j \geq m} \beta_{ij} x^i z^{j-m}$ with $\beta_{I'm} \neq 0$ and $\sum_{j \geq m} \beta_{ij} x^i z^{j-m}$ is not a zero divisor. Hence, $z^{\ell} z^m = 0$ and since $\hat{R}$ has no nilpotent elements, $z = 0$. Thus, $r = 0$ and $\hat{R}$ is an integral domain. QED

<u>Theorem 3.7</u>: If $\mathrm{Der}_k^n(R)$ is a free R-module for all n and if $\mathrm{Der}(R) = \mathrm{der}(R)$, then $\hat{R}$ is an integral domain.

<u>Proof</u>: Since $\mathrm{Der}_k^1(R)$ is a free R-module, by Theorem 1.8 there exists a derivation λ_1 and a monomial x_1 such that $\lambda_1(x_1) = 1$. Because λ_1 is a 1st order derivation, x_1 can only be x or y. If $f_X(x,y) \neq 0$, then the curve does not distinguish between x and y since $f_Y(x,y) \neq 0$. Thus, without loss of generality we may assume $x_1 = x$. If $f_X(x,y) = 0$, then $f_X(x,y)\lambda_1(x) + f_Y(x,y)\lambda_1(y) = 0$. Hence, $\lambda_1(y) = 0$ and so, $x_1 = x$. Hence, we shall assume $x_1 = x$. Further, since λ_1 and δ_1 agree on $k(x)$ and since both extend uniquely to $k(x,y)$, $\lambda_1 = \delta_1$.

Now if $\delta_n \in \mathrm{Der}_k^n(R)$ for all n, then by Theorem 3.6 $\hat{R}$ is an integral domain. Thus, the only case we need consider is if some $\delta_n \notin \mathrm{Der}_k^n(R)$. Since $\delta_n = \delta_{p^t}^{\alpha_t}/\alpha_t! \circ \cdots \circ \delta_1^{\alpha_0}/\alpha_0!$, when $n = \sum_{i=0}^{t} \alpha_i p^i$, there must exist a positive integer N such that $\delta_i\colon R \to R$ for $i < p^N$, but $\delta_{p^N} \notin \mathrm{Der}_k^{p^N}(R)$.

If $\delta_1(y) = (\alpha+s)/(1+t)$ where $\alpha \neq 0$, $\alpha \in k$, and $s,t \in m$, let $y' = y - \alpha x$. Note that $y' \neq 0$ since R is not regular. Now $\delta_1(y') = (\alpha+s)/(1+t) - \alpha = (s-\alpha t)/(1+t) \in m$. Then since $k[x,y] = k[x,y']$ and $(x,y) = (x,y')$, $(k[x,y'])_{(x,y')} = R$. Let $g(X,Y') = f(X,Y' + \alpha X)$. Then $g(x,y') = 0$. Also,

$g_{Y'}(x,y') = f_{Y'}(x,y' + \alpha x) = f_Y(x,y)\,dY/dY' =$

$f_Y(x,y)\ d(Y' + \alpha X)/dY' = f_Y(x,y) \neq 0$ by the chain rule. Thus $g_{Y'}(x,y') \neq 0$. Thus we may assume that $\delta_1(y) \in m$.

We have then the following assumptions on R:

(31) $\quad \mathrm{Der}_k^n(R)$ is a free R-module for all n

$\mathrm{Der}(R) = \mathrm{der}(R)$

$f_Y(x,y) \neq 0$

$\mathrm{Der}_k^1(R) = \langle \delta_1 \rangle$

$\delta_1(y) \in m.$

Now we define z_n for $n \leq N$ as we did in (30). That is,

$$z_1 = y + \sum_{i=1}^{p-1} (-1)^i \frac{\delta_1^i(y)x^i}{i!}$$

$$z_n = z_{n-1} + \sum_{i=1}^{p-1} (-1)^i \frac{\delta^i_{p^{n-1}}(z_{n-1})x^{ip^{n-1}}}{i!} .$$

Let $z = z_N$. As in the previous theorem, $\delta_i(z) = 0$ for $i < p^N$. Thus, by Proposition 3.5, there exists an irreducible polynomial $g(X^{p^N},Z)$ such that $g(x^{p^N},z) = 0$ and $g_Z(x^{p^N},z) \neq 0$. Also, $\delta_i z = z\delta_i$ for $i < p^N$. We observe that $z_1 = y + xr_1(x,y)$ with $r_1(x,y) \in m$ since $\delta_1(y) \in m$. Thus,

(32) $\quad z = y + xr(x,y)$ for some $r(x,y) \in (x,y)$.

We now consider the ring $R_1 = (k[x,z])_{(x,z)}$. We shall show that $R_1 \subseteq R$. Let $s(x,z)/t(x,z) \in R_1$, with $s,t \in k[x,z]$ and $t \notin (x,z)$. Since $k[x,z] \subseteq k(x,y)$, $s,t \in k[x,y]$. $t \notin (x,z)$ implies that $t = \alpha + h(x,z)$ with α a non-zero constant in k and $h(x,z) \in (x,z)$. Thus, $h(x,z) \in (x,y)$ since $(x,z) \subseteq (x,y)$ and so, t is a non-unit in R. Hence, $s/t \in R$. Thus, $R_1 \subseteq R$.

We now show that $\hat{R}_1 = \hat{R}$. Since $z = y + xr(x,y)$, $y = z - xr(x,y)$. Substituting for y on the right hand side of the equation and continuing this process gives that $y = \sum \alpha_{ij} x^i z^j$ for some $\alpha_{ij} \in k$. Thus, $y \in \hat{R}_1$ and so, $\hat{R}_1 = \hat{R}$.

Let $K_1 = k(x,z)$. K_1 is a separable algebraic extension of $k(x)$ since $g_Z(x^{p^N},z) \neq 0$. Thus, δ_n extends uniquely to K_1 for all n. Since $\delta_i z = z\delta_i$ for $i < p^N$, $\delta_i : k[x,z] \to k[x,z]$. Hence, $\delta_i \in \mathrm{Der}_k^i(R_1)$ for all $i < p^N$. In fact, $\mathrm{Der}_k^n(R_1) = \langle \delta_1, \cdots, \delta_n \rangle$ for $n < p^N$.

We shall show that $\mathrm{Der}_k^n(R_1)$ is a free R_1-module for all n. In order to do this, we shall need to know that there exist derivations λ_i and monomials $x_i \in k[x,z] \subseteq R_1$ such that $\mathrm{Der}_k^n(R) = \langle \lambda_1, \cdots, \lambda_n \rangle$ and $\lambda_i(x_j) = \begin{cases} 0 & j < i \\ 1 & j = i \end{cases}$. Thus, we show this first. For $i < p^N$, we let $\lambda_i = \delta_i$ and $x_i = x^i$. Then clearly we have satisfied the desired requirements for λ_i and x_i.

Now consider $Der_k^{p^N}(R)$. By Theorem 1.6 $Der_k^{p^N}(R) = Der_k^{p^N-1}(R) \oplus R\gamma = \langle \delta_1, \cdots, \delta_{p^N-1} \rangle \oplus R\gamma$ where $\gamma \in Der_k^{p^N}(R)$. Further, there exists an element $r \in R$ such that $\gamma(r) = 1$. Now $r \in R \subseteq \hat{R} = \hat{R}_1$ so, $r = \sum_{0 \leq i+j} \alpha_{ij} x^i z^j$. Thus, $1 = \gamma(r) = \sum_{1 \leq i+j} \alpha_{ij} \gamma(x^i z^j)$. This implies that $\gamma(x^I z^J)$ must be a unit in R for some I and J. Let $\lambda_{p^N} = (1/\gamma(x^I z^J))\gamma$. Then $Der_k^{p^N}(R) = \langle \lambda_1, \cdots, \lambda_{p^N} \rangle$ where $\lambda_i = \delta_i$ for $i < p^N$. And we have shown that there is a monomial $x_{p^N} \in k[x,z] \subseteq R_1$ such that $\lambda_{p^N}(x_{p^N}) = 1$.

We now proceed by induction. Suppose $Der_k^{n-1}(R) = \langle \lambda_1, \cdots, \lambda_{n-1} \rangle$ and that there are monomials $x_1, \cdots, x_{n-1} \in R_1$ such that $\lambda_i(x_j) = \begin{cases} 0 & j < i \\ 1 & j = i \end{cases}$. Again we are taking $\lambda_i = \delta_i$ and $x_i = x^i$ for $i < p^N$. Now by Theorem 1.6, $Der_k^n(R) = \langle \lambda_1, \cdots, \lambda_{n-1}, \gamma \rangle$ where $\gamma(x_i) = 0$ for $i < n$ and $\gamma(r) = 1$ for some $r \in R$. As before $r = \sum \alpha_{ij} x^i z^j$ and so, $\gamma(x^I z^J)$ is an unit in R for some I and J. Thus there exists a monomial $x_n \in k[x,z]$ such that $\gamma(x_n)$ is a unit in R. Let $\lambda_n = \gamma/\gamma(x_n)$. Then $Der_k^n(R) = \langle \lambda_1, \cdots, \lambda_n \rangle$ and $\lambda_n(x_i) = \begin{cases} 0 & i < n \\ 1 & i = n \end{cases}$ with x_n a monomial.

We want to show that the λ_i's which have just been found are in fact derivations from R_1 to R_1. In order to do this we shall need to know that $R \cap k(x,z) = R_1$. To see that this is the case we consider the following: $R_1 \subseteq k(x,z) \cap R \subseteq k(x,z) \cap \hat{R} = k(x,z) \cap \hat{R}_1$. Since $\otimes_{R_1} \hat{R}_1$ is exact [Cor. 17.11,p.57;5], $k(x,z) \cap \hat{R}_1 = R_1$ [Theorem 8.4,p.59;5]. Hence, $R_1 = k(x,z) \cap R$.

As we have already seen, $\lambda_1 = \delta_1 : R_1 \to R_1$. Suppose inductively that $\lambda_1, \cdots, \lambda_{n-1} : R_1 \to R_1$. Then $\lambda_i : K_1 \to K_1$ for $i < n$. Now $\lambda_1, \cdots, \lambda_n$ are a basis for $\mathrm{Der}^n_k(K)$ and $\delta_n \in \mathrm{Der}^n_k(K)$ so, $\delta_n = \sum_{i=1}^{n} r_i\lambda_i$ with $r_i \in K$ and $r_n \neq 0$. We show that $r_i \in K_1$. Since $\delta_n \in \mathrm{Der}^n_k(K_1)$, $\delta_n(x_1) = r_1 \in K_1$ (in fact, $r_1 = 0$). Suppose $r_1, \cdots, r_{j-1} \in K_1$. Then $\delta_n(x_j) = \sum_{i=1}^{n} r_i\lambda_i(x_j) = \sum_{i=1}^{j} r_i\lambda_i(x_j)$ which implies that $r_j = \delta_n(x_j) - \sum_{i=1}^{j-1} r_i\lambda_i(x_j) \in K_1$. Thus, $r_i \in K_1$ for $i = 1, \cdots, n$. Now $\lambda_n = \delta_n/r_n - \sum_{i=1}^{n-1} r_i\lambda_i/r_n$; $\lambda_n : R_1 \to R$ while $\delta_n/r_n - \sum_{i=1}^{n-1} r_i\lambda_i/r_n : R_1 \to K_1$. Thus, $\lambda_n : R_1 \to R \cap K_1 = R_1$.

Thus, for all i, $\lambda_i \in \mathrm{Der}^i_k(R_1)$. Also, there exist monomials $x_i \in R_1$ such that $\lambda_i(x_j) = \begin{cases} 0 & j < i \\ 1 & j = i \end{cases}$. Thus, by Theorem 1.5, $\mathrm{Der}^n_k(R_1)$ is a free R_1-module generated by $\lambda_1, \cdots, \lambda_n$; this holds for all n. Further, we have that $\lambda_i = \delta_i$ and $x_i = x^i$ for $i < p^N$.

By assumption $\delta_{p^N}: R \not\to R$. We want to show the same is true for R_1; that is, $\delta_{p^N}: R_1 \not\to R_1$. Since $\delta_1, \cdots, \delta_{p^N}$ are a free basis for $\mathrm{Der}_k^{p^N}(K)$, $\lambda_{p^N} = r\delta_{p^N} + \sum_{i=1}^{p^N-1} r_i\delta_i$. But $\lambda_{p^N}(x^i) = \lambda_{p^N}(x_i) = 0$ for $i < p^N$, so, $r_i = 0$ for $i < p^N$. Thus, $\lambda_{p^N} = r\delta_{p^N}$. Now $r = \lambda_{p^N}(x^{p^N}) \in R$. Since $\delta_{p^N}: R \not\to R$, $r \in (x,y)$. Also, $1 = \lambda_{p^N}(x_{p^N}) = r\delta_{p^N}(x_{p^N})$ so, $\delta_{p^N}(x_{p^N}) = 1/r \notin R$. Now $x_{p^N} \in R_1$; if $\delta_{p^N}: R_1 \to R_1$, then $1/r = \delta_{p^N}(x_{p^N}) \in R_1 \subseteq R$ which is a contradiction. Thus, $\delta_{p^N}: R_1 \not\to R_1$. And further we have

$$(33) \qquad \lambda_{p^N} = r\delta_{p^N} \quad \text{where} \quad r = \lambda_{p^N}(x^{p^N}) \in (x,z).$$

Finally for R_1, we show that $\mathrm{Der}(R_1) = \mathrm{der}(R_1)$. It suffices to show λ_n is generated by p^i-th order derivations for all n. Define $\gamma_m \in \mathrm{Der}_k^m(R)$ as follows:

$$(34) \qquad \gamma_m = \lambda_{p^M}^{\alpha_M}/\alpha_M! \circ \cdots \circ \lambda_1^{\alpha_0}/\alpha_0! \quad \text{where} \quad m = \sum_{i=0}^{M} \alpha_i p^i.$$

By Theorem 3.2 $\mathrm{Der}_k^n(R) = \langle \gamma_1, \cdots, \gamma_n \rangle$. So, $\lambda_n = \sum_{i=1}^{n} r_i\gamma_i$ with $r_i \in R$. On the other hand, it is clear that $\gamma_n \in \mathrm{Der}_k^n(R_1)$ so, $\gamma_n = \sum_{i=1}^{n} t_i\lambda_i$ with $t_i \in R_1$. By

Corollary 3.3 r_n and t_n are units in R. Thus, $r_n = 1/t_n \in K_1 \cap R = R_1$ and so, t_n is a unit in R_1.

So, $\lambda_n = \gamma_n/t_n - \sum_{i=1}^{n-1} t_i\lambda_i/t_n$. Assume by induction that for $i < n$, $\lambda_i = \sum_{j=1}^{i} s_{ij}\gamma_j$ with $s_{ij} \in R_1$. We can do this since $\lambda_1 = \gamma_1$. Then $\lambda_n = \gamma_n/t_n - \sum_{i=1}^{n-1} t_i(\sum_{j=1}^{i} s_{ij}\gamma_j)/t_n$. Hence, $\lambda_n - (1/t_n)\lambda_{p^t}^{\alpha_t}/\alpha_t! \circ \cdots \circ \lambda_1^{\alpha_1}/\alpha_0! \in \mathrm{Der}_k^{n-1}(R_1)$. Thus, λ_n is generated by composites of p^i-th order derivations. Hence $\mathrm{Der}(R_1) = \mathrm{der}(R_1)$.

We have shown then that the following hold for R_1:

(35) $\mathrm{Der}_k^n(R_1) = \langle \lambda_1, \cdots, \lambda_n \rangle$ where λ_i is also an i-th order derivation of R to R.

There exist $x_i \in R_1$ such that $\lambda_i(x_j) = \begin{cases} 0 & j < i \\ 1 & j = i \end{cases}$.

$\lambda_i = \delta_i$ and $x_i = x^i$ for $i < p^N$.

$\lambda_i z = z\lambda_i$ for $i < p^N$.

$\mathrm{Der}(R_1) = \mathrm{der}(R_1)$ and in fact $\mathrm{Der}_k^n(R_1) = \langle \gamma_1, \cdots, \gamma_n \rangle$ where $\gamma_m = \lambda_{p^M}^{\alpha_M}/\alpha_M! \circ \cdots \circ \lambda_1^{\alpha_0}/\alpha_0!$, $m = \sum_{i=0}^{M} \alpha_i p^i$.

Let $R_2 = (k[x^{p^N}, z])_{(x^{p^N}, z)}$. We still have $g(x^{p^N}, z) = 0$ and $g_z(x^{p^N}, z) \neq 0$. Just as R_1 was contained in R so too is $R_2 \subseteq R_1$. We shall show that all the assumptions on R which are given in (31) also hold for R_2. Before we do this however, we observe that if $\hat{R}_2$ is a domain then so is $\hat{R} = \hat{R}_1$. Suppose $\hat{R}$ is not a domain. Then there exists $r \neq 0$ and $s \neq 0$ such that $rs = 0$. By Chevalley's Theorem $\hat{R}$ has no nilpotent elements so, $r^{p^N} \neq 0$ and $s^{p^N} \neq 0$. But $r^{p^N} s^{p^N} = 0$ and $r^{p^N}, s^{p^N} \in \hat{R}_2$. Thus, if $\hat{R}_2$ is a domain, either $r = 0$ or $s = 0$.

An important relationship between the derivations λ_n and R_2 is that $\lambda_i(r) = 0$ and $\lambda_i r = r\lambda_i$ when $r \in R_2$ and $i < p^N$. Also, if $p^N \not| \, n$, then $\gamma_n(r) = 0$ for $r \in R_2$. To see this we write n in its p-adic expansion as $n = \sum_{i=0}^{t} \alpha_i p^i$. Since $p^N \not| \, n$, some $\alpha_i \neq 0$ for $i < N$. Let $I < p^N$ be the smallest i such that $\alpha_I \neq 0$. Then $\gamma_n = \lambda_{p^t}^{\alpha_t}/\alpha_t! \circ \cdots \circ \lambda_{p^I}^{\alpha_I}/\alpha_I!$. Since $\lambda_{p^I}(r) = 0$ for $r \in R_2$, $\gamma_n(r) = 0$. Since $\lambda_i = \delta_i$ for $i < p^N$, this relationship also holds for $\delta_n \in \mathrm{Der}_k^n(K)$. That is, if $p^N \not| \, n$, then $\delta_n(r) = 0$ for $r \in R_2$.

Before we study R_2 further, we make an observation about zero divisors in $\hat{R}$. For any $r \in (x,y)\hat{R}$, we write r as

$$(36) \qquad r = \sum_{i=1}^{p^N-1} \beta_i x^i + \sum_{i=0}^{p^N-1} r_i x^i$$

where $\beta_i \in k$ and $r_i \in (x^{p^N},z)k[[x^{p^N},z]]$; we can do this since $\hat{R} = \hat{R}_1$. If r is a zero divisor, then by Lemma 3.1 $\delta_n(r)$ is also a zero divisor for $n < p^N$. Since δ_n is linear with respect to R_2, we have

$$\delta_n(r) = \beta_n + \sum_{i=n+1}^{p^N-1} \beta_i \delta_n(x^i) + \sum_{i=0}^{p^N-1} r_i \delta_n(x^i).$$

Since all terms but the first are in $(x,y)\hat{R}$, β_n must zero. Thus, $\beta_i = 0$ for $i = 1,\cdots, p^N-1$. Hence, a zero divisor in $\hat{R}$ has the form

$$r = \sum_{i=0}^{p^N-1} r_i x^i \tag{37}$$

where $r_i \in (x^{p^N},z)k[[x^{p^N},z]]$.

We shall show that the derivations γ_{np^N}, $n=1,2,\cdots$, give rise to generators which freely generate $\mathrm{Der}_k^n(R_2)$ for all n. We make use of the fact that δ_{np^N} is an n-th order derivation on $k[x^{p^N}]$ [I, Theorem 14; 6] and that δ_{np^N} extends uniquely to $k(x^{p^N},z) = K_2$ and is an n-th order derivation on K_2.

Now consider γ_{np^N}; $\gamma_{np^N} = \sum_{i=1}^{np^N} r_i \delta_i$ with $r_i \in K$.

For $r \in R_2$, $\gamma_{np^N}(r) = \sum_{i=1}^{np^N} r_i \delta_i(r) = \sum_{j=1}^{n} r_{jp^N} \delta_{jp^N}(r)$.

So, $\gamma_{np^N} \in \mathrm{Der}_k^n(K_2,K)$.

We first show that there exist monomials $y_n \in k[x^{p^N},z]$ such that $\gamma_{np^N}(y_n)$ is a unit in R_1. Suppose $\gamma_{p^N}(r) \in (x,z)$ for all $r \in k[x^{p^N},z]$. Since $\gamma_{p^N}(k[x,z]) \not\subseteq (x,z)$, there exists some monomial x^iz^i such that $\gamma_{p^N}(x^iz^j)$ is a unit in R_1. Clearly $i > 0$, since $\gamma_{p^N}(k[x^{p^N},z]) \subseteq (x,z)$. Also, $p^N \nmid i$, otherwise $x^iz^j \in k[x^{p^N},z]$. Thus, there exists an element of the form $x^js \in k[x,z] \subseteq R_1$ such that $\gamma_{p^N}(x^js)$ is a unit in R_1, $s \in k[x^{p^N},z]$ and j is as small as possible with $0 < j < p^N$. Consider the derivation $\gamma_{p^N+(p^N-j)} = \gamma_{p^N} \circ \gamma_{p^N-j}$. For any x^tr where $0 \leq t < p^N$ and $r \in R_2$ we have

$$\gamma_{p^N} \circ \gamma_{p^N-j}(x^tr) = \gamma_{p^N} \circ \delta_{p^N-j}(x^tr)$$

$$= \gamma_{p^N}(r\delta_{p^N-j}(x^t)).$$

Now for $t \geq p^N-j$

$$\delta_{p^N-j}(x^t) =$$

$$\sum_{s=0}^{p^N-j-1} (-1)^s \binom{t}{p^N-j-s} \binom{t-p^N+j+s-1}{s} x^{t-p^N+j+s} \delta_{p^N-j}(x^{p^N-j-s})$$

$$= \binom{t}{p^N-j} x^{t-p^N+j}$$

[I, Prop. 9;6]. So,

$$\gamma_{p^N} \circ \gamma_{p^N-j}(x^t r) = \begin{cases} \binom{t}{p^N-j} \gamma_{p^N}(rx^{t-p^N+j}) & p^N-j \leq t < p^N \\ 0 & 0 \leq t < p^N-j \end{cases}$$

By assumption $\gamma_{p^N}(x^t r) \in m$ since $t-p^N+j < j$. Thus, $\gamma_{p^N+p^N-j}(s) \in m$ for all $s \in R_1$ which is a contradiction to Corollary 3.4. Thus, there exists a monomial $y_1 \in k[x^{p^N}, z]$ such that $\gamma_{p^N}(y_1)$ is a unit in R_1. Let $\gamma'_{p^N} = \gamma_{p^N}/\gamma_{p^N}(y_1)$.

Suppose we have found derivations $\gamma'_{ip^N} \in \mathrm{Der}_k^{ip^N}(R_1)$ and monomials $y_i \in k[x^{p^N}, z]$ such that the following hold:

$\gamma'_{ip^N} = r\gamma_{ip^N} + \sum_{j=1}^{i-1} r_j \gamma_{jp^N}$ with $r_j \in R_1$, r a unit in R_1

$$\gamma'_{ip^N}(y_j) = \begin{cases} 0 & j < i \\ 1 & j = i \end{cases}$$

for $i < n$. Let $\bar{\gamma}_{np^N} = \gamma_{np^N} - \sum_{i=1}^{n-1} r_i \gamma'_{ip^N}$ where $r_1 = \gamma_{np^N}(y_1)$, $r_j = \gamma_{np^N}(y_j) - \sum_{i=1}^{j-1} r_i \gamma'_{ip^N}(y_j)$. So, $r_i \in R_1$. Then by construction $\bar{\gamma}_{np^N}(y_i) = 0$ for $i < n$.

Suppose $\bar{\gamma}_{np^N}(r) \in (x,z)$ for all $r \in k[x^{p^N},z]$. By Corollary 3.4 there exists $s \in R_1$ such that $\bar{\gamma}_{np^N}(s)$ is a unit in R_1. Again choose j as small as possible so that $\bar{\gamma}_{np^N}(x^j\bar{r})$ is a unit in R_1, $0 < j < p^N$ and $\bar{r} \in k[x^{p^N},z]$. Then as before one shows that

$$\bar{\gamma}_{np^N} \circ \delta_{p^N-j} = \gamma_{np^N+p^N-j} + \sum_{i=1}^{n-1} r_i \gamma_{ip^N+p^N-j} : R_1 \to (x,z)$$

contradicting Corollary 3.4. Thus, there is a monomial $y_n \in k[x^{p^N},z]$ such that $\bar{\gamma}_{np^N}(y_n)$ is a unit in R_1. Let $\gamma'_{np^N} = \bar{\gamma}_{np^N}/\bar{\gamma}_{np^N}(y_n)$. This completes the induction step.

Thus, we have constructed derivations γ'_{np^N} and monomials $y_n \in k[x^{p^N},z]$ which satisfy the following properties:

γ'_{np^N} is an n-th order derivation from K_2 to K and and np^N-th order derivation from R_1 to R_1.

$\gamma'_{np^N} = r\gamma_{np^N} + \sum_{i=1}^{n-1} r_i \gamma_{ip^N}$ where $r_i \in R_1$ and r is a unit in R_1.

$$\gamma'_{np^N}(y_i) = \begin{cases} 0 & i < n \\ 1 & i = n \end{cases}.$$

If $p^N \nmid m$, define $\gamma'_m = \gamma_m$. So, γ'_n is defined for all n and $\gamma'_n \in \mathrm{Der}_k^n(R_1)$. We now show by induction that $\mathrm{Der}_k^n(R_1) = \langle \gamma'_1, \cdots, \gamma'_n \rangle$. The first step is clear.

Since $\delta_1 = \lambda_1 = \gamma_1 = \gamma_1'$, $\mathrm{Der}_k^1(R_1) = \langle \gamma_1' \rangle$. Suppose $\mathrm{Der}_k^{n-1}(R_1) = \langle \gamma_1', \cdots, \gamma_{n-1}' \rangle$. It suffices to show that $\gamma_n = \sum_{i=1}^{n} s_i \gamma_i'$ for some $s_i \in R_1$. If $p^N \nmid n$, $\gamma_n = \gamma_n'$. If $p^N \mid n$, so that $n = \bar{n}p^N$, then $\gamma_n = \gamma_{\bar{n}p^N} = \gamma'_{\bar{n}p^N}/r - \sum_{i=1}^{\bar{n}-1} r_i \gamma_{ip^N}/r = \gamma'_{\bar{n}p^N}/r + \sum_{i=1}^{\bar{n}p^N-1} s_i \gamma_i'$ by the induction hypothesis. Thus, $\mathrm{Der}_k^n(R_1) = \langle \gamma_1', \cdots, \gamma_n' \rangle$. We also have that $\mathrm{Der}_k^n(K_1) = \langle \gamma_1', \cdots, \gamma_n' \rangle$. So, $\delta_{np^N} = \sum_{i=1}^{np^N} t_i \gamma_i'$ for some $t_i \in K_1$. On R_2 we have $\delta_{np^N} = \sum_{j=1}^{n} t_{jp^N} \gamma'_{jp^N}$ since for $p^N \nmid i$, $\gamma_i'(s) = \gamma_i(s) = 0$ when $s \in R_2$.

We shall show that $\gamma'_{np^N}: R_2 \to R_2$ for all n. In order to do this, we shall need to know that $R_1 \cap K_2 = R_2$; so, we prove this first. Suppose $r(x^{p^N}, z)/s(x^{p^N}, z) = u(x,z)/v(x,z)$ in R_1 with $r,s,u,v, \in k[x,z]$ and $v(x,z)$ a unit in R_1. Then pulling back to $k[X,Z]$ gives

$$r(X^{p^N}, Z)v(X,Z) - s(X^{p^N}, Z)u(X,Z) = h(X,Z)g(X^{p^N}, Z).$$

Write $v(X,Z) = \sum_{i=0}^{p^N-1} v_i(X^{p^N}, Z)X^i$. Do the same for u and h. Then

$$r(X^{p^N},Z)(v_o+\cdots+v_{p^N-1}X^{p^N-1}) - s(X^{p^N},Z)(u_o+\cdots+u_{p^N-1}X^{p^N-1})$$
$$= (k_o+\cdots+k_{p^N-1}X^{p^N-1})g(X^{p^N},Z)$$

and so,

$$r(X^{p^N},Z)v_o(X^{p^N},Z) - s(X^{p^N},Z)u_o(X^{p^N},Z) = k_o(X^{p^N},Z)g(X^{p^N},Z)$$

since all other terms involve X^i, $0 < i < p^N$. Since $v(x,z)$ is a unit in R_1, $v(X,Z)$ begins with a constant term. Thus, $v_o(x^{p^N},z)$ is a unit in R_2. Hence, $r(x^{p^N},z)/s(x^{p^N},z) = u_o(x^{p^N},z)/v_o(x^{p^N},z) \in R_2$. Therefore, $K_2 \cap R_1 = R_2$.

We now show that $\gamma'_{np^N}:R_2 \to R_2$. We first consider γ'_{p^N}. Since $\gamma'_{p^N} = u\lambda_{p^N}$ where u is a unit in R_1, we have by (33) that $\gamma'_{p^N} = r\delta_{p^N}$ where $r = \gamma'_{p^N}(x^{p^N}) \in R_1$. We have $1 = \gamma'_{p^N}(y_1) = r\delta_{p^N}(y_1)$. Since $\delta_{p^N}:K_2 \to K_2$, $r = 1/\delta_{p^N}(y_1) \in K_2$. Now $\gamma'_{p^N}:R_2 \to R_1$ and $r\delta_{p^N}:R_2 \to K_2$; thus, $\gamma'_{p^N}:R_2 \to R_1 \cap K_2 = R_2$.

Inductively we assume $\gamma'_{ip^N}:R_2 \to R_2$ for $i < n$. Recall that δ_{np^N} when restricted to R_2 may be written as $\delta_{np^N} = \sum_{i=1}^{n} t_i\gamma'_{ip^N}$, with $t_i \in K_1$ and $t_n \neq 0$. Evaluating δ_{np^N} at y_i gives $t_i \in K_2$ since

$\delta_{np^N}: K_2 \to K_2$. So, $\gamma'_{np^N} = \delta_{np^N}/t_n - \sum_{i=1}^{n-1} t_i \gamma'_{ip^N}/t_n : R_2 \to R_1 \cap K_2 = R_2$. Thus, by Theorem 1.5 $\mathrm{Der}_k^n(R_2)$ is a free R_2-module generated by $\gamma'_{p^N}, \cdots, \gamma'_{np^N}$. We should again note that γ'_{np^N} is also an np^N-th order derivation from R to R.

Finally we show that $\mathrm{Der}(R_2) = \mathrm{der}(R_2)$. Let $\sigma_m = \gamma'^{\alpha_M}_{p^M}/\alpha_M! \circ \cdots \circ \gamma'^{\alpha_0}_1/\alpha_0!$ where the p-adic expansion of m is given by $m = \sum_{i=0}^{M} \alpha_i p^i$. By Theorem 3.4 $\mathrm{Der}_k^n(R_1) = \langle \sigma_1, \cdots, \sigma_n \rangle$. To prove that $\mathrm{Der}(R_2) = \mathrm{der}(R_2)$, it suffices to show for all n that

$$\gamma'_{np^N} = \sum_{i=1}^{n} r_i \sigma_{ip^N} \tag{38}$$

with $r_i \in R_2$. To see this suppose that (38) holds. We first observe that σ_{jp^N} is a j-th order derivation on R_2. We write $j = \sum_{i=0}^{J} \alpha_i p^i$. Then $jp^N = \sum_{i=0}^{J} \alpha_i p^{i+N}$. Thus, $\sigma_{jp^N} = \gamma'^{\alpha_J}_{p^{J+N}}/\alpha_J! \circ \cdots \circ \gamma'^{\alpha_0}_{p^N}/\alpha_0!$. Since $\gamma'_{ip^N}: R_2 \to R_2$, $\sigma_{jp^N}: R_2 \to R_2$. Further, since $\gamma'_{p^{n+i}}$ is a p^i-th order derivation on R_2, σ_{jp^N} has order $\sum_{i=0}^{J} \alpha_i p^i = j$. Now let $\lambda \in \mathrm{Der}(R_2)$ and suppose that n is the smallest integer such that $\lambda \in \mathrm{Der}_k^n(R_2)$. Write n

in its p-adic expansion as $n = \sum_{i=0}^{s} \alpha_i p^i$. Since $\mathrm{Der}_k^n(R_2) = \langle \gamma'_{p^N}, \ldots, \gamma'_{np^N} \rangle$, $\lambda = \sum_{i=1}^{n} t_i \gamma'_{ip^N}$ with $t_i \in R_2$ and $t_n \neq 0$. Using (38) and the above remark, we have that $\lambda - t_n r_n \sigma_{np^N} \in \mathrm{Der}_k^{n-1}(R_2)$. Thus, $\lambda - t_n r_n (\gamma'^{\alpha_s}_{p^{N+s}}/\alpha_s! \circ \cdots \circ \gamma'^{\alpha_0}_{p^N}/\alpha_0!) \in \mathrm{Der}_k^{n-1}(R_2)$ where $\gamma_{p^{N+i}} \in \mathrm{Der}_k^{p^i}(R_2)$ and $\sum_{i=0}^{s} \alpha_i p^i = n$. Thus, if (38) holds, $\mathrm{Der}(R_2) = \mathrm{der}(R_2)$.

We now show (38). The result is true for $n = 1$ since $\sigma_{p^N} = \gamma'_{p^N}$. Assume it holds for $i < n$. Now $\sigma_{np^N} \in \mathrm{Der}_k^{np^N}(R_2)$ so, $\sigma_{np^N} = \sum_{i=1}^{n} u_i \gamma'_{ip^N}$, $u_i \in R_2$. In R_1, $\gamma'_{np^N} = \sum_{i=1} t_i \sigma_i$ with $t_i \in R_1$. By Corollary 3.5 u_n and t_{np^N} are units in R_1, so, $t_{np^N} = 1/u_n \in K_2 \cap R_1 = R_2$. So, u_n is a unit in R_2. Hence, $\gamma'_{np^N} = \sigma_{np^N}/u_n - \sum_{i=1}^{n-1} u_i \gamma'_{ip^N}/u_n = \sigma_{np^N}/u_n + \sum_{i=1}^{n-1} r_i \sigma_{ip^N}$ with $r_i \in R_2$ and (38) is proven.

Thus we have shown that $\mathrm{Der}_k^n(R_2)$ is a free R_2-module for all n and $\mathrm{Der}(R_2) = \mathrm{der}(R_2)$.

We now examine $\mathrm{Der}_k^1(R_2)$ more closely. We know $g_Z(x^{p^N}, z) \neq 0$. We shall also show that $g_{x^{p^N}}(x^{p^N}, z) \neq 0$.

In $k(x^{p^N},z)g_{x^{p^N}}(x^{p^N},z)\delta_{p^N}(x^{p^N}) + g_z(x^{p^N},z)\delta_{p^N}(z) = 0$ since δ_{p^N} is a first order derivation on $k(x^{p^N},z)$. If $g_{x^{p^N}}(x^{p^N},z) = 0$, then $\delta_{p^N}(z) = 0$. Then by Proposition 3.5, $\delta_{p^N}z = z\delta_{p^N}$. If this were the case then $\delta_{p^N}:R_1 \to R_1$ which does not happen. Thus, $g_{x^{p^N}}(x^{p^N},z) \neq 0$.

Since y_1 is the monomial in $k[x^{p^N},z]$ paired with the first order derivation γ'_{p^N}, it must be either z or x^{p^N}. But $\gamma'_{p^N} = r\delta_{p^N}$ where $r = \gamma'_{p^N}(x^{p^N})$. Since $\delta_{p^N}:R_2 \not\to R_2$, $\gamma'_{p^N}(x^{p^N})$ is not a unit in R_2. Hence, y_1 must be z.

Let δ_i^2 represent the canonical derivations on $k[z]$. That is, $\delta_i^2(z^j) = \begin{cases} 0 & j<i \\ 1 & j=i \end{cases}$. Since $g_{x^{p^N}}(x^{p^N},z) \neq 0$, δ_i^2 extends uniquely to K_2. To summarize then, we have the following:

(39) $\quad\mathrm{Der}_k^n(R_2)$ is free for all n.

$\mathrm{Der}(R_2) = \mathrm{der}(R_2)$.

$g_{x^{p^N}}(x^{p^N},z) \neq 0$.

$\mathrm{Der}_k^1(R_2) = \langle \delta_1^2 \rangle$; in fact, $\delta_1^2 = \gamma'_{p^N}$.

$$\delta_1^2(x^{p^N}) \in (x^{p^N}, z).$$

Thus, all the hypotheses that we originally had for R, which are listed in (31), hold for R_2. Here z plays the role of x and x^{p^N} plays the role of y.

There are two cases. If $\delta_i^2: R_2 \to R_2$ for all i, then by Theorem 3.8 $\hat{R}_2$ is a domain. Hence, $\hat{R}$ is a domain. The second case is that there exists $N(1)$ such that $\delta_i: R_2 \to R_2$ for $i < p^{N(1)}$, but $\delta_{p^{N(1)}}: R_2 \not\to R_2$. We now proceed exactly as before and construct rings R_3 and R_4. $R_3 = (k[u,z])_{(u,z)}$ and $R_4 = (k[u, z^{p^{N(1)}}])_{(u, z^{p^{N(1)}})}$. Here u plays the same role that z played in R_1 and R_2. Hence, $u = x^{p^N} + zr(x^{p^N}, z)$ for some $r(x^{p^N}, z) \in (x^{p^N}, z)$; this is equation (32). Since $z \in (x,y)$, $u \in (x,y)^2$. We also have that $\mathrm{Der}_k^n(R_2) = < \delta_1^2, \cdots, \delta_n^2 >$ for $n < p^{N(1)}$ and $\delta_i^2 r = r\delta_i^2$ for $i < p^{N(1)}$ and $r \in R_4$. Further, δ_i^2, $i < p^{N(1)}$, may be viewed as a derivation on R since $\mathrm{Der}_k^n(R_2) = < \gamma'_{p^N}, \cdots, \gamma'_{np^N} >$ and $\gamma'_{ip^N}: R \to R$.

Now any element $r_i \in (x^{p^N}, z)\hat{R}_2$ may be written as

$$\text{(40)} \qquad r_i = \sum_{j=1}^{p^{N(1)}-1} \beta_{ij} z^j + \sum_{j=0}^{p^{N(1)}-1} r_{ij} z^j$$

where $\beta_{ij} \in k$ and $r_{ij} \in (u, z^{p^{N(1)}})k[[u, z^{p^{N(1)}}]]$.

This is just equation (36) with $\hat{R}_2$ playing the role of $\hat{R}$, u playing the role of z, and z playing the role of x.

We now consider $r \in (x,y)\hat{R}$. Suppose r is a zero divisor. Then by (37) r has the form $r = \sum_{i=0}^{p^N-1} r_i x^i$.

Using (40) we substitute for r_j:

$$r = \sum_{i=0}^{p^N-1} \sum_{j=1}^{p^{N(1)}-1} \beta_{ij} x^i z^j + \sum_{i=0}^{p^N-1} \sum_{j=0}^{p^{N(1)}-1} r_{ij} x^i z^j .$$

Here $\beta_{ij} \in k$ and $r_{ij} \in (u, z^{p^{N(1)}})k[[u, z^{p^{N(1)}}]] \subseteq (x,y)^2\hat{R}$.

We now apply $\delta^2_{p^{N(1)}-1} \circ \delta_{p^N-1}$ to r:

$$\delta^2_{p^{N(1)}-1} \circ \delta_{p^N-1}(r) = \beta_{p^{N}-1,\, p^{N(1)}-1}$$

$$+ \sum_{i=0}^{p^N-1} \sum_{j=0}^{p^{N(1)}-1} r_{ij}\, \delta^2_{p^{N(1)}-1} \circ \delta_{p^N-1}(x^i z^j) .$$

Since $\delta^2_{p^{N(1)}-1} \circ \delta_{p^N-1}(r)$ is a zero divisor,

$\beta_{p^N-1,\, p^{N(1)}-1} = 0$. If we continue evaluating r at

$\delta^2_{p^{N(1)}-2} \circ \delta_{p^N-1}, \ldots, \delta^2_1 \circ \delta_{p^N-1}, \delta^2_{p^{N(1)}-1} \circ \delta_{p^N-2}, \ldots, \delta^2_1,$

we get $\beta_{ij} = 0$ for $0 \leq i < p^N$ and $0 < j < p^{N(1)}$.

Thus, if r is a zero divisor $r \in (x,y)^2\hat{R}$.

We continue this process and construct a sequence of rings R_{2j} such that R_{2j} relative to $R_{2(j-1)}$ satisfies the analogous properties listed in (39). We denote the canonical derivations on R_{2j} by δ_i^{2j}. There are two cases. The first is that there exists j such that $\delta_i^{2s}: R_{2J} \to R_{2J}$ for all i. Then by Theorem 3.6, $\hat{R}_{2J}$ is a domain. This implies that $\hat{R}_{2(J-1)}$ is a domain. Hence, $\hat{R}$ is a domain. The second case is that for all j there exists N(j) such that $\delta^{2j}_{p^{N(j)}}: R_{2j} \not\rightarrow R_{2j}$. In this case we have that for a zero divisor $r \in \hat{R}$, $r \in (x,y)^n \hat{R}$ for all n. Since $\bigcap_n (x,y)^n \hat{R} = 0$, $r = 0$. Thus, in either case we have that $\hat{R}$ is an integral domain. QED

The next theorem gives a geometric interpretation to this result: $\hat{R}$ is an integral domain only if Γ is unibranched at the origin. Algebraically this means that $f(X,Y) = (\alpha X + \beta Y)^n + f_{n+1} + \cdots + f_m$.

Theorem 3.8: Let R be the local ring of the irreducible curve f(X,Y) at (0,0) over an algebraically closed field k. Suppose f has r distinct branches at (0,0). Then the integral closure $\bar{R}$ of R has r maximal ideals and the completion of R is $\hat{R} = R_1 \oplus \cdots \oplus R_r$.

Proof: Consider the integral closure $\bar{R}$ of R. It is a semilocal ring with maximal ideals $m_1, \cdots, m_t$. $\bar{R}_{m_i}$ is a discrete rank 1 valuation ring so, $\hat{\bar{R}}_{m_i} \cong k[[t]]$.

Hence, $R \longrightarrow k[[t]]$. Consider the image of (x,y) in $k[[t]]$, say, $(\xi(t),\eta(t))$. Since $f(x,y) = 0$, we have $f(\xi(t),\eta(t)) = 0$. Thus, m_i determines a branch of $f(x,y)$.

Now suppose $m_i \neq m_j$ determine the same branch. Then $\hat{\bar{R}}_{m_i} \underset{\theta_1}{\cong} k[[t]]$ with $(x,y) \xrightarrow{\theta_1} (\xi_1(t),\eta_1(t))$ and $\hat{\bar{R}}_{m_j} \underset{\theta_2}{\cong} k[[t]]$ with $(x,y) \xrightarrow{\theta_2} (\xi_2(t),\eta_2(t))$. Since m_i and m_j determine the same branch, there exists a substitution σ of order 1 such that $\sigma(\xi_1(t),\eta_1(t)) = (\xi_2(t),\eta_2(t))$ [Theorem 12.3; 8]. Let K be the quotient field of R. Since k is algebraically closed, K is the quotient field of $\hat{\bar{R}}_{m_i}$ and $\hat{\bar{R}}_{m_j}$. So, on K we have $\sigma \circ \theta_1 = \theta_2 : K \to k((t))$. Now since $m_i \neq m_j$ choose $r \in m_i$ such that $r \notin m_j$. Then $\theta_1(r) \in (t)$ so, $\sigma \circ \theta_1(r) \in (t)$ but $\theta_2(r) \notin (t)$; this is a contradiction. Therefore, distinct maximal ideals determine distinct branches. So, $t \leq r$.

Consider a branch γ_i. This branch determines a local homomorphism $\theta_i : R \to k[[t]]$. θ_i extends to K so, $\theta_i : K \to k[[t]]$. Consider $\theta_i^{-1}(t) \cap \bar{R}$; this is prime hence, maximal in $\bar{R}$. Suppose $\theta_i^{-1}(t) \cap \bar{R} = \theta_j^{-1}(t) \cap \bar{R} = m$.

Then

$$\begin{tikzcd} \hat{R}_m \arrow[r, "\theta_i"] \arrow[dr, "\theta_j"'] & k[[t]] \arrow[d, dotted, "\theta_i \circ \theta_j^{-1}"] \\ & k[[t]] \end{tikzcd}$$

$\theta_i \circ \theta_j^{-1}$ is an automorphism since $\theta_i^{-1}(t) \cap \bar{R} = \theta_j^{-1}(t) \cap \bar{R}$. Thus, $\theta_i \circ \theta_j^{-1}$ gives a substitution of order 1 and hence, γ_i and γ_j are the same branch. Thus, $r \leq t$.

Therefore $r = t$ and the number of maximal ideals in $\bar{R}$ equals the number of branches of f at $(0,0)$. Thus, $\hat{R} = R_1 \oplus \cdots \oplus R_r$. [Theorem 37.9; 5].

We have immediately the following corollaries.

<u>Corollary 3.9</u>: If $\hat{R}$ is an integral domain, then f has one distinct branch at $(0,0)$.

<u>Corollary 3.10</u>: If $\mathrm{Der}_k^n(R)$ is a free R-module for all n and if $\mathrm{Der}(R) = \mathrm{der}(R)$, then f has one distinct branch at $(0,0)$.

BIBLIOGRAPHY

BIBLIOGRAPHY

1. Grothendick, A., "Elements of Geometrie Algebrique," Part 4, Publications Mathematiques de L'IHES No. 32.

2. Lipman, J., "Free Derivation Modules on Algebraic Varieites," Amer. J. Math., 87 (1965), pp. 874-898.

3. Mount, K.R. and Villamayor, O.E., "On a Conjecture of Y. Nakai," Osaka J. Math. to appear.

4. __________, "Taylor Series and Higher Derivations," Universidad de Buenos Aries, No. 18.

5. Nagata, M., Local Rings, John Wiley and Sons, Inc., New York, 1962.

6. Nakai, Y., "High Order Derivations I," Osaka J. Math., 7 (1970), pp. 1-27.

7. Nakai, Y., et. al., "High Order Derivations II," J. Sci. Hiroshima Univ. Sci. A-I, 34 (1970), pp. 17-27.

8. Siedenberg, A., Elements of the Theory of Algebraic Curves, Addison-Wesley Publishing Company, Reading, Massachusetts, 1968.

9. Zariski, O. and Samuel, P., Commutative Algebra II, D. Van Nostrand Company, Inc., Princeton, 1960.