Can. J. Math., Vol. XXVIII, No. 1, 1976, pp. 9–18

ON THE ENDOMORPHISMS OF A POLYNOMIAL RING

JOHN DAVID

This paper arises in the attempt to solve the following problem related to the Zariski Problem. Let A be a polynomial ring in three variables over a field, k. Suppose there is a subring B of A such that $k \subseteq B$ and there is variable t over B such that $B[t] = A$. Then is it true that B is a polynomial ring over k?

The Zariski Problem was raised in 1949 at the Paris Colloquium on algebra, and is unsolved to this day (see [**2**] and [**4**]). The question at hand is still unsolved (see [**1**] and [**3**] for much completed work on this question).

For a review of the ideal-adic topology of a ring, and some properties of completion, see [**5**, p. 49; **6**, p. 129].

MAIN THEOREM. *Let R be a subring of a polynomial ring A, in three variables x', y', z' over a field $k \subseteq R$. Let the k-transcendence degree of the quotient field of R equal two and R be algebraically closed in A.*

(1) *Suppose that there exists a ring homomorphism $\sigma : A \to A$ such that $\sigma|_R = \mathrm{id}_R$ and kernel $\sigma = tA \neq (0)$.*

(2) *Suppose also that $z' \notin R$ and there exists an infinite subset S of N such that $p \in S$ implies there exists a ring homomorphism $\tau_p : A \to A$ such that $\tau_p(t) = (z' - c)^p$ where $c \in k$ equals the constant term of $\sigma(z')$ and such that $\tau_p|_R = \mathrm{id}_R$.*

Then $R[t]$ equals A.

Remark. All rings are commutative with identity and all maps are ring homomorphisms. In addition, all notation in the statement of the theorem remains constant.

Remark. The proof of this theorem is in two parts. The first shows $A \subseteq R[[t]]^*$ where $R[[t]]^*$ is the ring of all elements of $k[[x, y, z]]$ that can be written as $\sum_{i=0}^{\infty} c_i t^i$, $c_i \in R$, for a certain basis x, y, z of A. This part uses assumption (1), not (2). The second part shows that any element of A which does not lie in $R[t]$, cannot lie in $R[[t]]^*$. This part uses both assumptions.

LEMMA 1. *If p is prime in $A = k[x, y, z]$, x, y, z any basis of A, and $p|q \in A$ in $k[[x, y, z]]$, then $p|q$ in A (Assume $p \in (x, y, z)A$).*

Proof. By [**5**, 17.9], $pk[[x, y, z]] \cap A_{(x,y,z)} = pA_{(x,y,z)}$. Thus there exists $q' \in A$, $s \in A \backslash pA$ such that $pq' = qs$, as $pA \subseteq (x, y, z)A$. As p is prime and $p \nmid s$ in A, $p|q$ in A.

Received February 25, 1974 and in revised form, April 25, 1975.

https://doi.org/10.4153/CJM-1976-002-5 Published online by Cambridge University Press

Lemma 2. *There exists a basis* x, y, z *of* A *such that* $t \in (x, y, z)A$ *(By a basis, we mean* $k[x, y, z] = A$*).*

Proof. As $0 = \sigma(t(x', y', z')) = t(\sigma(x'), \sigma(y'), \sigma(z'))$, $t(a, b, c) = 0$ where $a, b, c \in k$ are the respective constant terms of $\sigma(x')$, $\sigma(y')$, and $\sigma(z')$ in the basis x', y', z'. Now write t as follows:

$$t(x', y', z') = t((x' - a) + a, (y' - b) + b, (z' - c) + c)$$

In terms of this new basis $x' - a$, $y' - b$, $z' - c$, therefore, the constant term of t is $t(a, b, c) = 0$.

Remark. In view of Lemma 2, there exists a basis x, y, z for A such that $\tau_p(t) = z^p$ and $t \in (x, y, z)A$. From here on, this will be the only basis we will deal with, and its notation will be preserved.

Definition. Let T be any subring of A. Then $T[[t]]^*$ is the set of all elements of $k[[x, y, z]]$ that can be expressed as $\sum_{i=0}^{\infty} a_i t^i$ where $a_i \in T$. This limit is taken in the (x, y, z)-adic topology.

Lemma 3. *Let* T *be any subring of* A. *Then* $T[[t]]^*$ *is a subring of* $k[[x, y, z]]$, *with the "natural" addition and multiplication. Furthermore, for any countable sequence* $\{a_i\}_{i=0}^{\infty}$ *of elements of* T, $\sum_{i=0}^{\infty} a_i t^i \in T[[t]]^*$.

Proof. As $t \in (x, y, z)$, $\{S_n = \sum_{i=0}^{n} a_i t^i\}_{i=0}^{\infty}$ forms a Cauchy sequence in the (x, y, z)-adic topology of A. That is,

for all $K > 0$, there exists $N_0 > 0$ such that $N, M > N_0$ implies

$$S_N - S_M \in (x, y, z)^K.$$

Thus $\sum_{i=0}^{\infty} a_i t^i \in k[[x, y, z]]$.

Now let $a_i, b_i \in T$. That $T[[t]]^*$ is additively closed follows from $\sum a_i t^i + \sum b_i t^i = \sum (a_i + b_i) t^i$. That $T[[t]]^*$ is multiplicatively closed is seen as follows: By 17.3 of [**5**],

$$\alpha = \left(\sum a_i t^i\right)\left(\sum b_i t^i\right) = \lim_n \left(\sum_{i=0}^{n} a_i t^i\right)\left(\sum_{i=0}^{n} b_i t^i\right).$$

We claim

$$\sum_{i=0}^{\infty} \left(\sum_{j+r=i} a_j b_r\right) t^i = \alpha.$$

Let $K > 0$. Then there exists N_0 such that $N > N_0$ implies

$$\alpha - \left(\sum_{i=0}^{N} a_i t^i\right)\left(\sum_{i=0}^{N} b_i t^i\right) \in (x, y, z)^K A.$$

Let $N_1 = \max(K, N_0)$. Then for $N > N_1 + 1$

$$\alpha - \sum_{i=0}^{N} \left(\sum_{j+r=i} a_j b_r\right) t^i = \alpha - \left(\sum_{i=0}^{N_1+1} a_i t^i\right)\left(\sum_{i=0}^{N_1+1} b_i t^i\right) - \sum_{i=N_1+2}^{N} \left(\sum_{j+r=i} a_j b_r\right) t^i$$

where $j > N_1 + 1$ or $r > N_1 + 1$. The difference of the first two terms lies in

$(x, y, z)^K A$ because $N_1 + 1 > N_0$. The last term is divisible by t^K as $K < N_1 + 1$. As $t \in (x, y, z)A$, it is in $(x, y, z)^K A$.

Remark. A is considered as a subring of $k[[x, y, z]]$ in the natural way, i.e., all finite sums of forms from A, with respect to the basis x, y, z.

LEMMA 4. *σ can be extended to $\sigma^* : A[[t]]^* \to A$. That is, $\sigma^*|_A = \sigma$.*

Proof. Consider any two elements $\sum a_i t^i = \alpha$ and $\sum b_i t^i = \beta$ of $A[[t]]^*$, where $a_i, b_i \in A$. Define $\sigma^*(\alpha) = \sigma(a_0)$. If $\alpha = \beta$ then $a_0 - b_0 = t\sum(a_i - b_i)t^{i-1}$. By Lemma 1, there exists $q \in A$ such that $a_0 - b_0 = t \cdot q$. Apply σ to this difference, remembering $\sigma(t) = 0$. Thus $\sigma^*(\alpha) = \sigma^*(\beta)$ and hence σ^* is well-defined. That σ^* is a ring homomorphism is seen from

$$\alpha + \beta = a_0 + b_0 + \sum (a_i + b_i)t^i \quad \text{and}$$

$$\alpha \cdot \beta = a_0 b_0 + \sum_{i=1}^{\infty} \left(\sum_{j+r=i} a_j b_r \right) t^i.$$

That σ^* agrees with σ on A is seen by writing any element a of A as $a + \sum_{i=1}^{\infty} 0 \cdot t^i$.

LEMMA 5. *t is transcendental over R.*

Proof. Let $r_n t^n + \ldots + r_1 t + r_0 = 0$ be an equation of minimal degree for t over R. Apply σ and deduce that $0 = \sigma(r_0) = r_0$.

LEMMA 6. Image $(\sigma) = R$.

Proof. As Image $(\sigma) \subseteq A$ is an affine ring over a field, containing at least two k-transcendentally independent elements from R, the Krull dimension of Image (σ) is two or three. As σ is not an isomorphism, the Krull dimension of Image (σ) is two. Thus q.f. (Image σ) has trans_k degree equal to two, thus is algebraic over q.f. (R). Thus Image (σ) is algebraic over R, and thus equals R (see [**6**, p. 193]).

THEOREM 1. $A \subseteq R[[t]]^*$.

Proof. By Lemma 5, tr_k q.f. $(R[t]) = 3$. As tr_k q.f. $(A) = 3$, q.f. A is algebraic over q.f. $R[t]$. Thus A is algebraic over $R[t]$. Thus A is algebraic over $R[[t]]^*$. Let $h_t \in A$, and let

(*e*) $a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0 = 0$ be a non-zero equation of minimal degree for h_t over $R[[t]]^*$. Thus $a_i \in R[[t]]^*$.

We will show this equation has a root $\sum h_i t^i$, $h_i \in R$, in $R[[t]]^*$. As $R[[t]]^*$ is a domain, $h_t \in R[[t]]^*$. Let $a_j = \sum_i r_{ji} t^i$, $r_{ji} \in R$. If the following equations all hold, for a sequence of $h_i \in R$, $i = 0, 1, \ldots$, then $\sum h_i t^i$ is a root of (*e*).

This is sufficient for $\sum h_i t^i$ to be a root, as will be seen below.

$$(t^0):\ r_{n,0}h_0^n + r_{n-1,0}h_0^{n-1} + \ldots + r_{1,0}h_0 + r_{0,0} = 0.$$

$$(t^1):\ r_{n,0}\binom{n}{1}h_0^{n-1}h_1 + r_{n,1}h_0^n + \ldots + r_{1,0}h_1 + r_{1,1}h_0 + r_{0,1} = 0.$$

Let

$$w_2 = r_{n,0}\binom{n}{2}h_1^2h_0^{n-2} + r_{n-1,0}\binom{n-1}{2}h_1^2h_0^{n-3} + \ldots + r_{2,0}h_1^2 + r_{n,1}\binom{n}{1}h_1h_0^{n-1} + r_{n-1,1}\binom{n-1}{1}h_1h_0^{n-2} + \ldots + r_{1,1}h_1 + r_{n,2}h_0^n + \ldots + r_{1,2}h_0 + r_{0,2}.$$

$$(t^2):\ r_{n,0}h_2h_0^{n-1}\binom{n}{1} + r_{n-1,0}h_2h_0^{n-2}\binom{n-1}{1} + \ldots + r_{1,0}h_2 + w_2 = 0.$$

In general, let w_K be the canonical R-coefficient of t^K in the expression

$$a_n\left(\sum_{i=0}^{K-1} h_it^i\right)^n + a_{n-1}\left(\sum_{i=0}^{K-1} h_it^i\right)^{n-1} + \ldots + a_0.$$

$$(t^K):\ r_{n,0}h_Kh_0^{n-1}\binom{n}{1} + r_{n-1,0}h_Kh_0^{n-2}\binom{n-1}{1} + \ldots + r_{1,0}h_K + w_K = 0.$$

Remark. The following equalities are all valid in $k[[x, y, z]]$ by Lemma 3.

To find h_0, we apply σ^* to the equation $a_nh_t^n + \ldots + a_0 = 0$ to get

$$r_{n,0}\sigma(h_t)^n + r_{n-1,0}\sigma(h_t)^{n-1} + \ldots + r_{0,0} = 0.$$

By Lemma 6, $\sigma(h_t) \in R$. Define $h_0 = \sigma(h_t)$. Thus h_0 satisfies (t^0).

To find h_1, we note the following:

$$a_n((h_t - h_0) + h_0)^n + \ldots + a_1((h_t - h_0) + h_0) + a_0 = 0.$$

As h_0 is a solution of (e), with coefficients $\sigma^*(a_i)$, it follows that

$$q = a_n \cdot \sum_{i=1}^{n} (h_t - h_0)^ih_0^{n-i}\binom{n}{i} + \left(\sum_{i=1}^{\infty} r_{n,i}t^i\right)h_0^n + \ldots + a_1(h_t - h_0) + \left(\sum_{i=1}^{\infty} r_{1,i}t^i\right)h_0 + \sum_{i=1}^{\infty} r_{0,i}t^i = 0.$$

As $\sigma(h_t - h_0) = 0$, $t|h_t - h_0$ in A.

We define $h_1 = \sigma((h_t - h_0)/t)$. We now can write q/t as a sum of elements from $A[[t]]^*$:

$$0 = q/t = r_{n,0}\frac{(h_t - h_0)}{t}h_0^{n-1}\binom{n}{1} + r_{n,1}h_0^n + \ldots + r_{1,0}\frac{(h_t - h_0)}{t} + r_{1,1}h_0 + r_{0,1} + (h_t - h_0)q_1 + tq_2,$$

where $q_1, q_2 \in A[[t]]^*$.

https://doi.org/10.4153/CJM-1976-002-5 Published online by Cambridge University Press

Thus $\sigma^*(q/t) = 0$, $\sigma^*(h_t - h_0) = 0$ and $\sigma^*(t) = 0$ implies

$$r_{n,0}h_1h_0^{n-1}\binom{n}{1} + r_{n,1}h_0^n + \ldots + r_{1,0}h_1 + r_{1,1}h_0 + r_{0,1} = 0.$$

So h_1 satisfies (t^1). By Lemma 6, $h_1 \in R$.

As

$$\sigma\left(\frac{h_t - h_0}{t} - h_1\right) = 0, \quad t \;\Big|\; \frac{h_t - h_0}{t} - h_1 \quad \text{in } A.$$

Therefore $t^2 | h_t - th_1 - h_0$ in A.

Suppose we have found $h_0, h_1, \ldots, h_{K-1} \in R$ such that they satisfy (t^i), $i = 1, 2, \ldots K - 1$, $K \geqq 2$, and such that $t^K | h_t - t^{K-1}h_{K-1} - t^{K-2}h_{K-2} - \ldots - th_1 - h_0$ in A. We will now find h_K. Let

$$V_{K-1} = t^{K-1}h_{K-1} + t^{K-2}h_{K-2} + \ldots + h_0.$$

We can assume $\sigma((h_t - V_{K-1})/t^i) = 0$ for $i < K$.

We have

$$a_n((h_t - V_{K-1}) + V_{K-1})^n + a_{n-1}((h_t - V_{k-1}) + V_{k-1})^{n-1} + \ldots + a_0 = 0,$$

as h_t is a root of (e). Thus

$$q' = a_n\left(\sum_{i=1}^{n} (h_t - V_{K-1})^i V_{K-1}^{n-i}\binom{n}{i}\right) + a_nV_{K-1}^n + \ldots$$
$$+ a_1(h_t - V_{K-1}) + a_1V_{K-1} + a_0 = 0,$$

where

$$a_nV_{K-1}^n + \ldots + a_1V_{K-1} + a_0 = w_Kt^K + w_{K+1}t^{K+1} + \ldots$$

$w_i \in R$; w_i is the canonical R-coefficient of t^i. We define

$$h_K = \sigma((h_t - V_{K-1})/t^K).$$

By Lemma 6, $h_K \in R$. Then q'/t^K can be written as a sum of elements from $A[[t]]^*$:

$$\left(\frac{h_t - V_{K-1}}{t^K}\right)\left(r_{n0}h_0^{n-1}\binom{n}{1} + \ldots + r_{10}\right)$$
$$+ w_K + tq_1 + \sum_{i=0}^{K-1}\left(\frac{h_t - V_{K-1}}{t^i}\right)q_i',$$

where q_1, $q_i' \in A[[t]]^*$. Applying σ^* to q'/t^K, as $\sigma((h_t - V_{K-1})/t^i) = 0$, $i < K$ we see

$$h_K(r_{n,0}h_0^{n-1}\binom{n}{1} + \ldots + r_{1,0}) + w_K = 0.$$

Thus h_K satisfies (t^K). As $\sigma((h_t - V_{K-1})/t^K - h_K) = 0$, $t | (h_t - V_{K-1})/t^K - h_K$

https://doi.org/10.4153/CJM-1976-002-5 Published online by Cambridge University Press

in A. Thus $t^{K+1}|h_t - t^K h_t - V_{K-1}$ in A. Also $\sigma((h_t - t^K h_K - V_{K-1})/t^i) = 0$, $i < K + 1$. This completes the inductive construction of the $h_i \in R$. The expression

$$\beta = a_n(\sum h_i t^i)^n + a_{n-1}(\sum h_i t^i)^{n-1} + \ldots + a_0,$$

(by [**5**], 17.3) is equal to $\lim_n \alpha_n$ where

$$\alpha_m = \left(\sum_{i=0}^{m} r_{n,i}t^i\right)\left(\sum_{i=0}^{m} h_i t^i\right)^n + \ldots + \sum_{i=0}^{m} r_{0,i}t^i.$$

Now let $K > 0$. For $m > K - 1$, $t^K|\alpha_m$, because our constructed h_i are solutions to (t^i). Thus $\alpha_m \in (x, y, z)^K$ and hence $\lim \alpha_m = 0$. Thus $\beta = 0$ in $k[[x, y, z]]$ and thus in $R[[t]]^*$. This completes the proof of Theorem 1.

We now proceed to the second part of the proof of the main theorem.

LEMMA 7. *If $\tau : A \to A$ such that $\tau|_R = \mathrm{id}_R$ and $\tau(t) = a \notin R$, then for all $\alpha \in A \backslash R[t]$, $\tau(\alpha) \notin R[a]$.*

Proof. We first calculate the kernel of τ. This is either of height one or zero, as $\mathrm{trans}_k \deg R = 2$ and $R \subseteq$ image (τ). If kernel $(\tau) = (p) \neq (0)$ where p is prime, then by Theorem 1, $t = \sum_{i=0}^{\infty} c_i p^i \in R[[p]]^*$, $c_i \in R$, and where there exists a basis x_0, y_0, z_0 of A such that $p \in (x_0, y_0, z_0)A$, by Lemma 2. Thus $t - c_0 = p \cdot c'$ where $c' \in k[[x_0, y_0, z_0]]$. By Lemma 1, there exists $c'' \in A$ such that $t - c_0 = p \cdot c''$. Hence $\tau(t) - \tau(c_0) = 0$, or $\tau(t) = c_0 \in R$, a contradiction. Thus kernel $(\tau) = (0)$.

Let $\alpha \in A$. Suppose $\tau(\alpha) = r_n a^n + \ldots + r_0$, $r_i \in R$. Then

$$\tau(\alpha - (r_n t^n + \ldots + r_0)) = 0.$$

Since kernel $(\tau) = (0)$, $\alpha = r_n t^n + \ldots + r_0$, it follows that $\alpha \in R[t]$.

LEMMA 8. *If $\tau : A \to A$ such that $\tau|_R = \mathrm{id}_R$ and $\tau(t) \in (x, y, z)A$, then $\tau(x)$, $\tau(y)$ and $\tau(z) \in (x, y, z)A$.*

Proof. We will do the proof for $\tau(x)$ only. By Theorem 1 and Lemma 1, $x = c_0 + c''t$, $c_0 \in R$ and $c'' \in A$. As $t \in (x, y, z)A$, $c_0 \in (x, y, z)A$. Apply $\tau : \tau(x) = c_0 + \tau(c'')\tau(t)$. Since both c_0 and $\tau(t)$ belong to $(x, y, z)A$, we are done.

LEMMA 9. *Let $\tau : A \to A$ be such that $\tau|_R = \mathrm{id}_R$ and $\tau(t) \in (x, y, z)A$. If $\sum c_i t^i$, $c_i \in R$, converges to an element α of A, in the (x, y, z)-adic topology, then $\sum c_i \tau(t)^i$ converges to $\tau(\alpha)$, in the same topology.*

Proof. For all $K > 0$ there exists n_0 such that $n > n_0$ implies

$$\alpha - \sum_{i=0}^{n} c_i t^i = g \in (x, y, z)^K A.$$

Apply τ:

$$\tau(\alpha) - \sum_{i=0}^{n} c_i \tau(t)^i = \tau(g).$$

By Lemma 8, $\tau(g) = g(\tau(x), \tau(y), \tau(z)) \in (x, y, z)^K A$.

LEMMA 10. *Let $\alpha \in A$. Then there exists $q > 0$, $K \geqq 0$, and $l \geqq 0$ such that $p > q$ implies* $\deg \tau_p(\alpha) < K \cdot p + l$ *(Assume $\tau_p(\alpha) \neq 0$ for all p).*

Proof. Here $\deg \beta \in A$ is the degree of its non-zero form of highest degree. If $\alpha \in R[t]$, then for $q = \max \{\deg c_i\}_{i=1}^{K}$,

$$\deg \tau_p(\alpha) = K \cdot p + l \text{ for } p > q,\ l = \deg c_K, \text{ where}$$
$$\alpha = c_K t^K + c_{K-1} t^{K-1} + \ldots + c_0,\ c_i \in R,\ c_K \neq 0$$

Suppose $\alpha \notin R[t]$. As A is algebraic over $R[t]$, we have:

$$(ee) \quad a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_0 = 0,\ a_i \in R[t], \text{ not all } a_i \neq 0.$$

For each a_i, there exists q_i, K_i, and l_i such that if $a_i \neq 0$, then

$$\deg \tau_p(a_i) = K_i p + l_i,\ p > q_i.$$

Let $q = \max \{q_i\}$, and let $p > q$. Apply τ_p to (ee). Two of the summands must have the same degree; that is, there exists $V_p \neq w_p$ such that $a_{V_p} \neq 0 \neq a_{w_p}$ and

$$\deg \tau_p(a_{V_p} \alpha^{V_p}) = \deg \tau_p(a_{w_p} \alpha^{w_p}).$$

Thus

$$\deg \tau_p(a_{V_p}) + \deg \tau_p(\alpha)^{V_p} = \deg \tau_p(a_{w_p}) + \deg \tau_p(\alpha)^{w_p}.$$

We derive

$$\deg \tau_p(\alpha) = \frac{K_{w_p} - K_{V_p}}{V_p - w_p} \cdot p + \frac{l_{w_p} - l_{V_p}}{V_p - w_p}.$$

As the differences $K_i - K_j$, $l_i - l_j$, and $i - j$ are finite in number, let

$$K = \max \left\{ \left[\frac{K_i - K_j}{j - i} \right]^+ + 1 \right\}_{i \neq j}$$

and

$$l = \max \left\{ \left[\frac{l_i - l_j}{j - i} \right]^+ + 1 \right\}_{i \neq j}$$

where $[w]^+$ indicates greatest positive integer in w, or zero, whichever is greater.

Then $\deg \tau_p(\alpha) < K \cdot p + l$, for all $p > q$.

https://doi.org/10.4153/CJM-1976-002-5 Published online by Cambridge University Press

THEOREM 2. *If $\alpha \in A \backslash R[t]$, then α cannot be expressed in the following form, as an element of $k[[x, y, z]]$:*

$$\sum_{i=0}^{\infty} c_i t^i, \quad c_i \in R.$$

The limit is taken in the (x, y, z)-adic topology.

Proof. Suppose $\alpha = \sum c_i t^i \in R[[t]]^*$, $c_i \in R$. By Lemma 10, there exists $K \geqq 0$, $l \geqq 0$, and $q > 0$ such that

$$\deg \tau_p(\alpha) \leqq K \cdot p + l, \; p > q.$$

By Lemma 9, $\{\sum_{i=0}^{n} c_i \tau_p(t)^i\}$ converges to $\tau_p(\alpha)$, in the (x, y, z)-adic topology. By Lemma 7, $\tau_p(\alpha) \neq 0 \notin R[z^p]$. Pick n large enough so that $n > K$. Select $p > q$ so that $\deg c_i < p$, $i \leqq n$, and $l < p$, and τ_p is defined.

As

$$\deg \tau_p(\alpha) \leqq K \cdot p + l < n \cdot p + p,$$

by Lemma 10, in the difference,

$$\tau_p(\alpha) - (c_0 + c_1 z^{1 \cdot p} + \ldots + c_n z^{n \cdot p} + c_{n+1} z^{np+p} + \ldots + c_m z^{m \cdot p}),$$

$m > n + 1$, no form in

$$\Omega = \tau_p(\alpha) - (c_0 + c_1 z^p + \ldots + c_n z^{n \cdot p})$$

can cancel with any form of

$$c_{n+1} z^{n \cdot p + p} + \ldots + c_m z^{m \cdot p}.$$

As $\tau_p(\alpha) - \sum_{i=0}^{m} c_i z^{i \cdot p}$ lies in higher and higher powers of $(x, y, z)A$ for higher values of m, $\Omega = 0$. Thus $\tau_p(\alpha) \in R[z^p]$. This contradicts Lemma 7, as $\tau_p(t) = z^p \notin R$; $z \in A \backslash R$ and R is algebraically closed in A. This completes the proof of Theorem 2, and thus the proof of the Main Theorem.

ADDENDUM

We note the following interesting corollary to the main theorem.

COROLLARY. *Let $B = k[a, b, c] \subseteq k[x, y, z]$. Let $\dim B = 2$, that is, the k-transcendence degree of the quotient field of B equals 2, and let t be the generator of the kernel of the homomorphism $k[x, y, z] \to B$ where $x \to a$, $y \to b$, and $z \to c$. Suppose t is transcendental over B and suppose every homomorphism $B[t] \to k[x, y, z]$ can be extended to a homomorphism $k[x, y, z] \to k[x, y, z]$; that is, $B[t]$ satisfies the "extension property". Then $B[t] = k[x, y, z]$. In simpler terms, we have $B[t] = k[x, y, z]$ if and only if $B[t]$ has the extension property. Let $A = k[x, y, z]$, as usual.*

Proof. Suppose $B[t]$ has the extension property. By this there exists $g_0: A \to A$, such that $g_0(t) = 0$ and $g_0|_B = \mathrm{id}_B$. Also for all $p \in N$ there exists $g_p: A \to A$ such that $g_p(t) = (z - c)^p$, $g_p|_B = \mathrm{id}_B$, where, without loss of generality, $z \notin B$ and $c =$ constant term of $g_0(z)$.

By the main theorem, if t is shown to be prime and thus the generator of the kernel of g_0, and if B is shown to be algebraically closed in A, then we are done. But t is obviously prime, as it is the principal equation of B.

To show B is algebraically closed in A, we first show $q \in$ image g_0 implies there exists $j \in N$ such that $g_0^j(q) = q$. Here, g_0^j indicates g_0 composed j times with itself. Now, $B \subseteq$ image g_0, dim $B = 2$, and g_0 not an isomorphism all imply that image g_0 is algebraic over B. Let $q \in$ image g_0. There exists $a_i \in B$ such that

$$a_n q^n + \ldots + a_0 = 0, \text{ not all } a_i = 0 \text{ (minimal equation for } q \text{ over } B.)$$

Apply g_0^i to this equation, $i \in N$:

$$a_n(g_0^i(q))^n + \ldots + a_0 = 0.$$

As the equation of q has only finitely many roots, there exists $i \neq j \in N \cup \{0\}$ such that $g_0^i(q) = g_0^{i+j}(q)$, $j \neq 0$. If $i = 0$, we are done. If $i > 0$, then note that

$$g_0^i\text{: image } g_0 \rightarrow g_0^i \text{ (image } g_0)$$

is an isomorphism, as B is contained in each, and thus the dimension on both sides is 2. Also both rings are affine. So $g_0^i(q) = g_0^i(g_0^j(q))$ implies $q = g_0^j(q)$.

We now can show image g_0 is algebraically closed in A. For, if $\alpha \in A\backslash$image g_0 and

$$a_n\alpha^n + \ldots + a_0 = 0, \text{ where } a_i \in \text{image } g_0, \text{ not all } a_i = 0,$$

is the minimal equation of α over image g_0, then applying g_0^s to this equation, where

$$s = \prod j_{a_n} \quad \text{and} \quad g_0^{j_{a_n}}(a_n) = a_n, \quad j_{a_n} \in N,$$

gives:

$$a_n(g_0^s(\alpha))^n + \ldots + a_0 = 0.$$

As $g_0^s(\alpha) \in$ image g_0, $s > 0$, one can reduce the equation of α, a contradiction.

We have image $g_0 \simeq A/_{\ker g_0} = A/_{tA}$. As t is the principal equation of B, $A/_{tA} \simeq B$. So

$$B \simeq \text{image } g_0, \text{ via } \theta.$$

By the extension property holding true for $B[t]$, this isomorphism can be extended to a map $\psi : A \rightarrow A$, such that $\psi(t) = t$. ψ must be an injection, as dim image $g_0[t] = 3$. To see this, note $t \notin$ image g_0, an algebraically closed ring in A, as $g_0^j(t) \neq t$ for all $j \in N$.

Now we get that B must also be algebraically closed in A. Let $a_n\alpha^n + \ldots + a_0 = 0$ be the minimal equation of $\alpha \in A$ over B, not all $a_i = 0$. Apply ψ to this equation:

$$\psi(a_n)\psi(\alpha)^n + \ldots + \psi(a_0) = 0.$$

As not all $\psi(a_i) = 0$ and $\psi(a_i) = \theta(a_i) \in$ image g_0, $\psi(\alpha)$ is algebraic over image g_0. Thus $\psi(\alpha) \in$ image g_0. So $\psi^{-1}(\psi(\alpha)) = \alpha \in B$ since ψ is an injection, and thus $\psi^{-1}(\psi(\alpha))$ can only be α, and $\psi(B) =$ image g_0. This completes the proof.

Remark. It is not always true that a subring of a polynomial ring in three variables over a field that has the extension property and is of dimension three is indeed the polynomial ring. It is easily shown if $B = k[x^2, x^3, y]$ then $B[z]$ has the extension property in $k[x, y, z]$, yet is not equal to it.

References

1. Shreeram Abhyankar, Paul Eakin, and William Heinzer, *On the uniqueness of the coefficient ring in a polynomial ring*, J. Algebra *23*, (1972), 310–342.
2. Claude Chevalley, *Fundamental concepts of algebra* (Academic Press, N.Y., N.Y., 1956).
3. Paul Eakin and William Heinzer, *A cancellation problem for rings*, Conference on Commutative Algebra, 311, *Lecture Notes in Mathematics* (Springer-Verlag, N.Y., N.Y., 1972).
4. M. Nagata, *A theorem on valuation rings and its applications*, Nagoya Math. J. *29* (1967), 85–91.
5. ——— *Local rings* (Interscience Publishers, N.Y., N.Y., 1962).
6. Oscar Zariski and Pierre Samuel, *Commutative algebra*, Vol. II (D. Van Nostrand Company Inc. Princeton, N.J. 1960).

Universidade Estadual de Campinas,
Campinas, Brazil