ALGEBRAIC PROPERTIES OF TWISTED POLYNOMIAL RINGS

MARIA NAIR DA SILVA
DAMATO PICCININI

ALGEBRAIC PROPERTIES OF TWISTED POLYNOMIAL RINGS

by

Ⓒ Maria Nair da Silva Damato Piccinini, B.Sc.

A Thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science

Department of Mathematics
Memorial University of Newfoundland

August 1975

St. John's Newfoundland

ABSTRACT

In this thesis, we study the twisted polynomial rings and determine several of their intrinsic properties.

In chapter I, we define the twisted polynomial ring $R_{\alpha,\psi}[x]$, prove is it a ring and establish some preliminary results.

In chapter II, we study the chain conditions; here the Hilbert basis theorem is extended to twisted polynomial rings.

In chapter III, we are concerned with the Noether radical of twisted polynomial rings with zero derivation.

In chapter IV, we describe the endomorphisms of a twisted polynomial ring which leave the coefficients unchanged.

In chapter V, we consider only twisted polynomial rings with zero derivation. Here we study the automorphisms which restrict to the identity map on the ring of coefficients. Complete results are obtained for commutative rings with a regular element.

If two twisted polynomial rings are isomorphic, what can be said about their rings of coefficients? We look into this question in chapter VI and, in chapter VII, we study in detail the example given by M. Hochster showing that not every ring is invariant.

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Dr. M. M. Parmenter, for his assistence, suggestions and encouragement which made the writing of this thesis not only a possible task but also a pleasant one. I would like to Thank Dr. M. Hochster for his help concerning the subject in chapter VII, and Dr. J.-B. Castillon for sending a copy of his thesis.

I would also like to thank my family for its moral and financial support.

Finally, I would like to thank Mrs. H. Tiller for typing this thesis.

TABLE OF CONTENTS

INTRODUCTION

Throughout this work the word ring will mean associative ring. Most of the notation used in this thesis is established in the beginning of Chapter I. We define the twisted polynomial ring $R_{\alpha,\psi}[x]$ where R is a ring, α an automorphism of R, ψ an α-derivation on R and x an indeterminate. Twisted polynomial rings may be defined also when α is a ring endomorphisms of R but then some restrictions are usually made on R and sometimes on ψ[5].

We study briefly ideals and quotient rings in $R_{\alpha,\psi}[x]$ and give a complete description of the center of $R_{\alpha,\psi}[x]$. When R is a field, not necessarily commutative, the center of $R_{\alpha,\psi}[x]$ has been described by J.B. Castillon in [2]. We also discuss the units of $R_{\alpha,\psi}[x]$ in some special cases.

In Chapter II, we extend the Hilbert basis theorem to twisted polynomial rings. For commutative rings and zero derivations, we prove that, unless R has identity, $R_{\alpha}[x]$ cannot be left (right) Noetherian. This extends a result of R.W. Gilmer [6]. For rings with identity and in some other cases, $R_{\alpha,\psi}[x]$ is not Artinian.

In Chapter III, we consider only zero derivations and assume that R has identity. Even under such restrictions, radicals such as the Jacobson radical, the prime radical and the Noether radical may not satisfy the Amitsur property [10]; by this we mean that the radical ϕ satisfies the condition $((\phi(R_{\alpha}[x]) \cap R)_{\alpha}[x] = \phi(R_{\alpha}[x])$, whenever this notation is meaningful. Consequently, calculation of such radicals seems much more difficult then with ordinary polynomials. At least, in proposition III,3, we describe the Noether radical of $R_{\alpha}[x]$ in terms of the coefficients of its elements.

In Chapter IV, we are concerned with those endomorphisms of $R_{\alpha,\psi}[x]$ which restrict to the identity map on R, i.e. the R-endomorphisms. We find specific conditions in special cases for substitution maps in $R_{\alpha,\psi}[x]$ to be R-endomorphisms. We then assume $\psi = 0$ and determine all R-endomorphisms of $R_\alpha[x]$ when R is commutative and has a regular element. This was done by R.W. Gilmer for the usual polynomial ring in [7].

For the R-automorphisms of $R_\alpha[x]$, we first restrict ourselves to commutative rings with a regular element. We note that if $t = t_o + t_1x + \ldots + t_nx^n$ induces an R-endomorphism of $R_\alpha[x]$ then $t' = t_1 + t_2x + \ldots + t_nx^{n-1}$ commutes with every element in R. Moreover, if t induces an R-automorphism of $R_\alpha[x]$, t' is a unit both in $R_\alpha[x]$ and in $R[x]$. Using these facts we are able to find necessary and sufficient conditions on the coefficients of a polynomial t for the induced substitution map to be an R-automorphism of $R_\alpha[x]$. For the case $\alpha = I$, theorem V.7 was proved by R.W. Gilmer in [7]. Theorem V.7 has also been proved in certain special cases by J.B. Castillon [2]. We close Chapter V by considering the case of a (not necessarily commutative) ring with identity. Here we use some results proved in [5].

In Chapter VI, we consider isomorphic twisted polynomial rings. Most of the results in ring theory used here were taken from [13]. We prove that if R and S are commutative Artinian rings with identity and $R_\alpha[x]$ is isomorphic to $S_\beta[x]$ then the rings $R/_{J(R)}$ and $S/_{J(S)}$ are subisomorphic. Generally, we could ask whether a ring isomorphism $R_\alpha[x] \cong S_\beta[x]$ would imply $R \cong S$. We know that this is not always true, for a counterexample was given by M. Hochster in [9]. We reserve Chapter VII for a detailed study of this counterexample.

CHAPTER I

Definitions and Preliminary Results

We begin this chapter by making some definitions and proving simple results on derivations. In doing so, we establish most of the notation used throughout this thesis.

Definition. Let R be a ring and α a ring automorphism of R. An endomorphism ψ of the underlying additive group of R is an α-derivation on R if it satisfies the property:

$$\forall a,b \in R \ , \quad \psi(ab) = \alpha(a)\psi(b) + \psi(a)b \qquad [5].$$

The sum of two α-derivations on R is an α-derivation. Also, if $c \in R$ and ψ is an α-derivation on R, $c\psi$, defined by $(c\psi)(r) = c\psi(r)$, is an α-derivation if $c \in C(R)$, the center of R.

We denote the group of the ring automorphisms of R by $\mathrm{Aut}(R)$; if γ is an endomorphism of the additive group of R, we use either $\gamma(r)$ or r^{γ} to indicate the image under γ of an element $r \in R$. Also, if $\gamma,\delta \in \mathrm{Aut}(R)$ and $r \in R$, $(r^{\gamma})^{\delta} = r^{\gamma\circ\delta}$.

Let $\alpha \in \mathrm{Aut}(R)$ and $a \in R$; we define $\psi_{a,\alpha}$ from R into R by $\psi_{a,\alpha}(b) = ab - b^{\alpha}a$ for each b in R. Then $\psi_{a,\alpha}$ is an α-derivation on R. In fact, $\psi_{a,\alpha}(0) = 0$, $\psi_{a,\alpha}(b + c) = a(b + c) - (b + c)^{\alpha}a = ab - b^{\alpha}a + ac - c^{\alpha}a = \psi_{a,\alpha}(b) + \psi_{a,\alpha}(c)$ and

$\psi_{a,\alpha}(bc) = abc - (bc)^{\alpha}a = abc - b^{\alpha}c^{\alpha}a + b^{\alpha}ac - b^{\alpha}ac = b^{\alpha}\psi_{a,\alpha}(c) + \psi_{a,\alpha}(b)c$.

If $a \in C(R)$, $\psi_{a,\alpha} = a(I - \alpha)$ where I is the identity automorphism of R. The derivations $\psi_{a,\alpha}$ are called inner derivations [5, pg. 295]. If R has identity, $\theta_{\alpha} = I - \alpha$ is then an inner derivation on R. If R has no identity no inner derivation equals θ_α but even so θ_α is an α-derivation on R. In fact, $\theta_\alpha(bc) = bc - (bc)^\alpha = bc - b^\alpha c^\alpha + b^\alpha c - b^\alpha c = b^\alpha \theta_\alpha(c) + \theta_\alpha(b)c$. Later on , we shall see that θ_α and all inner derivations are "trivial". However trivial, they do play an important role where the center of $R_{\alpha;\psi}[x]$ or its R-endomorphisms are concerned.

<u>Definition</u>. Let R be a ring, α an automorphism of R, ψ an α-derivation on R and x an indeterminate. The twisted polynomial ring $R_{\alpha,\psi}[x]$ is the set of all finite sums $\sum a_i x^i$ with coefficients in R, i.e.

$$R_{\alpha,\psi}[x] = \{ \sum_{i=0}^{n} a_i x^i \mid n \geq 0 \text{ and } a_i \in R \ \forall i \geq 0 \} ,$$

together with the operations:

1) $\sum\limits_{i=0}^{m} a_i x^i + \sum\limits_{i=0}^{n} b_i x^i = \sum\limits_{i=0}^{\max\{m,n\}} (a_i + b_i) x^i \quad \forall n,m \geq 0, \ \forall a_i, b_i \in R$ and filling up with zeros the places of the missing coefficients;

2) $(ax^o)(bx^n) = abx^n$ and

$$(ax^m)(bx^n) = (ax^{m-1})(b^\psi x^n) + (ax^{m-1})(b^\alpha x^{n+1}) \qquad \forall m > 0,$$

$\forall n \geq 0, \ \forall a,b \in R$ and extending this multiplication to any two elements of $R_{\alpha,\psi}[x]$ by linearity.

The symbol ax^o simply means the element a in $R_{\alpha,\psi}[x]$; we used it in 2) to emphasize the inductive definition of multiplication in $R_{\alpha,\psi}[x]$. For rings with identity the multiplication is defined simply by defining $xa = a^\psi + a^\alpha x$ as in [2], [5] and [12].

In order to prove that $R_{\alpha,\psi}[x]$ so defined is really a ring, we must show that multiplication is associative. To do this, we derive a formula for the multiplication of two monomials.

Let $m > 0$ and $i \geq 0$ be such that $m \geq i$. We define $S_m(i)$ to be the set of all possible permutations of i copies of α and $m - i$ copies of ψ. If $\xi \in S_m(i)$ and $b \in R$, b^{ξ} is the image of b under the composite ξ. We extend the symbol $S_m(i)$ to $m = 0$ by setting $S_0(i) = \{I_R\}$; if $m < i$, $m < 0$, or $i < 0$ we say that $b^{\xi} = 0 \ \forall \xi \in S_m(i)$, i.e. $S_m(i) = \{0\}$.

We have then the following equalities:

$$(1) \quad S_{m+1}(i) = \{\xi \circ \psi | \xi \in S_m(i)\} \cup \{\xi \circ \alpha | \xi \in S_m(i-1)\} = \{\psi \circ \xi | \xi \in S_m(i)\} \cup \{\alpha \circ \xi | \xi \in S_m(i-1)\} \quad \forall i,m \in Z.$$

__Proposition I.1.__ Let m,n be non-negative integers and $a,b \in R$. If the product $(ax^m)(bx^n)$ is defined as before, then

$$(2) \qquad (ax^m)(bx^n) = a \sum_{i=0}^{m} \sum_{\xi \in S_m(i)} b^{\xi} x^{i+n}$$

__Proof.__ We use induction on m. If $m = 0$, (2) is obviously true. We suppose that it holds for some $m \geq 0$ and proceed to prove that it is also true for $m + i$. We have

$$(ax^{m+1})(bx^n) = (ax^m)(b^{\psi}x^n) + (ax^m)(b^{\alpha}x^{n+1}) = a \sum_{i=0}^{m} \sum_{\xi \in S_m(i)} b^{\psi\circ\xi} x^{i+n} +$$

$$+ a \sum_{i=0}^{m} \sum_{\xi \in S_m(i)} b^{\alpha\circ\xi} x^{i+n+1} = a \sum_{i=0}^{m+1} \sum_{\xi \in S_m(i)} b^{\psi\circ\xi} x^{i+n} +$$

$$+ a \sum_{i=0}^{m+1} \sum_{\xi \ S_m(i-1)} b^{\alpha\circ\xi} x^{i+n}$$ and, because of (1), this equals

$$\sum_{i=0}^{m+1} \sum_{\xi \in S_{m+1}(i)} b^{\xi} x^{i+n},$$ q.e.d.

Proposition I.2. $R_{\alpha,\psi}[x]$ is a ring.

Proof. By the definition of $R_{\alpha,\psi}[x]$, the sum is commutative and the distributive laws hold. It remains to prove that the multiplication is associative and it is enough to show the associativity for monomials. We want to show that $\forall\ a,b,c \in R$ and $\forall\, m,n,\ell \geq 0$, $[(ax^m)(bx^n)](cx^\ell) = (ax^m)[(bx^n)(cx^\ell)]$. We use induction on m.

Let $m = 0$; then $[a(bx^n)](cx\ ) = (abx^n)(cx^\ell) = ab \sum_{i=0}^{n} \sum_{\xi \in S_n(i)} c^\xi x^{i+\ell}$, by proposition I.1.

On the other hand, $a[(bx^n)(cx^\ell)] = a(b \sum_{i=0}^{n} \sum_{\xi \in S_n(i)} c^\xi x^{i+\ell}) =$
$= ab \sum_{i=0}^{n} \sum_{\xi \in S_n(i)} c^\xi x^{i+\ell}$. Hence, associativity holds for $m = 0$.

We assume now that $\forall a,b,c \in R$, $\forall n,\ell \geq 0$
$[(ax^m)(bx^n)](cx^\ell) = (ax^m)[(bx^n)(cx^\ell)]$ for some $m \geq 0$ and show that this equality holds for $m + 1$. We first prove that

(3) $[(ax^{m+1})(bx^0)](cx^\ell) = (ax^{m+1})[(bx^0)(cx^\ell)]$. In fact,
$[(ax^{m+1})b](cx^\ell) = [(ax^m)b^\psi + (ax^m)(b^\alpha x)](cx^\ell) = (ax^m)[(b^\psi + b^\alpha x)(cx^\ell)]$ by the hypothesis for induction. And since
$(ax^m)[(b^\psi + b^\alpha x)(cx^\ell)] = (ax^m)(b^\psi cx^\ell + b^\alpha c^\psi x^\ell + b^\alpha c^\alpha x^{\ell+1}) =$
$= (ax^m)[(bc)^\psi x^\ell + (bc)^\alpha x^{\ell+1}] = (ax^{m+1})(bcx^\ell)$, this last equality by the definition of multiplication, then equality (3) is proved.

Next, $\forall a,b,c \in R$ and for $n \geq 1$, we have:

$[(ax^{m+1})(bx^n)](cx^\ell) = [(ax^m)(b^\psi x^n + b^\alpha x^{n+1})](cx^\ell) =$
(4) $(ax^m)[(b^\psi x^n + b^\alpha x^{n+1})(cx^\ell)]$, by the hypothesis for induction.

On the other hand, by proposition I.1, $(ax^{m+1})[bx^{n})(cx^{\ell})] =$ $= (ax^{m+1})[b \sum_{i=0}^{n} \sum_{\xi \in S_n(i)} c^{\xi}x^{i+\ell}]$ and this product is, according to (3), $[(ax^{m+1})b] \sum_{i=0}^{n} \sum_{\xi \in S_n(i)} c^{\xi}x^{i+\ell}$ which equals $[(ax^{m})(b^{\psi} + b^{\alpha}x)] \sum_{i=0}^{n} \sum_{\xi \in S_n(i)} c^{\xi}x^{i+\ell}$, because of the definition of multiplication in $R_{\alpha,\psi}[x]$. We now make use of the hypothesis for induction to conclude that

$$(ax^{m+1})[(bx^{n})(cx^{\ell})] = (ax^{m})[(b^{\psi} + b^{\alpha}x) \sum_{i=0}^{n} \sum_{\xi \in S_n(i)} c^{\xi}x^{i+\ell}] \qquad (5).$$

We want to show that the right hand-side of (4) equals the right hand-side of (5). We first note that $\forall\ b,c \in R$, $\forall\ n,\ell \geq 0$, $(bx) \sum_{i=0}^{n} \sum_{\xi \in S_n(i)} c^{\xi}x^{i+\ell} = b \sum_{i=0}^{n+1} \sum_{\xi \in S_{n+1}(i)} c^{\xi}x^{i+\ell}$ (6). In fact, by the definition of multiplication, $(bx) \sum_{i=0}^{n} \sum_{\xi \in S_n(i)} c^{\xi}x^{i+\ell} = b \sum_{i=0}^{n} \sum_{\xi \in S_n(i)} (c^{\xi\circ\psi}x^{i+\ell} + c^{\xi\circ\alpha}x^{i+\ell+1})$; the proof of (6) is then similar to that of (2).

Finally, we may write

$$(ax^{m})[(b^{\psi} + b^{\alpha}x) \sum_{i=0}^{n} \sum_{\xi \in S_n(i)} c^{\xi}x^{i+\ell}] = (ax^{m})[b^{\psi} \sum_{i=0}^{n} \sum_{\xi \in S_n(i)} c^{\xi}x^{i+\ell} +$$

$$b^{\alpha} \sum_{i=0}^{n+1} \sum_{\xi \in S_{n+1}(i)} c^{\xi}x^{i+\ell}] = (ax^{m})[(b^{\psi}x^{n})(cx^{\ell}) + (b^{\alpha}x^{n+1})(cx^{\ell})] =$$

$$= (ax^{m})[(b^{\psi}x^{n} + b^{\alpha}x^{n+1})(cx^{\ell})]. \qquad \text{q.e.d.}$$

In the case $\alpha = I$ and $\psi = 0$ we have the usual polynomial ring $R[x]$. In this case, $R[x]$ is commutative if and only if R is commutative. The next two propositions show that if either $\alpha \neq I$ or $\psi \neq 0$, $R_{\alpha,\psi}[x]$ is commutative if and only if it is isomorphic to $R[x]$ and R is commutative.

Proposition I.3. Let R be a ring with a regular element. Then $R_{\alpha,\psi}[x]$ is commutative if and only if R is commutative, $\alpha = I$ and $\psi = 0$.

Proof. If R is commutative, $R[x]$ is commutative. Conversely, if $R_{\alpha,\psi}[x]$ is commutative, it is immediate that R is commutative. Let $d \in R$ be regular; for each $a \in R$, $dxa = d(a^\psi + a^\alpha x)$, by the definition of multiplication in $R_{\alpha,\psi}[x]$. Since $R_{\alpha,\psi}[x]$ is commutative, $dxa = adx$ and $ad = da$. Hence, $dax = da^\psi + da^\alpha x$ and, because d is regular, $a^\psi = 0$ and $a^\alpha = a$ for each $a \in R$.

Proposition I.4. If the ring R has no regular element and $R_{\alpha,\psi}[x]$ is commutative, then $R_{\alpha,\psi}[x] = R[x]$.

Proof. Since $R_{\alpha,\psi}[x]$ is commutative, for each $a,b \in R$, $axb = bax$ and this implies $ab^\psi = 0$ and $ab^\alpha = ba = ab$. Then $\forall\, a,b \in R$, $\forall\, m,n \geq 0$,

$$ax^m bx^n = a \sum_{k=0}^{m} \sum_{\xi \in S_m(k)} b^\xi x^{k+n} = abx^{m+n}.$$

The mapping $\sigma : R_{\alpha,\psi}[x] \to R[x]$, defined by $\sigma(\sum a_i x^i) = \sum a_i x^i$, is clearly $1 - 1$, onto and additive. Moreover,

$$\sigma((\sum_{i=0}^{m} a_i x^i)(\sum_{i=0}^{n} b_i x^i)) = \sigma(\sum_{i+j=0}^{m+n} a_i b_j x^{i+j}) = \sigma(\sum_{i=0}^{m} a_i x^i)\, \sigma(\sum_{i=0}^{n} b_i x^i).$$

This proves that σ is a ring isomorphism. q.e.d.

If R is any ring and I is a nonempty subset of R, we know that I is a left (right) ideal in R if and only if $I[x]$ is a left (right) ideal in $R[x]$. We look now into the same question for the more general case $R_{\alpha,\psi}[x]$.

Proposition I.5. Let I be a nonempty subset of R. The subset $S = \{\sum a_i x^i \quad R_{\alpha,\psi}[x] \mid a_i \in I,\ \forall i \geq 0\}$ of $R_{\alpha,\psi}[x]$ is a right ideal in $R_{\alpha,\psi}[x]$ if and only if I is a right ideal in R.

Proof. $\forall a \in I$, $\forall r \in R$ and $\forall m,n \geq 0$, $ax^m rx^n = a \sum_{i=0}^{m} \sum_{\xi \in S_m(i)} r^{\xi} x^{i+n} \in S$ if and only if $\forall a \in I$ and $\forall r \in R$, $ar \in I$.

Proposition I.6. Let I be a nonempty subset of R. The subset $S = \{\sum a_i x^i \in R_{\alpha,\psi}[x] \mid a_i \in I,\ \forall i \geq 0\}$ is a left ideal in $R_{\alpha,\psi}[x]$ if and only if $\forall m \geq 0$ and $\forall i$ such that $0 \leq i \leq m$, then $R[(\sum_{\xi \in S_m(i)} \xi)(I)] \subseteq I$.

Proof. $\forall a \in I$, $\forall r \in R$ and $\forall m,n \geq 0$, $rx^m ax^n = r \sum_{i=0}^{m} \sum_{\xi \in S_m(i)} a^{\xi} x^{i+n} \in S$ if and only if $\forall a \in I$, $\forall r \in R$, $\forall m \geq 0$ and $\forall i$ such that $0 \leq i \leq m$, then $r \sum_{\xi \in S_m(i)} a^{\xi} \in I$.

Remark. If we set $m = 0$, the condition in proposition I.6 reads: I is a left ideal in R. More generally, for each $m \geq 0$ we have $R\psi^m(I) \subseteq I$ and $R\alpha^m(I) \subseteq I$, by setting $i = 0$ and $i = m$, respectively.

Let S be as in proposition I.6. Then:

Corollary I.7. If R has identity, S is a left ideal in $R_{\alpha,\psi}[x]$ if and only if I is a left ideal in R, $\psi(I) \subseteq I$ and $\alpha(I) \subseteq I$.

Proof. If S is a left ideal in $R_{\alpha,\psi}[x]$, we apply proposition I.6 setting $r = 1$ and considering the cases when $m = i = 0$, $m = 1$ and $i = 0$ and $m = i = 1$. The converse is true for any ring.

Let I be a nonempty subset of a ring R stable under the automorphism α and under the α-derivation ψ and let S be as above; propositions I.5

and I.6 tell us that S is an ideal in $R_{\alpha,\psi}[x]$ if and only if I is an ideal in R. If this is the case, we may form the quotient ring $R_{\alpha,\psi}[x]/_S$ and we would like to find some relation between this ring and the quotient ring $\bar{R} = R/_I$. If we make the additional hypothesis that $\alpha(I) = I$, S is then the ring $I_{\alpha,\psi}[x]$ and we can define also the mappings $\bar{\alpha}$, $\bar{\psi} : \bar{R} \to \bar{R}$ by $\bar{\alpha}(\bar{r}) = \overline{\alpha(r)}$ and $\bar{\psi}(\bar{r}) = \overline{\psi(r)}$, $\forall r \in R$. $\bar{\alpha}$ and $\bar{\psi}$ are additive mappings; $\bar{\alpha}$ is also multiplicative and onto and, since $\alpha(I) = I$, $\bar{\alpha}$ is injective. It is easy to verify that $\bar{\psi}$ is an $\bar{\alpha}$-derivation on $\bar{R}$. With these notations in mind, we may state the following proposition:

Proposition I.8. Let R be a ring, α an automorphism of R, ψ an α-derivative on R and I a two-sided ideal in R such that $\alpha(I) = I$ and $\psi(I) \subseteq I$. Then $\bar{R}_{\bar{\alpha},\bar{\psi}}[x] \simeq R_{\alpha,\psi}[x]/_{I_{\alpha,\psi}[x]}$.

Proof. We define $\sigma : R_{\alpha,\psi}[x] \to \bar{R}_{\bar{\alpha},\bar{\psi}}[x]$ by $\sigma(\sum r_i x^i) = \sum \bar{r}_i x^i$. Clearly, σ is additive. We now prove that it is also multiplicative and again it is enough to prove it on monomials. We have $\sigma(rx^m)\sigma(sx^n) = \bar{r}x^m\bar{s}x^n = \bar{r}\sum_{i=0}^{m}\sum_{\xi' \in S'_m(i)} s^{-\xi'}x^{i+n}$ where S'_m is the set of all possible permutations of i copies of $\bar{\alpha}$ and $m - i$ copies of $\bar{\psi}$. On the other hand,

$$\sigma(rx^m sx^n) = \sigma(r\sum_{i=0}^{m}\sum_{\xi \in S_m(i)} s^{\xi}x^{i+n}) = \bar{r}\sum_{i=0}^{m}\sum_{\xi \in S_m(i)} \overline{s^{\xi}}x^{i+n}.$$

Since the canonical epimorphism $\pi : R \to \bar{R}$ establishes a set isomorphism between $S_m(i)$ and $S'_m(i)$, we may write

$$\sigma(rx^m)\sigma(sx^n) = \sigma(rx^m sx^n).$$

σ is then a ring epimorphism with kernel $I_{\alpha,\psi}[x]$.

Hence,

$$\bar{R}_{\bar{\alpha},\bar{\psi}}[x] = R_{\alpha,\psi}[x]/I_{\alpha,\psi}[x].$$

We study now the center C of $R_{\alpha,\psi}[x]$. If R is a field, not necessarily commutative, J.B. Castillon used a different approach in [2, pg. 28] to find C. We collect some lemmas.

Lemma I.9. If $\sum_{i=0}^{m} a_i x^i$ is central in $R_{\alpha,\psi}[x]$ then $R(\psi(a_i) - \theta_\alpha(a_{i-1})) =$ $= 0$, $\forall\, i \geq 0$.

Remark. As usual, we set $a_i = 0$ $\forall\, i > m$ and also $a_{-1} = 0$. Then the notation above is clear and the lemma implies $R\psi(a_o) = 0$ and $R(a_m - a_m^\alpha) = 0$.

Proof. Let $b \in R$; since $\sum_{i=0}^{m} a_i x^i$ is central we have

$$b\sum_{i=0}^{m} a_i x^i = \sum_{i=0}^{m} a_i x^i b = \sum_{i=0}^{m} \sum_{k=0}^{i} \sum_{\xi \in S_i(k)} b^\xi x^k = \sum_{k=0}^{m} \sum_{i=k}^{m} a_i \sum_{\xi \in S_i(k)} b^\xi x^k$$

i.e. $ba_k = \sum_{i=k}^{m} a_i \sum_{\xi \in S_i(k)} b^\xi$ (1) , $\forall\, k \geq 0$.

We must also have $\sum_{i=0}^{m} a_i x^i bx = bx \sum_{i=0}^{m} a_i x^i$; this equality may be rewritten as

$$\sum_{k=0}^{m} \sum_{i=k}^{m} a_i \sum_{\xi \in S_i(k)} b^\xi x^{k+1} = b \sum_{i=0}^{m} a_i{}^\psi x^i + b \sum_{i=0}^{m} a_i{}^\alpha x^{i+1}, \text{ i.e. }, \forall\, k \geq 0$$

$$\sum_{i=k}^{m} a_i \sum_{\xi \in S_i(k)} b^\xi = ba_{k+1}^\psi + ba_k^\alpha \quad (2).$$

By comparing (1) and (2) we obtain $ba_k = ba_{k+1}^\psi + ba_k^\alpha$ or $b(\psi(a_{k+1}) - \theta_\alpha(a_k)) = 0$ $\forall\, b \in R$, $\forall\, k \geq 0$; this is also true for $k = -1$. We conclude that $R(\psi(a_i) - \theta_\alpha(a_{i-1})) = 0$ $\forall\, i \geq 0$.

Corollary I.10. If R is a ring with a regular element and $\sum_{i=0}^{m} a_i x^i$ is central in $R_{\alpha,\psi}[x]$, then $\psi(a_i) = \theta_\alpha(a_{i-1})$ $\forall i \geq 0$.

Proof. By lemma I.9, $R(\psi(a_i) - \theta_\alpha(a_i)) = 0$ $\forall i \geq 0$; let d be a regular element in R; then $d(\psi(a_i) - \theta_\alpha(a_{i-1})) = 0 \; \forall i \geq 0$ implies $\psi(a_i) = \theta_\alpha(a_{i-1})$ $\forall i \geq 0$.

Lemma I.11. Let $a_o, a_1 \ldots, a_m \in R$ be such that $\forall b \in R$ and $\forall i \geq 0$, $ba_i^{\psi} = ba_{i-1}^{\theta_\alpha}$. then $\forall j \geq 0$, $\forall k \leq j$, $\forall \xi \in S_j(k)$ and $\forall b \in R$, $ba_i^{\psi \circ \xi} = ba_{i-1}^{\theta_\alpha \circ \xi}$.

Proof. By induction on j. If $j = k = 0$, then $\xi = I$ and the lemma holds by its hypothesis.

Suppose it is true for any $j < j_o$, $j_o > 0$, and let $\xi \in S_{j_o}(k)$. Either $\xi = \xi' \circ \alpha$ with $\xi' \in S_{j_o-1}(k-1)$ or $\xi = \xi' \circ \psi$ with $\xi' \in S_{j_o-1}(k)$. In the first case, we have $ba_i^{\psi \circ \xi} = ba_i^{\psi \circ \xi' \circ \alpha} =$
$(b^{\alpha^{-1}} a_i^{\psi \circ \xi'})^{\alpha} = (b^{\alpha^{-1}} a_{i-1}^{\theta_\alpha \circ \xi'})^{\alpha} = ba_{i-1}^{\theta_\alpha \circ \xi' \circ \alpha} = ba_{i-1}^{\theta_\alpha \circ \xi}$.

In the second case, we have $(b^{\alpha^{-1}} a_i^{\psi \circ \xi'})^{\psi} = ba_i^{\psi \circ \xi' \circ \psi} + b^{\alpha^{-1} \circ \psi} a_i^{\psi \circ \xi'}$; hence

$$ba_i^{\psi \circ \xi} = (b^{\alpha^{-1}} a_i^{\psi \circ \xi'})^{\psi} - b^{\alpha^{-1} \circ \psi} a_i^{\psi \sigma \xi'} = (b^{\alpha^{-1}} a_{i-1}^{\theta_\alpha \circ \xi'})^{\psi} - b^{\alpha^{-1} \circ \psi} a_{i-1}^{\theta_\alpha \circ \xi'} =$$

$$ba_{i-1}^{\theta_\alpha \rho \xi' \circ \psi} + b^{\alpha^{-1} \circ \psi} a_{i-1}^{\theta_\alpha \circ \xi'} - b^{\alpha^{-1} \circ \psi} a_{i-1}^{\theta_\alpha \circ \xi'} = ba_{i-1}^{\theta_\alpha \circ \xi}.$$

Lemma I.12. Let $a_o, a_1, \ldots, a_m \in R$ be such that $ba_i^{\psi} = ba_{i-1}^{\theta_\alpha}$ $\forall b \in R$. and $\forall i \geq 0$. Then $\forall b \in R$ and $\forall j, t$ such that $0 \leq j \leq t \leq m$,

$$b \sum_{i=t-j}^{t} \sum_{\xi \in S_j(t-i)} a_i^{\xi} = ba_{t-j}.$$

<u>Proof</u>. By induction on t. Let $t = 0$; then $j = 0$ and $b \sum_{i=0}^{t} \sum_{\xi \in S_o(i)} a_i^{\xi} =$ $= ba_o = ba_{t-j}$. Suppose $b \sum_{i=t-1-j}^{t-1} \sum_{\xi \in S_j(t-1-i)} a_i^{\xi} = ba_{t-1-j}$ where $j \leq t - 1$; consider $b \sum_{i=t-j}^{t} \sum_{\xi \in S_j(t-i)} a_i^{\xi}$ with $j \leq t$. As before, we obtain

$$b \sum_{i=t-j}^{t} \sum_{\xi \in S_j(t-i)} a_i^{\xi} = b \sum_{i=t-j}^{t} \sum_{\xi \in S_{j-1}(t-i)} a_i^{\psi o \xi} + b \sum_{i=t-j}^{t} \sum_{\xi \in S_{j-1}(t-i-1)} a_i^{\alpha o \xi}$$

; by lemma I.11, this equals

$$b \sum_{i=t-j}^{t} \sum_{\xi \in S_{j-1}(t-i)} a_{i-1}^{\xi} - b \sum_{i=t-j}^{t} \sum_{\xi \in S_{j-1}(t-i)} a_{i-1}^{\alpha o \xi} + b \sum_{i=t-j}^{t} \sum_{\xi \in S_{j-1}(t-i-1)} a_i^{\alpha o \xi}.$$

The last two terms add up to zero, since $S_{j-1}(j) = S_{j-1}(-1) = \{0\}$.

Hence,

$$b \sum_{i=t-j}^{t} \sum_{\xi \in S_j(t-i)} a_i^{\xi} = b \sum_{i=t-j}^{t} \sum_{\xi \in S_{j-1}(t-i)} a_{i-1}^{\xi} = b \sum_{i=t-j-1}^{t-1} \sum_{\xi \in S_{j-1}(t-1-i)} a_i^{\xi} =$$

$= b \sum_{i=t-j}^{t-1} \sum_{\xi \in S_{j-1}(t-1-i)} a_i^{\xi}$; since $j \leq t$ implies $j - 1 \leq t - 1$, we may use our hypothesis for induction to conclude that

$$b \sum_{i=t-j}^{t} \sum_{\xi \in S_j(t-i)} a_i^{\xi} = ba_{t-j} .$$

<u>Lemma I.13</u>. Let $a_o, a_1, \ldots, a_m \in R$ be such that $ba_i^{\psi} = ba_{i-1}^{\theta_\alpha}$, $\forall b \in R$ and $\forall i \geq 0$. Then $\forall n \geq 0$ and $\forall b_o, b_1, \ldots, b_n \in R$,

$$\left(\sum_{j=0}^{n} b_j x^j\right)\left(\sum_{i=0}^{m} a_i x^i\right) = \sum_{t=0}^{m+n} \sum_{i+j=t} b_j a_i x^t \text{ in } R_{\alpha,\psi}[x].$$

<u>Proof</u>. According to propisition I.1, $\left(\sum_{j=0}^{n} b_j x^j\right)\left(\sum_{i=0}^{m} a_i x^i\right) =$ $= \sum_{i=0}^{m} \sum_{j=0}^{n} b_j \sum_{k=0}^{j} \sum_{\xi \in S_j(k)} a_i^{\xi} x^{k+i}$, where $0 \leq k + i \leq m + n$. If we set $k + i = t$ and put together similar terms, we obtain:

$$\left(\sum_{j=0}^{n} b_j x^j\right)\left(\sum_{i=0}^{m} a_i x^i\right) = \sum_{t=0}^{m+n} \sum_{i=0}^{t} \sum_{j=0}^{n} b_j \sum_{\xi \in S_j(t-i)} a_i^{\xi} x^t =$$

$$\sum_{t=0}^{m+n} \sum_{j=0}^{n} b_j \sum_{i=0}^{t} \sum_{\xi \in S_j(t-i)} a_i^{\xi} x^t = \sum_{t=0}^{m+n} \sum_{j=0}^{n} b_j \sum_{i=t-j}^{t} \sum_{\xi \in S_j(t-i)} a_i^{\xi} x^t ,$$ the

last equality being justified by the fact that $S_j(t - i) = \{0\}$ if $i < t - j$.

Then, by lemma I.12,

$$\left(\sum_{j=0}^{n} b_j x^j\right)\left(\sum_{i=0}^{m} a_i x^i\right) = \sum_{t=0}^{m+n} \sum_{j=0}^{n} b_j a_{t-j} x^t = \sum_{t=0}^{m+n} \sum_{j=0}^{t} b_j a_{t-j} x^t = \sum_{t=0}^{m+n} \sum_{i+j=t} b_j a_i x^t .$$

We now prove our main theorem describing the center of $R_{\alpha,\psi}[x]$.

<u>Theorem I.14.</u> Let C be the center of $R_{\alpha,\psi}[x]$. Then $\sum_{i=0}^{m} a_i x^i$ C if and only if $\forall b \in R$,

1) $ba_i^{\psi} = ba_{i-1}^{\theta_\alpha}$ $\forall i \geq 0$ and

2) $\sum_{i=k}^{m} \left(a_i \sum_{\xi \in S_i(k)} b^{\xi}\right) = ba_k$ $\forall k$ such that $0 \leq k \leq m$.

<u>Proof.</u> Suppose $\sum_{i=0}^{m} a_i x^i \in C$. By lemma I.9, $\forall b \in R$, $ba_i^{\psi} = ba_{i-1}^{\theta_\alpha}$ for each $i \geq 0$.

Let $b_0, b_1, \ldots, b_n \in R$ and consider the polynomial $\sum_{j=0}^{n} b_j x^j$.

Since $\sum_{i=0}^{m} a_i x^i \in C$, we have

$$\sum_{t=0}^{m+n} \sum_{j=0}^{t} \sum_{i=t-j}^{m} a_i \sum_{\xi \in S_i(t-j)} b_j^{\xi} x^t = \sum_{t=0}^{m+n} \sum_{i=0}^{t} \sum_{j=t-i}^{n} b_j \sum_{\xi \in S_j(t-i)} a_i^{\xi} x^t$$; because of

lemma I.13, we conclude that

$$\sum_{t=0}^{m+n} \sum_{j=0}^{t} \sum_{i=t-j}^{m} a_i \sum_{\xi \in S_i(t-j)} b_j^{\xi} x^t = \sum_{t=0}^{m+n} \sum_{i+j=t} b_j a_i x^t \qquad (1),$$

For the proof of 2), we proceed by induction on k, Consider $t = 0$ in (1); then

$\sum_{i=0}^{m} a_i \sum_{\xi \in S_i(0)} b_o^{\xi} = b_o a_o \quad \forall b_o \in R$; hence 2) holds for $k = 0$. Suppose it holds for any ℓ such that $0 \le \ell < k \le m$. In (1), take $t = k$. Then

$$\sum_{j=0}^{k} \sum_{i=k-j}^{m} a_i \sum_{\xi \in S_i(k-j)} b_j^{\xi} = \sum_{i+j=k} b_j a_i$$

; by the hypothesis for induction,

$$\sum_{j=1}^{k} \sum_{i=k-j}^{m} a_i \sum_{\xi \in S_i(k-j)} b_j^{\xi} = \sum_{j=1}^{k} b_j a_{k-j} .$$

By subtracting the last equality from the previous one, we obtain

$\sum_{i=k}^{m} a_i \sum_{\xi \in S_i(k-j)} b_o^{\xi} = b_o a_k \quad \forall b_o \in R$. Hence, 2) holds for any k such that $0 \le k \le m$.

Conversely, suppose $a_o, a_1, \ldots, a_m$ satisfy 1) and 2) ; let $\sum_{j=0}^{n} b_j x^j$ be any polynomial in $R_{\alpha,\psi}[x]$. By lemma I.13,

$(\sum_{j=0}^{n} b_j x^j)(\sum_{i=0}^{m} a_i x^i) = \sum_{t=0}^{m+n} \sum_{i+j=t} b_j a_i x^t$; on the other hand,

$(\sum_{i=0}^{m} a_i x^i)(\sum_{j=0}^{n} b_j x^j) = \sum_{t=0}^{m+n} \sum_{j=0}^{t} \sum_{i=t-j}^{m} a_i \sum_{\xi \in S_i(t-j)} b_j^{\xi} x^t =$

$\sum_{t=0}^{m} \sum_{j=0}^{t} b_j a_{t-j} x^t$, by 2). Hence, $(\sum_{j=0}^{n} b_j x^j)(\sum_{i=0}^{m} a_i x^i) =$

$(\sum_{i=0}^{m} a_i x^i)(\sum_{j=0}^{n} b_j x^j) \quad \forall \sum_{j=0}^{n} b_j x^j \in R_{\alpha,\psi}[x]$. Consequently,

$\sum_{i=0}^{m} a_i x^i \in C$. q.e.d.

Remark. If the ring R has a regular element and if we consider $\psi = 0$, the conditions in theorem I.14 will read as follows:

1) $a_i^{\alpha} = a_i \quad \forall i \ge 0$ and

2) $a_i b^{\alpha^i} = b a_i \quad \forall i \ge 0$.

In the case when R is a field, not necessarily commutative, this was proved by J.B. Castillon in [2].

The next corollary is also proved in [2] when R is a field, and $\psi = 0$.

Corollary I.15. Let R be a commutative integral domain, α an automorphism of R such that $\alpha^k \neq I \ \forall k > 0$ and ψ an α-derivation on R. Then the center of $R_{\alpha,\psi}[x]$ is equal to $\ker \psi \cap \ker \theta_\alpha$.

Proof. Let $\sum_{i=0}^{m} a_i x^i$ be central ; by theorem I.14, $a_m b^{\alpha^m} = ba_m \ \forall b \in R$. Since R is commutative, $a_m(b - b^{\alpha^m}) = 0 \ \forall b \in R$; since $\alpha^k \neq I \ \forall k > 0$ and since R is an integral domain, $a_m = 0 \ \forall m > 0$. Hence the central elements of $R_{\alpha,\psi}[x]$ are in R. By corollary I.10, if $a \in R$ is central in $R_{\alpha,\psi}[x]$, then $\psi(a) = 0$ and $\theta_\alpha(a) = \psi(0) = 0$.

For the converse we note that theorem I.14 implies that $\ker \psi \cap \ker \theta_\alpha \cap C(R)$ is contained in the center of $R_{\alpha,\psi}[x]$ in all cases.

Corollary I.16. Let R be a ring with a regular element. Then $\sum_{i=0}^{m} a_i x^i$ is central in $R_\alpha[x]$ if and only if $a_i \in \ker \theta_\alpha$ and $\psi_{a_i,\alpha^{-1}} = 0$ for each $i \geq 0$.

Proof. Let d be a regular element of R. Suppose $\sum_{i=0}^{m} a_i x^i$ is central. By theorem I.14, $d(\psi(a_i) - \theta_\alpha(a_{i-1})) = 0$, and since $\psi = 0$, we have $\theta_\alpha(a_{i-1}) = 0$. Condition 2) in theorem I.14 and $\psi = 0$ yeld $\psi_{a_i,\alpha^{-i}} = 0$.

The converse is a direct consequence of theorem I.14.

We consider now the case of a ring with identity and study $R_{\alpha;\psi}[x]^*$, the set of all invertible elements in $R_{\alpha,\psi}[x]$. Only very partial results are obtained here.

Proposition I.17. If R is an integral domain, $R_{\alpha,\psi}[x]^* = R^*$.

Proof. Of course, $R^* \subseteq R_{\alpha,\psi}[x]^*$.

Let $m > 0$ and let $\sum_{i=0}^{m} a_i x^i$ be invertible. Then, there exists $\sum_{j=0}^{n} b_j x^j$ in $R_{\alpha,\psi}[x]$ such that $(\sum_{i=0}^{m} a_i x^i)(\sum_{j=0}^{n} b_j x^j) = 1$; since $m > 0$, $a_m b_n^{\alpha^m} = 0$ as the coefficient of x^{m+n}. Hence $b_n = 0$ $\forall n \geq 0$. Continuing, we get $b_i = 0$ $\forall i \geq 0$ and thus $(\sum a_i x^i)0 = 1$. This contradiction came from supposing $m > 0$. Hence,

$$R_{\alpha,\psi}[x]^* = R^*.$$

Definition. Let R be a ring and α an automorphism of R. An element a of R is α-nilpotent if there exists $n \geq 0$ such that $aa^{\alpha} \ldots a^{\alpha^n} = 0$.

The next proposition was proved in [4] for $R[x]$ where R can be any ring.

Proposition I.18. Let R be a commutative ring with identity and α an automorphism of R. Then $R^* = (R_{\alpha}[x])^*$ if and only if R has no nonzero α-nilpotent elements.

Proof. Suppose R has no nonzero α-nilpotent elements. Let $f(x) = \sum_{i=0}^{m} a_i x^i$, $g(x) = \sum_{i=0}^{n} b_i x^i$ be such that $f(x)g(x) = 1$ in $R_{\alpha}[x]$.
Then $\sum_{i+j=0}^{m+n} a_i b_j^{\alpha^i} x^{i+j} = 1$ and this implies $a_o b_o = 1$. Hence, $a_o \in R^*$ and if $m = 0$, then $n = 0$. By symmetry if $m \geq 1$, then $n \geq 1$. In this case, we proceed by induction to reach a contradiction. We have $a_m b_n^{\alpha^m} = 0$; suppose that for each k such that $0 < k \leq p \leq m$,
$a_{m-k} b_n^{\alpha^{m-k}} b_n^{\alpha^{m-k+1}} \ldots b_n^{\alpha^m} = 0$. Since $a_m b_{n-p-1}^{\alpha^m} + a_{m-1} b_{n-p}^{\alpha^{m-1}} + \ldots +$

$a_{m-p}b_{n-1}^{\alpha^{m-p}} + a_{m-p-1}b_n^{\alpha^{m-p-1}} = 0$, as the coefficient of $x^{m+n-p-1}$, by multiplying this equation by $b_n^{\alpha^{m-p}} b_n^{\alpha^{m-p+1}} \ldots b_n^{\alpha^m}$, we obtain $a_{m-p-1}b_n^{\alpha^{m-p-1}} b_n^{\alpha^{m-p}} \ldots b_n^{\alpha^m} = 0$. By induction, $a_o b_n b_n^{\alpha} \ldots b_n^{\alpha^m} = 0$; since $a_o \in R^*$, b_n is α-nilpotent, hence zero. We have then $n \geq 1$ and $b_n = 0 \; \forall n \geq 1$. Hence $n = 0$ and $R_{\alpha}[x]^* = R^*$.

Now suppose that $R^* = R_{\alpha}[x]^*$ and let $aa^{\alpha} \ldots a^{\alpha^n} = 0$ for some $a \in R$ and some $n \geq 0$. Then,
$(1 - ax)(1 + ax + aa^{\alpha}x^2 + \ldots aa^{\alpha} \ldots a^{\alpha^{n-1}} x^n) = 1$. Hence, $1 - ax \in R^*$ which implies $a = 0$.

CHAPTER II

Chain Conditions

In this chapter, we deal mainly with rings with identity. We extend the Hilbert basis theorem and also a result by R.W. Gilmer Jr. in [6]. As a consequence we see that if a ring R is commutative, no twisted polynomial ring with coefficients in R and zero derivation is left (right) Noetherian without R and every twisted polynomial ring with coefficients in R being both left and right Noetherian (including $R[x]$). Finally, we prove that no twisted polynomial ring with coefficients in a ring with identity is either right or left Artinian. We also prove that if not every element in R is α-nilpotent, then $R_\alpha[x]$ is neither left nor right Artinian.

Definition. A ring R is left (right) Noetherian if for every ascending chain of left (right) ideals, $A_1 \subseteq A_2 \subseteq \ldots \subseteq A_i \subseteq \ldots$, there is a positive integer n such that $A_{n+k} = A_n$, $\forall k \geq 0$.

It is a well known result that a ring is left (right) Noetherian if and only if every left (right) ideal is finitely generated [11, pg. 22]. We need this result to prove the following proposition which extends the Hilbert basis theorem [11, pg. 70] to twisted polynomial rings.

Proposition II.1. Let R be a ring with identity. If R is left (right) Noetherian so is $R_{\alpha,\psi}[x]$ for every automorphism α of R and every α-derivation ψ on R.

Proof. Let A be alleft ideal in $R_{\alpha,\psi}[x]$. For each $i \geq 0$ we define the set

$$A_i = \{r \in R \mid \exists \sum_{j=0}^{i} a_j x^j \in A \text{ with } a_i = r^{\alpha^i}\}.$$

Each A_i is a left ideal in R: if $r, s \in A_i$, $\exists \sum_{j=0}^{i} a_j x^j$ and $\sum_{j=0}^{i} b_j x^j \in A$ with $a_i = r^{\alpha^i}$ and $b_i = s^{\alpha^i}$; hence, $\exists \sum_{j=0}^{i} (a_j + b_j)x^j \in A$ with $a_i + b_i = (r + s)^{\alpha^i}$. If $r \in A_i$ and $s \in R$, since $\sum_{j=0}^{i} a_j x^j \in A$ with $a_i = r^{\alpha^i}$, then $\sum_{j=0}^{i} s^{\alpha^i} a_j x^j \in A$ with $s^{\alpha^i} a_i = (sr)^{\alpha^i}$, i.e. $sr \in A_i$. Furthermore, $A_i \neq \emptyset$, for $0 \in A_i$, $i \geq 0$.

For each $i \geq 0$, $A_i \subseteq A_{i+1}$; in fact, let $r \in A_i$; then $\exists \sum_{j=0}^{i} a_j x^j \in A$ with $a_i = r^{\alpha^i}$. Since A is a left ideal, the polynomial $\sum_{j=0}^{i+1} b_j x^j = \sum_{j=0}^{i} a_j^{\psi} x^j + \sum_{j=0}^{i} a_j^{\alpha} x^{j+1} = x \sum_{j=0}^{i} a_j x^j \in A$ and $b_{i+1} = a_i^{\alpha} = r^{\alpha^{i+1}}$. Hence, $r \in A_{i+1}$.

We have therefore an ascending chain of left ideals in R. If R is left Notherian, $\exists\, n \geq 0$ such that $A_n = A_{n+k}$, $\forall k \geq 0$.

Since every A_i is finitely generated as a left ideal, we set $A_i = \sum_{j=1}^{k_i} Rb_{ij}$, $0 \leq i \leq n$. For each b_{ij}, choose $p_{ij}(x)$ in A of degree i with $b_{ij}^{\alpha^i}$ as leading coefficients.

Since A is a left ideal, we have

$$A' = \sum_{i=0}^{n} \sum_{j=1}^{k_i} R_{\alpha,\psi}[x] p_{ij}(x) \subseteq A.$$

We claim that $A' = A$ and prove it by contradiction. Suppose there exists $g(x) \in A$ with $g(x)$ not in A'. Of all such $g(x)$ we choose one with minimum degree m and let $c_m^{\alpha^m}$ be its leading coefficient. Then $c_m \in A_m$ (note that $A_m = A_n$ if $m \geq n$); hence, $c_m = \sum_{j=1}^{k_m} c_{mj} b_{mj}$ for convenient

c_{mj}'s in R. The polynomial $g(x) - \sum_{j=1}^{k_m} c_{mj}^{\alpha^m} p_{mj}(x)$ is in A but not in A' and has degree less than m which contradicts our choice of g(x). Hence A = A' and $R_{\alpha,\psi}[x]$ is therefore left Noetherian.

The previous proof is much the same as that given in [11] for right Noetherian in the case $\alpha = I$ and $\psi = 0$. To complete the proof of proposition II.1, we must still show that if R is right Noetherian, $R_{\alpha,\psi}[x]$ also is right Noetherian. We do that by following exactly the proof given in [11] with two changes:

In order to show that the sets $A_i = \{r \in R \mid \exists \sum_{j=0}^{i} a_j x^j \in A \text{ with } a_i = r\}$ are closed under right multiplication by elements s of R, we multiply $\sum_{j=0}^{i} a_j x^j$ by $s^{\alpha^{-i}}$ on the right and obtain the polynomial $\sum_{j=0}^{i} \sum_{k=0}^{j} \sum_{\xi \in S_j(k)} a_j s^{\xi\alpha^{-i}} x^k \in A$ with leading coefficient as.

To obtain the contradiction after choosing g(x) in A but not in A', we consider the polynomial $g(x) - \sum_{j=1}^{k_m} p_{mj}(x) c_{mj}^{\alpha^{-m}}$.

R.W. Gilmer has proved that if R is a commutative ring and R[x] is Noetherian, then R contains an identity [6]. We extend this result to twisted polynomial rings with zero derivation.

<u>Proposition II.2.</u> If $R_\alpha[x]$ is left (right) Noetherian, R is left (right) Noetherian.

<u>Proof.</u> Consider the mapping $\rho : f(x) \to f(0)$ of $R_\alpha[x]$ onto R. It is a ring homomorphism, for the constant term of the product of two polynomials in $R_\alpha[x]$ is the product of the constant terms of these polynomials.

Let $A_1 \subseteq A_2 \subseteq \ldots \subseteq A_n \subseteq \ldots$ be an ascending chain of left (right) ideals in R. Let $K_i = \rho^{-1}(A_i)$; we have then an ascending chain of left (right) ideals in $R_\alpha[x]$ and since this is a left (right) Noetherian ring there exists $n > 0$ such that $K_{n+\ell} = K_n$, $\forall \ell \geq 0$. Hence, $A_{n+\ell} = A_n$, $\forall \ell \geq 0$.

Proposition II.3. If R is a commutative ring and $R_\alpha[x]$ is left (right) Noetherian, then R contains an identity.

Proof. Suppose $R_\alpha[x]$ is left Noetherian. For each r in R consider the chain of left ideals $(r) \subseteq (r, r^\alpha x) \subseteq \ldots \subseteq (r, r^\alpha x, \ldots, r^{\alpha^i} x^i) \subseteq \ldots$. Because $R_\alpha[x]$ is left Noetherian, there exists $n \geq 0$ such that $r^{\alpha^{n+1}} x^{n+1} \in (r, r^\alpha x, \ldots, r^{\alpha^n} x^n)$, i.e. there exist polynomials $f_i(x) = \sum_j f_{ij} x^j$ in $R_\alpha[x]$ and integers n_i such that

$$r^{\alpha^{n+1}} x^{n+1} = \sum_{i=0}^{n} f_i(x) r^{\alpha^i} x^i + \sum_{i=0}^{n} n_i r^{\alpha^i} x^i \text{ ; hence, } r^{\alpha^{n+1}} = \sum_{i=0}^{n} f_{i,n-i+1} r^{\alpha^{n+1}} .$$

By setting $g_r = \sum_{i=0}^{n} f^{\alpha^{-n-1}}_{i,n-i+1}$, we associate to each element r in R another element g_r such that $r = g_r r$.

Let $\{r_1, r_2, \ldots, r_k\}$ be any finite subset of R. then, there exists $u \in R$ such that $r_i = ur_i$ for each i, $1 \leq i \leq k$. We prove this is true when $k = 2$; the general case follows by induction.

Let g_1 and g_2 be such that $r_1 = g_1 r_1$ and $r_2 = g_2 r_2$. Then, $r_1 = (g_1 + g_2 - g_2 g_1) r_1$ and $r_2 = (g_1 + g_2 - g_1 g_2) r_2$. We take $u = g_1 + g_2 - g_2 g_1$. Since R is commutative, $r_1 = ur_1$ and $r_2 = ur_2$.

By proposition II.2, R is Noetherian and is therefore finitely generated as an ideal in R. This means that we can find a finite subset T of R which generates R. Let $e \in R$ be an element such that $t = et$ for each $t \in T$.

Then e is the identity of R.

If $R_\alpha[x]$ is right Noetherian, we consider the ascending chain of right ideals $(r) \subseteq (r,rx) \subseteq \ldots \subseteq (r,rx, \ldots, rx^i) \subseteq \ldots$, and associate to the element r an element $g_r = \sum_{i=1}^{n} f_{i,n-i+1}^{\alpha^i}$ by following the previous proof, making the obvious changes.

Corollary II.4. Let R be a commutative ring. If for some automorphism α of R, $R_\alpha[x]$ is either left or right Noetherian, then $R_{\beta,\psi}[x]$ is both left and right Noetherian for each $\beta \in \mathrm{Aut}(R)$ and each β-derivation ψ on R.

Proof. Let $R_\alpha[x]$ be left (right) Noetherian; by proposition II.2, R is Noetherian and by proposition II.3, R has an identity. Let β be an automorphism of R and ψ a β-derivation on R. By proposition II.1, $R_{\beta,\psi}[x]$ is both left and right Neotherian.

Definition. A ring R is left (right) Artinian if for every descending chain of left (right) ideals $A_1 \supseteq A_2 \supseteq \ldots \supseteq A_i \supseteq \ldots$ there exists a positive integer n such that $A_{n+k} = A_n$, $\forall k \geq 0$.

Proposition II.5. Let R be a ring with identity, α an automorphism of R and ψ an α-derivation on R. Then $R_{\alpha,\psi}[x]$ is neither left nor right Artinian.

Proof. Consider the chain of left (right) ideals $(x) \supseteq (x^2) \supseteq \ldots \supseteq (x^i) \supseteq \ldots$ in $R_{\alpha,\psi}[x]$. Suppose there exists $n > 0$ such that $x^n \in (x^{n+1})$. Then, there exists $f(x) \in R_{\alpha,\psi}[x]$ $(g(x) \in R_{\alpha,\psi}[x])$, such that

$$x^n = f(x)x^{n+1} \qquad (x^n = x^{n+1}g(x))$$

which is clearly impossible.

The last proposition can be partially extended if we consider zero derivations.

Proposition II.6. If not every element in R is α-nilpotent, $R_\alpha[x]$ is neither left nor right Artinian.

Proof. Let $a \in R$ be such that $aa^\alpha \dots a^{\alpha^n} \neq 0$, $\forall n \geq 0$. Consider the descending chain of left (right) ideals $(ax) \supseteq (aa^\alpha x^2) \supseteq \dots \supseteq (aa^\alpha \dots a^{\alpha^{i-1}} x^i) \supseteq \dots$. If $R_\alpha[x]$ were left (right) Artinian, there should be an $n > 0$, an integer k and elements $b_0, b_1, \dots, b_m$ in R such that

$$aa^\alpha \dots a^{\alpha^{n-1}} x^n = \sum_{i=0}^{m} b_i a^{\alpha^i} a^{\alpha^{i+1}} \dots a^{\alpha^{i+n+1}} x^{i+n+1} + kx^{n+1}$$

$$\left(= \sum_{i=0}^{m} aa^\alpha \dots a^{\alpha^n} b_i^{\alpha^{n+1}} x^{i+n+1} + kx^{n+1} \text{ for right ideals}\right)$$

and therefore $aa^\alpha \dots a^{\alpha^{n-1}} = 0$ which contradicts our assumption.

CHAPTER III

The Noether Radical of $R_\alpha[x]$

Definition. A radical property ϕ is an Amitsur property if for every ring R, $\phi(R[x]) = (\phi(R[x]) \cap R)[x]$ [10].

The prime radical, the Noether radical and the Jacobson radical [13] properties are only a few examples of Amitsur properties. Others are given in [1] and in [10].

For twisted polynomial rings, the situation seems to be far more complicated. For instance, not even the Noether radical satisfies $\mathcal{N}(R_\alpha[x]) = (\mathcal{N}(R_\alpha[x]) \cap R)_\alpha[x]$ for every ring R and every automotphism α of R. We give in this chapter a description of $\mathcal{N}(R_\alpha[x])$ in terms of the coefficients of its elements. The Jacobson and prime radicals seem more difficult to describe.

Definition. Let R be a ring with identity. The Noether radical of R is the set

$$\mathcal{N}(R) = \{a \in R \mid aR \text{ is nilpotent}\} \text{ [13, pg. 59].}$$

Lemma III.1. $\mathcal{N}(R)$ is a nil ideal in R [13, pg. 58].

Proof. If $a, b \in \mathcal{N}(R)$, let $(aR)^k = 0$ and $(bR)^\ell = 0$. Then, $(a + b)R)^{k+\ell-1}$ $\subseteq (aR + bR)^{k+\ell-1}$ which equals a sum of products with $k + \ell - 1$ factors each. We consider in each product the first factor to the left; suppose it is aR. If aR appears at least k times in that product, since aR is a right ideal, the whole product is contained in $(aR)^k = 0$. If in that product aR appears less than k times, then it may be written as

$$(aR)^m \, bRP$$

where $m < k$ and P is a product containing at least $\ell - 1$ factors bR.

Hence the whole product is contained in $(aR)^m(bR)^\ell = 0$. Thus, $a + b \in \mathcal{N}(R)$.

Since $0 \in \mathcal{N}(R)$, $\mathcal{N}(R)$ is a subgroup.

If $a \in \mathcal{N}(R)$ and $r \in R$, $arR \subseteq aR$; if $(aR)^k = 0$, then $(arR)^k = 0$. Also, $raR \subseteq RaR$ and then

$(raR)^{k+1} \subseteq (RaR)^{k+1} = R(aR^2)^k aR \subseteq R(aR)^k R = 0$. Hence, ar, $ra \in \mathcal{N}(R)$.

Since $a \in \mathcal{N}(R)$ implies there exists $k > 0$ such that $a^k = 0$, the ideal $\mathcal{N}(R)$ is nil.

<u>Lemma III.2</u>. $\sum_{1=0}^{m} a_i x^i \in \mathcal{N}(R_\alpha[x])$ if and only if $a_i x^i \in \mathcal{N}(R_\alpha[x])$ $\forall i \geq 0$.

<u>Proof</u>. If $a_i x^i \in \mathcal{N}(R_\alpha[x])$ $\forall i \geq 0$, then $\sum_{i=0}^{m} a_i x^i \in \mathcal{N}(R_\alpha[x])$ because the Noether radical is a subgroup.

If $\sum_{i=0}^{m} a_i x^i \in \mathcal{N}(R_\alpha[x])$, there exists $k > 0$ such that

$\prod_{\ell=1}^{k} (\,^{m}_{i=0} a_i x^i) g_\ell = 0$ $\forall g_\ell = \sum_{j=0}^{n_\ell} g_{\ell,j} x^j \in R_\alpha[x]$. Consequently,

$\prod_{\ell=1}^{k} a_m x^m g_{\ell,n_\ell} x^{n_\ell} = 0$ $\forall g_{\ell,n_\ell} \in R$, $\forall n_\ell \geq 0$. Then $\forall h_i = \sum_{j=0}^{t_i} h_{i,j} x^j$ in $R_\alpha[x]$ we have $\prod_{i=1}^{k} a_m x^m h_i = \sum_{j=0}^{\max\{t_i\}} \prod a_m x^m h_{i,j} x^j = 0$, because each summand is zero.

Hence, $a_m x^m \in \mathcal{N}(R_\alpha[x])$. By induction, $a_i x^i \in \mathcal{N}(R_\alpha[x])$ $\forall i \geq 0$.

<u>Remark</u>. It seems very difficult to obtain the analogue of lemma III.2 for prime and Jacobson radicals.

We describe now the elements of $\mathcal{N}(R_\alpha[x])$ in terms of their coefficients. In view of the last lemma, it is enough to describe the coefficient of each monomial in $\mathcal{N}(R_\alpha[x])$.

Theorem III.3. Let $a \in R$ and $m \geq 0$. Then $ax^m \in \mathcal{N}(R_\alpha[x])$ if and only if there exists a positive integer k such that $\forall r_o, r_1, \ldots, r_{k-1} \in R$ and $\forall j_1, \ldots, j_{k-1}$ with $0 = j_o \leq j_1 \leq \ldots \leq j_{k-1}$, then

$$\prod_{i=0}^{k-1} a^{\alpha^{im+j_i}} r_i = 0.$$

Proof. Suppose that $ax^m \in \mathcal{N}(R_\alpha[x])$; then there exists $k > 0$ such that $\forall s_1, \ldots, s_k \in R$ and $\forall \ell_1, \ldots, \ell_k \geq 0$, $\prod_{i=1}^{k} ax^m s_i x^{\ell_i} = 0$; consequently, $as_1^{\alpha^m} a^{\alpha^{m+\ell_1}} s_2^{\alpha^{2m+\ell_1}} \ldots a^{\alpha^{(k-1)m+\ell_1+\ldots+_{k-1}}} s_k^{km+\ell_1+\ldots+\ell_{k-1}} = 0$. Let $r_o, r_1, \ldots, r_{k-1} \in R$ and $j_o, j_1, \ldots, j_{k-1}$ be such that $0 = j_o \leq j_1 \leq \ldots \leq j_{k-1}$. Take $\ell_1 = j_1$, $\ell_i = j_i - \ell_{i-1}$, for $1 < i < k$ (and $\ell_k \geq 0$); then, take $s_i = r_{i-1}^{\alpha^{-(im + \ell_1+\ldots+\ell_{i-1})}}$ with the understanding that $\ell_o = 0$. By substituting the r_i's and j_i's in the expression above, we obtain $ar_o a^{\alpha^{m+j_1}} r_1 \ldots a^{\alpha^{(k-1)m+j_{k-1}}} r_{k-1} = 0$; hence $\prod_{i=0}^{k-1} a^{\alpha^{im+j_i}} r_i = 0$ (1).

Conversely, suppose that $\forall r_o, r_1, \ldots, r_{k-1} \in R$ and $\forall j_1, \ldots, j_{k-1}$ with $o = j_o \leq j_1 \leq \ldots \leq j_{k-1}$, (1) holds. Let $s_1, \ldots, s_k \in R$ and $\ell_1, \ldots, \ell_k$ be non-negative integers. By taking $r_{i-1} = s_i^{\alpha^{im+\ell_1+\ldots+\ell_{i-1}}}$, with $\ell_o = 0$, and $j_i = \ell_o + \ell_1 + \ldots + \ell_i$ for convenient i's and using (1) we obtain $as_1^{\alpha^m} a^{\alpha^{m+\ell_1}} s_2^{\alpha^{2m+\ell_1}} \ldots a^{\alpha^{(k-1)m+\ell_1+\ldots+\ell_{k-1}}} s_k^{\alpha^{km+\ell_1+\ldots+\ell_{k-1}}} = 0$, i.e. $\prod_{i=1}^{k} ax^m s_i x^{\ell_i} = 0$.

Let $g_i = \sum_{j=0}^{n_i} g_{i,j} x^j \in R_\alpha[x]$; then $\prod_{i=1}^{k} ax^m g_i = \sum_{j=0}^{\max\{n_i\}} \prod_{i=1}^{k} ax^m g_{i,j} x^j = 0$ because each summand is zero. Hence, $ax^m \in \mathcal{N}(R_\alpha[x])$. q.e.d.

We note that the condition $0 = j_o \leq j_1 \leq \dots \leq j_{k-1}$ is equivalent to $0 \leq j_o \leq j_1 \leq \dots \leq j_{k-1}$. In fact, we may apply α or α^{-1} to any such expression as (1) by applying α or α^{-1} respectively to the fixed elements (in (1) they are $a^{\alpha^{im+j_i}}$) and leaving the arbitrary elements unchanged because α (and α^{-1}) is an isomorphism.

<u>Corollary III.4</u>. Let R be a commutative ring with identity, a an element of R and $m \geq 0$. Then $ax^m \in \mathcal{N}(R_\alpha[x])$ if and only if there exists $k > 0$ such that, $0 = j_o \leq j_1 \leq \dots \leq j_{k-1}$ implies $\prod_{i=0}^{k-1} a^{\alpha^{im+j_1}} = 0$.

<u>Proof</u>. Suppose $ax^m \in \mathcal{N}(R_\alpha[x])$ and take $r_o = r_1 = \dots = r_{k-1} = 1$ where k is given by theorem III.3. Then, by this theorem, $\prod_{i=0}^{k-1} a^{\alpha^{im+j_i}} = 0$, $\forall j_o, \dots, j_{k-1}$ such that $0 = j_o \leq j_1 \leq \dots \leq j_{k-1}$.

Conversely, let $k > 0$ be such that $\prod_{i=0}^{k-1} a^{\alpha^{im+j_i}} = 0$ $\forall j_o, \dots, j_{k-1}$ with $0 = j_o \leq j_1 \leq \dots \leq j_{k-1}$. Then $\forall r_o, \dots, r_{k-1} \in R$ and $\forall j_o, \dots, j_{k-1}$ such that $0 = j_o \leq j_1 \leq \dots \leq j_{k-1}$, $\prod_{i=0}^{k-1} a^{\alpha^{im+j_i}} r_i = (\prod_{i=0}^{k-1} a^{\alpha^{im+j_i}})(\prod_{i=0}^{k-1} r_i) = 0$. By theorem III.3, $ax^m \in \mathcal{N}(R_\alpha[x])$.

<u>Corollary III.5</u>. For every ring R, if $ax^m \in \mathcal{N}(R_\alpha[x])$, then $ax^{m+1} \in \mathcal{N}(R_\alpha[x])$.

<u>Proof</u>. Let $ax^m \in \mathcal{N}(R_\alpha[x])$. By theorem III.3, there exists $k > 0$ such that $\forall r_o, \dots, r_{k-1} \in R$ and $\forall\ 0 = j_o \leq \dots \leq j_{k-1}$, $\prod_{i=0}^{k-1} a^{\alpha^{im+j_i}} r_i = 0$. Since $\prod_{i=0}^{k-1} a^{\alpha^{i(m+1)+j_i}} r_i = \prod_{i=0}^{k-1} a^{\alpha^{im+\ell_i}} r_i$ with $0 = \ell_0 \leq \ell_1 \leq \dots \leq \ell_{k-1}$, we have $\prod_{i=0}^{k-1} a^{\alpha^{i(m+1)+j_i}} r_i = 0$ $\forall r_o, \dots, r_{k-1} \in R$ and $\forall j_o, \dots, j_{k-1}$ such that $0 = j_o \leq j_1 \leq \dots \leq j_{k-1}$. Hence, $ax^{m+1} \in \mathcal{N}(R_\alpha[x])$.

In attempting to prove the converse to corollary III.5, we encounter the difficulty of ending up with ℓ_i's which may not satisfy $0 = \ell_o \leq \ell_1 \leq \dots \leq \ell_{k-1}$. Of course, if $\alpha = I_R$, theorem III.3 says that $ax^m \in \mathcal{N}(R[x])$ if and only if there exists $k > 0$ such that $\prod_{i=1}^{k} ar_i = 0$ for all $r_1, \dots, r_k \in R$. Hence $ax^m \in \mathcal{N}(R_\alpha[x])$ if and only if $ax^{m+1} \in \mathcal{N}(R[x])$ and, in this case, $\mathcal{N}(R[x]) = (\mathcal{N}(R))[x]$.

CHAPTER IV

R-Endomorphisms of $R_{\alpha,\psi}[x]$

In this chapter, we are concerned with the ring endomorphisms of $R_{\alpha,\psi}[x]$ which restrict to the identity map on R and, for this reason, are called the R-endomorphisms of $R_{\alpha,\psi}[x]$. If $t \in R_{\alpha,\psi}[x]$, we denote by f_t the substitution map defined by $f_t(g) = g \circ t$ (or $f_t(g(x)) = g(t)$) of $R_{\alpha,\psi}[x]$. If R has an identity, any R-endomorphism of $R_{\alpha,\psi}[x]$ is a substitution map. We ask under what conditions on the coefficients of t is f_t an R-endomorphism? The answer to this question applies also to the case when R has no identity, but then there are R-endomorphisms of $R_{\alpha,\psi}[x]$ of other kinds. We prove that if R is commutative with a regular element, every R-endomorphism of $R_{\alpha,\psi}[x]$ is the restriction to $R_{\alpha,\psi}[x]$ of a T-endomorphism of $T_{\alpha,\psi}[x]$ where T is the total quotient ring of R. Our proof follows the one given by R.W. Gilmer in [7] for the case $\alpha = I_R$. If R is a commutative integral domain, we obtain specific results for $R_\alpha[x]$. We also determine the R-automorphisms of $R_{\alpha,\psi}[x]$ when R is an integral domain with identity and ψ is a non-trivial α-derivation on R.

Proposition IV.1. Let R be a ring with a left regular element and let $t = t_0 + t_1x + \dots + t_nx^n$ be a polynomial with coefficients t_i in R. Then f_t is an R-endomorphism of $R_{\alpha,\psi}[x]$ if and only if $tr = r^\psi + r^\alpha t$ for every r in R.

Proof. By definition, $f_t(g(x)) = g(t) = g \circ t$, $\forall g(x) \in R_{\alpha,\psi}[x]$. Hence, f_t is additive and restricts to the identity map on R.

If f_t is multiplicative, let d be a left regular element in R; then: $dt(x)r = f_t(dx)f_t(r) = f_t(dxr) = f_t(dr^\psi + dr^\alpha x) = dr^\psi + dr^\alpha t(x)$. Since d is left regular in R, it is also left regular in $R_{\alpha,\psi}[x]$; hence, $t(x)r = r^{\psi} + r^{\alpha}t(x)$.

Conversely, if $tr = r^{\psi} + r^{\alpha}t$ for every r in R, let $a,b \in R$ and $m,n \geq 0$. Then $f_t(ax^nbx^m) = f_t(ax^n)f_t(bx^m)$. In fact, this is trivial if $m = 0$ and, if $n > 0$, suppose it holds for $n - 1$, $\forall m \geq 0$, $\forall a,b \in R$. Then,

$$f_t(ax^nbx^m) = f_t(ax^{n-1}(b^{\psi}x^m + b^{\alpha}x^{m+1})) = f_t(ax^{n-1})f_t(b^{\psi}x^m + b^{\alpha}x^{m+1}) =$$

$$at^{n-1}(b^{\psi}t^m + b^{\alpha}t^{m+1}) = at^{n-1}(tbt^m) = at^nbt^m = f_t(ax^n)f_t(bx^m).$$

f_t, being multiplicative on monomials, is multiplicative. q.e.d.

Let $t = \sum_{i=0}^{n} t_ix^i$; by proposition I.1, $tr = \sum_{i=0}^{n}(t_i \sum_{k=0}^{i} \sum_{\xi \in S_i(k)} r^{\xi}x^k)$.

By putting together similar terms we obtain

$tr = \sum_{i=0}^{n} \sum_{k=i}^{n} \sum_{\xi \in S_k(i)} t_kr^{\xi}x^i$. We may therefore rewrite proposition IV.1 as follows:

<u>Proposition IV.1'</u>. Let R be a ring with a left regular element and $t = t_o + t_1x + \dots + t_nx^n$ a polynomial with coefficients t_i in R. Then f_t is an R-endomorphism of $R_{\alpha,\psi}[x]$ if and only if for each r in R the following conditions are verified:

0) $r^{\psi} + r^{\alpha}t_o = \sum_{k=0}^{n} t_kr^{\psi^k}$ and $\forall i > 0$

i) $r^{\alpha}t_i = \sum_{k=i}^{n} \sum_{\xi \in S_k(i)} t_kr^{\xi}$.

We have seen in chapter I that if $a \in R$ and we define $\psi_{a,\alpha}: R \to R$ by $\psi_{a,\alpha}(r) = ar - r^{\alpha}a$; then $\psi_{a,\alpha}$ is an α-derivation on R.

We have also seen that if $a \in C(R)$, then $\psi_{a,\alpha} = a\theta_\alpha$ where $\theta_\alpha = I_R - \alpha$; and that θ_α is an α-derivation on R even if R has no identity. We now show that θ_α and the inner derivations $\psi_{a,\alpha}$ are trivial, in the following sense:

Proposition IV.2. Let a be an element of R. The ring $R_{\alpha,\psi_{a,\alpha}}[x]$ is R-isomorphic to $R_\alpha[x]$.

Proof. Define $\sigma : R_{\alpha,\psi_{a,\alpha}}[x] \to R_\alpha[x]$ by $\sigma(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} a_i(x + a)^i$; σ is obviously additive and restricts to the identity map on R. In order to prove that σ is multiplicative it is enough to prove it is so on monomials of arbitrary degrees m,n. We shall only consider $n = 1$ and for the other cases one may proceed by induction as in proposition IV.1.

Let $b,c \in R$ and $m \geq 0$. Then $\sigma(bx)\sigma(cx^m) = b(x + a)\, c\, (x + a)^m =$ $= (bac + bc^\alpha x)(x + a)^m$; on the other hand, $\sigma(bxcx^m) =$ $\sigma(bc^\psi x^m + bc^\alpha x^{m+1}) = bc^\psi(x + a)^m + bc^\alpha(x + a)^{m+1} = (bac - bc^\alpha a)(x + a)^m +$ $(bc^\alpha x + bc^\alpha a)(x + a)^m = (bac + bc^\alpha x)(x + a)^m$.

If R has no identity, $R_{\alpha,\theta_\alpha}[x]$ is still R-isomorphic to $R_\alpha[x]$ by $\sigma(\sum a_i x^i) = \sum a_i(x + 1)^i$.

Corollary IV.3. If for some $a \in R$ f_a is an R-endomorphism of $R_{\alpha,\psi}[x]$, then $R_{\alpha,\psi}[x]$ is R-isomorphic to $R_\alpha[x]$.

Proof. If f_a is an R-endomorphism by proposition IV.1, $r^\psi + r^\alpha a = ar$. Hence, $\psi(r) = ar - r^\alpha a = \psi_{a,\alpha}(r)$. By proposition IV.2, $R_{\alpha,\psi}[x]$ is R-isomorphic to $R_\alpha[x]$.

The above results are interesting because they show that certain results proved in this and other chapters about $R_\alpha[x]$ actually apply a little more generally. See, for example, corollary IV.6 and Proposition IV.7.

We now consider the case of a commutative integral domain. If $\alpha = I_R$ and $\psi = 0$, we know that every polynomial in $R[x]$ induces an R-endomorphism of $R[x]$. If $\alpha = I_R$ and $\psi \neq 0$, only polynomials of degree 1 induce R-endomorphisms of $R_\psi[x]$ when R had identity and characteristic zero.

Proposition IV.4. Let R be a commutative integral domain with identity and of characteristic zero. If $\psi \neq 0$ is a derivation on R, the only R-endomorphisms of $R_\psi[x]$ are substitution maps $x \to a + x$.

Proof. If $t = a + x$, f_t is an R-endomorphism, according to Proposition IV.1.

If f_t is an R-endomorphism of $R_\psi[x]$, let n be the degree of t. If $n \geq 2$; condition n - 1) in proposition IV.1' reads $nt_n r^\psi = 0$, $\forall r \in R$, because R is commutative. Since $\psi \neq 0$ and R is an integral domain, $nt_n = 0$; since R has charasteristic zero, $t_n = 0$. Hence $n \leq 1$. Let $t = a + bx$; by condition 0), $r^\psi = br^\psi$ $\forall r \in R$. This implies $b = 1$ and $n = 1$.

The last proposition actually holds for any commutative ring R with identity, of characteristic zero, if ψ is such that $\psi(R)$ contains a regular element.

Proposition IV.5. Let R be a commutative integral domain and $\alpha\alpha$ an automorphism of R such that $\alpha^m \neq I$ $\forall m \neq 0$; then f_t is an R-endomorphism of $R_{\alpha,\psi}[x]$ if and only if $t = t_o + t_1 x$ and $\psi - t_1\psi = t_o\theta_\alpha$.

Proof. Suppose f_t is an R-endomorphism and let n be the degree of t. If $n > 1$, condition n) in proposition IV.1' is $t_n\theta_{\alpha^{n-1}} = 0$, because R is commutative. Since $\alpha^{n-1} \neq I_R$, $\theta_{\alpha^{n-1}} \neq 0$; hence $t_n = 0$, because R is an integral domain. Hence $t = t_o + t_1 x$ and $\psi - t_1\psi = t_o\theta_\alpha$ according to condition 0).

Conversely, if $t = t_0 + t_1x$ and $\psi - t_1\psi = t_0\theta_\alpha$, the coefficients of t_0 satisfy the conditions of proposition [illegible] and f_t is therefore an R-endomorphism.

Corollary IV.6. Let R be a commutative integral domain and α an automorphism of R such that $\alpha^m \neq I \ \forall m \neq 0$. Then f_t is an R-endomorphism of $R_\alpha[x]$ if and only if $t = rx$, r in R.

Proof. By proposition IV.5, f_t is an R-endomorphism of $R_\alpha[x]$ if and only if $t = t_0 + t_1x$ with $t_0\theta_\alpha = 0$. Since $\alpha \neq I$ and R is an integral domain, $t_0 = 0$.

Let α be an automorphism of the ring R such that for some integer $m \neq 0$, $\alpha^m = I$; recall that the order of α is the smallest positive integer k for which $\alpha^k = I$.

Proposition IV.7. Let R be a commutative integral domain and α an automorphism of R, of order $k > 1$. Then f_t is an R-endomorphism of $R_\alpha[x]$ if and only if $t = \sum_{i=0}^{n} t_i x^{ik+1}$.

Proof. In the case of a commutative ring and zero derivation, the conditions in proposition IV.1' may be written as ; i) $t_i\theta_{\alpha^{i-1}} = 0 \quad \forall i \geq 0$. Since R is an integral domain, $t_j \neq 0$ implies $\alpha^{j-1} = I$ and hence $j = ik + 1$ for some $i \geq 0$.

Let R be an integral domain with identity. If ψ is a trivial α-derivation on R, the R-automorphisms of $R_{\alpha,\psi}[x]$ may be obtained from the R-automorphisms of $R_\alpha[x]$ which we shall determine in chapter V. For the non-trivial derivations we have the following results:

Proposition IV.8. Let R be an integral domain with identity and ψ a nontrivial α-derivation on R. Then f_t is an R-homomorphism of $R_{\alpha,\psi}[x]$ onto $R_{\alpha,\psi}[x]$ if and only if $t = t_o + t_1x$ with $t_1 \in C(R)^*$, $\psi_{t_o,\alpha} = (1 - t_1)\psi$ and $(1 - t_1) \notin R^*$.

Proof. If t satisfies these conditions, f_t is an R-endomorphism, by proposition IV.1'; and we may write $x = f_t(-t_1^{-1}t_o + t_1^{-1}x)$ which shows that f_t is onto.

If f_t is an epimorphism, there exist $a_o, a_1, \ldots, a_m \in R$ such that $x = \sum_{i=0}^{m} a_i t^i$ in $R_{\alpha,\psi}[x]$; if n is the degree of t, mn cannot be less than 1. Consider $a_m \neq 0$, $t_n \neq 0$ and suppose $mn > 1$. Then $a_m t_n t_n^{\alpha^n} \ldots t_n^{\alpha^{(m-1)n}} = 0$ as the coefficient of x^{mn}. This is absurd because R is an integral domain. Hence, $m = n = 1$ and $x = a_o + a_1(t_o + t_1x)$. This implies $t_1 \in R^*$; f_t being an R-endomorphism, by proposition IV.1', $t_1 \in C(R)$ and $(1 - t_1)\psi = \psi_{t_o,\alpha}$. If $1 - t_1 \in R^*$, then $\psi = (1 - t_1)^{-1}\psi_{t_o,\alpha} = \psi_{(1-t_1)^{-1}t_o,\alpha}$ because $1 - t_1 \in C(R)$, and this contradicts the fact that ψ is not trivial. Hence $1 - t_1 \notin R^*$ and the proof is complete.

The next proposition shows that for nontrivial derivations on an integral domain, every R-endomorphism of $R_{\alpha,\psi}[x]$ is a monomorphism.

Proposition IV.9. Let R be an integral domain and ψ a nontrivial α-derivation on R. Then if t induces an R-endomorphism of $R_{\alpha,\psi}[x]$, f_t is a monomorphism.

Proof. Let f_t be an R-endomorphism of $R_{\alpha,\psi}[x]$ and let n be the degree of t. By the proof of proposition IV.3, $n \geq 1$. Suppose that $\sum_{i=0}^{m} a_i t^i = 0$. The coefficient of x^{nm} is $a_m t_n t_n^{\alpha^n} \ldots t_n^{\alpha^{(n-1)m}}$ if $nm \geq 1$ and, of course equals zero. Hence $a_m = 0$ $\forall m \geq 1$. Then $m = 0$ and $a_o = f_t(a_o) = 0$. Consequently, f_t is injective.

Until now we have studied the conditions on the coefficients of the polynomial $t \in R_{\alpha,\psi}[x]$ which are equivalent to f_t being an R-endomorphism of $R_{\alpha,\psi}[x]$. When R has identity, these are all the R-endomorphisms of $R_{\alpha,\psi}[x]$. If R is commutative, always with a regular element, we may still determine all R-endomorphisms of $R_\alpha[x]$ by embedding R into its total quotient ring.

Proposition IV.10. Let R be a commutative ring, α an automorphism of R, S a ring extending R such that every element regular in R is regular in S, $\mu : R_\alpha[x] \to S$ an R-homomorphism and d a regular element in R. Then μ is uniquely determined by its action on dx.

Proof. Let $\mu_1, \mu_2 : R_\alpha[x] \to S$ be R-homomorphisms such that $\mu_1(dx) = \mu_2(dx) = S$. Then $\forall a \in R$, $\forall n > 0$, $dd^\alpha \ldots d^{\alpha^{n-1}} \mu_i(ax^n) = a\mu_i(dd^\alpha \ldots d^{\alpha^{n-1}} x^n) = a\mu_i(dx)^n = as^n$, for $i = 1,2$. Hence $dd^\alpha \ldots d^{\alpha^{n-1}} \mu_1(ax^n) = dd^\alpha \ldots d^{\alpha^{n-1}} \mu_2(ax^n)$. Since $dd^\alpha \ldots d^{\alpha^{n-1}}$ is regular in R, it is regular in S. Hence $\mu_1(ax^n) = \mu_2(ax^n)$. This is enough to show that $\mu_i = \mu_2$.

Let R be a commutative ring and T its total quotient ring. Any automorphism α of R may be extended to an automorphism of T, which we still denote by α, by defining $\alpha(rd^{-1}) = \alpha(r)\alpha(d)^{-1}$ $\forall r \in R$ and $\forall d$ regular in R. It is easy to verify that α is an automorphism of T.

If μ is an R-endomorphism of $R_\alpha[x]$, we may extend it to a T-endomorphism of $T_\alpha[x]$. In fact, if $\mu(dx) = t(x)$ then, in $T_\alpha[x]$, $\mu(x) = d^{-1}t(x)$. This extension is obviously unique and shows that every R-endomorphism of $R_\alpha[x]$ is the restriction to $R_\alpha[x]$ of a T-endomorphism of $T_\alpha[x]$.

Actually, we must verify that $\forall s \in T$, $s^\alpha d^{-1}t(x) = d^{-1}t(x)s$. Let $s = rc^{-1}$; we have in $R_\alpha[x]$, $r^\alpha t(x)c = c^\alpha t(x)r$; this is also true in $T_\alpha[x]$. Hence, $r^\alpha(c^{-1})^\alpha t(x)cc^{-1} = (c^{-1})^\alpha c^\alpha t(x)rc^{-1}$ which is the same as $s^\alpha t(x) = t(x)s$.

Not all T-endomorphisms of $T_\alpha[x]$ restrict to endomorphisms of $R_\alpha[x]$. If t $T_\alpha[x]$ induces a T-endomorphism f_t , then the restriction g_t of f_t to $R_\alpha[x]$ is an R-homomorphism of $R_\alpha[x]$ into $T_\alpha[x]$. Clearly, g_t is an R-endomorphism of $R_\alpha[x]$ if and only if $Rt_i \subseteq R$ for each coefficient t_i of $t(x)$. (We note that $Rt_i \subseteq R$ emplies $Rt_i^{\alpha^j} \subseteq R \ \forall j$).

If d is a regular element in R, it is regular in T and then it is regular in $T_\alpha[x]$. We may therefore apply proposition IV.10 to conclude that $g_t = g_{t'}$ if and only if $t = t'$.

All this together adds up to the following result:

Theorem IV.11. Let R be a commutative ring with a regular element, T its total quotient ring and α an automorphism of R. Then μ is an R-endomorphism of $R_\alpha[x]$ if and only if there exists a unique polynomial t in $T_\alpha[x]$, satisfying $ts = s^\alpha t$ for each s in T and such that $Rt_i \subseteq R$ for each coefficient t_i of $t(x)$, which restricts to μ on $R_\alpha[x]$.

CHAPTER V

R-Automorphisms of $R_\alpha[x]$

This chapter is divided into three sections. In the first and second, R is a commutative ring with a regular element. For such on R, we have seen in Chapter IV that all R-endomorphisms of $R_\alpha[x]$ are substitution maps $f(x) \to f(t)$ where t is a polynomial in the variable x with coefficients in T, the total quotient ring of R, which satisfy certain conditions. As in chapter IV, we denote by α' the natural extension of α to T. We also denote by α the trivial extension of α to $T_\alpha[x]$; i.e., $h^\alpha = h_o^\alpha + h_1^\alpha x + \ldots + h_n^\alpha x^n$, where $h = h_o + h_1 x + \ldots + h_n x^n$ is any polynomial with coefficients h_i in T. Among the polynomial with coefficients h_i in T. Among the polynomials t with coefficients in T which induce R-endomorphisms of $R_\alpha[x]$, we search for those inducing monomorphisms and those inducing automorphisms. We obtain complete results which generalize the ones obtained by R.W. Gilmer in [7]. J.B. Castillon [2] has also proved theorem V.7 in some special cases. In the third section, R is a ring with identity, not necessarily commutative. We prove that, if R has either no nonzero nilpotent elements or no nonzero α-nilpotent elements the R-automorphisms of $R_\alpha[x]$ are of the form $t_o + t_1 x$ with $\psi_{t_o,\alpha} = 0$ and $t_1 \in R^*$.

Let R be a ring with a regular element. If $t \in R_\alpha[x]$ induces an R-endomorphism of $R_\alpha[x]$, proposition IV.1 tells us that $tr = r^\alpha t$, $\forall r \in R$, and that this condition is also a sufficient one. If $h = h_o + h_1 x + \ldots + h_n x^n$, we denote by h' the polynomial $h_1 + h_2 x + \ldots + h_n x^{n-1}$. Then, if $hr^{\alpha^{-1}} = rh$, we have $h'xr^{\alpha^{-1}} = rh'x$. But $h'xr^{\alpha^{-1}} = h'rx$, i.e. h' commutes with the element r. Let

$S = \{g \in R_\alpha[x] \mid gr = rg, \ \forall r \in R\}$. We note that if $g \in S$, left multiplication by g in $R_\alpha[x]$ coincides with right multiplication by g in $R[x]$. In fact, for each $r \in R$ and each $m \geq 0$, $grx^m = rgx^m$ in $R_\alpha[x]$ and $rx^m g = rgx^m$ in $R[x]$. Hence, if t induces an R-endomorphism of $R_\alpha[x]$, $t' \in S$ and then, left multiplication by t' in $R_\alpha[x]$ coincides with right multiplication by t' in $R[x]$. These remarks are used several times in this chapter. We also note that if R is commutative, S is also commutative. For if $g,h \in S$, gh in $R_\alpha[x]$ equals hg in $R[x]$ because $g \in S$; but $hg = gh$ in $R[x]$ and gh in $R[x]$ equals hg in $R_\alpha[x]$ because $h \in S$. Hence, $gh = hg$ in $R_\alpha[x]$.

Although we shall recall it from time to time, t will be throughout this chapter a polynomial inducing an R-endomorphism of $R_\alpha[x]$ when R has identity. When R has no identity, t will be in $T_\alpha[x]$.

The case of a commutative ring with identity.

As in chapter IV, we denote by f_t the R-endomorphism induced by t. Proposition IV.1' says, in the commutative case, that $t_i \in \mathrm{Ann}_R\theta_{\alpha^{i-1}} = \{a \in R \mid a(r - r^{\alpha^{i-1}}) = 0\}$. Hence, for each $r \in \mathrm{Ann}_R\theta_\alpha$ and for each $s \in R$, $t + r$ and st induce R-endomorphisms of $R_\alpha[x]$. This is so because $\mathrm{Ann}_R\theta_\alpha = \mathrm{Ann}_R\theta_{\alpha^{-1}}$ and $\mathrm{Ann}\theta_{\alpha^i}$ is an ideal $\forall i$.

Lemma V.1. Let $r \in \mathrm{Ann}\theta_\alpha$ and $u \in R^*$. If one of f_t, f_{t+r} and f_{ut} is surjective so are the other two.

Proof. Since t induces an R-endomorphism of $R_\alpha[x]$, for each $s \in R$, $ts = s^\alpha t$; this fact enables us to write $R_\alpha[t]$ for the range of f_t. The same is true for $t + r$ and ut.

The identity $t = t + r - r$ shows that t is in the range of f_{t+r}; then, $R_\alpha[t] \subseteq R_\alpha[t + r]$. By repeating this argument several times we conclude that $R_\alpha[t] = R_\alpha[t + r] = R_\alpha[ut]$. Thus the three endomorphisms have the same range and are therefore simultaneously onto.

<u>Lemma V.2.</u> Let $r \in \mathrm{Ann}\theta_\alpha$ and $u \in R^*$. If one of f_t, f_{t+r} and f_{ut} is injective, so are the other two.

<u>Proof</u>. Suppose f_t is 1 - 1; then $t \notin R$ and the same holds for $t + r$ and ut. Let $a_o + a_1x + \dots + a_kx^k$ be such that $a_o + a_1 (t + r) + \dots + a_k(t + r)^k = 0$. By expanding this expression in powers of t, we obtain a polynomial $g(x)$ with coefficients in R such that $g(t) = 0$. The leading coefficient of $g(t)$ is a_k and because f_t is 1 - 1, $a_k = 0$. So the degree of $a_o + a_1x + \dots + a_kx^k$ cannot be positive and this implies that this polynomial is zero. Because $t = t + r - r$, we have already proved that f_t is a monomorphism if and only if f_{t+r} is a monomorphism.

If $u \in R^*$, we have $f_{ut} (a_o + a_1x + \dots + a_kx^k) = $ $= f_t (a_o + a_iux + \dots + a_kuu^\alpha \dots u^{\alpha^{k-1}} x^k)$ and $a_i = 0$ if and only if $a_iuu^\alpha \dots u^{\alpha^{i-1}} = 0$, i.e. f_{ut} and f_t are simultaneously injective. This completes the proof of lemma V.2.

The next lemma does not require the presence of a regular element in the ring R. In the case $\alpha = I$, it was first proved by N.H. McCoy, then by A. Forsythe; we follow the proof given by W.R. Scott in [14] to extend it to the case of any automorphism α of R.

<u>Lemma V.3.</u> Let $h \in S = \{k \in R_\alpha[x] \mid kr = rk \quad \forall r \in R\}$; then h is a left zero divisor in $R_\alpha[x]$ if and only if there exists a nonzero element c in R such that $ch = 0$.

Proof. Deny the lemma and let $g \neq 0$ be a polynomial of minimum degree for which $hg = 0$. Then g has positive degree, for if $g \in R$, $gh = hg = 0$ against our assumption. Hence, we may write $g = g_o + g_1x + \ldots + g_mx^m$ with $g_m \neq 0$ and $m \geq 1$.

We note that if p and q are any two polynomials in $R_\alpha[x]$, $pq = 0$ if and only if $p^{\alpha^i}q^{\alpha^i} = 0 \;\; \forall i$; also, the action of α does not change the degree of a polynomial.

By our assumption, $g_mh \neq 0$; hence, $g_mh_i = h_ig_m^{\alpha^i} \neq 0$ for some $i \geq 0$ and this implies $h_ig^{\alpha^i} \neq 0$. Let $r \leq n =$ degree of h be the largest integer for which $h_rg^{\alpha^r} \neq 0$. Then

$$hg = (h_o + h_1x + \ldots + h_rx^r)g = 0.$$

The polynomial $h_rg^{\alpha^r}$ has degree smaller than m, for $h_rg_m^{\alpha^r} = 0$. However, $h^{\alpha^r}(h_rg^{\alpha^r}) = h_rh^{\alpha^r}g^{\alpha^r} = 0$, contradicting the minimality of m.

Conversely, if $c \in R$, $ch = 0$ and $c \neq 0$, then $hc = ch = 0$ which completes the proof.

Remark. Since R is commutative, if $\alpha = I$ the set S will be $R[x]$. Thus, another way to prove this lemma is to prove the corresponding proposition for $\alpha = I$, as stated in [14], and then observe that if $h \in S$, h is a left zero divisor in $R_\alpha[x]$ if and only if it is a zero divisor in $R[x]$.

Before starting the next proposition we recall that $t = t_o + t'x$ is a polynomial inducing an R-endomorphism of $R_\alpha[x]$ and that $t' \in S$.

Proposition V.4. A necessary and sufficient condition for f_t to be injective is that t' be left regular in $R_\alpha[x]$.

Proof. If t' is a left zero divisor in $R_\alpha[x]$, by lemma V.3, there exists $c \neq 0$ in R such that $ct' = 0$. By lemma V.2, we may consider $t_o = 0$. Then $f_t(cx) = ct'x = 0$ and f_t is not injective.

To show that the condition is also sufficient, we suppose f_t not injective. Again, assume $t_o = 0$. Let $g \neq 0$ be a polynomial of minimal degree for which $f_t(g) = 0$. Then $g_o = 0$ and $f_t(g) =$ $= t'x(g_1^{\alpha^{-1}} + g_2^{\alpha^{-1}} t + \ldots + g_m^{\alpha^{-1}} t^{m-1}) = t'xf_t(g'^{\alpha^{-1}}) = 0$. Since x is a regular element in $R_\alpha[x]$ and $f_t(g'^{\alpha^{-1}}) \neq 0$ because the degree of g' is smaller than the degree of g, t' is then a left zero divisor and our proof is complete.

E. Snapper has proved in [15] the following result:

Lemma V.5. Let $g = g_o + g_1x + \ldots + g_mx^m$ be a polynomial with coefficients in R. Then g is a unit in $R[x]$ if and only if $g_o \in R^*$ and g_i is nilpotent for each $i \geq 1$.

Proof. Let g be a unit in $R[x]$. If $P \neq R$ is a prime ideal in R, the quotient ring $\bar{R} = R/p$ is an integral domain. The units of $\bar{R}[x]$ are precisely those of $\bar{R}$. The natural ring epimorphism $R[x] \to \bar{R}[x]$, defined by $rx^i \to \bar{r}x^i$, takes units onto units so that $\bar{g}$ is a unit in $\bar{R}[x]$ and is therefore in $\bar{R}^*$; thus $\bar{g}_o \in \bar{R}^*$ and $\bar{g}_i = 0$ for $i \geq 1$. But this is true of any prime ideal $P \neq R$. Hence, g_o is a unit in R and g_i is nilpotent $\forall i \geq 1$.

Conversely, if g is such that g_o is a unit and g_i is nilpotent for each $i \geq 1$, then $g = g_o + (g_1x + \ldots + g_mx^m)$ is a unit in $R[x]$ as the sum of a unit and a nilpotent element.

Corollary V.6. Let $h = h_o + h_1x + \ldots + h_mx^m \in S = \{g \in R_\alpha[x] \mid rg = gr, \forall r \in R\}$. Then h is a left unit in $R_\alpha[x]$ if and only if $h_o \in R^*$ and h_i is nipotent for each $i \geq 1$.

Proof. Since $h \in S$, h is a left unit in $R_\alpha[x]$ if and only if h is a unit in $R[x]$; by lemma V.5, this is true if and only if $h_o \in R^*$ and h_i is nilpotent for each $i \geq 1$.

Theorem V.7. The R-endomorphism f_t of $R_\alpha[x]$ is surjective if and only if $t_1 \in R^*$ and t_i is nilpotent for each $i \geq 2$.

Proof. Suppose f_t is onto. By lemma V.1, we may assume $t_o = 0$. Since f_t is onto, there exist $a_o, a_1, \ldots, a_m \in R$ such that $\sum_{i=0}^{m} a_it^i = x$. Since $t_o = 0$, $a_o = 0$. For each $i > 0$ we have $t^i = (t'x)^i = t'(xt')^{i-1}x = t'(t'^{\alpha}x)^{i-1}x = t'(t^{\alpha})^{i-1}x$. Hence, $x = \sum_{i=0}^{m} a_it^i = \sum_{i=1}^{m} a_it'(t^{\alpha})^{i-1}x = t'(\sum_{i=0}^{m} a_i(t^{\alpha})^{i-1})x$. Since x is regular in $R_\alpha[x]$, $t'\sum_{i=1}^{m} a_i(t^{\alpha})^{i-1} = 1$. Hence, t' is a left unit in $R_\alpha[x]$. On the other hand, $t' \in S$, as we have remarked just before this section. Then, by corollary V.6, $t_1 \in R^*$ and t_i is nilpotent $\forall i \geq 2$.

Conversely, let $t_1 \in R^*$ and t_i be nilpotent for each $i \geq 2$. In view of lemma V.1, we may choose $t_o = 0$ and $t_1 = 1$ without loss of generality.

Let T be the ideal in R generated by the set $\{t_2, t_3, \ldots, t_n, t_2^{\alpha}, t_3^{\alpha}, \ldots, t_n^{\alpha}, \ldots, t_2^{\alpha^{n-2}}, t_3^{\alpha^{n-2}}, \ldots, t_n^{\alpha^{n-2}}\}$. We note that for every $\ell > 0$, every $i_j \geq 2$ and every $k_j \geq 0$ we have $t_{i_1} t_{i_2}^{\alpha^{k_2}} \ldots t_{i_\ell}^{\alpha^{k_\ell}} \in T^{\ell}$. In fact, since $t_{i_1} \in \text{Ann}\,\theta_{\alpha^{i_1-1}}$, $t_{i_1} t_{i_2}^{\alpha^{k_2}} \ldots t_{i_\ell}^{\alpha^{k_\ell}} = t_{i_1} t_{i_2}^{\alpha^{k'_2}} \ldots t_{i_\ell}^{\alpha^{k'_\ell}}$ where k'_j is the smallest nonnegative integer for which $k'_j \equiv k_j \pmod{i_1-1}$

and, therefore, $k'_j < i_1 - 1 \leq n - 1$, i.e., $k'_j \leq n - 2$.

Let ${}^1g = t - \sum_{i=2}^{n} t_i t^i$; since $t = x + t_2x^2 + \ldots + t_nx^n$, ${}^1g = x + \sum_{i=2}^{m_1} {}^1g_i x^i$ with ${}^1g_i \in T^2$ for each $i \geq 2$.

By induction, we define

${}^kg = {}^{k-1}g - \sum_{i=0}^{m_{k-1}} {}^{k-1}g_i g^i$; then ${}^kg = x + \sum_{i=2}^{m_k} {}^kg_i x^i \in T^{2^k}$. Let p be the order of nilpotence of the ideal T. Then there is an integer k such that $2^{k-1} < p \leq 2^k$. Hence, for this particular k, ${}^kg = x$. But ${}^kg$ is an R-linear combination of powers of t, which proves that f_t is onto. q.e.d.

In the proof of theorem V.7, we have seen that if f_t is surjective then t' (which is in S) is a left unit in $R_\alpha[x]$. It is also a right unit in $R_\alpha[x]$ for if $x = f_t(h)$ then $x = f_t(h'x) = f_t(h')t'x$. Hence $f_t(h')t' = 1$.

<u>Corollary V.8.</u> The R-endomorphism f_t of $R_\alpha[x]$ is surjective if and only if t' is a unit in $R_\alpha[x]$.

<u>Proof.</u> We have just seen that if f_t is surjective, then t' is a unit in $R_\alpha[x]$.

Conversely, if t' is a unit in $R_\alpha[x]$, it is also a unit in $R[x]$, because $t' \in S$. By lemma V.5, $t_1 \in R^*$ and t_i is nilpotent $\forall i \geq 2$. By theorem V.7, f_t is surjective.

<u>Corollary V.9.</u> If f_t is surjective, it is injective.

<u>Proof.</u> If f_t is surjective, by corollary V.8, t' is a unit. By proposition V.4, f_t is injective.

Summing up our results so far, we may state the following theorem:

Theorem V.10. Let R be a commutative ring with identity, α an automorphism of R and t a polynomial in the variable x with coefficients t_i in R. Then t induces an R-endomorphism f_t of $R_\alpha[x]$ if and only if $t_i \in \mathrm{Ann}_R\theta_{\alpha^{i-1}}$ for each $i \geq 0$; in this case, the following are equivalent:

1) f_t is a monomorphism
2) t' is left regular in $R_\alpha[x]$
3) $\bigcap_{i \geq 1} \mathrm{Ann}_R(t_i) = 0$;

also, the following are equivalent:

1) f_t is an epimorphism
2) f_t is an automorphism
3) t' is a unit in $R_\alpha[x]$
4) $t_1 \in R^*$ and t_i is nilpotent for each $i \geq 2$.

The case of a commutative ring with a regular element.

In this section, R is a commutative ring with a regular element, T the total quotient ring of R, t a polynomial in the indeterminate x, with coefficients t_i in T, inducing a T-endomorphism f_t, and g_t the restriction to $R_\alpha[x]$ of f_t. We have seen in theorem IV.11 that g_t is an R-endomorphism of $R_\alpha[x]$ if and only if $Rt_i \subseteq R$ for each coefficient t_i of t. Since we are interested only in R-endomorphisms of $R_\alpha[x]$ we assume in this section that $Rt_i \subseteq R$ for each $i \geq 0$.

Remark. If $a \in \mathrm{Ann}_T(\theta_{\alpha^i}(T))$, then $a \in \mathrm{Ann}_T(\theta_{\alpha^i}(R))$. The converse is also true. In fact, if $a \in \mathrm{Ann}_T(\theta_{\alpha^i}(R))$ let $s = rd^{-1} \in T$. We have $a(s - s^{\alpha^i}) = a(rd^{-1} - r^{\alpha^i}(d^{-1})^{\alpha^i}) = d^{-1}(d^{-1})^{\alpha^i} a(rd^{\alpha^i} - r^{\alpha^i} d)$. Since

$a \in \mathrm{Ann}_T(\theta_{\alpha^i}(R))$, $ard^{\alpha^i} = ad^{\alpha^i}r = adr = ard = ar^{\alpha^i}d$; hence, $a \in \mathrm{Ann}_T(\theta_{\alpha^i}(T))$. We may then refer only to $\mathrm{Ann}_T\theta_{\alpha^i}$. Also, since $\mathrm{Ann}_R\theta_{\alpha^i} = \mathrm{Ann}_T\theta_{\alpha^i} \quad R$, if we know where the element a is, we may write simply $\mathrm{Ann}\theta_{\alpha^i}$.

<u>Lemma V.11</u>. Let $s \in \mathrm{Ann}_T\theta_\alpha$, and $u \in T^*$ be such that $Rs \subseteq R$ and $Ru = R$. Then if one of g_t, g_{t+s} and g_{ut} is surjective so are the other two.

<u>Proof</u>. We first note that g_{t+s} and g_{ut} are R-endomorphisms of $R_\alpha[x]$. In fact, the coefficients of $t + s$ and of ut satisfy the conditions of theorem IV.12 because $Rs \subseteq R$ and $Ru = R$.

Suppose g_t is surjective. Given h with coefficients in R, there exist $a_o, a_1, \ldots, a_m \in R$ such that $\sum_{i=0}^{m} a_i t^i = h$, for some integer m. Then, if $v = u^{-1}$, $g_{ut}(\sum_{i=0}^{m} a_i vv^\alpha \ldots v^{\alpha^{i-1}} x^i) = \sum_{i=0}^{m} a_i vv^\alpha \ldots v^{\alpha^{i-1}}(ut)^i = h$; because $Rv \subseteq R$, g_{ut} is then onto. Furthermore, since $\sum_{i=0}^{m} a_i((t + s) - s)^i = h$ and $Rs \subseteq R$, h can be expressed as an R-linear combination of powers of $t + s$ which proves that f_{t+s} in onto.

We complete the proof by observing that $t = t + s - s = u^{-1}ut$ with $-s \in \mathrm{Ann}_T\theta_\alpha$, $u^{-1} \in T^*$, $R(-s) \subseteq R$ and $Ru^{-1} = R$.

<u>Lemma V.12</u>. g_t is surjective if and only if f_t is surjective and $Rt_1 = R$.

<u>Proof</u>. If g_t is surjective, given $h \in T_\alpha[x]$, consider a regular element d for which $dh \in R_\alpha[x]$ and the polynomial k for which $g_t(k) = dh$. Then $f_t(d^{-1}k) = d^{-1}g_t(k) = h$ and f_t is therefore surjective. By theorem V.7, t_1 is a unit. We may assume $t_o = 0$ (cf. lemmas V.1 and V.11). Let r be in R; since g_t is onto, there exists $h \in R_\alpha[x]$ such that $g_t(h) = rx$. Since

Since $t_o = 0$, $h_1 t_1 = r$ which shows that $R \subseteq Rt_1$. But we have assumed in this section that $Rt_1 \subseteq R$. Hence, $Rt_1 = R$.

Conversely, suppose that f_t is onto and $Rt_1 = R$. Since $t_1 \in T^*$ we also have $Rt_1^{-1} = R$. Then, by lemmas V.1 and V.11, we may suppose $t_o = 0$ and $t_1 = 1$. Let $h = h_o + h_1 x + \ldots + h_m x^m \in R_\alpha[x]$; because f_t is onto, there exists $k = k_o + k_1 x + \ldots + k_s x^s \in T_\alpha[x]$ such that $h = k_o + k_1 t + \ldots + k_s t^s$. Then $k_o = h_o \in R$. We assume now that for $i \geq 1$, $k_o, k_1, \ldots, k_{i-1} \in R$; then $h - k_o - k_1 t - \ldots - k_{i-1} t^{i-1} \in R_\alpha[x]$, i.e., $p = k_i t^i + k_{i+1} t^{i+1} + \ldots + k_s t^s \in R_\alpha[x]$. The coefficient of x^i in p is k_i; hence $k_i \in R$. By induction, $k_o, k_1, \ldots, k_s \in R$ and g_t is therefore onto.

<u>Lemma V.13.</u> g_t is injective if and only if f_t is injective.

<u>Proof.</u> If f_t is $1 - 1$, g_t is obviously $1 - 1$. If g_t is $1 - 1$, let h be a polynomial in $T_\alpha[x]$ such that $f_t(h) = 0$. Let d be a regular element for which $dh \in R_\alpha[x]$; then $g_t(dh) = df_t(h) = 0$. Consequently, $dh = 0$ and since d is regular also in $T_\alpha[x]$, $h = 0$.

By putting together the results of this section and theorem V.10, we may state the following theorem:

<u>Theorem V.14.</u> Let R be a commutative ring with a regular element, α an automorphism of R and T the total quotient ring of R. Then μ is an R-endomorphism of $R_\alpha[x]$ if and only if μ is a substitution map g_t defined by $\sum r_i x^i \to \sum r_i t^i$ where $r_i \in R$ and t is a polynomial in $T_\alpha[x]$ satisfying $t_i \in \mathrm{Ann}\,\theta_{\alpha^{i-1}}$ and $Rt_i \subseteq R$ for each $i \geq 0$. In this case, the following are equivalent:

1) g_t is a monomorphism

2) t' is left regular in $T_\alpha[x]$

3) $\bigcap_{i\geq 1} \mathrm{Ann}_T(t_i) = 0$;

also the following are equivalent:

1) g_t is an epimorphism

2) g_t is an automorphism

3) t' is a unit in $T_\alpha[x]$ and $Rt_1 = R$

4) $t_1 \in T^*$, t_i is nilpotent $\forall i \geq 2$ and $Rt_1 = R$.

The case of a ring with identity.

In this section we consider the R-automorphisms of $R_\alpha[x]$ where R is any ring with identity. We continue to assume that $t = t_o + t'_x$ induces an R-endomorphism of $R_\alpha[x]$, i.e. $tr = r^\alpha t$ $\forall r \in R$.

The following lemma was proved for commutative rings (lemma V.1 and V.2) but commutativity was not involved in the proofs.

Lemma V.15. Let $r \in R$ be such that $s^\alpha r = rs$ $\forall s \in R$. Then:

a) f_t is surjective if and only if f_{t+r} is surjective.

b) f_t is injective if and only if f_{t+r} is injective.

The remark after theorem V.7 tells us that if f_t is surjective, then t' is a unit in $R_\alpha[x]$. There again, the fact that R was commutative is irrelevant and we may use this result here.

Corollary V.9 holds also for noncommutative rings; we give here a direct proof which works for all rings with identity.

Lemma V.16. If f_t is surjective it is also injective.

Proof. Suppose f_t is surjective and $\sum_{i=0}^{m} a_i t^i = 0$; we may take $t_o = 0$ so that $a_o = 0$. Suppose now that $a_o = a_1 = \ldots = a_{k-1} = 0$ for some $k \leq m$. Then $\sum_{i\geq k} a_i t^i = 0$ and by factoring out x on the right and t' on the left, $t'(\sum_{i\geq k} a_i (t^\alpha)^{i-1})x = 0$. Since t' is a unit in $R_\alpha[x]$, we have $\sum_{i\geq k} a_i (t^\alpha)^{i-1} = 0$ which implies $a_k = 0$. By induction, $a_i = 0$ for all i.

We prove now the following result which can be found in [4].

Theorem V.17. f_t is an R-automorphism of $R[x]$ if and only if $t_1 \in R^*$ and t_i is nilpotent for each $i \geq 2$.

Proof. Let C be the centre of R; since f_t is an R-endomorphism of $R[x]$, $t \in C[x]$ (cf. proposition IV.1).

If f_t is an automorphism it takes $C[x] = C(R[x])$ onto $C[x]$, i.e. t induces a C-automorphism of $C[x]$; by theorem V.7, $t_1 \in C^* \subseteq R^*$ and t_i is nilpotent $\forall i \geq 2$.

Conversely, if $t_1 \in R^*$ and t_i is nilpotent for $i \geq 2$, we may apply theorem V.7 to $C[x]$, because t_i is in C and hence $t_1 \in C^*$. Thus t induces a C-automotphism of $C[x]$. Then, there exists $\sum a_i x^i \in C[x] \subseteq R[x]$ such that $x = \sum a_i t^i$. Hence, f_t is onto and, by lemma V.16, an isomorphism.

The following result was proved in [4]:

Lemma V.18. Let R be a ring with identity. Then $R[x]^* = R^*$ id and only if R has no nonzero nilpotent elements.

Proof. If $r^k = 0$ and $r \neq 0$, then $1 - rx$ is a unit in $R[x]$ with inverse $r^{k-1}x^{k-1} + r^{k-2}x^{k-2} + \dots + rx + 1$.

Conversely, if R has no nonzero nilpotent elements, suppose that $(\sum_{i=0}^{n} a_ix^i)(\sum_{i=0}^{m} b_ix^i) = \sum_{i=0}^{m} b_ix^i)(\sum_{i=0}^{n} a_ix^i) = 1$ with $n \geq 1$. Then $a_nb_m = 0$.

We assume for our proof that $a_nb_m = a_nb_{m-1} = \dots - a_nb_{m-k} = 0$ for some $k \geq 0$ and consider the coefficient of $x^{m+n-(k+1)}$. we have $a_nb_{m-k-1} + a_{n-1}b_{m-k} + \dots + a_{n-k-1}b_m = 0$. Since $a_nb_{m-j} = 0$ for $0 \leq j \leq k$, $(b_{m-j}a_n)^2 = b_{m-j}a_nb_{m-j}a_n = 0$ and then $b_{m-j}a_n = 0$.

By mutliplying the above equation on the right by a_n, we obtain $a_nb_{m-k-1}a_n = 0$. This shows that a_nb_{m-k-1} is nilpotent, hence, zero. By induction, $a_nb_o = 0$; but b_o is a unit since $a_ob_o = b_oa_o = 1$. Therefore, $a_n = 0$ and the only units of $R[x]$ are those of R.

Corollary V.19. If R is a ring without nonzero nilpotent elements, f_t is an R-automorphism of $R_\alpha[x]$ if and only if $t_1 \in R^*$ and $t_i' = 0$ $\forall i \geq 2$.

Proof. We have seen that such a polynomial t always induces an R-automorphism (provided it induces an R-endomorphism which is assumed here).

Conversely, if f_t is onto, by the remark after lemma V.15, $t' \in R_\alpha[x]^*$. Then, since t' is in S, its inverse is also in S. In fact if we set $h = (t')^{-1}$, $t'hr = rt'h = t'rh$ for each $r \in R$. Hence $hr = rh$ $\forall r \in R$. This means that $h \in S$ and that $t'h = ht' = 1$ also in $R[x]$. By lemma V.18, $t' \in R^*$. Consequently, $t_1 \in R^*$ and $t_i = 0$ $\forall i \geq 2$.

We have seen (cf. proposition I.18) that if R is a commutative ring with identity without nonzero α-nilpotent elements, then $R_\alpha[x]^* = R^*$. This may not be true for the noncommutative case but still we can state the following proposition:

Proposition V.20. If R is a ring without nonzero α-nilpotent elements, f_t is an R-automorphism of $R_\alpha[x]$ if and only if $t_1 \in R^*$ and $t_i = 0$ $\forall i \geq 2$.

Proof. As in corollary V.19, if $t = t_o + t_1 x$ and $t_1 \in R^*$, then f_t is an automorphism.

If f_t is an R-automorphism we know that t' is in $R_\alpha[x]^*$; let $t'^{-1} = h_1 + h_2 x + \ldots + h_m x^{m-1}$. Then $h_1 t_1 = 1 = t_1 h_1$, i.e., $h_1, t_1 \in R^*$. Also $h_m t_n{}^{\alpha^{m-1}} = 0$.

We assume for the proof that $h_{m-p} t_n^{\alpha^{m-p-1}} t_n^{\alpha^{m-p}} \ldots t_n^{\alpha^{m-1}} = 0$, $\forall\, 0 \leq p \leq k < m-1$.

Since $h_{m-k-1} t_n^{\alpha^{m-k-2}} + h_{m-k} t_{n-1}^{\alpha^{m-k-1}} + \ldots + h_m t_{n-k-1}^{\alpha^{m-1}} = 0$, as the coefficient of $x^{m+n-k-3}$, if we multiply this equation on the right by $t_n^{\alpha^{m-k-1}} \cdot t_n^{\alpha^{m-k}} \ldots t_n^{\alpha^{m-1}}$, we obtain

$$h_{m-k-1} t_n^{\alpha^{m-k-2}} \ldots t_n^{\alpha^{m-1}} + t_{n-1} h_{m-k} t_n^{\alpha^{m-k-1}} \ldots t_n^{\alpha^{m-1}} +$$

$$+ t_{n-2} t_n^{\alpha^{-1}} h_{m-k+1} t_n^{\alpha^{m-k}} \ldots t_n^{\alpha^{m-1}} + \ldots + t_{n-k-1} t_n^{\alpha^{-k}} \ldots t_n^{\alpha^{-1}} h_m t_n^{\alpha^{m-1}} = 0,$$

because $h_i x^{i-1} \in S$ for each $i \geq 1$. Hence, $h_{m-k-1} t_n^{\alpha^{m-k-2}} \ldots, t_n^{\alpha^{m-1}} = 0$. By induction, we conclude that $h_1 t_n t_n^{\alpha} \ldots t_n^{\alpha^{m-1}} = 0$. Since $h_1 \in R^*$ this implies that t_n is an α-nilpotent element in R; consequently, $t_n = 0$ $\forall n \geq 2$.

Although the next result is not directly related to the R-automorphisms, it suggests that corollary V.19 and proposition V.20 may not be completely independent.

Proposition V.21. Let $a \in R$ be such that for some $k \geq 0$, $ax^k \in S$. Then if a is nilpotent, a [illegible] nilpotent.

Proof. Let $ax^k \in S$ and $a^p = 0$ for some positive integer p. We consider the product $aa^{\alpha}a^{\alpha^2} \dots a^{\alpha^{k(p-1)}}$. We have

$$aa^{\alpha} \dots a^{\alpha^k} a^{\alpha^{k+1}} \dots a^{\alpha^{k(p-1)}} = a^{\alpha^{1-k}} a^{\alpha^{2-k}} \dots a^{\alpha^{-1}} aa^{\alpha^k} a^{\alpha^{k+1}} \dots a^{\alpha^{k(p-1)}} =$$

$$= a^{\alpha^{1-k}} \dots a^{\alpha^{-1}} a^2 a^{\alpha^{k+1}} \dots a^{\alpha^{k(p-1}} = (a^{\alpha^{1-k}} \dots a^{\alpha^{-1}})^2 a^2 a^{\alpha^{2k}} a^{\alpha^{2k+1}} \dots a^{\alpha^{k(p-1)}} =$$

$$= (a^{\alpha^{1-k}} \dots a^{\alpha^{-1}})^2 a^3 a^{\alpha^{2k+1}} \dots a^{\alpha^{k(p-1)}} = \dots = (a^{\alpha^{1-k}} \dots a^{\alpha^{-1}})^{p-1} a^p = 0$$

which proves our statement.

The next lemma is proved in [4]:

Lemma V.22. If the set N of the nilpotent elements of R is an ideal in R, then every unit in $R[x]$ has the form $r_o + r_1x + \dots + r_mx^m$ with $r_o \in R^*$ and r_i nilpotent for each $i \geq 1$.

Proof. Since $\pi : R[x] \to R/_N[x]$ is an epimorphism, every unit in $R[x]$ is mapped onto a unit in $R/_N[x]$. Hence, if g is a unit in $R[x]$, $\pi(g) = \bar{r}_o + \bar{r}_1 x + \dots + \bar{r}_m x^m$ is a unit in $R/_N[x]$; because $R/_N$ has no non-zero nilpotent elements, by lemma V.16, $\pi(g)$ $R/_N$. Hence $r_o \in R^*$ and $r_i \in N$ for each $i \geq 1$.

Proposition V.23. If the set N of the nilpotent elements of R is an ideal in R and f_t is an R-automorphism of $R_{\alpha}[x]$, then $t_1 \in R^*$ and t_i is nilpotent for each $i \geq 2$.

Proof. If f_t is onto $t' \in R[x]^*$ and by the previous lemma $t_1 \in R^*$ and t_i is nilpotent for each $i \geq 2$.

CHAPTER VI

Isomorphic Polynomial Rings

We consider here the situation in which two twisted polynomial rings are isomorphic. One question to ask is: does $R_{\alpha}[x] \approx S_{\beta}[x]$ imply $R \approx S$? When $\alpha = I_R$ and $\beta = I_S$, the answer is negative - a counter example was given by M. Hochster in [9] and we shall study it in detail next chapter.

In what follows, all rings have identity. We prove below that if R and S are commutative semisimple Artinian rings such that $R_{\alpha}[x] \approx S_{\beta}[x]$ for some $\alpha \in \mathrm{Aut}(R)$ and some $\beta \in \mathrm{Aut}(S)$, then R and S are sub-isomorphic, i.e., there exists ring monomorphisms $\mu : R \to S$ and $\nu : S \to R$. For the usual polynomial rings, D.B. Coleman and E.E. Enochs have proved in [4] that if R is a semisimple Artinian ring and $\sigma : R[x] \to S[x]$ is a ring isomorphism, then $\sigma(R) = S$. In this proof, the authors use the fact that $\sigma(x)$ induces an S-endomorphism of $S[x]$. For the twisted polynomial rings we could not use the above argument since there seems to be no reason why $\sigma(X)$ should induce an S-endomorphism of $S_{\beta}[x]$.

We need the following concepts and lemmas, most of which may be found in [13]:

<u>Definition.</u> A ring is simple when its only ideals are 0 and the ring itself.

<u>Definition.</u> A ring is semisimple when it is the direct sum of a family of simple rings.

<u>Lemma VI.1.</u> If I is a nilpotent ideal in R such that $\alpha(I) = I$, then $I_{\alpha}[x]$ is a nilpotent ideal in $R_{\alpha}[x]$.

Proof. By proposition I.5 and corollary I.7, $I_\alpha[x]$ is an ideal in $R_\alpha[x]$. Since I is nilpotent, there exists a positive integer k such that $I^k = 0$. Let $f_i = \sum f_{i,j}x^j \in I_\alpha[x]$, then,

$$\prod_{i=0}^{k} f_i = f_{1,j_1} f_{2,j_2}^{\alpha^{j_1}} \cdots f_{k,j_k}^{\alpha^{j_1+\cdots+j_{k-1}}} x^{j_1+\cdots j_k} = 0$$ because each product

$$f_{1,j_1} f_{2,j_2}^{\alpha^{j_1}} \cdots f_{k,j_k}^{\alpha^{j_1+\cdots+j_{k-1}}} \in I^k.$$

Lemma VI.2. [13, pg. 45]. If R is left Artinian and I is an ideal in R, $R/_I$ is left Artinian.

Proof. Let $J_1 \supseteq J_2 \supseteq \ldots \supseteq J_i \supseteq \ldots$ be a descending chain of left ideals in R. If $\pi : R \to R/_I$ is the canonical epimorphism, then $\pi^{-1}(J_1) \supseteq \pi^{-1}(J_2) \supseteq \ldots \supseteq \pi^{-1}(J_i) \supseteq \ldots$ is a descending chain of left ideals in R. Hence, there exists $n > 0$ such that $\pi^{-1}(J_n) = \pi^{-1}(J_{n+k})$, $\forall k \geq 0$. Consequently, $J_n = J_{n+k}$, $\forall k \geq 0$.

Lemma VI.3. If R is commutative and I is a nil ideal of R, then the idempotents of $R/_I$ can be lifted to idempotents of R [11, pg. 72].

Proof. Let R be a commutative ring, N a nil ideal of R and $\bar{r} \in R/_N$ an idempotent element. Then $s = r^2 - r \in N$.

Let $e = r + x(1 - 2r)$ with x to be determined by the equation $e^2 = e$. This equation is equivalent to $(1 + 4s)(x^2 - x) + s = 0$ which is satisfied by $x = \frac{1}{2}(2s - \binom{4}{2}s^2 + \binom{6}{3}s^3 - \ldots + (-1)^k\binom{2(k-1)}{k-1}s^{k-1})$, where k is a positive integer such that $s^k = 0$. Since $s \in N$, we have $x \in N$ and then $\bar{e} = \bar{r}$.

Let R be a ring, $J(R)$ its Jacobson radical and N the set of all nilpotent elements in R. In general there is no connection between $J(R)$ [illegible] and N. However, when R is a commutative Artinian ring, $J(R) = N$. This is proved in [13] in two steps: since R is commutative, N is a nil ideal and then $N \subseteq J(R)$ [13, pg. 68]; since R is Artinian, $J(R)$ is a nilpotent ideal [13, pg. 69] and hence $J(R) \subseteq N$. We use this fact in the proof of the next proposition.

Proposition VI.4. Let R and S be commutative Artinian rings. If there exist $\alpha \in \mathrm{Aut}(R)$ and $\beta \in \mathrm{Aut}(S)$ such that the rings $R_\alpha[x]$ and $S_\beta[x]$ are isomorphic, then $R/_{J(R)}$ and $S/_{J(S)}$ are sub-isomorphic.

Proof. Let $\sigma : R_\alpha[x] \to S_\beta[x]$ be a ring isomorphism. Since $J(R)$ is nilpotent and $\alpha(J(R)) = J(R)$, by lemma VI.1, $J(R)_\alpha[x]$ is a nilpotent ideal in $R_\alpha[x]$; hence, $I = \sigma(J(R)_\alpha[x])$ is a nilpotent ideal in $S_\beta[x]$. This implies that the constant term of every polynomial in I is nilpotent and therefore, an element of $J(S)$.

We are going to construct a monomorphism from $\bar{R} = R/_{J(R)}$ into $\bar{S} = S/_{J(S)}$. By proposition I.8, $\bar{R}_\alpha[x] \simeq R_\alpha[x]/_{J(R)_\alpha[x]}$ via $\tau : \sum \bar{r}_i x^i \to \overline{\sum r_i x^i}$; also, since $\sigma(J(R)_\alpha[x]) = I$, $\bar{\sigma} : R_\alpha[x]/_{J(R)_\alpha[x]} \to S_\beta[x]/_I$, defined by $\bar{\sigma}(\overline{\sum r_i x^i}) = \sigma(\sum r_i x^i) + I$, is a ring isomorphism.

According to lemma VI.2, $\bar{R}$ is Artinian; $\bar{R}$ is also semisimple [13, pg 69], because $J(R/_{J(R)}) = 0$. By the Wedderburn theorem [13, pg. 53], $\bar{R}$ is isomorphic to the direct sum of a finite number of square matrices with entries in some fields. Since $\bar{R}$ is commutative, these matrices have order 1 and each of them is a commutative field. It follows that each element of $\bar{R}$ is of the form ue where u is a unit and e is an idempotent element. In fact, if $(r_1, \ldots, r_k) \in F_1 \oplus \ldots \oplus F_k$ where each F_i is a field, we may write

$(r_1, \ldots, r_k) = (u_1, \ldots, u_k)(e_1, \ldots, e_k)$ with $u_i = r_i$ and $e_i = 1$, if $r_i \neq 0$, and $u_i = 1$ and $e_i = 0$ if $r_i = 0$.

We now define $\rho : S_\beta[x]/_I \rightarrow \bar{S}$ by $\rho(\sum s_i x^i + I) = \bar{s}_o$; ρ is well defined, for $\sum s_i x^i \in I$ implies $\sum s_i x^i$ is nilpotent in $S_\beta[x]$ and then, s_o is nilpotent and is therefore in $J(S)$. It is easy to verify that ρ preserves sums and products.

Finally, we define $\mu : \bar{R} \rightarrow \bar{S}$ by $\mu(\bar{r}) = \rho\bar{\sigma}\tau(\bar{r})$; we want to prove that μ is a monomorphism. If $\bar{r}$ is a unit, $\mu(\bar{r})$ is a unit because μ is a ring homomorphism. If $\bar{r} \neq 0$ is an idempotent, let $\bar{s}_o = \mu(\bar{r})$. Since $\bar{\sigma}\tau$ is an isomorphism, $\bar{\sigma}\tau(\bar{r}) = \sum s_i x^i + I$ is a nonzero idempotent. By lemma VI.3, we may choose $\sum s_i x^i$ to be an idempotent. Then $(\sum s_i x^i)^2 = \sum s_i x^i$ and consequently, $s_o^2 = s_o$. On the other hand, s_o cannot be zero; otherwise, we would obtain $s_1 = 0$ from $(\sum s_i x^i)^2 = \sum s_i x^i$, contradicting the fact that $\bar{\sigma}\tau(\bar{r}) \neq 0$. Hence, s_o is a nonzero idempotent; since $J(S)$ has no nonzero idempotents, $\bar{s}_o \neq 0$. Recalling that any $\bar{r} \neq 0$ in $\bar{R}$ can be written as $\bar{r} = ue$ where u is a unit and e is a nonzero idempotent we obtain $\mu(\bar{r}) = \mu(ue) = \mu(u)\mu(e) \neq 0$ since $\mu(u)$ is a unit and $\mu(e) \neq 0$ by the above remarks.

Symmetrically, we construct a monomorphism $\nu : \bar{S} \rightarrow \bar{R}$ and the proof is complete.

Corollary VI.5. If R and S are commutative semisimple Artinian rings and $R_\alpha[x] \simeq S_\beta[x]$, then R and S are sub-isomorphic.

Proof. We note that $R/_{J(R)} = R$, and $S/_{J(S)} = S$; then, by proposition VI.4, R and S are sub-isomorphic.

CHAPTER VII

A Noninvariant Ring

M. Hochster has shown in [9] that not every ring is invariant, by exibiting two nonisomorphic rings which yield isomorphic polynomial rings. In order to give a detailed account of this example, we need several concepts and results in commutative algebra. All rings will be commutative with identity.

We first define and construct a tensor algebra on an R-module; we then define symmetric algebra and prove the existence and uniqueness up to isomorphism of such an algebra. After that we prove some properties of symmetric algebras [3] which are used in the sequel. Finally, we define formally real domains [16] and prove two simple results about them. Then the example in [9] will be discussed in detail.

Definition. An R-algebra A is an R-module together with a bilinear mapping from $A \times A$ into A defining a multiplication in A which is associative and has identity.

Definition. Let A and B be R-algebras; an algebra homomorphism from A into B is an R-module homomorphism $f : A \to B$ such that for each $x,y \in A$, $f(xy) = f(x)f(y)$ and $f(1_A) = 1_B$.

Let A be an R-algebra and K an ideal in A. The module $A/_K$ may be turned into an R-algebra by defining $\bar{a} \cdot \bar{b} = \overline{ab}$, $\forall a,b \in A$. The algebra $A/_K$ is commutative if and only if $\forall a,b$ A, $ab - ba \in K$.

Definition. A tensor algebra on an R-module M is an R-algebra T together with an R-module homomorphism $\psi : M \to T$ such that if A is any R-algebra and $\phi : M \to A$ is an R-module homomorphism, then there exists a unique R-algebra homomorphism $f : T \to A$ with $f \circ \psi = \phi$.

Given an R-module M, we may construct a tensor algebra on M as follows: let $T = \bigoplus_{n \geq 0} T_n$ where $T_o = R$, $T_1 = M$ and $T_n = M \otimes \ldots \otimes M$ is a tensor product of n copies of M over R, when $n > 1$. For each $n \geq 0$ and each $s \geq 0$, we define $\theta_{n,s} : T_n \underset{R}{\otimes} T_s \rightarrow T_{n+s}$ by

$\theta_{n,s}((m_1 \otimes \ldots \otimes m_n) \otimes (m_1' \otimes \ldots \otimes m_s')) =$

$= m_1 \otimes \ldots \otimes m_n \otimes m_1' \otimes \ldots \otimes m_s'$ and extend this definition by linearity to $T_n \underset{R}{\otimes} T_s$. Since $T \underset{R}{\otimes} T = \bigoplus_{n,s>0} T_n \underset{R}{\otimes} T_s$, there exists a linear mapping $\theta : T \underset{R}{\otimes} T \rightarrow T$ extending all the above $\theta_{n,s}$'s [3, pg. 70]. Thus, the mapping from $T \times T$ into T given by $(x,y) \mapsto x \otimes y$ defines a multiplication in T which is associative (for the tensor product is associative) with identity $1_T = 1_R$. Here $\psi : M \rightarrow T$ is defined by $m \mapsto (0,m,0,\ldots)$ $\forall m \in M$.

Any two tensor algebras on the same R-module are isomorpgic [3, pg. 151]. Hence, when we refer to a tensor algebra on the R-module M, we may take it to be the one constructed above.

Definition. A symmetric algebra S on an R-module M is a commutative R-algebra together with a linear mapping $\psi : M \rightarrow S$ such that if A is a commutative R-algebra and $\phi : M \rightarrow A$ is a linear mapping, then there exists a unique R-algebra homomorphism $f : S \rightarrow A$ with $f \circ \psi = \phi$. Such an algebra is denoted by (S,ψ).

Proposition VII.1. If (S,ψ) is a symmetric algebra on the R-module, M, $\psi(M)$ generates S as an R-algebra.

Proof. Let S' be the subalgebra of S generated by $\psi(M)$, i.e.

$$S' = \{x \in S \mid x = \sum_{i=1}^{n(x)} (r_i \prod_{j=1}^{m_i(x)} y_{i,j}) \; , \; r_i \in R, \; y_{i,j} \in \psi(M) \cup \{1_S\}\}.$$

Since $\psi(M) \subseteq S'$, we may define $\psi' : M \to S'$ by $\psi'(m) = (m) \; \forall m \in M$. Hence, if $i : S' \to S$ is the natural inclusion, we have $i \circ \psi' = \psi$. By the definition of (S,ψ), there exists a unique R-algebra homomorphism $f : S \to S'$ such that $f \circ \psi = \psi'$. Thus, $i \circ f \circ \psi = i \circ \psi' = \psi$. On the other hand, $I_S \circ \psi = \psi$. By the uniqueness of the R-algebra homomprphism $g : S \to S$ such that $g \circ \psi = \psi$, we conclude that $i \circ f = I_S$; i is therefore onto and $S' = S$.

Proposition VII.2. If (S,ψ) and (S',ψ') are symmetric algebras on the R-module M, there exists a unique algebra isomorphism $J : S \to S'$ such that $J \circ \psi = \psi'$.

Proof. By definition, there exists a unique algebra homomorphism $J : S \to S'$ such that $J \circ \psi = \psi'$, and there exists a unique algebra homomorphism $J' : S' \to S$ such that $J' \circ \psi' = \psi$. Then, $J' \circ J \circ \psi = J' \circ \psi' = \psi$., i.e., $J' \circ J : S \to S$ fits in the definition of symmetric algebra as does I_S. By the uniqueness of such an algebra homomorphism, $J' \circ J = I_S$. Similarly, $J \circ J' = I_{S'}$ and J is therefore an isomorphism.

Proposition VII.3. Given an R-module M, there exists a symmetric algebra on M.

Proof. Let (T,θ) be a tensor algebra on M and let K be the ideal generated in T by the elements of the form $\theta(x)\theta(y) - \theta(y)\theta(x)$; $x,y \in M$. The quotient algebra $S = T/_K$ is commutative and if we set $\psi = \pi \circ \theta$, where $\pi : T \to S$ is the natural algebra homomorphism, then (S,ψ) is a symmetric algebra on M. In fact, let A be a commutative R-algebra and

$\phi : M \to A$ a linear mapping. By the definition of tensor algebra, there exists a unique algebra homomorphism $g : T \to A$ such that $g \circ \theta = \phi$. We define $f : S \to A$ by $f(\bar{t}) = g(t)$; since A is commutative, $g(K) = 0$ and f is therefore well defined. It is clearly an algebra homomorphism and $f \circ \psi = f \circ \pi \circ \theta = g \circ \theta = \phi$.

Since $\psi(M)$ generates S as an R-algebra, any algebra homomprphism $f' : S \to A$, such that $f' \circ \psi =$ [illegible] coincides with f. Hence f is unique and (S,ψ) is therefore a symmetric algebra on M. q.e.d.

By the construction given for the tensor algebra (T,θ) on M, the linear mapping $\theta : M \to T$ is simply the inclusion of M into T. Hence, by $\theta(x)\theta(y)$ in the proof of proposition VII .3, we mean $x \otimes y$. And by taking the quotient $S = T/_K$ we are just assuring that in S, $x \otimes y = y \otimes x$. In other words, $S = \bigoplus_{n \geq 0} S_n$ where $S_0 = R$, $S_1 = M$ and S_n is the commutative tensor product of n copies of M. Here, again, $\psi : M \to S$ is the inclusion.

From now on, all algebras will be commutative algebras.

Let A and B be R-algebras and consider an R-module $A \underset{R}{\otimes} B$. The mapping from $A \times B \times A \times B$ into $A \underset{R}{\otimes} B$ defined by $(a,b,a',b') \mapsto aa' \otimes bb'$ is linear in each factor. Hence, the mapping $a \otimes b \otimes a' \otimes b' \mapsto aa' \otimes bb'$ is linear from $A \underset{R}{\otimes} B \underset{R}{\otimes} A \underset{R}{\otimes} B$ into $A \underset{R}{\otimes} B$. By the associativity of the tensor product of modules, we have a linear mapping from $(A \underset{R}{\otimes} B) \times (A \underset{R}{\otimes} B)$ into $A \underset{R}{\otimes} B$ given by $(a \otimes b, a' \otimes b') \mapsto aa' \otimes bb'$ which supplies $A \underset{R}{\otimes} B$ with a multiplication. This multiplication is associative and commutative for so are the multiplications in A and in B. Moreover, $(1_A \otimes 1_B , 1_A \otimes 1_B)$ maps on $1_A \otimes 1_B$, the identity element for the multiplication in $A \underset{R}{\otimes} B$. Thus, $A \underset{R}{\otimes} B$ is an algebra, called the tensor product of the algebras A and B.

Let M,N be R-modules and (S_M,ψ_M), (S_N,ψ_N) symmetric algebras on M,N respectively. If $\mu : M \to N$ is a linear mapping, so is $\psi_N \circ \mu : M \to S_N$. By the definition of symmetric algebra, there exists a unique algebra homomorphism $f : S_M \to S_N$ such that $f \circ \psi_M = \psi_N \circ \mu$. This unique homomorphism f is called the prolongation of μ to S_M.

We now prove some properties of symmetric algebras.

Proposition VII.4. [3, pg. 215] Let $M = N \oplus P$ be an R-module and consider the symmetric algebras (S_M,ψ_M), (S_N,ψ_N) and (S_P,ψ_P) on M,N and P respectively. Then, there exists a unique algebra isomorphism $f : S_M \to S_N \underset{R}{\otimes} S_P$ such that $f(\psi_M(y + z)) = \psi_N(y) \otimes 1 + 1 \otimes \psi_P(z)$, for each y in N and each z in P.

Proof. Since $M = N \oplus P$, we have linear mappings $\pi_N : M \to N$ and $\pi_P : M \to P$ such that for each x in M, $x = \pi_N(x) + \pi_P(x)$. The mapping $\rho : M \to S_N \underset{R}{\otimes} S_P$, defined by $\rho(x) = \psi_N(\pi_N(x)) \otimes 1 + 1 \otimes \psi_P(\pi_P(x))$ is linear, as a composite of linear mappings. Since $S_N \underset{R}{\otimes} S_P$ is an algebra, there exists a unique algebra homomorphism $f : S_M \to S_N \underset{R}{\otimes} S_P$ such that $f \circ \psi_M = \rho$. Hence, for each y in N and for each z in P, $f \circ \psi_M(y + z) = \psi_N(y) \otimes 1 + 1 \otimes \psi_P(z)$.

Let $J_N : S_N \to S_M$ and $J_P : S_P \to S_M$ be the prolongations of the inclusions $j_N \to M$ and $j_P : P \to M$; hence $J_N \circ \psi_N = \psi_M \circ j_N$ and $J_P \circ \psi_P + \psi_M \circ j_P$. The mapping $g : S_N \underset{R}{\otimes} S_P \to S_M$, defined by $g(t \otimes u) = J_N(t)J_P(u)$, extended to $S_N \underset{R}{\otimes} S_P$ linearly, is an algebra homomorphism; also, for each y in N and for each z in P, $g \circ f(\psi_M(y + z)) = g(f \circ \psi_M(y + z)) = g(\psi_N(y) \otimes 1) + g(1 \otimes \psi_P(z)) = J_N \circ \psi_N(y) + J_P \circ \psi_P(z) = \psi_M \circ j_N(y) + \psi_M \circ j_P(z) = \psi_M(y + z)$.

Hence, $g \circ f$ and I_{S_M} coincide on ψ_M, a set of generators for S_M. Thus $g \circ f = I_{S_M}$ and f is therefore a monomorphism.

Since $\psi_N(N)$ generates S_N and $u \mapsto u \otimes 1$ is an algebra homomorphism, the subalgebra $f(S_M)$ of $S_N \underset{R}{\otimes} S_P$ contains $S_N \otimes \{1\}$; similarly, it contains $\{1\} \otimes S_P$. Hence, it contains $(S_N \otimes \{1\}) \cup (\{1\} \otimes S_P)$ which is a set of generators for $S_N \underset{R}{\otimes} S_P$. We conclude that $f(S_M) = S_N \underset{R}{\otimes} S_P$ and that f is therefore an isomorphism.

Proposition VII.5. Let A be an R-algebra. Then the R-algebras $A \underset{R}{\otimes} R[x]$ and $A[x]$ are isomorphic.

Proof. Consider the R-algebra homomorphism $f : A \otimes R[x] \to A[x]$ defined by $f(a \otimes x^i) = ax^i$; f is obviously onto. To prove that f is a monomorphism, we define $g : A[x] \to A \otimes R[x]$ by $g(\sum a_i x^i) = \sum(a_i \otimes x^i)$, which is an R-algebra homomorphism; then, $g \circ f$ and $I_{A \otimes R[x]}$ coincide on $\{a \otimes x | a \in A\} \cup \{a \otimes 1 | a \in A\}$, a set of generators for $A \otimes R[x]$, and the proof is complete.

Proposition VII.6. Let $\psi : R \to R[x]$ be defined by $\psi(1) = x$. Then $(R[x],\psi)$ is a symmetric algebra on R.

Proof. Let A be an R-algebra and $\mu : R \to A$ a linear mapping. Define $f : R[x] \to A$ by $f(\sum r_i x^i) = \sum r_i \mu(1)^i$. We have then an R-algebra homomorphism and $f \circ \psi = \mu$. Any other R-algebra homomorphism g such that $g \circ \psi = \mu$ must coincide with f on $\{1,x\}$ which generates $R[x]$. Hence f is unique.

Proposition VII.7. Let $\psi : R^n \to R[x_1, \ldots, x_n]$ be defined by $\psi(e_i) = x_i$

where $e_i = (\delta_{ij})_{1 \leq j \leq n}$, $1 \leq i \leq n$. Then $(R[x_1, \ldots, x_n],\psi)$ is a symmetric algebra on R^n.

Proof. Let $\rho : R \to R[x_n]$ be defined by $\rho(1) = x_n$; by proposition VII.6, $(R[x_n],\psi)$ is a symmetric algebra on R. We continue by induction: suppose that $(R[x_1, \ldots, x_{n-1}],\sigma)$ is a symmetric algebra on R^{n-1}, $\sigma : R^{n-1} \to R[x_1, \ldots, x_n]$ being defined by $\sigma(e'_i) = x_i$, $e'_i = (\delta_{ij})_{1 \leq j \leq n-1}$, $1 \leq i \leq n - 1$.

Let (S,ϕ) be a symmetric algebra on R^n; by proposition VII.4, there exists a unique algebra isomorphism $f : S \to R[x_1, \ldots, x_{n-1}] \otimes R[x_n]$ such that for each $(r_i)_{1 \leq i \leq n} \in R^n$, $f \circ \phi(r_1, \ldots, r_n) = \sigma(r_1, \ldots, r_{n-1}) \otimes 1 + 1 \otimes \rho(r_n) = (r_1x_1 + \ldots + r_{n-1}x_{n-1}) \otimes 1 + 1 \otimes r_nx_n$. Let $g : R[x_1, \ldots, x_{n-1}] \otimes R[x_n] \to R[x_1, \ldots, x_n]$ be the isomorphism defined in the proof of proposition VII.4. Then $g \circ f \circ \phi = \psi$, i.e., the unique algebra isomorphism $h : S \to R[x_1, \ldots, x_n]$ such that $h \circ \phi = \psi$ is the isomorphism $g \circ f$. Hence, $(R[x_1, \ldots, x_n],\psi)$ is a symmetric algebra on R^n.

Definition. An R-algebra A is regularly graded if it has submodules A_i, i being a natural number, such that $A = \bigoplus_{n=0}^{\infty} A_i$, A_o is a subalgebra isomorphic to R and if $a_i \in A_i$, $a_j \in A_j$, then $a_ia_j \in A_{i+j}$ $\forall i,j \geq 0$.

Let $A = \bigoplus_{i=0}^{\infty} A_i$ be a regularly graded algebra. The elements of the submodule A_i are called the homogeneous elements of A of degree i. Hence, every element of A is the sum of its homogeneous components. If a regularly graded R-algebra is generated over R by a subset $S \subseteq A$, then the submodule A_1 is generated over R by the homogeneous components of degree 1 of the elements of S.

By their constructions, we see that the tensor algebra and the symmetric algebra on an R-module M are regularly graded algebras.

At this point, we turn our attention to formally real domains.

Definition. A ring is a formally real domain if for each $n > 0$ and every $a_i \in R$, $\sum_{i=1}^{n} a_i^2 = 0$ implies $a_i = 0 \ \forall i$.

Lemma VII.8. If R is a formally real domain, so is R[x].

Proof. Let $\sum_{i=1}^{n} f_i^2 = 0$ with $f_i \in R[x]$ for each i. Consider the highest power $m \geq 0$ of x appearing in the f_i's. Then, $\sum_{i=1}^{n} f_{i,m}^2 = 0$, where $f_{i,m}$ is the coefficient of x^m in f_i. Since R is a formally real domain, $f_{i,m} = 0 \ \forall i$ and $\forall m \geq 0$. Hence, $f_i = 0$ for each i.

Lemma VII.9. Let R be a formally real domain. Then the solutions of $t_1^2 + t_2^2 + \ldots + t_n^2 = 1$ in R[x] lie in R.

Proof. Let $f_i = \sum_j f_{i,j}x^j \in R[x]$ and suppose that $\sum_{i=1}^{n} f_i^2 = 1$. If $m \geq 1$ is the highest power of x in the f_i's, we have $\sum_{i=1}^{n} f_{i,m}^2 = 0$; since R is a formally real domain, $f_{i,m} = 0$ for each i. Hence, $m = 0$ and the f_i's lie in R.

Lemma VII.10. The only ring automorphism of the ring of real numbers R is the identity map.

Proof. Let α be a ring automorphism of R; since $\alpha(1) = 1$, it follows that $\alpha(q) = q$ for all rational numbers q.

If $r > 0$, also $\alpha(r) > 0$. To see this, we take b in R such that $b^2 = r$; then, $\alpha(r) = \alpha(b^2) = \alpha(b)^2 > 0$.

Now assume that $s \in R$ is such that $\alpha(s) \neq s$. Take any rational number q between s and $\alpha(s)$, e.g. $s < q < \alpha(s)$. From $0 < q - s$ we obtain $0 < \alpha(q - s)$ and consequently $\alpha(s) < \alpha(q) = q$, contradicting the fact that $s < q < \alpha(s)$. q.e.d.

We are now ready to discuss the example given by M. Hochster in [9]. In what follows, R is the ring of real numbers and P, Q, t, U, V, W, X, Y and Z are indeterminates.

The ideal I generated in $R[X,Y,Z]$ by the polynomial $X^2 + Y^2 + Z^2 = 1$ is prime because this polynomial is irreducible in $R[X,Y,Z]$. It follows that the ring $A = R[X,Y,Z]/_I$ is an integral domain and is generated over R by the elements $x = \bar{X}$, $y = \bar{Y}$ and $z = \bar{Z}$ which satisfy $x^2 + y^2 + z^2 = 1$. Hence, for each $f(x,y,z)$ in A there exists $g(X,Y,Z)$ in $R[X,Y,Z]$ linear in Z, such that $g(x,y,z) = f(x,y,z)$.

Lemma VII.11. $A^* = R^*$.

Proof. Since R may be embedded in the ring A, $R^* \subseteq A^*$. Let $\bar{a} + \bar{b}z \in A^*$, $a,b \in R[X,Y]$; then there exist c,d in $R[X,Y]$ such that $(\bar{a} + \bar{b}z)(\bar{c} + \bar{d}z) = 1$. Let $K = X^2 + Y^2 - 1$. Then, $(a + bZ)(c + dZ) = 1 + h(Z)(K + Z^2)$ where $h \in R[X,Y]$. The polynomial in Z on the left-hand side has degree ≤ 2. Hence, $h(Z) \in R[X,Y]$ and $h(Z) = bd$. We may rewrite the equation above as $ac + (ad + bc)Z + bdZ^2 = 1 + bdK + bdZ^2$. Hence:

(1) $ac - bdK = 1$

(2) $ad + bc = 0$.

If we multiply (1) by d, (2) by $-c$ and add up the resulting equations, we obtain $-b(c^2 + d^2K) = d$, i.e., $b|d$. Similarly, $d|b$. Hence, there exists u in $R[X,Y]^* = R^*$ such that $d = ub$. From (2) we obtain $c = -ua$ and then, we may rewrite (1) as $a^2 + b^2K = -u^{-1}$ or $a^2 + b^2(X^2 + Y^2 - 1) = - u^{-1}$. Let a_m, b_n be the leading coefficients in $(R[X])[Y]$ of a,b respectively. Then, $a_m^2 + b_n^2 = 0$. Since R is a formally real domain, by lemma VII.8, R[X] is a formally real domain; hence, $a_m = b_n = 0$ for all $n \geq 0$. Then, $b = 0$ and $d = ub = 0$. From (1) we obtain $ac = 1$. Since $R[X,Y]^* = R^*$, we conclude that $A^* \subseteq R^*$.

<u>Lemma VII.12.</u> A is a formally real domain.

<u>Proof.</u> Let $\sum_{i=1}^{n} (a_i(x,y) + b_i(x,y)z)^2 = 0$. Then, $\sum_{i=1}^{n} (a_i(X,Y) + b_i(X,Y)Z)^2 = h(X^2 + Y^2 + Z^2 - 1)$ where $h \in R[X,Y]$, as in the proof of lemma VII.11. Consequently,

$\sum_{i=1}^{n} a_i^2 = h(X^2 + Y^2 - 1)$, $2 \sum_{i=1}^{n} a_ib_i = 0$ and $\sum_{i=1}^{n} b_i^2 = h$. Thus,

$$(3) \quad \sum_{i=1}^{n} a_i^2 + \sum_{i=1}^{n} b_i^2 = \sum_{i=1}^{n} b_i^2X^2 + \sum_{i=1}^{n} b_i^2Y^2.$$

Consider the terms of the a_i's and b_i's which are in R. The sum of their squares in zero. Hence, no a_i and b_i has any term in R^*. Next, consider all the terms in the a_i's and b_i's which are in R[X]. Let j be the maximum power of X which divides all those terms (thus, $j \geq 1$). From (3) we have

$$X^{2j}(\sum c_i^2 + \sum d_i^2) + F(X,Y) = X^{2j}(\sum d_i^2X^2 + \sum d_i^2Y^2) + G(X,Y)$$

where each c_i and each d_i is in R[X], all the terms in F and G depend on Y and for some i at least one of the c_i's and d_i's has a term in R^*. The sum of the squares of these terms in R^* being zero, we conclude that the a_i's and b_i's have no nonzero terms in R[X]. Symmetrically, they have no nonzero terms in R[Y]. Hence, all terms in the a_i's and b_i's depend on XY. Let j,k be the greatest power of X,Y, respectively, common to all terms. We have from (3) :

$X^{2j}Y^{2k}(\sum c_i^2 + \sum d_i^2) = X^{2j}Y^{2k}(\sum d_i^2X^2 + \sum d_i^2Y^2)$; hence,

$\sum c_i^2 + \sum d_i^2 = \sum d_i^2X^2 + \sum d_i^2Y^2$; This equation being the same as (3), we conclude that all terms in the c_i's and d_i's depend on XY, contradicting our choice of the numbers j and k. Hence, each a_i and each b_i must be zero.

Definition. A ring S is invariant if for each ring S' the isomorphism $S[X] \simeq S'[X]$ implies $S \simeq S'$.

Theorem VII.13. Consider the linear mappings $\phi : A^3 \to A$, defined by $\phi(a,b,c) = ax + by + cz$, and $\psi : A \to A^3$, defined by $\psi(a) = a(x,y,z)$. Since $\phi \circ \psi = I_A$, we have $A^3 \simeq E \oplus A$ where $E = \ker \phi$ is an A-module of rank 2. E is not free, otherwise we would be able to construct a continuous field of unit vectors over S^2, a contradiction to theorem 5.8.6 in [8, pg. 219]. In fact, suppose E is free. Let $\{(a_{11},a_{12},a_{13}) , (a_{21},a_{22},a_{23})\}$ be a basis for E. Then $\{(a_{11},a_{12},a_{13}) , (a_{21},a_{22},a_{23}) , (x,y,z)\}$ is a basis for A^3 and the matrix:

$$M(x,y,z) = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ x & y & z \end{pmatrix} \quad \text{where} \quad a_{ij} = a_{ij}(x,y,z) \text{ corresponds}$$

to an automorphism of A^3. It's determinant, being invertible in A, is a nonzero real number, by lemma VII.11. Hence, $F(x,y,z) = |M(x,y,z)| - r = 0$. Since (x,y,z) is a typical point of S^2, $F(a,b,c) = 0$ for each $(a,b,c) \in S^2$.

Let us now consider the function $\gamma : S^2 \to R^3$ defined by

$\gamma(a,b,c) = (a,b,c) \times (a_{21}(a,b,c), a_{22}(a,b,c), a_{23}(a,b,c))$, the vector product of two vectors in R^3. If we develop the determinant above by its first row, we see that $\gamma(a,b,c) = 0$ implies $|M(a,b,c)| = 0$ and we know that $|M(a,b,c)| = r \neq 0$. Hence, $\gamma(a,b,c) \neq 0$. As a composite of continuous functions, γ is continuous. Moreover, $\gamma(a,b,c) \cdot (a,b,c) \equiv 0$. Hence $\gamma/||\gamma||$ is a continuous field of unit vectors over S^2.

Let $S(A^3)$, $S(E)$ and $S(A)$ be symmetric algebras on the A-modules A^3, E and A, respectively. By proposition VII,4, $S(A^3) \simeq S(E) \otimes S(A)$; by proposition VII.7, $S(A^3) \simeq A[P,Q,t]$ and $S(A) \simeq A[t]$. Hence, $A[P,Q][t] \simeq A[P,Q,t] \simeq S(A^3) \simeq S(E) \otimes S(A) \simeq S(E) \otimes A[t] \simeq S(E)[t]$.

Now, we show that the rings $A[P,Q]$ and $S(E)$ are not isomorphic. Suppose there exists a ring isomorphism $h : A[P,Q] \rightarrow S(E)$; then $h(A[P,Q]^*) = S(E)^*$. Since A is an integral domain, $A[P,Q]^* = A^*$ and then, by lemma VII.11, $A[P,Q]^* = R^*$; since $S(E)^*$ is a subalgebra of $A[P,Q,t]$ containing R, we have $R^* \subseteq S(E)^* \subseteq A[P.Q,t]^* = R^*$. Thus, $h|_R(R) = R$, i.e. h restricts to a ring automorphism of R. The only ring automorphism of R is the identity (cf. lemma VII.10), This shows that h is an R-isomorphism.

Moreover, since by lemma VII.12, A is a formally real domain, the solutions of the equations $h(x)^2 + h(y)^2 + h(z)^2 = 1$ and $h^{-1}(x)^2 + h^{-1}(y)^2 + h^{-1}(z)^2 = 1$ in $A[P,Q,t]$ lie in A, according to lemmas VII.9 and VII.8; hence, the solutions of the former equation in S(E) lie in A and the solutions of the latter one in A[P,Q] also lie in A. Thus, $h(A) \subseteq A$ and $h^{-1}(A) \subseteq A$.

We now define $g : A[P,Q] \rightarrow S(E)$ by $g(\sum a_{ij}P^iQ^j) = h(\sum h^{-1}(a_{ij})P^iQ^j) = \sum a_{ij}h(P)^ih(Q)^j$. We have here an A-isomorphism of A[P,Q] and S(E).

Consequently, S(E) is generated over A by the two elements $g(P) = c_o + c_1 + \ldots$ and $g(Q) = c'_o + c'_1 + \ldots$ where the index i indicate the homogeneous component of degree i, as S(E) is a regularly graded algebra. The submodule of S(E) formed by the homogeneous elements of degree 1 is isomorphic to E and is generated over R by $\{c_1, c'_1\}$, according to the remark after proposition VII.7. But E requires three generators because it has rank two and is not free. Hence, A[P,Q] and S(E) cannot be isomorphic, which completes the proof of theorem VII.13.

REFERENCES

1. S.A.Amitsur, Radicals of polynomial rings, Canad.J.Math.8 (1956), 355-361.
2. J.-B.Castillon, Polynomes tordues-Etude d'une classe d'anneaux locaux non commutatifs, Notas e Comunicacoes de Matematica-Universidade Federal de Pernambuco, 55 (1973).
3. C.Chevalley, Fundamental concepts of algebra, Academic Press Inc. (1956).
4. D.B.Coleman and E.E.Enochs, Isomorphic polynomial rings, Proc. Amer. Math. Soc. 2 (1971), 247-252.
5. P. M. Cohn, Free rings and their relations, Academic Press (1971).
6. R.W.Gilmer Jr., If R[x] is Noetherian, R contains an identity, Amer. Math. Monthly 74 (1967), 700.
7. R.W.Gilmer Jr., R-automorphisms of R[x], Proc. London Math. Soc. (3) 18 (1968), 328-336.
8. P.J.Hilton and S.Wylie, Homology Theory, Cambridge University Press (1960).
9. M.Hochster, Nonuniqueness of coefficient rings in a polynomial ring, Proc. Amer. Math. Soc. 34 (1972), 81-82.
10. J.Krempa, On radical properties of polynomial rings, Bulletin de l' Academie Polonaise des Sciences, XX, 7 (1972), 545-548.
11. J.Lambek, Lectures on rings and modules, Blaisdell Publishing Co. (1966).
12. O.Ore, Theory of noncommutative polynomials, Ann. Math. 34 (1933), 480-508.

13. P.Ribenboim, Rings and modules, Interscience Publishers (1969).

14. W.R.Scott, Divisors of zero in polinomial rings, Amer. Math. Monthly 61 (1954), 336.

15. E.Snapper, Completely p-imary rings, I, Annals of Math. 52 (1950), 666-693.

16. B.L.van der Waerden, Modern algebra, vol.I, Frederick Ungar Publishing Co. (1953).