JOURNAL OF ALGEBRA 56, 315–342 (1979)

Prime Ideals of Ore Extensions over Commutative Rings

RONALD S. IRVING

Department of Mathematics, Brandeis University, Waltham, Massachusetts 02154

Communicated by D. Buchsbaum

Received January 13, 1978

1. INTRODUCTION

In this paper, we study the prime ideal structure of a class of non-commutative polynomial rings, called Ore extensions or twisted polynomial rings. Let φ be an endomorphism of the ring R. We define a new ring $A = R[x; \varphi]$, whose underlying additive group coincides with that of $R[x]$. Multiplication is determined by the distributive law and the rule

$$rx = x\varphi(r),$$

for all r in R. We call A the Ore extension of R with respect to φ. Observe that in the normal form for an element of A as a polynomial over R, the coefficients appear on the right side.

In 1933, Ore considered these rings in the case that R is a division ring [9]. Shortly thereafter, Jacobson determined the two-sided ideals of such rings, and analyzed finitely-generated modules over them [6]. Little work appeared on Ore extensions for some time after that. In 1952, Curtis proved that A is an Ore domain if R is and φ is injective [1, 4]. But otherwise such rings were used primarily as a source of counter-examples.

More recently, results have appeared which, in a sense, are generalizations of Hilbert's Nullstellensatz. One form of the Nullstellensatz, due to Krull and Goldman, states that a commutative ring R is a Jacobson ring if and only if $R[x]$ is, [3, 8]. In fact, Watters has proved that the assumption of commutativity is unnecessary [11]. Goldie and Michler have proved that for a noetherian ring R with automorphism φ, the associated Ore extension $A = R[x; \varphi]$ is Jacobson if and only if R is. Their proof rests on a study of the ideal structure of A. The assumption that R is noetherian is necessary, as an example of Stephenson and Pearson shows [10].

In this paper we study Ore extensions $A = R[x; \varphi]$, where R is a commutative ring and φ is an endomorphism. We show in Sections 3–5 that the prime ideals of A can be completely described in terms of certain ideals of R. In case R is

0021-8693/79/020315–28$02.00/0

noetherian, these ideals of R take on a satisfying form. In Section 6, we prove a theorem on the preservation of Goldie rank for A, which leads to the result that, for noetherian rings R, the prime factor rings of A are all Goldie. We study the Jacobson radical in Section 7, and prove that for R noetherian, the ring A is Jacobson if and only if R is. Then we turn to a family of examples, obtained by letting $R = k[y]$, and reinterpret our results for these rings. We classify all the finite-dimensional irreducible representations, and then consider the question of whether infinite-dimensional irreducible representations exist.

Many of the results of this paper form a part of my doctoral dissertation, submitted to the Massachusetts Institute of Technology [5]. I would like to thank Michael Artin, my thesis supervisor, for his sound advice and encouragement.

2. Preliminary Results

The Hilbert Basis Theorem states that a polynomial extension of a noetherian ring is noetherian, but the corresponding result for Ore extensions is not true. Let us review what positive results remain. Let φ be an endomorphism of an arbitrary ring R, with $A = R[x; \varphi]$ the associated Ore extension. The ring A can be viewed as a $(\mathbb{Z}[x], R)$-bimodule, with $\mathbb{Z}[x]$ acting on the left and R acting on the right. We say a bimodule is noetherian if the ascending chain condition holds for sub-bimodules, or equivalently, if every sub-bimodule is finitely generated.

Proposition 2.1. *Let R be right noetherian. Then A is noetherian as a $(\mathbb{Z}[x], R)$-bimodule.*

Proof. This is proved by an adaptation of the standard proof of the Hilbert Basis Theorem. Given a sub-bimodule I of A, we let $\mathbf{b}$ be the set of leading coefficients in R of polynomials in I. Then $\mathbf{b}$ is closed under addition because $xI \subset I$, so $\mathbf{b}$ is a right ideal of R. The proof now continues in the usual way.

Corollary 2.2. *Let R be right noetherian. Then A satisfies the ascending chain condition on (two-sided) ideals. Hence every semiprime ideal of A is a finite intersection of prime ideals, and every ideal has finitely many primes minimal over it.*

Proposition 2.3. *Let φ be an automorphism of the right noetherian ring R. Then the Ore extension A is right noetherian.*

Proof. We modify the proof sketched in 2.1 slightly. The surjectivity of φ implies that any element of A can be written as $\sum r_i x^i$, with the coefficients on the left. Adopting this as our normal form, we let $\mathbf{b}$ be the set of leading coefficients in R of a right ideal I. Because φ is surjective, the set $\mathbf{b}$ is a right ideal of R, and we continue as usual.

Let us record the classical theorems of Jacobson for R a field, as a source of comparison with the more general results to follow. The proofs may be found in [6].

THEOREM 2.4. *Let φ be an infinite order endomorphism of the field K. Then the ideals of $A = K[x; \varphi]$ are* (0) *and x^i, $i = 0, 1, 2,\ldots$ The only prime ideals are* (0) *and* (x), *and these are primitive.*

THEOREM 2.5. *Let φ be an automorphism of K with finite order n, and let k be the fixed field of φ. Then the ideals of A are generated by $x^i p(x^n)$, where p is a polynomial with coefficients in k.*

3. φ-INVARIANT IDEALS OF COMMUTATIVE RINGS

In this section we introduce some terminology and prove several basic facts which are essential for the main theorems of the next section. Let R be a commutative ring with endomorphism φ, and call an ideal I of R *φ-invariant* if $\varphi^{-1}(I) = I$.

LEMMA 3.1. *If I is φ-invariant, so is* $\operatorname{rad}(I)$.

Proof. Let r be in $\operatorname{rad}(I)$ and $r^m \in I$. Then I contains $\varphi(r^m)$, or $(\varphi(r))^m$. Hence $\varphi(r) \in \operatorname{rad}(I)$. Conversely, given $\varphi(r) \in I$, we can reverse the argument.

DEFINITION. (i) A φ-invariant ideal I is *φ-prime* if, given two ideals J and K such that $\varphi(J) \subset J$ and $JK \subset I$, either $J \subset I$ or $K \subset I$.

(ii) A φ-invariant ideal I is φ-semiprime if, given an ideal J such that $\varphi(J) \subset J$ and $J^2 \subset I$, then $J \subset I$. These notions can be re-expressed in terms of elements as follows:

LEMMA 3.2. (i) *The φ-invariant ideal I is φ-prime if and only if for any two elements r and s and integer n such that $\varphi^i(r)s \in I$ for all $i \geqslant n$, either r or s lies in I.*

(ii) *The φ-invariant ideal I is φ-semiprime if, for any element r and integer n such that $\varphi^i(r)r \in I$ for all $i \geqslant n$, the element r is in I.*

Proof. We will only prove (i). Suppose that I is φ-prime. Let J be the ideal generated by $\varphi^i(s)$ for $i \geqslant n$ and $K = sR$. Then $JK \subset I$ and $\varphi(J) \subset J$, so we can deduce that $\varphi^n(r)$ or s lies in I. By φ-invariance of I, the element $\varphi^n(r)$ is in I if and only if $r \in I$.

Conversely, if $K \not\subset I$, choose an element $s \in K - I$. For any $r \in J$, since

$\varphi(J) \subset J$, we have $\varphi^i(r) \in J$. Hence, $\varphi^i(r)s \in JK \subset I$, and we conclude that $r \in I$, so $J \subset I$.

It is obviously difficult to recognize φ-prime ideals. But fortunately there is a subclass which can be more easily described, and which yields all φ-prime ideals in case R is noetherian or φ has finite order.

DEFINITION. (i) An ideal $I \subset R$ is *φ-cyclic* if $I = p_1 \cap \cdots \cap p_n$, where the p_i are distinct prime ideals of R such that

$$\varphi^{-1}(p_{i+1}) = p_i \qquad \text{and} \qquad \varphi^{-1}(p_1) = p_n .$$

(ii) I is *φ-semicyclic* if $I = p_1 \cap \cdots \cap p_n$ and the operator φ^{-1} permutes these associated primes.

It is obvious that φ-(semi) cyclic ideals are φ-(semi) prime, and we can prove the converse in the following situation:

PROPOSITION 3.3. *Let I be a φ-(semi) prime ideal, and assume that I contains $\sqrt{I}^m$ for some m, and $\sqrt{I}$ has finitely many associated primes. Then I is φ-(semi) cyclic.*

Proof. Let I be φ-semiprime. By Lemma 3.1, $\sqrt{I}$ is φ-invariant, and so I must equal $\sqrt{I}$. By assumption, I has a reduced primary decomposition $p_1 \cap \cdots \cap p_m$. But I is φ-invariant, so

$$I = \bigcap_{i=1}^{m} \varphi^{-1}(p_i).$$

By the uniqueness of reduced primary decomposition, the set $\{\varphi^{-1}(p_i)\}$ must be a permutation of the set $\{p_i\}$, and I is φ-semicyclic.

Now assume that I is φ-prime. We must prove that the permutation φ^{-1} induces on the p_i is cyclic. Assume the primes are ordered so that $p_1, \ldots, p_r$ are cyclically permuted, and let

$$J = p_1 \cap \cdots \cap p_r$$
$$K = p_{r+1} \cap \cdots \cap p_m .$$

Then $JK \subset I$ and $\varphi(J) \subset J$. Since I is φ-prime, either $I = J$ or $I = K$. The second possibility yields a shorter reduced primary decomposition, which is impossible. Hence $I = J$ and the permutation is cyclic.

COROLLARY 3.4. *If R is noetherian, or has Krull dimension in the sense of Gabriel and Rentschler, then φ-(semi) cyclic and φ-(semi) prime ideals are the same.*

Even without restriction on R, certain φ-prime ideals must be φ-cyclic.

PROPOSITION 3.5. *Let I be a φ-prime ideal of R such that φ induces a finite order automorphism on R/I. Then I is φ-cyclic.*

Proof. We may as well set $I = 0$, and assume that $\varphi^n =$ identity on R. We first make a couple of elementary observations.

(i) If φ fixes a non-zero element r, then r must be regular.

Suppose $rs = 0$, then $\varphi^i(r) = r$ implies that $\varphi^i(r)s = 0$, for all i; but (0) is φ-prime, so $s = 0$.

(ii) If r is a zero-divisor, then $\prod_{i=1}^{n} \varphi^i(r) = 0$, for the product is fixed by φ, and is not regular.

The zero divisors of R are a union of prime ideals. Let p be one of them. Since φ is an automorphism, $\varphi^i(p)$ is also a prime consisting of zero-divisors. We wish to prove that

$$(0) = p \cap \varphi(p) \cap \cdots \cap \varphi^{n-1}(p).$$

Let s be an element of this intersection, and let S be the subring of R generated over $\mathbb{Z}$ by $s, \varphi(s),..., \varphi^{n-1}(s)$. Then S is closed under the action of φ, and is noetherian. Moreover, (0) must be a φ-prime ideal of S, as is easily seen using the element definition. Therefore, by 3.4, the ideal (0) is φ-cyclic in S. There exist prime ideals $q_1 ,..., q_m$ in S such that $(0) = \bigcap q_i$ and $\varphi(q_i) = q_{i+1}$, with $m \mid n$.

By (ii), any element of S which is a zero-divisor in R must be a zero-divisor in S as well. Hence the ideal $p \cap S$, consisting of zero-divisors, lies in $\bigcup q_i$. Since $p \cap S$ is prime, it must actually lie in q_j, for some j. Then

$$\varphi^i(p) \cap S \subset q_{j+i},$$

where the indices are taken modulo m, and

$$S \cap p \cap \cdots \cap \varphi^{n-1}(p) \subset \cap\, q_i = (0).$$

But $s \in S \cap p \cap \cdots \cap \varphi^{n-1}(p)$, and so $s = 0$. The element s is arbitrary, so

$$(0) = p \cap \cdots \cap \varphi^{n-1}(p).$$

It follows that (0) is φ-cyclic in R.

Remark. It is not true in general that a φ-prime ideal must be φ-cyclic. A counter-example is provided by a theorem of Pearson and Stephenson [10], which we shall mention at the end of Section 7.

4. Main Results

We can now state the main results on prime ideals of Ore extensions. Let φ be an endomorphism of the commutative ring R, and let $A = R[x; \varphi]$. Notice that a prime ideal of A which contains x can be viewed as an ideal of R, and so is in a sense known. We therefore concern ourselves with primes not containing x.

Theorem 4.1. *Let I be a semiprime ideal of A, none of whose minimal primes contains x. Then $I \cap R = \mathbf{b}$ is a φ-semiprime ideal of R. If I is prime, then $\mathbf{b}$ is a φ-prime ideal of R.*

Theorem 4.2. *Conversely, let $\mathbf{b}$ be a φ-semiprime ideal of R. Then $A\mathbf{b}A$ is a semiprime ideal of A. Moreover, if $\mathbf{b}$ is φ-prime, then $A\mathbf{b}A$ is prime.*

Thus, to analyze the prime ideals of A, it suffices to determine the primes of A lying over a fixed φ-prime ideal $\mathbf{b}$ of R. We may as well assume $\mathbf{b} = (0)$, and ask which primes of A intersect R in (0). There are two possibilities.

Theorem 4.3. *Let φ be an infinite order endomorphism of the φ-prime ring R. Then the only prime of A, not containing x, which lies over* (0) *in R is* (0).

Theorem 4.4. *Let R be a φ-prime ring and let φ be an automorphism of finite order n (so that R is actually φ-cyclic). Let Q denote the fixed subring R^{φ}. Then $Q[x^n]$ is the center of A. The primes of A which do not contain x and lie over* (0) *are in one-to-one correspondence with the primes of $Q[x^n]$ that do not contain x^n and intersect Q in* (0).

We will prove the last theorem in the next section, but can now directly prove the first three theorems.

Proof of 4.1. Assuming first that I is semiprime, let us show that $\mathbf{b}$ is φ-invariant. If r is in $\mathbf{b}$, then $rx = x\varphi(r)$ is in I. Thus $x\varphi(r)$ is in each of the primes J minimal over I. It follows that $xA\varphi(r)$ lies in J. To see this, let $s = \sum_i x^i s_i$ be an element of A. Then

$$xs\varphi(r) = \sum x^i(x\varphi(r))s_i ,$$

which is an element of J. Since J is prime and $x \notin J$, we find that $\varphi(r) \in J$. Therefore $\varphi(r) \in I$. Conversely, if $\varphi(r) \in I$, then $x\varphi(r) = rx \in I$. So $rAx \subset I \subset J$, which implies that $r \in J$, for every minimal prime J. Hence $r \in I$.

To check that $\mathbf{b}$ is φ-semiprime, suppose $\mathbf{c}$ is an ideal for which $\varphi(\mathbf{c}) \subset \mathbf{c}$ and $\mathbf{c}^2 \subset \mathbf{b}$. Then $\mathbf{c}x \subset x\mathbf{c}$, and more generally, $\mathbf{c}A \subset A\mathbf{c}$. As a result,

$$(A\mathbf{c}A)^2 \subset A\mathbf{c}^2 \subset A\mathbf{b} \subset I.$$

Since I is semiprime, $A\mathbf{c}A \subset I$ and $\mathbf{c} \subset \mathbf{b}$.

If I is prime, a similar argument applies. Suppose $\mathbf{cd} \subset \mathbf{b}$ and $\varphi(\mathbf{c}) \subset \mathbf{c}$. Then

$$(A\mathbf{c}A)(A\mathbf{d}A) \subset A\mathbf{cd}A \subset A\mathbf{b}A \subset I.$$

Since I is prime, either $\mathbf{c}$ or $\mathbf{d}$ must lie in $I \cap R = \mathbf{b}$.

Proof of 4.2. We may as well set $\mathbf{b} = (0)$ and assume that R is φ-semiprime. What we must show is that A is semiprime. Let I be a non-zero ideal of A such that $I^2 = (0)$. Choose $s = \sum_{i=0}^{n} x^i s_i$ in I and assume that $s_n \neq 0$. For any integer $j \geqslant 0$, $sx^j s = 0$. The highest degree term of this expression is

$$x^n s_n x^j x^n s_n = x^{2n+j} \varphi^{n+j}(s_n) s_n .$$

Therefore the coefficient $\varphi^{n+j}(s_n)s_n = 0$ for all j. The element criterion for (0) to be φ-semiprime implies that $s_n = 0$, a contradiction.

Now assume R is φ-prime. We want to show A is prime, so assume J and K are ideals whose product is (0), and $K \neq (0)$. Let $s = \sum_{i=0}^{n} x^i s_i$ be an element of K with $s_n \neq 0$ and let $r = \sum_{i=0}^{m} x^i r_i$ be an element of J. Since $JK = (0)$, the product $rx^j s = 0$ for any integer $j \geqslant 0$. The highest degree term of this expression is

$$x^{m+n+j} \varphi^{n+j}(r_m) s_n .$$

Therefore the coefficient $\varphi^{n+j}(r_m)s_n = 0$ for all j. The element criterion for (0) to be φ-prime now implies that $r_m = 0$. Hence $r = 0$ and $J = (0)$.

Proof of 4.3. Let I be a non-zero prime of A and assume $x \notin I$. We must show that $I \cap R$ is non-zero. Let $r = \sum_{i=0}^{m} x^i r_i$ be a non-zero element of I of minimal degree, with $r_m \neq 0$. If $m = 0$, then I contains r_m and the intersection is non-zero, so assume $m > 0$. Since φ has infinite order and is injective, there exists an element $s \in R$ such that $\varphi^i(s) \neq \varphi^m(s)$ for $i < m$. Otherwise we find that φ must have finite order $\leqslant m!$. The ideal I contains

$$\varphi^j(s) r - r\varphi^{m+j}(s),$$

which equals

$$\sum_{i=0}^{m} x^i r_i (\varphi^{i+j}(s) - \varphi^{m+j}(s)).$$

This is an element of lower degree than r, so it must equal 0. Therefore, $r_i(\varphi^{i+j}(s) - \varphi^{m+j}(s)) = 0$ for arbitrary $j \geqslant 0$ and each $i < m$. Since (0) is φ-prime and $\varphi^i(s) \neq \varphi^m(s)$, we deduce that $r_i = 0$ for all $i < m$.

Consequently, $r = x^m r_m$, but $x \notin I$ and $x^m A r_m \subset I$. We can conclude that $r_m \in I$, because I is prime.

5. Proof of Theorem 4.4.

We shall use a result on the behavior of prime ideals under central localization which is similar to the result of commutative theory. Let A be a ring with center

C and let $S \subset C$ be a multiplicatively closed subset. Then we can form the localization $S^{-1}A$ in the usual way. Any prime of $S^{-1}A$ restricts to a prime of A, and it is straightforward to prove

PROPOSITION 5.1. *The map* $\operatorname{Spec} S^{-1}A \to \operatorname{Spec} A$ *induced by restriction is injective, and the image is the set of primes of A which intersect S in the empty set.*

We will apply this theorem to algebras A which are finite as modules over their centers, in order to obtain localizations whose prime spectra omit ideals that are not of interest. The resulting localizations will turn out to be Azumaya algebra, whose centers are explicitly described. Thus we can picture the interesting primes of A as the restrictions of primes in an Azumaya algebra, which are merely the extended ideals of the primes in the center. (We recall the fact that the ideals of an Azumaya algebra are in $1-1$ correspondence with the ideals of its center, under extension and restriction [7].)

As an example, let $R = \prod_i K_i$ be a product of n copies of an algebraically closed field K. Define φ to be the automorphism of order n which maps

$$(a_1, ..., a_n) \mapsto (a_2, a_3, ..., a_1),$$

and let A be the Ore extension $R[x; \varphi]$. The fixed ring R^φ is the set of elements $(a, ..., a)$, which is isomorphic to K, so the center of A is $K[x^n]$.

Any prime ideal I of A that contains x^n also contains xAx^{n-1}, which implies that $x \in I$. Moreover, the primes of A which contain x correspond to the n primes of R. In order to focus on the remaining primes, we can invert x^n. Explicitly, let S be the multiplicatively closed set in $K[x^n]$ generated by x^n, and pass to

$$S^{-1}A = K[x^n, x^{-n}] \otimes_{K[x^n]} A.$$

PROPOSITION 5.2. *The algebra $S^{-1}A$ is an Azumaya algebra over its center,* $K[x^n, x^{-n}]$.

Proof. By a standard result on Azumaya algebras [7], it suffices to prove that for each maximal ideal $\mathbf{m}$ of $K[x^n, x^{-n}]$, the algebra $S^{-1}A/\mathbf{m}S^{-1}A$ is an Axumaya algebra. The maximal ideals of $K[x^n, x^{-n}]$ are principal ideals generated by $x^n - c$, for some $c \neq 0$, and $K[x^n, x^{-n}]/\mathbf{m}$ is isomorphic to K. We claim that $S^{-1}A/\mathbf{m}S^{-1}A$ is isomorphic to $M_n(K)$. The isomorphism is given by the following representation: Elements of R are mapped to diagonal matrices,

$$(a_1, ..., a_n) \to \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix}.$$

The element x is sent to the matrix

$$\bar{x} = \begin{pmatrix} 0 & & & & c \\ 1 & \cdot & & & \\ & \cdot & \cdot & & \\ & & \cdot & \cdot & \\ & & & 1 & 0 \end{pmatrix}.$$

Then $\bar{x}^n = cI$, and $\bar{x}$ commutes with the diagonal matrices according to the rule determined by φ. The kernel of the representations contains $(x^n - c)$, and assuming the map is onto, a comparison of dimensions shows that the kernel is no larger. Thus is suffices to prove surjectivity. This follows from the general criterion given below.

PROPOSITION 5.3. *Let D be a division ring and let x and y be matrices in $M_n(D)$. Assume that y is a diagonal matrix with distinct entries and x is a monomial matrix whose corresponding permutation generates a transitive subgroup of the symmetric group S_n. Then the subalgebra B generated over D by x and y is $M_n(D)$.*

Proof. Let V be an n-dimensional vector space over D^{op}, with standard basis $e_1, \dots, e_n$. Then $M_n(D)$ is the ring of endomorphisms of V, and by the density theorem it suffices to show that B acts irreducibly on V. For then B must contain a full set of basis elements of $M_n(D)$, and since B contains D, we have $B = M_n(D)$.

Let $v = \sum_{i=1}^{n} a_i e_i$ be an element of V with a_r and a_s not equal to 0, and suppose $ye_i = d_i e_i$. By assumption, the d_i are distinct, so the vector

$$(y - d_r)v = \sum_i (d_i - d_r)\, a_i v_i$$

has fewer non-zero coefficients, and is non-zero. Thus $B \cdot v$ must contain a basis vector e_i. The assumption on the matrix x implies that the powers of x map e_i to scalar multiples of all other basis elements, so $Bv = V$.

Using the fact that the ideals of an Azumaya algebra are exactly the extensions of the ideals in the center [7], we can conclude that the primes of the ring $S^{-1}A$ are (0) and $\{(x^n - c) \mid c \neq 0\}$. By Proposition 5.1, we obtain

COROLLARY 5.4. *The primes of A are* (0), $\{(x^n - c) \mid c \neq 0\}$, *and the primes which contain x.*

Let us consider a more general example. Let $R = \prod_i K_i$ be the product of m copies of an arbitrary field K, and let ψ be an automorphism of K of order m'. Then define the automorphism φ of R to be

$$\varphi(a_1, \dots, a_m) = (a_2, \dots, a_m, \psi(a_1)).$$

Observe that

$$\varphi^m(a_1, \ldots, a_m) = (\psi(a_1), \ldots, \psi(a_m)),$$

so φ must have finite order $n = mm'$. The fixed ring R^φ consists of elements of the form $(a, \ldots, a)$, for which $\psi(a) = a$. Thus R^φ is isomorphic to the fixed field k of K under ψ. Letting A be the Ore extension $R[x; \varphi]$, we see that the center of A is $k[x^n]$. Once again, the primes of A which contain x^n, and hence x, are of little interest, so we pass to the central localization of A by $S = \{x^{in}\}$:

$$S^{-1}A = k[x^n, x^{-n}] \otimes_{k[x^n]} A.$$

PROPOSITION 5.5. *The ring $S^{-1}A$ is an Azumaya algebra over its center $k[x^n, x^{-n}]$.*

Proof. A ring is an Azumaya algebra if it becomes one after extending scalars by a faithfully flat extension of the center [7]. In particular, we can change the base from $k[x^n, x^{-n}]$ to $\bar{k}[x^n, x^{-n}]$, to obtain the algebra

$$B = \bar{k} \otimes_k S^{-1}A = S^{-1}(\bar{k} \otimes_k A).$$

Let us examine the ring $\bar{k} \otimes_k K$. The automorphism ψ of K induces an automorphism $1 \otimes \psi$ of $\bar{k} \otimes_k K$, which can be pictured explicitly. The extension $k \subset K$ is Galois of degree m', so the normal basis theorem implies that there is an element $b \in K$ such that $\{b, \psi(b), \ldots, \psi^{m'-1}(b)\}$ forms a basis for K over k. As a vector space, K decomposes into the direct sum $\bigoplus_i (\psi^i(b))k$. Hence $\bar{k} \otimes K$ is a $\bar{k}$-space of the form $\bigoplus_i (\psi^i(b))\bar{k}$, and the action of ψ on $\bar{k} \otimes_k K$ cyclically permutes the factors.

As a result, $\bar{k} \otimes_k R$ splits into a direct sum of n copies of $\bar{k}$, and the action of $1 \otimes \varphi$ on $\bar{k} \otimes_k R$ cyclically permutes the n factors. In particular, φ^m acts on each component $\bar{k} \otimes_k K_i$ in the same way that ψ does on $\bar{k} \otimes_k K$. Thus the ring $\bar{k} \otimes_k R$ and the automorphism $1 \otimes \varphi$ have the form discussed in the preceding propositions. The algebra $\bar{k} \otimes_k A = \bar{k} \otimes_k R[x; \varphi]$ is isomorphic to

$$(\bar{k} \otimes_k R)[x; 1 \otimes \varphi],$$

and so by Proposition 5.2, $S^{-1}(\bar{k} \otimes_k A)$ is an Azumaya algebra. As observed, it follows that $S^{-1}A$ is an Azumaya algebra.

COROLLARY 5.6. *The prime ideals of $S^{-1}A$ are the extended ideals of the primes of $k[x^n, x^{-n}]$.*

This last example puts us in a position to prove Theorem 4.4. The setting is as follows: R is a φ-prime ring, where φ is an automorphism of finite order n, and $A = R[x; \varphi]$. We wish to determine the prime ideals of A that intersect R

in (0) and do not contain x. Let Q be the fixed subring of R under φ, and order the minimal primes $p_1, \ldots, p_m$ so that $\varphi^{-1}(p_i) = p_{i+1}$. The set of regular elements of R is precisely $S = R - \cup p_i$.

LEMMA 5.7. *The non-zero elements of Q are regular, and the center of A is the domain $Q[x^n]$.*

Proof. Given a non-zero element $r \in Q$, there is a prime p_i which does not contain r, since $\bigcap_j p_j = (0)$. But then $\varphi^{-j}(r) \notin p_{i+j}$, and $\varphi^{-j}(r) = r$. Hence r is in no associated prime of (0), which means r is regular.

In order to insure that a prime I of A which does not contain x intersects R in (0), it suffices to require that $I \cap S$ is empty. For I intersects R in some φ-prime ideal, by Theorem 4.1, and any φ-prime ideal larger than (0) must contain elements of S. Thus inverting the elements of S would throw out the primes which do contain elements of S, but such a process would not be a central localization. The next lemma says we can accomplish the same goal nonetheless.

LEMMA 5.8. *The map of fraction rings $R_{Q^*} \to R_S$ is an isomorphism, where $Q^* = Q - \{0\}$.*

Proof. Injectivity is clear, since the inverted elements are regular. Suppose $rs^{-1} \in R_S$ for some element $s \in S$. Let $u = r \prod_{i=1}^{n-1} \varphi^i(s)$ and $v = s \prod_{i=1}^{n-1} \varphi^i(s)$. Then $uv^{-1} = rs^{-1}$, and $v \in Q^*$.

Thus we may pass to the central localization $Q^{*^{-1}}A = A_{Q^*}$. Let T denote R_{Q^*}, and notice that the map φ extends to an isomorphism of T of order n, defined by $\varphi(rq^{-1}) = \varphi(r)q^{-1}$. The fixed ring of T is exactly the quotient field k of the domain Q. For if φ fixes rq^{-1}, then $\varphi(r)q^{-1} = rq^{-1}$, and $\varphi(r) = r$, so $r \in Q$. Let B be the Ore extension $T[x; \varphi]$. Then B is isomorphic to A_{Q^*}, and the center of B is $k[x^n]$. The diagrams below summarize the situation:

$$\begin{array}{ccc} R \subset T & \qquad & A = R[x; \varphi] \subset B = T[x; \varphi] \\ \cup \quad \cup & & \cup \qquad\qquad\qquad \cup \\ Q \subset k & & Q[x^n] \quad \subset \quad k[x^n] \end{array}.$$

The primes of A that we want to find are the restrictions of the primes of B, by 5.1. In order to discard the primes containing x, we may invert the central element x^n.

THEOREM 5.9. *The ring $B[x^{-n}]$ is an Azumaya algebra with center $k[x^n, x^{-n}]$.*

Proof. Let us take a closer look at T. The primes of T are the extensions of p_i, and all are maximal. Therefore by the Chinese Remainder Theorem, the map

$$T \to \prod_1^n T/p_i$$

is an isomorphism, and T is a product of fields. Let K_i denote the field T/p_i, and define the map θ_i to be the composition

$$T \xrightarrow{\varphi} T \longrightarrow T/p_{i-1}.$$

This is a surjection, with kernel $\varphi^{-1}(p_{i-1}) = p_i$. Hence θ_i maps K_i isomorphically to K_{i-1}, and the action of φ on $T = \prod_i K_i$ is given by

$$\varphi(s_1, \ldots, s_n) = (\theta_2(s_2), \ldots, \theta_m(s_m), \theta_1(s_1)).$$

It is now clear that we are in the situation of Proposition 5.5, so we may conclude that $B[x^{-n}]$ is Azumaya.

The primes of $B[x^{-n}]$ are therefore extensions of the primes of $k[x^n, x^{-n}]$, and they restrict to the primes of A for which we are looking. Since $k[x^n, x^{-n}]$ is the localization of $Q[x^n]$ with respect to the set $\{Q^*, x^{in}\}$, the primes of $k[x^n, x^{-n}]$ correspond to the primes of $Q[x^n]$ which do not contain any elements of the localizing set. We may then conclude

COROLLARY 5.10 (4.4). *The primes of A which intersect R in* (0) *and do not contain x are in one-to-one correspondence with the primes of the center $Q[x^n]$ which do not contain x^n and which intersect Q in* (0).

6. Preservation of Goldie Dimension and Non-Singularity

As noted in Section 2, an Ore extension of a noetherian ring need not be noetherian. However, some finiteness conditions may be preserved. It is well-known that a domain has finite Goldie dimension if and only if it has dimension one, or equivalently is an Ore domain. Thus the next theorem, due to Curtis and Hirsch, can be interpreted as saying that for domains, finite Goldie dimension is preserved under Ore extensions.

THEOREM 6.1 [1, 4]. *Let S be a right Ore domain and φ a monomorphism. Then $S[x; \varphi]$ is an Ore domain.*

For us, let R be a commutative φ-cyclic ring (for instance a noetherian φ-prime ring), with n primes associated to (0). It is easy to see that R has Goldie dimension n. For instance, observe that its full quotient ring is a product of n

fields. Theorem 6.1 says, then, that in case R has dimension 1, so does $R[x; \varphi]$. More generally

THEOREM 6.2. *Let R be a commutative φ-cyclic ring of Goldie dimension n. Then the Ore extension $R[x; \varphi]$ has right Goldie dimension n.*

Proof. Let $p_1, ..., p_n$ be the minimal primes of R, ordered so that $\varphi^{-1}(p_{i+1}) = p_i$. It suffices to construct n uniform right ideals of A which are pairwise independent and whose direct sum is an essential right ideal of A.

Such a family of ideals for R can be constructed easily. We define the ideals

$$q_i = p_i \cap \cdots \cap \hat{p}_i \cap \cdots \cap p_n .$$

Then for $i \neq j$, we see that $q_i \cap q_j = (0)$. The ideals are uniform since R is commutative, and their sum is clearly essential.

We construct the desired ideals in A using these ideals. Let J_i be the set of elements $\sum x^i r_i$ in A such that the coefficient $r_0 \in q_i$, the coefficient $r_1 \in q_{i+1}$, and more generally, $r_m \in q_{i+m}$, where the indices are taken modulo n. In other words, each coefficient is in all but one prime, the omitted prime being chosen in the unique manner required for $J_i x \subset J_i$.

It follows by this choice that each J_i is a right ideal, and $J_i \cap J_j = (0)$ for $i \neq j$. We claim that the direct sum of these right ideals is an essential right ideal. To show this, we must prove that for any $r \neq 0$ in A, the right ideal rA contains a non-zero element of the direct sum. Let

$$r = \sum_{i=0}^{m} x^i r_i$$

and suppose that $r_m \notin p_1$. Let s be an element in $q_1 - p_1$. Then rs is non-zero, and every coefficient is either 0 or an element of $q_1 - p_1$. Therefore each $x^i r_i s$ lies in some J_k, and

$$rs \in \bigoplus_k J_k .$$

Lastly, we prove that the J_i's are uniform. If r and s are elements of J_i, we must show that they have a non-zero common right multiple. Multiply each on the right by powers of x so that the two new elements have the same degree, a multiple of n. Next multiply both on the right by some $t \in q_i - p_i$. The result is a pair of polynomials in x^n with coefficients in q_i. Therefore the two elements r and s have non-zero right multiples in $q[x^n; \varphi^n]$. Since q is a commutative domain, Theorem 6.1 implies that $q[x^n; \varphi^n]$ is an Ore domain, and this completes the proof.

Non-singularity is also preserved under the Ore extension.

THEOREM 6.3. *Let R be a commutative φ-cyclic ring. Then $A = R[x; \varphi]$ is right non-singular.*

Proof. Assume that R has minimal primes $p_1, \ldots, p_t$, with $\varphi^{-1}(p_{i+1}) = p_i$, and let $r = \sum_{i=0}^{m} x^i r_i$ have an essential right annihilator $\mathbf{a}$ in A. We must show $r = 0$.

The right ideals

$$(\mathbf{a}: x^i) = \{a \in A: x^i a \in \mathbf{a}\}$$

are also right essential, so the ideal $\mathbf{a} \cap (\mathbf{a}: x) \cap \cdots \cap (\mathbf{a}: x^{t-1})$ is non-zero. Let $s = \sum_{i=0}^{n} x^i s_i$ be in the intersection, and assume that $s_n \neq 0$. The highest degree term of $rx^i s$ is

$$x^m r_m x^{i+n} s_n = x^{m+i+n} \varphi^{i+n}(r_m) s_n .$$

But $rx^i s = 0$ for any $i = 0, \ldots, t-1$, so $\varphi^{i+n}(r_m) s_n = 0$. Since $s_n \neq 0$, it does not lie in some minimal prime, say p_t. Then

$$\varphi^{i+n}(r_m) \in p_t$$

for $i \leqslant t-1$, and so $r_m \in p_i$ for every i. Hence $r_m = 0$ and $r = 0$.

COROLLARY 6.4. *Let R be a commutative φ-cyclic ring. Then $A = R[x; \varphi]$ is a prime right Goldie ring.*

Proof. The ring A is prime by 4.1, and it is well-known that a prime, finite-dimensional, non-singular ring is Goldie.

COROLLARY 6.5. *Let φ be an endomorphism of a commutative noetherian ring R, and let $A = R[x; \varphi]$. Then the prime images of A are right Goldie.*

Proof. Let I be a prime ideal. If $x \in I$, then A/I is an image of R, and so is noetherian. Assume $x \notin I$. If $I = A(I \cap R)A$, then A/I is an Ore extension of the φ-cyclic ring $R/I \cap R$, and Corollary 6.4 applies. In the only remaining case, by Theorem 4.3, φ induces a finite order automorphism on $R/I \cap R$, hence A/I is noetherian by Proposition 2.3.

7. THE JACOBSON RADICAL

Now that we can describe the prime ideals of an Ore extension, we would like to have information on the primitive ideals. To determine which prime ideals are primitive may be too much to ask, so let us ask instead how large the

Jacobson radical of a prime is. Recall that the Jacobson radical is the intersection of the primitive ideals containing a prime. The next result shows that the radical tends to be small.

THEOREM 7.1. *Let R be a φ-cyclic ring and let $A = R[x; \varphi]$. Then the Jacobson radical of A is zero.*

Proof. Assume that the radical J is non-zero. We can order the minimal primes $p_1, \ldots, p_t$ of R so that $\varphi^{-1}(p_i) = p_{i-1}$. Let $s = \sum_{i=0}^{n} x^i s_i$ be an element of J chosen so that if s_n is the highest non-zero coefficient, n is a multiple of t, and so that $s_0 = 0$. This is easily arranged, since we can multiply an arbitrary element of J on the left by a power of x and obtain the desired element. The element $1 + ss_n$ has an inverse $r = \sum_{i=0}^{m} x^i r_i$, where $r_0 = 1$ and $r_m \neq 0$. The highest degree term of the product $1 = r(1 + ss_n)$ is

$$x^m r_m x^n s_n s_n = x^{m+n} \varphi^n(r_m) s_n^{\,2},$$

so $\varphi^n(r_m)s_n^{\,2} = 0$. The minimal primes of R that do not contain s_n contain $\varphi^n(r_m)$. Since n is divisible by t, these primes contain r_m as well.

On the other hand, consider the degree m term of the product:

$$x^m r_m + x^m \left(\sum_{i=0}^{m-1} \varphi^{m-i}(r_i) s_{m-i} \right) s_n .$$

This term must also equal 0, so r_m is a multiple of s_n. Hence r_m is contained in the minimal primes which contain s_n, as well as the minimal primes that do not contain s_n. But then $r_m = 0$, a contradiction.

A ring is called a Jacobson ring if the Jacobson radical of every prime ideal equals the prime ideal itself. For Ore extensions over not necessarily commutative rings, the following result holds, due to Goldie and Michler [2]:

THEOREM 7.2. *Let φ be an automorphism of a noetherian Jacobson ring R. Then the Ore extension $R[x; \varphi]$ is Jacobson.*

If we restrict to commutative base rings, this result can be extended as follows:

THEOREM 7.3. *Let R be a commutative noetherian Jacobson ring, and let φ be an arbitrary endomorphism. Then the Ore extension $A = R[x; \varphi]$ is a Jacobson ring.*

Proof. Let I be a prime ideal. If I contains x, then A/I is an image of R, so A/I has radical (0) since R is Jacobson. Assume $x \notin I$. If $I = A(I \cap R)A$, then 7.1 applies to show that A/I has radical (0). In the only remaining case, φ is a finite order automorphism on $R/I \cap R$, and Theorem 7.2 applies.

Remark. The assumption that R is Jacobson is necessary, for if A is Jacobson, so is its image $A/(x)$, which is isomorphic to R.

Also, the assumption that R is noetherian is necessary, as Stephenson and Pearson have shown [10]. They have constructed a commutative Jacobson φ-prime ring R with automorphism φ such that $A = R[x; \varphi]$ has non-zero Jacobson radical, although A is prime. This shows, incidentally, that a φ-prime ideal need not be φ-cyclic.

8. The Case $R = k[y]$

In order to illustrate the preceding theory, we shall examine the results if the base ring R is a polynomial ring $k[y]$ over a field k. If k is real closed or algebraically closed, an explicit description of the irreducible representations of an Ore extension will be given.

Let φ be an endomorphism of R; the map φ is determined by assigning the value of $\varphi(y)$, which we will assume is $f(y)$. Then the Ore extension $A = R[x; \varphi]$ can be presented by generators x and y over k, with the relation

$$yx = xf(y).$$

Our first task is to determine the φ-prime ideals of R, which are all φ-cyclic, since R is noetherian. We need some terminology:

Definitions. (1) An element a of $\bar{k}$ is a *periodic point* of f if there exists an integer $n > 0$ such that $f^n(a) = a$, where $f^n(y)$ is the polynomial $f(f(f \cdots f(y) \cdots))$, iterated n times. The least such integer n is the period of a.

(2) Let $p_a(y)$ or $p(a, y)$ denote the monic irreducible polynomial of a over k; i.e., the monic generator of the kernel of the map from $k[y]$ to $\bar{k}$ given by sending y to a.

(3) Let a be a periodic point with period n. We define

$$q_a(y) = \prod_{i=1}^{m} p(f^i(a), y),$$

where m is the least integer such that $p(a, y) = p(f^m(a), y)$.

Proposition 8.1. *The φ-prime ideals of $k[y]$ are $(q_a(y))$, where a is a periodic point of f, and also (0) if φ is injective.*

Proof. The (0) ideal is prime, so it is φ-prime if and only if it is φ-invariant. This is the case if and only if φ is injective.

To determine the other ideals, consider the action of φ^* on Spec $k[y]$. The generator of a prime ideal $\mathbf{a}$ must be an irreducible polynomial $p(a, y)$ for some element $a \in \bar{k}$. The image $\varphi^*(\mathbf{a})$ is generated by $p(b, y)$, where b is chosen so that $p(b, f(y)) \in \mathbf{a}$. This implies that $p(b, f(a)) = 0$, so $f(a)$ is conjugate to b. But then $p(b, y) = p(f(a), y)$. As a result, a set of primes including $\mathbf{a}$ is cyclically permuted by φ^* if and only if a is periodic. The intersection of such a family of primes is precisely the ideal generated by $q_a(y)$.

Therefore, to determine the prime ideals of $A = (k[y])[x; \varphi]$, it suffices to treat rings B of the form $S[x; \varphi]$, where $S = k[y]/(q_a(y))$. Notice that the map

$$k[y]/(q_a(y)) \to \prod_{i=1}^{m} k[y]/(p(f^i(a), y)$$

is an isomorphism, and that each factor ring $k[y]/(p(f^i(a), y)$ is a finite field extension K_i of k. The situation is a special case of that which we saw in Theorem 5.9, and we can conclude again that the K_i are all isomorphic to a field K, and that φ acts on S by moving each K_i to K_{i-1}. Thus φ induces a map φ^m on K, and the fixed field F of K under this map is isomorphic to the fixed ring of S under φ. Therefore the center B is isomorphic to $F[x^n]$. Theorem 4.4 now translates into the following result:

THEOREM 8.2. *The prime ideals of A are:*

(0)	*if φ is injective,*
(x), $(q_a(y))$	*where a is f-periodic,*
$(x, p(b, y))$	*where b is arbitrary in $\bar{k}$, and*
$(q_a(y), h(x^n))$	*where a has period n and h is an irreducible polynomial in $F[x^n]$ other than x^n.*

COROLLARY 8.3. *The non-zero primitive ideals of A are maximal, and every non-faithful simple module of A is finite-dimensional over k.*

Proof. The ideal (x) is not primitive, since the factor ring $A/(x)$ is commutative but is not a field. Every other prime image of A is finite over its center, so cannot be primitive unless it is simple.

The corollary says that every primitive factor ring of A with non-zero kernel is in fact a finite-dimensional simple algebra over k. By Wedderburn's theorem, such a ring has the form $M_s(D)$, where s is a unique positive integer and D a unique division algebra, finite-dimensional over k. Thus an explicit determination of the simple images of A requires explicit information on the division algebras over k. It is not surprising then that we can determine s and D precisely if k is algebraically closed or real closed. The remainder of the section is devoted to this.

THEOREM 8.4. *Suppose k is algebraically closed. Then the maximal ideals of A have the form*

$$\begin{array}{ll} (x, y - c) & c \text{ arbitrary in } k, \\ (q_a(y), x^n - b) & a \text{ has period } n,\ b \neq 0, \text{ and} \end{array}$$

$q_a(y) = (y - a) \cdots (y - f^{n-1}(a))$. Moreover the factor ring of A by $(q_a(y), x^n - b)$ is isomorphic to $M_n(k)$, and an explicit map is given by

$$y \to \bar{y} = \begin{pmatrix} a & & & \\ & f(a) & & \\ & & \ddots & \\ & & & f^{n-1}(a) \end{pmatrix}, \quad x \to \bar{x} = \begin{pmatrix} 0 & & & & b \\ 1 & 0 & & & \\ & 1 & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1 & 0 \end{pmatrix}. \tag{1}$$

Proof. Since k is algebraically closed, the fields K_i and F of 8.2 are all isomorphic to k. Therefore the maximal ideals are as claimed, by 8.2.

The matrix $\bar{y}$ obviously has $q_a(y)$ as minimal polynomial, and the equations $x^n = b$ and $yx = xf(y)$ are satisfied. It remains to check that the image of A equals $M_n(k)$. This follows directly from 5.3.

If k is real closed, the possibilities for simple images of A are considerably more varied and interesting, but can still be surveyed. Frobenius's Theorem says that the only finite-dimensional division algebras over k are k itself, the algebraic closure $\bar{k} = k(i)$, and the quaternion algebra Q. We will present Q with generators i and j over k, where $i^2 = j^2 = -1$ and $ij = -ji$. Let $\bar{a}$ denote the conjugate of a in $\bar{k}$. There are three types of periodic points:

(I) $f^n(a) = a$ and $a \in k$,

(II) $f^n(a) = a$, with $a \in \bar{k} - k$, and $f^i(a) \neq \bar{a}$ for all $i < n$,

(III) $f^{2m}(a) = a$, and $f^m(a) = \bar{a}$, where $a \in \bar{k} - k$.

Let us consider the results case-by-case.

PROPOSITION 8.5. *Let k be real closed and assume that a is a periodic point of type I. Then the maximal ideals of A not containing x have the form $I = (q_a(y), p_b(x^n))$, where p_b is the irreducible polynomial of b over k, the element b is any non-zero element of $\bar{k}$, and $q_a(y) = (y - a) \cdots (y - f^{n-1}(a))$. The algebra A/I is isomorphic to $M_n(k(b))$ via the representation* (1).

Proof. In this situation, the fields K_i of 8.2 are all isomorphic to k, the integers n and m coincide, and the fixed field F is k. Thus we may apply 8.2 to conclude that the maximal ideals are as indicated. The ideal I is obviously contained in the kernel of the representation (1), and must be the entire kernel since it is maximal. Thus we need only check that the image of A is all of $M_n(k(b))$. By 5.3, this follows if the image contains $k(b)$, and this is the case since x^n maps to b.

PROPOSITION 8.6. *Let k be real closed and assume that a is a periodic point of type II. The maximal ideals of A which do not contain x have the form $I = (q_a(y), p_b(x^n))$, where p_b is the irreducible polynomial of b over k, with $b \neq 0$, and $q_a(y) = (y - a)(y - \bar{a}) \cdots (y - f^{n-1}(a))(y - \overline{f^{n-1}(a)})$. The algebra A/I is isomorphic to $M_n(\bar{k})$ via the representation* (1).

Proof. This time the fields K_i are all isomorphic to $\bar{k}$, the integers n and m still coincide, and F is $\bar{k}$. Again 8.2 applies to show that the maximal ideals are as claimed. The kernel of the representation (1) is exactly I, and the matrices $\bar{x}$ and $\bar{y}$ generate the full matrix ring over $\bar{k}$, by 5.3. Hence it suffices to prove that the image of A contains $\bar{k}$. The polynomial $(y - a) \cdots (y - f^{n-1}(a))$ is not defined over k. Therefore, denoting by S_i the ith symmetric polynomial in n variables, we see that there exists an i so that $S_i(a,..., f^{n-1}(a))$ is not in k. Let this scalar be d. Then the matrix $S_i(\bar{y},..., f^{n-1}(\bar{y}))$ is a scalar matrix in A/I with the value d. As a result, A/I contains $k(d)$, which equals $\bar{k}$.

The third case is the most interesting, requiring some representations other than (1). We will state the result in several parts.

PROPOSITION 8.7. *Let k be real closed and assume that a is a periodic point of type III. The maximal ideals of A which do not contain x have the form $I = (q_a(y), p_b(x^n))$, where p_b is the irreducible polynomial of b over k, the element b is any non-zero element of $\bar{k}$, and*

$$q_a(y) = (y - a) \cdots (y - f^{m-1}(a))(y - \bar{a}) \cdots (y - \overline{f^{m-1}(a)}).$$

Proof. The fields K_i are isomorphic to $\bar{k}$, but the integer $n = 2m$, and the fixed field F is k. The maximal ideals are as claimed by 8.2.

PROPOSITION 8.8. *Assume that k is real closed, a is periodic of type III, b is a non-real element of $\bar{k}$, and $I = (q_a(y), p_b(x^n))$. Then the algebra A/I is isomorphic to $M_n(\bar{k})$ via the representation* (1).

Proof. The proof is identical to that given for 8.6.

PROPOSITION 8.9. *Assume that k is real closed, a is periodic of type III, and b is a negative element of k. Let $I = (q_a(y), p_b(x^n))$. Then the algebra A/I is isomorphic to $M_m(Q)$, via the representation:*

$$y \to \bar{y} = \begin{pmatrix} a & & \\ & \ddots & \\ & & f^{m-1}(a) \end{pmatrix}, \qquad x \to \bar{x} = \begin{pmatrix} 0 & & & & (-b)^{1/2}j \\ 1 & 0 & & & \\ & 1 & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1 & 0 \end{pmatrix}.$$

Proof. Observe that $\bar{x}^m = (-b)^{1/2}j$, so $\bar{x}^n = \bar{x}^{2m} = -bj^2 = b$. To check that $\bar{y}\bar{x} = \bar{x}f(\bar{y})$, observe that

$$a((-b)^{1/2}j) = ((-b)^{1/2}j)\bar{a} = ((-b)^{1/2}j)f^m(a).$$

The relation can now be verified by multiplying the matrices and using the preceding equations. Also, it is clear that $q_a(y)$ is the minimal polynomial of the matrix $\bar{y}$ over k. Therefore the ideal I is in the kernel of the representation above, and must be the entire kernel. It remains to show that A maps onto the full matrix ring over Q.

The argument used in 8.6 applies again to show that $\bar{k}$ is contained in the image. The element x^m maps to $(-b)^{1/2}j$, so the image contains j. Since i and j generate Q over k, the image contains Q as well.

Thus the image of A/I is the subalgebra B of $M_m(Q)$ generated over Q by the matrices $\bar{x}$ and $\bar{y}$, and 5.3 once again applies to complete the proof.

Before considering the final possibility, let us recall that $\bar{k}$ embeds in $M_2(k)$ via the regular representation. Explicitly, if $c \in \bar{k}$, and $c = r + si$, then c is represented by the matrix $\left(\begin{smallmatrix} r & s \\ -s & r \end{smallmatrix}\right)$ which we will denote c^*.

PROPOSITION 8.10. *Assume that k is real closed, a is periodic of type III, and b is a positive element of k. Let $b = c^2$, and let $I = (q_a(y), p_b(x^n))$. Then the algebra A/I is isomorphic to $M_n(k)$ via the representation*

$$y \to \bar{y} = \begin{pmatrix} a^* & & & \\ & f(a)^* & & \\ & & \ddots & \\ & & & f^{m-1}(a)^* \end{pmatrix},$$

$$x \to \bar{x} = \begin{pmatrix} 0^* & & & & \begin{pmatrix} 0 & c \\ c & 0 \end{pmatrix} \\ 1^* & 0^* & & & \\ & 1^* & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1^* & 0^* \end{pmatrix}$$

where the matrices are written in 2×2 blocks.

Proof. The minimal polynomial of $\bar{y}$ is $q_a(y)$, since the minimal polynomial of the matrix $f^i(a)^*$ is $(y - f^i(a))(y - \overline{f^i(a)})$. Suppose $a = r + si$. Then the relation $\bar{y}\bar{x} = \bar{x}f(\bar{y})$ follows from

$$a^*\begin{pmatrix}0 & c\\ c & 0\end{pmatrix} = \begin{pmatrix}r & s\\ -s & r\end{pmatrix}\begin{pmatrix} & c\\ c & \end{pmatrix} = \begin{pmatrix} & c\\ c & \end{pmatrix}\begin{pmatrix}r & -s\\ s & r\end{pmatrix} = \begin{pmatrix} & c\\ c & \end{pmatrix}\bar{a}^* = \begin{pmatrix} & c\\ c & \end{pmatrix} f^m(a)^*.$$

Also observe that

$$\bar{x}^m = \begin{bmatrix} \begin{array}{cc|} & c\\ c & \\ \hline \end{array} & & \\ & \ddots & \\ & & \begin{array}{|cc} \hline & c\\ c & \end{array} \end{bmatrix}$$

and so $\bar{x}^{2m} = \bar{x}^n = c^2Id = bId$. Therefore I is the kernel of the representation, and we need only check that it is onto.

Let M be the 2×2 matrix

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -i\\ i & -1\end{pmatrix}.$$

Then $M^2 = Id$, and given a matrix of the form t^*, one can check that

$$Mt^*M = \begin{pmatrix}t & \\ & \bar{t}\end{pmatrix}, \qquad \text{and} \qquad M\begin{pmatrix}0 & c\\ c & 0\end{pmatrix}M = \begin{pmatrix}0 & -c\\ -c & 0\end{pmatrix}.$$

Let $\overline{M}$ be the matrix containing m copies of M along the diagonal. Then the above identities imply that, inside $M_n(\bar{k})$, the conjugates of $\bar{x}$ and $\bar{y}$ are

$$\overline{M}\bar{y}\overline{M} = \begin{pmatrix} a & & & & \\ & \bar{a} & & & \\ & & \ddots & & \\ & & & f^{m-1}(a) & \\ & & & & \overline{f^{m-1}(a)} \end{pmatrix},$$

and

$$\overline{M}\bar{x}\overline{M} = \begin{pmatrix} 0^* & & \begin{pmatrix}0 & -c\\ -c & 0\end{pmatrix} \\ 1^* & 0^* & \\ & 1 & \ddots \\ & & \ddots \quad \ddots \\ & & 1^* \quad 0^* \end{pmatrix}.$$

We can apply 5.3 to deduce that these conjugates generate $M_n(\bar{k})$ over $\bar{k}$, hence so do $\bar{x}$ and $\bar{y}$. As a result, the set of matrices $\{\bar{x}^i\bar{y}^j \mid 0 \leqslant i, j \leqslant n-1\}$ is independent over $\bar{k}$, and also over k. Therefore $\bar{x}$ and $\bar{y}$ generate the full matrix ring over k, and the map is onto.

9. Primitivity in the Case $R = k[y]$

The major question left unanswered about an Ore extension A is which of the prime ideals are primitive. In case $R = k[y]$ and A is an Ore extension of R, the only prime ideal in doubt is (0), by 8.2 and 8.3, so the question becomes: is A primitive? Notice that there are really two questions here, primitivity on the right and on the left. In this section, we will obtain partial results for right primitivity and complete results for left primitivity.

Let us first consider what happens when the endomorphism φ is not injective, or equivalently, when the image $f(y)$ of y under φ has degree 0. By 8.2, A is not even prime, so the issue of primitivity cannot arise. But let us see this in a more direct manner. Suppose $f(y) = a$, so that the defining relation of A is $yx = ax$. Substituting $y - a$ for y, we can assume that A is generated over k by elements x and y, which satisfy the relation $yx = 0$.

Theorem 9.1. *Let $A = k\{x, y\}/(yx)$. Then the ideal generated by xy is nilpotent, and xy lies in the prime radical. Hence the prime and primitive ideal structure of A corresponds to that of the commutative ring $k[x, y]/(yx)$.*

Proof. Just observe that for any $a \in A$, $xyaxy = 0$.

We turn now to the case that $f(y)$ has degree 1, or equivalently, φ is an automorphism. Let $A = k\{x, y\}/(yx - xf(y))$ and $f(y) = ay + b$, and assume that $f(y) \neq y$. There are two distinct possibilities:

(1) φ has finite order. This occurs if and only if a is a primitive nth root of unity, and $n > 1$. For

$$f^m(y) = a^m y + b(1 + a + \cdots + a^{m-1}).$$

In this case, A is a finite module over its center $k[x^n, y^n]$. Hence A is primitive only if A is simple, and this is not the case by 8.2.

(2) φ has infinite order.

Theorem 9.2. *Let $A = k\{x, y\}/(yx - x(ay + b))$, where a is not a primitive nth root of unity, $n > 1$. Then A is left and right primitive.*

Proof. The periodic points of f are those that satisfy

$$c = f^n(c) = ca^n + b(1 + a + \cdots + a^{n-1}),$$

or

$$c = b/(1 - a).$$

If $a = 1$, there are no periodic points, and otherwise the periodic point c has period 1. Therefore 8.2 implies that every factor ring of A by a non-zero prime ideal contains x in the center. So every non-zero prime contains $xy - yx$. If A is not left or right primitive, $xy - yx$ must lie in the Jacobson radical of A, which implies that $1 + xy - yx$ is invertible in A. But this is impossible, for no element in A of degree greater than 0 can be invertible.

A direct construction of a faithful, simple, module for A can be easily described, after a change of variables. We assume that $a \neq 1$, and substitute $y - b/(1 - a)$ for y, to obtain a ring of the form $k\{x, y\}/(yx - axy)$. (If $a = 1$, so that $yx - xy = bx$, then A is isomorphic to the enveloping algebra of a non-abelian two-dimensional Lie algebra, and faithful, simple modules for A are well-known.) Let V be the infinite dimensional vector space with basis $\{v_i : i \in \mathbb{Z}\}$. Make V into a left A-module by defining the action

$$xv_i = v_{i+1}, \qquad yv_i = a^i v_{i-1}.$$

Then $yxv_i = a^{i+1}v_i$, and $(axy)v_i = aa^iv_i = a^{i+1}v_i$, so the module is well-defined. The basis of V consists of eigenvectors for the element yx, each having a distinct eigenvalue. Thus, as in the proof of 5.3, yx can be used to obtain a basis vector in $A \cdot v$ for any non-zero vector v. The action of x and y on the basis vector then generates all of V, so $A \cdot v = V$.

We now turn to the case that $f(y)$ has degree greater than 1.

THEOREM 9.3. *Let $A = k\{x, y\}/(yx - xf(y))$, with the degree of $f(y)$ equal to $d > 1$. Then A is left primitive.*

Proof. We will construct an explicit infinite-dimensional simple A-module. By Corollary 8.3, it must be faithful. Let V be the k-vector space with basis $v_1, v_2, v_3, \ldots$. Let

$$y \cdot v_n = v_{n+1}$$

and

$$x \cdot v_n = 0 \qquad \text{if} \quad n < d,$$
$$x \cdot v_d = v_1.$$

The action of x on the rest of V is now automatically determined, if the relation $yx = xf(y)$ is to hold. We see this inductively.

For the relation to hold on v_1, we require that

$$yx \cdot v_1 = xf(y) \cdot v_1.$$

Let $f(y) = \sum_{i=0}^{d} a_i y^i$. Since $yx \cdot v_1 = 0$, we find that

$$0 = xf(y) \cdot v_1 = \sum_{i=0}^{d} a_i x \cdot v_{i+1},$$

so that

$$a_d x \cdot v_{d+1} = -\sum_{i=0}^{d-1} a_i x \cdot v_{i+1}.$$

Suppose inductively that x has been defined on v_i for $i < n + d$ and $yx = xf(y)$ on v_i for $i < n$. Then the condition that $yx = xf(y)$ on v_n forces the rule that

$$a_d x \cdot v_{n+d} = yx \cdot v_n - \sum_{i=0}^{d-1} a_i x \cdot v_{n+i}.$$

This defines the A module structure of V completely. It follows that if $n = rd+s$ for $s < d$ and $r > 0$, then

$$x \cdot v_n = c_n v_r + \text{(lower indexed vectors)}$$

for some scalar c_n. Moreover, if $n = rd$, then $c_n \neq 0$, as is easily proved by induction.

The simplicity of V follows. For let v be a non-zero vector of V. We can choose an m such that

$$y^m \cdot v = \sum_{i=0}^{n} b_i v_i,$$

with $b_n \neq 0$ and $n = d^t$. Then

$$x^t y^m \cdot v = cv_1,$$

where $c = b_n c_{d^t} \cdots c_d \neq 0$. Thus $A \cdot v$ contains v_1, and so $A \cdot v = V$.

A companion result is

THEOREM 9.4. *Let $A = k\{x, y\}/(yx - xf(y))$, with $f(y)$ a non-zero polynomial divisible by y^2. Then A is right primitive.*

Proof. Let $f(y) = a_r y^r + \cdots + a_s y^s$, with $r > 1$ and $a_r \neq 0 \neq a_s$. Let V be the k-vector space with basis $v_1, v_2, \ldots$. We define

$$\begin{aligned} v_n \cdot y &= v_{n-1} \quad \text{for} \quad n > 1 \\ v_1 \cdot y &= 0. \end{aligned}$$

We now choose, for each $n \geqslant 1$, constants $c(i, n)$ with $i = 1, \ldots, rn$ so that

$$v_n \cdot x = \sum_{i=1}^{rn} c(i, n) v_i .$$

We require also that $c(rn, n) \neq 0$ and that $yx = xf(y)$ is satisfied on v_n. This is done inductively on n. For $n = 1$, we may take $v_1 \cdot x = v_r$, and $yx = xf(y)$ holds on v_1. Assume we have fulfilled all our requirements below n. Then the choice of $c(i, n)$ must be made so that $v_n \cdot yx = v_n \cdot xf(y)$. Thus we require

$$\sum_{i=1}^{rn-r} c(i, n-1) v_i = v_{n-1} \cdot x = v_n \cdot xf(y) = \sum_{i=1}^{rn} (c(i, n) v_i) \cdot \left(\sum_{j=r}^{s} a_j y^j \right)$$

The constants $c(i, n)$ for $i \leqslant r$ may be chosen arbitrarily, since the corresponding terms on the right are annihilated by the powers of y. This leaves $rn - r$ constants to be chosen, and $rn - r$ equations for them. In fact, the v_{rn-r} term produces the equation

$$c(rn - r, n - 1) = c(rn, n) a_r .$$

Since a_r and $c(rn - r, n - 1)$ are non-zero, we obtain a non-zero value for $c(rn, n)$. Each succeeding term, involving v_j, produces an equation involving $c(i, n)$ for $i \geqslant j$, and may be solved for $c(j, n)$ by substituting the already determined values for $c(i, n)$ with $i > j$. Thus the constants are determined and V has a well-defined structure of right A-module.

For simplicity, let v be any non-zero vector. Then for some t, the element $v \cdot y^t$ equals cv_1 with $c \neq 0$. So $v \cdot A$ contains v_1, and it is clear that $v \cdot A = V$. Faithfulness follows by 8.3.

We would like to know precisely when A is right primitive. We can extend the family of right primitive rings slightly, by the following result:

THEOREM 9.5. *Let R be a dedekind domain and let φ be an injective endomorphism of R. Assume for some prime p of R that $\varphi^n(p) \subset p^t$ for some n and some $t > 1$. Then $A = R[x; \varphi]$ is right primitive.*

Remark. The assumption on p implies that $\varphi^{-n}(p^t)$ contains p, so $\varphi^{-n}(p) = p$. Thus if n is chosen minimally, the ideal $p\varphi^{-1}(p) \cdots \varphi^{-n+1}(p)$ is a φ-prime ideal of R. So if $R = k[y]$, with k algebraically closed, and $\varphi(y) = f(y)$, the assumption is the following: there exists an f-periodic point a of period n, and $t > 1$, such that $(y - a)^t$ divides $f^n(y) - a$. Theorem 9.4 is a special case with $a = 0$ and $n = 1$.

Before proving the theorem, we need an easy lemma. The p-order (or just the order) of an element x in R is the largest integer m for which $x \in p^m$. Equivalently, this is the exponent of p in the prime decomposition of the ideal xR. We define similarly the p-order of any ideal in R.

LEMMA 9.6. *Let p be a prime of R such that $\varphi^{-n}(p) = p$ with n minimal. Suppose $\varphi^n(p)$ has p-order t. Then for any $r \in p$ such that $\varphi^n(r)$ has order t, the element $\varphi^{in}(r)$ has order t^i.*

Proof. By assumption, $\varphi^n(r)R = p^t q_1 q_2 \cdots q_s$ with no q_i equal to p. Then

$$\varphi^n(\varphi^n(r)R) = \varphi^n(p)^t \varphi^n(q_1) \cdots \varphi^n(q_s).$$

Each $\varphi^n(q_i)$ has order 0, for otherwise $p = \varphi^{-n}(p) \supset q_i$, contrary to hypothesis. Since $\varphi^n(p)^t$ has order t^2, the ideal generated by $\varphi^{2n}(r)$ has order at most t^2. But $\varphi^{2n}(r) \in p^{t^2}$, so t^2 is exactly the order. We continue by induction.

Proof of 9.5. Let n be chosen minimally so that $\varphi^{-n}(p) = p$. We wish to choose an element r in

$$p\varphi^{-1}(p) \cdots \varphi^{-n+1}(p)$$

such that $\varphi^n(r)$ has p-order t. This can be done by choosing r_1 in p with $\varphi^n(r_1)$ of order t and r_2 in

$$\prod_{i=1}^{n-1} \varphi^{-i}(p) - p.$$

Then $r_1 r_2 = r$ is the desired element. For if $\varphi^n(r_1)\,\varphi^n(r_2)$ is in p^{t+1}, then $\varphi^n(r_2)$ must be in p, since p^{t+1} is primary. But then r_2 lies in $\varphi^{-n}(p) = p$.

Form the right ideal $\mathbf{a} = pA + (1 + x^n r)A$. The theorem follows if we can prove that $\mathbf{a}$ is a proper right ideal. For let $\mathbf{m}$ be a maximal right ideal containing $\mathbf{a}$. The module $A/\mathbf{m}$ is simple, with annihilator equal to the largest two-sided ideal I in $\mathbf{m}$. Either $I = (0)$ or, by Theorem 4.1, I contains x or a non-zero φ-prime ideal of R.

If $x \in I$, then $\mathbf{m}$ contains $x^n r$, and so $1 \in \mathbf{m}$. Alternatively, suppose $I \cap R$ equals the ideal

$$q\varphi^{-1}(q) \cdots \varphi^{-m+1}(q)$$

for some prime q such that $\varphi^{-m}(q) = q$. If no $\varphi^{-i}(q)$ equals p, then p is comaximal with their product, and $\mathbf{m}$ contains 1. Otherwise some $\varphi^{-i}(q) = p$, and $m = n$. Then r is in the product and $x^n r \in I \subset \mathbf{m}$, so $1 \in \mathbf{m}$. Thus we obtain a contradiction unless $I = 0$.

It suffices, then, to prove that $\mathbf{a}$ is proper. Suppose not, and let

$$1 = \sum r_i a_i + (1 + x^n r) \sum x^j s_j\,, \tag{2}$$

where the r_i are in p, the elements a_i are in A, and the s_j lie in R. We will obtain a contradiction by proving the

CLAIM. *The coefficient* s_0 *has order* 0 *and* s_{jn} *has order* $\sum_{i=0}^{j-1} t^i$.

Proof. Recall that the p-order is a valuation, so that $\mathrm{ord}(c+d) \geqslant \min\{\mathrm{ord}(c), \mathrm{ord}(d)\}$, and equality holds if $\mathrm{ord}(c) \neq \mathrm{ord}(d)$. Also 0 has infinite order.

The 1 on the left side of (2) has order 0, while the constant term of $\sum r_i a_i$ has order at least 1. By the previous comment, s_0 must have order 0.

The coefficient of x^n in $\sum r_i a_i$ has order at least t, since $r_i x^n = x^n \varphi^n(r_i)$ and $\varphi^n(r_i) \in \varphi^n(p) \subset p^t$. On the other hand, rs_0 has order equal to 1, since r was chosen with order 1. Since the overall coefficient of x^n must be 0, the coefficient s_n is required to have order 1.

We now continue inductively. The coefficient of x^{jn} in $\sum r_i a_i$ has order at least t^j, since

$$r_i x^{jn} = x^{jn} \varphi^{jn}(r_i),$$

and $\varphi^{jn}(r_i) \in \varphi^{jn}(p) \subset p^{t^j}$. The term arising from

$$x^n r x^{(j-1)n} s_{(j-1)n}$$

has as coefficient $\varphi^{(j-1)n}(r) s_{(j-1)n}$. By induction, the order of $s_{(j-1)n}$ is $\sum_{i=0}^{j-2} t^i$. By Lemma 9.6, the order of $\varphi^{(j-1)n}(r)$ is t^{j-1}. So their product has order $\sum_{i=0}^{j-1} t^i$. This is less than t^j, but the overall coefficient of x^{jn} is 0, so s_{jn} must have the same order as $\varphi^{(n-1)n}(r) s_{(j-1)n}$. This proves the claim, and the theorem.

The condition of Theorem 9.5 can be interpreted geometrically as saying that there exists a periodic point $x \in \operatorname{Spec} R$ of period n with respect to the map φ^*: $\operatorname{Spec} R \to \operatorname{Spec} R$ such that the map $d(\varphi^{*^n})$ on tangent spaces at x is 0. This raises the question of whether A is right primitive in the non-singular case. In particular, for $R = k[y]$, we know A is always left primitive when $f(y)$ has degree >1. But if A is not always right primitive, we will have a left but not right primitive ring which is easy to describe. We admit that the only evidence that A need not be right primitive is the breakdown in the proofs of Theorems 9.4 and 9.5 without the given assumptions.

Note added in proof. We have proved the converse of Theorem 9.5, assuming that R has infinitely many φ-periodic primes, thus settling the question raised in the final paragraph. Details will appear in an article entitled "On the primitivity of certain Ore extensions."

REFERENCES

1. C. W. CURTIS, A note on non-commutative polynomial rings, *Proc. Amer. Math. Soc.* 3 (1952), 965–969.

2. A. Goldie and G. Michler, Ore extensions and polycyclic group rings, *J. London Math. Soc* (2) **9** (1974), 337–345.
3. O. Goldman, Hilbert rings and the Hilbert Nullstellensatz, *Math. Z.* **54** (1951), 136–140.
4. R. D. Hirsch, A note on non-commutative polynomial rings subject to degree-preservation, *J. London Math. Soc.* **42** (1967), 333–335.
5. R. Irving, "Prime Ideals of Skew Polynomial Rings," Ph. D. dissertation, Massachusetts Institute of Technology, February 1977.
6. N. Jacobson, "The Theory of Rings," American Mathematical Society, Providence, R. I., 1943.
7. M.-A. Knus and M. Ojanguren, "Théorie de la Descente et Algèbres d'Azumaya," Springer–Verlag, Berlin/Heidelberg/New York, 1974.
8. W. Krull, Jacobsonsche ringe, Hilbertscher Nullstellensatz, dimensionstheorie, *Math. Z.* **54** (1951), 354–387.
9. O. Ore, Theory of non-commutative polynomials, *Ann. of Math.* (2) **34** (1933), 480–508.
10. K. R. Pearson and W. Stephenson, A skew polynomial ring over a Jacobson ring need not be a Jacobson ring, *Comm. Algebra* **5** (1977), 783–794.
11. J. Watters, Polynomial extensions of Jacobson rings, *J. Algebra* **36** (1975), 302–308.