COLLOQUIUM MATHEMATICUM

VOL. 96 2003 NO. 1

A REPRESENTATION THEOREM FOR CHAIN RINGS

BY

YOUSEF ALKHAMEES, HANAN ALOLAYAN and SURJEET SINGH (Riyadh)

Abstract. A ring A is called a *chain ring* if it is a local, both sided artinian, principal ideal ring. Let R be a commutative chain ring. Let A be a faithful R-algebra which is a chain ring such that $\overline{A} = A/J(A)$ is a separable field extension of $\overline{R} = R/J(R)$. It follows from a recent result by Alkhamees and Singh that A has a commutative R-subalgebra R_0 which is a chain ring such that $A = R_0 + J(A)$ and $R_0 \cap J(A) = J(R_0) = J(R)R_0$. The structure of A in terms of a skew polynomial ring over R_0 is determined.

Introduction. Let S be a finite local ring. As shown by Wirt [8, Theorem 2.2] and independently by Clark and Drake [4], S has a commutative local subring S_0 such that $S = S_0 + J(S)$ and $S_0 \cap J(S) = pS_0$, where $p = \operatorname{char}(S/J(S))$. This subring is called a *coefficient subring* of S. A ring is called a *chain ring* if it is a local, both sided artinian and principal ideal ring. Wirt [8] gave a representation of a finite chain ring S in terms of a homomorphic image of a skew polynomial ring over its coefficient subring. On the other hand, Alkhamees and Singh [1] generalized the results on the existence of coefficient subrings of finite local rings to certain non-finite local rings.

Let R be a commutative chain ring, and A be a local ring that is a faithful R-algebra. Then $J(R) = R \cap J(A)$. Let $\overline{A} = A/J(A)$ be a separable, algebraic field extension of $\overline{R}$, and let A be either a locally finite R-algebra or an artinian *duo* ring. As proved in [1], A has a commutative local R-subalgebra R_0 such that $A = R_0 + J(A)$ and $J(R_0) = R_0 \cap J(A) = J(R)R_0$. This subalgebra R_0 is also called a *coefficient subring* of A; such a subring is a commutative chain ring, and is a faithful R-algebra. The group of R-automorphisms of R_0 is investigated in Section 2. Wirt [8] introduced the concept of a distinguished basis of a bimodule over a Galois ring. In Section 3 an analogous concept for bimodules over R_0 is investigated.

The main purpose of this paper is to prove a representation theorem for A, in case A is a chain ring, in terms of an appropriate homomorphic image of a skew polynomial ring over its coefficient subring. Sections 4 and 5 are devoted to proving the main theorem (Theorem 5.5). By Cohen [5], any

2000 *Mathematics Subject Classification*: Primary 16S35; Secondary 16P10, 16P20.

commutative local artinian ring admits a coefficient subring. We outline an example given in [2] to show that a non-commutative local ring need not admit a coefficient subring. For such a ring an analogue of Theorem 5.5 cannot be proved.

1. Preliminaries. All rings considered in the paper have $1 \neq 0$. Let S be any ring. Then $J(S)$, $Z(S)$ denote its *Jacobson radical* and *center* respectively. For any subset X of S, $\mathcal{C}(X)$ denotes its *centralizer* in S. For any module M, $d(M)$ denotes its *composition length*. For any automorphism σ of S, $S[x,\sigma]$ denotes the left skew polynomial ring over S determined by σ. Its members are left polynomials $\sum_i a_i x^i$, $a_i \in S$, and $xa = \sigma(a)x$ for every $a \in S$.

Let R be a commutative local ring and $\overline{R} = R/J(R)$. For any $f(x) \in R[x]$, let $\overline{f}(x)$ denote its natural image in $\overline{R}[x]$. The ring R is called a *Hensel ring* if it has the following property: Given any monic polynomial $f(x) \in R[x]$, if $\overline{f}(x) = a(x)b(x)$ for some relatively prime monic polynomials $a(x), b(x) \in \overline{R}[x]$, then there exist monic polynomials $g(x), h(x) \in R[x]$ such that $f(x) = g(x)h(x)$, $\overline{g}(x) = a(x)$ and $\overline{h}(x) = b(x)$. By the Hensel lemma [9, p. 279], any commutative, complete local ring R is a Hensel ring. In particular any commutative local artinian ring is a Hensel ring.

Let A be an algebra over R. If A_R is finitely generated, then A is called a *finite* R-algebra. The algebra A is called *faithful* if for any $r \in R$, $rA = 0$ implies that $r = 0$; in that case R is regarded a subring of A. Moreover, A is called *unramified* if $J(A) = J(R)A$; *R-separable* if it is a commutative, local, finite, faithful and unramified R-algebra such that $\overline{A} = A/J(A)$ is a finite separable field extension of $R/J(R)$; and *locally separable* if it is a local, faithful, unramified R-algebra such that any finite subset of A is contained in a separable R-subalgebra. If A is a locally separable R-algebra, then $\overline{A}$ is a separable, algebraic field extension of $\overline{R}$.

A commutative chain ring R is called a *special primary ring* [7, p. 200]. A finite special pimary ring S such that $J(S) = pS$, where $p = \mathrm{char}(S/J(S))$, is a *Galois ring* (see [4]). A ring S in which every one-sided ideal is two-sided is called a *duo* ring.

2. Ring monomorphisms

LEMMA 2.1. *Let R be a Hensel ring and A be a commutative, local, finite, faithful R-algebra such that $J(R) = R \cap J(A)$.*

(i) *A is a Hensel ring.*

(ii) *Let $f(x) \in R[x]$ be a monic polynomial such that $\overline{f}(x) \in \overline{R}[x]$ is irreducible and separable. If for some $c \in \overline{A}$, $\overline{f}(c) = 0$, then there exists a unique $a \in A$ such that $f(a) = 0$ and $\overline{a} = c$.*

Proof. For (i) see [3, Theorem 32]. For (ii), see [1, Lemma 2.1].

Let A be a separable algebra over a Hensel ring R. An element $a \in A$ is said to be *lift algebraic* over R if there exists a monic polynomial $f(x) \in R[x]$ such that $f(x)$ is irreducible modulo $J(R)$ and $f(a) = 0$; we call $f(x)$ an *associated polynomial* of a. Throughout this section R is a *special primary ring* with $J(R) = \pi R = R\pi$ and n is the *index of nilpotency* of π.

LEMMA 2.2. *Let A be a commutative, local, faithful, unramified R-algebra such that $\overline{A}$ is a separable algebraic field extension of $\overline{R}$.*

(I) *A is a special primary ring with index of nilpotency of $J(A)$ the same as that of $J(R)$.*

(II) *Let $a, b \in A$ be lift algebraic over R.*

- (i) *Let $f(x) \in R[x]$ be a monic polynomial such that $\bar{f}(x)$ is irreducible over $\overline{R}$. Then $T = R[x]/\langle f(x)\rangle$ is an unramified, local finite R-algebra. If, in addition, $\bar{f}(x)$ is separable over $\overline{R}$, then T is a separable R-algebra.*
- (ii) *If $f(x) \in R[x]$ is an associated polynomial of a, then $R[a] \cong R[x]/\langle f(x)\rangle$, $R[a]$ is a separable R-algebra and $d_R(R[a]) = n \deg f(x)$, where $n = d_R(R)$.*
- (iii) *If $\overline{a} = \overline{b}$, then $R[a] = R[b]$.*
- (iv) *$R[b] \subseteq R[a]$ if and only if $\overline{R}[\overline{b}] \subseteq \overline{R}[\overline{a}]$.*

(III) *If A is an R-separable algebra, then there exists a lift algebraic element $a \in A$ such that $A = R[a]$.*

Proof. We have $J(R) = \pi R$ and $J(A) = \pi A$. As n is the index of nilpotency of π, we see that A is a special primary ring such that the index of nilpotency of $J(A)$ is n. This proves (I).

To prove (II)(i), observe that $J(T) = \langle \pi, f(x)\rangle/\langle f(x)\rangle = \pi T$, and $T/J(T) \cong \overline{R}[x]/\langle \bar{f}(x)\rangle$. To prove (ii), let $g(x)$ be a non-zero member of $R[x]$ such that $g(a) = 0$ and $\deg g(x) < \deg f(x)$. We can write $g(x) = \pi^k h(x)$ such that $\deg g(x) = \deg h(x)$ and $h(x) \in R[x] \setminus J(R[x])$. Then $h(a) \in J(A)$. This contradicts the fact that $f(x)$ modulo $J(R)$ is the minimal polynomial of $\overline{a}$. Hence $R[a] \cong R[x]/\langle f(x)\rangle$. The last part of (ii) follows from (i). Let $\overline{a} = \overline{b}$, and let $g(x) \in R[x]$ be an associated polynomial of b. As $R[a]$ is a Hensel ring, there exists $c \in R[a]$ such that $g(c) = 0$ and $\overline{c} = \overline{b}$. By 2.1, $b = c$. Since $R[a]$ and $R[b]$ have the same composition length as R-modules, we get $R[a] = R[b]$. Similar arguments prove (II)(iv).

In case A is a separable R-algebra, $\overline{A}$ is a simple extension of $\overline{R}$: for some lift algebraic element $a \in A$, $\overline{A} = \overline{R}[\overline{a}]$. Hence $A = R[a]$. This proves (III).

LEMMA 2.3. *Let A be a commutative, local, faithful unramified R-algebra such that $\overline{A}$ is a separable algebraic field extension of $\overline{R}$.*

(i) *For any subfield F of $\overline{A}$ is a finite extension of $\overline{R}$, there exists a unique R-separable subalgebra S of A such that $F = \bar{S}$. Further, there exists a lift algebraic element $a \in S$ such that $S = R[a]$.*

(ii) *For any subfield F of $\overline{A}$ containing $\overline{R}$, there exists a unique locally R-separable subalgebra S of A such that $\bar{S} = F$.*

Proof. (i) We have $F = \overline{R}[c]$ for some $c \in F$. Let $f(x) \in R[x]$ be a monic polynomial which modulo $J(R)$ is the minimal polynomial of c over $\overline{R}$. As A is a Hensel ring we get an $a \in A$ such that $f(a) = 0$ and $\overline{a} = c$. As in 2.2, $R[a]$ is an R-separable subalgebra isomorphic to $R[x]/\langle f(x)\rangle$. Put $S = R[a]$. Clearly $F = \bar{S}$. Let T be another such R-separable subalgebra of A. By 2.2(III) there exists $b \in T$ lift algebraic over R such that $T = R[b]$. As $\overline{R}[\overline{a}] = \overline{R}[\overline{b}]$, by 2.2(II)(iii) we have $R[a] = R[b]$, so $S = T$. This proves (i).

(ii) Let F be any subfield of $\overline{A}$ containing $\overline{R}$. Then $\overline{F}$ is a directed union of simple field extensions of $\overline{R}$. Apply (i) to complete the proof.

Lemma 2.4. *Let A be a commutative, local, faithful unramified R-algebra such that $\overline{A}$ is a separable algebraic field extension of $\overline{R}$. Let $a, b \in A$ be lift algebraic over R.*

(i) *There exists a $c \in A$ lift algebraic over R such that $R[a]+R[b] \subseteq R[c]$.*

(ii) *A is the union of all the subrings of the form $R[a]$, where a runs over all the elements of A that are lift algebraic over R.*

(iii) *A is a locally separable R-algebra.*

(iv) *If A' is a locally separable A-algebra, then A' is a locally separable R-algebra.*

Proof. As $\overline{a}$, $\overline{b}$ are both separable over $\overline{R}$, there exists a lift algebraic element $c \in A$ such that $\overline{R}[\overline{a}, \overline{b}] = \overline{R}[\overline{c}]$. Then 2.2(II)(iv) completes the proof of (i).

Let B be the union of all the subrings of A of the form $R[a]$, where a is any element of A lift algebraic over R. (i) shows that B is a subring and $\overline{B} = \overline{A}$. So $A = B + J(A) = B + \pi A$, as $J(R) = \pi R$. As π is nilpotent, we get $A = B$. This proves (ii); and (iii) is immediate from (ii).

For (iv), the hypothesis on A' gives $J(A') = J(A)A' = J(R)A'$, so A' is an unramified R-algebra. Also $\overline{A'}$ is a separable field extension of $\overline{R}$. Now (iii) completes the proof.

Theorem 2.5. *Let A and A' be two commutative, local, faithful, unramified algebras over a special primary ring R such that $\overline{A}$ and $\overline{A'}$ are both separable field extensions of $\overline{R}$. If there exists an $\overline{R}$-monomorphism $\sigma : \overline{A} \to \overline{A'}$, then σ has a unique lifting to an R-monomorphism $\eta : A \to A'$. Further, η is an automorphism if and only if σ is an automorphism.*

Proof. Consider any $a, b \in A$ lift algebraic over R. Let $f(x), g(x) \in R[x]$ be associated polynomials of a, b respectively. Now $\bar{f}(\overline{a}) = 0$ gives

$\bar{f}(\sigma(\overline{a})) = 0$. So we can find a unique $a' \in A'$ for which $f(a') = 0$ and $\overline{a'} = \sigma(\overline{a})$. But $R[a] \cong R[x]/\langle f(x)\rangle \cong R[a']$, so we get an R-isomorphism $\lambda_a : R[a] \to R[a']$ such that $\lambda_a(a) = a'$. Then $\overline{\lambda_a(a)} = \sigma(\overline{a})$. So λ_a lifts the restriction of σ to $\overline{R}[\overline{a}]$. Similarly, for b we get $b' \in A'$ such that $g(b') = 0$, $\overline{b'} = \sigma(\overline{b})$ and we have an R-isomorphism $\lambda_b : R[b] \to R[b']$ such that $\lambda_b(b) = b'$. Suppose $\overline{R}[\overline{a}] \subseteq \overline{R}[\overline{b}]$. Then $R[a] \subseteq R[b]$. Now $\overline{\lambda_b(a)} = \sigma(\overline{a})$ and $f(\lambda_b(a)) = 0 = f(a')$. This gives $\lambda_b(a) = \lambda_a(a)$. Hence λ_b is an extension of λ_a. As A is the union of all $R[a]$, where a is any element of A lift algebraic over R, the union of the maps λ_a gives the desired monomorphism $\eta : A \to A'$ which lifts σ. Clearly η is uniquely determined by σ. By using the arguments in the proof of 2.4(ii) it follows that η is an isomorphism if and only if σ is an isomorphism.

The following is immediate.

COROLLARY 2.6. *Let A, A' be two commutative, local, faithful unramified algebras over a special primary ring R such that $\overline{A}$ and $\overline{A'}$ are both separable algebraic field extensions of $\overline{R}$, let G be the set of all R-monomorphisms of A into A', and let $\overline{G}$ be the set of all $\overline{R}$-monomorphisms of $\overline{A}$ into $\overline{A'}$. Then there is a one-to-one correspondence between G and $\overline{G}$ given by $\eta \leftrightarrow \overline{\eta}$, where $\overline{\eta} \in \overline{G}$ is induced by $\eta \in G$. If $A = A'$, then this correspondence induces an isomorphism between* $\mathrm{Aut}_R(A)$ *and* $\mathrm{Aut}_{\overline{R}}(\overline{A})$.

THEOREM 2.7. *Let A be a commutative, local, faithful unramified algebra over a special primary ring R such that $\overline{A}$ is a separable, algebraic field extension of $\overline{R}$.*

(a) $\mathrm{Aut}_R(A) \cong \mathrm{Aut}_{\overline{R}}(\overline{A})$.

(b) *Let $\sigma : A \to A$ be an R-monomorphism.*

- (i) *σ is an automorphism of A and for any $b \in A$ lift algebraic over R, $b \in A^\sigma$ if and only if $\overline{b} \in \overline{A}^{\overline{\sigma}}$.*
- (ii) *The fixed ring A^σ of σ is a local, unramified R-algebra. If the order of σ is a positive integer k, then $[\overline{A} : \overline{A^\sigma}] = k$ and $A = A^\sigma[c]$ for some c lift algebraic over A^σ. The fixed ring of $\overline{\sigma}$ equals $\overline{A^\sigma}$.*

Proof. (a) is given in 2.6.

(b) Consider any finite subset T of $\overline{A}$. By adjoining all the conjugates of elements in T over $\overline{R}$, in $\overline{A}$, we get a finite set T' containing T such that $\eta(\overline{R}[T']) = \overline{R}[T']$ for any R-monomorphism $\eta : \overline{A} \to \overline{A}$. This in particular gives $\overline{\sigma}(\overline{A}) = \overline{A}$. Thus $\sigma(A) = A$, and hence σ is an automorphism. Let $b \in A$ be lift algebraic over R such that $\overline{b} \in \overline{A}^{\overline{\sigma}}$. Let $f(x) \in R[x]$ be an associated polynomial of b. Then $f(b) = 0$ gives $f(\sigma(b)) = 0$. But $\overline{b} = \overline{\sigma}(\overline{b})$. By 2.1, $b = \sigma(b)$. This proves (i).

Every finite separable field extension of $\overline{R}$ is simple. Let S be the set of all those $a \in A$ such that a is lift algebraic over R, and $\eta(R[a]) = R[a]$ for every

$\eta \in \mathrm{Aut}_R(A)$. Then $A = \bigcup_{a\in S} R[a]$. Now $\overline{R}[\overline{a}]^{\overline{\sigma}} = \overline{R}[\overline{b}_a]$ for some $b_a \in R[a]$ lift algebraic over R. It follows by using 2.4(i) that $A' = \bigcup_{a\in S} R[b_a]$ is an unramified local R-algebra, and $A' \subseteq A^\sigma$. Let $c \in A^\sigma$. Then $c \in R[a]$ for some $a \in S$. Thus for some $c_1 \in R[b_a]$ lift algebraic over $\overline{R}$, $\overline{c} = \overline{c}_1$ and $c = c_1 + \pi^r u_1$ for some $r > 0$ and a unit $u_1 \in R[a]$. If $\pi^r u_1 = 0$, we get $c \in A'$. Suppose $\pi^r u_1 \neq 0$. As $\pi^r u_1 \in A^\sigma$, we get $\pi^r(\sigma(u_1) - u_1) = 0$, so $\overline{u}_1 \in \overline{R}[\overline{b}_a]$. As for c, we get $u_1 = c_2 + \pi^s u_2$ for some $c_2 \in R[b_a]$, $s > 0$ and u_2 some unit in $R[a]$. Then $c = c_1 + \pi^r c_2 + \pi^{r+s} u_2$ and $r + s > r$. Continue the process with u_2 and so on. As π is nilpotent, we eventually get $c \in A'$. Clearly, A is unramified over A^σ. Suppose that the order of σ is a positive integer k; then so is the order of $\overline{\sigma}$. Consequently, $[\overline{A} : \overline{A^\sigma}] = k$. By 2.2(III), $A = A^\sigma[c]$ for some $c \in A$ lift algebraic over A^σ. Clearly $\overline{A^\sigma} \subseteq A''$, the fixed ring of $\overline{\sigma}$. Let $y \in A''$. Then for some $a \in S$, $y \in \overline{R}[\overline{b}_a]$. As $R[b_a]$ is R-separable, $y = \overline{c}$ for some $c \in R[b_a] \subseteq A^\sigma$. This proves the result.

3. Distinguished basis. Throughout this section R is a special primary ring and A is a commutative, locally separable R-algebra. Let H be the set of all R-subalgebras of A of the form $R[a]$ such that $a \in A$ is any element lift algebraic over R. By 2.4, H is an upper semi-lattice, and the union of members of H is A. Observe that any $R[a] \in H$ is projective as an R-module, so A_R is flat. As $J(R[a]) = J(R)[a]$ for each $R[a] \in H$, we have $J(A) = J(R)A$, i.e. A is an unramified R-algebra. Let $T = A \otimes_R A$. Then for any $R[a] \in H$, $T_a = A \otimes_R R[a] \subseteq T$ and T is the union of the set of all such subrings. The concept of a distinguished basis of a bimodule over a Galois ring is discussed by Wirt [8]. The results in this section are related to those by Wirt, but in contrast to [8], the underlying rings need not be finite. Also, there is a marked difference between the proofs in [8] and of similar results in this section. Any (A, A)-bimodule M is supposed to be such that $rx = xr$ for any $x \in M$ and $r \in R$.

LEMMA 3.1. *Let $a \in A$ be lift algebraic over R.*

(i) *$T_a = A \otimes_R R[a]$ is a finite direct sum of local rings each of which is a separable A-algebra* (*so also a locally separable R-algebra*)*. Further, T_a is an artinian principal ideal ring and $J(T_a) = J(R)T_a$. If $\overline{A}$ is a normal extension of $\overline{R}$, then T_a is a direct sum of copies of A.*

(ii) *For any maximal ideal P of T there is no ideal L of T such that $P^2 < L < P$. For any ideal C of T for which T/C is artinian, T/C is a principal ideal ring.*

(iii) *$J(T) = J(R)T$.*

Proof. (i) Let $f(x) \in R[x]$ be an associated polynomial of a. As A is a Hensel ring, $f(x) = \prod_{i=1}^t f_i(x)$ with each $f_i(x)$ monic, and modulo $J(A)$

irreducible over $\bar{A}$. Then

$$A \otimes_R R[a] \cong A \otimes_R R[x]/\langle f(x)\rangle \cong A[x]/\langle f(x)\rangle \cong \prod_{i=1}^{t} A[x]/\langle f_i(x)\rangle.$$

Now each $A[x]/\langle f_i(x)\rangle$ is a separable A-algebra. As A is an unramified R-algebra, by 2.4(iv), $A[x]/\langle f_i(x)\rangle$ is R-unramified. This gives $J(T_a) = J(R)T_a$. That T_a is a principal ideal ring follows from the fact that any locally separable R-algebra is a principal ideal ring. If $\bar{A}$ is a normal extension of $\overline{R}$, then each $f_i(x)$ is of degree one, so each $A[x]/\langle f_i(x)\rangle$ is isomorphic to A.

Suppose that, on the contrary, L is an ideal of T such that $P^2 < L < P$. For any $R[a] \in H$ let $P_a = P \cap T_a$ and $L_a = L \cap T_a$. As T_a is a principal ideal ring, there is no ideal of T_a properly between P_a and $(P_a)^2$. So $L_a = P_a$ or $L_a = P^2 \cap T_a$. The hypothesis implies that there exist $R[a], R[b] \in H$ such that $L_a \neq P^2 \cap T_a$ and $L_b \neq P_b$. Now there exists $R[c] \in H$ such that $R[a] \cup R[b] \subseteq R[c]$. Then $T_a \cup T_b \subseteq T_c$. If $L_c = P^2 \cap T_c$, then $L_a = P^2 \cap T_a$; if $L_c = P_c$, then $L_b = P_b$. This is a contradiction. Let C be any ideal of T such that T/C is artinian. Then for any prime ideal Q of T/C there is no ideal of T/C properly between Q and Q^2. Hence T/C is a principal ideal ring [7, Theorem 39.2].

(iii) follows from (i).

THEOREM 3.2. *Let A be a locally separable algebra over a special primary ring R, and M be an (A, A)-bimodule such that $d(_AM)$ is finite. Then $M = \oplus \sum_{i=1}^{n} A_i x_i$ with each A_i a separable A-algebra, and there exist R-monomorphisms $\sigma_i : A \to A_i$ such that $x_i a = \sigma_i(a)x_i$ for any $a \in A$. In case $\bar{A}$ is a normal extension of $\overline{R}$, each A_i can be taken to be A and each σ_i an R-automorphism of A.*

Proof. Let $T = A \otimes_R A$. Then M is a left T-module such that $(a \otimes b)x = axb$ for any $a, b \in A$ and $x \in M$. Then $d(_TM)$ is also finite. So there exists an ideal C of T such that T/C is artinian and $CM = 0$. As T/C is an artinian principal ideal ring, $M = \oplus \sum_{i=1}^{n} Tx_i$, where each Tx_i is a non-zero uniserial module [6, Theorem 25.4.2]. Consider any $x \in M$. For any $R[a] \in H$, $(A \otimes_R R[a])x = T_a x$ is a left A-submodule of Tx. There exists an $R[c] \in H$ such that $T_c x$ has maximal composition length as left A-module among all submodules $T_a x$. As T is the union of all the T_a's it follows from 2.4(i) that $Tx = T_c x$. For any $u \in T_c$, $T(ux) = u(Tx) = uT_c x = T_c(ux)$. This shows that any T_c-submodule of Tx is also a T-submodule. In addition, suppose that Tx is uniserial. Then Tx is also a uniserial T_c-module. By 3.1, T_c is a direct sum of rings which are separable A-algebras. This gives a summand A' of T_c such that A' is a separable A-algebra, $Tx = A'x$ and every A'-submodule of $A'x$ is a T-submodule. Hence for $1 \leq i \leq n$ we get

A-subalgebras A_i of T such that each A_i is a separable A-algebra and $Tx_i = A_i x_i$. Let $J(R) = \pi R$. Then $J(A) = \pi A$ and $J(A') = \pi A'$. For any $x \in M$, $x\pi = \pi x$. This gives that $D_i = \mathrm{r.ann}_A(x_i) = \pi^{k_i} A$ and $D_i' = \mathrm{l.ann}_{A_i}(x_i) = A_i \pi^{k_i}$. Consider $a \in A$; as $x_i a \in T x_i = A_i x_i$ there exists $a' \in A_i$ such that $x_i a = a' x_i$. This gives an R-monomorphism $\eta_i : A/D_i \to A_i/D_i'$ such that $\eta_i(a + D_i) = a' + D_i'$. By 2.5, η_i uniquely lifts to an R-monomorphism $\sigma_i : A \to A_i$. Clearly $x_i a = \sigma_i(a) x_i$ for every $a \in A$.

Let $\overline{A}$ be a normal extension of $\overline{R}$. By 3.1(i) each A_i is a copy of A, so $A_i = Ae_i$ for some indecomposable idempotent e_i in T, and $\sigma_i(a) = \eta_i(a)e_i$ for some R-automorphism η_i of A. Hence $M = \oplus \sum_{i=1}^{n} Ay_i$ with $y_i = e_i x_i$ and $y_i a = \eta_i(a) y_i$. This proves the result.

In case $\overline{A}$ is a normal extension of R, and M is an (A, A)-bimodule as in the above theorem, it follows from the above theorem that there exist finitely many distinct R-automorphisms $\sigma_1, \ldots, \sigma_s$ such that $M = N_1 \oplus \ldots \oplus N_s$ for some non-zero submodules N_i with the property that for any non-zero $x \in N_i$, $xa = \sigma_i(a)x$ for every $a \in A$.

COROLLARY 3.3. *Let A and T be as in the above theorem and $A/J(A)$ be a normal field extension of $\overline{R}$. Let M be an (A, A)-bimodule such that $d({}_A M) < \infty$.*

(i) *There exist uniquely determined R-automorphisms $\sigma_1, \ldots, \sigma_s$ of A such that for $1 \le i \le s$, $N_i = \{x \in M : xa = \sigma_i(a)x$ for every $a \in A\}$ is a non-zero submodule of M and $M = N_1 \oplus \ldots \oplus N_s$.*

(ii) *If the module ${}_T M$ is uniserial, then ${}_A M$ is uniserial.*

Proof. We have $M = N_1 \oplus \ldots \oplus N_s$ for some non-zero submodules N_i and distinct R-automorphisms σ_i of A such that $ya = \sigma_i(a)y$ for $y \in N_i$, $a \in A$. Suppose that for some R-automorphism η of A there exists a non-zero $x \in M$ such that $xa = \eta(a)x$ for every $a \in A$. Write $x = \sum x_i$, $x_i \in N_i$. Then $xa = \eta(a)x$ gives $\sum \eta(a)x_i = \sum \sigma_i(a)x_i$. For some j, $x_j \neq 0$. Then $(\eta(a) - \sigma_i(a))x_j = 0$ gives $\eta(a) - \sigma_j(a) \in J(A)$ for every $a \in A$. By 2.7(a), $\eta = \sigma_j$, and hence $x \in N_j$. This proves (i).

It has been seen in the proof of the above theorem that M is a direct sum of uniserial T-modules each of which is a uniserial left A-module. Hence, if M is a uniserial T-module it must be a uniserial left A-module.

Let S be a faithful R-algebra such that $\bar{S} = S/J(S)$ is a countably generated separable algebraic field extension of $\overline{R}$. If S is locally finite or is an artinian *duo* ring, then S has a coefficient subring T which is unique to within isomorphisms [1]. In particular any finite local ring S of characteristic p^n, where p is a prime number, can be regarded as an algebra over $\mathbb{Z}/\langle p^n \rangle$, so it has a coefficient subring T; this T is a Galois ring of order p^{nr} where the order of $S/J(S)$ is p^r.

THEOREM 3.4. *Let* (R,π) *be any special primary ring and* S *be a left artinian, faithful* R*-algebra such that* $\overline{S} = S/J(S)$ *is a countably generated, separable normal algebraic field extension of* $\overline{R}$. *Let* S *have a coefficient subring* R_0. *Then as an* (R_0,R_0)*-bimodule,* $S = R_0 \oplus (\oplus \sum_{i=1}^{n} R_0x_i)$ *such that for* $1 \leq i \leq n$, $x_i \in J(S)$ *and there exists a* $\sigma_i \in \mathrm{Aut}_R(R_0)$ *such that* $x_ia = \sigma_i(a)x_i$ *for every* $a \in A$. *These automorphisms are uniquely determined by* S.

Proof. (R_0,π) is a special primary ring and $d({}_{R_0}S) = d({}_SS)$. We regard S as an (R_0,R_0)-bimodule. Consider any unit $x \in S$ such that for some $\sigma \in \mathrm{Aut}_R(R_0)$, $xa = \sigma(a)x$ for every $a \in R_0$. But in $\bar{S}$, $\overline{xa} = \overline{ax}$, so $(\overline{a}-\overline{\sigma(a)})\overline{x} = \overline{0}$. Thus $a-\sigma(a) \in J(R_0)$ for every $a \in R_0$. By 2.7, $\sigma = I$, hence $x \in \mathcal{C}(R_0)$, the centralizer of R_0. By 3.3, there exist uniquely determined distinct R-automorphisms η_j, $1 \leq j \leq m$, such that $S = \oplus \sum_{i=1}^{m} B_i$ where $B_i = \{x \in S : xa = \eta_i(a)x \text{ for all } a \in R_0\} \neq 0$. For $x \in R_0$ and $a \in R_0$, $xa = ax$, so 3.3(i) shows that one of the η_i, say η_1, equals I. Then $B_1 = \mathcal{C}(R_0)$, and $S = \mathcal{C}(R_0) \oplus H$, where $H = \sum_{i>1} B_i$. For any $i \geq 2$, as seen above, no B_i can contain any unit of S. Thus $H \subseteq J(S)$. Now R_0 is self-injective (see [6]). By [6, Theorem 25.4.2], $\mathcal{C}(R_0) = R_0 \oplus (\oplus \sum_{j=1}^{p} R_0y_i)$. Suppose some y_i, say y_1, is a unit. Now $y_1 = z_1 + v_1$ for some $z_1 \in R_0$ and $v_1 \in J(S) \cap \mathcal{C}(R_0)$ with $R_0 \oplus R_0y_1 = R_0 + R_0v_1$. By comparing the composition lengths over R_0, it is immediate that $R_0 \oplus R_0y_1 = R_0 \oplus R_0v_1$. Thus we can take every y_i in $J(S)$. As each B_i is also a direct sum of uniserial R_0-modules, the result follows.

4. Chain rings. We start with the following elementary result.

LEMMA 4.1. (i) *Let* σ *be an automorphism of a ring* R *and* $f(x) \in R[x,\sigma]$ *be such that its leading coefficient is a unit, and* $\deg f(x) = n \geq 1$. *Then for any* $g(x) \in R[x]$, *we have* $g(x) = f(x)q(x) + r(x)$ *for some* $q(x), r(x) \in R[x]$ *with* $\deg r(x) < \deg f(x)$. *Further,* $R[x,\sigma]/f(x)R[x,\sigma]$ *as a right* R*-module is a direct sum of* n *copies of* R.

(ii) *Let* σ *be an automorphism of a division ring* D. *Then the left skew polynomial ring* $D[x,\sigma]$ *is a right as well as a left principal ideal domain.*

Henceforth R is a commutative local ring with maximal ideal J, and σ an automorphism of R. If J is nilpotent, it is obvious that $J[x,\sigma]$ is a nilpotent ideal of $R[x.\sigma]$.

LEMMA 4.2. *If* J *is nil and* σ *is of finite order, then the ideal* $J[x,\sigma]$ *of* $R[x,\sigma]$ *is nil.*

Proof. Consider any $f(x) \in J[x,\sigma]$, and let Y be the set consisting of all coefficients of $f(x)$ and their images under different powers of σ. As σ is of finite order, Y is a finite set, so the ideal A of R generated by Y is nilpotent. Clearly any coefficient of an $f(x)^k$ is in A^k. Hence $f(x)$ is nilpotent.

LEMMA 4.3. *Let* $f(x) = x^k + g(x)$ *be such that* $g(x) \in J[x,\sigma]$ *and* $\deg g(x) < k$, k *a positive integer, and* $\langle f(x)\rangle = f(x)R[x,\sigma]$.

(i) $\langle J,x\rangle/\langle f(x)\rangle$ *is the unique maximal ideal of* $S = R[x,\sigma]/\langle f(x)\rangle$.

(ii) *If* $J[x,\sigma]$ *is a nil ideal, then* S *is a local ring with* $J(S)$ *equal to* $\langle J,x\rangle/\langle f(x)\rangle$.

(iii) *If* R *is a special primary ring with* $J = \pi R$ *and* $g(x) = \pi u(x)$, *where the constant term of* $u(x)$ *is a unit, then* S *is a chain ring with* $J(S) = \langle \overline{x}\rangle$, *and the index of nilpotency of* $J(S)$ *is* kn, *where* n *is the index of nilpotency of* π. *Also,* $\pi^{n-1} \notin \langle f(x)\rangle$. *Further, for any positive integer* $m \le kn$, $T = R[x,\sigma]/\langle f(x), x^m\rangle$, *and the index of nilpotency of* $J(T)$ *is* m.

Proof. Set $B = \langle J,x\rangle$. As $R[x,\sigma]/B \cong R/J$ is a field, clearly $L = B/\langle f(x)\rangle$ is a maximal ideal of S. Let $h(x) \in R[x,\sigma]$ be such that $h(x) \notin B$. Then $\langle h(x)\rangle + B = R[x,\sigma]$, hence $\langle h(x)\rangle + B^k = R[x,\sigma]$. But $B^k \subseteq \langle J, x^k\rangle = \langle J, f(x)\rangle$, so $\langle h(x)\rangle + \langle J, f(x)\rangle = R[x,\sigma]$. Thus for $T = R[x,\sigma]/C$, where $C = \langle h(x)\rangle + \langle f(x)\rangle$, we have $TJ = T$. It follows from 4.1 that T is finitely generated as a right R-module. Thus, by [3, Theorem 5], $T = 0$. Hence $\langle h(x)\rangle + \langle f(x)\rangle = R[x,\sigma]$. This proves that $B/\langle f(x)\rangle$ is the only maximal ideal of S.

Let $J[x,\sigma]$ be nil. Then as $B^k \subseteq \langle J, f(x)\rangle$, $B/\langle f(x)\rangle$ is a nil ideal. Hence S is a local ring with $J(S) = B/\langle f(x)\rangle$.

Let R be a special primary ring with $J = \pi R$ and $g(x) = \pi u(x)$ with the constant term of $u(x)$ a unit. As J is nilpotent, so is $J[x,\sigma]$. Consequently, S is a local ring. Since $u(x)$ is a unit modulo $f(x)$, it follows that $\overline{\pi}S = \overline{x}^k S$ and $J(S) = \overline{x}S$. So S is a chain ring. It follows from 4.1 that $d(S_R) = kn$. As R/J and $S/J(S)$ are isomorphic as right R-modules, $d(S_S) = kn$. Hence the index of nilpotency of $J(S)$ is kn. This also yields $\pi^{n-1} \notin \langle f(x)\rangle$. The last part of (iii) follows from the fact that T is a homomorphic image of S and $J(S) = \overline{x}S$.

LEMMA 4.4. *Let* J *be nilpotent and let* $f(x) = x^k + g(x)$ *with* k *a positive integer, and* $g(x) \in J[x,\sigma]$ *be such that* $\langle f(x)\rangle = f(x)R[x,\sigma]$. *Then there exists an* $h(x) = x^k + q(x) \in R[x,\sigma]$ *with* $q(x) \in J[x,\sigma]$, $\deg q(x) < k$, $\langle f(x)\rangle = \langle h(x)\rangle = h(x)R[x,\sigma]$. *If the constant term of* $g(x)$ *belongs to* $J\backslash J^2$ *then* $h(x)$ *can also be chosen so that the constant term of* $h(x)$ *is in* $J\backslash J^2$.

Proof. Consider $A = \langle J, f(x)\rangle = \langle J, x^k\rangle$ and $S = R[x,\sigma]/\langle f(x)\rangle$. Then $SJ = A/\langle f(x)\rangle$, so $S/SJ \cong R[x,\sigma]/\langle J, x^k\rangle$ as right R-modules. So $\{x^i + SJ : 0 \le i \le k-1\}$ generates S/SJ as a right R-module. As J is nilpotent, it follows that S_R itself is generated by the set $\{x^i + \langle f(x)\rangle : 0 \le i \le k-1\}$. So there exists $h(x) = x^k - \sum_{i=0}^{k-1} a_i x^i \in \langle f(x)\rangle$ with $a_i \in R$. Then $h(x) =$

$(x^k + g(x))v(x)$ for some $v(x) \in R[x,\sigma]$. In $\overline{R[x,\sigma]} = R[x,\sigma]/J[x,\sigma]$, $\overline{h(x)} = \overline{x}^k\overline{v(x)}$. This gives $\overline{v(x)} = \overline{1}$ and $\overline{h(x)} = \overline{x}^k$. It follows that $v(x) = 1 + w(x)$ with $w(x) \in J[x,\sigma]$ and $\sum_{i=0}^{k-1} a_i x^i \in J[x,\sigma]$. As $v(x)$ is a unit in $R[x,\sigma]$, it is immediate that $\langle f(x)\rangle = h(x)R[x,\sigma] = \langle h(x)\rangle$. Finally, let the constant term of $g(x)$ be $b \in J\backslash J^2$. Then b is also the constant term of $f(x)$. If $c \in J$ is the constant term of $w(x)$, then the constant term of $h(x)$ is $b(1+c) \in J\backslash J^2$. This proves the result.

Lemma 4.5. *Let J be nilpotent, $f(x) = x^k + g(x) \in R[x,\sigma]$ with k a positive integer, and $g(x) \in J[x,\sigma]$ such that $\langle f(x)\rangle = f(x)R[x,\sigma]$. Then $R[x,\sigma]/\langle f(x)\rangle$ as a right R-module is isomorphic to a direct sum of k copies of R.*

Proof. Because of 4.4 we can take $\deg g(x) < k$. Now apply 4.1 to complete the proof.

Henceforth R is a special primary ring with $J = \pi R$, the index of nilpotency of J is n, and σ is such that $\sigma(\pi) = \pi$.

Lemma 4.6. *Let $f(x) \in R[x,\sigma]$ be such that its constant term or its leading coefficient is a unit in R. If $g(x) \in R[x,\sigma]$ is such that $f(x)g(x) \in \pi^s R[x,\sigma]$ for some non-negative integer s, then $g(x) \in \pi^s R[x,\sigma]$.*

Proposition 4.7. *Let $f(x) = x^k + \pi g(x) \in R[x,\sigma]$ be such that $\langle f(x)\rangle = f(x)R[x,\sigma]$ and the constant term of $g(x)$ is a unit in R. Then $S = R[x,\sigma]/\langle f(x)\rangle$ is a chain ring such that $J(S) = \langle\overline{x}\rangle$, and the index of nilpotency of $J(S)$ is kn, where n is the index of nilpotency of J. For $1 \le m \le kn$, $A = R[x,\sigma]/\langle f(x), x^m\rangle$ is a chain ring with m as the index of nilpotency of $J(A)$.*

Proof. Because of 4.4 we can take $\deg g(x) < k$. Then 4.3 completes the proof of the first part. The second part is an immediate consequence of the first part.

Proposition 4.8. *Let $f(x) = x^k + \pi g(x) + r_0 x^{m-1} \in R[x,\sigma]$ with $m - 1 > k > 0$ and with constant term of $g(x)$ a unit in R. Then $T = R[x,\sigma]/\langle f(x), x^m\rangle$ is a chain ring with $J(T) = \langle\overline{x}\rangle$. The index of nilpotency of $J(T)$ is at most kn.*

Proof. Set $A = \langle f(x), x^m\rangle$. Then $T = R[x,\sigma]/A$ and $A \subseteq \langle \pi, x\rangle$. As $\overline{x}$ is nilpotent in T, T is a local ring with $J(T) = \langle\overline{\pi}, \overline{x}\rangle$ a nilpotent ideal. As $\overline{1 + r_0 x^{m-k-1}}$ and $\overline{g(x)}$ are units in T,

$$\langle\overline{x}^k\rangle = \langle\overline{x^k + r_0 x^{m-1}}\rangle = \langle -\overline{\pi}\,\overline{g(x)}\rangle = \langle\overline{\pi}\rangle.$$

Thus the index of nilpotency of $\overline{x}$ is at most kn and $J(T) = \langle\overline{x}\rangle$.

Lemma 4.9. *Let $h(x) = x^k + \pi g(x) \in Z(R[x,\sigma])$ be such that the constant term of $g(x)$ is a unit and $\deg g(x) < k$. Let m be any positive integer* *such that* $k \le m-1 \le kn-1$, *and suppose the order of* σ *divides* $m-1$. *Let* $f(x) = h(x) + r_0 x^{m-1}$, *where* r_0 *is a unit in* R. *Then*:

(i) *If* $m-1 > k$, *then* $\langle f(x), x^m\rangle \neq \langle f(x), x^{m-1}\rangle$.

(ii) *If* $k = m-1$ *and* $1+r_0$ *is a unit*, *then* $\langle f(x),\, x^m\rangle \neq \langle f(x), x^{m-1}\rangle$.

Proof. Suppose the contrary. Set $A = \langle f(x), x^{m-1}\rangle = \langle h(x), x^{m-1}\rangle$ and $B = \langle f(x), x^m\rangle$.

Case I: $k < m-1$. So $x^{m-1} = (h(x) + r_0 x^{m-1})s(x) + x^m v(x)$ for some $s(x), v(x) \in R[x,\sigma]$. This gives $x^{m-1}(1-r_0 s(x)) = h(x)s(x) + x^m v(x)$. If $1 - r_0 s(x)$ is a unit modulo the ideal $C = \langle h(x), x^m\rangle$, we deduce that $x^{m-1} \in C$, and the index of nilpotency of the radical of $R[x,\sigma]/C$ is less than m. This contradicts 4.3(iii). Hence the constant term of $1 - r_0 s(x)$ is a non-unit. Thus, if s_0 is the constant term of $s(x)$, then s_0 must be a unit. Also the coefficient of x^k in $h(x)s(x) + x^m v(x)$ is 0. Thus $s_0 - \pi b = 0$ for some $b \in R$ and $s_0 \in J(R)$. This is a contradiction, which proves (i).

Case II: $k = m-1$ and $1+r_0$ is a unit. In this case $\pi g(x)s(x) \in \langle x^{m-1}\rangle$. By 4.6, $\pi s(x) = x^{m-1}\pi q(x)$. So $s(x) = x^{m-1}q(x) + \pi^{n-1}\lambda(x)$ for some $\lambda(x) \in R[x,\sigma]$. Thus

$$\begin{aligned} x^{m-1} &= (x^{m-1} + \pi g(x) + r_0 x^{m-1})(x^{m-1}q(x) + \pi^{n-1}\lambda(x)) + x^m v(x)\\ &= x^{m-1}(1+r_0)(x^{m-1}q(x) + \pi^{n-1}\lambda(x)) + x^{m-1}\pi g(x)q(x) + x^m v(x). \end{aligned}$$

Consequently, $1 = (1+r_0)(x^{m-1}q(x) + \pi^{n-1}\lambda(x)) + \pi g(x)q(x) + xv(x)$. This is not possible, as the constant term on the right hand side is not a unit. This proves (ii).

Remark. The hypothesis on $h(x)$ in the above theorem implies that $o(\sigma)$ divides k and $\pi g(x) \in Z(R[x,\sigma])$.

Theorem 4.10. *Let* (R,π) *be a special primary ring and* σ *be an automorphism of* R *of order* k', *a positive integer. Let* $h(x) = x^k + \pi g(x) \in Z(R[x,\sigma])$ *be such that the constant term of* $g(x)$ *is a unit in* R *and* $\deg g(x) < k$. *Let* m *be any positive integer such that* $k(n-1) < m \le kn$, $k \le m-1$ *and* k' *divides* $m-1$. *Let* $f(x) = h(x) + r_0 x^{m-1} \in R[x,\sigma]$ *with* $r_0 \in R$ *satisfying the following conditions*:

(i) *Either* $r_0 = 0$ *or* r_0 *is a unit.*

(ii) *If* $k = m-1$, *then* $1 + r_0$ *is a unit.*

Then for $A = \langle f(x), x^m\rangle$, $S = R[x,\sigma]/A$ *is a chain ring with* $J(S)$ *having index of nilpotency* m.

Proof. For $r_0 = 0$, the result follows from 4.3(iii). For $r_0 \neq 0$, it follows from 4.8 and 4.9.

5. A representation theorem. Throughout this section (R,π) is a special primary ring, A is a local, faithful R-algebra which is a chain ring, $J(R) = R \cap J(A)$, and $\overline{A} = A/J(A)$ is a countably generated normal, separable algebraic field extension of $\overline{R}$. As A is a *duo* ring, by [1], it has a coefficient subring R_0. Now $J(R_0) = R_0\pi$. Since A is an (R_0, R_0)-bimodule, by 3.4, it can be written as

$$A = R_0 \oplus \left(\oplus \sum_{i=1}^{n} R_0 x_i\right)$$

in such a way that $x_i \in J(A)$ for $1 \leq i \leq n$. As $J(A)$ is a principal right and left ideal, $J(A) = Ax_i = x_iA$ for some x_i; write θ for this x_i and σ for the corresponding σ_i. We call (θ, σ) a *distinguishing pair* of A with respect to R_0. Then $J(A) = \theta A = A\theta$ and $\theta a = \sigma(a)\theta$ for $a \in R_0$. As $\pi \in \theta A$, there exists a smallest positive integer k such that $\theta^k = \pi w$ for some unit $w \in A$. Let m and n be the indices of nilpotency of θ and π respectively. Then $m = (n-1)k + t$ for some $1 \leq t \leq k$.

As in [4] or in [8], we also have $A = R_0 \oplus R_0\theta \oplus \ldots \oplus R_0\theta^{k-1}$ with $R_0\theta^i \cong R_0$ for $1 \leq i < t$, and $R_0\theta^i \cong R_0/R_0\pi$ for $t \leq i < k$ as left R_0-modules. Suppose $\theta^k = 0$; then $\pi = 0$, R_0 is a field, and $A \cong R_0[x,\sigma]/\langle x^k\rangle$. So we are interested only in the case $\theta^k \neq 0$. Observe that if $x \in R$, then $x\theta^{m-1} = r\theta^{m-1}$ for some $r \in R_0$.

LEMMA 5.1. *If $\theta^k \neq 0$, then σ is of finite order and its order divides k. Also, $\theta^k \in Z(A)$.*

Proof. We have $\pi = w^{-1}\theta^k$. Then for any $a \in R_0$, $\pi a = a\pi$ yields $(aw^{-1} - w^{-1}\sigma^k(a))\theta^k = 0$ and $waw^{-1} - \sigma^k(a) \in J(A)$. But $A/J(A)$ is commutative. We get $a - \sigma^k(a) \in J(A) \cap R_0 = J(R_0)$. By 2.7, $\sigma^k = I$. Hence the order of σ is finite and it divides k. The second part is obvious from the first.

Henceforth we suppose that $\theta^k \neq 0$, k' is the order of σ, and $k_1 = k/k'$.

LEMMA 5.2. $\mathcal{C}(R_0) = \{\sum_{i=0}^{k_1-1} a_i\theta^{k'i} : a_i \in R_0\}$.

Proof. Let $x = \sum_{i=0}^{k-1} a_i\theta^i \in \mathcal{C}(R_0)$, $a_i \in R_0$. For any $a \in R_0$, $ax = xa$ yields $(a - \sigma^i(a))a_i\theta^i = 0$. If for some i, $a_i\theta^i \neq 0$, then $a - \sigma^i(a) \in J(R_0)$, by 2.7, $\sigma^i = I$ and hence k' divides i. This proves the result.

LEMMA 5.3. *Let $w \in A$ be a unit.*

(i) *If for some $l, q \geq 0$, $a(w\pi^l\theta^q) = (w\pi^l\theta^q)a$ for every $a \in A$, with $\pi^l\theta^q \neq 0$, then k' divides q.*

(ii) *If $\theta(w\pi^l\theta^q) = (w\pi^l\theta^q)\theta$ and $\pi^l\theta^{q+1} \neq 0$, then $w = s_0 + w_1\theta^u$ for some unit $s_0 \in R_0^\sigma$, $u \geq 1$ and some unit $w_1 \in A$. In addition, if $w \in R_0$, then $w = s + s'$ for some $s \in R_0^\sigma$ and $s' \in J^{m-q-1-kl} \cap R_0$.*

(iii) *Let* $L = \sum_{i=0}^{k_1-1} R_0^\sigma \theta^{ik'}$. *If* k' *does not divide* $m-1$, *then* $Z(A) = L$. *If* k' *divides* $m-1$, *then* $Z(A) = L + J(A)^{m-1}$.

Proof. (i) $a(w\pi^l\theta^q) = (w\pi^l\theta^q)a$ for every $a \in A$ with $\pi^l\theta^q \neq 0$ gives $(aw - w\sigma^q(a))\pi^l\theta^q = 0$, and as in 5.1, we find that k' divides q.

(ii) Suppose that $\theta(w\pi^l\theta^q) = (w\pi^l\theta^q)\theta$ and $\pi^l\theta^{q+1} \neq 0$. Now $w = r + v$ for some $r \in R_0$ and $v \in J$. The hypothesis gives $(\sigma(r) - r)\pi^l\theta^{q+1} = v\pi^l\theta^{q+1} - \theta v\pi^l\theta^{q+1} \in \pi^l\theta^{q+1}J$, so $(\sigma(r) - r) \in J \cap R_0$. By 2.7(b), $r = s_0 + r_1\pi^\alpha$ for some unit $s_0 \in R_0^\sigma$, $\alpha \geq 1$, and some unit $r_1 \in R_0$. Then $w = s_0 + r_1\pi^\alpha + v = s_0 + w_1\theta^u$ for some unit $w_1 \in A$, $u \geq 1$.

Suppose $w = r \in R_0$. Then $r = s_0 + r_1\pi^\alpha$ and $\theta(r_1\pi^{\alpha+l}\theta^q) = (r_1\pi^{\alpha+l}\theta^q)\theta$. If $\pi^{\alpha+l}\theta^{q+1} = 0$, then $r_1\pi^\alpha \in J^{m-q-1-kl} \cap R_0$, and we stop. Otherwise we continue with r_1 in place of r. Then $r_1 = a_1 + r_2\pi^\beta$ for some unit $a_1 \in R_0^\sigma$, r_2 a unit in R_0, and some $\beta \geq 1$. Then $r = s_1 + r_2\pi^{\alpha+\beta}$, $s_1 = s_0 + a_1\pi^\alpha \in R_0^\sigma$. Observe that $\alpha + \beta > \alpha$. Continue the process with r_2 and so on. As π is nilpotent, we shall finally get $r = s + r'\pi^p$ for some $s \in R_0^\sigma$ and $s' = r'\pi^p \in J^{m-q-1-kl} \cap R_0$.

(iii) If $k' = 1$, then $A = Z(A)$, and the result holds trivially. Let $k' > 1$. Let $x \in Z(A)$. Then $x \in \mathcal{C}(R_0)$, $x = \sum_{i=0}^{k_1-1} r_i\theta^{k'i}$, $r_i \in R_0$. As $\theta x = x\theta$ and $(k_1 - 1)k' + 1 < k$, we get $\theta(r_i\theta^i) = (r_i\theta^i)\theta$. By (ii), $r_i = s_i + a_i$ for some $s_i \in R_0^\sigma$ and $a_i \in J^{m-k'i-1}$. Hence $x = s + a$ with $s = \sum_i s_i\theta^{k'i} \in L$ and $a = \sum_i a_i\theta^{k'i} \in J^{m-1}$. Now $a \in Z(A)$. Suppose $a \neq 0$. Then $a = r\theta^{m-1}$ for some unit $r \in R$. By (i), k' divides $m-1$. Further, if k' divides $m-1$, then $J^{m-1} \subseteq Z(A)$. This proves (iii).

Lemma 5.4. *For* $\theta^k = \pi w$, *the following hold.*

(i) *If* k' *does not divide* $m-1$, *then* w *can be chosen in the form* $\sum_{i=0}^{k_1-1} s_i\theta^{k'i}$ *with* $s_i \in R_0^\sigma$, *and this element is in* $L \subseteq Z(A)$.

(ii) *If* k' *divides* $m-1$, *then* $w = w_0 + r_0\theta^{m-k-1}$ *with* $w_0 \in L$, *and* $r_0 \in R_0$ *is either zero or a unit.*

(iii) w *chosen in either of the above forms is in* $\mathcal{C}(R_0)$. *Further*, $\mathcal{C}(R_0)$ *is a special primary ring with radical* $\langle\theta^{k'}\rangle$.

(iv) $\theta^k = \pi h(\theta) + r\theta^{m-1}$, *where* $h(x) \in R_0^\sigma[x^{k'}]$, $\deg h(x) < k$, *the constant term of* $h(x)$ *is a unit*, $r = 0$ *if* k' *does not divide* $m-1$, *and* r *is zero or a unit in* R_0 *otherwise. Further*, *if* $k = m-1$, *then* $1 - r$ *is a unit.*

Proof. We have $\pi = w^{-1}\theta^k \in Z(A)$. If $k = m-1$, then $w^{-1}\theta^k = s_0\theta^k$ for some unit $s_0 \in R_0$, so we can take $w = s_0^{-1} = s_0^{-1}\theta^{m-k-1}$, which is of type given in (ii). Suppose $k < m-1$. By 5.3(ii), $w^{-1} = s_0 + w_1\theta^\alpha$ for some unit $s_0 \in R_0^\sigma$, a unit $w_1 \in A$, and some $\alpha \geq 1$. If $\theta^\alpha\theta^k = 0$, we stop. Suppose, $\theta^\alpha\theta^k \neq 0$. Then $0 \neq w_1\theta^\alpha\theta^k \in Z(A)$. By 5.3(i), k' divides α. If $w_1\theta^\alpha\theta^{k+1} = 0$, then $w_1\theta^\alpha \in J^{m-k-1}$. Suppose $w_1\theta^\alpha\theta^{k+1} \neq 0$. By 5.3(ii), $w_1 = a_1 + w_2\theta^\beta$ for some unit $a_1 \in R_0^\sigma$, a unit $w_2 \in A$, and some $\beta \geq 1$.

Then $w^{-1} = s_1 + w_2\theta^{\alpha+\beta}$ with $s_1 = s_0 + a_1\theta^{\alpha} \in Z(A)$. Clearly $\alpha + \beta > \alpha$. Continue this process with w_2 and so on. We get $w^{-1} = s + v\theta^p$ for some unit $s \in Z(A)$, a unit $v \in A$, and some $p \geq 1$ such that $v\theta^p\theta^{k+1} = 0$. If $v\theta^p\theta^k \neq 0$, then $p = m - k - 1$. Suppose $v\theta^p\theta^k = 0$. Then $\pi = s\theta^k$, and in this case we can take $w = s^{-1} \in Z(A)$. Suppose $v\theta^p\theta^k \neq 0$. Then $v\theta^p\theta^k = v\theta^{m-1} = r\theta^{m-1}$ for some unit $r \in R_0$, and k' divides $m - 1$. Then $\pi = (s + r\theta^{m-k-1})\theta^k$ and $\theta^k = \pi(s^{-1} - s^{-2}r\theta^{m-k-1}) = \pi(s^{-1} + r'\theta^{m-k-1})$ for some unit $r' \in R_0$, so we can take $w = s^{-1} + r'\theta^{m-k-1}$. By 5.3(iii), $s^{-1} = w_0 + r_1\theta^{m-1}$ for some $r_1 \in R_0$ and $w_0 \in L$. Thus $w_0 = h(\theta)$ for some $h(x) \in R_0^{\sigma}[x^{k'}]$ with $\deg h(x) < k$. Then $\theta^k = \pi(w_0 + r'\theta^{m-k-1})$, and we can take $w = w_0 + r'\theta^{m-k-1}$, which is of type given in (ii). All this proves that w can be chosen of the type given in (i) or (ii), and in any case this w is in $\mathcal{C}(R_0)$. Clearly, $\mathcal{C}(R_0) = R_0 + \langle\theta^{k'}\rangle$, $\mathcal{C}(R_0)$ is commutative, and $J(\mathcal{C}(R_0)) = \pi R_0 + \langle\theta^{k'}\rangle = \langle\theta^{k'}\rangle$, as $\pi = w^{-1}\theta^k \in \langle\theta^{k'}\rangle$. Hence $\mathcal{C}(R_0)$ is a chain ring.

In case k' divides $m-1$, we have $\theta^k = \pi h(\theta) + \pi r'\theta^{m-k-1} = \pi h(\theta) + r\theta^{m-1}$ for some $r \in R_0$. Once again consider the case when $k = m - 1$. As seen above, $\theta^k = \pi r_0$ for some unit $r_0 \in R$. Then $\theta\pi = 0$, and this gives $\theta^k = \pi + (r_0 - 1)\pi = \pi + r\theta^{m-1} = \pi h(\theta) + r\theta^{m-1}$ for some $r \in R_0$, $h(x) = 1$. Then $(1 - r)\theta^k = \pi h(\theta)$ shows that $1 - r$ is a unit, as $h(\theta)$ is a unit. This proves (iv).

The following theorem generalizes [8, Theorem 4.15].

THEOREM 5.5. *Let (R, π) be a special primary ring with $\pi \neq 0$, and A be a local, faithful R-algebra such that $J(R) = R \cap J(A)$ and $\overline{A} = A/J(A)$ is a countably generated separable algebraic field extension of $\overline{R}$. Then the following are equivalent.*

(a) *A is a chain ring with $J(A)$ having index of nilpotency m.*

(b) *There exists a commutative local ring R_0 which is a faithful unramified R-algebra, an R-automorphism σ of R_0 of order a positive integer k', a positive integer $k \leq m-1$ divisible by k', a polynomial $g(x) = x^k - \pi h(x)$ with $h(x) \in R_0^{\sigma}[x^{k'}]$, the constant term of $h(x)$ a unit and $\deg h(x) < k$, for which the following hold.*

(i) *If k' does not divide $m - 1$, then $A \cong R_0[x, \sigma]/\langle g(x), x^m\rangle$.*

(ii) *If k' divides $m - 1$ and $k < m - 1$, then there exists $r \in R_0$ which is either zero or a unit such that*

$$A \cong R_0[x, \sigma]/\langle g(x) - rx^{m-1}, x^m\rangle.$$

(iii) *If $k = m - 1$, then there exists $r \in R_0$ such that either $r = 0$ or both r and $1 + r$ are units in R_0, and*

$$A \cong R_0[x, \sigma]/\langle g(x) - rx^{m-1}, x^m\rangle.$$

Proof. Let A be a chain ring and m be the index of nilpotency of $J(A)$. Let R_0 be a coefficient subring of A, and (θ, σ) be a distinguishing pair of A with respect to R_0. Now, R_0 is an unramified R-algebra. There exists a positive integer k and a unit $w \in A$ such that $\theta^k = \pi w$. By 5.3, the order k' of σ divides k. We can write $\theta^k = \pi h(\theta) + r\theta^{m-1}$ where $h(x)$ and r are as specified in 5.4(iv). Let $f(x) = x^k - \pi h(x) - rx^{m-1}$. It follows from 4.7 and 4.10 that $S = R_0[x, \sigma]/B$, where $B = \langle f(x), x^m \rangle$, is a chain ring with $J(S)$ having index of nilpotency m. We have an R-epimorphism $\lambda : S \to A$ such that for any $q(x) \in R_0[x, \sigma]$, $\lambda(q(x) + B) = q(\theta)$. As the index of nilpotency of $J(A)$ is also m, λ is an R-isomorphism. Hence (a) implies (b). It follows from 4.7 and 4.10 that (b) implies (a).

EXAMPLE (see [2]). Let F be any field of characteristic 2 and x, y be two indeterminates. Consider a one-dimensional vector space V over $K = F(x, y)$. Fix a basis element α of V. Let L be the F-vector space of all finite formal sums $\sum a_{ij} x^i y^j$, $a_{ij} \in F$, where i, j are non-negative integers. Consider $S = L \oplus V$. Define

$$(x^n y^m) \circ (x^r y^s) = x^{n+r} y^{m+s} + mr\alpha x^{n+r-1} y^{m+s-1}.$$

In particular, $y \circ x = xy + \alpha$. For any $\alpha u, \alpha v \in V$ and $f \in L$, define $(\alpha u) \circ (\alpha v) = 0$ and $f \circ (\alpha u) = (\alpha u) \circ f = \alpha(uf)$. Extend this operation to S. This makes S a ring, with $T = 0 \times V$ an ideal such that $T^2 = 0$ and $y^m \circ x^{2n} = x^{2n} y^m$. For any $f \in L$, $f^2 \in Z(S)$. It follows that S satisfies the right as well as left Öre condition. Consequently, S admits a total right quotient ring A with $J(A) = T$ and $A/J(A) \cong K$. Suppose S admits a coefficient subring T. Then T is a field isomorphic to K. There exist $u = x + \alpha r$ and $v = y + \alpha s$ in T. As $u \circ v = v \circ u$, it follows that $x \circ y = y \circ x$. This is a contradiction. Hence this ring does not admit a coefficient subring.

REFERENCES

[1] Y. Alkhamees and S. Singh, *Inertial subrings of a locally finite algebra*, Colloq. Math. 92 (2002), 35–42.

[2] —, —, *A local artinian ring with no coefficient subring* (unpublished).

[3] G. Azumaya, *On maximally central algebras*, Nagoya Math. J. 2 (1951), 119–150.

[4] W. E. Clark and D. A. Drake, *Finite chain rings*, Abh. Math. Sem. Univ. Hamburg 39 (1973), 147–153.

[5] I. S. Cohen, *On the structure and ideal theory of complete local rings*, Trans. Amer. Math. Soc. 59 (1946), 54–106.

[6] C. Faith, *Algebra II*, *Ring Theory*, Grundlehren Math. Wiss. 191, Springer, New York, 1976.

[7] R. Gilmer, *Multiplicative Ideal Theory*, Pure Appl. Math. 12, Dekker, New York, 1972.

[8] B. R. Wirt, *Finite non-commutative local rings*, Ph.D. thesis, Univ. of Oklahoma, 1972.
[9] O. Zariski and P. Samuel, *Commutative Algebra*, *Vol. II*, Springer, New York, 1960.

Department of Mathematics
King Saud University
P.O. Box 2455, Riyadh 11451
Kingdom of Saudi Arabia
E-mail: ykhamees@ksu.edu.sa
hananamo@hotmail.com
ssingh@ksu.edu.sa

Received 27 May 2002;
revised 23 December 2002 (4227)