Canad. Math. Bull. Vol. **19** (3), 1976

FINITE PRINCIPAL IDEAL RINGS

BY
JAMES L. FISHER

This paper determines the structure of finite rings whose two sided ideals are principal as left ideals, and as right ideals. Such rings will be called principal ideal rings. Although finite rings have been studied extensively [1], [5], [12], [14] and the tools necessary for describing finite principal ideal rings have been available for thirty years, these structure theorems (which are essentially given in a more general setting in [4]) seem to have been overlooked. In particular, let σ be an endomorphism of a ring V. Define $V[[x;\sigma]]$ to be a ring of (skew) power series with indeterminate x, coefficients from V and which satisfies $xv=\sigma(v)x$. If S is any ring, denote the Jacobson radical of S by $J(S)$. Furthermore a v-ring V is defined (after [3]) to be a complete discrete commutative valuation domain whose maximal ideal is generated by the prime integer p (where p is the characteristic of $V/J(V)$). This paper proves that a finite principal ideal ring R is the direct sum $R_1\oplus R_2\oplus\cdots\oplus R_k\oplus N$ where R_i, $i=1,\ldots,k$ are complete $n_i\times n_i$ matrix rings (n_i positive integers) over rings of the form $V[[x;\sigma]]/(p-\varepsilon x^{\ell}, x^{s})$ where V is a v-ring with $V/J(V)$ a finite field, σ an automorphism of V, ε a unit in $V[[x;\sigma]]$, $p^{[s/\ell]}$ is the characteristic of R_i and s is the index of nilpotency of $J(R_i)$, and, in addition, N is a nilpotent principal ideal ring (whose structure is described in [5] and [11]). The rings $V[[x;\sigma]]/(p-\varepsilon x^{\ell}, x^{s})$ are exactly the completely primary rings with 1 whose two sided ideals are principal as left ideals and this gives a more detailed description of the finite chain rings of [2]. Furthermore the rings $V[[x;\sigma]]/(p-\varepsilon x^{\ell})$ are (local) principal right and principal left ideal domains, so that in the spirit of [7], every finite principal ideal ring with identity is the homomorphic image of a direct sum of matrix rings over principal ideal domains.

Direct sum decomposition. Following [9], a primary ring is defined to be a left artinian ring R with identity such that $R/J(R)$ is simple. If in addition $R/J(R)$ is a division ring then R is called completely primary. The following theorem is from [10, pp. 64, 36] and is a variation of one from [9].

THEOREM 1. *Let R be a primary ring in which $J(R)$ is a principal left ideal. Then R is equal to $(S)_n$, the ring of all $n\times n$ matrices over S where S is a completely primary principal left ideal ring.*

Received by the editors May 6, 1974 and, in revised form, September 11, 1974.

There are numerous decomposition theorems for principal ideal rings with identity. We give a variation of a theorem found in Jacobson [9, page 75] which does not require the ring R to have an identity. Thus a left ideal I of R is principal if there exists $c \in I$ such that $I = \{mc + rc : m$ is an integer, $r \in R\}$. Denote I by Rc. The analagous definition holds for principal right ideal.

THEOREM 2. *Let R be a finite principal ideal ring. Then R is an ideal direct sum $R_1 \oplus \cdots \oplus R_k \oplus N$ where R_i $i = 1, \ldots, k$ are primary principal ideal rings and N is a nilpotent principal ideal ring.*

Proof. Let R_1 be a minimal non-nilpotent ideal of R. By hypothesis $R_1 = Rc$ and since R_1 is a two sided ideal $cR \subseteq Rc$. Thus $RcRc \subseteq Rc^2$ which is non nilpotent so that $Rc^2 = Rc$, and by induction $Rc^i = Rc$. Thus for $r \in R$, $rc = mc^2 + sc^2$ for some integer m and $s \in R$. Hence $r = (r - (mc + sc)) + (mc + sc)$ and $R = \ell(c) + Rc$ as left ideals where $\ell(c) = \{x \in R : xc = 0\}$. Define $\ell_1(c) = \{(m, s) : m$ is an integer, $s \in R$, and $mc + sc = 0\}$. The sets $\ell_1(c^i)$, $i = 1, 2, 3, \ldots$ form an ascending chain which must terminate, say $\ell_1(c^n) = \ell_1(c^{n+j})$, j any positive integer. If $a \in \ell(c^n) \cap Rc^n$, then $a = mc^n + sc^n$ so that $0 = ac^n = mc^{2n} + sc^{2n}$ and $(m, s) \in \ell_1(c^{2n}) = \ell_1(c^n)$. Thus $a = 0$, and since $\ell(c)$ is in $\ell(c^n)$ and $Rc^n = Rc$, we have $R = \ell(c) \oplus Rc$ as left ideals. Again by hypothesis, $R_1 = c_1 R$ and by an argument similar to that above, $R = r(c_1) \oplus c_1 R$ as right ideals where $r(c_1) = \{s \in R : c_1 s = 0\}$. To show that $\ell(c)$ is two sided, it is sufficient to show $\ell(c) = r(c_1)$. First note that $Rc^2 = Rc$ implies $xc^2 = 0$ if and only if $xc = 0$. Thus for $b \in \ell(c)$, $b = r_1 + c_1 r_2$ with $r_1 \in r(c_1)$ and $0 = bc = r_1 c + c_1 r_2 c$. Hence $r_1 c \in r(c_1) \cap c_1 R$, so that $0 = r_1 c = c_1 r_2 c$ and $c_1 r_2 = 0$. This implies $b \in r(c_1)$, and $\ell(c)$ is two sided. This gives the decomposition $R = R_1 \oplus \cdots \oplus R_k \oplus N$ where R_i are two sided minimal non nilpotent ideals; and N is nilpotent. By lifting the identity of $R_i/J(R_i)$ to an idempotent e of R_i, we have $c = se + x$ where $s \in R$ and x is in $J(R_i)$. Since $x \in J(R_i)$, $x = x_1 c$ where $x_1 \in J(R_i)$. Thus formally $c = (1 - x_1)^{-1} se$, and since x_1 is nilpotent, c is in Re. Thus $Re = Rc = eR$ and e is the identity for R_i. Thus R_i is a primary principal ideal ring.

As in [11], the nilpotent ring N of theorem 2 can be decomposed further into a direct sum of n nilpotent rings of orders $p_i^{\alpha_i}$ where p_i, $i = 1, \ldots, n$ are distinct prime integers, α_i positive integers. In fact N is a finite nilpotent principal ideal ring iff N is a direct sum of n nilpotent principal ideal rings of orders $p_i^{\alpha_i}$ where p_i, $i = 1, \ldots, n$ are distinct prime integers.

Indecomposable finite principal ideal rings. Because of the first two theorems we need only investigate the structure of finite completely primary principal ideal rings. The following theorem is an analogue of [0, prop. 8.8], and shows that for finite completely primary rings it is sufficient to insist that $J(R)$ is principal as a left ideal.

THEOREM 3. *Let R be a finite completely primary ring. R is a principal ideal ring iff the dimension of $J(R)/J(R)^2$ as a left $R/J(R)$ space is at most one.*

Proof. It is clear that if R is a finite completely primary principal ideal ring, then $\dim_{R/J(R)} J(R)/J(R)^2$ is at most one. To show the implication in the other direction, choose $x \in J(R)$ such that $x \notin J(R)^2$. Since the dimension of $J(R)/J(R)^2$ is one, $Rx + J(R)^2 = J(R)$. Hence $Rx = J(R)$ if $Rx \supseteq J(R)^2$. Let $r \in Rx + J(R)^i$ so that $r = r_1 x + \sum_k \prod_j n_{kj}$ with $n_{kj} \in J(R)$. However $n_{kj} = r_{kj}x + m_{kj}$, $m_{kj} \in J(R)^2$. Thus $r = r_1 x + \sum_k \prod_j (r_{kj}x + m_{kj}) \in Rx + J(R)^{i+1}$, and r is in $Rx + J(R)^t$ for all positive integers t. Since $J(R)$ is nilpotent, we have $r \in Rx$ and $Rx = J(R)$. Since $J(R)/J(R)^2$ is finite, $\dim J(R)/J(R)^2$ as a left $R/J(R)$ space equals $\dim J(R)/J(R)^2$ *as a right* $R/J(R)$ space. Hence $J(R) = xR$.

THEOREM 4. *Let R be a finite completely primary ring. Then R contains a coefficient ring $\bar{V}$ of characteristic equal to the characteristic of R and with $\bar{V}/J(\bar{V})$ equal to $R/J(R)$. Furthermore $\bar{V}$ is a homomorphic image of a v-ring V.*

This result is proven in many places ([1], [4], [12]) and is essentially derived from [3].

***U* Central *V*–*V* bimodules.** Let V be a ring with U a subring of V. A U central V–V bimodule M is a left and right V–module satisfying $v(mw) = (vm)w$ for all $m \in M$, $v, w \in V$, and $mu = um$ for all $u \in U$. Since a finite completely primary ring R contains a coefficient ring which is a homomorphic image of a v-ring V and since V contains a sub v-ring U generated by the identity, then the radical $J(R)$ is a U central V–V bimodule. Hence knowing the structure of U central V–V bimodules will enable us to determine the structure of $J(R)$. This section determines the structure of U central V–V bimodules, $U \subseteq V$, U and V v-rings, such that $F = V/J(V)$ is a finite dimensional Galois extension of $K = U/J(U)$. This is a variation of results of [6] and [8].

The following lemma is an easy variation of a result of Cohen [3, page 68]. In the version stated below, we do not need the hypothesis that R is noetherian.

LEMMA 5. *Let R and S be commutative local rings with $R \subset S$ and R complete. If $S \cdot J(R) = J(S)$ and $S/J(S)$ is a finite algebraic extension of $R/J(R)$ then S is complete and $S = Ra_1 + \cdots + Ra_k$ where $a_1, \ldots, a_k$ is any lifting of a basis $\bar{a}_1, \ldots, \bar{a}_k$ of $S/J(S)$ over $R/J(R)$.*

Denote the field of quotients of a commutative domain S by $Q(S)$.

LEMMA 6. *If $\bar{a}_1, \ldots, \bar{a}_k$ is a basis for F over K and $a_1, \ldots, a_k$ is a set of elements of V mapping onto $\bar{a}_1, \ldots, \bar{a}_k$ under the natural map then $a_1, \ldots, a_k$ is both a basis for V over U and $Q(V)$ over $Q(U)$.*

Proof. Lemma 5 guarantees $V = Ua_1 + \cdots + Ua_k$. We must now show independence over U. Let ϕ be the (multiplicative) valuation determined by U. Suppose $0 = u_1a_1 + \cdots + u_ka_k$, $u_i \in U$, $i = 1, \ldots, k$, not all u_i zero. Define $n = \max\{\phi(u_i) : u_i \neq 0\}$. Thus $0 = 0 \cdot n^{-1} = n^{-1}u_1a_1 + \cdots + n^{-1}u_ka_k$ and $n^{-1}u_i \in U$, with at least one $n^{-1}u_i$ not in $J(U)$. Hence $0 = \overline{n^{-1}u_1}\,\overline{a_1} + \cdots + \overline{n^{-1}u_k}\,\overline{a_k}$ is a nontrivial relation in F, which is a contradiction. Thus all u_i are zero.

Since $Q(V) = \{v/p^\alpha : v \in V,\ \alpha$ is a non-negative integer$\}$ we have $v/p^\alpha = (u_1/p^\alpha)a_1 + \cdots + (u_k/p^\alpha)a_k$ so that $Q(V) = Q(U)a_1 + \cdots Q(U)a_k$. A linear dependency of the a_i in $Q(V)$ over $Q(U)$ would imply a linear dependency in V over U. Therefore $\{a_1, \ldots, a_k\}$ is indeed a basis for $Q(V)$ over $Q(U)$.

LEMMA 7. *If F is a Galois extension of K then there is an isomorphism between the group of automorphisms of V fixing U and the group of automorphisms of F fixing K. If σ is an automorphism of V then an isomorphism is given by $\sigma \to \bar{\sigma}$ where $\bar{\sigma}(\bar{v}) = \overline{\sigma(v)}$.*

Proof. Since F is Galois over K, F is the splitting field of a separable irreducible polynomial $\bar{f}(x) \in K[x]$. Suppose $\bar{f}(x) = (x - \bar{a}_1) \cdots (x - \bar{a}_k)$ in $F[x]$. We may suppose that $\bar{a}_1, \ldots, \bar{a}_k$ forms a normal basis for F over K. Choose $f(x) \in U[x]$ which maps onto $\bar{f}(x)$. By Hensel's lemma $\bar{a}_1, \ldots, \bar{a}_k$ can be raised to $\{a_1, \ldots, a_k\}$ contained in V such that $f(x)$ splits in $V[x]$ to $f(x) = (x - a_1) \cdots (x - a_k)$. By lemma 6, $\{a_1, \ldots, a_k\}$ is a basis for V over U and $Q(V)$ over $Q(U)$. This implies that $Q(V) = Q(U)a_1 + \cdots + Q(U)a_k$ is the splitting field of the separable irreducible polynomial $f(x)$ in $Q(U)[x]$, which proves that $Q(V)$ is a Galois extension of $Q(U)$. If σ is an automorphism of $Q(V)$ over $Q(U)$ then $\sigma(a_i) = a_{\pi(i)}$ where π is a permutation of $1, \ldots, k$. Hence $\sigma(V) = V$ and any automorphism of $Q(V)$ over $Q(U)$ restricts to an automorphism of V over U. Note that the map $\sigma \to \bar{\sigma}$ where $\bar{\sigma}(\bar{v}) = \overline{\sigma(v)}$ is a homomorphism of the Galois group of V over U into the Galois group of F over K. Since σ induces a permutation of $a_1, \ldots, a_k$, $\bar{\sigma}$ will induce the same permutation on $\bar{a}_1, \ldots, \bar{a}_k$. Hence $\sigma \neq 1$ implies $\bar{\sigma} \neq 1$ and $\sigma \to \bar{\sigma}$ is an isomorphism. To see that the isomorphism is onto we note that the Galois group G of V over U has order k as does the Galois group of F over K.

THEOREM 8. *Let V and U be v-rings with $V \supseteq U$ and $V/J(V)$ a finite Galois extension of $U/J(U)$. Let M be a U central V–V bimodule. Let $\sigma_1, \ldots, \sigma_k$ be the automorphisms of V over U. Then M is equal to $M_1 \oplus \cdots \oplus M_k$ where $mv = \sigma_i(v)m$ for all $m \in M_i$, M_i U central V–V bimodules.*

Proof. Since $F = V/J(V)$ is Galois over $K = U/J(U)$, there is a separable irreducible polynomial $f(x) \in U[x]$ which in $V[x]$ splits into $f(x) = (x - a_1) \cdots (x - a_k)$ with $a_1, \ldots, a_k$ a normal basis for V over U and furthermore $V = U(a_1)$. Define $f_i(x) = \prod_{j \neq i} (x - a_j)$. Since V is local and $a_i - a_j \notin J(V)$

https://doi.org/10.4153/CMB-1976-043-1 Published online by Cambridge University Press

for $i \neq j$ we have $f_i(a_i) \notin J(V)$. Therefore $(f_i(a_i))^{-1}$ exists in V and the polynomial $-1+\sum (f_i(a_i))^{-1} f_i(x)$ is of degree at most $k-1$ but has k roots in $V \subset Q(V)$. Thus the polynomial is identically zero, yielding $1=\sum (f_i(a_i))^{-1} f_i(x)$ in $V[x]$. We may now note that multiplication on the right of M by a_1 is a V linear transformation T on M as a left V module. Since $f(a_1)=0$ and since $f(x) \in U[x]$, we also have $f(T)=0$. Because of the identity in $V[x]$ we have $I=\sum (f_i(a_i))^{-1} f_i(T)$ so that $M=\sum (f_i(a_i))^{-1} f_i(T)M = M_1+\cdots+M_k$ where $M_i = (f_i(a_i))^{-1} f_i(T)M$. To show that this sum is direct suppose for example that $m \in M_1 \cap (M_2+\cdots+M_k)$. Since $m \in M_1$ we have $(T-a_1 I)m=0$, and since $m \in M_2+\cdots+M_k$ we have $(T-a_2 I)\cdots(T-a_k I)m=0$. This implies that $m = Im = \sum (f_i(a_i))^{-1} f_i(T)m = 0$ and the sum is direct. Now for every $m \in M_i$ we have since $f(T)=0$, $(T-a_i I)m=0$. Therefore $Tm = a_i m$. But $Tm = ma_1$. Since a_i is a root of $f(x)$, as is a_1, there is an automorphism σ_i of V over U which maps a_1 onto a_i. Therefore $ma_1 = \sigma_i(a_1)m$ and $mv = m(\sum_j u_j a_1^j) = \sum_j u_j m a_1^j = \sum u_j (\sigma_i(a_1))^j m = \sigma_i(\sum_j u_j a_1^j)m = \sigma_i(v)m$, and the theorem is proven.

Structure theorem. Knowing the structure of U central V–V bimodules enables us to prove

THEOREM 9. *Let R be a finite completely primary principal ideal ring. Then R is isomorphic to $V[[x;\sigma]]/(p-\varepsilon x^{\ell}, x^s)$ where ε is a unit of $V[[x;\sigma]]$, $p^{[s/\ell]}$ is the characteristic of R, s is the index of nilpotency of $J(R)$, and V is a v-ring with $V/J(V)$ isomorphic to $R/J(R)$.*

Proof. Since R is a finite completely primary principal ideal ring, theorem 3 shows $\dim_{R/J(R)} (J(R)/J(R)^2) \leq 1$. Let $\bar{V}$ be the homomorphic image of V in R (theorem 4). By theorem 8, $J(R) = Vm_1 \oplus \cdots \oplus Vm_t$ with $m_i v = \sigma_i(v) m_i$, σ_i automorphisms of V (not necessarily distinct). Exactly one of the m_i (call it m) has a nonzero image in $J(R)/J(R)^2$. It is clear that R is exactly the ring generated by $\bar{V}$ and m. The map from $V[[x;\sigma]]$ to R (where $mv = \sigma(v)m$) induced by $x \to m$ and $V \to \bar{V}$ is well defined since relations in $V[[x;\sigma]]$ map to relations in R. Since pR is an ideal of R, $pR = J(R)^{\ell}$ so that $p = \bar{\varepsilon} m^{\ell}$, $\bar{\varepsilon}$ a unit in R. Lift $\bar{\varepsilon}$ to a unit ε in $V[[x;\sigma]]$ (which is possible since $V[[x;\sigma]]$ is complete). I claim $V[[x;\sigma]]/(p-\varepsilon x^{\ell}, x^s)$ is isomorphic to R, where s is the index of nilpotency of $J(R)$ and $p^{[s/\ell]}$ is the characteristic. This will be proven if a relation $r = \bar{v}_0 + v_1 m + \cdots + v_k m^k$, $\bar{v}_0 \in \bar{V}$, $v_i \in V$, in R is a result of $p - \bar{\varepsilon} m^{\ell}$ and m^s. *If* $\bar{v}_o \notin pR$ then r is a unit and hence cannot be a relation. Thus $\bar{v}_0 = p\bar{v}_0'$, $\bar{v}_0' \in \bar{V}$. But $p = \bar{\varepsilon} m^i$ so that $\bar{v}_0 = \bar{\varepsilon} m^i \bar{v}_o'$. By this process, we may assume r is of the form $v_t m^t + \cdots + v_{s-1} m^{s-1}$ with v_t a unit in V and v_k, $k = t+1, \ldots, s-1$ units or 0 in V. Thus $(v_t + \cdots + v_{s-1} m^{s-1-t}) m^t$ is a relation which implies m^t is a relation. This contradicts $t < s$ so that the map in indeed an isomorphism.

It can be noted that if the characteristic of R is not p then σ^{ℓ} is the identity automorphism. The central element $\bar{p} = \overline{\varepsilon x^{\ell}}$ so that $\overline{\varepsilon x^{\ell}} v = \sigma^{\ell}(v)\overline{\varepsilon x^{\ell}} = \overline{v\varepsilon x^{\ell}}$. Hence $\bar{x}^{\ell} \neq 0$ (i.e. $\bar{p} \neq 0$) implies $\sigma^{\ell} = 1$.

As a result of theorem 9, we now can show

THEOREM 10. *A finite completely primary principal ideal ring R is a homomorphic image of a principal left and principal right ideal domain S. Furthermore all left and right ideals of S are two sided.*

Proof. By theorem 9, R is a homomorphic image of $S = V[[x;\sigma]]/(p - \varepsilon x^{\ell})$ where ε is a unit of $V[[x;\sigma]]$. I claim that S is a principal right and principal left ideal domain. Since $p = \varepsilon x^{\ell}$, we can write $s = \sum_{i=i_0}^{\infty} v_i x^i$ where v_{i_0} is a unit of V. Thus $s = (\sum_{i=i_0}^{\infty} v_i x^{i-i_0}) x^{i_0}$ where $\sum_{i=i_0}^{\infty} v_i x^{i-i_0}$ is a unit of S. Thus $Ss = Sx^{i_0}$ and the right ideals are exactly of the form Sx^i, $i = 1, 2, \ldots$. Since σ is an automorphism, the left ideals are also of that form. S is clearly a domain.

The theorems stated in the introduction now follow by application of theorem 2, theorem 1, theorem 9, and theorem 10. There are obvious generalizations to local principal left ideal rings which have large centers (in the sense that $R/J(R)$ is finite dimensional over the image of the center of R). These might be of interest in view of the fact that semiprime rings satisfying a polynomial identity do have such centers [13]. However, the added generality is overshadowed by the more cumbersome hypotheses (see [4]).

REFERENCES

0. M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

1. W. E. Clark, *A coefficient ring for finite non-commutative rings*, Proc. Amer. Math. Soc. **33** (1972), 25–28.

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

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

4. J. L. Fisher, *Structure theorems for non-commutative complete local rings*, Thesis, Calif. Inst. of Tech., 1969.

5. J. B. Fountain, *Nilpotent principal ideal rings*, Proc. London Math. Soc. **20** (1970), 348–364.

6. G. Hochschild, *Double vector spaces over division rings*, Amer. J. of Math. **71** (1949), 443–460.

7. T. W. Hungerford, *On the structure of principal ideal rings*, Pacific J. of Math. **25** (1968), 543–547.

8. N. Jacobson, *An extension of Galois theory to non-normal and non-separable fields*, Amer. J. of Math. **66** (1944), 1–29.

9. N. Jacobson, *The theory of rings*, Math. Surveys II, Amer. Math. Soc., 1943.

10. A. V. Jategaonkar, *Left principal ideal rings*, Lecture Notes in Math. **123** (1970), Springer Verlag.

11. K. R. McLean, *Commutative artinian principal ideal rings*, Proc. London Math. Soc. **26** (1973), 249–272.

12. R. Raghavendran, *Finite associative rings*, Compositio Math. **21** (1969), 195–229.
13. L. H. Rowen, *Some results on the center of a ring with polynomial identity*, Bull. Amer. Math. Soc. **79** (1973), 219–223.
14. R. S. Wilson, *On the structure of finite rings*, Compositio Math. **26** (1973), 79–93.

THE UNIVERSITY OF ALBERTA
EDMONTON, ALBERTA,
CANADA