PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 33, Number 1, May 1972

A COEFFICIENT RING FOR FINITE NON-COMMUTATIVE RINGS

W. EDWIN CLARK

ABSTRACT. We prove that every finite p-ring R contains a unique (up to isomorphism) subring S such that $S/pS \cong R/\mathrm{rad}\, R$. S is shown to be a direct sum of full matrix rings over rings of the form $Z_{p^n}[x]/(f(x))$ where $f(x)$ is monic and irreducible modulo p.

We consider only associative rings with identity. By a p-ring we mean a ring whose additive group is a p-group. It is well known that every finite ring is a direct sum of p-rings.

It is a consequence of Cohen's Structure Theorem for Complete Local Rings (see [**6**, p. 106]) that every finite *commutative* p-ring R contains a unique subring S satisfying $S/pS \cong R/\mathrm{rad}\, R$. Cohen called this the *coefficient ring* of R (in the local case). Actually the existence and structure of S for finite commutative rings was known to Krull as early as 1924 (see [**4**, §4, p. 20]). For finite commutative R it turns out that S is a direct sum of local rings of the form $Z_{p^n}[x]/(f(x))$ where $f(x)$ is monic and irreducible modulo p.

Following Janusz [**3**] who apparently independently rediscovered these rings we let $\mathrm{GR}(p^n, r) = Z_{p^n}[x]/(f(x))$ where $f(x)$ is monic of degree r and irreducible modulo p, and call such a ring a *Galois ring of characteristic p^n and rank r*. $\mathrm{GR}(p^n, r)$ is determined up to isomorphism by p, n and r (see [**3**] or [**4**]). Note that $\mathrm{GR}(p, r) = \mathrm{GF}(p^r)$, the Galois *field* of order p^r.

If a finite p-ring R has characteristic p, i.e., if R is an algebra over $\mathrm{GF}(p)$, then by the Wedderburn-Malcev Theorem [**2**, p. 491] R contains a unique (up to inner automorphism) subring S such that $S \cong R/\mathrm{rad}\, R$. S is finite and semisimple and therefore a direct sum of full matrix rings over Galois fields. The theorem in this paper generalizes this as well as the previously mentioned result on finite commutative rings.

The first two lemmas are taken from Clark and Drake [**1**]. They are repeated here for the convenience of the reader.

Received by the editors September 16, 1971.

AMS 1970 subject classifications. Primary 16A44, 16A46; Secondary 16A48.

Key words and phrases. Coefficient ring, Wedderburn-Malcev Theorem, Galois ring.

LEMMA 1. *If R is a finite p-ring, then R contains a subring S such that $S/pS\cong R/\text{rad } R$.*

PROOF. Let S be a subring of R minimal with respect to the property $S/\text{rad } S\cong R/\text{rad } R$. Since R is finite, $p^n=0$ for some n and so $pS\subset \text{rad } S$. Hence $\text{rad}(S/pS)=(\text{rad } S)/pS$. Now S/pS is an algebra over GF(p) and so by the Wedderburn-Malcev Theorem [2, p. 491], we have $S/pS=(T/pS)\oplus(\text{rad } S/pS)$, a direct sum qua abelian groups, for some subring T of S containing pS. It follows that $pS=\text{rad } T$ and that $T/\text{rad } T\cong S/\text{rad } S\cong R/\text{rad } R$. By the minimality of S, $T=S$ and hence $\text{rad } S=pS$.

LEMMA 2. *If R is a finite local p-ring, then R is a Galois ring if and only if pR is the radical of R.*

PROOF. By [5, §30, pp. 83 ff.], it suffices to show that R is commutative: Since R is local and finite, R/pR is a finite field and therefore has a cyclic multiplicative group of nonzero elements. If $h+pR$ is a generator for this group and if T is the subring of R generated by h and 1, then $T+pR=R$. It follows that $R=T+p(T+pR)=T+p^2R=\cdots=T+p^iR$. If we let i exceed the index of nilpotency of p, we obtain $R=T$. Hence R is commutative.

LEMMA 3. *Let R be a finite p-ring whose radical is pR. Then R is a direct sum of full matrix rings over Galois rings, and conversely.*

PROOF. Let $N=pR$ and write $1=\sum e_i^{(j)}$ where the $e_i^{(j)}$ are primitive pairwise orthogonal idempotents such that $Re_i^{(q)}\cong Re_j^{(r)}$ (as left R-modules) if and only if $q=r$. We wish to show that the left ideals $I_q=\sum Re_i^{(q)}$ are in fact ideals of R. To show this it suffices to prove that if e and f are primitive orthogonal idempotents such that Re is not isomorphic to Rf (as left R-modules) then $eRf=0$. Suppose $eRf\neq 0$. If $eRf\subset N=pR$, then $eRf=epRf=peRf$. It follows that $eRf=p^neRf=0$ where p^n is the characteristic of R. Thus if $eRf\neq 0$, $eRf\not\subset N$. It follows that Re is isomorphic to Rf (see, e.g., 54.11 and 54.12, pp. 372 ff. of [2]).

It follows that R is a direct sum of the ideals I_q each of which is a direct sum of n_q isomorphic principal indecomposable left ideals. Hence I_q is isomorphic to the ring of $n_q\times n_q$ matrices over $e_qI_qe_q=e_qRe_q$ where $e_q=e_1^{(q)}$. Since $\text{rad } R=pR$, we have $\text{rad } e_qRe_q=e_q(\text{rad } R)e_q=e_qpRe_q=pe_qRe_q$. Since e_q is primitive e_qRe_q is local and hence by Lemma 2 is a Galois ring.

The converse is left to the reader.

THEOREM. *Every finite p-ring R contains a unique (up to isomorphism) subring S such that $S/pS\cong R/\text{rad } R$. Moreover, S is a direct sum of full matrix rings over Galois rings.*

PROOF. The existence of a subring S satisfying $S/pS\cong R/\text{rad } R$ was established in Lemma 1. That S has the stated structure comes from Lemma 3. It remains only to show that S is unique up to isomorphism. If R is local, then clearly S is local, and since its radical is pS, by Lemma 2, $S=\text{GR}(p^n, r)$ where p^n is the characteristic of S (and hence of R) and p^r is the order of S/pS (and hence of $R/\text{rad } R$). Since as mentioned above $\text{GR}(p^n, r)$ is determined up to isomorphism by p, n and r, S is determined up to isomorphism by R. Thus we are done if R is local.

Let R be arbitrary with radical N. Let e and f be primitive idempotents in S and therefore also in R. We claim that $Re\cong Rf$ (as left R-modules) if and only if $Se\cong Sf$ (as left S-modules). As noted above $Re\cong Rf$ if and only if $eRf\not\subset N$. Also $Se\cong Sf$ if and only if $eSf\not\subset \text{rad } S$. With these observations the claim follows easily noting that since $S/pS\cong R/N$ we have $R=S+N$, $pS=\text{rad } S$ and $N\cap S\subset pS$. If $e_1, \cdots, e_k$ is a complete set of primitive pairwise orthogonal idempotents in S, then as in the proof of Lemma 3, S is a direct sum of k rings $(S_i)_{n_i}$ where $S_i=e_iSe_i$ and n_i is the number of principal indecomposable left ideals isomorphic to Se_i in any decomposition of S as a direct sum of such. It follows that the numbers k, n_1, $n_2, \cdots, n_k$ are uniquely determined by R.

Now suppose that T is also a subring of R satisfying $T/pT\cong R/N$. Let $f_1, \cdots .f_k$ be idempotents chosen as were the e_i for S and indexed so that $Re_i\cong Rf_i$. Then T is isomorphic to the direct sum of matrix rings $(T_i)_{n_i}$ where $T_i=f_iTf_i$.

From the above it suffices to show that if e and f are primitive idempotents in R such that $Re\cong Rf$ then $fTf\cong eSe$. Since Re and Rf are isomorphic left R-modules their endomorphism rings, eRe and fRf, are isomorphic. Since $S/pS\cong R/N$, it follows that $eSe/peSe\cong eRe/eNe$, and since e is primitive eRe is local; thus, we are reduced to the case already settled in the first paragraph of this proof.

REMARK. If R is commutative then it is known [**6**, p. 111] that the coefficient ring S is unique (absolutely!). In the case of finite algebras ($p=0$), by the Wedderburn-Malcev Theorem, S is unique up to an inner automorphism of R.

Problem. Is the subring S in the above theorem unique up to inner automorphism of R?

REFERENCES

1. W. E. Clark and D. A. Drake, *Finite chain rings* (to appear).

2. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Pure and Appl. Math., vol. 11, Interscience, New York, 1962. MR **26** #2519.

3. G. J. Janusz, *Separable algebras over commutative rings*, Trans. Amer. Math. Soc. **122** (1966), 461–479. MR **35** #1585.

4. W. Krull, *Algebraische theorie der ringe*. II, Math. Ann. **91** (1924), 1–46.

5. ———, *Idealtheorie*, Zweite, ergänzte Auflage, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 46, Springer-Verlag, Berlin and New York, 1968. MR **37** #5197.

6. M. Nagata, *Local rings*, Interscience Tracts in Pure and Appl. Math., no. 13, Interscience, New York, 1962. MR 27 #5790.

Department of Mathematics, University of South Florida, Tampa, Florida
33620