ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 3, Number 4, Fall 1973

FINITE LOCAL RINGS

G. GANSKE AND B. R. McDONALD

ABSTRACT. In this paper we examine finite local commutative rings which are the building blocks of finite commutative rings. For a finite local ring R our attention centers on the basic structural properties of R, the polynomial ring $R[X]$, the finite local extensions of R and the Galois theory of R. We show that this theory is nearly as complete as that well-known for finite fields.

1. Introduction.

The purpose of this paper is to examine the structure theory, theory of extensions and Galois theory of finite local commutative rings. The basic approach is to specialize the Chase-Harrison-Rosenberg [3] Galois theory for commutative rings to finite local rings and in this setting sharpen the results to approximately the level of the well-known theory for finite fields.

Since the purpose is to provide a foundation for the theory of finite commutative rings, we work entirely in this context. Thus, though some of the results may be stated more generally we refrain from this and likewise results which we reference we formulate in our setting.

To us the importance of this paper will lie mainly in its applications. Research on finite fields and their applications has been notably extensive, producing rich and deep results in finite geometries, algebraic coding theory, linear groups and other areas. Our work indicates similar results are obtainable over arbitrary finite commutative rings. One of the authors has already utilized portions of this paper on questions in the theory of algebraic cryptography and matrix theory here-to-now formulated only for finite fields and occasionally quotient rings of rational integers. These results appear in [15].

The Galois extensions of Z/Zp^n (called *Galois rings*) are particularly important. Finite noncommutative rings may be considered as algebras over these Galois rings and it now appears that much of the classical theory of algebras over fields may be extended to finite rings with identity ([4], [5], [6], [20], and [22]).

The second author would like to express his deep thanks to E.

Received by the editors March 4, 1971 and, in revised form, February 23, 1972.

AMS (MOS) subject classifications (1970). Primary 12C05, 12C30, 16A44; Secondary 13B05, 13B25.

Key words and phrases. Finite commutative rings, finite local rings, Galois theory, finite fields.

Ingraham for conversations on several occasions concerning separable algebras and for the use of an unpublished manuscript by him and F. DeMeyer on separable algebras and Galois theory. (This now appears as [**12**].)

2. **Background, preliminaries and notation.** Let R denote a finite commutative ring. The variety of such rings is illustrated by the fact that, although there exists only one finite field of four elements and only two Abelian groups of order four, a short computation yields nine commutative rings of order four. The local rings of order 4 are $Z/4Z$, $GF(2^2)$ and $(Z/2Z)[X]/(X^2)$.

If the Jacobson radical of R, rad R, is not zero and R does not have an identity then lift the orthogonal idempotents from $R/\text{rad } R$ (which is a direct sum of finite fields). One obtains a decomposition of R as a direct sum of local rings with identity and a nilpotent ring. Thus, modulo a nilpotent summand, the investigation of R reduces in most aspects to finite local commutative rings with identity. Price and Kruse have completed detailed investigations of noncommutative nilpotent rings which have specializations for the finite commutative nilpotent summand. A number of these results appear in [**19**].

For the remainder of this paper R will denote a finite local ring, m denotes the maximal ideal of R and $k = R/m$ the finite residue field of R. To summarize the well-known and elementary properties of R: R is trivially complete and thus Hensel, every element of R is nilpotent or a unit, m is nilpotent and obviously all proper ideals are in m. The set $\{u_1, \cdots, u_n\}$ forms a minimal basis for m if and only if their images give rise to a k-basis of m/m^2.

We call the nilpotency β (i.e., the least integer such that $m^\beta = 0$) of m the *nilpotency of* R and denote it by $\nu(R) = \beta$. The characteristic of R is denoted by $\chi(R)$; i.e., $\chi(R) = p^\lambda$ for some prime p and positive integer λ. If $\chi(R) = p^\lambda$, R contains a copy of the quotient ring of rational integers Z/Zp^λ.

We denote the natural ring morphism $R[X] \rightarrow (R/m)[X] = k[X]$ by μ. We sketch below the contents of §§(3), (4), (5), (6), and (7).

(3) This section concerns the polynomial ring $R[X]$ and, in particular, the subset of polynomials f where μf has distinct zeros in the algebraic closure of k. This class of polynomials is shown to admit unique factorization into irreducible polynomials. This section also contains a description of f when $R[X]/(f)$ is a local separable extension of R. Certain other results, such as a characterization of

finite fields in terms of the existence of monic prime irreducible polynomials, are given.

(4) This section contains a statement of the Chase-Harrison-Rosenberg Galois theory in the form we need. It is also shown that separable local extensions of finite rings possess primitive elements.

(5) This section sharpens the results of the previous section. Let S be a separable local extension of R with maximal ideals M and m, respectively. It is shown that S is R-free and thus a Galois extension of R. Further, the Galois group $\mathcal{G}_R(S)$ is isomorphic to $\mathcal{G}_{R/m}(S/M)$ and a primitive element α may be chosen so that $\mathcal{G}_R(S)$ is generated by a power map $\rho : \alpha \to \alpha^{|k|}$. The extension S is shown to be the *unique* Galois extension of R of degree $[S : R]$.

(6) This section provides a direct and simple proof of the Cohen Structure Theorem for finite local rings.

(7) This section discusses briefly the group of units of a finite local ring.

3. **The polynomial ring $R[X]$.** Throughout this section R denotes a finite local ring with maximal ideal m and residue field $k = R/m$. We record some facts in preparation for the section on the Galois theory.

We make extensive use of Hensel's Lemma: If f is a monic polynomial in $R[X]$ and $\mu f = \bar{g}\bar{h}$ where $\bar{g}$ and $\bar{h}$ are monic coprime polynomials in $k[X]$, then there exist monic coprime preimages g and h in $R[X]$ of $\bar{g}$ and $\bar{h}$ with $f = gh$. (See [23, p. 279].)

Using Hensel's Lemma the following is easy to show.

LEMMA 3.1. (a) *A polynomial f in $R[X]$ is a unit if and only if μf is a unit.*

(b) *If f is a monic irreducible polynomial in $R[X]$ then $\mu f = g^n$ where n is a positive integer and g is irreducible in $k[X]$. Thus, if μf is irreducible then f is irreducible.*

Despite the fact that irreducible polynomials in $R[X]$ do not necessarily have irreducible images in $k[X]$ we recall that in the Galois theory of finite fields the irreducible polynomials also have distinct zeros. We are led to the following class of polynomials in $R[X]$. *Let J denote the set of all polynomials f in $R[X]$ such that μf has distinct zeros in the algebraic closure of k.* The class J has been utilized briefly by some researchers in combinatorial theory (for example, see [8]) for the case of the polynomial ring $(Z/Zp^t)[X]$ but appears to have escaped explicit study. We first show that each polynomial in J has a monic "representative". We will then examine local extensions of R of the form $R[X]/(f)$ and illustrate how the existence of prime polynomials in J characterizes finite fields. Finally we show a polynomial in J has distinct zeros in local extensions of R, $R[X]/(f)$ (where f is monic) is a separable local extension if and only if f is an irreducible polynomial in J, and the polynomials in J admit unique factorizations into irreducible polynomials.

LEMMA 3.2. *Let f be in J. Then there exists a sequence $\{f_j\}$ of monic polynomials in J with*

$$\deg(f_j) = \deg(\mu f), \qquad f_j \equiv f_{j+1} \pmod{m^j},$$

and for some g_j in $m[X]$ and unit u_j in R

$$u_j f \equiv f_j + g_j f_j \pmod{m^j}.$$

PROOF. Let $f = \sum_{i=0}^{n} b_i X^i$ where $b_n \neq 0$ and $\deg(\mu f) = t \leqq n$. Choose $g_1 = 0$ and $f_1 = b_t^{-1}(\sum_{i=0}^{n} b_i X^i)$.

By induction assume $\{f_i\}_{i=1}^{j}$ have been selected to satisfy the lemma. Then $u_j f = f_j + g_j f_j + h$ where h is in $m^j[X]$. Since f_j is monic we may select q and r in $R[X]$ with $h = qf_j + r$ where $\deg(r) < \deg(f_j) = \deg(\mu f)$ or $r = 0$. Set $f_{j+1} = f_j + r$ and $g_{j+1} = g_j + q$.

We claim that g_{j+1} is in $m[X]$ and r is in $m^j[X]$. If $r = 0$ this statement is trivial. Otherwise suppose $f_j = a_0 + a_1 X + \cdots + a_{t-1}X^{t-1} + X^t$ and $q = c_0 + c_1 X + \cdots + c_S X^S$. In the product $f_j q$ the coefficient of X^{S+t} is c_S, of X^{t+S-1} is $c_S a_{t-1} + c_{S-1}$, etc. Since $h \equiv 0 \pmod{m^j}$ and $\deg(r) < \deg(f_j) = t$, it is easy to see that c_S, then c_{S-1}, then c_{S-2}, etc., are in m^j and consequently q is in $m^j[X]$. Then $r = h - qf_j$ is in $m^j[X]$.

Then

$$\begin{aligned} u_j f &= f_j + g_j f_j + h = (f_j + r) + (g_j + q)(f_j + r) - rg_j - rq \\ &= f_{j+1} + g_{j+1} f_{j+1} - r(g_j + q) \equiv f_{j+1} + g_{j+1} f_{j+1} \pmod{m^{j+1}}. \end{aligned}$$

THEOREM 3.3. *Let f be in J. Then there is a monic polynomial f^* in J with $\mu f = \mu f^*$ and, for an element a in R, $f(a) = 0$ if and only if $f^*(a) = 0$.*

PROOF. Let $\nu(R) = \beta$. Then by the lemma $\mu_\beta f = f_\beta + g_\beta f_\beta = (1 + g_\beta) f_\beta$ where f_β is monic, b_β and $1 + g_\beta$ (since g_β is in $m[X]$) are units and $\mu f = \mu f_\beta$. Thus let $f^* = f_\beta$.

It is interesting to note that the sequence in (3.2) terminates in at most $\nu(R) = \beta$ steps and that the unit u_j does not depend on j.

PROPOSITION 3.4. *If f is in J then f is irreducible if and only if μf is irreducible.*

Observe that for the polynomials $f = X^2 + X + 1$ and $g = X^2 + 3X + 1$ in $(Z/4Z)[X]$, f is irreducible but (f) is not a maximal ideal (hence f is not prime) and that f and g are distinct irreducibles but are not coprime.

LEMMA 3.5. *Let f and g be monic irreducible polynomials in J. Then $\mu f \neq \mu g$ if and only if f and g are coprime.*

PROOF. By (3.4) μf and μg are irreducible; thus, if $\mu f \neq \mu g$ there exist $\bar{h}$ and $\bar{j}$ in $k[X]$ with $\bar{h}(\mu f) + \bar{j}(\mu g) = 1$. Hence there are h and j in $R[X]$ with $\mu(hf + jg) = 1$. Consequently, $hf + jg$ is a unit and f and g are coprime. The converse is similar.

The following lemma is due to Azumaya [2, §E, Lemma 3] and is surprisingly difficult to prove.

LEMMA 3.6 (AZUMAYA'S LEMMA). *Let f be a monic polynomial in $R[X]$. Then $R[X]/(f) = I \oplus J$ where I and J are ideals in $R[X]/(f)$ if and only if there exist monic coprime polynomials h and g in $R[X]$ with $f = gh$ and $I = (g)/(f)$ and $J = (h)/(f)$.*

A polynomial f in $R[X]$ is called *local* if $R[X]/(f)$ is a local ring.

THEOREM 3.7. *A monic polynomial f in $R[X]$ is local if and only if μf is a power of an irreducible polynomial in $k[X]$.*

PROOF. If μf is not a power of an irreducible polynomial in $k[X]$ then by Hensel's Lemma f is not local. Conversely, if f is not local then $R[X]/(f)$ decomposes as a direct sum of ideals. Thus, by Azumaya's Lemma, f and, consequently, μf factor into monic coprime polynomials.

Edwin Clark has noted that the above may be proved directly without reference to Azumaya's Lemma. However we need this lemma later and so introduce it at this point. We have immediately the following corollary.

COROLLARY 3.8. *If f is a monic irreducible polynomial in $R[X]$ then $R[X]/(f^n)$ is a local ring for any positive integer n.*

Before examining local extensions further we note in the next several results how the existence of monic irreducible prime polynomials characterize finite fields. Recall $\text{Rad}(R[X]) = m[X]$ and that prime polynomials in $R[X]$ are irreducible; however, irreducible polynomials need not be prime.

LEMMA 3.9. *Let f be a monic irreducible polynomial in J. Then f is prime if and only if $m \subseteq (f)$.*

PROOF. If f is prime then $R[X]/(f)$ is a finite field. But for an element a in m the coset $a + (f)$ is nilpotent and hence zero. Thus a is in f.

Conversely, if $m \subseteq (f)$ then $m[X] \subseteq (f)$. Suppose that the coset $g + (f)$ is nilpotent. Then f divides g^n for some n and thus μf divides $(\mu g)^n$. Since f is irreducible and in J we have that μf divides μg; i.e., $\mu g = \bar{h}(\mu f)$. Let h be a preimage of $\bar{h}$. Then $hf = g + j$ where j is in $m[X]$. Thus g is in (f) and $R[X]/(f)$ is a field.

THEOREM 3.10 (CHARACTERIZATION OF FINITE FIELDS). *Let R be a finite local ring. The following are equivalent:*

(a) *R is a finite field.*

(b) *Every monic irreducible polynomial in $R[X]$ is prime.*

(c) *There exists at least one monic irreducible polynomial in J which is prime.*

PROOF. Clearly (a) implies (b) and (b) implies (c). We need only show that (c) implies (a). Suppose that R is not a field and let f be any monic irreducible polynomial in J. Let $a \neq 0$ be in m. If a is in (f) then f divides a which is impossible by observing their degrees and that f is monic. Thus m is not in (f), and by (3.9) f is not prime.

COROLLARY 3.11. *Let R be a finite local ring which is not a field. Then*

(a) *$R[X]$ has no principal prime ideals generated by monic polynomials.*

(b) *J contains no monic irreducible polynomials which are prime.*

An alternate approach to (3.10) and (3.11) and interesting in its own right is provided by the following observations.

If N is a maximal ideal in $R[X]$ then $N \cap R = m$ and the image of N under $\mu : R[X] \to k[X]$ is $(\bar{f})$ where $\bar{f}$ is an irreducible polynomial in $k[X]$. From this it is easy to deduce that every maximal ideal of $R[X]$ is of the form (m, f) where μf is an irreducible polynomial in $k[X]$; i.e., the maximal ideal is generated by m and f in $R[X]$. Consequently, f is an irreducible polynomial in J. Then, for an irreducible polynomial f in J, the ideal (f) is maximal if and only if $m = (0)$, i.e., R is a finite field.

Azumaya [2, §6, Lemma 4] has proven the following about the roots of a polynomial in $R[X]$.

THEOREM 3.12. *Let f be a monic polynomial in $R[X]$. If μf has a root $\bar{a}$ in k of multiplicity one then f has exactly one root a in R with $\mu a = \bar{a}$.*

COROLLARY 3.13. *A polynomial in J has no multiple roots in any local extension of R.*

PROOF. Replace the polynomial in J by its monic 'representative' (3.3) and then apply (3.12).

Let S and R be finite local rings with R a subring of S. The extension S or R is said to be *R-separable* if S is projective over its enveloping algebra $S \otimes_R S$. A polynomial f in $R[X]$ is called *separable* if f is monic and $R[X]/(f)$ is a separable extension of R. Finally, an element s of S is called *separable* over R if s is the root of a separable polynomial in $R[X]$.

Let f be a monic polynomial of degree n in $R[X]$. The free R-module $R[X]/(f)$ has a natural basis $X^0 = 1, X, \cdots, X^{n-1}$. Let π_i denote the projection of $R[X]/(f)$ onto the coefficient of X^i. Then the *trace map* $\mathrm{tr} : R[X]/(f) \to R$ is defined by

$$\mathrm{tr}(g) = \sum \pi_i(gX^i)$$

for g in $R[X]/(f)$. The following is due to Janusz [13, Theorem 2.2, part (5)]:

THEOREM 3.14. *Let f be a monic polynomial in $R[X]$. Then f is separable if and only if the determinant of the matrix $[\mathrm{tr}(X^iX^j)]$, $0 \leqq i, j \leqq \deg f$, is a unit of R.*

THEOREM 3.15. *A monic polynomial f in $R[X]$ is separable if and only if μf is square-free.*

PROOF. Let $\mathrm{tr} : R[X]/(f) \to R$ and $\overline{\mathrm{tr}} : k[X]/(\mu f) \to k$ be the trace maps. Note that $\mu(\det[\mathrm{tr}(X^iX^j)]) = \det[\overline{\mathrm{tr}}(X^iX^j)]$ and recall that a is a unit of R if and only if $\mu a \neq 0$. By direct computation $\det[\overline{\mathrm{tr}}(X^iX^j)] \neq 0$ if and only if μf is square-free. The last statement follows from the well-known relationship between $[\overline{\mathrm{tr}}(X^iY^j)]$ and the discriminant (for example see [9, pp. 29–31]).

The following provides the connection between separable polynomials, irreducible polynomials and J.

THEOREM 3.16. *Let f be a monic polynomial in $R[X]$. The following are equivalent:*

(a) *f is separable and local.*

(b) *f is irreducible and in J.*

(c) *μf is irreducible in $k[X]$.*

PROOF. This follows from (3.4), (3.7), and (3.15).

We now undertake to show that separable polynomials admit unique factorizations as products of irreducible polynomials in J. By Hensel's Lemma it is easy to show that if $f = f_1^{k_1} \cdots f_r^{k_r}$ and $f = g_1^{t_1} \cdots g_s^{t_s}$ where f_i and g_j are monic, pairwise coprime and irreducible polynomials in J then for each i there is a j with $\deg f_i = \deg g_j$ and $\mu f_i = \mu g_j$.

LEMMA 3.17. *Let f be a monic polynomial in $R[X]$. Suppose that $f = f_1 f_2 \cdots f_r$ where the f_i are monic, irreducible and pairwise coprime polynomials in J. Suppose, in addition, $f = g_1^{t_1} \cdots g_s^{t_s}$ where the g_i are monic irreducible polynomials in $R[X]$. Then $t_i = 1, 1 \leqq i \leqq s$, $s = r$ and the g_i may be ordered so that $\mu f_i = \mu g_i$.*

PROOF. Clearly $\mu f_i \neq \mu f_j$ for $i \neq j$ and the μf_i are irreducible thus μf is square-free. Hence $t_i = 1, 1 \leqq i \leqq s$, and the μg_i and thus the g_i are irreducible. Also $\mu g_i \neq \mu g_j$ for $i \neq j$ so $s = r$ and the result follows.

THEOREM 3.18. *Let f be a separable polynomial in $R[X]$. Then*

(a) *f factors uniquely as a product of distinct monic irreducible polynomials in $R[X]$. Further these factors lie in J.*

(b) *f has distinct zeros in any local extension of R.*

PROOF. Since f is separable by (3.15) μf is square-free. Then $\mu f = \bar{f}_1 \cdots \bar{f}_r$ where $\bar{f}_i$ are monic, pairwise coprime and irreducible in $k[X]$. By Hensel's Lemma there exist preimages f_i of $\bar{f}_i$ for $1 \leqq i \leqq r$ in J with $f = f_1 \cdots f_r$. The f_i are monic and irreducible. Suppose $f = g_1^{t_1} \cdots g_s^{t_s}$ is a second factorization of f into monic irreducible polynomials in $R[X]$. By (3.17) $r = s, t_i = 1$ and we may suppose that $\bar{f}_i = \mu g_i$. Since $\bar{f}_1$ and $(\mu g_2) \cdots (\mu g_r)$ are coprime in $k[X]$ there exist h_1 and h_2 in $R[X]$ with $h_1 f_1 + h_2(g_2 \cdots g_r) = 1$. Thus $g_1 = h_1 f_1 g_1 + h_2(g_1 g_2 \cdots g_r)$ and since f_1 divides $f = g_1 \cdots g_r$ then f_1 divides g_1. By symmetry $f_1 = g_1$. The proof follows by induction. Part (b) follows since $\bar{f}_i \neq \bar{f}_j$ $(i \neq j)$ and (3.12) imply the roots are distinct in any local extension of R.

To analyze the method of solution of a polynomial in $R[X]$ we extend the classical theory of higher order congruences.

If $\beta = \eta(R)$ we have the natural sequence

$$R = R/m^{\beta} \xrightarrow{\sigma_\beta} R/m^{\beta-1} \to \cdots \to R/m \xrightarrow{\sigma_1} 0$$

where the kernel of $\sigma_i = m^{i-1}/m^i$ is a k-vector space. Denote σ_i by σ and $\mu_i : R/m^i \to k$ by μ. Note that the action of k on m^{i-1}/m^i i given by $\bar{\alpha}m = \alpha m$ where $\mu\alpha = \bar{\alpha}$. Let $\dim_k(m^{i-1}/m^i) = t$ and $\{v_1, \cdots, v_t\}$ be a fixed k-basis for m^{i-1}/m^i. We now construct solutions of f in $(R/m^i)[X]$ from solutions of σf in $(R/m^{i-1})[X]$.

Let $\bar{a}$ in R/m^{i-1} be a solution of σf and let $\sigma a = \bar{a}$. Let $A = a + p$ for some p in m^{i-1}/m^i. The object is to select p so that $f(\mathrm{A}) = 0$ in R/m^i.

Since $(m^{i-1}/m^i)^2 = 0$,

$$f(\mathrm{A}) = f(a + p) = f(a) + pf'(a) + p^2Q = f(a) + pf'(a)$$

where f' is the formal derivative of f and Q is in R/m^i.

Requiring that $f(A) = 0$ implies

$$f(a) = -pf'(a) = \mu[f'(a)]p$$

since p is in m^{i-1}/m^i. Further, since $(\sigma f)(\bar{a}) = 0$, $f(a)$ is in m^{i-1}/m^i. Thus, relative to the k-basis $\{v_1, \cdots, v_t\}$,

$$f(a) = \sum_i b_i v_i \quad \text{and} \quad p = \sum_i a_i v_i$$

where a_i and b_i are in k. Hence

$$\begin{aligned} 0 &= \sum b_i v_i + \mu[f'(a)] \left(\sum a_i v_i \right) \\ &= \sum (b_i + \mu[f'(a)]\, a_i) v_i. \end{aligned}$$

Thus, for each i we must have

$$0 = b_i + \mu[f'(a)]\, a_i.$$

Three cases arise:

(a) $f'(a)$ is a unit. In this case, $\mu[f'(a)] \neq 0$ and each a_i is uniquely determined. Thus there is exactly one solution A of f with $\sigma A = \bar{a}$.

(b) $f'(a)$ is in m/m^i and there exists a $b_j \neq 0$. In this case there are no solutions A of f with $\sigma A = \bar{a}$.

(c) $f'(a)$ is in m/m^i and $b_j = 0$ for all j. In this case $f(A) = 0$ for any A with $\sigma A = \bar{a}$. Thus there exist $|k|^t = |k|^{\dim(m^{i-1}/m^i)} = |m^{i-1}/m^i|$ solutions A of f with $\sigma a = \bar{a}$.

Observe we obtain all solutions of f in this manner since if $f(a) = 0$ for f in $(R/m^i)[X]$ and a in R/m^i then σa satisfies σf in R/m^{i-1}.

Theorem 3.19. *Let f be a separable polynomial in $R[X]$. If μf has zeros $\bar{a}_1, \cdots, \bar{a}_t$ in k, then we may construct zeros $a_1, \cdots, a_t$ of f in R with $\mu a_i = \bar{a}_i$.*

Proof. Observe for each i, $1 \leqq i \leqq \eta(R)$, in the previous discussion the element $f'(a)$ is a unit for any preimage a of a root $\bar{a}$.

4. **The Galois Theory — Part I.** Throughout the remaining sections R denotes a finite local ring with maximal ideal m and residue field $k = R/m$. We let S denote a finite local ring with maximal ideal M and residue field $K = S/M$. We further assume that R is a subring o S. The purpose of this section is to describe the standard results con- cerning S and its R-automorphisms when S is a Galois extension of R.

If S is a separable R-algebra then S/mS is a separable field extensio of R/m [1]. The local ring S is called *unramified* if $M = mS$; i.e., m generates M in S. We have the following adaptation of a result b Auslander and Buchsbaum [1].

THEOREM 4.1. *The local ring S is a separable extension of R if an only if S is unramified over R.*

THEOREM 4.2 (PRIMITIVE ELEMENT THEOREM). *If S is separable ove R, then S is a simple extension of R; i.e., S has a primitive element.*

PROOF. By (4.1) $M = mS$. Since S/mS is a finite field it has a cycli group of units with generator $\bar{a}$. Let a be a preimage of $\bar{a}$ in S Since $S/mS = (R/m)[\bar{a}]$ we have $S = R[a] + mS$. By Nakayama' Lemma $S = R[a]$.

We note that for most classes of commutative rings there is not Primitive Element Theorem available. However, the presence of primitive element permits separable polynomials to play a central rol in the Galois theory (for discussion and example in the general cas see [**12**, p. 113]).

Let H be a group of R-ring automorphisms of S. Then

$$S^H = \{x \in S \mid \rho(x) = x \text{ for all } \rho \text{ in } H\}$$

is called the *fixed ring of H in* S. If G is the group of all R-ring auto morphisms of S and $S^G = R$, then S is called a *normal* extension of R A normal separable extension S of R is called a *Galois* extension an the group of all R-automorphisms of S is called the *Galois group* of over R and is denoted by $\mathcal{G}_R(S)$.

The local case provides information about the automorphism grou of any finite commutative ring. Suppose $\bar{S} = \oplus \sum_{i=1}^{n} S_i$ where S is a local extension of a local ring R_i. Let e_i be the identity of S_i an $\bar{R} = \oplus \sum R_i$. Let $\prod_j : \bar{S} \to S_j$ be the natural projection an $\lambda_j : S_j \to \bar{S}$ satisfying $\prod_K a^{(i)} = 0$, $K \neq i$, and $\prod_i a^{(i)} = a$. If ρ is a $\bar{R}$-automorphism of $\bar{S}$ then $\rho a^{(i)} = \rho(e_i{}^{(i)}a)$. But $e_i{}^{(i)}$ is in $\bar{R}$ thus $\rho a^{(i)} =$ $e_i{}^{(i)}\rho(a^{(i)})$ is in S_i and since ρ is an isomorphism $\rho S_i = S_i$. If $\rho_i = \prod_i \rho$ then ρ_i is an R_i-automorphism of S_i and $\rho = \rho_1 \oplus \cdots \oplus \rho_n$. Furth $\bar{S}$ is separable over $\bar{R}$ if and only if for each i, $1 \leqq i \leqq n$, S_i is R separable. A similar remark holds for normality. Thus $\mathcal{G}_{\bar{R}}(\bar{S}) =$ $\oplus \sum \mathcal{G}_{R_i}(S_i)$.

We now state the fundamental theorem of Chase, Harrison, and Rosenberg [3, Theorem 2.3], on the Galois theory of commutative rings in the form we need. A ring S is a *free* extension of R if S is free as an R-module.

THEOREM 4.3 (CHASE, HARRISON, ROSENBERG). *Let S be a Galois extension of R with $\mathcal{G} = \mathcal{G}_R(S)$. Then*

(a) *S is a free extension of R and* $|\mathcal{G}| = \dim_R S$.

(b) *There is a lattice inverting bijection between the subgroups of $\mathcal{G}$ and the set $\mathcal{S}$ of R-separable subrings of S containing R. Normal subgroups of $\mathcal{G}$ correspond to normal extensions of R in S.*

(c) *The correspondence of* (b) *is given by*

$$H \leftrightarrow S^H = \{x \text{ in } S \mid \rho x = x \text{ for all } \rho \text{ in } H\},$$

$$T \leftrightarrow \{\rho \text{ in } G \mid \rho x = x \text{ for all } x \text{ in } T\}$$

where H is a subgroup of $\mathcal{G}$ and T is in $\mathcal{S}$.

Any free local separable extension of R may be embedded in a normal extension. Precisely,

LEMMA 4.4 (JANUSZ). *Let S be a free separable extension of R. Then there exists a finite normal local extension T of R with S in T.*

LEMMA 4.5. *If S is a Galois extension of R with group $\mathcal{G}$, then* $|\mathcal{G}| = [S/M, R/m]$.

PROOF. The set $\{v_1, \cdots, v_n\}$ is a free R-basis for S if and only if $\{v_1 + M, \cdots, v_n + M\}$ is an R/m-basis for S/M.

5. **The Galois theory — Part II.** This section is devoted to a sharpening of the results in (4); in particular, we improve (4.3) to (5.11).

THEOREM 5.1 (AZUMAYA). *Let S be a free separable extension of R. Then if $\bar{\rho}$ is an R/m-automorphism S/M there exists exactly one R-automorphism ρ of S which induces ρ.*

PROOF. Note S/M is a finite field and $S/M = (R/m)[\bar{a}]$. Let $\bar{f} = \operatorname{Irr}(R/m, \bar{a})$ and suppose $n = \deg \bar{f} = [S/M, R/m]$. Let f be a preimage of $\bar{f}$ in J. By (3.12) there is precisely one element a in S which is a preimage of $\bar{a}$ and a root of f. The set $\{1, \bar{a}, \cdots, \bar{a}^{n-1}\}$ is an R/m-basis of S/M. Since S is R-free and thus minimal R-generating sets are free, the set $\{1, a, \cdots, a^{n-1}\}$ is a free R-basis of S. Let $\bar{\rho}(\bar{a}) = \bar{a}_0$. Then $\bar{a}_0$ is a root of $\bar{f}$. There is exactly one preimage a_0 of $\bar{a}_0$ which is a root of f. Define $\rho : S \to S$ by $\rho a = a_0$. Since $\{1, a, \cdots, a^{n-1}\}$ is R-free, ρ extends to a unique R-morphism of S. Clearly

ρ is a ring morphism. The set $\{1, a_0, \cdots, a_0^{n-1}\}$ also forms a free R-basis for S so ρ is surjective. Surjective R-morphisms of finitely generated modules are injective so ρ is an R-ring automorphism of S. Uniqueness follows from (3.12).

THEOREM 5.2. (a) *S is a free separable extension of R if and only if S is a Galois extension of R.*

(b) *If S is a Galois extension of R, then* $\mathcal{G}_R(S)$ *is isomorphic to* $\mathcal{G}_{R/m}(S/M)$ *and thus is a finite cyclic group.*

PROOF. Galois extensions are free separable extensions. Conversely, let H denote the group of R-automorphisms of S. If ρ is in H, then ρa is a unit (resp., nilpotent) if and only if a is a unit (resp., nilpotent). Thus M is characteristic under H, and hence ρ induces naturally an R/m-ring morphism $\bar{\rho}$ which is obviously an R/m-automorphism. Let $\pi : H \to \mathcal{G}_{R/m}(S/M)$ be given by $\pi\rho = \bar{\rho}$. Then π is a group morphism and injective by (5.1) thus an isomorphism. Hence H is cyclic. By (4.4) S may be embedded in a local Galois extension T of R. By the same argument $\mathcal{G}_R(T)$ is cyclic with normal subgroup H. Thus by (4.3) S is normal and thus a Galois extension of R.

The proof of the above result utilizes the full strength of the Chase-Harrison-Rosenberg Galois theory. There appears to be no simple way to provide a direct proof (short of redeveloping the Galois theory) as in other results.

In (5.2) "free and separable" is equivalent to "Galois". We now show that "free" may be omitted. This is a significant departure from the standard Galois theory of commutative rings.

THEOREM 5.3. *The following are equivalent:*

(a) *S is unramified over R.*

(b) *S is separable over R.*

(c) *S is a Galois extension of R.*

PROOF. By (4.1), (a) and (b) are equivalent. Further (5.1) shows that (c) implies (b). It remains to show that either (a) or (b) imply (c). Let $K = k[\bar{a}]$ and $\bar{f}$ be the minimal polynomial of $\bar{a}$ in $k[X]$. Let f be a monic preimage of $\bar{f}$ in $R[X]$ with $n = \deg(\bar{f}) = [K : k]$. Then, if a is a preimage of $\bar{a}$, since $S = R[a]$ we have $f(a) = \sum_{i=0}^{n-1} m_i a^i = g(a)$ where m_i are in M. Set $h(X) = f(X) - g(X)$, then $h(a) = 0$ and $\mu h = \bar{f}$ so h is monic and irreducible. We have a natural ring morphism $R[X] \to S$ by $X \to a$ which induces a surjective R-algebra morphism $\phi : R[X]/(h) \to S$. We claim that $|S| = |R[X]/(h)|$. If this is so, then ϕ is also injective, hence ϕ is an isomorphism, and since $R[X]/(h)$ is R-free, so is S.

We now show that if S is unramified over R then $|S| = |R[X]/(h)|$. Note $|R[X]/(h)| = |R|^{\deg(h)} = |R|^{[K:k]}$. Let β denote the nilpotency of M. We have the following natural sequence of surjective ring morphisms σ_i:

$$S = S/M^{\beta_\nu} \xrightarrow{\sigma_\beta} S/M^{\beta-1} \xrightarrow{\sigma_{\beta-1}} \cdots \xrightarrow{\sigma_2} S/M = K$$

where $\ker(\sigma_i) = M^{i-1}/M^i$. Clearly

$$|S| = |K| \prod_{i=2}^{\beta} |\ker(\sigma_i)| = |K| \prod_{i=2}^{\beta} |M^{i-1}/M^i|.$$

Using the facts that $M = Sm$ and $mS \otimes_R m^i \subseteq S \otimes_R m^i$ we have $M^{i-1}/M^i = Sm^{i-1}/Sm^i$

$$\begin{aligned} &\simeq (S \otimes_R m^{i-1})/(S \otimes_R m^i) \\ &\simeq (S \otimes_R m^{i-1})/(mS \otimes_R m^i + S \otimes_R m^i) \\ &\simeq (S/mS) \otimes_k (m^{i-1}/m^i) \simeq K \otimes_k (m^{i-1}/m^i). \end{aligned}$$

Thus

$$|M^{i-1}/M^i| = |m^{i-1}/m^i|^{[K:k]}$$

and

$$\begin{aligned} |S| &= |K| \left(\prod_{i=2}^{\beta} |m^{i-1}/m^i| \right)^{[K:k]} \\ &= \left(|k| \prod_{i=2}^{\beta} |m^{i-1}/m^i \right)^{[K:k]} = |R|^{[K:k]} \end{aligned}$$

and we are done.

The following result by Janusz [13, Corollary 2.8] is useful in finding Galois extensions.

Lemma 5.4. *Let S be a Galois extension of R and suppose for some a in S the subring $R[a]$ is a separable extension of R. Let $a = a_1, a_2, \cdots, a_n$ be the distinct images of the element a under $\mathcal{G}_R(S)$. If g is in $R[X]$ and $g(a) = 0$ then g is divisible by $f(X) = (X - a_1) \cdots (X - a_n)$.*

Using (5.2) and the observation that $R[X] \rightarrow R[a]$ is a surjective R-ring morphism the following is immediate.

COROLLARY 5.5. *Let S be a Galois extension of R. Then*

(a) *The Galois group $\mathcal{G}_R(S)$ permutes the roots of a separable polynomial f in $R[X]$ where f is satisfied by a primitive element a generating S over R.*

(b) *In addition to* (a), $\deg f = \dim_R S$ *and* $S = R[a] \simeq R[X]/(f)$.

Thus, by (3.16),

THEOREM 5.6. *Let S be an extension of R. Then S is a Galois extension of R if and only if S is R-algebra isomorphic to $R[X]/(f)$ where f is a monic irreducible polynomial in J.*

The next two results generalize a remark by Janusz.

THEOREM 5.7. *Let S be a Galois extension of R with* $\dim_R S = n$. *Let t denote the number of monic irreducible polynomials of degree n in J and r denote the number of primitive elements of S over R. Then $tn = r$.*

PROOF. Note that $t = \bar{t}|m|^n$ and $r = \bar{r}|M|$ where $\bar{t}$ and $\bar{r}$ are the analogous values for the extension S/M over R/m. It is well known that $\bar{t}[S/M : R/m] = \bar{t}n = \bar{r}$. Thus, it is necessary to show $|m|^n = |M|$. If a is a primitive element for S, then $\{1, a, \cdots, a^{n-1}\}$ is an R-basis for S and their images $\{\bar{1}, \cdots, \bar{a}^{n-1}\}$ form an R/m-basis for S/M. If $d_0 + d_1a + \cdots + d_{n-1}a^{n-1}$ is in M where the d_i are in R, then $\bar{d_0} + \cdots + \bar{d}_{n-1}\bar{a}^{n-1} = 0$ and $d_i = 0$, $0 \leqq i \leqq n-1$. Thus the d_i are in $R \cap M = m$. Conversely any element of the above form is in M. Hence $|M| = |m|^n$.

THEOREM 5.8 (UNIQUENESS OF GALOIS EXTENSION). *For each positive integer n there exists exactly one (up to R-algebra isomorphism) Galois extension S of R with* $\dim_R S = n$.

PROOF. The existence follows from (5.6). Observe a standard argument shows that the uniqueness of the Galois extension is equivalent to (5.7).

It is well known that if $v(n, k)$ denotes the number of monic irreducible polynomials of degree $n = p_1^{e_1} \cdots p_s^{e_s}$ in $k[X]$ then

$$v(n,k) = \frac{1}{n}\Big[\, |k|^n - \sum |k|^{n/p_i} + \sum |k|^{n/p_i p_j} - \cdots + (-1)^s |k|^{n/p_1p_2\cdots p_s}\Big] .$$

Thus, by (3.4), there exist

$$\begin{aligned} v(n, R) &= v(n, k)|m|^n \\ &= \frac{1}{n}|R|^n \Big[1 - \sum |k|^{1/p_i} + \sum |k|^{1/p_ip_j} \\ &\qquad\qquad - \cdots + (-1)^s |k|^{1/p_1\cdots p_s} \Big] \end{aligned}$$

monic irreducible polynomials in J of degree n. Hence $nv(n, R)$ primitive elements for a Galois extension S of R with $\dim_R S = n$.

Preliminary to two examples it is useful to note that if S is an extension of R and a is an element of S, then the subring $R[a]$ is a separable extension of R if and only if a is separable over R.

Example. Let $R = Z/(4)$ and $f(X) = X^3 + X + 1$ in $R[X]$. Since μf is irreducible, f is irreducible. Hence $S = R[X]/(f)$ is a Galois extension of R, $\dim_R S = 3$, $\mathcal{G}_R(S)$ is cyclic of order 3 and there are no proper R-separable subrings of S.

For finite local rings, although the Galois group is cyclic, the generating automorphism of the Galois group cannot be described as a power map on all the elements.

Example. Let $R = Z/(4)$ and $S = R[a]$ where a satisfies $X^2 + X + 1$. Then $\mathcal{G}_R(S) = \{1, \rho\}$ where $\rho a = 3a + 3$. Note that no power of $2a$ is $2a + 2 = \rho(2a)$. Also $\rho(3a + 1) = a + 2$ and it is easy to check that $a + 2$ is not a power of $3a + 1$. However, $\rho a = 3a + 3 = a^2$. Thus $\mathcal{G}_R(S)$ is generated by an automorphism which takes a primitive element to its square.

Lemma 5.9. *Let S be a Galois extension of R and f a monic irreducible polynomial in J. If a and b are roots of f in S,* then there exists *a monic irreducible polynomial g in J such that $a^{|k|}$ and $b^{|k|}$ are roots of g.*

Proof. It is easy to see that we may select a monic polynomial g in J with $g(a^{|k|}) = 0$. Consider the polynomial $h(X) = g(X^{|k|})$. Note that a satisfies h. By (5.4) h is divisible by f. Since b satisfies f, b must be a root of h. Hence $b^{|k|}$ is a root of g.

Theorem 5.10. *Let S be a Galois extension of R with* $\dim_R S = n$. *Then there exists a primitive element a of S over R such that the R-automorphism ρ of S given by $\rho a = a^{|k|}$ is a generator of $\mathcal{G}_R(S)$.*

Proof. Let f be a monic irreducible polynomial of degree n in J and a be a root of f. Set $A = \{g \text{ in } J \mid g \text{ is monic and } \mu g = \mu f\}$, $B = \{b \text{ in } S \mid b \text{ is a root of some polynomial in } A\}$, and let $B^j = \{b^j \mid b \text{ in } B\}$ for $j = 1, 2, \cdots$. Clearly $B \supseteq B^{|k|} \supseteq B^{|k|^2} \supseteq \cdots$. Since $\mu f(X) = (X - \bar{a})(X - \bar{a}^{|k|}) \cdots (X - \bar{a}^{|k|^{n-1}})$ where $\mu a = \bar{a}$ and each element of B is a preimage of one of $\{\bar{a}, \bar{a}^{|k|}, \cdots, \bar{a}^{|k|^{n-1}}\}$, each element of B has the form $a^j + c$ where c is in M and $j = 1, |k|, \cdots, |k|^{n-1}$. Hence there exists an s such that $B^s = B^{s+1} = \cdots$ and B^s has only n elements. Raising each element of B^s to the $|k|$th power results only in a reshuffling. By (5.1) and previous lemma there is an R-automorphism ρ of S given by $\rho t = t^{|k|}$ where t is in B^s. Consider $\bar{\rho}, \bar{\rho}^2, \cdots, \bar{\rho}^n$ in $\mathcal{G}_{R/m}(S/M)$. These R/m-automorphisms are distinct since the map $b \rightarrow b^{|k|}$ generates $\mathcal{G}_{R/m}(S/M)$. Thus ρ generates $\mathcal{G}_R(S)$.

The integer s in the above proof may easily be bounded. If $\eta(R) = \beta$ and $a^j = c$ is in B with c in M then $(a^j + c)^{|k|^\beta} = a^{j|k|^\beta}$ since all other terms in the binomial expansion are zero.

A Galois extension S of R is a *splitting ring* for a separable polynomial f in $R[X]$ if f is the product of linear factors in $S[X]$ and S is generated over R by the roots of f.

We summarize with

THEOREM 5.11. *Let S be a Galois extension of R. Then*

(a) *S is unramified over R, R-free, and $|\mathcal{G}_R(S)| = \dim_R S = \deg f$ where f is a monic irreducible polynomial in J. Further, $S = R[a]$ where a is a root of f, $S \simeq R[X]/(f)$, S is a splitting ring of f, and S is the unique Galois extension of R of this dimension.*

(b) *$\mathcal{G}_R(S)$ is cyclic, isomorphic to $\mathcal{G}_{R/m}(S/M)$ and generated by the power map*

$$\rho : a^{|R/m|^{\eta(R)}} \rightarrow a^{|R/m|^{\eta(R)+1}}.$$

(c) *There is a lattice preserving bijection between the subfields of K containing k and the separable subrings of S containing R. If T is a separable extension of R in S, then T is a Galois extension of R and*

$$1 \rightarrow \mathcal{G}_R(T) \rightarrow \mathcal{G}_R(S) \rightarrow \mathcal{G}_R(S) \rightarrow 1$$

is exact.

(d) *There exists an element a in S such that $\{\sigma a \mid \sigma \in \mathcal{G}_R(S)\}$ is a free R-basis of S, i.e., S has a normal basis over R.*

The parts above which we have not shown are immediate.

6. **The Cohen Structure Theorem.** The purpose of this short section is to sketch a simple proof of the Cohen Structure Theorem. Standard proofs (for example, Nagata [16] or Cohen [7]) necessitate the introduction of concepts which are not needed for the finite case. Indeed the theorem for complete local rings may be sharpened in this setting.

THEOREM 6.1 (COHEN). *Let R be a finite local ring with $\chi(R) = p^\lambda$. Let the maximal ideal m of R have minimal generating set $\{u_1, \cdots, u_n\}$. Then there exists a subring T of R such that*

(a) *T is a separable (hence simple) extension of the prime ring $Z/Z_p{}^\lambda$.*

(b) *$T/(m \cap T) \simeq R/m$.*

(c) *R is the ring homomorphic image of $T[X_1, \cdots, X_n]$ and hence by* (a) *of $(Z/Zp^\lambda)[X_1, \cdots, X_n, X_{n+1}]$.*

Finally, the subring T (called the coefficient ring of R) is unique (absolutely!) and is the largest Galois extension of Z/Zp^λ in R.

PROOF. Let $\bar{v}$ be the generator of the group of units of R/m and let $\bar{f}$ be the $\mathrm{Irr}(\bar{v}, Z/Zp)$ in $(Z/Zp)[X]$. Let f be a monic preimage of $\bar{f}$ in J. By (3.12) R contains an element v with $f(v) = 0$ and $\mu v = \bar{v}$. Since v is separable, $(Z/Zp^\lambda)[v] \simeq (Z/Zp^\lambda)[X]/(f)$ is a separable extension of Z/Zp^λ. Let $T = (Z/Zp^\lambda)[v]$. Note there exists a natural injective ring morphism $T/(m \cap T) \to R/m$. Since $\bar{v}$ generates the units of R/m, the map is a surjection and $T/(m \cap T) \simeq R/m$. It now suffices to show that $T[u_1, \cdots, u_n] = R$. Obviously $T[u_1, \cdots, u_n]$ is a subset of R. Let c be in R. By the above $c \equiv a \bmod m$ for some a in T. Construct $\{c_j\}_{j=0}^{\beta-1} (\beta = \eta(R))$ such that $c \equiv c_j \bmod m^{j+1}$ and c_j is in $T[u_1, \cdots, u_n]$. This is done by letting $c_0 = a$, and, if $j \geqq 1$, $c_j = c - \sum b_i w_i$ where w_i is a power product of $\{u_1, \cdots, u_n\}$. There is an a_i in T with $b_i \equiv a_i \bmod m$, thus

$$c - c_j \equiv \sum a_i w_i \mod m^{j+2}.$$

Then set $c_{j+1} = c_j + \sum a_i w_i$. Since $m^\beta = 0$, $c = c_{\beta-1}$ and c is in $T[u_1, \cdots, u_n]$.

Note properties (a) and (b) of (6.1) together with the natural bijection between the lattice of separable subrings of T and the subfields of R/m imply that T is the largest separable, and thus, Galois extension of Z/Zp^λ in R. Uniqueness, in the sense that there is only one such ring T in R, is given by [**16**, (31.10), p. 111].

The emphasis of the above is on the maximal ideal of R. If instead we examine the units R^* of R a second semitrivial "structure" theorem is possible.

THEOREM 6.2. *Let R be a finite local ring with $\chi(R) = p^\lambda$. If $\{a_1, \cdots, a_s\}$ are the generators of the group of units of R, then R is a ring homomorphic image of $(Z/Zp^\lambda)[X_1, \cdots, X_s]$.*

PROOF. Consider the subring $(Z/Zp^\lambda)[a_1, \cdots, a_s]$ of R. Clearly this subring contains each unit of R. Let a be in the maximal ideal m. For b a unit, $a - b = c$ is a unit. Thus $a = b + c$ is in $(Z/Zp^\lambda)[a_1, \cdots, a_s]$.

We note several special cases. Hungerford [**11**] showed that if the maximal ideal is principal, then R is the homomorphic image of a principal ideal domain S and thus has the form S/Sp^n for some prime p of S.

The Galois extensions of the quotient rings of the rational integers Z/Zp^n (p prime) are particularly interesting: We let $GR(p^n, r)$ denote the Galois extension of Z/Zp^n of degree r and call this the *Galois ring* of degree r over Z/Zp^n. These rings were perhaps first noticed by Krull in 1924 [**14**]. They were rediscovered by Janusz [**13**] (and we recently noted also by Raghavendran [**20**]). Note that $GR(p^n, r)$ is a principal ideal ring and thus a homomorphic image of a principal ideal domain, $GR(p^n, 1) = Z/Zp^n$ and $GR(p, r) = GF(p^r)$. They are proving useful since finite noncommutative rings may be naturally considered as algebras over Galois rings.

7. **Units of finite rings.** Let R^* denote the group of units of a local ring R. The decomposition of a finite commutative ring into local rings induces a natural decomposition of the group of units; hence, our interest will be in the units of the local ring R.

All local rings R with R^* cyclic were determined by Gilmer [**10**] (also proofs are given in [**20**], [**17**]). Pearson and Schneider have found all R where R^* is generated by two elements. Clark has investigated R^* where the ideals form a chain and has shown that if $p \geqq 3$, $n \geqq 2$ and $r \geqq 2$, then the units of the Galois ring $GR(p^n, r)$ are a direct sum of a cyclic group of order $p^r - 1$ and r cyclic groups of order p^{n-1} (this was also done independently by Raghavendran [**20**]).

Let R have maximal ideal m of nilpotency β and let $\phi_i = |m^{i-1}/m^i|$, $1 \leqq i \leqq \beta$, where $R = m^0$. Then it is easy to see that

$$|R^*| = \left(\prod_{i=2}^{\beta} \phi_i\right)(\phi_1 - 1) = (\text{power of } p)\,(|R/m| - 1).$$

Thus $R^* \simeq$ (Abelian p-group) × (cyclic group of order $|R/m| - 1$). We conjecture that the p-group is intimately connected with the R/m-spaces m^{i-1}/m^i for $1 \leqq i \leqq \beta$. Below we provide a solution for $\beta = 2$ (of interest to some).

Denote the order of a unit u by $o(u)$ and consider the natural ring morphism $\sigma_i : R/m^i \to R/m^{i-1}$ for some i, $1 \leqq i \leqq \beta$.

LEMMA 7.1. *If u is a unit in R/m^{i-1} with $o(u) = t$ and $\sigma_i w = u$ then w is a unit in R/m^i and $o(w) = t$ or $o(w) = pt$.*

PROOF. Suppose $t' = o(w)$. Then t divides t'. But $\sigma_i(w^t) = 1$, so $w^t = 1 + v$ for some v in m^{i-1}/m^i. Then

$$(w^t)^p = (1 + v)^p = 1 + pQ = 1$$

where Q is in m^{i-1}/m^i (thus $pQ = 0$). Thus $o(w)$ divides pt. Hence $o(w) = t$ or $o(w) = pt$.

Let $\epsilon(u)$ denote the cyclic group of order u.

PROPOSITION 7.2. *Let R be a finite local ring with $\eta(R) = 2$. Then*

$$R^* = \left(\oplus \sum_{i=1}^{nt} \epsilon(p) \right) \oplus \epsilon(|k| - 1)$$

where $n = \dim_k(m/m^2)$ and $|k| = p^t$.

PROOF. Let A denote the p-group summand of R^*. The group A is a direct sum of cyclic p-groups. Suppose the generators of A are $\{e_1, \cdots, e_s\}$. Since $o(e_i)$ is a power of p and p does not divide $|k| - 1$, we must have $\sigma_2(e_i) = 1$, $1 \leqq i \leqq s$. Hence, by (7.1), $o(e_i) = p$. Thus A is a direct sum of cyclic groups of order p. Finally,

$$|A| = \mathrm{Ker}(\sigma_2)| = |m/m^2| = |k|^n = p^{tn}.$$

BIBLIOGRAPHY

1. M. Auslander and D. A. Buchsbaum, *On the ramification theory in noetherian rings*, Amer. J. Math. 81 (1959), 749-765. MR 21 #5659.

2. G. Azumaya, *On maximally central algebras*, Nagoya Math. J. 2 (1951), 119-150. MR 12, 669.

3. S. U. Chase, D. K. Harrison and A. Rosenberg, *Galois theory and cohomology of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965), 15-33. MR 33 #4118.

4. W. E. Clark, *A coefficient ring for finite non-commutative rings* (submitted).

5. W. E. Clark and D. A. Drake, *Finite chain rings* (submitted).

6. W. E. Clark and J. J. Liang, *Enumeration of finite commutative chain rings* (submitted).

7. I. S. Cohen, *On the structure and ideal theory of complete local rings*, Trans. Amer. Math. Soc. 59 (1946), 54-106. MR 7, 509.

8. R. W. Davis, *Certain matrix equations over rings of integers*, Duke Math. J. 35 (1968), 49-59. MR 36 #3809.

9. M. Eichler, *Introduction to the theory of algebraic numbers and functions*, Birkhäuser, Basel, 1963; English transl., Pure and Appl. Math., vol. 23, Academic Press, New York, 1966. MR 29 #5821; 35 #160.

10. R. W. Gilmer, *Finite rings having a cyclic group of units*, Amer. J. Math. 85 (1963), 447-452. MR 27 #4828.

11. T. W. Hungerford, *On the structure of principal ideal rings*, Pacific J. Math. 25 (1968), 543-547. MR 37 #2744.

12. E. Ingraham and F. DeMeyer, *Separable algebras over commutative rings*, Lecture Notes in Math., vol. 181, Springer-Verlag, Berlin and New York, 1971. MR 43 #6199.

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

14. W. Krull, *Algebraische Theorie der Ringe,* Math. Ann. **92** (1924), 183–213.

15. B. R. McDonald, *Involutory matrices over finite local rings,* Canad. J. Math. (to appear).

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

17. K. R. Pearson and J. E. Schneider, *Rings with a cyclic group of units,* J. Algebra **16** (1970), 243–251. MR **42** #315.

18. ———, *On the group of units of a finite commutative ring* (to appear).

19. D. Price and R. Kruse, *Nilpotent rings,* Gordon and Breach, New York, 1969. MR **42** #1858.

20. R. Raghavendran, *Finite associative rings,* Compositio Math. **21** (1969), 195–229. MR **40** #174.

21. ———, *A class of finite rings,* Compositio Math. **22** (1970), 49–57. MR **41** #8475.

22. R. Wirt and B. R. McDonald, *On the theory of finite rings and finite local rings* (submitted).

23. O. Zariski and P. Samuel, *Commutative algebra,* Vol. II, University Series in Higher Math., Van Nostrand, Princeton, N. J., 1960. MR **22** #11006.

Whitworth College, Spokane, Washington 99218

University of Oklahoma, Norman, Oklahoma 73069