THE UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

FINITE LOCAL RINGS

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

degree of

DOCTOR OF PHILOSOPHY

BY

GARY LAYTON GANSKE

Norman, Oklahoma

1971

FINITE LOCAL RINGS

APPROVED BY

Bernard R. McDonald

John C. Brixey

George M. Ewing

Gene Levy

Leonard R. Rubin

DISSERTATION COMMITTEE

ACKNOWLEDGMENTS

I am grateful to my dissertation advisor, Professor Bernard McDonald, who suggested the topic and gave me the guidance and encouragement without which this paper would not have been completed.

I also wish to thank my wife, Karen, for her aid in typing this paper and for her encouragement and understanding during its preparation.

TABLE OF CONTENTS

Page

INTRODUCTION 1

Chapter

I. SURVEY OF FINITE COMMUTATIVE RINGS 3

II. THE POLYNOMIAL RING OF A FINITE LOCAL RING .. 22

III. GALOIS THEORY OF FINITE LOCAL RINGS 35

IV. A STRUCTURE THEOREM 50

V. SOLUTIONS OF POLYNOMIALS OVER FINITE LOCAL RINGS 53

BIBLIOGRAPHY 56

INTRODUCTION

The well-known theory of separable extensions of field theory and its Galois theory gives rise to the question: How much of the theory mentioned above can be generalized for some class of rings. One of the best known developments in this area came in 1965 when Chase, Harrison and Rosenberg [5.] proved a theorem analagous to the Galois theorem for fields. Then in 1966 Janusz [10.] generalized the concepts of separable elements and polynomials.

This paper has been in large motivated by the following consideration: In finite fields the results on separable extensions are much sharper than the general theorems. For example any finite extension of a finite field is separable and its Galois group is cyclic. Hence to what extent can these sharper results for finite fields be extended to finite rings.

Chapters I and IV are essentially specializations of well-known results to finite commutative rings. For completeness the proofs of most of the theorems of Chapter I are given and follow those of the general theorems. Also in Chapter I the consideration of problems dealt with in Chapters II and III are reduced to considerations of finite local rings.

In Chapter II we consider elementary facts concerning the polynomial ring R[x], R a finite local ring. We have also characterized certain classes of polynomials in R[x] which arise naturally in the investigations of Chapter III.

In Chapter III we generalize the basic theorems of finite fields and their extensions. As a corollary to his results on homomorphic images of Dedekind domains, G. J. Janusz [10.] has proven some of these theorems for finite separable extensions of the ring generated by the identity. We have shown that these theorems are true for finite extensions of any finite local ring.

In Chapter V we touch on the solutions of congruences over finite local rings which includes the classical case of congruences over the integers modulo the power of a prime.

CHAPTER I

SURVEY OF FINITE COMMUTATIVE RINGS

The object of this chapter is threefold. First to survey the decomposition theory of finite commutative rings. Second to introduce the basic definitions that will be needed later. Third to prove the primitive element theorem for a given class of finite rings.

The Decomposition Theory of Finite Commutative Rings

In this section we specialize more general decomposition theorems and sketch their proofs.

Recall the following basic definitions:

Definition 1.1. A *commutative ring* R is a set with two binary operations, denoted by + and juxtaposition such that:

(i) (R, +) is a commutative group.

(ii) (R, .) is a commutative semigroup.

(iii) If a, b and c are elements of R then $(a + b)c = ac + bc$.

Throughout this section R denotes a finite commutative ring.

Definition 1.2. A proper ideal P of R is a *prime ideal* if whenever a and b are elements of R and ab is in P then a is in P or b is in P.

Definition 1.3. A proper ideal M of R is a *maximal ideal* if whenever $M \subsetneq N \subseteq R$ for an ideal N of R then N = R.

Since R has only finitely many ideals the existence of maximal ideals is guaranteed if $R \neq 0$. However in general R may not have any prime ideals.

Example 1.1. Let $R = 2Z/8Z$ where Z is the rational integers. The ideals of R are 0, (4) and R. Hence R has the maximal ideal (4) but has no prime ideals.

Definition 1.4. The prime radical P(R) of R is the intersection of all prime ideals in R (If R has no prime ideals then P(R) = R).

Definition 1.5. The nil radical N(R) of R equals $\{x \text{ in } R\colon x^n = 0 \text{ for some natural number } n\}$. An element of N(R) is called a nilpotent element.

Definition 1.6. The Jacobson radical J(R) of R is the intersection of all the maximal ideals of R.

Example 1.2. Let $R = 2Z/8Z$. Then $J(R) \subsetneq N(R) = P(R)$.

Theorem 1.1. If R is a finite commutative ring then N(R) and P(R) are equal.

Proof: If P(R) = R then $N(R) \subseteq P(R)$. If $P(R) \neq R$ then let P_i $i = 1, \ldots , n$ be the prime ideals of R. If x is an element of N(R) then $x^m = 0$ is in P_i for some positive integer m. Since P_i is prime x is in P_i. Hence $N(R) \subseteq P(R)$.

Conversely, suppose x is not in N(R) then $T = \{x, \ldots , x^n, \ldots\}$ does not contain 0. Hence we can find an ideal P which is maximal with respect to the exclusion of T. The proof will be complete once we show P is prime. If a and b are in R and ab is in P and a and b are not in P then P + aR and P + bR meet T. Hence x^n is in $(P + aR)(P + bR) \subseteq P$

for some positive integer n. But this is a contradiction since $P \cap T = \emptyset$.

It is advantageous to know when a finite commutative ring has an identity.

Theorem 1.2. A finite commutative ring R has an identity if and only if R contains an idempotent element e which is a non-zero divisor. If e exists then e is an identity.

Proof: Let r be an element of R; then $(r - re)e = 0$. Hence $r = re$ and e is an identity.

Although the above is trivial it does provide us with insight into the next two proofs.

Theorem 1.3. If R is a finite commutative ring with at least one non-zero divisor then R has an identity.

Proof: Let a be a non-zero divisor in R. Let $a, a_2, \ldots, a_n$ be the elements of R. Since a is a non-zero divisor, $a^2, aa_2, \ldots, aa_n$ are all distinct, hence are all the elements of R. So there exists a_i in R such that $aa_i = a$. Thus $aa_i = aa_i^2$. So a_i is an idempotent. From $a = aa_i$ it is clear that a_i is a non-zero divisor. The result now follows from Theorem 1.2.

Corollary. If R is a finite integral domain then R is a finite field.

Theorem 1.4. If R is a finite commutative ring and $N(R) = 0$ then R has an identity.

Proof: Let L be a minimal ideal of R and b a non-zero element of L. Since $N(R) = 0$, $b^2 \neq 0$. Hence $bL = L$. Thus there exists e in L such that $be = b$. Let $I = \{x \text{ in } L\text{: } xb = 0\}$. Clearly, I is an ideal of

R and is contained in L. But e is not in I. Hence, by the minimality of L, I = 0. But $e^2 - e$ is in I, so e is a non-zero idempotent. We must find an idempotent which is a non-zero divisor. For each idempotent e in R let $M_e = \{r \text{ in } R: re = 0\}$. Choose e such that M_e is minimal in $\{M_e\}$. If $M_e \neq 0$ then M_e contains a minimal ideal. Hence from the first part M_e contains a non-zero idempotent e_1. Let $e_2 = e + e_1$. Since $ee_1 = 0$, e_2 is an idempotent. One checks that $M_{e_2} \subsetneq M_e$. This contradicts the minimality of M_e. Hence $M_e = 0$ and e is the desired element.

In the case R has an identity we can improve Theorem 1.1.

<u>Theorem</u> 1.5. Let R be a finite commutative ring with identity 1. Then P is a prime ideal in R if and only if P is a maximal ideal in R.

<u>Proof</u>: If P is a prime ideal in R then R/P is a finite integral domain, hence a field. However if R/P is a field then P is a maximal ideal. The equivalence is completed by noting that in a ring with identity any maximal ideal is prime.

<u>Corollary</u>. If R is a finite commutative ring with identity then J(R) = N(R) = P(R).

Actually, if R does not have an identity then $J(R) \subseteq N(R)$ and any prime ideal is maximal. If P is a prime ideal in R then $N(R) \subseteq P$. So N(R/P) = 0. Then by Theorem 1.4, R/P has an identity and hence is a finite integral domain. But then R/P is a field. By the correspondence theorem we conclude that P is maximal.

Since N(R/N(R)) = 0, R/N(R) has an identity. It might be hoped that if we knew something about rings with identity this would provide information about R. This is indeed the case.

Theorem 1.6. If R is a finite commutative ring with $N(R) = 0$ then R is the direct sum of finite fields.

Proof: Let $M_1, \dots , M_n$ be the maximal ideals in R. Then R/M_i is a finite field. Let $\pi_i: R \longrightarrow R/M_i$ be the natural projection. Then $(\pi_1, \dots , \pi_n)(r) = (\pi_1(r), \dots , \pi_n(r))$ is an epimorphism of R onto the direct sum $\sum \oplus R/M_i$ with kernel $\bigcap M_i = J(R)$. By Theorem 1.4, R has an identity. So $J(R) = N(R) = 0$. Thus $R \simeq \sum \oplus R/M_i$.

Corollary. The ring $R/N(R)$ is isomorphic to the direct sum of finite fields.

Since $R/N(R)$ has idempotents we would like to pull them back to idempotents in R.

Lemma. If z is in $N(R)$ then there exists z_1 in $N(R)$ such that $z_1{}^2 - z_1 = z$.

Proof: Let $z_1 = \sum_{n=1}^{\infty}(1/2n - 1)\binom{2n - 1}{n}(-z)^n$. Since z is nilpotent this is a finite sum and z_1 is in $N(R)$. One checks that z_1 is the desired element.

Theorem 1.7. Let $\pi: R \longrightarrow R/N(R)$ be the natural projection and u an idempotent in $R/N(R)$. Then there exists an idempotent e in R such that $\pi(e) = u$.

Proof: Let x be in R such that $\pi(x) = u$. Then $x^2 - x = z$ is in $N(R)$. Consider $\sum_{n=1}^{\infty} 4^{n-1}(-z)^n$. Since z is nilpotent this is a finite sum and is an element of $N(R)$. By the lemma there exists z in $N(R)$ such that $z_1{}^2 - z_1 = \sum_{n=1}^{\infty} 4^{n-1}(-z)^n$. Let $e = x - 2xz_1 + z_1$. Then $\pi(e) = \pi(x) = u$. It is a routine computation to show e is an idempotent.

Theorem 1.8. If $\{u_i\}_{i=1}^{n}$ is a finite set of mutually orthogonal idempotents in $R/N(R)$ then there exists a set $\{e_i\}_{i=1}^{n}$ of mutually orthogonal idempotents in R such that $\pi(e_i) = u_i$ for $i = 1, \ldots , n$.

Proof: It is true for $n = 1$ by Theorem 1.7. Assume true for m and let $\{u_i\}_{i=1}^{m+1}$ be a set of mutually orthogonal idempotents in $R/N(R)$. Let $e_1, \ldots , e_m$ be a set of mutually orthogonal idempotents with $\pi(e_i) = u_i$. Let $e = \sum e_i$. By Theorem 1.7 choose an idempotent e' in R such that $\pi(e') = u_{m+1}$. Let $e_{m+1} = e' - ee'$. Then $\{e_i\}_{i=1}^{m+1}$ is the desired set of idempotents of R.

The first of the two decomposition theorems we will prove is:

Theorem 1.9. If R is a finite commutative ring then R is the direct sum of a nilpotent ring and a ring with identity.

Proof: By the corollary to Theorem 1.6, $R/N(R) = \sum \oplus F_i$ where F_i is a finite field. Let u_i be the identity of F_i. Then by Theorem 1.8 there exists mutually orthogonal idempotents e_i in R such that $\pi(e_i) = u_i$. Let $e = \sum e_i$. Then $\pi(e) = 1$ in $R/N(R)$. If r is in R then $r = er + r - er$. If $(1 - e)R = \{r - er: r \text{ in } R\}$ then $R = (1 - e)R \oplus eR$. Let r be in R then $\pi(r - er) = \pi(r) - \pi(e)\pi(r) = \pi(r) - \pi(r) = 0$. Hence $(1 - e)R \subseteq N(R)$ and thus is nilpotent. Since the e_i are mutually orthogonal idempotents, e is an idempotent. It is clear that e is the identity of eR.

The study of finite commutative rings then breaks up into the study of nilpotent commutative rings and finite commutative rings with identity. This paper will only be concerned with the latter.

Definition 1.7. A commutative ring R with identity is said to be local if R has a unique maximal ideal.

The last decomposition theorem in this section will further reduce the part with identity. Henceforth R will denote a finite commutative ring with identity.

Lemma. Let $\{M_1, \ldots, M_n\}$ be the set of maximal ideals in R. If $I = M_1 \ldots M_n$ then I is nilpotent.

Proof: Note $I \subseteq \bigcap M_i = J(R) = N(R)$. So each element of I is nilpotent. There are only finitely many elements in I so I must be nilpotent.

Definition 1.8. Proper ideals I and J of R are comaximal if $I + J = R$.

Lemma. Let $M_1, \ldots, M_m$ be the maximal ideals in R. Then if n is a positive integer we have M_i^n and M_j^n are comaximal when $i \neq j$.

Proof: If $M_i^n + M_j^n \neq R$ then $M_i^n + M_j^n \subseteq M_k$ for some maximal ideal M_k. So $M_i^n \subseteq M_k$ and $M_j^n \subseteq M_k$. Hence $M_i \subseteq M_k$ and $M_j \subseteq M_k$. So $i = k = j$ since the M_i are maximal.

Theorem 1.10. Let R be a finite commutative ring with 1. Then R is the direct sum of finite local rings.

Proof: Let $I = M_1 \ldots M_n$ where the M_i are all the maximal ideals in R. Then I is nilpotent. Hence there exists a positive integer m such that $I^m = 0$. So $M_1^m \ldots M_n^m = 0$. From the above lemma the M_i^m are pairwise comaximal. Hence by the Chinese Remainder Theorem, $R \simeq R/M_1^m \oplus R/M_2^m \oplus \ldots \oplus R/M_n^m$. By the correspondence theorem the ideals of R/M_i^m are in one to one lattice preserving correspondence with the ideals of R containing M_i^m. But there is only one maximal ideal of R containing M_i^m, namely M_i. Hence M_i/M_i^m is the unique maximal ideal of R/M_i^m.

Before leaving this section note that if $S = \sum \oplus S_i$ then $(S)_n$ is the direct sum of $(S_i)_n$ where $(S)_n$ is the ring of n x n matrices over S.

Also $S[x]$ is the direct sum of $S_i[x]$ where $S[x]$ is the ring of polynomials over S. Further $U(S)$ is the direct sum of the $U(S_i)$ where $U(S)$ is the group of units in S. Hence, in most cases, to study S it suffices to study its local components.

Properties of Finite Local Rings

Unless otherwise stated in this section R denotes a finite local ring. Before proceeding to properties of R we give two elementary examples.

Example 1.3. The following are finite local rings:

(i) A finite field (0 is the maximal ideal).

(ii) The integers Z modulo a power of a prime p, i.e. Z/Zp^n (Zp/Zp^n is the maximal ideal).

These examples provide much of the motivation for the work done in this paper.

Theorem 1.11. (Characterization of finite local rings) If R is a finite ring with identity then the following are equivalent:

1. R is a local ring.
2. R has 0 and 1 as its only idempotents.
3. Every subring of R is local.
4. Every element of R is either a unit or a nilpotent element.
5. If $R = I \oplus J$ then $R = I$ or $R = J$.

Proof: (1.) implies (2.). Suppose e is an idempotent in R. Then $e(1 - e) = 0$. Let M be the maximal ideal of R then M is prime. So e is in M or $1 - e$ is in M. If e is in M then e is nilpotent and hence $e = 0$. If $1 - e$ is in M then $1 - e = 0$ since it is also an idempotent.

(2.) implies (1.). By Theorem 1.10, $R = \sum \oplus R_i$ where the R_i are finite local rings. But if this decomposition is non-trivial then R has more idempotents than 0 and 1. So R is local.

(1.) implies (3.). Since 1 and 2 are equivalent, just note that any idempotent in a subring of R is an idempotent in R.

(3.) implies (1.). Obvious.

(1.) implies (4.). If M is the maximal ideal of R then $M = J(R) = N(R)$. Hence any element in M is nilpotent. Since M is the unique maximal ideal of R any element of R which is not in M is a unit.

(4.) implies (1.). The set of nilpotent elements of R is an ideal M. Since any element not in M is a unit, it is clear that M is maximal. If N is a proper ideal of R then N contains no units and hence $N \subseteq M$. So R is a local ring.

(2.) is equivalent to (5.). This follows from the relation between idempotents and direct sum decompositions of R.

<u>Corollary</u> 1. If R is a finite local ring then r is a unit in R if and only if $\bar{r} \neq 0$. (Where $\bar{r}$ denotes the image of r under the natural projection π of R onto R/M.)

<u>Proof</u>: The map π is a ring homomorphism so units are carried to units.

Conversely, if r is not a unit then $r^n = 0$ for some n and hence $\bar{r}^{\,n} = 0$. Since R/M is a field $\bar{r} = 0$.

<u>Corollary</u> 2. A finite local ring R is a finite field if and only if $M = 0$.

One of the interesting properties of a finite field F is that F has p^n elements for some positive integer n and prime p. The same is true for finite local rings.

Theorem 1.12. If R is a finite local ring then R has p^n elements for some prime p and positive integer n.

Proof: Suppose false. Then there exist integers m and n such that R has mn elements and (m, n) = 1. Let I be the ideal generated by m1 and J the ideal generated by n1. There exist integers s and t such that ms + tn = 1. So sm1 + tn1 = 1. Let x be in R then x = xsm1 + xtn1. So I + J = R. If x is in I $\cap$ J then x = x_1m1 = x_2n1 for some x_1 and x_2 in R. Note mn1 = 0. Hence 0 = $x_1$tnm1 = xtn1 and 0 = $x_2$snm1 = xsm1. Thus 0 = xtn1 + xsm1 = x. Thus R = I $\oplus$ J. By Theorem 1.11, it follows that R is not local.

Let M be the maximal ideal of R. Then R/M is a field and (R/M)[x] is a unique factorization domain. The following property relates R[x] and (R/M)[x].

Definition 1.9. Let R be a local ring with maximal ideal M. For f(x) in R[x] let $\bar{f}(x)$ be the polynomial obtained from f(x) by reducing the coefficients modulo M. Hensel's Lemma holds for a monic polynomial f(x) in R[x] if whenever $\bar{f}(x) = \bar{g}(x)\ \bar{h}(x)$ where $\bar{g}(x)$ and $\bar{h}(x)$ are monic polynomials in (R/M)[x] which are relatively prime then there exist monic representatives g(x) and h(x) in R[x] of $\bar{g}(x)$ and $\bar{h}(x)$, respectively, such that f(x) = g(x) h(x). We call R a Hensel ring if Hensel's Lemma holds for every monic polynomial in R[x].

We note that the representatives g(x) and h(x) described above are relatively prime. For $1 = \bar{g}(x)\ \bar{s}(x) + \bar{h}(x)\ \bar{t}(x)$ for some $\bar{s}(x)$ and $\bar{t}(x)$ in (R/M)[x]. Hence g(x) s(x) + h(x) t(x) + k = 1 where s(x) and t(x) are representatives of $\bar{s}(x)$ and $\bar{t}(x)$, respectively, and k is a nilpotent element in $R[x]$. It then follows that $g(x)\ s(x) + h(x)\ t(x)$ is a unit and the result is proven.

Theorem 1.13. Every finite local ring R is a Hensel ring.

Before beginning the proof of the theorem we need a fact about polynomials over a field.

Lemma. Suppose $f(x)$ and $g(x)$ are relatively prime monic polynomials in $F[x]$, F a field. If $p(x)$ is in $F[x]$ then there exist $a(x)$ and $b(x)$ in $F[x]$ with $\deg a(x) \leq \deg g(x)$ and either $b(x) = 0$ or $\deg b(x) < \deg f(x)$ such that $p(x) = a(x)\ f(x) + b(x)\ g(x)$.

Proof: A simple modification of a result in Dean [6., page 157] provides the result.

Proof of the theorem: Let M be the maximal ideal of R. Suppose $f(x)$ is a monic polynomial in $R[x]$ and $\deg f(x) = n$. Suppose also that $\bar{f}(x) = \bar{g}(x)\ \bar{h}(x)$ where $\bar{g}(x)$ and $\bar{h}(x)$ are monic relatively prime polynomials in $(R/M)[x]$. We will construct two sequences $\{g_k(x)\}$ and $\{h_k(x)\}$ in $R[x]$ such that:

(i) $f_k(x)$ has degree r and $\deg g_k(x) \leq n - r$,

(ii) $f_{k+1}(x) = f_k(x) \bmod M^{k+1}$,

(iii) $g_{k+1}(x) = g_k(x) \bmod M^{k+1}$,

(iv) $f(x) = g_k(x)\ h_k(x) \bmod M^{k+1}$.

since $M^t = 0$ for some t, we note that $f(x) = g_t(x)\ h_t(x)$. Since $f(x)$ is monic we see that $g_t(x)$ has a unit for its lead coefficient. Hence we can make an adjustment in $g_t(x)$ and $h_t(x)$ so that they satisfy the conditions. Namely, if u is the lead coefficient then take $u^{-1}g_t(x)$ and $uh_t(x)$. We will construct the two sequences inductively. Let $g_o(x)$ and $h_o(x)$ be polynomials in $R[x]$ such that $\bar{g}_o(x) = \bar{g}(x)$ and $\bar{h}_o(x) = \bar{h}(x)$.

Hence we have the conditions satisfied for $n = 0$. Suppose we have constructed $g_0(x), \ldots, g_k(x)$ and $h_0(x), \ldots, h_k(x)$ satisfying (i) - (iv). Since M^{k+1} is finite, $M^{k+1} = Rw_1 + \ldots + Rw_m$ where the w_i are in M^{k+1}. Let $g_{k+1}(x) = g_k(x) + \sum w_i r_i(x)$ and $h_{k+1}(x) = h_k(x) + \sum w_i s_i(x)$ where $r_i(x)$ is a polynomial in $R[x]$ of degree less than r and $s_i(x)$ is a polynomial in $R[x]$ of degree less than or equal to $n - r$. Note that $g_0(x), g_1(x), \ldots, g_{k+1}(x)$ and $h_0(x), h_1(x), \ldots, h_{k+1}(x)$ satisfy (i) - (iii). To complete the proof it suffices to show that $r_i(x)$ and $s_i(x)$ can be chosen in such a manner so that (iv) holds. Suppose $f(x) = g_{k+1}(x)\ h_{k+1}(x) \bmod M^{k+2}$. Then

$$f(x) - g_{k+1}(x)\ h_{k+1}(x) = f(x) - g_k(x)\ h_k(x) - \sum w_i(s_i(x)\ g_k(x)$$
$$+ r_i(x)\ h_k(x)) - \sum_{i,j} w_i w_j r_i(x)\ s_j(x).$$

By induction $f(x) - g_k(x)\ h_k(x) = \sum w_i p_i(x)$ where $p_i(x)$ is a polynomial whose degree is at most n. Hence

$$f(x) - g_{k+1}(x)\ h_{k+1}(x) = \sum w_i(p_i(x) - s_i(x)\ g_k(x) -$$
$$r_i(x)\ h_k(x)) \mod M^{k+2}.$$

We would be done if we could find $r_i(x)$ and $s_i(x)$ in $R[x]$ such that

$$p_i(x) = s_i(x)\ g_k(x) - r_i(x)\ h_k(x) \mod M.$$

Since $g_k(x) = g_0(x) \mod M$ and $h_k(x) = h_0(x) \mod M$, then the above equation reduces to

$$p_i(x) = s_i(x)\ g_0(x) + r_i(x)\ h_0(x) \mod M.$$

Since $\bar{g}_0(x)$ and $\bar{h}_0(x)$ are relatively prime in $(R/M)[x]$, we may apply the lemma to conclude that there exist polynomials $a_i(x)$ and $b_i(x)$ in $(R/M)[x]$ such that

$$\bar{p}_i(x) = a_i(x)\ \bar{g}_0(x) + b_i(x)\ \bar{h}_0(x)$$

with deg $a_i(x) \leq$ deg $\bar{h}_0(x)$ and deg $b_i(x) <$ deg $\bar{g}_0(x)$ (or $b_i(x) = 0$). Let $r_i(x)$ and $s_i(x)$ be chosen in $R[x]$ such that $\bar{r}_i(x) = a_i(x)$ with deg $r_i(x)$ = deg $a_i(x)$ and $\bar{s}_i(x) = b_i(x)$ with deg $s_i(x)$ = deg $b_i(x)$. Then $r_i(x)$ and $s_i(x)$ are the desired polynomials.

Modules Over Finite Local Rings

Unlike a field not every module over a finite local ring R is a free R-module. In fact this occurs if and only if R is a field (Wedderburn-Artin Theorem). However we have:

Theorem 1.14. Let R be a finite local ring with maximal ideal M and let N be a finitely generated, projective R-module. Suppose $n_1 + MN, n_2 + MN, \dots, n_t + MN$ is a free basis for N/MN over R/M. Then $n_1, \dots, n_t$ is a free R-basis for N.

Proof: Note that if N is finitely generated it is finite. Let $\varphi: R^{(t)} \longrightarrow N$ be defined by $\varphi((a_1, \dots, a_t)) = \Sigma a_i n_i$. Since the $n_i + MN$ generate N/MN we have $\Sigma Rn_i + MN = N$. Then by Nakayama's lemma it follows that the n_i generate N. Let $(a_1, \dots, a_t)$ be in $\ker(\varphi)$. Then $\Sigma a_i n_i = 0$, hence $\Sigma a_i n_i + MN = 0$. But the $n_i + MN$ are linearly independent, thus the a_i are in M. So $\ker(\varphi) \subseteq MR^{(t)}$. Since N is projective, the exact sequence

$$0 \longrightarrow \ker(\varphi) \longrightarrow R^{(t)} \longrightarrow N \longrightarrow 0$$

splits. So $R^{(t)} = L \oplus \ker(\varphi)$ for some submodule L. Now $\ker(\varphi) \subseteq MR^{(t)} \cap \ker(\varphi) = (M\ker(\varphi) \oplus ML) \cap \ker(\varphi) = M\ker(\varphi)$. It now follows by Nakayama's lemma that $\ker(\varphi) = 0$.

We note that Kaplansky [11.] has proven the above theorem without any finiteness conditions. But we will not have any use for the strengthened result.

Separability and Ramification

In this section we will give the definition of a separable ring extension as given by Auslander and Buchsbaum [3.] and prove a primitive element theorem.

Definition 1.10. A ring S is an extension of the ring R if R is a subring of S.

Definition 1.11. For a commutative R-algebra A with 1 we call $A \otimes_R A$ the enveloping algebra of A and denote it by A^e.

Note that A can be considered an A^e-module under $(a_1 \otimes a_2)a = a_1a_2a$. Also $\mu : A^e \longrightarrow A$ given by $\mu(a \otimes b) = ab$ is an A^e-epimorphism. If J is the kernel of μ then we have the A^e exact sequence

$$0 \longrightarrow J \longrightarrow A^e \xrightarrow{\mu} A \longrightarrow 0.$$

It is easy to see that J is the ideal of A^e generated by $\{1 \otimes a - a \otimes 1 \colon a \text{ is in } A\}$.

Definition 1.12. A commutative R-algebra A with 1 is called separable if A is a projective A^e-module.

Theorem 1.15. The following conditions for a commutative R-algebra A are equivalent:

(1) A is a separable R-algebra.

(2) $0 \longrightarrow J \longrightarrow A^e \xrightarrow{\mu} A \longrightarrow 0$ is A^e split exact.

(3) There exists e in A^e such that $\mu(e) = 1$ and $Je = 0$.

Proof: (1) and (2) are equivalent from elementary properties of projective modules.

Suppose the sequence splits. Then there exists ψ in $\mathrm{Hom}_{A^e}(A, A^e)$ such that $\mu\psi = 1_A$. Let $e = \psi(1)$. One checks that e is the desired element.

Conversely, if there exists e in A^e such that Je = 0 and $\mu(e) = 1$ then define $\psi: A \longrightarrow A^e$ by $\psi(a) = (a \otimes 1)e$. One checks that ψ is the desired A^e-homomorphism.

Let e be an element of A^e satisfying (3) above. Then $\mu(e - (1 \otimes 1))$ is zero. So $e^2 - e = (e - (1 \otimes 1))e$ is in Je = 0. Hence e is an idempotent and is called a separability idempotent for A.

We recall the following fact from homological algebra. See, for example, Ingraham and DeMeyer [8.].

Theorem 1.16. Let A be a commutative R-algebra with identity 1. Then A is a separable R-algebra if and only if $\mathrm{Hom}_{A^e}(A, -)$ is right exact.

Theorem 1.17. Let A be a separable commutative R-algebra with identity 1 and I an ideal in A. Then A/I is a separable R-algebra.

Proof: We will show that $\mathrm{Hom}_{(A/I)^e}(A/I, -)$ is right exact. Let N be an $(A/I)^e$-module. We can make N into an A^e-module under $(a_1 \otimes a_2)n = ((a_1 + I) \otimes (a_2 + I))n$. The proof will be complete if we show that $\mathrm{Hom}_{(A/I)^e}(A/I, N) \simeq \mathrm{Hom}_{A^e}(A, N)$ as groups. Let f be in $\mathrm{Hom}_{A^e}(A, N)$. Then f(1) is in N. Define $\psi: \mathrm{Hom}_{A^e} A, N) \longrightarrow \mathrm{Hom}_{(A/I)^e}(A/I, N)$ by $\psi(f)(a + I) = ((a + I) \otimes (1 + I))\, f(1)$. One checks that if f is in $\mathrm{Hom}_{A^e}(A, N)$ then $\psi(f)$ is in $\mathrm{Hom}_{(A/I)^e}(A/I, N)$. If g is an $(A/I)^e$-homomorphism of $(A/I)^e$ into N then define $\varphi(g)(a) = g(a + I)$. It is easy to check that $\varphi(g)$ is in $\mathrm{Hom}_{A^e}(A, N)$. Then $\varphi\psi(f) = f$ and $\psi\varphi(g) = g$. And the result is proven.

Let A be a commutative R-algebra with identity and K an ideal in R such that $K \subseteq \mathrm{Ann}_R A$ then A is an R/K- algebra. Also note that in this case A^e is an R/K-module and $A \otimes_{R/K} A$ is an A-module. Also we see that $\otimes_R$: $A \times A \longrightarrow A^e$ is R/K-linear and $\otimes_{R/K}$: $A \times A \longrightarrow A \otimes_{R/K} A$ is R-linear. From these remarks it follows that $A^e \simeq A \otimes_{R/K} A$ and A is R-separable if and only if A is R/K-separable. Hence from the above and Theorem 1.17 we have:

Theorem 1.18. If S is a finite local separable extension of R and M is the maximal ideal of R then S/SM is a separable extension of R/M.

Theorem 1.19. Let S be a finite local separable extension of R. If N is a S-module which is R-free then N is S-free.

Proof: Since free and projective are equivalent over finite local rings, we suppose N is projective over R and show it is projective over S. Let $0 \longrightarrow L \longrightarrow P \xrightarrow{\eta} N \longrightarrow 0$ be an exact sequence of S-modules. The sequence then R-splits. Let ψ be in Hom_R (N, P) such that $\eta\psi = 1_N$. Let $e = \sum x_i \otimes y_i$ be a separability idempotent for S. Define ψ': $N \longrightarrow P$ by $\psi'(n) = \sum x_i \psi(y_i n)$, for n in N. One checks that ψ' is a S-splitting homomorphism for the above sequence.

We are now in a position to show that this definition of separability is a generalization of that for fields.

Theorem 1.20. If S is a finite local separable extension of a finite field R then S is a finite field.

Proof: Let N be an S-module. Note N is also an R-module. Since R is a field, N is a free R-module. Thus by Theorem 1.19, N is S-free. By the Wedderburn-Artin Theorem (see Jans [9.] for statement and proof) S is semi-simple with minimum condition. Hence S has zero radical. It follows from Corollary 2 to Theorem 1.11 that S is a field.

Definition 1.13. Let S be a finite local extension of R. We say S is unramified over R if whenever M and m are the maximal ideals of S and R respectively then M = mS.

We are now in a position to prove a result due to Auslander and Buchsbaum [3.].

Theorem 1.21. Let S be a finite local separable extension of R then S is unramified over R.

Proof: Since S is separable over R, S/mS is a separable extension of R/m. But R/m is a field. Hence from Theorem 1.20 S/mS is a field. Thus mS is a maximal ideal and hence is M. Thus S is unramified.

Although we will not need it here Auslander and Buchsbaum [3.] have also shown the converse of the above theorem is true for Noetherian rings.

One of the essential properties of local separable extensions is the following:

Theorem 1.22. (Primitive Element Theorem) Let S and R be finite local rings. If S is a separable extension of R then S has a primitive element.

Proof: Let m and M be the maximal ideals of R and S respectively. Then by Theorem 1.21, M = mS. So S/mS is a finite field. Hence S/mS has a cyclic group of units. Let u be in S such that $\bar{u}$ is a generator of the group of units of S/mS. Then S/mS = (R/m)[$\bar{u}$]. Hence S = R[u] + mS. Then by Nakayama's Lemma S = R[u]. Hence S has a primitive element.

Although every finite local separable extension of a finite ring is a simple extension, the converse is false.

Example 1.4. Let $R = Z/(2)$ and consider $S = R[x]/(x^2)$. Then $S = \{0, 1, \bar{x} + 1, x\}$. We notice that S is not a field and hence can not be a separable extension of R.

We now turn our attention to the R-automorphisms of S where S is an extension of R.

Definition 1.14. Let S be an extension of R and H a group of R-ring automorphisms of S then $S^H = \{x \in S\colon \sigma(x) = x \text{ for all } \sigma \in H\}$. The set S^H is called the fixed ring of H in S.

Definition 1.15. If S is an extension of R and G is the group of all R-ring automorphisms of S then S is a normal extension of R if $S^G = R$.

Definition 1.16. If S is an extension of R then S is said to be Galois over R if S is a normal separable extension of R. The group of R-automorphisms of S is then called the Galois group of S over R and denoted by G(S, R).

To see that the local case provides us with information about the Galois group of any finite ring consider the following: Let S be a finite ring with identity then $S = \sum \oplus S_i$ where each S_i is a finite local ring with identity e_i. Then if R_i is a subring of S_i then S_i is a local extension of the local ring R_i. Let $R = \sum \oplus R_i$ and $a^{(i)}$ be the element of S which has a as its i^{th} component and zeroes otherwise. Let σ be an R-isomorphism of S then $\sigma(a^{(i)}) = \sigma(e_i^{(i)}a^{(i)})$. But $e_i^{(i)}$ is in R, hence $\sigma(a^{(i)}) = e_i^{(i)}\sigma(a^{(i)}) \subseteq S_i$. Since σ is an isomorphism $\sigma(S_i) = S_i$. Now let $\sigma_i = \pi_i \sigma$ where π_i is the i^{th} projection of S onto S_i. Clearly σ_i is an R_i-isomorphism of S_i and $\sigma = (\sigma_1, \ldots, \sigma_n)$ where $(\sigma_1, \ldots, \sigma_n)(a_1, \ldots, a_n) =$

$(\sigma_1(a_1), \ldots, \sigma_n(a_n))$. Further S is separable over R if and only if S_i is separable over R_i, for every i (see Ingraham and DeMeyer [8.]). A similar remark holds for normality. Hence $G(S, R) \simeq \sum \oplus G(S_i, R_i)$.

CHAPTER II

THE POLYNOMIAL RING OF A FINITE LOCAL RING

If F and G are fields and F is a finite extension of G then for each a in F there exists a monic polynomial $g(x)$ in $G[x]$ such that $g(a) = 0$. For rings we have:

Definition 2.1. An extension S of R is said to be integral over R if whenever a is in S there exists a monic polynomial $f(x)$ in $R[x]$ such that $f(a) = 0$.

Theorem 2.1. Let R and S be finite rings with S an extension of R then S is integral over R.

Proof: Let u be in S and consider $\{\Sigma r_n u^n : r_n \text{ is in } R\} = A$. Since S is finite so is A. For each distinct element in A choose a representative with least degree as a polynomial in u. Let B be the set of these representatives. Let m be the greatest degree of any polynomial in B. Now u^{m+1} is in A. Hence $u^{m+1} = p(u)$ where $p(u)$ is in B. So u satisfies the monic polynomial $x^{m+1} - p(x)$. Hence S is integral over R.

However unlike the field case an element may not satisfy any monic irreducible polynomial.

Example 2.1. Let R be a field. Consider the ring extension $R[b] \simeq R[x]/(x^2)$. Then b satisfies the monic polynomial x^2 but does not satisfy any monic irreducible polynomial over R.

Unless otherwise stated R denotes a finite local ring with maximal ideal M. We first examine the unit, prime and irreducible elements of R[x].

Theorem 2.2. A polynomial f(x) is a unit in R[x] if and only if $\bar{f}(x)$ is a unit in R/M.

Proof: If f(x) is a unit in R[x] then $\bar{f}(x)$ is a unit in (R/M)[x]. But R/M is a field. Hence $\bar{f}(x)$ is a unit in R/M.

Conversely, suppose f(x) is a unit in R/M then $f(x) = \sum a_i x^i$. Applying the projection map and equating coefficients we conclude that a_i is in M for $i \neq 0$ and a_o is a unit. Hence for $i \neq 0$, a_i is nilpotent. Thus f(x) is a unit.

Definition 2.2. An element b of a ring is prime if the principal ideal (b) is prime.

Before we can make any statement concerning primes in R[x], we need to consider what happens to irreducibles in R[x] under the natural map from R[x] onto (R/M)[x]. We see that the image of a monic irreducible polynomial in R[x] need not be irreducible in (R/M)[x].

Example 2.2. Let $f(x) = x^2 + 2x + 2$ be in (Z/4Z)[x]. It is easy to check that f(x) is irreducible in (Z/4Z)[x]. However $\bar{f}(x) = x^2$ is not irreducible in (Z/2Z)[x].

We are led to the following set of polynomials in R[x].

Definition 2.3. Let J denote the set of all polynomials f(x) in R[x] such that $\bar{f}(x)$ has distinct roots in the algebraic closure of R/M.

Lemma. Let f(x) be in J. Then there exists a sequence $\{f_j(x)\}$ of monic polynomials in J with

$$\deg f_j(x) = \deg \bar{f}(x)$$

$$f_j(x) \equiv f_{j+1}(x) \mod M^j$$

and for some $g_j(x)$ in $M[x]$ and unit b_j in R

$$b_j f(x) \equiv f_j(x) + g_j(x) f_j(x) \mod M^j.$$

Proof: Let $f(x) = \sum_{i=1}^{n} b_i x^i$ where $b_n \neq 0$ and $\deg \bar{f}(x) = t \leq n$. Choose $g_1(x) = 0$ and $f_1(x) = b_t^{-1}(\sum_{i=1}^{n} b_i x^i)$. By induction assume $\{f_i(x)\}_{i=1}^{j}$ have been selected to satisfy the lemma. Then $b_j f(x) = f_j(x) + g_j(x) f_j(x) + h(x)$ where $h(x)$ is in $M^j[x]$. Since $f_j(x)$ is monic we may select $q(x)$ and $r(x)$ in $R[x]$ with $h(x) = q(x) f_j(x) + r(x)$ where $\deg r(x) < \deg f_j(x) = \deg \bar{f}(x)$ or $r(x) = 0$. Set $f_{j+1}(x) = f_j(x) + r(x)$ and $g_{j+1}(x) = g_j(x) + q(x)$. We claim that $g_{j+1}(x)$ is in $M[x]$ and $r(x)$ is in $M^j[x]$. If $r(x) = 0$ this statement is trivial. Otherwise suppose $f_j(x) = a_0 + a_1 x + \dots + a_{t-1} x^{t-1} + x^t$ and $q(x) = c_0 + c_1 x + \dots + c_m x^m$. In the product $f_j(x)q(x)$ the coefficient of x^{t+m} is c_m, of x^{t+m-1} is $c_m a_{t-1} + c_{m-1}$, etc. Since $h(x) \equiv 0 \mod M^j$ and $\deg r(x) < \deg f_j(x) = t$, it is easy to see that c_m, then c_{m-1}, then c_{m-2}, etc. are in M^j and consequently $q(x)$ is in $M^j[x]$. Then $r(x) = h(x) - q(x) f_j(x)$ is in $M^j[x]$. Then

$$\begin{aligned} b_j f(x) &= f_j(x) + g_j(x) f_j(x) + h(x) \\ &= (f_j(x) + r(x)) + (g_j(x) + q(x))(f_j(x) + r(x)) \\ &\qquad - r(x) g_j(x) - r(x) q(x) \\ &= f_{j+1}(x) + g_{j+1}(x) f_{j+1}(x) - r(x)(g_j(x) + q(x)) \\ &\equiv f_{j+1}(x) + g_{j+1}(x) f_{j+1}(x) \mod M^{j+1}. \end{aligned}$$

Corollary. Let f be in J. Then there exists a monic polynomial $f^*(x)$ in J with $\bar{f}(x) = \bar{f}^*(x)$ and, for an element a in R, $f(a) = 0$ if and only if $f^*(a) = 0$.

Proof: Let t be the degree of nilpotency of R. Then by the lemma $b_t f(x) = f_t(x) + g_t(x)f_t(x) = (1 + g_t(x))f_t(x)$ where $f_t(x)$ is monic, b_t and $1 + g_t(x)$ (since $g_t(x)$ is in $M[x]$) are units, and $\bar{f}(x) = \bar{f}_t(x)$. Thus let $f^*(x) = f_t(x)$.

Theorem 2.3. Let f(x) be a monic polynomial in R[x].

(a.) If $\bar{f}(x)$ is irreducible in $(R/M)[x]$ then f(x) is irreducible.

(b.) If f(x) is irreducible then $\bar{f}(x) = (g(x))^n$ where n is a positive integer and g(x) is irreducible in $(R/M)[x]$.

(c.) If f(x) is in J then f(x) is irreducible if and only if $\bar{f}(x)$ is irreducible in $(R/M)[x]$.

Proof: To prove (b.) suppose $\bar{f}(x)$ is not the power of an irreducible. Then $\bar{f}(x) = \bar{g}(x)\ \bar{h}(x)$ where $\bar{g}(x)$ and $\bar{h}(x)$ are relatively prime. By Hensel's Lemma there exist monic relatively prime polynomials g(x) and h(x) in R[x] such that $f(x) = g(x)\ h(x)$. Thus f(x) is not irreducible.

For (a.) suppose $\bar{f}(x)$ is irreducible over R/M and $f(x) = g(x)\ h(x)$. Then $\bar{f}(x) = \bar{g}(x)\ \bar{h}(x)$. But $\bar{f}(x)$ is irreducible over a field hence either $\bar{g}(x)$ or $\bar{h}(x)$ is a unit in R/M. Suppose $\bar{h}(x)$ is a unit. Then by Theorem 2.2, h(x) is a unit in R[x]. So f(x) is irreducible. Similarly if $\bar{g}(x)$ is a unit.

The final statement follows from (a.) and (b.) and the definition of J.

Corollary. There exist monic irreducible polynomials in J of degree n for any natural number n. Hence there are infinitely many monic irreducible polynomials in R[x].

We are now in a position to prove a theorem on primes in R[x].

Theorem 2.4. If $f(x)$ is a monic prime polynomial in $R[x]$ then $f(x)$ is irreducible and in J.

Proof: If $f(x)$ is prime then $(f(x))$ is a prime ideal. So $R[x]/(f(x))$ is a finite integral domain. But finite integral domains are fields. Thus $(f(x))$ is a maximal ideal. Consider the natural map of $R[x]$ onto $(R/M)[x]$. Since this is an epimorphism and $(\bar{f}(x))$ is the image of $(f(x))$ under this map, $(\bar{f}(x))$ is maximal. So $\bar{f}(x)$ is irreducible. Hence $f(x)$ is irreducible and in J.

Note that many of the properties of polynomials in $F[x]$, F a field fail to carry over to polynomials over finite local rings. For example we have the following characterization of maximal ideals in $R[x]$.

Theorem 2.5. If M is the maximal ideal of R then an ideal I in $R[x]$ is maximal if and only if $I = (M, f(x))$ where $f(x)$ is a monic irreducible polynomial in J.

Proof: First observe that $I \cap R$ is prime, hence maximal. Since R is local $I \cap R = M$. Further $(R/M)[x] \simeq R[x]/MR[x]$ where $MR[x]$ is the smallest extension of M in $R[x]$. Hence I contains the kernel of the natural surjection of $R[x]$ onto $(R/M)[x]$. Let I' be the homomorphic image of I in $(R/M)[x]$. Then I' is maximal. Since R/M is a field, $I' = (\bar{f}(x))$ where $\bar{f}(x)$ is a monic irreducible polynomial in $(R/M)[x]$. Let $f(x)$ be a monic preimage of $\bar{f}(x)$ in $R[x]$. Then $f(x)$ is also in J. By Theorem 2.3, $f(x)$ is irreducible in $R[x]$. Since I' is the homomorphic image of $(M, f(x))$, we conclude by the Correspondence Theorem that $(M, f(x)) = I$.

Example 2.3. Irreducible polynomials need not be prime even if they are in J. If $f(x)$ is irreducible, prime and in J then $R[x]/(f(x))$ is a finite integral domain, hence a field. Thus $f(x)$ generates a maximal ideal. From Theorem 2.5 we see this is not the case if R is not a field.

Example 2.4. Irreducible polynomials need not be relatively prime. Consider the polynomials $x^2 + x + 1$ and $x^2 + 3x + 1$ where the coefficients are from $Z/4Z$. However we do have:

Theorem 2.6. Let $f(x)$ and $g(x)$ be monic irreducible polynomials in J. If $\bar{f}(x) \neq \bar{g}(x)$ in $(R/M)[x]$ then $f(x)$ and $g(x)$ are relatively prime and conversely.

Proof: By Theorem 2.3 $\bar{f}(x)$ and $\bar{g}(x)$ are irreducible in $(R/M)[x]$. Since R/M is a field and $\bar{f}(x)$ and $\bar{g}(x)$ are distinct, they are relatively prime in $(R/M)[x]$. Hence there exist polynomials $\bar{f}_1(x)$ and $\bar{g}_1(x)$ in $(R/M)[x]$ such that $\bar{f}_1(x)\ \bar{f}(x) + \bar{g}_1(x)\ \bar{g}(x) = 1$. Let $f_1(x)$ and $g_1(x)$ be preimages in $R[x]$ of the polynomials $\bar{f}_1(x)$ and $\bar{g}_1(x)$, respectively. Now $f_1(x)\ f(x) + g_1(x)\ g(x)$ is a unit by Theorem 2.2. Hence $f(x)$ and $g(x)$ are relatively prime.

Conversely, suppose that $f(x)$ and $g(x)$ are relatively prime. Then there exist polynomials $f_1(x)$ and $g_1(x)$ in $R[x]$ such that $f_1(x)\ f(x) + g_1(x)\ g(x) = 1$. Hence $\bar{f}(x)$ and $\bar{g}(x)$ are relatively prime. Thus since $\bar{f}(x)$ and $\bar{g}(x)$ are not units, $\bar{f}(x) \neq \bar{g}(x)$.

The following lemma can be found in [4.] and is due to Nakayama. It will be needed to characterize a certain class of polynomials.

Lemma. Let $f(x)$ be a monic polynomial in $R[x]$. If $R[x]/(f(x)) = I \oplus J$ where I and J are ideals in $R[x]/(f(x))$ then there exist relatively prime, monic polynomials $g(x)$ and $h(x)$ in $R[x]$ such that

$g(x)\ h(x) = f(x)$ and $I = (g(x))/(f(x))$ and $J = (h(x))/(f(x))$.

If F is a field and $f(x)$ is an irreducible polynomial in $F[x]$ we obtain a field extension of F by considering $F[x]/(f(x))$. In the case of finite local rings it will be important to find a way of generating local extensions of R. Hence we are led to the following:

Definition 2.4. A monic polynomial $f(x)$ in $R[x]$ is said to be local if $R[x]/(f(x))$ is a local ring.

Theorem 2.7. (Characterization of local polynomials) A monic polynomial $f(x)$ in $R[x]$ is local if and only if $\bar{f}(x)$ is the power of an irreducible polynomial in $(R/M)[x]$.

Proof: If $\bar{f}(x)$ is not the power of an irreducible polynomial in $(R/M)[x]$ then $\bar{f}(x) = \bar{g}(x)\ \bar{h}(x)$ where $\bar{g}(x)$ and $\bar{h}(x)$ are monic relatively prime polynomials in $(R/M)[x]$. Then by Hensel's Lemma there exist monic relatively prime polynomials $g(x)$ and $h(x)$ in $R[x]$ such that $f(x) = g(x)\ h(x)$. By the Chinese Remainder Theorem $R[x]/(f(x)) \cong R[x]/(h(x)) \oplus R[x]/(g(x))$. Thus $R[x]/(f(x))$ is not local. Hence $f(x)$ is not a local polynomial.

Conversely, if $f(x)$ is not local then $R[x]/(f(x)) = I_1 \oplus I_2$ for some ideals I_1 and I_2 of $R[x]/(f(x))$. But by the above Lemma, $I_1 = (g(x))/(f(x))$ and $I_2 = (h(x))/(f(x))$ for some $g(x)$ and $h(x)$ in $R[x]$ where the $g(x)$ and $h(x)$ are relatively prime and $g(x)\ h(x) = f(x)$. Since $g(x)$ and $h(x)$ are relatively prime, there exist $g_1(x)$ and $h_1(x)$ in $R[x]$ such that $g_1(x)\ g(x) + h_1(x)\ h(x) = 1$. But under the canonical map we see that this implies that $\bar{g}(x)$ and $\bar{h}(x)$ are relatively prime. Since $g(x)$ and $h(x)$ are monic neither $\bar{g}(x)$ nor $\bar{h}(x)$ are units. Hence $g(x)\ h(x) = f(x)$ is not the power of an irreducible in $(R/M)[x]$.

<u>Corollary</u>. If $f(x)$ is a monic irreducible polynomial in $R[x]$ then $R[x]/(f^n(x))$ is local for any n.

<u>Proof</u>: Since R is a Hensel ring, $\bar{f}(x) = g^n(x)$ where $g(x)$ is an irreducible polynomial in $(R/M)[x]$. Hence $f(x)$ is local by the theorem.

We conclude this chapter with some remarks about factorization in $R[x]$.

<u>Remark</u>. Let
$$\begin{aligned} f(x) &= f_1(x)^{k_1} \dots f_r(x)^{k_r} \\ &= g_1(x)^{t_1} \dots g_s(x)^{t_s} \end{aligned}$$
where $f_i(x)$ and $g_j(x)$ are monic irreducible polynomials in J. Then for every i there exists a j such that deg $f_i(x)$ = deg $g_j(x)$ and $\bar{f}_i(x) = \bar{g}_j(x)$. A corresponding statement holds with $f_i(x)$ and $g_j(x)$ interchanged.

<u>Proof</u>: Let π: $R[x] \longrightarrow (R/M)[x]$ be the map which reduces the coefficients of $f(x)$ in $R[x]$ modulo the maximal ideal M. Since R is a Hensel ring, π preserves monic irreducible polynomials in J. If $\bar{f}(x)$ denotes the image of $f(x)$ under π then
$$\begin{aligned} \bar{f}(x) &= \bar{f}_1(x)^{k_1} \dots \bar{f}_r(x)^{k_r} \\ &= \bar{g}_1(x)^{t_1} \dots \bar{g}_s(x)^{t_s}. \end{aligned}$$
Since $(R/M)[x]$ is a unique factorization domain, $\bar{f}_i(x) = \bar{g}_j(x)$ for some j and the result follows.

<u>Lemma</u> A. Let R be a finite local ring, $f(x)$ a monic polynomial in $R[x]$. Suppose $f(x) = f_1(x) \dots f_r(x)$ where $f_i(x)$ is a monic irreducible polynomial in J. If the $f_i(x)$ are pairwise relatively prime and $f(x) = g_1(x)^{k_1} \dots g_s(x)^{k_s}$ where $g_i(x)$ is a monic irreducible polynomial then $k_i = 1$ for $i = 1, \dots , s$, $s = r$, the $g_i(x)$ can be ordered

so that $\bar{f}_i(x) = \bar{g}_i(x)$ and $g_i(x)$ is in J.

Proof: Recall that R is a Hensel ring and that (R/M)[x] is a unique factorization domain. Since $f_i(x)$ is in J, $\bar{f}_i(x)$ is irreducible. Hence $\bar{f}_1(x) \ldots \bar{f}_r(x)$ is the unique factorization of f(x) into primes. Since the $f_i(x)$ are pairwise relatively prime, $\bar{f}_i(x) \neq \bar{f}_j(x)$ for $i \neq j$. So $\bar{f}(x)$ is square-free. Let $q_i(x)^{n_i} = \bar{g}_i(x)$ where $q_i(x)$ is a monic irreducible polynomial in (R/M)[x]. So $\bar{f}(x) = q_1(x)^{n_1} \ldots q_s(x)^{n_s}$ is a factorization of $\bar{f}(x)$ into primes. Comparing the two factorizations of $\bar{f}(x)$, we conclude that $n_i = 1$ for $i = 1, \ldots, s$. Hence $s = r$, $q_i(x) = \bar{g}_i(x)$ and there exists an ordering so that $\bar{g}_i(x) = \bar{f}_i(x)$. Since $q_i(x) = \bar{g}_i(x)$ is irreducible, we conclude that $g_i(x)$ is in J.

Lemma B. Let R be a finite local ring and f(x), $f_1(x)$ and $f_2(x)$ be polynomials in R[x] with f(x) and $f_1(x)$ monic irreducible polynomials in J. If $\bar{f}(x) \neq \bar{f}_1(x)$ and f(x) divides $f_1(x)\ f_2(x)$ then f(x) divides $f_2(x)$.

Proof: Since $\bar{f}(x) \neq \bar{f}_1(x)$ and f(x) and $f_1(x)$ are monic irreducible polynomials in J, f(x) and $f_1(x)$ are relatively prime. Hence there exist g(x) and $g_1(x)$ in R[x] such that $f(x)\ g(x) + f_1(x)\ g_1(x) = 1$. So $f(x)\ g(x)\ f_2(x) + f_1(x)\ f_2(x)\ g_1(x) = f_2(x)$. Thus f(x) divides $f_2(x)$.

Lemma C. Let R be a finite local ring. If $f(x) = f_1(x)\ f_2(x)$ where $f_i(x)$ is a monic irreducible polynomial in J and $\bar{f}_1(x) \neq \bar{f}_2(x)$ then f(x) factors uniquely into monic irreducible polynomials.

Proof: Suppose $f(x) = g_1(x)^{k_1} \ldots g_r(x)^{k_r}$ is a factorization of f(x) into monic irreducible polynomials. By Lemma A, $k_i = 1$ and r = 2 and $g_i(x)$ is in J. Without loss of generality we may suppose that $\bar{f}_1(x) = \bar{g}_1(x)$ and $\bar{f}_2(x) = \bar{g}_2(x)$. Hence $f_1(x)$ divides $g_1(x)\ g_2(x)$. But $\bar{f}_1(x) \neq \bar{g}_2(x)$. Thus by Lemma B, $f_1(x)$ divides $g_1(x)$. Since they are monic irreducible polynomials of the same degree we may conclude that $f_1(x) = g_1(x)$. A similar argument shows that $f_2(x) = g_2(x)$.

Corollary. Let R be a finite local ring. If $f(x) = f_1(x) \dots f_r(x)$ where the $f_i(x)$ are monic irreducible polynomials in J with $\bar{f}_i(x) \neq \bar{f}_j(x)$ for $i \neq j$, then f(x) factors uniquely into monic irreducible polynomials.

Proof: Similar argument to that of the proof of Lemma C and induction on r.

In general the above does not characterize all monic polynomials which factor uniquely into monic irreducible polynomials in J. For example, if R is a finite field then all monic polynomials factor uniquely into monic irreducible polynomials in J. However we see below that in some cases there are only those described above.

Theorem 2.8. Let R be a finite local ring with principal maximal ideal M. Let p be a generator for M. Suppose n is the degree of nilpotency of M. Suppose R is not a field. If $f_1(x)$ and $f_2(x)$ are monic irreducible polynomials in J such that $\bar{f}_1(x) = \bar{f}_2(x)$ then $f_1(x)\ f_2(x)$ is not uniquely factorable into monic irreducible polynomials in J if any one of the following holds:

(i) deg $f_1(x)$ is greater than 1.

(ii) deg $f_1(x) = 1$ and $f_1(x) - f_2(x) \neq p^{n-1}$.

(iii) deg $f_1(x) = 1$, $f_1(x) - f_2(x) = p^{n-1}$ and $2p^{n-1} \neq 0$.

Proof: Suppose (i) holds. Note that deg $f_1(x) =$ deg $f_2(x) = s$. Then $f_1(x) - f_2(x) = \sum_{i=1}^{s-1} m_i x^i$ where m_i is in M and hence divisible by p.

So $f_1(x) - f_2(x) = p\sum_{i=1}^{s-1} m_i' x^i$ for some m_i' in R. Consider $h(x) = f_1(x) + p^{n-1}(p - 1)$ and $q(x) = f_2(x) + p^{n-1}$. Then h(x) and q(x) are monic irreducible polynomials in J since $\overline{h}(x)$ and $\overline{q}(x)$ are irreducible polynomials in (R/M)[x]. But

$$\begin{aligned} h(x)\ q(x) &= f_1(x)\ f_2(x) + p^{n-1}(p - 1)\ f_2(x) + f_1(x)\ p^{n-1} \\ &\qquad + p^{n-1}(p - 1)p^{n-1} \\ &= f_1(x)\ f_2(x) + p^{n-1}(p - 1)\ f_2(x) + p^{n-1}(f_2(x) \\ &\qquad + \sum m_i x^i) + p^{2n-2}\ t \\ &= f_1(x)\ f_2(x) + (p^{n-1}(p - 1) + p^{n-1})\ f_2(x) \\ &\qquad + \sum p^{n-1} m_i x^i \\ &= f_1(x)\ f_2(x) + \sum p^{n-1} m_i x^i \\ &= f_1(x)\ f_2(x). \end{aligned}$$

Where t above is some element in R[x]. To complete the proof we need only show that $h(x) \neq f_1(x)$ and $h(x) \neq f_2(x)$. Suppose $h(x) = f_1(x)$. Then $p^{n-1}(p - 1) = 0$. This is impossible. If $h(x) = f_2(x)$ then $f_1(x) - f_2(x) = p^{n-1}$. This is possible. If this is the case let $h_1(x) = f_1(x) + p^{n-1}(p - 1)\ x$. One then checks that $h_1(x)\ q(x)$ gives another factorization of $f_1(x)\ f_2(x)$. We note that the above proof fails if the degree of $f_1(x)$ is one. Suppose (ii) holds. Then the above proof also suffices. Suppose (iii) holds. Then $f_1(x) = x + a$ for some a in R and $f_2(x) = x + a - p^{n-1}$. In this case let $h(x) = x + a + p^{n-1}$ and $q(x) = x + a - 2p^{n-1}$. Again one checks that h(x) q(x) equals $f_1(x)\ f_2(x)$.

The following example shows that Theorem 2.8 can not be improved.

Example 2.5. Let R be the integers modulo 4. The maximal ideal of R generated by 2. Let $f_1(x) = x + 1$ and $f_2(x) = x + 3$. These polynomials do not satisfy any of the conditions of Theorem 2.8. Note that $(x + 1)(x + 3) = x^2 + 3$. If $x + a$ and $x + b$ are in $(Z/4Z)[x]$ and $(x + a)(x + b) = x^2 + 3$ then $a + b = 0$ and $ab = 3$. It is impossible to find a pair other than 1, 3 in $Z/4Z$ which satisfies these conditions. Hence $f_1(x)\ f_2(x)$ is uniquely factorable into monic irreducible polynomials in $R[x]$.

Earlier we noted that any polynomial in $R[x]$ which is prime is also irreducible and in J. However we noted that an irreducible polynomial need not be prime. We now show that this property distinguishes finite fields and finite local rings which are not fields.

Lemma. Let $f(x)$ be a monic irreducible polynomial in J. Then $f(x)$ is prime if and only if $M \subseteq (f(x))$.

Proof: If $f(x)$ is prime then $R[x]/(f(x))$ is a finite integral domain. Hence $R[x]/(f(x))$ is a field and $(f(x))$ is maximal. Thus by Theorem 2.7, $M \subseteq (f(x))$.

Conversely, if $M \subseteq (f(x))$ then $(f(x), M) = (f(x))$ is a maximal ideal. Hence $f(x)$ is prime.

Theorem 2.9. (Characterization for finite fields) The following are equivalent if R is a finite local ring:

1. R is a finite field.

2. Every irreducible polynomial in $R[x]$ is prime.

3. There exists at least one monic irreducible polynomial in $R[x]$ which is prime.

Proof: (1.) implies (2.). If R is a field then $R[x]$ is a unique factorization domain. Hence irreducible and prime are equivalent.

(2.) implies (3.). By the Corollary to Theorem 2.3 there are infinitely many monic irreducible polynomials in R[x]. Hence the result follows.

(3.) implies (1.). If R is not a field then $M \neq 0$. We will show that R[x] has no monic primes. Let f(x) be a monic prime polynomial in R[x]. By Theorem 2.4, f(x) is irreducible and in J. Hence by the above lemma, $M \subseteq (f(x))$. Let a be a non-zero element of M. Since $M \subseteq (f(x))$ there exists a non-zero g(x) in R[x] such that $a = g(x)\ f(x)$. But f(x) is monic, so $\deg g(x)\ f(x) = \deg g(x) + \deg f(x) \geq 1$. But this is a contradiction since deg a is not greater than or equal to 1.

Corollary. Let R be a finite local ring which is not a field. Then

i. No monic polynomial is prime.

ii. No prime ideal is generated by a monic polynomial.

CHAPTER III

GALOIS THEORY OF FINITE LOCAL RINGS

One of the most renowned theorems in mathematics is the Fundamental Theorem of Galois Theory for fields. The theorem gives a lattice inverting correspondence between the separable subfields of a finite Galois extension F of a field K and the subgroups of the group of all K-automorphisms of F. S. Chase, D. K. Harrison and A. Rosenberg [5.] have proven its analog for commutative rings with finitely many idempotents. Theorem 3.1 is the statement of the Chase, Harrison, Rosenberg theorem in the context of finite local rings.

In this section R denotes a finite local ring with maximal ideal m.

Theorem 3.1. Let S be a finite local Galois extension of R. Let G be the group of all R-automorphisms of S. Then G is finite and $[G : 1] = \mathrm{Rank}_R (S)$ and there is a one to one lattice inverting bijection between the subgroups of G and the subrings of S which contain R and are separable over R. Normal subgroups correspond to normal extensions. The correspondence is given by $H \longleftrightarrow S^H$ and $T \longleftrightarrow \{\sigma \text{ in } G\text{: } \sigma(x) = x \text{ for all } x \text{ in } T\}$ where s^H is the subgroup of G whose elements leave S elementwise fixed.

The following is the ring analog of the theorem in field theory which states that any finite extension can be embedded in a finite normal extension.

Theorem 3.2. Let S be a finite free local separable extension of R. Then there exists a finite normal local separable extension N of R with S an extension of R contained in N.

Proof: See Ingraham and DeMeyer [8.].

Before we proceed we need to make an observation on finite Galois extensions.

Lemma. If S is a finite local Galois extension of R then S is a free R-module. Further $[S : R] = [S/mS : R/m]$.

Proof: By Theorem 1.15 there exists e in S^e, $e = \sum s_i \otimes t_i$ such that $\sum s_i t_i = 1$ and $(1 \otimes x - x \otimes 1)e = 0$. Let f_j be in $\mathrm{Hom}_R(S, R)$ be given by $f_j(x) = \sum_{\sigma \in G} \sigma(xt_j)$. Then $f_1, \ldots, f_n; s_1, \ldots, s_n$ form a "dual" basis for S over R. Thus S is projective and hence free over R. The last statement is now an immediate consequence of Theorem 1.14.

The following is due to G. Azumaya [4.]. We state it for finite local rings.

Theorem 3.3. Let f(x) be a monic polynomial in R[x], R a finite local ring. If $\bar{f}(x)$ has a non-multiple root $\bar{a}$ in R/m then f(x) has one and only one root in R which is a representative of $\bar{a}$.

Proof: Suppose $\bar{a}$ is a non-multiple root of $\bar{f}(x)$ in R/m then there exists a monic polynomial $\bar{f}_1(x)$ in (R/m)[x] such that $(x - \bar{a})\bar{f}_1(x) = \bar{f}(x)$ and $\bar{f}_1(\bar{a}) \neq 0$. Since R is a Hensel ring, there exist monic representatives $f_1(x)$ and $x - a$ in R[x] of $\bar{f}_1(x)$ and $x - \bar{a}$ respectively such that $(x - a)\, f_1(x) = f(x)$. Clearly a is a root of f(x) in R. If a_1 is a root of f(x) such that $\bar{a} = \bar{a}_1$ then $\bar{f}_1(\bar{a}_1) \neq 0$. Hence $\bar{f}_1(\bar{a}_1)$ is a unit in R/m. Thus $f_1(a_1)$ is a unit in R. Hence $(a_1 - a)\, f_1(a_1) = f(a_1) = 0$.

Thus $a_1 = a$.

Corollary. If f(x) is a monic irreducible polynomial in J then f(x) has no multiple roots in any local extension of R.

Goro Azumaya [4.] has also shown how to obtain R-automorphisms of S from R/m-automorphisms of S/mS.

Theorem 3.4. Let S be a finite local separable free extension of R then for any R/m-isomorphism $\bar{\sigma}$ of S/mS there exists one and only one R-isomorphism σ of S which induces $\bar{\sigma}$.

Proof: Since S/mS is a finite field, S/mS = (R/m)[$\bar{a}$]. Let $\bar{f}(x)$ be Irr (R/m, $\bar{a}$) and suppose [S/mS : R/m] = deg $\bar{f}(x)$ = n. Let f(x) be a representative of $\bar{f}(x)$ in R[x]. From Theorem 3.3 there exists one and only one a in S such that a is a root of f(x) and a representative of $\bar{a}$. Now 1, $\bar{a}$, ... , $\bar{a}^{n-1}$ is a basis of S/mS over R/m. Since S is R-free it follows that 1, a, ... , a^{n-1} is a free R-basis of S. Let $\bar{a}_o = \bar{\sigma}(\bar{a})$. Then $\bar{a}_o$ is a root of $\bar{f}(x)$. Hence there exists one and only one root a_o of f(x) which is a representative of $\bar{a}_o$. Define $\sigma(a) = a_o$. This extends to a unique ring homomorphism of S which fixes the elements of R. Since 1, a_o, ... , a_o^{n-1} is also a free R-basis of S it follows that σ is injective. Since the set is finite we conclude that σ is an isomorphism. Uniqueness follows from the preceeding result.

G. J. Janusz [10.] has introduced the concept of separable element and separable polynomial and investigated some of their properties.

Definition 3.1. A monic polynomial f(x) in R[x] is said to be separable if R[x]/(f(x)) is a separable extension of R.

Definition 3.2. If S is an extension of R then an element s in

S is <u>separable</u> if s is the root of some separable polynomial in R[x].

<u>Definition</u> 3.3. Let f(x) be a monic polynomial in R[x] with deg f(x) = n and 1 + (f(x)), x + (f(x)), ... , x^{n-1} + (f(x)) be a basis for R[x]/(f(x)) over R. Let f_i be the natural module projections from R[x]/(f(x)) onto R. Define t: R[x](f(x)) $\longrightarrow$ R by

$$t(s) = \sum_j f_j(sx_j + (f(x)).$$

The map t is called the <u>trace</u> of R[x]/(f(x)) over R.

The following is due to Janusz [10.].

<u>Theorem</u> 3.5. Let f(x) be a monic polynomial in R[x], then f(x) is separable if and only if the following is true:

Let t be the trace map of the free R-module R[x]/(f(x)) and let y = x + (f(x)). If n = degree of f(x) and if we let $[t(y^i\ y^j)]$ be the n x n matrix whose i + 1, j + 1 entry is $t(y^i\ y^j)$ then the determinant of $[t(y^i\ y^j)]$ is a unit in R.

The separablity of the following example is an immediate consequence of the above theorem.

<u>Corollary</u>. Let R be a finite local ring. Let R have p^n elements where p is a rational prime. Then for n greater than 1 and a in R, the polynomial x^n - a is separable if and only if a is a unit and p and n are relatively prime.

<u>Theorem</u> 3.6. A monic polynomial f(x) in R[x] is separable if and only if $\overline{f}(x)$ is square-free in (R/M)[x].

<u>Proof</u>: Let t and t' be the trace maps of <u>R[x]/(f(x))</u> and (R/m)[x]/($\overline{f}$(x)) respectively. Then we see that det $[t(y^i\ y^j)]$ = det $[t'(y'^i\ y'^j)]$ where y = x + (f(x)) and y' = x + ($\overline{f}$(x)). Then by Theorem 3.5, f(x) is separable over R if and only if det $[t(y^i\ y^j)]$ is

a unit in R. However det $[t(y^i\ y^j)]$ is a unit in R if and only if det $[t'(y^i\ y^j)] \neq 0$ in R/m. The result now follows from the next lemma.

Lemma. Let f(x) be a monic polynomial in F[x], F a finite field. Then f(x) is separable over F if and only if f(x) is square-free.

Proof: By a proof similar to the proof of Theorem 1.20 it can be shown that F[x]/(f(x)) is separable over F if and only if F[x]/(f(x)) is the direct sum of separable field extensions of F. If F[x]/(f(x)) is separable then it has no nilpotent elements other than zero. Hence f(x) must be square-free.

Conversely, if $f(x) = p_1(x) \ldots p_n(x)$ where the $p_i(x)$ are distinct irreducible polynomials in F[x] then R[x]/(f(x)) = $\sum\oplus$ F[x]/(p_i(x)). But F[x]/(p_i(x)) is a finite field extension of F and hence is separable since F is perfect.

The following result gives the connection between separable and irreducible polynomials in R[x].

Theorem 3.7. A monic polynomial f(x) in R[x] is separable and local if and only if f(x) is an irreducible polynomial in J.

Proof: Let f(x) be a monic polynomial in R[x]. Recall f(x) is local if and only if $\bar{f}(x)$ is the power of an irreducible polynomial in (R/m)[x]. But f(x) is separable if and only if $\bar{f}(x)$ is square-free. Thus we have f(x) is separable and local if and only if $\bar{f}(x)$ is irreducible. The result follows from Theorem 2.3.

Corollary. Let f(x) be a separable polynomial in R[x] then f(x) has distinct roots in any local extension of R.

Proof: Let a and b be roots of f(x) in some local extension of of R. Then $\bar{a}$ and $\bar{b}$ are roots of $\bar{f}(x)$ in some extension of R/m. But

$\bar{f}(x)$ has distinct roots in any extension. Hence $\overline{a - b}$ is a unit. But then $a - b$ is a unit and the result follows.

In the following result we prove the analog of the theorem for finite fields which states that if F and K are finite fields and K is an extension of F then K is normal over F and the Galois group is cyclic.

Theorem 3.8. Let S and R be finite local rings. Let S be a separable extension of R. Let M and m be the maximal ideals of S and R respectively. If S is free over R then S is normal over R and G(S, R), the Galois group of S over R, is isomorphic to G(S/M, R/m). Hence G(S, R) is cyclic.

Proof: Let H be the group of R-automorphisms of S. If σ is in H then $\sigma(a)$ is a unit or a nilpotent depending on whether a is a unit or a nilpotent. Hence σ induces an R/m-homorphism of S/M. Call it $\bar{\sigma}$. We note that it is actually an automorphism. For $\bar{\sigma}(\bar{a}) = 0$ if and only if $\sigma(a)$ is in M. But from above we know $\sigma(a)$ is in M if and only if a is. But then $\bar{a} = 0$. Since S/M is finite and $\bar{\sigma}$ is one to one, it is also onto. Let π be the map from H into G(S/M, R/m) given by $\pi(\sigma) = \bar{\sigma}$. It is clear that π is a group homomorphism. However by an application of Theorem 3.4 we conclude that π is also a one to one correspondence and hence an isomorphism. Since S/M is a finite field we conclude that H is cyclic. By Theorem 3.2 we can imbed S in a Galois extension of R which is local. From the above argument we know that its Galois group is cyclic. By Theorem 3.1 we can conclude that S is normal over R.

From an earlier lemma we see that the condition of being S-free is not extra. What we have shown is that to require S to be free and separable is equivalent to S being Galois.

The following result is due to Janusz [10.] and is extremely useful in finding Galois extensions.

Theorem 3.9. Let S be a local Galois extension of R and suppose a is an element of S with R[a] a separable extension of R. Let $a = a_1$, a_2, ... , a_m be all the distinct images of a under the Galois group of S. If g(x) is any polynomial in R[x] such that g(a) = 0, then g(x) is a multiple of $f(x) = (x - a_1) \dots (x - a_m)$ by an element of R[x].

Theorem 3.10. Let S be a local Galois extension of R.

(1.) The Galois group of S over R permutes the roots of a separable local polynomial f(x) in R[x] where f(x) is satisfied by some primitive element of S and deg f(x) = [S : R].

(2.) If f(x) is a polynomial described above and a is a primitive element of S over R satisfying f(x) then $S \simeq R[a] \simeq R[x]/(f(x))$.

Proof: This is an immediate corollary of Theorem 3.9 and the observation that $R[x] \longrightarrow R[a]$ is an R-epimorphism.

We are now in a position to give a characterization of Galois extensions of finite local rings.

Theorem 3.11. If R is a finite local ring then S is a local Galois extension of R if and only if S is isomorphic to R[x]/(f(x)) where f(x) is a monic irreducible polynomial in J.

Proof: Suppose S is a local Galois extension of R then by Theorem 1.22, S has a primitive element over R -- say a. By Theorem 3.10, $S \simeq R[x]/(f(x))$. Hence f(x) is separable and local. But then by Theorem 3.7, f(x) is an irreducible polynomial in J.

Conversely, if f(x) is irreducible and in J then f(x) is local and separable. It follows from the remark following Theorem 3.8 that

$R[x]/(f(x))$ is also normal and hence Galois.

In the case of finite fields the following result follows from the uniqueness (up to isomorphism) of the splitting field of a polynomial of the form $x^{p^n} - x$ for some rational prime p and natural number n.

Theorem 3.12. For any rational prime p and natural number n there exists a unique finite field with p^n elements.

Related to the above is the following well-known result,

Theorem 3.13. Let $GF(q^r)$ and $GF(q)$ be the Galois fields of q^r and q elements respectively. Let n be the number of primitive elements of $GF(q^r)$ over $GF(q)$ and t the number of monic irreducible polynomials in $GF(q)[x]$. Then $tr = n$.

Proof: Recall $GF(q^r) = GF(q)[a]$ where a satisfies a monic irreducible polynomial of degree r. Conversely a root of a monic irreducible polynomial of degree r is a primitive element for $GF(q^r)$ over $GF(a)$. This follows from the uniqueness of Galois fields. Also the irreducible polynomials of degree r have r distinct roots. Hence $tr = n$.

A closer examination of the above proof reveals that the above theorem is actually equivalent to the uniqueness theorem for Galois fields. Since our characterization of local Galois extensions in the commutative ring case is identical to that of the field case, we see that the following two theorems are equivalent.

Theorem 3.14. Let S be a local Galois extension of rank r over R, R a finite local ring. Let t_1 be the number of monic irreducible polynomials of degree r in J and n_1 the number of primitive elements of S over R then $t_1 r = n_1$.

Theorem 3.15. For each natural number r and finite local ring R there exists exactly one (up to isomorphism) local Galois extension S such that $[S : R] = r$.

Proof: The existence part of Theorem 3.15 follows from the corollary to Theorem 2.3. Let S be a local Galois extension of rank r over R. Let M and m be the maximal ideals of S and R respectively. Then $t_1 = t|m|^r$ and $n_1 = n|M|$, where t and n are the corresponding values for S/M. Now $tr = n$. Hence $t_1 r = n_1$ if and only if $|M| = |m|^r$. Now note that if a is a primitive element for S then $1, a, \ldots, a^{r-1}$ is a basis for S over R since $1, \bar{a}, \ldots \bar{a}^{r-1}$ is a basis for S/M over R/m. If $d_0 + d_1 a + \ldots + d_{r-1} a^{r-1}$ is in M where d_i is in R then $\bar{d}_0 + \bar{d}_1 \bar{a} + \ldots + \bar{d}_{r-1} \bar{a}^{r-1} = 0$. But $1, \bar{a}, \ldots, \bar{a}^{r-1}$ is a basis for S/M over R/m. Hence $\bar{d}_i = 0$. Hence d_i is in $R \cap M = m$.

Conversely, any element of the above form is in M. So $|M| = |m|^r$ and the theorems above are proven.

We conclude this section with some miscellaneous observations and examples.

The following is a special case of a theorem of Janusz [10.] and will be useful in the examples.

Theorem 3.16. Let S be a local Galois extension of R and a an element of S. Then R[a] is a R-separable extension of R if and only if a is a separable element over R.

It is then immediate from this result that any primitive element of S over R is separable.

Example 3.1. Let $R = Z/4Z$. Then R is a finite local ring with maximal ideal $2Z/4Z$. Consider $f(x) = x^3 + x + 1$ in R[x]. Since $\bar{f}(x) =$

$x^3 + x + 1$ in $(Z/2Z)[x]$ is irreducible, $f(x)$ is irreducible. Hence $S = R[x]/(f(x))$ is a local Galois extension of R. The rank of S over R is 3. Hence by the Fundamental Theorem G(S, R) is a cyclic group of order 3 and there are no proper R-separable subrings of S other than R.

Example 3.2. Let $R = Z/4Z$ and $f(x) = x^4 + x^3 + x^2 + x + 1$ be in $R[x]$. Since $f(x)$ is irreducible, $S = R[x]/(f(x))$ is a local Galois extension of R. Thus $G(S, R) = \langle\sigma\rangle$ is a cyclic group of order 4. Thus we have the following chain of R-separable extensions of R: $R \subseteq T \subseteq S$ where $T \simeq R[x]/(g(x))$ and $g(x) = x^2 + x + 1$. By Theorem 3.4 we can construct the R-automorphisms of S from those of G(S/M, R/m). One first checks that if a is a root of $f(x)$ in S then

$$f(x) = (x - a)\ (x - a^2)\ (x - a^3)\ (x - (3a^3 + 3a^2 + 3a + 3)).$$

Now $1, a, a^2, a^3$ is a basis of S over R. Hence

$$\sigma(a) = a^2$$
$$\sigma^2(a) = 3a^3 + 3a^2 + 3a + 3$$
$$\sigma^3(a) = a^3$$
$$\sigma^4(a) = a.$$

This suffices to define σ, σ^2, σ^3 and σ^4 = identity. Now $g(x) = x^2 + x + 1 = (x - (a^3 + a^2 + 2))\ (x - (3a^3 + 3a^2 + 1))$. Notice that

$$\begin{aligned}(a^3 + a^2 + a) &= (\sigma^2(a))^3 + (\sigma^2(a))^2 + 2\\ &= 3a^9 + a^8 + 2a^7 + 3a^6 + 2a^5 + 3a^4 + 2a^3 + a^2 + 3a + 2\\ &= a^3 + a^2 + 2.\end{aligned}$$

So $a^3 + a^2 + 2$ is in the fixed ring of σ^2. Also $R[a^3 + a^2 + 2]$ is a separable R-subring of S by Theorem 3.16. In fact $T = R[a^3 + a^2 + 2]$.

Let us recall the following theorem from field theory:

Theorem 3.17. Let K be a field of degree n over GF(q), the

Galois field with q elements. Then the Galois group of K over GF(q) is the cyclic group of order n generated by the automorphism $x \longrightarrow x^q$.

For a proof one can see Albert [1.].

For the ring case although the Galois group is cyclic the generating map cannot be described as a power map on all the elements.

Example 3.3. Let R be the integers modulo 4 and S = R[a] where a satisfies $x^2 + x + 1$. Then if M and m are the maximal ideals of S and R respectively then $|G(S/M, R/m)| = [S/M : R/m] = 2$. Let $\{\bar{1}, \bar{\sigma}\} = G(S/M, R/m)$. Note that $x^2 + x + 1 = (x - a)(x - (3a + 3))$ in S[x]. The proof of Theorem 3.4 yields that $G(S, R) = \{1, \sigma\}$ where σ is given by $\sigma(a) = 3a + 3$. Now no power of 2a is $2a + 2 = \sigma(2a)$. Also $\sigma(3a + 1) = 3\sigma(a) + 1 = 3(3a + 3) = a + 2$. It is easy to check that a + 2 is not a power of 3a + 1. However $\sigma(a) = 3a + 3 = a^2$. Hence G(S, R) is generated by an automorphism which takes a primitive element to its square.

Lemma. Let S be a finite local Galois extension of R, m the maximal ideal of R and f(x) a monic irreducible polynomial in J. If a and b are roots of f(x) in S then there exists a monic irreducible polynomial g(x) in J such that a^q and b^q are roots of g(x) where $q = |R/m|$.

Proof: Let f(x) be a monic irreducible polynomial in J with a and b roots of f(x). Since f(x) is irreducible in J, $\bar{f}(x)$ is irreducible in (R/m)[x]. So $\bar{f}(x) = \text{Irr}(R/m, \bar{a})$. Since R/m is a finite field with q elements $\bar{a}^q$ is also a root of $\bar{f}(x)$. So $f(a^q) = t$ is in m. Let $g(x) = f(x) - t$. Clearly $\bar{g}(x) = \bar{f}(x)$. So g(x) is a monic irreducible polynomial in J. Further $g(a^q) = f(a^q) - t = 0$. Consider the polynomial $h(x) = g(x^q)$ in $R[x]$. Note that a is a root of $h(x)$. By Theorem 3.9, $h(x)$ is divisible by $f(x)$. Since b is a root of $f(x)$, b must be a root of $h(x)$. Hence b^q is a root of $g(x)$.

Theorem 3.18. Let S be a finite local Galois extension of R, M and m the maximal ideals of S and R respectively. Let $[S : R] = n$ and $q = |R/m|$. Then there exists a primitive element t with $S = R[t]$ such that the R-automorphism σ of S given by $\sigma(t) = t^q$ is a generator of the Galois group of S over R.

Proof: Let $f(x)$ be a monic irreducible polynomial of degree n in J and a a root of $f(x)$. Let $A = \{g(x) \text{ in } R[x]\colon \bar{f}(x) = \bar{g}(x)\}$. Let $B = \{b \text{ in } S\colon b \text{ is a root of some polynomial in } A\}$. Let $B^k = \{b^k\colon b \text{ is in } B\}$ and k is a natural number. Now $B \geqq B^q \geqq B^{q^2} \geqq \ldots$. Further $\bar{f}(x) = (x - \bar{a})\,(x - \bar{a}^{\,q}) \ldots (x - \bar{a}^{\,q^{n-1}})$. Hence each element of B is a representative of one of the following: $\bar{a}, \bar{a}^{\,q}, \ldots, \bar{a}^{\,q^{n-1}}$. So each element of B has the form $a^k + c$ where c is in M and $k = 1, q, \ldots, q^{n-1}$. Hence there exists an s such that $B^s = B^{s+1} = \ldots$ and such that B^s has only n elements. Raising these to the q^{th} power only results in a shuffling of their order. By Theorem 3.4 and the lemma above there exists an R-automorphism σ of S given by $\sigma(t) = t^q$ where t is in B^s. Consider $\bar{\sigma}, \bar{\sigma}^2, \ldots, \bar{\sigma}^n$. These are all distinct since $G(S/M, R/m)$ is generated by the map $x \longrightarrow x^q$. Hence σ generates $G(S, R)$.

We note that the s in the above proof can easily be bounded. Let r be the degree of nilpotency of the maximal ideal m of R. Then if $(a^k + c)$ is in B where a and c are described in the proof of Theorem 3.18 then

$$(a^k + c)^{q^r} = a^{kq^r} + \binom{q^r}{1}(a^k)^{q^r-1} c + \dots + \binom{q^r}{1} a^k c^{q^r-1} + c^{q^r}.$$

But recall that $q = p^m$ for some prime p and natural number m. Also the characteristic of R is a power of the same prime p. Hence q is in the maximal ideal of R. Also q^{r-1} divides $\binom{q^r}{i}$ for any i. Thus, the above equation becomes $(a^k + c)^{q^r} = a^{kq^r}$, $k = 1, q, \dots, q^{n-1}$. Thus we summarize our results on the Galois group:

Theorem 3.19. Let S and R be finite local rings with maximal ideals M and m respectively. Let r be the degree of nilpotency of the maximal ideal m and q the number of elements in the residue field R/m. If S is a Galois extension of degree n over R then the Galois group G(S, R) of S over R is a cyclic group of order n and is generated by the map σ where $\sigma(a^{q^r}) = a^{q^{r+1}}$ and a is a root of a monic irreducible polynomial of degree n in J.

Definition 3.4. If a ring S is a Galois extension of R then we say S has a normal basis over R if there exists an a in S such that $\{\sigma(a)\colon \sigma \text{ in } G(S, R)\}$ is a basis for S over R.

Theorem 3.20. (Normal Basis Theorem) Let S and R be finite local rings. If S is a Galois extension of R then S has a normal basis over R.

Proof: The result holds for finite fields. We can conclude it holds for any finite local ring by using Theorem 3.4 and Theorem 1.14.

Theorem 3.21. Let S be a local Galois extension of R. Then there exists a lattice preserving bijection between the subfields of S/mS containing R/m and the separable subrings of S containing R.

Proof: Let m be the maximal ideal of R. Consider the relation

$T \longleftrightarrow T/mT$ from the set of separable subrings of S containing R and the set of separable subfields of S/mS containing R/m. We know by the Fundamental Theorems of Galois theory for both rings and fields that there exists a lattice inverting one-to-one correspondence between the separable subrings or subfields and the subgroups of the corresponding Galois group. But G(S, R) is isomorphic to G(S/mS, R/m). Composing the isomorphisms and the correspondences completes the proof.

Corollary 1. Let S, S_1 and S_2 be finite local Galois extensions of R with S_1 and S_2 contained in S. If m is the maximal ideal of R and $S_1/mS_1 = S_2/mS_2$ then $S_1 = S_2$.

Corollary 2. Let S be a finite local Galois extension of R and m the maximal ideal of R. If T is a separable extension of R contained in S then $G(S, T) \simeq G(S, R)/G(T, R)$.

Janusz [10.] has introduced a generalization of the concept of a splitting field.

Definition 3.5. A Galois extension S of a commutative ring R is a splitting ring for a separable polynomial f(x) in R[x] if f(x) is the product of linear factors in S[x] and S is generated over R by the roots of f(x).

Recall that if F and G are finite fields with F an extension of G then F is the splitting field of some monic irreducible polynomial in G[x]. A similar result holds for finite local rings.

Theorem 3.22. If S is a finite local Galois extension of degree n over R then S is a splitting ring for any monic irreducible polynomial in J of degree n.

Proof: Let f(x) be a monic irreducible polynomial in J of degree n. Now [S/M : R/m] = n. So f(x) splits in S/M. The result follows immediately from Theorems 3.4 and 3.15.

Let k = R/m then it is well-known, for example see Dickson [7.], that if v(n, k) denotes the number of monic irreducible polynomials of degree n where $n = p_1^{e_1} \cdots p_s^{e_s}$ in k[x] then

$$v(n, k) = (1/n)[|k|^n - \sum_i |k|^{n/p_i} + \sum_{i \neq j} |k|^{n/p_ip_j} - \cdots + (-1)^s |k|^{n/p_1p_2 \cdots p_s}].$$

Thus by Theorem 2.3, there exist

$$v(n, R) = (1/n)|R|^n[1 - \sum_i |k|^{1/p_i} + \sum_{i \neq j} |k|^{1/p_ip_j} - \cdots + (-1)^s |k|^{1/p_1p_2 \cdots p_s}].$$

monic irreducible polynomials in J. Hence n v(n, R) primitive elements for a Galois extension S of R with rank S over R equal to n.

We conclude this chapter with one remark concerning elementwise separablity. In the field case separablity is defined elementwise. However the following is false: S is a separable extension of R if and only if each element in S is separable over R.

Example 3.4. Consider (Z/4Z)[a] where a satisfies the polynomial $x^2 + x + 1$ in (Z/4Z)[x]. Let b = 2a. Recall that by Theorem 3.16, b is separable if and only if R[b] is a separable extension of R. The Galois group of (Z/4Z)[a] over Z/4Z is the cyclic group of order 2. Hence by the Fundamental Theorem there do not exist any separable subrings of (Z/4Z)[a] strictly between (Z/4Z)[a] and Z/4Z. Thus since b is not a primitive element of S it follows that b is not separable.

CHAPTER IV

A STRUCTURE THEOREM

In this chapter we show that finite local rings are homomorphic images of certain polynomial rings.

Let R be a finite local ring with maximal ideal M. Consider generating sets of M over R. Since these are finite sets there exist minimal sets among them. The following shows that this number is an invariant of M.

Theorem 4.1. The elements $\{u_1, \ldots, u_n\} \subseteq M$ form a minimal generating set for M if and only if modulo M^2 they give rise to an R/M-basis of M/M^2. The number of elements is thus equal to the dimension of M/M^2 over R/M.

Recall that the characteristic of R is p^k for some prime p and natural number k. Also R/M has characteristic p. Two cases could then arise. One where the characteristics are equal and one where they are not. Following Nagata [13.] we shall handle both cases simultaneously.

Theorem 4.2. Let R be a finite local ring with characteristic p^k and maximal ideal M such that M has minimal generating set $\{u_1, \ldots, u_n\}$. Then there exists a subring T of R such that

(1) T is a separable hence simple extension of Z/Zp^k.

(2) $T/(M \cap T) \simeq R/M$.

(3) R is the homomorphic image of $T[x_1, \ldots, x_n]$.

Proof: Since R/M is a finite field it has a cyclic group of units. Let $\bar{v}$ be a generator of the group of units of R/M. If $\bar{f}(x)$ is the minimal polynomial of $\bar{v}$ in $(Z/Zp)[x]$, let $f(x)$ be a monic preimage of $\bar{f}(x)$ in $(Z/Zp^k)[x]$. Since $\bar{f}(x)$ is irreducible, $f(x)$ is irreducible in $(Z/Zp^k)[x]$ and is also in J. By Theorem 3.3, R contains an element v such that $f(v) = 0$ and $\bar{v}$ is the image of v under the natural map $\pi: R \longrightarrow R/M$. Since $f(x)$ is irreducible and in J it is separable and hence $(Z/Zp^k)[x]/(f(x))$ is a separable extension of Z/Zp^k. Further since $f(v) = 0$, $(Z/Zp^k)[v]$ is a homomorphic image of $(Z/Zp^k)[x]/(f(x))$. Hence $(Z/Zp^k)[v]$ is a separable extension of Z/Zp^k. Let $T = (Z/Zp^k)[v]$. Also there exists a natural ring injection of $T/(M \cap T)$ into R/M. Since $\bar{v}$ generates $R/M - \{0\}$ it is clear that this is a surjection and hence $T/(M \cap T) \simeq R/M$. The proof will be complete if we show that $T[u_1, \ldots, u_n] = R$. Clearly $T[u_1, \ldots, u_n] \subseteq R$. Let c be in R. We will construct a sequence $\{c_s\}$ such that $c \equiv c_s \bmod M^{s+1}$ and c_s is in $T[u_1, \ldots, u_n]$. Since M is nilpotent this will complete the proof. From the isomorphism above $c \equiv a \bmod M$ for some a in T. So let $c_o = a$. Suppose c_s has been constructed. Then $c_s = c - q$ where q is in M^{s+1}. Since $\{u_i\}$ generate M over R, $q = \sum a_i v_i$ where a_i is in R and v_i is a power product of the $\{u_i\}$ of degree s + 1. Now $a_i \equiv b_i \bmod M$ for some b_i in T. So

$$c - c_s \equiv \sum b_i v_i \mod M^{s+2}.$$

Let

$$c_{s+1} = c_s + \sum b_i v_i.$$

Clearly c_{s+1} is in $T[u_1, \ldots, u_n]$. Also

$$c_{s+1} - c = c_s + \sum b_i v_i - c \equiv 0 \bmod M^{s+2}.$$

Note that the conditions (1) and (2) along with the correspondence between the lattices of separable subrings of T and subfields of R/M imply that T is unique. The subring T is called the coefficient ring of R and is the largest separable extension of Z/Zp^k contained in R.

CHAPTER V

SOLUTIONS OF POLYNOMIALS OVER FINITE LOCAL RINGS

Consider the following problem: If m is a positive integer and f(x) is in Z[x] find all x such that f(x) = 0 (mod m). This is, of course, a problem in the theory of congruences. It can be stated algebraically as follows: Find the roots of f(x) in Z/(m). Recall that this question is then reduced to finding the roots of f(x) in $Z/(p^k)$ where $m = \prod p_i^{k_i}$, where the p_i are distinct primes. But notice this is what occurs when a finite commutative ring with identity is decomposed into finite local rings. Thus the analogous question for finite commutative rings with identity is reduced to finite local rings.

Let R be a finite local ring with maximal ideal M and residue field R/M = K. Let n be the degree of nilpotency of M. Then there exists a natural sequence of surjective homomorphisms:

$$R = R/M^n \xrightarrow{\sigma_n} R/M^{n-1} \longrightarrow \cdots \longrightarrow R/M^i \xrightarrow{\sigma_i} R/M^{i-1} \longrightarrow \cdots \longrightarrow R/M = K$$

where $\ker \sigma_i = M^{i-1}/M^i$. Further each M^{i-1}/M^i is a K-vector space. Notice the action of K on M^{i-1}/M^i is given by $\bar{k}m = km$ where k is a preimage of $\bar{k}$ in R/M^i under the surjection from R/M^i to K. Let $\dim_K (M^{i-1}/M^i) = \psi_i(R)$. The approach is then similiar to that of solving congruences. We illustrate by constructing solutions of f(x) in $(R/M^i)[x]$ from the solutions of $\bar{f}(x)$ in $(R/M^{i-1})[x]$. For convenience let $\dim_K(M^{i-1}/M^i) = t$ and $\{v_1, \ldots, v_t\}$ be a K-basis for M^{i-1}/M^i. Let $\bar{A}$ be a solution of $\bar{f}(x)$ in R/M^{i-1} and A a preimage of $\bar{A}$ in R/M^i. Let $a = A + m$ where m is in M^{i-1}/M^i. Notice $(M^{i-1}/M^i)^2 = 0$. Thus by Taylor's Theorem

$$\begin{aligned} f(a) &= f(A + m) \\ &= f(A) + m\, f'(A) + m^2\, Q \\ &= f(A) + m\, f'(A) \end{aligned}$$

where $f'(x)$ is the formal derivative and Q is some element in R/M^i. If $f(a) = 0$ then

$$f(A) = -\, m\, f'(A) = -\, \overline{f'(A)}\, m \qquad (1)$$

and $f(A)$ is in M^{i-1}/M^i. Since $\{v_1, \ldots, v_t\}$ is a basis of M^{i-1}/M^i over K, we have

$$f(A) = \sum_{i=1}^{t} b_i\, v_i$$

and

$$m = \sum_{i=1}^{t} a_i\, v_i$$

where b_i, a_i are in K. Hence (1) becomes

$$\begin{aligned} 0 &= \sum_{i=1}^{t} b_i\, v_i + \overline{f'(A)}\, (\sum_{i=1}^{t} a_i\, v_i) \\ &= \sum_{i=1}^{t} [b_i + \overline{f'(A)}\, a_i]\, v_i. \end{aligned}$$

Hence for each i, $0 = b_i + a_i\, \overline{f'(A)}$. Three cases arise.

(I.) $f'(A)$ is a unit.

Then $\overline{f'(A)}$ is a unit and each a_i is uniquely determined. In this case there is only one solution of $f(x)$ for $\bar{A}$.

(II.) $f'(A)$ is in M and there exists a $b_i \neq 0$.

In this case there are no solutions of $f(x)$ for $\bar{A}$.

(III.) $f'(A)$ is in M and $b_i = 0$ for all i.

In this case $f(A) = 0$ for any preimage of $\bar{A}$. Thus there are $|K|\ t = |K|\,\psi_i(R)$ solutions for $\bar{A}$.

We conclude that we obtain all solutions of $f(x)$ in R/M^i. For if a is a solution of $f(x)$ in R/M^i then $\bar{f}(\bar{a}) = \overline{f(a)} = 0$ and hence $\bar{a}$ is solution of $\bar{f}(x)$.

BIBLIOGRAPHY

1. Albert, A. Adrian. Fundamental Concepts of Higher Algebra. Chicago: University of Chicago Press, 1956.

2. Atiyah, Michael F. and MacDonald, Ian G. Introduction to Commutative Algebra. Reading, Mass.: Addison-Wesley Publishing Company, 1969.

3. Auslander, Maurice and Buchsbaum, David. "On Ramification Theory in Noetherian Rings," American Journal of Mathematics, 81 (1959), pp. 367-409.

4. Azumaya, Goro. "On Maximally Central Algebras," Nagoya Mathematics Journal, 3 (1951), pp. 119-150.

5. Chase, S. U., Harrison, D. K., and Rosenberg, Alex. A Galois Theory and Cohomology of Commutative Rings. Memoirs 52. Providence: American Mathematical Society, 1965.

6. Dean, Richard A. Elements of Abstract Algebra. New York: John Wiley and Sons, Inc., 1966.

7. Dickson, Leonard Eugene. Linear Groups. New York: Dover Publications, Inc., 1958.

8. Ingraham, Edward D. and DeMeyer, Frank. Separable Algebras over Commutative Rings. Lecture Notes in Mathematics, Number 181. New York: Springer-Verlag, 1971.

9. Jans, James P. Rings and Homology. New York: Holt, Rinehart and Winston, 1964.

10. Janusz, G. J. "Separable Algebras over Commutative Rings," Transactions of the American Mathematical Society, 122 Number 2 (1966), pp. 461-479.

11. Kaplansky, Irving. "Projective Modules," Annals of Mathematics. 68 (1958), pp. 372-377.

12. McDonald, Bernard R. "Notes on Finite Commutative Rings," Lectures presented at The University of Oklahoma, Norman, Oklahoma, Summer 1969.

13. Nagata, Masayoshi. Local Rings. New York: Interscience Publishers, 1962.