363649

(En)
0153.3
K17

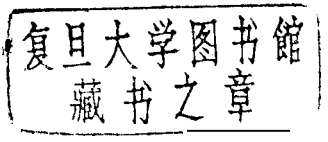
i

Commutative Rings

Revised Edition

IRVING KAPLANSKY





The University of Chicago Press
Chicago and London

To Chellie

IRVING KAPLANSKY is George Herbert Mead Distinguished Service Professor in the Department of Mathematics, the University of Chicago. He is the author of numerous books and articles and is the general editor of the Chicago Lectures in Mathematics series published by the University of Chicago Press. [1974]

The University of Chicago Press, Chicago 60637
The University of Chicago Press, Ltd., London

© 1970, 1974 by The University of Chicago
All rights reserved. Revised edition published I974
Printed in the United States of America

International Standard Book Number: 0-226-42454-3
Library of Congress Catalog Card Number: 71-102759

Contents

Preface ix

Preface to the Revised Edition xi

Chapter 1 **Prime Ideals and Integral Extensions** 1
1-1 Prime Ideals 1
1-2 Integral Elements, I 8
1-3 G-ideals, Hilbert Rings, and the Nullstellensatz 12
1-4 Localization 22
1-5 Prime Ideals in Polynomial Rings 25
1-6 Integral Elements, II 27

Chapter 2 **Noetherian Rings** 47
2-1 The Ascending Chain Condition 47
2-2 Zero-divisors 54
2-3 Integral Elements, III 66
2-4 Intersections of Quasi-local Domains 75

Chapter 3 **Macaulay Rings and Regular Rings** 84
3-1 R-sequences and Macaulay Rings 84
3-2 The Principal Ideal Theorem 104
3-3 Regular Rings 115

Chapter 4 **Homological Aspects of Ring Theory** 123
4-1 Homology 123
4-2 Unique Factorization 130
4-3 The Euler Characteristic 137
4-4 Change of Rings for Injective Dimension 149
4-5 Gorenstein Rings 156
4-6 Duality 165

Notes 169
Bibliography 171
Index of Theorems 174
Index of Topics 181

Preface

This account of commutative rings has grown over the years through various stages. The first version was an appendix to the notes on homological dimension issued in 1959 (these notes, without the appendix, have now appeared as Part III of [26]). The second was a crude 49 page dittoed manuscript written in 1961. This account was expanded in the 1965–6 course presented at Queen Mary College. I owe an enormous debt to Professor Paul M. Cohn of Bedford College for his expert job in writing up the course; large parts are incorporated here with only small changes. **A** draft of the book was prepared during the summer of 1968, and was used for a course at Chicago during 1968–9.

No attempt has been made to achieve scholarly completeness. References to sources have been made only in scattered instances where it seemed particularly desirable, and the bibliography contains only items to which there is an actual reference. My intention is to give an account of some topics in the theory of commutative rings in a way that is accessible to a reader with a modest background in modern algebra; I assume only an acquaintance with the definitions and most elementary properties of rings, ideals, and modules. More exactly, this is true till §4-1, where I presuppose the theory of homological dimension as developed in [26], and §4-4 where use of the long exact sequence for Ext begins. **I** hope that readers will find it feasible to go on from this book to a deeper study of the literature. It would be most urgent to learn the theory of completion and the Cohen structure theorems.

I have inserted numerous exercises, partly to cover additional material of lesser importance, and partly to give the reader a chance to test his growing skill. There is occasional reliance on the exercises as part of the exposition, and I hope no reader will find this inconvenient.

In the style of Landau, or Hardy, and Wright, **I** have presented the

material as an Unbroken series of theorems. I prefer this to the n-place decimal system favored by some authors, and I have also grown tired of seeing a barrage of lemmas, propositions, corollaries, and scholia (whatever they are). I admit that this way the lowliest lemma gets elevated to the same eminence as the most awesome theorem. Also, the number of theorems becomes impressive, so impressive that I felt the need to add an index of theorems.

All rings have a unit element, except for a fleeting instant in **Ex.** 22 of §2-2. All rings are commutative except in several (not quite so fleeting) isolated passages. Somewhat erratically, the adjective "noncommutative" is occasionally inserted, merely for emphasis.

I am very grateful to Joel Cohen, David Eisenbud, Graham Evans, Marshall Fraser, Ross Hamsher, William Heinzer, Martin Isaacs, Stanley Kochman, Peter Kohn, Stephen McAdam, Judith Sally, and Wolmer Vasconcelos for numerous valuable suggestions. If fully credited, their names would be everywhere dense. Robert Gilmer was especially generous in reading the manuscript critically and enlightening me on many points.

Final thanks go to Joyce Bolden and Diane Moore for a splendid job of typing, and to Sylvia Clark, Gerald Curtis, and Mary Johnson of Allyn and Bacon, Inc. for their fine cooperation.

IRVING KAPLANSKY

Preface to the Revised Edition

In this reprinting of *Commutative* ***Rings*** minor slips have been corrected and several more substantial changes have been made (largely in the exercises). I am indebted to many students and colleagues; they are too numerous to list, but I am none the less appreciative.

In a brief new section entitled "Notes" I have added some comments which are in the nature of afterthoughts rather than a revision of the text.

CHAPTER 1

Prime Ideals and Integral Extensions

1-1 PRIME IDEALS

Prime ideals play a central role in the theory of commutative rings, and it is appropriate to devote the first section to a collection of observations concerning them.

We recall the definition: in a commutative ring R, the ideal I is prime if $ab \in I$ implies $a \in I$ or $b \in I$. Alternatively: I is prime if R/I is an integral domain. The convention that R itself is not regarded as a prime ideal is fairly universally accepted now, and we shall adhere to it (except, no doubt, for occasional slips). In the ring of integers there is an analogous convention that 1 is not a prime.

Let S be the set-theoretic complement of an ideal I. Then the definition of a prime ideal can be recast as follows: I is prime if and only if S is multiplicatively closed. Now it goes without saying that I is maximal with respect to the exclusion of S. Krull discovered a very useful converse.

Theorem 1. *Let S be a multiplicatively closed set in a ring R and let I be an ideal in R maximal with respect to the exclusion of S. Then I is prime.*

Proof. Given $ab \in I$ we must show that a or b lies in I. Suppose the contrary. Then the ideal (I, a) generated by I and a is strictly larger

than I and therefore intersects S. Thus there exists an element $s_1 \in S$ of the form $s_1 = i_1 + xa$ $(i_1 \in I,\ x \in R)$. Similarly we have $s_2 \in S$, $s_2 = i_2 + yb$. But then

$$s_1 s_2 = (i_1 + xa)(i_2 + yb) \tag{1}$$

and all four terms on the right of (1) lie in I (the first three because a factor lies in I and the fourth because $ab \in I$). Hence $s_1 s_2 \in I$, a contradiction.

We note that, given any ideal J disjoint from a multiplicatively closed set S, we can by Zorn's lemma expand J to an ideal I maximal with respect to disjointness from S. Thus we have a method of constructing prime ideals.

Before proceeding, let us examine more closely the complement of a prime ideal. It is not any old multiplicatively closed set; it has the further property of being ***saturated*** in the sense that along with an element x it contains all the divisors of x. We are led to the following theorem, in essence a sharpening of Theorem 1.

Theorem 2. ***The following statements on a set S in a ring R are equivalent: (1) S is a saturated multiplicatively closed set, (2) the complement of S is a set-theoretic union of prime ideals in R.***

Proof. That (2) implies (1) is immediate from the definitions. To prove that (1) implies (2) take x in the complement of S. Then the principal ideal (x) is disjoint from S, since S is saturated. Expand (x) to an ideal I maximal with respect to disjointness from S (Zorn). By Theorem 1, I is prime. Thus every x not in S has been inserted in a prime ideal disjoint from S, proving (2).

Remarks. 1. In Theorem 2 it would have been reasonable to exclude the possibility $0 \in S$. A saturated multiplicatively closed set containing 0 is the whole ring, and its complement is the null set, which is vacuously but not very convincingly a union of prime ideals.

2. When we express the complement of S as a union of prime ideals we can of course discard any prime ideals not maximal within the complement in favor of the maximal ones.

Let us give two illustrations.

1. The set consisting of 1 is multiplicatively closed. Its saturation is the set of all units. The prime ideals maximal in the complement are just the ordinary maximal ideals.

2. Let S be the set of all non-zero-divisors in R. S is a saturated multiplicatively closed set. **So:** the zero-divisors in R are a union of prime ideals. The prime ideals maximal among these might be called the "maximal primes of zero-divisors."

Both of these illustrations admit appropriate generalizations to modules: in the first case take all elements of R that act one-to-one and onto as multiplications of the given R-module; in the second case take all non-zero-divisors on the module. This second case is important enough to merit a definition.

Definition. Let R be any commutative ring, A any non-zero R-module. The prime ideals maximal within the zero-divisors on A are called the ***maximal primes*** of A. When A has the form R/I, I an ideal in R, we say maximal primes of I, rather than of R/I; the danger of ambiguity is slight.

At this point we shall briefly discuss unique factorization domains (UFD's). They can be characterized by a suitable interplay between prime ideals and principal ideals (Theorem 5). In the course of the discussion we encounter an instructive example of a saturated multiplicatively closed set, and a typical application of Theorem 1.

Notice that for a principal ideal (p) to be prime, p must have the following property: $p \mid ab$ implies $p \mid a$ or $p \mid b$ (the vertical line means "divides"). Let us for brevity call p a ***principal prime*** if the principal ideal (p) is prime and non-zero.

Theorem 3. *If **an element in an integral domain is expressible as a product $p_1 p_2 \ldots p_n$ of principal primes, then that expression is unique, up to a permutation of the p's, and multiplication of them by unit factors.***

We leave the standard proof to the reader.

Theorem 4. ***Let R be an integral domain. Let S be the set of all elements in R expressible as a product of principal primes. Then S is a saturated multiplicatively closed set.***

Proof. Obviously S is multiplicatively closed. To prove that S is saturated we assume $ab \in S$ and have to prove that a and b lie in S. So suppose $ab = p_1 \cdots p_n$, a product of principal primes. Then p_1 must divide a or b. Say $a = p_1 a_1$. Then $a_1 b = p_2 \ldots p_n$. By induction on n we have that both a_1 and b are in S, and hence $a, b \in S$.

Theorem 5. ***An integral domain is a UFD if and only if every non-zero prime ideal in R contains a principal prime.***

Proof. (a) Assume R is a **UFD** and P a non-zero prime ideal in R. Unless R is a field (a trivial case we are tacitly ignoring), P will contain an element a that is neither 0 nor a unit. When a is written as a product of principal primes, $a = p_1 \cdots p_r$, one of the factors p_i must be contained in P.

(b) Assume that every non-zero prime ideal in R contains a principal prime. As in Theorem 4, denote by S the set of all products of principal primes. It suffices for us to show that S contains every element in R that is neither 0 nor a unit, for Theorem 3 will then complete the proof. Suppose on the contrary that c is an element of R that is not 0, not a unit, and not in S. Since S is saturated, the principal ideal (c) is disjoint from S. Expand (c) to a prime ideal P disjoint from S (Theorem 1). By hypothesis, P contains a principal prime, a contradiction.

In the next two theorems we exhibit two ways of constructing prime ideals without using a multiplicatively closed set. Theorem 6 is due to Herstein; Theorem 7 and its immediate corollary, Theorem 8, are due to I. S. Cohen [12].

Theorem 6. ***Let R be a ring and A an R-module. Let Z be an ideal in R that is maximal among all annihilators of non-zero elements of A. Then Z is prime.***

Proof. Say Z is the annihilator of $x \in A$ (notation: $Z = \operatorname{ann}(x)$). Given $ab \in Z$ we must prove that a or b lies in I. Assume $a \notin I$. Then $ax \neq 0$. We note that $\operatorname{ann}(ax) \supset I$. By hypothesis it cannot be properly larger. Hence $\operatorname{ann}(ax) = I$. Now b annihilates ax; hence $b \in I$.

Theorem 7. ***Let Z be an ideal in R. Suppose Z is not finitely generated, and is maximal among all ideals in R that are not finitely generated. Then Z is prime.***

Proof. We make an indirect proof, assuming $ab \in I$ with neither a nor b in I. Then the ideal (I, a) is properly larger than Z and consequently is finitely generated. As generators for it we may pick elements of the form $i_1 + x_1 a, \ldots, i_n + x_n a$ $(i_1, \ldots, i_n \in I)$. Now let J be the set of all y in R with $ya \in I$. Then J contains both I and b, hence is properly larger than I, hence is finitely generated. We claim that

$$Z = (i_1, \ldots, i_n, Ja).$$

Take an arbitrary element z in I. Then all the more so z lies in (I, a), so we have an expression

$$z = u_1(i_1 + x_1 a) + \cdots + u_n(i_n + x_n a)$$

Here we see that $u_1 x_1 + \cdots + u_n x_n$ lies in J. Hence $z \in (i_1, \ldots, i_n, Ja)$, as required. We have verified $Z = (i_1, \ldots, i_n, Ja)$, which implies that Z is finitely generated, a contradiction.

Now any ideal that is not finitely generated can be enlarged to one that is maximal with this property (this is a good illustration for children cutting their teeth on Zorn's lemma). We are ready for the next theorem, but first we introduce the most basic definition of all.

Definition. A commutative ring R is Noetherian if every ideal in R is finitely generated, or equivalently, if the ideals in R satisfy the ascending chain condition.

Remark. The designation honors Emmy Noether, whose revolutionary paper [38] inaugurated the use of chain conditions in algebra.

Theorem 8. ***If every prime ideal in a ring R is finitely generated, then R is Noetherian.***

We conclude this section with some remarks on the set $\mathcal{S}$ of prime ideals in a ring R. It seems reasonable to think of the partial ordering on $\mathcal{S}$ as its first, basic structure. Question: can an arbitrary partially

ordered set be the partially ordered set of prime ideals in a ring? There is a first negative answer, which is fairly immediate: ***in $\mathcal{S}$ every chain has a least upper bound and a greatest lower bound.*** This follows from Theorem 9.

Theorem 9. ***Let $\{P_i\}$ be a chain of prime ideals in a ring R. Then both $\cup P_i$ and $\cap P_i$ are prime ideals in R.***

Proof. Our task becomes even easier when we pass to the complements S_i, it being quite evident that $\cap S_i$ and $\cup S_i$ are multiplicatively closed.

The fact that Theorem 9 works for intersections gives us an unusual opportunity to use Zorn's lemma going down.

Theorem 10. ***Let I be any ideal in a ring R, P a prime ideal containing I. Then P contains a prime ideal minimal among all prime ideals containing I.***

Proof. Embed P in a maximal chain $\{P_i\}$ of prime ideals containing I (Zorn). By Theorem 9, $\cap P_i$ is prime and it is clearly minimal.

We return to the partially ordered set $\mathcal{S}$ of prime ideals. It does have another (perhaps slightly unexpected) property: between any two elements we can find a pair of "immediate neighbors."

Theorem 11. ***Let $P \subset Q$ be distinct prime ideals in a ring R. Then there exist distinct prime ideals P_1, Q_1 with***

$$P \subset P_1 \subset Q_1 \subset Q \tag{2}$$

such that there is no prime ideal properly between P_1 and Q_1.

Proof. Insert (Zorn) a maximal chain $\{P_i\}$ of prime ideals between P and Q. Take any element x that is in Q but not in P. Define Q_1 to be the intersection of all P_i's containing x, P_1 the union of all P_i's not containing x. By Theorem 9, P_1 and Q_1 are prime. Obviously (2) holds. None of the P_i's can be properly between P_1 and Q_1, for if $x \in P_i$ then $P_i \supset Q_1$ and if $x \notin P_i$ then $P_i \subset P_1$. By the maximality of $\{P_i\}$, no prime ideal at all can lie properly between P_1 and Q_1.

I do not know of any further conditions that $\mathcal{S}$ has to satisfy. In other words, it is conceivable that if a partially ordered set satisfies the conclusions of Theorems 9 and 11 then it is isomorphic to the partially ordered set of prime ideals in some commutative ring.

Let us peek ahead, for a moment, at facts we shall learn later in the Noetherian case. We shall find four further restrictions on $\mathcal{S}$, the first of which is of course immediate.

(a) The ascending chain condition.
(b) The descending chain condition in the strong sense that there is a uniform bound on the lengths of chains descending from a fixed prime ideal.
(c) The number of prime ideals between two given ones is zero or infinite.
(d) There are a finite number of minimal prime ideals.

Again we can speculate on whether we have found all conditions on $\mathcal{S}$ for R Noetherian.

EXERCISES

1. Let R be a ring. Suppose that every ideal in R (other than R) is prime. Prove that R is a field.

2. Let us say that a saturated multiplicatively closed set S is ***generated*** by $\{x,\}$ if S is the smallest such set containing the x's. Prove that if S is finitely generated in this sense, then it can be generated by a single element.

3. Let P be a finitely generated prime ideal with annihilator 0. Prove that the annihilator of the module P/P^2 is P. ***(Hint:*** if $p_1, \ldots, p_r$ generate P and x annihilates P/P^2, then $xp_i = \Sigma a_{ij}p_j$, $a_{ij} \in P$. Take determinant.)

4. (The purpose of this exercise is to show that in Ex. 3 we cannot drop the requirement that P is prime.) Let K be a field. Let R be the ring of polynomials in x over K, subject to the condition that they contain no terms in x or x^2. Let I be the ideal in R generated by x^3 and x^4. Prove: $x^5 \notin I$, and $x^5 I \subset I^2$.

5. Let $P = (p)$ be a principal prime ideal and $J = \cap P^n$.
(a) If Q is a prime ideal properly contained in P, prove that $Q \subset J$. ***(Hint:*** for $q \in Q$, write $q = pq_1$. Here $pq_1 \in Q$, $p \notin Q$, so $q_1 \in Q$. Continue.)
(b) Assume further that p is a non-zero-divisor. Prove: $J = pJ$. ***(Hint:*** for $j \in J$, write $j = px$. From $j \in P^n$ for all n deduce $x \in J$.***)***

(c) Again assuming that p is a non-zero-divisor, prove that J is prime. ***(Hint:*** suppose $ab \in J$ with neither a nor b in J. Write $a = p^m a_1$, $b = p^n b_1$ with $a_1, b_1 \notin P$. Use $ab \in P^{m+n+1}$ to get a contradiction.)

(d) Assume that R is a domain and that J is finitely generated. Prove that $J = 0$ and that there is no prime ideal properly between P and 0. ***(Hint:*** from $J = pJ$, deduce $J = 0$ by a determinant argument as in Ex. 3. Get the final statement from part (a).)

(e) Assume merely that J is finitely generated. Prove that there cannot exist a distinct chain $P \supset Q_1 \supset Q_2$ of prime ideals. ***(Hint:*** pass to R/Q_2 and quote part (d).)

6. Let P be a prime ideal in R, Z the ideal generated by all the idempotents in P. Prove that R/I has no non-trivial idempotents. ***(Hint:*** if e is an idempotent in R/I, pick $u \to e$. Then $u(1 - u) \in I \subset P$. We can assume $u \in P$. There exists an idempotent f in Z such that $f(u^2 - u) = u^2 - u$. Then $(1 - f)u$ is an idempotent in P, hence in Z, hence $u \in I$, $e = 0$. This result is due to **D.** Lazard.)

7. Let (p) and (q) be non-zero principal prime ideals in a ring. Suppose that $(p) \subset (q)$ and that p is a non-zero-divisor. Prove: $(p) = (q)$.

8. (This exercise is offered as a modernization of Euclid's theorem on the infinitude of primes.) Prove that an infinite integral domain with with a finite number of units has an infinite number of maximal ideals.

9. (This exercise is a naive version of Gauss's lemma.) Let f and g be polynomials in an indeterminate over a ring R. Suppose that the ideal generated by the coefficients off is R, and that the same is true for g. Prove that the coefficients of fg also generate R. ***(Hint:*** if the coefficients of fg lie in a maximal ideal M, consider the highest coefficients of f and g that do not lie in M.)

10. **(M.** Isaacs) In a ring R let Z be maximal among non-principal ideals. Prove that Z is prime. ***(Hint:*** adapt the proof of Theorem 7. We have $(I, a) = (c)$. This time take J = all x with $xc \in I$. Since $J \supset (I, b)$, J is principal. Argue that $Z = Jc$ and so is principal.)

11. In a ring R let Z be maximal among ideals that are not countably generated. Prove that Z is prime.

1-2 INTEGRAL ELEMENTS, I

This brief section is devoted to developing the theory of integral elements up to the point needed in §1-3.

We introduce the concept of an ***R-algebra*** over a commutative ring R: a ring T that is an R-module and satisfies the standard axioms, notably

$$a(xy) = (ax)y = x(ay)$$

for $a \in$ R and $x, y \in T$. We are allowing T to be non-commutative. Perhaps the most important example is a ring T containing R in its center.

Definition. Let R be a commutative ring and T an R-algebra. An element $u \in T$ is said to be ***integral*** over R if it satisfies an equation of the form

$$u^n + a_1 u^{n-1} + \ldots + a_n = 0 \qquad (a_i \in \mathrm{R}) \tag{3}$$

i.e., a polynomial equation with coefficients in R and highest coefficient 1. We say that T is integral if all its elements are integral.

The next theorem provides a criterion that is often easier to use.

Theorem 12. ***Let*** R ***be a commutative ring, T an R-algebra, $u \in T$. The following statements are equivalent: (a) u is integral over R, (b) there exists a finitely generated R-submodule A of T such that $uA \subset A$ and the left annihilator of A in T is 0.***

Proof: (a) implies (b). If u satisfies an equation (3) of degree n, take A to be the R-submodule spanned by $1, u, \ldots, u^{n-1}$.

(b) implies (a). Say A is spanned over R by $a_1, \ldots, a_n$. We have equations,

$$ua_i = \sum \lambda_{ij} a_j \qquad (\lambda_{ij} \in \mathrm{R},\ i, j = 1, \ldots, n) \tag{4}$$

Bring all the terms in (4) to the left-hand side. The theory of linear equations applies, and if A is the determinant

$$\begin{vmatrix} u - A_{11} & -\lambda_{12} & \cdots & -\lambda_{1n} \\ -\lambda_{21} & u - A_{22} & \cdots & -\lambda_{2n} \\ & \cdots & & \\ -\lambda_{n1} & -\lambda_{n2} & \cdots & u - A_n \end{vmatrix}$$

we find that A left-annihilates $a_1, \ldots, a_n$. By hypothesis, $A = 0$. Expanding A gives us an equation that shows that u is integral.

Remark. In practice the condition that the left annihilator of A is 0 is usually assured by having $1 \in A$. Note that, as the proof of Theorem 12 showed, we can always pick A to contain 1.

We put Theorem 12 to work at once.

Theorem 13. *Let T be an algebra over the commutative ring* R, *and suppose that $u, v \in T$ are commuting integral elements. Then $u+v$ and uv are integral.*

Proof. We can work within the subalgebra generated by u and v, so T might as well be commutative. Take, by Theorem 12, modules A and B working for u and v. It makes life a little easier to arrange (as we can) $1 \in A, B$. Then the product AB is finitely generated, contains 1, and satisfies both $(u+v)AB \subset AB$ and $(uv)AB \subset AB$. We apply Theorem 12 again.

The next theorem is an immediate corollary.

Theorem 14. *Let T be a commutative algebra over the commutative ring R. Then the elements of T integral over R form a subring of T.*

The following theorem will be used in proving Theorem 16, which in turn will be used in §1-3. Theorem 15 will also be applied in §1-6.

Theorem 15. *Let R be a commutative ring, u an invertible element of a ring containing R. Then u^{-1} is integral over R if and only if $u^{-1} \in R[u]$.*

Proof. If u^{-1} is integral over R, we have

$$u^{-n} + a_1 u^{-(n-1)} + \cdots + a_n = 0 \qquad (a_i \in R) \tag{5}$$

Multiply (5) through by u^n and rearrange to get

$$u(a_1 + a_2 u + \cdots + a_n u^{n-1}) = -1$$

showing that $u^{-1} \in R[u]$. The argument is reversible.

Theorem 16. *Let* R *be an integral domain contained in a field L. If L is integral over R then R is a field.*

Proof. For $u \neq 0$ in R we have that u^{-1} is integral over R. By Theorem 15, $u^{-1} \in R[u] = R$. Hence R is a field.

We conclude this section with a remark on finitely generated rings vs. finitely generated modules. Let T be a commutative R-algebra. We say that T is a finitely generated ring over R if there exists a finite set of elements generating T as a ring over R. This does not at all imply that T is a finitely generated R-module. For instance, if $T = R[x]$ with x an indeterminate, then, as a ring over R, T is generated by one element, but T is not a finitely generated R-module. Note that by Theorem 12, if T is a finitely generated R-module, then T is integral over R. The exact connection is given in Theorem 17.

Theorem 17. *Let T be a commutative algebra over the commutative ring R. The following statements are equivalent: (1) T is a finitely generated R-module, (2) T is a finitely generated ring over* R *and is integral over* R.

Proof. We have already noted that (1) implies (2). Conversely, assume that T is generated as a ring over R by $u_1, \ldots, u_k$, and suppose that the equation showing u_i to be integral has degree n_i. Then the elements

$$u_1^{r_1} u_2^{r_2} \cdots u_k^{r_k}$$

where r_i ranges from 0 to $n_i - 1$, span T over R.

EXERCISES

1. In the setup of Theorem 12, assume $uA \subset JA$ where J is an arbitrary ideal of R. Prove that u satisfies an equation (3) with $a_r \in J^r$ for all r.

2. Let $R \subset T$ be commutative rings with T integral over R. Let J be an arbitrary ideal of R, and assume $u \in JT$. Prove that u satisfies an equation (3) with $a_r \in J^r$. *(Hint:* say $u = j_1 t_1 + \cdots + j_n t_n$. Let A be the

subring of T generated over R by the t's. Observe that A is finitely generated as an R-module and that $uA \subset JA$. Use Ex. 1.)

3. Let R be an integral domain, P a finitely generated non-zero prime ideal in R, and Z an ideal in R properly containing P. Let x be an element in the quotient field of R satisfying $xI \subset R$. Prove that x is integral over R. *(Hint:* observe that $IxP \subset P$ and deduce $xP \subset P$.*)*

4. (This exercise generalizes half of Theorem 15.) Let R be a ring, and u an invertible element of a ring containing R. Prove that $R[u] \cap R[u^{-1}]$ is integral over R. *(Hint:* if v is a polynomial in u of degree m, and a polynomial in u^{-1} of degree n, prove that $vA \subset A$ where A is the module spanned by $1, u, \ldots, u^{m+n-1}$.*)*

1-3 G-IDEALS, HILBERT RINGS, AND THE NULLSTELLENSATZ

Our main objective in this section is the *Nullstellensatz*, Theorems 32 and 33. Thus we seek information on the maximal ideals of $K[x_1, \ldots, x_n]$, where K is a field. Now the modern style is to study the problem one variable at a time, that is, we look at the maximal ideals of $R[x]$ with R a more or less arbitrary commutative ring. The first thing to do with a maximal ideal M in $R[x]$ is to contract it back to the ideal $M \cap R$ in R. When we do this we certainly get a prime ideal, but we wish it were a maximal ideal (for instance, so that an inductive procedure will work smoothly). A close examination of the facts leads to the sequence of ideas: G-domain, G-ideal, and Hilbert ring.

Theorem 18. *Let R be an integral domain with quotient field K. The following two statements are equivalent: (1) K is a finitely generated ring over R, (2) as a ring, K can be generated over R by one element.*

Proof. Of course (2) implies (1). To prove that (1) implies (2), we suppose $K = R[a_1/b_1, \ldots, a_n/b_n]$. Then with $c = b_1 \cdots b$, we have $K = R[1/c]$.

Definition. An integral domain satisfying either (hence both) of the statements in Theorem 18 is called a G-domain.

The name honors Oscar Goldman. His paper [20] appeared at virtually the same time as a similar paper by Krull [27]. Since Krull already has a class of rings named after him, it seems advisable not to attempt to honor Krull in this connection. G-domains were also considered by Artin and Tate in [1]. Further results concerning the material in this section appear in Gilmer's paper [18].

Some remarks will precede the development of the theory of G-domains. Of course any field is a G-domain. To get more examples, we examine principal ideal domains. We see immediately that a principal ideal domain is a G-domain if and only if it has only a finite number of primes (up to units).

Later we shall determine exactly which Noetherian domains are G-domains, the precise condition being that there are only a finite number of non-zero prime ideals, all of which are maximal. For non-Noetherian domains the facts are more complex, and we seem to lack even a reasonable conjecture concerning the structure of general G-domains. At any rate, examples show that the Noetherian facts do not at all generalize. It is easy to exhibit a valuation domain that is a G-domain but nevertheless possesses comparable non-zero prime ideals. Also (this is more difficult)' there exist G-domains in which all non-zero prime ideals are maximal and there are an infinite number of them.

The next two theorems are simple but useful. Note that any G-domain has an element u of the type occurring in Theorem 19; note also that as a corollary of Theorem 19, in a G-domain the intersection of all non-zero prime ideals is non-zero.

Theorem 19. *Let R be an integral domain with quotient field K. For a non-zero element u in R the following three statements are equivalent:*

(1) Any non-zero prime ideal contains u;

(2) Any non-zero ideal contains a power of u;

(3) $K = R[u^{-1}]$.

Proof. (1) implies *(2)*. Let Z be a non-zero ideal. If Z contains no power of u, then (Theorem 1) I can be expanded to a prime ideal P disjoint from $\{u^n\}$, a contradiction.

(2) implies (3). Take any $b \neq 0$ in R. From *(2)* we have that *(b)* contains some u^n, say $u^n = bc$. Then $b^{-1} = cu^{-n} \in R[u^{-1}]$. This being true for any non-zero b, we have $R[u^{-1}] = K$.

(3) implies (1). Take a non-zero prime ideal P and any non-zero element b in it. Since $R[u^{-1}] = K$ we have $b^{-1} = cu^{-n}$ for suitable $c \in R$ and n. Then $u^n = bc \in P$, whence $u \in P$.

Theorem 20. *Let R be a G-domain with quotient field K and let T be a ring lying between R and K. Then T is a G-domain.*

Proof. If $K = R[u^{-1}]$, then $K = T[u^{-1}]$ all the more so.

To use the notion of a G-domain effectively, we need to know how it behaves under ring extensions. The next two theorems, together with Ex. 1, give fairly complete information.

Theorem 21. *If R is an integral domain and x is an indeterminate over R, then $R[x]$ is never a G-domain.*

Proof. Let K be the quotient field of R. If $R[x]$ is a G-domain, so is $K[x]$. But $K[x]$ is a principal ideal domain. So we will achieve our goal if we show that $K[x]$ has an infinite number of primes. Now if K is infinite, this is clear; just take all $x - a$ as a runs over K. If K is finite, we can cite from field theory the existence of extensions of K of arbitrarily large degree, yielding irreducible polynomials of arbitrarily large degree. But this is unduly sophisticated, for there is a pleasant opportunity here for Euclid's trick to enjoy a repeat performance. Suppose that $p_1, \ldots, p_k$ are all the irreducible monic polynomials and form $1 + p_1 \cdots p_k = q$. Then q is divisible by none of the p_i's, a contradiction.

Theorem 22. *Let $R \subset T$ be integral domains and suppose that T is algebraic over R and finitely generated as a ring over R. Then R is a G-domain if and only if T is a G-domain.*

Remark. In saying that T is algebraic over R we mean that every element of T satisfies a polynomial equation with coefficients in R, no attempt being made to have the highest coefficient 1; this is equivalent to saying that the quotient field of T is algebraic over the quotient field of R.

Proof. Let K, L be the quotient fields of R, T. Suppose first that R is a G-domain; say $K = R[u^{-1}]$. Then $T[u^{-1}]$ is a domain algebraic over the field K, hence is itself a field, necessarily equal to L. Thus T is a G-domain.

(Note that this half of the proof did not require T to be a finitely generated ring. But the second half does; for instance, T might even be the quotient field of R, which is algebraic over R by default, and is a G-domain no matter what R is.)

We assume that T is a G-domain, $L = T[v^{-1}]$ and $T = R[w_1, \ldots, w_k]$. The elements $v^{-1}, w_1, \ldots, w_k$ are algebraic over K and consequently satisfy equations with coefficients in R which lead off, say

$$av^{-m} + \cdots = 0$$
$$b_i w_i^{n_i} + \cdots = 0 \qquad (i = 1, \ldots, k)$$

Adjoin $a^{-1}, b_1^{-1}, \ldots, b_k^{-1}$ to R, obtaining a ring R_1 between R and K. The field L is generated over R by $w_1, \ldots, w_k, v^{-1}$. A fortiori these elements generate L over R_1. Now, over R_1 we have arranged that $w_1, \ldots, w_k, v^{-1}$ are integral. Hence (Theorem 13 or Theorem 14), L is integral over R_1. By Theorem 16, R_1 is a field, necessarily K. So K is a finitely generated ring over R and R is a G-domain, as required.

For convenience we add a theorem, which is immediate from Theorems 21 and 22.

Theorem 23. *Let R be a domain, u an element of a larger domain. If $R[u]$ is a G-domain, then u is algebraic over R and R is a G-domain.*

So far there has been no sign that G-domains have anything to do with maximal ideals in polynomial rings. The next theorem exhibits the connection.

Theorem 24. *An integral domain R is a G-domain if and only if there exists in the polynomial ring $R[x]$ an ideal M which is maximal and satisfies $M \cap R = 0$.*

Proof. Suppose that R is a G-domain, say $K = R[u^{-1}]$ where K is the quotient field of R. We can map $R[x]$ homomorphically into K by sending x into u^{-1}. The image is all of K, so the kernel M is maximal.

Since the homomorphism is one-to-one on R, we have $M \cap R = 0$. (*Remark:* M can be identified as the principal ideal $(ux - 1)$, a fact we leave as Ex. 2.)

Conversely, let M be maximal in $R[x]$ and satisfy $M \cap R = 0$. Denote the image of x in the natural homomorphism $R[x] \to R[x]/M$ by y. Then $R[y]$ is a field. By Theorem 23, R is a G-domain.

Remark. An attentive reader might note that in this application of Theorem 23 (really Theorem 22) only one element was involved; hence Theorem 13 was not needed. However, a second application of Theorem 23 lies ahead in the proof of Theorem 31. On tracing the sequence of arguments, we find that Theorem 13 for two elements (which means essentially the full force of Theorem 13) is needed for Theorem 31.

In order to discuss maximal ideals of $R[x]$ that do not contract to 0 in R, the following definition is pertinent.

Definition. A prime ideal P in a commutative ring R is a *G-ideal* if R/P is a G-domain.

We insert at this point a celebrated theorem of Krull. Recall that in a commutative ring the set of all nilpotent elements forms an ideal called the *nilradical* of R. Krull's theorem asserts that the nilradical is equal to the intersection of all prime ideals. This is immediately deducible from Theorem 1, but we delayed it to this point in order to sharpen it a little.

Theorem 25. *The nilradical N of any commutative ring R is the intersection of all G-ideals in R.*

Proof. Clearly a nilpotent element lies in every prime ideal. Conversely, suppose $u \neq N$. We must construct a G-ideal excluding u. The ideal 0 is disjoint from $\{u^n\}$; we can expand it to an ideal P maximal with respect to disjointness from $\{u^n\}$. We know that P is prime (Theorem 1). We show further that P is a G-ideal. In the domain $R^* = R/P$, let u^* denote the image of u. The maximality of P tells us that every non-zero prime ideal in R^* contains u^*. By Theorem 19, R^* is a G-domain, and P is a G-ideal.

Remark. This is a good point at which to make the belated observation that the most frequently encountered multiplicatively closed set is one consisting of the powers of an element u (with u preferably non-nilpotent to avoid degeneracy). From the present point of view these multiplicatively closed sets get a place of honor because they are inextricably linked with G-ideals. Note also Ex. 2 in §1.

We wish to apply Theorem 25 to the homomorphic images of R as well as to R itself. For this purpose we define the *radical* J of an ideal I to be the set of all elements in R having some power in I. If we pass to the ring R/I, then J/I is the nilradical. We call I a radical ideal if it is equal to its radical.

Theorem 26. *Let I be any ideal in a commutative ring R. Then the radical of I is the intersection of all G-ideals containing I.*

This is immediate from Theorem 25 and the definitions.

Let I be any ideal in a ring R. We write R^* for the quotient ring R/I. In the polynomial ring $R[x]$ there is a smallest extension $IR[x]$ of I. The quotient ring $R[x]/IR[x]$ is in a natural way isomorphic to $R^*[x]$. In treating many problems, we can in this way reduce to the case $I = 0$, and we shall often do so. As a first sample we generalize Theorem 24 (no further proof is needed).

Theorem 27. *An ideal I in a ring R is a G-ideal if and only if it is the contraction of a maximal ideal in the polynomial ring $R[x]$.*

Next we discuss how to generate a maximal ideal of a polynomial ring in the favorable case when the contraction is maximal.

Theorem 28. *Let M be a maximal ideal in $R[x]$ and suppose that the contraction $M \cap R = N$ is maximal in R. Then M can be generated by N and one more element f. We can select f to be a monic polynomial which maps mod N into an irreducible polynomial over the field R/N.*

Proof. We can reduce to the case $N = 0$, i.e., R a field, and then the statement is immediate. ∎

When the field R/N is algebraically closed we get a still simpler result.

Theorem 29. *Suppose, in addition to the hypothesis of Theorem 28, that R/N is algebraically closed. Then $M = (N, x - a)$ for some $a \in R$.*

Proof. In this case an irreducible polynomial over R/N must be linear.

Any maximal ideal is a G-ideal. The nice class of rings is where the reverse holds.

Definition. A commutative ring R is a *Hilbert ring* if every G-ideal in R is maximal. (Krull's designation was *Jacobson ring*, and Bourbaki has followed this terminology.)

We note the trivial fact that any homomorphic image of a Hilbert ring is a Hilbert ring.

The best examples of Hilbert rings are those that arise from Theorem 31 below. We note (Ex. 4) that, except for the trivial case where all prime ideals are maximal, a Hilbert ring must have an infinite number of maximal ideals. Later, after we acquire the principal ideal theorem, we shall be able to describe exactly which Noetherian rings are Hilbert rings.

From the definition and Theorem 26 we derive:

Theorem 30. *In a Hilbert ring the radical of any ideal I is the intersection of the maximal ideals containing I.*

Theorem 31. *A commutative ring R is a Hilbert ring if and only if the polynomial ring $R[x]$ is a Hilbert ring.*

Proof. If $R[x]$ is a Hilbert ring, so is its homomorphic image R.

Conversely, assume that R is a Hilbert ring. Take a G-ideal Q in $R[x]$; we must prove that Q is maximal. Let $P = Q \cap R$; we can reduce the problem to the case $P = 0$, which, incidentally, makes R a domain. Let u be the image of x in the natural homomorphism $R[x] \to R[x]/Q$. Then $R[u]$ is a G-domain. By Theorem 23, u is algebraic over R and R is a G-domain. Since R is both a G-domain and a Hilbert ring, R is a field. But this makes $R[u] = R[x]/Q$ a field, proving Q to be maximal.

Theorem 32. *(Nullstellensatz, first version.) Let K be an algebraically closed field and let $x_1, \ldots, x_n$ be indeterminates over K. Then any maximal ideal in $K[x_1, \ldots, x_n]$ is of the form $(x_1 - a_1, \ldots, x_n - a_n)$, $a_i \in K$, i.e., it consists of all polynomials vanishing at a point.*

Proof. Let $R = K[x_1, \ldots, x_{n-1}]$. R is a Hilbert ring by iterated use of Theorem 31. We are given a maximal ideal M in $R[x_n]$. Let N be its contraction to R. By Theorem 27, N is a G-ideal in R, hence maximal. We make an induction on n, assuming $N = (x_1 - a_1, \ldots, x_{n-1} - a_{n-1})$. This shows that R/N is in a natural way isomorphic to K and thus is algebraically closed. By Theorem 29, $M = (N, x_n - a_n)$, as required.

Theorem 33. *(Full Nullstellensatz.) Let K be an algebraically closed field and $f, g_1, \ldots, g_r$ polynomials in n variables with coefficients in K. Assume that f vanishes at all common zeros of $g_1, \ldots, g_r$. Then some power of f lies in the ideal $(g_1, \ldots, g_r)$.*

Proof. In the light of Theorem 32, our hypothesis says that f lies in the intersection of all maximal ideals containing $(g_1, \ldots, g_r)$. Since (Theorem 31) $K[x_1, \ldots, x_n]$ is a Hilbert ring; Theorem 30 is applicable and shows that f is in the radical of $(g_1, \ldots, g_n)$.

EXERCISES

1. Let $R \subset T$ be domains with T finitely generated as a ring over R, and not algebraic over R. Prove that T is not a G-domain. *(Hint:* pass from R to T by a sequence of transcendental elements, followed by an algebraic extension. Use Theorems 21 and 22.)

2. (This exercise arose in connection with the proof of Theorem 24.) Let R be a domain with quotient field K, and u a non-zero element of R. Let J be the kernel of the homomorphism from $R[x]$ into K given by $x \to u^{-1}$. Prove: $J = (ux - 1)$. *(Hint:* say $f = ax^n + \cdots + b \in J$. Write $f + b(ux - 1) = xg$. Then $xg \in J$, $x \notin J$, $g \in J$ since J is prime. Use induction.)

3. Let R be an integral domain having only a finite number of prime ideals. Prove that R is a G-domain. *(Hint:* argue that the intersection of the non-zero prime ideals is non-zero, and use Theorem 19.)

4. Let R be a Hilbert ring having only a finite number of maximal ideals. Prove that these are the only prime ideals in R. *(Hint:* by Theorem **30** every prime ideal is an intersection of maximal ideals.)

5. Let R be an integral domain with quotient field K. Assume that K is countably generated as a ring over R. Prove that R is a G-domain if and only if K cannot be expressed as the union of a properly ascending sequence of subrings containing R.

6. Let K be any field (not necessarily algebraically closed). Prove that any maximal ideal in $K[x_1, \ldots, x_n]$ can be generated by n elements. *(Hint:* use Theorems 28 and **31**.)

7. (Generalization of Ex. **6.)** Let R be a Hilbert ring such that every maximal ideal in R can be generated by k elements, k fixed. Prove that any maximal ideal in $R[x_1, \ldots, x_n]$ can be generated by $k + n$ elements.

8. Let R be a Hilbert ring in which every maximal ideal is finitely generated. Prove that the same is true for $R[x]$.

9. Prove that the following statements are equivalent:

(a) R is a Hilbert ring;

(b) Every radical ideal in R is an intersection of maximal ideals;

(c) Every prime ideal in R is an intersection of maximal ideals;

(d) Every G-ideal in R is an intersection of maximal ideals.

10. Let M be a maximal ideal in $T = R[x_1, \ldots, x_n]$ satisfying $M \cap R = 0$. Prove that M can be generated by $n + 1$ elements. *(Hint:* let K be the quotient field of R. R is a G-domain, $K = R[u^{-1}]$. There exists $g \in T$ with $ug \equiv 1 \pmod{M}$. Pass to the ring $T/(ug - 1)$, which contains a copy of K, and argue thus that n more generators will suffice for M.)

11. Let K be algebraically closed and $R = K[x_1, \ldots, x_n]$. Let $f_1, \ldots, f_m \in R$. Then the equations $f_1 = 0, \ldots, f_m = 0$ have a simultaneous solution if and only if there do not exist $g_1, \ldots, g_m \in R$ with $\Sigma g_i f_i = 1$.

12. (This exercise sketches the transition to the language of algebraic geometry,) Let K be a field and write A_n for the vector space of n-ples over K. Given an ideal $I \subset K[x_1, \ldots, x_n]$ we write $V(I)$ for the subset of A_n consisting of all points in A_n where all the polynomials in I vanish, and we call such a set a *variety*. Given a subset S of A_n, we write $J(S)$ for the ideal of polynomials vanishing on S. Assume K algebraically closed.

(a) Prove that $J(V(I))$ is the radical of I.

(b) Prove that the map $S \to J(S)$ sets up a one-to-one correspondence between all varieties and all radical ideals.

(c) Prove that under set-theoretic inclusion the set of radical ideals is a complete lattice and that the set of varieties likewise is a complete lattice. Prove further that the correspondence of part (b) is order-inverting. (*Remark:* in each case the intersection is merely the set-theoretic intersection, but the union is the smallest object containing the radical ideals or varieties in question. Note, however, the extra information in part (d).)

(d) In the lattice of varieties of part (c), prove that the union of a *finite* number of varieties is just the set-theoretic union.

(e) Prove that in the correspondence of part (b) an ideal is prime if and only if the corresponding variety is *irreducible,* in the sense that it cannot be exhibited as the union of two properly smaller varieties.

13. (The homogeneous *Nullstellensatz.*) K is a field, $R = K[x_1, \ldots, x_n]$. Call an ideal I in R *homogeneous* if along with a polynomial f, I contains the homogeneous constituents of f. Call a variety V a *cone* if $(a_1, \ldots, a_n) \in V$ implies $(ta_1, \ldots, ta_n) \in V$ for all $t \in K$.

(a) If I is homogeneous, prove that $V(I)$ is a cone.

(b) If V is a cone, and K is infinite, prove that $J(V)$ is homogeneous. Give an example to show that we need to assume K infinite.

(c) Thus, or otherwise, prove that when K is algebraically closed, the radical of a homogeneous ideal is homogeneous. (This is actually true for any field.)

(For a reader familiar with projective geometry, we sketch the facts in that language. From a homogeneous ideal I we pass to a projective variety V in $(n-1)$-dimensional projective space, Assume K algebraically closed. V is the null set if and only if I contains a power of the ideal $(x_1, \ldots, x_n)$. If we rule out this case the passage

$$I \to V(I) \to J(V(I))$$

leads to the radical of I. Prime homogeneous ideals correspond to irreducible varieties. In particular, points correspond to "submaximal" homogeneous prime ideals, i. e., homogeneous prime ideals directly below $(x_1, \ldots, x_n)$.)

14. Prove: an element x in a ring R is nilpotent if and only if it is a zero-divisor on every R-module. *(Hint:* use Theorem *25.)*

15. Let K be a field, L a field containing K, which is finitely generated as a ring over K. Prove that L is finite-dimensional over K.

16. Let $R \subset T$ be rings with R a Hilbert ring and T finitely generated as a ring over R. Prove that any maximal ideal in T contracts to a maximal ideal in R.

17. Let $R_1 \subset R_2 \subset R_3$ be rings with R_3 finitely generated as a ring over R_1. Let P_3 be an ideal in R_3 and P_1, P_2 its contractions to R_1, R_2. Prove: if P_1 and P_3 are maximal, so is P_2. *(Hint:* by switching to R_1/P_1 reduce to the case where R_1 is a field.)

1-4 LOCALIZATION

The technique of localization is by now such a standard part of commutative ring theory that we shall be brief about it. In this section we give the basic definitions and properties; further facts will be developed as needed.

Let S be a multiplicatively closed set in R. (It is a good idea to assume that $0 \notin S$; otherwise everything in sight will collapse to 0.) Let A be an R-module. We define A_S to be the set of equivalence classes of pairs (a, s) with $a \in A$, $s \in S$, the equivalence relation being: $(a, s) \sim (a_1, s_1)$ if there exists s_2 in S with $s_2(s_1 a - s a_1) = 0$. This is indeed an equivalence relation.

We make A_S into an abelian group by

$$(a, s) + (a_1, s_1) = (s_1 a + s a_1, s s_1)$$

and then into an R-module by

$$x(a, s) = (xa, s)$$

In both cases we have to check that the definitions are independent of the choice of representatives, and then mechanically verify a flock of axioms.

Our notation for the equivalence class of (a, s) will be a/s. We identify a with $a/1$ when there is no danger (but sometimes there is).

Remark. It is harmless to assume that S is saturated, and it is at any rate convenient to assume that $1 \in S$.

When the construction is carried out on R itself the resulting object R_S carries a ring structure:

$$(x, s)(x_1, s_1) = (xx_1, ss_1),$$

and then A_S becomes an R_S-module:

$$(x, s)(a, s_1) = (xa, ss_1).$$

If the operation is iterated, nothing new happens: $(A_S)_S$ is identifiable with A_S. This has as a result the following useful observation: any R_S-module has the form A_S for a suitable R-module A (for instance take A to be A_S itself). For use in a Noetherian setup we shall need the

further easy observation: if B is finitely generated over R_S, then we can arrange to have $B = A_S$ with A finitely generated over R.

There is a natural R-module homomorphism from A into A_S and a natural ring homomorphism from R into R_S. In each case the kernel is the set of elements annihilated by some member of S.

Especially important is the case where S is the complement of a prime ideal P. We then, by "abuse of notation," write A_P, R_P instead of A_S, R_S. (It is true that P itself is also a multiplicatively closed set, but it would be ludicrous to take this seriously, for $0 \in P$.)

We proceed to discuss the connection between ideals in R and R_S. Given an ideal I in R it maps to the ideal I_S in R_S. We note again that I_S consists of all i/s with $i \in I$, $s \in S$. The ideal I "explodes" to R_S (i. e., $I_S = R_S$) if and only if I contains an element of S, and it collapses to 0 if every element of I is annihilated by some element of S.

Given an ideal J in R_S there is a well-defined complete inverse image I in R; it consists of all x with $x/1 \in J$. However, a handier way to think of it is to write a typical $j \in J$ as $j = y/s$ with $y \in$ R. The representation is not unique, so be generous and take all possible representations. Then collect all numerators that arise; this is the same ideal I.

If we go from J to I and then back to I_S, we find $I_S = J$. But if we start with $I \subset$ R, pass to I_S, and then return to an ideal of R, we generally get a larger ideal. (For instance, if I contains an element of S, on returning I will have grown to R.)

The correspondence improves if we stick to prime ideals.

Theorem 34. ***The mappings described above implement a one-to-one order-preserving correspondence between all the prime ideals in R_S and those prime ideals in*** R ***disjoint from S.***

Proof. We leave to the reader the routine steps of the proof except for thefollowing: start with P prime in R and disjoint from S, and see that P_S returns to P. That is, given $x \in$ R, $s \in S$ with $x/s \in P_S$ we must prove that $x \in P$. Now we are given $x/s = p/s_1$ for some $p \in P$, $s_1 \in S$. This says $s_2(s_1 x - sp) = 0$, $s_2 \in S$. Hence $s_2 s_1 x \in P$ and $x \in P$, since P is prime, S is multiplicatively closed, and $P \cap S$ is void.

Note that the maximal ideals in R_S are exactly the maximal primes disjoint from S discussed in §1-1.

The special case of R_P is so important that it deserves to have the theorem stated all over again.

Theorem 35. ***The mappings described above implement a one-to-one order-preserving correspondence between all the prime ideals in R_P and all the prime ideals in R contained in P.***

In particular: R_P has exactly one maximal ideal. The procedure has the effect of making the selected prime ideal P the "big daddy" in R_P. Our notation for the unique maximal ideal of R_P is, sadly enough, P_P. We are going to call such a ring (i. e., one with exactly one maximal ideal) ***quasi-local.***

EXERCISES

1. Let P be prime and S multiplicatively closed in R. Compare the integral domains R/P and R_S/P_S. Is the second a suitable localization of the first? Note especially the relation between the integral domain RIP and the field R_P/P_P.

2. Let S, T be multiplicatively closed in R; write T^* for the image of T in R_S. Compare $(R_S)_{T^*}$ and R_{ST}.

3. Let S be multiplicatively closed in a **UFD.** Prove that R_S is a **UFD.**

4. (a) Let A be an R-module, x an element of A. If x maps to zero in A_M for every maximal ideal M in R, prove that $x = 0$. (***Hint:*** if the annihilator I of x is not R, take $M \supset I$.)

(b) If $A_M = 0$ for every M, prove that $A = 0$.

5. Let B, C be submodules of an R-module A. Assume that $B_M \subset C_M$ for every maximal ideal M in R. Prove: $B \subset C$. (***Hint:*** apply Ex. 4 to the module $(B + C)/C$.)

6. Let R be a ring with no non-zero nilpotent elements, and let P be a minimal prime ideal in R. Prove that R_P is a field.

7. Let T be a localization of R, and assume that T is quasi-local. Prove that T has the form R_P with P a prime ideal in R.

8. Let R be an integral domain with quotient field K, $R \neq K$. Prove that the following two statements are equivalent: (a) R has exactly one non-zero prime ideal, (b) the only localizations of R are R and K.

9. Prove that a ring has an infinite number of distinct localizations if and only if it has an infinite number of prime ideals.

10. Let R be an integral domain. If a localization R_S is integral over R, prove that $R = R_S$.

1-5 PRIME IDEALS IN POLYNOMIAL RINGS

In this short section we derive some preliminary results concerning the nature of the prime ideals in a polynomial ring $R[x]$.

Such a prime ideal contracts to a prime ideal in R. Nearly always, we can reduce the latter to 0. ***So*** we ask: with R a domain, what are the prime ideals in $R[x]$ that contract to 0? Theorem ***36*** provides the answer.

Theorem 36. ***Let R be an integral domain with quotient field K, and let x be an indeterminate. Then there is a one-to-one correspondence between prime ideals in R[x] that contract to 0 in R and prime ideals in K[x].***

Proof. Let S be the set of non-zero elements in R. Then $R_S = K$ and $R[x]_S$ is, in a natural way, $K[x]$. We quote Theorem **34.**

Now the prime ideals in $K[x]$ are instantly surveyed: we have 0, and an infinite number of maximal ideals corresponding to irreducible polynomials over K. For any prime ideal P in a general ring R, we then derive a picture of the prime ideals in $R[x]$ contracting to P: we have the expansion $PR[x]$, and an infinite number of prime ideals sitting directly above $PR[x]$. One corollary of this is important enough to warrant an explicit theorem.

Theorem 37. ***Let R be any ring. There cannot exist in R[x] a chain of three distinct prime ideals with the same contraction in R.***

We introduce at this point one of the basic concepts in the subject: the rank of a prime ideal. Counting as the Romans did, we say that a chain of distinct prime ideals

$$P = P_0 > P_1 \supset \cdots \supset P_n \tag{6}$$

is of length n, even though $n + 1$ prime ideals appear in **(6).** We say that P has ***rank n*** if there exists a chain of length n descending from P, but no longer chain. We say that P has rank ∞ if there exist arbitrarily long chains descending from P. Thus a minimal prime ideal has rank 0;

a prime ideal of rank 1 is not minimal but sits directly above a minimal prime ideal, etc. Note that in a domain the only truly minimal prime ideal is 0. So in a domain it is customary to call a rank 1 prime minimal.

Remark. Other terminology in use in place of "rank" includes "height" or "altitude."

Theorem 38. ***Let P be a prime ideal of rank n in R. In the polynomial ring R[x], write P* = PR[x], and let Q be a prime ideal in R[x] that contracts to*** P ***in R and contains P* properly. Then***

$$(a) \qquad n \leqq rank(P^*) \leqq 2n,$$
$$(b) \qquad n+1 \leqq rank(Q) \leqq 2n+1.$$

Proof. Say the chain *(6)* descends from **P.** Using * for the expansion of an ideal to $R[x]$ we exhibit the chain **of** prime ideals

$$Q \supset P_0^* \supset P_1^* \supset \cdots \supset P_n^*$$

This proves the first inequality in both (a) and (b).

Take a chain descending from P^* and contract it to R. Only P^* can contract to P, and by Theorem *37* the others collapse at most two to one. This completes the proof of (a), and the handling of (b) is similar.

Examples show that the bounds in Theorem *38* can be attained. See Seidenberg **[46], [47].** For Noetherian rings it is possible to sharpen Theorem *38.* We abstract a portion of the argument at this point in order to exhibit the fact that it is quite elementary, and because of the possible usefulness of the generalization.

Call a domain R an S-domain if for every prime ideal P of rank 1, P^* again has rank 1. **(As** above, P^* is the expansion $PR[x]$ of P to the polynomial ring $R[x]$.) Call a ring R a ***strong S-ring*** if for every prime ideal N in R, R/N is an S-domain.

Theorem 39. ***Let n,*** P, ***and Q be as in Theorem 38. Assume that R is a strong S-ring. Then rank(P*) = n and rank(Q) = n*** + 1.

Proof. In view of Theorem *38,* we need only prove the inequalities $\text{rank}(P^*) \leqq n$, $\text{rank}(Q) \leqq n+1$.

Suppose $\text{rank}(P^*) > n$. Then we have $P^* \supset P_0$ with P_0 of rank n.

Let P_1 be the contraction of P_0 to R. Clearly P_1 is properly contained in P, and so $\text{rank}(P_1) < n$. Then (by induction) the only possible way to have P_0 of rank n is to have $\text{rank}(P_1) = n-1$, and P_0 properly larger than $P_1R[x]$. However, it follows from our hypothesis (by the usual passage to the ring R/P_1) that there are no prime ideals properly between P^* and $P_1R[x]$. This contradiction proves $\text{rank}(P^*) = n$.

It is now easy to prove $\text{rank}(Q) = n+1$. Take a prime ideal Q_1 properly contained in Q. If it contracts to P, then (Theorem *37)* $Q_1 = P^*$. If it contracts to a smaller prime, then $\text{rank}(Q_1) \leqq n$, by induction. In either case, $\text{rank}(Q_1) \leqq n$, whence $\text{rank}(Q) \leqq n+1$.

EXERCISES

1. Let Q be a prime ideal in $R[x]$, contracting to P in R. Prove that Q is a G-ideal if and only if P is a G-ideal and Q properly contains $PR[x]$.
2. Let Q be a G-ideal in $R[x_1, \ldots, x_n]$ contracting to P in R. Prove: $\text{rank}(Q) \geqq n + \text{rank}(P)$.
3. In the notation of Theorem *38,* shaw that we have $\text{rank}(Q) = 1 + \text{rank}(P^*)$.

1-6 INTEGRAL ELEMENTS, II

There is a considerable amount of choice in the order of presentation of topics in commutative rings. From one point of view the theory of integral elements in this section is more advanced than a good deal of later material. But we have preferred to delay till the last moment the introduction of chain conditions.

We continue with the theory of integral elements where §1-2 left off, but we abandon the extra generality that was briefly in evidence in §1-2. We work with a pair of commutative rings $R \subset T$. We recall (Theorem *14)* that the elements of T integral over R form a subring of T. It is called the integral ***closure*** of R in T.

We prove next the transitivity of the integral property.



Theorem 40. *Let* R $\subset$ *T be rings and u an element of a ring containing T. Suppose that u is integral over T and that T is integral over* R. *Then u is integral over* R.

Proof. Say

$$u^n + a_1u^{n-1} + \cdots + a_n = 0 \qquad (a_i \in T)$$

exhibits the fact that u is integral over T. Let $R_1 = R[a_1, \cdots, a_n, u]$. We easily argue that R_1 is a finitely generated R-module, and so (Theorem 12) u is integral over R.

We are interested in relations between the prime ideals of R and those of T where R $\subset$ T. We are principally concerned with the case where T is integral over R, but we formulate definitions and some minor results in greater generality.

We list four properties that might hold for a pair R, T.

Lying over (LO). For any prime P in R there exists a prime Q in T with Q $\cap$ R $= P$.

Going up (GU). Given primes $P \subset P_0$ in R and Q in T with $Q \cap$ R $= P$, there exists Q_0 in T satisfying Q $\subset Q_0$, $Q_0 \cap$ R $= P_0$.

Going down (GD). The same with $\subset$ replaced by $\supset$.

Incomparable (INC). Two different primes in T with the same contraction in R cannot be comparable.

Some of the simpler facts concerning these four properties appear in Exs. 2, **3,** and **16.**

Let rings R $\subset$ T be given, and let P be a prime ideal in R. In any attempt to study the relation between P and the prime ideals of T, the following construction is quite natural. Let S denote the set-theoretic complement of P in R. Then S may equally well be regarded as a multiplicatively closed set in T. It is still disjoint from 0, so we may expand 0 to a prime ideal Q in T that is maximal with respect to the exclusion of S. The ideal $Q \cap$ R is a prime ideal contained in P, and Q is maximal among prime ideals in T having this property. Does Q actually contract to P? This question is evidently crucial. It turns out we can characterize GU and INC in this way.

Theorem 41. *The following two statements are equivalent for rings* R $\subset$ *T:*

(a) GU holds.

(b) If P is a prime ideal in R, S *is the complement of P in* R, *and* Q *is an ideal (necessarily prime) in T maximal with respect to the exclusion of* S, *then* $Q \cap$ R $= P$.

Proof. (b) $\Rightarrow$ (a). Let $P_0 \subset P$ be given, and suppose Q_0 in T contracts to P_0. Then Q_0 is disjoint from S. Expand it to Q, maximal with respect to the exclusion of S. By hypothesis, Q $\cap$ R $= P$, proving GU.

(a) $\Rightarrow$ (b). Let Q be maximal with respect to the exclusion of S, the complement of P in R. Granted GU, we have to prove $Q \cap$ R $= P$. In any event, Q lies over the prime ideal $Q \cap$ R, and GU permits **us** to expand Q to a prime ideal Q_1 lying over P. The maximality of Q then tells us Q $= Q_1$.

Since (as we noted above) we can always construct a prime ideal maximal with respect to the exclusion of S, Theorem 41 has the following corollary.

Theorem 42. *For any pair of rings,* ***GU*** *implies LO.*

The proof of the next theorem is immediate, and is left to the reader.

Theorem 43. *The following statements are equivalent for rings* R $\subset$ *T:*

(a) ***INC*** *holds.*

(b) If P is a prime ideal in R, *and Q is a prime ideal in T contracting to P in* R, *then Q is maximal with respect to the exclusion of S, the complement of P in* R.

We now turn to integral extensions.

Theorem 44. ***Let*** R $\subset$ *T be rings with T integral over* R. *Then the pair* R, *T satisfies* ***INC*** *and GU (and thus also, by Theorem* ***42,*** *LO).*

Proof. We first prove GU. We make use of Theorem 41; so, in the notation of that theorem, we must prove Q $\cap$ R $=$ P. Of course Q $\cap$ R $\subset P$. If equality does not hold, take $u \in P$, $u \notin Q \cap$ R. Then of course $u \notin$ Q and the ideal (Q, u) is properly larger than Q. It must therefore intersect S, say in the elements where $s = q + au$ $(q \in Q, a \in T)$.

Let

$$a^n + c_1 a^{n-1} + \cdots + c_n = 0 \qquad (c_i \in R) \tag{7}$$

be an equation showing that a is integral over R. Multiply (7) by u^n;

$$(au)^n + c_1 u(au)^{n-1} + \cdots + c_n u^n = 0$$

Now $au = s - q$, i.e., $au \equiv s \pmod{Q}$. Hence

$$s^n + c_1 u s^{n-1} + \cdots + c_n u^n \equiv 0 \pmod{Q} \tag{8}$$

But the left side of (8) lies in R, hence in $Q \cap R$, hence in P. Since $u \in$ P we get $s^n \in P$, $s \in P$, a contradiction.

To prove INC we make use of Theorem **43** in a similar way. This time we assume $Q \cap R = P$ and have to show that Q is maximal with respect to the exclusion of S. Suppose on the contrary that Q is properly contained in an ideal J with $J \cap S$ void. Pick $u \in J$, $u \notin Q$. By hypothesis u is integral over R. We proceed to pick for u a "polynomial of least degree mod Q." Precisely: among all monic polynomials f with coefficients in R such that $f(u) \in Q$ we pick one of least degree, say

$$u^n + a_1 u^{n-1} + \cdots + a_n \tag{9}$$

Necessarily $n \geqq 1$. Since the expression in (9) lies in Q, which is contained in J, we deduce that $a_n \in J$. Hence $a_n \in J \cap R \subset \mathrm{P} \subset Q$. Thus

$$u(u^{n-1} + a_1 u^{n-2} + \cdots + a_{n-1})$$

lies in Q, but neither factor is in Q, a contradiction.

We proceed to deduce some consequences concerning the ranks of prime ideals in R and T.

Theorem 45. *Assume that the rings $R \subset T$ satisfy ZNC. Let P, Q be prime ideals in R, T with $Q \cap R = P$. Then $\mathrm{rank}(Q) \leqq \mathrm{rank}(P)$.*

Proof. If

$$Q = Q_0 \supset Q_1 \supset \cdots \supset Q_n$$

is a chain of length n descending from Q, then by INC, the contractions $Q_i \cap R$ are all distinct. Hence $\mathrm{rank}(P) \geqq \mathrm{rank}(Q)$.

Equality may fail here, even if T is integral over R (see Ex. **25**). GD gives equality, in a manner dual to Theorem **47** below. However, we have:

Theorem 46. *Assume that the rings $R \subset T$ satisfy GU. Let P be a prime ideal in R of rank n ($n < \infty$). Then there exists in T a prime ideal Q lying over P and having $\mathrm{rank}(Q) \geqq n$. If, further, INC holds, then $\mathrm{rank}(Q) = n$.*

Proof. Given a chain

$$\mathrm{P} = P_0 \supset P_1 \supset \cdots \supset P,$$

we construct Q_n in T lying over P, (since LO holds by Theorem **42**) and build up a chain

$$Q_n \subset Q_{n-1} \subset \cdots \subset Q_0 = Q$$

with Q_i contracting to P_i by iterated use of GU. Thus $\mathrm{rank}(Q) \geqq n$. The final statement follows from Theorem **45**.

Remark. William Heinzer has constructed an example showing that Theorem **46** can fail for $n = \aleph_0$.

Define the *corank* of a prime ideal P to be the sup of the lengths of chains of prime ideals *ascending* from P. (Alternative terminology: *dimension.*)

Remark. We shall in due course prove that in a Noetherian ring the rank of any prime ideal is finite. Manifestly this is a strong descending chain condition on prime ideals ("strong" meaning that we get a uniform bound on chains descending from a fixed P). As for chains ascending from P, of course by axiom we have in a Noetherian ring the ascending chain condition on all ideals, let alone prime ideals. However the corank can still be infinite; see the first of the "bad" examples at the end of [37].

Theorem 47. *Assume that the rings $R \subset T$ satisfy GU and ZNC. Let Q be a prime ideal in T and $\mathrm{P} = Q \cap R$. Then $\mathrm{corank}(P) = \mathrm{corank}(Q)$.*

Proof. By repeated use of GU any chain ascending from P can be matched by one ascending from Q. By INC, any chain ascending from Q contracts to a distinct chain ascending from P. Together, these two statements prove the theorem.

We also introduce at this point the *dimension* of R itself as the sup of all lengths of chains of prime ideals (or equivalently, the sup of all ranks of prime ideals, or the sup of all ranks of maximal ideals, or the sup of coranks of prime ideals, or the sup of coranks of minimal prime ideals). Sometimes we shall call this the *Krull dimension* if there is danger of confusion with other dimensions. Theorem **48** is immediate from Theorem 47 or Theorem 46.

Theorem **48.** ***Assume*** *that the rings $R \subset T$ satisfy GU and INC. (In particular, this applies if T is integral over R.) Then the dimension of T equals the dimension of R.*

Definition. An integral domain is said to be *integrally closed* if it is integrally closed in its quotient field.

See Exs. 4 and **5** for perhaps the simplest examples of domains that are not integrally closed.

On the affirmativeside of the ledger, ideas going back to Gauss show that any unique factorization domain is integrally closed. To get a little more mileage from this method we introduce the concept of a GCD-domain (Bourbaki's term is "pseudo-Btzout").

Definition. **An** integral domain R is a *GCD-domain* if any two elements in R have a greatest common divisor.

Examples of GCD-domains include unique factorization domains and valuation domains (defined below). It should be carefully noted that we are not assuming that the greatest common divisor is a linear combination of the two elements. This stronger assumption can be recast as saying that all finitely generated ideals are principal, and these domains have been called Btzout domains.

We adopt the ad hoc notation $[a,b]$ for the greatest common divisor of a and b. Of course $[a, b]$ is determined only up to a unit, and we can allow this ambiguity in our discussion.

Theorem **49.** *In a GCD-domain:*
(a) $[ab, ac] = a[b, c]$
(b) *If* $[a, b] = d$, *then* $[a/d, b/d] = 1$
(c) *If* $[a, b] = [a, c] = 1$, *then* $[a, bc] = 1$

Proof. (a) Say $[ab,ac] = \mathbf{x}$. Then since a divides ab and ac, a divides $\mathbf{x}$, say $\mathbf{x} = ay$. Since $\mathbf{x}$ divides ab and ac, y divides b and c. If z divides b and c, then az divides ab and ac, az divides $\mathbf{x} = ay$, z divides y. Hence $[b,c] = y$, as required.

(b) This is immediate from (a).

(c) Suppose that t divides a and bc. Then a fortiori t divides ab and bc, hence divides $[ab,bc]$, which is b by part (a). **So** t divides a and b, $t = 1$.

Theorem 50. *A GCD-domain is integrally closed.*

Proof. Let R be the given GCD-domain, K its quotient field. We suppose that $u \in K$ and that u satisfies an equation

$$u^n + a_1u^{n-1} + \cdots + a_n = 0 \qquad (a_i \in R) \tag{10}$$

Write $u = s/t$, $s, t \in R$. We can divide s and t by $[s,t]$. After we do so, the resulting elements have greatest common divisor 1 by part (b) of Theorem 49. **So** we can start again, assuming $u = s/t$ with $[s, t] = 1$. From (10) we get

$$s^n + a_1s^{n-1}t + \cdots + a_nt^n = 0 \tag{11}$$

and then from (11) we see that t divides s^n. But $[s^n, t] = 1$ by part (c) of Theorem 49. Hence t is a unit, $u \in R$.

We proceed to investigate how integral closure behaves relative to localization.

Theorem **51.** *If R is an integrally closed domain and if S a multiplicatively closed set in R, then R_S is integrally closed.*

Proof. Suppose that the element u in the quotient field is integral over R_S; we have to prove that $u \in R_S$. We are given, say

$$u^n + (a_1/s_1)u^{n-1} + \cdots + (a_n/s_n) = 0$$

with $a_i \in R$, $s_i \in S$. Put $s = s_1 \cdots s_n$ and $t_i = s/s_i$. Then

$$su^n + t_1a_1u^{n-1} + \cdots + t_na_n = 0 \tag{12}$$

If we multiply (12) by s^{n-1} we get an equation asserting that su is integral over R. Hence $su \in R$, $u \in R_S$.

Theorem 52. ***Let $\{R_i\}$ be a family of integral domains all contained in one large domain, and suppose that each R_i is integrally closed. Then $\cap R_i$ is integrally closed.***

The proof is quite obvious.

Now it is a fact, easily proved, that for any integral domain R, $R = \cap R_M$, the intersection ranging over the maximal ideals of R. Using Theorems 51 and **52** we deduce the following: R is integrally closed if and only if each R_M is integrally closed. However the use of maximal ideals in this statement is unnecessarily extravagant. We get a stronger result if we use smaller prime ideals, and an attempt to do as well as possible leads us to use maximal primes of principal ideals. We shall recall again what these are, and at the same time introduce the notation for zero-divisors that we shall be using henceforth.

Let R be a commutative ring, A an R-module $\neq 0$. We recall that the zero-divisors on A are the elements of R that annihilate some non-zero element of A. We write $\mathcal{Z}(A)$ for the set of zero-divisors on A.

Note. It is perhaps treacherous to try to talk about zero-divisors on the zero module, so (except no doubt for occasional forgetfulness) we shall not do so.

We recall further that $\mathcal{Z}(A)$ is the complement of a saturated multiplicatively closed set, and consequently is the set-theoretic union of prime ideals, which are unique if they are confined to those maximal inside $\mathcal{Z}(A)$. These we named (§1-1) the maximal primes of A. If $A = R/I$ we call them the maximal primes of I, in the firm belief that no danger of confusion exists. Finally, if I is principal, we have the prime ideals to be used in Theorem **53.**

Theorem 53. ***Let R be any integral domain. Then*** $R = \cap R_P$, ***the intersection ranging over all maximal primes of principal ideals,***

Proof. Let $u \in \cap R_P$, and write $u = a/b$ $(a, b \in R)$. Let I = the set of all y in R with $ya \in (b)$. If I = R then $a \in (b)$, $u \in$ R, and all is done. ***So*** assume that $I \neq R$, i. e., $a \notin (b)$. We have $I \subset \mathcal{Z}(R/(b))$. We can expand I to a maximal prime P of (b). Then, by hypothesis, $u \in R_P$, so $u = a/b = c/s$ $(c \in$ R, $s \notin P)$. The equation $sa = bc$ shows that $s \in I \subset P$, a contradiction.

Theorems 51, 52, and **53** together yield:

Theorem 54. ***An integral domain*** R ***is integrally closed if and only if R_P is integrally closed for every maximal prime P of a principal ideal.***

We shall later make use of Theorem 54 in a context where it will be known that every R_P is a "discrete valuation ring." In that case, an integrally closed R will be an intersection of discrete valuation rings. But a useful theorem due to Krull (Theorem 57) shows that if we allow ourselves to use arbitrary valuation rings, then the result will hold for any integrally closed domain. Two theorems will precede Theorem 57; in the first we use the term "survives" in the following sense: if R $\subset T$ are rings, and if I is an ideal in R, then I survives in T if $IT \neq T$.

Theorem 55. ***Let*** R $\subset T$ ***be rings, let u be a unit in T, and let I be an ideal in*** R, $I \neq R$. ***Then I survives either in $R[u]$ or in $R[u^{-1}]$.***

Proof. Suppose the conclusion fails. Then we have equations

$$a_0 + a_1u + \cdots + a_nu^n = 1 \qquad (a_i \in I) \tag{13}$$

$$b_0 + b_1u^{-1} + \cdots + b_mu^{-m} = 1 \qquad (b_i \in I) \tag{14}$$

Here we may, by symmetry, assume that $n \geqq m$, and we may further assume that n has been chosen as small as possible. Multiplying (14) by u^n we get

$$(1 - b_0)u^n = b_1u^{n-1} + \cdots + b_mu^{n-m} \tag{15}$$

Now multiply (13) by $(1 - b_0)$ and substitute for $(1 - b_0)u^n$ from (15). The result is an equation of the same type with smaller n, a contradiction.

We introduce the concept of a valuation ring.

Definition. **A** commutative ring R is said to be a ***valuation ring*** if for any a and b in R either a divides b or b divides a.

In the present context we are dealing with domains and so the designation "valuation domain" seems appropriate. For an integral do-

main R with quotient field K we have the following obviously equivalent way of defining R to be a valuation domain: for any $u \neq 0$ in K either u or u^{-1} lies in R.

Theorem 56. *Let K be a field, R a subring of K, and I an ideal in R, $I \neq R$. Then there exists a valuation domain V, $R \subset V \subset K$, such that K is the quotient field of V and I survives in V.*

Proof. The proof is an application of Theorem 55, plus a good exercise on Zorn's lemma. Consider all pairs R_α, I_α, where R_α is a ring between R and K, and I_α is an ideal in R_α, $I_\alpha \neq R_\alpha$, $I \subset I_\alpha$. We partially order the pairs by decreeing inclusion to mean both $R_\alpha \supset R_\beta$ and $I_\alpha \supset I_\beta$. Zorn's lemma is applicable to yield a maximal pair V, J. We shall prove the following: if $u \in K$ then either u or u^{-1} is in V; this will prove both that V is a valuation domain and that K is the quotient field of V. Suppose not; then by Theorem 55, J survives in $V[u]$ or $V[u^{-1}]$. Either way we have contradicted the maximality of the pair V, J.

Theorem 57. *Let R be an integrally closed integral domain with quotient field K. Then $R = \cap V_\alpha$ where the V_α's are valuation domains between R and K.*

Remark. Conversely any such intersection is integrally closed, for by Theorem 50 any valuation domain is integrally closed, and by Theorem 52 an intersection of integrally closed domains is integrally closed.

Proof. Let $y \in \cap V_\alpha$, the intersection ranging over all valuation domains between R and K; we must show $y \in R$. It suffices to show that y is integral over R. Suppose not, and write $u = y^{-1}$. By Theorem 15, u is not invertible in $R[u]$, i. e., (u) survives in $R[u]$. By Theorem 56 we can enlarge $R[u]$ to a valuation domain V inside K in such a way that (u) survives in V. But by hypothesis $y \in V$, i. e., $u^{-1} \in V$, and we have our contradiction.

As an application of Theorem 57 we show in Ex. 10 how to prove that if R is integrally closed, the polynomial ring $R[x]$ is also integrally closed.

We proceed to discuss domains that are locally valuation domains. We first need the concept of the invertibility of an ideal.

Definitions. Let R be an integral domain with quotient field K. By a *fractional* ideal I we mean an R-submodule of K. (We do not insist, as is sometimes done, that $xI \subset R$ for some $x \neq 0$ in R. When there is no danger of misunderstanding we may drop the adjective "fractional.") By I^{-1} (the *inverse* of I) we mean the set of all x in K with $xI \subset R$; I^{-1} is again a fractional ideal. We say that I is *invertible* if $II^{-1} = R$ (note that $II^{-1} \subset R$ is automatic).

Theorem 58. *Any invertible ideal is finitely generated.*

Proof. From $II^{-1} = R$ we get $\Sigma a_i b_i = 1, a_i \in I, b_i \in I^{-1}$. We claim that the a_i's generate I. For if $x \in I$ we have

$$x = x\sum a_i b_i = \sum (xb_i)a_i$$

and the elements xb_i lie in R.

Any non-zero principal ideal is invertible; for if $I = (a), a \neq 0$ (a need not be in R but is in the quotient field), then $I^{-1} = (a^{-1})$ and $II^{-1} = (a)(a^{-1}) = R$.

Recall that a quasi-local ring is one with exactly one maximal M. Note that M consists precisely of all non-units.

The proof of Theorem 59 is so easy that we record it separately, although we promptly supersede it in Theorem 60.

Theorem 59. *Any invertible ideal in a quasi-local domain is principal.*

Proof. We use the notation of the proof of Theorem 58. The elements $a_i b_i$ lie in R and their sum is 1. Hence one of them, say $a_1 b_1$, is a unit. We deduce that $I = (a_1)$.

Theorem 60. *Let R be an integral domain with a finite number of maximal ideals. Then any invertible ideal in R is principal.*

Proof. Let $M_1, \ldots, M_n$ denote the maximal ideals in R, and let I be invertible. Since $II^{-1} = R$, we can, for each i from 1 to n, find $a_i \in I$ and $b_i \in I^{-1}$ such that $a_i b_i \notin M_i$. Moreover, M_i cannot contain the intersection of the remaining maximal ideals. Hence we can find an ele-

ment u_i that is not in M_i but does lie in all the other maximal ideals. Set $v = u_1b_1 + \cdots + u_nb_n$. Note that $v \in I^{-1}$ so that vI is an ideal in R. We claim that vI lies in no maximal ideal. Suppose, for instance, that $vI \subset M_1$. Then $va_1 \in M_1$. However

$$va_1 = (u_1b_1 + u_2b_2 + \cdots + u_nb_n)a_1$$

and in this expression $u_1b_1a_1 \notin M_1$ while all other terms lie in M_1. Hence $vI \subset M_1$ is impossible. We have proved $vI = R$ and $I = (v^{-1})$ is principal.

We proceed to the behavior of invertibility under localization.

Theorem 61. *Let I be an invertible ideal in an integral domain R, and let S be a multiplicatively closed set in R. Then I_S is invertible in R_S.*

The proof is routine and is left to the reader.

Theorem 62. *Let I be a finitely generated ideal in an integral domain R. Then I is invertible if and only if I_M is principal for every maximal ideal M.*

Proof. If I is invertible then I_M is invertible (Theorem 61) and hence principal (Theorem 59). Conversely assume that each I_M is principal. If $II^{-1} \neq R$, embed it in a maximal ideal M. In R_M, I_M is by hypothesis principal. The generator can be selected to be an element i of I. Let $a_1, \ldots, a_n$ be generators of I. We have $s_ja_j \in (i)$ for suitable elements $s_j \in R$, $s_j \notin M$. Write $s = s_1 \cdots s_n$. Then si^{-1} throws all the a_j's into R, whence $si^{-1} \in I^{-1}$. But now

$$s = si^{-1}i \in I^{-1}I \subset M$$

a contradiction.

Definition. A *Prüfer domain* is an integral domain in which every non-zero finitely generated ideal is invertible. (Recall that a Bézout domain is slightly more special in that every finitely generated ideal is required to be principal.)

Theorem 63. *A quasi-local domain is a valuation domain if and only if it is a Bézout domain.*

Proof. That valuation domains are Bézout is trivial. Conversely let R be quasi-local and Btzout. Given two elements in R, say a and b, we must show that one divides the other. We can divide a and b by their greatest common divisor, so we may assume that $(a, b) = R$. Thus $xa + yb = 1$. One of xa, yb must be a unit, say xa. Then a is a unit and divides b.

Theorem 64. *The following statements are equivalent for an integral domain R:*

(1) R is Prüfer;

(2) For every prime ideal P, R_P is a valuation domain;

(3) For every maximal ideal M, R_M is a valuation domain.

Proof. (1) implies (2). Let J be a finitely generated non-zero ideal in Rp. If J is generated by $a_1/s_1, \ldots, a_n/s_n$ $(a_i, s_i \in R, s_i \notin P)$, then $J = I_P$ where $I = (a_1, \ldots, a_n)$. By hypothesis I is invertible; hence (Theorems 61 and 59), J is principal. By Theorem 63, R is a valuation domain.

(2) implies (3). Trivial.

(3) implies (1). Let I be a non-zero finitely generated ideal in R. Then every I_M is principal, so (Theorem 62) I is invertible.

Theorem 65. *Let R be a Prufer domain with quotientfield K, and let V be a valuation domain between R and K. Then $V = R_P$ for some prime ideal P in R.*

Proof. Let M be the unique maximal ideal of V and set $P = M \cap R$. For any s in R but not in P we must have $s^{-1} \in V$, for otherwise $s \in M$ and so $s \in P$. Thus $R_P \subset V$. (So far R could have been arbitrary and V merely quasi-local.)

To prove that $V \subset R_P$ we note (Theorem 64) that R_P is a valuation domain. So if we take $v \in V$ and find $v \notin R_P$ we must have $v^{-1} \in R_P$, say $v^{-1} = a/s$, $a, s \in R$, $s \notin P$. Here $a \in P$ for otherwise a/s would be a unit in R_P and $v \in R_P$, which we assumed is not the case. Hence $a \in M$ and $av \in M$, $s = av \in M \cap R = P$, again a contradiction.

Theorem 65 has a corollary, which can be taken as the starting point of the theory of algebraic functions of one variable.

Theorem 66. *Let K be a field, x an indeterminate over K, and $K(x)$ the field of rational functions in x with coefficients in K. Let V be a valuation domain between K and $K(x)$, $V \neq K(x)$, V having quotient field $K(x)$. Then V is either a localization of $K[x]$ with respect to a non-zero prime ideal (i. e., $V = K[x]_P$, $P = (f)$, f irreducible), or $V = K[x^{-1}]$ localized at (x^{-1}).*

Proof. Either x or x^{-1} must lie in V. If $x \in V$ then $V \supset K[x]$ and the form of V is given by Theorem 65. If $x \notin V$, then $V \supset K[x^{-1}]$ and has the form $K[x^{-1}]_Q$ again by Theorem 65. Since $x \notin V$, x^{-1} must lie in Q and $Q = (x^{-1})$.

We conclude this section with two additional theorems. The first will be used in §2-3. It is in essence due to Seidenberg [46].

Theorem 67. *Let R be a quasi-local integrally closed domain, and let u be an element of the quotient field of R. Assume that u satisfies a polynomial equation with coefficients in R having at least one coefficient a unit in R. Then: either u or u^{-1} lies in R.*

Proof. Say the equation for u is

$$au^n + bu^{n-1} + \cdots = 0$$

If a is a unit then u is integral over R, $u \in R$. So we may assume a unit coefficient occurs further down the equation. Since

$$(au)^n + b(au)^{n-1} + \cdots = 0$$

we have, again by the integral closure, $au \in R$. If au is a unit, then $u^{-1} \in R$. We assume au a non-unit. We have

$$(au + b)u^{n-1} + \cdots = 0$$

If b is a unit then, since R is quasi-local, $au + b$ is a unit. If b is not a unit, there is a unit coefficient later in the equation. In any event some coefficient is a unit, and induction on n concludes the proof.

The final theorem in this section (also due to Seidenberg [46]) relates valuation rings to the strong S-rings defined just prior to Theorem 39.

Theorem 68. *Any valuation ring is a strong S-ring.*

Proof. Any homomorphic image of a valuation ring is a valuation ring. Thus we may assume that R is a valuation domain, and that we are given a rank 1 prime ideal P in R. We are to prove that P^*, the expansion of P to $R[x]$, again has rank 1. Suppose on the contrary that N is a prime ideal in $R[x]$ lying properly between 0 and P*. Necessarily $N \cap R = 0$. Say $0 \neq f \in N$. One coefficient of f, say a_i, can be selected so as to divide all the others. Write $f = a_i g$. Then g has 1 for one of its coefficients; hence $g \notin P^*$ and, all the more so, $g \notin N$. Also, $a_i \notin N$ since $N \cap R = 0$. This contradiction concludes the proof.

EXERCISES

1. Let $R \subset T$ be rings and P a minimal prime ideal in R. (We mean truly minimal, i. e., 0 if R is a domain.) Prove that there exists in T a prime ideal contracting to P.

2. Let $R \subset T$ be rings with R zero-dimensional. Prove that LO holds. Observe that GU and GD hold vacuously.

3. Let $T = R[x]$ with x an indeterminate. Prove that LO and GD hold but that INC does not. Prove that GU fails if R is at least one-dimensional. *(Hint:* for the last point it can be assumed that R is a domain. If P is a non-zero prime ideal in R, take $p \neq 0$ in P, observe that $(1 + px)$ is prime in $R[x]$ and contracts to 0; try to go up from it to a prime over P.)

4. Let R be the ring of all Gaussian integers with even imaginary part, i. e., all $a + 2bi$, a and b integers, $i^2 = -1$. Prove that R is not integrally closed. What is its integral closure?

5. Let K be any field and R the ring of all formal power series in x with coefficients in K and no term in x, i. e., all series

$$a_0 + a_2x^2 + a_3x^3 + \cdots \qquad (a_i \in K)$$

Prove that R is not integrally closed. What is its integral closure?

6. Let R be an integral domain with integral closure T, and S a multiplicatively closed set in R. Prove that the integral closure of R_S is T_S.

7. Suppose, in a GCD-domain, that $[u, a] = 1$ and u divides ab. Prove that u divides b. *(Hint:* by Theorem 49, $b = [ub, ab]$.)

8. Let R be a GCD-domain. We say that a polynomial in the variable x with coefficients in R is *primitive* if the GCD of the coefficients is 1. Prove Gauss's lemma: the product of two primitive polynomials is primitive. (This can be done by a variant on the usual proof. We illustrate with $a + bx$ and $c + dx$. If t divides ac, $ad + bc$, and bd, let $[t,a] = u$. Then u divides bc and bd, hence their GCD, b. Hence $u = 1$. By Ex. 7, t divides c, similarly d.)

9. If R is a GCD-domain, prove that $R[x]$ is a GCD-domain.

10. If R is integrally closed, prove that $R[x]$ is integrally closed. (Use Theorem 57 to reduce to the case where R is a valuation domain. Then use Ex. 9. But note that Ex. 8 is a good deal easier when R is a valuation domain.)

11. Let R be a GCD-domain and P a prime ideal in $R[x]$ contracting to 0 in R. Prove that P is principal. (*Hint:* use Ex. 8.)

12. Suppose that (a, b) is an invertible ideal in a domain, and n a positive integer. Prove that $(a, b)^n = (a^n, b^n)$.

13. Prove that in a Priifer domain, any finitely generated non-zero prime ideal is maximal.

14. Prove that in a valuation ring, any radical ideal is prime.

15. Prove that in a GCD-domain any invertible ideal is principal.

16. Assume GU holds for $R \subset T$. Prove that the contraction of a maximal ideal in T is maximal in R.

17. (This is a globalization of Theorem 67.) Let R be integrally closed. Let $u = a/b$ be an element of the quotient field of R. Assume that u satisfies a polynomial equation such that the ideal generated by the coefficients is invertible. Prove that the ideal (a, b) is invertible.

18. (This is a step in the direction of showing that Theorem 68 is the best possible.) Let R be a one-dimensional quasi-local integrally closed domain that is not a valuation domain. Let M be its maximal ideal. Prove that $\operatorname{rank}(M^*) = 2$, where $M^* = MR[x]$ is the expansion of M to the polynomial ring $R[x]$. (*Hint:* pick u in the quotient field with neither u nor u^{-1} in R. Let N be the kernel of the homomorphism on $R[x]$ given by $x \to u$. Using Theorem 67, prove that N is contained in M^*.)

19. Let R be a one-dimensional integrally closed quasi-local domain. Let $T = R[u]$ with u in the quotient field of R. Assume that LO and INC hold for the pair R, T. Prove: $T = R$. (*Hint:* form N as in the preceding exercise. If $N \subset M^*$, INC is violated. If $N \subset M^*$, u or u^{-1} lies in R by Theorem 67. Rule out u^{-1} by LO.)

20. (This is a sharpening of Theorem 53.) Let R be an integral domain. For each a and b with $a \notin (b)$ let $I(a, b)$ denote the set of all x in R with $xa \in (b)$. Show that for a set of prime ideals to satisfy $\bigcap R_P = R$ it is necessary and sufficient that every $I(a, b)$ be contained in some prime ideal of the set.

21. If I and J are ideals in a domain, and IJ is invertible, prove that I is invertible.

22. For any ideals I, J, K in a ring prove

$$(I + J + K)(JK + KI + IJ) = (J + K)(K + I)(I + J)$$

23. Let R be a domain in which every ideal generated by two elements is invertible. Prove that R is Priifer. (*Hint:* use Exs. 21 and 22. Alternatively, localize, after which "invertible" can be replaced by "principal.")

24. Let $(a_1, \ldots, a_n)$ be an invertible ideal in a domain. Let k be a fixed integer. Let J be an ideal generated by $a_1^k, \ldots, a_n^k$ and any additional number of products of k of the a_i's. Prove that J is invertible. (*Hint:* after localizing, argue that one of the a_i's divides all the others and hence one of the terms a_i^k divides all the generators of J. Cf. Ex. 12.)

25. In the ring R, let M be a maximal ideal of rank k. Let T be the ring $R \oplus R/M$. Regard R as embedded in T by sending $a \in R$ into (a, a^*), where a^* is the 'image of a in R/M. Prove that T is integral over R. Prove that T contains two prime ideals lying over M, and that they have ranks 0 and k.

26. Let P be a prime ideal in a domain. If $PP^{-1} \neq P$, prove that P is minimal over a suitable principal ideal. (*Hint:* pick $p \in P$ with $pP^{-1} \not\subset P$. Shrink P to Q, minimal over (p). If $Q \neq P$, $(pP^{-1})P \subset Q$ yields the contradiction $pP^{-1} \subset Q$. ***Remark:*** if R is Noetherian, Theorem 142 will enable us to conclude that P has rank 1.)

27. Let R be an integral domain with quotient field K. Suppose that every ring between R and K is integrally closed. Prove that R is Priifer. (*Hint:* it can be assumed that R is quasi-local. For $u \in K$ we have $u \in R[u^2]$. Use Theorem 67.)

28. Let R be an integral domain with quotient field K. Assume that any ring between R and K is a localization of R. Prove that R is Priifer. (*Hint:* use Ex. 10 in §1-4 and Ex. 27.)

29. Let R be an integral domain with quotient field K. Prove that the following are equivalent: (a) R is a valuation domain of dimension $\leqq 1$, (b) there are no rings properly between R and K.

30. Let $R \subset T$ be domains with R integrally closed in T, and let S be multiplicatively closed in R. Prove that R_S is integrally closed in T_S.

31. Let $R \subset R[u]$ be rings with R quasi-local and integrally closed in $R[u]$. (a) Suppose that u satisfies an equation with coefficients in R

and one coefficient a unit. Prove that u or u^{-1} lies in R. *(Hint:* review the proof of Theorem **67.)** (b) Suppose that u satisfies no such equation. If M is the maximal ideal of R, prove that $R[u]/MR[u] \cong (R/M)[x]$ where x is an indeterminate.

32. Let R be an integral domain of characteristicp. Let T be a domain containing R and purely inseparable over R: for any $u \in T$, some $u^{p^n} \in$ R. Prove that the map $Q \to Q \cap R$ induces a one-to-one correspondence between the prime ideals of T and those of R.

33. Let $R \subset T$ be domains with T finitely generated as a ring over R. Prove that there exists a non-zero element $a \in$ R such that any maximal ideal in R not containing a survives in T. *(Hint:* if T is algebraic over R, take a to be the product of leading coefficients of polynomials for a set of generators of T, observing that $T[a^{-1}]$ is integral over $R[a^{-1}]$. In the general case, insert R_0 between R and T with T algebraic over R_0 and R_0 purely transcendental over R. Treat the pair $R_0 \subset T$ as above, and then take a to be any coefficient of the resulting polynomial.)

34. Let R be a domain, M a maximal ideal in R, and K a field containing R. Prove that there exists a valuation domain V with quotient field K and maximal ideal N, such that $N \cap R = M$ and V/N is algebraic over R/M. *(Hint:* review the proof of Theorem **56.)** State and prove the analogous strengthening of Theorem **57.**

35. Let $R \subset T$ be domains such that T is algebraic over R and R is integrally closed in T. Prove that T is contained in the quotient field of R. *(Hint:* if $u \in T$ and $au^n + \cdots = 0$, note that au is integral over R.)

36. **(S.** McAdam) Let the ideal I in an integral domain be maximal among all non-invertible ideals. Prove that I is prime. *(Hint:* modify appropriately the hint for Ex. 10 in §1-1.)

37. (This exercise is devoted to a partial analysis of GD.) Let $R \subset T$ be rings, P a prime ideal in R. Prove that the following four statements are equivalent:

(i) Any prime ideal in T minimal over PT contracts to P;

(ii) ("Going down to P") Given a prime $P_1 \supset P$, and a prime Q_1 in T contracting to P_1, we can shrink Q_1 to a prime contracting to P;

(iii) For any prime Q minimal over PT, PT is disjoint from $(R - P)(T - Q)$;

(iv) If J is the radical of PT, then the torsion submodule of T/PT, as an (R/P)-module, is contained in J/PT. (The torsion submodule of a module over an integral domain is the set of all elements with a non-zero annihilator. A reader familiar with flatness will recognize (iv) as a weakened version of flatness of T as an R-module.)

(Hint: we sketch the proofs of six implications.

(i) $\Rightarrow$ (ii). Lower Q_1 to a prime minimal over PT.

(ii) $\Rightarrow$ (i). Let N be a minimal over PT, set $N \cap R = P_1$, and go down.

(i) $\Rightarrow$ (iii). Suppose $u \in PT \cap (R - P)(T - Q)$. Then $u \in Q$, but both $R - P$ and $T -$ Q are disjoint from Q.

(iii) $\Rightarrow$ (i). Given Q minimal over PT, we are to prove that $Q \cap R = P$. Enlarge PT to Q_0, maximal with respect to disjointness from

$$(R - P)(T - Q).$$

Then $Q_0 \subset Q$, $Q_0 \cap R \subset P$. By the minimality of Q, $Q_0 = Q$.

(iii) $\Rightarrow$ (iv). Given $x \in R - P$, $y \in T$ with $xy \in PT$, we have to prove $y \in J$. That is, we must show that y lies in every prime Q minimal over PT. But $y \notin Q$ means $xy \in (R - P)(T - Q)$.

(iv) $\Rightarrow$ (iii). Let $x = \Sigma p_i t_i \in PT$, $x = su$, $s \in R - P$, $u \in T -$ Q. Let u^* be the image of u in T/PT. Then u^* lies in the torsion submodule of T/PT, $u^* \in J/PT$, $u \in J \subset$ Q, a contradiction.)

38. Let $R \subset T$ be a pair of rings satisfying GD. Let P be a prime ideal in R with $PT \neq T$. Prove that there exists in T a prime ideal contracting to P, that is, LO holds for all primes surviving in T. *(Hint:* use the implication (ii) $\Rightarrow$ (i) of the preceding exercise.)

39. (a) Let R be an integrally closed integral domain, and let I be an ideal in R such that I^{-1} is finitely generated. Prove that $(II^{-1})^{-1} = R$. *(Hint:* if x $\in (II^{-1})^{-1}$, then $xII^{-1} \subset$ R, $xI^{-1} \subset I^{-1}$.)

(b) Let I and J be ideals in a domain R, and suppose that

$$I^{-1} = J^{-1} = R.$$

Prove that $(IJ)^{-1} =$ R.

(c) Let R be a one-dimensional quasi-local integrally closed domain. Assume that I^{-1} is finitely generated for every finitely generated ideal in R. Prove that R is a valuation domain. *(Hint:* $J = II^{-1}$ is also finitely generated. By part (a), $J^{-1} =$ R. By part (b), $(J^k)^{-1} =$ R for every k. Pick any x which is not zero or a unit. By the one-dimensionality of R, some power of Jlies in (x) if J $\neq$ R, a contradiction.)

40. Let $R \subset T$ be domains with T integral over R. Call an ideal I in R *contracted* if it has the form $I = J \cap R$ with J an ideal in T. Prove that any non-zero ideal in R contains a non-zero contracted ideal, provided T is a finitely generated R-module. (This exercise is adapted from the paper, "The converse to a well known theorem on Noetherian rings" by P. M. Eakin, Jr., *Math. Annalen* **177** (1968), 278–82.)

(Hint: a number of steps are needed, and are sketched in (b)–(f).

(a) Remark: the hypothesis that T is a finitely generated R-module

cannot be omitted. An example showing this can, for instance, be adapted from Ex. **15** in §2–3.

(b) Temporarily call the pair R $\subset T$ "good" if it satisfies the conclusion of the exercise (every non-zero ideal contains a non-zero contracted ideal). It is routine to see that goodness is transitive. Furthermore if R $\subset T \subset U$ and R $\subset U$ is good, then R $\subset T$ is good.

(c) By (b) we can reduce to the case $T = R[u]$.

(d) Suppose that $T \cap K =$ R, where K is the quotient field of R. Then every principal ideal in R is the contraction of its extension to T. Hence R $\subset T$ is good.

(e) Suppose that T $\subset K$ and let D be the conductor: the set of all x in R with $xT \subset$ R. If $D \neq 0$ then R $\subset T$ is good; for given $I \neq 0$ in R, $I \supset ID \neq 0$ and ID is an ideal in both R and T.

(f) To handle the general case $T = R[u]$, let

$$u^n + a_1u^{n-1} + \cdots + a_n = 0$$

be the irreducible equation for u over K. Let $R^* = R[a_1, \ldots, a_n]$, $T^* = R^*[u]$. The a_i's are integral over R, being polynomials in the conjugates of u. So R^* is a finitely generated R-module, and therefore the conductor of R^* relative to R is non-zero. It follows from (e) that R $\subset R^*$ is good. Part (d) is applicable to show that $R^* \subset T^*$ is good, since $T^* \cap K = R^*$ is easily verified from the fact that T^* is a free R*-module with basis $1, u, \ldots, u^{n-1}$. By part (b) we get in succession that R $\subset T^*$ is good and that R $\subset$ T is good.)

41. Let R be an integral domain, T a ring between R and its quotient field, and D the conductor of T relative to R. (a) If R is Noetherian and $D \neq 0$, prove that T is a finitely generated R-module. (b) Let P be a prime ideal in R not containing D and let Q be a prime ideal in T contracting to P. Prove that $R_P = T_Q$. (Hint: for u in T_Q and z in D but not in P, multiply the numerator and denominator of u by z.) (c) Assume that T is a finitely generated R-module. Let P be a prime ideal in R with complement S. If $R_P = T_S$ prove that $P \not\supset D$. (d) Assume that T is the integral closure of R and is a finitely generated R-module. Let P be a prime ideal in R. Prove that R_P is integrally closed if and only if P $\not\supset D$.

CHAPTER 2

Noetherian Rings

2-1 THE ASCENDING CHAIN CONDITION

We recall that a commutative ring R is Noetherian if every ideal in R is finitely generated, or equivalently, if the ideals in R satisfy the ascending chain condition, and we state and prove at once the Hilbert basis theorem.

Theorem 69. *If* R is Noetherian so is $R[x]$.

Proof. Let J be an ideal in $R[x]$ and let $\mathfrak{Z}_n$ be the set of leading coefficients of polynomials of degree $\leqq$ n in J. Then I_n is an ideal in R and

$$J \cap R = I_0 \subset I_1 \subset I_2 \subset \cdots$$

Let $\mathfrak{Z} = \cup I_n$. We prove the following slight sharpening of the theorem: if $\mathfrak{Z}$ and all the I_n's are finitely generated, then so is J. Let $f_1, \ldots, f_k$ be polynomials in J whose leading coefficients generate $\mathfrak{Z}$. Say N is the maximum of the degrees of thef's. For each j from 0 to N – 1 similarly pick a finite number of polynomials $g_{j1}, g_{j2}, \ldots$ whose leading coefficients generate I_j. Then one easily sees that the f's and g's together generate J.

Remark. Justly celebrated though this proof is, it leaves one somewhat dissatisfied, since the condition that I and the I_n's be finitely generated is by no means necessary for J to be finitely generated.

The ring of formal power series $R[[x]]$ in a variable x is the set of all expressions

$$a_0 + a_1x + \ldots + a_nx^n + \ldots$$

with the natural operations of addition and multiplication. The analogue of the Hilbert basis theorem holds (Theorem **71).** We choose to prove it by making use of Cohen's theorem (Theorem 8), which reduces our problem to the case of prime ideals, and for prime ideals in $R[[x]]$ we are able to pinpoint exactly what is needed.

Theorem 70. *Let P be a prime ideal in $R[[x]]$ and let P^* be the image of P in the natural homomorphism $R[[x]] \to R$ obtained by mapping x to 0. Then P is finitely generated if and only if P^* is finitely generated. If P^* is generated by r elements, then P can be generated by $r + 1$ elements, and by r if $x \notin P$.*

Proof. If P is finitely generated so is its image P^*.

Suppose that $P^* = (a_1, \ldots, a_r)$. We distinguish two cases. If $x \in P$ then $P = (a_1, \ldots, a_r, x)$. Assume that $x \notin P$. Let $f_1, \ldots, f_r \in P$ be series leading off with $a_1, \ldots, a_r$. We claim that $P = (f_1, \ldots, f_r)$. For take any $g \in P$. If g leads off with b then $b = \Sigma b_i a_i$ and $g - \Sigma b_i f_i$ can be written xg_1. Here $xg_1 \in P$ and therefore $g_1 \in P$ since we are assuming that $x \notin P$. In the same way we write $g_1 = \Sigma c_i f_i + xg_2$ with $g_2 \in P$. Continuation of the process leads us to $h_1, \ldots, h_r \in R[[x]]$,

$$h_i = b_i + c_i x + \ldots$$

satisfying $g = h_1f_1 + \ldots + h_rf_r$.

Theorem 71. *If R is Noetherian,* so *is $R[[x]]$.*

The argument we gave in proving Theorem 70 can yield an extra bonus.

Theorem 72. *If R is a principal ideal domain then $R[[x]]$ is a unique factorization domain.*

Proof. Using Theorem **5** we only need to prove that any non-zero prime ideal P in $R[[x]]$ contains a non-zero principal prime. Now if $x \in P$, there is our principal prime. If $x \notin P$ we note that (in the notation of Theorem **70)** P^* is principal. By the last statement in Theorem **70, P** itself is principal.

Remark. We shall later (Theorem 188) prove a much stronger result than Theorem **72.** But we note [45] that the theorem one would really like is not true: it is possible for R to be a unique factorization domain while $R[[x]]$ is not.

In the next theorem, modules enter the picture. We assume that the reader knows the following: if R is Noetherian and A is a finitely generated R-module, then every submodule of A is finitely generated, or equivalently, the submodules of A satisfy the ascending chain condition.

Theorem 73. *Let R be a Noetherian ring, I an ideal in R, A a finitely generated R-module, and B a submodule of A. Let C be a submodule of A which contains IB and is maximal with respect to the property $C \cap B = IB$. Then $I^nA \subset C$ for some n.*

Proof. Since I is finitely generated it evidently suffices to prove that for any x in I there exists an integer m with $x^mA \subset C$. Define D_r to be the submodule of A consisting of all $a \in A$ with $x^ra \in C$. The submodules D_r form an ascending chain that must become stable, say at $r = m$. We claim that

$$(x^mA + C) \cap B = IB \tag{16}$$

That IB is contained in the left side of (16) is clear since $IB = C \cap B$. Conversely, suppose that t is an element of the left side. Then $t \in B$ and also $t \in x^mA + C$, say $t = x^ma + c$ $(a \in A, c \in C)$. Then $xt \in xB \subset IB \subset C$. Hence $x^{m+1}a \in C$. By the choice of m we have $x^ma \in C$, whence $t \in C$, and $t \in C \cap B = IB$. We have proved (16). By the maximal property of C, this gives $x^mA \subset C$.

Theorem 74. *(The Krull intersection theorem.) Let R be a Noetherian ring, I an ideal in R, A a finitely generated R-module, and $B = \cap I^nA$. Then $IB = B$.*

Remark. Krull proved this using primary decomposition and related technical devices. Nowadays it is usually proved via the Artin-Rees Lemma. The present still more elementary proof (really embodied in Theorem 73) is due to Herstein.

Proof. Among all submodules of A containing IB, pick C maximal with respect to the property $C \cap B = IB$. *(Note:* we could do this by Zorn's lemma, but the ascending chain condition on submodules makes this unnecessary.) By Theorem 73, we have $I^n A \subset C$ for some n. But $B \subset I^n A$; hence $B \subset C$ and $B = IB$.

Interesting conclusions can be drawn from Theorem 74. We first prepare the ground.

Theorem 75. *Let R be a ring, I an ideal in R, A an R-module generated by n elements, and x an element of R satisfying $xA \subset IA$. Then: $(x^n + y)A = 0$ for some $y \in I$.*

Proof. Say $a_1, \ldots, a_n$ generate A. We have $xa_i = \Sigma y_{ij} a_j$ for suitable elements y_{ij} in I. Bringing everything to the left, we get the system of equations

$$\begin{aligned} (x - y_{11})a_1 - y_{12}a_2 - \cdots - y_{1n}a_n &= 0 \\ -y_{21}a_1 + (x - y_{22})a_2 \cdots - y_{2n}a_n &= 0 \\ \cdots & \\ -y_{n1}a_1 - y_{n2}a_2 \cdots + (x - y_{nn})a_n &= 0 \end{aligned} \tag{17}$$

Hence the determinant of the coefficients in (17) annihilates all the a_i's, i. e., annihilates A. This determinant has the form $x^n + y$, $y \in I$.

If we apply Theorem 75 with $x = 1$ we obtain:

Theorem 76. *Let R be a ring, I an ideal in R, A a finitely generated R-module satisfying $IA = A$. Then $(1 + y)A = 0$ for some $y \in I$.*

We shall now apply Theorem 76 in two contexts that enable us to prove that $\cap I^n A = 0$. In the first, the key additional hypothesis is the absence of zero-divisors.

Definition. Let R be an integral domain, A an R-module. We say that A is torsion-free if $xa = 0$ $(x \in R, a \in A)$ implies $x = 0$ *or* $a = 0$.

Theorem 77. *Let R be a Noetherian integral domain, I an ideal in R, $I \neq R$, and A a finitely generated torsion-free R-module. Then: $\cap I^n A = 0$.*

Proof. Write $B = \cap I^n A$. By Theorem 74, $B = IB$. By Theorem 76, $(1 + y)B = 0$ for $y \in I$. Hence either $B = 0$ or $1 + y = 0$. But $y = -1$ is ruled out since $I \neq R$.

In the second application the conclusion that something vanishes will come from assumptions concerning the Jacobson radical. We can quote Theorem 76 again, but it is instructive to use the Nakayama lemma (which will, in any case, have lots of later applications).

We assume the reader to be familiar with a little ring theory. Let R be any (not necessarily commutative) ring with unit element. The intersection of the maximal left ideals of R turns out to coincide with the intersection of the maximal right ideals of R and thus is a two-sided ideal J; we call it the *Jacobson radical.* For any x in J, $1 + x$ is invertible (has a two-sided inverse).

Theorem 78 is sometimes stated with a subset of J allowed instead of J. But note that the theorem gets its maximal force when the hypothesis is $JA = A$.

Theorem 78. *(The Nakayama lemma.) Let R be a (not necessarily commutative) ring, let A be a finitely generated left R-module, and assume that $JA = A$ where J is the Jacobson radical of R. Then $A = 0$.* ▮

Remark. See pp. 212–3 of [37] for the history of this lemma.

Proof. Let $a_1, \ldots, a_r$ be a minimal generating set of A. (Here "minimal" can be taken to mean that none of the a_i's can be omitted, or it can be taken in the stronger sense that A cannot be generated by fewer than r elements.) We assume that $r > 0$ and shall reach a contradiction. We have

$$a_1 = j_1 a_1 + \cdots + j_r a_r$$

for $j_1, \ldots, j_r \in J$, *or*

$$(1 - j_1)a_1 = j_2 a_2 + \cdots + j_r a_r$$

Since $1 - j_1$ is invertible, this enables us to express a_1 in terms of the remaining a's, a contradiction.

Theorem 79. *Let R be a commutative Noetherian ring with Jacobson radical J, and A a finitely generated R-module. Then $\cap J^n A = 0$.*

Proof. With $B = \cap J^n A$ we have $B = JB$. Either Theorem **76** or Theorem **78** yields $B = 0$.

EXERCISES

1. If R satisfies the ascending chain condition on finitely generated ideals, prove that R is Noetherian.

2. Prove: if R satisfies the ascending or descending chain condition on prime ideals, then so does $R[x]$.

3. If R satisfies the ascending chain condition on radical ideals, prove that the same is true for $R[x]$. (This is not easy. See pp. **45–8** of [24].)

4. Let R be a ring, A an R-module, y an element of R such that $1 + y$ annihilates A. Then, for any ideal I containing y, prove that $IA = A$. (This is a relatively trivial converse of Theorem **76.)**

5. (The purpose of this exercise is to provide an illustrative example for Ex. 18 in §1–6.) Let $K \subset L$ be fields with K algebraically closed in L, $K \neq L$. For instance, we can take L to be a simple transcendental extension of K. Let R be the subring of $L[[x]]$ consisting of those power series with constant term in K. Prove that R is one-dimensional, quasi-local, and integrally closed, but not a valuation domain. Note that L is infinite-dimensional over K, and that R is non-Noetherian.

6. (This exercise is concerned with Gauss's lemma in the version that refers to the ideals generated by the coefficients, rather than GCD's as in Ex. 8 of §1-6.) *Notation:* polynomials f, g with coefficients in R; I, J, K the ideals generated by the coefficients off, g, andfg respectively.

(a) Prove that $K \subset IJ$.

(b) **An** example where $K \neq IJ$: take R as in Ex. 4 of §1-6, and let $f = 2 + 2ix$, $g = 2 - 2ix$.

(c) If $I = R$, prove that $K = J$. ***(Hint:*** this can be reduced to the quasi-local case. Then argue that $K + MJ = J$. Compare Ex. 9 in §1-1.)

(d) If R is a domain and I is invertible, prove that $K = IJ$. ***(Hint:*** localize and use part (c).)

(e) If R is an integrally closed domain, prove that $K^{-1} = (IJ)^{-1}$. ***(Hint:*** get $K^{-1} \supset (IJ)^{-1}$ by quoting part (a) and taking inverses. In getting the other inclusion argue that, by Theorem **57,** R can be assumed to be a valuation domain.)

(f) If R is an integrally closed domain and $K = (K^{-1})^{-1}$, prove that $K = IJ$. ***(Hint:*** $(K^{-1})^{-1} = ((IJ)^{-1})^{-1} \supset IJ \supset K$, the equality coming from part (e).)

7. Let R be a Noetherian ring, A a finitely generated R-module. Prove that there exists a series of submodules

$$A = A_0 \supset A_1 \supset \cdots \supset A_{n-1} \supset A_n = 0$$

such that each A_i/A_{i+1} is isomorphic to R/P, for P, a prime ideal in R. ***(Hint:*** use Theorem 6 to get A_{n-1}. Pass to A/A_{n-1}, etc., using the ascending chain condition on submodules of A to get the procedure to terminate.)

8. Let R be any (not necessarily commutative) ring, A an R-module, B a submodule.

(a) If B and A/B are finitely generated, prove that A is finitely generated. ***(Hint:*** combine generators for B with lifted generators for A/B.)

(b) If B and A/B satisfy the ascending chain condition on submodules, prove that the same is true for A. ***(Hint:*** the problem is to prove that every submodule of A is finitely generated, knowing that this holds for B and A/B. The question can be reduced to part (a).)

9. Let R be a commutative ring, and let $I_1, \ldots, I_n$ be ideals in R such that $I_1 \cap \cdots \cap I_n = 0$ and each R/I_j is Noetherian. Prove that R is Noetherian. ***(Hint:*** embed R in $R/I_1 \oplus \cdots \oplus R/I_n$ and use Ex. **8.** For an alternative discussion see Theorem 3.16 on page 11 of [37].)

10. If a ring R admits a faithful module (one with annihilator 0) that satisfies the ascending chain condition on submodules, prove that R is Noetherian. ***(Hint:*** reduce the problem to Ex. 9.)

11. (M. Isaacs) Give an alternative proof of Theorem **7** as follows (using the notation of its proof). Observe that R/I is Noetherian. Write $A = (I, a)$, $B = (I, b)$. Note that A/AB is a finitely generated (R/I)-module, and hence so is its submodule I/AB. Since AB is finitely generated, so is I.)

12. **An** integral domain R with quotient field K is ***completely integrally closed*** if, for a and u in K with $a \neq 0$, $au^n \in R$ for all n implies $u \in R$.

(a) If R is completely integrally closed, prove that R is integrally closed.

(b) Prove that the converse of (a) holds if R is Noetherian.

(c) Prove that a valuation domain is completely integrally closed if and only if it has dimension $\leqq 1$.

(d) Let R be completely integrally closed and I a non-zero ideal in R. Prove that $(II^{-1})^{-1} = R$. ***(Hint:*** obviously $II^{-1} \subset R$, $(II^{-1})^{-1} \supset R$. If

$x \in (II^{-1})^{-1}$, then $xII^{-1} \subset R$, $xI^{-1} \subset I^{-1}$, $x^nI^{-1} \subset I^{-1}$ for all n, $x^nII^{-1} \subset R$, $x \in R$ by complete integral closure.)

13. Let R be a ring containing ideals I, J, and N satisfying the following conditions: R/I and R/J are Noetherian, J and N are finitely generated, and $IJ \subset N \subset I \cap J$. Prove that I is finitely generated. ***(Hint:*** by Ex. **9,** $R/(I \cap J)$ is Noetherian, so $I/(I \cap J)$ is finitely generated. J/N is a finitely generated (R/I)-module, hence so is its submodule $(I \cap J)/N$. Thus I/N is finitely generated.)

14. For a general ring R (not necessarily Noetherian) call an R-module Noetherian if, as in Ex. 8 and **10,** it satisfies the ascending chain condition on submodules. Let $R \subset T$ be rings and let J be an ideal in T maximal with respect to the property that T/J is not a Noetherian R-module. Prove that J is prime. ***(Hint:*** assume that $ab \in J$ with neither a nor b in J. Then $T/(J, a)$ is a Noetherian R-module. Let $(J, b) \cap R = I$. Then $T/(J,b)$ is a faithful Noetherian (R/I)-module. By Ex. 10, R/I is a Noetherian ring. The module $(J,a)/J$ is a cyclic T-module annihilated by (J,b), hence it is a cyclic $(T/(J, b))$-module, hence it is a finitely generated (R/I)-module, and therefore it is a Noetherian R-module. By Ex. *8, T/J* is a Noetherian *R*-module, a contradiction.)

15. Let $R \subset T$ be rings with T Noetherian and T a finitely generated R-module. Prove that R is Noetherian. ***(Hint:*** by Ex. 14 reduce to the case where T is **a** domain and T/J is a Noetherian R-module for every non-zero ideal J in T. Let I be a non-zero ideal in R. By Ex. 40 in §1-6, I contains a non-zero contracted ideal. Hence R/I is Noetherian. Since this is true for every non-zero I, it follows that R is Noetherian. This proof is a modification of the proof given by Eakin in the paper cited in Ex. 40 of §1-6. Nagata has another proof in "A type of subrings of a Noetherian ring," ***J. Math. Kyoto Univ.*** 8(1968), **465–7.** David Eisenbud discovered still another proof, which makes use of injective modules and yields a non-commutative generalization.)

2-2 ZERO-DIVISORS

The results thus far derived concerning the zero-divisors on a module A, $\mathcal{Z}(A)$, and the maximal primes of A, have been relatively shallow. Noetherian assumptions make deeper theorems possible.

Theorem 80. ***Let*** R ***be a Noetherian ring, A a finitely generated non-zero R-module. Then: there are only a finite number of maximal primes of A, and each is the annihilator of a non-zero element of A.***

Proof. Consider the set of all annihilators of non-zero elements of A. Each annihilator is contained in a maximal one (by the ascending chain condition, not by Zorn's lemma!). Evidently $\mathcal{Z}(A)$ is the set-theoretic union of these maximal ones. By Theorem **6,** each of them is prime.

We next show that there are only finitely many. Denote them by $\{P_i\}$ and let P_i be the annihilator of a_i. The submodule spanned by the a_i's is finitely generated and therefore spanned, say, by $a_1, \ldots, a_n$. If any further a's exist we have an equation

$$a_{n+1} = x_1a_1 + \cdots + x_na_n \qquad (x_i \in R) \tag{18}$$

From **(18)** we deduce

$$P_1 \cap \cdots \cap P_n \subset P_{n+1} \tag{19}$$

and (19) implies that some P_j $(j = 1, \cdots, n)$ must be contained in P_{n+1}, contradicting the maximality of P_j. Hence there are no further a's or P's.

To complete the proof of Theorem 80 it will suffice to prove that any ideal contained in $\mathcal{Z}(A)$ is contained in one of $P_1, \ldots, P_n$. We abstract the argument for this, since it will be useful several times in the future. The sharp formulation we give in Theorem 81 is due to McCoy [35].

Theorem 81. ***Let*** R ***be a commutative ring,*** $J_1, \ldots, J_n$ ***a finite number of ideals in*** R, ***and S*** a ***subring*** of R ***that is contained in the set-theoretic union*** $J_1 \cup \cdots \cup J_n$. ***Assume that at least*** $n - 2$ ***of the J's are prime. Then S is contained in some*** J_k.

Remark. We are momentarily violating (here and in Theorems 82 and 83) the widely respected convention that a subring has to contain the unit element of the big ring.

Proof. We argue by induction on n. For every k we may assume

$$S \not\subset J_1 \cup \cdots \cup \hat{J}_k \cup \cdots \cup J_n \tag{20}$$

(the notation $\hat{J}_k$ means that J_k is omitted). Note that when we delete J_k we preserve and perhaps strengthen the hypothesis that at most two of

the J's are non-prime. Pick $x_k \in S$ but not in the right side of (20). Then x_k must lie in J_k, since it lies in S but does not lie in any of the other J's. We note that the theorem is trivial for $n = 1$. For $n = 2$, we set $y = x_1 + x_2$ and obtain the contradiction that y lies in S but in none of the J's; this case is really a piece of group theory. For $n > 2$ at least one of the J's must be prime, and we can assume it to be J_1. Set $y = x_1 + x_2x_3 \cdots x_n$. Again $y \in S$ but y lies in none of the J's.

By combining Theorems 80 and 81 we obtain a result that is among the most useful in the theory of commutative rings.

Theorem 82. *Let R be a commutative Noetherian ring, A a finitely generated non-zero R-module, and S a subring contained in $\mathfrak{Z}(A)$. Then there exists a single non-zero element a in A with $Sa = 0$.*

We rephrase this: *although, a priori, each element of S needs a different element of A to exhibit the fact that it is a zero-divisor, nevertheless we have proved that a suitable element of A can do this uniformly.*

Can Theorem **82** be generalized? To discuss this, we drop the module and just consider an ideal I in a commutative ring R, I consisting of zero-divisors. If Z is not assumed to be finitely generated, examples abound to show that I need not be annihilated by a single element. If we insist that I be finitely generated, the matter is not so simple, but counterexamples still exist (see Ex. **7).**

The following theorem is an immediate corollary of Theorem 81. We record it because it will be convenient to quote it in this form.

Theorem **83.** *Let R be a commutative ring, S a subring of R, and I an ideal of R contained in S. Suppose that $I \neq S$ and that*

$$S - I \subset P_1 \cup \cdots \cup P_n$$

where $P_1, \ldots, P_n$ are prime ideals in R, and $S - I$ denotes the set-theoretic complement of I in S. Then $S \subset P_i$ for some i.

Proof. We observe that

$$S \subset I \cup P_1 \cup \cdots \cup P_n$$

We quote Theorem 81. Since $S \subset I$ is ruled out, we deduce that S is contained in some P_i.

We move to the other extreme and give some attention to minimal prime ideals. The first such theorem needs no finiteness assumptions.

Theorem **84.** *Let A be a non-zero R-module, I the annihilator of A, and P a prime ideal in R minimal over I. Then $P \subset \mathfrak{z}(A)$.*

Proof. Let S denote the set of all elements ab in R where $a \notin P$ and $b \notin \mathfrak{z}(A)$. S is clearly a multiplicatively closed set. We claim that it is disjoint from I, for suppose that $baA = 0$, $b \notin \mathfrak{z}(A)$, $a \notin P$. Then $aA = 0$, $a \in I \subset P$, a contradiction. Enlarge I to a prime ideal Q, maximal with respect to disjointness from S. Then $Q \subset \mathfrak{Z}(A)$ and $I \subset Q \subset P$. By the minimality of P, we have $Q = P$ and so $P \subset \mathfrak{z}(A)$.

In the Noetherian case we can strengthen Theorem **84.** The proof is a good illustration of the use of localization, and so we seize this moment to record a nearly obvious theorem that we need.

Theorem **85.** *Any localization R_S of a Noetherian ring is Noetherian.*

Proof. We know that any ideal in R_S has the form Is with I a suitable ideal in R. Since I is finitely generated, so is I_S.

Theorem *86. Let R be Noetherian and let A be a finitely generated non-zero R-module with annihilator I. Let P be a prime ideal in R minimal over I. Then P is the annihilator of a non-zero element of A.*

Proof. We pass to R_P, which is again Noetherian (Theorem 85), and A_P, which is again finitely generated. We need first to check $A_P \neq 0$. Now (since A is finitely generated) the meaning of the vanishing of A_P is $sA = 0$ where $s \in S$, the complement of P. However, the annihilator Z of A is disjoint from S.

Now $I_PA_P = 0$, so that I_P is contained in the annihilator of A_P. As a matter of fact, I_P is the annihilator of A_P (see Ex. 10). We do not need this, however. It suffices for us to verify that P_P is minimal over I_P and hence, all the mork so, minimal over the annihilator of A_P. For suppose there exists a prime ideal in R_P, containing I_P and properly contained in P_P. Necessarily (Theorem **35)** it has the form Q_P, with Q a prime ideal in R properly contained in P. We claim $I \subset Q$. For if $i \in Z$, then $i/1$, as an element of I_P, lies in Q_P. This gives us $s'(si - q) = 0$ for suitable

$q \in Q$ and s, $s' \notin P$. Since $Q \subset P$ we get s, $s' \notin Q$ and hence $i \in Q$. We have upheld the claim $I \subset Q$, and have thereby violated the assumption that P is minimal over I.

Thus P_P is minimal over I_P and we can apply Theorem 84 to get $P_P \subset Z(A_P)$. Then by Theorem 80 there exists a non-zero element of A_P annihilated by P_P, an element that can be taken to be of the form $a/1$ with $a \in A$. The statement that $a/1$ is annihilated by P_P translates to $sPa = 0$, for some $s \notin P$. Write $b = sa$. We claim that P is exactly the annihilator of b. For if $xb = 0$ we have that x/1 annihilates $a/1$, and hence $x/1 \in P_P$, $s_1 x \in P$ for $s_1 \notin P$, and hence $x \in P$.

This is as far as we shall go in the direction of primary decomposition and the primes associated with a module. We have identified the maximal and minimal ones, but we are ignoring the intermediate ones.

We wish next to show that above an ideal I in a Noetherian ring R there are only finitely many minimal prime ideals. *(Note:* if $I = 0$ and R is a domain, we mean (by way of exception) truly minimal prime ideals, that is, 0.) It turns out that this is demonstrable with a weaker chain condition. Since the ideas are useful in differential algebra (see pp. **48–9** of [24]) we present the result in this greater generality.

Theorem **87.** *Let R be a commutative' ring satisfying the ascending chain condition on radical ideals. Then any radical ideal in R is the intersection of a finite number of prime ideals.*

Proof. If not, let I be a radical ideal maximal among those for which the assertion fails (the existence of a maximal one following, not from **Zorn's** lemma, but from the postulated ascending chain condition on radical ideals). Of course, I is not prime. Take a and b with $ab \in I$, $a \notin I$, $b \notin I$. Let J be the radical of (I, a) and K the radical of (I, b). Since I is maximal, J and K are each expressible as a finite intersection of prime ideals. We shall reach a contradiction by proving that $I = J \cap K$. Let $x \in J \cap K$. Then some power x^m lies in (I, a), say

$$x = i_1 + ya \quad (i_1 \in I,\ y \in R).$$

Similarly $x^n = i_2 + zb$ $(i_2 \in I, z \in R)$. By multiplying these two equations we get $x^{m+n} \in I$, x $\in I$, as required.

Remark. Since any prime ideal above a given ideal contains a minimal one (Theorem 10), the intersection in Theorem **87** might as well be confined to the prime ideals minimal over the radical ideal. In that case one readily sees that the expression is unique, and that the prime ideals that occur are exactly all the minimal primes over the radical ideal. This leads us to the next theorem.

Theorem 88. *Let R be a commutative ring satisfying the ascending chain condition on radical ideals, and let I be an ideal in R. Then there are only a finite number of prime ideals minimal over I.*

Proof. **A** prime ideal contains I if and only if it contains the radical of I. Theorem 88 now follows from the remark made just preceding it.

We conclude this section with some useful results on O-dimensional and l-dimensional rings. We recall that the dimension (or Krull dimension if there is danger of ambiguity) is the sup of lengths of chains of prime ideals. **A** ring is O-dimensional if all prime ideals are maximal (and we really mean all; a O-dimensional integral domain is a field). **An** integral domain is 1-dimensional if all non-zero prime ideals are maximal.

We shall also need the Jordan-Holder theorem. We phrase it in terms of composition series. **A** *composition series* for. a module A is a chain

$$A = A_0 \supset A_1 \supset \cdots \supset A, = 0$$

of submodules, beginning at A and ending in 0, such that each A_i/A_{i+1} is irreducible (i. e., has no proper submodule). Theorem: **f** *A has a composition series, then any chain of submodules of* **A** *can be refined to a composition series, and any two composition series have the same length.* We then say that A *has finite length.*

Theorem 89. *Let R be a commutative ring. The following three statements are equivalent:*

(1) R is Noetherian and O-dimensional;

(2) Any finitely generated R-module has finite length;

(3) *R as an R-module has finite length.*

Proof. (1) implies **(2).** If R is O-dimensional, all its prime ideals are both minimal and maximal. By Theorem 88 there are only a finite number of them, say $M_1, \ldots, M_n$. We have

$$M_1 \cdots M_n \subset M_1 \cap \cdots \cap M_n = J$$

J the Jacobson radical of R. By Theorem **25,** J is a nil ideal. Since J is finitely generated, it is actually nilpotent. So $(M_1 \ldots M_n)^k = 0$ for some k.

Now let A be a finitely generated R-module. We can interpolate between A and 0 a string of nk submodules, a typical intermediate step being

$$A \supset \cdots \supset B \supset M_iB \supset \cdots \supset 0$$

where B is the result of multiplying A by a product of M_j's (repetition allowed). Now B/M_iB is a finitely generated module over the field RIM,, and so it is a finite-dimensional vector space. We can thus interpolate a finite number of further submodules between B and M_iB until all quotients are irreducible. We obtain a composition series for A.

(2) implies **(3).** Trivial.

(3) implies (1). If R has finite length it is certainly Noetherian. It remains to be seen that R is O-dimensional. Our problem is to rule out the existence of distinct prime ideals $P \supset Q$. Since we can switch to the domain R/Q, we recast the problem as follows: prove that a domain R of finite length is a field. Let I be a minimal ideal in R and pick $x \neq 0$ in I. Then $xI \subset I$ and must equal I. In particular $x = xi$ for some $i \in I$. This gives $i = 1$, $I = $ R, so R must be a field.

Remark. There is a fourth equivalent statement, formally weaker than **(3):** that R satisfies the descending chain condition on ideals. That the descending chain condition implies the ascending chain condition works even in the non-commutative case (Hopkins' Theorem). We shall not use this refinement, and therefore we have omitted it.

An immediate corollary of Theorem **89** is worth **a** separate statement.

Theorem 90. *The following statements are equivalent for an integral domain* R: *(1)* R *is Noetherian and of dimension* $\leqq 1$, *(2) for any non-zero ideal* I *in* R, R/I *has finite length.*

We conclude this section with a useful theorem concerning **rings** between a one-dimensional Noetherian domain and its quotient field. The proof we give is essentially the one in **[12];** for an alternative proof see **[9], Ch.** VII, p. **29.** Two theorems will precede it.

Theorem 91. ***In*** a *zero-dimensional ring, any non-zero-divisor is a unit.*

Proof. The maximal ideals are also minimal prime ideals and hence (Theorem **84)** consist of zero-divisors.

Theorem 92. ***Let*** *R be a one-dimensional integral domain, let a and c be non-zero elements of R, and let J be the set of x in R satisfying* $xa^n \in (c)$ *for some n. Then* $(J, a) = R$.

Proof. Alternatively, we may describe J as the set of elements which throw some power of a into (c). One of these is c itself. Thus $J \neq 0$ and hence, by Theorem 91, every non-zero-divisor in R/J has an inverse. Let a^* be the image of a in R/J. We assert that a^* is not a zero-divisor. For if $a^*y^* = 0$ for $y^* \in R/J$, we have $ay \in J$ where y maps on y^*, i.e. some $a^m ay \in$ (c), $y \in J$, $y^* = 0$. It follows that a^* is a unit in R/J, i.e. $(J, a) = R$.

Theorem **93.** ***Let*** R *be a one-dimensional Noetherian domain with quotient field K, and T any ring between* R *and K. Then T is again Noetherian and its dimension is at most* 1.

Proof. Let a be an arbitrary non-zero element of R. Our plan is to prove that T/aT is a finitely generated R-module. (We might note that it would be hopeless to try to prove that T itself is a finitely generated R-module; for instance T might be K itself, and K is a finitely generated R-module only when R = K.) This will prove the theorem; for any non-zero ideal in T contains a non-zero element of R, and we then apply Theorem **90.**

Write $I_m = (a^mT \cap$ R, $aR)$. We note that $\{I_m\}$ is a descending chain of ideals in R, all of them containing aR. By Theorem **89** or Theorem **90** the chain becomes stable, say at I_n. For this n we assert that

$$T \subset \frac{\mathrm{R}}{a^n} + aT \tag{22}$$

To prove **(22)** we take $t \in T$ and write $t = b/c$, $b, c \in R$. For these elements' a and c we cite Theorem **92,** i. e. **(J,** a) = R where J is the ideal defined there. We can write $1 = j + za$ ($j \in J$, $z \in R$). Then $t = bj/c + tza$. Now, by the definition of J, $ja^h \in$ (c) for some h, so

$$\frac{bj}{c} = \frac{b}{c}\,ja^h \quad \mathrm{R}$$

whence

$$t \in \frac{R}{a^h} + aT \tag{23}$$

for some h. Let us suppose that (23) has been arranged with the smallest possible value of h. If $h \leqq n$, (22) follows from (23). We shall prove that $h \leqq n$ does hold. Suppose $h > n$. We write out (23) explicitly:

$$t = \frac{u}{a^h} + at_1 \qquad (u \in R,\ t_1 \in T) \tag{24}$$

Equation (24) gives us $u = a^h(t - at_1) \in a^hT$. So $u \in a^hT \cap R \subset I_h$. Since $h > n$ we have $I_h = I_{h+1}$. This means that we can write

$$u = a^{h+1}t_2 + au_1 \qquad (t_2 \in T,\ u_1 \in R) \tag{25}$$

Substitute (25) in (24). The result is

$$t = \frac{u_1}{a^{h-1}} + a(t_1 + t_2)$$

contradicting our minimal choice of h. We have proved (22). It shows T/aT to be a submodule of a cyclic R-module, hence a finitely generated R-module.

EXERCISES

1. Let A_i be a non-zero R-module for each i ranging over an index set. Let A be the direct sum of all A_i. Prove: $\mathcal{Z}(A) = \cup\mathcal{Z}(A_i)$.

2. Given a set-theoretic union $\cup P_i$ of prime ideals in a commutative ring R, prove that $\cup P_i = \mathcal{Z}(A)$ for a suitable R-module A.

3. Let B be a non-zero R-module, and A a submodule different from 0 or B. Prove:

$$\mathcal{Z}(A) \subset \mathcal{Z}(B) \subset \mathcal{Z}(A) \cup \mathcal{Z}(B/A)$$

4. Let A be a non-zero module, x an element with $x \notin <(A)$, $xA \neq A$. Prove: $\mathcal{Z}(A/xA) = \mathcal{Z}(A/x^rA)$ for any r.

5. Let R be Noetherian, S a subring of R, A_i $(i = 1, \cdots, n)$ finitely generated R-modules, $A = A_1 \oplus \cdots \oplus A_n$. If $S \subset <(A)$, prove that $S \subset \mathcal{Z}(A_i)$ for some i.

6. Let R be a UFD, but not a principal ideal domain. (For instance, R can be the ring of polynomials in two variables over a field.) Let the

R-module A be the direct sum of all $R/(p)$, p ranging over the primes of R. Prove that $\mathcal{Z}(A)$ = the set of all non-units in R. Let p, q be distinct primes such that $I = (p, q) \neq R$. Prove that $I \subset <(A)$, but that the annihilator of I in A is 0.

7. We modify the example in Ex. 6 so as to "absorb" the module into the ring. This is done by a semi-direct sum T of R and A. $T = R + A$ is an additive direct sum, and the rule of multiplication is

$$(r_1 + a_1)(r_2 + a_2) = r_1r_2 + (r_1a_2 + r_2a_1)$$

where $r_i \in R$, $a_i \in A$. With the same $\mathcal{Z}$ as in Ex. 6, prove that $J \subset \mathcal{Z}(T)$, but that no non-zero element of T annihilates J, where $J = IT$.

8. Let I be a finitely generated ideal contained in a minimal prime ideal of a ring R. Prove that I annihilates a non-zero element of R. (*Hint:* pass to R_P and observe that its maximal ideal P_P is nil.)

9. Let R be Noetherian, A a non-zero finitely generated R-module, P a maximal prime of A, S a multiplicatively closed set disjoint from P. Prove that P_S is a maximal prime of A_S.

10. Let R be any ring, A a finitely generated R-module with annihilator I. Let S be multiplicatively closed in R. Prove that the annihilator of A_S is I_S.

11. Let R be a domain, and let T be a ring containing R such that every non-zero element of R is a non-zero-divisor in T (in other words, T is torsion-free as an R-module). Prove that the contraction of a minimal prime ideal in T is necessarily equal to 0 in R. (*Hint:* use Theorem 84. Note that the conclusion is a piece of the GD condition on R, T and observe the dual version in Ex. 16, §1-6. The hypothesis of the present exercise is used in the "going down theorem" of Cohen and Seidenberg [13], and the conclusion can advantageously replace it.)

12. Let P and Q be prime ideals in a commutative ring R. Assume that no prime ideal of R is contained in both P and Q. Prove that there exist elements a and b with $ab = 0$, b in P but not in Q, and a in Q but not in P. (*Hint:* let S and T be the set-theoretic complements of P and Q, respectively. Argue that 0 must lie in ST, for otherwise a prime ideal could be constructed excluding ST, and it would be contained in both P and Q. So we have a in S, b in T with $ab = 0$.)

13. Let R be a ring with no non-zero nilpotent elements. Prove: $\mathcal{Z}(R) = \cup P_i$, the union being taken over all minimal prime ideals. (*Hint:* if $ab = 0$ with $b \neq 0$, then $b \notin$ some P_i, since $\cap P_i = 0$.)

14. Let R be a ring with no non-zero nilpotent elements. Assume that every element in R is either a unit or a zero-divisor. Prove that if R has finitely many minimal prime ideals, it has dimension 0.

15. Let R be a ring such that in every homomorphic image of R, any element is either a zero-divisor or a unit. Prove that R is zero-dimensional. *(Hint:* if P $\subset$ Q are different prime ideals, pass to RIP.)

16. Let R be any ring, and let A be an R-module possessing a series of submodules

$$A = A_0 \supset A_1 \supset \cdots \supset A_{n-1} \supset A, = 0$$

such that each A_i/A_{i+1} is isomorphic to R/P_i for P_i a prime ideal in R. Let Q be a prime ideal in R such that Q is the annihilator of a non-zero element in A. Prove that Q equals one of the P_i's. *(Hint:* say Q is the annihilator of a; let B be the submodule generated by a. Observe that the annihilator of any non-zero element of B is again Q. If $B \cap A_1 \neq 0$, use induction. If $B \cap A_1 = 0$, prove that $Q = P_0$.)

17. Combine Ex. 16 and Ex. 7 in §2-1 to give alternative proofs of the finiteness of the number of maximal or minimal prime ideals attached to a finitely generated module over a Noetherian ring.

18. Let Z be a radical ideal in an arbitrary ring. Prove that I is prime if and only if it is not expressible as an intersection of two properly larger radical ideals. *(Hint:* see the proof of Theorem 87. Note the connection with part (e) of Ex. 12 in §1-3.)

19. (This exercise continues the transition to the geometric language where Ex. 12 in §1-3 left off.) Prove that any variety is expressible as a finite union of irreducible varieties. *(Hint:* one can derive this directly from the ascending chain condition in $K[x_1, \ldots, x_n]$, or from Theorem 87.)

20. Let R be an integral domain with quotient field K. Suppose that every ring between R and K is Noetherian. Prove that the dimension of R is at most 1. *(Hint:* if not, take $x \neq 0$, $x \in$ Q $\subset$ P, Q and P distinct primes. Then take $y \in$ P, where y is not a member of any prime minimal over x. Let T be the ring generated over R by all xy^{-i}, I the ideal in T they generate. If Z is finitely generated, it is generated by some xy^{-i}. Derive a contradiction. Note that this exercise is a converse to Theorem 93.)

21. Let R be a one-dimensional Noetherian domain, let P be a prime ideal in R, and let T be a ring lying between R and its quotient field. Prove that in T there are only a finite number of prime ideals lying over P. *(Hint:* combine Theorems 93 and 88.)

22. (In this exercise we waive the requirement of a unit element.) A ring is *von Neumann regular* if for any a there exists an x with $axa = a$. Let R be a zero-dimensional commutative ring with no non-zero nilpotent elements. Prove that R is von Neumann regular. *(Hint:* for given a, let S be the set of all $a^n - a^{n+1}y$. If 0 is not in the multiplicatively closed set S, construct P maximal with respect to exclusion of S. The hypothesis of zero-dimensionality implies that R/P is a field. If z is an inverse of a mod P, then $a^2z - a$ is in P, a contradiction. Hence some $a^n - a^{n+1}y = 0$, and $a - a^2y$ is nilpotent.)

23. (This exercise comes from an unpublished manuscript of A. Brumer and P. Sally.) In Theorem 81 assume that all the J's are prime. Prove the theorem by the technique of localization. *(Hint:* pass to R_S, where S is the complement of the union of the J's.)

24. Let the ideal Z in the ring R be such that every prime ideal containing Z is finitely generated. Prove that every ideal containing Z is finitely generated. *(Hint:* if some ideal containing I fails to be finitely generated, it can be enlarged by Zorn's lemma so as to be maximal with respect to this failure. Apply Theorem 7 to get the desired contradiction.)

25. Let R be a ring satisfying the ascending chain condition on prime ideals and having the property that any radical ideal is the intersection of a finite number of prime ideals. Prove that R satisfies the ascending chain condition on radical ideals. *(Hint:* if not, let $I_1 \subset I_2 \subset I_3 \cdots$ be a properly ascending sequence of radical ideals. Let $I_1 = P_1 \cap \cdots \cap$ P,. Writing *rad* for the radical of an ideal, we have

$$\text{P,} = rad(I_1 + P_i) \subset rad(I_2 + \text{P,}) \subset rad(I_3 + \text{P,}) \cdots$$

for each i from 1 to r. Suppose that for every i this sequence ultimately becomes constant, say at the **n-th** term. Then we get the contradiction $I_n = I_{n+1}$. For let u be an element of I_{n+1}. We have $u \in rad(I_n + \text{P,})$. For a suitable power u^k we get $u^k = y_i + z_i$ with $y_i \in$ I,, $z_i \in$ P,. Then

$$(u^k - y_1) \cdots (u^k - y,) = z_1 \cdots z, \in I_1 \subset I_n \quad ,$$

whence $u \in I_n$. The process can thus be iterated to yield a properly ascending sequence of prime ideals.)

26. Call an ideal a *J-ideal* if it is an intersection of maximal ideals. Prove that the following conditions on a ring R are equivalent: (a) the ascending chain condition on J-ideals, (b) every J-ideal in R is the intersection of a finite number of prime J-ideals. *(Hint:* that (a) implies (b) can be proved by a minor modification of the proof of Theorem 87. To prove that (b) implies (a) assume on the contrary that $I_1 \subset I_2 \subset I_3 \cdots$ is a strictly ascending sequence of J-ideals. For each k there exists a maximal ideal M_k containing I_k but not I_{k+1}. Let Z be the ideal generated by $I_1, M_1I_2, M_1M_2I_3, \ldots$. Then Z is contained in all the M's. We

claim that M_k is a minimal prime over Z. For suppose that $Z \subset P \subset M_k$ with P a prime ideal properly contained in M_k. Since

$$M_1 M_2 \cdots M_k I_{k+1} \subset Z \subset P$$

and no M_i is contained in P we get $I_{k+1} \subset P$, and then the contradiction $I_{k+1} \subset M_k$. Let Y be the J-ideal $\cap M_i$. Since there are infinitely many minimal primes over Y, Y cannot be the intersection of a finite number of prime ideals. This proof is due to William Heinzer.)

27. Let a be a non-zero-divisor in a ring R, and let J be any ideal in R. Prove: $\mathcal{Z}(R/J) \subset \mathcal{Z}(R/aJ)$. *(Hint:* if $x \in \mathcal{Z}(R/J)$ then $xu \in J$ for $u \notin J$. Deduce that $xau \in aJ$ and $au \notin aJ$.)

28. Let R be a UFD and I an ideal in R, $I \neq R$. Prove that the following are equivalent: (a) I is principal, (b) $\mathcal{Z}(R/I)$ is a finite union of principal prime ideals, (c) if a prime ideal P is contained in $\mathcal{Z}(R/I)$ then P is principal. *(Hint:* only (c) $\Rightarrow$ (a) offers any difficulty. Write $I = aJ$, where the GCD of the elements of J is 1. If $J \neq R$, observe that any prime ideal minimal over J has rank at least 2. Use hypothesis (c) and the preceding exercise.)

29. Let P be a fixed prime ideal in the ring R and let A be an R-module. Let I be maximal among those annihilators of non-zero elements of A which lie inside P. Prove that I is prime. *(Hint:* suppose on the contrary that $xy \in I$, $x \notin I$, $y \notin I$. Then $ann(xa)$ contains I and y, so can not be contained in P. Take $s \notin P$, $sxa = 0$. Note that $sa \neq 0$. $Ann(sa)$ is contained in P and contains (I, x), a contradiction. This exercise is a strengthened form of Theorem **6.**)

30. Prove Theorem **86** by using the preceding exercise. *(Hint:* deduce from the assumption that A is finitely generated, the fact that P contains the annihilator of some element of A. Enlarge the latter to a maximal annihilator inside P. Exs. **29** and 30 are due to **S.** McAdam.)

2-3 INTEGRAL ELEMENTS, III

The main purpose of this section is to establish the basic properties of Dedekind rings, and prove that the Dedekind property is preserved in suitable integral extensions.

We begin with the local case — but first we have to define a local ring.

Definition. A ring is local if it is Noetherian and has exactly one maximal ideal.

To shorten the statements of the next theorems, and to mesh with later work on grade, we define grade 1.

Definition. An ideal I in a ring R has *grade* 1 if it contains a non-zero-divisor x such that $I \subset \mathcal{Z}(R/(x))$.

Theorem 94. *Let I be an ideal of grade 1 in a Noetherian domain R. Then I^{-1} properly contains R.*

Remark. For a converse see Exs. 1 and 2 in §3-1.

Proof. We have $I \subset \mathcal{Z}(R/(x))$. By Theorems *80* and 81 there exists $y \notin (x)$ with $Iy \subset (x)$. Then y/x is in I^{-1} but not in R.

Theorem 95. *Let R be a local domain with maximal ideal M. Assume that R is integrally closed and that M has grade 1. Then M is principal.*

Proof. By Theorem **94,** M^{-1} properly contains R. Now MM^{-1} contains M, is contained in R, and therefore equals M or R. But if $MM^{-1} = M$ then M^{-1} is integral over R (Theorem 12), hence is contained in R since R is integrally closed. This contradiction proves that M is invertible, and hence (Theorem **59)** principal.

We discuss a little further the properties of the domain R of Theorem **95.** A very easy argument shows that every ideal is principal; thus R is a principal ideal domain with just one prime. It is also a valuation domain. This kind of valuation domain is called a discrete valuation ring (DVR).

Theorem 96. *For an integral domain R the following statements are equivalent:*

(1) Every non-zero ideal of R is invertible;

(2) R is Noetherian, integrally closed, and of dimension $\leqq 1$;

(3) R is Noetherian, and for each maximal ideal M, R_M is a DVR.

Proof. (1) implies (2). In each R_M all ideals are principal (Theorem 59), so R_M is a DVR. R is Noetherian by Theorem **58.** R is integrally closed by Theorem **54.**

(2) implies **(3)** is covered by Theorem 95.

(3) implies **(1)** follows from Theorem 62.

An integral domain satisfying any (hence all) of the conditions in Theorem 96 is called a *Dedekind ring.* Another property of Dedekind rings appears as Theorem 97.

Theorem 97. *In a Dedekind ring any non-zero ideal is uniquely a product of prime ideals.*

Proof. Given I, it is contained in some prime ideal P. Since P is invertible we have $I = (IP^{-1})P$. This factorization can be continued till we reach a product of prime ideals, the process terminating since I is properly contained in IP^{-1}, etc.

If $I = P_1 \cdots P_m = Q_1 \cdots Q_n$ (all P's and Q's prime ideals) then $Q_1 \cdots Q_n \subset P_1$, so some $Q_i \subset P_1$. Since non-zero prime ideals are maximal we must have $Q_i = P_1$. Since P_1 is invertible we can cancel it on both sides. Continuation of the process proves uniqueness.

Remark. Conversely, if a domain R has the property that every ideal is a product of prime ideals (no further assumptions are needed), one can prove that R is Dedekind. This theorem is due to Matusita. See [12].

We consider the following setup: R is an integrally closed domain with quotient field K, L is an algebraic extension of K, and T is the integral closure of R in L (the "ring of R-integers" in L). It is an easy exercise that T has quotient field L. (A little more is true: any element of L is expressible as a quotient with numerator in T and denominator in R.) The following little picture may help visualize the relationships.

$$\begin{array}{ccc} R & \subset & T \\ \downarrow & & \downarrow \\ K & \subset & L \end{array}$$

The classical version of the problem is the case where R is the ring of integers, K the field of rational numbers, and L a finite algebraic extension of K (i. e. an algebraic number field). More generally, let R be a principal ideal domain and $[L:K]$ finite. It was a great discovery of the 19th century that T need not be a principal ideal domain, but that it is a Dedekind ring. Having gone that far, we might as well let R be a Dedekind ring.

Theorem 98. *Let* R *be a Dedekind ring with quotient field* K. *Let* L *be a field finite-dimensional over* K, *and let* T *be the integral closure of* R *in* L. *Then* T *is a Dedekind ring.*

Proof. We head for statement (2) of Theorem 96. T is integrally closed by Theorem 40, and has dimension $\leqq 1$ by Theorem 48. It remains to argue that T is Noetherian.

We can find a vector space basis of L over K consisting of elements of T (first take any basis, then multiply by suitable elements of R to throw the basis into T). Say $u_1, \ldots, u_n$ is the basis. Then $T_0 = R[u_1, \ldots, u_n]$ is Noetherian; indeed it is a finitely generated R-module. By another application of Theorem 48, $\dim(T_0) = 1$. Since T lies between T_0 and its quotient field L, T is Noetherian by Theorem 93.

Another method of proof is available if L is separable over K, and shows that T is a finitely generated R-module; see [51]. But it is not always true that T is a finitely generated R-module. We present, in a slightly recast version, a pertinent example of **F.** K. Schmidt (Theorem 100). The main change from Schmidt is to switch the point of view (à la Artin's Galois theory) from going up to going down.

So we start with an integral domain T, its quotient field L, and a subfield K of L; we define $R = T \cap K$. At present we place no restrictions on the pair of fields $K \subset L$. For a number of facts that hold in this context, see **Exs.** 1–5.

We introduce at this point the *value group* of a valuation domain. We can in fact define it for any integral domain R. Let U be the group of units in R, and let K^* be the multiplicative group of non-zero elements in the quotient field K. We call K^*/U the value group of R. Divisibility (relative to R) induces on K^*/U the structure of a partially ordered group, and the ordering is total if and only if R is a valuation domain. This totally ordered group is cyclic if and only if R is a DVR. We leave the routine verification of these statements to the reader.

Theorem 99. *Let T be a valuation domain with quotient field L, let K be any subfield of L, and set $R = T \cap K$. Then R is a valuation domain with quotient field K. Its value group is in a natural way a subgroup of that of T. If T is a DVR, so is R.*

Proof. Given $a \neq 0$ in K we have that a or a^{-1} lies in T and therefore in R. This proves that R is a valuation domain with quotient field K. The inclusion $R \subset T$ induces a homomorphism from the value group of R into the value group of T. Saying that this is an isomorphism amounts to the following: if $x \in R$ is a unit in T, prove that x is a unit in R; this is clear since $x^{-1} \in T \cap K = R$. The final statement of the theorem is immediate, since a subgroup of a cyclic group is cyclic.

Theorem 100. *Let k be a field of characteristic 2, and $T = k[[x]]$, the power series ring in an indeterminate. With $u \in T$, let $K = k(x, u^2)$ and $L = k(x, u)$ (field adjunction), $R = T \cap K$, $S = T \cap L$. Then $[L:K] \leqq 2$, R and S are discrete valuation rings with quotient fields K and L, and S is the integral closure of R in L. If $[L:K] = 2$, then S is not a finitely generated R-module.*

Remark. It is possible to arrange $[L:K] = 2$, for instance, by taking x and u to be algebraically independent over k, for which we need a transcendental power series u. We have a choice of a cardinal number argument when k is countable (then T has the power of the continuum) or the use of suitable gaps, à la Liouville.

Proof. We illustrate the various rings and fields in the figure:

$$\begin{array}{ccccc} & & R & \subset & S & \subset & T \\ & & \downarrow & & \downarrow & & \downarrow \\ k & \subset & K & \subset & L & \subset & M \end{array}$$

where M is the quotient field of T. The statement $[L:K] \leqq 2$ is obvious, since L is obtained from K by adjoining a square root of an element of K. Theorem 99 tells us that both R and S are DVR's, with quotient fields K and L, respectively. Since S contains R, has quotient field L, is integrally closed, and is integral over R (by characteristic 2), it follows that S is the integral closure of R.

We now assume $[L:K] = 2$ and shall prove that S is not a finitely generated R-module. Suppose on the contrary that it is. Then S is spanned

over R by elements $a_i + \beta_i u$ $(i = 1, \cdots, r)$ where $a_i, \beta_i \in K$. (In fact, r can be 2, but there is no need for us to insist on this.) We note that any element of M can be thrown into T by multiplication by a sufficiently high power of x. It follows that any element of K can be thrown into R by multiplication by a suitable power of x. If we pick x^m to satisfy $x^m \alpha_i \in R$ and $x^m \beta_i \in R$ for all i, we get $x^m S \subset R + Ru$. Suppose

$$u = a_0 + a_1 x + a_2 x^2 + \cdots$$

We set

$$v = (u - a_0 - a_1 x - \cdots - a_m x^m) x^{-m-1}$$

and note that v is again an element of T. (The minus signs might as well be plus signs since the characteristic is 2; however we thought the reader's eye would this way more easily catch the cancellation of all powers of x up to x^m.) Thus the expression for the element v takes the form

$$v = (a_{m+1} x^{m+1} + a_{m+2} x^{m+2} + \cdots) x^{-m-1}$$

making it apparent that v lies in T. Since v is also in L, we see that $v \in S$. So $x^m v \in R + Ru$. But the unique expression for $x^m v$ in the form $R + Ru$ has to have x^{-1} for its coefficient of u, a contradiction since x^{-1} is not in R (it is not even in T).

There is a Priifer analogue of Theorem 98.

Theorem 101. *Let R be a Priifer domain with quotient field K. Let L be an algebraic extension of K (possibly infinite-dimensional), and let T be the integral closure of R in L. Then T is a Priifer domain.*

Proof. Let N be a typical maximal ideal in T. It will suffice, by Theorem **64,** to prove that T_N is a valuation domain. Thus, given $u \in L$, we must prove that u or u^{-1} lies in T_N. If $N \cap R = P$, then R_P is a valuation domain. Now u satisfies a polynomial equation with coefficients that can be taken to be in R_P, and we can normalize so that one coefficient is a unit. We can equally well regard the coefficients as lying in T_N, for $R_P \subset T_N$. We quote Theorem **67.**

Remarks. 1. This proof is taken from [19].

2. Instead of quoting Theorem **67,** we could use the globalized version: **Ex. 17** in §1-6.

3. An alternative proof of Theorem **98** would begin by quoting Theorem 101. It would then remain to prove T Noetherian, presumably exactly as was done in the proof of Theorem **98.**

What examples are there of non-Dedekind Priifer domains? The main ones are as follows.

(1) Valuation domains. For instance, it is possible to construct a valuation domain with any preassigned value group.

(2) The ring of entire functions, an example due to Helmer [22]. This is a good example to keep in mind if you are looking for a Priifer domain with unusual properties.

(3) Examples obtained from a given Priifer domain by the use of Theorem 101.

Examples (1) and (2) are in fact Btzout domains (all finitely generated ideals are principal). In the hope of getting away from the Btzout property, one might try, under the heading (3), the ring of algebraic integers. But this too is Btzout, as is mentioned in passing in [15]. This follows from the existence of so-called class fields in algebraic number theory. There is, however, a more elementary proof due to John Thompson, and it works in more general circumstances. (For another proof, see p. **86** of [33].)

We recall that the *class* group of a Dedekind domain is the group of invertible ideals modulo principal ideals, and that for the ring of integers in an algebraic number field the class group is finite.

Theorem *102. Let R be a Dedekind domain with quotient jield K, let L be the algebraic closure of* K, *and let T be the integral closure of R in L. Assume that for any finite algebraic extension of K the ring of integers has* a *torsion class group. Then T is a Bézout domain.*

Proof. Let I be a finitely generated ideal in T, generated say by $a_1, \ldots, a_n$. The a's generate a finite-dimensional extension L_0 of K; let T_0 be the ring of integers in L_0 and I_0 the ideal generated by $a_1, \ldots, a_n$ in T_0. By hypothesis some power of I_0 is principal; say $I_0^k = bT_0$, $b \in T_0$. Let $c \in L$ be a k-th root of b. In the ring T_1 of integers in $L_0(c)$ we have $(I_0T_1)^k = (c^k)$. It follows from unique factorization into prime ideals (Theorem **97)** that $I_0T_1 = (c)$. Hence the ideal I in T is also principal.

EXERCISES

In exercises 1–5, $K \subset L$ are fields, T has quotient field L, and $R = T \cap K$.

1. Let S be a multiplicatively closed subset of R. Prove: $R_S = T_S \cap K$.

2. If T is integrally closed, prove that R is integrally closed.

3. If R is a valuation domain with maximal ideal M, prove that M survives in T.

4. If T is quasi-local, prove that R is quasi-local.

5. (This exercise is intended to give a reasonably simple example in which the quotient field of R is not K.) Let k be any field, and let x and y be indeterminates over k. Set $K = k(x)$, $L = k(x, y)$, $T = k[y, y/x]$. Prove that $R = k$, and thus does not have quotient field K.

6. Suppose that R is a Priifer, Bézout, or valuation domain, and S is multiplicatively closed in R. Prove that R_S has the same property.

7. Let R be Bézout with quotient field K and let T be a ring between R and K. Prove that $T = R_S$ for a suitable S.

8. Let R be any integral domain, Q a prime ideal in $R[x]$ that contracts to 0 in R. Prove that $R[x]_Q$ is a DVR.

9. Let R be a domain' with quotient field K. (a) Suppose that R contains a principal prime p such that $R[p^{-1}] = K$. Prove that R is a DVR. (b) Suppose that R contains a set $\{p_i\}$ of principal primes such that adjoining all the elements p_i^{-1} to R yields K. Prove that R is a UFD.

10. Let R be a given integral domain. Assume that R_M is Noetherian for every maximal ideal M in R, and that any non-zero element of R lies in only a finite number of maximal ideals. Prove that R is Noetherian. *(Hint:* argue that for an ascending chain of ideals $I_1 \subset I_2 \subset \ldots$ there exists n such that from n on the chain is stable in each R_M. Then use Ex. 5 in §1-4.)

11. Prove: if every prime ideal in a domain R is invertible, then R is Dedekind.

12. Prove: if every maximal ideal in a Noetherian domain R is invertible then R is Dedekind. (This problem was suggested by *J. C.* Robson.)

13. Let R be a one-dimensional Noetherian domain. Prove that the integral closure of R is a Dedekind domain. *(Hint:* Theorems *93* and **96.)**

14. Let R be a one-dimensional local domain. Prove that the integral closure of R is a principal ideal domain with a finite number of primes. *(Hint:* Ex. *13,* Ex. 21 in §2-2, and Theorem **60.)**

15. Let R_i $(i = 0, 1, 2, \ldots)$ be a sequence of rings with each R, properly contained in R_{i+1}. Let T be the set of polynomials in an indeterminate x with the coefficient of x^n allowed to range over R_n. Prdve that T is a ring and is not Noetherian. *(Hint:* pick a_i in R_{i+1} but not in R_i, and use the a_i's to build a strictly ascending sequence of ideals in T. This exercise can be applied to a one-dimensional Noetherian domain with integral closure not a finitely generated module (Theorem 100). It yields a two-dimensional Noetherian domain with a non-Noetherian ring between it and its Noetherian integral closure.)

16. Let R be any ring. Let S be the set of all polynomials in $R[x]$ with the property that their coefficients generate R.

(a) Prove that S is multiplicatively closed. *(Hint:* see Ex. 9 in §1-1.) Write $T = R[x]_S$.

(b) Exhibit a natural one-to-one correspondence between the maximal ideals of R and those of T. In particular, verify that T is quasi-local if R is; if M, N are the unique maximal ideals of R, T, prove that T/N is isomorphic to rational functions in one variable over R/M.

(c) If R is a valuation ring, prove that T is a valuation ring.

(d) If R is a valuation domain, prove that the value groups of R and T are isomorphic (more precisely, the map discussed in connection with Theorem 99 is an isomorphism).

(e) Let R be a domain, and let f, g be polynomials with I, J the ideals generated by their coefficients. Assume that $I \subset J$ and that J is invertible. Prove that $f/g \in T$. *(Hint:* let h be a polynomial whose coefficients generate [redacted] Write $f/g = fh/gh$ and use Ex. 6(d) in §2-1.)

(f) If R is a Priifer domain, prove that T is a Bézout domain. (Remark: it is immediate from part (c) that T is Priifer; the subtler fact that T is Bézout is deducible from part (e).)

(g) If R is a Dedekind domain, prove that T is a principal ideal domain.

Exs. 17–19 are due to M. Isaacs. They provide an alternative proof of Theorem **98.**

17. Let R be a ring, A an R-module. Call an ideal I in R *pleasant* if B/IB is a Noetherian R-module for every submodule B of A. Otherwise, I is *unpleasant.* Prove: if I is maximal among unpleasant ideals then I is prime. *(Hint:* if not, suppose that $ab \in I$ with neither a nor b in I. Then (I, a) and (I, b) are pleasant. Let B be a submodule of A. The R-module $B/(I, a)B$ is Noetherian. From the pleasantness of (I, b) relative to the submodule $(I, a)B$ we see that $(I, a)B/(I, b)(I, a)B$ is a Noetherian R-module. By Ex. 8 of §2-1, $B/(I, b)(I, a)B$ is a Noetherian R-module and so is its homomorphic image B/IB, a contradiction.)

18. Let R be a Priifer domain and let A be a torsion-free R-module of finite rank n. (This means that any $n + 1$ elements of A are linearly dependent over R.) Prove that for any maximal ideal M in R, A/MA is finite-dimensional over R/M, with dimension at most n. *(Hint:* we have to prove that $n + 1$ elements $a_1^*, \ldots, a_{n+1}^*$ in A/MA must be linearly dependent. With a_i in A mapping on a_i^* we have $\Sigma u_i a_i = 0$ with u_i elements in R that are not all 0. Let $I = (u_1, \ldots, u_{n+1})$. We can find $x \in I^{-1}$ with $xI \not\subset M$. From the fact that A is torsion-free we deduce $\Sigma(xu_i)a_i = 0$. Since at least one xu_i is not in M we get the required linear dependence of the a_i^*'s.)

19. Let R be a Dedekind domain with quotient field K, let L be a finite-dimensional extension of K, and let T be the integral closure of R in L. Prove that T is Noetherian. *(Hint:* apply Ex. 17 with T playing the role of the module A. By Ex. 18 every maximal ideal in R is pleasant. Hence the only possible unpleasant ideal is 0. It suffices to prove T/J Noetherian for J a non-zero ideal in T. Since $J \cap R = I$ is non-zero, T/IT is a Noetherian R-module, and so is its homomorphic image T/J.)

20. Let R be an integral domain and Q a maximal ideal in $R[x]$ that satisfies $Q \cap R = 0$. Prove that Q is invertible. *(Hint:* use Ex. **8,** Ex. 10 in §1-3, and Theorem 62.)

21. Let R be a local one-dimensional domain with maximal ideal M, and let T be the integral closure of R. Let u be an element of T that lies in the radical of MT but not in M. Let Q be the kernel of the natural homomorphism $R[x] \to R[u^{-1}]$. Prove that Q is invertible but not principal. *(Hint:* deduce from Ex. **2** in §1-2 that u satisfies an equation $u^n + a_1u^{n-1} + \cdots + a_n = 0$ with $a_i \in M$. Thus Q contains $a_nx^n + \cdots + a_1x + 1$. It follows that Q is maximal, for any prime ideal properly containing Q must contain M. By Ex. 20, Q is invertible. If Q is principal its generator must be a linear polynomial $bx + c$. Here $c \in M$ for otherwise $u = -bc^{-1} \in R$, a contradiction since the radical of MT contracts to M.)

2-4 INTERSECTIONS OF QUASI-LOCAL DOMAINS

We begin this section with two theorems on integrally closed Noetherian domains. These theorems are fairly immediate corollaries of earlier results.

Theorem 103. *In an integrally closed Noetherian domain R every prime ideal P of grade 1 has rank 1, and R_P is a DVR.*

Proof. The idea of the proof is to localize and then use Theorem 95. However, there is a technical difficulty that needs to be circumvented, for we must localize so as to preserve the grade 1 property.

We have $0 \neq x \in P$ and $P \subset Z(R/(x))$. Enlarge P to a maximal prime Q of (x). Then (Theorem 80) Q is the annihilator of a non-zero element in $R/(x)$. Otherwise stated, we have an element $y \notin (x)$ such that $Qy \subset (x)$. We pass to R_Q and note that it is Noetherian and integrally closed. Furthermore, Q_Q has grade 1, the same element x working. The key point is that $y \notin (x)$ still holds in R_Q, for if $y = (a/s)x$ with $a, s \in R$ and $s \notin Q$ then $sy = ax$ whence $s \in Q$, a contradiction. By Theorem 95, R_Q is a **DVR,** and in particular Q has rank 1. This forces $Q = P$, and proves all the statements of the theorem.

The next theorem follows directly from Theorems 53 and 103.

Theorem 104. *If R is an integrally closed Noetherian domain, then $R = \bigcap R_P$ where P ranges over the prime ideals of rank 1.*

With this as motivation we proceed to investigate representations of R of the form $R = \bigcap V_i$, where the V_i's are quasi-local domains lying between a domain R and its quotient field K. Mostly, the V_i's are assumed to be valuation domains (as the letter "V" suggests), but as far as possible we allow them to be quasi-local.

The mere existence of such a representation does not say much. By Theorem **53,** any domain is an intersection of quasi-local domains. To say that $R = \bigcap V_i$ with the V_i's valuation domains merely says that R is integrally closed (Theorem **57).** It is when we assume "local finiteness" of the intersection that interesting things follow.

Definition. Let R be an integral domain with quotient field K. Let V_i be quasi-local domains between R and K. Let Q_i be the maximal ideal of V_i. Assume $R = \bigcap V_i$. We say that this representation is *locally finite* if any non-zero element of R lies in only a finite number of the Q_i's (i.e., is a unit in all but a finite number of the V_i's).

Remark. The representation given by Theorem **104** is locally finite, as follows from Theorem 88. We shall prove below (Theorem 123) that

any Noetherian domain admits a representation as a locally finite intersection of quasi-local domains. This is not true for every domain, but there do not seem to exist easy examples to show this.

The simplest locally finite intersection is one where there are only a finite number of V_i's all together. In this context our first theorem treats the case where the V_i's are already known to be localizations.

Theorem 105. *Let R be a domain, and $P_1, \ldots, P_n$ prime ideals in R, no two of which are comparable. Assume that*

$$R = R_{P_1} \cap R_{P_2} \cap \ldots \cap R_{P_n}$$

Then $P_1, \ldots, P_n$ are exactly the maximal ideals of R.

Proof. Let x be a non-unit in R. We claim $x \in P_1 \cup \cdots \cup P_n$. If not, then $x^{-1} \in R_{P_i}$ for all i, whence $x^{-1} \in R$, which is nonsense. If M is a maximal ideal, then $M \subset P_1 \cup \cdots \cup P_n$, from which it follows that M is contained in some P_i, i. e., $M = P_i$. From this the theorem easily follows.

Theorem 105 enhances the interest in proving that the quasi-local domains occurring in a finite decomposition are localizations. For valuation domains we get a decisive result (Theorem 107). The next theorem is a prelude.

Theorem 106. *Let x be a unit in a quasi-local ring R. There exists an integer k (depending on x) such that for any integer m prime to k, $1 + x + \cdots + x^{m-1}$ is a unit in R.*

Proof. Let M be the maximal ideal of R, and write $L = R/M$ (L is called the *residue class field).* Write x^* for the image of x in L. Our problem is to ensure $1 + x^* + \cdots + (x^*)^{m-1} \neq 0$. We distinguish two cases.

Case I. $x^* = 1$. k = the characteristic of L will do (meaning $k = 1$ if L has characteristic 0).

Case II. $x^* \neq 1$. Since

$$1 + x^* + \ldots + (x^*)^{m-1} = \frac{1 - (x^*)^m}{1 - x^*}$$

we need to ensure $(x^*)^m \neq 1$. If x^* is not a root of unity, take $k = 1$. Otherwise take k to be the order of x^*.

Theorem 107. *Let a domain R be the intersection $V_1 \cap \cdots \cap V_n$, where the V_i's are valuation domains between R and its quotient field. Then each V_i has the form R_{P_i} for a suitable prime ideal P_i in R. R is a Bhout domain. If no two V_i's are comparable, then $P_1, \ldots, P_n$ are precisely the maximal ideals of R.*

Proof. Let Q_i be the maximal ideal of V_i, and set $P_i = Q_i \cap R$. We shall show that P_i does what is required. To prove, for instance, that $V_1 = R_{P_1}$, we take $x \in V_1$ and have to find $s \in R$, $s \notin P_1$, such that $sx \in R$. For each V_i such that x is a unit in V_i we find a corresponding k_i as in Theorem 106. Take m $\geqq 2$ prime to all the k_i's, and $= 2$ if there are no k_i's. Then $s = (1 + x + \cdots + x^{m-1})^{-1}$ will do. We note the behavior of s at a given V_i, distinguishing the three possibilities.

(a) If $x \in Q_i$, then s is a unit in V_i.

(b) If x is a unit in V_i, we have arranged that s is a unit in V_i.

(c) If x is not in V_i, then $x = y^{-1}$ with $y \in Q_i$ (this is the crucial place we use the hypothesis that V_i is a valuation domain). Then

$$s = y^{m-1}/(1 + y + \cdots + y^{m-1})$$

so that $s \in Q_i$.

Thus in all cases $s \in V_i$. Hence $s \in R$. Since $x \in V_1$ we have (see (a) and (b) above) that s is a unit in V_1, whence $s \notin P_1$. Finally, we have to see that $sx \in R$, i. e., that $sx \in$ every V_i. Only in case (c) above do we need to argue further. Then

$$sx = y^{m-2}/(1 + y + \cdots + y^{m-1}) \in V_i$$

We have proved that each $V_i = R_{P_i}$. Now the representation $R = \cap V_i$ can be shortened to be irredundant in the sense that no two V_i's are comparable. Let us suppose this has already been done. Then it follows that no two P_i's are comparable. We can quote Theorem 105 to deduce that $P_1, \ldots, P_n$ are exactly the maximal ideals of R. That R is Bézout follows from Theorems **64** and **60.**

Theorem **107** fails if we assume the V_i's merely to be quasi-local. Let $F \subset G$ be fields and let F_1, F_2 be intermediate fields properly larger than F and satisfying $F_1 \cap F_2 = F$. Let R, V_1, V_2 be the subrings of $G[[x]]$ obtained by insisting that the constant term lie in F, F_1, and F_2, respectively. Then R, V_1, V_2 are all quasi-local and one-dimensional; V_1, V_2 lie between R and its quotient field; V_1 and V_2 are properly larger than R; and $V_1 \cap V_2 = R$. Of course V_1, V_2 are not localizations of R.

However, there are still some affirmative statements that can be made, and the full facts remain to be explored; Theorem 109 is a sample. We need Theorem 108 as a prelude (and it will be used again later in this section).

Theorem 108. *Let a, b be non-zero, non-invertible elements in a one-dimensional quasi-local domain R. Then some power of a is divisible by b.*

Proof. The ring $R/(b)$ has exactly one prime ideal, which is consequently nil (Theorem 25). The image of a in $R/(b)$ is therefore nilpotent, i. e., some power of a is divisible by b.

Theorem 109. *Let the domain R be equal to $V_1 \cap V_2$, where the V's lie between R and its quotient field. Assume that each V_i is quasi-local, has maximal ideal Q_i, and that $Q_i \cap R = P_i$. Assume further that P_1 and P_2 are incomparable, and that each V_i is one-dimensional. Then $V_i = R_{P_i}$.*

Proof. Given $x \in V_1$, we must prove $x \in R_{P_1}$, i. e., we must find $s \in R$, $s \notin P_1$, such that $sx \in R$. We have an element t that lies in P_2 but not in P_1. Write $x = y/z$ with y and z in V_2. Since V_2 is one-dimensional and t lies in its maximal ideal, we have (Theorem 108) that in V_2, z divides some power of t, say $t^n = zz_1$. Then $x = yz_1/t^n$, $t^n x = yz_1$. The element $s = t^n$ does the trick. For s, like t, lies in P_2 but not in P_1. We have $sx \in V_1$ since $s \in R$ and $x \in V_1$. Finally, $sx = yz_1$ lies in V_2 since y and z_1 both do.

We turn to what can be said for infinite intersections. The notation set forth in Theorem 110 will be used in the next four theorems as well.

Theorem 110. *Let the domain R be a locally finite intersection $\cap V_i$ of one-dimensional quasi-local domains lying between R and its quotient field. Let Q_i be the maximal ideal of V_i, and $P_i = Q_i \cap R$. Let N be a non-zero prime ideal of R. Then $N \supset$ some P_i.*

Remark. Note that R_{P_i} is necessarily contained in V_i but need not be equal to it. We are, of course, interested in the possibility of proving equality from suitable hypotheses.

Proof. Assume the contrary. Let t be a non-zero element of N. Let $P_1, \ldots, P_r$ be the finite number of P's containing t. Pick u_j in P_j but not in N $(j = 1, \ldots, r)$. Because of the one-dimensionality of V_j we have (Theorem 108) that $u_j^{n_j}$ is a multiple of t (in V_j) for sufficiently large n_j. Then $u = u_1^{n_1} \cdots u_r^{n_r}$ is a multiple of t in $V_1, \ldots, V_r$ by construction, and is also a multiple of t in all other V_i's since t is a unit there. Hence u is a multiple of t in R, $u \in N$, a contradiction since each u_i is not in N.

Theorem 111. *Suppose, in addition to the hypotheses of Theorem 110, that a multiplicatively closed set in R is given: let it be denoted by S. Then R_S is a locally finite intersection of the V_i's that contain R_S.*

Proof. Let us use the subscript j for a typical V_j containing R_S. To prove $R_S = \cap V_j$ we take $x \in \cap V_j$ and have to prove $x \in R_S$. Let $W_1, \ldots, W_r$ be the finite number of V_i's not containing x. (Observe that, by the local finiteness, any element of the quotient field of R lies in all but a finite number of the V_i's and, moreover, is a unit in all but a finite number of the V_i's.) Then there exists $s_k \in S$ with $s_k^{-1} \notin W_k$, for otherwise $R_S \subset W_k$ and W_k would be one of the V_j's. Thus s_k is a non-unit in W_k. By Theorem 108, $s_k^{n_k} x \in W_k$ for some n_k. Then with $s = \Pi s_k^{n_k}$ we have $sx \in R$ and so $x \in R_S$. That the representation $R_S = \cap V_j$ is again locally finite is immediate.

Theorem 112. *Suppose, in addition to the hypotheses of Theorem 110, that each V_i is a valuation domain and that R itself is quasi-local and one-dimensional. Then R is one of the V_i's.*

Proof. If M is the maximal ideal of R, each $P_i = M$ or 0. Now if $P_i = 0$, the corresponding V_i is the quotient field of R. This is an uninteresting possibility, which we could have ruled out in advance; but in any case our hypothesis that V_i is one-dimensional dismisses it. So each $P_i = M$. Local finiteness then tells us that there are only a finite number of V_i's. This makes Theorem 107 applicable. Since R has only

one maximal ideal, there can be only one V_i left when we make the intersection irredundant, and R must equal that V_i. (As a matter of fact, there can be only one V_i present, as follows from the easily proved fact that there are no rings properly between a one-dimensional valuation domain and its quotient field.)

Theorem 113. *Suppose, in addition to the hypotheses of Theorem 110, that each V_i is a valuation domain. Let N be a minimal prime ideal in R. Then R_N is one of the V_i's.*

Proof. By Theorem 111, R_N is a locally finite intersection of the V_j's that contain it. We apply Theorem 112 to R_N.

Let us call a valuation domain *rational* if its value group is isomorphic to a subgroup of the additive group of rational numbers.

Theorem 114. *Suppose, in addition to the hypotheses of Theorem 110, that each V_i is a rational valuation domain. Then $R = \cap V_j$, where the intersection is taken over those V_i's that have the form R_N, N a minimal prime ideal in R.*

Remark. Examples, discovered independently by Ohm [41] and Griffin [21] show that we cannot delete "rational" in Theorem 114.

Proof. Let us (hopefully) call the V_i's of the form R_N "essential", and the others "inessential." We begin by showing that *one* inessential component can be deleted. So let W be inessential, and write Q for its maximal ideal, $P = Q \cap R$. We can assume that the rank of P is at least 2. For if P is minimal, then (Theorem 113) R_P = one of the V_i's; since $R_P \subset W$ this tells us that W contains an essential V_i and so certainly can be deleted. (Actually, W itself would be essential; see the analogous remark in the proof of Theorem 112.)

We proceed to prove that the V_i's with W deleted still intersect in R. Suppose the contrary. Then we have an element x, that lies in every V_i other than W but not in W.

Since $\operatorname{rank}(P) \geq 2$, P properly contains a non-zero prime ideal which in turn, by Theorem 110, contains a P_k, which we fix for the argument that follows. Pick any non-zero y in P_k. The hypothesis that W is a rational valuation domain allows us to find positive integers m, n such

that $z = x^m y^n$ is a unit in W. Since $x \in V_k$ and $y \in Q_k$, we have $z \in Q_k$. At any V_i other than W or V_k we have that x and y both lie in V_i and hence so does z. In sum: z lies in every V_i (hence $z \in R$); z is a unit in W; and z is a non-unit in V_k. This contradicts the inclusion $P_k \subset P$.

From the ability to suppress one inessential component we pass stepwise to the suppression of a finite number. Ordinarily this would be as far as one could go. However, local finiteness enables us to complete the job simply and swiftly. Suppose the element u lies in every essential V_i; we have to prove $u \in R$. Now in any event, u lies in all but a finite number of the V_i's. The troublesome components, which do not contain u, are of course inessential. We have just seen that they can be omitted. Hence $u \in R$.

Let us call a domain R a ***Krull domain*** if it satisfies the three following conditions:

(1) For every minimal prime ideal P, R_P is a **DVR.**

(2) $R = \cap R_P$, the intersection being taken over all minimal prime ideals.

(3) Any non-zero element of R lies in only a finite number of minimal prime ideals.

Theorems 103 and 104 show that any integrally closed Noetherian domain is a Krull domain. It is evident that any **UFD** is a Krull domain. Since neither of these classes of domains includes the other, Krull domains are useful as a unifying concept. Also significant is the following fact (its proof is beyond the scope of this book): the integral closure of a Noetherian domain need not be Noetherian, but it is a Krull domain.

We can state the following corollary of Theorem 114: if a domain R is a locally finite intersection of **DVR's** within its quotient field, then R is a Krull domain. Moreover, the given **DVR's** must include every R_P, P minimal.

EXERCISES

1. In a Noetherian integrally closed domain, let x be neither 0 nor a unit, and let P be a prime ideal minimal over (x). Prove that P has rank 1. ***(Hint:*** use Theorems 84 and 103. This is a special case of the principal ideal theorem, and the point is that the integrally closed case admits this alternative proof.)

2. Prove that a one-dimensional Krull domain is a Dedekind domain. ***(Hint:*** see **Ex.** 10 in §2-3.)

3. Under the hypotheses of Theorem 114, prove that every non-zero prime ideal contains a minimal prime ideal..

4. (a) Under the hypotheses of Theorem 110, prove that any non-zero element of R lies in only a finite number of minimal prime ideals. ***(Hint:*** review the proof of Theorem 110.)

(b) Assume in addition that each P_i is of rank 1. Prove that for any $a \neq 0$ in R we have

$$\mathcal{Z}(R/(a)) = P_1 \cup \cdots \cup P_n$$

where $P_1, \ldots, P_n$ are the minimal prime ideals containing a. Prove also that every prime ideal of grade 1 has rank 1.

5. In the notation used throughout this section, let $R = V_1 \cap V_2$ with V_1 a one-dimensional valuation domain, V_2 quasi-local, and $V_2 \not\subset V_1$. Prove that V_2 is a localization of R. ***(Hint:*** take $x \in V_2$, $x \notin V_1$. By adding 1 if necessary, adjust x to be a unit in V_2. For any $u \in V_2$, $ux^{-n} \in R$ for sufficiently large n.)

6. Prove: if R is a Noetherian integrally closed domain, then $R[[x]]$ is integrally closed. ***(Hint:*** use Theorem 104 to reduce to the case where R is a **DVR.** Then Theorem 72 is applicable. The stronger result can be proved: that if R is completely integrally closed (cf. **Ex.** 12 in §2-1) so is $R[[x]]$. For a thorough study of this circle of ideas, see the paper [41] by Ohm.)

7. Let R be a Krull domain and P a minimal prime ideal in R. Let p be an element of P that generates P_P in R_P. Prove that there exists an element u with $u \notin P$, $uP \subset (p)$. ***(Hint:*** let $P_2, \ldots, P_n$ be the remaining minimal prime ideals containing p. Take u in a sufficiently high power of $P_2 \ldots P_n$.)

8. Let R be a Krull domain in which all prime ideals of rank $\geqq 2$ are finitely generated. Prove that R is Noetherian. ***(Hint:*** it must be proved that a typical minimal prime ideal P is finitely generated. Observe that R/P is Noetherian. Pick $p \in P$ generating P_P, pick u in P but in no other minimal prime containing p, let $N = (p, u)$, and let J be the set of all x with $xP \subset N$. Note that P is the only minimal prime containing N. Note further that $N \subset J$ and that $J \not\subset P$ by **Ex.** 7. Hence every prime ideal containing J has rank $\geqq 2$. By **Ex.** 24 in §2-2, R/J is Noetherian and J is finitely generated. The hypotheses of **Ex.** 13 in §2-1 are now fulfilled, with P playing the role of I.)

CHAPTER 3

Macaulay Rings and Regular Rings

3-1 R-SEQUENCES AND MACAULAY RINGS

The theory of R-sequences is a comparatively recent addition to the theory of commutative rings, but there seems to be no doubt that it will have a permanent place in the subject. In this section we develop the basic properties of R-sequences and the related topic of Macaulay rings.

Definition. Let R be any commutative ring, A any R-module. The (ordered sequence of) elements $x_1, \ldots, x_n$ of R is said to be an *R-sequence* on A if

(a) $(x_1, \ldots, x_n)A \neq A$;
(b) For $i = 1, \ldots, n$, $x_i \notin Z(A/(x_1, \ldots, x_{i-1})A)$.

Stated more completely, (b) says that x_1 is not a zero-divisor on A, x_2 is not a zero-divisor on A/x_1A, $\ldots, x_n$ is not a zero-divisor on $A/(x_1, \ldots, x_{n-1})A$.

The case $A = \mathrm{R}$ is of special importance. We then simply say that the sequence $x_1, \ldots, x_n$ **is** an R-sequence. The property can be restated in a suggestive way: x_1 **is** neither a unit nor a zero-divisor in R, the image of x_2 is neither a unit nor a zero-divisor in the ring $R/(x_1)$, the image of x_3 is neither a unit nor a zero-divisor in the ring $R/(x_1, x_2)$, etc.

The assumption (a) in the definition of an R-sequence is a mere matter of technical convenience. In the first place, it guarantees that

the modules A, $A/x_1A, \ldots, A/(x_1, \ldots, x_{n-1})A$ are all non-zero so that we are entitled to discuss their zero-divisors. And further, it tells us that the module $A/(x_1, \ldots, x_n)A$ is non-zero, which is reassuring in case further work with zero-divisors is needed. The equivalent form given in Theorem 76 should be noted.

It is assumption (b) that really matters. As a partial motivation we give one example. Let S be any commutative ring and let

$$\mathrm{R} = S[x_1, \ldots, x_n]$$

be the polynomial ring over S in n indeterminates. For the R-module we take R itself. Then it is evident that the elements $x_1, \ldots, x_n$ constitute an R-sequence in R.

To some extent, the resemblance between R-sequences and independent indeterminates can be pursued. Let R be a commutative ring containing a field F, and let $a_1, \ldots, a_n$ be an R-sequence in R. Then it can be shown that the a's are independent indeterminates over F; the proof is sketched in [25].

To push the analogy further, we note that Theorem 121 is an analogue of the invariance of the transcendence degree of a field extension.

We begin our discussion by handling a number of technical points.

Theorem 115. *Let I, J be ideals in a ring* R, A *an R-module, and write $B = A/IA$. Then B/JB is isomorphic to $A/(I+J)A$.*

Proof. Consider the natural homomorphisms $A \to B \to B/JB$. The kernel of the induced map from A to B/JB contains IA and JA, hence $(I+J)A$. Conversely if x belongs to the kernel, then x maps into JB in the map $A \to B$, hence differs from an element of JA by an element of IA. Thus $x \in (I+J)A$.

Theorem 116. *Let i be an integer less than n. Let A be an R-module, $x_1, \ldots, x_n$ elements in* R. *Then the following statements are equivalent.*

(a) $x_1, \ldots, x_n$ is an R-sequence on A,

(b) $x_1, \ldots, x_i$ is an R-sequence on A and $x_{i+1}, \ldots, x_n$ is an R-sequence on $A/(x_1, \ldots, x_i)A$.

Proof. Apply Theorem 115 with $\mathbf{Z} = (x_1, \ldots, x_i)$ and J successively replaced by (x_{i+1}), (x_{i+1}, x_{i+2}), ...

Theorem 117. *Let $x, y \in R$ be an R-sequence on the R-module A. Then $x \notin Z(A/yA)$.*

Proof. Suppose that $t^* \in A/yA$ and $xt^* = 0$. Pick any t in A mapping on t^*. Then $xt \in yA$, say $xt = yu$. Since $y \notin Z(A/xA)$, this implies $u \in xA$, say $u = xu_1$. Since $x \notin Z(A)$, we can cancel x in the equation $xt = xyu_1$, getting $t = yu_1$, $t^* = 0$, as required.

Examples show that in Theorem 117 we cannot conclude that y, x is an R-sequence, i. e., the conclusion $y \notin <(A)$ fails. If we assume $y \notin <(A)$ outright then we can make the interchange of x and y; in the next theorem we extend this remark to longer sequences.

Theorem 118. *Let $x_1, \ldots, x$, be an R-sequence on A. Then the sequence obtained by interchanging x_i and x_{i+1} is an R-sequence on A if and only if $x_{i+1} \notin Z(A/(x_1, \ldots, x_{i-1})A)$.*

Proof. This is immediate from Theorems 116 and 117.

With Noetherian and radical assumptions the interchange can be effected.

Theorem 119. *Let* R *be Noetherian, A a finitely generated R-module, and $x_1 \ldots, x_n$ elements in the Jacobson radical of* R *constituting an R-sequence on A. Then any permutation of the x's is also an R-sequence on A.*

Proof. Any permutation on n things can be achieved by successive interchanges of neighboring elements, By Theorem 118 it therefore suffices to do the case $n = 2$. We change notation for the R-sequence to x, y and (by Theorem 117 or 118) it suffices to prove $y \notin <(A)$. Let S be the submodule of A annihilated by y. We shall prove $S = 0$. Take $s \in S$. Since $y \notin Z(A/xA)$, we have $s \in xA$, say $s = xs_1$. Now $ys = 0$ gives us $xys_1 = 0$ and then $ys_1 = 0$ since $x \notin <(A)$. Hence $s_1 \in S$. We have proved $S = xS$. By the Nakayama lemma (Theorem 78), $S = 0$.

Remark 1. Diana Taylor (Chicago thesis, 1966) has proved a partial converse to Theorem 119: if a Noetherian ring R possesses an R-sequence of length 3, and if in R every permutation of an R-sequence is an R-sequence, then R is local. See Ex. 7 for a simple example showing that the radical assumption in Theorem 119 cannot be deleted.

Remark 2. Inspection of the proof shows that in Theorem 119 we need not assume that x, is in the radical; it suffices to know this for the remaining $n - 1$ elements.

Theorem 120. *If $x_1, \ldots, x$, is an R-sequence on a module A, then the ideals $(x_1), (x_1, x_2), \ldots, (x_1, x_2, \ldots, x,)$ form a properly ascending chain.*

Proof. Suppose on the contrary that $(x_1, \ldots, x,) = (x_1, \ldots, x_{i+1})$. Then x_{i+1} is a linear combination of $x_1, \ldots, x_i$ so that

$$x_{i+1}A \subset (x_1, \ldots, x_i)A.$$

This shows that x_{i+1} annihilates the module $A/(x_1, \ldots, x_i)A$, whereas it is supposed to be a non-zero-divisor.

Theorem 120 shows that if R is Noetherian and A is a non-zero R-module, then maximal R-sequences on A exist. But, of course, we do not yet know that any two such maximal R-sequences have the same length, or even that there is a fixed upper bound to their lengths. This is settled in the next theorem.

Theorem 121. *Let* R *be a Noetherian ring, I an ideal in* R, *and A a finitely generated R-module. Assume that $IA \neq A$. Then: any two maximal R-sequences on A contained in I have the same length.*

Proof. It evidently suffices to prove the following: if $x_i, y_i \in I$, $x_1, \ldots, x_n$ is a maximal R-sequence on A, and $y_1, \ldots, y_n$ is an R-sequence on A, then $y_1, \ldots, y_n$ is maximal. We do this by induction on n, the case $n = 1$ requiring separate discussion.

$n = 1$. After a change of notation we have the following setup: x and y are in I, they are non-zero-divisors on A, and the element x constitutes a maximal R-sequence on A. It then *follows* that I consists of zero-divisors on A/xA; for if $t \in I$ is a non-zero-divisor on A/xA, then the sequence x, t is an R-sequence on A, the condition $(x,t)A \neq A$ being fulfilled in view of the hypothesis $IA \neq A$. Our task is to prove that I consists of zero-divisors on A/yA. The vital information is provided by

Theorem 82, which tells us that a single non-zero element u^* of A/xA is annihilated by I. Restating this in A, we have u in A but not in xA such that $Iu \subset xA$. In particular, $yu \in xA$, say $yu = xv$. We claim $v \notin yA$ and $Iv \subset yA$. For the first point, if $v = yw$ then $yu = xyw$. The factor y can be cancelled, leaving the contradiction $u = xw$. For the second point, we have $xIv = yIu \subset yxA$. In this inclusion the factor x is cancellable, yielding $Iv \subset yA$. If v^* denotes the image of v in A/yA, then $v^* \neq 0$ and $Iv^* = 0$, as required.

General n. For brevity let us write $B_i = A/(x_1, \ldots, x_{i-1})A$, $C_i = A/(y_1, \ldots, y_{i-1})A$ for $i = 1, \ldots, n$. In particular, $B_1 = C_1 = A$. The existence of the elements x_i, y_i shows that $I \not\subset \mathfrak{P}(\&)$, $I \not\subset \mathfrak{P}(C_i)$ for any i. From this we can deduce the existence of an element z lying in I but in none of $\mathfrak{P}(B_i)$, $\mathfrak{P}(C_i)$. One way to see this is to form the set-theoretic union of all the sets $\mathfrak{P}(B_i)$, $\mathfrak{P}(C_i)$, observe that it is a finite union of prime ideals by Theorem 80, and employ Theorem 81 to get the desired element z. Perhaps a neater alternative is to form the direct sum

$$D = B_1 \oplus \cdots \oplus B_n \oplus C_1 \oplus \cdots \oplus C_n$$

and deduce $I \not\subset \mathfrak{P}(D)$ from Theorem 82. It then suffices to take $z \in I$, $z \notin \mathfrak{P}(D)$.

In any event the resulting element z is a non-zero-divisor on B_n, while x_n constitutes a maximal R-sequence on B_n. By the case $n = 1$, z is also a maximal R-sequence on B_n. Now the fact that z is not a member of any of $\mathfrak{P}(B_{n-1})$, $\mathfrak{P}(B_{n-2})$, $\ldots$, $\mathfrak{P}(B_1)$, together with Theorem 118, allows us to push z ahead of the x's one step at a time till we reach the conclusion that $z, x_1, \ldots, x_{n-1}$ is an R-sequence on A. Evidently it is a maximal R-sequence on A. In exactly the same way, we have that $z, y_1, \ldots, y_{n-1}$ is an R-sequence on A but we do not yet know it to be maximal. Now we pass to the module A/zA on which we have two R-sequences of length $n - 1$: $x_1, \ldots, x_{n-1}$ and $y_1, \ldots, y_{n-1}$, the first of which we know to be maximal. By our inductive assumption we deduce that $y_1, \ldots, y_{n-1}$ is a maximal R-sequence on A/zA, which in turn implies that $y_1, \ldots, y_{n-1}, z$ is a maximal R-sequence on A. By another application of the case $n = 1$, we reach the desired conclusion that $y_1, \ldots, y_{n-1}, y_n$ is a maximal R-sequence on A. This concludes the proof of Theorem 121.

Remark. This proof is due to Northcott and Rees [40]. The appendix to this section presents an alternative homological proof, due in essence to Rees [43].

Definition. Let R be a Noetherian ring, I an ideal in R, A a finitely generated R-module satisfying $IA \neq A$. The common length of all maximal R-sequences in I on A is called the grade of I on A and written $G(I, A)$.

Remarks. 1. $G(I, A)$ could at least be defined without finiteness assumptions. It might be infinite, and we would have to cope with the possible existence of maximal R-sequences of different lengths. But there are so few theorems on non-Noetherian grade available as yet that introduction of the general notion does not seem to be warranted. Note that the "grade one" terminology used in §2-3 is, for Noetherian rings, in agreement with the present definition.

2. In the original terminology of Auslander and Buchsbaum, the designation was "codimension" of I on A. The sense in which grade is complementary to some kind of dimension can only be revealed later when the homological invasion is in full swing (see Theorem 173). It is sometimes suggestive, sometimes misleading, to think of grade as complementary to dimension. On the whole, the "grade" terminology (due to Rees) seems preferable. *Note:* the French school has introduced "profondeur," translated as "depth."

3. Two cases are specially important. If $A = R$ we call $G(I, R)$ simply the grade of I and write it $G(I)$. Note that this is defined for any ideal I different from R and that $G(I)$ is the maximal length of an R-sequence in I. On the other hand, if R is a local ring with maximal ideal M, and A is any non-zero finitely generated R-module, we call $G(M, A)$ simply the grade of A and write it $G(A)$. Note that $G(A)$ is defined since $MA \neq A$ by the Nakayama lemma. (There is a possible ambiguity in the notation $G(I)$ since we might mean $G(I, R)$ or $G(M, I)$; it should however always be clear from the context which is intended.)

4. When R is local it is reasonable to write $G(R)$ for $G(M, R)$ and call it simply the grade of the ring. We shall do so systematically, but we shall avoid using the symbol $G(R)$ if R is not local.

For ease of reference we record explicitly a simple result.

Theorem 122. Let I be an ideal in a Noetherian ring R, A *a finitely* generated R-module with $IA \neq A$. Then I can be embedded *in* a prime ideal P satisfying $G(P, A) = G(I, A)$.

Proof. Let $x_1, \ldots, x_k$ be a maximal R-sequence in I on A, and write $J = (x_1, \ldots, x_k)$. Then $I \subset \mathfrak{Z}(A/JA)$. We enlarge I to a maximal prime ideal P of the module A/JA. Then P contains the annihilator of A, and it follows readily from Theorem 76 that $PA \neq A$. Thus $G(P, A)$ is defined, and evidently it is equal to $\boldsymbol{k}$.

We interpolate at this point a theorem that was promised in the preceding section.

Theorem **123.** *Let* R *be a Noetherian domain. Then the representation given in Theorem* **53** *(i.e., the expression* $R = \bigcap R_P$, P *ranging over the maximal primes of non-zero principal ideals) is locally finite.*

Proof. Given an element x in R, not 0 and not a unit, we must show that x lies in only a finite number of the P's in question. Now a typical ideal P is a maximal prime, say of (y). Then y is a maximal R-sequence in P, and it follows from Theorem 121 (just the case $n = 1$ is needed) that x is a maximal R-sequence in P, i.e., $P \subset \mathfrak{Z}(R/(x))$. Moreover, since the same argument is applicable to any prime ideal containing P, it follows further that P is a maximal prime of (x). By Theorem 80 there are only a finite number of maximal primes of (x); this proves the present theorem.

We proceed to a result we call the "generalized unmixedness theorem." Actually we prove two such theorems, a first (Theorem 125), which is valid globally, and a second (Theorem 129), which only holds locally but is slightly stronger.

The next preparatory theorem is due to **E.** Davis.

Theorem **124.** *Let* $P_1, \ldots, P_n$ *be prime ideals in a commutative ring* R, *let* I *be an ideal in* R, *and* x *an element of* R *such that* $(x, I) \not\subset P_1 \cup \cdots \cup P_n$. *Then there exists an element* $i \in I$ *such that* $x + i \notin P_1 \cup \cdots \cup P_n$.

Proof. We may assume that no two of the P's are comparable, for any P_k contained in another can simply be deleted without changing the problem. Suppose for definiteness that x lies in $P_1, \ldots, P_r$, but not in any of $P_{r+1}, \ldots, P_n$. (The extreme cases $r = 0$ and $r = n$ are admitted;

if $r = 0$, $i = 0$ will do, and if $r = n$ the following proof applies with the simplification that y can be taken as 1.) We have $I \not\subset P_1 \cup \ldots \cup P_n$, for otherwise $(x, I) \subset P_1 \cup \cdots \cup P_r$ contrary to hypothesis. There exists an element $i_0 \in I$ not lying in any of $P_1, \ldots, P_r$. Next we select y in $P_{r+1} \cap \cdots \cap P$, but *not* in $P_1 \cup \cdots \cup P_r$. Such a selection is possible, for otherwise $P_{r+1} \cap \cdots \cap P \subset P_1 \cup \ldots \cup P_n$, whence by Theorem 81, $P_{r+1} \cap \cdots \cap P \subset P_j$ for some j $(1 \leqq j \leqq r)$, and $P_k \subset P_j$ $(r+1 \leqq k \leqq n)$ for some k, a contradiction. The element $i = yi_0$ then fulfills *our* requirements.

Theorem 125. *Let* R *be Noetherian, A a finitely generated R-module, J an ideal in* R *that can be generated by k elements. Assume* $JA \neq A$. *Then:*

(a) $G(J, A) \leqq k$;

(b) If $G(J, A) = k$, *then J can be generated by k elements forming an R-sequence on A.*

Proof. Write $J = (x_1, \cdots, x_k)$. We shall find elements

$$u_1 = x_1 + (\text{linear combination of } x_2, \ldots, x_k),$$
$$u_2 = x_2 + (\text{linear combination of } x_3, \ldots, x_k), \ldots$$

constituting a sort of triangular change of basis, such that the u's form an R-sequence on A. We do this by repeated applications of Theorem 124.

The theorem being presumably vacuous for $\boldsymbol{k} = 0$, we assume $\boldsymbol{k} > 0$. If $G(J, A) = 0$, no further proof is needed. So we assume $J \not\subset \mathfrak{Z}(A)$. We apply Theorem 124 with $x = x_1$, $I = (x_2, \cdots, x_k)$ and $P_1 \cup \cdots \cup P_n = \mathfrak{Z}(A)$. With i the element furnished by Theorem 124, we set $u_1 = x_1 + i$. If $G(J, A) = 1$, we are through. So we assume $J \not\subset \mathfrak{Z}(A/u_1A)$. From this it follows that $(x_2, \ldots, x_k) \not\subset \mathfrak{Z}(A/u_1A)$. For suppose the contrary. An arbitrary element j of J can be written as

$$j = a_1x_1 + a_2x_2 + \cdots + a_kx_k \qquad (a, \in \mathrm{R})$$

and this can be rewritten as

$$j = a_1u_1 + b_2x_2 + \cdots + b_kx_k \qquad (b, \in \mathrm{R})$$

Since a_1u_1 annihilates A/u_1A and $b_2x_2 + \cdots + b_kx_k$ is a zero-divisor on A/u_1A, we get $j \in \mathfrak{Z}(A/u_1A)$, i.e., $J \subset \mathfrak{Z}(A/u_1A)$. This contradiction shows that $(x_2, \ldots, x_k) \not\subset \mathfrak{Z}(A/u_1A)$. We now apply Theorem 124 with $x = x_2$, $I = (x_3, \ldots, x_k)$, and $P_1 \cup \cdots \cup P_n = \mathfrak{Z}(A/u_1A)$, and if i is the resulting element, we set $u_2 = x_2 + i$. We continue in this fashion as long

as possible. The process terminates in one of two ways: either $G(J, A) < k$; or if $G(J, A) = k$, the elements $u_1, \ldots, u_k$ exhaust J. This completes the proof of Theorem 125.

Theorem 126. *Let* R *be a Noetherian ring, A a finitely generated non-zero R-module, x an element in the radical of* R *but not in $\mathcal{Z}(A)$. Let I be an ideal in* R *contained in $<(A)$. Then: $(I, x) \subset \mathcal{Z}(A/xA)$.*

Proof. Since x annihilates A/xA, the conclusion really just states $I \subset \mathcal{Z}(A/xA)$. Let S be the submodule of A annihilated by I. By Theorem 82, $S \neq 0$. If $S \not\subset xA$, we are through, for the image of S in A/xA will be non-zero and annihilated by I. So suppose on the contrary that S is contained in xA. Any $s \in S$ can then be written $s = xa$, $a \in A$. We have $Ixa = Is = 0$. Since $x \notin \mathcal{Z}(A)$, this implies $la = 0$, $a \in S$. Hence $S = xS$. But then $S = 0$ by the Nakayama lemma (Theorem 78), a contradiction.

Remark. This proof is really the same as that of Theorem 119. We have given it twice for expository reasons.

Theorem 127. *Let* R *be a Noetherian ring, I an ideal in* R, *x an element of* R, *and $J = (I, x)$. Let A be a non-zero finitely generated R-module. Assume that J is contained in the radical of* R. *Then:*

$$G(J, A) \leqq 1 + G(I, A).$$

Proof. Let $G(I, A) = m$ and let $x_1, \ldots, x_m$ be a maximal R-sequence in I on A. We switch the scene of action to the module $A/(x_1, \ldots, x_m)A$. After a change of notation we may thus assume $G(I, A) = 0$, and we have to prove that $G(J, A) \leqq 1$. Of course, if $J \subset \mathcal{Z}(A)$ there is nothing to prove. So we assume that J contains a non-zero-divisor on A, and now we have to prove that $G(J, A) = 1$. If $<(A) = P_1 \cup \cdots \cup P_s$, then the hypotheses of Theorem 124 are fulfilled, and we have that $x + i \notin \mathcal{Z}(A)$ for some $i \in I$. We might as well replace $x + i$ by x. Now we have $x \notin \mathcal{Z}(A)$. To see that $G(J, A) = 1$ it remains to verify

$$J \subset \mathcal{Z}(A/xA).$$

This is asserted by Theorem 126.

By a slight variant of the proof of Theorem 127, we can prove the following useful result.

Theorem 128. *Let* R *be a local ring with maximal ideal M. Let I be an ideal in* R, *$I \subset M$, and let A be a finitely generated non-zero R-module. Assume $G(I, A) < G(M, A)$. Then there exists a prime ideal P with $G(P, A) = 1 + G(I, A)$ and such that $P \supset I$.*

Proof. Let $x_1, \ldots, x_k$ be a maximal R-sequence on A contained in I, and write $J = (x_1 \ldots, x_k)$. Since $G(M, A) > k$, there exists in M an element y with $y \notin \mathcal{Z}(A/JA)$. Then $G((I, y), A) \geqq k + 1$. By Theorem 126 or Theorem 127, $G((I, y), A) = k + 1$. We quote Theorem 122 to enlarge (I, y) to the desired prime ideal P.

Theorem 129. *Let* R *be a Noetherian ring, let $I = (x_1, \ldots, x_k)$ where the x's lie in the radical of* R, *and let A be a finitely generated non-zero R-module. Then $G(I, A) = n$ if and only if the elements $x_1, \ldots, x_k$ constitute an R-sequence on A.*

Proof. The "if" part is obvious. We prove the "only if" part by induction on n. Write $J = (x_1, \ldots, x_{n-1})$. If $G(J, A) < n - 1$, then by Theorem 127, $G(I, A) < n$. Hence $G(J, A) = n - 1$. By our inductive assumption, $x_1, \ldots, x_{n-1}$ is an R-sequence on A. It remains to see that $x_n \notin \mathcal{Z}(A/JA)$. But the contrary assumption leads to $I \subset \mathcal{Z}(A/JA)$, so that $x_1, \ldots, x_{n-1}$ is a maximal R-sequence in I on A, in contradiction to $G(I, A) = n$.

The strengthened form we obtained in passing from Theorem 125 to Theorem 129 really requires that the x's be in the radical — see Ex. 7. Note also that in proving Theorem 129 we have furnished an alternative proof of Theorem 119.

We have referred to Theorems 125 and 129 as "generalized unmixedness theorems" but there is no sign yet of anything being unmixed. An explanation is overdue.

Let I be an ideal in a Noetherian ring R. I has a certain grade, say k. Let $P_1, \ldots, P_s$ be the maximal primes of I, that is, $\mathcal{Z}(R/I) = P_1 \cup \cdots \cup P_s$, and the P_i's are maximal within $\mathcal{Z}(R/I)$. Any ideal containing I has grade $\geqq k$; this is in particular true of the P_i's. Simple examples show that some or all of the P_i's can indeed have a grade exceeding k. In the favorable case where they all have grade k, we call I *grade-unmixed.*

Suppose I is generated by an R-sequence $x_1, \ldots, x_k$. Then for a

maximal prime P_i belonging to I we have that $x_1, \ldots, x_k$ is a maximal R-sequence in P_i. Hence $G(P_i) = k$ and Z is grade-unmixed.

We return to Theorem **125,** and simplify the discussion by dropping the module A, or more precisely, by replacing it by R. We may state:

Theorem 130. *Let the ideal* Z *in a Noetherian ring have grade k and be generated by k elements. Then* Z *is grade-unmixed.*

In the classical theorem that foreshadowed Theorem **130,** "rank" played the role of "grade." Ideals with rank equal to the number of generators corresponded to varieties defined by the "right number of equations," and the unmixedness of such ideals was a significant simplification.

We proceed to build a bridge between the grade and rank versions of unmixedness. The first thing that needs to be done is to define the rank of a general ideal (so far we have defined it only for prime ideals).

Definition. In any commutative ring R the rank of an ideal Z is the minimum of rank(P), P ranging over the prime ideals containing Z. Equivalently, we can let P range over the minimal prime ideals over Z.

The first result connecting grade and rank (Theorem **132)** is quite easy, as is attested by the fact that it is valid without any chain conditions. An equally easy theorem serves as a prelude.

Theorem 131. *Let* P *be a prime ideal in a commutative ring R, and let* $x \in P$ *be an element lying in no minimal prime ideal of R. Write* $R^* = R/(x)$, $P^* = P/(x)$. *Let the rank of* P^* *in* R^* *be k. Then the rank of P in R is at least* $k + 1$.

Note. If R is a domain, the word "minimal" is meant literally, i. e., $x \neq 0$ is all that is assumed. Observe that the hypothesis on x is fulfilled if x is not a zero-divisor (Theorem **84).**

Proof. We assume k finite (the case k infinite is quite evident). We lift the chain

$$P^* = P_0^* \supset \cdots \supset P_k^*$$

to a chain

$$P = P_0 \supset \cdots \supset P_k \tag{26}$$

of length k descending from P (P_i is the complete inverse image of P_i^*). Since x lies in no minimal prime ideal, the chain **(26)** can be extended at least one more step.

Theorem 132. *If an ideal* Z *in a commutative ring contains an R-sequence of length n, then* $\text{rank}(I) \geqq n$.

Proof. It is evidently harmless to assume that Z is prime, and we accordingly change notation to P. Write $R^* = R/(x_1)$, $P^* = P/(x_1)$. Then P^* contains an R-sequence of length $n - 1$, namely the images of $x_2, \ldots, x_n$. By induction, $\text{rank}(P^*) \geqq n - 1$, and by Theorem **131,** $\text{rank}(P) \geqq n$.

Remark. For an analogue for modules, see Ex. **22.**

Thus rank $\geqq$ grade holds under very general conditions. The two need not be equal; for perhaps as simple a counterexample as any, see Ex. 8. The condition that rank and grade coincide is a significant restriction. Moreover, it is very useful to know that the assumption of equality of grade and rank for maximal ideals implies equality for all ideals. **So** we define Macaulay rings by the weak property, and in Theorem **136** pass to the strong property.

Definition. A ***Macaulay ring*** is a Noetherian ring in which $G(M) = \text{rank}(M)$ for every maximal ideal M.

Remark. In Nagata's terminology **[37,** p. 82] this is a locally Macaulay ring. For a Macaulay ring, Nagata requires in addition that all maximal ideals have the same rank.

Some needed facts about the behavior of grade under localization are presented in the next three theorems. We give a direct proof of Theorem **133,** but it should be noted that the gist of it is that localization preserves exact sequences.

Theorem 133. *Let R be any ring, A a non-zero R-module, and* $x_1, \ldots, x_n$ *an R-sequence on A. Let S be a multiplicatively closed set in R, and denote by* x_i^* *the image of* x_i *in* R_S. *Assume* $(x_1^*, \ldots, x_n^*)A_S \neq A_S$. *Then:* $x_1^*, \ldots, x_n^*$ *is an R-sequence on* A_S.

Proof. We must show that x_i^* is a non-zero-divisor on

$$A_S/(x_1^*, \ldots, x_{i-1}^*)A_S.$$

Suppose that

$$x_i^* b^* = \sum_{j=1}^{i-1} x_j^* a_j^* \tag{27}$$

where $b^*, a_j^* \in A_S$. Say $b^* = b/s$, $a_j^* = a_j/s_j$. We multiply (27) through by $ss_1 \ldots s_{i-1}$ and then return to an equation in A itself (which calls for a further multiplication by an element of S). Change notation by replacing the a's by suitable c's. The result: $s_0 x_i b - \Sigma x_j c_j = 0$ with $s_0 \in S$. By hypothesis $s_0 b \in (x_1, \ldots, x_{i-1})A$. Hence $b^* \in (x_1^*, \ldots, x_{i-1}^*)A_S$, as required.

The precaution we exercised in Theorem 133, by assuming

$$(x_1^*, \ldots, x_n^*)A_S \neq A_S,$$

is really needed, as simple examples show. But let us note a useful case where degeneration is impossible. Let the module be R, let the localization take place with respect to a prime ideal P, and assume $x_1, \ldots, x_n \in$ P. Then the localized module R_P is not 0, and the elements $x_1^*, \ldots, x_n^*$ are non-units in the local ring R_P. Hence the condition needed in Theorem 133 is fulfilled and $x_1^*, \ldots, x_n^*$ is an R-sequence. We deduce:

Theorem 134. ***Let*** R ***be a Noetherian ring,*** P ***a prime ideal in*** R, ***I an ideal in R contained in*** P. ***Then*** $G(I) \leqq G(I_P)$.

We note next that it is possible to localize to preserve the grade of a given ideal.

Theorem 135. ***Let R be a Noetherian ring and I an ideal in*** R, $I \neq$ R. ***Then there exists a maximal ideal M such that*** $G(I) = G(I_M)$.

Proof. Suppose $G(I) = n$, let $x_1, \ldots, x_n$ be a maximal R-sequence in I, and set $J = (x_1, \ldots x_n)$. Then $I \subset \mathcal{Z}(R/J)$ so that (Theorem 82) there exists an element $u \notin J$ with $Iu \subset J$. Let K denote the set of all elements y in R such that $yu \in J$. Then K is an ideal in R containing I and different from R. Embed K in a maximal ideal M. We claim that

$G(I_M) = n$. Theorem **134** asserts that $G(I_M) \geqq n$; indeed the observations above show that the elements $x_1, \ldots, x_n$ map into an R-sequence in R_M contained in I_M. It remains to prove the maximality of this R-sequence, i. e., we must show $\mathbf{I}_M \subset \mathcal{Z}(R_M/J_M)$. If u^* is the image of u in R_M, we have $I_M u^* \subset J_M$. Further $u^* \notin J_M$; for $u^* \in J_M$ implies $su \in J$ for $s \notin M$, whereas $s \in K \subset M$ by the definition of K.

Theorem 136. ***Grade and rank coincide for every ideal in a Macaulay ring.***

Proof. We first note that it is sufficient to prove the theorem for prime ideals. For by the definition of rank we have rank(I) = min rank(P) taken over all prime ideals containing I, and the same is true for grade, by Theorem **122.**

Next we reduce the problem to the local case. Let P be a prime ideal for which we hope to prove grade and rank to be equal. By Theorem 135 there is a maximal ideal M containing P such that $G(P) = G(P_M)$. Furthermore, P and P_M have the same rank. **So** it suffices to prove the equality of grade and rank for P_M. Note that our hypothesis is preserved in the ring R_M, for the grade of M cannot rise in the passage from R to R_M since it must not exceed the rank.

So we now assume R to be local with maximal ideal M. If there exists a prime ideal P with grade less than rank, choose P to be maximal among such. We must have $P \neq M$. Thus rank$(M) >$ rank(P). Since the grade and rank of M coincide, we have $G(M) > G(P)$. By Theorem **128,** P can be enlarged to a prime ideal Q with $G(Q) = 1 + G(P)$. Since rank(Q) necessarily exceeds rank(P), we have rank$(Q) > G(Q)$, a contradiction.

We are in a position to state what might be called the "classical unmixedness theorem." Note that the final statement in Theorem 137 concerning minimality is an immediate consequence, since two comparable prime ideals can have the same rank only if they are equal. In the language of primary decomposition, the ideal I of Theorem 137 has no "embedded" primes.

Theorem 137. ***In a Macaulay ring let I be an ideal of rank n, which can be generated by n elements. Then all maximal primes belonging to I have rank n and are minimal over I.***

In Macaulay rings we can prove that chains of prime ideals behave well. In discussing this we shall find it convenient to introduce a variant of the notion of rank.

Definition. The *little rank* of a prime ideal P is the length of the shortest saturated chain of prime ideals descending from P to a minimal prime ideal. A chain is said to be saturated if no further prime ideals can be inserted.

The first instance where we observe a difference between little rank and rank is illustrated in Fig. 1, where it is to be understood that the

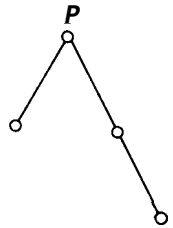


FIGURE 1

indicated chains are saturated, and the bottom prime ideals are minimal. On the assumption that there are no longer chains descending from P, we have little rank$(P) = 1$, rank$(P) = 2$. We shall shortly see that this possibility is excluded in Macaulay rings, but it should be noted that it is not to be regarded as at all pathological; for instance, such behavior is easily exhibited in a suitable homomorphic image of a polynomial ring over a field.

It is a more penetrating question to ask if little rank and rank can differ in a domain. The first possible instance is illustrated in Fig. 2.

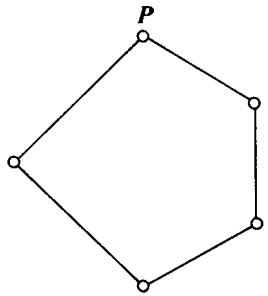


FIGURE 2

Here the chains are again to be saturated, and the bottom prime ideal is 0; assuming again that there are no longer chains descending from P, we have little rank$(P) = 2$, rank$(P) = 3$. For many years it was an open question whether this could happen in a Noetherian ring or, for that matter, in any commutative ring. Then Nagata exhibited an example to show that it could; it appears among his examples of bad behavior at the end of [37].

We shall say that a commutative ring satisfies the *saturated chain condition* if any two saturated chains of prime ideals between two fixed ones have the same length. We leave it to the reader to see that equality of little rank and rank implies the saturated chain condition. More exactly, it is equivalent to the saturated chain condition in the stronger form referred to above: all saturated chains descending from a fixed prime to the bottom have the same length.

The advantage we gain in introducing the little rank is that we are able to prove that

$$\text{grade}(P) \leqq \text{little rank}(P) \tag{28}$$

holds for any prime ideal in *any* Noetherian ring. We can of course lengthen (28) to

$$\text{grade}(P) \leqq \text{little rank}(P) \leqq \text{rank}(P) \tag{29}$$

Now in a Macaulay ring the two end members of (29) are equal, trapping the little rank between them.

Theorem 138. *For any prime ideal* P *in any Noetherian ring* R, $G(P) \leqq$ *little rank*(P).

Proof. If this is false, take P to be an offender. We can harmlessly pass from R to R_P, for the little rank of P will remain the same, while the grade can only go up, increasing the offense. So we can start over with R local, M its maximal ideal, and $G(M) >$ little rank$(M) = n$, say. We can find a prime ideal Q directly underneath M with little rank$(Q) = n - 1$. We make an induction on the little rank, the case of little rank 0 being immediate. So we have $G(Q) \leqq n - 1$. But then there is a jump of at least two from $G(Q)$ to $G(M)$, contrary to Theorem 128.

We wind up this section with three theorems concerning the stability of the Macaulay property. Three others (Theorems 151, 156, and 157) have to await the principal ideal theorem.

Theorem 139. *If is Macaulay and* S *a multiplicatively closed set in* R, *then* R_S *is Macaulay.*

Proof. Given a maximal ideal N in R_S we must show that its grade and rank are equal. Now N has the form P_S with P maximal within the complement of S. We have $G(P) = \text{rank}(P)$ by Theorem **136** and we know $\text{rank}(P) = \text{rank}(P_S)$. In going from P to P_S the grade can only go up, but $G(P_S)$ cannot exceed $\text{rank}(P_S)$. Hence they are equal.

Theorem **140.** *Let* R *be Noetherian and assume* R_M *Macaulay for every maximal ideal* M. *Then* R *is Macaulay.*

Proof. Our hypothesis tells us that the grade and rank of M_M are equal, say to n. $\text{Rank}(M)$ is this same number n, and so is $G(M)$, for by Theorem **135,** $G(M) = G(M_M)$.

Theorem **141.** *Let* x *be a non-zero-divisor in a Macaulay ring* R. *Then* $R^* = R/(x)$ *is a Macaulay ring.*

Proof. Given a maximal ideal M^* in R*, we must prove its grade and rank to be equal. Now M^* has the form $M/(x)$ with M maximal in R, and we know the grade and rank of M to be equal. Furthermore $G(M) = 1 + G(M^*)$, for we may begin a maximal R-sequence in M with x. As for rank, we have $\text{rank}(M) \geqq 1 + \text{rank}(M^*)$ by Theorem **131;** but inequality cannot be tolerated here, for it would make the rank of M^* fall below its grade.

APPENDIX 3-1.

In this appendix we outline the proof of Theorem 121 that uses homological algebra. We first note a trivial lemma.

Lemma. *Let* C *and* D *be R-modules, and suppose there exists an element* x *in* R *satisfying* $xC = 0$ *and* $x \notin Z(D)$. *Then* $\text{Hom}_R(C, D) = 0$.

Proof. Let f be a homomorphism from C ↄ D. Then for any $c \in C$ we have $0 = f(xc) = xf(c)$, whence $f(c) = 0$.

Theorem. *Let* A *and* B *be R-modules. Assume that the elements* $x_1, \ldots, x$, *in* R *constitute an R-sequence on* A *and that* $(x_1, \ldots, x_n)B = 0$. *Then*

$$\text{Ext}^n_R(B, A) \cong \text{Hom}_R(B, A/(x_1, \ldots, x_n)A)$$

Proof. Since x_1 is a non-zero-divisor on A we have the exact sequence

$$0 \to A \xrightarrow{x_1} A \to A/x_1A \to 0$$

where the indicated map is multiplication by x_1. This yields the exact sequence

$$\text{(30)}\quad \text{Ext}^{n-1}_R(B, A) \to \text{Ext}^{n-1}_R(B, A/x_1A) \to \text{Ext}^n_R(B, A) \xrightarrow{x_1} \text{Ext}^n_R(B, A)$$

Since $x_1B = 0$, the last map in **(30)** is zero. Furthermore, by induction on n,

$$\text{(31)}\qquad \text{Ext}^{n-1}_R(B, A) \cong \text{Hom}(B, A/(x_1, \ldots, x_{n-1})A)$$

The right side of **(31)** vanishes by the lemma, applied with x_n playing the role of x. Hence in **(30)** we can replace both end terms by 0, thus obtaining the isomorphism of the two inner terms. We make a second application of our inductive assumption of the truth of the theorem for $n - 1$, and this completes the proof.

We now apply the theorem to the case where $B = R/I$, where R is Noetherian and I is an ideal in R, $I \neq$ R. The condition

$$\text{(32)}\qquad \text{Hom}_R(R/I, A/(x_1, \ldots, x_n)A) \neq 0$$

is equivalent to the statement that there is a non-zero element of $A/(x_1, \ldots, x_n)A$ annihilated by I, and **(32),** by Theorem **82,** is equivalent to the assertion

$$\text{(33)}\qquad I \subset Z(A/(x_1, \ldots, x_n)A)$$

In the presence of $IA \neq A$, **(33)** says that the R-sequence $x_1, \ldots, x$, on A is maximal within I.

In summary, we arrive at the following homological characterization of $G(I, A)$: it is the smallest integer n such that $\text{Ext}^n_R(R/I, A) \neq 0$.

EXERCISES

1. Let I be an ideal in a domain R. If I contains an R-sequence of length 2, prove that $I^{-1} = R$.

2. Let R be a Noetherian domain, I a non-zero ideal in R. Prove: $I^{-1} = R$ if and only if $G(I) \geqq 2$.

3. Let a, b be an R-sequence in a domain R. Prove that $(a + bx)$ is a prime ideal in $R[x]$. ***(Hint:*** consider the homomorphism $x \to -a/b$. For this exercise and the next two we waive the requirement $(a, b) \neq R$.)

4. Let a, b be elements in a domain R such that $(a + bx)$ is prime in $R[x]$. Prove that a, b is an R-sequence. ***(Hint:*** if $sa = tb$ with t not a multiple of a, observe that $b(t + sx)$ is divisible by $a + bx$.)

5. Prove: in a GCD-domain two elements form an R-sequence if and only if they are relatively prime.

6. Let a, b be an R-sequence in a ring R, and let $y = a + bx$ where x is any element in R. Prove that b maps into a non-zero-divisor in the ring $R/(y)$.

7. (a) Let $R = K[x, y, z]$, K a field. Prove that the elements x, $y(1 - x)$, $z(1 - x)$ form an R-sequence, but in the order $y(1 - x)$, $z(1 - x)$, x they do not.

(b) If I is the ideal generated by $y(1 - x)$ and $z(1 - x)$, prove that $G(I) = 1$, $G(I, x) = 3$. (This shows that radical assumptions cannot be omitted in Theorem 127.)

8. Let K be a field, $R = K[x, y]/(x^2, xy)$. Let M be the image of (x, y) in R. Prove that $G(M) = 0$, $\operatorname{rank}(M) = 1$.

9. Prove: if a ring satisfies the saturated chain condition for prime ideals, so do its homomorphic images.

10. Let $P \subset Q$ be prime ideals in a Macaulay ring. Suppose there is no prime ideal properly between them. Prove: $G(Q) = 1 + G(P)$, $\operatorname{rank}(Q) = 1 + \operatorname{rank}(P)$.

11. If $x_1, \ldots, x_r$ is an R-sequence on the module A, prove that $x_i \notin \mathcal{Z}(A/(x_1, \ldots, \hat{x}_i, \ldots, x_n)A)$.

12. Let A be a non-zero module over a commutative ring R, and let $x_1, \ldots, x_n$ be elements of R. Suppose $x_i = ab$.

(a) If $x_1, \ldots, x_{i-1}, a, x_{i+1}, \ldots, x_n$ and the same sequence with b in place of a are R-sequences on A, prove that $x_1, \ldots, x_i, \ldots, x_r$ is an R-sequence on A.

(b) If $x_1, \ldots, x_i, \ldots, x$, **is** an R-sequence on A and

$$(x_1, \cdots, a, \cdots, x_n)A \neq A,$$

prove that $x_1, \ldots, a, \ldots, x$, **is** an R-sequence on A.

(c) Deduce from (a) and (b) the following: for any integers $k_1, \ldots, k$, the sequence $x_1, \ldots, x_n$ is an R-sequence on A if and only if $x_1^{k_1}, \ldots, x_n^{k_n}$ is an R-sequence on A.

13. Let R be a commutative ring (not necessarily Noetherian), A an R-module. Let $x_1, \ldots, x_m$ be an R-sequence on A, and write

$$I = (x_1, \ldots, x_m).$$

(a) Prove that $\mathcal{Z}(A/I^nA) = \mathcal{Z}(A/IA)$ for any n.

(b) Prove that $I^nA/I^{n+1}A$ is isomorphic to a direct sum of copies of A/IA.

14. Let R be a Noetherian ring,

$$0 \to A \to B \to C \to 0$$

a short exact sequence of R-modules. Let I be an ideal in R with $IA \neq A$, $IB \neq B$, $IC \neq C$. Prove:

(1) If $G(I, B) < G(I, C)$, then $G(I, A) = G(I, B)$;
(2) If $G(I, B) > G(I, C)$, then $G(I, A) = G(I, C) + 1$;
(3) If $G(I, B) = G(I, C)$, then $G(I, A) \geqq G(I, B)$.

(Hint: if $G(I, B)$ and $G(I, C)$ are both positive we can find in I a non-zero-divisor x on both B and C; the sequence

$$0 \to A/xA \to B/xB \to C/xC \to 0$$

is still exact and all grades are down by 1. So assume $G(I, B)$ or $G(I, C)$ zero. If $G(I, B) = 0$, $Ib = 0$, either $b \in A$ or b maps onto a non-zero element of C, falling under (1) or (3). If $G(I, C) = 0$, $Ic = 0$, pick $b \to c$, and x in I not a zero-divisor on B. Then $xb \notin xA$, but $Ixb \subset xA$, $G(I, A) = 1$.)

15. Let a, b be elements in a Noetherian UFD, $(a, b) \neq R$. Prove that any maximal prime of (a, b) has grade $\leqq 2$.

16. Let R be a DVR with maximal ideal (p). Let $T = R[x]$, x an indeterminate. Show that x, p is a maximal R-sequence in T, and that the single element $1 - px$ is also a maximal R-sequence in T. (This example shows that the condition $IA \neq A$ cannot be omitted in Theorem 121.)

17. (This exercise shows that Theorem 124 cannot be extended to an infinite union of prime ideals.) In the ring of integers let $x = 3$, $I = (5)$ and let P_i range over all prime ideals. Prove that $(x, I) \not\subset \bigcup P_i$, but that for every $i \in I$, $x + i \in \bigcup P_i$.

18. Let R be a Macaulay ring. Let T be a ring containing R, and suppose that as an R-module it is free and finitely generated. Prove that T is a Macaulay ring.

19. Let P be a prime ideal in a Macaulay ring R, let x be any element not in P such that (x, P) $\neq$ R, and let Q be a minimal prime ideal over (x, P). Prove that $\operatorname{rank}(Q) = 1 + \operatorname{rank}(P)$. Deduce that there are no prime ideals properly between P and Q.

20. Let R be a valuation ring, A an R-module. Prove that R cannot contain an R-sequence of length 2 on A.

21. Let R be local, let A be a finitely generated non-zero module, let P be a maximal prime of A, and write k for the Krull dimension of R/P. Prove: $G(A) \leqq k$. *(Hint:* the case $G(A) = 0$ is trivial. For $G(A) > 0$ take $x \notin \mathcal{Z}(A)$. By Theorem 126, $(P, x) \subset \mathcal{Z}(A/xA)$. Enlarge (P, x) to a maximal prime of A/xA and use induction on $G(A)$.)

22. Let R be an n-dimensional ring (not necessarily Noetherian). Let A be an A-module. Prove that R cannot contain an R-sequence on A of length $n + 1$. *(Hint:* we can assume A faithful. If x starts an R-sequence on A, then x is not in any minimal prime ideal. Pass to $R/(x)$ and A/xA.)

23. Let $x_1, \ldots, x_n$ be an R-sequence in a Noetherian ring. Prove that the ideal $(x_1, \ldots, x)$ can be generated by n elements that form an R-sequence in any order. *(Hint:* change $x_2, \ldots, x_n$ successively, making appropriate use of Theorems 118 and 124.)

24. Let R be a local Macaulay ring with maximal ideal M, and let I be an ideal generated by a maximal R-sequence. Let J be the set of all x in R with $Mx \subset I$. Prove that the dimension of J/I, as a vector space over R/M, is independent of the choice of I. *(Hint:* deduce this from the theorem in the appendix.)

25. Prove that any integrally closed Noetherian domain of dimension $\leqq 2$ is Macaulay.

3-2 THE PRINCIPAL IDEAL THEOREM

The principal ideal theorem of Krull is probably the most important single theorem in the theory of Noetherian rings. Its statement is as follows:

Theorem 142. *Let x be a non-unit in a Noetherian ring and* P *a prime ideal minimal over* (x). *Then the rank of* P *is at most 1.*

The proof we give is adapted from a brilliant note of Rees [42]. This is the note that introduced the Artin-Rees lemma, at about the same time as unpublished lectures of Artin. We are, so to speak, using the underlying idea but not the Artin-Rees lemma itself.

As a prelude to Theorem 142, we isolate a preparatory result. Its effect is to show, under the stated hypothesis, that the module $(u, y)/(u^2)$ and its submodule $(u^2, y)/(u^2)$ are "piecewise isomorphic," as illustrated in Fig. 3.

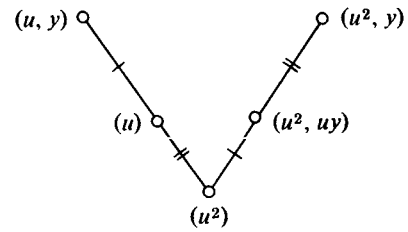


FIGURE 3

Theorem 143. *Let u, y be non-zero elements in an integral domain. Then:*

(a) The modules $(u, y)/(u)$ and $(u^2, uy)/(u^2)$ are isomorphic.

(b) Assume further that $tu^2 \in (y)$ implies $tu \in (y)$. Then the modules $(u)/(u^2)$ and $(u^2, y)/(u^2, uy)$ are isomorphic.

Proof. (a) Multiplication by u induces a module isomorphism of (u, y) onto (u^2, uy), sending the kernel (u) onto the kernel (u').

(b) The module $(u)/(u^2)$ is of course cyclic, with annihilating ideal (u). The module $(u^2, y)/(u^2, uy)$ is also cyclic, for the generator u^2 is superfluous. Moreover the annihilator contains u. It remains to prove that the annihilator is exactly (u). That is, from

$$ky = au^2 + buy \tag{34}$$

we must deduce $k \in (u)$. Now (34) gives us $au^2 \in (y)$ so that by hypothesis, $au \in (y)$, say $au = cy$. Then (34) can be rewritten

$$ky = cuy + buy \tag{35}$$

In (35) we can cancel y, and we find $k \in (u)$, as required.

Before presenting the proof of Theorem 142, we remark that if we assume P to be actually principal, instead of minimal over a principal

ideal, the result is a good deal easier. It is so easy in fact that we were able to place it as Ex. **5** in §1-1 (note also the refinement in Theorem **163).**

Proof of Theorem 142. We assume that, on the contrary, there is a chain $P \supset P_1 \supset P_2$ of distinct prime ideals (see Fig. 4). We make two

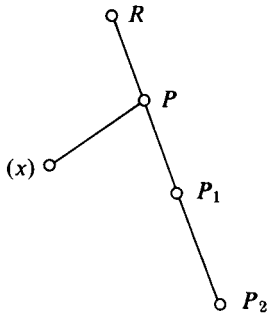


FIGURE 4

successive reductions. First we pass to the integral domain R/P_2; the image of P is still minimal over the image of (x) and has rank $\geqq 2$. Then we localize the integral domain R/P_2 with respect to the image prime ideal P/P_2; again minimality and rank are preserved.

Let us start the notation fresh after these reductions. We have a local domain R with maximal ideal M, a non-zero element x such that M is a minimal prime ideal over (x), and a non-zero prime ideal Q properly contained in M. We shall find this setup to be impossible.

Select a non-zero element y in Q. Let I_k denote the ideal of all elements t with $tx^k \in (y)$. Evidently $I_1 \subset I_2 \subset \cdots$ is an ascending chain of ideals, which must become stable, say at I_n. Then $tx^{2n} \in (y)$ implies $tx^n \in (y)$. Set $u = x^n$; then we have $tu^2 \in (y)$ implies $tu \in (y)$.

The ring $T = R/(u^2)$ has exactly one prime ideal. Hence (Theorem 89) any finitely generated T-module has finite length. This applies in particular to the module $(u, y)/(u^2)$, which is an R-module annihilated by u^2, and thus at our pleasure a T-module. It follows from Theorem 143 that its submodule $(u^2, y)/(u^2)$ has the same length. This is possible only if $(u, y) = (u^2, y)$, i. e. $u \in (u^2, y)$, say $u = cu^2 + dy$. Since $1 - cu$ is a unit (u is a non-unit in the local ring R) we deduce $u \in (y) \subset$ Q. But M is minimal over (x) and hence also minimal over $(u) = (x^n)$. This contradiction completes the proof of Theorem 142.

Very shortly we shall subject the principal ideal theorem to two successive improvements. But we pause at this point to give a number of immediate applications. First we prove the theorem on prime ideals that was promised in §1-1.

Theorem 144. ***Let $P \subset$ Q be prime ideals in a Noetherian ring. If there exists a prime ideal properly between them, then there are infinitely many.***

Proof. It is harmless to pass to R/P, so we assume $P = 0$. Suppose that $P_1, \ldots, P_n$ are the sole prime ideals properly between 0 and Q. By Theorem 81 we cannot have $Q \subset P_1 \cup \cdots \cup P_n$. **So** we may pick $x \in$ Q, $x \notin$ any P_i. Then Q is minimal over (x). Theorem 142 now furnishes a contradiction, for the existence of at least one prime ideal between 0 and Q makes $\operatorname{rank}(Q) \geqq 2$.

To get ready for Theorem 146 we note an easy application of Theorem 88.

Theorem 145. ***Let* R *be an integral domain satisfying the ascending chain condition on radical ideals. Suppose* R *has an infinite number of minimal prime ideals (i. e. prime ideals of rank* 1*). Then their intersection is 0.***

Proof. If x is a non-zero element lying in all prime ideals P_i of rank 1, then each P_i is minimal over x, contradicting Theorem 88.

We determine which G-domains are Noetherian.

Theorem 146. ***A Noetherian domain* R *is a G-domain if and only if $\dim(R) \leqq 1$ and* R *has only a finite number of maximal ideals (or equivalently, prime ideals).***

Proof. Half the theorem is covered by **Ex.** 3 in §1-3. Conversely, suppose that R is a G-domain. Then (Theorem 19) the intersection of the non-zero prime ideals in R is non-zero. Hence (Theorem 145) R has only a finite number of minimal prime ideals, and Theorem 144 then tells us $\dim(R) \leqq 1$, so that there are only a finite number of prime ideals in all.

We can also determine when a Noetherian ring R is a Hilbert ring. In the first place (Ex. 4 in §1-3) it is necessary, whether or not R is Noetherian, that every homomorphic image of R of dimension $\geqq 1$ have an infinite number of maximal ideals. This condition is in fact sufficient for Noetherian rings. In Theorem 147 we prefer to state it in a form that is formally weaker, but obviously equivalent.

Theorem **147.** *A necessary and sufficient condition for a Noetherian ring* R *to be a Hilbert ring is the following: for every prime ideal P such that* $\dim(R/P) = 1$, *there must exist infinitely many maximal ideals containing P.*

Proof. Our problem is to show that any G-ideal P is maximal. Now R/P is a G-domain, so by Theorem 146 the dimension of R/P is at most 1, and there are only finitely many maximal ideals containing P. But then our hypothesis tells us that P must be maximal.

As Krull remarks in [27], Theorem 147 deflates the significance for Noetherian rings of the Hilbert ring axiom down to the mere distinction between finite and infinite.

We proceed to the Noetherian improvement on Theorem 38; in the language used in Theorem 39, we are proving that Noetherian rings are S-rings (and hence also strong S-rings).

Theorem 148. *Let R be a Noetherian domain and P a minimal prime ideal in R. Let* $P^* = PR[x]$ *be the expansion of P to the polynomial ring* $R[x]$. *Then* P^* *is a minimal prime ideal in* $R[x]$.

Proof. Let c be any non-zero element in P. Then P is minimal over cR. We claim that P^* is likewise minimal over $cR[x]$; if sustained, this claim and Theorem 142 finish the proof. Suppose that $P^* \supset Q \supset cR[x]$. Then $Q \cap R$ *is* a prime ideal in R containing c and contained in P. Hence $Q \cap R = P$ and $Q = P^*$.

For convenience of reference we record the result of combining Theorems 148 and 39.

Theorem 149. *Let* R *be a Noetherian ring, P a prime ideal in R,* $\mathrm{rank}(P) = n$. *Denote by* $P^* = PR[x]$ *the expansion of P to* $R[x]$, *and let*

$Q \neq P^*$ *be a prime ideal in* $R[x]$ *with* $Q \cap R = P$. *Then:* $\mathrm{rank}(P^*) = n$, $\mathrm{rank}(Q) = n + 1$.

We note at this point an application to polynomial rings. Let K be any field, and let $R = K[x_1, \ldots, x_n]$ where the x's are indeterminates. Let M be a maximal ideal in R. We know that the contraction N of M to $K[x_1, \ldots, x_{n-1}]$ is maximal, and that M lies properly above NR. By induction, we may assume $\mathrm{rank}(N) = n - 1$. By Theorem 149, $\mathrm{rank}(M) = n$. Thus: *every maximal ideal* in $K[x_1, \ldots, x_n]$ *has rank n.* (For generalizations, see Exs. 3 and **4.)**

The next application we make of Theorem 142 is to show that the Macaulay property is inherited by polynomial rings. We first need a remark about polynomial rings; its very simple proof was shown me by J. Shamash.

Theorem 150. *Let* R *be any commutative ring, and M a maximal ideal in the polynomial ring* $R[x]$. *Then M cannot consist entirely of zero-divisors.*

Proof. Assume the contrary. Then $x \notin M$ since x is not a zero-divisor. Hence $(x, M) = R[x]$ and we may write $1 = xf + g$ with $f \in R[x]$ and $g \in M$. But clearly $g = 1 - xf$ cannot be a zero-divisor.

Theorem 151. R *is a Macaulay ring if and only if* $R[x]$ *is a Macaulay ring.*

Proof. Suppose R *is* Macaulay. For M a maximal ideal in $R[x]$ we must show the equality of the grade and rank of M. Let $M \cap R = P$. Then, since R is a Macaulay ring, $G(P) = \mathrm{rank}(P) = n$, say. We know that $M \neq PR[x]$; hence (Theorem 149) $\mathrm{rank}(M) = n + 1$. We shall prove $G(M) \geqq n + 1$; since the grade can never exceed the rank this will prove the theorem. Let $x_1, \ldots, x_n$ be a maximal R-sequence in P. It is evident that it remains an R-sequence when considered in the ring $R[x]$. We employ the usual device of dividing both rings by the ideal $(x_1, \ldots, x_n)$; this depresses the grade of M by n. Our problem now is to show $G(M) \geqq 1$, i. e., that M does not consist entirely of zero-divisors. We quote Theorem 150.

Conversely, if $R[x]$ is Macaulay, *so* is R; this is a special case of Theorem 141.

Of course we can iterate Theorem 151 to obtain the same result with several indeterminates. In particular: *if K is a field, and $R = K[x_1, \ldots, x_n]$ with the x's indeterminates, then R is a Macaulay ring.* If we combine the resulting equal chain condition with the fact that any maximal ideal in R has rank n, we obtain a very satisfactory picture of the prime ideals in R: every saturated chain of prime ideals running from the top to the bottom has length n. If the prime ideal P has rank r, then any saturated chain descending from P to 0 has length r, and any saturated chain ascending from P to a maximal ideal has length $n - r$. In §1-6 we called $n - r$ the corank of P. Algebraic geometers call $n - r$ the *dimension* of the variety attached to P, and they identify it with the transcendence degree of R/P over K (for a generalization see Ex. 5).

In this context it is worth noting a corollary of the principal ideal theorem. Let P again have rank r in $R = K[x_1, \ldots, x_n]$ and let f be an element in $R, f \notin P, (P, f) \neq R$. Let Q be a prime ideal minimal above (P, f). The principal ideal theorem tells us that Q lies directly above P. Because of the equal chain condition, we can state $\operatorname{rank}(Q) = r + 1$.

Let K be algebraically closed and let us pass to the geometric language. The preceding result may be stated as follows: let V be an irreducible variety of dimension d, and let W be an irreducible variety of codimension 1 (a *hypersurface*). Suppose that $V \cap W$ is non-empty and that $V \not\subset W$. Then every component of $V \cap W$ has dimension $d - 1$. (See, for instance, Theorem 11 on page 36 of [28].) From this, one passes to the full intersection theorem, given in the corollary on page 38 of [28], by the device of introducing the product of the two varieties and intersecting it with the diagonal.

Theorem 152 provides the first of two successive improvements on Theorem 142, the principal ideal theorem. The proof of Theorem 152 embodies a simplification, due to Akizuki, of Krull's original proof.

Theorem 152. (*Generalized principal ideal theorem.*) *Let R be a Noetherian ring and let $\mathfrak{Z} \neq R$ be an ideal generated by n elements $a_1, \ldots, a_n$ in R. Let P be a prime ideal in R minimal over $\mathfrak{Z}$. Then: rank$(P) \leqq n$.*

Proof. By the device of passing to R_P we may assume that R is local, with P as its unique maximal ideal.

Suppose on the contrary that there exists a chain $P = P_0 \supset P_1 \supset \cdots \supset P_{n+1}$ of length $n + 1$. Here we may assume that there is no prime ideal properly between P_1 and P. We cannot have $\mathfrak{Z} \subset P_1$, for this would contradict the minimality of P over $\mathfrak{Z}$. Say for definiteness that $a_1 \notin P_1$.

Then (a_1, P_1) contains P_1 properly and P is therefore the only prime ideal containing (a_1, P_1). In other words, in the ring $R/(a_1, P_1)$ the image of P is the unique prime ideal and hence (Theorem 25) is nilpotent. This means that some power of P lies in (a_1, P_1). By choosing t sufficiently large we can arrange

$$a_i^t = c_i a_1 + b_i, \qquad (c_i \in R,\ b_i \in P_1,\ i = 2, \ldots, n)$$

Let $J = (b_2, \ldots, b_n)$ and note that J is contained in P_1. Since the rank of P_1 exceeds $n - 1$ we have, by induction on n, that P_1 properly contains a prime ideal Q that contains J (see Fig. 5). The ideal (a_1, Q) contains

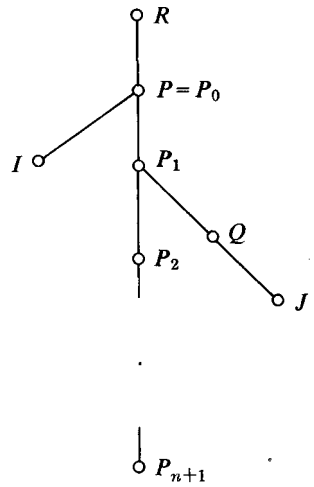


FIGURE 5

some power of each of the a's. It follows, by the minimality of P, that P is the only prime ideal containing (a_1, Q). We now pass to the ring R/Q, using * for the homomorphic images of elements or ideals. We have that P^* is minimal over (a_1^*), but there is a chain of length 2, namely $P^* \supset P_1^* \supset 0$, descending from P^*. This contradicts Theorem 142.

Remarks. 1. A naive proof, simply iterating Theorem 142, leads to the result that the little rank of P is at most n. So this is valid if we weaken the Noetherian assumption on R to the hypothesis that every homomorphic image of R satisfies the principal ideal theorem. But as a matter of fact, a small rearrangement of the proof of Theorem 152 gives the full result from the weaker hypothesis (see Ex. 6).

2. There is an interesting application of Theorem 152 to polynomial equations. Let K be algebraically closed, and let $R = K[x_1, \ldots, x_n]$ with the x's indeterminates. Let $I \neq R$ be generated by $n - 1$ polynomials $f_1, \ldots, f_{n-1}$. Then by Theorem 152 any prime ideal P minimal over I has rank $\leqq n - 1$. Since every maximal ideal has rank n, P is not maximal. Hence P is contained *in* an infinite number of maximal ideals (see Theorem 147 and recall that R is a Hilbert ring). In other words, the equations $f_1 = 0, \ldots, f_{n-1} = 0$ have an infinite number of solutions if they have any. A useful alternative way of putting this is to take polynomials $f_1, \ldots, f_{n-1}$ having *no* constant terms. The solution $x_1 = \cdots = x_n = 0$ is dismissed as trivial, and the conclusion we have is that there exist infinitely many non-trivial ones.

Theorem 152 has a useful converse.

Theorem 153. *Let* R *be Noetherian and P a prime ideal in* R *of rank n. Then there exist elements* $a_1, \ldots, a_n$ *such that P is minimal over* $(a_1, \ldots, a_n)$.

Proof. For $n = 0$ the assertion is vacuous, so we assume $n > 0$ and use induction on n. By Theorem 88, R has only a finite number of minimal prime ideals, say $Q_1, \ldots, Q_k$ (we mean truly minimal, i. e. 0 if R is a domain). Since $\operatorname{rank}(P) \geqq 1$, P is not contained in any Q_i, and therefore (Theorem 81) $P \not\subset Q_1 \cup \cdots \cup Q_k$. Pick $a_1 \in P, a_1 \notin$ any Q_i. Now pass to $R^* = R/(a_1)$, $P^* = P/(a_1)$. By Theorem 131, $\operatorname{rank}(P^*) \leq n - 1$. By induction P^* is minimal over $(a_2^*, \ldots, a_n^*)$. If we pick any a_i mapping on a_i^* $(i = 2, \ldots, n)$ we find P to be minimal over $(a_1, a_2, \ldots, a_n)$.

Remark. Theorem 153 is not at all of the same depth as the principal ideal theorem. In fact, the proof really used just the ascending chain condition on radical ideals and was available right after Theorems 81 and 88.

We are ready for the ultimate generalization of the principal ideal theorem. The technique is similar to that used in Theorem 153.

Theorem 154. *(Principal ideal theorem, generalized still further.) Let* R *be a Noetherian ring, I an ideal in* R *generated by n elements,* $I \neq$ R. *Let P be a prime ideal containing I. Assume that the rank of* P/I *in the ring* R/I *is k. Then the rank of P in* R *is at most* $n + k$.

Proof. The case $k = 0$ is Theorem 152. We argue by induction on k, assuming $k > 0$. Then P is not minimal over I. Let $P_1, \ldots, P_s$ denote all the prime ideals minimal over I (they are finite in number by Theorem 88). P is not contained in any P_i; hence by Theorem 81 we can find $y \in P, y \notin P_1 \cup \cdots \cup P_s$. Let $J = (I, y)$. The rank of P/J in R/J is at most $k - 1$, for a chain of prime ideals from P to J terminates at a prime not yet minimal over I. By induction, the rank of P in R is at most $(k - 1) + (n + 1) = k + n$.

The case $n = 1$ of Theorem 154 is important enough to be repeated, and we do so with a supplement, which is covered by Theorem 131.

Theorem 155. *Let P be a prime ideal in a Noetherian ring R and let* x *be an element in P. Suppose the rank of P in* R *is k. Then the rank of* $P/(x)$ *in* $R/(x)$ *is k or* $k - 1$. *If* x *is not contained in any minimal prime ideal of* R *(and so, in particular if x is a non-zero-divisor) the rank of* $P/(x)$ *in* $R/(x)$ *is* $k - 1$.

We are ready for still another theorem on the stability of the Macaulay property.

Theorem 156. *If* R *is Noetherian,* x *is a non-zero-divisor in the Jacobson radical of* R, *and* $R^* = R/(x)$ *is Macaulay then* R *is Macaulay.*

Proof. Let M be a maximal ideal of R; we must prove that its grade and rank are equal. We have $x \in M$ and we write $M^* = M/(x)$. By hypothesis, the grade and rank of M^* in R^* are equal. Now $G(M) = 1 + G(M^*)$, for x can be the beginning of a maximal R-sequence in M. By Theorem 155, $\operatorname{rank}(M) = 1 + \operatorname{rank}(M^*)$. Hence $G(M) = \operatorname{rank}(M)$.

We record a corollary of Theorems 156 and 141.

Theorem 157. R *is a Macaulay ring if and only if* $R[[x]]$ *is a Macaulay ring.*

EXERCISES

1. Let **x** be a non-zero-divisor in a Noetherian ring, P a prime ideal minimal over **(x).** Prove that P has rank 1.

2. Let **x** be nilpotent in R (not necessarily Noetherian) and let P be minimal over **(x).** Prove that P has rank 0.

3. Let R be a Noetherian Hilbert ring where every maximal ideal has rank k. Prove that every maximal ideal in $R[x_1, \ldots, x_n]$ has rank $k + n$.

4. Let R be Noetherian, Q a G-ideal in $R[x_1, \ldots, x_n]$ and $P = Q \cap R$. Prove that $\operatorname{rank}(Q) = n + \operatorname{rank}(P)$.

5. The transcendence degree of an integral domain over a subdomain is defined to be the transcendence degree of the big quotient field over the little one. If Q is a prime ideal in $T = R[x_1, \ldots, x_n]$, and $P = Q \cap R$, observe that R/P can be regarded as a subdomain of T/Q. If R is Noetherian, prove that

$$\operatorname{rank}(Q) - \operatorname{rank}(P) + \text{tr. deg.} \left(\frac{T/Q}{R/P}\right) = n$$

(Hint: use Theorem 149, and the additivity of transcendence degrees in a tower of extensions.)

6. Let R be a ring such that every domain that is a homomorphic image of R satisfies the principal ideal theorem. Show that Theorem 152 is valid for R. *(Hint:* modify the proof as follows. Among all chains $P \supset P_1 \supset \cdots \supset P_{n+1}$ pick one so that P_1 contains as many as possible of the a's. Say $a_1 \notin P_1$. Then once more P is the only prime ideal containing (a_1, P_1). The rest is unchanged.)

7. Show that for the elements $a_1, \ldots, a_n$ constructed in Theorem 153, and for any i $(1 \leqq i \leqq n)$, every prime ideal minimal over $(a_1, \ldots, a_i)$ has rank i.

8. Let K be a field, **x** and y indeterminates. Let R be the ring of polynomials in **x** and y over K, subject to the condition that no terms in a power of **x** only are permitted. Let M be the ideal in R consisting of all polynomials with constant term 0. Prove: (a) R satisfies the ascending chain condition on principal ideals; (b) M is minimal over @); **(c)** $\operatorname{rank}(M) \geqq 2$. (This example, due to Graham Evans, shows that the ascending chain condition on principal ideals is too weak to imply the principal ideal theorem.)

9. (a) Let $R \subset T$ be any rings. Let Q be a prime ideal in T, let $Q \cap R = P$, and assume P is minimal. Let Q^* denote the image of Q in T/PT. Prove: $\operatorname{rank}(Q) = \operatorname{rank}(Q^*)$. *(Hint:* observe that any prime ideal contained in Q must contain PT.)

(b) With the notation of part (a), assume that R and T are Noetherian, and drop the assumption that P is minimal. Prove: $\operatorname{rank}(Q) \leqq \operatorname{rank}(P) + \operatorname{rank}(Q^*)$. *(Hint:* proceed by induction on the rank k of P, noting that part (a) covers $k = 0$. Pick $x \in P$ not in any minimal prime ideal. Pass to the rings $R/(xT \cap R)$ and T/xT, and use Theorem 155.)

10. Let $R \subset T$ be domains with R Noetherian, T algebraic over R, and T generated over R by n elements. Let Q be prime in T and $P = Q \cap R$. Let d be the transcendence degree of T/Q over RIP.

(a) Prove: $\operatorname{rank}(Q) \leqq \operatorname{rank}(P) - d$. *(Hint:* reduce to $n = 1$ and use Theorem 149. Compare with Ex. 5.)

(b) Show that equality holds in (a) if the polynomial ring in n indeterminates over R satisfies the saturated chain condition.

(c) Observe that $d = 0$ if Q is a G-ideal, and in particular if it is a maximal ideal.

11. Let $R \subset T$ be domains with R Noetherian and T algebraic over R (but not necessarily a finitely generated ring over R). Let Q be prime in T and $P = Q \cap R$. Prove: $\operatorname{rank}(Q) \leqq \operatorname{rank}(P)$. *(Hint:* if $Q = Q_0 \supset Q_1 \supset \cdots \supset Q_{n+1}$, pick v_i in Q_{i-1} but not in Q_i. Drop down to the ring $R[v_1, \ldots, v_{n+1}]$ and quote Ex. 10.)

12. Let R be a Noetherian ring in which the classical unmixedness theorem holds: if an ideal I generated by n elements has rank n then I is rank-unmixed. Prove that R is Macaulay. *(Hint:* the problem is to construct an R-sequence of length m inside a given maximal ideal M of rank m. If Z is generated by an R-sequence of length i in M, $i < m$, argue that, by the rank-unmixedness of I, M cannot consist of zero-divisors on R/I. Thus the construction can continue.)

3-3 REGULAR RINGS

We need to examine minimal sets of generators for the maximal ideal M of a local ring R. We do it more generally for a module.

Theorem 158. *Let R be a local ring with maximal ideal M, and let A be a finitely generated R-module. Let $a_1, \ldots, a_n$ be elements of A. Then $a_1, \ldots, a_n$ generate A if and only if their images generate A/MA.*

Proof. Since the "only if" part is obvious, we assume that the images of $a_1, \ldots, a_r$ generate A/MA. Let B denote the submodule of A generated by $a_1, \ldots, a_r$; we must prove $B = A$. We have $B + MA = A$, whence $M(A/B) = A/B$. By the Nakayama lemma, $A/B = 0$.

Note that A/MA is an R-module annihilated by M, in other words a vector space over the field R/M. It follows that minimal generating sets for A correspond to vector space bases of A/MA. We shall call such a minimal generating set a *minimal basis* for A. In the important case $A = M$, the number of elements in a minimal basis will be called the V-dimension of R written $V(R)$. We note again that $V(R)$ is the dimension of M/M^2 as a vector space over the field R/M.

Theorem 159. *Let* R *be a local ring with maximal ideal* M. *Let* x *be any element in* $M - M^2$, *and write* $R^* = R/(x)$. *Then* $V(R^*) = V(R) - 1$.

Proof. Let $y_1^*, \ldots, y_r^*$ be a minimal basis of $M^* = M/(x)$, the maximal ideal of R*. Pick any $y_i \in M$ mapping on y_i^*. We claim that $x, y_1, \ldots, y_r$ form a minimal basis of M. It is immediate that they span M. To prove the minimality we take a linear combination

$$dx + c_1y_1 + \cdots + c_ry_r$$

which lies in M^2, and we must prove that each coefficient lies in M. We pass to R^* and find

$$c_1^*y_1^* + \cdots + c_r^*y_r^* \in (M^*)^2$$

whence $c_i^* \in M^*$ by the minimality of $y_1^*, \ldots, y_r^*$. Hence $c_i \in M$. This gives us $dx \in M^2$, which implies $d \in M$ since $x \notin M^2$.

By Theorem 152 we have $\dim(R) \leqq V(R)$. The local ring R is called *regular* if we have equality.

We show at once that there is a connection with R-sequences.

Theorem 160. *Let* R *be a local ring with maximal ideal* M. *Suppose that* M *can be generated by an R-sequence. Then* R *is regular. Moreover, the length of the R-sequence is equal to the common value of* $\dim(R)$ *and* $V(R)$.

Proof. Let k be the length of the R-sequence in question. We have

$$k = G(R) \leqq \operatorname{rank}(M) \leqq V(R) \leqq k \tag{36}$$

Here the first inequality follows from Theorem 132, the second (as noted above) from Theorem 152, and the last is immediate since $V(R)$ is the smallest number of elements that can generate M. The collapse of all the integers in (36) to equality gives us both conclusions of the theorem.

The converse of Theorem 160 is also valid (Theorem 169 below), but we are not quite ready to prove it.

We proceed in the next two theorems to investigate the behavior of regularity in the passage from R to $R/(x)$.

Theorem 161. *Let* R *be a regular local ring with maximal ideal* M, *and* x *an element in* $M - M^2$. *Then* $R^* = R/(x)$ *is regular.*

Proof. By Theorem 159, $V(R^*) = V(R) - 1$. By Theorem 155 $\dim(R^*) = \dim(R)$ or $\dim(R) - 1$. But we must have $\dim(R^*) \leqq V(R^*)$. Hence $\dim(R^*) = \dim(R) - 1 = V(R^*)$.

Theorem 162. *Let* R *be a local ring with maximal ideal* M *and* x *an element in* $M - M^2$ *that does not lie in any minimal prime ideal of* R. *Assume that* $R^* = R/(x)$ *is regular. Then* R *is regular.*

Proof. By Theorem 159, $V(R^*) = V(R) - 1$. By Theorem 155 $\dim(R^*) = \dim(R) - 1$. Hence R is regular.

Remark. The two theorems are not quite symmetric. But in fact the hypothesis of Theorem 161 implies that x lies in *no* minimal prime ideal, since we shall shortly prove that a regular local ring is an integral domain. Before doing so, we need a result that could have been done a good deal earlier (indeed right after Theorem 79).

Theorem 163. *Let* R *be a local ring that is not a domain. Then any principal prime ideal* P *in* R *is minimal.*

Proof. Let Q be a prime ideal properly contained in P. By Ex. **5** in §1-1, $Q \subset \bigcap P^n$. By Theorem 79, $\bigcap P^n = 0$. Thus $Q = 0$, contradicting our hypothesis that R is not a domain.

Theorem 164. *A regular local ring is an integral domain.*

Proof. We argue by induction on the dimension of the regular local ring R. If $\dim(R) = 0$, then R by definition is a field. We assume $\dim(R) > 0$ and then have $M \neq 0$, so that $M \neq M^2$, where M is the maximal ideal of R. Pick $x \in M - M^2$. By Theorem 161, $R^* = R/(x)$ is regular. By Theorem 159, $\dim(R^*) < \dim(R)$ (in fact it is smaller exactly by 1). By induction, R^* is a domain, i. e. (x) is prime. Now we assume R is not a domain and seek a contradiction. By Theorem 163, (x) is a minimal prime ideal. We know this to be true for any $x \in M - M^2$. Hence

$$M - M^2 \subset P_1 \cup \cdots \cup P_k$$

where the P_i's are the minimal prime ideals (finite in number by Theorem 88). From Theorem **83** we deduce $M \subset$ some P_i. But this means $\dim(R) = 0$, the desired contradiction.

Sooner or later everything in the subject of Noetherian rings gets globalized. Let us globalize the definition of regularity.

Definition. A Noetherian ring R is *regular* if R_M is regular for every maximal ideal M in R.

Our next objective is to generalize Theorem 164 by proving that any regular ring is a direct sum of integral domains. The ideas involved have a broader scope, and we develop them in some detail, starting with the Chinese remainder theorem.

Theorem 165. *Let I, J, K be ideals in a commutative ring* R. *Suppose that $I + J =$ R and $I + K = R$. Then $I + (J \cap K) =$* R.

Proof. Say $i + j = 1$, $i' + k = 1$ with $i, i' \in I$, $j \in J$, $k \in K$. Then

$$1 = (i + j)(i' + k) \in I + JK \subset I + (J \cap K).$$

Theorem 166. *Let I, J be ideals in a commutative ring* R. *Assume $I + J = R$, $(IJ)^n = 0$. Then $I^n \wedge J^n = 0$, $I^n + J^n =$* R, *i.e.* R *is the direct sum of I^n and J^n.*

Proof. We have $1 = i + j$, $i \in I, j \in J$. Then $1 = (i + j)^{2n-1} \in I^n + J^n$. Further, $I^n \wedge J^n = (I^n + J^n)(I^n \cap J^n) = 0$.

Now let R be a regular Noetherian ring. Each R_M is an integral domain by Theorem 164. In particular, each R_M has a unique minimal prime ideal (namely 0). This can be formulated in R itself as the statement that each M contains a unique minimal prime ideal, and we use this as the hypothesis of the next theorem.

Theorem 167. *Let* R *be a Noetherian ring in which every maximal ideal contains a unique minimal prime ideal. Then* R *is the direct sum of a finite number of rings, each of which has a unique minimal prime ideal.*

Proof. Let $P_1, \ldots, P_r$ denote the minimal prime ideals of R, and let N be their intersection; N is the nilradical of R (Theorem 25). Thus $N^n = 0$ for a suitable n. We have $P_i + P_j =$ R for $i \neq j$, for otherwise $P_i + P_j$ can be enlarged to a maximal ideal containing two distinct minimal prime ideals. By repeated use of Theorem 165 we get $P_1 + J =$ R, where $J = P_2 \cap \cdots \cap P_r$. Also $(P_1 J)^n \subset N^n = 0$. By Theorem 166, $\mathrm{R} = P_1^n \oplus J^n$. Iteration of the procedure yields the desired result.

Theorem 168. *Let* R *be a Noetherian ring such that R_M is an integral domain for every maximal ideal M. (In particular,* R *can be any regular Noetherian ring.) Then* R *is the direct sum of a finite number of integral domains.*

Proof. If $a \in$ R is nilpotent, then a maps into 0 in each R_M. Hence (Ex. 4 in §1-4) R has no non-zero nilpotent elements. Now apply Theorem 167.

We proceed to prove the converse of Theorem 160.

Theorem 169. *Let* R *be an n-dimensional regular local ring with maximal ideal M. Then M can be generated by an R-sequence of length*

n consisting of elements not in M^2. In fact, any minimal basis of M will do.

Proof. Start the R-sequence with any element $x \in M - M^2$, use Theorem 161 and induction.

Theorem 169 makes it clear that any regular local ring is Macaulay. By Theorem 140 this globalizes:

Theorem 170. ***Any regular ring is Macaulay.***

The relation between the regularity of R and that of $R[[x]]$ is manageable. We leave it as Ex. **5**. The relation between the regularity of R and that of $R[x]$ cannot be treated by the tools available up to this point — it runs into the stumbling block that we need to know that regularity of R implies regularity of Rp. As a way of putting off the homological invasion just a little longer, we invent a definition that will be obsolete as soon as the next chapter begins.

Definition. A ***super-regular*** ring is a Noetherian ring R such that R_P is regular for every prime ideal in R.

Theorem **171.** ***If*** R ***is*** a ***super-regular ring*** so ***is*** $R[x]$.

Proof. We take a prime ideal Q in $R[x]$ and its contraction $P = Q \cap R$. We know that R_P is regular. Let S be the complement of P in R. We localize both R and $R[x]$ with respect to S as a harmless adjustment.

After this we may start over with R regular local, M its maximal ideal, $T = R[x]$, N prime in T with $N \cap R = M$. Our problem is to prove T_N regular. By Theorem 160 it will suffice to prove that N can be generated by an R-sequence. By Theorem 169, M is generated by an R-sequence, say $a_1, \ldots, a_r$. There are two cases. If $N = MR[x]$, N is generated by $a_1, \ldots, a_r$ in $R[x]$ and this sequence remains an R-sequence in T. If N properly contains $MR[x]$, N is generated by M and a suitable f (Theorem 28). The elements $a_1, \ldots, a_r, f$ form an R-sequence.

Remark. Any Dedekind domain is obviously super-regular. Iterated use of Theorem 171 thus gives us a fair-sized collection of super-regular rings, which can be augmented by using Ex. 9.

EXERCISES

1. Let R be a local ring with maximal ideal M. (a) Suppose that $V(R) = 1 + G(R)$. Prove that R is Macaulay. (b) Suppose that $V(R) = 2 + G(R)$ and that R is not Macaulay. Prove that $\dim(R) = 1 + G(R)$.

2. Let R be a local ring with maximal ideal M, let $x \neq 0$ be an element of M^2, and write $R^* = R/(x)$. Prove that $V(R^*) = V(R)$, and that R^* is not regular.

3. Let R be a regular ring, and let x be an element not lying in the square of any maximal ideal of R. Prove that $R/(x)$ is regular.

4. Let R be a Noetherian domain, and let x be an element that is in the Jacobson radical of R but not in the square of any maximal ideal of R. Suppose that $R/(x)$ is regular. Prove: R is regular.

5. Let R be a Noetherian ring. Prove that R is regular if and only if $R[[x]]$ is regular.

6. Let R be a Noetherian integral domain, $\dim(R) \leqq 1$. Prove that R is regular if and only if it is a Dedekind domain.

7. Let R be a local ring in which the maximal ideal is principal. Prove:

(a) If R is an integral domain, then R is a principal ideal domain with (up to associates) exactly one prime, i. e., a **DVR.**

(b) If R is not an integral domain, then $\dim(R) = 0$ and furthermore every ideal is a power of the maximal ideal.

8. Let R be a Noetherian ring in which, for every maximal ideal M, the maximal ideal of R_M is principal (note that this is in particular true if every ideal in R is principal). Prove that R is the direct sum of a finite number of rings, each of which is either a Dedekind domain or a zero-dimensional local ring with a principal maximal ideal.

9. If R is super-regular, prove that every localization R_S is super-regular.

10. Let R be a Hilbert regular ring. Prove that $R[x]$ is regular.

11. (a) In a domain R let $P = (p)$ be a principal prime ideal. If $S = \{p^n\}$, prove that $R = R_P \cap R_S$. ***(Hint:*** if x lies in the intersection, $x = a/s = b/p^n$ with $s \notin P$. From $p^n a = sb$ get $p^n | b$.)

(b) Assume further that $\cap P^n = 0$ and that R_S is integrally closed. Prove that R is integrally closed. ***(Hint:*** observe that R_P is a DVR.)

12. Prove that any super-regular local ring is integrally closed. ***(Hint:*** pick $p \notin M^2$, observe that (p) is prime, use Ex. 11 and induction.)

13. Let R be a regular local ring and let I be an ideal in R such that

R/I is regular. Prove that $Z = (x_1 \cdots, x_n)$ where the x's form part of a minimal generating set for the maximal ideal of R.

14. Let R be Noetherian and P a prime ideal of rank k such that R_P is regular. Prove that there exist elements $a_1, \ldots, a_k$ in P whose images in R_P generate P_P, and such that $\operatorname{rank}(a_1, \cdots, a_k) = k$. *(Hint:* suppose suitable elements $a_1, \ldots, a_{k-1}$ are already chosen. Let $J =$ all x with $sx \in (a_1, \ldots, a_{k-1}, P^2)$ for some $s \notin P$. Observe that J is an ideal properly contained in P. Use Theorem 83 to see that $P - J$ is not contained in the union of the minimal primes over $(a_1, \ldots, a_{k-1})$, and select a_k accordingly.)

15. (S. Kochman) Let R be any Noetherian ring. Prove that R is the direct sum of a zero-dimensional ring and a ring in which every maximal ideal has rank at least 1. *(Hint:* if there exist any maximal ideals of rank 0, use a Chinese remainder procedure.)

CHAPTER 4

Homological Aspects of Ring Theory

4-1 HOMOLOGY

This chapter will present a number of results concerning the area in which homological algebra has greatly changed the subject of Noetherian rings.

We shall build on the account of homological dimension given in Part III of [26]. For convenience of reference we summarize the pertinent definitions and list the theorems we shall use. These theorems will be designated by letters.

A module is *projective* if it is a direct summand of a free module. Modules A and B are *projectively equivalent* if there exist projective modules P and Q such that $A \oplus P$ is isomorphic to $B \oplus$ Q. An exact sequence

$$0 \to K \to P \to A \to 0$$

with P projective is a *short projective resolution* of A. The projective equivalence class of K does not depend on the choice of the resolution and is denoted by $\mathfrak{R}A$. The operation of forming $\mathfrak{R}A$ can be iterated. The *homological dimension* of A is the smallest n such that $\mathfrak{R}^n A$ is the class of projective modules. If there is no such n, the homological dimension of A is infinite. Instead of homological dimension we sometimes say projective dimension, especially when we wish to emphasize the contrast with injective dimension. Our notation for homological dimension is $d(A)$, or $d_R(A)$ if it is urgent to call attention to the ring.

Theorems A, B, C, **D,** E are Theorems 1, 2, 3, **8, 9** of Part III of [26].

Theorem **A.** *(Schanuel's lemma) Let*

$$0 \to K \to P \to A \to 0, \quad 0 \to K_1 \to P_1 \to A \to 0$$

be shortprojective resolutions of A. Then $K \oplus P_1$ *is isomorphic to* $K_1 \oplus P$.

Theorem B. *Let B be a submodule of A and write,* $C = A/B$.
(1) If two of the dimensions d(A), d(B), d(C) arefinite, so is the third.
(2) If $d(A) > d(B)$, *then* $d(C) = d(A)$.
(3) *If* $d(A) < d(B)$, *then* $d(C) = d(B) + 1$.
(4) *If* $d(A) = d(B)$, *then* $d(C) \leqq d(A) + 1$.

Theorem C. *Let R be a ring with unit and x a central element of R which is a non-zero-divisor. Write* $R^* = R/(x)$. *Let A be a non-zero R*-module with* $d_{R^*}(A) = n < \infty$. *Then* $d_R(A) = n + 1$.

Theorem D. *Let R be a ring with unit, x a central element in R; write* $R^* = R/(x)$. *Let A be an R-module and suppose that x is a non-zero-divisor on both R and A. Then:* $d_{R^*}(A/xA) \leqq d_R(A)$.

Theorem E. *Let R be a left Noetherian ring, x a central element in the Jacobson radical of R; write* $R^* = R/(x)$. *Let A be a finitely generated R-module. Assume that x is a non-zero-divisor on both R and A. Then:* $d_{R^*}(A/xA) = d_R(A)$.

The following theorem is an immediate consequence of Theorems C and E.

Theorem 172. *Let R be a local ring, A a finitely generated non-zero R-module with* $d(A) < \infty$. *Let x be a non-unit in* ***R,*** *not a zero-divisor on either* ***R*** *or A. Then* $d(A/xA) = 1 + d(A)$.

We prove at once an important 'connection between the grade of a module and its homological dimension. This theorem explains the use by Auslander and Buchsbaum of the term "codimension."

Theorem 173. *Let R be a local ring with maximal ideal M, A a finitely generated non-zero R-module with* $d(A) < \infty$. *Then* $G(R) = G(A) + d(A)$.

Proof. We begin by noting that the result is evident if A is free, for then $d(A) = 0$ and $G(A) = G(R)$. Next we note that if $G(R) = 0$ then $d(A) = 0$; this follows from Lemma **4** on page **182** of **[26],** a result which we shall generalize in Theorem **191.** We make an induction on $G(R)$, and for a given $G(R)$ we make a secondary induction on $G(A)$.

Thus we assume $G(R) > 0$ and proceed to treat the case $G(A) = 0$. By Theorem 82, we have an element $a \neq 0$ in A with $Ma = 0$. Resolve A:

$$0 \to K \to F \to A \to 0 \tag{37}$$

with F free. Pick u in F mapping on a. Then $u \notin K$ and $Mu \subset K$. Since $M \not\subset Z(R)$ we can pick $x \in M$, $x \notin Z(R)$. Then $x \notin Z(K)$, since K is a submodule of a free module. We have $xu \in K$, $xu \notin xK$, $Mxu \subset xK$. This means that the image of xu in K/xK is non-zero, and is annihilated by M. We may look at K/xK as an R*-module, where $R^* = R/(x)$, and then the image of xu is annihilated by the maximal ideal M^* of R^*. Hence

$$G(K/xK) = 0 \tag{38}$$

We have

$$d_{R^*}(K/xK) = d_R(K) = d_R(A) - 1 \tag{39}$$

the first equality following from Theorem **E,** and the second from (37), since we may assume that A is not free. In particular we have $d_{R^*}(K/xK) < \infty$. Since

$$G(R^*) = G(R) - 1 \tag{40}$$

we can apply induction to get

$$d_{R^*}(K/xK) + G(K/xK) = G(R^*) \tag{41}$$

By combining equations (38)–(41) we get $G(R) = d(A)$, as required.

Now assume $G(A) > 0$. We have $M \not\subset Z(R)$, $M \not\subset <(A)$, so we can pick $x \in M$ not in $Z(R)$ or $Z(A)$ (use Theorem 81 to avoid all the prime ideals involved). Then

$$d_R(A/xA) = 1 + d_R(A) \tag{42}$$

by Theorem 172. Since x can start an R-sequence on A, we have

$$G(A/xA) = G(A) - 1 \tag{43}$$

Then by our secondary induction

$$G(R) = G(A/xA) + d_R(A/xA) \tag{44}$$

By combining (42)–(44) we get $G(R) = G(A) + d_R(A)$

Theorem 173 can be regarded as asserting that when $d(A) < \infty$, it is not a new invariant; it is defined in terms of grades by $G(R) - G(A)$. This is a kind of deflation of homological dimension in favor of the "shallower" concept of grade, except that the "deep" property then becomes whether $d(A)$ is finite or infinite.

We proceed to a second connection between grade and homological dimension. Theorem 174 is due to Rees [44]; the proof that follows, to Chase.

Theorem 174. Let R be a Noetheriun ring, A a non-zero *finitely* generated R-module. Then for any maximal prime P of A we have $G(P) \leq d(A)$.

Proof. We switch the problem to R_P. We still have (Ex. 9 in §2-2) that P_P is a maximal prime ideal belonging to A_P. In the transition, G may increase and d may decrease, but luckily both work in our favor. So we may start over with R local, M its maximal ideal, A a non-zero R-module and M belonging to A, i. e., $M \subset <(A)$. We have to prove $G(R) \leqq d(A)$. If $d(A)$ is infinite, we never had a problem. If $d(A)$ is finite then $d(A) = G(R)$ by Theorem 173.

To investigate the situation further, we let I be the annihilator of A. We have $I \subset P$ and so $G(I) \leqq G(P) \leqq d(A)$. If $G(I) = d(A)$ we have equality throughout. This motivates the next definition.

Definition. Let A be a non-zero finitely generated module over a Noetherian ring, I its annihilator. We say A is perfect if $G(I) = d(A)$.

The remark above proves Theorem 175.

Theorem 175. A perfect module A is grade-unmixed in the sense that all maximal primes of A have grade equal to the grade of the annihilator of A.

In the important special case where A is cyclic, $A = R/J$, we say that J is perfect, meaning strictly speaking that R/J is perfect. An example of a perfect ideal is furnished by $J = (a_1, \ldots, a_k)$ where the elements form an R-sequence, for we have $G(J) = k$, and $d(R/J) = k$ by iterated use of Theorem C.

What other perfect ideals are known? A result essentially going back to Macaulay asserts that if I is generated by an R-sequence, then any power of I is perfect. In [25] this was generalized to certain ideals generated by monomials in an R-sequence, an investigation carried further by Diana Taylor in her thesis (Chicago, 1966).

As an application of Theorems 173 and 174 we determine the homological dimension in a regular local ring of a prime ideal lying directly beneath the maximal ideal. Let R be n-dimensional regular local, and P a prime ideal of rank $n - 1$. We have $d(R/P) \geqq n - 1$ by Theorem 174 (R is Macaulay, so grade = rank). Since $M \not\subset Z(R/P)$, we have $d(R/P) < n$ by Theorem 173. We record this along with two extreme cases in Theorem 176.

rank(P)	$d(R/P)$
0	0
1	1
2	2
3	3

rank(P)	$d(R/P)$
0	0
1	1
2	2 or 3
3	3
4	4

EXERCISES

1. Let R be any ring and I an ideal in R generated by an R-sequence of length n. Prove: $d(I) = n - 1$.

2. Let R be local with maximal ideal M, and let A be a finitely generated R-module. Suppose that $\mathrm{Ext}(A, R/M) = 0$. Prove that A is free. *(Hint:* form a minimal resolution $0 \to K \to F \to A \to 0$. Any homomorphism from K to R/M is extendible to F. From this and $K \subset MF$ deduce $K = 0$.)

3. Let R be local with maximal ideal M. If the injective dimension of R/M is finite, prove that R is regular. *(Hint:* let the injective dimension of R/M be k. For any R-module A we have $\mathrm{Ext}(A, \mathfrak{s}^k R/M) = 0$, $\mathrm{Ext}(\mathfrak{R}^k A, R/M) = 0$. For A finitely generated deduce $\mathfrak{R}^k A = 0$ from Ex. 2.)

4. Let R be a regular local ring, T a Macaulay local ring containing R. Suppose that T is a finitely generated R-module. Prove that T is R-free. *(Hint:* apply Theorem 173 to T. See [53] for a discussion of the case where T is not local. Compare Ex. 11.)

5. Let R be local with $G(R) = k$. (a) Show that for a finitely generated R-module A, $d(A)$ is an integer from 0 to k, or ∞, and that all the integers $0, \ldots, k$ are eligible. (b) Show that for an ideal Z in R, $d(I)$ is an integer from 0 to $k - 1$, or ∞, and that all the integers $0, \cdots, k - 1$ are eligible. (c) Show that for a prime ideal P in R, P not maximal, $d(P)$ is an integer from 0 to $k - 2$, or ∞.

6. Let R be local, let $G(R) = k$, and let A be a finitely generated nonzero R-module. Assume that $d(A) < \infty$, and that some maximal prime P of A satisfies $G(P) = k - 1$. Prove: $d(A) = k - 1$. *(Hint:* apply Theorem 174.)

7. Let R be local with maximal ideal M, let $G(R) = k$, and let P be a prime ideal lying directly beneath M. Prove: $d(R/P) = k - 1$, or ∞, $d(P) = k - 2$, or ∞.

8. In an arbitrary ring R let $a_1, \ldots, a_n$ be an R-sequence and let $I = (a_1, \ldots, a_n)$. Let F be a free R-module with basis $u_1, \ldots, u_n$. Resolve Z

$$0 \to K \to F \to I \to 0$$

by sending u_i into a_i. Prove that K is spanned by the elements $a_j u_i - a_i u_j$.

9. Let R be a Noetherian ring, let $a_1, \ldots, a_n$ be elements in the Jacobson radical of R, and let $Z = (a_1, \ldots, a_n)$. Resolve Z as in Ex. 8. Assume that K is spanned by the elements $a_j u_i - a_i u_j$. Prove that the a's form an R-sequence. *(Hint:* from the hypotheses one can easily deduce that $ta_n \in (a_1, \cdots, a_{n-1})$ implies $t \in (a_1, \cdots, a_{n-1})$. It remains to make an inductive reduction. Write K^* for K intersected with the submodule spanned by $u_1, \ldots, u_{n-1}$. Let H^* be the submodule spanned by $u_i a_j - u_j a_i$ for $i, j \leqq n - 1$. We must prove $H^* = K^*$. Do this by verifying $K^* \subset H^* + a_n K^*$ and applying the Nakayama lemma.)

10. Let R be an n-dimensional regular local ring with maximal ideal M. Prove: $G(M, M) = 1$. *(Hint:* note that $d(M) = n - 1$ and use Theorem 173.)

11. Let R and T be local rings, f a homomorphism of R into T carrying the maximal ideal M of R into the maximal ideal N of T. Note that f makes T an R-module; we assume this module to be finitely generated. Let A be a finitely generated T-module (thereby a finitely generated R-module).

(a) Prove that the grade of A is the same, whether computed as a T-module or as an R-module. *(Hint:* this can be reduced to two cases: where T is a homomorphic image of R, or where $R \subset T$. The first is immediate. For the second, note that $M \subset N$ and that MT contains some power of N. This looks after grade 0. Divide by a maximal R-sequence on A contained in M.)

(b) If $d_T(A)$ and $d_R(T)$ are finite, prove that $d_R(A)$ is their sum. *(Hint:* reduce this to part (a) by using Theorem 173.)

12. Let $R \subset T$ be local rings with the maximal ideal M of R contained in the maximal ideal N of T. Assume that T is regular, that T is a finitely generated R-module, and that $d_R(T)$ is finite. Prove that R is regular. *(Hint:* observe that T/N is a direct sum of a finite number of copies of R/M.)

13. Let $x_1, \ldots, x_n$ be an R-sequence in a ring R, and let

$$I = (x_1, \cdots, x_n).$$

Prove that $\mathrm{Ext}^i_R(R/I, R) \neq 0$ if and only if $i = n$. *(Hint:* see the appendix to §3-1.)

14. (R. Hamsher) Let R be an integral domain such that for every finitely generated R-module A with $d(A) < \infty$, the annihilator I of A satisfies $d(I) < \infty$. Prove that $d(J) < \infty$ for every finitely generated ideal J in R. *(Hint:* to prove $d(x, y) < \infty$, note that $(x) \cap (y)$ is the annihilator of $R/(x) \oplus R/(y)$, and that $(x)/(x) \cap (y) \cong (x, y)/(y)$. Continue stepwise.)

15. Let R be a Noetherian ring, A an R-module such that $\mathrm{Ext}(R/P, A) = 0$ for every prime ideal P. Prove that A is injective. *(Hint:* use Ex. 7 of §2-1.)

16. Let R be a one-dimensional Noetherian domain, A an R-module such that $\mathrm{Ext}(R/M, A) = 0$ for every maximal ideal M. Prove that A is injective.

17. Let R be local with maximal ideal M, and let x be a non-zero-divisor in R that is not contained in M^2. Write $R^* = R/(x)$. Let A be a finitely generated R-module annihilated by x (thereby an R*-module). If $d_R(A) < \infty$, prove that $d_{R^*}(A) < \infty$. ***(Hint:*** resolve

$$0 \to K^* \to F^* \to A \to 0$$

with F^* free over R*. Since $d_R(F^*) = 1$, this reduces the problem to the case $d_R(A) = 1$. In that case form a minimal resolution

$$0 \to K \to F \to A \to 0$$

over R, where F is free on $u_1, \ldots, u_n$. We have $xF \subset K$, and K is free. Observe that, since $x \notin M^2$ and $K \subset MF$, the elements $xu_1, \ldots, xu_r$ are linearly independent mod MK. Hence they can form part of a free basis of K. In this way, argue that xF/xK is a direct summand of K/xK with complementary summand K/xF. Thus the R*-resolution of A

$$0 \to K/xF \to F/xF \to A \to 0$$

splits.)

18. In Ex. 14 of §3-1, assume that R is local and that the modules involved have finite projective dimension. Give an alternative proof by using Theorem **173** and Theorem B.

4-2 UNIQUE FACTORIZATION

We prove in this section that any regular local ring is a **UFD,** and we do it in a slightly generalized form.

The literature contains at least four proofs that may be considered reasonably different.

(1) The original proof of Auslander and Buchsbaum **[3]** which, in turn, made important use of earlier work, especially results of Zariski and Nagata.

(2) The proof that Auslander and Goldman found as a by-product of their work in [5].

(3) A proof that I discovered in early **1960.** It is reproduced by Samuel on page 88 of [45].

(4) The paper [32] of MacRae proves a good deal more, and allows zero-divisors in the ring. **He** makes important use of an idea found independently by M. Auslander and D. Mumford. For an integral domain, MacRae's theorem is proved a lot more simply in [31].

The proof I give here was announced at the Varenna conference on rings in August, **1965** and is sketched in the notes issued after that conference. The key idea is the same as that in (3), the third of the four proofs just mentioned, but it is supplemented by the old trick of adjoining an indeterminate. The theorem has the merit of ***characterizing*** UFD's (even non-Noetherian ones).

We need two preliminary theorems. The first embodies a useful device, which Nagata introduced in [36].

Theorem 177. ***Let*** R ***be an integral domain satisfying the ascending chain condition on principal ideals. Let*** $\{p_i\}$ ***be a set of principal primes, and let S be the multiplicatively closed set they generate. Then: if*** R_S ***is a UFD,*** so ***is*** R.

Proof. There **is** no difficulty in a direct assault: assembling the primes (roughly speaking, the p_i's together with those of R_S), and showing the possibility and uniqueness of factorization. But since we have Theorem **5** available, let us use it.

Let then Q be a non-zero prime ideal in R; we have to show that Q contains a principal prime. If some $p_i \in Q$, we are finished. So we assume the contrary. Now Q_S must contain some principal prime of R_S. We can choose it to be an element q of R, and this entails $q \in Q$. Furthermore we can choose a q not divisible by any p_i. For if q is divisible by p_i, we can pass to q/p_i and we still have $q/p_i \in Q$, since $p_i \notin Q$. We keep dividing by p_j's, a procedure that the ascending chain condition on principal ideals will terminate in a finite number of steps. Thus we may normalize q so as not to be divisible by any p_i. Now we claim that (q) is prime. For suppose $ab \in (q)$. We pass to the ring R_S and there we find that a, let us say, is divisible by q. This gives us an equation $sa = cq$, $s \in S$; that is,

$$p_{i_1} \cdot \cdots \cdot p_{i_r} a = cq \tag{45}$$

Since each p_i is prime and does not divide q, it must divide c. We can therefore cancel the p_i's in (45) one after another, till we get a divisible by q. We have thus proved that q is a principal prime, and this completes the proof of Theorem 177.

The second preliminary theorem might be described as a local characterization of UFD's.

Theorem 178. *Let* R *be an integral domain. The following three conditions are necessary and sufficient for R to be a UFD:*

(1) R_M is a UFD for every maximal ideal M;

(2) Every minimal prime ideal in R is finitely generated;

***(3)** Every invertible ideal in R is principal.*

Proof. The necessity needs little attention. Every localization of a UFD is a UFD (Ex. 3 in §1-4); in a UFD every minimal prime ideal is in fact principal; (3) is covered by Ex. 15 in §1-6.

Suppose R satisfies (1)-(3). We use Theorem **5,** and therefore take a non-zero prime ideal P and seek to prove that P contains a principal prime. Now for any maximal ideal $M \supset P$, R_P is a localization of R_M and is therefore a UFD. From this we deduce that P contains a minimal prime ideal Q (take one in R_P and transfer it back to R). Now for each maximal ideal $\boldsymbol{M}$, Q_M maps either into all of R_M or into a minimal prime ideal in R_M. In either case Q_M is principal. It follows from Theorem 62 that $\boldsymbol{Q}$ is invertible, hence principal by hypothesis.

We now present our main characterization of UFD's. We recall that we have defined what it means, even in non-Noetherian rings, for an ideal I to have grade $1: I$ must contain a non-zero-divisor a such that $I \subset \mathcal{Z}(R/(a))$.

Theorem 179. *Let* R *be an integral domain. The following four conditions are necessary and sufficient for R to be a UFD:*

(1) R satisfies the ascending chain condition on principal ideals;

(2) In the polynomial ring $R[x]$ all minimal prime ideals are finitely generated;

***(3)** For any prime ideal P of grade one in* R, R_P *is a UFD;*

***(4)** In any localization of $R[x]$ all invertible ideals are principal.*

Comment. If R is Noetherian we can forget about (1) and (2); **(3)** becomes equivalent to integral closure (Theorem 95). So for a Noetherian integrally closed domain, all we are assuming is that certain invertible ideals are principal. If it were true (of course it is not) that all invertible ideals are principal, then every integrally closed Noetherian domain would be a UFD.

Proof. Necessity. The remarks made in connection with Theorem 178 need two supplements, of which the first is obvious and the second standard: any UFD satisfies the ascending chain condition on principal ideals; if R is a UFD so is $R[x]$.

Sufficiency. We shall actually prove that $R[x]$ is a UFD; it is standard and easy that then R is a UFD. We abbreviate $R[x]$ to T. It is also easy (much easier than Hilbert's basis theorem) that the ascending chain condition on principal ideals is inherited by T.

Let S be the set of all finite products of principal primes in T (actually we only need the primes $a + bx$ discussed below). By Theorem 177 it suffices to prove that $T_S = U$ is a UFD. (This is the only localization of T to which we shall apply our fourth hypothesis.)

We shall prove U to be a UFD by verifying that it satisfies the three conditions in Theorem 178. Now (2) is obviously transmitted from T to U, and (3) is fulfilled by hypothesis. It remains to check that U_M is a UFD for every maximal ideal M in U. Note that M has the form Q_S for $\boldsymbol{Q}$ a suitable prime ideal in T disjoint from S. Let $P = Q \cap R$. We claim that $P = 0$ or has grade 1. For otherwise P contains an R-sequence a, b of length 2. (Take any $a \neq 0$ in P; if $P \not\subset \mathcal{Z}(R/(a))$ we get the desired b.) But then Q contains the principal prime $a + bx$ (Ex. 3 in §3-1), a contradiction. Now by hypothesis R_P is a UFD. So is T_Q, a localization of $R_P[x]$, and U_M, a localization of T_Q. Theorem 179 is proved.

It still remains to be seen whether Theorem 179 is applicable to regular local rings. For this we have some spade work to do. We introduce finite free resolutions, and develop some material concerning them.

Definition. A *finite free resolution* (FFR) of a module $\boldsymbol{A}$ is an exact sequence

$$0 \to F_n \to \cdots \to F_1 \to F_0 \to \boldsymbol{A} \to 0$$

where each F_i is finitely generated and free. We say that a module is FFR if it possesses an FFR.

Theorem 180. *If a projective module $\boldsymbol{A}$ has an FFR, then it has a free complement; that is, there exists a finitely generated free module $\boldsymbol{G}$ such that $\boldsymbol{A} \oplus \boldsymbol{G}$ is free.*

Proof. We prove this by induction on the length of the resolution. Say the resolution starts by mapping F onto A with kernel K:

$$0 \to K \to F \to A \to 0 \tag{46}$$

By induction, $K \oplus G$ is free with G free and finitely generated. Since A is projective, (46) splits: $A \oplus K \cong F$. Then

$$A \oplus K \oplus G \cong F \oplus G$$

proves the theorem.

Theorem 181. ***If an invertible ideal Z in an integral domain has an FFR, then Z is principal.***

Proof. Z is projective, so we have Z $\oplus$ free = free. Now Lemma 1 in [23] asserts that for any ideals $I_1, \ldots, I_n, J_1, \ldots, J_n$ in an integral domain, if $I_1 \oplus \cdots \oplus I_n$ and $J_1 \oplus \cdots \oplus J_n$ are isomorphic, then $I_1 \ldots I_n$ and $J_1 \ldots J_n$ are isomorphic. It follows that the ideal Z is principal.

Theorem 182. ***Let R be a commutative Noetherian ring with the property that any finitely generated R-module has an FFR. Then the same is true for the polynomial ring $R[x]$.***

We sketch a proof due to Borel and Serre (Prop. 8 on p. 116 of [8]); the present formulation was given by Swan. This proof actually yields a more general result; in stating it, we find it convenient to introduce the notion of a family of modules: a collection S of modules with the property that when two members of a short exact sequence lie in S so does the third. Examples of families: all modules, all modules of finite homological dimension, all torsion modules over an integral domain. When R is Noetherian we have the further example of all finitely generated modules, and finally the pertinent example of all FFR modules.

Since any intersection of families is again a family, we may speak of the family generated by a set of modules.

One sees readily that Theorem 182 is a consequence of Theorem 183.

Theorem 183. ***Let R be a commutative Noetherian ring, and let $S = R[x]$. Then the set of modules $A \otimes_R S$, where A ranges over all finitely generated R-modules, generates the family of all finitely generated S-modules.***

Proof. Write S for the family generated by the $A \otimes_R S$'s. By an induction based on the ascending chain condition we can assume that all S-modules with a non-zero annihilator in R lie in S. By Ex. 7 in §2-1 it will suffice for us to treat S-modules having the form S/P where P is a prime ideal in S. Since we may assume that the annihilator of S/P in R is 0, we have that R is an integral domain. Let f be a polynomial of least degree in P. Then the principal ideal generated by f is isomorphic to S and is of course in S, while $P/(f)$ has a non-zero annihilator in R and therefore also lies in S.

Over a regular local ring every finitely generated module has an FFR; this is clear since projective modules over local rings are free. Thus Theorem 184 is applicable to regular local rings.

Theorem 184. ***Let R be a Noetherian domain with the property that every finitely generated module has an FFR. Then R is a UFD.***

Proof. We check off the hypotheses of Theorem 179. The Noetherian hypothesis looks after (1) and (2). The FFR hypothesis is inherited by $R[x]$ (Theorem 182) and by its localizations (since localization preserves exact sequences and freedom). Theorem 181 now looks after (4). As for (3), if P is a prime ideal of grade 1, then $\operatorname{rank}(P) = 1$ since R is regular and hence Macaulay. Thus R_P is a one-dimensional regular local ring, i. e., a DVR.

By combining Theorem 184 with Theorem 178 we can sharpen the result a little.

Theorem 185. ***Let R be a regular Noetherian domain in which every invertible ideal is principal. Then R is a UFD.***

In concluding this section we prove a theorem of Samuel, which states that if R is a regular UFD so is $R[[x]]$. We generalize a little.

Theorem 186. ***Let T be an integral domain, x an element in the Jacobson radical of T, and $R = T/x$, a domain with every invertible***

ideal in R principal. Suppose further that $\bigcap x^n T = 0$. ***Then every invertible ideal in T is principal.***

Proof. We first investigate more generally the nature of a finitely generated projective T-module P. We have that $P \oplus Q = F$ with F free and finitely generated over T. Then $P/xP \oplus Q/xQ = F/xF$. Here F/xF is a free R-module, of the same dimension over R as the dimension of F over T. Thus P/xP is R-projective. In particular it is torsion-free and has a well-defined rank. We claim that this rank is at most equal to the rank, say $k - 1$, of P. For let $u_1, \cdots, u_k \in P/xP$, and pick $v_1, \cdots, v_k \in P$ mapping on the u's. We have $\Sigma a_i v_i = 0$, where the a's are elements of T, not all 0. We map this equation mod x, and have the desired dependence of the u's over R, unless every a_i is divisible by x. In that case we can cancel x in $\Sigma a_i v_i = 0$. We continue the procedure, and the hypothesis $\bigcap x^n T = 0$ guarantees that it ends in a finite number of steps.

The same argument, of course, applies to the ranks of Q and Q/xQ. But since the possibly depressed ranks of P/xP and Q/xQ add up to the dimension of F/xF, which equals the dimension of F, we must have equality between the rank of P and the rank of P/xP. Since an invertible ideal is the same thing as a projective module of rank 1, we have that if P is an invertible ideal in T, then P/xP is isomorphic to an invertible ideal in R. By the hypothesis the latter is principal, i. e., isomorphic to $R = T/(x)$.

We are faced now with the following problem: given that P and N are finitely generated projective modules over T and that P/xP and N/xN are isomorphic, prove that P and N are isomorphic. (This part of the argument works with (x) generalized to any ideal in the Jacobson radical, and the rings can be noncommutative.) In the diagram we have a map from N to P/xP. Since N is projective we can lift it to $f : N \to P$.

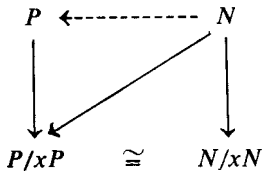


FIGURE 6

Likewise we get $g : P' \to N$. We need to prove the products fg and gf to be automorphisms. Now $fg : P \to P$ is a map that induces the identity on P/xP. Take $P \oplus Q = F$ with F free, and combine fg on P with the

identity on Q. Now we have a map on F to itself, which is the identity mod xF. In matrix terms we have a matrix that is the identity mod x. It is a well-known and easy consequence of x being in the Jacobson radical that such a matrix is invertible. This concludes the proof of Theorem 186.

Theorem 187. ***Let T be a Noetherian domain, let x be an element in the Jacobson radical of T, and*** $R = T/(x)$. ***Assume that x does not lie in the square of any maximal ideal of T. Then: if R is a regular UFD, so is T.***

Proof. By Ex. 4 in §3-3, T is regular. By Theorem 186 every invertible ideal in T is principal (the needed hypothesis $\bigcap x^n T = 0$ is supplied by Theorem 79). Apply Theorem 185.

The hypotheses of Theorem 187 are fulfilled if $T = R[[x]]$. Hence we have:

Theorem 188. ***If*** R ***is a regular UFD, so is*** $R[[x]]$.

4-3 THE EULER CHARACTERISTIC

In this section we shall define the Euler characteristic of an **FFR** module and study some of its properties.

The first step will be to extend Schanuel's lemma (Theorem **A)** to long projective resolutions. Commutativity is irrelevant for this theorem, and it is understood that all modules are left.

Theorem 189. ***Let*** R ***be any ring, A an R-module. Suppose given two exact sequences***

$$0 \to K \to P_n \to P_{n-1} \to \cdots \to P_1 \to A \to 0$$
$$0 \to L \to Q_n \to Q_{n-1} \to \cdots \to Q_1 \to A \to 0$$

where the P's and Q's are projective. Then

$$K \oplus Q_n \oplus P_{n-1} \oplus \cdots \cong L \oplus P_n \oplus Q_{n-1} \oplus \cdots \tag{47}$$

Here, if n is odd, the direct sums in (47) terminate in Q_1 and P_1 respectively; if n is even they terminate in P_1 and Q_1.

Proof. Let K_0 be the kernel of the homomorphism from P_1 to A and let L_0 be similarly defined. Then we have the short exact sequences

$$0 \to K_0 \to P_1 \to A \to 0$$
$$0 \to L_0 \to Q_1 \to A \to 0$$

By Schanuel's lemma,

$$K_0 \oplus Q_1 \cong L_0 \oplus P_1 \tag{48}$$

Now there is a truncated exact sequence

$$0 \to K \to P_n \to \cdots \to P_2 \to K_0 \to 0$$

It is harmless to add a direct summand Q_1 to the terms P_2 and K_0, taking the mapping on Q_1 to be the identity. We now have

$$0 \to K \to P_n \to \cdots \to P_3 \to P_2 \oplus Q_1 \to K_0 \oplus Q_1 \to 0 \tag{49}$$

and in the same way

$$0 \to L \to Q_n \to \cdots \to Q_3 \to Q_2 \oplus P_1 \to L_0 \oplus P_1 \to 0 \tag{50}$$

By (48), the final terms in (49) and (50) may be identified. We can now apply induction to the sequences (49) and (50), and the result is the statement to be proved.

Let the ring R be commutative (see Appendix 4-3(a) for a discussion of the non-commutative case). Let A be an FFR module with the resolution

$$0 \to F_n \to F_{n-1} \to \cdots \to F_1 \to A \to 0$$

The rank of F_i (number of elements in a free basis) is an invariant, which we denote by f_i. We define the Euler characteristic $\chi(A)$ of A to be

$$\chi(A) = f_1 - f_2 + f_3 \cdots - (-)^{n+1} f_n$$

If we have a second FFR, we can (by inserting harmless zeros) assume it to have the same length:

$$0 \to G_n \to G_{n-1} \to \cdots \to G_1 \to A \to 0$$

Theorem 189 tells us that

$$f_n + g_{n-1} + f_{n-2} + \cdots = g_n + f_{n-1} + g_{n-2} + \cdots \tag{51}$$

where g_i is the rank of G_i. From (51) we see that $\chi(A)$ is indeed an invariant of A, independent of the particular FFR.

Remark. It is possible to develop a more general theory, which allows projective modules in the resolutions. This can be done by using the theorem that, after a suitable decomposition of the ring into a direct sum, a finitely generated projective module has a well-defined constant rank in each summand. Alternatively, the Euler characteristic could be allowed to take values in an appropriately defined Grothendieck group. On the other hand, some problems can simply be treated by localization (see Ex. 7).

Let S be multiplicatively closed in R. Given an FFR of an R-module A, we obtain by localization a precisely analogous FFR of A_S over R_S. Hence:

Theorem 190. *Let A be an FFR module over the ring R, and let S be a multiplicatively closed set in R. Then A_S is FFR over R_S, and $\chi(A_S) = \chi(A)$.*

Our basic method will be to take advantage of Theorem 190 by forming suitable localizations. For this purpose we formulate the next theorem.

Theorem 191. *Let R be a quasi-local ring with maximal ideal M. Suppose that every finite subset of M possesses a non-zero annihilator. Then every FFR R-module is free.*

Proof. It suffices for us to treat a module with a short FFR:

$$0 \to F_2 \to F_1 \to A \to 0 \tag{52}$$

for then we merely iterate this result. We can assume the resolution (52) to be minimal. Minimality tells us that $F_2 \subset MF_1$. If we think of F_1 and F_2 with fixed bases, then only a finite number of elements of M are involved. By hypothesis, these are annihilated by a non-zero element z. Hence $zF_2 = 0$, which is possible only if $F_2 = 0$, and A is free.

Remarks. 1. For R Noetherian we are simply saying (Theorem 82) that M consists of zero-divisors.

2. Whether or not R is Noetherian, the hypothesis of Theorem 191 is fulfilled if M is nil. We make use of this in proving the next theorem.

Theorem 192. *For any FFR module A over a commutative ring R, we have $\chi(A) \geqq 0$.*

Proof. Let P be a minimal prime ideal in R. The ring R_P is quasi-local with a nil maximal ideal. By Theorem 190, $\chi(A) = \chi(A_P)$. By Theorem 191, A_P is free, whence $\chi(A_P) \geqq 0$.

The major theorems of this section are Theorems 194 and 195 below. We first prove a preliminary result.

Theorem 193. *In the ring R assume $\mathfrak{Z}(R)$ is a finite union $P_1 \cup \cdots \cup P_n$ of prime ideals. Let A be a finitely generated module and let I be its annihilator. Then $A_{P_i} = 0$ for all i if and only if I contains a non-zero-divisor.*

Proof. The statement $A_{P_i} = 0$ is equivalent to the annihilation of A by an element not in P_i, i. e. $I \not\subset P_i$. If this is true for every i, then by Theorem 81, I contains a non-zero-divisor.

Theorem 194. *Let R be a Noetherian ring, A an FFR module with annihilator I. If $\chi(A) = 0$, then I contains a non-zero-divisor.*

Proof. Let $P_1, \ldots, P_n$ be the maximal primes of 0 in R. Then $\mathfrak{Z}(R) = P_1 \cup \cdots \cup P_n$, and each P_i is the annihilator of a non-zero element. It follows readily that in R_{P_i} the maximal ideal consists of zero-divisors. Hence (Theorem 191) A_{P_i} is free. In view of $\chi(A) = \chi(A_{P_i}) = 0$, we deduce $A_{P_i} = 0$. The conclusion now follows from the preceding theorem.

Theorem 195. *Let R be a Noetherian ring, A an FFR module satisfying $\chi(A) \neq 0$. Then A is faithful.*

Proof. Let I be the annihilator of A, and J the annihilator of I (in R). We proceed as in the last theorem. This time, from $\chi(A) \neq 0$ we conclude that each A_{P_i} is a non-zero free module, and its annihilator is 0. Hence $I_{P_i} = 0$ for all i. Now we can apply Theorem 193, with I and J playing the roles of A and I respectively. The conclusion that J contains a non-zero-divisor tells us that I must be 0.

Theorems 194 and 195 were implicit in the discussion to be found in [2]; the following corollary of these two theorems was given explicitly.

Theorem 196. *Let R be a Noetherian ring, A an FFR module with annihilator I. Then either $I = 0$ or I contains a non-zero-divisor. In particular, if the ideal J in R is an FFR module, then either $J = 0$ or J contains a non-zero-divisor.*

We observe that the last sentence in Theorem 196 is obtained by nating that R/J is FFR and that its annihilator is J.

It seems conceivable that Theorems 194 and 195 are actually valid verbatim without the Noetherian hypothesis. We can offer three pieces of evidence on the affirmative side.

The first is that for a module A with a short resolution

$$0 \to F_2 \to F_1 \to A \to 0$$

both theorems hold. We see this by picking bases for F_1, F_2. The module A is fully determined by the resulting matrix. We drop down to the subring R_0 generated by the entries of the matrix. The ring R_0 is Noetherian, and we readily see that the problem can be switched to R_0.

The second piece of evidence is the following theorem, where a weaker conclusion than that of Theorem 195 is derived without chain conditions.

Theorem 197. *Let A be an FFR module with $\chi(A) \neq 0$. Then the annihilator of A is nil.*

Proof. Let I be the annihilator of A. Let P be a typical minimal prime ideal in R. As we noted above, A_P is a free R_P-module, necessarily non-zero. Thus $I_P = 0$. For every $x \in I$, we have $sx = 0$ for $s \notin P$. This yields $x \in P$, $I \subset P$. This being true for every P, we deduce that I is nil.

Lastly, we prove the following theorem, due to Stallings [48]. In comparing it with Theorem 195, note that by strengthening the hypothesis $\chi(A) \neq 0$ to the assumption that $\chi(A)$ is a non-zero-divisor in R, we get the desired conclusion $I = 0$.

Theorem 198. *For any* FFR *module A with annihilator I we have* $\chi(A)I = 0$.

Proof. Let y be an element in the annihilator of A. In Fig. 7, the

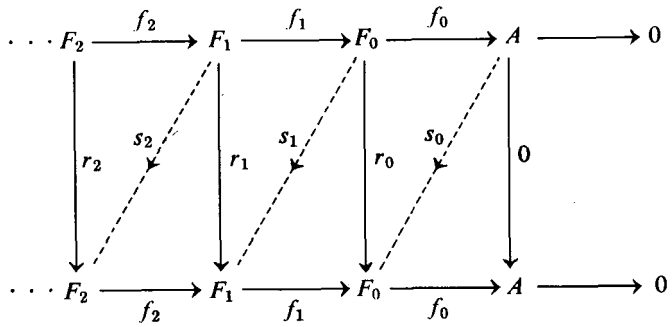


FIGURE 7

vertical map $A \to A$ is 0, and $r_i : F_i \to F_i$ is multiplication by y. Note that the diagram commutes. It is possible (see p. 81 of [11]) to construct contracting homotopies s_i, as indicated, so as to satisfy $s_0 = 0$ and

$$s_i f_i + f_{i+1} s_{i+1} = r_i \qquad (i = 0, 1, \cdots) \tag{53}$$

We take the trace of the endomorphisms in (53) and then form the alternating sum. All terms on the left side cancel in pairs and we get $\chi(A)y = 0$, as required.

We insert at this point an interesting theorem due to Vasconcelos [52].

Theorem 199. *Let I be an ideal in a local ring* R. *Assume that $d(I)$ is finite and that I/I^2 is a free (R/I)-module. Then I can be generated by an R-sequence.*

Remarks. 1. The converse is also true. See Ex. 13 in §3-1 and Ex. 1 in §4-1.

2. Theorem 199 gives us a fresh proof that a local ring of finite global dimension is regular. For if M is the maximal ideal, we obviously have that M/M^2 is free over the field R/M. Hence $d(M) < \infty$ implies that M can be generated by an R-sequence, whence (Theorem 160) R is regular. We see also from this that the condition $d(I) < \infty$ cannot be omitted in the theorem: take $I = M$ in a non-regular local ring.

Proof. We dismiss the case $I = 0$. Then by Theorem 196, I contains a non-zero-divisor. By Theorem 83 we can sharpen this to the statement that $I - MI$ contains a non-zero-divisor x. The element x can be completed to a set $x, y_1, \ldots, y_k$ of elements of I that map into a free basis of the free (R/I)-module I/I^2. The plan of the proof is to pass to the ideal $I^* = I/(x)$ in the ring $R^* = R/(x)$ and use induction. We have two things to verify: that $I^*/(I^*)^2$ is a free R^*/I^*-module, and that $d_{R^*}(I^*)$ is finite. The first of these is a routine verification, which we leave to the reader. For the second, we quote Theorem E to get $d_{R^*}(I/xI) < \infty$. It will therefore suffice to see that $I/(x)$ is a direct summand of I/xI. Let $J = (xI, y_1, \cdots, y_k)$. Evidently $(x) + J = I$. We need $(x) \cap J = xI$. If $y \in (x) \cap J$ we get an equation

$$y = ax = b_1 y_1 + \cdots + b_k y_k + z$$

where $a, b_i \in$ R and $z \in xI$. Then

$$ax - b_1 y_1 - \ldots - b_k y_k \in I^2$$

Since the elements $x, y_1, \ldots, y_k$ map into a free (R/I)-basis of I/I^2, we deduce $a \in I$, so that $y \in xI$, as required.

Our final theorem in this section is a generalization of the commutative case of a theorem of Swan [49] (see Appendix 4–3(a) for the noncommutative case). The theorem concerns what we might call "partial" Euler characteristics. Let A be a module admitting a resolution by finitely generated free modules:

$$\cdots F_1 \to F_0 \to A \to 0 \tag{54}$$

We now admit the possibility that the resolution never terminates. Write f_i again for the rank of F_i. Define $g_0 = f_0$, $g_1 = f_1 - f_0$, $g_2 = f_2 - f_1 + f_0$, and in general

$$g_n = f_n - f_{n-1} + \cdots + (-)^n f_0$$

Of course the g's are not at all invariant. But if we define $\chi_n(A) = \inf g_n$, taken over all resolutions, we are able to prove the result stated in Theorem 200.

We make a comment on why χ_n is defined in this way (by inf rather than sup). As regards χ_0, we note that there is no upper bound for f_0: we can generate A extravagantly by an arbitrarily large number of elements. There is a lower bound for f_0, and in fact $\chi_0(A)$ is simply the smallest number of elements that can generate A. Similarly, there is no upper bound for $f_1 - f_0$ (or if we used $f_0 - f_1$, there would be no lower bound): we can hold F_0 fixed, and enlarge F_1 by throwing in superfluous generators. On the other hand, it is reasonable that there is a lower bound for $f_1 - f_0$. In an attempt to make it very small (that is, negative and numerically large), one would takefo large; but it is plausible that this would force us to take f_1 correspondingly large.

Theorem 200. *Let A be an R-module admitting a resolution (54) by jinitely generated free modules. Define $\chi_n(A)$ as above. Then $\chi_n(A) > -\infty$.*

Proof. Let K denote the kernel of $F_{n-1} \to F_{n-2}$. Given a second resolution by modules H_i, let L be the kernel of $H_{n-1} \to H_{n-2}$. By the long Schanuel lemma (Theorem 189) we have

$$K \oplus H_{n-1} \oplus F_{n-2} \oplus \cdots \cong L \oplus F_{n-1} \oplus H_{n-2} \oplus \cdots$$

Now K can be generated by f_n elements. The free module $F_{n-1} \oplus H_{n-2} \oplus \cdots$ has rank $f_{n-1} + h_{n-2} + \cdots$ and cannot be generated by fewer elements. Hence

$$f_n + h_{n-1} + f_{n-2} + \cdots \geqq f_{n-1} + h_{n-2} + \cdots$$

and we deduce

$$f_n - f_{n-1} + f_{n-2} + \cdots \geqq -h_{n-1} + h_{n-2} + \cdots \tag{55}$$

Think of the H-resolution as fixed, while the F-resolution is variable. Then the right side of (55) provides us with a fixed lower bound to the variable expression on the left. Hence

$$\chi_n(A) \geqq -h_{n-1} + h_{n-2} \cdots > -\infty$$

APPENDIX 4-3(a). THE NON-COMMUTATIVE CASE

(1) The first question that arises when we generalize to a non-commutative ring R is the invariance of the number of basis elements in a free R-module. Call this condition IBN. A general ring R need not satisfy IBN. We could transact some business without IBN (for example in the Grothendieck style) but we shall take the easy way out and assume IBN outright. Then $\chi(A)$ is well defined for any FFR module.

(2) Theorem 192, asserting the positivity of the Euler characteristic, fails in the non-commutative case, as easy examples show.

(3) Stallings's result (Theorem 198) survives in the form $\chi(A)T(y) = 0$ where y is a central element in the annihilator of A, and T is the trace that is definable in an arbitrary ring R. (Let C be the set of all sums of additive commutators $ab - ba$. Make R/C into an additive group, and let T be the natural mapping $R \to R/C$.)

In Stallings's application, R is the integral group ring ZG of a group G, and A is Z, made into a module by having G act trivially. The annihilator of A is the augmentation ideal I_G (the set of all elements $\Sigma n_i g_i$ in ZG with $\Sigma n_i = 0$). One concludes easily: if A is FFR, then G has no finite conjugate classes $\neq 1$.

(4) Swan's result (Theorem 200) works in the non-commutative case provided we strengthen IBN to the following statement: a free R-module on n basis elements cannot be spanned by fewer than n elements (see [14] for a full discussion of these two conditions and a still stronger IBN).

APPENDIX 4-3(b). THE FITTING INVARIANTS

We shall sketch the definition and properties of the Fitting invariants, and exhibit an extension of Theorems 194–96 in which the exact value of the Euler characteristic plays a role.

Let R be any ring and let A be a finitely generated R-module. Pick generators $a_1, \ldots, a_n$ for A. Let F be a free R-module with basis $u_1, \ldots, u_n$. Resolve A:

$$0 \to K \to F \to A \to 0$$

by sending u_i into a_i. We define the first Fitting invariant $F_1(A)$ of A to be the ideal in R generated by all $n \times n$ determinants whose rows are elements of K. In detail: we form matrices (c_{ij}) where, for each i, $c_{i1}u_1 + \cdots + c_{in}u_n \in K$, and let $F_1(A)$ be the ideal generated by the determinants $|c_{ij}|$. It is clear that instead of using all possible rows of K, we could equally well restrict ourselves to a set of rows spanning K.

More generally, for each integer k from 1 to n, define $F_k(A)$ to be the ideal generated by all $n+1-k \times n+1-k$ subdeterminants of the matrices (c_{ij}). Finally, for $k > n$, $F_k(A)$ is defined to be R.

We outline the proof that the F's are indeed invariant. It suffices to compare the F's obtained from the generating set $a_1, \ldots, a_n$ with those obtained when an additional generator b is added, for by successive steps of this kind we can compare two generating sets $a_1, \ldots, a_n$ and $b_1, \ldots, b_m$ with the big set $a_1, \ldots, a_n, b_1, \ldots, b_m$. Suppose $t_1a_1 + \cdots + t_na_n + b = 0$. Then as a spanning set of relations on $a_1, \ldots, a_n, b$, we can take a spanning set on $a_1, \ldots, a_n$ augmented with a zero at the end, together with the one additional relation

$$t_1, \ldots, t_n, 1$$

Routine facts about determinants then show that the F's are the same for both generating sets of A.

$F_1(A)$ is closely connected with the annihilator J of A: it is easily seen that $J^n \subset F_1 \subset J$.

Further facts we need are: **(1)** the Fitting invariants behave perfectly under localization, that is, $F_k(A_S) = F_k(A)_S$; *(2)* if A is free on m generators, then $F_k(A) = 0$ for $k \leqq m$ and $F_k(A) = R$ if $k > m$. Then the methods of Theorems 194–95 lead to the following result.

Theorem. *Let A be an FFR module over a Noetherian ring, and suppose that $\chi(A) = m$. Then $F_k(A) = 0$ for $k \leqq m$ and $F_k(A)$ contains a non-zero-divisor for $k > m$.*

This theorem is, strictly speaking, not a generalization of Theorems **194–95,** since we have replaced the annihilator of A by the (slightly different) first Fitting invariant of A. We can maintain the point of view of annihilators by switching to the invariants proposed by Auslander and Buchsbaum in [4]: the annihilators of the exterior powers of A. For them the theorem under discussion is likewise true.

We close by noting that there is a connection between the above theorem and a theorem of McCoy.

McCoy's Theorem. *Let there be given n linear homogeneous equations in m variables over a ring R. Then there is a non-trivial solution if and only if there exists a non-zero element of R annihilating all $m \times m$ subdeterminants of the matrix of coefficients.*

We do not discuss the virtually trivial "only if" part. In proving the "if" part we may assume that R is Noetherian, since we may drop down to the subring generated over the integers by the finite number of elements involved. Now assume there is no non-trivial solution. This says that the m columns of the coefficient matrix are linearly independent. We may take them as the relations for a module A with n generators. We have that A is FFR with $\chi(A) = n - m$. Since Euler characteristics are non-negative, $n \geqq m$. By the previous theorem, $F_{n-m+1}(A)$ contains a non-zero-divisor. But this is a contradiction, since $F_{n-m+1}(A)$ is the ideal generated by the $m \times m$ subdeterminants,

See [17] for a thorough study of McCoy's theorem in the language of multilinear algebra.

EXERCISES

1. Let

$$0 \to A \to B \to C \to 0$$

be an exact sequence of FFR modules. Prove $\chi(B) = \chi(A) + \chi(C)$. Generalize to long exact sequences.

2. Let $I \neq 0$ be an FFR ideal. Prove: $\chi(I) = 1$, $\chi(R/I) = 0$.

The next three exercises are the analogues, for FFR modules, of the three change of ring theorems of [26]. In all three, R is not necessarily commutative, x is a central non-zero-divisor, and $R^* = R/(x)$.

3. If A is an FFR R*-module, prove that A is an FFR R-module.

4. If A is an FFR R-module and x is a non-zero-divisor on A, prove that A/xA is an FFR R*-module.

5. With the ring R left Noetherian, x in the Jacobson radical, and A a finitely generated R-module on which x is a non-zero-divisor, prove that if A/xA is **FFR** over R^*, then A is **FFR** over R. *(Note:* the following companion statement does not seem to yield to these methods, and we leave it as an open question: if A/xA is **FFR** over R, then A is **FFR** over R.)

6. Let Z be a finitely generated ideal in a ring R. Suppose that for every maximal ideal M, I_M is either all of R_M or 0. Prove that Z is a direct summand of R (that is, $Z = eR$ with e an idempotent).

7. Let R be a Noetherian ring with no idempotents other than 0 and 1. Let A be a finitely generated R-module with $d(A) < \infty$. Prove that the annihilator of A is either zero or contains a non-zero-divisor. *(Hint:* localize, use Theorem **196,** and then use Ex. **6.)**

8. Let R be any Noetherian ring and let A be an R-module with a resolution

$$0 \to G \to F \to A \to 0$$

where F and G are free on n, $n-1$ generators respectively. Pick bases in F and G, thereby getting an $n \times n-1$ matrix. Let $d_1, \ldots, d_n$ be the minors of order $n-1$. Assume $\mathcal{Z}(A) \subset \mathcal{Z}(R)$.

(a) Prove that A is module-isomorphic to the ideal $(d_1, \ldots, d_n)$. *(Hint:* let $a_1, \ldots, a_n$ be the indicated generators of A. Verify $d_i a_j = d_j a_i$ by elementary linear algebra. Observe that there is a non-zero divisor $u = \Sigma t_i d_i$. With $b = \Sigma t_i a_i$, $u a_i = d_i b$.)

(b) Suppose given elements $r, s \in R$ such that $r d_i \in (s)$ for all i and r is a non-zero-divisor. Prove that r is a multiple of s. *(Hint:* note that s must also be a non-zero-divisor. Argue indirectly. Pass to the ring $R/(s)$ and use McCoy's theorem to get a non-trivial solution of the resulting h e a r equations. Move the result back to R, and use the fact that we have all relations on $a_1, \ldots, a_n$ to achieve a contradiction.)

(c) Assume that A is an ideal in R. Prove that $A = t(d_1, \ldots, d_n)$ for some non-zero-divisor t. *(Hint:* combine parts (a) and (b). This exercise is taken from the paper [10] of Burch, and the method comes from the paper [50] of Towber.)

9. Let R be local and A a finitely generated faithful R-module with $d(A) < \infty$. Suppose that $x \in$ R is a non-zero-divisor on both R and A. Prove that the annihilator of A/xA is (x). *(Hint:* with $R^* = R/(x)$ we have $d_{R^*}(A/xA) < \infty$ by Theorem D. By a determinant argument, any y in R annihilating A/xA has a power y^n divisible by x. Use Theorem 196 to deduce that the annihilator of A/xA in R^* must be 0.)

4-4 CHANGE OF RINGS FOR INJECTIVE DIMENSION

In this section we turn to the study of injective dimension. We first summarize the relevant definitions and record two theorems which we shall use.

A module is *injective* if it is a direct summand of any module containing it. Modules A and B are *injectively equivalent* if there exist injective modules P and Q such that $A \oplus$ P is isomorphic to $B \oplus Q$. An exact sequence

$$0 \to A \to Q \to L \to 0$$

with Q injective is a *short injective resolution* of A. The injective equivalence class of L does not depend on the resolution and is denoted by $\mathfrak{I}A$. Injective dimension is now defined in precisely the same way as homological (or projective) dimension. Our notation for it is $id(A)$ or $id_R(A)$.

The following theorem is the injective dual of Theorem B. Its dual proof is left to the reader.

Theorem F. *Let C be a submodule of A and write $B = A/C$.*

(1) If two of the dimensions $id(A)$, $id(B)$, $id(C)$ are finite, so is the third.

(2) If $id(A) > id(B)$, then $id(C) = id(A)$.

(3) If $id(A) < id(B)$, then $id(C) = id(B) + 1$.

(4) If $id(A) = id(B)$, then $id(C) \leqq id(A) + 1$.

Toward the end of the proof of Theorem 202, the law of diminishing returns sets in, and it becomes economical to use the Ext machinery. From that point on, we shall do so freely. We drop the ring subscript when there is no danger of ambiguity, and we write Ext for Ext^1 where appropriate. The following result is Theorem 19 in Part III of [26].

Theorem G. *For any modules A and B, $\mathrm{Ext}(\Re A, B) = 0$ if and only if $\mathrm{Ext}(A, \mathfrak{I}B) = 0$.*

We proceed to prove three theorems concerning change of rings for injective dimension. They are the injective duals of Theorems C, D, and E. Before proving the first we need a preliminary theorem.

Theorem 201. *Let* R *be any ring (not necessarily commutative). Let* x *be a central non-zero-divisor in* R, *and write* $R^* = R/(x)$. *Let* A *be an R-module which is injective as an R*-module. Let* C *be an R-module with* $x \notin Z(C)$. *Then:* $\mathrm{Ext}_R(C, A) = 0$.

Proof, We attack the problem directly by proving that the extensions in question split. **So** we let

$$0 \to A \to E \to C \to 0$$

be an exact sequence. We are to prove that A is a direct summand of E. We note that $A \cap xE = 0$, for if $a \in A \cap xE$, write $a = xe$, $e \in$ E. Then the image of a in E/A is 0. But x is a non-zero-divisor on E/A. Hence $e \in A$, $a \in xA = 0$.

In view of $A \cap xE = 0$, we may look at A as a submodule of E/xE. **As** such (since A is R*-injective), it is a direct summand. From this it is routine to see that A is a direct summand of E.

Theorem 202. *(First theorem on injective change of rings.) Let R be any ring (not necessarily commutative). Let* x *be a central non-zero-divisor in* R, *and write* $R^* = R/(x)$. *Let* A *be a non-zero R*-module with* $id_{R^*}(A) = n < \infty$. *Then* $id_R(A) = n + 1$.

Remark. There is an inequality that is valid under very general circumstances. Let R and T be rings and let a ring homomorphism $R \to T$ be given. Let A be a left T-module. The homomorphism from R to T enables us to look at A as an R-module, and we have $id_R(A) \leqq id_T(A)$ + (weak right dimension of T over R). This appears as the second part of Ex. 5 on page 360 of [113. A proof of the exercise can be given by an appropriate extension of the idea in Theorem 201.

Proof, We argue by induction on n, and begin by treating the case n = 0. We first note that A is not R-injective. For if it were, it would be divisible by x (any homomorphism from (x) into A could be extended to R), and this is compatible with $xA = 0$ only if $A = 0$. **So** it suffices to prove $id_R(A) \leqq 1$. This requires us to prove that $\mathfrak{J}A$ is injective, for which we need to know that $\mathrm{Ext}(B, \mathfrak{J}A) = 0$ for every R-module B. By Theorem G it is equivalent to prove $\mathrm{Ext}(\mathfrak{R}B, A) = 0$. Now any module representing $\mathfrak{R}B$ is a submodule of a projective R-module, and

so has the property that x is not a zero-divisor on it. From Theorem 201 we deduce $\mathrm{Ext}_R(\mathfrak{R}B, A) = 0$.

We have finished the case $n = 0$. Induction on n works quite simply, except when we run into the "ambiguous" case at $n = 1$.

Form an R*-injective resolution of A:

$$0 \to A \to Q \to D \to 0$$

We have $id_{R^*}(D) = n - 1$, so that $id_R(D) = n$ by induction. Also $id_R(Q) = 1$. By Theorem F we conclude $id_R(A) = n + 1$, except that when $n = 1$ we only get the inequality $id_R(A) \leqq 2$.

To complete the proof we assume $id_{R^*}(A) = 1$, $id_R(A) \leqq 1$ and achieve the contradiction that A is R*-injective. It suffices to verify $\mathrm{Ext}_{R^*}(R^*/I^*, A) = 0$ for any left ideal I^* in R*. Since I^* has the form $I/(x)$ with I a left ideal in R containing x, $R^*/I^* \cong R/I$, and so it is equivalent to check $\mathrm{Ext}_{R^*}(R/I, A) = 0$ for such an I. Here in place of R/I we can take the isomorphic module $(x)/xI$.

Next we prove that $\mathrm{Ext}_{R^*}(I/xI, A) = 0$. To do this we begin by noting that $\mathrm{Ext}_R(R/I, \mathfrak{J}A) = 0$ holds since $id_R(A) \leqq 1$. Hence $\mathrm{Ext}_R(\mathfrak{R}R/I, A) = 0$, i. e., $\mathrm{Ext}_R(I, A) = 0$. Take a free resolution of I over R:

$$0 \to K \to F \to I \to 0$$

Note that since $x \notin Z(I)$, we have an induced free resolution of I/xI over R*:

$$0 \to K/xK \to F/xF \to I/xI \to 0$$

$\mathrm{Ext}_R(I, A) = 0$ implies that any homomorphism from K into A can be extended to F. Since $xA = 0$, this is exactly the same as saying that any homomorphism from K/xK can be extended to F/xF. We can derive (Theorem 16 [26]) $\mathrm{Ext}_{R^*}(I/xI, A) = 0$.

The proof of Theorem 202 can now be quickly concluded by an application of the homology sequence for Ext. In view of the exact sequence

$$0 \to \frac{(x)}{xI} \to \frac{I}{xI} \to \frac{I}{(x)} \to 0$$

we have

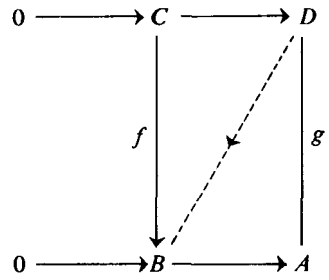
$$\mathrm{Ext}^1_{R^*}(I/xI, A) \to \mathrm{Ext}^1_{R^*}((x)/xI, A) \to \mathrm{Ext}^2_{R^*}(I/(x), A). \tag{56}$$

We have just proved that the left member of (56) vanishes. The right member vanishes since $id_{R^*}(A) = 1$. Hence the middle member vanishes, and we have seen that this suffices to finish the proof of Theorem 202.

We proceed to dualize Theorem **D.** There are in fact two duals. Our real objective is Theorem 205, but we prove it by first proving the dual version given by Theorem 204. Theorem 203 is a preliminary one that will also be used below in proving Theorem 207. Note that the dual of Theorem 203 is the assertion that A/IA is projective if A is projective. (Compare Propositions 6.1 and 6.1*a* on page 30 of [11].)

Theorem 203. *Let I be a two-sided ideal in a (not necessarily commutative) ring* R, *let A be an injective R-module, and let B be the submodule of A annihilared by I. Then, as an (R/I)-module, B is injective.*

Proof. To test R/I-injectivity of **B,** we take R/I-modules $C \subset D$ and a homomorphism $f : C \to B$; we must extend f to D. In the diagram,



the composite map $C \to A$ extends to $g : D \to A$ since A is R-injective. But since D is annihilated by I, the image of g has to lie in **B,** as required.

Theorem 204. *Let* R *be a (not necessarily commutative) ring and x a central non-zero-divisor in* R. *Write $R^* = R/(x)$. Let A be an* R*-module satisfying $A = xA$, and let ${}_xA$ be the submodule of A annihilated by x. Then: $id_{R^*}({}_xA) \leqq id_R(A)$.*

Proof. The proof is exactly dual to that of Theorem **D,** but we give it for completeness.

If $id_R(A) = \infty$, there is nothing to prove. Assume $id_R(A) = n < \infty$. We make an induction on n. If $n = 0$, we quote Theorem 203. Assume $n > 0$, and make an injective resolution of A:

$$0 \to A \to Q \to D \to 0 \tag{57}$$

From this we get the exact sequence

$$0 \to {}_xA \to {}_xQ \to {}_xD \to 0 \tag{58}$$

the subscript x preceding each module denoting passage to the submodule annihilated by **x.** The exactness of (58) is routine except for the verification that ${}_xQ \to {}_xD$ is onto. So let $d \in D$ satisfy $xd = 0$. We have some $q \in$ Q mapping into d. Then xq lies in the kernel A. Since $A = xA$ we can write $xq = xa$ with $a \in A$. We thereupon correct q to $q_1 = q - a$, and have $xq_1 = 0, q_1 \to d$. (What we have just done amounts to a part of the snake diagram mentioned below.)

Now $id_R(D) = n - 1$, from (57). Furthermore, $xD = D$ since xQ = Q. By induction, $id_{R^*}({}_xD) \leqq n - 1$. Since ${}_xQ$ is R*-injective by Theorem 203, we derive $id_{R^*}({}_xA) \leqq n$ from *(58).*

Theorem 205. *(Second theorem on injective change of rings.) Let* R *be a (not necessarily commutative) ring and x a central element in* R. *Write $R^* = R/(x)$. Let A be an R-module and suppose* **x** *is a non-zero-divisor on both* R *and A. Then:*

$$id_{R^*}(A/xA) \leqq id_R(A) - 1$$

except when A is R-injective (in which case $A = xA$).

Proof. We may assume $id_R(A) = n$ with $1 \leqq n < \infty$. Perform the injective resolution **(57),** so that $id_R(D) = n - 1$. We claim that

$${}_xD \cong {}_xQ \oplus A/xA \tag{59}$$

Since $id_{R^*}({}_xD) \leqq n - 1$ by Theorem 204, $id_{R^*}(A/xA) \leqq n - 1$ is a consequence of (59). Thus, a proof of (59) will suffice.

An attractive proof of (59) can be based on the exact sequence

$$0 \to {}_xA \to {}_xQ \to {}_xD \to A/xA \to Q/xQ \to D/xD \to 0$$

obtained from the snake diagram. Here ${}_xA = 0$ since $x \notin Z(A)$, $Q/xQ = 0$ since Q is injective and $x \notin Z(R)$, and ${}_xQ$ is R*-injective by Theorem 203. We deduce (59).

We sketch a direct alternative discussion. Let E be the image of ${}_xQ$ in ${}_xD$. For any $a \in A$ we can write $a = xq$ ($q \in$ Q), since Q = xQ; then send q into its image in D. This induces *an* isomorphism of A/xA into ${}_xD$ and the image is a complementary direct summand of E.

For Theorem 206 we do not have an analogue of the method used in proving Theorem E. We rely therefore on the alternative method outlined on p. 179 of [26], and this forces us to assume that the underlying ring is commutative.

Theorem ***206.*** ***(Third theorem on injective change of rings.) Let*** R ***be a commutative Noetherian ring, x an element in the Jacobson radical of*** R, ***and write*** $R^* = R/(x)$. ***Let A be a finitely generated non-zero R-module with*** $x \notin Z(A)$. ***Then*** $id_R(A) = id_R(A/xA)$. ***If further*** $x \notin Z(R)$, $id_R(A) = 1 + id_{R^*}(A/xA)$.

Proof. From the exact sequence

$$0 \to A \xrightarrow{x} A \to A/xA \to 0$$

where the x above the arrow identifies the map as multiplication by x, we derive

$$\text{(60)} \qquad \operatorname{Ext}^n_R(B, A) \xrightarrow{x} \operatorname{Ext}^n_R(B, A) \to \operatorname{Ext}^n_R(B, A/xA) \to \operatorname{Ext}^{n+1}_R(B, A)$$

where B is any R-module. Assume $id_R(A/xA) = n - 1 < \infty$. Then the second to last term of (60) vanishes. If B is finitely generated, so is $\operatorname{Ext}^n_R(B, A)$. By (60) and the Nakayama lemma, $\operatorname{Ext}^n_R(B, A) = 0$. The knowledge that this holds for every finitely generated B is sufficient for us to conclude $id_R(A) \blacksquare n - 1$.

Conversely, assume $id_R(A) \blacksquare n - 1$. Then the second and fourth terms of (60) vanish. Hence the third vanishes as well. We deduce $id_R(A/xA) \leqq n - 1$. This, together with the result in the preceding paragraph, shows that $id_R(A)$ and $id_R(A/xA)$ are equal. ***(Note:*** the reasoning in this paragraph can be replaced by a reference to the injective dual of Theorem **B.)**

Now assume $x \notin Z(R)$ as well. If $id_R(A) = \infty$, then $id_R(A/xA) = \infty$ as we have just seen. Then by Theorem 202, $id_{R^*}(A/xA) = \infty$. If $id_R(A)$ is finite, then $id_{R^*}(A/xA)$ is finite by Theorem 205. Theorem 202 then yields the final statement of the theorem.

Remark. When the injective dimensions occurring in Theorem 206 are finite, the facts follow from the identification with grade to be given in Theorem 214. (The proof of Theorem 214 will not use Theorem 206, so this reasoning is not circular.) However, we think it useful to give both proofs.

EXERCISES

1. Prove the following fourth version of the second change of rings theorem: if x is a central element in R, $R^* = R/(x)$, A is an R-module that is not projective, and x is a non-zero-divisor in R with $xA = A$, then $d_{R^*}(_xA) = d_R(A) - 1$. ***(Hint:*** deduce this from Theorem C just as Theorem 205 was deduced from Theorem 204.)

2. The following theorem was proved by Rees in [43]: if x is a central element in R, $R^* = R/(x)$, A and B are R-modules, $xB = 0$, and x is a non-zero-divisor on both R and A, then

$$\operatorname{Ext}^n_R(B, A) \cong \operatorname{Ext}^{n-1}_{R^*}(B, A/xA)$$

Use Rees's theorem to give a brief proof of Theorem 205.

3. Prove the following dual of Rees's theorem: with the notation of Ex. 2

$$\operatorname{Ext}^n_R(A, B) \cong \operatorname{Ext}^n_{R^*}(A/xA, B)$$

(Hint: one method is to use a short free resolution

$$0 \to K \to F \to A \to 0$$

and the induced resolution

$$0 \to K/xK \to F/xF \to A/xA \to 0$$

Assuming the result for $n - 1$, we have $\operatorname{Ext}^n_R(A, B) \cong \operatorname{Ext}^{n-1}_R(K, B) \cong \operatorname{Ext}^{n-1}_{R^*}(K/xK, B) \cong \operatorname{Ext}^n_{R^*}(A/xA, B)$. Special arguments are needed for $n = 0, 1$. ***Note:*** this identity (for $n = 1$) can replace the portion of the argument in Theorem 202 that deduced $\operatorname{Ext}_{R^*}(I/xI, A) = 0$ from $\operatorname{Ext}_R(I, A) = 0$.)

4. Prove the two remaining duals of the Rees theorem. With R, x, R^* as usual, $A = xA$ and $xB = 0$,

$$\operatorname{Ext}^n_R(A, B) \cong \operatorname{Ext}^{n-1}_{R^*}(_xA, B)$$
$$\operatorname{Ext}^n_R(B, A) \cong \operatorname{Ext}^n_{R^*}(B, {}_xA)$$

(See [39] for more on theorems of this type.)

4-5 GORENSTEIN RINGS

We begin this section with a summary of essential extensions and injective envelopes, a theory due to Eckmann and Schopf **[16]**; see also pages **102–3** of **[30]**. The base ring is allowed to be non-commutative. Proofs that are not routine are sketched.

(1) Let A $\subset B$ be modules. We say that B is an *essential* extension of A if for any non-zero submodule of S of B, $S \cap$ A $\neq 0$.

(2) If A $\subset B \subset C$, B is an essential extension of A, and C is an essential extension of B, then C is an essential extension of A.

(3) Let $\{B_i\}$ be a chain of modules lying between modules A and C. If each B_i is an essential extension of A, so is $\cup B_i$.

From (3) we deduce:

(4) Let A $\subset C$ be modules. Then any essential extension of A within C can be enlarged to a maximal essential extension of A.

(5) Let A be a submodule of C and let B be a submodule of C maximal with respect to disjointness from A. Then A may be regarded as a submodule of C/B; as such, C/B is essential over A.

(6) Let A $\subset Q$ be modules with Q injective, and let E be an intermediate module that is a maximal essential extension of A. Then E is a direct summand of Q, and therefore is injective. In fact, any submodule B of Q that is maximal with respect to disjointness from E forms a complementary summand. To see this, we treat E as a submodule of Q/B. By (5), Q/B is essential over A. The map from Q/B to

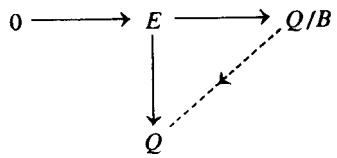


FIGURE 8

Q in Figure 8 exists since Q is injective. Its kernel is 0 by the essentiality of Q/B over E. Hence we may regard the chain of modules A $\subset E \subset Q/B$ as being placed inside Q. The maximality of E therefore forces Q/B = E, i. e., $B + E = Q$, and Q is the direct sum of E and B, as required.

(7) Thus any module admits an essential injective extension. We proceed to the uniqueness.

(8) Let E and E_1 be essential injective extensions of A. Then there exists an isomorphism of E onto E_1, which is the identity on A. To see this, note that the map A $\rightarrow E_1$ can be extended to E since E_1 is injective. By the essentiality of E over A, the extended map has kernel 0. The image is thus a direct summand of E_1, and must be all of E_1 since E_1 is essential over A.

The uniqueness justifies our calling an essential injective extension of A an *injective envelope* of A. Our notation will be $E(A)$.

We proceed to the study of local rings which admit a non-zero finitely generated module of finite injective dimension. In the, first instance we assume the module to be injective.

Theorem *207.* ***Let*** *R be a local ring.* R *admits a finitely generated non-zero injective module if and only if* R *is zero-dimensional.*

Proof. Suppose A $\neq 0$ is finitely generated and injective. We make an indirect proof, supposing $\dim(R) \geqq 1$. We claim that for some prime ideal P different from the maximal ideal, R/P admits a non-zero homomorphism into A. For we know that A contains a submodule isomorphic to R/Q for some prime ideal Q. If $Q \neq M$, we are done, while if $Q = M$, any R/P admits a homomorphism onto R/M.

Take such a prime ideal P, and write B = R/P. Let **x** be a non-unit not contained in P; then **x** is a non-zero-divisor on B. In Figure 9 for any $f: B \rightarrow$ A the dotted map g exists since A is injective. Hence, Hom(B, A) = x Hom(B, A), and Hom(B, A) = 0 by the Nakayama lemma, a contradiction.

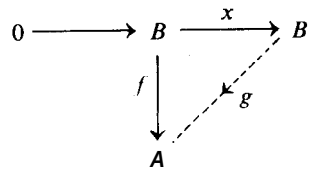


FIGURE 9

Conversely, suppose R is zero-dimensional. We claim that A = $E(R/M)$ is finitely generated. If $M^n = 0$, we prove this by induction on n. Let B be the submodule of A annihilated by M^{n-1}. By Theorem **203,** B is R*-injective, where $R^* = R/M^{n-1}$. Evidently $B = E(R^*/M^*)$

where M^* is the maximal ideal of R*. By induction, B is finitely generated. Hence so is MA, since MA $\subset$ B. Now let $x_1, \ldots, x$, be a set of generators of M. In the homomorphism

$$A \to x_1 A \oplus \ldots \oplus x_m A$$

obtained by mapping a ϵ A into the m-ple $x_1 a, \ldots, x_m a$, the image is finitely generated and the kernel is isomorphic to R/M (since A is essential over R/M). Hence A is finitely generated.

In the next two theorems we allow the module A to be non-finitely-generated ; possibly this will be useful in future investigations.

Theorem 208. Let R be local with maximal ideal M. Let B be a finitely generated R-module satisfying $d(B) = 1$. Let A be an R-module, not necessarily finitely generated, satisfying $\mathrm{Ext}(B, A) = 0$. Then: A = MA.

Proof. Form a minimal resolution

$$0 \to K \to F \to B \to 0$$

of B, so that K $\subset$ MF and K is free and non-zero. From $\mathrm{Ext}(B, A) = 0$ we deduce that any homomorphism from K to A can be extended to F. Any element of A is eligible to be in the range of such a homomorphism; hence A = MA.

Theorem 209. Let R be local with maximal ideal M, and let A be an R-module, not necessarily finitely generated. Assume $id(A) < G(R)$. Then: A = MA.

Proof. Let $G(R) = n$. There exists a finitely generated R-module B with $d(B) = n$; for instance we may take R divided by an R-sequence of length n. Then $d(\mathfrak{R}^{n-1}B) = 1$. Since $id(A) < n$ we have $\mathrm{Ext}(\mathfrak{R}^{n-1}B, A) = 0$. We quote Theorem 208.

From Theorem 209 and the Nakayama lemma we deduce at once:

Theorem 210. Let R be local with maximal ideal M, and let A be a finitely generated non-zero R-module. Then: $id(A) \geqq G(R)$.

Our first main objective is Theorem **214**; we will need three preliminary theorems.

Theorem 211. Let R be local with maximal ideal M, and let P be a prime ideal *different* from M. Let A be a finitely generated R-module. Assume that $\mathrm{Ext}^{i+1}(R/Q, A) = 0$ for every prime ideal Q properly containing P. Then: $\mathrm{Ext}^i(R/P, A) = 0$.

Proof. Pick x in M but not in P. Write $B = R/P$. Then x $\notin \mathcal{Z}(B)$ and the exact sequence

$$0 \to B \xrightarrow{x} B \to B/xB \to 0$$

induces

$$\mathrm{Ext}^i(B, A) \xrightarrow{x} \mathrm{Ext}^i(B, A) \to \mathrm{Ext}^{i+1}(B/xB, A), \tag{61}$$

Now $B/xB \cong R/(P, x)$. We apply Ex. 7 in §2-1 to the module B/xB, noting that the modules that occur in the resulting series are of the form R/Q with Q a prime ideal properly containing P. By the "additivity" of the vanishing of Ext, we deduce that the last term of (61) vanishes. By the Nakayama lemma, $\mathrm{Ext}^i(B, A) = 0$.

Theorem 212. Let R be local with maximal ideal M, let A be afinitely generated R-module, and let n be an integer $\geqq$ 1. Assume $\mathrm{Ext}^i(R/M, A) = 0$ *for all* $i \geqq n$. Then: $id(A) < n$.

Proof. By iterated use of Theorem 211 we get that $\mathrm{Ext}^i(R/P, A) = 0$ for every prime ideal P. From this (Ex. 7 in §2-1) we deduce that $\mathrm{Ext}^i(C, A) = 0$ for every finitely generated R-module C, and this implies $id(A) < n$.

The next theorem is a simple property of Ext, valid over arbitrary rings; it is explicitly recorded for the reader's convenience.

Theorem 213. Let

$$0 \to C \to D \to D/C \to 0$$

be an exact sequence of R-modules, and A another R-module. If for some integer k we have $\mathrm{Ext}^k(D, A) = 0$ and $\mathrm{Ext}^{k+1}(D/C, A) = 0$, then $\mathrm{Ext}^k(C, A) = 0$.

Proof. This is immediate from the exact sequence

$$\mathrm{Ext}^k(D, A) \to \mathrm{Ext}^k(C, A) \to \mathrm{Ext}^{k+1}(D/C, A)$$

Theorem 214. *Let* R *be local with maximal ideal M and let A be a non-zero finitely generated R-module with* $id(A) < \infty$. *Then* $id(A) = G(R)$.

Proof. Let $G(R) = n$. Theorem 210 gives us $id(A) \geqq n$ and it remains to prove $id(A) \leqq n$. Assume on the contrary that $id(A) = k > n$.

Let $x_1, \ldots, x_n$ be a maximal R-sequence in R, and write

$$D = R/(x_1, \ldots, x_n).$$

Since $M \subset \mathcal{Z}(D)$ we have that R/M is isomorphic to a submodule C of D. We have $\mathrm{Ext}^k(D, A) = 0$ since $d(D) = n$ and $k > n$. We have $\mathrm{Ext}^{k+1}(D/C, A) = 0$ since $id(A) = k$. By Theorem 213, $\mathrm{Ext}^k(C, A) = 0$. Since $\mathrm{Ext}^i(C, A)$ also vanishes for $i > k$, we deduce from Theorem 212 the contradiction $id(A) \leqq k - 1$.

Definition. A local ring R is called a *Gorenstein* ring if $id(R) < \infty$.

Theorem 215. *A local Gorenstein ring* R *is Macaulay.*

Proof. Let $id(R) = n$. By Theorem 214, $G(R) = n$. We argue by induction on n.

$n = 0$. Then R is injective and we quote Theorem 207.

$n > 0$. There exists in M a non-zero-divisor x. Write $R^* = R/(x)$. By Theorem 205, $id_{R^*}(R^*) < \infty$, i. e., R^* is a Gorenstein ring. By induction R^* is Macaulay, and by Theorem 156, R is Macaulay.

Remark. This is the first time in the present section that we have made use of the change of rings theorems of §4-4. Thus Theorems 207–214 could have preceded §4-4.

The next result is Theorem 2.2 in [29].

Theorem 216. *Let* R *be a local Gorenstein ring, A a finitely generated R-module. Then A has finite projective dimension if and only if it has finite injective dimension.*

Proof. Suppose $d(A) < \infty$. Then, since finitely generated free R-modules have finite injective dimension, an obvious induction on $d(A)$ shows that $id(A) < \infty$.

Suppose $id(A) < \infty$. We make an induction on $n = G(R)$. If $n = 0$, then (Theorem 215 or 207) R is zero-dimensional. Furthermore, A and

R are injective. One easily sees that any finitely generated injective R-module is a direct sum of copies of $E(R/M)$. (As a matter of fact, $R \cong E(R/M)$.) Hence A is free.

So we assume $n > 0$. Pick $x \notin \mathcal{Z}(R)$, and write $R^* = R/(x)$. We form the resolution

$$0 \to K \to F \to A \to 0$$

with F free. Since $id_R(F) < \infty$, we have $id_R(K) < \infty$. By Theorem 205, $id_{R^*}(K/xK) < \infty$. Since $G(R^*)$ is smaller than n, and (as we noted in the proof of Theorem 215), R^* is Gorenstein, we have $d_{R^*}(K/xK) < \infty$. Then, by Theorem E, $d_R(K) < \infty$, and $d_R(A) < \infty$ is a consequence.

Theorem 217. *Let* R *be a local ring with* $G(R) = n$. *Let A and* B *be finitely generated non-zero R-modules with* $id(A) < \infty$. *Then:* $\mathrm{Ext}^r(B, A) = 0$ *for* $r > n - G(B)$.

Proof. We proceed by induction on $G(B)$. If $G(B) = 0$, the conclusion is immediate, since $id(A) = n$ by Theorem 214.

Assume $G(B) > 0$ and take $x \notin \mathcal{Z}(B)$. From the exact sequence

$$0 \to B \xrightarrow{x} B \to B/xB \to 0$$

we get the exact sequence

$$\mathrm{Ext}^r(B, A) \xrightarrow{x} \mathrm{Ext}^r(B, A) \to \mathrm{Ext}^{r+1}(B/xB, A) \to \mathrm{Ext}^{r+1}(B, A) \tag{62}$$

We have $\mathrm{Ext}^{r+1}(B/xB, A) = 0$ by induction, since $G(B/xB) = G(B) - 1$ and $(r + 1) + G(B/xB) > n$. We deduce $\mathrm{Ext}^r(B, A) = 0$ from (62) and the Nakayama lemma.

Theorem 218. *Let* R, *n, A and B be as in Theorem 217. Assume* $G(B) \leqq n$, *and set* $r = n - G(B)$. *Then* $\mathrm{Ext}^r(B, A) \neq 0$.

Remark. We shall see in a moment (Theorem 219) that the hypothesis $G(B) \leqq n$ is redundant. However, the proof of Theorem 219 uses Theorem 218.

Proof. First assume $G(B) = 0$. Suppose, by way of contradiction, that $\mathrm{Ext}^r(B, A) = 0$. Since $G(B) = 0$, B contains an isomorphic copy (say C) of R/M. From Theorem 213, with k replaced by n and D by B, we get $\mathrm{Ext}^n(R/M, A) = 0$. Furthermore, $\mathrm{Ext}^i(R/M, A) = 0$ for $i > n$

since $id(A) = n$ by Theorem 214. Then Theorem 212 gives us the contradiction $id(A) < n$.

We assume $G(B) > 0$ and proceed by induction on $G(B)$. Let x be a non-zero-divisor on B. Applying our induction to B/xB we get $\mathrm{Ext}^{r+1}(B/xB, A) \neq 0$. Furthermore, by Theorem 217, $\mathrm{Ext}^{r+1}(B, A) = 0$. These facts, in conjunction with (62), yield $\mathrm{Ext}^{r}(B, A) \neq 0$.

Theorem 219. ***Let*** R ***be a local ring that admits a non-zero finitely generated module A with finite injective dimension. Then any finitely generated non-zero R-module*** B ***has grade at most*** $G(R)$.

Proof. Suppose the contrary. Then, by dividing B by a suitable R-sequence, we can reach a module C with $G(C) = n + 1$, where $n = G(R)$. Then, with $x \notin Z(C)$, $G(C/xC) = n$. By Theorem 218, with C/xC playing the role of B, we have $\mathrm{Hom}(C/xC, A) \neq 0$. Hence $\mathrm{Hom}(C, A) \neq 0$. However,

$$\mathrm{Hom}(C, A) \xrightarrow{x} \mathrm{Hom}(C, A) \to \mathrm{Ext}^1(C/xC, A)$$

is exact, and $\mathrm{Ext}^1(C/xC, A) = 0$ by Theorem 217 (with $r = 1$ and B replaced by C/xC). This contradicts the Nakayama lemma.

We now exhibit a chain of five successive statements that can be made about a local ring R.

I. R is regular.

II. R is Gorenstein.

III. R is Macaulay.

IV. R admits a finitely generated non-zero module with finite injective dimension.

V. The grade of any finitely generated module is at most $G(R)$.

We have I $\Rightarrow$ II and II $\Rightarrow$ III, and these implications cannot be reversed. III $\Rightarrow$ IV, for if J is an ideal generated by a maximal R-sequence in R, we need only take a non-zero finitely generated injective (R/J)-module (Theorems 207 and 202). IV $\Rightarrow$ V by Theorem 219. Note that III $\Rightarrow$ V follows from Ex. 22 in §3-1, and so what we have done is to "factor" that implication into two parts of independent interest.

Examples can be found in which property V holds but not IV. In [29] Levin and Vasconcelos prove IV $\Rightarrow$ III for rings of grade 1. Also noteworthy is their proof that if $id(A) < \infty$ then the annihilator of A is zero or contains a non-zero-divisor, the exact injective analogue of Theorem 196.

EXERCISES

In exercises 1–8, R is local with maximal ideal M, and A is a finitely generated R-module.

1. Suppose that M can be generated by $1 + G(R)$ elements. Prove that R is a Gorenstein ring. ***(Hint:*** by dividing by an element x that is not a zero-divisor and not in M^2, you can reduce successively down to the case where M is principal. Note that this is an improvement on Ex. 1(a) in §3-3.)

2. If $\mathrm{Ext}^i(M, A) = 0$ for all $i \geqq n$, prove that $id(A) \leqq n$. ***(Hint:*** $\mathrm{Ext}^i(M, A) \cong \mathrm{Ext}^{i+1}(R/M, A)$.)

3. If $id(A) = n$, prove that $\mathrm{Ext}^n(R/M, A) \neq 0$.

4. If $id(A) = \infty$, prove that $\mathrm{Ext}^i(R/M, A) \neq 0$ for infinitely many i.

5. If $x \notin Z(R)$, prove that R is Gorenstein if $R/(x)$ is Gorenstein. ***(Note:*** the converse also is true, and came up in the proofs of Theorems 215 and 216.)

6. If $id(M) < \infty$ prove that R is regular. ***(Hint:*** for $x \notin M^2$ use the fact that $M/(x)$ is a direct summand of M/xM to make a reduction to $R/(x)$.)

7. Assume that $id(A) = k < \infty$. Let B be a finitely generated R-module. Prove that $G(B)$ equals the largest integer m such that $\mathrm{Ext}^{k-m}(B, A) \neq 0$.

8. Suppose R is k-dimensional, and that $\mathrm{Ext}^i(R/M, R)$ vanishes for $k + 1$ consecutive values of i. Prove that R is Gorenstein.

9. Let R be any ring, S a multiplicatively closed set in R, A and B R-modules. Construct a natural map f from $(\mathrm{Hom}_R(A, B))_S$ to $\mathrm{Hom}_{R_S}(A_S, B_S)$.

(a) If A is finitely generated, prove that f is one-to-one.

(b) If A is finitely presented, prove that f is onto. (A module A is finitely presented if it is finitely generated, and when it is resolved

$$0 \to K \to F \to A \to 0$$

with F free and finitely generated, then K is finitely generated. Note that by Schanuel's lemma this does not depend on the choice of the resolution.)

10. Suppose that R is Noetherian, and that A is an injective R-module. Prove that A_S is R_S-injective for any multiplicatively closed set S. ***(Remark:*** it is furthermore true that A_S is R-injective; indeed any injective R_S-module is also R-injective.)

11. Let R be a Gorenstein local ring, and let P be a prime ideal in R. Prove that R_P is Gorenstein.

We define a global Gorenstein ring R by the assumptions that R is Noetherian and that the localization R_M is Gorenstein for any maximal ideal M.

12. If R is Gorenstein and S multiplicatively closed, prove that R_S is Gorenstein.

13. If R is Gorenstein and x is a non-zero-divisor in R, prove that $R/(x)$ is Gorenstein.

14. Suppose that R is Noetherian, that x is a non-zero-divisor in the Jacobson radical of R, and that $R/(x)$ is Gorenstein. Prove that R is Gorenstein.

15. Let R be Noetherian, and let $A \subset B$ be R-modules with B an essential extension of A. Prove that for any multiplicatively closed set S, B_S is an essential extension of A_S. *(Hint:* given a non-zero element c^* in B_S, we have to prove that As meets the submodule spanned by c^*. Pick $c \in B$ mapping on the numerator of c^*. Among all elements $sc (s \in S)$, pick one, say d, with maximal annihilator. Use the fact that $A \cap Rd \neq 0$.)

16. Let R be Noetherian, and A an R-module such that A_M is R_M-injective for every maximal ideal M. Prove that A is injective. *(Hint:* localize an essential injective resolution of A, and use Ex. **15.)**

17. Let R be a Noetherian ring. Prove that the following statements are equivalent: (a) $id(R) = n < \infty$, (b) R is Gorenstein and has Krull dimension n.

18. Let R be a Gorenstein ring, and A a finitely generated R-module. Prove that for any n, the annihilator J of $\mathrm{Ext}^n(A, R)$ is either R or has rank $\geqq n$. *(Hint:* for P a prime ideal with rank $(P) < n$, it suffices to prove $J \not\subset P$. This is equivalent to $\mathrm{Ext}^n(A_P, R_P) = 0$.)

19. (This exercise is the injective dual of Ex. 17 in §4-1.) Let R be local with maximal ideal M, let x be a non-zero-divisor not contained in M^2, and let A be a finitely generated R-module annihilated by x. Write $R^* = R/(x)$. Prove: if $id_R(A) < \infty$, then $id_{R^*}(A) < \infty$. *(Hint:* we have $\mathrm{Ext}^n_R(M, A) = 0$ for large n. By the dual Rees theorem of Ex. **3** in §4-4, $\mathrm{Ext}^{n-1}_{R^*}(M/xM, A) = 0$. But $M/xM \cong M^* \oplus R^*/M^*$, where M^* is the maximal ideal of R^* (see the proof of Theorem 13 **[26].)** Hence $\mathrm{Ext}^{n-1}_{R^*}(R^*/M^*, A) = 0$ for large n. Use Theorem **212.)**

20. Treat Ex. 17 in §4-1 itself by the method of the preceding exercise. *(Hint:* use the Rees theorem (Ex. **2** in §4–4) and Ex. **2** in §4-1.)

4-6 DUALITY

In this section we shall show that for dimension $\leqq 1$ the Gorenstein property is equivalent to an appropriately formulated duality.

In the zero-dimensional case the decisive argument is given in Theorem **220.** It is routine to proceed from Theorem **220** to the full duality of modules of finite length (see Ex. 1).

Theorem *220. Let R be local with maximal ideal M, let E denote an injective envelope of R/M, let* A *be an R-module of finite length, and write $B = Hom_R(A, E)$. Then B also has finite length, and its length is equal to that of* **A.**

Proof. To emphasize the potential duality between A and **B,** we shall use the inner product notation (a, b) to denote the value of the homomorphism b at the element a.

Since A has finite length, we have $M^n A = 0$ for some power M^n. We insert between A and 0 the chain of submodules

$$A \supset MA \supset M^2A \supset \cdots \supset M^{n-1}A \supset M^nA = 0$$

Each quotient $M^iA/M^{i+1}A$ is a finite-dimensional vector space over the field R/M.

The module B is likewise annihilated by M^n. Let **B,** be the submodule of B annihilated by M^i. We insert the'intermediate submodules

$$0 \subset B_1 \subset B_2 \subset \cdots \subset B_{n-1} \subset B_n = B$$

We shall prove that the vector space B_{i+1}/B_i is paired to $M^iA/M^{i+1}A$ in non-singular fashion; this will evidently prove that the length of B is finite and equal to the length of A. We have that (MA, B_{i+1}) is annihilated by M. We denote by E_1 the submodule of E annihilated by M and note that E_1 is isomorphic to R/M (since E is an injective envelope of R/M). We obtain in this way a pairing of $M^iA/M^{i+1}A$ and B_{i+1}/B_i. In order to see that this pairing is non-singular we have two things to prove.

(a) If $y \in B_{i+1}$ and $(MA, y) = 0$, then $y \in B$,. For we have $(A, M^iy) = 0$ and hence $M^iy = 0$.

(b) If $x \in MA$ and $(x, B_{i+1}) = 0$, then $x \in M^{i+1}A$. For suppose on the contrary that $x \notin M^{i+1}A$. Let x^* denote the image of x in $M^iA/M^{i+1}A$;

note that $Mx^* = 0$. We can start a homomorphism of $M^iA/M^{i+1}A$ into E by sending x^* into a non-zero element of E_1, and then we can extend by the injectivity of E. In this way we get a homomorphism of MIA into E that annihilates $M^{i+1}A$ but not x, a contradiction to $(x, B_{i+1}) = 0$. This concludes the proof of Theorem 220.

Theorem 221. *Let* R *be a zero-dimensional local ring with maximal ideal* M. *Then* R *is Gorenstein if and only if the annihilator of* M *is one-dimensional (as a vector space over* R/M).

Proof. Suppose that R is Gorenstein, and that consequently R is injective as an R-module. Let Z denote the annihilator of M, let I_0 be a one-dimensional subspace of I, and let J be an injective envelope of I_0 within R. Then J is a direct summand of R. Since R is local, this entails J = R. Hence R is an essential extension of I_0, and therefore I must coincide with I_0.

Conversely, suppose that I is one-dimensional. We note that every non-zero ideal of R contains a non-zero element annihilated by M, and hence contains I. Let E be an injective envelope of I. The isomorphism of I into E extends to a homomorphism of R into E which, by what we have just remarked, is necessarily one-to-one. By Theorem 220, R and E have the same length. Hence R $\cong E$ and R is injective, as required.

Remark. In the literature zero-dimensional Gorenstein rings are usually called ***quasi-Frobenius,*** and the non-commutative generalization has been thoroughly studied.

We proceed, in Theorem 222, to a characterization of one-dimensional local Gorenstein domains. As a prelude, it will be useful to discuss duality for an arbitrary integral domain R.

Given any R-module A, we think of Hom(A, R) as a dual of A, and write A^* for it. There is a natural homomorphism from A to A^{**}, and we call A ***reflexive*** if this homomorphism is both one-to-one and onto.

Let F be a free R-module on a finite number of basis elements. We write G for F^* to emphasize the potentially symmetric roles of F and G, and we use an inner product notation (f, g) for the value of g at f. This is equally well the value off at g, for F is in a natural way G^*.

For any submodule A of F we write A' for the set of all g in G with $(A, g) = 0$. A similar definition is made for submodules of G. As usual in such a setup, we have $A \subset A''$, $A' = A'''$. We call a submodule of F

or G *closed* if it is equal to its double prime, and we observe that priming sets up a one-to-one correspondence between the closed submodules of F and those of G.

In the present context we can define a ***pure*** submodule of F or G to be one such that the quotient module is torsion-free. One can easily see that for any A, A' is pure. Furthermore, any pure submodule is closed, as follows from the fact that a finitely generated torsion-free module admits a complete set of homomorphisms into R. Thus we can restate the remarks of the preceding paragraph as follows: priming induces a one-to-one correspondence between the pure submodules of F and those of G.

For any submodule of A of F, A' is, by definition, the module of all homomorphisms from F to R that vanish on A. In other words, $A' \cong (F/A)^*$. To complete the usual picture of duality, we would like to identify A^* with G/A'. Now by restricting homomorphisms $F \to$ R to A we get a mapping from G into A^*. The kernel is precisely A'. Thus, G/A' is isomorphic to a submodule of A^*, namely the submodule consisting of all homomorphisms from A to R that are extendible to F.

In Theorem 222 we shall, for one-dimensional local Gorenstein domains, supply the crucial point that these homomorphisms extend.

Theorem 222. *Let* R *be a one-dimensional local domain. The following three statements are equivalent: (a)* R *is Gorenstein, (b) all finitely generated torsion-free R-modules are reflexive, (c) for any non-zero ideal* I *in* R, $(I^{-1})^{-1} = I$.

Proof. (a) implies (b). We continue the discussion of duality where it left off above. Let B be a finitely generated torsion-free module. We resolve

$$0 \to A \to F \to B \to 0$$

and use F for the free module of the above discussion. Note that A is a pure submodule of F and thus is closed ($A = A''$). Since $id_R(R) = 1$, and B can be embedded into a free module, we have Ext(B, R) = 0, which says that every homomorphism from A to R can be extended to F. This supplies what was needed above in order to see that $A^* \cong G/A'$.

Now recall that we saw that $A' \cong (F/A)^* = B^*$ holds for any integral domain. Apply what was proved in the preceding paragraph to get $(A')^* \cong F/A'' = F/A = B$. This proves the required reflexivity of B.

(b) implies (c). For a non-zero ideal I we have I^* = Hom(I, R) $\cong I^{-1}$.

(c) implies (a). Let M be the maximal ideal of R. We first show that

M^{-1}/R, which can be regarded as a vector space over R/M, is one-dimensional. Otherwise there would exist a (fractional) ideal J lying properly between R and M^{-1}. Take inverses in the inclusions $R \subset J \subset M^{-1}$, obtaining $R \supset J^{-1} \supset M$. Hence $J^{-1} = R$ or M. On taking the inverse again, we find $J = R$ or M^{-1}, a contradiction.

Now pick x to be an element of R, not 0 or a unit. It suffices for us to prove that $R/(x)$ is Gorenstein. Let I be the set of ally with $My \subset (x)$. By Theorem 221, our task is to prove that $I/(x)$ is a one-dimensional vector space over R/M. We observe that $I = xM^{-1}$. Since $xM^{-1}/(x) \cong M^{-1}/R$, the proof is finished.

Theorem 222 can be improved. It is valid for R Noetherian (that is, not necessarily local). With suitable precautions, zero-divisors can be allowed. Moreover, hypothesis (b) or (c) implies that R is at most one-dimensional. For these results and others, and for the historical background, Bass's paper [7] should be consulted. Many aspects are pushed further in the paper [34] of Matlis.

EXERCISES

1. Let R be a local ring with maximal ideal M, and let E be an injective envelope of R/M. Let A be an R-module of finite length, and let B be its dual $\mathrm{Hom}(A, E)$. Prove that A is in a natural way the dual of B. Let C be any submodule of A, and C' its annihilator in B. Prove that this mapping sets up a one-to-one correspondence between all submodules of A and all submodules of B, and that C and B/C' are duals of each other.

2. Let R be a local Macaulay ring. Prove that the following statements are equivalent: (a) R is Gorenstein, (b) for any maximal R-sequence $x_1, \ldots, x_r$, the annihilator of M in $R/(x_1, \ldots, x_r)$ is one-dimensional. *(Hint:* use Ex. 24 in §3-1.)

3. Let R be a local one-dimensional Gorenstein domain. Let I and J be ideals in R with $I \supset J$. Prove that I/J and J^{-1}/I^{-1} have the same length.

4. Let R be a two-dimensional regular local ring, and let x and y be a minimal basis for the maximal ideal M. Let $T = R/(x^2, y^3)$, and let N be the maximal ideal of T. Prove that T is Gorenstein. Prove further that $N^4 = 0$ and that the vector spaces T/N, N/N^2, N^2/N^3, and N^3 have dimensions 1, 2, 2, 1.

Notes

Page 7. There are indeed further restrictions on the partially ordered set of prime ideals of a ring. It is helpful to view this question in conjunction with the standard topology that is placed on the set of prime ideals, making it a topological space called ***Spec.*** For a thorough study see M. Hochster, "Prime ideal structure in commutative rings," ***Trans. Amer. Math. Soc.*** 142(1969), 43–60. Two of Hochster's results are noteworthy assertions which do not refer to the topology. (1) Any finite partially ordered set is eligible to be the partially ordered set of prime ideals of a ring. (2) If a partially ordered set P is eligible, so is the one obtained from P by reversing its order.

The list of four properties which hold in the Noetherian case can also be substantially enlarged. Probably the augmented list will in turn soon be obsolete.

Page 54. The paper of Eisenbud referred to at the end of Exercise 15 has appeared: "Subrings of Artinian and Noetherian rings", ***Math. Annalen*** 185(1970), 247–249.

Page 66. McAdam's paper (Exercises 29 and **30)** has appeared: "Primes and annihilators," ***Bull. Amer. Math. Soc.*** 76(1970), 92.

Section 3-1 (pages 84–104). This section should be amplified by including a treatment of Macaulay modules. Here is a sketch. First let R be Noetherian, P a prime ideal in R, and A a faithful finitely generated R-module satisfying $PA \neq A$; then $G(P, A)$ is at most the little rank of P. This generalizes Theorem 138, and the proof needs only small changes. With R local, call a finitely generated R-module A Macaulay if $G(A)$ equals the dimension of R/(annihilator of A). If R admits a faithful Macaulay module, we deduce the saturated chain condition on the prime ideals of R.

Here is an instructive example. Let T be the ring of all formal power series in two variables over a field, R the subring of those power series with no linear terms. Then R is a two-dimensional local domain of grade 1, while T is an R-module of grade 2. Thus R admits a faithful Macaulay module but is not Macaulay.

Page 110. **An** attractive alternative proof of Theorem 152 is provided by the lemma on page 240 of Volume **I** of [54].

Pages 127 and 135. Rather abruptly, on both of these pages, the finiteness of the global dimension of **a** regular local ring is used without explanation. Reference: Theorem 12 on page 183 of [26].

Page 134, sixth line from the bottom. The assertion that FFR modules form a family is a bit abrupt. One way to prove this is to follow the plan of the proof of Theorem **B.**

Pages 140–141. The hope that Theorems 194 and 195 might survive without the Noetherian hypothesis was promptly fulfilled in a paper by Vasconcelos: ''Annihilators of modules with a finite free resolution", ***Proc. Amer. Math.*** *Soc.* 29(1971), 440–442. However, the conclusion in Theorem 194 that I contains a non-zero-divisor must (as an example shows) be weakened to the statement that the annihilator of I is 0.

Bibliography

1. E. ARTIN and J. **T.** TATE, **"A** note **on** finite ring extensions," ***J.*** of ***Math. Soc. of Japan*** **3(1951), 74–77.**

2. M. **AUSLANDER** and **D. BUCHSBAUM,** "Codimension and multiplicity," ***Ann. of Math.*** **68(1958), 625–657.**

3. ———, "Unique factorization in regular local rings," ***Proc. Nat. Acad. Sci. U.S.A.*** **45(1959), 733–734.**

4. ———, "Invariant factors and two criteria **for** projectivity of modules," ***Trans. Amer. Math. Soc.*** **104(1962), 516–522.**

5. M. **AUSLANDER** and **O.** GOLDMAN, "Maximal orders," ***Trans. Amer. Math. Soc.*** **97(1960), 1–24.**

6. H. **BASS,** "Injective dimension in Noetherian rings," ***Trans. Amer. Soc.*** **102(1962), 18–29.**

7. ———, **"On** the ubiquity **of** Gorenstein rings," ***Math. Zeit.*** **82(1963), 8–28.**

8. A. BOREL and J.–P. **SERRE,** "Le théorème de Riemann–Roch," ***Bull. Soc. Math. France*** **86(1958), 97–136.**

9. N. BOURBAKI, ***Algèbre Commutative,*** Paris: Hermann, **1961–65.**

10. L. **BURCH,** ''On ideals of finite homological dimension in local rings," ***Proc. Camb. Phil. Soc.*** **64(1968), 941–948.**

11. H. CARTAN and **S. EILENBERG,** ***Homological Algebra,*** Princeton: Princeton University Press, **1956.**

12. I. **S. COHEN,** "Rings with restricted minimum condition," ***Duke Math. J.*** **17(1950), 27–42.**

13. I. *S.* **COHEN** and **A. SEIDENBERG,** "Prime ideals and integral dependence," ***Bull. Amer. Math. Soc.*** **52(1946), 252–261.**

14. P. M. COHN, ''Some remarks **on** the invariant basis property," ***Topology*** **5(1966), 215–228.**

15. ———, ''Bézout rings and their subrings." ***Proc. Cumb. Phil. Soc.*** **64(1968), 251–264.**

16. B. ECKMANN and **A. SCHOPF,** ''Über injektive Moduln," ***Arch. Math.*** **4(1953), 75–78.**

17. H. FLANDERS, "Systems of linear equations and exterior powers," ***J. of Alg.*** **7(1967), 1–24.**

18. R. W. GILMER, JR., ''The pseudo-radical of a commutative ring," ***Pac. J. Math.*** **19(1966), 275–284.**

19. ———, ***Multiplicative Ideal Theory,*** Queen's University Papers on Mathematics no. **12,** Kingston, Ontario, **1968.**

20. **O.** GOLDMAN, "Hilbert rings and the Hilbert Nullstellensatz," ***Math. Z.*** **54(1951), 136–140.**

21. M. GRIFFIN, "Families of finite character and essential valuations," ***Trans. Amer. Math. Soc.*** **130(1968),** *75–85.*

22. O. HELMER, "Divisibility properties of integral functions," ***Duke Math. J.*** **6(1940), 345–356.**

23. I. KAPLANSKY, "Modules over Dedekind rings and valuation rings," ***Trans. Amer. Math. Soc.*** **72(1952), 327–340.**

24. ———, ***An Introduction to Differential Algebra,*** Paris: Hermann, **1957.**

25. ———, "R-sequences and homological dimension," ***Nagoya Math.*** **J. 20(1962), 195–199.**

26. ———, ***Fields and Rings,*** Chicago: Univ. of Chicago Press, **1969.**

27. W. KRULL, "Jacobsonsche Ringe, Hilbertscher Nullstellensatz, Dimensionstheorie," ***Math. Z.*** **54(1951), 354–387.**

28. S. LANG, ***Zntroduction*** to ***Algebraic Geometry,*** New York : Interscience, **1958.**

29. G. LEVIN and W. VASCONCELOS, ''Homological dimensions and Macaulay rings," ***Pac. J. of Math.*** **25(1968), 315–323.**

30. S. MAC LANE, ***Homology,*** New York: Springer, **1963.**

31. R. MACRAE, ''On the homological dimension of certain ideals," ***Proc. Amer. Math. Soc.*** **14(1963), 746–750.**

32. ———, ''On an application of the Fitting invariants," ***J. of Alg.*** **2(1965), 153–169.**

33. H. B. MANN, ***Zntroduction to Algebraic Number Theory,*** Columbus, Ohio, **1955.**

34. E. MATLIS, ''Reflexive domains," ***J. of Alg.*** **8(1968), 1–33.**

35. N. H. MCCOY, ''A note on finite unions of ideals and subgroups," ***Proc. Amer. Math. Soc.*** **8(1957), 633–637.**

36. M. NAGATA, **"A**remark on the unique factorization theorem," ***J. Math. Soc. Japan*** **9(1957), 143–145.**

37. ———, ***Local Rings,*** New York: Interscience, **1962.**

38. E. NOETHER, ''Idealtheorie in Ringbereichen," ***Math. Ann.*** **83(1921), 24–66.**

39. D. NORTHCOTT, "Simple reduction theorems for extension and torsion functors," ***Proc. Camb. Phil. Soc.*** **57(1961), 483–488.**

40. D. NORTHCOTT and D. REES, "Extensions and simplifications of the theory of regular local rings," ***J. Lon. Math. Soc.*** **32(1957), 367–374.**

41. J. OHM, ''Some counterexamples related to integral closure in D[[X]],'' ***Trans. Amer. Math. Soc.*** **122(1966), 321–333.**

42. D. REES, "Two classical theorems of ideal theory," ***Proc. Camb. Phil. Soc.*** **52(1956), 155–157.**

43. ———, **"A** theorem of homological algebra," ***Proc. Camb. Phil. Soc.*** **52(1956), 605–610.**

44. ———, ''The grade of an ideal or module," ***Proc. Camb. Phil. Soc.*** **53(1957), 28-42.**

45. P. SAMUEL, ***Anneaux Factoriels,*** Sao Paulo, **1963.**

46. A. SEIDENBERG, **"A** note on the dimension theory of rings,'' ***Pac. J. Math.*** **3(1953), 505–512.**

47. ———, ''On the dimension theory of rings, **II,"** ***Pac. J. Math.*** **4(1954), 603–614.**

48. J. STALLINGS, ''Centerless groups — an algebraic formulation of Gottlieb's theorem," ***Topology*** **4(1965), 129–134.**

49. R. G. SWAN, ''Minimal resolutions for finite groups," ***Topology*** **4(1965), 193–208.**

50. **J.** TOWBER, ''Complete reducibility in exterior algebras over free modules," ***J. of Alg.*** **10(1968), 299–309.**

51. B. L. VAN DER WAERDEN, ***Moderne Algebra,*** vol. **II.** Numerous editions and English translation.

52. W. VASCONCELOS, "Ideals generated by R-sequences," ***J. of Alg.*** **6(1967), 309–316.**

53. ———, "Extensions of Macaulay rings," ***An. da Acad. Bras.*** **39(1967), 211–4.**

54. O. ZARISKI and P. SAMUEL, ***Commutative Algebra,*** New York: ***D. Van Nostrand,*** Vol. I, **1958,** Vol. II, **1960.**

Index of Theorems

THEOREM	PAGE	BRIEF DESCRIPTION
1	1	Exclusion of multiplicatively closed set
2	2	Complement of union of prime ideals
3	3	Uniqueness of prime factorization
4	3	Products of primes are saturated
5	4	Characterization of UFD
6	4	Maximal annihilator is prime
7	**5**	Maximal non-finitely-generated ideal is prime
8	**5**	Primes finitely generated $\Rightarrow$ Noetherian
9	6	Union and intersection of primes
10	6	Existence of minimal primes
11	6	Next neighboring primes
12	9	Characterization of integral
13	10	Sum and product are integral
14	10	Integral elements form a subring
15	10	u^{-1} integral over R $\circ$ $u^{-1} \in R[u]$
16	11	Field integral over $R \Rightarrow R$ field
17	11	When a ring is a finitely generated module
18	12	**Two** definitions of G-domain
19	13	**Three** forms of $K = R[u^{-1}]$
20	14	Intermediate ring a G-domain
21	14	$R[x]$ never a G-domain
22	14	Stability of G-domain property
23	15	$R[u]$ a G-domain $\Rightarrow R$ a G-domain and u algebraic
24	15	G-domain $\Leftrightarrow$ existence of a maximal contracting to 0
25	16	Nilradical $= \bigcap$ of G-ideals
26	17	Radical of $I = \bigcap$ of G-ideals containing I
27	17	I is a G-ideal $\Leftrightarrow$ Z is contraction of a maximal ideal
28	17	Structure of a maximal ideal

THEOREM	PAGE	BRIEF DESCRIPTION
29	18	Improvement of Theorem 28 when field is algebraically closed
30	18	In a Hilbert ring, a radical ideal $= \bigcap$ of maximals
31	18	R is Hilbert $\Leftrightarrow R[x]$ is
32, 33	19	Two versions of the Nullstellensatz
34	23	Primes in R and R_S
35	24	Special case of R_P
36	25	Primes in $R[x]$ contracting to 0
37	25	No chain of 3 primes in $R[x]$ with same contraction
38	26	Rank of primes in $R[x]$
39	26	Improvement of Theorem 38 for S-rings
40	28	Integral property is transitive
41	28	Characterization of GU
42	29	GU implies LO
43	29	Characterization of INC
44	29	Integral $\Rightarrow$ GU and INC
45	30	INC $\Rightarrow$ ranks decrease
46	31	GU $\Rightarrow$ existence of a prime over P with rank $\geqq$ rank(P)
47	31	GU, INC $\Rightarrow$ equality of coranks
48	32	GU, INC $\Rightarrow$ preservation of dimension
49	32	Properties of a GCD-domain
50	33	GCD domain is integrally closed
51	33	Preservation of integral closure under localization
52	34	Intersections are integrally closed
53	34	Representation of R as $\bigcap R_P$
54	35	Characterization of integral closure
55	35	Survival of an ideal in $R[u]$ or $R[u^{-1}]$
56	36	Existence of a valuation domain in which an ideal survives
57	36	An integrally closed domain is an intersection of valuation domains
58	37	Invertible $\Rightarrow$ finitely generated
59	37	Invertible, quasi-local $\Rightarrow$ principal
60	37	Invertible, finite number of maximal ideals $\Rightarrow$ principal
61	38	Preservation of invertibility under localization
62	38	Local characterization of invertibility
63	38	Quasi-local Bézout domains are valuation
64	39	Local characterization of Priifer
65	39	Priifer $\Rightarrow$ intermediate valuation domains are localizations
66	40	Valuation domains inside $K(x)$

THEOREM	PAGE	BRIEF DESCRIPTION
67	40	Under suitable hypotheses on u and R, u or u^{-1} lies in R
68	41	Valuation ring is strong S
69	47	Hilbert basis theorem
70–1	48	Power series ring case
72	48	R principal ideal domain $\Rightarrow R[[x]]$ UFD
73–4	49	Krull intersection theorem
75–7, 79	50–51	Theorems connected with the Krull intersection theorem
78	51	Nakayama lemma
80	55	Noetherian $\mathcal{Z}(A)$ is a finite union of primes
81	55	$S \subset$ union of ideals, all but 2 prime $\Rightarrow S \subset$ one of them
82	56	Existence of an annihilator for an ideal of zero-divisors
83	56	Sharpening of Theorem 81
84	57	Minimal primes consist of zero-divisors
85	57	Localization of Noetherian is Noetherian
86	57	Noetherian improvement on Theorem 84
87	58	ACC on radical ideals $\Rightarrow$ finite intersection of primes
88	59	ACC on radical ideals* finite number of minimal primes
89	59	Characterization of 0-dimensional rings
90	60	Characterization of 1-dimensional domains
91	60	In a 0-dimensional ring, non-zero-divisors are units
92	61	Lemma for Theorem 93
93	61	Rings between a 1-dimensional Noetherian domain and its quotient field
94	67	Z grade $1 \Rightarrow I^{-1}$ properly contains R
95	67	Characterization of **DVR**
96	67	Characterization of Dedekind ring
97	68	A Dedekind ring has unique factorization of ideals
98	69	Preservation of Dedekind property
99	70	Descent for valuation domains
100	70	Integral closure need not be a finitely generated module
101	71	Stability of Prüfer
102	72	Ring of all algebraic integers is Bézout
103	76	In integrally closed Noetheriah domain, grade $1 \Rightarrow$ rank 1
104	76	In integrally closed Noetherian domain, $R = \bigcap R_P$, P ranging over rank-1 primes
105	77	Intersection of a finite number of localizations

THEOREM	PAGE	BRIEF DESCRIPTION
106	77	Lemma for Theorem 107
107	78	Intersection of a finite number of valuation domains
108	79	Divisibility of powers in a quasi-local one-dimensional domain
109	79	Intersection of two quasi-local one-dimensional domains
110–4	79–81	Properties of locally finite intersections of quasi-local domains
115–8	85–86	Technicalities on R-sequences
119	86	With Noetherian and radical assumptions, any permutation of an R-sequence is an R-sequence
120	87	Partial ideals of an R-sequence form an ascending chain
121	87	Maximal R-sequences have the same length
122	89	Can enlarge Z to P, maintaining $G(I, A)$
123	90	Local finiteness of $\bigcap R_P$
124	90	Avoiding a union of prime ideals with a specified element
125	91	Global unmixedness
126–8	92–93	Preliminaries for Theorem 129
129	93	Local unmixedness
130	94	Grade unmixedness
131	94	Comparison of rank of P and its image in $R/(x)$
132	95	Grade $\leqq$ rank
133–5	95–96	Behavior of grade under localization
136	97	Grade = rank in a Macaulay ring
137	97	Unmixedness in a Macaulay ring
138	99	Grade $\leqq$ little rank
139	100	Localization of Macaulay is Macaulay
140	100	Local Macaulay $\Rightarrow$ global Macaulay
141	100	Lifting Macaulay mod a non-zero-divisor
142	104	Principal ideal theorem
143	105	Lemma for the principal ideal theorem
144	107	Existence of infinitely many intermediate primes
145	107	Lemma for Theorem 146
146	107	Determination of Noetherian G-domains
147	108	Determination of Noetherian Hilbert rings
148–9	108–109	Ranks of prime ideals in a Noetherian polynomial ring
150	109	A maximal ideal in $R[x]$ cannot consist of zero-divisors
151	109	Stability of Macaulay for polynomial rings
152	110	Generalized principal ideal theorem

THEOREM	PAGE	BRIEF DESCRIPTION
153	112	Converse of Theorem 152
1'54	112	Ultimate principal ideal theorem
155	113	Case $n = 1$ of Theorem 154
156	113	Lifting of Macaulay property mod a radical element
157	113	Stability of Macaulay for power series rings
158	115	Minimal generation of a module over a local ring
159	116	Stability of minimal generation of maximal ideals
160	116	Generation of M by an R-sequence $\Rightarrow$ regularity
161–2	117	Stability of regularity
163	117	Lemma for Theorem 164
164	118	A regular local ring is a domain
165	118	Chinese remainder theorem
166	119	Lemma for Theorem 167
167–8	119	Decomposition of Noetherian rings
169	119	Converse of Theorem 160
170	120	Regular $\Rightarrow$ Macaulay
171	120	Stability of super-regularity
172	124	$d(A/xA) = 1 + d(A)$ under suitable hypotheses
173	125	Grade and projective dimension are complementary
174	126	Rees's inequality connecting grade and projective dimension
175	26	Perfect $\Rightarrow$ grade-unmixed
176	27	Ranks 0, $n - 1$, and n are perfect
177	31	Nagata's lemma for UFD's
178	32	Local characterization of UFD's
179	32	Global characterization of UFD's
180	33	Projective FFR $\Rightarrow$ free complement
181	34	Invertible FFR $\Rightarrow$ principal
182	134	Stability of FFR
183	134	Lemma for Theorem 182
184	135	Noetherian domain with FFR is UFD
185	135	Regular, invertibles principal $\Rightarrow$ UFD
186	135	Lemma for Theorem 187
187–8	137	Stability of regular UFD
189	137	Long Schanuel lemma
190	139	Localization of FFR modules
191	139	Grade 0 $\Rightarrow$ FFR modules free
192	140	Non-negativity of Euler characteristic
193–8	140–142	Theorems on the annihilator of an FFR module
199	142	Characterization of ideals generated by R-sequences
200	144	Finiteness of partial Euler characteristics
201	150	Lemma for Theorem 202
202	151	First injective change of rings

THEOREM	PAGE	BRIEF DESCRIPTION
203	152	Injective modules over a quotient ring
204	152	Dual of second projective change of rings
205	153	Second injective change of rings
206	154	Third injective change of rings
207	157	Only 0-dimensional rings admit finitely generated injectives
208–9	158	Lemmas for Theorem 210
210	158	Injective dimension is at least the grade of the ring
211–3	159	Theorems preliminary to Theorem 214
214	160	Injective dimension equals grade of the ring
215	160	Gorenstein $\Rightarrow$ Macaulay
216	160	In a Gorenstein ring, finiteness of projective dimension coincides with finiteness of injective dimension
217–8	161	Characterization of grade by vanishing of Ext
219	162	Existence of module with finite injective dimension $\Rightarrow$ grades bounded by grade of ring
220	165	Duality of modules of finite length
221	166	Characterization of 0-dimensional Gorenstein
222	167	Characterization of 1-dimensional Gorenstein

Index of Topics

Algebra, 9
Annihilator, 4, 9, ***55***

Bézout domain, 32, 72, 78

Chinese remainder theorem, 118
Class group, 72
Closed submodule, 167
Composition series, 59
Conductor, 46
Corank, 31

Dedekind ring, 66, 68, 83, 120
Dimension
  homological, 123
  injective, 123, 149
  Krull. 32, 59
  of variety, 110
  projective, 123

Essential extension, 156
Euler characteristic, 137
  partial, 143

Family (of modules), 134
Fitting invariants, 145
Formal power series, 48, 135

GCD-domain, 32
G-domain, 12, 107
G-ideal, 12
Going down (GD), 28.44
Going up (GU), 28
Gorenstein ring, 160, 164
Grade, 67, 89, 124, 132
Grade-unmixed, 93, 126

Hilbert ring, 12, 108

Ideal
  contracted, ***44***
  fractional, 37
  invertible, 37
  maximal, 3, 12
  maximal of zero-divisors, 3
  prime, 1
  radical, 17, 58
  radical of, 17
Incomparable (INC), 28
Injective
  dimension, 123, 149
  envelope, 156
  equivalence, 149
  module, 149
  resolution, 149
Integral
  closure, 27
  element, 9
Integrally closed, 32, 75
  completely, 53
Inverse (of ideal), 37

Jacobson radical, 51
J-ideal, 65
Jordan-Holder theorem, ***59***

Krull domain, 82
Krull intersection theorem, 49

Length (of module), 59
Local ring, 67
Localization, 22, 33, 38
Lying over (LO), 28

Macaulay ring, 84, 95, 109, 113, 120, 160
Maximal prime (of module), 3, 34, 54
Minimal
  basis, 116
  prime, 6, 25, 57
Multiplicatively closed set, 1, 16, 22
  saturated, 2, 3, 22, 34

Nakayama lemma, 51
Nilradical, 16
Noetherian
  ring, 5, 7, 13, 47
  module, 54, 74
Nullstellensatz, 12, 19
  homogeneous, 21

Perfect, 126
Principal ideal theorem, 82, 99, 104, 110, 112
Principal prime, 3, 131
Projective
  dimension, 123
  equivalence, 123
  module, 123
  resolution, 123
Prüfer domain, 38, 71
Pure submodule, 167

Quasi-Frobenius. 166
Quasi-local, 24, 37, 76

Radical (of ideal), 17
  Jacobson, 51
Rank, 25, 94
  little, 98, 111
Reflexive, 166
Regular, 118, 135
  local, 116, 130
  super, 119
  von Neumann, 64
Residue class field, 77
Resolution
  finite free (FFR), 133, 137
  injective, 149
  projective, 123
R-sequence, 84, 116, 119

Saturated
  chain, 98
  chain condition, 99
  multiplicatively closed set, 2, 3, 22, 34
Schanuel's lemma, 124, 137
S-domain, 26, 108
Strong S-ring, 26, 40, 108

Torsion-free, 50

Unique factorization domain (UFD), 3, 48, 82, 130
Unmixedness, 90, 93, 97
  grade, 93, 126

Valuation ring, 35
  discrete (DVR), 35, 67, 76
  domain, 32, 35, 76
  rational, 81
Value group, 69
Variety, 20, 64
V-dimension. 116

Zero-divisor, 3, 34, 54