Conference Board of the Mathematical Sciences

CBMS

Regional Conference Series in Mathematics

Number 24

Topics in the Homological Theory of Modules Over Commutative Rings

Melvin Hochster

American Mathematical Society
with support from the
National Science Foundation

Selected Titles in This Series

(Continued in the back of this publication)

This page intentionally left blank

http://dx.doi.org/10.1090/cbms/024

Conference Board of the Mathematical Sciences

CBMS

Regional Conference Series in Mathematics

Number 24

Topics in the Homological Theory of Modules Over Commutative Rings

Melvin Hochster

Published for the
Conference Board of the Mathematical Sciences
by the
American Mathematical Society
Providence, Rhode Island
with support from the
National Science Foundation

Expository Lectures
from the CBMS Regional Conference
held at the University of Nebraska
June 24–28, 1974

2000 *Mathematics Subject Classification.* Primary 13-XX;
Secondary 20-XX.

Library of Congress Cataloging-in-Publication Data

Hochster, Melvin, 1943–
Topics in the homological theory of modules over commutative rings.
(Regional conference series in mathematics; no. 24)
"Expository lectures from the CBMS regional conference held at the University of Nebraska, June 24–28, 1974."
Bibliography: p.
1. Commutative rings. 2. Modules (Algebra) 3. Homology theory. I. Conference Board of the Mathematical Sciences. II. Title. III. Series.
QA1.R33 no. 24 [QA251.3] 510′.8s [512′.4] 75-1325
ISBN 0-8218-1674-8
CIP

---

11 10 9 8 7 6 5 06 05 04 03 02 01

Contents

This page intentionally left blank

Acknowledgements

I want to thank the many people at Nebraska who did so much in arranging the conference and making it so pleasant to visit Lincoln.

Particular thanks go to Max Larsen, who did an excellent job of organizing.

I also want to express my appreciation to Roger Wiegand who read and edited the manuscript and arranged for it to be reproduced on extremely short notice. The simple form of the argument on pp. 32–33 is due to him.

A special word of thanks goes to Carol Portsche who did a remarkable job of accurate typing in a very short time.

I want to thank the students and faculty of Århus University, particularly Sven Toft Jensen, Niels Nygaard, and Torgny Svanes, who listened patiently to many versions (both correct and incorrect) of arguments given in these notes.

Finally, I want to thank the Rocky Mountain Mathematics Consortium and the National Science Foundation for sponsoring and supporting the conference.

This page intentionally left blank

http://dx.doi.org/10.1090/cbms/024/01

0. Introduction

These talks deal mainly with recent developments and still open questions in the homological theory of modules over commutative (usually, Noetherian) rings. A good deal of attention is given to the role "big" Cohen-Macaulay modules play in clearing up some of the open questions.

§1 develops necessary background material, while §2 attempts to clarify the relationships among some of the many open questions (rigidity, multiplicities, existence of various kinds of Cohen-Macaulay modules, Bass' question, the intersection conjecture, etc.). §3 explores with fairly complete proofs the consequences of the existence of Cohen-Macaulay modules. In particular, it contains proofs of some of the implications of §2. §4 develops the necessary machinery to prove the existence of "big" Cohen-Macaulay modules in characteristic $p > 0$, while §5 first gives an expository account (without proofs) of the theory of Henselian rings, Artin approximation, and then part of the reduction of the proof of the existence of big Cohen-Macaulay modules from the case where R contains a field of characteristic 0 to the case where R contains a field of characteristic $p > 0$. §§3, 4, 5 yield a fairly complete proof of the intersection theorem, Bass' conjecture, the zerodivisor conjecture, etc. for local rings containing a field.

After §5 very few results are proved in full. I have frequently given sketches of proofs in which perhaps one important lemma is proved carefully, or, sometimes, a special case which imparts the basic ideas is dealt with fully. At certain points I have taken the liberty of including some wild (or, worse, extremely vague) conjectures.

§6 deals with the phenomenon of depth-sensitivity including the Buchsbaum-Eisenbud criteria for acyclicity of certain complexes and related results which go in a somewhat different direction. §7 begins with a discussion of the Buchsbaum-Eisenbud structure theorems for finite free acyclic complexes (with a sketchy proof) and then goes on to a discussion of just what it might mean to give a "best possible" structure theorem in terms of describing generic free acyclic complexes with prescribed Betti numbers. The program is carried out in detail for complexes of length 2 (with partial proofs). This leads into a discussion of linear algebraic groups in §8 and their rings of invariants. Only a few proofs are given. It seems clear that there are subtle and important connections between the study of modules of finite projective dimension and the study of linear algebraic groups.

§9 is mostly independent. It contains two applications of homological methods to problems (cancellation of indeterminates, the Zariski-Lipman conjecture) which do not a priori involve homological ideas. It also surveys some open questions about the spectrum of a Noetherian ring (as an ordered set) one of which has some connection with the existence of big Cohen-Macaulay modules.

I hope that these talks will illuminate a point on which I feel strongly.

It is dangerous to work in too isolated a fashion within commutative rings. It will be apparent in §9 that even in trying to deal with a fairly seemingly innocent problem in "pure" algebra, it comes in handy to have some knowledge of (a) the behavior of vector bundles in topology and (b) the theory of schemes.

It is worth noting that we shall be able to consider here only a small fraction of what is being done with the homological theory of commutative rings right now. We shall not touch on the study of Poincaré series and their rationality, canonical modules, deformation theory, the beautiful results described in [0] on projective dimension of big modules, or many other topics.

Finally, I want to remark that the treatment of big Cohen-Macaulay modules here serves as a reminder that algbera, after all, has to do with solving equations. Abstract algebra is the daughter of the theory of equations (in the broadest sense) and perhaps its best theorems (like M. Artin's approximation theorem) still deal with that subject. In any case, we shall see here that even in abstruse homological matters it is best not to forget this fact.

http://dx.doi.org/10.1090/cbms/024/02

1. Preliminaries

Throughout these talks, ''ring'' means commutative ring with identity and ''local ring'' means *Noetherian* ring with a unique maximal ideal. ''(R, P) is local'' means that R is a local ring and P is the unique maximal ideal. Modules are assumed to be unital.

Our goal in this section is to recall the basic facts about modules of finite type and finite projective dimension over a Noetherian ring and the relation between the study of these modules and the notion of ''depth''. We shall give all definitions and outline some proofs. We shall assume basic familiarity with Tor and Ext. For more detailed information, we refer the reader to [AB_1], [AB_2], [K], [N, Chapter IV], [R], [S], and [Mat].

Recall that a module M has projective dimension n if there is an exact sequence

$$0 \to P_n \xrightarrow{d_n} \cdots \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \to 0$$

with each P_i projective and no shorter such sequence. We shall then say that the complex $\mathcal{K}$,

$$0 \to P_n \xrightarrow{d_n} \cdots \xrightarrow{d_1} P_0 \to 0,$$

is a projective resolution of M of length n. If M has no finite projective resolution, we shall say that the projective dimension of M is infinite. We abbreviate ''projective dimension of M (over R)'' to ''pd M ($\mathrm{pd}_R M$)''. We may also say that $\mathcal{K} \xrightarrow{d_0} M \to 0$ is a projective resolution of M. (This definition is interpreted to mean that pd $M = 0$ if and only if M is a *nonzero* projective: pd $0 = -1$.) It is easy to show that pd M is the least integer $m \geq -1$ such that $\mathrm{Ext}_R^i(M, N) = 0$ for every $i > m$ and every R-module N. If

$$0 \to M_1 \to P_0 \to M \to 0$$

is exact and P_0 is projective, we call M_1 a *first module of syzygies* (or *relations*) for M. We can then define an ith *module of syzygies* by induction (i.e., an $(i+1)$th module of syzygies is a first module of syzygies of an ith module of syzygies). Or we can simply say that if

$$0 \to M_i \to P_{i-1} \to \cdots \to P_0 \to M \to 0$$

is exact and each P_j is projective, then M_i is an ith module of syzygies of M. Then one can easily show that if $n \geq 0$, pd $M \leq n$ if and only if any nth module of syzygies of M is projective. Moreover, if $1 \leq \text{pd } M = n < \infty$ and M_i is an ith module of syzygies, $i \leq n$, then pd $M_i = n - i$.

Let R be a ring, M an R-module, and $\mathbf{x} = x_1, \cdots, x_n$ a sequence of elements of R. We shall say that $\mathbf{x}$ is M-*regular* or that M is $\mathbf{x}$-*regular* if the following two conditions hold:

(1) $(\mathbf{x})M \neq M$.

(2) For each i, $0 \leq i < n$, x_{i+1} is not a zerodivisor on $M/(x_1, \cdots, x_i)M$. (In other words, for each such i, $(x_1, \cdots, x_i)M$: $(x_{i+1}R) = (x_1, \cdots, x_i)M$.)

One of the most important points we want to make is that *the existence of non-trivial examples of modules of finite type and finite projective dimension over a Noetherian ring R is due almost entirely to the presence of R-regular sequences in R. We* shall come back to this point several times.

If x is not a zerodivisor on R then the complex $\mathcal{K}_.(x; R)$,

$$0 \to R \xrightarrow{x} R \to 0$$

(where $\mathcal{K}_0$ is the right-hand copy of R), is acyclic, and it follows that R/xR has finite projective dimension 1.

If $x_1, \cdots, x_n$ is an R-sequence one may check that $\mathcal{K}_.(x_1, \cdots, x_n; R)$, which is defined as the tensor product (over R) of the complexes $\mathcal{K}_.(x_i; R)$, is acyclic and gives a (shortest) projective resolution of $R/(x_1, \cdots, x_n)R$. Thus, in general, $R/(x_1, \cdots, x_n)R$ has finite projective dimension n when $x_1, \cdots, x_n$ is an R-sequence. One point we want to make is that the modules of this form are somehow "typical" of R-modules of finite projective dimension.

We should also mention that $\mathcal{K}_.(x_1, \cdots, x_n; R)$, which is called *the Koszul complex* (of R with respect to $x_1, \cdots, x_n$), can be described explicitly as follows: Let $\mathcal{K}_i$ be the free module on $\binom{n}{i}$ generators denoted $u(j_1, \cdots, j_i)$, $1 \leq j_1 < \cdots < j_i \leq n$, and define $d_i: \mathcal{K}_i \to \mathcal{K}_{i-1}$ by

$$d_i(u(j_1, \cdots, j_i)) = \sum_{t=1}^{i} (-1)^{t-1} x_{j_t} u(j_1, \cdots, \hat{j}_t, \cdots, j_i).$$

If there are only two x's, we get

$$0 \to R \xrightarrow{d_2} R^2 \xrightarrow{d_1} R \to 0$$

where the generators of R^2 map to x_1, x_2, respectively, while d_2 takes the generator of R to $(x_2, -x_1)$. If we think of $\mathcal{K}_i$ as $\Lambda^i(R^n)$ then the d_i give a derivation of degree -1 on the exterior algebra $\Lambda(R^n)$. $\mathcal{K}_.(x_1, \cdots, x_n; R)$ is often thought of in this way. We refer the reader to [AB$_2$] for a detailed study of the Koszul complex.

We should note that if $\mathbf{x} = x_1, \cdots, x_n$, then the complex $\mathcal{K}_.(\mathbf{x}; R) \otimes M$, where M is any R-module, is referred to as the *Koszul comlpex of M* with respect to $x_1, \cdots, x_n$.

If R is Noetherian, I an ideal of R, and M an R-module of finite type, then if $IM \neq$

M it turns out that any two maximal M-regular sequences in I have the same length.

This follows from the following:

Proposition 1.1. *If R, I, M are as above and, $x_1, \cdots, x_g$ is any maximal M-regular sequence in I, then g is the least integer i such that* $\mathrm{Ext}^i_R(R/I, M) \neq 0$.

Proof. Use induction on g and the long exact sequence for Ext coming from

$$0 \to M \xrightarrow{x_1} M \to M' \to 0,$$

where $M' = M/x_1M$. The case $g = 0$ is an easy exercise. Q.E.D.

Thus, if R is Noetherian, M is an R-module of finite type, and $IM \neq M$, we define $\mathrm{depth}_R(I, M)$ (or $\mathrm{depth}(I, M)$) as, equivalently, either

(a) the length of any maximal M-sequence in I, or

(b) the least nonnegative integer g such that $\mathrm{Ext}^g_R(R/I, M) \neq 0$.

If $IM = M$ it is convenient to define $\mathrm{depth}_R(I, M) = +\infty$.

If (R, P) is local then $\mathrm{depth}_R M$ denotes $\mathrm{depth}_R(P, M)$. (*Note*: If $M \neq 0$, $PM \neq M$ since M is of finite type.)

If R is an arbitrary Noetherian ring and I is an ideal, depth I usually means $\mathrm{depth}(I, R)$. In the local case, the notation is ambiguous, but if we mean to talk about depth I where I is to be regarded as a module, we shall write the explicit form $\mathrm{depth}(P, I)$.

We note the following result, which shows that the Koszul complex is "depth-sensitive".

Proposition 1.2. *Let R be a Noetherian ring, $I = (x_1, \cdots, x_n)R$ any ideal, and M an R-module of finite tpye such that $IM \neq M$. Let $\mathbb{K}_.$ denote the Koszul complex $\mathbb{K}_.(x_1, \cdots, x_n; M)$. Let d be the greatest integer such that $H_d(\mathbb{K}_.) \neq 0$. (Note: $H_0(\mathbb{K}_.) \cong M/IM \neq 0$, so that $0 \leq d \leq n$.) Then* $\mathrm{depth}_R(I, M) = n - d$. *In other words,* $\mathrm{depth}_R(I, M)$ *is the number of consecutive vanishing Koszul homology modules, counting from the left.*

This "classical" depth-sensitivity is established in [AB_2]. We shall see later how some recent results of Buchsbaum and Eisenbud (see §6) may be regarded as generalizations of Proposition 1.2, after one makes the key observation that, in the special case where $x_1, \cdots, x_n$ is an R-sequence, $\mathbb{K}_.(\mathrm{x}; R)$ is a projective (in fact, free) resolution of $R/(\mathrm{x})R$.

We want to recall two results relating depth and projective dimension which are basic and have been known for a relatively long time.

Proposition 1.3. *If M is a module of finite type over a local ring R,* $\mathrm{pd}_R M$ *is finite, and $M \neq 0$, then*

$$\mathrm{pd}_R\, M = \mathrm{depth}\, R - \mathrm{depth}\, M.$$

See, for example, [N, Chapter IV].

E.g., if depth $R = 0$, i.e., if P consists entirely of zerodivisors, and M is of finite type, then pd $M < \infty$ implies M is free.

Proposition 1.4. *If $M \neq 0$ is a module of finite type over a Noetherian ring R and $I = \operatorname{Ann} M$, then* depth $I \leq \mathrm{pd}_R\, M$.

Proof. See Rees [R].

Next, we want to recall the basic facts about regular local rings. A local ring (R, P) is called regular if P can be generated by n elements where $n =$ Krull dim R. (The definition is motivated by algebraic geometry: if V is a variety over the complex numbers, V is nonsingular or smooth at a point x if and only if the local ring of V at x is regular.) It is not hard to show (e.g., by induction on Krull dim R) that if R is regular then R is a domain. Moreover, if $x \in P - P^2$ and R is regular then R/xR is again regular, hence, a domain. Let $x_1, \cdots, x_n$ be a minimal set of generators of P (equivalently, a maximal set of elements of P whose residues modulo P^2 are linearly independent). Then, by our remark above, each $R/(x_1, \cdots, x_i)R$ is a domain and x_{i+1} is not a zerodivisor on $R/(x_1, \cdots, x_i)R$. In other words, $x_1, \cdots, x_n$ is an R-sequence. It follows that $\mathcal{K}_\bullet(\mathbf{x}; R)$ is a projective resolution of $K = R/P = R/(x_1, \cdots, x_n)R$.

We prove in part:

Proposition 1.5 (Auslander-Buchsbaum-Serre). *The following conditions on a local ring (R, P) are equivalent:*

(1) *R is regular.*

(2) pd *K is finite, where $K = R/P$.*

(3) *For every R-module M of finite type,* pd M *is finite.*

(4) *For every R-module M,* pd $M \leq$ dim R.

Proof. We have already indicated the proof of (1) $\Rightarrow$ (2). To see why (2) $\Rightarrow$ (3), let M be a module of finite type, and let $\mathcal{K} \to M \to 0$ be a free resolution such that, for each i, the generators of $\mathcal{K}_i$ map onto a minimal basis for the kernel of $(\mathcal{K}_{i-1} \to \mathcal{K}_{i-2})$. This is equivalent to the assertion that, for each i, Im $\mathcal{K}_{i+1} \subset P\mathcal{K}_i$. Then, if $\mathcal{K}_i \neq 0$, we have $\mathrm{Tor}_i(M, K) = 0$, for Im $\mathcal{K}_{i+1} \subset P\mathcal{K}_i$ implies that all the maps are zero in the complex $\mathcal{K} \otimes_R K$, and $\mathrm{Tor}_\bullet(M, K) = H_\bullet(\mathcal{K} \otimes_R K)$, so that $\mathrm{Tor}_i(M, K) \cong \mathcal{K}_i \otimes_R K$. If $\mathrm{pd}_R\, K = n$, then $\mathrm{Tor}_i(M, K) = 0$ if $i > n$ and hence $\mathcal{K}_i = 0$ if $i > n$. Thus, pd $M \leq$ pd K. For (3) $\Rightarrow$ (4) $\Rightarrow$ (1) we refer the reader to [N, Chapter IV], and [S].

We mention two important corollaries.

Proposition 1.6. *If R is a regular local ring and Q is any prime ideal then R_Q is regular.*

Proof. Since R is regular, R/Q has a finite projective resolution $\mathcal{K}$ over R. But then $\mathcal{K} \otimes_R R_Q$ is the finite projective resolution of R_Q/QR_Q over R_Q. Q.E.D.

Proposition 1.7 (Auslander-Buchsbaum). *A regular local ring (R, P) is a unique factorization domain.*

Proof (Kaplansky). We use induction on Krull dim R and leave the cases of low dimension (0, 1) to the reader. Assume dim $R \geq 2$ and let $x \in P - P^2$. Then R/xR is regular, so that x is prime, and it suffices to show that R_x is a UFD. Let Q be a minimal nonzero prime of R_x, and let $Q^* = Q \cap R$. It will suffice to show that Q is principal. If P_0 is any prime of R_x, $(R_x)_{P_0}$ is a UFD by the induction hypothesis, and $Q(R_x)_{P_0}$ is either a minimal nonzero prime, hence, principal, or $Q(R_x)_{P_0} = (R_x)_{P_0}$. In either case $Q(R_x)_{P_0}$ is free of rank one. Thus Q, as an R_x-module, is locally free of rank one, and, therefore, projective. Now, Q^* has a free resolution over R. If we apply $\otimes_R R_x$ we see that Q is a projective with a finite free resolution over R_x. It follows easily by induction on the length of the resolution that Q has a finite free complement, i.e. there are nonnegative integers p, q such that $Q \oplus R_x^p \cong R_x^q$. Since Q is locally free of rank one, $q = p + 1$, i.e., $Q \oplus R_x^p \cong R_x^{p+1}$. Then, over R_x, $R_x \cong \Lambda^{p+1}(R_x^{p+1}) \cong \Lambda^{p+1}(Q \oplus R_x^p) \cong \Lambda^0 Q \otimes \Lambda^{p+1} R_x^p \oplus \Lambda^1 Q \otimes \Lambda^p R_x^p \oplus 0$ (since $\Lambda^i Q = 0$, $i \geq 2$; Q is locally free of rank one) $\cong 0 \oplus Q \otimes R_x \cong Q$, i.e. $Q \cong R_x$ and hence Q is principal. Q.E.D.

We conclude this section of preliminaries by recalling that an R-module M has *injective* dimension n if there is an exact sequence $0 \to M \to I_0 \to \cdots \to I_n \to 0$ with each I_i injective and no shorter such sequence. We shall write $\mathrm{id}_R M = n$ in this case. Many of the same general remarks as for projective dimension apply to injective dimension (or, better, the "dual" remarks apply: injective dimension is projective dimension in the opposite or dual abelian category). E.g. $\mathrm{id}_R M$ is the least integer $m \geq -1$ such that $\mathrm{Ext}_R^i(N, M) = 0$ for every $i > m$ and every R-module N.

http://dx.doi.org/10.1090/cbms/024/03

2. Some Open Questions

In this section we shall describe some open questions in what might be described as the homological theory of modules over a local ring. Some of these questions are phrased for arbitrary Noetherian rings, but, in almost every case, there is an immediate reduction to the local case. Usually, one may even reduce to the complete local case.

We put each question as a conjecture.

Conjecture (1) (Rigidity conjecture). *Let M, N be modules of finite type over a Noetherian ring R, and suppose $\mathrm{pd}_R M$ is finite. If $\mathrm{Tor}_i^R(M, N) = 0$, then $\mathrm{Tor}_j^R(M, N) = 0$ for all $j \geq i$. (If M satisfies this condition, for all N, i, it is called rigid.)*

There is no loss of generality in assuming that R is complete local, that $i = 1$, and that $\mathrm{Tor}_j^R(M, N)$ has finite length, $j \geq 1$.

Conjecture 1 is known [L] if R is regular (then $\mathrm{pd}_R M < \infty$ is automatic), and if $\mathrm{pd}\, M = 1$. If $\mathrm{pd}_R M = 2$ the result is known [PS] if $\mathrm{Ann}\, M \neq 0$. Conjecture I is also known if $M = R/(x_1, \cdots, x_n)R$, where $x_1, \cdots, x_n$ is an R-sequence.

M. Auslander observed that Conjecture (1) has the following consequence:

Conjecture (2) (Zerodivisor conjecture). *Let R be a local ring and let M be an R-module of finite type and finite projective dimension. If $x \in R$ is not a zerodivisor on M, then x is not a zerodivisor on R.*

This was established if R is a local ring containing a field of characteristic $p > 0$ or if R is the localization at a prime of an algebra of finite type over a field by Peskine and Szpiro [PS]. ("Algebra of finite type" means finitely generated as an algebra.) An interesting point in the proof is that something better holds:

Conjecture (3) (Intersection conjecture). *If R is local and $M \neq 0$, N are R-modules of finite type such that $M \otimes_R N$ has finite length, then* $\dim N \leq \mathrm{pd}_R M$.

Of course, this is vacuous unless $\mathrm{pd}_R M < \infty$; $\dim N$ is, by definition, $\mathrm{Krull}\dim R/\mathrm{Ann}\, N$. If $J = \mathrm{Ann}\, N$ we can replace N by R/J without affecting the validity of Conjecture (3).

Then Peskine and Szpiro prove $(1) \Longrightarrow (3) \Longrightarrow (2)$ for any class of local rings closed under the operations

(a) completion,

(b) localization at a prime,

(c) passage to a homomorphic image.

Utilizing the Frobenius functor (see [PS] or §4 here) and local cohomology they prove (3) for local rings of positive prime characteristic p. We shall give a different proof later.

In [H_2] the present author observed that (3) is equivalent to:

Conjecture (4) (Homological height conjecture). *Let $R \to S$ be a homomorphism of Noetherian rings, and let M be an R-module of finite type and finite projective dimension. Let $I = \operatorname{Ann}_R M$ and let Q be a minimal prime of IS. Then $\operatorname{ht} Q \leq \operatorname{pd}_R M$.*

Here, $\operatorname{ht} Q$ denotes the height of Q, i.e. Krull dim R_Q. Note that if $IS = S$, e.g. if $M = 0$, then IS has *no* minimal primes, and Conjecture (4) is vacuous. Conjecture (4) may be reduced at once to the case where R, S are complete local rings. Note that (4) $\Rightarrow$(3) is obvious. To prove (3), we need only consider the case $N = R/J$, and we may then let $S = R/J$ and apply (4). Conjecture (3) also reduces at once to the case where R is complete.

Peskine and Szpiro also made considerable progress on a question of Bass [B], which is now refererd to as Bass' conjecture (although as far as I know Bass only raised the question and did not actually make the conjecture).

First, we recall that a module M of finite type over a local ring R is called a *Cohen-Macaulay* module if depth M = dim M. In general, depth $M \leq$ dim $M \leq$ dim R. If depth M = dim M = dim R we call M a *maximal* Cohen-Macaulay module. If R itself is a Cohen-Macaulay module then R is called a Cohen-Macaulay ring. We refer the reader to [S] for a proof of the following result:

Proposition 2.1. *Let M be a module of finite type over a local ring R and let J = Ann M. The following conditions are equivalent:*

(1) *M is a Cohen-Macaulay R-module.*

(2) *Some system of parameters of R/J is an M-sequence.*

(3) *Every system of parameters of R/J is an M-sequence.*

(Recall that $x_1, \cdots, x_n$ is a system of parameters for a local ring (R, P) if and only if $n = \dim R$ and equivalently

(a) $\operatorname{Rad}(x_1, \cdots, x_n) = P$,

(b) for each k, $0 \leq k \leq n$, $\dim R/(x_1, \cdots, x_k)R = \dim R - k$.)

The reader will see easily that the following conditions are equivalent as well:

(4) *M is a Cohen-Macaulay module over R/J_0 for some $J_0 \subset J$.*

(5) *M is a Cohen-Macaulay module over R/J_0 for every $J_0 \subset J$.*

(6) *M is a maximal Cohen-Macaulay module over R/J.*

Moreover, it is shown in [S] that if M is a Cohen-Macaulay module over R, then, for each $Q \in \operatorname{Supp} M$, M_Q is a Cohen-Macaulay module over R_Q.

Thus, a local ring R is Cohen-Macaulay if and only if some (equivalently, every) system of parameters is an R-sequence.

Conjecture (5) (Bass' conjecture). *If a local ring R possesses a nonzero module T of finite type and finite injective dimension, then R is Cohen-Macaulay.*

(The converse is true: if R is Cohen-Macaulay and $x_1, \cdots, x_n$ is a system of parameters, the injective hull E of $R/(x_1, \cdots, x_n)R = S$ as an S-module has finite length and the fact that it is injective over S implies that it is of finite injective dimension over R.)

Peskine and Szpiro prove (5) in many of the same cases for which they prove (3). In fact, they prove (3) $\Rightarrow$ (5) for the class of local rings closed under (a), (b).

Thus:

$$\begin{tikzcd}
 & \text{(1) Rigidity} \arrow[d, Rightarrow] & \\
 & \text{Intersection (3)} \arrow[r, Leftrightarrow] \arrow[dl, Rightarrow] \arrow[dr, Rightarrow] & \text{(4) Homological height} \\
\text{(2) Zerodivisor} & & \text{(5) Bass}
\end{tikzcd}$$

We indicate briefly how the argument (3) $\Rightarrow$ (5) runs.

If there is a counterexample to (5), choose one of least Krull dimension, say n, and complete it (see [LV]): We then have (R, P) complete, $T \neq 0$ an R-module of finite type, and id $T < \infty$. We must show R is Cohen-Macaulay. Choose a prime p of R such that $\dim R/p = n$. There may be a $Q \in \operatorname{Supp} T$ such that $P \supsetneqq Q \supset p$. If so there is such a Q with $\dim R/Q = 1$. Since $T_Q \neq 0$ and R has minimal Krull dim for a counterexample, R_Q is Cohen-Macaulay. Since R/p is a complete local domain of dimension n, depth $R_Q = \dim R_Q = \operatorname{ht} Q \geq \operatorname{ht} Q/p = n - 1$. By [PS, Proposition 4.7, p. 341], depth R (= id T) = $\dim R/Q$ + depth $R_Q \geq 1 + (n-1) = n$, as required.

Thus, we may suppose no $Q \in \operatorname{Supp} T$ except P contains p, i.e. $\operatorname{Supp}(T \otimes R/p) = \{P\}$. Let E be the injective hull of R/P. Then $M = \operatorname{Ext}_R^d(E, T)$, where d = depth R, is an R-module of finite type and finite *projective* dimension with the same support as T, by [PS, Theorem 4.10, p. 342]. Thus, $\operatorname{Supp}(M \otimes R/p) = \{P\}$, whence, assuming that (3) holds for R, we have $\dim R = n = \dim R/p \leq \operatorname{pd} M \leq$ depth R, and R is Cohen-Macaulay. Q.E.D.

We next want to look at the following question and connect it up with the others:

Conjecture (6) (Small Cohen-Macaulay modules conjecture). *If R is a complete local ring, then R has a maximal Cohen-Macaulay module.*

Peskine and Szpiro had observed [PS] that (6) $\Rightarrow$ (5) while I had observed in [H_2] that (6) and even the much weaker Conjecture (7) below implies (3).

Conjecture (7) (Big Cohen-Macaulay modules conjecture). *If R is a local ring and $x_1, \cdots, x_n$ is a system of parameters, then there exists an R-module M (not necessarily of finite type) such that $x_1, \cdots, x_n$ is an M-sequence.*

Note that we then have both

$$(x_1, \cdots, x_n)M \neq M \quad \text{and} \quad (x_1, \cdots, x_i)M : x_{i+1}R = (x_1, \cdots, x_i)M, \quad 0 \leq i < n.$$

Of course, (6) $\Rightarrow$ (7). If M is a maximal Cohen-Macaulay module over $\hat{R}$, the completion of R, then, for every system of parameters $x_1, \cdots, x_n$ of R, $x_1, \cdots, x_n$ is an M-sequence.

Remark. There exist two-dimensional local domains R which do not have a maximal Cohen-Macaulay module, i.e. for every module M over R of finite type, depth $M \leq 1$. See $[\mathrm{H}_2, \S 1]$ and [FR].

We shall give a proof that (7)$\Longrightarrow$(3). For the moment we simply keep track of the situation:

$$
\begin{tikzcd}
 & \text{(6) Small C-M modules} \arrow[d, Rightarrow] & \\
\text{Rigidity (1)} \arrow[dr, Rightarrow] & \text{(7) Big C-M modules} \arrow[d, Rightarrow] & \\
 & \text{Intersection (3)} \arrow[r, Leftrightarrow] \arrow[dl, Rightarrow] \arrow[dr, Rightarrow] & \text{(4) Homological height} \\
\text{Zerodivisor (2)} & & \text{(5) Bass}
\end{tikzcd}
$$

We shall devote some time to a proof of (7) in the case where R_{red} (i.e. $R/$(nilpotents)) contains a field.

In the preceding diagram most of the interesting consequences of (6) can be seen to follow from the weaker Conjecture (7). However, (6) has implications for the theory of multiplicities which do not seem to follow from (7).

Let (R, P) be a regular local ring and let M, N be R-modules of finite type such that $M \otimes N$ has finite length. It is then known that $\dim M + \dim N \leq \dim R$.

In this situation each $\mathrm{Tor}_i^R(M, N)$ is annihilated by $\mathrm{Ann}\, M + \mathrm{Ann}\, N$ and hence by a power of P, so that each $\mathrm{Tor}_i(M, N)$ has finite length, and it makes sense to define the intersection multiplicity $e(M, N)$ by

$$e(M, N) = \sum_i (-1)^i \ell(\mathrm{Tor}_i^R(M, N))$$

where ℓ denotes length. The terms are 0 except for $0 \leq i \leq \dim R$.

To understand a little bit of the geometric signifigance of this notion, let K be an algebraically closed field and let R be the local ring at the origin of $\mathbf{A}_K^2$, the plane, i.e. $R = K[x, y]_{(x,y)}$. Let C_1, C_2 be curves through the origin, where C_1 is defined by $f = 0$ and C_2 by $g = 0$, $f, g \in K[x, y]$. Let us assume that f, g have no common component through the origin. This is equivalent to the assertion that if $M = R/(f)$, $N = R/(g)$, then $M \otimes N$ has finite length. In this case $e(M, N)$ is the intersection multiplicity of C_1 and C_2 at the origin.

If the lowest degree form in f is f_d, a homogeneous polynomial of degree d in two variables, then f_d factors completely into linear forms which correspond geometrically to the tangent lines to C_1 at the origin. Suppose that f_d is square-free, and that the lowest degree form g_e (of degree e) in g is also square-free, and suppose also that

C_1 and C_2 have no common tangent at the origin, i.e., f_d and g_e are relatively prime. It is natural to think of f and g crossing each other de times. And, in fact, in this case it can be shown that $e(M, N)$ (i.e. $e(R/(f), R/(g))$) *is* de.

If R is a regular local ring which contains a field, or if R is regular, characteristic $R/P = p$, $\mathbf{Z} \subset R$, but $p \notin P^2$, R is called *unramified.* If R is unramified it is known that $\hat{R}$ is isomorphic to a formal power series ring over a complete discrete valuation ring. Now Serre [S] proved the following good properties for his multiplicity function $e(M, N)$ in the unramified case (more generally, if $\hat{R}$ is a formal power series ring over a complete discrete valuation ring).

Theorem 2.2. *Let R be a regular local ring such that $\hat{R}$ is a formal power series ring over a complete discrete valuation ring (e.g. suppose R is unramified). Let M, N be R-modules of finite type such that $M \otimes N$ has finite length. Then:*

(M_1) *If* $\dim M + \dim N < \dim R$, *then* $e(M, N) = 0$.

(M_2) *If* $\dim M + \dim N = \dim R$, *then* $e(M, N) > 0$.

As Serre remarks, it is natural to conjecture that this result holds for any regular local ring. Explicitly:

Conjecture (8) (Serre's conjecture). (M_1) *and* (M_2) *hold for an arbitrary regular local ring* R.

This is true for $\dim R \leq 4$ [H_2].

A much more general conjecture on which Peskine and Szpiro have made progress in the graded case is:

Conjecture (9) (Strong multiplicities conjecture). *Let R be a local ring and let M, N be modules of finite type such that* $\operatorname{pd} M$ *is finite and $M \otimes N$ has finite length. Then, again, it makes sense to define $e(M, N)$ as* $\sum_i (-1)^i \ell(\mathrm{Tor}_i(M, N))$ ($\mathrm{Tor}_i(M, N) = 0$ *unless* $0 \leq i \leq \operatorname{pd} M$). *Then*

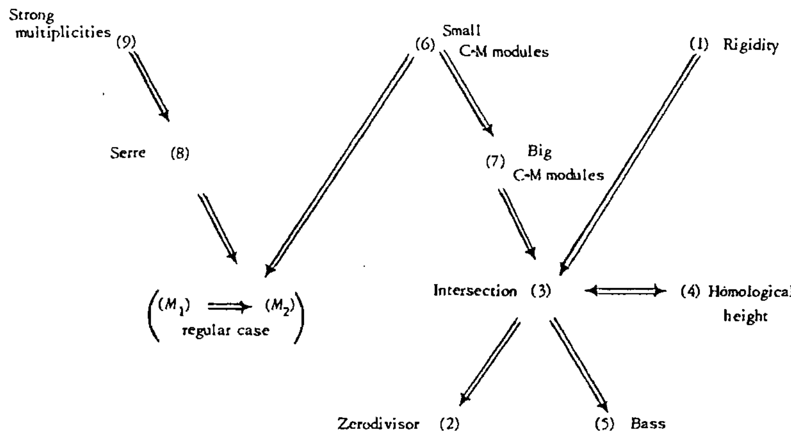
(M_0) $\dim M + \dim N \leq \dim R$.

(M_1) *If* $\dim M + \dim N < \dim R$, $e(M, N) = 0$.

(M_2) *If* $\dim M + \dim N = \dim R$, $e(M, N) > 0$.

Of course, $(9) \Rightarrow (8)$. The relationship of (8) to (6) is that, in the presence of (6), $(\mathrm{M}_1) \Rightarrow (\mathrm{M}_2)$ in the regular case. We shall prove this in §3.

We now have the following relationships:



We shall next examine two related conjectures of a seemingly very elementary nature which follow from (6) or even (7) (thus, are known if the local ring R contains a field) but which seem to be quite resistant in the general case.

Conjecture (10) (Direct summand conjecture). *Let R be a regular Noetherian ring (i.e. the local rings of R are regular) and let S be a module-finite extension algebra of R. Then R is a direct summand of S as R-modules.*

This question is studied in [H_3]. One may reduce to the case where R is local and complete, and S is a domain. Let $x_1, \cdots, x_n$ be a regular system of parameters for R. It is shown in [H_3] that R is then a direct summand of S if and only if, for every positive integer t,

$$(*) \qquad x_1^t \cdots x_n^t \notin (x_1^{t+1}, \cdots, x_n^{t+1})S.$$

This is established in [H_3] for the case that S contains a field, and (*) is also shown to hold if S has a module M such that $x_1, \cdots, x_n$ is an M-sequence.

In [H_3] the following conjecture is also established in the case that R contains a field or if there is a module M such that $x_1, \cdots, x_n$ is an M-sequence.

Conjecture (11) (Monomial conjecture). *Let S be a local ring and let $x_1, \cdots, x_n$ be a system of parameters. Then, for every positive integer t,*

$$(*) \qquad x_1^t \cdots x_n^t \notin (x_1^{t+1}, \cdots, x_n^{t+1})S.$$

Then, obviously, (11) $\Rightarrow$ (10), for the system of parameters $x_1, \cdots, x_n$ for R is also a system of parameters for S.

Both (10) and (11) seem to be open questions for the case $n = 3$, and (11) seems to be open even when $t = 2$, $n = 3$ (if S does not contain a field).

We conclude this section with a brief discussion of the relationship of the conjectures considered here and the conjectures (a)–(f) considered in [PS, Chapter II, §0].

(a) $\equiv$ (M_0) of the strong multiplicities conjecture, (9).

(b) $\equiv$ the zerodivisor conjecture, (2).

(c) $\equiv$ rigidity conjecture (1).

(d) $\equiv$ intersection conjecture, (3).

(e) We have not previously considered. It is:

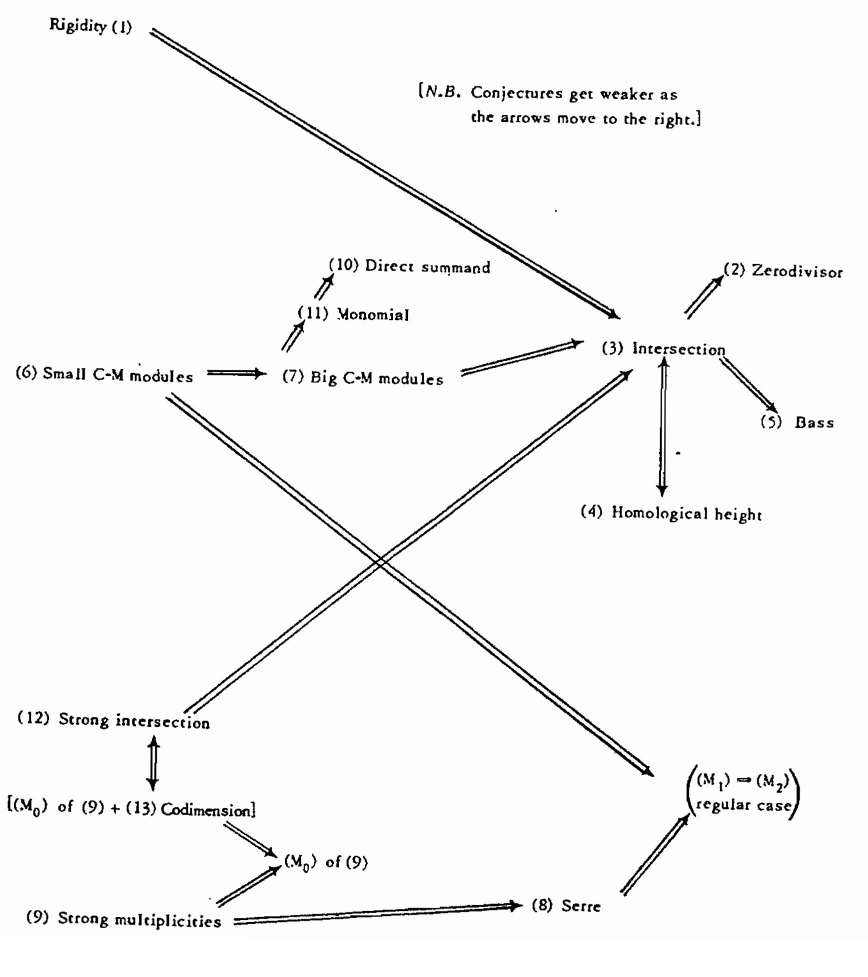
Conjecture (12) (Strong intersection conjecture). *Let* (R, P) *be a local ring and let* M, N *be* R*-modules of finite type such that* $\operatorname{pd} M < \infty$ *and* $\operatorname{Supp}(M \otimes N) = P$. *Let* $I = \operatorname{Ann} M$. *Then* $\dim N \le \operatorname{depth} I$ *(as an ideal).*

(f) is also new. It is:

Conjecture (13) (Codimension conjecture). *If* R *is a local ring,* $M \neq 0$ *is a module of finite type with* $\operatorname{pd} M < \infty$, *and* $I = \operatorname{Ann} M$, *then* $\dim M + \operatorname{depth} I = \dim R$.

We now consider the relationships of all thirteen conjectures, incorporating the new facts $(12) \Rightarrow (3)$ and $(12) \Leftrightarrow (M_0)$ of (9) *and* (13) proved in Theorem 0.10 of [PS]. (*Note*: (d) $\Leftarrow$ (b) on p. 357 of [PS] is not proved there, was inserted by error, and is not known. (d) $\Rightarrow$ (b) is correct.)

We now have:



http://dx.doi.org/10.1090/cbms/024/04

3. Consequences of the Existence of Cohen-Macaulay Modules

We want to discuss in greater detail the implications of Conjectures (6) and (7) of the previous section. We shall also indicate proofs, sometimes sketchily, sometimes in detail, of the results (7) $\Rightarrow$ (3), (7) $\Rightarrow$ (11), (6) $\Rightarrow$ ((M_1) $\Rightarrow$ (M_2), regular case), etc. stated without proof in the preceding section.

We shall first look at (6) a bit more closely. Let R be a complete local ring of dimension n. Let p be a prime such that $\dim R/p = n$. If M is a maximal Cohen-Macaulay module over R/p, then it is also a maximal Cohen-Macaulay module over R. Thus, in considering Conjecture (6), one may assume that R is a complete local domain. Then R is a finite module over a complete regular local ring A. If $M \neq 0$ is an R-module of finite type, then $\operatorname{depth}_R M = n$ if and only if $\operatorname{depth}_A M = n$. But $\operatorname{depth}_A M = n \Leftrightarrow \operatorname{pd}_A M = \dim A - \operatorname{depth}_A M = n - n = 0$, i.e. if and only if M is a nonzero free A-module. This yields two conjectures which are equivalent to Conjecture (6):

Conjecture (6′). *If A is a complete regular local ring and R is a module-finite extension domain, then, for some positive integer t, A^t has the structure of an R-module.*

Conjecture (6″). *If A is a complete regular local ring and R is a module-finite extension domain then there is an embedding $R \to \mathfrak{M}_t(A)$ for some $t \geq 1$, where $\mathfrak{M}_t(A)$ is the ring of $t \times t$ matrices with coefficients in A.*

(We have omitted two statements: in (6′), the R-module structure of A^t should extend its A-module structure, while in (6″) the map $R \to \mathfrak{M}_t(A)$ should extend the obvious embedding $A \to \mathfrak{M}_t(A)$ as the $t \times t$ scalar matrices.)

Conjecture (6) is known in only very few instances. If R is a complete local domain and $\dim R \leq 2$, its integral closure is Cohen-Macaulay and, in fact, is a Cohen-Macaulay R-module of finite type (cf. [LV]). Several other arguments for the case $\dim R \leq 2$ are given in [H_2].

If R is a graded algebra of finite type over a field of characteristic $p > 0$ and P is the irrelevant ideal, then if $\dim R = 3$ it is known that there exists a graded R-module of finite type M such that $\operatorname{depth}(P, M) = 3$. This result is in the Brandeis preprint *Notes sur un air de Bass* by Peskine and Szpiro but has not been published. The argument uses the Frobenius and the fact that the local cohomology modules $H^{\bullet}_P(R)$ are graded.

But (6) seems to be open in dimension 3, even for rings of the form $\hat{R}_P$, where R is a graded domain of finite type over an algebraically closed field K of characteristic 0, $R_0 = K$, $\dim R = 3$, and P is the irrelevant ideal.

We next indicate the proof of (6) $\Rightarrow$ ((M_1) $\Rightarrow$ (M_2), regualr case).

Proposition 3.1. *Let R be a regular local ring and suppose that*:

(a) (M_1) *holds for* $\hat{R}$.

(b) *Every domain which is a homomorphic image of* $\hat{R}$ *has a maximal Cohen-Macaulay module.*

Then (M_2) *holds for* R *and* $\hat{R}$.

Thus, if a class of local rings is closed under completion and passage to homomorphic images and Conjecture (6) *holds for the complete local rings in this class, then* $(\mathrm{M}_1) \Rightarrow (\mathrm{M}_2)$ *for the regular local rings in the class.*

Proof. If M, N are R-modules of finite type, where R is local, then $M \otimes_R N$ has finite length if and only if $\hat{M} \otimes_{\hat{R}} \hat{N}$ does, and $\mathrm{Tor}_i^{\hat{R}}(\hat{M}, \hat{N}) \cong \mathrm{Tor}_i^R(M, N) \otimes_R \hat{R}$ and this implies $\mathrm{Tor}_i^{\hat{R}}(\hat{M}, \hat{N}) \cong \mathrm{Tor}_i^R(M, N)$ if $M \otimes N$ has finite length. Moreover, $\dim M = \dim \hat{M}$, $\dim N = \dim \hat{N}$, and to show that (M_2) holds for a regular local ring R, it suffices to prove it for $\hat{R}$.

Thus, we may assume that R is a complete regular local ring, that every R/Q, Q prime, has a maximal Cohen-Macaulay module, and that (M_1) holds for R, and we must prove that (M_2) holds for R.

If $0 \to M' \to M \to M'' \to 0$ is a short exact sequence of moduels of finite type and N is of finite type, then $M \otimes N$ has finite length if and only if $M' \otimes N$ and $M'' \otimes N$ do. In this case, it follows easily from the long exact sequence for Tor that $e(M, N) = e(M', N) + e(M'', N)$. It follows that if

$$0 = M_0 \subset M_1 \subset \cdots \subset M_r = M \tag{A}$$

is a filtration of M then

$$e(M, N) = \sum_{i=1}^{r} e(M_i/M_{i-1}, N)$$

and if we also have a filtration

$$0 = N_0 \subset N_1 \subset \cdots \subset N_s = N \tag{B}$$

then

$$e(M, N) = \sum_{i=1}^{r} \sum_{j=1}^{s} e(M_i/M_{i-1}, N_j/N_{j-1}).$$

Now suppose $M \otimes N$ has finite length and $\dim M + \dim N = \dim R$. We can choose filtrations (A), (B) as above such that, for each i, j, M_i/M_{i-1}, N_j/N_{j-1} have the form R/Q, where Q is prime. $\dim M = \max\{\dim R/Q : R/Q$ occurs in the filtration of $M\}$, and likewise for $\dim N$. By (M_1), $e(R/Q, R/Q')$ (where these occur in the filtrations) vanishes unless $\dim R/Q = \dim M$, $\dim R/Q' = \dim N$.

It follows that we may assume $M = R/Q$, $N = R/Q'$. Let M^*, N^* be maximal Cohen-Macaulay modules over R/Q, R/Q', respectively. Since R/Q is a domain, every nonzero nonunit is part of a system of parameters, hence not a zerodivisor on M^*, and M^* is torsion-free over R/Q. Thus, M^* contains a nonzero free (R/Q)-module, say $F = (R/Q)^a$, such that M^*/F is a torsion module over R/Q, and likewise, N^* contains a nonzero free (R/Q')-module, say $G = (R/Q')^b$, such that N^*/G is a torsion module over R/Q'. Then $e(M^*, N^*) = e(F, G) + e(F, N^*/G) + e(M^*/F, G) + e(M^*/F, N^*/G)$, and the last three terms vanish by (M_1). Hence $e(M^*, N^*) = e(F, G) = ab \cdot e(R/Q, R/Q')$, $a > 0$, $b > 0$. Thus, to show $e(R/Q, R/Q') > 0$, it suffices to show $e(M^*, N^*) > 0$. Thus, the whole result follows from

Lemma 3.2. *Let R be a regular local ring and let M^*, N^* be Cohen-Macaulay modules (of finite type) such that $M^* \otimes N^*$ has finite length, and* $\dim M^* + \dim N^* = \dim R$. *Then*

$$\mathrm{Tor}_i^R(M^*, N^*) = 0, \quad i \geq 1,$$

so that $e(M^*, N^*) = \ell(M^* \otimes N^*) > 0$.

Proof. All we need to prove is the assertion about the vanishing of the Tor's. This follows from the following weak depth-sensitivity result (which will also be used in the proof that (7) $\Rightarrow$ (3)):

Proposition 3.3. *Let R be a ring, let M be an R-module of finite* Tor *dimension $\leq s$ (i.e. for all N, $\mathrm{Tor}_i^R(M, N) = 0$ if $i > s$), let $x_1, \cdots, x_k \in I = \mathrm{Ann}\, M$, and let E be an R-module.*

Suppose that

(a) $M \otimes E \neq 0$ *and*

(b) $(x_1, \cdots, x_i)E \colon x_{i+1}R = (x_1, \cdots, x_i)E$, $0 \leq i < k$.

Then $x_1, \cdots, x_k$ is an E-sequence, and if d is the biggest integer such that $\mathrm{Tor}_d^R(M, E) \neq 0$, $0 \leq d \leq s$ and $d + k \leq s$.

Proof. To see that $x_1, \cdots, x_k$ is an E-sequence, we must show that $(x_1, \cdots, x_k)E \neq E$. But if $J \subset I = \mathrm{Ann}\, M$, we have $M \otimes (E/JE) \cong M \otimes (R/J) \otimes E \cong (M/JM) \otimes E \cong M \otimes E \neq 0$, so that $E \neq JE$. We use induction on k. If $k = 0$, the result is obvious. If $k > 0$, let $x = x_1$, and let $E' = E/xE$. Thus E' satisfies the same hypptheses as E with $k' = k - 1$ (the E'-sequence is $x_2, \cdots, x_k$) and we need only show that d', the number of the highest nonvanishing Tor for E', is $d + 1$, for then the induction hypothesis yields $k' + d' = (k - 1) + (d + 1) = k + d \leq s$. We have a short exact sequence

$$0 \longrightarrow E \xrightarrow{x} E \longrightarrow E' \longrightarrow 0$$

and since $x \in \mathrm{Ann}\, M$ the long exact sequence for Tor breaks up into short exact sequences

$$0 \longrightarrow \mathrm{Tor}_i(M, E) \longrightarrow \mathrm{Tor}_i(M, E') \longrightarrow \mathrm{Tor}_{i-1}(M, E) \longrightarrow 0$$

(because for all i the map $x\colon \mathrm{Tor}_i(M, E) \to \mathrm{Tor}_i(M, E)$ is 0). Then, clearly, $\mathrm{Tor}_i(M, E') = 0$ if $i > d + 1$, and $\mathrm{Tor}_{d+1}(M, E') \cong \mathrm{Tor}_d(M, E) \neq 0$, so that $d' = d + 1$. Q.E.D.

Completion of the proof of Lemma 3.2. We want to apply the above result with $M = M^*$, $E = N^*$. Since $M^* \neq 0$, $N^* \neq 0$, $M^* \otimes N^* \neq 0$. If k is the length of a maximal N^*-sequence in $I = \mathrm{Ann}\, M^*$ and d is the biggest integer with $\mathrm{Tor}_i(M^*, N^*) \neq 0$, then

$d+k \leq \mathrm{pd}\, M^*$. Now, let $J = \mathrm{Ann}\, N^*$. Since $M^* \otimes N^*$ has finite length, $I+J$ is primary to the maximal ideal P of R. Then $K = \mathrm{depth}(I, N^*) = \mathrm{depth}(I+J, N^*)$ (since $JN^* = 0$) $= \mathrm{depth}(P, N^*) = \mathrm{depth}\, N^* = \dim N^*$ (since N^* is Cohen-Macaulay) $= \dim R - \dim M^*$ (since $\dim M^* + \dim N^* = \dim R$) $= \dim R - \mathrm{depth}\, M^*$ (since M^* is Cohen-Macaulay) $=$ $\mathrm{pd}\, M^*$ (since R is regular). Then $d+k \leq \mathrm{pd}\, M^*$ says $d + \mathrm{pd}\, M^* \leq \mathrm{pd}\, M^*$ or $d \leq 0$, and $\mathrm{Tor}_i(M^*, N^*) = 0$ for $i \geq 1$. Q.E.D.

We shall now apply the same result, Proposition 3.3, to show that (7) $\Rightarrow$ (3), and even something slightly better:

Proposition 3.4. *Let R be a local ring, and suppose that for each prime Q of R there is a system of parameters $y_1, \cdots, y_k$ for R/Q and an (R/Q)-module E such that $y_1, \cdots, y_k$ is an E-sequence.*

Then if $M \neq 0$, N are R-modules of finite type such that $M \otimes_R N$ has finite length, then $\dim N \leq \mathrm{pd}_R M$. *In other words, the intersection conjecture* (3) *holds for R.*

Thus, if the big Cohen-Macaulay modules conjecture (7) *holds for a class of local rings closed under passage to homomorphic images, then so does the intersection conjecture* (3).

Proof. We need only prove the assertion of the second paragraph, given the assumption of the first paragraph. If $N = 0$ or if $\mathrm{pd}\, M = \infty$, the result is trivial. Thus, we may assume $N \neq 0$, and $\mathrm{pd}\, M$ is finite. Let $I = \mathrm{Ann}\, M$, $J = \mathrm{Ann}\, N$. The assertion that $M \otimes N$ has finite length is equivalent to the assertion that $I + J$ is primary to the maximal ideal P of R. Hence, we might as well assume $N = R/J$.

Let $Q \supset J$ be a prime such that $\dim R/Q = \dim R/J$ ($= \dim N$). By hypothesis, we can choose $y_1, \cdots, y_k$, a system of parameters for R/Q, and an (R/Q)-module E such that $y_1, \cdots, y_k$ is an E-sequence. Let $y_1^*, \cdots, y_k^* \in P$ be elements whose residues modulo Q are $y_1, \cdots, y_k$. Since $I+J$ is primary to P, we may assume, after replacing the y_i and y_i^* by their tth powers for a suitably large t, that $y_1^*, \cdots, y_k^* \in I+J$, and then $y_1^*, \cdots, y_k^*$ form an E-sequence. In fact, since $J \subset Q$ and $QE = 0$, we can find elements $x_1, \cdots, x_k \in I$ such that $y_i^* = x_i + z_i$, $z_i \in J$, $1 \leq i \leq k$, and then $x_1, \cdots, x_k$ is an E-sequence.

What is more, $M \otimes E \neq 0$. To see this, it will suffice to show that $(R/P) \otimes E \neq 0$, for then $(R/P) \otimes (M \otimes E) \cong (R/P \otimes M) \otimes (R/P \otimes E)$ is the tensor product of two nonzero vector spaces over R/P, hence, is not zero, and so $M \otimes E \neq 0$. Since $y_1, \cdots, y_k$ is an E-sequence, $(y_1, \cdots, y_k)E \neq E$. Since $QE = 0$, if we let P_0 be the inverse image of $(y_1, \cdots, y_k)$ in R, $P_0 E \neq E$. Since $y_1, \cdots, y_k$ is a system of parameters for R/Q, P_0 is primary to P, say $P^t \subset P_0$. Then $PE \neq E$, for $PE = E \Rightarrow P^s E = E$ for all positive integers $s \Rightarrow P^t E = E \Rightarrow P_0 E = E$, a contraction. Thus $PE \neq E$, and $(R/P) \otimes E \neq 0$.

But we may now apply Proposition 3.3 and conclude $d + k \leq \mathrm{pd}\, M$.

Here, $0 \leq d \leq \mathrm{pd}\, M$, since d is the biggest integer such that $\mathrm{Tor}_d(M, E) \neq 0$, and k is the length of a system of parameters for R/Q, i.e. $k = \dim(R/Q) = \dim(R/J) =$ $\dim N$. Thus, certainly $k = \dim N \leq \mathrm{pd}\, M$. Q.E.D.

We next want to indicate how (7) $\Rightarrow$ (11).

Proposition 3.5. *Let S be any ring and let $x_1, \cdots, x_n$ be elements of S. Suppose there is a module E over S such that:*

(1) $(x_1, \cdots, x_n)E \neq E$.

(2) The first Koszul homology module $H_1 = H_1(\mathcal{K}_.(x_1, \cdots, x_n; E)) = 0$. (This is automatic if $x_1, \cdots, x_n$ is an E-sequence.)

Then, for every integer $t \geq 1$, $x_1^t \cdots x_n^t \notin (x_1^{t+1}, \cdots, x_n^{t+1})S$.

Proof. Let $\mathbf{Z}$ be the integers. Let $X_1, \cdots, X_n$ be indeterminates over $\mathbf{Z}$, let $B = \mathbf{Z}[X_1, \cdots, X_n]$, and make S into a B-algebra by mapping X_i to x_i, $1 \leq i \leq n$. We can think of $\mathbf{Z} = B/(X_1, \cdots, X_n)B$ as a B-module, and then $H_1 \cong \mathrm{Tor}_1^B(\mathbf{Z}, E) = 0$.

Let $I = (X_1^t, \cdots, X_n^t) \subset B$ and let $J = (X_1^t, \cdots, X_n^t, X_1^{t+1}, \cdots, X_n^{t+1}) \subset B$. It is easy to see that $J/I \cong \mathbf{Z}$.

Let I_0 be any ideal of B generated by monomials in $X_1, \cdots, X_n$ which contains a power of each X_i, $1 \leq i \leq n$. We shall show that B/I_0 has a filtration in which all factors are copies of $\mathbf{Z}$. For if $I_0 \neq B$ there is a monomial $U \notin I_0$ such that $X_iU \in I_0$, $1 \leq i \leq n$, and then $(I_0 + UB)/I_0 \cong \mathbf{Z}$, and the result follows from Noetherian induction on I_0, since $I_0 + UB$ is a larger ideal of the same form.

Since condition (2) of the proposition yields that $\mathrm{Tor}_1^B(\mathbf{Z}, E) = 0$, it follows that for I_0 as above, $\mathrm{Tor}_1^B(B/I_0, E) = 0$. Since $0 \to I_0 \to B \to B/I_0 \to 0$ is exact, $0 \to I_0 \otimes_B E \to B \otimes_B E$ is injective, and $I_0 \otimes_B E \cong I_0E$ for each I_0. Thus, $I \otimes_B E \cong IE$ and $J \otimes_B E \to JE$. We have the exact sequence $0 \to I \to J \to J/I \to 0$ and $J/I \cong \mathbf{Z}$. Applying $\otimes_B E$ and recalling that $\mathrm{Tor}_1^B(\mathbf{Z}, E) = 0$, we have that $0 \to IE \to JE \to \mathbf{Z} \otimes E \to 0$ is exact, and $\mathbf{Z} \otimes_B E \cong E/(X_1, \cdots, X_n)E \neq 0$, by (1), so that $IE \subsetneqq JE$. But then $IS \subsetneqq JS$, certainly, and so $x_1^t, \cdots, x_n^t \notin (x_1^{t+1}, \cdots, x_n^{t+1})$. Q.E.D.

For further applications of Conjectures (6)–(7) the reader may wish to see Theorems 6, 7, 8 of [H_6].

http://dx.doi.org/10.1090/cbms/024/05

4. Modifications and the Existence of Big Cohen-Macaulay Modules in Characteristic $p > 0$

Henceforth, it will be convenient to make two more terminological conventions: we abbreviate "system of parameters" to "s.o.p.", and if x denotes the sequence $x_1, \cdots, x_n$ in a ring R and M is an R-module, then we use the phrase "M is x-regular" to mean precisely the same thing as the phrase "$x_1, \cdots, x_n$ is an M-sequence".

We shall construct big Cohen-Macaulay modules over a local ring R containing a field by an extremely naive direct limit process in which we get rid of "bad" relations more or less "one at a time" by "enlarging" the module in as "free" as possible a manner so as to trivialize the bad relation. This very trivially creates a module E in the direct limit such that $(x_1, \cdots, x_k)E: x_{k+1}R = (x_1, \cdots, x_k)E$, $0 \leq k < n$, but there is an obstruction: one does not know that $(x_1, \cdots, x_n)E \neq E$.

In this section we analyze this set-up, "isolate" the obstruction and show that our idea works if R contains a field of characteristic $p > 0$ by a trick involving the Frobenius functor.

In the next section we show that our direct limit idea also works if R contains a field of characteristic 0; we may use a trick involving M. Artin's approximation theorem and results on "generic flatness" to reduce to the characteristic $p > 0$ case. Further details may be found in [H_4]. The results are announced in [H_7].

Let (R, P) be a local ring and $\mathrm{x} = x_1, \cdots, x_n$ an s.o.p. for R. Let M be an R-module and $a \in M$. If $x_1m_1 + \cdots + x_{k+1}m_{k+1} = 0$, $0 \leq k < n$, we refer to $\rho = (m_1, \cdots, m_{k+1}) \in M^{k+1}$ as a *type* k *relation for* x *on* M. If we let $\mathrm{v} = m_{k+1} \oplus (x_1, \cdots, x_k) \in M \oplus R^k$ we have obvious maps

$$M \to M \oplus R^k, \quad M \oplus R^k \twoheadrightarrow (M \oplus R^k)/R\mathrm{v}$$

and hence a map $M \to (M \oplus R^k)/R\mathrm{v} = M'$. Let a' be the image of a in M'. We call (M', a') a (*first*) *modification of* (M, a) (*of type* k). We also have a map $(M, a) \to (M', a')$ (i.e. a map $M \to M'$ which takes a to a').

In general, we may have a sequence

$$(M, a) = (M_0, a_0) \to (M_1, a_1) \to \cdots \to (M_r, a_r) = (M', a')$$

in which (M_{i+1}, a_{i+1}) is a modification of (M_i, a_i) with respect to a relation ρ_i on M_i of type k_{i+1}, $0 \leq i < r$. We then say that (M', a') is an (rth) modification of (M, a) of type $(k_1, \cdots, k_r)$.

The main point about modifications is the following almost trivial but quite useful result.

Theorem 4.1. *Let (R, P) be an n-dimensional local ring and let $\mathrm{x} = x_1, \cdots, x_n$ be an s.o.p. Then the following two conditions are equivalent:*

(1) *R possesses an* x*-regular module.*

(2) *For every modification (M, a) of $(R, 1)$, $a \notin (\mathrm{x})M$.*

Proof. Assume (1). Let E be x-regular and choose $b \in E - (\mathrm{x})E$. There is a unique map $\phi: (R, 1) \to (E, b)$. To prove (2), it will suffice to show that it is possible to define $\psi: (M, a) \to (E, b)$ so that the diagram

$$\begin{tikzcd}
(M, a) \arrow[dr, "\psi"] & \\
(R, 1) \arrow[u, "\mu"] \arrow[r, "\phi"'] & (E, b)
\end{tikzcd}$$

commutes. For then $a \in (\mathrm{x})M$ would yield $b = \psi(a) \in (\mathrm{x})\psi(M) \subset (\mathrm{x})E$, a contradiction. Proceeding by induction we may suppose that (M, a) is the modification of (M^*, a^*) with respect to some type k relation $\rho = (m_1, \cdots, m_{k+1})$ (i.e. $\sum_{i=1}^{k+1} x_i m_i = 0$) and if $\mu^*: (R, 1) \to (M^*, a^*)$ is the modification map then there is a $\psi^*: (M^*, a^*) \to (E, b)$ such that $\phi = \psi^* \mu^*$.

Thus, $M = (M^* \oplus R^k)/R\mathrm{v}$, where $\mathrm{v} = m_{k+1} \oplus (x_1, \cdots, x_k)$, and to define ψ it suffices to specify images $e_1, \cdots, e_k$ in E for the generators of R^k such that $\psi^*(m_{k+1}) + x_1 e_1 + \cdots + x_k e_k = 0$ in E. That is, we are looking for a map $\sigma: R^k \to E$ such that $\psi^* \oplus \sigma$ kills v. This will be possible if $\psi^*(m_{k+1}) \in (x_1, \cdots, x_k)E$. But $x_{k+1}\psi^*(m_{k+1}) = \psi^*(x_{k+1}m_{k+1}) = -\sum_{i=1}^{k} x_i \psi^*(m_i) \in (x_1, \cdots, x_k)E$, and since E is x-regular the result follows. Thus, $(1) \Rightarrow (2)$.

The proof of $(2) \Rightarrow (1)$ is even easier. Form a sequence of successive modifications of $(R, 1)$, say $(R, 1) = (M_0, a_0) \to (M_1, a_1) \to (M_2, a_2) \to \cdots$, and, while doing so, choose for each M_i a finite set of generators for the type k relations on M_i, $0 \leq k < n$. The reader should have no difficulty in seeing that such a sequence can be formed so that it satisfies the following condition: For each $i \geq 0$, for each k, $0 \leq k < n$, and for each specified generator ρ for the type k relations on M_i, there is a $j \geq i$ such that the relation used in forming (M_{j+1}, a_{j+1}) from (M_j, a_j) is the image of ρ (under the map $M_i^k \to M_j^k$ induced by the modification map $M_i \to M_j$). Let $E = \varinjlim_i M_i$ for such a sequence and let b be the image of 1 in E. Then it is quite clear from our construction that for each i there is a $j \geq i$ such that the image of $(x_1, \cdots, x_k)M_i : Rx_{k+1}$ in M_j is contained in $(x_1, \cdots, x_k)M_j$, $0 \leq k < n$, and it follows that $(x_1, \cdots, x_k)E : x_{k+1}R = (x_1, \cdots, x_k)E$, $0 \leq k < n$. Thus, E will be x-regular provided $b \notin (\mathrm{x})E$. But $b \notin (\mathrm{x})E$ since, by (2), $a_i \notin (\mathrm{x})M_i$ for every i. Q.E.D.

We now want to describe in an explicit way what an rth modification of $(R, 1)$ of type $\mathbf{k} = (k_1, \cdots, k_r)$ looks like, $0 \leq k_i < n$, $1 \leq i \leq r$, and what it means if condition (2) of Theorem 4.1 fails for such a modification.

In working with vectors, it will be convenient to identify a vector of length q with the vector of length $q + q'$ whose last q' entries are 0.

It will also be convenient to define $k_0 = 1$.

Let $(M_0, a_0) \to \cdots \to (M_i, a_i) \to \cdots \to (M_r, a_r)$ be the sequence of modifications considered, where $(R, 1) = (M_0, a_0)$. For each i we may identify M_i with $\Sigma \bigoplus_{j=0}^{i} R^{k_j} / \Sigma_{j=1}^{i-1} R\mathbf{v}_j$ where $\mathbf{v}_j$ may be regarded as a vector in $R \oplus \cdots \oplus R^{k_j}$ and for each i, $1 \leq i \leq r$,

$$(*) \qquad \mathbf{v}_i = \mathbf{w}_i \oplus (x_1, \cdots, x_{k_i})$$

and each $\mathbf{w}_i$ satisfies

$$(**) \qquad \sum_{j=1}^{k_i} x_j \mathbf{u}_{ji} + x_{k_i+1} \mathbf{w}_i + \sum_{j=1}^{i-1} z_{ij} \mathbf{v}_j = 0$$

for suitable choices of the vectors $\mathbf{u}_{ji}$ and elements $z_{ij} \in R$. (Thus, the image of $(\mathbf{u}_{1i}, \cdots, \mathbf{u}_{k_i,i}, \mathbf{w}_i)$ modulo $R\mathbf{v}_1 + \cdots + R\mathbf{v}_{i-1}$, i.e. in M_i, is a relation of type k_i.) The failure of condition (2) of Theorem 1.1 for (M_r, a_r) is then expressed by the existence of vectors $\mathbf{t}_1, \cdots, \mathbf{t}_n$ and elements $y_1, \cdots, y_r$ such that

$$(***) \qquad (1, 0, \cdots, 0) + \sum_{j=1}^{n} x_j \mathbf{t}_j + \sum_{j=1}^{r} y_j \mathbf{v}_j = 0.$$

Now let us forget, for the moment, the specific local ring (R, P), but let us remember only the integers n, r and the r-tuple $\mathbf{k} = (k_1, \cdots, k_r)$. (Of course, r can be recovered from $\mathbf{k}$.) Thus, $0 \leq k_i < n$, $1 \leq i \leq r$, and, as before, we set $k_0 = 1$ and make the usual convention for identifying vectors of different lengths. We introduce indeterminates (over the integers) as follows:

$X_1, \cdots, X_n$ are indeterminates.

$\mathbf{W}_i$ is a vector of indeterminates of length $k_0 + \cdots + k_{i-1}$, $1 \leq i \leq r$.

$\mathbf{V}_i$ is a vector of indeterminates of length $k_0 + \cdots + k_i$, $1 \leq i \leq r$.

$\mathbf{U}_{ji}$, $1 \leq j \leq k_i$, $1 \leq i \leq m$, is a vector of indeterminates of length $k_0 + \cdots + k_r$.

Z_{ij}, $1 \leq i \leq r$, $1 \leq j \leq i-1$, are indeterminates.

Y_j, $1 \leq j \leq r$, are indeterminates.

$\mathbf{T}_j$ is a vector of indeterminates of length $k_0 + \cdots + k_r$, $j = 1, \cdots, n$.

Consider the system of polynomial equations $\xi(n, \mathbf{k})$ obtained by setting all the individual entries of the vectors

$(*)$ $\mathbf{V}_i - (\mathbf{W}_i \oplus (X_1, \cdots, X_{k_i}))$, $1 \leq i \leq r$,

$(**)$ $\Sigma_{j=1}^{k_i} X_j \mathbf{U}_{ji} + X_{k_i+1} \mathbf{W}_i + \Sigma_{j=1}^{i-1} Z_{ij} \mathbf{V}_j$, $1 \leq i \leq r$,

$(***)$ $(1, 0, \cdots, 0) + \Sigma_{j=1}^{n} X_j \mathbf{T}_j + \Sigma_{j=1}^{r} Y_j \mathbf{V}_j$,

equal to 0. Then we may assert the following: *Condition* (2) *of Theorem* 4.1 *fails for some rth modification of* $(R, 1)$ *of type* $\mathbf{k}$ *with respect to the s.o.p.* $\mathbf{x}$ *if and only if there is a solution of* $\xi(n, \mathbf{k})$ *in* R *in which* $X_i = x_i$, $1 \leq i \leq n$.

We restate slightly more formally the conclusion of this analysis:

Proposition 4.2. *Let n, r be positive integers and let $\mathbf{k} = (k_1, \cdots, k_r)$ be an r-tuple of integers such that $0 \le k_i < n$ for each i. Then there are positive integers q, h depending (only) on n, $\mathbf{k}$, and a system of h polynomial equations in $n + q$ variables $X_1, \cdots, X_n$ and $Y_1, \cdots, Y_q$ over the integers $\mathbf{Z}$,*

$$\xi(n, \mathbf{k}) \qquad \begin{aligned} F_1(X_1, \cdots, X_n, Y_1, \cdots, Y_q) &= 0, \\ &\cdots \\ F_h(X_1, \cdots, X_n, Y_1, \cdots, Y_q) &= 0 \end{aligned}$$

(where $F_1, \cdots, F_h \in \mathbf{Z}[X_1, \cdots, X_n, Y_1, \cdots, Y_q]$) such that, for every local ring R of dimension n and every s.o.p. $x_1, \cdots, x_n$ for R, condition (2) of Theorem 4.1 fails for some rth modification of $(R, 1)$ of type $\mathbf{k}$ with respect to the s.o.p. $x_1, \cdots, x_n$ if and only if $\xi(n, \mathbf{k})$ has a solution in R in which $X_i = x_i$, $1 \le i \le n$.

We want to emphasize here that $\xi(n, \mathbf{k})$ does not depend in any way on R or $x_1, \cdots, x_n$; only on the numerical parameters n, $(k_1, \cdots, k_r)$. (Note that r is recoverable from $\mathbf{k}$.)

In the sequel (§5) we shall only need the fact that there exist equations $\xi(n, \mathbf{k})$ with the above property; we shall not need to know the precise form.

In the rest of this section, we shall not need to talk about these equations at all. In proving the existence of big Cohen-Macaulay modules in characteristic $p > 0$ we work with condition (2) of Theorem 4.1 directly, not equations.

It will be convenient to call a modification (M, a) of $(R, 1)$ *bad* if $a \in (x_1, \cdots, x_n)M$.

We can now proceed with the proof of the existence of big Cohen-Macaulay modules in characteristic $p > 0$. Explicitly, we shall show:

Theorem 4.3. *Let (R, P) be a local ring of positive prime characteristic p, and let $\mathbf{x} = x_1, \cdots, x_n$ be any s.o.p. Then there exists an $\mathbf{x}$-regular R-module M.*

Proof. We first reduce to the case where R is a module-finite, separable local domain extension of the formal power series ring $K[[x_1, \cdots, x_n]]$. (In this case $\mathbf{x}$ will be an amiable s.o.p. for R, and we then prove a key lemma to handle the amiable case. See the paragraph preceding Lemma 4.4.)

First note that we are free to replace R by R', where R' is a local ring of characteristic p such that under a homomorphism $R \to R'$, the image of $\mathbf{x}$ is an s.o.p. for R'. For if M is an $\mathbf{x}$-regular R'-module, it will also be an $\mathbf{x}$-regular R-module.

We first replace R by its completion. We then enlarge the residue class field to a perfect field and complete again. Fourth, we divide out by a prime of coheight n. Thus, we may assume that R is a complete local domain with a perfect residue class field K. Then R contains a copy of K, and R will be module-finite over a formal power series ring $K[[x_1, \cdots, x_n]] \subset R$, by the analytic independence of an s.o.p. [ZS, pp. 292–293]. The corresponding extension of fraction fields may be inseparable. However, let $y_i = x_i^{1/p^e}$. Since K is perfect, $K[[y_1, \cdots, y_n]]$ contains p^e roots of all elements of

$K[[x_1, \cdots, x_n]]$, and for suitably large e, $R' = R[y_1, \cdots, y_n]$ is separable and module-finite over $K[[y_1, \cdots, y_n]]$. If we can construct a y-regular module M over R', it is easy to see that M is x-regular over R' $(x_i = y_i^{p^e})$ and hence x-regular over R.

Hence, it will suffice to show that if R is a module-finite domain extension of $K[[x_1, \cdots, x_n]]$, a formal power series ring, and the corresponding extension of fraction fields is separable, then there exists an x-regular R-module.

We say that an s.o.p. x for (R, P) is *amiable* if there is an element $c \in R$, not nilpotent, such that, for all k, $0 \le k < n$, and for all positive integers t,

$$c((x_1^t, \cdots, x_k^t)R\colon x_{k+1}^t R) \subset (x_1^t, \cdots, x_k^t)R.$$

Lemma 4.4. *Let (R_0, P_0) be an integrally closed Cohen-Macaulay local domain,* x *any s.o.p., and let R be a module-finite local extension domain whose fraction field is separable over the fraction field of R_0. Then* x *is an amiable s.o.p. for R.*

Proof. It follows easily from the separability and the theorem on the primitive element that there is a $\theta \in R$ such that $R_0[\theta]$ has the same fraction field as R. (First choose θ in the field: then multiply it by a suitable element of R_0.) Since R_0 is integrally closed, the monic irreducible polynomial f of θ over the fraction field of R_0 has coefficients in R_0, and $R_0[\theta] \cong R[Y]/f(Y)$, where Y is an indeterminate. $R_0[\theta]$ is local (since R is) and is Cohen-Macaulay: for R_0 is Cohen-Macaulay, hence so is $R_0[Y]$, and $f(Y)$ is a non-zerodivisor in $R[Y]$. Clearly, x is an s.o.p. for $R_0[\theta]$ and R as well as R_0.

Now, since R is module-finite over $R_0[\theta]$ and has the same fraction field we can choose $c \in R - \{0\}$ such that $cR \subset R_0[\theta]$. Let $s \in (x_1^t, \cdots, x_k^t)R\colon x_{k+1}^t R$ be given, so that $sx_{k+1}^t = \Sigma_{i=1}^k s_i x_i^t$. We need only show that $cs \in (x_1^t, \cdots, x_k^t)R$. But $(cs)x_{k+1}^t = \Sigma_{i=1}^k (cs_i)x_i^t$ and $cs, cs_1, \cdots, cs_k \in R_0[\theta]$. Since $R_0[\theta]$ is Cohen-Macaulay and x is an s.o.p., $cs \in (x_1^t, \cdots, x_k^t)R_0[\theta] \subset (x_1^t, \cdots, x_k^t)R$. Q.E.D.

Applying this result with $R_0 = K[[x_1, \cdots, x_n]]$, we see that to complete the proof of Theorem 4.3 it suffices to prove one crucial fact:

Lemma 4.5. *Let (R, P) be a local ring of positive prime characteristic p and let* x *be an amiable s.o.p. Then there exists an* x*-regular R-module M.*

Proof. Assuming the contrary, there will exist (by Theroem 4.1) an integer r and a bad sequence of modifications

$$(*) \qquad (R, 1) = (M_0, a_0) \longrightarrow \cdots \longrightarrow (M_i, a_i) \longrightarrow \cdots \longrightarrow (M_r, a_r)$$

such that $a_r \in \mathrm{x}M_r$. We shall work with this sequence and obtain a contradiction. Choose $c \in R$ as in the definition of amiable s.o.p. Since c is not nilpotent, $c^r \neq 0$, and we can choose e so large that $c^r \notin (x_1^{p^e}, \cdots, x_n^{p^e})R$ (since $\bigcap_e (x_1^{p^e}, \cdots, x_n^{p^e})R \subset \bigcap_e P^{p^e} R = 0$).

Now, let ${}^eR$ denote R regarded as an algebra over itself via the eth iteration of the Frobenius $s \mapsto s^{p^e}$ and let F be the functor from R-modules to R-modules which assigns to E the module $E \otimes_R {}^eR$ with the R-module structure $r(e \otimes s) = e \otimes (rs)$, where rs is computed regarding s in R, not ${}^eR$. (The same functor is considered in [PS].) We write E' for $F(E)$. F is right exact, takes R to R, but changes the entries of the matrix of a map of free modules by raising them to the p^eth power. Note that $E \to E'$ given by $d \to d \otimes 1 = d'$ is not R-linear: rather $(sd)' = s^{p^e}(d')$. $R \to R' = R$ is the map $s \mapsto s^{p^e}$.

If we apply F to the sequence (*) we get a sequence

$$(R, 1) = (M_0', a_0') \to (M_1', a_1') \to \cdots \to (M_r', a_r')$$

(for $(R', 1') = (R, 1)$), but now each (M_{i+1}', a_{i+1}') is a modification of (M_i', a_i') with respect to the s.o.p. $x_1^{p^e}, \cdots, x_n^{p^e}$ (since F is right exact and $E \to E'$ is linear relative to the eth Frobenius). Moreover, $a_r \in (x_1, \cdots, x_n)M_r$ implies $a_r' \in (x_1^{p^e}, \cdots, x_n^{p^e})M'$. We shall now obtain a contradiction by proving that there exists a commutative diagram

$$\begin{array}{ccccccc}
(M_0', a_0') & \to & (M_1', a_1') & \to & \cdots & \to & (M_r', a_r') \\
\phi_0 \downarrow & & \phi_1 \downarrow & & & & \phi_r \downarrow \\
(R, 1) & \xrightarrow{c} & (R, c) & \xrightarrow{c} & \cdots & \xrightarrow{c} & (R, c^r)
\end{array}$$

in which $\phi_0 = \mathrm{id}_R$. If we can prove this we have the required contradiction, for then $a_r' \in (x_1^{p^e}, \cdots, x_n^{p^e})M_r'$ implies $c^r = \phi_r(a_r') \in (x_1^{p^e}, \cdots, x_n^{p^e})\phi_r(M_r') \subset (x_1^{p^e}, \cdots, x_n^{p^e})R$, which contradicts our choice of e.

We prove the existence of ϕ_i by induction on i. Thus, we assume that

$$\begin{array}{ccccc}
(M_0', a_0') & \to & \cdots & \to & (M_i', a_i') \\
\phi_0 \downarrow & & & & \phi_i \downarrow \\
(R, 1) & \xrightarrow{c} & \cdots & \xrightarrow{c} & (R, c^i)
\end{array}$$

commutes, $i < r$, and we show that ϕ_{i+1} may be chosen so that

$$\begin{array}{ccc}
(M_i', a_i') & \to & (M_{i+1}, a_{i+1}') \\
\phi_i \downarrow & & \downarrow \phi_{i+1} \\
(R, c^i) & \xrightarrow{c} & (R, c^{i+1})
\end{array}$$

commutes.

For a certain integer k, $0 \leq k < n$, we will have

$$(**) \qquad \sum_{j=1}^{k+1} m_j x_j^{p^e} = 0$$

where the $m_j \in M_i'$, and

$$M'_{i+1} = (M'_i \oplus R^k)/R\mathrm{v}$$

where $\mathrm{v} = m_{k+1} \oplus (x_1^{p^e}, \cdots, x_k^{p^e})$. To construct ϕ_{i+1} it is only necessary to give a map $\sigma\colon R^k \to R$ such that $c\phi_i \oplus \sigma$ kills v, and we can choose such a o provided $c\phi_i(m_{k+1}) \in (x_1^{p^e}, \cdots, x_x^{p^e})R$. By virtue of the relation (**) above,

$$x_{k+1}^{p^e}\, \phi_i(m_{k+1}) \in (x_1^{p^e}, \cdots, x_k^{p^e})R$$

i.e. $\phi_i(m_{k+1}) \in (x_1^{p^e}, \cdots, x_k^{p^e})R : x_{k+1}^{p^e}R$ and $c\phi_i(m_{k+1}) \in (x_1^{p^e}, \cdots, x_k^{p^e})R$ then follows from the role of c in the definition of the amiability of x. Q.E.D. for Lemma 4.5 and Theorem 4.3.

http://dx.doi.org/10.1090/cbms/024/06

5. Henselian Rings, M. Artin's Approximation Theorem, and Big Cohen-Macaulay Modules over Fields of Characteristic 0

In this section we want to conclude the proof of the following result:

Theorem 5.1. *Let R be a local ring such that R_{red} contains a field, and let* $\mathbf{x} = x_1, \cdots, x_n$ *be an s.o.p. for R. Then there exists an* $\mathbf{x}$*-regular R-module M.*

Since the images of $x_1, \cdots, x_n$ are again an s.o.p. in R_{red} it suffices to consider the case where R contains a field, and we have already proved the result (§4) when R contains a field of characteristic $p > 0$. Thus, we need only prove the result when R contains a field of characteristic 0.

We shall accomplish this by using quite a general result, Theorem 5.2 below, which allows the reduction of many problems about local rings R containing a field of characteristic 0 to the case where R contains a field of characteristic $p > 0$.

Suppose R contains a field of characteristic 0, $\dim R = n$, $x_1, \cdots, x_n$ is an s.o.p., and $R, x_1, \cdots, x_n$ is a counterexample to Theorem 5.1. By Theorem 4.1 there exists an integer $r \geq 1$ and integers $k_1, \cdots, k_r$, $0 \leq k_i < n$, $1 \leq i \leq r$, such that an rth modification of $(R, 1)$ of type $(k_1, \cdots, k_r)$ is bad. By Proposition 4.2, this means that the system of equations $\xi(n, \mathbf{k})$ has a solution in R with $X_i = x_i$, $1 \leq i \leq n$. The following general result allows us to obtain a contradiction at once:

Theorem 5.2. *Let ξ be a system of polynomial equations in $n + q$ variables $X_1, \cdots, X_n, Y_1, \cdots, Y_q$ over $\mathbf{Z}$, say*

$$F_1(X_1, \cdots, X_n, Y_1, \cdots, Y_q) = 0,$$

$$\cdots$$

$$F_h(X_1, \cdots, X_n, Y_1, \cdots, Y_q) = 0.$$

Suppose that ξ has a solution in a local ring R which contains a field of characteristic 0 such that $\dim R = n$ *and the values $x_1, \cdots, x_n$ for $X_1, \cdots, X_n$ is an s.o.p. for R.*

Then there exists a local ring S containing a field of characteristic $p > 0$ such that $\dim S = n$ *and there is a solution of ξ in S such that the values $x_1', \cdots, x_n'$ of $X_1, \cdots, X_n$ is an s.o.p. for S.*

(In fact S may be chosen to be of the form T_Q, where T is a domain of finite type over a finite field F and Q is a maximal ideal of T such that $T/Q \cong F$.)

We shall defer the proof of Theorem 5.2 for a while. First, let us see how it enables us to complete the proof of Theorem 5.1.

If $\xi(n, \mathbf{k})$ has a solution in a local ring R such that the values of $X_1, \cdots, X_n$ are an s.o.p. (of course $\dim R = n$) and R contains a field of characteristic 0, then by Theorem 5.2 it also has a solution in an n-dimensional local ring S containing a field of characteristic $p > 0$ such that the values of $X_1, \cdots, X_n$ are an s.o.p. $x_1', \cdots, x_n'$ for S. But then, by Proposition 4.2, S has a bad rth modification of type $\mathbf{k}$ and, by Theorem 4.1, S has no $(x_1', \cdots, x_n')$-regular modules. Since we have already proved Theorem 4.1 if S contains a field of characteristic $p > 0$, we have a contradiction. Q.E.D. for Theorem 5.1.

It remains to prove Theorem 5.2. We shall do this in two steps. We first consider the easier and more standard step: suppose that R is a localization at a maximal ideal of an algebra of finite type over a field K of characteristic 0. (Of course, the second, harder step is to reduce the general case to this situation.)

In this first case:

(a) We may enlarge the field to be algebraically closed.

(b) We may assume R is a domain (dividing out by a prime of maximal coheight).

(c) We can assume that the system ξ has a solution in a domain S of finite type over the algebraically closed field K such that the values $x_1, \cdots, x_n$ of the X_i lie in a maximal ideal P of height n such that $P = \mathrm{Rad}(x_1, \cdots, x_n)$. (After (b) we can arrange this in S_P; but then we can arrange it after localizing at finitely many elements of $S - P$.) Moreover, we have that $S/P \cong K$ (since K is algebraically closed), and hence we have $S = K \oplus P$ (over K).

(d) We can choose a finitely generated $\mathbf{Z}$-subalgebra C of K, a finitely generated C-algebra S_C, and a prime ideal P_C of height n such that:

(1) $S_C \cong C \oplus P_C$ (over C).

(2) $S_C \subset S$ and $S = K \otimes_C S_C$.

(3) The solution $x_1, \cdots, x_n, y_1, \cdots, y_q$ for ξ is in S_C.

(4) $P_C = \mathrm{Rad}(x_1, \cdots, x_n)S_C$.

This is just a matter of making sure that S_C contains sufficiently many "relevant" coefficients. For more details, we refer the reader to [H_4].

We note, moreover, that if we replace C by C_c for any $c \in C - \{0\}$ (and each algebra, ideal, etc. by its tensor product over C with C_c), then all these conditions continue to hold.

We now apply the following theorem:

Theorem 5.3 (Generic flatness). *Let C be a Noetherian domain, and let S be a C-algebra of finite type. Let E be an S-module of finite type. Then there is a $c \in C - \{0\}$ such that E_c is free over C_c and, hence, flat over C_c. In particular, there is a $c \in C_c$ such that S_c is flat over C_c.*

We refer the reader to [Mat] for the usual treatment of this theorem and to [HR_1, §8] for a different treatment which produces stronger results.

By virtue of Theorem 5.3 and our remarks above we may also assume

(5) S_C is flat over C.

Now let $\mathfrak{m}$ be any maximal ideal of C. Since C is a finitely generated $\mathbf{Z}$-algebra, $F = C/\mathfrak{m}$ is a finite field. Let us use $'$ for the effect of applying $\otimes_C C/\mathfrak{m}$. ξ has a solution $x_1', \cdots, x_n', y_1', \cdots, y_q'$ in S_C'. Moreover P_C' is such that $S_C' = F \oplus P_C'$ (over $C/\mathfrak{m} = F$), so that P_C' is a maximal ideal of S_C' and $S_C'/P_C' \cong F$. We still have $P_C' = \mathrm{Rad}(x_1', \cdots, x_n')S_C'$. Hence, if $\mathrm{ht}\, P_C' = n$ we can arrange everything we want (we may need to divide out by a prime p of maximal coheight of S_C' to get the domain property, but then $(S_C'/p)_{P_C'/p}$ will satisfy all the requirements (even of the last paragraph) of Theorem 5.2).

To see why $\mathrm{ht}\, P_C' = n$ we recall the following easy result on flatness:

Proposition 5.4. *Let $(A, \mathfrak{A})$, $(B, \mathfrak{B})$ be local rings and $\phi: A \to B$ a homomorphism such that $\phi(\mathfrak{A}) \subset \mathfrak{B}$. Suppose B is flat over A. Then B is faithfully flat over A, ϕ is injective, and* $\dim B = \dim A + \dim B/\mathfrak{A}B$.

For a proof, we refer the reader to [Mat]. Now, returning to our situation, we wish to see why $\mathrm{ht}\, P_C' = n$. Let $Q = \mathfrak{m} + P_C$ ($= \mathfrak{m} \oplus P_C$ as C-modules). Then Q is a maximal ideal of S_C lying over $\mathfrak{m}$ in C, and since S_C is C-flat, $(S_C)_Q$ is $C_\mathfrak{m}$-flat. By Proposition 5.4 above, we then have

$$(*) \qquad \dim (S_C)_Q = \dim A_\mathfrak{m} + \dim (S_C)_Q/\mathfrak{m}(S_C)_Q.$$

Now $(S_C)_Q/\mathfrak{m}(S_C)_Q \cong (S_C')_{P_C'}$ so that

$$\mathrm{ht}\ P_C' = \dim (S_C)_Q/\mathfrak{m}(S_C)_Q = \dim (S_C)_Q - \dim A_\mathfrak{m},$$

by $(*)$ above. Since S_C is a domain of finite type as a $\mathbf{Z}$-algebra and P_C is a prime ideal, we have

$$\dim (S_C)_Q = \mathrm{ht}\ P_C(S_C)_Q + \dim (S_C)_Q/P_C S_Q = \mathrm{ht}\ P_C + \dim A_\mathfrak{m} = n + \dim A_\mathfrak{m}$$

and $\mathrm{ht}\ P_C' = \dim (S_C)_Q - \dim A_\mathfrak{m} = n$, just as we wanted. Q.E.D. for Theorem 5.2 in the case R is the localization at a maximal ideal of an algebra of finite type over a field of characteristic 0.

Before we give the second part of Theorem 5.2 we shall digress and discuss Henselian rings, Henselization, and M. Artin's approximation theorem, which are essential tools in the sequel. We refer the reader to [N] and [Ray] for proofs.

A *quasilocal* ring (R, P) (i.e. a commutative ring R having a unique maximal ideal P) is called *Henselian* if for each monic polynomial $f \in R[x]$ in one variable over R and each factorization $\bar{f} = g^*h^*$, where $\bar{\ }$ denotes reduction modulo P or $PR[x]$, g^*, h^* are monic polynomials in $(R/P)[x]$, and g^*, h^* generate the unit ideal in $(R/P)[x]$, there are monic polynomials $g, h \in R[x]$ such that $f = gh$ and $\bar{g} = g^*$, $\bar{h} = h^*$. Of course, a homomorphic image of a Henselian ring is Henselian, and a well-known theorem, Hensel's lemma, asserts that complete local rings are Henselian.

There are many interesting characterizations. A normal (i.e. integrally closed in its fraction field) quasilocal domain (R, P) is Henselian if and only if for each integral extension domain S of R, there is a *unique* prime of S lying over P.

Another nice characterization comes out of the implicit function theorem for Henselian rings:

Theorem 5.5. *Let (R, P) be a Henselian quasilocal ring and let*

$$F_1(X_1, \cdots, X_n) = 0,$$
$$\cdots$$
$$F_n(X_1, \cdots, X_n) = 0$$

be n polynomial equations in n unknowns over R. Let $^{-}$ denote reduction modulo P and let $K = R/P$. Suppose that the system $\bar{F}_i(X_1, \cdots, X_n) = 0$, $1 \leq i \leq n$, has a solution $(\lambda_1, \cdots, \lambda_n)$ in K such that

$$\det \left(\frac{\partial \bar{F}_i}{\partial X_j} \right) \Bigg|_{(\lambda_1, \cdots, \lambda_n)} \neq 0.$$

Then the system $F_i(X_1, \cdots, X_n) = 0$, $1 \leq i \leq n$, has a solution $(r_1, \cdots, r_n)$ in R such that $(\bar{r}_1, \cdots, \bar{r}_n) = (\lambda_1, \cdots, \lambda_n)$.

In fact, the conclusion of Theorem 5.5, even for the case $n = 1$, implies that (R, P) is Henselian, so that the Henselian rings are precisely those for which Theorem 5.5 holds.

Every quasilocal ring (R, P) has a *Henselization* (R^h, P^h) or, better, α: $(R, P) \to (R^h, P^h)$, where R^h is Henselian, which is characterized up to *canonical* R-isomorphism by the following universal property:

If ϕ: $(R, P) \to (S, Q)$ where S is Henselian then there is a unique ψ: $(R^h, P^h) \to (S, Q)$ such that the diagram

$$\begin{tikzcd} (R^h, P^h) \arrow[dr, "\psi"] & \\ (R, P) \arrow[u, "\alpha"] \arrow[r, "\phi"'] & (S, Q) \end{tikzcd}$$

commutes. (If R is a normal quasilocal domain let L be a separable algebraic closure of the fraction field L_0 of R, let T be the integral closure of R in L, let Q be a maximal ideal of T, let $G = \mathrm{Gal}(L/L_0)$, the Galois group, let $H = \{g \in G: g(Q) = Q\}$, let $S = \{t \in T: h(t) = t$ for all $h \in H\}$, and let $Q' = Q \cap S$. Then $(S_{Q'}, Q'S_{Q'})$ is a Henselization of (R, P). See [N]. If (R, P) is arbitrary, write $R = R^*/I$, where R^* is a normal quasilocal domain. Then R^{*h}/IR^{*h} is a Henselization of R.)

Here are some key points about the Henselization of a quasi-local ring (R, P) (again, we refer the reader to [N], [Ray] for proofs).

(1) $R/P \to R^h/P^h$ is an isomorphism, and $P^h = PR^h$. Hence, for every t, $(P^h)^t = P^tR^h$.

(2) R^h is a directed union of rings of the form $R[\theta]_{P+(\theta)}$ where θ satisfies a monic polynomial $f(x)$ over R such that the constant term is in P but the coefficient of x is not. Hence, R^h is faithfully flat over R, and is a directed union of localizations of module-finite extensions.

(3) If R is Noetherian so is R^h and $\hat{R} \cong \widehat{R^h}$. There are canonical maps

$$\begin{tikzcd} & & \hat{R} \arrow[d, "\cong"] \\ R \arrow[r] & R^h \arrow[ur] \arrow[dr] & \\ & & \widehat{R^h} \end{tikzcd}$$

such that the diagram commutes.

Now, for many purposes it would be useful to have a class of local rings R with the following property: $(\mathcal{P})$ If a system of polynomial equations in finitely many variables with coefficients in R has a solution in $\hat{R}$, then it has a solution in R.

From either the definition or the implicit function theorem characterization, it is easy to see that for R to have property $(\mathcal{P})$, R must be Henselian.

However, the condition that R be Henselian is not sufficient. To see this, let K be a field of characteristic $p > 0$ such that $[K: K^p] = \infty$, and let $\theta_1, \cdots, \theta_n, \cdots \in K$ be linearly independent over K^p. Let $B = K[[x]]$ and let A be the subring of B generated by K and $K^p[[x]]$. See [N, p. 206, (E 3.1)]. Then (A, xA) is a DVR, $\hat{A} = B$, and $B^p \subset A$. Since $A \subset A^h \subset B$ and A^h is separable over A, $A^h = A$, i.e. A is Henselian. Let $b = \sum_{i\geq 0} \theta_i x^i$. Let $a = b^p \in A$. Then $Z^p - a = 0$ has a solution in $\hat{A} = B$, namely $Z = b$, but not in the Henselian ring A. (Thanks go to Andy Magid for correcting this example.)

Nonetheless, M. Artin has proved some beautiful theorems which show that some good Henselian rings do have property $(\mathcal{P})$. The result we need here is the main theorem of [A]:

Theorem 5.6 (Artin approximation). *Let R be the Henselization of a local ring essentially of finite type over a field or over an excellent discrete valuation ring. Let ξ be a system of polynomial equations with coefficients in R in n indeterminates $X_1, \cdots, X_n$. Let I be a proper ideal of R (e.g. the maximal ideal P) and let $\hat{R}^I$ be the I-adic completion of R. Suppose that ξ has a solution $(u_1, \cdots, u_n)$ in $\hat{R}^I$. Let a positive integer t be given. Then ξ has a solution $(r_1, \cdots, r_n)$ in R such that $r_i \equiv u_i (\text{modulo } I^t\hat{R}^I)$, $1 \leq i \leq n$.*

We refer the reader not familiar with excellent rings to [Mat]. We only remark that

(a) complete local rings are excellent, (b) algebras essentially of finite type over an excellent ring are excellent, and (c) $\mathbf{Z}$, the integers, is excellent.

Remarks. It is not hard to reduce to the case $I = P$, and this is the only case we need. Moreover, the congruence conditions can be reformulated as extra equations, so that Theorem 5.6 really does not assert more than that R has property $(\mathcal{P})$. It is even possible to reduce to the case where R is the Henselization of the localization of $V[y_1, \cdots, y_m]$ (V a discrete valuation ring, $y_1, \cdots, y_m$ indeterminates) at the ideal generated by the maximal ideal of V and $y_1, \cdots, y_m$. For our present purpose we only need the case where R is the Henselization of the localization of $K[y_1, \cdots, y_m]$, K a field of characteristic 0, at the maximal ideal $(y_1, \cdots, y_m)$.

The following lemma is clearly all we need to complete the proof of Theorem 5.2 (and, hence, of Theorem 5.1).

Lemma 5.7. *Let ξ be a system of polynomial equations over $\mathbf{Z}$ in $n+q$ variables $X_1, \cdots, X_n, Y_1, \cdots, Y_q$, say*

$$F_1(X, Y) = 0,$$
$$\cdots$$
$$F_h(X, Y) = 0.$$

Suppose that ξ has a solution in a local ring R which contains a field of characteristic 0 such that $\dim R = n$ and the values $x_1, \cdots, x_n$ of $X_1, \cdots, X_n$ are an s.o.p. for R. Then ξ also has a solution in a local ring R' which is the localization of an algebra of finite type over a field of characteristic 0 at a maximal ideal such that $\dim R' = n$ and the values $x_1', \cdots, x_n'$ for $X_1, \cdots, X_n$ are an s.o.p. for R'.

Proof. Let $x_1, \cdots, x_n, y_1, \cdots, y_q$ be a solution for ξ in an n-dimensional local ring R containing the rationals such that $x_1, \cdots, x_n$ is an s.o.p. for R. If $g: (R, P) \to (R^*, P^*)$ is a homomorphism which takes $x_1, \cdots, x_n$ to an s.o.p. $g(x_1), \cdots, g(x_n)$ for R^*, then $g(x_1), \cdots, g(x_n), g(y_1), \cdots, g(y_q)$ is a solution of ξ in R^* and we may consider R^* instead of R. Thus, we may complete R and then divide out by a prime p such that ht $R/p = n$. In this way we reduce to the case where R is a complete local domain. Then there is a field $L \cong R/P$ contained in R and R is a module-finite extension domain of $L[[x_1, \cdots, x_n]]$, where $x_1, \cdots, x_n$ are analytically independent over L. See [ZS, pp. 292–293].

Let $S = L[x_1, \cdots, x_n]$, let $Q = (x_1, \cdots, x_n)S$, and let $A = S_Q$. Thus $\hat{A} = L[[x_1, \cdots, x_n]]$.

For each y_j there is an integer d_j and a monic polynomial $Y_j^{d_j} + z_{j,1}Y_j^{d_j-1} + \cdots + z_{j,d_j} = 0$ having y_j as a root, where the $z_{ij} \in \hat{A}$. Introduce new indeterminates Z_{ij} and let

$$G_j(Y, Z) = Y_j^{d_j} + Z_{j,1}Y_j^{d_j-1} + \cdots + Z_{j,d_j}, \quad 1 \le j \le q.$$

Let Ω be the field $L(x_1, \cdots, x_n)$. The system of equations, in the variables Y, Z,

$$F_i(x, Y) = 0, \quad 1 \leq i \leq h,$$
$$G_j(Y, Z) = 0, \quad 1 \leq j \leq q$$

(which results from putting $X_t = x_t$, $1 \leq t \leq n$, in each F_i), has coefficients in Ω.

Let $B = \Omega[Z]$, a polynomial ring, and let $C = B[Y]/(F_i(x, Y), G_j(Y, Z))$. Then C is integral over (the image of) B, so a prime q of B lies under a prime of C if and only if $q \supset (H_1(Z), \cdots, H_m(Z))$, where the H_i generate the kernel of the homomorphism $B \longrightarrow C$. (This is just the lying over theorem.) By clearing denominators, we may assume without loss of generality that $H_1, \cdots, H_m \in A[Z]$.

Let F be any algebraically closed field containing Ω, and let u_{ij} (same indexing as the Z_{ij}) be elements of F. Then the sytsem

$$(\#) \qquad F_i(x, Y) = 0, \quad G_j(Y, u) = 0$$

has a solution for the Y's in F if and only if $H_t(u) = 0$, $1 \leq t \leq m$. For the kernel q of the map $B \longrightarrow F$ consisting of evaluation at (u) lies under a prime of C if and only if the equations (#) are consistent (i.e. do not generate the unit ideal of $F[Z]$, and this is equivalent, by Hilbert's Nullstellensatz, to their having a solution in F). But this is also equivalent to the condition $q \supset (H_1(Z), \cdots, H_m(Z))$, i.e. each $H_t(Z)$ vanishes at (u), as required.

Now, if we put $u_{ij} = z_{ij}$ then (#) has the solution $Y = y$ in $\hat{A}$ (hence, in the algebraic closure of the fraction field of $\hat{A}$), and so $H_t(z) = 0$, $1 \leq t \leq m$, and the H_i have coefficients in $A \subset A^h$, while the $z_{ij} \in \hat{A}$. By M. Artin's approximation theorem there are elements u_{ij} in A^h such that $H_t(u) = 0$, $1 \leq t \leq m$. Let F be the algebraic closure of the fraction field of A^h. Then there are elements y_j', $1 \leq j \leq q$, of F such that

$$F_i(x, y') = 0, \quad 1 \leq i \leq h,$$
$$G_j(y', u) = 0, \quad 1 \leq j \leq q,$$

by our choice of the H's. Since the u's $\in A^h$, each y_j' is integral over A^h. Now let $R^* = A^h[y_1', \cdots, y_q']$. Then R^* is a module-finite domain extension of A^h, R^* is local (since A^h is Henselian), $x_1, \cdots, x_n$ is an s.o.p., and $x_1, \cdots, x_n, y_1', \cdots, y_n'$ is a solution of ξ. But A^h is a directed union of localizations at maximal ideals of module-finite extensions of A. Hence, we can choose a localization R' of a module-finite extension of A at a maximal ideal so that it contains $y_1', \cdots, y_q'$. Then $\dim R' = n$, $x_1, \cdots, x_n$ is an s.o.p., and $x_1, \cdots, x_n, y_1', \cdots, y_q'$ is a solution of ξ in R'. R' satisfies all our requirements. Q.E.D. for Lemma 5.7, Theorem 5.3, and Theorem 5.1.

Remark. Of course, the existence of big Cohen-Macaulay modules over an arbitrary local ring is open. However, for suitably chosen s.o.p.'s the idea of the proof of Lemma 5.7 allows a reduction to the case of local rings of the form R_P, where R is a domain of finite type over a complete DVR and P is a maximal ideal.

http://dx.doi.org/10.1090/cbms/024/07

6. Depth-Sensitivity Theorems and Exactness Criteria

In their recent papers $[BE_1]$ and $[BE_2]$ Buchsbaum and Eisenbud have considered, in particular, a complex $\mathcal{K}$,

$$0 \to F_n \to \cdots \to F_0 \to 0,$$

of free modules of finite type over a Noetherian ring R and examined under what conditions it will be acyclic (i.e. exact, except possbily at F_0), so that it will provide a free resolution of its *augmentation*

$$M = \operatorname{Coker}(F_1 \to F_0).$$

Their results seem to generalize, at least in part, to the non-Noetherian case $[EN_2]$. In $[BE_1]$ they give necessary and sufficient conditions for $\mathcal{K}$ to be acyclic which have two types: numerical conditions on certain integer parameters associated with $\mathcal{K}$, and requirements which take the form that the depths of certain ideals associated with $\mathcal{K}$ be sufficiently large. In fact, they consider not only $\mathcal{K}$ itself but also the complexes $\mathcal{K} \otimes E$. In this generality their result becomes, in a certain sense, a generalization of the depth-sensitivity of the Koszul complex. (See Proposition 1.2 of §1 and also the related Proposition 3.3 in §3.) We note that some related non-Noetherian generalizations (including Proposition 3.3) may be found in $[H_5]$.

In $[BE_2]$ they prove some very interesting and subtle relationships among the subdeterminants of the matrices of the maps in an acyclic free complex such as $\mathcal{K}$ above.

In this section we shall describe some of their results with partial proofs, as well as other depth-sensitivity theorems, and give some corollaries and applications to indicate the usefulness of these ideas.

Before proceeding to these results we want to introduce some new notions.

Let M be a module of finite type over a Noetherian ring R.

Lemma 6.1. *Let V_i or $V_i(M)$ denote the set $\{P \in \operatorname{Spec}(R)\colon \operatorname{pd}_{R_P} M_P \geq i\}$. Then V_i is Zariski-closed. If we let $\mathfrak{A}_i(M) = \{r \in R : \operatorname{pd}_{R_r} M_r < i\}$ then $\mathfrak{A}_i(M)$ is a radical ideal and V_i is the set of primes containing $\mathfrak{A}_i(M)$.*

Proof. In case $i = 0$, $V_0 = \operatorname{Supp} M$ and $\mathfrak{A}_0(M) = \operatorname{Rad} \operatorname{Ann} M$, so that the result is well known and rather trivial.

If $i = 1$, the assertion that V_1 is closed is equivalent to the statement that the set of primes $P \in \operatorname{Spec}(R)$ such that M_P is R_P-free is open. To see why this is true, simply note that if M_P is R_P-free then there is a map $\phi: R^t \to M$ for some t such that ϕ becomes an isomorphism upon applying $\otimes_R R_P$. Then some element $r \in R - P$ kills both $\ker \phi$ and $\operatorname{Coker} \phi$, so that $M \otimes_R R_r$ is free, and M_Q is free for $Q \not\ni r$.

If $i > 1$, consider an exact sequence $0 \to M' \to F \to M \to 0$ where F is free of finite type. For $i > 1$, $V_i(M) = V_{i-1}(M')$, and the result that $V_i(M)$ is closed follows by induction.

Now, $r \in \bigcap\{P: P \in V_i\}$ if and only if for $Q \not\ni r$, $\operatorname{pd}_{R_Q} M_Q < i$. But

$$\operatorname{pd}_{R_r} M_r = \operatorname{Sup}\{\operatorname{pd}_{R_Q} M_Q : Q \not\ni r\}$$

so $r \in \bigcap\{P: P \in V_i\} \Leftrightarrow \operatorname{pd}_{R_r} M_r < i \Leftrightarrow r \in \mathfrak{A}_i(M)$, as required. Q.E.D.

We shall refer to $\mathfrak{A}_i(M)$ as the ith *homological annihilator* of M.

Lemma 6.2. *With R, M as above,* $\operatorname{depth}(\mathfrak{A}_i(M)) \geq i$. *(This includes the possibility $\mathfrak{A}_i(M) = R$.)*

Proof. If $\mathfrak{A}_i(M)$ has depth $< i$, choose a prime $P \supset \mathfrak{A}_i(M)$ such that depth $R_P < i$. Then $i >$ depth $R_P \geq \operatorname{pd} M_P \geq i$, a contradiction. Q.E.D.

Now let $\mathbb{K}$, $0 \to F_n \to \cdots \to F_0 \to 0$, be a complex of free modules of finite type over a Noetherian ring R and suppose that bases have been chosen for each F_i. We shall make some notational conventions for this situation. We shall write b_i for rank F_i and refer to it as the ith Betti number of $\mathbb{K}$. We write M for $\operatorname{Coker}(F_1 \to F_0)$.

We define, recursively,

$$r_n = b_n,$$

$$r_i = b_i - r_{i+1}, \quad i \geq 0.$$

Thus, $r_i = b_i - b_{i+1} + b_{i+2} - \cdots \pm b_n$. We call the r_i the *expected matrix ranks* of $\mathbb{K}$.

If A is an m by m' matrix we write $I_t(A)$ for the ideal generated by the t by t minors of A. (If $t = 0$, $I_0(A) = R$. If $t > \min\{m, m'\}$, $I_t(A) = (0)$.) The following is basically a piece of the main theorem of [BE$_1$].

Proposition 6.3. *Let notation be as above, and suppose that $\mathbb{K}$ is acyclic, i.e. that $\mathbb{K} \to M \to 0$ is simply a finite free resolution of M.*

Then the following statements hold:

(a) $I_{r_i}(A_i) \neq 0$, *while* $I_{r_i+1}(A_i) = 0$. *In other words, the (determinantal) rank of the matrix A_i is r_i.*

(b) depth $I_{r_i}(A_i) \geq 1$. *Hence, for any prime P of R, the determinantal rank of $(A_i)_P$ (the image of A_i under $R \to R_P$) is r_i.*

(c) $\mathfrak{A}_i(M) = \operatorname{Rad}(I_{r_i}(A_i))$.

(d) depth $I_{r_i}(A_i) \geq i$, *for each* $i \geq 1$.

Proof. Let S be the multiplicative system of non-zerodivisors in R and let $T = S^{-1}R$, the total quotient ring of R. Then T has finitely many maximal ideals (corressponding to the maximal associated primes of (0) in R). If Q is one of these, depth $T_Q = (0)$.

Since pd M is finite, $\mathrm{pd}_{T_Q} M_Q$ is finite and $\leq$ depth T_Q. Thus, M_Q is free, and necessarily of rank $r_0 = \Sigma_{i=0}^{r}(-1)^i b_i$ for each Q. But then $S^{-1}M$ must be free over T (it is locally free of constant rank), and, reasoning similarly, $S^{-1}\mathcal{K}$ breaks up into short exact sequences of locally free modules of constant rank which are actually then free.

Let A be a p by q matrix (representing a map $B^p \longrightarrow B^q$) over a *local* ring B. Then Coker A is free of rank t if and only if the $q-t$ by $q-t$ minors of A generate the unit ideal of B and the $q-t+1$ by $q-t+1$ minors vanish. Hence, the same holds if $B = T$ is semilocal. It follows that $S^{-1}I_{r_i}(A_i) = T$ while $S^{-1}I_{r_i+1}(A_i) = 0$. Since S consists of non-zerodivisors we obtain both (a) and (b).

To see why (c) holds, let P by a prime of R. Then

$$\begin{aligned} P \supset \mathfrak{A}_i(M) &\Leftrightarrow \mathrm{pd}_{R_P} M_P \geq i \\ &\Leftrightarrow \ker((A_{i-1})_P) \text{ is } \textit{not} \text{ free} \Leftrightarrow \mathrm{Coker}((A_i)_P) \text{ is } \textit{not} \text{ free} \\ &\Leftrightarrow I_{r_i}(A_i)R_P \neq R_P \text{ (using (b), } r_i = \text{det rank } A_i \\ &\qquad\qquad\qquad \text{regardless of what } P \text{ is)} \\ &\Leftrightarrow P \supset I_{r_i}(A_i) \end{aligned}$$

and so $\mathfrak{A}_i(M) = \mathrm{Rad}\, I_{r_i}(A_i)$.

Once we know this, (d) is immediate from 6.2. Q.E.D.

This result suggests a possible converse, which, in fact, is true. The following is the main result of [BE_1]:

Theorem 6.4 (Buchsbaum-Eisenbud). *Let $\mathcal{K}$ be a finite free complex over a Noetherian ring R, and let E be an R-module of finite type. Let r_i be the ith expected rank, as above. Then $\mathcal{K} \otimes_R E$ is acyclic if and only if the following conditions hold*:

(1) $I_{r_i+1}(A_i)E = 0$, $i \geq 1$.

(2) $\mathrm{depth}(I_{r_i}(A_i), E) \geq i$ *for* $i \geq 1$.

(*If* $IE = E$, *we make the convention that* $\mathrm{depth}(I, E) = +\infty$, *so that* (2) *is satisfied if* $I_{r_i}(A_i)E = E$.)

In the special case $E = R$ we have

Corollary 6.5. $\mathcal{K}$ *is acyclic if and only if, for each* $i \geq 1$, det rank $A_i = r_i$ *and* depth $I_{r_i}(A_i) \geq i$.

Of course we have proved the "only if" part of Corollary 6.5 in 6.3. We shall not give the full proof of 6.4 here, but refer the reader to [BE_1].

We want to point out that the conditions of Corollary 6.5 do give a very concrete way of checking whether a given free complex $\mathcal{K}$ is acyclic, particularly if the base ring R is Cohen-Macaulay. For the numerical conditions on the determinantal ranks are of a rather simple sort, while the condition depth $I_{r_i}(A_i) \geq i$, which may be quite hard to check for an arbitrary R, is much easier in a Cohen-Macaulay R, for then depth $J \geq i$ if and only if ht $J \geq i$ (where ht $J = \min\{\text{ht } P\colon P$ a prime, $P \supset J\}$), and heights are ordinarily much easier to compute than depths.

In fact, a specific application of Corollary 6.5 of this sort is made in [Po] to verify that a conjectured free resolution for a certain determinantal ideal is, in fact, a resolution.

We shall return to this point in §7.

We also remark that Theorem 6.4 for the case $E = R$ brings home in a rather strong way the statement of §1 that the existence of nontrivial modules of finite type and finite projective dimension over a Noetherian ring R is almost entirely due to the existence of R-sequences.

We note the following corollary:

Corollary 6.6. *Let $R \to S$ be a homomorphism of Noetherian rings which takes R-sequences to S-sequences. Let M be an R-module of finite type with a finite free resolution. Then* $\operatorname{Tor}_i^R(M, S) = 0$, $i \geq 1$, *and $M \otimes S$ has finite projective dimension over S.*

Proof. Let $0 \to \mathcal{K} \to M \to 0$ be a free resolution. Then since $\mathcal{K}$ satisfies (1), (2) of 6.5, it is immediate that $\mathcal{K} \otimes S$ does, and hence $\mathcal{K} \otimes S$ is acyclic. But then $\operatorname{Tor}_i(M, S) = 0$, $i \geq 1$, and $\mathcal{K} \otimes S$ is a free resolution of $M \otimes S$. Q.E.D.

Corollary 6.7 (Peskine-Szpiro). *Let R be a Noetherian ring of characteristic $p > 0$ and let M be an R-module of finite type and finite projective dimension. Let S be R regarded as an R-algebra via the Frobenius homomorphism $f^e\colon r \to r^{p^e}$.*

Then if M is an R-module of finite type and finite projective dimension, $M \otimes_R S$ is an S-module of finite projective dimension. Moreover $\operatorname{Tor}_i^R(M, S) = 0$, $i \geq 1$.

Proof. The issue is local on R, so that we may suppose R local and M has a finite free resolution. If $r_1, \cdots, r_k$ is an R-sequence, then $r_1^{p^e}, \cdots, r_k^{p^e}$ is an S-sequence. Hence, Corollary 6.6 applies. Q.E.D.

We now want to look closely at a different special case of Theorem 6.4, the case where $\mathcal{K}$ is a free resolution of a perfect module.

We recall that a module $M \neq 0$ of finite type over a Noetherian ring R is called *perfect* if depth Ann $M = \operatorname{pd}_R M$. In general, depth Ann $M \leq \operatorname{pd}_R M$. If M is perfect and $P \in \operatorname{Spec}(R)$, then there are two possibilities:

(1) $M_P = 0$.

(2) M_P is perfect of the same projective dimension as M.

For if $M_P \neq 0$, i.e. $P \supset$ Ann M, we have, if $I =$ Ann M,

$$\begin{aligned} \text{depth } I = \operatorname{pd}_R M &\geq \operatorname{pd}_{R_P} M_P \\ &\geq \text{depth Ann}_{R_P} M_P = \text{depth } IR_P \geq \text{depth } I \end{aligned}$$

and hence all the inequalities are really equalities, so that $\operatorname{pd}_R M = \operatorname{pd}_{R_P} M_P =$ depth $\operatorname{Ann}_{R_P} M_P$, and M_P is perfect of projective dimension equal to $\operatorname{pd}_R M$.

Hence:

Proposition 6.8. *If R is Noetherian and M is perfect with* $\mathrm{pd}_R M = n$, *then*

$$\mathfrak{A}_n(M) = \mathfrak{A}_{n-1}(M) = \cdots = \mathfrak{A}_1(M) = \mathfrak{A}_0(M) = \mathrm{Rad\ Ann}\ M.$$

(Of course, $\mathfrak{A}_t(M) = R$ for $t > n$.)

As soon as we know this we obtain at once, from Theorem 6.4,

Corollary 6.9. *Let R be a Noetherian ring, M a perfect R-module with* $\mathrm{pd}_R M = n$, *let* $I = \mathrm{Ann}\ M$ *and let E be an R-module of finite type such that $IE \neq E$ (i.e. $M \otimes E \neq 0$). Then* depth (I, E) *is $n - d$, where d is the biggest integer such that* $\mathrm{Tor}_d^R(M, E) \neq 0$.

Proof. One can reduce to the local case, so that M has a finite free resolution $\mathcal{K} \longrightarrow M \longrightarrow 0$.

Then the last t homology groups of $\mathcal{K} \otimes E$ vanish if and only if $\mathcal{K} \otimes E$ is acyclic, where $\mathcal{K}'$ is

$$0 \longrightarrow F_n \longrightarrow \cdots \longrightarrow F_{n-t+1} \longrightarrow F_{n-t},$$

and this occurs if and only if, for the jth ideal associated with $\mathcal{K}'$, call it I_j, depth$(I_j, E) \geq j$, $1 \leq j \leq t$. But all the ideals associated with $\mathcal{K}'$ are among those associated with $\mathcal{K}$, and all these have the same radical as I. Hence, the last t homology groups vanish if and only if depth $(I, E) \geq t$, and the result follows. Q.E.D.

One may easily show that it is even permissible to allow a change of rings $R \longrightarrow S$, and state 6.9 thus:

Corollary 6.10. *Let $R \longrightarrow S$ be a homomorphism of Noetherian rings, let M be a perfect R-module with* $\mathrm{pd}_R M = n$, *let E be an S-module of finite type, and suppose $M \otimes_R E \neq 0$, i.e. $IE \neq E$, where* $I = \mathrm{Ann}\ M$. *Then* depth (IS, E) *is $n - d$, where d is the biggest integer such that* $\mathrm{Tor}_d^R(M, E) \neq 0$.

The argument is essentially the same as in the proof of 6.9.

Moreover, we leave it to the reader to see that if M is not necessarily perfect but still has finite projective dimension we have at least

Proposition 6.11. *Let $R \longrightarrow S$ be a homomorphism of Noetherian rings, let $M \neq 0$ be an R-module of finite type with* $\mathrm{pd}_R M < \infty$, *let* $I = \mathrm{Ann}\ M$, *and let E be an S-module of finite type with $M \otimes_R E \neq 0$. Let d be the biggest integer such that* $\mathrm{Tor}_d^R(M, E) \neq 0$. *Then*

$$\mathrm{depth}\ (IS, M) + d \leq \mathrm{pd}_R M.$$

(Just use 6.4 again.)

If we apply 6.10 to the case where $R = \mathbf{Z}[x_1, \cdots, x_n]$, $M = R(x_1, \cdots, x_n)R$ (so that $\mathcal{K}_\cdot(x_1, \cdots, x_n; R)$ is a projective resolution of M) then we see that 6.10 asserts, in this special case, the depth-sensitivity of the Koszul complex. Since 6.10 is immediate from 6.4, we see that 6.4 is really a highly subtle and sophisticated depth-sensitivity theorem. Even 6.11 is a sort of weak (but quite useful) depth-sensitivity result.

We should also note that 6.11 is really just a special case of Proposition 3.3, which we proved by a very elementary method in §3, so 6.11 generalizes nicely to the non-Noetherian case (and this sort of generalization was something we really wanted, in order to prove that

(existence of big Cohen-Macaulay modules) $\Rightarrow$ (intersection conjecture).

Eagon and Northcott [EN_2] have generalized part of 6.4 to the non-Noetherian case by extremely elementary techniques (no Tor's or Ext's, no exterior algebra), and it seems quite certain that all of these results generalize, although one must be careful to use the right definition of "depth" in the non-Noetherian case.

Moreover 6.10 and 6.11 generalize extremely well. We indicate these generalizations briefly. Let R be any ring, I an ideal, and M an R-module.

The following two conditions are equivalent:

(a) If S is faithfully flat over R and $s_1, \cdots, s_n$ is a sequence of elements in IS such that

$$(s_1, \cdots, s_i)(M \otimes S): s_{i+1}S = (s_1, \cdots, s_i)(M \otimes S), \quad 1 \leq i < n,$$

then $(s_1, \cdots, s_n)(M \otimes S) \neq M \otimes S$.

(b) If $i_1, \cdots, i_n \in I$, then, for some t,

$$H_t(\mathcal{K}_.(i_1, \cdots, i_n; M)) \neq 0.$$

If these equivalent conditions hold we call (I, M) admissible. If (I, M) is admissible, then the following three coincide:

(1) The supremum of lengths of $(M \otimes S)$-sequences in $I \otimes S$, where S is a polynomial ring (in several variables) over R.

(2) The supremum of lengths of $(M \otimes S)$-sequences in $I \otimes S$, where S is faithfully flat over R.

(3) The supremum of integers $n - d$, where $i_1, \cdots, i_n$ is some sequence of elements in I and d is the biggest inetger such that $H_d(\mathcal{K}_.(i_1, \cdots, i_n; M)) \neq 0$.

If R is Noetherian and M of finite type then (I, M) is admissible if and only if $IM \neq M$, and these all give depth(I, M). If R is not Noetherian or M is not of finite type we take any of (1), (2), or (3) as our definition of depth(I, M). (Eagon and Northcott call this "polynomial depth.") It is first investigated in [Bar]. In [H_5] it is denoted $G(I, M)$ (G for grade). The equivalence of these three notions is shown in [H_5]. We now recall two results from [H_5].

Theorem 6.12 (The Tor inequality). *Let $R \to S$ be any ring homomorphism, let M be any R-module, and let $I = \{r \in R: M_r = 0\}$. Let E be any S-module. Suppose that some* $\mathrm{Tor}_i^R(M, E) \neq 0$ *and let d be the biggest integer such that* $\mathrm{Tor}_d^R(M, E) \neq 0$. *Then (IS, E) is admissible, and*

$$\operatorname{depth}(IS, E) + d \leq \operatorname{Tor}\dim^R M.$$

This is, of course, a highly polished form of Propositoin 3.3. It is Theorem 1 of [H_5].

Theorem 6.13. *Let R be a ring and let $M \neq 0$ be an R-module which has a finite resolution by projectives of finite type. Then* $\operatorname{Tor}\dim^R M = \operatorname{pd}_R M$. Suppose *that M is perfect in the sense that* depth $I = \operatorname{pd}_R M$, *where* $I = \{r \in R: M_r = 0\}$. *Let $R \to S$ be a homomorphism and let E be an S-module such that some* $\operatorname{Tor}_i^R(M, E) \neq 0$, *let d be the biggest integer such that* $\operatorname{Tor}_d^R(M, E) \neq 0$. *Then*

$$\text{(\#)} \qquad \operatorname{depth}(IS, E) + d = \operatorname{pd}_R M.$$

We note that (#) fails if M is not perfect for the case $S = E = R$.

The author believes that the result 6.4 can be made to work in the same kind of generality if the correct notion of grade is utilized, but so far no one has written down all the details of a treatment of the most general case.

We next want to return to some more concrete situations to see how 6.12 (or even 6.11) can be applied to a down-to-earth problem like proving that a specific ideal (i.e. with given generators) in a polynomial ring is prime.

We shall proceed in vary modest generality. First, we should observe:

Proposition 6.14. *Let M be a perfect module over a Noetherian ring R and let* $I = \operatorname{Ann} M$. *Let $\mathcal{K}$ be a projective resolution of M. Let* $n = \operatorname{depth} I = \operatorname{pd}_R M$.

Suppose $R \to S$ is a homomorphism of Noetherian rings and depth $IS \geq n$. *Then* depth $IS = n$, *and $M \otimes_R S$ is either 0 (if $IS = S$) or else a perfect S-module with* $\operatorname{pd}_S(M \otimes_R S) = n$. *Moreover, $\mathcal{K} \otimes_R S$ is a projective resolution of $M \otimes_R S$.*

Proof. From 6.12 we have (with $E = S$) that

$$\operatorname{depth} IS + d \leq n = \operatorname{pd}_R M,$$

where d is the biggest integer such that $\operatorname{Tor}_d(M, S) \neq 0$. (We may assume $M \otimes S \neq 0$, i.e. $IS \neq S$.) Since depth $IS \geq n$, $d = n -$ depth $IS = 0$, whence $d = 0$. Thus, depth $IS = n$, and $\operatorname{Tor}_i^R(M, S) = 0$, $i \geq 1$, which implies that $\mathcal{K} \otimes S$ is acyclic and hence provides a projective resolution of $M \otimes S$. If we apply this when $\mathcal{K}$ is a resolution of length n we conclude $\operatorname{pd}_S(M \otimes S) \leq n$. But then, since $\operatorname{Rad} IS = \operatorname{Rad}(\operatorname{Ann}_S M \otimes S)$,

$$n = \operatorname{depth} IS = \operatorname{depth} \operatorname{Ann}_S M \otimes S \leq \operatorname{pd}_S M \otimes S \leq n$$

and it follows that all the inequalities are equalities, so that $M \otimes S$ is perfect over S of projective dimension n.

We shall refer to the phenomenon of this proposition as the "persistence" of "stability" of perfectness: a perfect module remains perfect (with, essentially, the same projective resolution) under a change of rings which satisfies the single nondegeneracy condition that it not decrease the depth of the annihilator.

We have the following result:

Proposition 6.15. *If M is a perfect module over a Noetherian ring R, the associated primes of M all have the same depth,* $\operatorname{pd}_R M$, *and so if R is Cohen-Macaulay they all have the same height.*

If R is Cohen-Macaulay and I is an ideal such that R/I is perfect, then R/I is Cohen-Macaulay.

Proof. Let $P \in \operatorname{Ass}(M)$. Let $I = \operatorname{Ann} M$. Then

$$\begin{aligned} n &= \operatorname{depth} I \leq \operatorname{depth} P \\ &\leq \operatorname{depth} R_P = \operatorname{pd}_{R_P} M_P + \operatorname{depth}_{R_P} M_P \\ &= n + 0 \quad (\operatorname{pd}_{R_P} M_P = n \text{ since } M \text{ is perfect and} \\ &\qquad\qquad P \supset I, \text{ and depth } M_P = 0 \text{ because } P \in \operatorname{Ass}(M)). \end{aligned}$$

Thus, all the inequalities are equalities and depth P = depth $R_P = n$. If R is Cohen-Macaulay, we then have ht P = depth $R_P = n$ as well. This completes the proof of all statements of the first paragraph.

Finally, to prove the assertion of the second paragraph it suffices to consider the case where R is local (we may localize at $P \supset I$ without affecting the issues: the question of whether R/I is Cohen-Macaulay is local on the primes containing I). But then R/I is Cohen-Macaulay because

$$\operatorname{depth}(R/I) = \operatorname{depth} R - \operatorname{pd}(R/I) = \dim R - \operatorname{depth} I$$

(depth $R = \dim R$, since R is Cohen-Macaulay, and $\operatorname{pd}(R/I)$ = depth I, since R/I is perfect). By the first part, all associated primes of I have height n. Hence $\dim R -$ depth $I = \dim R - n = \dim(R/I)$, and $\operatorname{depth}(R/I) = \dim(R/I)$, as required. Q.E.D.

An ideal $I \neq R$ of a Noetherian ring R is called *perfect* if R/I is a perfect R-module, i.e. $\operatorname{pd}_R R/I$ = depth I.

Corollary 6.16. *If I is a perfect ideal of a Noetherian ring R, of depth n, then all associated primes of I have depth n. If R is Cohen-Macaulay then I is unmixed, all associated primes of I have height n, and R/I is again Cohen-Macaulay.*

If $R \longrightarrow S$ is a homomorphism of Noetherian rings depth $IS \geq$ depth I, *and $IS \neq S$, then IS is a perfect ideal of depth n.*

Example 6.17. The ideal $I_t(x_{ij})$ generated by the $t \times t$ minors of an r by s matrix of indeterminates (x_{ij}) over the integers in the ring $R = \mathbf{Z}[x_{ij}]$ is known [HE] to be perfect of depth $(r-t+1)(s-t+1)$ for every t, $1 \leq t \leq \min\{r, s\}$. In special cases a specific minimal free resolution for $R/I_t(x_{ij})$ is known (e.g. $t = r \leq s$: see [EN_1]).

Now let S be any Noetherian ring and (s_{ij}) an r by s matrix over S. There is a unique homomorphism $R \longrightarrow S$ which takes $x_{ij} \longrightarrow s_{ij}$, for each i, j. Then $I_t(x_{ij})S = I_t(s_{ij})$, clearly. Hence, if depth $I_t(s_{ij}) \geq (r-t+1)(s-t+1)$ (which it is in the generic case), then $I_t(s_{ij})$ is perfect of depth $(r-t+1)(s-t+1)$. Moreover, if a resolution for $I_t(x_{ij})$ is known, one has a resolution for $I_t(s_{ij})$ as well.

These ideas can be used to show that ideals $J = (f_1, \cdots, f_m)$ are prime in some cases. One proceeds as follows:

(1) Show that J has a unique minimal prime Q.

(2) Show that J is perfect, so that, if the ring is Cohen-Macaulay, the elements of $R - Q$ are non-zerodivisors modulo J.

(3) Show that $JR_Q = QR_Q$ (usually, one shows that J becomes prime after localization at a single nonzero element).

Example 6.18. Let us apply the above idea in a completely specific instance.

In fact, let us show that if K is a field and x_{ij} are rs indeterminates over K then $I = I_t(x_{ij})$ is prime in $R = K[x_{ij}]$, using the fact that I is perfect.

Let $Y = (y_{ik})$ and $Z = (z_{kj})$ be r by $t-1$ and $t-1$ by s matrices of indeterminates. Let P be the kernel of the map $\phi\colon K[x_{ij}] \to K[y_{ik}, z_{kj}]$ which takes the entries of $X = (x_{ij})$ to those of the product matrix YZ. One sees easily that $P \supset I$. Moreover, if Q is a prime which contains I and L is the fraction field of R/Q, the image (x'_{ij}) of (x_{ij}) in L has rank $< t$, and so factors $(y'_{ik})(z'_{kj})$ over L, where (y'_{ik}) is r by $t-1$ and (z'_{kj}) is $t-1$ by s. By mapping $y_{ik} \to y'_{ik}$, $z_{kj} \to z'_{kj}$ we obtain a commutative diagram:

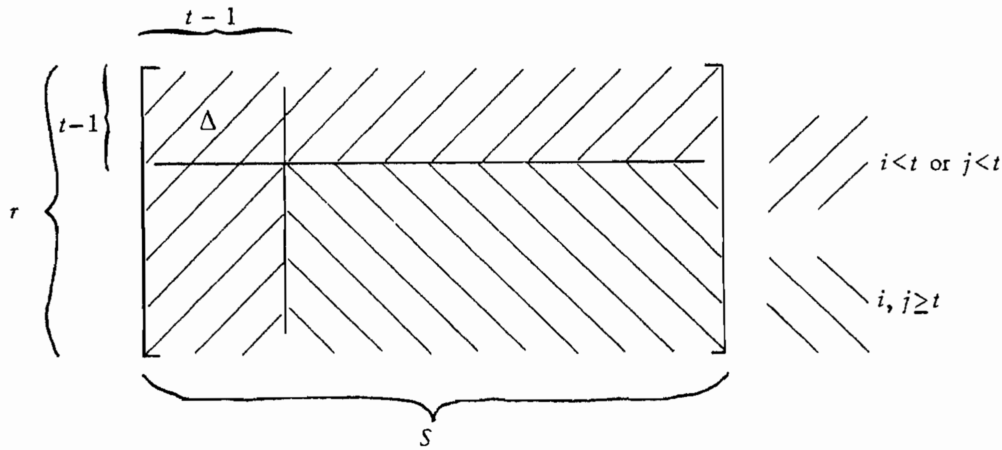
$$\begin{array}{ccc} K[x_{ij}] & \xrightarrow{\phi} & K[y_{ik}, z_{kj}] \\ \downarrow & & \downarrow \\ R/Q & \hookrightarrow & L \end{array}$$

It follows at once that $Q \supset \ker \phi = P$, i.e. if $Q \supset I$, then $Q \supset P$. Thus, $P = \operatorname{Rad} I$, and P is the only minimal prime of I. Consider a $t-1$ by $t-1$ minor Δ of (x_{ij}). Then $\Delta \notin P$, for if $\Delta \in P$, by considerations of symmetry all the $t-1$ by $t-1$ minors of (x_{ij}) must be in P, and then $\operatorname{ht} P = \operatorname{ht} I_t(x_{ij}) = \operatorname{ht} I_{t-1}(x_{ij})$, a contradiction.

Now, since I is perfect and P is the only minimal prime, P is the only associated prime. Hence, Δ is not a zerodivisor modulo I, and $(R/I)_\Delta \supset R/I$. It will suffice to show that R_Δ/IR_Δ is a domain. For convenience, we may suppose that Δ lies in the upper left-hand corner (i.e. is formed as $\det(x_{ij})$, $1 \le i \le t-1$, $1 \le j \le t-1$). Let x_{ij} be such that $i \geq t$ and $j \geq t$. There is a unique t by t minor Δ_{ij} of (x_{ij}) which is formed from Δ and the row and column of x_{ij}. Moreover, the equation $\Delta_{ij} = 0$ can be rewritten $x_{ij} = (1/\Delta)u_{ij}$ where u_{ij} is a polynomial in the variables x_{ij} where $i < t$ or $j < t$. Moreover, if we substitute $x_{ij} = (1/\Delta)u_{ij}$, $i, j \geq t$ in (x_{ij}), we obtain a matrix all of whose t by t minors vanish. Thus,

$$R_\Delta/IR_\Delta \cong K[x_{ij}\colon\ i < t \quad \text{or} \quad j < t][1/\Delta]$$

is a domain, as required. Thus, $I = P$ is prime.



The same technique can be applied in many other examples to show that $I_t(A)$ is prime for a certain matrix A, and the same is true for many ideals of a certain "form" when ideals of that form are known to be perfect in a "generic" case.

http://dx.doi.org/10.1090/cbms/024/08

7. Modules of Projective Dimension 2, Generic Modules of Finite Projective Dimension, and the Buchsbaum-Eisenbud Structure Theorems

We begin with a digression from linear algebra. Let A, B be r by t and t by s matrices over a field K, and suppose

(a) $t = r + s$,

(b) A has rank r,

(c) $AB = 0$.

The r by r minors of A are indexed by the set $T_{(r)}$ of r element subsets of $T = \{1, \cdots, t\}$. The s by s minors of B are indexed by $T_{(s)}$, the set of $s = t - r$ element subsets of T. There is an obvious bijection

$$T_{(r)} \rightleftarrows T_{(s)}$$

induced by taking complements in T. Thus, there is a one-one correspondence between r by r minors of A and s by s minors of B. If $\mu \in T_{(r)}$ let A_μ, B_μ be the minors of A, B respectively corresponding to μ. (Thus, B corresponds, really, to $T - \mu$.) Define

$$\operatorname{sgn}(\mu) = (-1)^{\Sigma},$$

where Σ is the sum of the elements of μ. *Then there is a unique* $c \in K$ such that, for all $\mu \in T_{(r)}$,

$$B_\mu = c \operatorname{sgn}(\mu) A_\mu.$$

(In fact, if the rows of A are regarded as a basis for an r-dimensional subspace $V^r \subset K^t = V$ then the r by s minors of A are Grassmann-Plücker coordinates of V^r under the Plücker embedding

$$\mathcal{G}r_r(V) \to \mathrm{P}^{\binom{t}{r}-1}$$

where $\mathcal{G}r_r(V)$ is the Grassmann variety of r-dimensional subspaces of V and $\mathrm{P}^{\binom{t}{r}-1}$ is projective $(\binom{t}{r} - 1)$-space. Up to multiplication by a nonzero scalar, these coordinates are independent of the choice of basis for V^r. In the nondegenerate case where rank $B = s$ (otherwise all the s by s minors vanish), the s by s minors of B give the Grassmann-Plücker coordinates for the orthogonal complement W^s of V^r in the dual $V^* = \operatorname{Hom}(V, K)$. The existence of c simply exhibits in a pleasant way the isomorphism $\mathcal{G}r_r(V) \cong \mathcal{G}r_s(V^*)$ induced by taking orthogonal complements.)

If we assume that B is t by s^* where s^* is arbitrary and let $s = t - r$, then from our original statement we deduce at once:

Let A be r by t, $r \le t$, let B be t by s^*, and let $s = t - r$. Suppose rank $A = r$ *and suppose $AB = 0$. Then for any s columns of B there is a unique c such that if B' is the submatrix of B formed by these s columns then, for each $\mu \in T_{(r)}$, $B'_\mu = c \operatorname{sgn}(\mu) A_\mu$.*

This result extends to the situation in which one has a long exact sequence of vector spaces in a pleasant way. In fact, suppose we have a complex

$$0 \to V_n \xrightarrow{A_n} V_{n-1} \xrightarrow{A_{n-1}} \cdots \xrightarrow{A_2} V_1 \xrightarrow{A_1} V_0 \to 0$$

where $V_i = K^{b_i}$, K a field, and the complex is acyclic Let r_i be the expected rank (which is, in fact, the rank) of A_i. Then we have the following result:

(*) *Let T_i be the set of integers $\{1, \cdots, b_i\}$. Let $T_i(m)$ denote the set of m-element subsets of T_i. Since $b_i = r_{i+1} + r_i$, there is a one-one correspondence between $T_i(r_{i+1})$ and $T_i(r_i)$ induced by complementation.*

Then, for each i, $1 \le i \le n$, there is a unique set of elements c^i_μ of R indexed by $\mu \in T_{i-1}(r_i)$, which we call the ith vector of multipliers, satisfying the following conditions:

(1) $c^n_\mu = (A_n)_\mu$, *the r_n by r_n* (or b_n *by* b_n) *minor of A_n indexed by μ.*

(2) *If $1 \le i \le n-1$, then for each r_i columns of A_i, i.e. for each $\sigma \in T_{i-1}(r_i)$, let $v_{i\sigma}$ denote the vector of r_i by r_i minors coming from those columns, with their signs adjusted according to a fixed rule of position (which we shall not specify here). The entries of $v_{i\sigma}$ are indexed by $T_i(r_i)$ and hence by $T_i(r_{i+1})$. Let μ_{i+1} be the vector indexed by $T_i(r_{i+1})$ whose entries are the $(i+1)$th vector of multipliers.*

Then:

$$v_{i\sigma} = c^i_\sigma u_i.$$

This may sound more complicated than it is. In the orginal result, for each appropriate size set of columns of A_{n-1}, the appropriate size minors can be written

$$\begin{pmatrix}\text{vector of } r_{n-1} \\ \text{size minors of} \\ \text{chosen columns}\end{pmatrix} = \begin{pmatrix}\text{single} \\ \\ \text{multiplier}\end{pmatrix}\begin{pmatrix}\text{vector of} \\ \\ \text{previous minors}\end{pmatrix}$$

with signs adjusted. This gives rise to a vector of multipliers. At the next stage:

$$\begin{pmatrix}\text{vector of } r_{n-2} \\ \text{size minors of} \\ \text{chosen columns}\end{pmatrix} = \begin{pmatrix}\text{single new} \\ \\ \text{multiplier}\end{pmatrix}\begin{pmatrix}\text{vector of} \\ \\ \text{old multipliers}\end{pmatrix}$$

with signs adjusted, and so on.

The first main structure theorem of Buchsbaum and Eisenbud is then this:

Theorem 7.1. *The statement* (*) *above holds for any finite free acyclic complex over a Noetherian ring.*

We shall sketch a proof of this result, but first we make some remarks.

Remark 1. The result for $n = 2$ and $b_0 = 1$ (corresponding to our original linear algebra theorem) was basically known to Hilbert. In the form of greatest generality, it seems to be due to L. Burch [Bu]. But it has been rediscovered countless times in between.

Remark 2. Eagon and Northcott give an argument for Theorem 7.1 which is in many ways simpler than the original argument of Buchsbaum and Eisenbud. In fact, Eagon and Northcott suppress all the exterior algebra which is needed into a few elementary facts about matrices and determinants, and use no homological algebra at all. Moreover, their arguments show the following:

(a) The theorem is valid without the hypothesis that R be Noetherian.

(b) Instead of assuming that the complex is acyclic, we need only assume that

(1) the expected ranks coincide with actual ranks,

(2) the depths of the key determinantal ideals $I_{r_i}(A_i)$ satisfy

$$\begin{aligned} &\text{depth } I_{r_1}(A_1) \geq 1, \\ &\text{depth } I_{r_i}(A_i) \geq 2, \quad \text{if } i \geq 2. \end{aligned}$$

(For the complex to be acyclic we would need depth $I_{r_i}(A_i) \geq i$, $i \geq 1$.)

(c) Buchsbaum and Eisenbud express these results much more slickly in terms of factorization of maps of exterior algebras. Moreover, they have further results about lower order minors which are incomplete, and some of which are only conjectured.

Sketch of the proof of Theorem 7.1.

Step 1. Localize at the multiplicative system S of all non-zerodivisors. Then the augmentation becomes free, and the complex breaks up into short *split* exact sequences of free modules. One checks the existence and uniqueness for the multipliers easily if the bases are chosen compatible with this break-up and the splittings. Then one checks that thier existence and uniqueness is independent of the choice of bases.

To paraphrase: localization at S puts us in, essentially, a linear algebra situation, where things are easy.

Step 2. We now have unique vectors of multipliers $v_n, v_{n-1}, \cdots$ with the correct properties, but their entries lie in $S^{-1}R$. One shows by reverse induction on t that the entries of v_t lie in R and generate an ideal I_t of depth at least 2 if $t \geq 2$. If $t = n$, this is clear: v_n is the vector of actual minors of A_n and has depth ≥ 2 if $n \geq 2$. Assume the result for v_t, $t \geq 2$. To prove it for v_{t-1}, note that from condition (2) of (*), the set of products of elements of v_{t-1} and v_t is, up to signs, the set of r_{t-1} size minors of A_{t-1}. Hence, for each entry c of v_{t-1}, $I_t c \subset R$. Since depth $I_t \geq 2$, this implies $c \in R$. But we also have

$$I_t I_{t-1} = I_{r_{t-1}}(A_{r_{t-1}}) = J.$$

If $t-1 \geq 2$, depth $J \geq 2$ and so depth $I_{t-1} \geq 2$. Q.E.D.

The question raised by Burch's theorem and the Buchsbaum-Eisenbud structure theorems is this:

What is the best possible result on the "structure" of finite free resolutions? How does one know one has found it?

In the remainder of this section we shall formulate a point of view which we feel provides a good way to look at these questions, and helps to make them more concrete.

Let R be a ring and $\mathcal{K}$ an acyclic complex of finitely generated free R-modules with specified bases, and suppose $\mathcal{K}$ has finite length n and Betti numbers $b_0, \cdots, b_n$. Then we shall say that $(R, \mathcal{K})$ is a *pair* of type $(b_0, \cdots, b_n)$. If S is any R-algebra then in a natural way $(S, S \otimes_R \mathcal{K})$ is again a pair of type $(b_0, \cdots, b_n)$ *provided that* $S \otimes_R \mathcal{K}$ *is again acyclic*. If this is true, we shall say that $(S, S \otimes_R \mathcal{K})$ is a *specialization* of $(R, \mathcal{K})$.

If R, S are Noetherian then a necessary and sufficient condition that $S \otimes_R \mathcal{K}$ be acyclic is that depth $I_{r_i}(A_i)S \geq 2$, $1 \leq i \leq n$. Here, the r_i are the expected ranks and the A_i are the matrices of the maps in $\mathcal{K}$, as usual.

Of course, the assertion that $S \otimes_R \mathcal{K}$ is acyclic only depends, really, on the augmentation module $M = H_0(\mathcal{K})$ and S, for the homology of $S \otimes_R \mathcal{K}$ is $\mathrm{Tor}^R_{\bullet}(S, M)$, so that $S \otimes_R \mathcal{K}$ is acyclic if and only if $\mathrm{Tor}^R_i(S, M) = 0$ for $i \geq 1$.

Suppose we fix n, $(b_0, \cdots, b_n)$. Let us say that a family of pairs $(R_\lambda, \mathcal{K}_\lambda)$ of type $(b_0, \cdots, b_n)$, where each R_λ is Noetherian, is *generic* if for every Noetherian pair $(S, \mathcal{L})$ of type $(b_0, \cdots, b_n)$ there is a λ and a homomorphism $R_\lambda \to S$ such that $(S, \mathcal{L})$ is a specialization of $(R_\lambda, \mathcal{K}_\lambda)$.

The point is this: if we have a "small" generic family $(R_\lambda, \mathcal{K}_\lambda)$ then we can "understand" all free acyclic complexes of type $(b_0, \cdots, b_n)$ by "understanding" the members of the generic family. E.g. the existence of multipliers as in the Buchsbaum-Eisenbud theorems evidently follows at once if one knows it in the generic examples.

More generally suppose ξ is a system of polynomial equations over $\mathbf{Z}$ involving the entries of the matrices A_i and certain unknowns y_j, and one wants to assert that there is always a solution in R. If one has a generic family it is only necessary to prove the assertion for the complexes in the family.

Now, I conjecture that *for every sequence of Betti numbers which can occur, there is a generic family consisting of just one pair* $(R, \mathcal{K})$. I conjecture, moreover, that R *can be taken to be a* $\mathbf{Z}$*-algebra of finite type.*

If this were true, there would exist a rather down-to-earth acyclic complex $\mathcal{K}$ of type $(b_0, \cdots, b_n)$ such that *all* free acyclic complexes over Noetherian rings arise from it by "change of rings", i.e. by tensoring.

The structure of $\mathcal{K}$ then carries with it all "structure theorems" for finite free resolutions of its type. The problem then becomes two-fold: to find $\mathcal{K}$, and to understand $\mathcal{K}$.

This conjecture is true for $n \leq 2$. In fact, something much better is true. (The situation for $n \leq 1$ is extremely trivial, but the result for $n = 2$ is not at all trivial.) Let us make the following definition: call a Noetherian pair $(R, \mathcal{K})$ of type $(b_0, \cdots, b_n)$ *universal* if for every Noetherian pair $(S, \mathcal{L})$ there is a *unique* homomorphism $R \to S$ such that $\mathcal{L} \cong S \otimes_R \mathcal{K}$ (as complexes of free modules with specified basis). A universal pair is not only generic: it is determined up to unique isomorphism as well.

While I do not conjecture that universal pairs exist for $n \geq 3$, they do exist for $n \leq 2$. Moreover, for $n = 2$ the ring R is an integrally closed finitely generated graded $\mathbf{Z}$-algebra.

Before looking at the case $n = 2$, let us briefly examine the case $n = 1$. We have the restriction $b_1 \leq b_0$ (or else there are no free acyclic complexes of type (b_1, b_0)), and in this case let $R = \mathbf{Z}[x_{ij}]$, where (x_{ij}) is a b_1 by b_0 matrix of indeterminates, and let $\mathcal{K}$ be the complex

$$0 \to R^{b_1} \xrightarrow{(x_{ij})} R^{b_0} \to 0.$$

(We assume $b_1 > 0$. If $b_1 = 0$, take $R = \mathbf{Z}$ and let $\mathcal{K}$ be $0 \to 0 \to \mathbf{Z}^{b_0} \to 0$.)

Now, we shall look in detail at the case $n = 2$. As a first approximation we might let $R_0 = \mathbf{Z}[x_{ij}, y_{jk}]$, where (x_{ij}) is a b_2 by b_1 matrix of indeterminates and (y_{jk}) is a b_1 by b_0 matrix of indeterminates. (We shall assume, to avoid degenerate cases, that $1 \leq b_2 < b_1$, $1 \leq b_0 < b_1$, and $b_1 \leq b_0 + b_2$.) But then

$$0 \to R_0^{b_2} \xrightarrow{(x_{ij})} R_0^{b_1} \xrightarrow{(y_{jk})} R_0^{b_0} \to 0$$

is not a complex. Let J_0 be the ideal generated by the entries of the product matrix $(x_{ij})(y_{jk})$. Let $R_1 = R/J_0$. Then

$$0 \to R_1^{b_2} \xrightarrow{(\bar{x}_{ij})} R_1^{b_1} \xrightarrow{(\bar{y}_{jk})} R_1^{b_0} \to 0$$

is a complex but is *not* acyclic. In fact the b_2 by b_2 minors of $(\bar{x}_{ij})$ ($^-$ denotes reduction modulo J_0) are zerodivisors (simultaneously), or, to put it better, $I_{b_2}(\bar{x}_{ij})$ has depth 0. Now, it is easy to see that if we localize at any b_2 by b_2 minor of $(\bar{x}_{ij})$, J_0 expands to a prime, and the contraction Q of this prime to R_0 is independent of the choice of the minor. Let $R_2 = R_0/Q$, a domain, and let $'$ denote reduction modulo Q.

$$0 \to R_2^{b_2} \xrightarrow{(x'_{ij})} R_2^{b_1} \xrightarrow{(y'_{jk})} R_2^{b_0} \to 0$$

is a much better attempt, but still is not acyclic: it can be shown that $I_{b_2}(x'_{ij})$ is contained in a height one prime.

But now, suppose we enlarge R_2 as follows: let $I = I_{b_2}(x'_{ij})$, let F be the fraction field of R_2, and let $R = \{f \in F\colon \text{for some } t, I^t f \in R_2\}$.

It turns out that

Theorem 7.2.

$$0 \to R^{b_2} \xrightarrow{(x'_{ij})} R^{b_1} \xrightarrow{(y'_{jk})} R^{b_0} \to 0$$

is acyclic, and this is the required $\mathcal{K}$: $(R, \mathcal{K})$ *is universal for* (b_0, b_1, b_2).

Sketch of the proof of Theorem 7.2. To see that $\mathcal{K}$ is acyclic, it suffices to see that R is Noetherian, that

$$\operatorname{rank}(x'_{ij}) = b_2,$$
$$\operatorname{rank}(y'_{jk}) = b_1 - b_2,$$

and that

$$\operatorname{depth} I_{b_2}(x'_{ij}) \geq 2, \quad \text{i.e. depth } I \geq 2.$$

For R is a domain and so depth $I_{b_1-b_2}(y'_{jk}) \geq 1$ is automatic. It is easy to check that the ranks are correct. It is also easy to check that if Δ is any b_2 by b_2 minor of (x'_{ij}) then $R_\Delta = (R_2)_\Delta$ is regular of dimension $1 + b_2^2 + b_1 b_0$, and that dim $R = 1 + b_2^2 + b_1 b_0$.

The multipliers of the Buchsbaum-Eisenbud theorem, which exist and are unique in F, are certainly in R, for if the multipliers are $c_1, \cdots, c_t$ then, for each j, $Ic_j \subset R$. Let $R^* = R_2[c_1, \cdots, c_t]$. We shall show that R is the integral closure of R^*. First note that dim $R^* =$ dim $R = 1 + b_2^2 + b_1 b_0$. If q is a prime of R^* which contains I then one can show that, since $I_{b_1-b_2}(y'_{ij}) \subset q$ also,

$$\dim R/q \leq b_2^2 + b_1 b_0 - 1,$$

so that ht $IR^* \geq 2$. Let R' be the integral closure of R^*, a finite R^*-module. Then depth $IR' \geq 2 \Rightarrow \{f \in F\colon I^t f \in R\} \subset R' \Rightarrow R \subset R'$. Then I has depth 2 in R, since, by construction, $I^t f \in R \Rightarrow f \in R$. But then R is integrally closed, for if q is a prime such that R_q has depth 1 but is not a DVR, then every b_2 by b_2 minor of (x'_{ij}) is in q, i.e. $q \supset I$, which contradicts depth $R_q = 1$.

It remains to see that if $\mathcal{L}$,

$$0 \to S^{b_2} \xrightarrow{(s_{ij})} S^{b_1} \xrightarrow{(t_{jk})} S^{b_0} \to 0,$$

is an acyclic complex over a Noetherian S then there is a unique homomorphism $R \to S$ such that

$$(S, \mathcal{L}) \cong (S, S \otimes_R \mathcal{K}).$$

Consider the map $\phi_0\colon R_0 \to S$ which takes $x_{ij} \to s_{ij}$, $y_{jk} \to t_{jk}$. We must show there is a unique map $\phi\colon R \to S$ such that the diagram

$$\begin{tikzcd} R_0 \arrow[r, "\phi_0"] \arrow[d] & S \\ R_1 \arrow[d] & \\ R_2 \arrow[d] & \\ R \arrow[uuur] & \end{tikzcd}$$

commutes. Clearly, ϕ_0 kills J_0, hence induces a unique ϕ_1: $R_1 \to S$. Since each minor of $(\bar{x}_{ij})$ has a power which kills Q/I_0, $I_{b_2}(\bar{x}_{ij})$ has a power which kills Q/I_0. When we map to S, $I_{b_2}(\bar{x}_{ij})$ maps to $I_{b_2}(s_{ij})$, which contains a non-zerodivisor. Hence, Q maps to 0, and there is a unique ϕ_2: $R_2 \to S$ which makes the diagram commute.

Finally, if $I^t f \in R_2$ we can choose a unique $f^* \in S$ such that, for all $r \in I^t$, $\phi_2(rf) = \phi_2(r)f^*$ (there is a unique f^* in the total quotient ring of S because depth $IS \geq 1$, and this f^* is in S because depth $IS \geq 2$).

Thus, $(R, \mathcal{K})$ is universal for (b_0, b_1, b_2). Q.E.D.

I would not expect universal pairs for $n \geq 3$. However, I believe that there may be a kind of "superstructure" associated with a free acyclic complex for $n \geq 3$ and a universal (complex + superstructure). The superstructure would consist of a specific solution for a certain system of equations involving the entries of the matrices of the complex. The simplicity of the case $n \leq 2$ would simply be a consequence of the fact that the superstructure is uniquely determined by the complex in that case.

If this is true then the ultimate "structure theorem" for free acyclic complexes would consist of

(a) a good description of the superstructure (and the assertion that it "exists," i.e. that a certain system of equations has a solution), and

(b) the "universal" example.

Remark 7.3. It is worth pointing out that our knowledge is incomplete even in projective dimension 2. For example, we do not know whether $R = R^*$ (i.e. whether adjoining the multipliers to R_2 already forces integral closure). If there is more to the integral closure then there is a better structure theorem (than Burch's) even in projective dimension 2.

Note that the rigidity conjecture is not known even for projective dimension 2 if $b_1 \lneqq b_2 + b_0$.

The next question that arises is this: *What good properties does one hope for in the ground ring R occurring in a universal object classifying finite free acyclic complexes of a given type + superstructure?*

We note that one will have a complex $\mathcal{K}$ in this set-up which we want to prove exact, and the exactness will follow if certain key ideals have the right depth. If $\mathcal{K}$ really works, it should not be hard, by dimension arguments, to show that they have the right height. But I think it may be extremely difficult to show that they have the right depth unless R is Cohen-Macaulay (in which case, depth = height).

I would hope that if this kind of problem has a solution at all, then it has a solution with R a Cohen-Macaulay, normal, graded domain of finite type over $\mathbf{Z}$. Moreover, I have reason to suspect that R will be embeddable in a polynomial ring. In the case $n = 2$, where we have a specific R, R can be embedded in a polynomial ring in an interesting way: it is the ring of invariants of an algebraic group scheme (over $\mathbf{Z}$) acting on the polynomial ring.

This is interesting because there are recent results asserting that many such rings of invariants are Cohen-Macaulay. We shall pursue this issue in the next section.

http://dx.doi.org/10.1090/cbms/024/09

8. Linear Algebraic Groups

In order to simplify definitions we shall work, in this section, over an algebraically closed field K. (For some of our purposes it would be more natural to work over $\mathbf{Z}$, but it is quite reasonable not to worry about this too much. Working over $\mathbf{Z}$ is usually equivalent, in our context, to working "uniformly" over all algebraically closed fields.)

We do not want to assume very much algebraic geometry. Therefore, we shall take a completely naive point of view. By an affine *K-variety* we shall mean a (not necessarily irreducible) Zariski-closed set V in K^n for some n. We shall usually suppress K, which will be fixed, in our terminology. If $V \subset K^n$, $W \subset K^m$ a *morphism* f is a map $f\colon V \to W$ such that, for suitable polynomials $f_1, \cdots, f_m \in K[x_1, \cdots, x_n]$ for all $v \in V$, $f(v) = (f_1(v), \cdots, f_m(v))$. The category of K-varieties is then anti-equivalent to the category of reduced K-algebras of finite type via

$$V \longrightarrow \mathrm{Mor}(V, K) = K[V].$$

In practice, if V is a variety, X is a set, and $g\colon X \to V$ is a bijection, then we may (and shall) think of X as a variety isomorphic to V.

Let $GL(n, K)$ denote the group of n by n invertible matrices over K. If (x_{ij}) is an n by n matrix of indeterminates over K, y an extra indeterminate, and $\Delta = \det(x_{ij})$, then the Zariski closed set in K^{n+1} defined by $\Delta y - 1 = 0$ is in bijective correspondence with $GL(n, K)$, so that $GL(n, K)$ has the structure of a variety.

We shall say that a group G which also has the structure of a variety is a *linear algebraic group* if there is a map $f\colon G \to H$, where H is a Zariski-closed subgroup of some $GL(n, K)$, such that f is both a group isomorphism and an isomorphism of varieties.

By a *homomorphism* of linear algebraic groups we mean a group homomorphism which is a morphism of varieties. For further information on linear algebraic groups and invariant theory we refer the reader to [B_0], [Mum], [W], [DC], and [F].

Examples. $GL(n, K)$ is a linear algebraic group. In particular, we may regard $G_m = GL(1, K)$, the multiplicative group of K, as a linear algebraic group. B_n, the n by n upper triangular matrices, is an l.a.g. (linear algebraic group), as is its subgroup U_n of those matrices in B_n all of whose main diagonal entries are 1.

U_2 is obviously identifiable with the additive group G_a of K which thus has the structure of an l.a.g.

$SL(n, K) = \{A \in GL(n, K)\colon \det A = 1\}$ is clearly a closed subgroup of $GL(n, K)$, as is the orthogonal group $O(n, K) = \{A \in GL(n, K)\colon AA^t = \mathrm{id}\}$. $SO(n, K) = SL(n, K) \cap O(n, K)$ is likewise an l.a.g.

Any finite group is an l.a.g.: view it as a group of permutations of the standard basis for K^n.

A standard theorem asserts that if G is an l.a.g., then G^0, the connected component of the identity, is a closed normal subgroup of finite index.

We next want to discuss actions of l.a.g.'s on K-vector spaces. If V is a finite-dimensional K-vector space the group $GL(V) = \mathrm{Aut}_K V$ is isomorphic to $GL(n, K)$, where $n = \dim V$. We need only choose a basis for V to get an isomorphism. A different choice of basis gives the same l.a.g. structure. (The different isomorphisms $GL(V) \to GL(n, K)$ "differ" by an inner automorphism of $GL(n, K)$.)

By a *representation* or *action* of an l.a.g. G on a finite-dimensional vector space V we simply mean a homomorphism $G \to GL(V)$ as l.a.g.'s. (Of course, this also gives a map $G \times V \to V$.)

If V is infinite dimensional, by an action of G on V we mean a homomorphism $G \to \mathrm{Aut}_K V$ such that V is a directed union of finite-dimensional subspaces W, closed under the action of G, such that $G \to GL(W)$ is a homomorphism of l.a.g.'s for each W.

Given an action of G on V, we always have a map $G \times V \to V$, and we shall say that V is a *G-module*. A G-module V is *trivial* if $G \to \mathrm{Aut}\, V$ is trivial, i.e. $\mathrm{Im}\, G = \{\mathrm{id}_V\}$. If $W \subset V$ is such that $G(W) \subset W$ (W is a vector space), then we say that W is *G-stable*, *invariant under G*, or is a *G-submodule*. G-modules is an abelian category with arbitrary direct sums (coproducts) and one can test for exactness and locate kernels, cokernels, direct sums, etc. as K-vector spaces by working with the vector space structure alone.

We note that every G-module V has a largest trivial submodule V^G which, as a vector space, is defined by

$$V^G = \{v \in V\colon g(v) = v \text{ for all } g \in G\}.$$

If we give K the trivial G-module structure then there is a natural isomorphism $V^G \cong \mathrm{Hom}_G(K, V)$.

It follows that $V \to V^G$ is a left exact functor from G-modules to trivial G-modules (i.e. K-vector spaces).

The functor $V \to V^G$ is not usually exact. But there is an important class of groups, including the classical groups in characteristic 0, for which it is. First, a G-module is called *irreducible* or *simple* if it has no proper nonzero submodules. (Of course, then it is finite-dimensional.)

Theorem 8.1. *The following conditions on an l.a.g. G are equivalent*:

(1) *If $W \subset V$ are finite-dimensional G-modules, then W has a G-stable complement W', i.e. $V = W \oplus W'$ as G-modules.*

(2) *Every finite-dimensional G-module is a direct sum of irreducibles.*

(3) *If $W \subset V$ are G-modules, then W has a G-stable complement.*

(4) *Every G-module is a direct sum of irreducibles.*

(5) *Given a map of G-modules* $f: V \to K$, *where* K *has the trivial G-module structure, if* f *is surjective then there is an invariant* $v \in V^G$ *such that* $f(v) = 1$, *i.e.* f *splits.*

(6) *The functor* $V \to V^G$ *is exact.*

(See [F] and [Mum].)

A group G which satisfies these conditions is called *linearly reductive.* Note that condition (5) (or (6)) says that K, with the trivial structure, is projective, while (3) says that every exact sequence splits, so that every G-module is both projective and injective.

This theorem does not really give any clues as to which groups *are* linearly reductive. It turns out that there are very few in characteristic $p > 0$, but the situation is much better in characteristic 0. The following complete classification of the linearly reductive groups is due to Nagata $[N_2]$:

Theorem 8.2. *If the characteristic of* $K = p > 0$, *then an l.a.g.* G *is linearly reductive if and only if* G^0 *is a product of copies of* G_m *and the order of the finite group* G/G^0 *is not divisible by* p.

If the characteristic of $K = 0$, *then an l.a.g.* G *is linearly reductive if and only if the largest closed connected solvable normal subgroup of* G^0 *(which, by a theorem, exists) is isomorphic to a product of copies of* G_m.

A product of copies of G_m is called a *torus.* The largest closed connected solvable normal subgroup of G^0 is called its *radical.* An l.a.g. is called *semisimple* if its radical is $\{e\}$.

Another characterization of the linearly reductive groups in characteristic 0 is this: G is linearly reductive if and only if $G^0/(\text{finite group}) \cong (\text{semisimple group}) \times$ torus. (Moreover, over the complexes, G is linearly reductive if and only if it is the complexification of a compact real Lie group.)

Thus, in characteristic 0, the classical groups $GL(n, K)$, $SL(n, K)$, $O(n, K)$ and the symplectic group are linearly reductive, and so are the finite groups. The torus is linearly reductive over any field.

The "bad" (non-(linearly reductive)) groups are the ones with a closed connected solvable normal subgroup H such that H contains a copy of G_a in its composition series (a connected solvable l.a.g. has a composition series in which all the factors are copies of G_a and G_m: if G_a does not occur, it is a torus). Thus, G_a is not linearly reductive, and neither is U_n.

Let G be a linearly reductive linear algebraic group. We want to discuss the *Reynolds operator* associated with G.

If G acts on V, then there exists a direct sum decomposition $V = V^G \oplus E$ as G-modules. It is easy to see that the G-module complement E for V^G is *unique.* It follows that there is a *unique* G-module retraction $\rho: V \to V^G$, which is called the *Reynolds operator* (see [Mum], [HE], and [F]).

If G is finite of order n and p = the characteristic of K does not divide n, then the Reynolds operator is defined by averaging:

$$\rho(v) = \frac{1}{n}\left(\sum_{g \in G} g(v)\right).$$

Now, let R be a K-algebra. We shall say that G *acts* on R if it acts on R as a K-vector space by K-algebra automorphisms. Then R^G is a ring, called the ring of invariants. Let us prove something:

Theorem 8.3. *Let G be a linearly reductive l.a.g. acting on a K-algebra R. Then the Reynolds operator $R \to R^G$ is an R^G-module homomorphism.*

Moreover, it follows that:

(a) *If R is Noetherian, so is R^G.*

(b) *If R is of finite type over K, so is R^G.*

Proof. Let $R = R^G \oplus E$ be the unique G-module decomposition, and let F be any irreducible submodule of E. It suffices to show that if $a \in R^G$, $aF \subset E$. Since $a \in R^G$ and F is irreducible, a: $F \to aF$ (multiplication) is either 0 or an isomorphism. If $aF = 0$, we are done. If $F \cong aF$ (as G-modules) then $aF \cap R^G = 0$ (or else $aF \cap R^G = aF \Rightarrow aF$ is a trivial G-module $\Rightarrow F$ is a trivial G-module $\Rightarrow F \subset R^G$, a contradiction). Then $R^G + aF = R^G \oplus aF$ has a G-module complement, E', in R, and

$$R = R^G \oplus (aF \oplus E').$$

Since E is unique, $E = aF + E'$, and $aF \subset E$.

Thus, E is an R^G-module. It follows that, for each ideal I of R^G, $IR \cap R^G = (I \oplus IE) \cap (R^G \oplus 0) = I \oplus 0 = I$. Hence, if R is Noetherian and $I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ is a chain of ideals, I_nR is eventually stable, and hence $(I_nR) \cap R^G = I_n$ is eventually stable, and R^G is Noetherian.

Now suppose R is of finite type over K. Let $u_1, \cdots, u_m$ generate R. Then there is a finite-dimensional K-subspace of R, stable under G, which contains $u_1, \cdots, u_m$; call it V, and let $\dim V = n$. Let $x_1, \cdots, x_n$ be a basis for V. Let S be the symmetric algebra $S_K(V)$ of V, which we may identify with the polynomial ring $K[x_1, \cdots, x_n]$. The action of G on the one-forms $V = \Sigma_i Kx_i$ of S extends uniquely to an action of G on S.

The inclusion $V \subset R$ induces a unique K-algebra homomorphism ϕ: $S \to R$ which is immediately seen to be a G-module homomorphism as well. ϕ is surjective, since V contains a set of generators of R.

Since G is linearly reductive, the induced map $S^G \to R^G$ is surjective.

Thus, it will suffice to show that S^G is finitely generated over K. The action of G on S preserves degrees, so that S^G is a graded K-algebra. But S is Noetherian, so that S^G is a graded *Noetherian* K-algebra. This implies that S^G is finitely generated. Q.E.D.

On the other hand, examples of Nagata [N_3] indicate that one does not expect rings of invariants of linear algebraic groups G in, say, characteristic 0, acting on finitely generated K-algebras to be finitely generated very often if G is not linearly reductive. (In characteristic $p > 0$ it seems that it may be enough that the radical be a torus, just as in characteristic 0, even though this does not imply linear reductivity.)

We now want to discuss the relationship between this material on invariant theory and linear algebraic groups and the study of modules of finite projective dimension.

First connection. It turns out that rings of invaraints of actions of linearly reductive groups on regular K-algebras are Cohen-Macaulay. To be precise:

Theorem 8.4. *Let G be a linearly reductive linear algebraic group over K acting on a regular Noetherian K-algebra S. Then the ring of invariants $R = S^G$ is Cohen-Macaulay.*

It frequently turns out, in fact, that R has the form $K \otimes_{\mathbf{Z}} R_0$, where R_0 is a finitely generated flat Cohen-Macaulay $\mathbf{Z}$-algebra, and R_0 can be represented as T/I, where $T = \mathbf{Z}[X_1, \cdots, X_n]$ is a polynomial ring. In this way one gets perfect ideals I from actions of linearly reductive groups, and if $\mathcal{K}$ is a resolution of T/I over T then $\mathcal{K}$ remains a resolution after specializing the X_i to elements of any Noetherian ring A in such a way that IA has the same depth as I. These examples of perfect ideals as well as their "tendency" to stay perfect under nondegenerate specialization are both useful in the study of modules of finite projective dimension.

Theorem 8.4 is the main result of [HR$_1$] and was announced in [HR$_2$].

We now want to give some examples of actions, and the corresponding rings of invariants and defining ideals.

Example 8.5. Let X, Y be r by t and t by s matrices of indeterminates, respectively, and let $G = GL(t, K)$ act on $S = K[X, Y]$ (the polynomial ring generated by the entries of X and Y over K) as follows: if $A \in G$, A maps the entries of X to those of XA^{-1}, and the entries of Y to those of AY. Then if the characteristic of $K = 0$, S^G is $K[XY]$, the ring generated over K by the entries of XY. If U is an r by s matrix of indeterminates and if, for any matrix A over a ring B, $I_m(A)$ denotes the ideal generated by the size m minors of A, then

$$K[U]/I_{t+1}(U) \cong K[XY].$$

See [HE]. Thus, Theorem 8.4 guarantees that $I_{t+1}(U)$ is perfect if characteristic $K = 0$, for $GL(t, K)$ is linearly reductive if the characteristic of $K = 0$. But it turns out that if U is a matrix of indeterminates over $\mathbf{Z}$, then $I_{t+1}(U)$ is a perfect prime ideal of $\mathbf{Z}[U]$ in this case too. That is, "determinantal ideals" are, so to speak, generically perfect.

Example 8.6. Let X be an r by s matrix over K and let $G = SL(r, K)$ act on $S = K[X]$ as follows: if $A \in G$, A takes the entries of X to those of AX. Then $R = S^G$, regardless of characteristic, is generated over K by the r size minors of X. This R has been long studied: it is the homogeneous coordinate ring of the Grassmann variety of r-dimensional subspaces of s-space. Let U_i be $\binom{s}{r}$ indeterminates. Then $R \cong$

$K[U_i]/I$ where I is generated by certain quadratic forms, the well-known *Plücker relations* (see [HP], [H_8]). In fact there is an ideal I in $\mathbf{Z}[U_i]$ such that

$$K[r \text{ size minors of } X] \cong K[U_i]/IK[U_i]$$

for every field K (in fact, for every commutative ring K).

Now, if K is a field of characteristic 0, then Theorem 8.4 guarantees that $IK[U_i]$ is perfect, but it turns out ([H_8], [Lak], [Mus]) that $I \subset \mathbf{Z}[U_i]$ is already perfect.

Example 8.7. Let $G = O(r, K)$ act on $S = K[X]$, where X is an r by s matrix of indeterminates, as follows: if $A \in G$, A takes the entries of X to those of AX. Then, if K has characteristic 0, $S^G = K[X^tX]$, where X^t is the transpose of X. Now X^tX is an s by s symmetric matrix. Let $U = (u_{ij})$ be an s by s symmetric matrix of indeterminates. Then

$$(*) \qquad K[U]/I_{t+1}(U) \cong K[X^tX]$$

and $I_t(U)$ is perfect. But (*) holds over $\mathbf{Z}$ as well, and $I_{t+1}(U)$ is perfect over $\mathbf{Z}$ as well [Ku].

Example 8.8. Let $G = GL(1, K)^m$ act on $S = K[x_1, \cdots, x_n]$ as follows: fix mn integers $t_{ij} \in \mathbf{Z}$, and if $a = (a_1, \cdots, a_m) \in G$ let a map x_j to $a_1^{t_{1j}} \cdots a_m^{t_{mj}} x_j$.

Then S^G is generated by those monomials $x_1^{h_1} \cdots x_n^{h_n}$ such that $(h_1, \cdots, h_n)$ is a solution, in the nonnegative integers, of the system of linear equations

$$(*) \qquad \begin{array}{c} t_{11}H_1 + \cdots + t_{1n}H_n = 0, \\ \cdots \\ t_{m1}H_1 + \cdots + t_{mn}H_n = 0 \end{array}$$

for the H's. It was shown in [H_9] that S^G is Cohen-Macaulay, and this follows again from Theorem 8.4 (in all characteristics, for $GL(1)^m$ is linearly reductive in all characteristics). In [H_9] is it shown as a consequence that any normal ring generated over a field K by finitely many monomials in indeterminates is Cohen-Macaulay.

If R is Cohen-Macaulay and $\mathfrak{M}$ is the set of monomials whose exponents satisfy (*), $R[\mathfrak{M}]$ is Cohen-Macaulay. In particular, this works over $\mathbf{Z}$. The defining ideal of relations on the monomials is generated by differences $m_1^{t_1} \cdots m_k^{t_k} - m_{k+1}^{t_{k+1}} \cdots m_s^{t_s}$ which cancel "formally", where $m_1, \cdots, m_s$ is any set of generators of $\mathfrak{M}$.

We note that if K is a field the unique G-module complement for $S^G = K[\mathfrak{M}]$ in S is simply the K-vector space spanned by monomials not in $\mathfrak{M}$.

Example 8.9. Let G be a finite group whose order is invertible in the Cohen-Macaulay ring S. Then S^G is Cohen-Macaulay [HE]. (This even has a partial converse: see [HE, Proposition 16], and [C].) This is false in general if $G = GL(1, K)$ and S is not regular [HE, p. 1036], or if the order of G is not invertible and S is regular [HR_1, Example 2.4] and [Ber].

Remark 8.10. If (x_{ij}) is an r by s matrix of indeterminates over $\mathbf{Z}$, then $I_t(x_{ij})$ is a perfect ideal of $\mathbf{Z}[x_{ij}]$, $1 \le t \le \min\{r, s\}$, and it is known that

$$\mathrm{pd}_{\mathbf{Z}[x_{ij}]}\mathbf{Z}[x_{ij}]/I_t(x_{ij}) = (r-t+1)(s-t+1).$$

However, the problem of finding an explicit projective resolution for $\mathbf{Z}[x_{ij}]/I_t(x_{ij})$ has resisted strenuous efforts. If $t = r \leq s$ the Eagon-Northcott complex [EN$_1$] gives the minimal resolution, while the Buchsbaum-Rim "generalized Koszul complex" [BR] gives a nonminimal resolution which is more functorial in some ways and admits a multiplicative structure [Gov].

If $t = r - 1$, $s = r$, the resolution is known [GN], and also if $t = r - 1$, $s = r + 1$ [Ko]. As far as I know, resolutions are not known in other cases. See [Sv] for a proof that the rings $\mathbf{Z}[x_{ij}]/I_t(x_{ij})$ are Gorenstein precisely if $t = 1$ or $r = s$.

Remark 8.11. I conjecture the following purely algebraic generalization of Theorem 8.4:

Conjecture 8.12. *Let S be a regular Noetherian ring and let R be a subring of S which is pure in S. (I.e. for every R-module M, the map $M \to M \otimes_R S$ is injective. This holds, in particular, when R is a direct summand of S as an R-module.) Then R is Cohen-Macaulay.*

This conjecture implies Theorem 8.4 because in the situation of Theorem 8.4 the existence of the Reynolds operator $S \to R = S^G$ implies that R is a direct summand of S.

The conjecture is proved for the case where S contains a field of characteristic p in [HR$_1$] using the interplay between the Frobenius and local cohomology. (The case of the group is handled by "reduction to characteristic p", an oddity because there are few linearly reductive groups in characteristic p.)

Second connection. The second connection between the study of modules of finite projective dimension is related to the first. It is the follow-up to the remarks at the end of §7. The universal base ring for free acyclic complexes turns out to be a ring of invariants of a linear algebraic group, at least if we pass to a base field K of characteristic 0 (but probably, in general).

Unfortunately, the group in question is not linearly reductive, so that Theorem 8.4 does not apply, but I conjecture that the base ring is Cohen-Macaulay, and hope that some better theorem than 8.4 will imply it (and not just in the case of projective dimension two).

For the moment, we shall simply explain how the base ring arises as a ring of invariants (in the "field of characteristic 0" case). The proof is too long and complicated to give here.

Consider the universal pair $(R, \mathbb{K})$ of Theorem 7.2. To fit in with our linear algebraic group set-up, we shall work over an algebraically closed field K (algebraic closure is not really necessary) instead of over $\mathbf{Z}$. (We keep our old notation $(R, \mathbb{K})$ for the universal pair; the new pair is obtained by applying $K \otimes_{\mathbf{Z}}$, or by making the same construction as before, but starting with $K[x_{ij}, y_{ij}]$.)

Then I *conjecture* that R is a ring of invariants of an l.a.g. acting on a polynomial ring, and can prove this if the characteristic of $K = 0$.

To be quite specific, assume, as usual, that $1 \le b_0$, $b_2 < b_1$ and that $b_1 \le b_0 + b_2$. If A is a square matrix, let A^* denote the transpose of the cofactor matrix (the classical adjoint), so that

$$AA^* = A^*A = (\det A)\mathrm{id}.$$

Let $U = (u_{ij})$ and $V = (v_{ij})$ be b_1 by b_1 and $b_1 - b_2$ by b_0 matrices of indeterminates. Let G be the subgroup of $GL(b_1, K)$ consisting of matrices whose first b_2 rows are identical with those of the identity matrix. We shall describe an action of G on $K[u_{ij}, v_{ij}]$ such that the ring of invariants is R (if char $K = 0$ and, conjecturally, in general).

Note that G has a normal subgroup H consisting of matrices of the form:

$$\left[\begin{array}{c|c} \mathrm{id}_{b_2} & O_{b_2\times(b_1-b_2)} \\ \hline A_{(b_1-b_2)\times b_2} & \mathrm{id}_{b_1-b_2} \end{array}\right]$$

where A is arbitrary, and also a subgroup G' consisting of matrices of the form:

$$\left[\begin{array}{c|c} \mathrm{id}_{b_2} & O_{b_2\times(b_1-b_2)} \\ \hline O_{(b_1-b_2)\times b_2} & A_{(b_1-b_2)\times(b_1-b_2)} \end{array}\right]$$

where A is an arbitrary element of $GL(b_1 - b_2, K)$. It is easy to see that there is a homomorphism $\phi\colon G \longrightarrow GL(b_1 - b_2, K)$ wihch maps each $B \in G$ into its $(b_1 - b_2) \times (b_1 - b_2)$ lower right-hand corner such that

(1) ϕ is surjective,

(2) $\phi|G'$ is an isomorphism of $G' \in G$ with $GL(b_1 - b_2, K)$,

(3) $\ker \phi = H$.

Thus, G is the semidirect product of $GL(b_1 - b_2, K)$ and the solvable (even nilpotent) group H.

Now let G act on $K[U, V]$ ($= K[u_{ij}, v_{ij}]$) as follows: if $B \in G$, then B sends the entries of U to BU, while B sends the entries of V to $(\phi(B)^*)^{-1}V = (\det V)^{-1}\phi(B)V$.

Let U_1 be the matrix formed from the first b_2 rows of U (U_1 is b_2 by b_1) and let U_2 be the matrix formed from the last $b_1 - b_2$ columns of U^*. It is easy to see that the entries of U_1 and of the product matrix U_2V are invariant under the action of G.

If the characteristic of $K = 0$ then I can show that $K[U, V]^G$ is the set of elements in the fraction field of $K[U_1, U_2V]$ which are multiplied into the ring by a power of $I_{b_2}(U_1)$.

Now, if we map $R_0 = K[x_{ij}, y_{jk}]$ (where (x_{ij}) is b_2 by b_1 and (y_{jk}) is b_1 by b_0) into $K[U, V]$ by taking (x_{ij}) to U and (y_{jk}) to V, it is not hard to see that the kernel contains the ideal J_0 generated by the entries of $(x_{ij})(y_{jk})$ and that it is, in fact, the unique minimal prime Q of J_0 which does not contain some (equivalently, any) b_2 by b_2 minor of (x_{ij}). This induces a map of $R_1 = K[x_{ij}, y_{jk}]/I$ into $K[U, V]^G$ and an injection of

$$R_2 = K[x_{ij}, y_{jk}]/Q \rightarrow K[U, V]^G,$$

If the characteristic of $K = 0$, then this injection induces an isomorphism $R \cong K[U, V]^G$ by virtue of the definition of R and the characterization of $K[U, V]^G$ given above.

Thus, at least over a field of characteristic 0, the universal base ring R is a ring of invariants of a linear algebraic group acting on a polynomial ring. Proofs will be given in [H_{10}].

http://dx.doi.org/10.1090/cbms/024/10

9. Applications of Homological Methods and Some More Open Questions

In this section I want to discuss some applications of homological methods to apparently nonhomological questions, one concerning ''cancellation'' of indeterminates (i.e. uniqueness of the coefficient ring in a polynomial ring), and the other concerning modules of derivations. My objective is to point out that while the theory of regular local rings provided much of the original impetus for the study of modules of finite projective dimension (and the spectacular success there is certainly convincing motivation) the homological techniques prove useful in a variety of situations, some of which are a little unexpected.

I also want to point out here that some of the open questions we have discussed are related to questions about the Spec of a Noetherian ring.

Finally, I want to raise some questions which I think are relevant and important, although they are vague.

First, let us consider the cancellation problem, which we phrase this way:

If $A[x_1, \cdots, x_n] = B[y_1, \cdots, y_n]$ (where the x's are indeterminates over A and the y's are indeterminates over B), under what conditions can one assert that $A \cong B$?

(Those familiar with algebraic geometry will see easily that this is an analogue of the problem of cancelling copies of $\mathbf{R}^n$ in products of topologcial spaces.)

One can give easy examples of the above type with $A \ncong B$ using symmetric algebras and the failure of cancellation for free direct summands of modules.

Recall that if M is an R-module then the symmetric algebra $\mathrm{Symm}_R(M)$ of M is a commutative R-algebra, graded by the nonnegative integers, together with an R-module map $M \to (\mathrm{Symm}_R(M))_1$ (the subscript denotes "first graded piece") with the following property: if S is any (graded) commutative R-algebra and $\phi: M \to S$ is any R-module homomorphism (respectively, such that $\phi(M) \subset S_1$), then there is a unique (graded) R-algebra homorphism ψ: $\mathrm{Symm}_R(M) \to S$ such that the diagram

$$\begin{tikzcd} \mathrm{Symm}_R(M) \arrow[rr, "\psi"] & & S \\ & M \arrow[ul] \arrow[ur, "\phi"'] & \end{tikzcd}$$

commutes. One can identify $(\mathrm{Symm}_R(M))_n$ with

$$\underbrace{(M \otimes M \otimes \cdots \otimes M)}_{n \text{ copies}}/E_n$$

where E_n is generated by elements of the form

$$\cdots \otimes m \otimes \cdots \otimes m' \otimes \cdots - \cdots \otimes m' \otimes \cdots \otimes m \cdots$$

Moreover, if $M = F/N$ where F is the free module on elements x_j and N is generated by certain relations $\Sigma_i\, a_{ij} x_j$ (all but finitely many $a_{ij} = 0$), then $\mathrm{Symm}_R(M)$ may be identified with $R[X_j]/I$ where the X_j are indeterminates corresponding to the x_j and I is the ideal generated by the elements $\Sigma_i\, a_{ij} X_j$.

One can check easily that $\mathrm{Symm}_R(M \oplus N) \cong (\mathrm{Symm}_R M) \otimes_R (\mathrm{Symm}_R N)$ (as graded R-algebras).

Now, let $\mathbf{R}$ be the reals and let

$$A = \mathbf{R}[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1) = \mathbf{R}[x, y, z].$$

Map ϕ: $A^3 \longrightarrow A$ by $(u, v, w) \longrightarrow xu + yv + zw$ and let E be the kernel. Then since $u \longrightarrow u(x, y, z)$ splits ϕ we have

$$A^3 \cong E \oplus A \quad \text{or} \quad A^2 \oplus A \cong E \oplus A.$$

On the other hand, E is known to be a projective A-module which is not free (cf. [EaH] or $[\mathrm{H}_{11}]$ for more details). But then

$$\mathrm{Symm}_A(A^3) \cong A[y_1, y_2, y_3] \cong \mathrm{Symm}_A E \otimes_A \mathrm{Symm}_A A \cong S \otimes_A A[Z] \cong S[Z]$$

as A-algebras, where $S = \mathrm{Symm}_A E$. On the other hand, it is shown in $[\mathrm{H}_{11}]$ (and in [EaH]) that $S \not\cong A[Z_1, Z_2]$, even as rings.

Remark 9.1. The real algebraic variety corresponding to S is the tangent bundle $T(S^2)$ to the real 2-sphere (the points of this "real" variety correspond to homomorphisms of S *onto* $\mathbf{R}$); the real varieties corresponding to $S[Z]$ and $A[y_1, y_2, y_3]$ are $T(S^2) \times \mathbf{R}$ and $S^2 \times \mathbf{R}^3$, respectively. Thus, this algebraic example is inspired by a topologcial example of failure of cancellation for vector bundles: $T(S^2)$ is not trivial but $T(S^2) \times \mathbf{R} \approx S^2 \times \mathbf{R}^3$. This is well known in topology. This example indicates the danger of isolating commutative rings from other branches of mathematics. (The only proof I know that the module E is not free depends on the topological fact that there is no continuous nonvanishing vector field on S^2.)

We next want to examine a question closely related to the original cancellation question:

Suppose $A[x_1, \cdots, x_{n+k}] = B[y_1, \cdots, y_n]$ and $A \subset B$. Under what circumstance can one conclude $B = A[z_1, \cdots, z_k]$ (where the y's and z's are indeterminates over A and the y's are indeterminates over B).

The preceding example shows that one cannot conclude this, in general, even if $k = 2$. For with $n = 1$, $B = S$, $x_1, x_2, x_3 = z_1, z_2, z_3$, and $y_1 = z$, we have

$$A[x_1, x_2, x_3] = B[y_1],\ A \subset B \quad \text{and} \quad B \not\cong A[z_1, z_2].$$

But if $k = 1$ it seems possible that the result might hold and one cannot construct a counterexample using symmetric algebras of projective modules.

For suppose $A[x_1, \cdots, x_{n+1}] = B[y_1, \cdots, y_n]$ and $B = \mathrm{Symm}_A E$, where E is projective. Then

$$\mathrm{Symm}_A A^{n+1} \cong A[x_1, \cdots, x_{n+1}] = B[y_1, \cdots, y_n]$$
$$\cong (\mathrm{Symm}_A E) \otimes_A \mathrm{Symm}_A A^n \cong \mathrm{Symm}(E \oplus A^n).$$

If C is any A-algebra of the form $\mathrm{Symm}_A P$, where P is a projective module of finite type, we can recover P from C: for $\mathrm{Der}_A(C, A) \cong \mathrm{Hom}(P, A)$ (by restriction) and $P \cong \mathrm{Hom}(\mathrm{Hom}(P, A), A)$. Thus,

$$\mathrm{Symm}_A A^{n+1} \cong \mathrm{Symm}(E \otimes A^n) \Rightarrow A^{n+1} \cong E \oplus A^n \Rightarrow E \cong A$$

(just as in the proof (1.7) of unique factorization in regular local rings: apply Λ^{n+1} to both sides). Then $B \cong \mathrm{Symm}_A A \cong A[x]$.

Thus, we pose the following question:

If $A[x_1, \cdots, x_{n+1}] = B[y_1, \cdots, y_n]$, $A \subset B$, is $B \cong A[x]$ as an A-algebra?

This question is first considered in detail in [AEH], where an affirmative answer is given for the case where A is a UFD.

In [Ha], the question is settled rather completely as follows:

(a) The answer is yes if A contains the rationals.

(b) The answer is yes if A is a seminormal ring (more about this below).

(c) The answer, in general, is no.

The interesting fact is that the proof of (b) (which is a tool in the proof of (a)) depends on exactly the same ideas as in the proof (1.7) of unique factorization in regular local rings. This gives an instance where homological techniques come up somewhat unexpectedly. Fact (c) is also quite interesting: in characteristic p there are examples of failure of cancellation of indeterminates unrelated to failure of cancellation for modules, and not involving the symmetric algebra trick.

What we want to do here is take a look at the "homological" portion of the proof of (b).

Let R be a reduced algebra essentially of finite type over a field K. (This is much less than the generality one can work in.) Then the following two conditions are equivalent:

(1) If a is an element of the total quotient ring of R such that $a^2, a^3 \in R$, then $a \in R$.

(2) For all n, the natural map $\mathrm{Pic}(R) \to \mathrm{Pic}(R[x_1, \cdots, x_n])$ is an isomorphism.

($\mathrm{Pic}(R)$ is the group of isomorphism classes of rank one projectives under $\otimes$.)

If R satisfies these equivalent conditions we call R *seminormal*. (Seminormality is defined in much greater generality in [T]. The equivalence of (1) and (2) is proved in [Ha].)

Now, suppose A is seminormal (reduced) and $A[x_1, \cdots, x_{n+1}] = B[y_1, \cdots, y_n]$. We have

$$\begin{tikzcd} B \arrow[r, hook] \arrow[drr, "\beta"'] & B[y_1, \cdots, y_n] = A[x_1, \cdots, x_{n+1}] \arrow[dr, "\alpha"] & \\ & & A \end{tikzcd}$$

where α is the map which kills the x_i. Let $I = \ker \beta$.

First consider the case where A is local. Then we can show that I is principal, in fact, free on one generator.

For let $T = A[x_1, \cdots, x_{n+1}]$. Then if we regard $A = T/(x_1, \cdots, x_{n+1})T$ as a T-module via α, $\mathrm{pd}_T A = n + 1 < \infty$. (In fact, the Koszul complex gives a resolution.) But T is B-free, so that $\mathrm{pd}_B A \leq n + 1 < \infty$, where A is a B-module via β. Hence, $\mathrm{pd}_B I = \mathrm{pd}_B A - 1 \leq n < \infty$, by virtue of the exact sequence $0 \to I \to B \to A \to 0$.

Since A is local B has a unique maximal ideal m containing I, whence $\mathrm{pd}_B A = \mathrm{pd}_{B_m} A_m$. But

$$\mathrm{pd}_{B_m} A_m = \text{depth } B_m - \text{depth } A_m.$$

Now, T is A-free and B is a direct summand of T as a B-module. Hence, B is A-flat and, in fact, B_m is faithfully flat over A_m. But if a local ring (D, q) is faithfully flat over a local ring (C, p) then (see [Mat])

$$\text{depth } D = \text{depth } C + \text{depth } D/pD.$$

Hence,

$$\begin{aligned} \text{depth } B_m - \text{depth } A_m &= \text{depth } B_m - \text{depth } A \\ &= \text{depth } B_m/pB_m, \end{aligned}$$

where p is the maximal ideal of A. Let $K = A/p$. Then

$$\begin{aligned} K[x_1, \cdots, x_{n+1}] &\cong (B/pB)[y_1, \cdots, y_n] \\ &\Longrightarrow B/pB \cong K[x] \\ &\Longrightarrow \text{depth } (B/pB)_m = 1. \end{aligned}$$

Thus $\mathrm{pd}_B A = \mathrm{pd}_{B_m} A_m = \text{depth } B_m - \text{depth } A_m = 1$ and $\mathrm{pd}_B I = 0$, i.e. I is projective, and easily seen to be of rank one.

Since A is seminormal and *local*, $\mathrm{Pic}(A) = 0$. Thus, $\mathrm{Pic}(T) = 0$ and hence $\mathrm{Pic}(B) = 0$. Thus, I is free and generated by a non-zerodivisor, say $I = xB$.

It is then easy to see that $B = A[x]$. (If not, let b be an element of least total degree in $x_1, \cdots, x_{n+1}$ not in $A[x]$. Then $\beta(b) \in A$ and $b - \beta(b) \in xB$, say $b = \beta(b) + xb'$, where $b' \in B$ and has smaller total degree than b.)

This takes care of the case where A is local. In the general case, for each prime P of A there is an element z_P of B_P, unique up to multiplication by a unit, with the following two properties:

(1) As an element of $A_P[x_1, \cdots, x_{n+1}]$, z_P has constant term 0.

(2) $B_P = A_P[z_P]$.

While z_P is not unique, the submodule $E_{(P)} = A_P z_P$ which it spans is unique, and is characterized by the following properties:

(1) Any element of $E_{(P)}$, regarded as an element of $A_P[x_1, \cdots, x_{n+1}]$, has 0 constant term, i.e. $E_{(P)} \subset (x_1, \cdots, x_{n+1})A_P[x_1, \cdots, x_{n+1}]$,

(2) $E_{(P)} \cong A_P$, and

(3) the map $\mathrm{Symm}_{A_P}(E_{(P)}) \to B_P$ induced by the inclusion $E_{(P)} \subset B_P$ is an isomorphism.

It is then easy to show that there exists a unique A-submodule E of B such that, for each prime P of A, the inclusion $E \to B$ induces an isomorphism of E_P $(= E \otimes_A A_P)$ with $E_{(P)}$. (One uses Grothendieck's equivalence between the category of quasicoherent sheaves of modules on an affine scheme Spec(A) and the category of A-modules. It is easy to construct a quasicoherent subsheaf $\mathcal{E}$ of $\tilde{B}$ such that the stalks of $\mathcal{E}$ are the $E_{(P)}$, for if $B = A_P[z_P]$ then there is an $r \notin P$ such that $B_r = A_r[z_r]$, where $z_r \in B_r$ is an element whose image in B_P is z_P. On the open set $D(r)$ in Spec(A), the $E_{(Q)}$, $Q \not\ni r$, are the stalks of the subsheaf $z_r A_r$ of B_r.) Then E is easily seen to be a rank one projective of finite type and the inclusion $E \subset B$ induces a map $\mathrm{Symm}_A(E) \to B$ which is an isomorphism (because it is an isomorphism when we localize at any $P \in$ Spec(A)). Thus, B is of the special form mentioned earlier, and $B \cong A[x]$. Q.E.D.

We refer the reader to [AEH], the expository paper [EaH], and to [Ha] for more information about cancellation.

Remark 9.2. The reader not familiar with Grothendieck's method of viewing commutative rings as local ringed spaces (sheaves of rings of a certain type) is referred to [EGA]. The argument demonstrates the need for the scheme-theoretic point of view even in what seems to be pure commutative algebra.

We note that the result (b) can be used to prove the result (a) when A contains the rationals (one of the main theorems of [Ha]). One first makes a reduction to the case where A is of finite type over Q, the rationals, and then to the case where A is reduced. Then, just as in the proof of (b) one can assume that A is local. The theorem ($B = A[x]$) becomes true if A is enlarged to a seminormal ring. By taking A to be a sort of maximal counterexample one can assume that there is a local counterexample (A, P) (essentially of finite type over Q) with $A[x_1, \cdots, x_{n+1}] = B[y_1, \cdots, y_n]$, $B \neq A[x]$, but $B[a] = A[a][x]$ for a certain a in the total quotient ring of A with the properties $a^2 \in A$, $a^3 \in A$, $Pa \subset A$. By tricks involving modules of derivations one then shows that $B \subset A[a][x]$ is closed under ordinary differentiation with respect to x. (All this would work over a field of characteristic p too.) But then $Q \subset A$ yields a contradiction.

A closer examination in the characteristic p case yields counterexamples.

Example 9.3. Let K be a field of characteristic $p > 0$, let a, z be indeterminates over K, and let

$$A = K[a^2, a^3] \subset K[a] \quad \text{and} \quad B = A[z - az^p, z^p] \subset K[a, z].$$

It is not hard to show that $B \ncong A[x]$. However, if x_1, x_2, y are new indeterminates we do have $A[x_1, x_2] \cong B[y]$ as A-algebras. The two (inverse) homomorphisms are determined by

$$x_1 \mapsto z - a(z + ay)^p = (z - az^p) + a^{p+1}y^p,$$
$$x_2 \mapsto y + (z + ay)^p = y + z^p + a^p y^p$$

and

$$z \mapsto (x_1 + ax_2) - a(x_2 - (x_1 + ax_2)^p),$$
$$y \mapsto x_2 - (x_1 + ax_2)^p$$

(the second pair of arrows determine a $K[a]$-homomorphism $K[a, z, y] \to K[a, x_1, x_2]$ which takes $B[y]$ into $A[x_1, x_2]$).

We now leave the topic of cancellation and consider very briefly a second application of homological methods: to the so-called Zariski-Lipman conjecture. Let R be the local ring at a closed point of an algebraic variety over an algebraically closed field K of characteristic 0. That is, R is the localization, at a maximal ideal, of a domain finitely generated over K. Then the conjecture asserts that if the module of derivations $\mathrm{Der}_K(R, R)$ is free, then R is regular.

It is shown in [Lip] that R must be normal, and the case when the variety is a hypersurface is known. Very little else is known except for the case of homogeneous complete intersections.

The homogeneous form of the conjecture asserts that if R is a finitely generated graded domain over K (K as before) and $\mathrm{Der}_K(R, R)$ is free, then R is a polynomial ring. This is proved in [Mo] if R is a homogeneous complete intersection, i.e., R is of the form $K[x_1, \cdots, x_n]/(f_1, \cdots, f_m)$ where the x_i are indeterminates and the f_i form a regular sequence. Let $\bar{\ }$ denote reduction modulo $(f_1, \cdots, f_m)$. Then the key points in the proof of the Zariski-Lipman conjecture in this case (see [Mo] for details) are that, if $\mathrm{Der}_K(R, R)$ is free there is an acyclic free complex

$$0 \to R^{n-m} \xrightarrow{A_2} R^n \xrightarrow{A_1} R^m \to 0$$

where $A_1 = (\partial f_j/\partial x_i)^{-}$ and the first row of A_2 is $(x_1 \ \cdots \ x_n)$. (If f is homogeneous, $\Sigma_i x_i(\partial f/\partial x_i) = (\deg f)f$.) A contradiction is then obtained from the fact that, by the [BE_2] theorem, the vector of m by m minors of A_1 (with suitable signs) is a multiple (multiplier in R) of the vector of $n-m$ by $n-m$ minors of A_2. (Moen works from the pleasant paper [MacR] rather than from the [Bu]-[BE_2] theorems.)

We now leave our study of applications of homological methods and consider some questions about the prime spectrum of a Noetherian ring. Oddly enough, it seems that such questions are related to the problem of proving the existence of big Cohen-Macaulay modules in the unequal characteristic case.

There are many open questions about the Spec of a Noetherian ring. For example, it is not known whether an integrally closed Noetherian ring R must satisfy the saturated chain condition (i.e. whether if $P \subset Q$ are primes of R, all saturated chains of primes from P to Q have the same length).

Another interesting question is this: let R be an arbitrary Noetherian ring and suppose P_0, $Q \neq Q'$ are primes of R with $P_0 \subset Q \cap Q'$ and both $\mathrm{ht}(Q/P_0)$ and $\mathrm{ht}(Q'/P_0)$ ≥ 2. Is there a prime P with $P_0 \subsetneqq P \subset Q \cap Q'$? (One can easily reduce to the case where $P_0 = 0$, $\mathrm{ht}\, Q = \mathrm{ht}\, Q' = 2$, and R is semilocal with two maximal ideals: Q and Q'. In fact, one can even suppose, in addition, that R is integrally closed.) See §10F.

The fact that even the above simple question is open (it was raised by Kaplansky, informally) makes it apparent that there are very great difficulties inherent in the following question:

What ordered sets can occur as Spec(R) for R Noetherian?

If R is Noetherian, every closed set is a finite union of closures of points, and the closure of a point (whether R is Noetherian or not) is the set of primes which contain it. Thus, when R is Noetherian the order on Spec(R) determines the topology and conversely. Thus, an equivalent question is:

What topological spaces can occur as Spec(R) for R Noetherian?

If R is allowed to be any commutative ring the answer is given in [H_1]: Spec(R) may be homeomorphic to any topological space X with the following properties:

(1) X is T_0.

(2) X is quasicompact.

(3) The intersection of two quasicompact open subsets is quasicompact.

(4) The quasicompact open subsets are a basis for the open sets.

(5) Every nonempty closed subspace which is irredcuible (i.e. not the union of two proper closed subsets) is the closure of one of its points (i.e. has a generic point).

These conditions are equivalent to the assertion that X is an inverse (or projective) limit of finite T_0 spaces.

If we impose the condition that R be Noetherian we immediately get the condition:

(N_1) D.C.C. holds for closed sets in X,

where $X = \mathrm{Spec}(R)$, i.e. that X be a *Noetherian* topological space. This is equivalent to:

(N_1') Every open (equivalently, every) subset of X is quasicompact.

Note that from (N_1) and (5):

(N_2) Every closed set is a finite union of closures of points.

But this is far from the whole story. For example, a three element linearly ordered set satisfies all the above conditions but is not a possible Spec(R). For the following condition holds:

(N_3) Let Y be a closed set and $x_1, \cdots, x_k, y$ points of Y such that $\{x_1, \cdots, x_k\}$ is disjoint from $\mathrm{cl}\{y\}$, i.e. $y \not\leq x_i$, each i. Then there is an $x \in Y$ such that $x \not\leq x_i$, each i, $x \leq y$, and $\mathrm{ht}_Y x \leq 1$.

Here, $\mathrm{ht}_Y x$ denotes the supremum of lengths of chains of primes in Y with largest element x. (To see this, work modulo the defining ideal of Y, i.e. assume $Y = X$. Let $P_1, \cdots, P_n, Q$ be the primes corresponding to $x_1, \cdots, x_n, y$, respectively. Then $Q \not\subset P_i$, any $i \Rightarrow Q \not\subset \bigcup P_i$. Let $q \in Q - \bigcup P_i$. Some minimal prime P of (q) is contained in Q. Let x correspond to P.)

These conditions are far from sufficient. If $X = \mathrm{Spec}(R)$, R Noetherian, then one may take as a closed basis the set $\mathcal{O}$ of closed sets of the form $V(r)$, $r \in R$. From Krull's height theorem we have:

(N_4) X has a closed basis $\mathcal{O}$ such that, for each closed set Y of X and each $y \in Y$, $\mathrm{ht}_Y y = n$ if and only if there exist $V_1, \cdots, V_n \in \mathcal{O}$ such that $\mathrm{cl}\{y\}$ is an irreducible component of $Y \cap V_1 \cap \cdots \cap V_n$, and this is not true for any smaller n.

I do not know how to circumvent the inelegant device of quantifying over the set of bases.

But even these conditions do not seem to suffice. By virtue of the results of [HRa], there will frequently exist primes P in $\mathrm{Spec}(R)$ such that the saturated chain condition holds for all $Q \subset Q'$ such that $Q' \subset P$, and the results of [McA] give new and subtle properties of good behavior in $\mathrm{Spec}(R)$. The whole situation is mysterious, at best.

Now let us return to the question of the existence of big Cohen-Macaulay modules. The problem, in the mixed characteristic case, is to show that certain systems of equations ξ of the form

$$F_1(X, Y) = 0,$$
$$\cdots$$
$$F_h(X, Y) = 0$$

where X denotes $X_1, \cdots, X_n$, Y denotes $Y_1, \cdots, Y_q$, and $F_1, \cdots, F_h$ are polynomials in X, Y with coefficients in $\mathbf{Z}$, do not have a solution in a local ring R of dimension n in which the values of the X_i are a system of parameters.

By using Artin approximation one can reduce this to showing that no solution exists in an R essentially of finite type over an excellent discrete valuation ring V. Let

$$S = V[X, Y]/(F_1, \cdots, F_m).$$

Let $I = (X_1, \cdots, X_n)S$. Then what we want to show is that if we adjoin additional indeterminates Z and divide out by a prime Q we still have $\mathrm{ht}(I^e + Q/Q) < n$.

Let u generate the maximal ideal of V. If the big Cohen-Macaulay modules conjecture is false then we can find a prime Q in $T = S[Z]$ and a minimal prime P of $IT + Q$ such that $\mathrm{ht}\, P/Q = n$.

Now, since we have proved the conjecture in the case where the ring contains a field, we must have $u \in P$.

I believe it should be possible to show that u is not in any minimal prime of I in the case above, where $F_1, \cdots, F_h$ come from the big Cohen-Macaulay modules problem. If so, the existence of big Cohen-Macaulay modules would follow from an affirmative answer to the following question, which is phrased purely in terms of properties of Spec of a Noetherian ring.

Question. Let $X = \mathrm{Spec}\, T$, where T is Noetherian, let Y be a closed subset of X, and let $x_1, \cdots, x_r$ be points of height ≤ 1 such that no $\mathrm{cl}\{x_i\}$ contains an irreducible component of Y. Suppose there exist points z, v such that $\mathrm{cl}\{v\}$ is an irreducible component of $Y \cap \mathrm{cl}\{z\}$ and $\mathrm{ht}_{\mathrm{cl}\{z\}} v \geq n$.

Do there exist points z^*, v^* such that $\mathrm{cl}\{v^*\}$ is an irreducible component of $Y \cap \mathrm{cl}\{z^*\}$, $\mathrm{ht}_{\mathrm{cl}\{z^*\}} v^* \geq n$ and v^* is not in the closure of any x_i?

If we let the x_i correspond to the minimal primes of uT, Y be the set of primes containing IT and z, v correspond to Q, P, respectively, it is clear that an affirmative answer to this question (plus the information that u is not in any minimal prime of IT) will yield a proof of the existence of big Cohen-Macaulay modules in general.

For then P^*, Q^* (corresponding to v^*, z^*) yield a solution for the equations in the local ring $(T/Q^*)_{P^*}$ which contains a field (for $u \notin P^*$).

Probably, it is not very likely that the question has an affirmative answer in the generality of this question. But we can relax conditions in many ways for the purpose of handling big Cohen-Macaulay modules: e.g. we need only consider the case where T is of finite type over an excellent discrete valuation ring and we can allow T to be modified by adjoining more indeterminates before asking for the existence of z^*, v^*. Moreover, much more information about T, I is available.

I put the question as above to make the point that, quite possibly, an investigation of something as apparently simple-minded as the order of the primes in a (good) Noetherian ring may yield a solution to the problem of whether big Cohen-Macaulay modules exist.

Finally, I want to raise a couple of questions more concerning Cohen-Macaulay modules, and also to pose an (unfortunately rather vague) metaconjecture.

First, suppose S is a module-finite local domain over a complete regular local ring (R, P). In the cases where the direct-limit-of-modifications procedure works, can it be modified to produce S-modules M which are R-free and $PM \neq M$? (I believe that it is possible to produce S-modules M such that M is R-flat and $\bigcap_t P^t M = 0$ in this way.)

Second, if one can get S-modules which are R-free, can one get finitely generated ones by some trick (e.g. perhaps finding a finitely generated direct summand). Can one give some sort of classification of Cohen-Macaulay modules over S, even big ones (say, the R-free S-modules) in the case $S = R[\theta]$, where θ is integral over the regular ring R? To what extent (if any) do finitely generated R-free $R[\theta]$-modules of big rank have to split? See §10H.

Last, I would like to put forth the problem of finding some precise statement which reflects the sentiment of the following hopelessly vague

Metaconjecture. *Let $\mathfrak{T}$ be a "homological" statement about local rings which is true for local rings containing a field and can be proved for local rings which contain a field of characteristic 0 by "reduction to positive characteristic p". Then $\mathfrak{T}$ is true for all local rings.*

(Example of a bad $\mathfrak{T}$: "every local ring contains a field".)

http://dx.doi.org/10.1090/cbms/024/11

10. Supplement

The preceding sections were written before the talks were given. This brief section deals with some extra material which was discussed during the conference but not referred to in the earlier notes.

A. C. Peskine and L. Szpiro and, independently, P. Roberts, have proved a generalization of the intersection conjecture (which they call the "new intersection conjecture") for local rings of prime characteristic $p > 0$ and local rings essentially of finite type over a field, etc. See [zPS]. We shall not discuss this result here, except to mention that it follows for all equicharacteristic local rings from the existence of big Cohen-Macaulay modules by much the same argument as the original intersection conjecture. [zPS] also contains announcements of proofs of many conjectures for the graded case.

B. R. Fossum, H.-B. Foxby, and P. Griffith [zFFG] have used the existence of big Cohen-Macaulay modules in the equicharacteristic case to prove the following result in general: if (R, P) is local, M is of finite type, and $0 \to M \to I_0 \to \cdots \to I_t \to \cdots$ is a minimal injective resolution of M, then for every integer t such that depth $M \leq t \leq \mathrm{id}_R M$ (which may be infinite) the injective hull E of $R/P = K$ occurs as a direct summand in I_t. (That is, $\mathrm{Ext}_R^t(K, M) \neq 0$, for E occurs a number of times equal to $\dim_K \mathrm{Ext}_R^t(K, M)$. See [B].)

C. If Δ is a finite simplicial complex with vertices $x_1, \cdots, x_n$, and K is a field, then let $K[\Delta] = S/I$, where $S = K[x_1, \cdots, x_n]$, a polynomial ring, and I is the ideal generated by those monomials $x_1^{h_1}, \cdots, x_n^{h_n}$ such that $\{x_1, \cdots, x_n\}$ is *not* a face of Δ. Then Krull dim $K[\Delta] = \dim \Delta + 1$ and $K[\Delta]$ is Cohen-Macaulay if and only if $\mathrm{pd}_S K[\Delta] = n - (\dim \Delta + 1)$. Using these facts, an old result of Macaulay [zM] and results from [H_9], Richard Stanley [zSt] has given a new proof of the upper bound conjecture for simplicial polytopes and, more generally, he has shown that it holds for all constructible simplicial complexes (see [H_9]). The results of the thesis [zReis], which characterize those Δ such that $K[\Delta]$ is Cohen-Macaluay, should yield a proof of the upper bound conjecture at least for all combinatorial spheres. The whole topic provides an unexpected application of homological methods in commutative rings to combinatorics.

D. In connection with the material of §8, I want to raise the following question. Let K be, say, an algebraically closed field and let G be a linear algebraic group over K acting on the polynomial ring $S = K[x_1, \cdots, x_n]$ so as to preserve degrees. Suppose that there are only finitely many distinct orbits of G in K^n, or, equivalently, that there are only finitely many prime ideals $P_1, \cdots, P_m$ of S which are G-stable. Then is each S/P_i Cohen-Macaulay?

Example. Let $G = GL(r, K) \times GL(s, K)$ act on $K[x_{ij}]$ where (x_{ij}) is an r by s matrix of indeterminates, $r \leq s$, so that $(A, B) \in G$ maps the entries of (x_{ij}) to those of $A(x_{ij})B^{-1}$. Then two matrices are in the same orbit if and only if they have the same rank t, i.e., there are $r+1$ orbits. The G-stable primes correspond to the closures of these orbits, and are the ideals $I_t(x_{ij})$, $0 \leq t \leq r$. Thus, the question has an affirmative answer in this case.

E. I want to refer the reader to the paper [BE_2] for a discussion of applications of structure theorems for finite free resolutions to Serre's conjecture on multiplicities.

F. S. McAdam and L. J. Ratliff, Jr. have shown, in connection with the question of Kaplansky near the top of p. 67, that if there exists an example with only finitely prime P such that $P_0 \subsetneqq P \subset Q \cap Q'$, then there exists an example with no such P.

Added in proof. G. S. McAdam (preprint, University of Texas, Austin) has recently settled F completely. There is an example with finitely many and, hence, also, with no such P.

H. Concerning the two questions raised just prior to the metaconjecture on p. 69: P. Griffith (preprint, University of Illinois, Urbana) has shown that if a complete local domain S which is a finite module over a complete regular local ring R possesses a big Cohen-Macaulay module, then there is a countably generated S-module which is R-free. Moreover, R-free $R[\theta]$-modules hardly need to split if they have big rank, unless $R[\theta]$ is very special. A better question is: do R-free $R[\theta]$-modules of finite type and big rank (respectively, countably infinite rank) have to have an $R[\theta]$-submodule of finite type which is a direct summand as an R-module (Griffith's question)?

References

[A] M. Artin, *Algebraic approximation of structures over complete local rings*, Inst. Hautes Études Sci. Publ. Math., No. 36, Paris, 1969, 23–58. MR 42 #3087.

[AB_1] M. Auslander and D. A. Buchsbaum, *Homological dimension in local rings*, Trans. Amer. Math. Soc. 85 (1957), 390–405. MR 19, 249.

[AB_2] ———, *Codimension and multiplicity*, Ann. of Math. (2) 68 (1958), 625–657. MR 20 #6414.

[AEH] S. S. Abhyankar, P. Eakin and W. Heinzer, *On the uniqueness of the coefficient ring in a polynomial ring*, J. Algebra 23 (1962), 310–342. MR 46 #5300.

[B] H. Bass, *On the ubiquity of Gorenstein rings*, Math. Z. 82 (1963), 8–28. MR 27 #3669.

[Bar] S. F. Barger, *Generic perfection and the theory of grade*, Thesis, Univ. of Minnesota, 1970; see also Proc. Amer. Math. Soc. 36 (1972), 365–368.

[Ber] M.-J. Bertin, *Anneaux d'invarients d'anneaux de polynômes, en caractéristique p*, C. R. Acad. Sci. Paris Sér. A–B 264 (1967), A653–A656. MR 35 #6661.

[BE_1] D.A. Buchsbaum and D. Eisenbud, *What makes a complex exact?*, J. Algebra 25 (1973), 259–268. MR 47 #3369.

[BE_2] ———, *Some structure theorems for finite free resolutions*, Advances in Math. 12 (1974), 84–139.

[Bo] A. Borel, *Linear algebraic groups* (Notes taken by Hyman Bass), W. A. Benjamin, New York, 1969. MR 40 #4273.

[BR] D. A. Buchsbaum and D. S. Rim, *A generalized Koszul complex*. II. *Depth and multiplicity*, Trans. Amer. Math. Soc. 111 (1964), 197–242. MR 28 #3076.

[Bu] L. Burch, *On ideals of finite homological dimension in local rings*, Proc. Cambridge Philos. Soc. 64 (1968), 941–948. MR 37 #5208.

[C] C. Chevalley, *Invariants of finite groups generated by reflections*, Amer. J. Math. 77 (1955), 778–782. MR 17, 354; 1436.

[DC] J. A. Dieudonné and J. B. Carrell, *Invariant theory, old and new*, Academic Press, New York-London, 1971. MR 43 #4828.

[EaH] P. M. Eakin, Jr. and W. J. Heinzer, *A cancellation problem for commutative rings*, Proc. Kansas Commutative Algebra Conference, Lecture Notes in Math., No. 311, Springer-Verlag, Berlin, 1973, pp. 61–77.

[EGA] A. Grothendieck (with J. Dieudonné), *Éléments de géométrie algébrique*, I. *Le langage des schémas*, Inst. Hautes Études Sci. Publ. Math., No. 4, Paris, 1960. MR 36 #177a.

[EN_1] J. A. Eagon and D. G. Northcott, *Ideals defined by matrices and a certain complex associated with them*, Proc. Roy. Soc. Ser. A 269 (1962), 188–204. MR 26 #161.

[EN_2] ———, *On the Buchsbaum-Eisenbud theory of finite free resolutions*, J. Reine Angew. Math. 262/263 (1973), 205–219.

[F] J. Fogarty, *Invariant theory*, Benjamin, New York, 1969. MR 39 #1458.

[FR] D. Ferrand and M. Raynaud, *Fibres formelles d'un anneau local Noethérien*, Ann. Sci. École Norm. Sup. (4) 3 (1970), 295–311. MR 42 #7660.

[GN] T. H. Gulliksen and O. G. Negård, *Un complexe résolvent pour certains idéaux déterminentiels*, C. R. Acad. Sci. Paris Sér. A 274 (1972), A16–A19.

[Gov] E. H. Gover, *Multiplicative structure of generailzed Koszul complexes*, Trans. Amer. Math. Soc. 185 (1973), 287–307.

[H_1] M. Hochster, *Prime ideal structure in commutative rings*, Trans. Amer. Math. Soc. 142 (1969), 43–60. MR 40 #4257.

[H_2] ———, *Cohen-Macaulay modules*, Proc. Kansas Commutative Algebra Conference, Lecture Notes in Math., No. 311, Springer-Verlag, Berlin, 1973, pp. 120–152.

[H_3] ———, *Contracted ideals from integral extensions of regular rings*, Nagoya Math. J. 51 (1973), 25–43.

[H_4] ———, *Deep local rings (preliminary version)*, Århus University preprint series, December 1973.

[H_5] ———, *Grade-sensitive modules and perfect modules*, Proc. London Math. Soc. (3) 29 (1974), 55–76.

[H_6] ———, *Constraints on systems of parameters*, Proc. Oklahoma Ring Theory Conference, Marcel-Dekker, New York, 1974, pp. 121–161.

[H_7] ———, *The equicharacteristic case of some homological conjectures on local rings*, Bull. Amer. Math. Soc. 80 (1974), 683–686.

[H_8] ———, *Grassmannians and their Schubert subvarieties are arithmetically Cohen-Macaulay*, J. Algebra 25 (1973), 40–57. MR 47 #3383.

[H_9] ———, *Rings of invariants of tori, Cohen-Macaulay rings generated by monomials, and polytopes*, Ann. of Math. (2) 96 (1972), 318–337. MR 46 #3511.

[H_{10}] ———, *Generic modules of projective dimension* 2, (in preparation).

[H_{11}] ———, *Nonuniqueness of coefficient rings in a polynomial ring*, Proc. Amer. Math. Soc. 34 (1972), 81–82. MR 45 #3394.

[Ha] E. Hamann, *On the R-invariance of* $R[x]$, Thesis, Univ. of Minnesota, 1973; J. Algebra (to appear).

[HE] M. Hochster and J. A. Eagon, *Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci*, Amer. J. Math. 93 (1971), 1020–1058. MR 46 #1787.

[HP] W.V.D. Hodge and D. Pedoe, *Methods of algebraic geometry*, Vols. I and II, Cambridge Univ. Press, Cambridge, 1947 and 1952. MR 10, 396; MR 13, 972.

[HR_1] M. Hochster and J. L. Roberts, *Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay*, Advances in Math. 13 (1974), 115–175.

[HR_2] ———, *Actions of reductive groups on regular rings and Cohen-Macaulay rings*, Bull. Amer. Math. Soc. 80 (1974), 281–284.

[HRa] M. Hochster and L. J. Ratliff, Jr., *Five theorems on Macaulay rings*, Pacific J. Math. 44 (1973), 147–172. MR 47 #3384.

[K] I. Kaplansky, *Commutative rings*, Allyn and Bacon, Boston, 1970. MR 40 #7234.

[Ku] R. E. Kutz, *Cohen-Macaulay rings and ideal theory in rings of invariants of algebraic groups*, Thesis, Univ. of Minnesota, 1971; Trans. Amer. Math. Soc. 194 (1974), 115–129.

[L] S. Lichtenbaum, *On the vanishing of* Tor *in regular local rings*, Illinois J. Math. 10 (1966), 220–226. MR 32 #5688.

[Lak] D. Laksov, *The arithmetic Cohen-Macaulay character of Schubert schemes*, Acta Math. 129 (1972), 1–9. MR 46 #9051.

[Lip] J. Lipman, *Free derivation modules on algebraic varieties*, Amer. J. Math. 87 (1965), 874–898. MR 32 #4130.

[LV] G. Levin and W. V. Vasconcelos, *Homological dimensions and Macaulay rings*, Pacific J. Math. 25 (1968), 315–323. MR 37 #6275.

[MacR] R. E. MacRae, *On an application of the Fitting invariants*, J. Algebra 2 (1965), 153–169. MR 31 #2296.

[Mat] H. Matsumura, *Commutative algebra*, Benjamin, New York, 1970. MR 42 #1813.

[McA] S. McAdam, *Saturated chains of primes in Noetherian rings*, Indiana J. Math. 23 (1974), 719–728.

[Mo] S. Moen, *Free derivation modules and a criterion for regularity*, Proc. Amer. Math. Soc. 39 (1973), 221–227. MR 47 #1794.

[Mum] D. Mumford, *Geometric invariant theory*, Ergebnisse der Math. und ihrer Grenzgebiete, Band 34, Academic Press, New York; Springer-Verlag, Berlin-New York, 1965. MR 35 #5451.

[Mus] C. Musili, *Postulation formula for Schubert varieties*, J. Indian Math. Soc. 36 (1972), 143–171.

[N_1] M. Nagata, *Local rings*, Interscience, Tracts in Pure and Appl. Math., No. 13, Interscience, New York, 1962. MR 27 #5790.

[N_2] ———, *Complete reducibility of rational representations of a matric group*, J. Math. Kyoto Univ. 1 (1961/62), 87–99. MR 26 #236.

[N_3] ———, *Lectures on the fourteenth problem of Hilbert*, Notes by M. P. Murthy, Lectures on Math., No. 31, Tata Institute of Fundamental Research, Bombay, 1965. MR 35 #6663.

[O] B. L. Osofsky, *The subscript of* $\aleph_n$, *projective dimension, and the vanishing of* $\varprojlim^{(n)}$, Bull. Amer. Math. Soc. 80 (1974), 6–26.

[Po] K. Y. Poon, *A resolution of certain perfect ideals defined by some matrices*, Thesis, Univ. of Minnesota, 1973.

[PS] C. Peskine and L. Szpiro, *Dimension projective finie et cohomologie locale*, Inst. Haute Études Sci. Publ. Math., No. 42, Paris, 1973, 323–395.

[R] D. Rees, *The grade of an ideal or module*, Proc. Cambridge Philos. Soc. 53 (1957), 28–42. MR 18, 637.

[Ray] M. Raynaud, *Anneaux locaux henséliens*, Lecture Notes in Math., No. 169, Springer-Verlag, Berlin-New York, 1970. MR 43 #3252.

[S] J.-P. Serre, *Algèbre locale multiplicités*, Lecture Notes in Math., No. 11, Springer-Verlag, Berlin, 1965. MR 34 #1352.

[Sv] T. Svanes, *Coherent cohomology on Schubert subschemes of flag schemes and applications*, Advances in Math. 14 (1974), 369–453.

[T] C. Traverso, *Seminormality and Picard group*, Ann. Scuola Norm. Sup. Pisa (3) 24 (1970), 585–595. MR 43 #3275.

[W] H. Weyl, *The classical groups. Their invariants and representations*, 2nd ed., Princeton Univ. Press, Princeton, 1946. MR 1, 42.

[ZS] O. Zariski and P. Samuel, *Commutative algebra*, Vol. II, The University Series in Higher Mathematics, Van Nostrand, Princeton, 1960. MR 22 #11006.

[zFFG] R. Fossum, H.-B. Foxby and P. Griffith, *Minimal injective resolutions*, Univ. of Illinois, Urbana-Champaign (preprint). A modified version with I. Reiten is to appear in Publ. Math., I.H.E.S.

[zM] F. S. Macaulay, *Some properties of enumeration in the theory of modular systems*, Proc. London Math. Soc. 26 (1927), 531–555.

[zPS] C. Peskine and L. Szpiro, C. R. Acad. Sci. Paris Sér. A-B 278 (1974), 1421–1424.

[zReis] G. A. Reisner, *Cohen-Macaulay quotients of polynomial rings*, Thesis, Univ. of Minnesota, 1974.

[zSt] R. P. Stanley, *Cohen-Macaulay rings and constructible polytopes*, M.I.T. (preprint).

Selected Titles in This Series

(*Continued from the front of this publication*)

(See the AMS catalog for earlier titles)

ISBN 0-8218-1674-8

9 780821 816745

CBMS/24