BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 84, Number 5, September 1978

SOME APPLICATIONS OF THE FROBENIUS IN CHARACTERISTIC 0

BY MELVIN HOCHSTER[1]

ABSTRACT. Several applications are given of the technique of proving theorems in char 0 (as well as char p) by, in some sense, "reducing" to char p and then applying the Frobenius. A "metatheorem" for reduction to char p is discussed and the proof is sketched. This result is used later to give the idea of the proof of the existence of big Cohen-Macaulay modules in the equicharacteristic case. Homological problems related to the existence of big Cohen-Macaulay modules are discussed. A different application of the same circle of ideas is the proof that rings of invariants of reductive linear algebraic groups over fields of char 0 acting on regular rings are Cohen-Macaulay. Despite the fact that this result is false in char p, the proof depends on reduction to char p. A substantial number of examples of rings of invariants is considered, and a good deal of time is spent on the question, what does it really mean for a ring to be Cohen-Macaulay?

The paper is intended for nonspecialists.

1. Introduction. The objective of this paper is to describe and relate for a general audience several areas in commutative rings and algebraic geometry in which progress has been made recently by the following general method: translate the original problem into one of showing that certain equations cannot have a solution, and then apply the Frobenius to make these equations, which at first look merely unlikely, obviously absurd. This technique, which seems a priori limited to the char $p > 0$ case, can be made to yield results for arbitrary Noetherian rings containing a field, by using the "metatheorem" (2.1) described in §2. The approximation theorem of M. Artin is the key to this kind of reduction.

Both the main results which we shall discuss in detail involve the notion of a "regular sequence" on a module. Let R be a ring (all rings are commutative, with identity) and M an R-module (i.e. a unital R-module). Then $x_1, \ldots, x_n$ in R is called a *regular sequence on M* or *M-sequence* if:

(1) $\Sigma_j x_j M \neq M$ and

(2) for each i, $1 \leq i \leq n$, x_i is not a zerodivisor on $M/\Sigma_{j<i} x_j M$.

(See [AB$_1$], [AB$_2$], [AB$_3$], [K$_1$], [M], [N$_2$], [Rees], and [ZS].)

If R is a local ring, i.e. a Noetherian ring with a unique maximal ideal $\mathfrak{m}$, then dim R denotes, equivalently, the supremum of lengths h of chains of

This paper is based on an invited address presented at the Eighty-second Annual Meeting of the American Mathematical Society, at San Antonio, Texas, on January 24, 1976; received by the editors October 3, 1977.

AMS (MOS) subject classifications (1970). Primary 13-02, 13E05, 13J10, 13H10, 13D05; Secondary 13C15, 13H05, 13H15, 14B15, 14M05, 14M15, 20G15.

[1]The author was supported by Purdue University, the University of Michigan, and a grant from the National Science Foundation.

prime ideals $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_h$ (R is *not* regarded as a prime in R), or the least integer n such that there exist n elements $x_1, \ldots, x_n$ in $\mathfrak{m}$ and a positive integer N with $\mathfrak{m}^N \subset \Sigma_j x_j R$. The set of elements $x_1, \ldots, x_n$ is then called a *system of parameters* (s.o.p. for short) for R. (The first definition of dimension is used even when R is neither local nor Noetherian: but then one may not even have $\dim R[x] = 1 + \dim R$. See **[Sei₁]**, **[Sei₂]**, and the expository paper **[Gil]**.)

Note that any Noetherian ring has lots of local rings associated with it: for any prime P let $R_P = R[x_s: s \in R - P]/I$, where I is the ideal generated by the elements $\{sx_s - 1: s \in R - P\}$. Then R_P is a local ring called the *local ring of R at P*. (See **[K₁]**, **[M]**, **[N₂]**, and **[ZS]** for more details.)

Life is really worth living in a Noetherian ring R when all the local rings have the property that every s.o.p. is an R-sequence. Such a ring is called *Cohen-Macaulay* (C-M for short). Many more illuminating properties of these rings are discussed in §3. One example is the ring of formal (or convergent) power series in n variables $x_1, \ldots, x_n$. In either case one s.o.p. which is obviously an R-sequence is $x_1, \ldots, x_n$. An s.o.p. which is less obviously an R-sequence is $x_1^{m_1}, x_2^{m_2} + f_2, x_3^{m_3} + f_3, \ldots, x_n^{m} + f_n$, where f_i is in the ideal generated by $x_1, \ldots, x_{i-1}$, $2 \leq i \leq n$.

Local rings $(R, \mathfrak{m})$ in which $\mathfrak{m}$ is generated by an s.o.p. are called *regular*, and an arbitrary Noetherian ring R is called *regular* if all its local rings are regular. (Let x be a point of an analytic variety or of an algebraic variety over an algebraically closed field. Then x is a smooth (simple) point if and only if the local ring at x is regular. Cf. **[Z₃]**, **[Fu]**, **[Mu₂]**, or **[Mu₄]**.) Formal or convergent power series rings over a field are regular, while their quotients by an R-sequence turn out to be C-M but not usually regular.

The first of the main results we shall discuss is:

(1.1). THEOREM (M. HOCHSTER AND J. ROBERTS). *Let K be a field and let G be a linearly reductive linear algebraic group over K acting K-rationally by K-algebra automorphisms on a regular Noetherian K-algebra S. Then the fixed ring S^G is Cohen-Macaulay.*

"Linearly reductive" means that every finite dimensional (K-rational) representation is a direct sum of irreducible representations. [E.g. if $K = \mathbf{C}$, this means G is the complexification of a compact real Lie group, while if K is algebraically closed of char $p > 0$ then G^0, the connected component of the identity of G, must be an algebraic torus (i.e. a finite product of copies of the multiplicative group G_m of K) while G/G^0 must be (finite) of order prime to p. See **[Bor]**, **[Mu₁]**, **[N₁]**, and **[N₃]**.]

A surprising fact is that while (1.1) is mainly a char 0 theorem (it is false for reductive G in char $p > 0$), the proof depends on somehow passing to char $p > 0$.

When a local ring R is not C-M, life is much harder, but some of the agony can be assuaged if one at least knows that a s.o.p. $x_1, \ldots, x_n$ is a regular sequence on *some* R-module M (which is then called a big C-M module for R: "big", because M is not required to be finitely generated). The existence of such modules (which is an open question in mixed characteristic) seems to be the key to settling a whole slew of homological problems (see §4). Many of these problems were first suggested and explored by M. Auslander [$\mathbf{Au_1}$], [$\mathbf{Au_2}$], while the first real progress later was made by Peskine-Szpiro [$\mathbf{PS_2}$]. Now one can by and large recover the known results on these homological problems from the existence of big C-M modules in the equicharacteristic case (the case where R contains a field), and their existence in that case is the second main result we want to discuss: again, one uses the technique of passage to char $p > 0$. The explicit result is:

(1.2) THEOREM. *If R is a local ring which contains a field and $x_1, \ldots, x_n$ is a system of parameters, then there exists an R-module M such that $x_1, \ldots, x_n$ is a regular sequence on M.*

The reader is referred to [$\mathbf{Ho_5}$], [$\mathbf{Ho_8}$], [$\mathbf{Ho_9}$], [$\mathbf{Ho_{10}}$] for more information.

The rest of this paper explores insights into the uses of (1.1) and (1.2), gives sketches of parts of the ideas of their proofs, and surveys some related results and open questions. Since one main theme is "how to prove it" using the Frobenius in char p, we single out one consequence of (1.2) and give a detailed proof of it in char p (§4). In §3 we try to give some feeling for what rings of invariants of linearly reductive groups may be like, and also some insight into what it really means for a ring to be Cohen-Macaulay.

2. Artin approximation and a metatheorem for reduction to char p. In this section we describe and sketch the proof of a result which permits reduction of many problems for Noetherian rings which contain a field to the case of Noetherian rings finitely generated over a field of char $p > 0$. The most important tool is Artin approximation. Our result is expressed in terms of solvability of equations with a height condition.

If $I \subsetneq R$, a Noetherian ring, height I or ht I denotes

$$\min\{\dim R_P \colon I \subset P, P \text{ is prime}\}.$$

By a "system of equations with height condition" over a ring A we mean a set of polynomial equations:

$$\mathcal{E}\begin{cases} F_1(X, Y) = 0, \\ \quad \cdots \\ F_h(X, Y) = 0 \end{cases}$$

where $X = X_1, \ldots, X_n$, $Y = Y_1, \ldots, Y_q$, and the F's are polynomials in the variables X, Y with coefficients in A. If R is an A-algebra, we say that $x = x_1, \ldots, x_n, y = y_1, \ldots, y_q$ is a *solution* of $\mathcal{E}$ in R if

(1) height $\Sigma_i x_i R = n$, and

(2) $F_i(x, y) = 0$, $1 \leq i \leq h$.

Condition (1) is meant to imply, in particular, that $\Sigma_i x_i R \neq R$ (height $R = +\infty$, by convention). If $\Sigma_i x_i R \neq R$ then, by the Krull height theorem (see [$\mathbf{N_2}$, p. 26, Theorem (9.3)]), $ht \Sigma_i x_i R \leq n$. Condition (1) may be viewed as a sort of nondegeneracy condition on the x's.

We can now state:

(2.1) METATHEOREM. *Let $\mathcal{T}$ be a theorem about Noetherian rings which is* *true for finitely generated domains over finite fields.*

Suppose that $\mathfrak{T}$ *is equivalent to the statement that for a certain family* $\{\mathfrak{S}_\lambda\}_{\lambda\in\Lambda}$ *of systems of equations with height condition over* $\mathbf{Z}$ (n, q, *and* h *may vary with* λ), *no system in the family has a solution.*

Then $\mathfrak{T}$ *is true for all Noetherian rings R which contain a field, regardless of characteristic.*

We first remark that if a system $\mathfrak{S}$ has a solution in R and P is a minimal prime of $\Sigma_i x_i R$, then the images of x, y in R_P constitute a solution as well: moreover, the new values for the X_i are a system of parameters for the local ring R_P. By a local solution $x_1, \ldots, x_n, y_1, \ldots, y_q$ of a system $\mathfrak{S}$ we mean a solution in a (necessarily n-dimensional) local ring $(R, \mathfrak{m})$ such that $x_1, \ldots, x_n$ is a s.o.p. for $(R, \mathfrak{m})$. Since we may always pass from solutions to local solutions, the metatheorem follows from:

(2.2) THEOREM. *Let* $\mathfrak{S}$ *be a system of equations with height condition over* $\mathbf{Z}$. *Suppose that* $\mathfrak{S}$ *has a local solution in a local ring which contains a field. Then it has a solution in a domain R finitely generated over a finite field K, and also a local solution in* $R_\mathfrak{m}$ *for a maximal ideal* $\mathfrak{m}$ *of R such that* $R/\mathfrak{m} \cong K$.

We want to sketch the proof of this result (for more details see [**Ho**$_5$, Theorem 3.1], [**Ho**$_8$, Lemma 3], or [**Ho**$_9$, Theorem 5.2]). However, we first need to discuss completion of local rings, which is a major tool for making reductions in the theory of Noetherian rings. The trick of reducing first to the local and then the complete local case works remarkably often.

The point is that if $(R, \mathfrak{m})$ is local we may complete in the $\mathfrak{m}$-adic topology to obtain a new local ring $(\hat{R}, \hat{\mathfrak{m}})$, where $\hat{\mathfrak{m}} = \mathfrak{m}\hat{R}$ = the closure of $\mathfrak{m}$. In fact, we may complete any finitely generated R-module M and get a finitely generated $\hat{R}$-module $\hat{M}$ (which is $\cong \hat{R} \otimes_R M$). An alternative point of view is that $\hat{M} = \text{proj lim}_t\, M/\mathfrak{m}^t M$. The completion functor is faithfully exact on finitely generated R-modules. Moreover, $\dim \hat{R} = \dim R$. Of course, R may already be $\mathfrak{m}$-adically complete: in this case, we call R a *complete* local ring. We refer the reader to [**C**], [**N**$_2$], and [**ZS**] for further information.

The advantages of working over a complete local ring are enormous. For example, here is a weak form of a recent result from [**PP**] (long known in many special cases, e.g. for uncountable algebraically closed residue class fields) for solving equations over complete local rings:

(2.3) THEOREM (PFISTER-POPESCU). *Let* $\mathfrak{S}$ *be a system of polynomial equations over a complete local ring* $(R, \mathfrak{m})$. *Then* $\mathfrak{S}$ *has a solution in R if and only if* $\mathfrak{S}$ *has a solution modulo* $\mathfrak{m}^N$ *for all positive integers N.*

"Only if", of course, is trivial. "If" is a deep result utilizing the same circle of ideas needed to prove M. Artin's approximation theorem, which we discuss next.

Some of the best, most useful results in algebra make assertions of the following type: that once we have adjoined "a few" obviously needed quantities to our ring to serve as solutions to equations of a certain kind, we can actually solve a tremendous bunch of other equations as well. For example:

(1) Once an integral domain A has been enlarged to its fraction field K (i.e. throw in the solutions of the equations $bx = a$, a, $b \in A$, $b \neq 0$), any simultaneous system of linear equations which has a solution in some extension field has a solution in K.

(2) *The fundamental theorem of algebra.* Once we adjoin a solution of $x^2 = -1$ to the real numbers $\mathbf{R}$, every nonconstant polynomial equation in one variable has a root.

(3) *Hilbert's Nullstellensatz.* Once we enlarge a field K to its algebraic closure $\bar{K}$ (throw in all roots of single polynomial equations in *one* variable), then any *system* of polynomial equations

$$f_1(X_1, \ldots, X_n) = 0,$$
$$\ldots$$
$$f_h(X_1, \ldots, X_n) = 0$$

which has a solution in some extension field of K (equivalently, such that $1 \notin \Sigma_i f_i T$, where $T = K[X_1, \ldots, X_n]$) has a solution in $\bar{K}$. (See [$\mathbf{K_2}$] for a very simple proof when $\bar{K} = \mathbf{C}$.)

Our discussion of complete local rings indicated that one has a better theory for solving equations over $\hat{R}$ than over R, and it turns out to be important to study the question: for which R is it true that every finite system of polynomial equations over R with solutions in $\hat{R}$ has solutions in R? (Note that it is easy to see that if R has this property, then so does every local ring which is (a finite module over) a homomorphic image.) M. Artin has proved two beautiful and important theorems along these lines. Let us say that a local ring $(R, \mathfrak{m})$ is an approximation ring if it satisfies the following two equivalent conditions:

(1) Whenever a system of polynomial equations over R has a solution in $\hat{R}$, then it has a solution in R.

(2) If a system of polynomial equations over R has a solution $(s_1, \ldots, s_n)$ with the s_i in $\hat{R}$, then for every integer $t > 0$ there is a solution $(r_1, \ldots, r_n)$ with the r_i in R such that

$$s_i \equiv r_i \quad \text{modulo } \mathfrak{m}^t R, \qquad 1 \leqslant i \leqslant n.$$

(Thus, the solutions over R of a system over R are $\mathfrak{m}$-adically dense in the solutions over $\hat{R}$.)

The conditions (1) and (2) are equivalent because the extra congruence condition can be expressed by using auxiliary equations and unknowns.

The first of Artin's results [$\mathbf{Ar_1}$] is this:

(2.4) THEOREM (M. ARTIN). *Every analytic local ring is an approximation ring.*

By an *analytic* local ring we mean a homomorphic image of the convergent power series ring ${}_n\mathcal{O} = \mathbf{C}\{X_1, \ldots, X_n\} \subset \mathbf{C}[[X_1, \ldots, X_n]]$ for some n.

The result we really need here for the metatheorem, however, is a special case of an algebraic version of this theorem which Artin proves in [$\mathbf{Ar_2}$].

Let $R = K[X_1, \ldots, X_n]$ be a polynomial ring over a field K, let $\mathfrak{m} = \Sigma_i X_i R$, and let $A = R_{\mathfrak{m}}$. The special case of Artin's theorem we need tells us what the smallest approximation ring containing A is.

To describe this ring, let B be the integral closure of A in $\hat{A} = K[[X_1, \ldots, X_n]]$, i.e. B consists of all formal power series in the X_i which satisfy monic polynomials over A, let $q = \mathfrak{m}\hat{A} \cap B$, which is a maximal ideal of B, and let $A^h = B_q$. (Readers familiar with Henselization will recognize A^h as the Henselization of A: see [N_2].) Then:

(2.5) THEOREM (M. ARTIN). *A^h is an approximation ring.*

Clearly, A^h is the smallest ring which might work. We note that $(A^h, \mathfrak{m}A^h)$ is a local ring, that $\otimes_A A^h$ is faithfully exact, and that the completion of A^h is $\hat{A}$.

Theorem (2.5) falls into the classic pattern described earlier of adjoining a few solutions (the elements of $\hat{A}$ algebraic over A) and getting all one needs to solve any polynomial *system* which can be solved over $\hat{A}$.

(2.6). SKETCH OF THE PROOF OF THEOREM (2.2). We start with a local solution in a Noetherian ring R containing a field of char 0 (the char $p > 0$ case is much simpler: we leave it to the reader). By completing R we see that there is a solution in a complete local ring: moreover, we know that R is a finite module over $B = K[[x_1, \ldots, x_n]]$, a formal power series ring over a field, where the x_i are the values of the X_i (see [C], [N_2]). We may even enlarge K to be algebraically closed.

Let $T = K[x_1, \ldots, x_n]$, let $Q = \Sigma_i x_i T$, and $A = T_Q$, so that $\hat{A} = B$. The first important reduction is to obtain a local solution in an algebra which is a finite module over A^h (instead of over $\hat{A}$). The idea of the proof is simple: use Artin approximation (2.5) on the "algebra structure" of R as well as (simultaneously) on the local solution of the system of equations. (The algebra structure is given by a multiplication table for a finite basis.) The details are a bit messy and we omit them.

The next step is to use the fact that A^h is a direct limit of localizations of finitely generated K-algebras at maximal ideals to show that there is a solution in such a ring. It is then possible to "unlocalize", i.e. to pass to a solution in a finitely generated K-algebra: the condition that $x_1, \ldots, x_n$ be a s.o.p. is replaced by the weaker condition that $\mathrm{Rad}(\Sigma_i x_i R)$ be a maximal ideal of height n.

The rest of the argument is almost standard these days: certainly, it is an increasingly common motif. One can often make a reduction from the case of finitely generated algebras over fields of char 0 to those over fields of char $p > 0$: we refer the reader to [PS_2], [HR_1], and [HR_2] for further examples (and to [Bs_2] and its bibliography for examples outside commutative rings and algebraic geometry).

We complete our sketch of the proof of Theorem (2.2) with a brief outline of how such arguments usually run. One generally starts with a set-up (which may include K-algebras, modules, maps, schemes, sheaves, morphisms, etc.) "defined" over a field K of char 0. One then observes that everything in sight is, in fact, "defined" over a carefully chosen finitely generated $\mathbf{Z}$-subalgebra C of K (generated by coefficients of defining equations, etc.). One then uses facts like generic freeness (i.e. finitely generated modules E over finitely generated algebras over a Noetherian domain C have the property that E_c is C_c-free for suitable $c \neq 0$ in C, and more: see, for example, [HR_1, Lemma 8.1] and [$\mathbf{HR}_2$, Lemma 3.8]) closedness of bad (e.g. non-Cohen-Macaulay or singular) loci in schemes, etc. to show that after adjoining finitely many inverses for nonzero elements of C (the "new" C is still a finitely generated $\mathbf{Z}$-algebra) the result one wants to prove for K, if it fails, will also fail upon applying $\otimes_C C/m$ for any maximal ideal m of C. But C/m is a finite field! Q.E.D.

Note that certain facts which one has automatically in char 0 but not always in char p can often be preserved in passing to char p in this type of argument: it is almost as though one can assume both char 0 and char p simultaneously.

(2.7). REMARK. In a finitely generated $\mathbf{Z}$-algebra which contains $\mathbf{Z}$ only finitely many prime integers have inverses. Hence:

(2.8). *The conclusion of the Metatheorem* (2.1) *holds under the weaker hypothesis that* $\mathfrak{T}$ *is true for finitely generated domains over finite fields of* char $p > 0$ *for infinitely many* p.

(2.9). REMARK. Suppose that $\mathfrak{T}$ is a theorem of the type described in the second paragraph of the statement of the Metatheorem (2.1) Then:

(2.10). *If* $\mathfrak{T}$ *is true for domains finitely generated over a field or complete discrete valuation ring, then* $\mathfrak{T}$ *is true for all Noetherian rings.*

One proceeds exactly as in the proof (2.6) of Theorem (2.2). One completes, gets a local solution in a complete domain, which one represents as a finite module over a formal power series ring over a field or complete discrete valuation ring. One then uses the "mixed characteristic" algebraic form of Artin approximation [$\mathbf{Ar}_2$] to descend to a finitely generated V-algebra, just as in the proof of Theorem (2.2).

3. Cohen-Macaulay rings and invariant theory. The purpose of this section is to explain some of the consequences of Theorem (1.1). Part of our objective is to explain what it "really means" for a ring to be Cohen-Macaulay. Another part is to illustrate, by a substantial set of examples, what rings of invariants can be like. We shall see that Theorem (1.1) is naturally motivated even in terms of the goals of classical invariant theory.

In the sequel we assume, for simplicity, that K is an algebraically closed field. Let G be a linear algebraic group, i.e. a subgroup of some $\mathrm{Gl}(n, K)$ which is defined by the condition that the entries of the matrices $A = (a_{ij})$ in G satisfy certain polynomial equations over K (e.g. $\mathrm{Sl}(n, K)$ is defined by $\det A = 1$). By a K-rational representation of G on V, where V is a finite-dimensional K-vector space, we mean a group action $G \times V \to V$ in the usual sense which is also a K-morphism of varieties (equivalently, the induced map $G \to \mathrm{Gl}_K(V)$ is both a group homomorphism and a K-morphism of varieties). If V is infinite-dimensional, we mean that V is a directed union of finite-dimensional subspaces W stable under G such that the action of G on each W is K-rational. If G acts K-rationally on V, we also say that V is a *G-module*. When R is a K-algebra and G acts on R, we tacitly assume that G acts by K-algebra automorphisms, so that we may speak of the *fixed ring* R^G (in general, V^G is just a vector space). See [**Bor**], [**DC**], [$\mathbf{Mu}_1$], [$\mathbf{N}_1$], and [$\mathbf{N}_3$] for further details.

The main case occurs when G acts linearly on the polynomial ring in n

variables over K (to give such an action is the same as to give an action of G on the vector space of forms of degree one). Hilbert's fourteenth problem, while phrased somewhat more generally, is basically motivated by the question of whether, in this situation, R^G must be finitely generated (cf. [DC], [$\mathbf{Mu_3}$], and [$\mathbf{N_3}$]). We shall return to this question later.

When it does happen that R^G is finitely generated, there are two fundamental problems (in the terminology of [Weyl]): first, determine generators $u_1, \ldots, u_m$ of R^G as a K-algebra, and, second, determine a finite set of generators for the ideal of algebraic relations on $u_1, \ldots, u_m$ (R^G is usually not a polynomial ring itself). Of course, one can ask many other questions.

To give some feeling for these problems, we consider a number of examples:

EXAMPLE 1. Let $R = K[x_1, \ldots, x_r, y_1, \ldots, y_s]$ and let $G = G_m$. Let G act on R by a: $(x_1, \ldots, x_r, y_1, \ldots, y_s) \mapsto (a^{-1}x_1, \ldots, a^{-1}x_r, ay_1, \ldots, ay_s)$. Then $R^G = K[x_iy_j]_{i,j}$. If $r, s > 1$ then these generators are not algebraically independent. In fact if $U = (u_{ij})$ denotes a new $r \times s$ matrix of indeterminates and we map $K[U] \twoheadrightarrow R^G$ by $u_{ij} \mapsto x_iy_j$ the kernel is $I_2(U)$. Here, for any matrices $U_1, \ldots, U_r$, $K[U_1, \ldots, U_r]$ denotes the K-algebra generated by the entries of the U_i, and for any matrix U, $I_t(U)$ is the ideal generated by the $t \times t$ minors (subdeterminants) of U.

We can generalize this example in two ways:

EXAMPLE 2. Let $R = K[X, Y]$, where X, Y are $r \times t$ and $t \times s$ matrices of indeterminates, resp., and let $G = \mathrm{Gl}(t, K)$ act by A: $(X, Y) \mapsto (XA^{-1}, AY)$. The preceding example is the case $t = 1$. Then $R^G = K[XY]$ and if we map $K[U] \twoheadrightarrow K[XY]$ (where U is a new $r \times s$ matrix of indeterminates), the kernel is $I_{t+1}(U)$. Cf. [Weyl], [HE], and [DPr].

EXAMPLE 3. Let $R = K[x_1, \ldots, x_n]$ and let $G = G_m^r$, an algebraic torus. Suppose that G acts on R so that $(a_1, \ldots, a_r)$: $(x_1, \ldots, x_n) \mapsto (a_1^{t_{11}}a_2^{t_{21}} \cdots a_r^{t_{r1}}x_1, \ldots, a_1^{t_{1n}}a_2^{t_{2n}} \cdots a_r^{t_{rn}}x_n)$. Then the ring of invariants is spanned as a K-vector space by all monomials $x_1^{h_1} \cdots x_n^{h_n}$ such that $(h_1, \ldots, h_n)$ is a nonnegative integer solution of the linear homogeneous system:

$$\sum_{j=1}^{n} t_{ij}h_j = 0, \qquad 1 \leqslant i \leqslant r.$$

It is not hard to exhibit generators for the algebraic relations (see [$\mathbf{Ho_1}$], [KKMS]).

EXAMPLE 4. Let $R = K[x_1, x_2]$ and let G_1 be generated by $(x_1, x_2) \mapsto (x_1, -x_2)$ and $(x_1, x_2) \mapsto (-x_1, x_2)$ (assume char $K \neq 2$), so that $G_1 \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2$. Let $G_2 \cong \mathbf{Z}_2$ be the subgroup spanned by $(x_1, x_2) \mapsto (-x_1, -x_2)$. Then $R^{G_1} = K[x_1^2, x_2^2]$, a polynomial ring, while $R^{G_2} = K[x_1^2, x_1x_2, x_2^2]$.

This illustrates the following theorem [ST]: if we identify the linear automorphisms of $R = \mathbf{C}[x_1, \ldots, x_n]$ with $\mathrm{Gl}(n, \mathbf{C})$, and G is a finite subgroup of $\mathrm{Gl}(n, \mathbf{C})$, then R^G is always finitely generated, but R^G is a polynomial ring if and only if G is generated by pseudoreflections (a matrix A is a pseudoreflection if it is conjugate to a diagonal matrix in which one diagonal entry is a root of unity and the other entries are all equal to one).

A tremendous amount is known about the finite group case (R^G is always finitely generated, even if char K divides $|G|$), and even more is known when

$|G|$ is invertible in K. E.g. in the case of a linear action the formal power series $\Sigma_i(\dim_K[R^G]_i)z^i$ which "summarizes" the vector space dimensions of the graded pieces $[R^G]_i$ of R^G is equal to $(1/|G|)\Sigma_{A\in G}1/\det(1 - zA)$ (Molien's formula: see [Mol]).

EXAMPLE 5. Let $G = \mathrm{Sl}(r, K)$ act on $R = K[X]$, where X is an $r \times s$ matrix of indeterminates, by A: $X \mapsto AX$. Then $R^G = K[\bigwedge^r X]$, the ring generated by the $r \times r$ minors of X. This ring is familiar to algebraic geometers as the usual homogeneous coordinate ring for the Grassmann variety of affine r-dimensional vector subspaces of affine s-space. (The relations on the minors are well known: they are the quadratic Plücker relations. See [HP].) Cf. [Ho_4], [Lk], and [Mus].

EXAMPLE 6. Assume char $K = 0$. Consider the same representation as in Example 5, but now let $G = O(r, K)$, the orthogonal group, act. Let $'$ denote "transpose". Then $K[X]^G = K[X'X]$ (cf. [Weyl]), and if U is a *symmetric* $s \times s$ matrix of indeterminates, then $\mathrm{Ker}(K[U] \twoheadrightarrow K[X'X])$ is $I_{r+1}(U)$. See [Ku].

EXAMPLE 7. Let $G = \mathrm{Gl}(n, K)$, and let $R = K[X_1, \ldots, X_m]$, where each X_i is an $n \times n$ matrix of indeterminates. Let $A \in G$ act by $(X_1, \ldots, X_m) \mapsto (AX_1A^{-1}, \ldots, AX_nA^{-1})$. Then any monomial $Y = X_{i_1}^{t_1} \cdots X_{i_k}^{t_k}$ is mapped to AYA^{-1} and hence the coefficients of the characteristic polynomial of any such Y are fixed by G. These coefficients generate R^G. (In char 0, the traces of these monomials are enough.) The relations may also be described: see [Pr].

The reader may have gained the impression from these examples that R^G is always finitely generated. The first counterexample was given by Nagata: see [N_3]. Finite generation can fail, in char 0, even if (in fact, especially if) G is a direct sum of copies of the additive group of K. However, for a very important class of groups, the reductive groups, finite generation holds. This has been known for a long time in char 0 but is a quite recent result (a consequence of Haboush's proof of Mumford's conjecture) in char p.

Recall that a connected group G is *reductive* if its radical, i.e. its maximal normal connected solvable subgroup, is an algebraic torus. This is equivalent to asserting that modulo a finite subgroup, G is the product of a semisimple group (radical trivial) and an algebraic torus. In char 0, reductive and linearly reductive (every representation is completely reducible) are equivalent notions, and this is what makes the proof of finite generation relatively easy. However, in char p, there are almost no such groups: the only connected ones are tori. To remedy the situation, one wants a representation-theoretic property weaker than complete reducibility which is still strong enough to imply finite generation.

With this in mind, let us examine the notion of linear reductivity a bit more closely. We first note that G is linearly reductive if and only if whenever $V \twoheadrightarrow W$ is a surjection of G-modules, then $V^G \to W^G$ is also surjective. If G is finite and $|G|$ is invertible in K, it is easy to see that this surjectivity property holds: if $v \mapsto w$ and $w \in W^G$, then $(1/|G|)\Sigma_{g\in G}g(v) \in V^G$ and maps to w. The key point is that there is a natural retraction operator ρ: $V \twoheadrightarrow V^G$. If G is a compact real Lie group one can also average, and the existence of a similar natural retraction $V \twoheadrightarrow V^G$, the Reynolds operator, after complexifying, may be viewed as an instance of the inertia of truth. In any case, it is not hard to show that G is linearly reductive if and only if there is a natural G-module retraction ρ_V: $V \twoheadrightarrow V^G$ for all G-modules V. An apparently weaker but still equivalent statement is that if K is the trivial G-module and f: $V \twoheadrightarrow K$ is a G-module surjection, then there is an invariant element $v \in V$ such that $f(Kv) = K$ (i.e. $V^G \to K^G = K$ is surjective).

Let $S_K^n(V)$ denote the nth symmetric power of the vector space V over K. Mumford conjectured that the following weakening of the last characterization of linear reductivity would hold for reductive groups in char $p > 0$: If K is given the trivial G-module structure and $V \twoheadrightarrow K$ is a surjection of G-modules (V finite-dimensional), then for some positive integer e, if $n = p^e$, the map $S_K^n(V)^G \to S_K^n(K)^G = K$ is surjective. If G has this property it is called "geometrically reductive", and so Mumford's conjecture can be reformulated as asserting that reductive groups are geometrically reductive. Moreover, one can reduce at once to the semisimple case. Nagata had shown quite some time ago (cf. [N_3]) that if G is geometrically reductive and acts on a finitely generated K-algebra R, then R^G is finitely generated. Finally, Haboush [**Ha**] proved Mumford's conjecture, thereby getting invariant theory really going in char p. We note that in our earlier examples, the groups G were all reductive.

We now consider briefly again the first and second fundamental problems of invariant theory with the idea of relating them to the question of whether rings of invariants are Cohen-Macaulay. Assume then that R is a polynomial ring, that G is a linear algebraic group acting linearly, and also that R^G is finitely generated (which will be true if G is reductive). The first fundamental problem was then to give explicit generators, which is equivalent to giving an explicit K-homomorphism of a polynomial ring S over K onto R^G. The second fundamental problem is to find generators for the ideal I of "relations" on the algebra generators, which is equivalent to giving explicitly an exact sequence of S-modules:

$$S^{n_1} \to S \to R^G \to 0,$$

where the images of the free generators for S^{n_1} are the specified generators of I. Call these generators of I $i_1, \ldots, i_{n_1}$. Then, in the same vein, we can ask for S-module generators for the module of S-relations (or syzygies) on $i_1, \ldots, i_{n_1}$, i.e. n_1-tuples $(s_1, \ldots, s_{n_1})$ such that $\Sigma_j s_j i_j = 0$. This amounts to explicitly extending the former exact sequence to an exact sequence:

$$S^{n_2} \to S^{n_1} \to S \to R^G \to 0,$$

and this may be construed as a "third fundamental problem". In a precisely similar fashion there are fourth, fifth, sixth, etc. fundamental problems, and a kind of overall fundamental problem, to wit, determine an explicit free resolution of R^G as an S-module. We recall at this point that by Hilbert's syzygy theorem, at some point $\operatorname{Ker}(S^{n_{i+1}} \to S^{n_i})$, the $(i + 1)$th module of syzygies of R^G, is itself projective ($\Leftrightarrow$ free in the polynomial ring case), and so there exists a shortest free resolution:

$$0 \to S^{n_r} \to \ldots \to S^{n_2} \to S^{n_1} \to S \to R^G \to 0.$$

While one would, of course, like to know the whole resolution, several more modest goals suggest themselves. For example, it is not at all obvious that the length r of a shortest projective (i.e. free) resolution of R^G over S will be. This number tells us where the sequence of fundamental problems ends. We denote the length of a shortest projective resolution of M over S by $\mathrm{pd}_S M$. Now, general theorems from commutative rings assert that

$$\mathrm{pd}_S R^G \geqslant \dim S - \dim R^G.$$

When does equality hold? The answer is, precisely when R^G is Cohen-Macaulay!

Thus, Theorem (1.1) tells us that if G is linearly reductive then when R^G, R regular, is represented as a homomorphic image of a polynomial ring S, the sequence of fundamental problems stops at the earliest possible point: $r = \dim S - \dim R^G$.

To bring all this down to earth, let us consider a specific

EXAMPLE. Let X and Y be as in Example 2 (or Example 1) with $r = 2$, $s = 3$, and $t = 1$, and let $R = K[X, Y]$ so that $R^G = K[XY] \cong K[U]/I_2(U)$. Let $S = K[U]$. Then we should have $\mathrm{pd}_S R^G = \dim S - \dim R^G = 6 - 4 = 2$ if R^G is Cohen-Macaulay, and, indeed, the resolution is

$$0 \to S^2 \xrightarrow{U} S^3 \xrightarrow{D} S \to R^G \to 0,$$

where D may be identified with $\bigwedge^2 U'$, the matrix whose entries are the 2×2 minors of U.

It has been a longstanding problem to resolve explicitly $R^G = K[U]/I_{t+1}(U)$ over $K[U]$ in the general situation of Example 2. The complete answer is still not known if char $K = p$ (see [EN], [GN], [Po] for special cases), but there has been a quite recent breakthrough [Las] in char 0, and the resolution in that case is now known.

The rest of this section is devoted mostly to the objective of giving insight into the Cohen-Macaulay property. Of course, each result about C-M rings we mention is yet another fact about rings of invariants of linearly reductive groups acting on regular rings. We begin with a sequence of examples of individual rings and classes of rings which are C-M, as well as others which are not. Incorporated into some examples are various comments upon, observations about, and characterizations of the Cohen-Macaulay property.

EXAMPLE A. 0-dimensional rings. All 0-dimensional Noetherian rings are Cohen-Macaulay.

EXAMPLE B. 1-dimensional rings. All 1-dimensional local rings without nilpotents are C-M. $K[x, y]/(y^2)$ is C-M, while $K[x, y]/(x^2, xy)$ is not.

Several comments are in order here. Cohen-Macaulayness is often the right hypothesis for extending a theorem about (reduced) curves to higher dimension (without bringing spectral sequences into the picture). A good example is the simple form which Serre-Grothendieck duality for locally free coherent sheaves takes on Cohen-Macaulay projective varieties: see [AK].

The fact that $K[x, y]/(x^2, xy)$ is not C-M is tied in with the fact that the ideal (0) is mixed in this ring (corresponding to the fact that (x^2, xy) has an embedded prime in its primary decomposition: $(x^2, xy) = (x) \cap (x^2, y)$). This cannot happen in a C-M ring. Since embedded primes are hard to interpret in a classical geometric sense, the C-M property will tend to imply that the geometry in many situations is a good reflection of what is happening algebraically. Unmixedness was a major concern of Macaulay [**Mac$_1$**], who was amazingly far ahead of his time.

EXAMPLE C. 2-dimensional rings. All 2-dimensional normal Noetherian domains are C-M, where "normal" means integrally closed in its fraction field. Neither of the nonnormal rings $K[x^2, x^3, y, xy]$, $K[x^4, x^3y, xy^3, y^4]$ (both subrings of $K[x,y]$) is C-M [note the relation $xy(x^2) = x^3(y)$ (resp. $(xy^3)^2x^4 = (x^3y)^2y^4$) which implies that x^2, y (resp. x^4, y^4) is not a regular sequence]. On the other hand the nonnormal 2-dimensional ring $K[x^2, x^3, y]$ is C-M.

Normality plays a crucial role in algebraic geometry, both in understanding maps as in Zariski's Main Theorem (see [**R**], [**Z$_2$**]) and in the study of resolution of singularities (see, e.g. [**Ab**], [**Z$_1$**]). An important point is that if R is C-M then R is normal if and only if the singular locus has codimension at least 2. (In the general case what one needs is that the ideal defining the singular locus is either the unit ideal or contains a regular sequence of length 2. But this is hard to check if one does not know the ring is C-M.)

As we shall see shortly below, normality (even unique factorization) does not guarantee that the ring will be Cohen-Macaulay in higher dimensions.

In connection with checking Cohen-Macaulayness in graded rings like those above, we mention the following criterion: suppose that S is a finitely generated graded K-algebra with $S_0 = K$. Then S can always be represented as finite module over a "polynomial" subring, i.e. a K-subalgebra R generated by dim S algebraically independently forms of positive degree. Whenever this is done, S is C-M if and only if S is R-free (the same holds if S is a local ring which is a finite module over a regular local subring R). From this point of view, $K[x^2, x^3, y, xy]$ is not C-M because if we take $R = K[x^2, y]$ then $1, x^3, xy$ is a minimal homogeneous basis but not a free basis. (The local freeness of S over R, R regular, S module-finite, may be thought of somewhat more geometrically as the fact that the scheme-theoretic fibers of the finite morphism Spec $S \to$ Spec R all have the same length.)

EXAMPLE D. Complete intersections. The following fact characterizes C-M rings: if $x_1, \ldots, x_n$ is a sequence such that for each i, $1 \leqslant i \leqslant n$, x_i is not in any *minimal* prime of $\sum_{j<i} x_jR$, then $x_1, \ldots, x_n$ is a regular sequence. Moreover if R *is* C-M and $x_1, \ldots, x_n$ satisfies the above condition, then $R/\sum_{i=1}^n x_iR$ is again C-M. In particular, if R is regular local and $x_1, \ldots, x_n$ is part of a s.o.p., then $R/\sum_i x_iR$ is C-M. These rings are called (local) complete intersections. Such rings are, in fact, Gorenstein (which means that they have finite injective resolutions as modules over themselves). If S is regular local, it turns out that S/I is Gorenstein if and only if it is C-M and its minimal projective resolution over S is isomorphic to its own dual (into S). See [**Bs$_1$**] and [**K$_1$**]. Gorenstein rings come in handy in duality theory [**GH**].

EXAMPLE E. Determinantal loci. Let R be a C-M ring and (x_{ij}) an r by s matrix with entries in R. Suppose that $I_{t+1}(x_{ij})$ has height $\geqslant (r-t)(s-t)$. Then it has height exactly $(r-t)(s-t)$ and $R/I_{t+1}(x_{ij})$ is again C-M. See [**HE**]. We note that this "biggest possible height" $(r-t)(s-t)$ for $I_{t+1}(x_{ij})$ is achieved when the x_{ij} are indeterminates over a field or **Z** and R is the polynomial ring generated by the indeterminates.

If R is a regular local ring and I has height two and is such that R/I is C-M, then, conversely, I must be determinantal: in fact, I is the ideal of $r \times r$ minors of an $r \times r + 1$ matrix with entries in the maximal ideal of R, where $r + 1$ is the minimum number of generators of I. No such classification is known for height three ideals with C-M quotients. They are not all determinantal.

Note that complete intersections are determinantal with $r = 1, t = 0$.

EXAMPLE F. Generic families of loci. Let A be a regular Noetherian domain and J an ideal of height d such that A/J is C-M. Let $\phi: A \to R$ be any ring homomorphism into a C-M ring R and let $I = \phi(J)R$. Suppose that I has height $\geqslant d$. Then I has height exactly d, and R/I is again C-M. Thus, any ideal J in A such that A/J is C-M defines a whole family of C-M rings which, in some sense, have the same "form" as J. Example E is the special case where $A = \mathbf{Z}[x_{ij}]$ and $J = I_{t+1}(x_{ij})$.

By Theorem (1.1), whenever we solve the first and second fundamental problems for a linearly reductive group acting on a regular ring, we obtain a generic family of this sort. Cf. **[HE]**.

EXAMPLE G. Unique factorization. For a while, no examples were known of UFD's which are not C-M. There is one interesting positive result along these lines (Raynaud-Boutot): if R is a *complete* local UFD with an *algebraically closed* residue class field of char *zero*, and dim $R \leqslant 4$, then R is C-M. See **[Lip]** as well as **[Bou$_2$]** and **[HO]** (where the same result is obtained in a slightly more restricted setting). On the other hand, since the question was raised in **[Sam]** there have been several counterexamples.

The first was given in **[Bt]**. Let S be the polynomial ring in four variables over a field of char 2 and let $\mathbf{Z}_4$ act by cyclically permuting the variables. Then the ring of invariants R is a four-dimensional non-C-M UFD. A three-dimensional example is derived from this in **[Ho$_{14}$]**, and many related examples are pointed out in **[HR$_1$]**. **[FG]** shows that some of these char p examples may be completed. The first counterexample in char 0 is analytic **[FK]** (but Artin approximation shows that the completion of this 60-dimensional analytic local ring is also a counterexample). Many other counterexamples in char 0 may be found in **[Mo]**.

A very interesting fact is that the ring of invariants in the example **[Bt]** is also the ring of invariants of a connected semisimple group acting linearly on a polynomial ring: a trick for doing this was pointed out to the author in correspondence by R. Richardson. Hence, Theorem (1.1) is false for connected reductive groups in char $p > 0$!

EXAMPLE H. Rings associated with simplicial complexes. Let K be a field and let Δ be an abstract finite simplicial complex with vertices $x_1, \ldots, x_n$. Regard the x's as indeterminates over K and let $S = K[x_1, \ldots, x_n]$. Let I_Δ be the ideal spanned as a K-vector space by the monomials in the x's such that the set of variables which occur in the monomials is *not* a face of Δ. (In case $K = \mathbf{R}$, Δ may be recovered from $K[\Delta]$ as the intersection of the corresponding variety in $\mathbf{R}^n$ with the convex hull of the standard basis.) G. Reisner has shown that $K[\Delta]$ is C-M if and only if for Δ itself and all links L of Δ, the reduced (simplicial) cohomology with coefficients in K vanishes except in the top dimension [**Rei**]. Moreover, it is easy to see (as observed by Munkres) that this property is a topological invariant. R. Stanley [**$\mathbf{St_1}$**], [**$\mathbf{St_2}$**], using Reisner's result, proved that any triangulation of a sphere satisfies the Upper Bound Conjecture in combinatorics (which gives conjectured upper bounds for the numbers of faces of various dimensions in a triangulation of a d-sphere which has n vertices). The point is that Macaulay gave [**$\mathbf{Mac_2}$**] certain inequalities which the Hilbert function of C-M graded K-algebra must satisfy. These inequalities, applied to the Hilbert function of $K[\Delta]$, imply the Upper Bound Conjecture. We refer the reader to [**MS**], where the problem was first solved for convex polytopes, for further background.

To illustrate Reisner's criterion we note the following examples:

(0) If $\dim \Delta = 0$, $K[\Delta]$ is C-M.

(1) If $\dim \Delta = 1$, $K[\Delta]$ is C-M if and only if $|\Delta|$ is connected.

(2) If $\dim \Delta = 2$, $K[\Delta]$ is C-M if and only if $|\Delta|$ is connected, $H^1(\Delta) = 0$, and the link of each vertex is connected. If Δ is the union of two 2-simplices with one vertex in common, then $K[\Delta]$ is not C-M. If $|\Delta|$ is a connected two-manifold (possibly with boundary) then $K[\Delta]$ is C-M if and only if $H^1(\Delta) = 0$. A circular cylinder cannot have a C-M $K[\Delta]$. But if Δ is a triangulation of a real projective plane, then $K[\Delta]$ is C-M if and only if $\operatorname{char} K \neq 2$.

The reader might also wish to consult the exposition in [**$\mathbf{Ho_{12}}$**]. One interesting point is that the proofs in [**Rei**] involve the action of Frobenius on local cohomology and reduction to $\operatorname{char} p > 0$ (the circle of ideas of [**$\mathbf{HR_1}$**], [**$\mathbf{HR_2}$**]).

Example I. Cohen-Macaulay rings and vanishing of cohomology on projective varieties. Here, we need to assume some slight familiarity with sheaf cohomology of coherent sheaves on projective varieties (Čech cohomology in the Zariski topology): see [**$\mathbf{S_2}$**]. However, we shall try to be as self-contained as possible. Let $R = \bigoplus_{i=0}^{\infty} R_i$ be a finitely generated graded K-algebra with $R_0 = K$ such that R_1 generates R. Then there is a projective scheme $(X, \mathcal{O}_X) = \operatorname{Proj} R$ associated with R and a very ample sheaf $\mathcal{O}_X(1)$. While X does not determine R, given a projective embedding $X \hookrightarrow \mathbf{P}^n$, if X is reduced we may find one such R: $R = K[x_0, \ldots, x_n]/I$, where I is the ideal generated by the homogeneous polynomials which vanish at all points of X. In this case the corresponding $\mathcal{O}_X(1)$ is the pullback of the hyperplane section bundle on $\mathbf{P}^n$, i.e. the unique very ample invertible sheaf on $\mathbf{P}^n$ which generates $\operatorname{Pic} \mathbf{P}^n$. $\mathcal{O}_X(t)$ denotes $\mathcal{O}_X(1)^{\otimes t}$.

By Serre's results [**$\mathbf{S_1}$**], if $\dim R \geqslant 2$, R is Cohen-Macaulay if and only if the following two conditions hold:

(1) The natural map $R \to \bigoplus_{t \in \mathbf{Z}} H^0(X, \mathcal{O}_X(t))$ is bijective, and

(2) $H^i(X, \mathcal{O}_X(t)) = 0$, $1 \leqslant i < \dim X$, $t \in \mathbf{Z}$.

In particular, if R is C-M, $H^i(X, \mathcal{O}_X) = 0$, $1 \leqslant i < \dim X$. Moreover, (1) is automatic if R is normal, while if R is a UFD, every invertible sheaf on X is of the form $\mathcal{O}_X(t)$ for some t. Hence, if R is a UFD, R is C-M if and only if for every invertible sheaf $\mathcal{L}$ on X, $H^i(X, \mathcal{L}) = 0$, $1 \leqslant i < \dim X$.

When G is semisimple and acts linearly on a polynomial ring S, S^G is a UFD (cf. [**$\mathbf{HR_1}$**]). It follows (considering Example 5) that all invertible sheaves on the Grassmann varieties have vanishing cohomology in the intermediate dimensions.

It follows (cf. [Ch], [HR$_1$, §14]) also that if C is a smooth projective curve of genus $g \geqslant 1$ then $X = C \times \mathbf{P}^1$ cannot have a C-M homogeneous coordinate ring. For $\dim X = 2$ and $H^1(X, \mathcal{O}_X)$ would have to vanish, while by the Künneth formula it turns out to be

$$H^1(C, \mathcal{O}_C) \otimes_K H^0(\mathbf{P}^1, \mathcal{O}_{\mathbf{P}^1}) \cong H^1(C, \mathcal{O}_C) \cong K^g \neq 0.$$

E.g. let $R = K[X_1, X_2, X_3]/(X_1^3 + X_2^3 + X_3^3) = K[x_1, x_2, x_3]$ (char $K \neq 3$), which is a homogeneous coordinate ring for an elliptic curve C. If y_1, y_2 are new indeterminates, let $S = R[y_1, y_2]$ and $T = K[x_iy_j]_{i,j} \subset S$, where $1 \leqslant i \leqslant 3$, $1 \leqslant j \leqslant 2$. Then T is a homogeneous coordinate ring for $C \times \mathbf{P}^1$ and thus not C-M. Note that T has an isolated singularity at the origin and is normal. In fact, $T = S^G$, where $G = G_m$ acts on S by a: $(x_1, x_2, x_3, y_1, y_2) \mapsto (ax_1, ax_2, ax_3, a^{-1}y_1, a^{-1}y_2)$. Hence a ring of invariants of a torus acting on a C-M ring (even a hypersurface) need not be C-M! This shows that the hypothesis that R be regular in Theorem (1.1) cannot be weakened too much.

This concludes our list of classes of examples of C-M and non-C-M rings. However, by way of attempting to explain more of the geometric consequences of the Cohen-Macaulay property, we shall discuss its significance in the theory of intersection multiplicities. We refer the reader to [S$_4$], [Weil], [Mu$_4$], [N$_2$], [ZS], [AB$_3$], [AR], [Mal$_1$], [Mal$_2$], and [PS$_3$] for further information.

Let X and Y be (for simplicity) irreducible closed affine varieties in $\mathbf{A}^n$ (although the results are essentially the same in any smooth ambient space) having the origin $x = (0, \ldots, 0)$ as an isolated point of intersection. For convenience we also assume that $\dim X + \dim Y = n$ ($\leqslant n$ is automatic); if $\dim X + \dim Y < n$ the multiplicity we are defining turns out to be zero. Let R denote the local ring of $\mathbf{A}^n$ at the origin x and let I, J be the images of the defining ideals of X, Y resp. in R. Thus, R/I, R/J are the local rings of X, Y resp. at x. We want to define the intersection multiplicity $i_x(X, Y)$ of X and Y at x. We note that the fact that x is isolated in the intersection is equivalent to the fact that $l(R/I + J)$ is finite, where l denotes length (of a filtration in which all factors are $\cong K$) and is the same as vector space dimension over K when R contains a copy of its residue class field K (which is true in this case). Also note that $R/I + J \cong (R/I) \otimes_R (R/J)$.

Before proceeding further with the general case we stop to consider the situation when we intersect a curve and a line in the plane.

In fact, consider the intersection of $Y = X^2$ and $Y = 0$ in $\mathbf{A}^2$. Two methods of defining the intersection multiplicity suggest themselves. One depends on noticing that when we shift $Y = 0$ slightly to $Y = c$, $c \neq 0$, we get two points of intersection (char $K \neq 2$), and then concluding that when $c = 0$ the intersection multiplicity still ought to be two. Note that what we are doing is counting the number of points in a set-theoretic fiber of the mapping from $Y = X^2$ to $\mathbf{A}^1$ obtained by restricting the function given by Y on $\mathbf{A}^2$ to the curve, excluding the fiber over the origin in $\mathbf{A}^1$.

A somewhat different point of view is to calculate the intersection "algebraically" (i.e. scheme-theoretically) by simply killing both defining equations and localizing (although localizing turns out not to be necessary in this case): we get $K[X, Y]/(Y - X^2, Y) = K + K\bar{X}$ (where $\bar{X}^2 = 0$). The fact that $\bar{X}$ lives in the intersection corresponds to the geometric fact that $Y = X^2$ and $Y = 0$ have more in common than a point at the origin: they have a tangent direction in common. In any case, one is led to attempt to define multiplicity in this case as $l(K + K\bar{X}) = 2$. [Note that if $c \neq 0$,

$$K[X, Y]/(Y - X^2, Y - c) \cong K[X]/(X^2 - c)$$

also has length 2: here, the length reflects the fact that there are two points of intersection.]

Both ideas for computing multiplicities generalize easily to higher dimensions: but they give different answers (for curves they agree). First note that one can reduce the problem of defining multiplicities to the case where Y is linear, by regarding the problem of intersecting X and Y as isomorphic with the problem of intersecting $X \times Y$ with $\Delta_{\mathbf{A}^n}$ in $\mathbf{A}^n \times \mathbf{A}^n \cong \mathbf{A}^{2n}$: the diagonal $\Delta_{\mathbf{A}^n}$ is a linear subvariety.

Now suppose X, Y are in $\mathbf{A}^n$ and that Y is linear. Suppose $\dim X = d$, $\dim Y = n - d$, and let $L_1, \ldots, L_d$ be linear forms which define Y. Then, proceeding by analogy with the curve case, we can map $X \to \mathbf{A}^d$ by $p \mapsto (L_1(p), \ldots, L_d(p))$. Near the origin in $\mathbf{A}^d$ this map is finite-to-one and off a proper subvariety of $\mathbf{A}^d$ the set-theoretic fibers have constant cardinality. It is this number that we want for the multiplicity.

On the other hand, we can kill both sets of defining equations in the local ring and compute $l((R/I) \otimes_R (R/J))$.

The answer obtained this way is not usually the same as the cardinality of the typical fiber of the linear projection. It is this cardinality which one wants for the multiplicity.

One is then led to ask, for which X and Y do the "multiplicities" computed in these two different ways agree? (Y is no longer necessarily linear now.) The answer is, if and only if both X and Y are Cohen-Macaulay!

In particular, in the case where Y is linear ($\Rightarrow$ C-M) X is Cohen-Macaulay if and only if the two versions of multiplicity agree.

Finally, we note that Serre [S4] "corrects" the single term $l((R/I) \otimes_R (R/J))$ by using instead the Euler characteristic of Tor, to wit, $\Sigma_j(-1)^j l(\mathrm{Tor}_j^R(R/I, R/J))$. Thus

$$l\big(\mathrm{Tor}_0^R(R/I, R/J)\big) = l\big((R/I) \otimes_R (R/J)\big)$$

is just a "first approximation". This Euler characteristic is Serre's definition of multiplicity. It turns out to agree with the cardinality of the typical fiber in the linearized set-up, but, as we shall see in the next section, makes sense in a much broader context.

The point about Cohen-Macaulayness is that it makes the higher Tor's vanish!

[COMMENT. We have been remiss in not observing what the multiplicity is in the simplest and most natural case of all: suppose C_1, C_2 are irreducible curves in $\mathbf{A}^2$ having x as an isolated point of intersection, that C_i has m_i tangents (i.e. the lowest degree form of the defining equation of C_i written with x as the origin is m_i) and C_1, C_2 have no common tangent. Then

$i_x(C_1, C_2) = m_1m_2$. If C_1 and C_2 have a common tangent, then $i_x(C_1, C_2) > m_1m_2$. See [**Fu**] for an elementary discussion.]

We next want to make some remarks about the proof of Theorem (1.1). The idea is to use local cohomology (see [**GH**], [**HR$_1$**], [**HR$_2$**], [**HS**], [**PS$_2$**] and [**Sh**]) to compute the obstruction to Cohen-Macaulayness. The key point is to exploit the fact that the Frobenius acts on the local cohomology of a local ring (support at the closed point) in char p! (See [**PS$_2$**] and [**HS**]. The expository paper [**Bou$_1$**] may be helpful.) We shall not give any details here (the reader can find them in [**HR$_1$**]). However, we do want to put forth some observations.

The most obvious point is that Theorem (1.1) is primarily a char 0 theorem, since there are so few linearly reductive groups in char p, and the result is false for reductive groups in char p. However, by "semistandard tricks" in the circle of ideas mentioned in the last part of (2.6) one can pass to char p and get a contradiction. It's actually quite a bit more subtle than the kind of situation to which the Metatheorem (2.1) applies directly, but the principle is the same. The difficulty is that one starts in char 0 knowing that the ring of invariants is a direct summand as a module over itself of the original (regular) ring, but it does not seem possible to preserve this while passing to char p. Instead, one uses various tricks to show that there is a sort of minimal counterexample in a graded situation, and then, working with one graded piece at a time, one passes to char p while preserving "finitely many consequences" of the existence of the Reynolds operator in char 0.

Oddly enough, the only way the regularity comes in is that in char p, if R is regular, the Frobenius $F: R \to R$ makes R into a flat algebra over itself. (But this actually characterizes regularity!) The ring $T = K[x_iy_j] = S^G$ considered in Example I above shows that it is not enough to assume that S is C-M rather than regular.

REMARK. In the finite group case, where $1/|G| \in K$, it is enough to assume that R is C-M in order to get that R^G is C-M. The point is that a s.o.p. in R^G (say, for simplicity, that both R^G and R are graded or local) will be a s.o.p. for R, hence, an R-sequence. But then, since R^G is a direct summand, it will also be an R^G-sequence. Q.E.D.

However, in the general case, when G is not finite, an s.o.p. for R^G need not be an s.o.p. for R. E.g. consider again Examples 1 and 5 from the list of examples of rings of invariants. In Example 1, let $r = 1$, $s > 1$. Then the maximal ideal $(x_1y_1, \ldots, x_1y_s)$ of R^G has height s in R^G but generates a height one ideal of R. In Example 5, suppose $s = r + 1$. Then the maximal ideal generated by the maximal minors in R^G has height $r + 1$, but expands to a height 2 ideal in R.

REMARK. There is a theorem related to (1.1) which *is* true in char p: If R is regular of char $p > 0$ and A is a subring which is a direct summand of R as an A-module, then A is Cohen-Macaulay. (See [**HR$_1$**].)

I conjecture that this is true for any regular Noetherian ring R, but I don't know it even for finitely generated algebras over fields of char 0!

It is natural to look for stronger properties of rings of invariants than Cohen-Macaulayness. Some recent results indicate that if R is regular and G linearly reductive then R^G has rational singularities.

We digress momentarily to discuss the meaning of this. Assume that K is an algebraically closed field of char 0 and that X is a normal irreducible variety over K. Then it is always possible [Hi] to map a smooth variety S onto X such that, if f is the map $S \to X$,

(1) f is proper (if $K = \mathbf{C}$, this means that inverse images of strongly compact sets are strongly compact), and

(2) if we delete the singular locus from X and its inverse image from S, the restriction f: $S - f^{-1}(X_{\text{sing}}) \to X - X_{\text{sing}}$ is an isomorphism (in particular, f is birational).

Such an f: $S \to X$ is called a *desingularization* of X. Then X is said to have *rational singularities* if for some (equivalently, every) desingularization f: $S \to X$, $R^if_*(\mathcal{O}_S) = 0$, $i \geqslant 1$. This is a local condition on X. If X is affine, we may rephrase it to the statement that $H^i(S, \mathcal{O}_S) = 0$, $i \geqslant 1$. We shall say that R has rational singularities if Spec R does.

An important point is that if X has rational singularities, then X is C-M (i.e. all its local rings are C-M). In fact, if X is normal and C-M then X has rational singularities if and only if every highest order regular differential form on $X - X_{\text{sing}}$ is the restriction of a highest order regular differential form on S (identifying $X - X_{\text{sing}}$ with $S - f^{-1}(X_{\text{sing}})$). (This condition turns out to be independent of the desingularization f.)

A number of authors have proved Cohen-Macaulayness and, in fact, rational singularities, for important classes of varieties, many of the form Spec R^G, by explicit desingularization and related techniques. We refer the reader to [KKMS], [Ke$_1$], [Ke$_2$], [Ke$_3$], [D], and [Sv].

I know of no counterexample to the conjecture that if G is linearly reductive and R has rational singularities, then R^G has rational singularities. This is true if G is finite. It is also known if G acts linearly on a polynomial ring R in two cases: if G is a torus [KKMS], or if G is semisimple [Ke$_3$].

4. Homological questions. This section centers around issues related to Theorem (1.2). We want to explain how it fits in with other central problems in the homological theory of local rings (Serre's conjecture on multiplicities, M. Auslander's question about rigidity of finite projective resolutions, and the related family of questions studied by Peskine-Szpiro [PS$_2$]), what implications it has for the subject, what the open questions are about C-M modules, and, finally, we want to give some insight into the proof of Theorem (1.2).

For background one the homological theory of local rings, we refer the reader to [AB$_1$], [AB$_2$], [AB$_4$], [Ho$_2$], [Ho$_6$], [Ho$_7$], [Ho$_8$], [Ho$_9$], [K$_1$], [M], [N$_2$], [Rees], [S$_1$], and [S$_4$], while for more information about the specific homological problems we consider, we refer the reader to [Au$_1$], [Au$_2$], [Ei], [F$_1$], [F$_2$], [F$_3$], [FT], [Gr], [Ho$_3$], [Ho$_{10}$], [Iv], [K$_2$], [LV], [Lic], [PS$_1$], [PS$_2$], [PS$_3$], and [Ro].

M. Auslander raised the following problem (cf. [Au$_1$], [Au$_2$]), as well as many of the others we shall consider: his contributions to the subject cannot be overstated. We state it in the form of a conjecture:

(4.1). RIGIDITY CONJECTURE. *Let R be a Noetherian ring and let M, N be finitely generated modules such that M has a finite projective resolution, i.e.*

$\mathrm{pd}_R M < \infty$. *Suppose* $\mathrm{Tor}_i^R(M, N) = 0$ *for a certain* i. *Then* $\mathrm{Tor}_j^R(M, N) = 0$ *for all* $j \geq i$.

REMARKS. One can reduce at once to the case where R is local or even complete local and $i = 1$. The question seems to be open even if $\mathrm{pd}_R M = 2$ and N has finite length.

Even when $(R, \mathfrak{m})$ is a regular local ring, (4.1) is a difficult result. [By definition, R regular means that $\mathfrak{m}$ is generated by $\dim R$ elements (which one can easily show turn out to be an R-sequence). By an important theorem (Auslander-Buchsbaum-Serre: see [**AB**$_1$], [**AB**$_2$], [**S**$_1$]), this is equivalent to the fact that every R-module has finite projective dimension. The homological theory of local rings got tremendous impetus from the solution by Auslander-Buchsbaum [**AB**$_4$] of the longstanding problem of proving that regular local rings are UFD's using the homological ideas. To this day, all proofs of unique factorization in regular local rings are homological.] Auslander proved it in several important cases (e.g. if R contains a field) when R is regular, and the general proof was found by Lichtenbaum [**Lic**]. Auslander observed that (4.1) would imply:

(4.2). ZERODIVISOR CONJECTURE. *Let R be local and $M \neq 0$ a finitely generated module with* $\mathrm{pd}_R M < \infty$. *Suppose that $x \in R$ is not a zerodivisor on M. Then x is not a zerodivisor on R.*

No progress was made for a long time. Then Peskine-Szpiro proved [**PS**$_2$] (4.2) in char p and many other cases by showing that (4.3) below implies (4.2). They proved (4.3) using the action of the Frobenius on local cohomology.

(4.3). INTERSECTION CONJECTURE. *Let R be local and let M, N be finitely generated nonzero modules with $(M \otimes_R N)$ finite. Then* $\dim N \leq \mathrm{pd}_R M$. [Here, $\dim N$ denotes the Krull dimension of $R/\mathrm{Ann}_R N$.]

Of course, this is uninteresting unless $\mathrm{pd}_R M$ is finite. Peskine and Szpiro also showed that (4.1) $\Rightarrow$ (4.3), and that (4.3) implies an affirmative answer to a question raised by Bass [**Bs**$_1$]:

(4.4). BASS' CONJECTURE. *Let R be a local ring and let $T \neq 0$ be a finitely generated module which has a finite injective resolution. Then R is Cohen-Macaulay.*

It is worth mentioning the following conjecture [**Ho**$_2$] which is easily shown to be equivalent to (4.3).

(4.5). HOMOLOGICAL HEIGHT CONJECTURE. *Let R be a Noetherian ring, M a finitely generated R-module of finite projective dimension, and let* $I = \mathrm{Ann}_R M$. *Let $R \to S$ be a homomorphism to a Noetherian ring S and let Q be a minimal prime of IS. Then* height $Q \leq \mathrm{pd}_R M$.

We leave it to the reader to see that when $R = \mathbf{Z}[X]$, $M = R/XR$, this reduces to the principal ideal theorem of Krull [**Kr**]: the first really deep theorem in the abstract theory of Noetherian rings.

Having discussed rigidity a bit and some of the other questions it suggests, we turn next to one of the other central problems in the homological theory of local rings: Serre's conjecture on multiplicities.

We proceed in slightly greater generality than necessary, and then specialize. Let R be a local ring and M, N finitely generated R-modules such that:

(1) $l(M \otimes_R N)$ is finite (as in §3, l denotes length), and

(2) M has a finite projective resolution.

Then $\operatorname{Tor}_i^R(M, N)$ has finite length for all i and vanishes for large i. Hence, assuming (1) and (2) we may define

$$e(M, N) = \sum_{i=0} (-1)^i l(\operatorname{Tor}_i^R(M, N)).$$

Now if R is regular, $M = R/I$, $N = R/J$ (note that condition (1) holds automatically when R is regular), then, as already remarked in §3, $e(R/I, R/J)$ agrees with the geometric notion of intersection multiplicity defined via cardinalities of fibers, but makes sense much more generally. In [S_4] Serre proves that this notion has some of the properties which one would like for large classes of regular local rings, and conjectures the same for all regular local rings. Specifically:

(4.6). SERRE'S CONJECTURE ON MULTIPLICITIES. *Let R be a regular local ring and let M, N be finitely generated R-modules. Suppose that $l(M \otimes_R N)$ is finite. Then*:

(a) $\dim M = \dim N \leqslant \dim R$.

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

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

Serre establishes (a) for all regular local rings R and (b), (c) if R contains a field or R is a formal power series ring over a discrete valuation ring. (It is possible to entertain the same conjecture under the weaker hypotheses discussed earlier: R is not assumed regular but it is assumed that $\mathrm{pd}_R M < \infty$. In this case, (a), (b), and (c) are all unknown, except in the graded case [**PS_3**].) We note that (4.6) *is* known if $\dim R \leqslant 4$ [**Ho_2**] or if both M and N are killed by the characteristic p of the residue class field [**Mal_1**], [**Mal_2**].

We note that efforts to prove (4.6) by lifting modules formed at least part of the motivation for [**BE_1**], [**BE_2**], [**BE_3**] (see [**Nas**] for a discussion of the relevance of lifting to multiplicities); however, recent results (see [**K1**], [**Lau**], [**S_3**], and [**Ho_{11}**]) make this approach look almost hopeless.

A. Weil has raised the lack of a satisfactory theory of multiplicities as a reason for not attempting to do algebraic geometry in the kind of generality introduced by Grothendieck in [**G**]. See [**Weil**, p. 305]. Whether one accepts this point of view or not, the importance of settling (4.6) is clear.

Before discussing how C-M modules come into the picture, we want to mention a few other conjectures.

(4.7). NEW INTERSECTION CONJECTURE. *Let R be a local ring, and let F_* be a finite free complex of finitely generated modules of length d*

$$0 \to F_d \to \cdots \to F_0 \to 0$$

such that all the homology modules $H_i(F_*)$ have finite length, and not all $H_i(F_*)$ vanish. Then $\dim R \leqslant d$.

It is not hard to show that (4.7) $\Rightarrow$ (4.3). (4.7) was first proved in char p by Peskine-Szpiro [**PS_3**] and, independently, by P. Roberts [**Ro**].

The following two conjectures are known to be equivalent (cf. [**Ho_3**], [**Ho_{13}**], although the equivalence is not quite proved in these papers):

(4.8). MONOMIAL CONJECTURE. *Let R be a local ring with system of parameters $x_1, \ldots, x_n$. Then for every positive integer t,*

$$x_1^t \cdots x_n^t \notin \sum_i x_i^{t+1} R.$$

(4.9). DIRECT SUMMAND CONJECTURE. *Let R be a regular Noetherian ring and $S \supset R$ an extension ring which is a finite module over R. Then R is a direct summand of S as an R-module.*

(4.10). EISENBUD-EVANS PRINCIPAL IDEAL CONJECTURE. *Let M be a torsion-free module of torsion-free rank r over a local domain $(R, \mathfrak{m})$, and let $u \in \mathfrak{m}M$. Let Q be a minimal prime of* $\operatorname{Trace}(u)$ $(= \{\phi(u): \phi \in \operatorname{Hom}(M, R)\})$. *Then* height $Q \leq r$.

The key point about conjectures 2, 3, 4, 5, 7, 8, 9, 10 is that all would follow from the existence, in the general case, of big C-M modules. (Note: we systematically refer to conjectures as "n" instead of "(4.n)" in the rest of this section.) Moreover, 2, 3, 4, 5, 7, and 10 (see [EE]) were first completely established in the equicharacteristic case as consequences of (1.2). The central role of the existence of big C-M modules should now be clear!

We might mention that big C-M modules were also used to obtain important information about the behavior of the Bass numbers μ^i (see [Bs_1]) in [FFGR]; however, their use was bypassed in [Ro] (cf. also [F_1], [F_2], [F_3], [FT], as well as the basic reference [Mat]).

We next want to discuss small C-M modules, i.e. finitely generated ones (see [S_4], [Ho_2]). If M is a finitely generated module over the local ring $(R, \mathfrak{m})$ and $M \neq 0$, then if $x_1, \ldots, x_n$ is a s.o.p. for R which is an M-sequence, then every s.o.p. for R is an M-sequence. Not every local domain possesses a small C-M module, even if the dimension is 2: one can base counterexamples either on Nagata's counterexamples to the chain condition or on the pathological Noetherian rings in [FR]: see [Ho_2]. However, it is an open question whether every complete local domain possesses a small C-M module, even in dimension 3 (in all characteristics). In dimension 2 one may use the integral closure (cf. [LV], [Ho_2]). The graded case in char p in dim 3 is known, by an argument of Hartshorne-Peskine-Szpiro [PS_1], also given in [Ho_{10}]. The complete case is crucial for the cases of other good local rings, for if S is a regular ring whose Henselization ([N_2], [R]) S^h is an approximation ring (§2) and R is a homomorphic image of S, then some pointed étale extension of R has a small C-M module if and only if $\hat{R}$ does.

Small C-M modules may not be crucial, but there is one application their existence has which I do not know how to get from the existence of big C-M modules: to wit, if complete local rings always have small C-M modules, then 6b $\Rightarrow$ 6c in the multiplicities conjecture (regular case). See [Ho_2].

The existence of small C-M modules comes down to the complete local domain case, and such a domain R is always a finite module over a complete regular local subring A which may even be chosen to be a formal power series ring over a field or discrete valuation ring. In this case it is easy to show that a finitely generated R-module M is C-M if and only if it is A-free. Thus, R has a small C-M module if and only if R is embeddable in the ring $\mathfrak{M}_n(A)$ of $n \times n$ matrices over A (extending the embedding of A as scalar matrices) for some positive integer n. It is tempting to try to deduce the existence of small C-M modules from the existence of big ones. The following beautiful result of P. Griffith [Gr] is a step in the right direction.

(4.11). THEOREM (P. GRIFFITH). *Let R be a complete local domain which is a finite module over the complete regular local ring A. Suppose that R has some big C-M module. Then R has a nonzero countably generated module which is free over A.*

The next question we consider is, what is known about the existence of big C-M modules for (let us say) complete local domains such that the characteristic of the residue class field is positive but the characteristic of the fraction field is 0: the mixed characteristic case. Of course, in dimension ≤ 2 one has even small C-M modules. But in dimension 3 or more, almost nothing is known. There is a result [Ho_{10}] for rings embeddable in a ring of "generalized" Witt vectors in a sufficiently good way (cf. [Bg] for ordinary Witt vectors), but there are no satisfactory criteria for when rings are so embeddable. (The construction depends on showing that if R is a local ring of char $p > 0$, then there exists a big C-M module for R which is an algebra without identity such that the Frobenius is an automorphism.)

We conclude this section and this paper with some remarks on the proof of Theorem (1.2). We refer the reader to [Ho_8] or [Ei] for a quick sketch of the argument and to [Ho_9] for details. Our objective here is only to get across the ideas of the proof.

The basic points are as follows: Start with R itself as an "approximation" to the big C-M module, and 1 as an element outside $\sum_i x_i R$. One then starts "killing" unwanted relations $x_{k+1}m_{k+1} = \sum_{i=1}^{k} x_i m_i$ by adjoining new elements $u_1, \ldots, u_k$ to the module one has and imposing the relation $m_{k+1} = \sum_{i=1}^{k} x_i u_i$. Passing carefully to a direct limit of such "modifications" one obtains a module E which must work if anything does. The difficulty is in showing that if e is the image of $1 \in R$ in E, then $e \notin \sum_{i=1}^{n} x_i E$. One comes down to this: R has a module E such that $x_1, \ldots, x_n$ is an E-sequence if and only if for any module M obtained from R by successive modifications of the type described, the image of $1 \in R$ is not in $\sum_{i=1}^{n} x_i M$.

This condition can be translated into the condition that a certain family of systems of equations with height condition has no local solution in a Noetherian ring R which contains a field (see §2). By the Metatheorem (2.1) one need only prove this in char $p > 0$!

We now come to the main theme: one applies the Frobenius to the equations which would have to hold if there were a solution, and thus obtains a contradiction. This argument is a bit too technical to give in detail here. Instead, we shall examine the same technique in a closely related example.

It is easy to show that if $x_1, \ldots, x_n$ is an M-sequence on any module M, then for every positive integer t,

$$x_1^t \cdots x_n^t \notin \sum_i x_i^{t+1} R.$$

Thus, part of the problem of proving (1.2) in char p is to show that the equation with height condition:

$$X_1^t \cdots X_n^t = X_1^{t+1} Y_1 + \cdots + X_n^{t+1} Y_n \qquad (*)$$

has no solution in which the values of the X's are a s.o.p. This equation with height condition is too simple to be typical of the family of systems one really needs to deal with, but it will serve to illustrate the method. (Note that we shall be proving conjecture (4.8) in char p.) Suppose one has a solution of (*), x, y. If we complete and kill a suitable minimal prime we get a solution x, y in a complete local domain S which is a finite module over its regular subring $R = K[[x_1, \ldots, x_n]]$. Let $\mathfrak{M} = \sum_i x_i R$. S is torsion-free as an R-module and hence can be embedded in R^d for some d. By composing with a suitable product projection we obtain an R-linear map ϕ: $S \to R$ such that $a = \phi(1) \neq 0$. We can pick e so large that $a \notin \mathfrak{m}^q$, where $q = p^e$. If we put our solution x, y into (*), raise both sides to the qth power, and then apply ϕ, we obtain $x_1^{tq} \cdots x_n^{tq}\phi(1) = \sum_i x_i^{tq+q}\phi(y_i^q)$, i.e. $x_1^{tq} \cdots x_n^{tq}a \in \sum_i x_i^{tq+q}R$. But $x_1, \ldots, x_n$ is an R-sequence, whence ([EH] or [T]) $a \in \sum_i x_i^q R \subset \mathfrak{m}^q$, a contradiction. Q.E.D.

REFERENCES

[Ab] S. S. Abhyankar, *Local uniformization on algebraic surfaces over a ground field of characteristic* $p \neq 0$, Ann. of Math. **63** (1956), 491–526.

[AK] A. Altman and S. Kleiman, *Introduction to Grothendieck duality theory*, Lecture Notes in Math., vol. 146, Springer-Verlag, Berlin and New York, 1970.

[Ar$_1$] M. Artin, *On the solutions of analytic equations*, Invent. Math. **5** (1968), 277–291.

[Ar$_2$] ______, *Algebraic approximation of structures over complete local rings*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 23–56.

[Au$_1$] M. Auslander, *Modules over unramified regular local rings*, Illinois J. Math. **5** (1961), 631–645.

[Au$_2$] ______, *Modules over unramified regular local rings*, Proc. Internat. Congress of Math., 1962, pp. 230–233.

[AB$_1$] M. Auslander and D. A. Buchsbaum, *Homological dimension in Noetherian rings*, Proc. Nat. Acad. Sci. U.S.A. **42** (1956), 36–38.

[AB$_2$] ______, *Homological dimension in local rings*, Trans. Amer. Math. Soc. **85** (1957), 390–405.

[AB$_3$] ______, *Codimension and multiplicity*, Ann. of Math. **68** (1958), 625–657; corrections, Ann. of Math. **70** (1959), 395–397.

[AB$_4$] ______, *Unique factorization in regular local rings*, Proc. Nat. Acad. Sci. U.S.A. **45** (1959), 733–734.

[AR] M. Auslander and D. S. Rim, *Ramification index and multiplicity*, Illinois J. Math. **7** (1963), 566–581.

[Bs$_1$] H. Bass, *On the ubiquity of Gorensten rings*, Math. Z. **82** (1963), 8–28.

[Bs$_2$] ______, *Euler characteristics and characters of discrete groups*, preprint.

[Bg] G. M. Bergman, Lecture 26 in *Lectures on curves on an algebraic surface* by D. Mumford, Ann. of Math. Studies No. 59, Princeton Univ. Press, Princeton, N. J., 1966.

[Bt] M.-J. Bertin, *Anneaux d'invariants de polynômes, en caractéristique p*, C. R. Acad. Sci. Paris Sér. A-B **264** (1967), 653–656.

[Bor] A. Borel, *Linear algebraic groups*, Benjamin, New York, 1969.

[Bou$_1$] J.-F. Boutot, *Frobenius et cohomologie locale*, Séminaire Bourbaki, Exp. 453, 1974.

[Bou$_2$] ______, *Schéma de Picard local*, C. R. Acad. Sci. Paris Sér. A-B **277** (1973), 691–694.

[BE$_1$] D. A. Buchsbaum and D. Eisenbud, *Lifting modules and a theorem on finite free resolutions*, Ring Theory, Academic Press, New York, 1972, pp. 63–74.

[BE$_2$] ______, *Remarks on ideals and resolutions*, Symposia Math. **11** (1973), 193–204.

[BE$_3$] ______, *Some structure theorems for finite free resolutions*, Advances in Math. **12** (1974), 84–139.

[Ch] W. L. Chow, *On unmixedness theorem*, Amer. J. Math. **86** (1964), 799–822.

[C] I. S. Cohen, *On the structure and ideal theory of complete local rings*, Trans. Amer. Math. Soc. **59** (1946), 54–106.

[DPr] C. DeConcini and C. Procesi, *A characteristic free approach to invariant theory*, Advances in Math. **21** (1976), 330–354.

[D] M. Demazure, *Désingularisations de variétés de Schubert généralisés*, Ann. Sci. École Norm. Sup. (4) **7** (1974), 53–88.

[DC] J. A. Dieudonné and J. B. Carrell, *Invariant theory, old and new*, Academic Press, New York, 1971.

[EH] J. A. Eagon and M. Hochster, *R-sequences and indeterminates*, Quart. J. Math. Oxford Ser. (2) **25** (1974), 61–71.

[EN] J. A. Eagon and D. G. Northcott, *Ideals defined by matrices and a certain complex associated with them*, Proc. Roy. Soc. London Ser. A **269** (1962), 188–204.

[Ei] D. Eisenbud, *Some directions of recent progress in commutative algebra*, Proc. Sympos. Pure Math., vol 29, Amer. Math. Soc., Providence, R.I., 1975, pp. 111–128.

[EE] D. Eisenbud and E. G. Evans, *A generalized principal ideal theorem*, Nagoya Math. J. **62** (1976), 41–53.

[FR] D. Ferrand and M. Raynaud, *Fibres formelles d'un anneau local noethérien*, Ann. Sci. École Norm. Sup. (4) **3** (1970), 295–311.

[FFGR] R. Fossum, H.-B. Foxby, P. Griffith, and I. Reiten, *Minimal injective resolutions with applications to dualizing modules and Gorenstein modules*, Inst. Hautes Études Sci. Publ. Math. **45** (1975), 193–215.

[FG] R. Fossum and P. Griffith, *Complete local factorial rings which are not Cohen-Macaulay in characteristic p*, Ann. Sci. École Norm. Sup. (4) **8** (1975), 189–200.

[F_1] H.-B. Foxby, *On the μ^i in a minimal injective resolution*, Math. Scand. **29** (1971), 175–186.

[F_2] ______, *Applications of isomorphisms between complexes*, Copenhagen University, preprint.

[F_3] ______, *On the μ^i in a minimal injective resolution*. II, Copenhagen Math. Inst. Preprint Series, No. 20. 1976.

[FT] H.-B. Foxby and A. Thorup, *Minimal injective resolutions under flat base change*, Copenhagen Math. Inst. Preprint Series, No. 22, 1976.

[FK] E. Freitag and R. Kiel, *Algebraische Eigenschaften der lokalen Ringe in den Spitzen der Hilbertschen Modulgruppen*, Invent. Math. **24** (1974), 121–148.

[Fu] W. Fulton, *Algebraic curves*, Benjamin, New York, 1969.

[Gil] R. Gilmer, *Dimension sequences of commutative rings*, Ring Theory, Proc. of the Oklahoma Conference, Marcel Dekker, New York, 1974.

[Gr] P. Griffith, *A representation theorem for complete local rings*, J. Pure Appl. Algebra **7** (1976), 303–315.

[G] A. Grothendieck (with J. Dieudonné), *Éléments de géometrie algébrique*. I–IV, Inst. Hautes Études Sci. Publ. Math. **4**, **8**, **11**, **17**, **20**, **24**, **28**, **32**, (1960)–(1967).

[GH] A. Grothendieck (notes by R. Hartshorne), *Local cohomology*, Lecture Notes in Math., vol. 41, Springer-Verlag, Berlin and New York, 1967.

[GN] T. Gulliksen and O. Negard, *Un complexe résolvent pour certains idéaux déterminantiels*, C. R. Acad. Sci. Paris Ser. A-B **274** (1972), 16–19.

[Ha] W. J. Haboush, *Reductive groups are geometrically reductive*, Ann. of Math. **102** (1975), 67–83.

[HO] R. Hartshorne and A. Ogus, *On the factoriality of local rings of small embedding codimension*, Comm. Algebra **1** (1974), 415–437.

[HS] R. Hartshorne and R. Speiser, *Local cohomological dimension in characteristic p*, preprint.

[Hi] H. Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic* 0, Ann. of Math. **79** (1964), 205–326.

[Ho_1] M. Hochster, *Rings of invariants of tori, Cohen-Macaulay rings generated by monomials, and polytopes*, Ann. of Math. (2) **96** (1976), 318–337.

[Ho_2] ______, *Cohen-Macaulay modules*, Proc. Kansas Commutative Algebra Conference, Lecture Notes in Math., vol. 311, Springer-Verlag, Berlin and New York, 1973, pp. 120–152.

[Ho_3] ______, *Contracted ideals from integral extensions of regular rings*, Nagoya Math. J. **51** (1973), 25–43.

[Ho_4] ______, *Grassmannians and their Schubert subvarieties are arithmetically Cohen-Macaulay*, J. Algebra **25** (1973), 40–57.

[Ho_5] ______, *Deep local rings*, preliminary preprint (no longer available), Aarhus University preprint series, 1973.

[Ho_6] ______, *Grade-sensitive modules and perfect modules*, Proc. London Math. Soc. (3) **29** (1974), 55–76.

[Ho_7] ______, *Constraints on systems of parameters*, Ring Theory, Proc. of the Oklahoma Conference, Marcel Dekker, New York, 1974, pp. 121–161.

[Ho_8] ______, *The equicharacteristic case of some homological conjectures on local rings*, Bull. Amer. Math. Soc. **80** (1974), 683–686.

[Ho_9] ______, *Topics in the homological theory of modules over commutative rings*, C. B. M. S. Regional Conf. Ser. in Math. No. 24, Amer. Math. Soc., Providence, R. I., 1975.

[Ho_{10}] ______, *Big Cohen-Macaulay modules and algebras and embeddability in rings of Witt vectors*, Proc. of the Queen's University Commutative Algebra Conference (Kingston, Ontario, Canada, 1975), Queen's Papers in Pure and Appl. Math. **42**, 106–195.

[Ho_{11}] ______, *An obstruction to lifting cyclic modules*, Pacific J. Math. **61** (1975), 457–463.

[Ho_{12}] ______, *Cohen-Macaulay rings, combinatorics, and simplicial complexes*, Proc. of the Second Oklahoma Ring Theory Conference (March, 1976), Marcel Dekker, New York, 1977.

[Ho_{13}] ______, *Cyclic purity versus purity in excellent Noetherian rings*, Trans. Amer. Math. Soc. **231** (1977), 463–488.

[Ho_{14}] ______, *Properties of Noetherian rings stable under general grade reduction*, Arch. Math. **24** (1973), 53–65.

[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.

[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] ______, *The purity of the Frobenius and local cohomology*, Advances in Math. **20** (1976), 117–172.

[HP] W. V. D. Hodge and D. Pedoe, *Methods of algebraic geometry*. I, II, Cambridge Univ. Press, 1947 and 1952.

[Iv] B. Iversen, *Amplitude inequalities for complexes*, Aarhus University Preprint Series No. 36 (1976/77).

[K_1] I. Kaplansky, *Commutative rings*, Allyn and Bacon, Boston, 1970. Revised ed., 1974.

[K_2] ______, *Commutative rings*, First Jeffery-Williams Lecture, University of Manitoba, 1968, Canadian Math. Congress; reproduced in Proc. Kansas Commutative Algebra Conference, Lecture Notes in Math., vol. 311, Springer-Verlag, Berlin and New York, 1973.

[Ke_1] G. Kempf, *Images of homogeneous vector bundles and varieties of complexes*, Bull. Amer. Math. Soc. **81** (1975), 900–901.

[Ke_2] ______, *On the collapsing of homogeneous bundles*, Invent. Math. **37** (1976), 229–239.

[Ke_3] ______, *Some quotient varieties have rational singularities*, preprint.

[KKMS] G. Kempf, F. Knudsen, D. Mumford and B. St. Donat, *Toroidal embeddings*. I, Lecture Notes in Math., vol. 339, Springer-Verlag, Berlin and New York, 1973.

[Kl] J. Kleppe, *Liftings (deformations) of graded algebras*, Oslo University Math. Preprint Series, No. 101 (1976).

[Kr] W. Krull, *Primidealketten in allgemeinen Ringbereichen*, S.-B. Heidelberger Akad. Wiss. Math.-Natur. Kl. 7 (1928).

[Ku] R. E. Kutz, *Cohen-Macaulay rings and ideal theory in rings of invariants of algebraic groups*, Thesis, University of Minnesota, 1977; and Trans. Amer. Math. Soc. **194** (1974), 115–129.

[Lk] D. Laksov, *The arithmetic Cohen-Macaulay character of the Schubert schemes*, Acta Math. **129** (1972), 1–9.

[Las] A. Lascoux, *Polynômes symétriques, foncteurs de Schur, et grassmanniennes*, Thesis, Université Paris VII, 1977.

[Lau] O. A. Laudal, *Sections of functors and the problem of lifting (deforming) algebraic structures*. I, II, III, Oslo University Math. Preprint Series, No. 18 (1975), No. 24 (1975), No. 6 (1976).

[LV] G. Levin and W. Vasconcelos, *Homological dimensions and Macaulay rings*, Pacific J. Math. **25** (1968), 315–328.

[Lic] S. Lichtenbaum, *On the vanishing of* Tor *in regular local rings*, Illinois J. Math. **10** (1966), 220–226.

[Lip] J. Lipman, *Unique factorization in complete local rings*, Proc. Sympos. Pure Math., vol. 29, Amer. Math. Soc., Providence, R. I., 1975.

[Mac_1] F. S. Macaulay, *Algebraic theory of modular systems*, Cambridge Tracts No. 19, Cambridge, 1916.

[Mac_2] ______, *Some properties of enumeration in the theory of modular systems*, Proc. London Math. Soc. **26** (1927), 531–555.

[Mal_1] M.-P. Malliavin-Brameret, *Une remarque sur les anneaux locaux reguliers*, Sem. Dubreil-Pisot, 24^e annee, 1970/71, no. 13.

[Mal_2] ______, *Structure d'anneaux locaux reguliers et caracteristiques d'Euler-Poincaré*, Bull. Soc. Math. France (2) **97** (1973), 81–88.

[Mat] E. Matlis, *Injective modules over Noetherian rings*, Pacific J. Math. **8** (1958), 511–528.

[M] H. Matsumura, *Commutative algebra*, Benjamin, New York, 1970.

[MS] P. McMullen and G. C. Shephard, *Convex polytopes and the upper bound conjecture*, London Math. Soc. Lecture Note Series 3, Cambridge Univ. Press, 1971.

[Mol] T. Molien, *Über die Invarianten der linearen Substitutionsgruppen*, Sitzungsber. König. Preuss. Akad. Wiss. (1897), 1152–1156.

[Mo] S. Mori, *On affine cones associated with polarized varieties*, preprint.

[Mu_1] D. Mumford, *Geometric invariant theory*, Springer-Verlag, Berlin and New York, 1965.

[Mu_2] ______, *Introduction to algebraic geometry*, Lecture Notes, Harvard University, 1966.

[Mu_3] ______, *Hilbert's fourteenth problem–the finite generation of subrings such as rings of invariants*, Proc. Sympos. Pure Math., vol. 28 (Part 2) Amer. Math. Soc., Providence, R. I., 1976, pp. 431–444.

[Mu_4] ______, *Algebraic geometry*. I: *Complex projective varieties*, Die Grundlehren der math. Wissenschaften, Band 221, Springer-Verlag, Berlin and New York, 1976.

[Mus] C. Musili, *Postulation formula for Schubert varieties*, J. Indian Math. Soc. **36** (1972), 143–171.

[N_1] M. Nagata, *Complete reducibility of rational representation of a matric group*, J. Math. Kyoto Univ. **1** (1961), 87–99.

[N_2] ______, *Local rings*, Interscience, New York, 1962.

[N_3] ______, *Lectures on the fourteenth problem of Hilbert*, Lecture Notes in Math., vol. 31, Tata Institute, Bombay, 1965.

[Nas] H.-J. Nastold, *Zur Serreschen Multiplizitätstheorie in der arithmetischen Geometrie*, Math. Ann. **143** (1973), 323–395.

[PS_1] C. Peskine and L. Szpiro, *Notes sur un air de H. Bass*, Unpublished preprint (Brandeis University).

[PS_2] ______, *Dimension projective finie et cohomologie locale*, Inst. Hautes Études Sci. Publ. Math. **42** (1973), 323–395.

[PS_3] ______, *Syzygies et multiplicités*, C. R. Acad. Sci. Paris Sér. A-B **278** (1974), 1421–1424.

[PP] G. Pfister and D. Popescu, *Die strenge Approximationseigenschaft lokaler Ring*, Invent. Math. **30** (1975), 145–174.

[Po] K. Y. Poon, *A resolution of certain perfect ideals defined by some matrices*, Thesis, University of Minnesota, 1973.

[Pr] C. Procesi, *The invariant theory of $n \times n$ matrices*, Advances in Math. **19** (1976), 306–381.

[R] M. Raynaud, *Anneaux locaux Henséliens*, Lecture Notes in Math., vol. 169, New York, 1970.

[Rees] D. Rees, *The grade of an ideal or module*, Proc. Cambridge Philos. Soc. **53** (1957), 28–42.

[Rei] G. Reisner, *Cohen-Macaulay quotients of polynomial rings*, Advances in Math. **21** (1976), 30–49.

[Ro] P. Roberts, *Two applications of dualizing complexes over local rings*, Ann. Sci. École Norm. Sup. (4) **9** (1976), 103–106.

[Sam] P. Samuel, *Lectures on unique factorization domains*, Lecture Notes in Math., vol. 30, Tata Institute, Bombay, 1964.

[Sei_1] A. Seidenberg, *A note on the dimension theory of rings*, Pacific J. Math. **3** (1953), 505–512.

[Sei_2] ______, *On the dimension theory of rings*. II, Pacific J. Math. **4** (1954), 603–614.

[S_1] J.-P. Serre, *Sur la dimension homologique des anneaux et des modules Noethériens*, Proc. Internat. Sympos. Algebraic Number Theory, Tokyo, 1955, pp. 175–189.

[S_2] ______, *Faisceaux algébriques cohérents*, Ann. of Math. **61** (1955), 197–278.

[S_3] ______, *Exemples de variétés projectives en caractéristique p non relèvables en caractéristique zéro*, Proc. Nat. Acad. Sci. U.S.A. **47** (1961), 108–109.

[S_4] ______, *Algèbre locale. Multiplicités*, Lecture Notes in Math., vol. 11, Springer-Verlag, Berlin and New York, 1965.

[Sh] R. Y. Sharp, *Local cohomology theory in commutative algebra*, Quart. J. Math. Oxford Ser. (2) **21** (1970), 425–434.

[ST] G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canad. J. Math. **6** (1954), 274–304.

[St_1] R. Stanley, *Cohen-Macaulay rings and constructible polytopes*, Bull. Amer. Math. Soc. **81** (1975), 133–135.

[St_2] ———, *The upper bound conjecture and Cohen-Macaulay rings*, Studies in Appl. Math. **54** (1975), 135–142.

[Sv] T. Svanes, *Coherent cohomology on Schubert subschemes of flag schemes and applications*, Advances in Math. **14** (1974), 369–453.

[T] D. Taylor, *Ideals generated by monomials in an R-sequence*, Thesis, University of Chicago, 1966.

[Weil] A. Weil, *Foundations of algebraic geometry*, Amer. Math. Soc. Colloq. Publ., vol. 29, Amer. Math. Soc., Providence, R. I., 1946. Revised ed. 1962.

[Weyl] H. Weyl, *The classical groups*, Princeton Univ. Press, Princeton, N. J., 1946.

[Z_1] O. Zariski, *The reduction of the singularities of an algebraic surface*, Ann. of Math. **40** (1939), 639–689.

[Z_2] ———, *Foundations of a general theory of birational correspondences*, Trans. Amer. Math. Soc. **53** (1943), 490–542.

[Z_3] ———, *The concept of a simple point of an abstract algebraic variety*, Trans. Amer. Math. Soc. **62** (1947), 1–52.

[ZS] O. Zariski and P. Samuel, *Commutative algebra*. Vols. 1, 2, Van Nostrand, Princeton, N. J., 1958, 1960.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, ANN ARBOR, MICHIGAN 48109