INEQUALITIES RELATED TO CERTAIN COUPLES OF LOCAL RINGS

BY

CHRISTER LECH

Uppsala

Let Q be a (Noetherian) local ring with maximal ideal $\mathfrak{m}$, and let $\mathfrak{p}$ be a prime ideal in Q such that $\dim \mathfrak{p} + \operatorname{rank} \mathfrak{p} = \dim Q$. Serre showed, using homological means, that if Q is regular, then the local ring $Q_{\mathfrak{p}}$ is also regular ([8], Theorem 5, p. 186). Under a special assumption Nagata obtained what might be considered a quantitative extension of this result. He proved that if $\mathfrak{p}$ is analytically unramified, then the multiplicity of $\mathfrak{p}$ is not larger than that of $\mathfrak{m}$ ([5], Theorem 10, p. 221). In the present paper it will be shown that under a slightly different special assumption much more can be said. In fact, under that assumption there holds an inequality between certain sum-transforms of the Hilbert functions of $\mathfrak{p}$ and of $\mathfrak{m}$. One seems free to believe that a similar inequality would hold true also in the general case. To prove this it would suffice to prove an analogous statement concerning flat couples of local rings. We shall actually derive a theorem which implies a particular instance of that statement. As a consequence we obtain a generalization and a new proof of Serre's result. Introducing a natural measure of how much a local ring deviates from being regular, we prove that $Q_{\mathfrak{p}}$ is not more irregular than Q. Our methods of proof are non-homological in the sense that they do not involve any homological resolutions.

We shall now describe our results more closely.[1]

Let Q be a local ring with maximal ideal $\mathfrak{m}$. For each non-negative integer n, define $H(\mathfrak{m}; n)$ as the length of the Q-module $\mathfrak{m}^n/\mathfrak{m}^{n+1}$. Put

---

[1] The necessary facts about local rings can be found in Nagata's book [6], where however the terminology is different in some respects. In particular the concepts which we have called rank and dimension of an ideal and dimension of a ring, are termed height and depth of an ideal and altitude of a ring. Concerning flatness, which is dealt with in the Sections 18 and 19 of the book, cf. e.g. the appendix of [4].

$$H^{(0)}(\mathfrak{m}; n) = H(\mathfrak{m}; n), \quad n = 0, 1, 2, \ldots,$$

$$H^{(k+1)}(\mathfrak{m}; n) = \sum_{\nu=0}^{n} H^{(k)}(\mathfrak{m}; \nu) \quad n, k = 0, 1, 2, \ldots.$$

As functions of n the $H^{(k)}(\mathfrak{m}; n)$ $(k = 0, 1, 2, \ldots)$ were referred to above as sum-transforms of $H(\mathfrak{m}; n)$, which itself is called the Hilbert function of $\mathfrak{m}$. All these functions record some information about Q and are equivalent in this respect. In particular their behavior for large values of n determines the dimension and multiplicity of Q, and their values for $n = 1$ give the minimum number of generators of $\mathfrak{m}$. In fact, for large values of n each $H^{(k)}(\mathfrak{m}; n)$ is a polynomial in n, and if we denote the degree and leading coefficient of this polynomial by $d(k)$ and $a(k)$ resp., then, for $k \geqslant 1$, Q has the dimension $d(k) + 1 - k$ and the multiplicity $d(k)!\, a(k)$. The minimum number of generators of $\mathfrak{m}$ is equal to $H^{(k)}(\mathfrak{m}; 1) - k$. We shall call the difference between the minimum number of generators of $\mathfrak{m}$ and the dimension of Q the *regularity defect* of Q, or, of $\mathfrak{m}$. Like the multiplicity, the regularity defect of Q can be calculated from $H^{(k)}(\mathfrak{m}; n)$ without any reference to the index k. It is a non-negative integer, which is equal to zero if and only if Q is regular, and gives a measure of how much this ring deviates from being regular.

If $\mathfrak{p}$ is a prime ideal of a Noetherian ring R, then by *the local ring associated with* $\mathfrak{p}$ we shall understand the ring of quotients $R_{\mathfrak{p}}$ of R with respect to $\mathfrak{p}$. We extend our notation by putting $H(\mathfrak{p}; n) = H(\mathfrak{p}R_{\mathfrak{p}}; n)$, $H^{(k)}(\mathfrak{p}; n) = H^{(k)}(\mathfrak{p}R_{\mathfrak{p}}; n)$. Similarly we define the regularity defect of $\mathfrak{p}$ by putting it equal to that of $\mathfrak{p}R_{\mathfrak{p}}$, i.e. to $H(\mathfrak{p}; 1) - \operatorname{rank} \mathfrak{p}$.

An integral domain S with field of quotients K will be said to *have a finite integral closure* if the integral closure of S in K is a finitely generated S-module.

Now we can state our first theorem.

THEOREM 1. *Let* $\mathfrak{m}$ *and* $\mathfrak{p}$ *be two prime ideals of a Noetherian ring,* $\mathfrak{m}$ *containing* $\mathfrak{p}$. *Assume that* $\operatorname{rank} \mathfrak{m}/\mathfrak{p} = 1$ *and that the local ring associated with* $\mathfrak{m}/\mathfrak{p}$ *has a finite integral closure. Then there exists a non-negative integer* k *such that*

$$H^{(k+1)}(\mathfrak{p}; n) \leqslant H^{(k)}(\mathfrak{m}; n) \quad n = 0, 1, 2, \ldots.$$

The proof can shortly be described as follows. We show by direct calculations that the result holds true with $k = 1$ if the local ring associated with $\mathfrak{m}/\mathfrak{p}$ is regular. Then we reduce the proof of the theorem to this special case by utilizing the properties of suitably chosen prime ideals in a free polynomial extension of the original ring.

The significance of the theorem is most readily seen if one makes the additional hypothesis that $\operatorname{rank} \mathfrak{p} = \operatorname{rank} \mathfrak{m} - 1$. This condition is necessary and sufficient in order that $H^{(k+1)}(\mathfrak{p}; n)$ and $H^{(k)}(\mathfrak{m}; n)$ shall have the same degree as polynomials in n for n large, and if it is fulfilled, one can conclude from the theorem, by taking $n = 1$ and $n \to \infty$, that the regularity defect and multiplicity of $\mathfrak{p}$ do not exceed the corresponding numbers for $\mathfrak{m}$. (The multiplicity part of this conclusion is contained in the above-mentioned result of Nagata, cf. below.)

The assumption that $\operatorname{rank} \mathfrak{m}/\mathfrak{p} = 1$, does not indicate an absolute limit for the applicability of the theorem. It has rather the effect of restricting the attention to a crucial case. For suppose that $\mathfrak{m}$ and $\mathfrak{p}$ are prime ideals in a Noetherian ring such that $\mathfrak{m} \supset \mathfrak{p}$ and $\operatorname{rank} \mathfrak{m}/\mathfrak{p} = r > 1$. Then there is a chain of prime ideals,

$$\mathfrak{m} = \mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \ldots \supset \mathfrak{p}_r = \mathfrak{p},$$

in which $\operatorname{rank} \mathfrak{p}_{i-1}/\mathfrak{p}_i = 1$ $(i = 1, 2, \ldots, r)$. If now the theorem is applicable to each link of this chain, i.e. if, for $i = 1, 2, \ldots, r$, the local ring associated with $\mathfrak{p}_{i-1}/\mathfrak{p}_i$ has a finite integral closure, then, putting together the results for each link, we infer that there exists a non-negative integer k such that

$$H^{(k+r)}(\mathfrak{p}; n) \leqslant H^{(k)}(\mathfrak{m}; n) \quad n = 0, 1, 2, \ldots .$$

If, in addition, $\operatorname{rank} \mathfrak{m} = \operatorname{rank} \mathfrak{m}/\mathfrak{p} + \operatorname{rank} \mathfrak{p}$, then $H^{(k+r)}(\mathfrak{p}; n)$ and $H^{(k)}(\mathfrak{m}; n)$ have the same degree as polynomials in n for n large and it follows in particular from the inequality that the regularity defect and multiplicity of $\mathfrak{p}$ do not exceed the corresponding numbers for $\mathfrak{m}$. Thus we can state results for $\operatorname{rank} \mathfrak{m}/\mathfrak{p} > 1$ that are quite analogous to those for $\operatorname{rank} \mathfrak{m}/\mathfrak{p} = 1$. Let us note that when $\operatorname{rank} \mathfrak{m}/\mathfrak{p}$ equals one, our assumptions, including the additional hypothesis that $\operatorname{rank} \mathfrak{p} = \operatorname{rank} \mathfrak{m} - 1$, are equivalent to those of Nagata in his result on the multiplicities of $\mathfrak{m}$ and $\mathfrak{p}$. For, by a theorem of Krull, a one-dimensional local integral domain has a finite integral closure if and only if it is analytically unramified (see [1]).

In view of what has been said, the generality of the theorem is restricted primarily by the assumption that the local ring associated with $\mathfrak{m}/\mathfrak{p}$ has a finite integral closure. One may ask if not to a large extent the theorem would be valid also without this assumption. Trying to show this, we are lead to the following considerations. Let $\mathfrak{m}$ and $\mathfrak{p}$ be prime ideals in a Noetherian ring R such that $\mathfrak{m} \supset \mathfrak{p}$ and $\operatorname{rank} \mathfrak{m}/\mathfrak{p} = 1$. Denote by R^* the completion of the local ring associated with $\mathfrak{m}$, by $\mathfrak{m}^*$ the maximal ideal of R^*, and by $\mathfrak{p}^*$ a minimal prime ideal of $\mathfrak{p}R^*$. Consider the diagram of prime ideals,

By the theorem of Krull just mentioned, we can apply Theorem 1 to $\mathfrak{m}^*$ and $\mathfrak{p}^*$. We should like to transfer the result to $\mathfrak{m}$ and $\mathfrak{p}$. Since the Hilbert functions of $\mathfrak{m}$ and $\mathfrak{m}^*$ are identical, it would suffice to prove a suitable inequality interrelating the Hilbert functions of $\mathfrak{p}$ and $\mathfrak{p}^*$. Now $R^*_{\mathfrak{p}^*}$ is $R_{\mathfrak{p}}$-flat, as is easily derived from the well-known fact that R^* is $R_{\mathfrak{m}}$-flat (see [6], (18.10)). Hence we see that it would suffice to prove, and apply to the couple $(R_{\mathfrak{p}}, R^*_{\mathfrak{p}^*})$, the following statement (cf. [4], the introduction):

Let (Q_0, Q) be a couple of local rings with maximal ideals $(\mathfrak{m}_0, \mathfrak{m})$. Suppose that Q contains Q_0 and is a flat Q_0-module and that $\mathfrak{m}_0 Q$ is an $\mathfrak{m}$-primary ideal. Then there exists a non-negative integer k such that

$$H^{(k)}(\mathfrak{m}_0; n) \leqslant H^{(k)}(\mathfrak{m}; n) \quad n = 0, 1, 2, \ldots .$$

Thus we arrive at the problem *to decide whether this statement is true, or, rather, to what extent it is true*; by proving a part or a weakened form of it, we will in general get a corresponding result concerning our original question. From one point of view this new problem seems advantageous. Without loss of generality we can assume that Q_0 and Q are complete, since, if they are not so from the beginning, we can pass to their completions. Thus for instance the structure theorems of Cohen are available.

The supposition of the statement entails that Q_0 and Q have the same dimension (see e.g. [4], p. 85). The statement therefore says in particular that the regularity defect and multiplicity of $\mathfrak{m}_0$ do not exceed the corresponding numbers for $\mathfrak{m}$. We can partly confirm these assertions. In a previous paper we have shown that if the dimension of Q_0 and Q is not larger than two, then the multiplicity of $\mathfrak{m}_0$ does not exceed that of $\mathfrak{m}$ ([4]). Here we shall show, this being one of our main objects, that the regularity defect of $\mathfrak{m}_0$ in no case exceeds that of $\mathfrak{m}$. Actually we shall prove the following theorem which has this result as an immediate consequence.

THEOREM 2. *Let Q be a local ring, $\mathfrak{m}$ its maximal ideal, and $\mathfrak{q}$ an $\mathfrak{m}$-primary ideal. Assume that the ring $Q/\mathfrak{q}$ is equicharacteristic and that $\mathfrak{q}/\mathfrak{q}^2$ is a free $Q/\mathfrak{q}$-module. Then the minimum number of generators of $\mathfrak{q}$ is not larger than the minimum number of generators of $\mathfrak{m}$.*

We get the result on the regularity defects of $\mathfrak{m}_0$ and $\mathfrak{m}$ by applying the theorem to the local ring Q and the $\mathfrak{m}$-primary ideal $\mathfrak{m}_0 Q$. This application is possible: the ring $Q/\mathfrak{m}_0 Q$ is equicharacteristic since it contains a subring isomorphic to the field $Q_0/\mathfrak{m}_0$, and $\mathfrak{m}_0 Q/\mathfrak{m}_0^2 Q$ is a free $Q/\mathfrak{m}_0 Q$-module since $\mathfrak{m}_0/\mathfrak{m}_0^2$ is a free $Q_0/\mathfrak{m}_0$-module and Q is Q_0-flat (see below p. 78). It is also true that $\mathfrak{m}_0$ and $\mathfrak{m}_0 Q$ have the same minimum number of generators. Thus, by the theorem, $H(\mathfrak{m}_0; 1) \leqslant H(\mathfrak{m}; 1)$, hence also $H(\mathfrak{m}_0; 1) - \operatorname{rank} \mathfrak{m}_0 \leqslant H(\mathfrak{m}; 1) - \operatorname{rank} \mathfrak{m}$.

Returning to our original question, we obtain the result that follows.

THEOREM 3. *Let* $\mathfrak{m}$ *and* $\mathfrak{p}$ *be two prime ideals of a Noetherian ring,* $\mathfrak{m}$ *containing* $\mathfrak{p}$. *Then*

$$H(\mathfrak{p}; 1) + \operatorname{rank} \mathfrak{m}/\mathfrak{p} \leqslant H(\mathfrak{m}; 1).$$

In particular, if $\operatorname{rank} \mathfrak{m} = \operatorname{rank} \mathfrak{m}/\mathfrak{p} + \operatorname{rank} \mathfrak{p}$, *then the regularity defect of* $\mathfrak{p}$ *is not larger than that of* $\mathfrak{m}$.

This theorem contains the announced generalization of Serre's result. It also shows the correctness of a conjecture by Guérindon ([3], p. 4144) stating that the supremum of $H(\mathfrak{p}; 1)$ taken over all prime ideals $\mathfrak{p}$ of a fixed local ring, is finite.

The proof of Theorem 2 is divided into two cases. When $Q/\mathfrak{q}$ is a ring of characteristic $p > 0$, we give a direct proof by taking advantage of the simple formula for the pth power of a sum in such a ring. When $Q/\mathfrak{q}$ has characteristic 0, we reduce the proof to the first case by introducing a coefficient field of $Q/\mathfrak{q}^2$ and specializing that field. Thus in the second case we use the structure theorems of Cohen. By the aid of these theorems it is also possible to derive the following complementary result.

ADDENDUM TO THEOREM 2. *If the minimum number of generators of* $\mathfrak{q}$ *is not more than one unit less than the minimum number of generators of* $\mathfrak{m}$, *then there exists a non-negative integer* r *such that* $Q/\mathfrak{q}$ *has the form*

$$K[[x_1, \ldots, x_r]]/(c_1, \ldots, c_r),$$

where K *is a field and* $K[[x_1, \ldots, x_r]]$ *a ring of formal power series in* r *indeterminates over* K.

The proofs of Theorem 1, Theorem 2, and the Addendum to Theorem 2 follow below, each in a separate section. We conclude the paper by some remarks which especially concern the statement about Q_0 and Q on the preceding page.

Proof of Theorem 1

We begin by proving two lemmata, of which the first represents a special case of the theorem and the second states a fundamental fact concerning Hilbert functions of prime ideals in free polynomial extensions.

LEMMA 1. *In a local ring Q with maximal ideal $\mathfrak{m}$, let $\mathfrak{p}$ be a prime ideal strictly contained in $\mathfrak{m}$ such that $\mathfrak{m}=(f)+\mathfrak{p}$ for some element f of Q. Then*

$$H^{(2)}(\mathfrak{p};n)\leqslant H^{(1)}(\mathfrak{m};n) \quad n=0,1,2,\ldots.$$

Remark. Obviously one can express part of the assumption by saying that $Q/\mathfrak{p}$ is regular.

Proof. $H^{(1)}(\mathfrak{m};n)$ is equal to the length of the ideal $(f,\mathfrak{p})^{n+1}$.(1) We shall estimate this length from below. Since for $k=0,1,2,\ldots$ the power $\mathfrak{p}^k$ is contained in the symbolic power $\mathfrak{p}^{(k)}$, i.e. $\mathfrak{p}^kQ_{\mathfrak{p}}\cap Q$, we can, as a first simplification, exchange the ideal

$$(f,\mathfrak{p})^{n+1}=\sum_{i+k=n+1} f^i\mathfrak{p}^k$$

for

$$\sum_{i+k=n+1} f^i\mathfrak{p}^{(k)}.$$

Consider the operation of adding to this ideal successively $f^i\mathfrak{p}^{(k)}$, $0\leqslant i+k\leqslant n$, in order according to decreasing lexicographic height of $(i+k,k)$. By this operation the length of the ideal is successively reduced to zero. Denote by $D(i,k)$ the decrease in length that corresponds to the addition of $f^i\mathfrak{p}^{(k)}$. The total length of the ideal is then equal to the sum of the $D(i,k)$, $0\leqslant i+k\leqslant n$, and it suffices to estimate each of these numbers. Using an isomorphism of the form $\mathfrak{a}+\mathfrak{b}/\mathfrak{b}\approx\mathfrak{a}/\mathfrak{a}\cap\mathfrak{b}$, we see that $D(i,k)$ is equal to the length of the Q-module

$$f^i\mathfrak{p}^{(k)}\Big/f^i\mathfrak{p}^{(k)}\cap\left(\sum_{\iota+\varkappa>i+k} f^i\mathfrak{p}^{(\varkappa)}+\sum_{\iota+\varkappa=i+k,\varkappa>k} f^i\mathfrak{p}^{(\varkappa)}\right).$$

The denominator of this factor module is contained in

$$f^i\mathfrak{p}^{(k)}\cap((f^{i+1})+\mathfrak{p}^{(k+1)}),$$

(1) The length of a $\mathfrak{p}$-primary ideal $\mathfrak{q}$ in a Noetherian ring R is defined as the length of the $R_{\mathfrak{p}}$-module $R_{\mathfrak{p}}/\mathfrak{q}R_{\mathfrak{p}}$. We shall use this notion only when $\mathfrak{p}$ is a maximal ideal, in which case it can be equivalently defined as the length of the R-module $R/\mathfrak{q}$.

which, in view of the fact that $\mathfrak{p}^{(k)}:f=\mathfrak{p}^{(k)}$ $(k=0,1,2,\ldots)$, can be written on the form

$$f^i(\mathfrak{p}^{(k)}\cap((f)+\mathfrak{p}^{(k+1)})),$$

or, still simpler,

$$f^i(f\mathfrak{p}^{(k)}+\mathfrak{p}^{(k+1)}).$$

Thus $D(i,k)$ is at least as large as the length of the Q-module

$$f^i\mathfrak{p}^{(k)}/f^i(f\mathfrak{p}^{(k)}+\mathfrak{p}^{(k+1)}).$$

Since $(0):f^i\subseteq\mathfrak{p}^{(k+1)}:f^i=\mathfrak{p}^{(k+1)}$, this module is isomorphic to

$$\mathfrak{p}^{(k)}/(f\mathfrak{p}^{(k)}+\mathfrak{p}^{(k+1)}),$$

or, since $\mathfrak{m}=(f,\mathfrak{p})$ and $\mathfrak{p}\mathfrak{p}^{(k)}\subseteq\mathfrak{p}^{(k+1)}$, to

$$\mathfrak{p}^{(k)}/(\mathfrak{p}^{(k+1)}+\mathfrak{m}\mathfrak{p}^{(k)}).$$

The length of a Q-module which can be written on this form is equal to the number of elements in a minimal system of generators of the Q-module $\mathfrak{p}^{(k)}/\mathfrak{p}^{(k+1)}$. Such a system represents in a natural way a system of generators of the $Q_\mathfrak{p}$-module $\mathfrak{p}^kQ_\mathfrak{p}/\mathfrak{p}^{k+1}Q_\mathfrak{p}$. The number of elements is therefore not less than $H(\mathfrak{p};k)$. Thus we have shown that $D(i,k)\geqslant H(\mathfrak{p};k)$. It follows that

$$H^{(1)}(\mathfrak{m};n)\geqslant\sum_{0\leqslant i+k\leqslant n}D(i,k)\geqslant\sum_{0\leqslant i+k\leqslant n}H(\mathfrak{p};k)=\sum_{i=0}^{n}H^{(1)}(\mathfrak{p};n-i)=H^{(2)}(\mathfrak{p};n),$$

and the proof is complete.

LEMMA 2. *Let Q be a Noetherian ring, $Q[z]$ a polynomial ring over Q in one variabel z, and $\mathfrak{m}$ and $\mathfrak{M}$ prime ideals in Q and $Q[z]$ resp. such that $\mathfrak{M}\cap Q=\mathfrak{m}$. Then*

$$H(\mathfrak{M};n)=\begin{cases}H(\mathfrak{m};n) & \text{for } \mathfrak{M}=\mathfrak{m}Q[z]\\ H^{(1)}(\mathfrak{m};n) & \text{for } \mathfrak{M}\neq\mathfrak{m}Q[z]\end{cases}\qquad n=0,1,2,\ldots.$$

Proof. Without loss of generality we can assume that Q is a local ring with the maximal ideal $\mathfrak{m}$, for if necessary we can replace Q, $\mathfrak{m}$, and $\mathfrak{M}$ by $Q_\mathfrak{m}$, $\mathfrak{m}Q_\mathfrak{m}$, and $\mathfrak{M}Q_\mathfrak{m}[z]$.

When $\mathfrak{M}=\mathfrak{m}Q[z]$, it suffices to observe that $Q[z]$ is a free and hence a flat Q-module and that therefore $Q[z]_\mathfrak{M}$ is Q-flat (see [6], (19.1)).

Assume then that $\mathfrak{M}\neq\mathfrak{m}Q[z]$. By factoring the ring homomorphism $Q[z]\to Q[z]/\mathfrak{M}$ on the form $Q[z]\to(Q/\mathfrak{m})[z]\to Q[z]/\mathfrak{M}$ we see that $\mathfrak{M}$ is generated by $\mathfrak{m}$ and a poly-

nomial $f \in Q[z]$ of positive degree and with the leading coefficient 1. We further see that $\mathfrak{M}$ is a maximal ideal and that consequently

$$H(\mathfrak{M}; n) = \text{length}_{Q[z]}(\mathfrak{M}^n/\mathfrak{M}^{n+1}).$$

Form the ideal $(\mathfrak{m}, f)$ of the ring $Q[f]$. As a Q-module $(\mathfrak{m}, f)^n$ is a direct sum

$$\sum_{\nu=0}^{\infty} \mathfrak{m}^{n-\nu} f^\nu,$$

where $\mathfrak{m}^{n-\nu}$ shall be understood as Q for $\nu \geqslant n$. By comparing this expression with the corresponding one for $(\mathfrak{m}, f)^{n+1}$ we find that, as a Q-module, $(\mathfrak{m}, f)^n/(\mathfrak{m}, f)^{n+1}$ is isomorphic to the direct sum of $H^{(1)}(\mathfrak{m}; n)$ copies of $Q/\mathfrak{m}$. In view of this and of the fact that $Q[z]$ is a free and hence a flat $Q[f]$-module (the number of basis elements is equal to the degree of the polynomial f), we get by the fundamental laws for flatness and for tensor products the $Q[z]$-isomorphisms

$$\begin{aligned}\mathfrak{M}^n/\mathfrak{M}^{n+1} &\approx ((\mathfrak{m}, f)^n/(\mathfrak{m}, f)^{n+1}) \otimes_{Q[f]} Q[z] \approx ((\mathfrak{m}, f)^n/(\mathfrak{m}, f)^{n+1}) \otimes_Q (Q[z]/(f)) \\ &\approx \text{the direct sum of } H^{(1)}(\mathfrak{m}; n) \text{ copies of } (Q/\mathfrak{m}) \otimes_Q (Q[z]/(f)) \\ &\approx \text{the direct sum of } H^{(1)}(\mathfrak{m}; n) \text{ copies of } Q[z]/\mathfrak{M}.\end{aligned}$$

Thus
$$\text{length}_{Q[z]}(\mathfrak{M}^n/\mathfrak{M}^{n+1}) = H^{(1)}(\mathfrak{m}; n),$$

which gives the result.

To prove Theorem 1 we can assume without loss of generality that the prime ideal $\mathfrak{m}$ of the theorem is the maximal ideal of a local ring Q. The supposition then means that $\mathfrak{p}$ is a one-dimensional prime ideal in Q such that $Q/\mathfrak{p}$ has a finite integral closure, say $(Q/\mathfrak{p})[c_1, \ldots, c_j]$, and we have to show that there exists a non-negative integer k such that

$$H^{(k+1)}(\mathfrak{p}; n) \leqslant H^{(k)}(\mathfrak{m}; n) \quad n = 0, 1, 2, \ldots .$$

Let $z_1, \ldots, z_j$ be a system of j independent indeterminates over Q and consider the naturally formed, composed homomorphism

$$Q[z_1, \ldots, z_j] \to (Q/\mathfrak{p})[z_1, \ldots, z_j] \to (Q/\mathfrak{p})[c_1, \ldots, c_j],$$

where for $i = 1, 2, \ldots, j$ the indeterminate z_i is carried into the element c_i. Let $\mathfrak{P}$ and $\mathfrak{M}$ be the inverse images in $Q[z_1, \ldots, z_j]$ of the zero ideal and an arbitrary maximal ideal resp. in $(Q/\mathfrak{p})[c_1, \ldots, c_j]$.

It is clear that $\mathfrak{P}$ and $\mathfrak{M}$ are prime ideals and that $\mathfrak{P} \cap Q = \mathfrak{p}$. Moreover, it is not difficult to show that $\mathfrak{M} \cap Q = \mathfrak{m}$ and that rank $\mathfrak{M}/\mathfrak{P} = 1$ (see [6], Section 10). Since $(Q/\mathfrak{p})[c_1, \ldots, c_j]$ is integrally closed, the local ring associated with $\mathfrak{M}/\mathfrak{P}$ is also integrally closed. Hence its maximal ideal can be generated by a single element (see [6], Section 12). Thus we can apply Lemma 1 to the local ring associated with $\mathfrak{M}$ and the prime ideal in this ring generated by $\mathfrak{P}$. This gives

$$H^{(2)}(\mathfrak{P}; n) \leqslant H^{(1)}(\mathfrak{M}; n) \quad n = 0, 1, 2, \ldots .$$

We can calculate $H(\mathfrak{P}; n)$ by applying Lemma 2 to the j extensions which are obtained by successive adjunction of the indeterminates $z_1, \ldots, z_j$ to Q. The definition of $(Q/\mathfrak{p})[c_1, \ldots, c_j]$ implies that for $i = 1, 2, \ldots, j$ there are elements a_i, b_i in $Q/\mathfrak{p}$ with $a_i \neq 0$ such that $a_i c_i - b_i = 0$. This means that there are elements x_i, y_i in Q with $x_i \notin \mathfrak{P}$ such that $x_i z_i - y_i \in \mathfrak{P}$. It follows that $\mathfrak{P} \cap Q[z_1, \ldots, z_i]$ for no value of i is generated by $\mathfrak{P} \cap Q[z_1, \ldots, z_{i-1}]$. Hence we obtain

$$H(\mathfrak{P}; n) = H^{(j)}(\mathfrak{p}; n) \quad n = 0, 1, 2, \ldots .$$

By a similar but less detailed discussion one finds that among the numbers $0, 1, \ldots, j$ there is a number i such that

$$H(\mathfrak{M}; n) = H^{(i)}(\mathfrak{m}; n) \quad n = 0, 1, 2, \ldots,$$

so that certainly

$$H(\mathfrak{M}; n) \leqslant H^{(j)}(\mathfrak{m}; n) \quad n = 0, 1, 2, \ldots .$$

(Actually one can show that equality holds.)

Insertion of the expressions for $H(\mathfrak{P}; n)$ and $H(\mathfrak{M}; n)$ that have now been obtained, in the inequality previously derived gives

$$H^{(j+2)}(\mathfrak{p}; n) \leqslant H^{(j+1)}(\mathfrak{m}; n) \quad n = 0, 1, 2, \ldots,$$

which completes the proof of Theorem 1.

Proof of Theorem 2

Let us first introduce a new notion and settle a question of notation.

Let R be a commutative ring with unity element and let $f_1, \ldots, f_s$ be elements of R. The elements $f_1, \ldots, f_s$ are called *independent in* R, or if no confusion is to be feared, *independent*, if for every system $a_1, \ldots, a_s$ of s elements in R it is true that

$$a_1 f_1 + \ldots + a_s f_s = 0 \text{ implies } a_1, \ldots, a_s \in (f_1, \ldots, f_s).$$

This condition can also be expressed by the inclusions

$$(f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_s) : f_i \subseteq (f_1, \ldots, f_s) \quad i = 1, 2, \ldots, s.$$

It entails, if we put $(f_1, \ldots, f_s) = \mathfrak{q}$, that $\mathfrak{q}/\mathfrak{q}^2$ is a free $R/\mathfrak{q}$-module in which $f_1, \ldots, f_s$ represent a basis. Conversely, if R is a *local ring* and if $\mathfrak{q}$ is an ideal in R such that $\mathfrak{q}/\mathfrak{q}^2$ is a free $R/\mathfrak{q}$-module with a basis consisting of s elements, then every minimal system of generators of $\mathfrak{q}$ consists of s elements which are independent in R. Let us finally note that if $f_1, \ldots, f_s$ are independent in R and if R_1 is a unitary R-flat extension of R, then $f_1, \ldots, f_s$ are independent also in R_1 (cf. e.g. [4], the appendix).

The length of a primary ideal $\mathfrak{q} = (q_1, \ldots, q_s)$ of a Noetherian ring (cf. note (1) p. 74) will be denoted by $L(\mathfrak{q})$ or, alternatively, $L(q_1, \ldots, q_s)$. If $\mathfrak{q} = (q_1, \ldots, q_s) = (1)$ we put $L(\mathfrak{q}) = L(q_1, \ldots, q_s) = 0$.

We shall prove four lemmata, the last of which represents that case of the theorem in which the characteristic of $Q/\mathfrak{q}$ is positive.

LEMMA 3. *Let $f_1, \ldots, f_s, g_1$ be elements in a commutative ring with unity element. Suppose that $f_1, \ldots, f_s$ are independent and that $f_1 \in (g_1)$. Then $g_1, f_2, \ldots, f_s$ are also independent. Moreover,*

$$(f_2, \ldots, f_s) : g_1 \subseteq (f_1, \ldots, f_s).$$

Proof. Given a relation $a_1 g_1 + a_2 f_2 + \ldots + a_s f_s = 0$, it follows from the supposition, by multiplication with an element h_1 for which $g_1 h_1 = f_1$, that $a_1 \in (f_1, \ldots, f_s)$, say $a_1 = b_1 f_1 + \ldots + b_s f_s$. Insertion of this expression for a_1 in the given relation results in a linear relation between $f_1, \ldots, f_s$ with the coefficient $a_i + b_i g_1$ for f_i $(i = 2, \ldots, s)$, whence, by the supposition, $a_i \in (g_1, f_2, \ldots, f_s)$ $(i = 2, \ldots, s)$. What has now been established concerning $a_1, \ldots, a_s$ proves the lemma.

LEMMA 4. *Let $f_1, \ldots, f_s, g_1, h_1$ be elements of a local ring. Suppose that $f_1, \ldots, f_s$ are independent, that the ideal $(f_1, \ldots, f_s)$ is zero-dimensional, and that $f_1 = g_1 h_1$. Then*

$$L(f_1, \ldots, f_s) = L(g_1, f_2, \ldots, f_s) + L(h_1, f_2, \ldots, f_s).$$

Proof. The length of $(f_1, \ldots, f_s)$ equals the sum of the lengths of $(f_1, \ldots, f_s, g_1)$ and $(f_1, \ldots, f_s) : g_1$ (cf. [6], (1.5), p. 3). By Lemma 3 the latter ideal is equal to $(h_1, f_2, \ldots, f_s)$. Hence the result.

LEMMA 5. *Let $f_1, \ldots, f_s$ be elements of a local ring Q with the maximal ideal $\mathfrak{m} = (u_1, \ldots, u_r)$. Let p be a prime number, n a natural number, and k a non-negative integer. Then there exists an extension Q_1 of Q with the following properties:*

(i) Q_1 *is a free* Q*-module;*

(ii) Q_1 *is a local ring whose maximal ideal is generated by* $\mathfrak{m}$*;*

(iii) *each of the elements* $f_1, \ldots, f_s$ *can be written on the form*

$$\sum_{i_1+\ldots+i_r<k} a_{i_1,\ldots,i_r} u_1^{i_1} \ldots u_r^{i_r} + g,$$

where $g \in \mathfrak{m}^k Q_1$ *and where the coefficients* $a_{i_1,\ldots,i_r}$ *are* p^n*:th powers of elements in* Q_1.

Proof. By induction on primarily s and k the proof of the lemma can be reduced to a proof of the following assertion: If a is an element of a local ring Q with maximal ideal $\mathfrak{m} = (u_1, \ldots, u_r)$, and if p is a prime, then there is an extension Q_1 of Q such that the conditions (i) and (ii) of the lemma are fulfilled and such that a is congruent modulo $\mathfrak{m}Q_1$ to a pth power in Q_1. This assertion is trivially true if a represents a pth power in $Q/\mathfrak{m}$ in which case we can take $Q_1 = Q$. Otherwise we can choose $Q_1 = Q[z]/(z^p - a)$ where z is a variable over Q. Obviously this choice makes Q_1 in a natural way an extension of Q satisfying the condition (i). Since moreover Q_1 is integral over Q, every maximal ideal of Q_1 must contain $\mathfrak{m}Q_1$ (see [6], Section 10). On the other hand, $\mathfrak{m}Q_1$ is a maximal ideal, since $Q_1/\mathfrak{m}Q_1$ has the form $(Q/\mathfrak{m})[z]/(z^p - \bar{a})$, where $\bar{a}$ is the residue class represented by a in $Q/\mathfrak{m}$, and where consequently the polynomial $z^p - \bar{a}$ is irreducible (cf. [9], the end of § 56). Hence the condition (ii) is also satisfied. It is finally evident that a is congruent modulo $\mathfrak{m}Q_1$ to a pth power in Q_1.

LEMMA 6. *Let* Q *be a local ring,* $\mathfrak{m}$ *its maximal ideal, and* $\mathfrak{q}$ *an* $\mathfrak{m}$*-primary ideal. Assume that* $Q/\mathfrak{m}$ *and* $Q/\mathfrak{q}$ *have the characteristic* $p > 0$ *and that* $\mathfrak{q}/\mathfrak{q}^2$ *is a free* $Q/\mathfrak{q}$*-module. Then the minimum number of generators of* $\mathfrak{q}$ *is not larger than the minimum number of generators of* $\mathfrak{m}$.

Proof. Denote by r and s the minimum numbers of generators of $\mathfrak{m}$ and $\mathfrak{q}$ resp. Put $\mathfrak{m} = (u_1, \ldots, u_r)$ and $\mathfrak{q} = (f_1, \ldots, f_s)$. Choose natural numbers n and k such that $p^n > L(\mathfrak{q})$ and $\mathfrak{m}^k \subseteq \mathfrak{m}\mathfrak{q}$. Determine Q_1 according to Lemma 5 so that the conditions (i)–(iii) of this lemma become fulfilled for the quantities now actual. Put

$$Q_2 = Q_1[z_1, \ldots, z_r]/(z_1^{p^n} - u_1, \ldots, z_r^{p^n} - u_r),$$

where $z_1, \ldots, z_r$ are independent indeterminates over Q. Then Q_2 is in a natural way an extension of Q and is free and hence flat over this ring. Moreover, Q_2 is a local ring, say with the maximal ideal $\mathfrak{m}_2$, and $L(\mathfrak{m}Q_2) = p^{nr}$. Each of the elements $f_1, \ldots, f_s$

can be written as a sum of p^nth powers of elements in $\mathfrak{m}_2$ plus an element of $\mathfrak{m}^k Q_2 \subseteq \mathfrak{m}_2 \mathfrak{q}$. Since $p \in \mathfrak{q}$, it follows that there are elements $g_1, \ldots, g_s$ in $\mathfrak{m}_2$ such that f_i is congruent modulo $\mathfrak{m}_2\mathfrak{q}$ to the p^nth power of g_i $(i = 1, 2, \ldots, s)$. This implies that $\mathfrak{q}Q_2$ is generated by the p^nth powers of $g_1, \ldots, g_s$ (cf. [6], (4.1)).

Since Q_2 is Q-flat, it follows that

$$L(\mathfrak{q}Q_2) = L(\mathfrak{m}Q_2)\, L(\mathfrak{q}) = p^{nr} L(\mathfrak{q})$$

(see [6], (19.1)).

On the other hand, $f_1, \ldots, f_s$ are independent in Q and therefore, on account of the flatness, also in Q_2. This implies that also the p^nth powers of $g_1, \ldots, g_s$ are independent in Q_2. Hence, by repeated application of Lemma 3 and Lemma 4,

$$L(\mathfrak{q}Q_2) = p^{ns} L((g_1, \ldots, g_s)\, Q_2) \geqslant p^{ns}.$$

This gives a contradiction for $s > r$ as, by our choice of n, p^n is larger than $L(\mathfrak{q})$. Thus $s \leqslant r$, and the lemma is proved.

To prove Theorem 2 we shall show that if there were a counter-example to this theorem, we could construct one to Lemma 6.

Let Q be a local ring, $\mathfrak{m}$ its maximal ideal, and $\mathfrak{q}$ an $\mathfrak{m}$-primary ideal. In order that this triplet of objects shall be a counter-example to Theorem 2 it is necessary and sufficient that there exist integers r and s such that $r = \text{length}_Q(\mathfrak{m}/\mathfrak{m}^2)$, $s = \text{length}_Q(\mathfrak{q}/\mathfrak{m}\mathfrak{q})$, $\text{length}_Q(\mathfrak{q}/\mathfrak{q}^2) = sL(\mathfrak{q})$, and $s > r$. The necessity is obvious. Suppose on the other hand that the conditions are fulfilled. Then $\mathfrak{q}/\mathfrak{q}^2$ can be generated by s elements, and consequently there is a Q-homomorphism of the direct sum of s copies of $Q/\mathfrak{q}$ onto $\mathfrak{q}/\mathfrak{q}^2$. This homomorphism must be an isomorphism as the modules constituting its domain and range have the same length. Thus $\mathfrak{q}/\mathfrak{q}^2$ is a free $Q/\mathfrak{q}$-module. Hence the sufficiency. We note that to test if the condition is satisfied in a special case, it suffices to know the lengths of the ideals $\mathfrak{m}^2$, $\mathfrak{q}$, $\mathfrak{m}\mathfrak{q}$, and $\mathfrak{q}^2$.

Suppose that the triplet Q_1, $\mathfrak{m}_1$, $\mathfrak{q}_1$ is a counter-example to Theorem 2. Without loss of generality we can assume that $\mathfrak{q}_1^2 = (0)$, so that in particular Q_1 is zero-dimensional and hence complete, for if necessary we can pass from Q_1 to $Q_1/\mathfrak{q}_1^2$. On account of Lemma 6 the characteristic of $Q_1/\mathfrak{m}_1$ must be zero. Denote the minimum number of generators of $\mathfrak{m}_1$ by r. By the structure theorems of Cohen there is a ring homomorphism $K[x] \to Q_1$ (onto), where $K[x]$ is a polynomial ring in r variables $x_1, \ldots, x_r$ over a field K of characteristic zero, and where the inverse image of $\mathfrak{m}_1$ is $(x_1, \ldots, x_r)$. Using from now on a notation which does not quite agree with that of the theorem, let us denote the inverse images of $\mathfrak{m}_1$, $\mathfrak{q}_1$, and (0) under $K[x] \to Q_1$ by $\mathfrak{m}$, $\mathfrak{q}$, and $\mathfrak{a}$ resp.,

so that especially $\mathfrak{m} = (x_1, \ldots, x_r)$. Then $\mathfrak{m}^2 \supseteq \mathfrak{a}$ and, for a suitable choice of the natural number n, $\mathfrak{q} \supseteq \mathfrak{a} \supseteq \mathfrak{q}^2 \supseteq \mathfrak{m}^n$. When $\mathfrak{m}$ is given as $(x_1, \ldots, x_r)$, these inclusions assure us in particular that the ideals $\mathfrak{q}$ and $\mathfrak{a}$ are $\mathfrak{m}$-primary. Let now $\bar{K}$ be a field of positive characteristic and let $\bar{K}[\bar{x}] = \bar{K}[\bar{x}_1, \ldots, \bar{x}_r]$ be a polynomial ring over $\bar{K}$ in r variables. Let further $\bar{\mathfrak{a}}$ and $\bar{\mathfrak{q}}$ be ideals in $\bar{K}[\bar{x}]$ and put $\bar{\mathfrak{m}} = (\bar{x}_1, \ldots, \bar{x}_r)$. Applying the necessary and sufficient condition derived above, we see that the triplet $\bar{K}[\bar{x}]/\bar{\mathfrak{a}}$, $\bar{\mathfrak{m}}/\bar{\mathfrak{a}}$, $\bar{\mathfrak{q}}/\bar{\mathfrak{a}}$ will be a counter-example to Lemma 6 if the following conditions are fulfilled: $\bar{\mathfrak{m}}^2 \supseteq \bar{\mathfrak{a}}$; $\bar{\mathfrak{q}} \supseteq \bar{\mathfrak{a}} \supseteq \bar{\mathfrak{q}}^2 \supseteq \bar{\mathfrak{m}}^n$; the lengths of the ($\bar{\mathfrak{m}}$-primary) ideals $\bar{\mathfrak{q}}$, $\bar{\mathfrak{m}}\bar{\mathfrak{q}} + \bar{\mathfrak{a}}$, and $\bar{\mathfrak{a}}$ coincide with the lengths of the ideals $\mathfrak{q}$, $\mathfrak{m}\mathfrak{q} + \mathfrak{a}$, and $\mathfrak{a}$. We shall show how one can construct $\bar{K}$, $\bar{\mathfrak{q}}$, and $\bar{\mathfrak{a}}$ from K, $\mathfrak{q}$, and $\mathfrak{a}$ so that these conditions become satisfied.

Refine the chain

$$K[x] \supset \mathfrak{q} \supseteq \mathfrak{m}\mathfrak{q} + \mathfrak{a} \supseteq \mathfrak{a} \supseteq \mathfrak{q}^2 \supseteq \mathfrak{m}^n$$

to a composition chain $\quad \mathfrak{q}_0 \supset \mathfrak{q}_1 \supset \ldots \supset \mathfrak{q}_k.$

Choose elements $f_0 = 1, f_1, f_2, \ldots, f_{k-1}$ of $K[x]$ such that

$$f_\nu \in \mathfrak{q}_\nu, \quad f_\nu \notin \mathfrak{q}_{\nu+1} \qquad (\nu = 0, 1, \ldots, k-1).$$

Denote the power products of degree n in $x_1, \ldots, x_r$ by $f_k, \ldots, f_m$. Then $\mathfrak{q}_\nu = (f_\nu, f_{\nu+1}, \ldots, f_m)$ $(\nu = 0, 1, \ldots, k)$. Determine h, i, and j such that $\mathfrak{q}_h = \mathfrak{q}$, $\mathfrak{q}_i = \mathfrak{m}\mathfrak{q} + \mathfrak{a}$ and $\mathfrak{q}_j = \mathfrak{a}$. Consider the following, actually valid inclusions:

$$(x_1, \ldots, x_r)\,(f_\nu) \subseteq \mathfrak{q}_{\nu+1} \quad (\nu = 0, 1, \ldots, k-1);$$

$$\mathfrak{q}_i \subseteq (x_1, \ldots, x_r)\,\mathfrak{q}_h + \mathfrak{q}_j;$$

$$(x_1, \ldots, x_r)\,\mathfrak{q}_h + \mathfrak{q}_j \subseteq \mathfrak{q}_i;$$

$$\mathfrak{q}_h^2 \subseteq \mathfrak{q}_j.$$

Within these inclusions, replace first everywhere $\mathfrak{q}_\mu$ by $(f_\mu, f_{\mu+1}, \ldots, f_m)$ $(\mu = 0, 1, \ldots, k)$ and then every ideal-product of the form $(\ldots a_\mu \ldots)(\ldots b_\nu \ldots)$ by $(\ldots a_\mu b_\nu \ldots)$. In each of the inclusions thus obtained, express every polynomial that occurs as a basis element on the left-hand side as a linear combination of the polynomials that occur as basis elements on the right-hand side. Let those polynomials which appear as coefficients in these linear combinations, in conjunction with the polynomials $f_0, f_1, \ldots, f_m$, form the set S.

Suppose now that we can find a valuation of K with valuation ring $\mathfrak{o}$ and residue class field $\bar{K}$ such that $\bar{K}$ has positive characteristic and such that $S \subseteq \mathfrak{o}[x]$. Let $\bar{K}[\bar{x}]$ be a polynomial ring over $\bar{K}$ in r variables $\bar{x}_1, \ldots, \bar{x}_r$. Then there is a natural ring

6 — 642906 *Acta mathematica* 112. Imprimé le 21 septembre 1964.

homomorphism $\mathfrak{o}[x] \to \bar{K}[\bar{x}]$ mapping $\mathfrak{o}$ onto $\bar{K}$ and carrying x_ν into $\bar{x}_\nu$ $(\nu = 1, 2, \ldots, r)$. For $f \in \mathfrak{o}[x]$, let $\bar{f}$ be the image of f under this homomorphism. Define the ideals $\bar{\mathfrak{q}}_\nu$ $(\nu = 0, 1, \ldots, k)$, $\bar{\mathfrak{q}}$, and $\bar{\mathfrak{a}}$ in $\bar{K}[\bar{x}]$ by putting $\bar{\mathfrak{q}}_\nu = (\bar{f}_\nu, \bar{f}_{\nu+1}, \ldots, \bar{f}_m)$, $\bar{\mathfrak{q}} = \bar{\mathfrak{q}}_h$, and $\bar{\mathfrak{a}} = \bar{\mathfrak{q}}_j$. Obviously, these ideals, except $\bar{\mathfrak{q}}_0$, which equals (1), are primary for $(\bar{x}_1, \ldots, \bar{x}_r)$. Moreover, it is seen that the inclusions which were considered above, remain valid if x_μ, f_μ, and $\mathfrak{q}_\mu$ are replaced by $\bar{x}_\mu$, $\bar{f}_\mu$, and $\bar{\mathfrak{q}}_\mu$ for all possible values of the index μ. It follows, first that $L(\bar{\mathfrak{q}}_\nu) - L(\bar{\mathfrak{q}}_{\nu-1}) \leqslant 1$ $(\nu = 1, 2, \ldots, k)$, and hence, as evidently $L(\bar{\mathfrak{q}}_k) - L(\bar{\mathfrak{q}}_0) = k$, that $L(\bar{\mathfrak{q}}_\nu) = \nu$ $(\nu = 0, 1, \ldots, k)$, then that the ideals $\bar{\mathfrak{q}}$, $\bar{\mathfrak{m}}\bar{\mathfrak{q}} + \bar{\mathfrak{a}}$, and $\bar{\mathfrak{a}}$ have the same lengths h, i, and j as the ideals $\mathfrak{q}$, $\mathfrak{m}\mathfrak{q} + \mathfrak{a}$, and $\mathfrak{a}$. Furthermore, it is clear that $\bar{\mathfrak{m}}^2 \supseteq \bar{\mathfrak{a}}$ and that $\bar{\mathfrak{q}} \supseteq \bar{\mathfrak{a}} \supseteq \bar{\mathfrak{q}}^2 \supseteq \bar{\mathfrak{m}}^n$. Thus $\bar{K}$, $\bar{\mathfrak{q}}$, and $\bar{\mathfrak{a}}$ satisfy all the conditions posed.

It only remains to find a valuation of the indicated kind. Let α_ν $(\nu = 1, 2, \ldots, N)$ be the elements of K that occur as coefficients of the polynomials in the set S. Let $\varkappa_1, \ldots, \varkappa_k$ be a transcendence basis of the subfield of K generated by the α_ν, and let for $\nu = 1, 2, \ldots, N$ the element α_ν be a zero of a polynomial

$$a_\nu X^{n_\nu} + b_\nu X^{n_\nu - 1} + \ldots$$

with coefficients in the ring $Z[\varkappa_1, \ldots, \varkappa_k]$ generated by $\varkappa_1, \ldots, \varkappa_k$ over the ring Z of rational integers. Fix a homomorphism $Z[\varkappa_1, \ldots, \varkappa_k] \to Z$ and choose a prime number p such that none of the elements a_ν is carried into 0 under the composed homomorphism

$$Z[\varkappa_1, \ldots, \varkappa_k] \to Z \to Z/(p).$$

Obviously every valuation that belongs to an extension $K \to \{\bar{K}, \infty\}$ of this composed homomorphism meets the requirements. That there exists at least one such extension, follows from the theorem on extension of homomorphisms (specializations) (see e.g. [10], Chap. 6, Theorem 5′, p. 13).

Thus we have shown that a counter-example to Theorem 2 leads to a counter-example to Lemma 6. This proves the theorem since the lemma has already been established.

Proof of the Addendum to Theorem 2

The reasoning will largely run parallel to that of the proof of Theorem 2 and will partly be presented in a summary fashion.

Under the assumptions of Theorem 2 we have to show that if the difference between the minimum number of generators of $\mathfrak{m}$ and the minimum number of generators of $\mathfrak{q}$ is not larger than one unit, then $Q/\mathfrak{q}$ has the form

$$K[[x_1, \ldots, x_r]]/(c_1, \ldots, c_r).$$

The assertion can be given the seemingly stronger but equivalent wording that in any representation of $Q/\mathfrak{q}$ on the form $K[[x_1, \ldots, x_r]]/\mathfrak{c}$ the ideal $\mathfrak{c}$ can be generated by r elements. For if $\mathfrak{c}$ is an ideal (not necessarily zero-dimensional) of $K[[x_1, \ldots, x_r]]$, and if R is a ring and $\mathfrak{d}$ an ideal of R such that there are ring isomorphisms

$$R \approx K[[x_1, \ldots, x_r]], \qquad R/\mathfrak{d} \approx K[[x_1, \ldots, x_r]]/\mathfrak{c},$$

then $\mathfrak{d}$ can be generated by as few elements as $\mathfrak{c}$. To see this, one can first, by a simple argument, pass to the case where $\mathfrak{c} \subseteq (x_1, \ldots, x_r)^2$. In $R/\mathfrak{d}$ there are a well-determined field and r well-determined elements which correspond by the isomorphism to K and $x_1, \ldots, x_r$ resp. By lifting this field (cf. the method in [2]) and these r elements in an arbitrary way from $R/\mathfrak{d}$ to R, one obtains in a natural manner an isomorphism between R and $K[[x_1, \ldots, x_r]]$ which induces the given isomorphism between $R/\mathfrak{d}$ and $R/\mathfrak{c}$ and consequently carries the ideals $\mathfrak{d}$ and $\mathfrak{c}$ into one another. Hence the result.

We shall consider separately the two cases in which the characteristic of $Q/\mathfrak{m}$ and $Q/\mathfrak{q}$ is zero and different from zero resp. As in the proof of the theorem, a counter-example belonging to the first case can be transformed into one belonging to the second. To show this, let us suppose that there exists a counter-example belonging to the first case. Using a temporary notation, we can assume (cf. p. 80) that it has the form $K[x]/\mathfrak{a}$, $\mathfrak{m}/\mathfrak{a}$, $\mathfrak{q}/\mathfrak{a}$ where K denotes a field of characteristic zero, x a set of r variables $x_1, \ldots, x_r$ over K, $\mathfrak{m}$ the ideal $(x_1, \ldots, x_r)$, and $\mathfrak{q}$ and $\mathfrak{a}$ ideals such that $\mathfrak{m}^2 \supseteq \mathfrak{a}$ and $\mathfrak{q} \supseteq \mathfrak{a} \supseteq \mathfrak{q}^2 \supseteq \mathfrak{m}^n$, n being some natural number. The integer $\text{length}_{K[x]}(\mathfrak{q}/\mathfrak{m}\mathfrak{q})$ which gives the minimum number of generators of the ideal $\mathfrak{q}K[[x]]$, must be larger than r. In view of the alternative wording of the assertion, it suffices to derive from K, $\mathfrak{q}$, $\mathfrak{a}$ a new triplet $\bar{K}$, $\bar{\mathfrak{q}}$, $\bar{\mathfrak{a}}$ satisfying the same conditions as in the proof of the theorem and in addition the condition that the length of $\bar{\mathfrak{m}}\bar{\mathfrak{q}}$ shall coincide with that of $\mathfrak{m}\mathfrak{q}$. To meet these requirements we have, roughly speaking, to find a specialization which to a sufficient degree preserves the *two* chains

$$K[x] \supset \mathfrak{q} \supseteq \mathfrak{m}\mathfrak{q} + \mathfrak{a} \supseteq \mathfrak{a} \supseteq \mathfrak{q}^2 \supseteq \mathfrak{m}^n,$$

$$K[x] \supset \mathfrak{q} \supseteq \mathfrak{m}\mathfrak{q} \supseteq \mathfrak{m}^n.$$

This can be done by treating separately each of the chains as in the proof of the theorem, say by introducing the refinements $\{\mathfrak{q}_\nu\}_0^k$ and $\{\mathfrak{q}'_\nu\}_0^k$ resp., yet choosing a common valuation which shall moreover satisfy conditions sufficient to preserve the inclusions

$$\mathfrak{q}_h \subseteq \mathfrak{q}'_h, \quad \mathfrak{q}'_h \subseteq \mathfrak{q}_h,$$

h being the length of $\mathfrak{q}$, so that we can put $\bar{\mathfrak{q}} = \bar{\mathfrak{q}}_h = \bar{\mathfrak{q}}'_h$. We content ourselves with these indications.

It remains to consider the second case. Thus we assume that the characteristic of $Q/\mathfrak{m}$ and $Q/\mathfrak{q}$ is a prime p. Without loss of generality we can further assume that Q is zero-dimensional. Let us denote the minimum number of generators of $\mathfrak{m}$ and $\mathfrak{q}$ by r and s resp., and let n be an arbitrary natural number. We introduce new objects according to the following list.

C — a coefficient ring of Q in accordance with the structure theorems of Cohen;

$C[x_1, \ldots, x_r]$ — a polynomial ring over C in r variables;

$C[x_1, \ldots, x_r] \to Q$ — a ring homomorphism which carries C into itself and $x_1, \ldots, x_r$ into a system of generators of $\mathfrak{m}$;

$\mathfrak{A}$ — the kernel of the above homomorphism;

$F_1, \ldots, F_s$ — elements of the ideal $(x_1, \ldots, x_r)$ of $C[x_1, \ldots, x_r]$ which under the above homomorphism are carried into a system of generators of $\mathfrak{q}$;

C_1 — an extension of C with the following properties (cf. Lemma 5):

(i) C_1 is a free C-module,

(ii) C_1 is a local ring whose maximal ideal, like that of C, is generated by p,

(iii) if we form in a natural way the common extension $C_1[x_1, \ldots, x_r]$ of C_1 and $C[x_1, \ldots, x_r]$, then in this extension each of the elements $F_1, \ldots, F_s$ is congruent modulo $p(x_1, \ldots, x_r)$ to a polynomial whose coefficients are p^nth powers of elements of C_1 and whose constant term is zero;

$C_1[z_1, \ldots, z_r]$ — a polynomial ring over C_1 in r variables, in which $C[x_1, \ldots, x_r]$ is imbedded by inclusion of C in C_1 and identification of $x_1, \ldots, x_r$ with the p^nth powers of $z_1, \ldots, z_r$ resp.;

$G_1, \ldots, G_s$ — elements of $C_1[z_1, \ldots, z_r]$ such that in this ring the congruences

$$F_i \equiv G_i^{p^n} \bmod p(z_1, \ldots, z_r)$$

hold true for $i = 1, 2, \ldots, r$ (cf. the proof of Lemma 6).

Let us write x for the set $\{x_1, \ldots, x_r\}$, similarly F for $\{F_1, \ldots, F_s\}$, etc. If R is a Noetherian ring and if $A_1, \ldots, A_t$ are elements or sets of elements in R which together generate a zero-dimensional primary ideal of R, we shall denote the length of this ideal by $L_R(A_1, \ldots, A_t)$.

Obviously $C_1[z]$ is a flat $C[x]$-module, and it is easy to see that the ideal $(p, x)C_1[z]$ has the length p^{nr}. Hence (see [6], (19.1))

$$L_{C_1[z]}(F, \mathfrak{A}) = p^{nr} L_{C[x]}(F, \mathfrak{A}).$$

The ideals $(F, \mathfrak{A})$ and $(G^{p^n}, \mathfrak{A})$ in $C_1[z]$ differ at most by elements in $p(z)$. As $p \in (F, \mathfrak{A})$ and as $(\mathfrak{A})$ contains a power of (z), it follows that they are equal (cf. [6], (4.1)). Thus we can substitute the set of the p^nth powers of $G_1, \ldots, G_s$ for F on the left-hand side of the equality. Moreover, the elements represented by these p^nth powers in $C_1[z]/\mathfrak{A}C_1[z]$ must be independent (cf. the introduction to the proof of Theorem 2). By repeated application of Lemma 3 and Lemma 4 we therefore obtain (similarly as in the proof of Lemma 6)

$$p^{ns} L_{C_1[z]}(G, \mathfrak{A}) = p^{nr} L_{C[x]}(F, \mathfrak{A}).$$

Since the ideals on both sides contain p, we can pass to the respective residue class rings modulo (p). Denote the images of C, C_1, $\mathfrak{A}$, F, G, x, and z under the natural homomorphism of $C_1[z]$ onto $C_1[z]/pC_1[z]$ by K, K_1, $\mathfrak{a}$, f, g, x, and z resp. The images of $x_1, \ldots, x_r$ and $z_1, \ldots, z_r$ which are thus denoted by the same symbols as their originals, are obviously each a set of independent variables over K and K_1. Observing that $C[x]/pC[x]$ is naturally included in $C_1[z]/pC_1[z]$ as $C_1[z]$ is $C[x]$-flat, we deduce

$$L_{K_1[z]}(g, \mathfrak{a}) = p^{n(r-s)} L_{K[x]}(f, \mathfrak{a}).$$

Let σ be the isomorphism of $K_1[z]$ into itself that carries every element into its pth power. Application of σ^n to the ring and the ideal on the left-hand side gives

$$L_{K_1^{\sigma^n}[x]}(f, \mathfrak{a}^{\sigma^n}) = p^{n(r-s)} L_{K[x]}(f, \mathfrak{a}).$$

In this formula we first replace $K_1^{\sigma^n}$ and K by an infinite common extension field M. This does not affect the significance or validity of the formula: the ideals on both sides remain primary and their lengths unaltered (cf. [6], (19.1)). Evidently we can then replace $M[x]$ by the local ring R associated with $(x)M[x]$. Observing finally that the image of $\mathfrak{a}$ under σ^n is contained in the p^nth power of $\mathfrak{a}$, we derive

$$L_R(f, \mathfrak{a}^{p^n}) \leqslant p^{n(r-s)} L_R(f, \mathfrak{a}). \qquad (*)$$

As any (x)-primary ideal of $K[x]$ generates an ideal of the same length in R, we may express the assertion to be proved as follows: if $s=r$ or $s=r-1$, then the ideal $(\mathfrak{a}, f)$ of R can be generated by r elements. We shall deduce this from (*).

From now on, let (f), $(\mathfrak{a}, f)$, $(\mathfrak{a}^{p^n}, f)$, and, later, (a, f) be understood as ideals of R.

Assume first that $s=r$. Then, by (*), $\mathfrak{a} \subseteq (f, \mathfrak{a}^{p^n})$. As $\mathfrak{a}$ is contained in the maximal ideal of R and as n may be taken arbitrarily large, we deduce that $\mathfrak{a} \subseteq (f)$ (cf. [6], (4.2)), whence the result.

Assume then that $s=r-1$. In view of (*) the dimension of the local ring $R/(f)$ cannot be larger than one. This ring must therefore be a one-dimensional Macaulay local ring (see e.g. [6], Section 25, esp. (25.4)). Since M was chosen as an infinite field, we can, by a result of Northcott and Rees, find an element a of $(\mathfrak{a}, f)$ such that $(\mathfrak{a}, f)/(f)$ is integral over $(a, f)/(f)$ and consequently has the same multiplicity as this ideal (see [7]). Then

$$e((\mathfrak{a}, f)/(f)) = \lim_{n\to\infty} \frac{1}{p^n} L((\mathfrak{a}^{p^n}, f)) \leqslant L((\mathfrak{a}, f)) \leqslant L((a, f)) = e((a, f)/(f)) = e((\mathfrak{a}, f)/(f)),$$

where $e(\ )$ denotes the multiplicity of the ideal within the parentheses. The second step of this chain of equalities and inequalities follows by (*), and the two last steps by the fact that $R/(f)$ is a Macaulay local ring and by the choice of a resp. Since the outer terms of the chain are equal, the two middle ones must also be so. This gives $(\mathfrak{a}, f) = (a, f)$ and hence the result.

The proof of the Addendum to Theorem 2 is thereby finished.

Remarks

1. *Concerning Theorem 2.*

I do not know if it is necessary to assume that $Q/\mathfrak{q}$ is equicharacteristic. I should rather expect that it is not.

2. *Concerning the Addendum to Theorem 2.*

One cannot cancel the assumption that the minimum number of generators of $\mathfrak{q}$ is not more than one unit less than the minimum number of generators of $\mathfrak{m}$. Example: $Q = K[x, y, z]/((x)^2 + (y, z)^n)$ (K a field, x, y, z variables, $n \geqslant 2$), $\mathfrak{q}$ = the ideal generated by the element represented by x.

3. *Some alternatives to the statement about Q_0 and Q on p. 72.*

If $\mathfrak{p}$ is a prime ideal of a Noetherian ring, let $f(\mathfrak{p}; z)$ denote the function

$$\sum_{\nu=0}^{\infty} H(\mathfrak{p}; \nu) z^{\nu} \quad 0 < z < 1.$$

(Samuel's result on the polynomial behavior of $H(\mathfrak{p};\nu)$ for ν large entails that $f(\mathfrak{p};z)$ can be represented by an element of $P[z,(1-z)^{-1}]$, P being the field of rationals.)

In the statement on p. 72 it is assumed that (Q_0, Q) is a couple of local rings with maximal ideals $(\mathfrak{m}_0, \mathfrak{m})$, that Q contains Q_0 and is Q_0-flat, and that $\mathfrak{m}_0 Q$ is $\mathfrak{m}$-primary. It is asserted that there exists an integer k such that

$$H^{(k)}(\mathfrak{m}_0; n) \leqslant H^{(k)}(\mathfrak{m}; n) \quad n = 0, 1, 2, \ldots .$$

Instead of this assertion one may consider the following alternative assertions:

A_1. $$H^{(1)}(\mathfrak{m}_0; n) \leqslant H^{(1)}(\mathfrak{m}; n) \quad n = 0, 1, 2, \ldots .$$

A_2. $$f(\mathfrak{m}_0; z) < f(\mathfrak{m}; z) \quad \text{for} \quad 0 < z < 1$$
$$\text{unless } f(\mathfrak{m}_0; z) \equiv f(\mathfrak{m}; z).$$

A_3. $$f(\mathfrak{m}_0; z) \leqslant f(\mathfrak{m}; z) \quad \text{for} \quad 0 < z < 1.$$

One can show that A_2 is equivalent to the original assertion. Thus A_1, A_2, and A_3 form a sequence of assertions of decreasing strength. Each of them would, if valid, make it possible to extend Theorem 1 or, in case of A_3, an essential part of this theorem to the general case where there is no restriction on the integral closure of $\mathfrak{m}/\mathfrak{p}$. The consideration of A_3 is suggested by the proof of Theorem 1 which seems to indicate that the least value of k answering the claims of that theorem, may increase indefinitely with the minimum number of generators that are needed to form the integral closure of the local ring associated with $\mathfrak{m}/\mathfrak{p}$, and that therefore only a limit result, corresponding to $k = \infty$, can be valid if this integral closure is allowed to be infinite. As to A_1, cf. below.—A priori, none, one, two, or all three of the statements A_1, A_2, A_3 might be valid. I have no clear opinion about which of these four possibilities is most probable.

4. *A case in which A_1 is valid.*

Keeping the notation just employed, I can show that if, for some natural number r, $Q/\mathfrak{m}_0 Q$ has the form

$$K[[x_1, \ldots, x_r]]/(c_1, \ldots, c_r),$$

$K[[x_1, \ldots, x_r]]$ being a ring of formal power series in r indeterminates over a field K, then A_1 holds true. Thus, in view of the Addendum to Theorem 2, A_1 will in particular hold true if $H(\mathfrak{m}_0; 1) \geqslant H(\mathfrak{m}; 1) - 1$.

In outline the proof runs as follows. One may assume that Q_0 and Q are zero-dimensional. These rings can then be represented on the forms $C_0[[u]]/\mathfrak{a}_0$ and $C[[z]]/\mathfrak{a}$

resp., C_0 and C being coefficient rings, u and z standing for sets of r indeterminates, and the inclusion of Q_0 in Q being induced by an injection $\varphi : C_0[[u]] \to C[[z]]$ which, as a result of the special assumption about $Q/\mathfrak{m}_0 Q$, can be chosen so that $\mathfrak{a} = \varphi(\mathfrak{a}_0)\, C[[z]]$. By varying φ in a way that reminds of specialization in algebraic geometry, one can reduce the demonstration to the trivial case in which φ carries each of the indeterminates u into a corresponding indeterminate z.

5. *On the connexions between generalizations of Theorem 1 and statements of the types* A_1, A_2, A_3.

We know that A_1, A_2, and A_3 each would imply a generalization of Theorem 1. I can prove the following partial converse.

Suppose (as in A_1, A_2, A_3) that (Q_0, Q) is a couple of local rings with maximal ideals $(\mathfrak{m}_0, \mathfrak{m})$, that Q contains Q_0 and is Q_0-flat, and that $\mathfrak{m}_0 Q$ is $\mathfrak{m}$-primary. Suppose further that Q_0 and Q are equicharacteristic and that $Q/\mathfrak{m}$ is a separabel extension of its natural subfield $Q_0/\mathfrak{m}_0$. Then there exists a Noetherian ring with prime ideals $\mathfrak{m}_1$ and $\mathfrak{p}_1$ such that $\mathfrak{m}_1 \supset \mathfrak{p}_1$, $\operatorname{rank} \mathfrak{m}_1/\mathfrak{p}_1 = 1$, and

$$H(\mathfrak{p}_1; n) = H(\mathfrak{m}_0; n), \quad n = 0, 1, 2, \ldots,$$

$$H(\mathfrak{m}_1; n) = H^{(1)}(\mathfrak{m}; n) \quad n = 0, 1, 2, \ldots.$$

This means that any result similar to Theorem 1 but general enough to apply to $\mathfrak{m}_1$ and $\mathfrak{p}_1$, would imply a corresponding result concerning Q_0 and Q.

The Noetherian ring that contains $\mathfrak{m}_1$ and $\mathfrak{p}_1$ is obtained by a variation of Akizuki's example of a one-dimensional local domain without finite integral closure ([1]); actually the local ring associated with $\mathfrak{m}_1/\mathfrak{p}_1$ will not have a finite integral closure except when $\mathfrak{m}_0 Q = \mathfrak{m}$. As to the rôle of the assumption that $Q/\mathfrak{m}$ is a separable extension of $Q_0/\mathfrak{m}_0$, cf. [2].

References

[1]. Akizuki, Y., Einige Bemerkungen über primäre Integritätsbereiche mit Teilerkettensatz. *Proc. Phys.-Math. Soc. Japan*, 17 (1935), 327–336.

[2]. Geddes, A., On coefficient fields. *Proc. Glasgow Math. Assoc.*, 4 (1958), 42–48.

[3]. Guérindon, J., Dimension caractéristique d'un anneau noethérien. *C. R. Acad. Sci. Paris*, 256 (1963), 4143–4146.

[4]. Lech, Chr., Note on multiplicities of ideals. *Ark. Math.*, 4 (1960), 63–86.

[5]. Nagata, M., The theory of multiplicity in general local rings. *Proc. of the international symposium on algebraic number theory, Tokyo-Nikko* 1955, pp. 191–226. Science Council of Japan, Tokyo 1956.

[6]. NAGATA, M., *Local rings*, New York 1962.

[7]. NORTHCOTT, D. G., & REES, D., Reductions of ideals in local rings. *Proc. Cambridge Philos. Soc.*, 50 (1954), 145–158.

[8]. SERRE, J.-P., Sur la dimension homologique des anneaux et des modules noethériens. *Proc. of the international symposium on algebraic number theory, Tokyo-Nikko* 1955, pp. 175–189. Science Council of Japan, Tokyo 1956.

[9]. VAN DER WAERDEN, B. L., *Algebra I*, 5th ed. Berlin 1960.

[10]. ZARISKI, O. & SAMUEL, P., *Commutative algebra*. Princeton 1960.

Received February 26, 1964