

COMPOSITIO MATHEMATICA

BALWANT SINGH

**A numerical criterion for the permissibility
of a blowing-up**

Compositio Mathematica, tome 33, n° 1 (1976), p. 15-28

http://www.numdam.org/item?id=CM_1976__33_1_15_0

© Foundation Compositio Mathematica, 1976, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (<http://www.compositio.nl/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

A NUMERICAL CRITERION FOR THE PERMISSIBILITY OF A BLOWING-UP

Balwant Singh

Introduction

Let \mathcal{O} be a noetherian local ring and \mathfrak{p} a proper ideal of \mathcal{O} . The concept of the permissibility of \mathfrak{p} in \mathcal{O} (more precisely, of $\text{Spec}(\mathcal{O}/\mathfrak{p})$ in $\text{Spec} \mathcal{O}$ at the closed point) as a center for blowing-up was introduced by Hironaka in his paper [3] on the resolution of singularities. If the center of a blowing-up $\mathcal{O} \rightarrow \mathcal{O}'$ is permissible in \mathcal{O} then the singularity of \mathcal{O}' is no worse than that of \mathcal{O} . Here, as a measure of singularity, we may take either the characters ν^* , τ^* defined by Hironaka in [3] in case \mathcal{O} is given as the quotient of a regular local ring, or the Hilbert functions of \mathcal{O} and \mathcal{O}' (See [1], [4], [6]). In this note we give a numerical criterion for the permissibility of a blowing-up, i.e. of its center (Theorem 1) and study the effect of an arbitrary blowing-up on the Hilbert function of a local ring (Theorems 2 and 3). As a corollary to Theorem 1, we get yet another criterion for the permissibility of a blowing-up (Corollary (1.4)). The criterion in Theorem 1 leads to the definition of a numerical function $D_{\mathfrak{p}}$ such that \mathfrak{p} is permissible in \mathcal{O} if and only if $D_{\mathfrak{p}} = 0$. (See Remark 2.) A significance of this function $D_{\mathfrak{p}}$ is that it appears explicitly in a comparison between the Hilbert functions of \mathcal{O} and \mathcal{O}' , where $\mathcal{O} \rightarrow \mathcal{O}'$ is a blowing-up of \mathcal{O} with center \mathfrak{p} . (See Theorems 2 and 3.) In Remark 3 below we indicate how the criterion in Theorem 1 compares with a numerical criterion for normal flatness given by Bennett [1].

In order to state our results more precisely, we need some notation. By a *numerical function* H we mean a map $H: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$. If H is a numerical function, we get from H a sequence $\{H^{(r)}\}_{r \geq 0}$ of numerical functions by successive 'integration' as follows: $H^{(0)} = H$ and, for $r \geq 1$,

$$H^{(r)}(n) = \sum_{i=0}^n H^{(r-1)}(i).$$

If H_1, H_2 are numerical functions, then by $H_1 \geq H_2$ we shall always mean the total order inequality, i.e. $H_1(n) \geq H_2(n)$ for every $n \in \mathbb{Z}^+$.

Let \mathcal{O} be a noetherian local ring. For a *proper* ideal \mathfrak{p} of \mathcal{O} we define a numerical function $H_{\mathfrak{p}}$ by

$$H_{\mathfrak{p}}(n) = \dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{p}^n / \mathfrak{m}\mathfrak{p}^n,$$

where \mathfrak{m} is the maximal ideal of \mathcal{O} . This gives us a sequence $\{H_{\mathfrak{p}}^{(r)}\}_{r \geq 0}$ of numerical functions. We write $H_{\mathcal{O}}^{(r)}$ for $H_{\mathfrak{m}}^{(r)}$, so that $\{H_{\mathcal{O}}^{(r)}\}_{r \geq 0}$ is the usual sequence of the Hilbert functions of \mathcal{O} .

We denote by $\dim \mathcal{O}$ the Krull dimension of \mathcal{O} and by $\text{emdim } \mathcal{O}$ the embedding dimension of \mathcal{O} , i.e. $\text{emdim } \mathcal{O} = H_{\mathcal{O}}^{(0)}(1)$.

Recall that a proper ideal \mathfrak{p} of \mathcal{O} is said to be *permissible* in \mathcal{O} (as a center for a blowing-up) if the following two conditions are satisfied:

- (i) *regularity*: \mathcal{O}/\mathfrak{p} is regular
- (ii) *normal flatness*: \mathcal{O} is normally flat along \mathfrak{p} , i.e. the graded \mathcal{O}/\mathfrak{p} -algebra $\text{gr}_{\mathfrak{p}}(\mathcal{O}) = \bigoplus_{n \geq 0} \mathfrak{p}^n / \mathfrak{p}^{n+1}$ is \mathcal{O}/\mathfrak{p} -flat.

THEOREM 1: *Let \mathcal{O} be a noetherian local ring and \mathfrak{p} a proper ideal of \mathcal{O} . Let $d = \dim \mathcal{O}/\mathfrak{p}$ and $e = \text{emdim } \mathcal{O}/\mathfrak{p}$. Then we have $H_{\mathcal{O}}^{(0)} \leq H_{\mathfrak{p}}^{(e)}$. Further, the following three conditions are equivalent:*

- (i) \mathfrak{p} is permissible in \mathcal{O}
- (ii) \mathcal{O}/\mathfrak{p} is regular and $H_{\mathcal{O}}^{(0)} = H_{\mathfrak{p}}^{(d)}$
- (iii) $H_{\mathcal{O}}^{(0)} = H_{\mathfrak{p}}^{(e)}$.

We prove this theorem in § 1.

REMARK 1: For the implication (i) \Rightarrow (ii), cf. [3, Chapter II, Proposition 1].

REMARK 2: For a proper ideal \mathfrak{p} of \mathcal{O} , let us define $D_{\mathfrak{p}} = H_{\mathfrak{p}}^{(e)} - H_{\mathcal{O}}^{(0)}$, where $e = \text{emdim } \mathcal{O}$. Theorem 1 shows that $D_{\mathfrak{p}}$ is a numerical function, and \mathfrak{p} is permissible in \mathcal{O} if and only if $D_{\mathfrak{p}} = 0$. We may therefore call $D_{\mathfrak{p}}$ the *permissibility defect* of \mathfrak{p} . Another justification for the use of this term is provided by Theorem 2, which states, roughly, that if $\mathcal{O} \rightarrow \mathcal{O}'$ is a blowing-up of \mathcal{O} with center \mathfrak{p} , then $H_{\mathcal{O}}^{(0)} - H_{\mathcal{O}'}^{(0)} \geq -D_{\mathfrak{p}}$, where δ is the residue transcendence degree of \mathcal{O}' over \mathcal{O} . In the case when \mathfrak{p} is permissible in \mathcal{O} , the inequality $H_{\mathcal{O}}^{(0)} - H_{\mathcal{O}'}^{(0)} \geq 0$ is already known [6]. One can thus say that under a blowing-up the singularity of \mathcal{O} can become worse only to the extent that the blowing-up is non-permissible, this non-permissibility being measured by the numerical function $D_{\mathfrak{p}}$.

REMARK 3: Bennett has given a numerical criterion for the permissibility of \mathfrak{p} in \mathcal{O} in the case when \mathcal{O}/\mathfrak{p} is regular [1, Theorem (3) and (2.1.2)]. He has shown that if \mathcal{O}/\mathfrak{p} is regular of dimension d then \mathfrak{p} is permissible in \mathcal{O} if and only if $H_{\mathcal{O}}^{(0)} = H_{\mathcal{O}/\mathfrak{p}}^{(d)}$. Let us compare this criterion with the one given in Theorem 1 above. Suppose that \mathcal{O} is excellent. Then we have $H_{\mathcal{O}/\mathfrak{p}}^{(d)} \leq H_{\mathcal{O}}^{(0)}$, where $d = \dim \mathcal{O}/\mathfrak{p}$. (See [1, Theorem (2)] and [6, page 202].) In this case, therefore, the difference $D'_{\mathfrak{p}} = H_{\mathcal{O}}^{(0)} - H_{\mathcal{O}/\mathfrak{p}}^{(d)}$ is a numerical function, and \mathfrak{p} is permissible in \mathcal{O} if and only if $D'_{\mathfrak{p}} = 0$. However, the definition of this measure $D'_{\mathfrak{p}}$ of the deviation of \mathfrak{p} from being permissible requires, in the first place, that \mathfrak{p} be a prime ideal. Even then it is apparently defined (i.e. is non-negative) only for \mathcal{O} excellent, it being not known whether the inequality $H_{\mathcal{O}/\mathfrak{p}}^{(d)} \leq H_{\mathcal{O}}^{(0)}$ holds for non-excellent \mathcal{O} . Moreover, in order that $D'_{\mathfrak{p}} = 0$ imply the permissibility of \mathfrak{p} in \mathcal{O} , we have to assume already that \mathcal{O}/\mathfrak{p} is regular. Finally, $D'_{\mathfrak{p}}$ does not seem to intervene directly in a formula for the difference $H_{\mathcal{O}}^{(0)} - H_{\mathcal{O}}^{(d)}$ as $D_{\mathfrak{p}}$ does. (Here $\mathcal{O} \rightarrow \mathcal{O}'$ is a blowing-up as in Remark 2.) It is interesting, however, to note that if \mathcal{O} is excellent and \mathcal{O}/\mathfrak{p} is regular of dimension d then we have

$$(*) \quad H_{\mathcal{O}/\mathfrak{p}}^{(d)} \leq H_{\mathcal{O}}^{(0)} \leq H_{\mathfrak{p}}^{(d)}$$

and one of these inequalities is an equality if and only if the other is. One may therefore ask: What is the relationship, in this case, between $D_{\mathfrak{p}} = H_{\mathfrak{p}}^{(d)} - H_{\mathcal{O}}^{(0)}$ and $D'_{\mathfrak{p}} = H_{\mathcal{O}}^{(0)} - H_{\mathcal{O}/\mathfrak{p}}^{(d)}$?

REMARK 4: The inequalities (*) of Remark 3 yield another interesting criterion for the permissibility of \mathfrak{p} in \mathcal{O} . (See Corollary (1.4) in § 1.)

REMARK 5: With the notation of Theorem 1, we do not, in general, have the inequality $H_{\mathcal{O}}^{(0)} \leq H_{\mathfrak{p}}^{(d)}$. *Example:* Let \mathcal{O} be a non-regular Cohen-Macaulay local ring of dimension 1 (e.g., $\mathcal{O} = k[[X, Y]]/(Y^2 - X^3)$, where k is a field). Choose any non-zero divisor x in the maximal ideal of \mathcal{O} , and let $\mathfrak{p} = \mathcal{O}x$. Then $d = 0$, $H_{\mathfrak{p}}^{(0)}(n) = 1$ for every n , but $H_{\mathcal{O}}^{(0)}(1) \geq 2$.

REMARK 6: With the notation of Theorem 1, the equality $H_{\mathcal{O}}^{(0)} = H_{\mathfrak{p}}^{(d)}$ alone does not imply that \mathfrak{p} is permissible in \mathcal{O} . *Example:* Let \mathcal{O} be a regular local ring of dimension 1. Let x be any non-zero element in the square of the maximal ideal of \mathcal{O} and let $\mathfrak{p} = x\mathcal{O}$.

We now proceed to state Theorems 2 and 3. Let $\mathcal{O} \rightarrow \mathcal{O}'$ be a blowing-up of \mathcal{O} with center a proper ideal \mathfrak{p} of \mathcal{O} . Let $e = \text{emdim } \mathcal{O}/\mathfrak{p}$. Choose t_1, \dots, t_e in the maximal ideal \mathfrak{m} of \mathcal{O} such that $\mathfrak{m} = \mathfrak{p} + \sum_{i=1}^e t_i \mathcal{O}$. Let

$t_0 \in \mathfrak{p}$ be such that $\mathfrak{p}\mathcal{O}' = t_0\mathcal{O}'$. For such a choice of $t = (t_0, t_1, \dots, t_e)$ we define, for every i , $0 \leq i \leq e$, a sequence $\{\alpha_{t,i}(n)\}_{n \geq 0}$ of ideals of \mathcal{O}' as follows:

$$\alpha_{t,i}(n) = \{f \in \mathcal{O}' \mid t_i f \in \mathfrak{m}'^{n+1} + \sum_{j=0}^{i-1} t_j \mathcal{O}'\},$$

where \mathfrak{m}' is the maximal ideal of \mathcal{O}' . Clearly, $\alpha_{t,i}(n) \supset \mathfrak{m}'^n + \sum_{j=0}^{i-1} t_j \mathcal{O}'$ for every i and n . Let $L_{t,i}$, $0 \leq i \leq e$, be the numerical functions defined by

$$L_{t,i}(n) = \text{length}_{\mathcal{O}'} \alpha_{t,i}(n) / (\mathfrak{m}'^n + \sum_{j=0}^{i-1} t_j \mathcal{O}').$$

THEOREM 2: *Let \mathfrak{p} be a proper ideal of a noetherian local ring \mathcal{O} and let $e = \text{emdim } \mathcal{O}/\mathfrak{p}$. Let $\mathcal{O} \rightarrow \mathcal{O}'$ be a blowing-up of \mathcal{O} with center \mathfrak{p} and let δ be the residue transcendence degree of \mathcal{O}' over \mathcal{O} . Then, for any choice of $t = (t_0, t_1, \dots, t_e)$ as above, we have*

$$H_{\mathcal{O}}^{(0)} - H_{\mathcal{O}'}^{(\delta)} \geq \sum_{i=0}^e L_{t,i}^{(i+\delta)} - D_{\mathfrak{p}} \geq -D_{\mathfrak{p}}.$$

In particular, if \mathfrak{p} is permissible in \mathcal{O} , then

$$H_{\mathcal{O}}^{(0)} - H_{\mathcal{O}'}^{(\delta)} \geq \sum_{i=0}^e L_{t,i}^{(i+\delta)} \geq 0.$$

In the case when $\mathcal{O} \rightarrow \mathcal{O}'$ is residually rational, we can give a more precise formula for the difference $H_{\mathcal{O}}^{(0)} - H_{\mathcal{O}'}^{(0)}$. As above, let $t_0 \in \mathfrak{p}$ be such that $\mathfrak{p}\mathcal{O}' = t_0\mathcal{O}'$. Then \mathcal{O}' is obtained as a localization of the subring $\{f/t_0^n \mid n \geq 0, f \in \mathfrak{p}^n\}$ of \mathcal{O}_{t_0} . We define a sequence $\{\mathfrak{b}_{t_0}(n)\}_{n \geq 0}$ of ideals of \mathcal{O} by

$$\mathfrak{b}_{t_0}(n) = \{f \in \mathfrak{p}^n \mid f/t_0^n \in \mathfrak{m}'^{n+1} + \mathfrak{m}\mathcal{O}'\},$$

where $\mathfrak{m}, \mathfrak{m}'$ are the maximal ideals of $\mathcal{O}, \mathcal{O}'$, respectively. Clearly, $\mathfrak{b}_{t_0}(n) \supset \mathfrak{m}\mathfrak{p}^n$ for every n . Let L_{t_0} be the numerical function defined by

$$L_{t_0}(n) = \text{length}_{\mathcal{O}} \mathfrak{b}_{t_0}(n) / \mathfrak{m}\mathfrak{p}^n.$$

THEOREM 3: *Let the notation be as in Theorem 2. Assume, moreover, that $\mathcal{O} \rightarrow \mathcal{O}'$ is residually rational. Then for any choice of $t = (t_0, t_1, \dots, t_e)$ as above, we have*

$$H_{\mathcal{O}}^{(0)} - H_{\mathcal{O}'}^{(0)} = L_{t_0}^{(e)} + \sum_{i=0}^e L_{t,i}^{(i)} - D_{\mathfrak{p}}.$$

In particular, if \mathfrak{p} is permissible in \mathcal{O} , then

$$H_{\mathcal{O}}^{(0)} - H_{\mathcal{O}'}^{(0)} = L_{t_0}^{(e)} + \sum_{i=0}^e L_{t,i}^{(i)}.$$

Theorems 2 and 3 are proved in § 2.

1. Proof of Theorem 1

(1.1) Let \mathcal{O} be a noetherian local ring with maximal ideal \mathfrak{m} . For any ideal \mathfrak{p} of \mathcal{O} we define

$$\mu(\mathfrak{p}) = \dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{p}/\mathfrak{m}\mathfrak{p},$$

so that $\mu(\mathfrak{p})$ is the cardinality of a minimal set of generators of \mathfrak{p} . Note that, if \mathfrak{p} is a proper ideal of \mathcal{O} , then $\mu(\mathfrak{p}^n) = H_{\mathfrak{p}}^{(0)}(n)$ for every n .

(1.2) LEMMA :

(1) Let \mathfrak{a}_i , $1 \leq i \leq r$, be ideals of \mathcal{O} such that $\mu(\sum_i \mathfrak{a}_i) = \sum_i \mu(\mathfrak{a}_i)$. If S_i is a minimal set of generators of \mathfrak{a}_i , then $\bigcup_i S_i$ is a minimal set of generators of $\sum_i \mathfrak{a}_i$. In particular, for every j , $1 \leq j \leq r$, we have

$$S_j \cap (\mathfrak{m}(\sum_i \mathfrak{a}_i) + \sum_{i \neq j} \mathfrak{a}_i) = \emptyset.$$

(2) Let $\mathfrak{p}, \mathfrak{q}$ be proper ideals of \mathcal{O} and let $\mathfrak{a} = \mathfrak{p} + \mathfrak{q}$. Let $e = \mu(\mathfrak{q})$. Then $H_{\mathfrak{a}}^{(0)} \leq H_{\mathfrak{p}}^{(e)}$.

(3) With the notation of (2), suppose that $H_{\mathfrak{a}}^{(0)} = H_{\mathfrak{p}}^{(e)}$. Then, for every $m, n \geq 0$, we have

$$(a) \mu(\mathfrak{q}^n) = \binom{n+e-1}{e-1}$$

$$(b) \mu(\mathfrak{p}^m \mathfrak{q}^n) = \mu(\mathfrak{p}^m) \mu(\mathfrak{q}^n)$$

$$(c) \mu(\mathfrak{a}^{n+1}) = \mu(\mathfrak{q}^{n+1}) + \mu(\mathfrak{a}^n \mathfrak{p}).$$

PROOF: (1) is immediate. To prove (2) and (3), we have only to observe the following easily verified facts:

$$(i) \mu(\mathfrak{a}^n) \leq \sum_{i=0}^n \mu(\mathfrak{p}^{n-i} \mathfrak{q}^i) \leq \sum_{i=0}^n \mu(\mathfrak{p}^{n-i}) \mu(\mathfrak{q}^i).$$

$$(ii) \mu(\mathfrak{q}^n) \leq \binom{n+e-1}{e-1}.$$

(iii) For any numerical function $H = H^{(0)}$ we have

$$H^{(e)}(n) = \sum_{i=0}^n \binom{i+e-1}{e-1} H^{(0)}(n-i).$$

(1.3) LEMMA : (Bennett). *Let \mathcal{O} be a noetherian local ring and \mathfrak{p} an ideal of \mathcal{O} such that \mathcal{O}/\mathfrak{p} is regular. Let $d = \dim \mathcal{O}/\mathfrak{p}$. Then \mathfrak{p} is permissible in \mathcal{O} if and only if $H_{\mathcal{O}}^{(0)} = H_{\mathcal{O}/\mathfrak{p}}^{(d)}$.*

For a proof of this lemma, see [1, Theorem (3) and 0(2.1.2)].

Before coming to the proof of Theorem 1, we note the following corollary to Theorem 1:

(1.4) COROLLARY : *Suppose \mathcal{O} is excellent¹ and \mathcal{O}/\mathfrak{p} is regular. Then \mathfrak{p} is permissible in \mathcal{O} if and only if $\mu(\mathfrak{p}^n) = \mu(\mathfrak{p}^n \mathcal{O}_{\mathfrak{p}})$ for every $n \geq 0$.*

PROOF: As mentioned in Remark 3 of the Introduction, we have

$$H_{\mathcal{O}/\mathfrak{p}}^{(d)} \leq H_{\mathcal{O}}^{(0)} \leq H_{\mathfrak{p}}^{(d)}.$$

(The second inequality follows from Theorem 1 and the first from [1, Theorem (2)] and [6, page 202].) By Theorem 1, $H_{\mathcal{O}}^{(0)} = H_{\mathfrak{p}}^{(d)}$ if and only if \mathfrak{p} is permissible in \mathcal{O} . By Lemma (1.3), \mathfrak{p} is permissible in \mathcal{O} if and only if $H_{\mathcal{O}/\mathfrak{p}}^{(d)} = H_{\mathcal{O}}^{(0)}$. Therefore, \mathfrak{p} is permissible in \mathcal{O} if and only if $H_{\mathcal{O}/\mathfrak{p}}^{(d)} = H_{\mathfrak{p}}^{(d)}$. Now, clearly, $H_{\mathcal{O}/\mathfrak{p}}^{(d)} = H_{\mathfrak{p}}^{(d)}$ if and only if $H_{\mathcal{O}/\mathfrak{p}}^{(0)} = H_{\mathfrak{p}}^{(0)}$. This proves the corollary, since $\mu(\mathfrak{p}^n) = H_{\mathcal{O}}^{(0)}(n)$ and $\mu(\mathfrak{p}^n \mathcal{O}_{\mathfrak{p}}) = H_{\mathcal{O}/\mathfrak{p}}^{(0)}(n)$.

PROOF OF THEOREM 1: Let \mathfrak{m} be the maximal ideal of \mathcal{O} and let $k = \mathcal{O}/\mathfrak{m}$.

Since $e = \text{emdim } \mathcal{O}/\mathfrak{p}$, there exists an ideal \mathfrak{q} of \mathcal{O} such that $\mathfrak{m} = \mathfrak{p} + \mathfrak{q}$ and $\mu(\mathfrak{q}) = e$. Therefore, the inequality $H_{\mathcal{O}}^{(0)} \leq H_{\mathfrak{p}}^{(e)}$ follows from Lemma (1.2)(2).

¹ It was pointed out by W. Vogel that the proof of this corollary goes through also for non-excellent \mathcal{O} . For it follows, from Lemma 1 of [A. Ljungström, "An inequality between Hilbert functions of certain prime ideals one of which is immediately included in the other", Preprint, University of Stockholm, 1975] that $H_{\mathcal{O}/\mathfrak{p}}^{(d)} \leq H_{\mathcal{O}}^{(0)}$ for arbitrary \mathcal{O} if \mathcal{O}/\mathfrak{p} is regular of dimension d . It was precisely for this inequality that we assumed the excellence of \mathcal{O} . For a more direct proof of this corollary, see [R. Achilles, P. Schenzel and W. Vogel, "Einige Anwendungen der normalen Flachheit", Preprint, Martin-Luther-Universität, 1975].

We now proceed to show that conditions (i), (ii) and (iii) of Theorem 1 are equivalent.

(i) \Rightarrow (ii). Since \mathfrak{p} is permissible in \mathcal{O} , we have $d = e$, and for every $n \geq 0$, $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ is \mathcal{O}/\mathfrak{p} -flat, hence \mathcal{O}/\mathfrak{p} -free. Therefore, we have

$$\begin{aligned} H_{\mathfrak{p}}^{(0)}(n) &= \dim_k \mathfrak{p}^n / \mathfrak{m} \mathfrak{p}^n \\ &= \dim_k \mathfrak{p}^n / \mathfrak{p}^{n+1} \otimes_{\mathcal{O}/\mathfrak{p}} k \\ &= \text{rank}_{\mathcal{O}/\mathfrak{p}} \mathfrak{p}^n / \mathfrak{p}^{n+1} \\ &= \dim_{\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\mathfrak{p}}} \mathfrak{p}^n \mathcal{O}_{\mathfrak{p}} / \mathfrak{p}^{n+1} \mathcal{O}_{\mathfrak{p}} \\ &= H_{\mathcal{O}_{\mathfrak{p}}}^{(0)}(n). \end{aligned}$$

Thus $H_{\mathfrak{p}}^{(0)} = H_{\mathcal{O}_{\mathfrak{p}}}^{(0)}$, so that $H_{\mathfrak{p}}^{(d)} = H_{\mathcal{O}_{\mathfrak{p}}}^{(d)} = H_{\mathcal{O}}^{(0)}$, the last equality by Lemma (1.3).

(ii) \Rightarrow (iii). Since \mathcal{O}/\mathfrak{p} is regular, we have $d = e$.

(iii) \Rightarrow (ii). We have only to show that \mathcal{O}/\mathfrak{p} is regular. Choose $t_1, \dots, t_e \in \mathfrak{m}$ such that their canonical images $\bar{t}_1, \dots, \bar{t}_e$ in $\bar{\mathcal{O}} = \mathcal{O}/\mathfrak{p}$ form a (necessarily minimal) set of generators of $\bar{\mathfrak{m}} = \mathfrak{m}/\mathfrak{p}$. Let $\mathfrak{q} = \sum_{i=1}^e t_i \mathcal{O}$. Then $\mathfrak{m} = \mathfrak{p} + \mathfrak{q}$ and $e = \mu(\mathfrak{q})$. Therefore, the assumption $H_{\mathcal{O}}^{(0)} = H_{\mathfrak{p}}^{(e)}$ implies, by Lemma (1.2)(3), that we have

$$\mu(\mathfrak{q}^n) = \binom{n+e-1}{e-1}$$

(*)

$$\mu(\mathfrak{m}^{n+1}) = \mu(\mathfrak{q}^{n+1}) + \mu(\mathfrak{m}^n \mathfrak{p})$$

for every $n \geq 0$. Let $S_n = \{t^\alpha \mid |\alpha| = n\}$. (Here we have used the standard notation: $t^\alpha = t_1^{\alpha_1} \dots t_e^{\alpha_e}$ and $|\alpha| = \alpha_1 + \dots + \alpha_e$ for $\alpha = (\alpha_1, \dots, \alpha_e) \in (\mathbb{Z}^+)^e$.) It follows from (*) and Lemma (1.2)(1) that the following two statements are true for every $n \geq 0$.

- (1)_n S_n is a minimal set of generators of \mathfrak{q}^n .
- (2)_n If T_n is any minimal set of generators of $\mathfrak{m}^n \mathfrak{p}$, then $T_n \cup S_{n+1}$ is a minimal set of generators of \mathfrak{m}^{n+1} .

Suppose now that \mathcal{O}/\mathfrak{p} is not regular. Then there exists $r \in \mathbb{Z}^+$ and $\alpha = (\alpha_1, \dots, \alpha_e) \in (\mathbb{Z}^+)^e$ with $|\alpha| = r$ such that

$$\bar{t}^\alpha \in \sum_{\substack{|\beta| = r \\ \beta \neq \alpha}} \bar{t}^\beta \bar{\mathcal{O}} + \bar{\mathfrak{m}}^{r+1}.$$

This means that

$$t^\alpha \in \sum_{x \in \mathcal{S}_r - \{t^\alpha\}} x\mathcal{O} + \mathfrak{m}^{r+1} + \mathfrak{p}.$$

We can therefore write $t^\alpha = y + p$ with $p \in \mathfrak{p}$ and

$$y \in \sum_{x \in \mathcal{S}_r - \{t^\alpha\}} x\mathcal{O} + \mathfrak{m}^{r+1}.$$

If $p \neq 0$, let $s \in \mathbb{Z}^+$ be such that $p \in \mathfrak{m}^s \mathfrak{p} - \mathfrak{m}^{s+1} \mathfrak{p}$. Then there exists a minimal set T of generators of $\mathfrak{m}^s \mathfrak{p}$ such that $p \in T$. If $p = 0$, we put $s = \infty$. Now consider the three cases $s+1 < r$, $s+1 = r$ and $s+1 > r$.

Case (1). $s+1 < r$. Then $p = t^\alpha - y \in \mathfrak{m}^r \subset \mathfrak{m}^{s+2}$. This contradicts (2)_s, since we may take $T_s = T$, so that $p \in T_s$.

Case (2). $s+1 = r$. In this case we have

$$t^\alpha = y + p \in \sum_{x \in \mathcal{S}_r - \{t^\alpha\}} x\mathcal{O} + p\mathcal{O} + \mathfrak{m}^{s+2},$$

which again contradicts (2)_s, by taking $T_s = T$.

Case (3). $s+1 > r$. In this case $p \in \mathfrak{m}^s \mathfrak{p} \subset \mathfrak{m}^{r+1}$, so that we have

$$t^\alpha = y + p \in \sum_{x \in \mathcal{S}_r - \{t^\alpha\}} x\mathcal{O} + \mathfrak{m}^{r+1},$$

which contradicts (2)_{r-1}.

This shows that \mathcal{O}/\mathfrak{p} is regular and $d = e$, which proves (ii).

(ii) \Rightarrow (i). We prove this implication by induction on d . The case $d = 0$ is trivial. We shall now prove:

(A) *The implication (ii) \Rightarrow (i) for $d = 1$.*

(B) *The inductive step from $d-1$ to d , assuming (A).*

We first prove (B). Let $d \geq 1$ and let $t_1, \dots, t_d \in \mathfrak{m}$ be such that $\mathfrak{m} = \mathfrak{p} + \sum_{i=1}^d t_i \mathcal{O}$. Let $\mathfrak{n} = \mathfrak{p} + \sum_{i=1}^{d-1} t_i \mathcal{O}$. Then $\mathfrak{m} = \mathfrak{n} + t_d \mathcal{O}$. Therefore $H_{\mathcal{O}}^{(0)} \leq H_{\mathfrak{n}}^{(1)}$, by Lemma (1.2)(2). Also $H_{\mathfrak{n}}^{(0)} \leq H_{\mathfrak{p}}^{(d-1)}$, by Lemma (1.2)(2). Therefore $H_{\mathcal{O}}^{(0)} \leq H_{\mathfrak{n}}^{(1)} \leq H_{\mathfrak{p}}^{(d)}$. Since $H_{\mathcal{O}}^{(0)} = H_{\mathfrak{p}}^{(d)}$, we get $H_{\mathcal{O}}^{(0)} = H_{\mathfrak{n}}^{(1)}$. Now \mathcal{O}/\mathfrak{n} is regular of dimension 1. Therefore, by (A), $H_{\mathcal{O}}^{(0)} = H_{\mathfrak{n}}^{(1)}$ implies that \mathfrak{n} is permissible in \mathcal{O} . Hence

$$(*) \quad H_{\mathcal{O}}^{(0)} = H_{\mathcal{O}_{\mathfrak{n}}}^{(1)}$$

by Lemma (1.3). Thus $H_{\mathcal{O}_{\mathfrak{n}}}^{(1)} = H_{\mathfrak{p}}^{(d)}$, which gives $H_{\mathcal{O}_{\mathfrak{n}}}^{(0)} = H_{\mathfrak{p}}^{(d-1)}$. This implies that $H_{\mathcal{O}_{\mathfrak{n}}}^{(0)} \geq H_{\mathfrak{p}}^{(d-1)}$, since $\mu(\mathfrak{p}^n \mathcal{O}_{\mathfrak{n}}) \leq \mu(\mathfrak{p}^n)$ for every n . On the other hand, by Lemma (1.2)(2), we have $H_{\mathcal{O}_{\mathfrak{n}}}^{(0)} \leq H_{\mathfrak{p}}^{(d-1)}$, since

$$\mathfrak{n} \mathcal{O}_{\mathfrak{n}} = \mathfrak{p} \mathcal{O}_{\mathfrak{n}} + \sum_{i=1}^{d-1} t_i \mathcal{O}_{\mathfrak{n}}.$$

Thus $H_{\mathcal{O}_n}^{(0)} = H_{\mathfrak{p}\mathcal{O}_n}^{(d-1)}$. This implies, by induction hypothesis, that $\mathfrak{p}\mathcal{O}_n$ is permissible in \mathcal{O}_n , since $\mathcal{O}_n/\mathfrak{p}\mathcal{O}_n$ is regular of dimension $d-1$. Therefore $H_{\mathcal{O}_n}^{(d-1)} = H_{\mathcal{O}_n}^{(0)}$, by Lemma (1.3). This gives $H_{\mathcal{O}_n}^{(d)} = H_{\mathcal{O}_n}^{(1)} = H_{\mathcal{O}_n}^{(0)}$, by (*). Therefore, by Lemma (1.3), \mathfrak{p} is permissible in \mathcal{O} , and (B) is proved.

We now turn to the proof of (A). We are given that \mathcal{O}/\mathfrak{p} is a discrete valuation ring and $H_{\mathcal{O}}^{(0)} = H_{\mathfrak{p}}^{(1)}$. We have to show that $\text{gr}_{\mathfrak{p}}(\mathcal{O})$ is \mathcal{O}/\mathfrak{p} -flat or, equivalently, that $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ is \mathcal{O}/\mathfrak{p} -free for every $n \geq 0$. Choose $t \in \mathfrak{m}$ such that its image \bar{t} in \mathcal{O}/\mathfrak{p} is a uniformising parameter for \mathcal{O}/\mathfrak{p} . It is then enough to show that \bar{t} is a non-zero divisor in $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ for every $n \geq 0$.

By the choice of t , we have $\mathfrak{m} = \mathfrak{p} + t\mathcal{O}$. Therefore the equality $H_{\mathcal{O}}^{(0)} = H_{\mathfrak{p}}^{(1)}$ implies, by Lemma (1.2)(3), that $\mu(t^m \mathfrak{p}^n) = \mu(\mathfrak{p}^n)$ for all $m, n \geq 0$, so that $\mu(\mathfrak{m}^n) = \sum_{i=0}^n \mu(t^i \mathfrak{p}^{n-i})$.

Suppose now that there exists $n \geq 0$ such that \bar{t} is a zero-divisor in $\mathfrak{p}^n/\mathfrak{p}^{n+1}$. Then there exists $p \in \mathfrak{p}^n - \mathfrak{p}^{n+1}$ such that $tp \in \mathfrak{p}^{n+1}$. We consider the two cases $p \notin \mathfrak{m}\mathfrak{p}^n$ and $p \in \mathfrak{m}\mathfrak{p}^n$.

Case (1). $p \notin \mathfrak{m}\mathfrak{p}^n$. In this case p can be completed to a minimal set, say S , of generators of \mathfrak{p}^n . Then $tS = \{tx | x \in S\}$ is a minimal set of generators of $t\mathfrak{p}^n$, since $\mu(t\mathfrak{p}^n) = \mu(\mathfrak{p}^n)$, as noted above. But this is a contradiction, by Lemma (1.2)(1), of the equality

$$\mu(\mathfrak{m}^{n+1}) = \sum_{i=0}^{n+1} \mu(t^i \mathfrak{p}^{n+1-i}),$$

since $tp \in tS \cap \mathfrak{p}^{n+1}$.

*Case (2)*² $p \in \mathfrak{m}\mathfrak{p}^n$. Since $\mathfrak{m}\mathfrak{p}^n = (\mathfrak{p} + t\mathcal{O})\mathfrak{p}^n = \mathfrak{p}^{n+1} + t\mathfrak{p}^n$, we can write $p = q'_{n+1} + t^{\alpha_0-1}p_n$ with $q'_{n+1} \in \mathfrak{p}^{n+1}$, $p_n \in \mathfrak{p}^n$ and α_0 an integer ≥ 2 . Since $p \notin \mathfrak{p}^{n+1}$, we may choose q'_{n+1} , α_0 and p_n to be such that $p_n \in \mathfrak{p}^n - \mathfrak{m}\mathfrak{p}^n$. Now $tp = tq'_{n+1} + t^{\alpha_0}p_n$. Put $q_{n+1} = t^{\alpha_0}p_n = tp - tq'_{n+1}$. Then $q_{n+1} \in \mathfrak{p}^{n+1}$. Suppose $q_{n+1} \in \mathfrak{m}\mathfrak{p}^{n+1} = \mathfrak{p}^{n+2} + t\mathfrak{p}^{n+1}$. Then we can write $q_{n+1} = q_{n+2} - t^{\alpha_1}p_{n+1}$ with $q_{n+2} \in \mathfrak{p}^{n+2}$, $\alpha_1 \geq 1$ and $p_{n+1} \in \mathfrak{p}^{n+1}$. Now, if $q_{n+1} \notin \mathfrak{p}^{n+2}$, we may assume (by choosing q_{n+2} , α_1 , p_{n+1} suitably) that $p_{n+1} \in \mathfrak{p}^{n+1} - \mathfrak{m}\mathfrak{p}^{n+1}$. If $q_{n+1} \in \mathfrak{p}^{n+2}$, then we put $q_{n+2} = q_{n+1}$, $p_{n+1} = 0$ and $\alpha_1 = \alpha_0 + 1$. We get $q_{n+2} = t^{\alpha_0}p_n + t^{\alpha_1}p_{n+1}$. Proceeding thus, we write

$$(**) \quad q_{n+r+1} = t^{\alpha_0}p_n + t^{\alpha_1}p_{n+1} + \dots + t^{\alpha_r}p_{n+r},$$

² The author wishes to express his thanks to the referee for pointing out a correction in the proof of this case.

where $q_{n+r+1} \in \mathfrak{p}^{n+r+1}$ and for every $i, 0 \leq i \leq r$, either $p_{n+i} \in \mathfrak{p}^{n+i} - m\mathfrak{p}^{n+i}$ and $\alpha_i \geq 1$ or $p_{n+i} = 0$ and $\alpha_i = \alpha_0 + 1$. Now suppose we have obtained q_{n+r+1} for a given $r \geq 0$. For this r , let

$$\alpha = \inf \{ \alpha_0, \alpha_1 + 1, \dots, \alpha_r + r \}$$

and let

$$J = \{ j | 0 \leq j \leq r \text{ and } \alpha = \alpha_j + j \}.$$

Then J is not empty, $\alpha_j = \alpha - j$ for every j in J and from (***) we get

$$(***) \quad q_{n+r+1} \equiv \sum_{j \in J} t^{\alpha-j} p_{n+j} \pmod{m^{n+\alpha+1}}.$$

Now, since $p_{n+j} \in \mathfrak{p}^{n+j} - m\mathfrak{p}^{n+j}$ for every $j \in J$, we can complete p_{n+j} to a minimal set of generators of \mathfrak{p}^{n+j} . Therefore, since we have

$$\mu(m^{n+\alpha}) = \sum_{i=0}^{n+\alpha} \mu(t^{n+\alpha-i} \mathfrak{p}^i),$$

we see by Lemma (1.2) that the set $\{t^{\alpha-j} p_{n+j} | j \in J\}$ can be completed to a minimal set of generators of $m^{n+\alpha}$. In particular, $\sum_{j \in J} t^{\alpha-j} p_{n+j}$ is not in $m^{n+\alpha+1}$, since J is non-empty. Therefore, by (***), q_{n+r+1} is not in $m^{n+\alpha+1}$. Therefore, since $q_{n+r+1} \in \mathfrak{p}^{n+r+1}$, we conclude that $n+r+1 < n+\alpha+1$, so that $r < \alpha \leq \alpha_0$.

This shows that the process of generating the q_{n+r+1} cannot go on indefinitely, i.e. we must eventually come to an r for which q_{n+r+1} is not in $m\mathfrak{p}^{n+r+1}$. For this r , q_{n+r+1} can be completed to a minimal set of generators of \mathfrak{p}^{n+r+1} and hence of m^{n+r+1} by Lemma (1.2), since by hypothesis

$$\mu(m^{n+r+1}) = \sum_{i=0}^{n+r+1} \mu(t^i \mathfrak{p}^{n+r+1-i}).$$

Now if $\alpha > r+1$ then (***) shows that $q_{n+r+1} \in m^{n+r+2}$, which is a contradiction. If $\alpha = r+1$ then, by Lemma (1.2), the set

$$\{q_{n+r+1}\} \cup \{t^{\alpha-j} p_{n+j} | j \in J\}$$

can be completed to a minimal set of generators of $m^{n+\alpha}$. This contradicts (***) .

Thus (A) is proved, and the proof of the theorem is complete.

2. Proof of Theorems 2 and 3

(2.1) The proof of Theorems 2 and 3 is contained essentially in the proof of the Main Theorem in [6]. What is needed is elaboration of certain points. We do this in the proof below, referring frequently to [6].

(2.2) We have the following situation: \mathfrak{p} is a proper ideal of \mathcal{O} , and $\mathcal{O} \xrightarrow{h} \mathcal{O}'$ is a blowing-up of \mathcal{O} with center \mathfrak{p} . We have $e = \text{emdim } \mathcal{O}/\mathfrak{p}$ and $\delta = \text{tr.deg}_k k'$, where $k \rightarrow k'$ is the residue field extension induced by h . We are given $t = (t_0, t_1, \dots, t_e)$ with $t_0 \in \mathfrak{p}$ such that $\mathfrak{p}\mathcal{O}' = t_0\mathcal{O}'$ and $t_i \in \mathfrak{m}$, $1 \leq i \leq e$, such that $\mathfrak{m} = \mathfrak{p} + \sum_{i=1}^e t_i\mathcal{O}$. The ideals $\mathfrak{a}_{t_i}(n)$ of \mathcal{O}' and $\mathfrak{b}_{t_0}(n)$ of \mathcal{O} and the numerical functions L_{t_i} , $1 \leq i \leq e$, and L_{t_0} are defined as in the Introduction. Let $\mathcal{O}'' = \mathcal{O}'/\mathfrak{m}\mathcal{O}'$.

With the notation of (2.2) we shall prove the following three lemmas:

(2.3) LEMMA:

$$H_{\mathcal{O}'}^{(0)} = H_{\mathcal{O}''}^{(e+1)} - \sum_{i=0}^e L_{t_i}^{(i)}.$$

(2.4) LEMMA: If $k = k'$ then $H_{\mathfrak{p}}^{(0)} = H_{\mathcal{O}''}^{(1)} + L_{t_0}$.

(2.5) LEMMA: $H_{\mathfrak{p}}^{(0)} \geq H_{\mathcal{O}''}^{(1+\delta)}$.

Assume these three lemmas for the moment. Then we get an immediate

PROOF OF THEOREMS 2 AND 3: Since $D_{\mathfrak{p}} = H_{\mathfrak{p}}^{(e)} - H_{\mathcal{O}'}^{(0)}$, we have

$$\begin{aligned} H_{\mathcal{O}'}^{(0)} - H_{\mathcal{O}'}^{(\delta)} &= H_{\mathfrak{p}}^{(e)} - H_{\mathcal{O}'}^{(\delta)} - D_{\mathfrak{p}} \\ &= H_{\mathfrak{p}}^{(e)} - H_{\mathcal{O}''}^{(e+1+\delta)} + \sum_{i=0}^e L_{t_i}^{(i+\delta)} - D_{\mathfrak{p}} \end{aligned} \quad (\text{Lemma (2.3)})$$

$$\geq \sum_{i=0}^e L_{t_i}^{(i+\delta)} - D_{\mathfrak{p}} \quad (\text{Lemma (2.5)}).$$

This proves Theorem 2. Now, if $k = k'$, then

$$\begin{aligned} H_{\mathcal{O}'}^{(0)} - H_{\mathcal{O}'}^{(0)} &= H_{\mathfrak{p}}^{(e)} - H_{\mathcal{O}''}^{(e+1)} + \sum_{i=0}^e L_{t_i}^{(i)} - D_{\mathfrak{p}} \quad (\text{as above, since } \delta = 0) \\ &= L_{t_0}^{(e)} + \sum_{i=0}^e L_{t_i}^{(i)} - D_{\mathfrak{p}} \end{aligned} \quad (\text{Lemma (2.4)}).$$

This proves Theorem 3.

PROOF OF LEMMA (2.3): Since $\mathcal{O}'' = \mathcal{O}' / \sum_{i=0}^e t_i \mathcal{O}'$, the lemma follows from [6, Theorem 1] and a straightforward induction on e .

PROOF OF LEMMA (2.4): Let \mathfrak{m}'' be the maximal ideal of \mathcal{O}'' . It is enough to show that there exists an exact sequence

$$(*) \quad 0 \rightarrow \mathfrak{b}_{t_0}(n)/\mathfrak{m}\mathfrak{p}^n \rightarrow \mathfrak{p}^n/\mathfrak{m}\mathfrak{p}^n \xrightarrow{\varphi} \mathcal{O}''/\mathfrak{m}''^{n+1} \rightarrow 0$$

of k -vector spaces. For we have

$$H_{\mathfrak{p}}^{(0)}(n) = \dim_k \mathfrak{p}^n/\mathfrak{m}\mathfrak{p}^n, \quad H_{\mathcal{O}''}^{(1)}(n) = \dim_k \mathcal{O}''/\mathfrak{m}''^{n+1}$$

and

$$L_{t_0}(n) = \text{length}_{\mathcal{O}} \mathfrak{b}_{t_0}(n)/\mathfrak{m}\mathfrak{p}^n = \dim_k \mathfrak{b}_{t_0}(n)/\mathfrak{m}\mathfrak{p}^n.$$

To show the existence of (*) we have only to define φ suitably. Since $\mathfrak{p}\mathcal{O}' = t_0\mathcal{O}'$, we can identify \mathcal{O}' with a localization of the subring $\{f/t_0^n | n \geq 0, f \in \mathfrak{p}^n\}$ of \mathcal{O}_{t_0} . Define $\psi: \mathfrak{p}^n \rightarrow \mathcal{O}''$ by $\psi(f) = \eta(f/t_0^n)$, where $\eta: \mathcal{O}' \rightarrow \mathcal{O}''$ is the canonical homomorphism. Then ψ induces a k -homomorphism $\bar{\psi}: \mathfrak{p}^n/\mathfrak{m}\mathfrak{p}^n \rightarrow \mathcal{O}''$. We define φ to be the composite of $\bar{\psi}$ and the canonical homomorphism $\mathcal{O}'' \rightarrow \mathcal{O}''/\mathfrak{m}''^{n+1}$. It was proved in [6, (3.3), Proof of Lemma 2] that φ is surjective if $k = k'$. Also, it is clear from the definition of $\mathfrak{b}_{t_0}(n)$ that $\ker \varphi = \mathfrak{b}_{t_0}(n)/\mathfrak{m}\mathfrak{p}^n$. Thus (*) is exact and the lemma is proved.

PROOF OF LEMMA (2.5): By Lemma (2.4), we already have the inequality $H_{\mathfrak{p}}^{(0)} \geq H_{\mathcal{O}''}^{(1+\delta)}$ in the case $k = k'$. The inequality in the general case can now be proved by a standard inductive procedure used in [1], [4] and [6]. What we do is the following: Choose an element $\alpha \in k' - k$. If $\delta \geq 1$, we assume that α is transcendental. If $\delta = 0$, we assume that α is either separable or purely inseparable. Let $\bar{f}(Z) \in k[Z]$ be the minimal monic polynomial of α over k . (If α is transcendental, we take $\bar{f}(Z) = 0$.) Let $f(Z) \in \mathcal{O}[Z]$ be a monic lift of $\bar{f}(Z)$ such that, for every $i \geq 0$, if the coefficient of Z^i in $\bar{f}(Z)$ is 0 then the coefficient of Z^i in $f(Z)$ is also 0. Let $\tilde{\mathcal{O}}$ be the localization of $0[Z]/f(Z)\mathcal{O}[Z]$ at the prime ideal $\mathfrak{n} = (\mathfrak{m}[Z] + f(Z)\mathcal{O}[Z])/f(Z)\mathcal{O}[Z]$, where \mathfrak{m} is the maximal ideal of \mathcal{O} . Let $\eta: \mathcal{O} \rightarrow \tilde{\mathcal{O}}$ be the canonical homomorphism. Let a be a lift of α to \mathcal{O}' and let $\tilde{\mathcal{O}}'$ be the localization of $\mathcal{O}'[Z]/f(Z)\mathcal{O}'[Z]$ at the maximal ideal

$$\mathfrak{n}' = (\mathfrak{m}'[Z] + (Z - a)\mathcal{O}'[Z])/f(Z)\mathcal{O}'[Z],$$

where \mathfrak{m}' is the maximal ideal of \mathcal{O}' . Let $\eta': \mathcal{O}' \rightarrow \tilde{\mathcal{O}}'$ be the canonical homomorphism. Then there exists a commutative diagram

$$\begin{array}{ccc} \mathcal{O} & \xrightarrow{h} & \mathcal{O}' \\ \eta \downarrow & & \downarrow \eta' \\ \tilde{\mathcal{O}} & \xrightarrow{\tilde{h}} & \tilde{\mathcal{O}}' \end{array}$$

such that

(i) \tilde{h} is a blowing-up of $\tilde{\mathcal{O}}$ with center $\tilde{\mathfrak{p}} = \mathfrak{p}\tilde{\mathcal{O}}$;
(ii) the residue field extension induced by \tilde{h} is the k -inclusion $k(\alpha) \rightarrow k'$. (See [6, (4.3), (4.6)].) Let $\tilde{\delta} = \text{tr.deg}_{k(\alpha)} k'$. If $\delta \geq 1$, then $\tilde{\delta} = \delta - 1$. If $\delta = 0$, then $[k':k(\alpha)] < [k':k]$. Therefore, by an obvious induction, we may assume that $H_{\tilde{\mathfrak{p}}}^{(0)} \cong H_{\tilde{\mathcal{O}}'}^{(1+\tilde{\delta})}$, where $\tilde{\mathcal{O}}'' = \tilde{\mathcal{O}}'/\tilde{\mathfrak{m}}\tilde{\mathcal{O}}'$, $\tilde{\mathfrak{m}}$ being the maximal ideal of $\tilde{\mathcal{O}}$. Now, in order to complete the proof of the lemma, it is clearly enough to prove the following three statements:

- (1) $H_{\mathfrak{p}}^{(0)} = H_{\tilde{\mathfrak{p}}}^{(0)}$.
- (2) $H_{\tilde{\mathcal{O}}''}^{(0)} \cong H_{\mathcal{O}''}^{(0)}$ if $\tilde{\delta} = \delta = 0$.
- (3) $H_{\tilde{\mathcal{O}}''}^{(0)} = H_{\mathcal{O}''}^{(1)}$ if $\tilde{\delta} = \delta - 1$.

PROOF OF (1): Let $\tilde{k} = k(\alpha)$ be the residue field of $\tilde{\mathcal{O}}$. For every $n \geq 0$, we have $H_{\tilde{\mathfrak{p}}}^{(0)}(n) = \dim_{\tilde{k}} \tilde{\mathfrak{p}}^n \otimes_{\tilde{\mathcal{O}}} \tilde{k} = \dim_{\tilde{k}} \mathfrak{p}^n \otimes_{\mathcal{O}} \tilde{k}$, since, $\tilde{\mathcal{O}}$ being \mathcal{O} -flat, we have $\tilde{\mathfrak{p}}^n \approx \mathfrak{p}^n \otimes_{\mathcal{O}} \tilde{\mathcal{O}}$. Now $\mathfrak{p}^n \otimes_{\mathcal{O}} \tilde{k} \approx (\mathfrak{p}^n \otimes_{\mathcal{O}} k) \otimes_k \tilde{k}$. Therefore,

$$\dim_{\tilde{k}} \mathfrak{p}^n \otimes_{\mathcal{O}} \tilde{k} = \dim_k \mathfrak{p}^n \otimes_{\mathcal{O}} k = H_{\mathfrak{p}}^{(0)}(n).$$

PROOF OF (2) AND (3): Let \mathfrak{m}'' be the maximal ideal of \mathcal{O}'' . Then $\tilde{\mathcal{O}}'' = \tilde{\mathcal{O}}'/\tilde{\mathfrak{m}}\tilde{\mathcal{O}}' = \tilde{\mathcal{O}}'/\mathfrak{m}\tilde{\mathcal{O}}' = (\mathcal{O}''[Z]/f(Z)\mathcal{O}''[Z])_{\mathfrak{m}''}$, where

$$\mathfrak{m}'' = (\mathfrak{m}''[Z] + (Z - a)\mathcal{O}''[Z])f(Z)\mathcal{O}''[Z].$$

Now, if $\tilde{\delta} = \delta - 1$, then α is transcendental and $f(Z) = 0$. Therefore the equality $H_{\tilde{\mathcal{O}}''}^{(0)} = H_{\mathcal{O}''}^{(1)}$ is clear in this case. This proves (3). If $\delta = 0$ and α is separable then $\tilde{f}(Z)$ being a separable polynomial, $\mathcal{O}'' \rightarrow \tilde{\mathcal{O}}''$ is etale, so that in this case we have, in fact, $H_{\tilde{\mathcal{O}}''}^{(0)} = H_{\mathcal{O}''}^{(0)}$. Now suppose $\delta = 0$ and α is purely inseparable. Then $\tilde{f}(Z) = Z^q - \beta$, where q is a power of char k and $\beta = \alpha^q \in k$. This implies that $f(Z) = Z^q - b$, where $b \in \mathcal{O}$ is some lift of β . Let \bar{b} be the canonical image of b in \mathcal{O}'' . Since $\mathcal{O}''[Z]/(Z^q - \bar{b})\mathcal{O}''[Z]$ is already a local ring, we have

$$\tilde{\mathcal{O}}'' = \mathcal{O}''[Z]/(Z^q - \bar{b})\mathcal{O}''[Z].$$

Let \bar{a} be the canonical image of a in \mathcal{O}'' and let $t = \bar{b} - \bar{a}^q$. Then $t \in \mathfrak{m}''$. Let $Y = Z - \bar{a}$. Then $\tilde{\mathcal{O}}'' = \mathcal{O}''[Y]/(Y^q - t)\mathcal{O}''[Y]$. Now, the inequality $H_{\tilde{\mathcal{O}}''}^{(0)} \geq H_{\mathcal{O}''}^{(0)}$ follows from [6, Lemma (4.5)]. This proves (2).

REFERENCES

- [1] BENNET, B. M.: On the characteristic functions of a local ring. *Ann. of Math.* 91 (1970) 25–87.
- [2] GROTHENDIECK, A.: *Eléments de géométrie algébrique. Publications Mathématiques* (1960).
- [3] HIRONAKA, H.: Resolution of singularities, *Ann. of Math.* 79 (1964) 109–326.
- [4] HIRONAKA, H.: Certain numerical characters of singularities. *J. Math. Kyoto Univ.* 10–1 (1970) 151–187.
- [5] NAGATA, M.: *Local Rings, Interscience*, 1962.
- [6] SINGH, B.: Effect of a permissible blowing-up on the local Hilbert functions. *Inventiones math.* 26 (1974) 201–212.

(Oblatum 20–XII–1974 & 6–1–1976)

School of Mathematics
Tata Institute of Fundamental Research
Colaba, Bombay 400 005