Communicated 12 October 1955 by OTTO FROSTMAN and LARS GARDING

On the associativity formula for multiplicities

By CHRISTER LECH

This paper is concerned with a theorem of Chevalley on multiplicities in a local ring ([1], Theorem 5, p. 25). We shall present a generalized form of this theorem, for which we can give a new and rather simple proof. Before stating our theorem we introduce some notations. If q is a primary ideal belonging to the maximal ideal of a local ring, then e(q) means its multiplicity, defined according to Samuel, and L(q) its length; if a is an arbitrary ideal† in a Noetherian ring R and \mathfrak{p} a minimal prime ideal of a, then we define $e(\alpha; \mathfrak{p}) = -e(\alpha R_{\mathfrak{p}})$ and $L(\alpha; \mathfrak{p}) = L(\alpha R_{\mathfrak{p}})$, where $R_{\mathfrak{p}}$ denotes the generalized ring of quotients with respect to \mathfrak{p} . It may be pointed out here that our result depends in an essential way on Samuel's notion of multiplicity, which is more general than Chevalley's original notion.

Our theorem reads:

Theorem 1. Let Q be a local ring of dimension r and let $\{x_1, \ldots, x_r\}$ be a system of parameters in Q. Put $q = (x_1, \ldots, x_r)$ and $\mathfrak{o} = (x_{m+1}, \ldots, x_r)$, where $0 \le m \le r$. Let \mathfrak{p} range over those minimal prime ideals of \mathfrak{o} for which dim \mathfrak{p} + rank $\mathfrak{p} = \dim Q$. Then

$$e(\mathfrak{q}) = \sum_{\mathfrak{p}} e((\mathfrak{q} + \mathfrak{p})/\mathfrak{p}) e(\mathfrak{o}; \mathfrak{p}).$$

Chevalley's theorem is restricted to local rings which admit a nucleus. (It is formulated for the even smaller class of geometric local rings.) In his theorem, \mathfrak{p} ranges over all minimal prime ideals of \mathfrak{o} . This difference from our theorem comes from the fact that in a local ring which admits a nucleus it is true for every prime ideal \mathfrak{p} that dim \mathfrak{p} + rank \mathfrak{p} = dim Q. Chevalley's theorem as well as ours has its greatest importance in the algebro-geometric theory of intersection-multiplicities.

We begin our proof by deriving a certain expression for the multiplicity of an ideal generated by a system of parameters (Theorem 2, Section 1). Theorem 1 is then proved by induction on the dimension of Q (Sections 2 and 3). The proof is based directly on the fundamental properties of Noetherian rings and of local rings.[†] The local rings which occur during the demonstrations are

[†] By an ideal we shall always mean a proper ideal; in other words, the whole ring does not count as an ideal.

[‡] As a general reference, also for the terminology, see [2].

either general local rings or submitted to restrictions which refer only to the dimension and to the primary components of the zero ideal.

Following Northcott and Rees ([4], [5]) one can obtain a generalization of Theorem 1 in terms of analytically disjoint ideals. This is outlined in Section 4 below, the result being stated as Theorem 3.

The concluding Section 5 contains a couple of simple formulas obtained as side-results.

1. Before we enter on the proper subject of this section we recall some well-known facts, fundamental to the whole paper. Let Q be a local ring, \mathfrak{m} its maximal ideal and let \mathfrak{q} be an \mathfrak{m} -primary ideal.

The length L(q) of q is defined as the maximum of the number λ of steps in a chain

$$Q = \mathfrak{q}_0 \supset \mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_{\lambda} = \mathfrak{q},$$

where each inclusion is strict and where, apart from q_0 , each term is an mprimary ideal. A way of viewing this situation is to regard Q as a module with itself as a multiplicative operator domain. The permitted submodules are then the ideals of Q; and L(q) is equal to the length of a Jordan-Hölder composition series of the Q-module Q/q. Notice that, if q' is another m-primary ideal contained in q, then L(q') - L(q) is equal to the length of a composition series of the Q-module q/q'. By saying that two modules are Q-isomorphic we shall mean that they are isomorphic regarded as Q-modules.

The dimension of Q can be equivalently defined in two quite different ways. According to one, dim Q is the minimum number of generators of an *m*-primary ideal. (The number of generators of (0) is thereby counted as zero.) A system of elements which generate an *m*-primary ideal and whose number is dim Q, is called a system of parameters in Q. According to the other way of definition, dim Q is the maximum of the number ρ of steps in a chain

$$\mathfrak{m} = \mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_{\varrho},$$

where each inclusion is strict and each term is a prime ideal in Q. If \mathfrak{a} is any ideal and \mathfrak{p} any prime ideal in Q, then by definition, dim $\mathfrak{a} = \dim (Q/\mathfrak{a})$ and rank $\mathfrak{p} = \dim Q_{\mathfrak{p}}$. Using the correspondence between the prime ideals in Q on one hand and those in Q/\mathfrak{p} and in $Q_{\mathfrak{p}}$ on the other, we see that we always have dim $\mathfrak{p} + \operatorname{rank} \mathfrak{p} \leq \dim Q$.

Let now the dimension of Q be r. Samuel has shown that, for n sufficiently large, $L(q^n)$ is a polynomial in n, whose degree is exactly r (see [6], pp. 24-28, or [3]; cf. the formula (5) below). He defines e(q) as r! times the leading coefficient of this polynomial. From this definition it can easily be concluded that e(q) is a positive integer. On the other hand, it is plain that we can write

$$e(\mathbf{q}) = \lim_{n \to \infty} \frac{(r!) L(\mathbf{q}^n)}{n^r}, \qquad (1)$$

and we shall take this expression as our starting point.

The main object of the present section is to derive another similar expression for e(q) in the case where q is generated by a system of parameters. At the same time we shall get an independent proof of the fact that the above limit exists for such a q. For simplicity we write $e(x_1, \ldots, x_r)$ instead of $e((x_1, \ldots, x_r))$, etc. Our result is as follows.

Theorem 2. If $\{x_1, \ldots, x_r\}$ is a system of parameters in a local ring, then

$$e(x_1, \ldots, x_r) = \lim_{(\min n_i) \to \infty} \frac{L(x_1^{n_1}, \ldots, x_r^{n_r})}{n_1 \ldots n_r}.$$

Denote by Q the local ring referred to in the theorem, by \mathfrak{m} its maximal ideal and by \mathfrak{q} the ideal (x_1, \ldots, x_r) . Let \mathfrak{a} be an arbitrary ideal in Q. Applying a method which goes back to Krull we shall deduce an expression (the formula (5), p. 304) for $L(\mathfrak{a}+\mathfrak{q}^n)$ in terms of certain "form ideals" (cf. [6], p. 19, and [3], Section 4). This expression will then be used for estimating $L(x_1^{n_1}, \ldots, x_r^{n_r})$.

Fix a composition series from Q to q,

$$Q = \mathfrak{q}_0 \supset \mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_l = \mathfrak{q},$$

so that l=L(q). Multiplying the terms of this chain successively by $Q=q^0$, q, \ldots, q^{n-1} and linking together the chains so obtained, we get a chain

$$\mathfrak{q}_0 \supset \mathfrak{q}_1 \supset \cdots \supset \mathfrak{q}_{l-1} \supset \mathfrak{q} \supset \mathfrak{q}_1 \mathfrak{q} \supset \mathfrak{q}_2 \mathfrak{q} \supset \cdots \supset \mathfrak{q}_{l-1} \mathfrak{q} \supset \mathfrak{q}^2 \supset \cdots \supset \mathfrak{q}^n,$$

which is of course in general no composition series. Adding a to each term of this chain, we get a chain from $Q = a + q_0$ to $a + q^n$, from which we obtain

$$L(\mathfrak{a}+\mathfrak{q}^n) = \sum_{\mu=0}^{n-1} \sum_{\nu=0}^{l-1} \operatorname{length}_{\varphi} ((\mathfrak{a}+\mathfrak{q}_{\nu}\mathfrak{q}^{\mu})/(\mathfrak{a}+\mathfrak{q}_{\nu+1}\mathfrak{q}^{\mu})), \qquad (2)$$

where length ρ of a Q-module denotes the length of a composition series for this Q-module. The final formula for $L(\mathfrak{a}+\mathfrak{q}^n)$ will be obtained from (2) by replacing

$$(a + q_{\nu} q^{\mu})/(a + q_{\nu+1} q^{\mu})$$

by a Q-isomorphic image. As a first step in this direction, we note that, by one of the isomorphism theorems for groups, there is a Q-isomorphism

$$(\mathfrak{a} + \mathfrak{q}_{\nu} \mathfrak{q}^{\mu})/(\mathfrak{a} + \mathfrak{q}_{\nu+1} \mathfrak{q}^{\mu}) \simeq \mathfrak{q}_{\nu} \mathfrak{q}^{\mu}/(\mathfrak{a} \cap \mathfrak{q}_{\nu} \mathfrak{q}^{\mu} + \mathfrak{q}_{\nu+1} \mathfrak{q}^{\mu}).$$
(3)

Now put $K = Q/\mathfrak{m}$. Form the polynomial ring $K[X_1, \ldots, X_r] = K[X]$, where the X_i are indeterminates. Denote by F_{μ} the K-module consisting of all the forms of degree μ in K[X]. For each $\nu (0 \le \nu \le l-1)$ we shall define an ideal $I_{\nu}(\mathfrak{a})$ in K[X].

Without reducing the structure we may consider every Q-module annihilated by m as a K-module. Now $\mathfrak{m}\mathfrak{q}_{\nu} \subset \mathfrak{q}_{\nu+1}$ (for otherwise $\mathfrak{q}_{\nu+1} + \mathfrak{m}\mathfrak{q}_{\nu}$ would be an ideal strictly between \mathfrak{q}_{ν} and $\mathfrak{q}_{\nu+1}$, cf. [2], Proposition 1, p. 65). Hence the

modules in (3) are K-modules and the symbol "length_Q" in (2) may be replaced by "dim_K". Furthermore, the module $q_{\nu}/q_{\nu+1}$ is a K-module and, as it is irreducible, it is actually K-isomorphic to K. Let us fix such an isomorphism between $q_{\nu}/q_{\nu+1}$ and K.

For $\mu = 0, 1, 2, \ldots$ we shall define a mapping

$$T_{\nu,\mu}: F_{\mu} \to q_{\nu} q^{\mu}/q_{\nu+1} q^{\mu}.$$

Let f be a form of F_{μ} . A representative φ in $q_{\nu}q^{\mu}$ of its image under $T_{\nu,\mu}$ is obtained as follows. Replace in the form f the indeterminates X_i by the corresponding elements x_i and the coefficients in K by a representative in q_{ν} of the corresponding elements in $q_{\nu}/q_{\nu+1}$. (The form f is then a kind of a leading form of φ . Cf. [3], p. 71.) We write

$$T_{\nu,\mu}f = \varphi + \mathfrak{q}_{\nu+1}\mathfrak{q}^{\mu}.$$

Notice that

$$T_{\nu, \mu+1}(X_i f) = x_i \varphi + q_{\nu+1} q^{\mu+1} \qquad (i = 1, 2, ..., r).$$
(4)

As is easily verified, the mapping $T_{\nu,\mu}$ is a K-homomorphism onto $q_{\nu}q^{\mu}/q_{\nu+1}q^{\mu}$. It induces a further K-homomorphism

$$F_{\mu} \rightarrow q_{\nu} q^{\mu} / (a \cap q_{\nu} q^{\mu} + q_{\nu+1} q^{\mu}),$$

the kernel of which we denote by $K_{\nu,\mu}(a)$. We have

$$K_{\boldsymbol{\nu},\mu}(\mathfrak{a}) = \{f \mid f \in F_{\mu}, T_{\boldsymbol{\nu},\mu} f \subset (\mathfrak{a} \cap \mathfrak{q}_{\boldsymbol{\nu}} \mathfrak{q}^{\mu} + \mathfrak{q}_{\boldsymbol{\nu}+1} \mathfrak{q}^{\mu})\}.$$

Using (4), we see that

$$X_i K_{\nu,\mu}(\mathfrak{a}) \subset K_{\nu,\mu+1}(\mathfrak{a}) \qquad (i=1, 2, \ldots, r).$$

Therefore the set

$$\bigcup_{\mu=0}^{\infty}K_{\nu,\,\mu}\left(\mathfrak{a}\right)$$

is the set of forms in a homogeneous ideal of K[X]. We denote this ideal by $I_{\nu}(\mathfrak{a})$. The ideals $I_{\nu}(\mathfrak{a})$ ($\nu = 0, 1, ..., l-1$) may be called form ideals of \mathfrak{a} . Note that

$$\mathfrak{a} \subset \mathfrak{b}$$
 implies $I_{\nu}(\mathfrak{a}) \subset I_{\nu}(\mathfrak{b})$.

According to the definitions of $K_{\nu,\mu}(\mathfrak{a})$ and $I_{\nu}(\mathfrak{a})$ there is a K-isomorphism

$$F_{\mu}/(I_{\nu}(\mathfrak{a}) \cap F_{\mu}) \simeq q_{\nu} q^{\mu}/(\mathfrak{a} \cap q_{\nu} q^{\mu} + q_{\nu+1} q^{\mu}).$$

Hence, from (2) and (3), after changing the order of summation in (2),

$$L(\mathfrak{a}+\mathfrak{q}^n)=\sum_{\nu=0}^{l-1}\sum_{\mu=1}^{n-1}\dim_{K}(F_{\mu}/(I_{\nu}(\mathfrak{a})\cap F_{\mu})).$$
(5)

This is the desired formula for $L(\mathfrak{a}+\mathfrak{q}^n)$. If \mathfrak{a} is an m-primary ideal, we get from (5), by taking n large and summing over μ ,

$$L(\mathfrak{a}) = \sum_{\nu=0}^{l-1} \dim_{K} (K[X]/I_{\nu}(\mathfrak{a})).$$
(6)

For exactly e(q) values of ν we have $I_{\nu}(0) = (0)$. In fact, if we apply (5) with a = (0), we see that those values of ν for which $I_{\nu}(0) = (0)$ will contribute to $L(q^n)$ with an amount $n^r/r! + O(n^{r-1})$, the other values of ν with merely $O(n^{r-1})$. The assertion therefore follows from (1). At the same time we see that the limit in (1) exists for $q = (x_1, \ldots, x_r)$. The number of values of ν for which $I_{\nu}(0) = (0)$ cannot exceed l. For later use we may thus note with Samuel that

$$e(x_1, \ldots, x_r) \leq L(x_1, \ldots, x_r).$$
 (7)

(It may be remarked that the analytic independence of $\{x_1, \ldots, x_r\}$ means precisely that $I_0(0) = (0)$, hence implies that $e(x_1, \ldots, x_r) > 0$.)

The formula (6) applied to $\mathfrak{a} = (x_1^{n_1}, \ldots, x_r^{n_r})$ will now be used to get an upper estimate for $L(x_1^{n_1}, \ldots, x_r^{n_r})$. Since

$$I_r(x_1^{n_1}, \ldots, x_r^{n_r}) \supset (X_1^{n_1}, \ldots, X_r^{n_r}),$$

we have, for $\nu = 0, 1, ..., l-1$,

$$\dim_{K} (K[X]/I_{r}(x_{1}^{n_{1}}, \ldots, x_{r}^{n_{r}})) \leq \dim_{K} (K[X]/(X_{1}^{n_{1}}, \ldots, X_{r}^{n_{r}})) = n_{1} \ldots n_{r}.$$

This estimate is appropriate when $I_r(0) = (0)$. For those values of v for which $I_r(0) = (0)$ we consider, instead of $(X_1^{n_1}, \ldots, X_r^{n_r})$, an ideal $(X_1^{n_1}, \ldots, X_r^{n_r}, f)$, where f is an arbitrarily chosen non-zero form of $I_r(0)$. Order the power products of K[X] lexicografically on the basis of the sequence of their exponents. Let $X_1^{q_1} \ldots X_r^{q_r}$ be the highest power product occurring in f. Then every power product divisible by $X_1^{q_1} \ldots X_r^{q_r}$ is the highest power product in some homogeneous multiple of f. By subtracting a suitable multiple of f one can therefore from any form in K[X] derive another form of the same degree in which the power products divisible by $X_1^{q_1} \ldots X_r^{q_r}$, if occurring at all, have a lower maximum height than in the first form. It follows by induction that modulo (f) every form in K[X] is congruent to a form which contains no power products divisible by $X_1^{q_1} \ldots X_r^{q_r}$. Therefore $K[X]/(X_1^{n_1}, \ldots, X_r^{n_r}, f)$ is generated over K by those power products $X_1^{\tau_1} \ldots X_r^{\tau_r}$ which satisfy the r inequalities

$$0 \leq \tau_i < n_i$$
 $(i = 1, 2, ..., r)$

and in addition at least one of the inequalities

$$\tau_i < \sigma_i \qquad (i=1, 2, \ldots, r).$$

Hence

$$\dim_{\mathcal{K}} (K[X]/(X_1^{n_1},\ldots,X_r^{n_r},f)) \leq n_1 \ldots n_r \left(\frac{\sigma_1}{n_1}+\cdots+\frac{\sigma_r}{n_r}\right).$$

22*

Thus, if $f \in I_{\nu}(0)$,

$$\dim_K (K[X]/I_{\nu}(x_1^{n_1},\ldots,x_r^{n_r})) \leq n_1 \ldots n_r \left(\frac{\sigma_1}{n_1}+\cdots+\frac{\sigma_r}{n_r}\right).$$

Putting together our two types of estimates we get from (6)

$$L(x_1^{n_1},\ldots,x_r^{n_r}) \leq n_1 \ldots n_r \left(e(\mathfrak{q}) + \frac{A}{\min_i n_i}\right)$$

where A is a constant, independent of the n_i . Hence

$$\underbrace{\lim_{\substack{(\min \ n_i \ r_i) \to \infty}}}_{i} \frac{L\left(x_1^{n_1}, \ldots, x_r^{n_r}\right)}{n_1 \ldots n_r} \le e\left(q\right) = e\left(x_1, \ldots, x_r\right).$$
(8)

Next we prove a reverse to (8), namely: If n_1, \ldots, n_r are any natural numbers, then

$$e(x_1^{n_1}, \ldots, x_r^{n_r}) \ge n_1 \ldots n_r e(x_1, \ldots, x_r).$$
(9)

Choose m_1, \ldots, m_r such that $m_1 n_1 = \cdots = m_r n_r$. An application of (8) gives

$$\lim_{t \to \infty} \frac{L(x_1^t, \ldots, x_r^t)}{t^r} \le \frac{1}{n_1 \ldots n_r} \lim_{n \to \infty} \frac{L((x_1^{n_1})^{m_1 n_1}, \ldots, (x_r^{n_r})^{m_r n_r})}{(m_1 n) \ldots (m_r n)} \le \frac{e(x_1^{n_1}, \ldots, x_r^{n_r})}{n_1 \ldots n_r}.$$
(10)

Applying (7), we have, for every value of t,

$$L(x_1^t, \ldots, x_r^t) \ge e(x_1^t, \ldots, x_r^t) \ge e((x_1, \ldots, x_r)^t) = t^r e(x_1, \ldots, x_r).$$

In particular

$$\lim_{t\to\infty}\frac{L\left(x_1^t,\ldots,x_r^t\right)}{t^r}\geq e\left(x_1,\ldots,x_r\right).$$

Combining this inequality with (10), we get (9).

By applying (7) with $\{x_1, \ldots, x_r\}$ replaced by $\{x_1^{n_1}, \ldots, x_r^{n_r}\}$ we deduce from (9) that

 $L(x_1^{n_1}, \ldots, x_r^{n_r}) \ge n_1 \ldots n_r e(x_1, \ldots, x_r).$

This inequality, together with (8), proves Theorem 2.

The lemma which follows will be used in Section 3 as a complement to Theorem 2.

Lemma 1. Let Q be a local ring of dimension r, m its maximal ideal and let (x_1, \ldots, x_s) , where s > r, be an m-primary ideal. Then

$$\lim_{n\to\infty}\frac{L\left(x_1^n,\ldots,x_s^n\right)}{n^s}=0.$$

It is sufficient to show that

$$\overline{\lim_{n\to\infty}} \frac{L(x_1^n,\ldots,x_s^n)}{n^r} < \infty$$

As $(x_1^n, \ldots, x_s^n) \supset (x_1, \ldots, x_s)^{sn}$, we have $L(x_1^n, \ldots, x_s^n) \le L((x_1, \ldots, x_s)^{sn})$. Hence

$$\overline{\lim_{n\to\infty}} \frac{L\left(x_1^n,\ldots,x_s^n\right)}{n^r} \leq \lim_{n\to\infty} \frac{L\left((x_1\,\ldots,\,x_s)^{sn}\right)}{n^r} = \frac{s^r}{r!} e\left(x_1,\,\ldots,\,x_s\right) < \infty,$$

which was to be proved.

2. Via the Lemmata 2 and 3 we prove Lemma 4, which is essentially the one-dimensional case of Theorem 1.

Lemma 2. Let q be primary to \dagger the maximal ideal in a local ring Q, and let $\varphi \in Q$. Then

$$L(\mathfrak{q}) = L(\mathfrak{q} + (\varphi)) + L(\mathfrak{q}:(\varphi)).$$

Proof. The transformation which transforms $\rho \in Q$ into $\varphi \rho \in \varphi Q = (\varphi)$ is a Q-homomorphism with the kernel $(0): (\varphi)$. As $q: (\varphi) \supset (0): (\varphi)$, it follows from one of the two isomorphism theorems for groups that

$$Q/(\mathfrak{q}:(\varphi)) \simeq \varphi Q/\varphi (\mathfrak{q}:(\varphi)).$$

From the other isomorphism theorem we get

$$\varphi Q/\varphi (\mathfrak{q} : (\varphi)) = (\varphi)/((\varphi) \cap \mathfrak{q}) \simeq ((\varphi) + \mathfrak{q})/\mathfrak{q}.$$

Hence

$$Q/(q:(\varphi)) \simeq ((\varphi) + q)/q,$$

from which the lemma follows readily (cf. the beginning of Section 1).

If m is the maximal ideal and φ an element of a local ring, then, given any integer s > 0, one can determine n so that

$$\mathfrak{m}^n:(\varphi)\subset(0):(\varphi)+\mathfrak{m}^s.$$

This fact is a corollary of a well-known theorem of Chevalley (see [6], Corollary 2, p. 10). We shall prove it directly, using the idea of the proof of his theorem. Put $I = \bigcap_{\nu=1}^{\infty} (\mathfrak{m}^{\nu}:(\varphi) + \mathfrak{m}^{s})$. We have $I = (0):(\varphi) + \mathfrak{m}^{s}$. For, if $\alpha \in I$, then $\varphi \alpha \in \bigcap_{\nu=1}^{\infty} (\varphi \mathfrak{m}^{s} + \mathfrak{m}^{\nu}) = \varphi \mathfrak{m}^{s}$. Thus there is an element $\mu \in \mathfrak{m}^{s}$ so that $\varphi (\alpha - \mu) = 0$ and hence $(\alpha - \mu) \in (0):(\varphi)$. This shows $I \subset (0):(\varphi) + \mathfrak{m}^{s}$. The reverse inclusion is obvious. On the other hand one can find an integer n such that $I = \mathfrak{m}^{n}:(\varphi) + \mathfrak{m}^{s}$.

 $[\]dagger$ By an ideal primary to \mathfrak{p} we mean a primary ideal belonging to (the prime ideal) \mathfrak{p} or, what is the same, a \mathfrak{p} -primary ideal.

For there can only be a finite number of different ideals among the ideals $\mathfrak{m}^{\nu}:(\varphi)+\mathfrak{m}^{\mathfrak{s}}$ $(\nu=1, 2, ...)$, since they form a descending chain and all contain $\mathfrak{m}^{\mathfrak{s}}$. From $I=(0):(\varphi)+\mathfrak{m}^{\mathfrak{s}}=\mathfrak{m}^{\mathfrak{n}}:(\varphi)+\mathfrak{m}^{\mathfrak{s}}$ we get the desired result,

$$\mathfrak{m}^n:(\varphi)\subset(0):(\varphi)+\mathfrak{m}^s$$

The lemma which follows contains a similar but sharper result in a special case.

Lemma 3. Let Q be a one-dimensional local ring in which not every non-unit is a zero divisor. If φ is an element of Q and x a parameter, then there exists a non-negative integer k such that for n > k

$$(x^n):(\varphi) \subseteq (0):(\varphi) + (x^{n-k}).$$

According to what we have just proved there exists an integer $k \ge 0$ such that

$$(x^{k+1}):(\varphi) \subset (0):(\varphi) + (x).$$

We shall show by induction on *n* that this integer *k* has the property required by the lemma. This is true for n = k + 1. Suppose n > k + 1 and let $y \in (x^n) : (\varphi)$. Then certainly $y \in (x^{k+1}) : (\varphi)$, and we can write $y = \pi + xz$ with $\pi \in (0) : (\varphi), z \in Q$. It follows that $xz \in (x^n) : (\varphi)$. According to the assumptions, *x* cannot be a zero divisor. Therefore $z \in (x^{n-1}) : (\varphi)$. By the induction hypothesis this implies $z \in (0) : (\varphi) + (x^{n-k-1})$. Hence $xz \in (0) : (\varphi) + (x^{n-k})$ and thus

$$y = \pi + xz \in (0) : (\varphi) + (x^{n-k}),$$

which proves the lemma.

Before stating the next lemma we shall slightly extend our notation. Let \mathfrak{n} be an arbitrary primary ideal in a Noetherian ring R and let \mathfrak{p} be the prime ideal belonging to \mathfrak{n} . By $L(\mathfrak{n})$ we shall denote the length of \mathfrak{n} . In terms of our previous notation this notion can be defined by $L(\mathfrak{n}) = L(\mathfrak{n}; \mathfrak{p}) = L(\mathfrak{n} R_{\mathfrak{p}})$. However, taking into account the correspondence between the \mathfrak{p} -primary ideals in R and the $(\mathfrak{p} R_{\mathfrak{p}})$ -primary ideals in $R_{\mathfrak{p}}$, we see that $L(\mathfrak{n})$ can also be characterized as being the maximum number of steps in a chain $R \supset \mathfrak{p} \supset \cdots \supset \mathfrak{n}$ where, apart from R, each term is a \mathfrak{p} -primary ideal.

Lemma 4. Let Q be a one-dimensional local ring with the parameter x. Let \mathfrak{p}_i $(i=1, 2, \ldots, s)$ be the minimal prime ideals in Q and \mathfrak{n}_i $(i=1, 2, \ldots, s)$ the corresponding primary components of the zero ideal. Then

$$e(x) = \sum_{i=1}^{s} e((x) + p_i/p_i) L(n_i).$$

As $e((0); \mathfrak{p}_i) = L((0); \mathfrak{p}_i) = L(\mathfrak{n}_i)$, the statement of Lemma 4 coincides with the case r = m = 1 of Theorem 1.

To prove the lemma we shall use induction with respect to the number $t = \sum_{s}^{s} L(\mathbf{n}_{s})$.

$$c = \sum_{i=1}^{\infty} L(\mathbf{r})$$

Put (x) = q and let m be the maximal ideal of Q. If a is an arbitrary onedimensional ideal in Q, we have, since $((q+a)/a)^n = (q^n + a)/a$, that

$$e\left((\mathfrak{q}+\mathfrak{a})/\mathfrak{a}\right) = \lim_{n\to\infty}\frac{1}{n}L\left(\mathfrak{q}^n+\mathfrak{a}\right). \tag{11}$$

Suppose that we can write $a = a_0 \cap q_0$, where q_0 is an m-primary ideal. Let us show that then

$$e\left((\mathfrak{q}+\mathfrak{a})/\mathfrak{a}\right) = e\left((\mathfrak{q}+\mathfrak{a}_0)/\mathfrak{a}_0\right). \tag{12}$$

There is a Q-isomorphism

$$(\mathfrak{q}^n + \mathfrak{a}_0)/(\mathfrak{q}^n + \mathfrak{a}) \simeq \mathfrak{a}_0/(\mathfrak{q}^n \cap \mathfrak{a}_0 + \mathfrak{a}),$$

and for large values of n we have $q^n \subset q_0$ so that $a_0/(q^n \cap a_0 + a) = a_0/a$. It follows that $L(q^n + a) - L(q^n + a_0)$ is constant for large values of n (cf. the beginning of Section 1). Hence we get (12) from (11). (This result is contained in [6], Proposition 3, p. 32, and also in [3], Theorem 8, p. 77.)

For each value of t we can reduce our proof to the case where the zero ideal in Q has no primary component belonging to \mathfrak{m} . In fact, if the zero ideal in Q has the form

$$(0) = \mathfrak{n}_1 \cap \cdots \cap \mathfrak{n}_s \cap \mathfrak{q}_0,$$

where q_0 is m-primary and irredundant, then we pass from Q to $Q/\bigcap_{i=1}^{s} \mathfrak{n}_i$ and replace x, \mathfrak{p}_i and \mathfrak{n}_i by their residues modulo $\bigcap_{i=1}^{s} \mathfrak{n}_i$. Thereby the multiplicities and lengths occurring in Lemma 4 will not change their values. This is seen for e(x) from (12) applied to $\mathfrak{a} = (0)$, for $e((x) + \mathfrak{p}_i/\mathfrak{p}_i)$ for instance from (11), and is obvious for $L(\mathfrak{n}_i)$. As the zero ideal in $Q/\bigcap_{i=1}^{s} \mathfrak{n}_i$ has apparently no primary component belonging to the maximal ideal, our assertion follows.

When t=1 there is nothing more to prove. Suppose that t>1 and that $(0) = \bigcap_{i=1}^{s} \mathfrak{n}_{i}$. If $\mathfrak{n}_{1} = \mathfrak{p}_{1}$, choose $\mathfrak{n}'_{1} \supset \mathfrak{n}_{1}$ primary to \mathfrak{p}_{1} , such that $L(\mathfrak{n}_{1}) - L(\mathfrak{n}'_{1}) = 1$. If $\mathfrak{n}_{1} = \mathfrak{p}_{1}$, put $\mathfrak{n}'_{1} = Q$. Choose

$$\varphi \in \mathfrak{n}'_1 \cap \mathfrak{n}_2 \cap \cdots \cap \mathfrak{n}_s, \quad \varphi \neq 0.$$

We shall write down a primary decomposition of the ideal (φ) . As $\mathfrak{p}_1, \ldots, \mathfrak{p}_s, \mathfrak{m}$ are the only prime ideals in Q, and as, for each i, every \mathfrak{p}_i -primary ideal must contain \mathfrak{n}_i , we have

$$(\varphi) = \mathfrak{n}'_1 \cap \mathfrak{n}_2 \cap \cdots \cap \mathfrak{n}_s \cap \mathfrak{q}_0,$$

where q_0 is an m-primary ideal, possibly redundant. Furthermore (cf. the fact that $mq_r \subset q_{\nu+1}$, p. 303),

$$(0): (\varphi) = \mathfrak{p}_1. \tag{13}$$

By Lemma 2, we have

$$L(x^{n}) = L((x^{n}) + (\varphi)) + L((x^{n}) : (\varphi)).$$

Divide by *n* in this formula and let *n* tend to infinity. The left-hand side will tend to e(x). The first term of the right-hand side will tend to $e((x) + (\varphi)/(\varphi))$. By the induction hypothesis we can apply Lemma 4 to the ring $Q/(\varphi)$. In this way we get

$$e\left((x)+(\varphi)/(\varphi)\right)=e\left((x)+\mathfrak{p}_1/\mathfrak{p}_1\right)\left(L\left(\mathfrak{n}_1\right)-1\right)+\sum_{i=2}^{\circ}e\left((x)+\mathfrak{p}_i/\mathfrak{p}_i\right)L\left(\mathfrak{n}_i\right).$$

Thus, in order to prove Lemma 4, it remains to show that

$$\lim_{n\to\infty}\frac{L\left((x^{n}):(\varphi)\right)}{n}=e\left((x)+\mathfrak{p}_{1}/\mathfrak{p}_{1}\right). \tag{14}$$

Since, by our assumption, $(0) = \bigcap_{i=1}^{n} n_i$, we deduce from Lemma 3 that there exists an integer k such that for n > k

$$(x^n):(\varphi) \subset (0):(\varphi) + (x^{n-k}).$$

On the other hand it is obvious that

$$(x^n):(\varphi)\supset(0):(\varphi)+(x^n).$$

Because of (13), these two inclusions imply

$$L\left((x^{n-k})+\mathfrak{p}_1\right) \leq L\left((x^n):(\varphi)\right) \leq L\left((x^n)+\mathfrak{p}_1\right).$$

The formula (14) now follows from (11). Thus the proof of Lemma 4 is complete.

3. Proof of Theorem 1. Assume Q to be an r-dimensional local ring, m its maximal ideal and $\{x_1, \ldots, x_r\}$ a system of parameters in Q. Denote by \mathfrak{S} the set of sequences

$$(p_0, p_1, ..., p_r)$$

of r+1 prime ideals in Q which satisfy the condition that, for $k=0, 1, \ldots, r-1$,

$$\mathfrak{p}_k \supset \mathfrak{p}_{k+1}, \ \mathfrak{p}_k \neq \mathfrak{p}_{k+1} \quad \text{and} \quad \mathfrak{p}_k \supset (x_{k+1}, \ldots, x_r).$$

If $(p_0, \ldots, p_r) \in \mathfrak{S}$, then, for each k, dim $\mathfrak{p}_k + \operatorname{rank} \mathfrak{p}_k = \dim Q$, and dim $\mathfrak{p}_k = k = \dim (x_{k+1}, \ldots, x_r)$, so that \mathfrak{p}_k is a minimal prime ideal of (x_{k+1}, \ldots, x_r) . In particular, it follows that \mathfrak{S} is a finite set. Let us show that, if \mathfrak{p}_m is a minimal prime ideal of (x_{m+1}, \ldots, x_r) such that dim $\mathfrak{p}_m + \operatorname{rank} \mathfrak{p}_m = \dim Q$ (and hence dim $\mathfrak{p}_m = m$, rank $\mathfrak{p}_m = r - m$), then \mathfrak{p}_m occurs in some element of \mathfrak{S} . By passing to the rings Q/\mathfrak{p}_m and $Q_{\mathfrak{p}_m}$, and sets analogous to \mathfrak{S} in these rings, we may reduce the demonstration to showing that the set \mathfrak{S} is necessarily nonvoid. Now an element $(\mathfrak{p}_0, \ldots, \mathfrak{p}_r)$ of \mathfrak{S} may be constructed as follows. Choose \mathfrak{p}_r as a minimal prime ideal of (0) such that dim $\mathfrak{p}_r = r$. Then dim $((x_r) + \mathfrak{p}_r) = r - 1$. Choose \mathfrak{p}_{r-1} as a minimal prime ideal of $(x_r) + \mathfrak{p}_r$ such that dim $\mathfrak{p}_{r-1} = r - 1$. Form $(x_{r-1}) + \mathfrak{p}_{r-1}$, etc.

We introduce the abbreviation

$$E(x; \mathfrak{p}, \mathfrak{a}) = e((x) + \mathfrak{a}/\mathfrak{a}; \mathfrak{p}/\mathfrak{a}),$$

where it is assumed that x is an element and a an ideal of a Noetherian ring, and that p is a minimal prime ideal of (x) + a. Notice that, if (x) + a is an m-primary ideal in Q, then

$$E(x; \mathfrak{m}, \mathfrak{a}) = e((x) + \mathfrak{a}/\mathfrak{a}).$$

We shall prove the following formula:

$$e(x_{1}, ..., x_{r}) = \sum_{(\mathfrak{p}_{0}, ..., \mathfrak{p}_{r}) \in \mathfrak{S}} E(x_{1}; \mathfrak{p}_{0}, \mathfrak{p}_{1}) E(x_{2}; \mathfrak{p}_{1}, \mathfrak{p}_{2}) ... E(x_{r}; \mathfrak{p}_{r-1}, \mathfrak{p}_{r}) L((0); \mathfrak{p}_{r}).$$
(15)

Let us first show that (15) implies Theorem 1. Let \mathfrak{p}_m be the (m+1)th prime ideal in an element of \mathfrak{S} . We shall apply (15) to the ring Q/\mathfrak{p}_m and the parameters in this ring represented by x_1, \ldots, x_m . In order to write down the resulting formula in a suitable form, we observe that the prime ideals in Q/\mathfrak{p}_m are precisely the ideals $\mathfrak{p}/\mathfrak{p}_m$ where \mathfrak{p} is a prime ideal in Q containing \mathfrak{p}_m , and that, furthermore, the symbol $E(x; \mathfrak{p}, \mathfrak{a})$, if defined, does not change its value when x, \mathfrak{p} and \mathfrak{a} are replaced by their residues modulo an ideal contained in \mathfrak{a} . Thus we get

$$e\left((x_1,\ldots,x_m)+\mathfrak{p}_m/\mathfrak{p}_m\right)=\sum_{(\mathfrak{p}_0,\ldots,\mathfrak{p}_m)\in\mathfrak{S}^*(\mathfrak{p}_m)}E\left(x_1;\mathfrak{p}_0,\mathfrak{p}_1\right)\ldots E\left(x_m;\mathfrak{p}_{m-1},\mathfrak{p}_m\right)L\left(\mathfrak{p}_m;\mathfrak{p}_m\right),$$

where $\mathfrak{S}'(\mathfrak{p}_m)$ denotes the set of those sequences of m+1 prime ideals in Q that end with \mathfrak{p}_m and can be extended to elements of \mathfrak{S} . Similarly, by applying (15) to the ring $Q_{\mathfrak{p}_m}$ and the parameters x_{m+1}, \ldots, x_r , we obtain

$$e\left((x_{m+1}, \ldots, x_r); \mathfrak{p}_m\right) = \sum_{(\mathfrak{p}_m, \ldots, \mathfrak{p}_r) \in \mathfrak{S}''(\mathfrak{p}_m)} E\left(x_{m+1}; \mathfrak{p}_m, \mathfrak{p}_{m+1}\right) \ldots \dots E\left(x_r; \mathfrak{p}_{r-1}, \mathfrak{p}_r\right) L\left((0); \mathfrak{p}_r\right),$$

where $\mathfrak{S}''(\mathfrak{p}_m)$ denotes the set of those sequences of r-m+1 prime ideals in Q that begin with \mathfrak{p}_m and can be extended to elements of \mathfrak{S} . Using these two formulas and the fact that $L(\mathfrak{p}_m; \mathfrak{p}_m)=1$, we derive Theorem 1 from (15) by performing the summation in two stages, keeping \mathfrak{p}_m fix in the first stage.

It remains to prove (15). When r=0, the formula (15) follows from the fact that in a zero-dimensional local ring e(0) = L(0). When r=1, the formula (15) follows from Lemma 4. We proceed by induction on r and assume $r \ge 2$. The ideals (x_2^n, \ldots, x_r^n) $(n=1, 2, \ldots)$ have the same minimal prime ideals, all of dimension 1. Let \mathfrak{p} range over these minimal prime ideals. Apply Lemma 4 to the ring $Q/(x_2^n, \ldots, x_r^n)$ and the parameter in this ring represented by x_1 . This yields

$$e((x_1) + (x_2^n, \ldots, x_r^n)/(x_2^n, \ldots, x_r^n)) = \sum_{\mathfrak{p}} E(x_1; \mathfrak{m}, \mathfrak{p}) L((x_2^n, \ldots, x_r^n); \mathfrak{p}).$$

Dividing by n^{r-1} and expressing the multiplicity on the left-hand side according to (1), we obtain

$$\lim_{k \to \infty} \frac{L\left(x_1^t, x_2^n, \ldots, x_r^n\right)}{t n^{r-1}} = \sum_{\mathfrak{p}} E\left(x_1; \mathfrak{m}, \mathfrak{p}\right) \frac{L\left((x_2^n, \ldots, x_r^n); \mathfrak{p}\right)}{n^{r-1}}.$$

On account of Theorem 2 and Lemma 1 we can take n so large that for any given $\varepsilon > 0$

$$\left| \lim_{t \to \infty} \frac{L\left(x_{1}^{\varepsilon}, x_{2}^{\varepsilon}, \dots, x_{r}^{n}\right)}{t n^{r-1}} - e\left(x_{1}, \dots, x_{r}\right) \right| < \varepsilon,$$

$$\left| \frac{L\left((x_{2}^{n}, \dots, x_{r}^{n}); \mathfrak{p}\right)}{n^{r-1}} - e\left((x_{2}, \dots, x_{r}); \mathfrak{p}\right) \right| < \varepsilon \quad \text{when rank } \mathfrak{p} = r - 1,$$

$$\left| \frac{L\left((x_{2}^{n}, \dots, x_{r}^{n}); \mathfrak{p}\right)}{n^{r-1}} \right| < \varepsilon \quad \text{when rank } \mathfrak{p} < r - 1.$$

Hence

$$e(x_1, \ldots, x_r) = \sum_{\operatorname{rank} \mathfrak{p}=r-1} E(x_1; \mathfrak{m}, \mathfrak{p}) e((x_2, \ldots, x_r); \mathfrak{p})$$

By expressing $e((x_2, ..., x_r); p)$ according to the induction hypothesis we arrive at the formula (15). Q.E.D.

4. In analogy with a result of Northcott and Rees and by means of a method of theirs one can deduce from Theorem 1 the following, more general theorem ([4], [5]; esp. [4], Theorem 1, p. 158).

Theorem 3. Let a and b be analytically disjoint ideals in a local ring Q, and assume that a + b is primary to the maximal ideal of Q. Then

$$e(\mathfrak{a}+\mathfrak{b})=\sum_{\mathfrak{p}}e((\mathfrak{a}+\mathfrak{p})/\mathfrak{p})e(\mathfrak{b};\mathfrak{p}),$$

where \mathfrak{p} ranges over those minimal prime ideals of \mathfrak{b} for which dim $\mathfrak{p} + \operatorname{rank} \mathfrak{p} = = \dim Q$.

The notion of analytical disjointness has to be explained. Let m be the maximal ideal and a an arbitrary ideal of Q. For large values of n the dimension of $a^n/a^n m$ over Q/m is equal to a polynomial in n, whose degree increased by 1 is called the "analytic spread" of a and is denoted by l(a). The null polynomial is thereby considered to be of degree -1. Two ideals a and b are called "analytically disjoint" if l(a+b) = l(a) + l(b). It is always true that $l(a+b) \leq l(a) + l(b)$. If q is an m-primary ideal, then $l(q) = \dim Q$. If $\{x_1, \ldots, x_n\}$ is a system of parameters in Q, then, for each $m(0 \leq m \leq r)$, the ideals (x_1, \ldots, x_m) and (x_{m+1}, \ldots, x_r) are analytically disjoint, which shows that Theorem 3 includes Theorem 1.

We shall outline the deduction of Theorem 3 from Theorem 1. Let c be an ideal of a Noetherian ring R. An element x of R is said to be "integrally de-

pendent" on c if it satisfies an equation of the type

$$x^n + \gamma_1 x^{n-1} + \cdots + \gamma_n = 0,$$

where $\gamma_{\nu} \in \mathfrak{c}^{\nu}$ for $\nu = 1, 2, ..., n.\dagger$ The integral closure of \mathfrak{c} , i.e. the set of elements integrally dependent on \mathfrak{c} , is denoted by $\hat{\mathfrak{c}}$. An ideal \mathfrak{c}' such that $\mathfrak{c}' \subset \mathfrak{c} \subset \hat{\mathfrak{c}}'$ is called a "reduction" of \mathfrak{c} . One proves the statements (A)-(D) below: \ddagger

(A) \hat{c} is an ideal;

(B) $\hat{c} = \hat{c};$

(C) c and \hat{c} have the same minimal prime ideals; if p denotes any one of these, then $e(\hat{c}; p) = e(c; p)$;

(D) If c is an ideal in a local ring, then there exists a natural number ν such that c^{ν} , and, in consequence, each of the ideals $c^{\mu\nu}$ ($\mu = 1, 2, ...$), has a reduction generated by l(c) elements.

Let now a and b be the ideals of Theorem 3. According to (D), choose ν such that a' and b' have reductions a'_{ν} and b'_{ν} generated by l(a) and l(b) elements resp. Then $a'_{\nu} + b'_{\nu}$ is m-primary. As $l(a) + l(b) = l(a + b) = \dim Q$, we can apply Theorem 1 with $q = a'_{\nu} + b'_{\nu}$, $v = b'_{\nu}$. We get

$$e(\mathfrak{a}'_{\nu}+\mathfrak{b}'_{\nu})=\sum_{\mathfrak{p}}e((\mathfrak{a}'_{\nu}+\mathfrak{p})/\mathfrak{p})e(\mathfrak{b}'_{\nu};\mathfrak{p}),$$

where \mathfrak{p} ranges over those minimal prime ideals of \mathfrak{b}'_{ν} for which dim $\mathfrak{p} + \operatorname{rank} \mathfrak{p} = \dim Q$. From (A), (B) and the definitions one can infer that the following ideals have two and two the same integral closure: $(\mathfrak{a} + \mathfrak{b})^{\nu}$ and $(\mathfrak{a}'_{\nu} + \mathfrak{b}'_{\nu})$, $(\mathfrak{a}^{\nu} + \mathfrak{p})/\mathfrak{p}$ and $(\mathfrak{a}'_{\nu} + \mathfrak{p})/\mathfrak{p}$, \mathfrak{b}^{ν} and \mathfrak{b}'_{ν} . Hence, by (C),

$$e\left((\mathfrak{a}+\mathfrak{b})^{\nu}\right)=\sum_{\mathfrak{p}}e((\mathfrak{a}^{\nu}+\mathfrak{p})/\mathfrak{p})\ e\left(\mathfrak{b}^{\nu};\ \mathfrak{p}\right).$$

This is the formula of Theorem 3 except for a factor $\nu^{\dim Q}$ in both members. A noteworthy special case of Theorem 3 is obtained by taking for b the zero ideal and for a an arbitrary m-primary ideal. Part of that result has been proved by Northcott and Rees for equicharacteristic local rings ([5], Theorem 1, p. 354).

5. The formulas given below are simple consequences of our previous results. They do not seem to have been proved before without some extra condition for the local rings in question.

In a one-dimensional local ring where x and x' are parameters we have

$$e(xx') = e(x) + e(x').$$
 (16)

[†] There are other equivalent definitions, cf. [4], Theorems 1-3, pp. 155-156, and Definition 1, p. 145, Notice that our "integral dependence" is termed "analytical dependence" in [4].

⁽A)-(C) are inherent in [4], Sections 1 and 7, except for a detail, marked by the presence of the notion of "relevant ideal" in Theorem 3, p. 156. Actually, we indicate in our outline an approach which is slightly different from that of [4], but which seems to us more suggestive. (D) follows by an argument similar to that given in [5], proof of the Theorems 1-4, pp. 355-357.

Proof. Using Lemma 4 (or the first part of its proof) we may assume that x and x' are not zero divisors. Then $(x^n x'^n): (x^n) = (x'^n)$, and hence, by Lemma 2,

$$L(x^{n} x'^{n}) = L(x^{n}) + L(x'^{n}).$$

Hence (16).

Combining (16) with Theorem 1, the case m = 1, we obtain

If $\{x_1, x'_1, x_2, \ldots, x_r\}$ is a system of parameters in a local ring, then

$$e(x_1 x'_1, x_2, \ldots, x_r) = e(x_1, x_2, \ldots, x_r) + e(x'_1, x_2, \ldots, x_r).$$

A repeated application of this formula gives

If $\{x_1, \ldots, x_r\}$ is a system of parameters in a local ring, then

$$e(x_1^{n_1}, \ldots, x_r^{n_r}) = n_1, \ldots, n_r e(x_1, \ldots, x_r).$$

This formula, which is well known in the equicharacteristic case, is also an immediate consequence of Theorem 2.

REFERENCES

- CHEVALLEY, C., Intersections of algebraic and algebroid varieties. Trans. Amer. Math. Soc. 57 (1945), 1-85.
- NORTHCOTT, D. G., Ideal theory. Cambridge Tracts in Math. and Math. Phys. 42. Cambridge 1953. 111 pp.
- 3. ——, Hilbert's function in a local ring. Quart. J. Math. (2), 4 (1953), 67-80.
- NORTHCOTT, D. G. and REES, D., Reductions of ideals in local rings. Proc. Cambridge Phil. Soc. 50 (1954), 145-158.
- 5. ——, A note on reductions of ideals with an application to the generalized Hilbert function. Proc. Cambridge Phil. Soc. 50 (1954), 353-359.
- 6. SAMUEL, P., Algèbre locale. Mémorial Sci. Math. 123. Paris 1953. 76 pp.

Added in proof: In January 1956 a research note by D. Rees appeared, where by means of a beautifully simple argument he proves a great generalization of Lemma 3 of this paper (Rees, D., Two classical theorems of ideal theory, Proc. Cambridge Phil. Soc. 52 (1956), 155–157; the Corollary on p. 156 may be formulated: If a is an ideal and x an element of a Noether ring, there exists an integer k such that $a^n : x < 0 : x + a^{n-k}$ if n > k). Using this result we could have given a more direct final proof of Theorem 1 by first proving a more general Lemma 4, covering the case m = r of Theorem 1 instead of merely the case m = r = 1.

Tryckt den 17 februari 1956

Uppsala 1956. Almqvist & Wiksells Boktryckeri AB