SOME RESULTS ON LOCAL RINGS

by

Mohammed Reza Adranghi

A thesis submitted for the degree of

Master of Philosophy

FACULTY OF MATHEMATICAL STUDIES

The University of Southampton

January 1978

UNIVERSITY OF SOUTHAMPTON

ABSTRACT

FACULTY OF MATHEMATICAL STUDIES

Master of Philosophy

SOME RESULTS ON THE LOCAL RINGS

by Mohammed Reza Adranghi

The main aim of this thesis is to present a certain lattice associated with a local ring and to determine this lattice when the local ring is one-dimensional and has multiplicity two.

For, a one-dimensional local ring Northcott produces a tree of neighbourhood rings by localizing the first neighbourhood ring at its maximal ideals and resolving again and again. We prefer to generalize the first neighbourhood ring and so produce a lattice of finite extension rings of a local ring.

For the application to multiplicity two, we rely on the basic result due to Matlis. In 1973 he showed that when the one-dimensional local ring Q has multiplicity two, then every ideal of the local ring can generated by two elements and that the local ring has a superficial element of degree one which belongs to the maximal ideal of the local ring. With this as starting point we determine the lattice of the local ring Q. The idea of using the lattice to characterize local rings was suggested by D.Kirby in the geometric case, but we are concerned with the abstract case. It is shown that the lattice of finite extension rings of Q is totally ordered either finite if the integral closure of Q is a finite Q-module or infinite in the opposite case.

Contents

Introduction

The main purpose of this thesis is in the first place to study the lattice $\mathcal{L}(Q)$ of extension rings of a local ring Q which are finite Q-modules, and in the second place to determine $\mathcal{L}(Q)$ when Q is one-dimensional of multiplicity $e(Q) = 2$.

In the first chapter we introduce the notion of a superficial element of an ideal of Q, a notion which is due to Samuel [15] and [16]. We give various known results on superficial elements in particular establishing their existence and including five equivalent defining properties.

In the second chapter we consider the characteristic or Hilbert function of a local ring, the basic work is due to P.Samuel [16], and Northcott [7] generalized such a function. Here we establish its existence in a new way by using superficial elements. In the dimension one case the characteristic function is of the form $en-\rho$, and we give some known relationships between e and ρ.

In the third chapter we consider the first neighbourhood ring of a local ring Q which is due to Northcott. He produces a tree of the neighbourhood ring by localizing the first neighbourhood ring R_1 at its maximal ideals and resolving again, instead we prefer to generalize the first neighbourhood ring Q by producing the lattice of finite extension rings of Q.

In chapter four we study the lattice $\mathcal{L}(Q)$ where Q is one-dimensional local ring of multiplicity two in this case $\mathcal{L}(Q)$ is totally ordered, so the lattice $\mathcal{L}(Q)$ of finite extension rings $\mathcal{L}(Q)$ will either be finite

$$R_0 \subset R_1 \subset R_2 \subset \ldots \subset R_n$$

where R_n is integral closure $\hat{Q}$ of the local ring Q

or $$R_0 \subset R_1 \subset \ldots. \subset R_i \subset \ldots.$$

where each R_i is a local ring with multiplicity two.

Our system of reference throughout the thesis is as follows:

When a reference is made to (4.5.1) it means the first result or definition of section 5 in chapter 4. A reference such as [6] refers to the list of references at the end of the thesis.

Acknowledgements

I would like to express my grateful thanks to Dr. D. Kirby for his unfailing help during the period of my research in the University of Southampton.

Chapter I

Superficial elements

(1.1) Introduction.

Throughout this chapter, Q will be a local ring, m will denote its maximal ideal, q will denote an ideal of Q which is not the whole ring i.e. $m \supseteq q$.

In [15] and [16] Samuel introduces the idea of a superficial element of an ideal q of a Noetherian ring Q, where $\bigcap_{n=0}^{\infty} q^n = 0$, in fact Samuel gave two equivalent defining properties for superficial elements, one of which shows their existence. And Northcott [13] and [10] used such elements in the dilatations of a local ring, when Q is a local ring and $q = m$. In addition, Northcott [10] gave a third defining property which applies when Q is one-dimensional local ring. Then Kirby [1] by using the ring of q-forms in the general local ring gave a set of five equivalent defining properties of superficial element.

In this chapter we repeat some of Samuel's and Kirby's work and give five equivalent defining properties for such elements. Then we establish the existence of superficial elements. Also we consider the one-dimensional case when we apply the results of the five equivalent defining properties.

(1.2) The ring of q-forms.

Let Q be a local ring, m be the maximal ideal of Q and let q be an m-primary ideal, so that $\bigcap_{n=0}^{\infty} q^n = (0)$, in particular Q/q

is a Noetherian ring. It is clear that $F_n(q) = q^n/q^{n+1}$ is (Q/q) -module where, $n = 0,1,2,\ldots$. From this, it follows, for every non-null element x of Q, there is a unique integer and such that $x \in q^s$ and $x \notin q^{s+1}$ which has a unique image in $F_s(q)$, that is $\bar{x} = (x+q^{s+1})/q^{s+1}$ which is called as the q-form of x and s is called the degree of $\bar{x}$. If $\bar{x} \in F_s(q)$ and $\bar{y} \in F_t(q)$ we define $\bar{\bar{x}}\bar{\bar{y}}$ as follows: Let x and y be elements of q^s and q^t respectively such that $x \in \bar{x}$ and $y \in \bar{y}$ and, then we define $\bar{\bar{x}}\bar{\bar{y}} = (xy+q^{s+t+1})/q^{s+t+1}$ $(\in F_{s+t}(q))$. It is easy to verify that $\bar{\bar{x}}\bar{\bar{y}}$ is independent of the choice of $x \in \bar{x}$ and $y \in \bar{y}$. This multiplication defines a ring structure in the direct sum $F(q)$ of all the $F_n(q)$, and $F(q)$ becomes a commutative graded ring. Since $F_n(q) = q^n/q^{n+1}$ it follows that $F_n(q) = (F_1(q)^n)$, which implies that $F(q)$ is a homogeneous ring. This homogeneous ring $F(q)$ is called the ring of q-forms and

$$F(q) = \sum_{n=0}^{\infty} q^n/q^{n+1}$$

(1.2.1) Proposition: The ring of q-forms $F(q)$ is Noetherian.

Proof. Suppose that the ideal q admits a finite fixed base $q = (u_1,u_2,\ldots,u_r)$ where, however, this base of q need not be minimal. Let $\phi(u) = \phi(u_1,\ldots u_r)$ be a form of degree $s \geq 0$ in the u_i with coefficients in Q and such that not all the coefficients of ϕ are in q, further let $\bar{\phi}(X) = \bar{\phi}(X_1,X_2,\ldots X_r)$ be obtained from ϕ by replacing each u_i by indeterminates X_i and each coefficient by its residue modulo q, thus making $\bar{\phi}(X)$ a form in the polynomial ring $(Q/q)[X_1,X_2,\ldots X_r]$. Since Q/q is Noetherian so $(Q/q)[X_1,X_2,\ldots X_r]$

is Noetherian. We map a form ϕ of degree s in $(Q/q)[X_1, X_2, \ldots X_r]$ onto an element of $F_s(q)$ by replacing the coefficients by elements of Q and X_i by u_i and so obtain a representative in q^s of the unique image of ϕ in $F_s(q)$. We thus obtain a (Q/q)-homomorphism of $(Q/q)[X_1, X_2, \ldots X_r]$ on to $F(q)$. The kernel of the homomorphism is a homogeneous ideal N_o of $(Q/q)[X_1, X_2, \ldots X_r]$. Hence the rings $(Q/q)[X_1, \ldots X_r]/N_o$ and $F(q)$ are isomorphic and since the former is Noetherian so $F(q)$ is Noetherian.

Let us now introduce the ideal $\bar{I}$ of the ring $F(q)$ generated by the q-forms of strictly positive degree i.e.

$$\bar{I} = \sum_{n=1}^{\infty} q^n/q^{n+1} = F(q) - F_0(q)$$

(1.2.2) Proposition. q is nilpotent if and only if $\bar{I}$ is nilpotent.

Proof. ~~Let $\bar{I}$ be an ideal of the q-forms, then~~ We have

$$\bar{I}^k = F(q) - \sum_{j=0}^{k-1} F_j(q)$$

If q is nilpotent so $q^k = 0$ for some k then $q^t = 0$ for $t \geq k$ and $\bar{I}^k = F(q) - \sum_{j=0}^{k-1} F_j(q) = 0$

Conversely, if $\bar{I}^k = 0$ it is clear that $q^t = q^{t+1}$ for $t \geq k$ so $q^t \subseteq \bigcap_{n=1}^{\infty} q^n = 0$

Hence $q^t = 0$ i.e. q is nilpotent.

It will now be convenient to introduce some more notations.

(1.2.3) We denote by b the isolated component of the zero ideal of Q determined by the prime ideals which belong to the zero-ideal and do not contain q, more precisely b is the set of elements x such that $xq^k = 0$ for some k.

Also we denote by $\bar{N}$ the homogeneous ideal in $F(q)$ whose elements $\bar{x}$ satisfy $\bar{x}\,\bar{I}^k = 0$ for some k. We suppose neither q nor $\bar{I}$ is nilpotent, so neither b nor $\bar{N}$ is the whole ring and from the definition of b and $\bar{N}$ we can deduce that for some k large enough,

$$q^k \cap b = 0\,,\quad \bar{I}^k \cap \bar{N} = 0,\quad b:q = b,\quad \bar{N}:\bar{I} = \bar{N}\,.$$

In fact, if $\bar{I}^k \cap \bar{N} = 0$, it can be shown that $q^k \cap b = 0$.

(1.2.4) Theorem. Let $x \in q^s$ and $x \notin q^{s+1}$ and let $\bar{x}$ be the q-form of x. The following three conditions are equivalent

(i) $\bar{N}:(\bar{x}) = \bar{N}$

(ii) $q^{n+s} \cap Qx = xq^n$ for all n large enough, and $b:(x) = b$

(iii) $(q^{n+s}:Qx) \cap q^c = q^n$ for some integer c and all $n \geq c$.

Proof. It will be shown first that (i) and (iii) are equivalent and then that (iii) and (ii) are equivalent.

Assume that (i) is true then we consider $y \in (q^{n+s}:Qx) \cap q^t$ where $\bar{N} \cap \bar{I}^t = 0$.

Now let us choose an integer r such that $y \in q^r$ and $y \notin q^{r+1}$; then $r \geq t$ and $\bar{y}$ the unique image of y in $F_r(q)$ would belong to $\bar{I}^t$. Thus $\bar{x}\bar{y}$ has degree $r+s$ and also $xy \in q^{n+s}$. If $r < n$, then we have $xy \in q^{r+s+1}$, so that $\bar{x}\bar{y} = 0$ therefore it is clear that $\bar{y} \in 0:(\bar{x}) \subseteq \bar{N}:(\bar{x}) = \bar{N}$.

But $\bar{y} \in \bar{I}^t$ and so $\bar{y} \in \bar{N} \cap \bar{I}^t = 0$, this however, is contradiction because $y \notin q^{r+1}$.

Consequently $r \geq n$ and $(q^{n+s}:Qx) \cap q^t \subseteq q^n$. Since the opposite inclusion is obvious for $n \geq t$, then (iii) is proved.

Assume that (iii) is true and choose $\bar{y} \in \bar{N}:(\bar{x})$ with degree n. Then $\bar{\bar{x}}\bar{\bar{y}}\,\bar{I}^t = 0$.

Let $\bar{y}$ be the q-form of y with $y \in q^n$ and $y \notin q^{n+1}$. Let now α be any element of q^k, where $k = \max(t,c)$; then $\bar{\bar{\alpha}}\bar{\bar{x}}\bar{y} = 0$ and $\alpha xy \in q^{n+s+k+1}$.

Therefore $$\alpha y \in (q^{n+s+k+1}: Qx) \cap q^c = q^{n+k+1}$$

and consequently $y\,q^k \subseteq q^{n+k+1}$ or $\bar{\bar{y}}\bar{I}^k = 0$.

Thus $\bar{y}$ belong to $\bar{N}$ and $\bar{N}:(\bar{x}) \subseteq \bar{N}$. Again the opposition inclusion is obvious. So (i) is proved.

Next we prove that (ii) and (iii) are equivalent.

Suppose that (iii) is true, then let $z = xy \in q^{n+s} \cap Qx$. Then by Rees lemma [14] we have $y \in q^{n+s}: Qx \subseteq 0:Qx+q^{n+s-k}$ for some $k(\geq s)$ and all $n \geq k-s$. Suppose $n \geq k-s+c$ and call $k-s+c = n_0$ then, for some $y' \in q^{n+s-k} = q^{n+c-n_0} \subseteq q^c$ we have $x(y-y') = 0$. Therefore $z = xy = xy' \in q^{n+s}$ and

$$y' \in (q^{n+s}: Qx) \cap q^c = q^n .$$

Hence $z \in x\,q^n$ and $q^{n+s} \cap Qx \subseteq xq^n$ for $n \geq n_0$. Since $x \in q^s$, we have $(q^{n+s} \cap Qx) \supseteq x\,q^n$, and therefore $q^{n+s} \cap Qx = x\,q^n$.

In order to prove (ii) we must also show that $b:(x) = b$. For this let us suppose y belongs to $b:(x)$, so that xy belongs to b. Then $xy\,q^t = 0 \subseteq q^{n+s}$. Now we put $k = \max(t,c)$; from this it follows immediately that

$$yq^k \subseteq (q^{n+s}: Qx) \cap q^c = q^n \quad \text{for all } n \geq c.$$

Hence $yq^k \subseteq \bigcap_{n=1}^{\infty} q^n = 0$ and $y \in b$. Therefore $b:(x) = b$, so the second part of (ii) is established.

Finally assume that (ii) is true then we consider $y \in q^{n+s} : Qx$. If (ii) holds for $n \geq n_o$ we have

$$xy \in q^{n+s} \cap Qx = xq^n \qquad \text{for } n \geq n_o$$

Hence $$y \in q^n + 0 : Qx \subseteq q^n + b : Qx = q^n + b$$

i.e. $$q^{n+s} : Qx \subseteq q^n + b .$$

Let us put $c = \max(t, n_o)$. Then

$$(q^{n+s} : Qx) \cap q^c \subseteq (q^n + b) \cap q^c = q^n + b \cap q^c = q^n \quad \text{for } n \geq c.$$

Also for $n \geq c$ we have

$$(q^{n+s} : Qx) \cap q^c \supseteq q^n$$

since $x \in q^s$. Therefore

$$(q^{n+s} : Qx) \cap q^c = q^n \quad \text{for } n \geq c.$$

The proof of the theorem is thus complete.

(1.2.5) Definition. An element x is said to be a superficial element of degree s with respect to q when $x \in q^s$ and there is an integer c such that

$$(q^{n+s} : Qx) \cap q^c = q^n \qquad \text{for } n \geq c .$$

Note. If $x \in q^{s+1}$, then $(q^{n+s} : Qx) \cap q^c \supseteq q^{n-1} \supset q^n$ for $n > c$, so for x to be superficial element of degree s it is necessary that $x \notin q^{s+1}$.

(1.2.6) Example. Suppose $Q = k[[t^2, t^3]]$ be a power series ring and $q = (t^2, t^3)$, then a superficial element of degree 1 is $x = t^2$. However $t^3 \in q - q^2$ is not superficial element of degree 1 $(t^{2n-1} \in (q^{n+1} : Qt^3) - q^n$ for $n > 1)$.

This shows that the above necessary condition is not sufficient in the general case. It is nevertheless sufficient whenever $F(q)$ is an integral domain.

Another instance in which the existence of such an element is guaranteed is given by the following theorem.

(1.2.7) Theorem. Let Q be local ring and q be an ideal of Q there exist an integer s and an element x of Q such that x is superficial element of degree s.

Proof. We consider in the ring of q-forms $F(q)$, the associated prime ideals p_j of the zero-ideal (0), and we assume that p_j does not contain the ideal $\bar{I}$ for $1 \leq j \leq \ell$ of the $F(q)$. Otherwise $p_j \supseteq \bar{I}$ for $\ell+1 \leq j \leq k$. It is easily seen that there exists a homogeneous element $\bar{x}$ of positive degree say s such that $\bar{x} \notin p_j$ for $1 \leq j \leq \ell$. To prove this, we replace the set $\{p_j\}$ for $1 \leq j \leq \ell$ by $\{p_\mu\}$ of maximal elements in the set. Since $\bar{I} \not\subseteq p_\mu$ there exists a homogeneous element β_μ of $\bar{I}$ of degree one such that $\beta_\mu \notin p_\mu$. On the otherhand, for $\mu' \neq \mu$ there exists a homogeneous element $X_{\mu\mu'}$, in $p_{\mu'}$, where $X_{\mu\mu'} \notin p_\mu$. We set

$X_\mu = \left(\beta_\mu^{n(\mu)} \prod_{\mu' \neq \mu} X_{\mu\mu'}\right)$, the exponents $n(\mu) \geq 1$. are chosen in such a way that the elements X_μ have the same degree. So $X_\mu \notin p_\mu$ and $X_\mu \in p_{\mu'}$, for $\mu \neq \mu'$.

Hence the homogeneous element $\bar{x} = \sum_\mu X_\mu$ satisfies the conditions $\bar{x} \notin p_\mu$ for $1 \leq \mu \leq \ell$. Let q_j be a primary componant

of (0) corresponding to p_j. For $\ell+1 \leq j \leq k$, q_j contains some power of $\bar{I}$. Let c be an integer such that $\bar{I}^c \subseteq \bigcap_{j=\ell+1}^{k} q_j$. Suppose now that $\alpha \in \bar{N} : (\bar{x})$, then $\alpha \bar{x} \in \bar{N}$ and $\alpha \bar{x} \bar{I}^{\ell} = (0)$ by definition of $\bar{N}$. As $\bar{x} \notin p_\mu$ for $1 \leq \mu \leq \ell$ this implies that

$$\alpha \bar{I}^{\ell} \subseteq \bigcap_{j=1}^{\ell} q_j$$

Also

$$\bar{I}^c \subseteq \bigcap_{j=\ell+1}^{k} q_j$$

so

$$\alpha \bar{I}^{\ell+c} \subseteq \bigcap_{j=1}^{k} q_j = (0)$$

Therefore α belongs to $\bar{N}$ and $\bar{N}:(x) = \bar{N}$ which by (1.2.4) means $\bar{x}$ is the form in $F(q)$ of a superficial element of q.

(1.2.8) Remark. There does not always exist a superficial element of given degree.

(1.2.9) Example. Suppose $Q = F_2[[X,Y]]/(XY(X+Y))$. In fact if x and y denote the classes of X,Y in Q then take $q = (x,y)$. It is clear that the ring of the q-forms is

$$F_2[X,Y]/XY(X+Y)$$

Meanwhile the only elements of degree one of Q namely x,y and $x+y$ (F_2 is field of two elements) are not superficial elements.

However the freedom of choice of the exponent $n(\mu)$ in the proof of (1.2.7) can be used to show that q' has superficial elements of every sufficiently large degree.

(1.2.10) Now we consider some more notation.

It is clear that the $Q/b = Q'$ is a local ring with maximal ideal image $m' = m/b$. Also put $q' = (q + b)/b$ the image of q in Q'. Thus we can construct the commutative graded ring $F(q')$ of q'-forms, and the homogeneous ideal $\bar{I}'$ and $\bar{N}'$ of $F(q')$ can be defined as before.

We denote the ideal

$$\sum_{n=0}^{\infty} (b \cap q^n + q^{n+1})/q^{n+1}$$

of $F(q)$ by $\bar{b}$ and establish the following relationship between $F(q)$ and $F(q')$.

(1.2.11) Theorem. $\bar{N} \supseteq \bar{b}$; and there is a canonical homomorphism of $F(q)$ onto $F(q')$ which has $\bar{b}$ as kernel in which $\bar{I}'$ and $\bar{N}'$ are the images of $\bar{I}$ and $\bar{N}$.

Proof: As page 23 [1]

The next theorem which is proved on page 25 [1] explores the relation between superficial elements of q and superficial elements of the image q' of q in Q'.

(1.2.12) Theorem. (i) Let $x \in Q$ and let x' be its image in Q'. If x is a superficial element of q of degree s, then x' is a superficial element of q' of degree s.

(ii) Let $x' \in Q'$ and let x be a representative of x' in Q. Let x' be a superficial element of q' of degree s. x is a superficial element of q if and only if the degree of $\bar{x}$ is s.

(1.2.13) With these two theorems and theorem (1.2.4) Kirby [1] gave other equivalent conditions for superficial elements.

(i) x is superficial element of q.

(ii) $(q^{n+s} + b) \cap (Qx + b) = xq^n + b$ for n large and $b:(x) = b$

(iii) $(q^{n+s} + b):Qx = q^n + b$ for large n.

In fact we have five equivalent conditions for the superficial element of q.

(1.2.14) In addition we must note that the following facts.

(a) The superficial elements of degree zero are the units of Q

(b) If x_s and x_t are superficial elements of degree s and t respectively, then $x_s.x_t$ is a superficial element of degree $t + s$.

Proof. (a) is trivial

Proof. (b) If $\bar{x}_s$ and $\bar{x}_t$ be the q-forms of x_s and x_t respectively then we have $\bar{x}_s.\bar{y}_t = x_s y_t + q^{1+s+t}/q^{1+s+t}$ so by condition (i) of theorem (1.2.4) we have

$$\bar{N} : (\bar{x}_s.\bar{x}_t) = (\bar{N} : (\bar{x}_s)) : (\bar{x}_t) = \bar{N} .$$

(1.3) One-dimensional case.

Throughout this section, Q is a one-dimensional local ring and m is the maximal ideal of Q and q is an m-primary ideal.

In fact if Q is one-dimensional local ring then it follows that $\dim b = 1$.

(1.3.1) Theorem. Let $x \in q^r$ and $x \notin q^{r+1}$, then x is superficial element of degree r with respect q if and only if $q^{n+r} = x\,q^n$ for n large enough.

Proof. Suppose x is superficial element of degree r then by theorem (1.2.13) we have

$$(q^{n+r} + b) \cap (Qx + b) = xq^n + b$$

for n sufficiently large and $b : Qx = b$.

Since $\dim b = 1$ and $b:Qx = b$ we deduce $Qx + b$ is m-primary ideal of Q. Therefore for n sufficiently large $b + Qx$ contains $q^{n+r} + b$, consequently

$$q^{n+r} + b = xq^n + b \qquad (1.1)$$

for n sufficiently large. Now we intersect both sides of the equation (1.1) with q^t then we have

$$(q^{n+r} + b) \cap q^t = (xq^n + b) \cap q^t \qquad (1.2)$$

It is clear that if $n+r \geq t$ where $q^t \cap b = 0$ then the equation (1.2) is just

$$q^{n+r} = xq^n \quad \text{for} \quad n \geq n_o$$

Conversely, suppose $q^{n+r} = xq^n$ for $n \geq n_o$ it is obvious that $q^{n+r} \cap Qx = xq^n$ for $n \geq n_o$.

Further if y belongs to $b:Qx$, then b contains yQx which also contains yq^{n+r}. Hence $yq^k \subseteq q^t \cap b = 0$ where $k = \max(n_o + r, t)$ and $y \in b$, therefore $b:Qx = b$ and $q^{n+r} \cap Qx = xq^n$ for n sufficiently large. Consequently by condition (ii) of theorem (1.2.4) x is superficial element of degree r with respect to q.

(1.3.2) Now we consider the ring of q-forms $F(q)$ and the homogeneous ideal $\tilde{I} = \sum_{n=0}^{\infty} mq^n/q^{n+1}$.

We denote by $\bar{M}$ the set of elements $\bar{x}$ such that $\bar{x}\,\bar{I}^k \in \tilde{I}$ for some k. It follows that $\bar{M}$ is a homogeneous ideal of the ring of q-forms, none of the primes belonging to $\bar{M}$ contains $\bar{I}$ and $\bar{M} \supseteq \bar{N}$. Again in $F(q')$ we consider $\tilde{I}' = \sum_{n=0}^{\infty} m'q'^n/q'^{n+1}$ and construct $\bar{M}'$. By theorem 7 of [1] (x is superficial element of q if and only if $\bar{M}:(\bar{x}) = \bar{M}$ where $\bar{x}$ is the q-form of x), the theorem provides an easy way of finding the superficial element of q where $\dim b = 1$. For this: instead of considering the ring of q-forms $F(q)$ we construct the ring $\sum_{n=0}^{\infty} q^n/mq^n$. Of course this is a homomorphic image of $K[X_1.....X_r]$ where $K = Q/m$. In fact this homomorphism is constructed in the manner of (1.2.1). If $\bar{a}$ is the kernel of the homomorphism, it is obvious that $\bar{a}$ is a one-dimensional homogeneous ideal and

$$K[X_1....X_r]/\bar{a} \simeq \sum_{n=0}^{\infty} q^n / mq^n .$$

Suppose $y \in Q$ which satisfies $y \in q^r$ and $y \notin q^{r+1}$ gives rise to a form $\bar{y}$ of degree r in the ring $\sum_{n=0}^{\infty} q^n / mq^n$. Let $\bar{y}_1$ be a representative of $\bar{y}$ in $K[X_1....X_r]$ such that $\bar{y}_1$ is a form of degree r, then it is obvious that y is a superficial element of q if and only if $\bar{y}_1$ is contained in none of the one-dimensional prime ideals belonging to $\bar{a}$.

Chapter II

(2.1) Hilbert functions and multiplicity.

Introduction. Throughout this chapter Q is a local ring, m its maximal ideal of Q, and q is an m-primary ideal of Q.

Our aim in this chapter is to introduce the characteristic or Hilbert function of a local ring, a notion which is due to P.Samuel [16].

In [7] Northcott introduced the generalized Hilbert function, here we repeat some of his work, then we prove the existence of such function by using superficial elements.

In section five we introduce the coefficients $e_i(q)$ of the abstract Hilbert function in the local ring of dimension $d \geq 0$ [6].

If $d = 1$, then characteristic or Hilbert function takes the form $en - \rho$, where e is called the multiplicity of Q and ρ the reduction number of Q.

Subsequently, we quote some relationships between e and ρ from [3] and [4].

(2.2) Elementary properties.

(2.2.1) The length of a primary ideal.

Suppose q is an m-primary ideal in the local ring Q, where m is the maximal ideal of Q and suppose also that $q_1, q_2, \ldots, q_\ell$ are m-primary ideals such that $m = q_1 \supset q_2 \supset \cdots \supset q_\ell = q$ where all the inclusions are strict. We shall describe this situation

by saying that $[q_1,q_2,\ldots,q_\ell]$ is a primary chain from m to q. If now $[q_1,q_2,\ldots,q_\ell]$ and $[q_1', q_2',\ldots,q_k']$ are two primary chains from m to q, then we shall say that $[q_1',q_2',\ldots,q_k']$ is a refinement of $[q_1,q_2,\ldots,q_\ell]$ if every q_i occurs among the q_j'. Moreover, if, in addition, the two chains are not identical then we shall say that $[q_1',q_2',\ldots,q_k']$ is a proper refinement of $[q_1,q_2,\ldots,q_\ell]$.

A primary chain from m to q will be called a composition series for q if it has no proper refinement. If $q = m$ then there is only one-primary chain from m to q, namely $[m]$, and this is also a composition series for m.

(2.2.2) Definition. A Noetherian ring, which has only one proper prime ideal, will be called a primary ring.

We can now make a further simplification.

Since every proper prime ideal which contains q must contain m and since m is maximal ideal of Q, it follows that m is the only proper prime ideal which contains q. This shows that $Q/q = A$ is a Noetherian ring which has only one proper prime ideal, namely $p = m/q$. Also there is 1-1 correspondence between chains of ideals from m to q and chains of ideals from p to the zero ideal of A.

(2.2.3) The number of terms in a composition series of a primary ring A does not depend on the composition series.

Suppose A is a primary ring then we can find a decreasing chain $P = C_1 \supset C_2 \supset \ldots \supset C_h = (0)$ of h ideals, stretching from the only proper prime ideal P to (0), such that for each i there is no ideal strictly between C_i and C_{i+1}. Suppose now that M is some

finitely generated A-module, say

$$M = A\lambda_1 + A\lambda_2 + \ldots + A\lambda_\ell$$

If $\lambda_1, \lambda_2, \ldots, \lambda_\ell$ are independent, i.e. if

$$\alpha_1\lambda_1 + \alpha_2\lambda_2 + \ldots + \alpha_\ell\lambda_\ell = 0$$

where $\alpha_i \in A$, only when all the α_i are zero, then a composition series composed of submodules of M will contain exactly ℓh terms, if $\lambda_1, \lambda_2, \ldots, \lambda_\ell$ are not independent, a composition series of submodules of M will contain fewer than ℓh terms.

Let us denote the number of terms in a composition series for M by $\dim_A M$; then, for example, if q = m,A will be a field and $\dim_A M$ will have its usual meaning. Also note that, if E_1 and E_2 are submodules of M, with respect to A then.

$$\dim_A(E_1 + E_2) + \dim_A(E_1 \cap E_2) = \dim_A E_1 + \dim_A E_2$$

because, using a familiar theorem on isomorphisms,

$$\dim_A(E_1 + E_2) - \dim_A E_1 = \dim_A(E_1 + E_2)/E_1$$

$$= \dim_A E_2/(E_1 \cap E_2)$$

$$= \dim_A E_2 - \dim_A(E_1 \cap E_2).$$

(2.2.4) Definition. If q is a primary ideal in a Noetherian ring, then the number of terms in a composition series for q will be called the length of q.

(2.3) Hilbert's function in a local ring.

Suppose that K is a field and I is a homogeneous ideal in the polynomial ring $K[X_0,X_1,\ldots X_r] = K[X]$. If $f(s,I)$ is the vector space over K consisting of all the forms of degree s contained in I and if $f(s)$ is the vector space of all forms of degree s then

$$\chi(s,I) = \dim_K f(s) - \dim_K f(s,I)$$

is called the Hilbert function of I. Let us now pass to the ring of quotients of $K[X]$ with respect to the prime ideal $(X_0,X_1,\ldots.X_r)=(X)$ which we shall denote by Q.$Q$is a local ring with maximal ideal $m = Q(X)$. Since I is a homogeneous ideal if we write $I' = QI$, then $I' \cap K[X] = I$. It is easily verified that

$$\dim_K f(s,I) = \dim_K (I' \cap m^s / I' \cap m^{s+1})$$

and (as a special case)

$$\dim_K f(s) = \dim_K m^s/m^{s+1}$$

Accordingly, if we write $\chi(s,I') = \chi(s,I)$ then

$$\chi(s,I') = \dim_K (m^s/m^{s+1}) - \dim_K (I' \cap m^s/I \cap m^{s+1})$$

This formula together with $K = Q/m$ provides a mean of extending the definition of the characteristic or Hilbert function $\chi(s,I)$.

(2.4) The generalized Hilbert function.

Let I be an arbitrary ideal of Q. Then for any $s \geq 0$ we have $q(I \cap q^s) \subseteq I \cap q^{s+1}$ and so $(I \cap q^s)/(I \cap q^{s+1})$ is an A-module which is, moreover finitely generated accordingly by the previous notations.

$$\dim_A(I \cap q^s) \,/\, (I \cap q^{s+1})$$

is defined and is finite, consequently put

$$\chi_q(s,I) = \dim_A(q^s/q^{s+1}) - \dim_A(I \cap q^s)/(I \cap q^{s+1})$$

and call $\chi_q(s,I)$ the Hilbert function or characteristic function of I with respect to q.

In fact, from the isomorphism theorem as in (2.2.3), it is easily verified that (7 page 69)

$$\chi_q(s,I) = \dim_A(I + q^s)/(I + q^{s+1})$$

and therefore $\chi_q(s,I)$ is the length of a composition series of ideals from $I + q^s$ to $I + q^{s+1}$.

Suppose now that I is a proper ideal then we put

$$\bar{Q} = Q/I \quad , \quad \bar{q} = (I + q)/I \ .$$

Of course, $\bar{Q}$ is a local ring with maximal ideal $\bar{m} = m/I$ and $\bar{q}$ is an $\bar{m}$-primary ideal. Moreover $I + q^s$, $\bar{q}^s$ are corresponding ideals. If $(\bar{0})$ be the zero ideal of $\bar{Q}$ then it is clear that:

(2.4.1) Theorem. Let I be a proper ideal of Q. Let $\bar{q} = (I + q)/I$ and let $(\bar{0})$ denote the zero ideal of $\bar{Q} = Q/I$, then $\chi_q(s,I) = \chi_{\bar{q}}(s,\bar{0})$.

(2.4.1.1) Corollary 1. $\chi_q(s,I) = \chi_{q+I}(s,I)$.

This follows from the theorem immediately.

(2.4.1.2) Corollary 2. $\sum_{s=0}^{n-1} \chi_q(s,I) = P_{\bar{q}}(n)$ where $P_{\bar{q}}(n)$ denotes the length of the primary ideal $\bar{q}^n$,

Proof: As we described that $\chi_q(s,I)$ is equal to the length of a composition series of ideals from $\bar{q}^s$ to $\bar{q}^{s+1}$. The corollary follows by summation.

(2.4.2) It is one of Samuel's basic results that $P_{\bar{q}}(n)$ is a polynomial in n for sufficiently large values of n and that the degree of this polynomial is the dimension, $\dim\bar{Q}$ of $\bar{Q}$.

The polynomial to which $P_{\bar{q}}(n)$ is equal for large values of n is called the characteristic polynomial of the ideal $\bar{q}$. We shall denote it by $\bar{P}_{\bar{q}}(n)$, and sometimes by $P_{\bar{q}}(n)$ when we are dealing with large values of n. As ([17] page 233) we find also here that, if $\bar{P}_{\bar{q}}(n)$ is a polynomial of degree d, its coefficients are integral multiples of $1/d!$.

Now we prove some simple results about characteristic functions.

(2.4.2.1) Lemma 1. Let $\bar{q}$ be an $\bar{m}$-primary ideal of the local ring $\bar{Q}$, then $P_{\hat{\bar{Q}}\bar{q}}(n) = P_{\bar{q}}(n)$ where $\hat{\bar{Q}}$ is the completion of the local ring $\bar{Q}$

Proof. It is clear that $\bar{Q}/\bar{q}^n$ and $\hat{\bar{Q}}/\hat{\bar{Q}}\bar{q}^n$ are isomorphic ([17] chapter VIII, §2, theorem 6).

(2.4.2.2) Lemma 2. If $\bar{q}$ and $\bar{q}'$ are $\bar{m}$-primary ideals of the local ring $\bar{Q}$ and if $\bar{q} \subset \bar{q}'$ then $P_{\bar{q}}(n) \geq P_{\bar{q}'}(n)$ for all n.

Proof: Obvious.

(2.4.2.3) Lemma 3. Let $\bar{q}$ be an $\bar{m}$-primary ideal of the local ring $\bar{Q}$ and let x be an element of $\bar{q}$, then

$$P_{\bar{q}/\bar{Q}x}(n) = P_{\bar{q}}(n) - \lambda(\bar{q}^n : \bar{Q}x) .$$

Proof. In fact $(\bar{Q}/\bar{Q}x)/(\bar{q}/\bar{Q}x)^n \simeq \bar{Q}/(\bar{q}^n + \bar{Q}x)$.

whence

$$P_{\bar{q}}(n) - P_{\bar{q}/\bar{Q}x}(n) = \text{length}\,(\bar{Q}/\bar{q}^n) - \text{length}\,(\bar{Q}/(\bar{q}^n + \bar{Q}x))$$

$$= \text{length}\,(\bar{q}^n + \bar{Q}x/\bar{q}^n) = \text{length}\,(\bar{Q}x/(\bar{q}^n \cap \bar{Q}x))$$

then

$$P_{\bar{q}}(n) - P_{\bar{q}/\bar{Q}x}(n) = \text{length}\,(\bar{Q}x/(\bar{Q}x.(\bar{q}^n:\bar{Q}x)))$$

$$= \text{length}\,(\bar{Q}/\bar{q}^n:\bar{Q}x)$$

$$= \lambda(\bar{q}^n:\bar{Q}x) .$$

In fact Samuel proves ([16] chapter 2, theorem 1, 2) that there exists a non-negative integer n_o such that for all $n \geq n_o$

$$P_{\bar{q}}(n) = a_o\binom{n}{d} + a_1\binom{n}{d-1} + \ldots + a_{d-1}\binom{n}{1} + a_d$$

where the a_i are integers, where $a_o > 0$, and where $d = \dim \bar{Q}$. The $\binom{n}{k}$ denotes, of course, the familiar binomial coefficient. Since by (2.4.1.2)

$$P_{\bar{q}}(n+1) - P_{\bar{q}}(n) = \chi_q(n,I)$$

we have for all $n \geq n_o$

$$\chi_q(n,I) = a_o\binom{n}{d-1} + a_1\binom{n}{d-2} + \ldots + a_{d-1}$$

where $a_o > 0$ and where $d = \dim I$

Thus, for sufficiently large n, $\chi_q(n,I)$ is a polynomial in n of

degree dim I-1. Call a_o the order of I with respect to q and denote it by $\operatorname{ord}_q I$.

The proposition below gives an alternative proof making use of superficial elements.

(2.4.3) Proposition: Let Q be a (Krull) d-dimensional local ring, m be the maximal ideal of Q and q be an m-primary ideal of Q. Then the length (Q/q^n), the length of Q-module Q/q^n, is equal to a polynomial in n of degree d for n sufficiently large.

Proof. The proof is by induction on d. When d = 0, the zero ideal (0) is m-primary, so q is nilpotent and $\operatorname{length}_Q(Q/q^n) = \operatorname{length}_Q(Q)$ is constant, for all n large enough. Hence $\operatorname{length}(Q/q^n)$ is a polynomial $P_0(n,q)$ of degree 0 for all n large.

Now suppose that $d \geq 1$, and the proposition holds for all local rings of dimension d-1.

If x is a superficial element, with respect to q, the condition b:(x) = b of (1.2.4. (ii)) shows that x is in none of the minimal prime ideals of Q. Therefore Q/(x) is a (d-1)-dimensional local ring.

In accordance with the remark following the proof of (1.2.7) choose an integer s such that, there exists superficial elements x_s of degree s and x_{s+1} of degree s+1 with respect to Q.

The isomorphisms

$$(q^{n+s} + Qx_s)/q^{n+s} \simeq Qx_s/(Qx_s \cap q^{n+s}) = Qx_s/q^n x_s \simeq Q/(q^n + 0:x_s)$$

for n sufficiently large, give

$$\operatorname{Length}(Q/q^{n+s}) = \operatorname{length}(Q/(q^{n+s} + Qx_s)) + \operatorname{length}(Q/(q^n + 0:x_s)).$$

Also

$$\operatorname{Length}(Q/(q^n + 0:x_s)) = \operatorname{length}(Q/q^n) - \operatorname{length}(q^n + 0:x_s)/q^n).$$

and $(q^n + 0:x_s)/q^n \simeq 0:x_s/(q^n \cap 0:x_s)$.

However by the Lemma of Artin-Rees ([5] page 9)

$$q^n \cap (0:x_s) \subseteq q^n \cap (b:x_s) = q^n \cap b = q^{n-r}(q^r \cap b) \subseteq q^{n-r}b = 0$$

for n large. So

$$\text{length}(Q/q^{n+s}) - \text{length}(Q/q^n) = \text{length}(Q/q^{n+s}+Qx_s) - \text{length}(0:x_s)$$

for n large enough, and we denote this equation by (A)

Similarly for x_{s+1} we have,

$$\text{length}(Q/q^{n+s}) - \text{length}(Q/q^{n-1}) = \text{length}(Q/q^{n+s}+Qx_{s+1}) - \text{length}(0:x_{s+1})$$

for n large enough, and we denote this equation by (B)

consequently we have, if we subtract (A) from (B);

$$\text{length}(Q/q^n) - \text{length}(Q/q^{n-1}) = \text{length}(Q/q^{n+s}+Qx_{s+1}) - \text{length}(Q/q^{n+s}+Qx_s) + \\ + \text{length}(0:x_s) - \text{length}(0:x_{s+1})$$

Put $Q' = Q/Qx_s$, $Q'' = Q/Qx_{s+1}$, $q' = q/Qx_s$ and $q'' = q/Qx_{s+1}$, then

$$\text{length}_Q(Q/q^{n+s} + Qx_{s+1}) = \text{length}_{Q''}(Q''/q''^{n+s})$$

and $$\text{length}_Q(Q/q^{n+s} + Qx_s) = \text{length}_{Q'}(Q'/q'^{n+s}) .$$

By the inductive hypothesis, for n large enough, these are polynomials of degree d-1 in n. Hence

$$\text{length}(Q/q^n) - \text{length}(Q/q^{n-1}) = \text{length}(q^{n-1}/q^n),$$

for n large, is a polynomial $P_{d-1}(n)$ in n of degree (d-1) or less for n large.

When d = 1, the degree must be (d-1); otherwise $q^{n-1} = q^n$ for n

large. This would imply q is nilpotent contrary to $\dim Q = 1$. When $d > 1$ the degree again must be $(d-1)$; otherwise returning to A we would have

$$P_{d-1}(n+s,q') = \text{length}(Q'/q'^{n+s})$$

of degree less then $d-1$, contrary to the inductive hypothesis. Now write

$$\text{length}(Q/q^n) = \sum_{r=1}^{n} \text{length}(q^{r-1}/q^r) = \sum_{r=1}^{n} P_{d-1}(r) + \sum_{r=1}^{n} (\text{length}(q^{r-1}/q^r) - P_{d-1}(r)).$$

The first term on the right-hand side is a polynomial of degree d in n, and for n large enough the second term is constant. Hence for n large enough

$$\text{length}(Q/q^n) = P_q(n)$$

is a polynomial of degree d in n.

Example. Let K be a field and Q be the power-series rings $K\{[u^4, u^3v, uv^3, v^4]\}$ with maximal ideal $m=(u^4, u^3v, uv^3, v^4)$. For $n \neq 2$ a composition series from m^n to m^{n-1} can be obtained by adding to m^n

the principal ideals with generators,

$$u^{4n-4}, u^{4n-5}v, u^{4n-6}v^2, \ldots\ldots, v^{4n-4};$$

its length is thus $4n-3$. Similarly a composition series from m to m^2 is obtained by adjoining u^4, u^3v, uv^3, v^4 to m^2, its length is $4 = (4.2-3)-1$. Therefore, for $n \geq 2$.

$$P_m(n) = \text{length}(Q/m^n) = \sum_{r=1}^{n} \text{length}(m^{r-1}/m^r) = \sum_{r=1}^{n} (4r-3) - 1$$

$$= 4.\frac{n(n+1)}{2} - 3n - 1 = 4\binom{n}{2} + \binom{n}{1} - \binom{n}{0} \quad .$$

As a second example take $q = (u^4, v^4)$. A composition series from q^{n-1} to q^n can be constructed by adjoining

$$u^{4n+2}v^2,\ u^{4n-2}v^6,\ u^{4n-6}v^{10},\ \ldots\ ,\ u^2v^{4n+2},\ u^{4n-1}v,\ u^{4n-3}v^3,\ \ldots$$

$$\ldots\ldots,\ uv^{4n-1},\ u^{4n-4},\ u^{4n-8}v^4,\ \ldots\ ,\ v^{4n-4} \text{ to } q^n \text{ in turn giving}$$

for all $n \geq 1$

$$\text{length}\ (q^{n-1}/q^n) = (n+1) + 2n + n = 4n + 1 \ .$$

So for all $n \geq 0$

$$P_q(n) = \sum_{r=1}^{n} (4r + 1) = 4\binom{n}{2} + 5\binom{n}{1} \quad .$$

(2.5) Normalized Hilbert Coefficients.

Let Q be d-dimensional ($d \geq 0$) local ring, m be its maximal ideal and q be an m-primary ideal of Q. Then $\text{length}_Q(Q/q^n)$, the length of Q-module Q/q^n, is equal to the characteristic polynomial $P_q(n)$ in n for a sufficiently large value of n.

$$P_q(n) = e_o\binom{n+d-1}{d} - e_1\binom{n+d-2}{d-1} + \ldots\ldots \quad + (-1^d)e_d$$

where $e_i = e_i(q)$, $i = 0,1,\ldots,d$ are uniquely determined by q called normalized Hilbert Coefficients of q . The coefficients e_i are easily shown to be integer by taking successive differences of

$P_q(n)$, $\Delta P_q(n) = P_q(n+1) - P_q(n)$, ..., which produces sequences of integers.

(2.6) "One-dimensional case".

Let Q be one-dimensional local ring and let m be maximal ideal of Q and residue field $K = Q/m$, it will be assumed that not every element of m is a zero-divisor, but no other restricting hypothesis will be made. In particular Q and K may have unequal characteristics and K may be finite. If M is Q-module, then we shall use $\text{length}_Q(M)$ to denote its length, in many circumstances this number will be infinite.

The theory of generalized Hilbert function shows that for sufficiently large value of n.

$$\text{Length}_Q(Q/m^n) = en - \rho,$$

where, as we mentioned e and ρ are non-negative integers which are independent of n. e is called the multiplicity of Q and ρ is called the reduction number of Q ([17] chapter VIII, §10, and [12]). It follows that length $(m^n/m^{n+1}) = e$ is constant for large n, and from this we see that e is a positive integer.

It will now be convenient to introduce some relationships between the multiplicity e and reduction number ρ of the local ring Q.

(2.6.1) Definition: The first neighbourhood ring R of Q is the set of all elements (in the full ring of quotients $\hat{Q}$ of Q) of the form y/x, where $y, x \in m^s$ and x is superficial element of degree s. Since the set of superficial elements of Q is obviously multiplicatively

closed, it is clear that R is indeed a subring of $\hat{Q}$ containing Q.

The idea receives more attention in the next chapter.

(2.6.2) Now, let us note that the ideal Rm of R is principal and is generated by a non-zero-divisor (prop 1 |4|). Northcott has proved that length$(R/Q) = \rho$, thus showing that $\rho \geq 0$ ([12] theorem 1).

In fact by proposition 3 of [4],

$$\text{length}(R/Rm) = e \quad \text{and} \quad \text{length}(R/Q) = \rho$$

Furthermore $\text{length}\ (R/Rm^n) = en$ for all $n > 0$.

Suppose $x \in m^s$ and let I be a finitely generated Q-submodule of $\hat{Q}$ such that I contains a non-zero-divisor then length $(I/xI) \geq se$ and length$(I/xI) = se$ if and only if x is superficial element for m of degree s (proposition 4, [4]).

(2.6.3) Proposition. Every m-primary ideal of Q can be generated by e elements.

Proof. We need to prove length$(I/mI) \leq e$.

We give the proof only in the case when m has a superficial element x of degree 1. The general case then follows by a device due to Rees(see Mathis [4] , p 277); namely adjoining an indeterminate to Q and localizing. This has the effect of making sure the new local ring has infinite residue field (so the maximal ideal has superficial elements of degree 1), whilst leaving lengths of corresponding modules unaffected.

As $x \in m$ we have

$$\text{length}(I/mI) \leq \text{length}\ (I/xI) = e$$

and the proposition is proved in the special case.

(2.6.4) Proposition. There exists an integer $\nu \geq 0$ such that $\text{length}(m^n/m^{n+1}) = e$ for all $n \geq \nu$ and $\text{length}(m^n/m^{n+1}) < e$ if $n < \nu$.

Proof. Again we give the proof for the case in which m has a superficial element x of degree 1. The general case follows as in the proof of (2.6.3).

Let ν be the smallest integer such that $\text{length}(m^n/m^{n+1}) = e$ for all $n \geq \nu$. Let $r \geq 0$ be any integer, then we have

$$\text{length}(m^r/m^{r+1}) = \text{length}(m^r/m^r x) - \text{length}(m^{r+1}/m^r x)$$

$$= e - \text{length}(m^{r+1}/m^r x).$$

Therefore $\text{length}(m^r/m^{r+1}) \leq e$ and $\text{length}(m^r/m^{r+1}) = e$ if and only if $m^{r+1} = m^r x$. But if $m^{r+1} = m^r x$, then $m^{n+1} = m^n x$ for all $n \geq r$ and hence by proposition 4 of [4], $\text{length}(m^n/m^{n+1}) = e$ for all $n \geq r$. In this case $r \geq \nu$ and this proves the proposition.

(2.6.5) Proposition. $\rho \geq e-1$

Proof. We can write

$$\text{length}(R/m) = \text{length}(R/Q) + \text{length}(Q/m) = \rho + 1$$

since $m \subseteq Rm$ and $\text{length}(R/Rm) = e$ we have

$$\rho + 1 \geq e .$$

In addition. Mathis [4] gives five necessary and sufficient conditions for ρ to equal $e-1$.

(2.6.6). Proposition. The following statements are equivalent.

(1). Every ideal of Q is principal(i.e. Q is a discrete valuation ring)

(2). $P_m(n) = n$ where $P_m(n)$ is Hilbert polynomial of m

(3). $\rho = 0$

(4). $e = 1$

Proof. The implications (1) $\longrightarrow$ (2) $\longrightarrow$ (3) are trivial and (3) $\longrightarrow$ (4) follows from (2.6.5). Hence assume (4); that is $e = 1$. Then length$(Q/m) = 1 = e$ and $\nu = 0$ by (2.6.4). In particular length $(m/m^2) = 1$, m is a principal ideal. Therefore Q is a discrete valuation ring.

(2.6.7). Theorem. The following statements are equivalent:

(i) Every ideal of Q can be generated by two elements, but Q is not a discrete valuation ring.

(ii) $P_m(n) = 2n - 1$, where $P_m(n)$ is the Hilbert polynomial of m

(iii) $\rho = 1$

(iv) $e = 2$

If any of these conditions hold, then Q has a superficial element of degree one.

Proof of this theorem as page 281 [4] .

(2.6.8) Now let $x_0, x_1, \ldots, x_d$ $(d \geq 0)$ be indeterminates over the field $K = Q/m$, and let $R_n(d)$ be the K-space of forms of degree n in the polynomial ring $K[x_0, x_1, \ldots, x_d] = R(d)$.

Let $I = \sum_{n \geq 0} I_n$ be a graded ideal of the graded ring $R(d) = \sum_{n \geq 0} R_n(d)$.

(2.6.9) Proposition. If $\text{length}(m^n/m^{n+1}) \leq n$, then $\text{length}(m^r/m^{r+1}) \geq \text{length}(m^s/m^{s+1})$, where $n \leq r \leq s$.

Proof. It needs to be proved that $\text{length}(m^n/m^{n+1}) \leq n$ implies $\text{length}(m^n/m^{n+1}) \geq \text{length}(m^{n+1}/m^{n+2})$. We can prove this by induction, so, let m have a generating set of $d + 1$ elements without loss of generality it may be assumed $d \geq 1$ so the ring $S = \sum_{n \geq 0} m^n/m^{n+1}$ is a homomorphic image of the polynomial ring $R(d)$, so the kernel of the homomorphism I is a graded ideal of $R(d)$. Suppose $\text{length}(m^n/m^{n+1}) \leq n$, then in the notation of (theorem 1 of [3])

$$\dim_K(I_n) = \binom{n+d}{d} - \text{length}(m^n/m^{n+1}) = \sum_{i=0}^{d-2} \binom{n+d-i-1}{d-i} + \binom{a}{1}$$

where $a = n - \text{length}(m^n/m^{n+1}) + 1$ so by theorem 1 of [3]

$$\binom{n+d+1}{d} - \text{length}(m^{n+1}/m^{n+2}) = \dim_K(I_{n+1}) \geq \sum_{i=0}^{d-2} \binom{n+d-i}{d-i} + \binom{a+1}{1}$$

$$= \binom{n+d+1}{d} - \text{length}(m^n/m^{n+1})$$

i.e. $\text{length}(m^n/m^{n+1}) \geq \text{length}(m^{n+1}/m^{n+2})$.

(2.6.10) Theorem. $\nu \lesssim e - 1 \lesssim \rho \lesssim \frac{1}{2}e(e-1)$

Proof. The existence of ν ensures that the sequence $\text{length}(m^s/m^{s+1})$ where $s = 0,1,2,\ldots$ is decreasing only from the point $s = \nu$. However if $e \lesssim \nu$ then

$$\text{length}(m^{\nu-1}/m^{\nu}) \lesssim e-1 \lesssim \nu - 1$$

and by (2.6.9) the sequence decreases from the point $s = \nu - 1$. This contradiction establishes that

$$\nu \lesssim e - 1$$

Again as $\text{length}(m^n/m^{n+1}) \lesssim n$ implies that the sequence is decreasing from the point $s = n$ it must also imply that $n \gtrsim \nu$. Consequently we have

$$\text{length}(Q/m) = 1$$

$$e > \text{length}(m^n/m^{n+1}) \gtrsim n + 1 \qquad \text{for } n = 1,2, \ldots \nu - 1$$

$$e = \text{length}(m^n/m^{n+1}) > n + 1 \qquad \text{for } n = \nu,\nu+1,\ldots e-2$$

$$e = \text{length}(m^n/m^{n+1}) \qquad \text{for } n > e-1 .$$

Hence for $n \gtrsim e$ we can write

$$(n-1)e + 1 \gtrsim \sum_{s=0}^{n-1} \text{length}(m^s/m^{s+1}) \gtrsim (n-e+1)e + \tfrac{1}{2}e(e-1)$$

therefore by proposition 9 of [4] we have

$$\sum_{s=0}^{n-1} \text{length}(m^s/m^{s+1}) = \text{length}(Q/m^n) = en - \rho$$

consequently $en - (e-1) \gtrsim en-\rho \gtrsim en - \frac{1}{2} e(e-1)$

or $e-1 \lesssim \rho \lesssim \frac{1}{2} e(e-1)$

which completes the proof.

(2.6.10.1) Corollary 1. $\rho = e-1$ if and only if $\nu \lesssim 1$.

Proof. $\rho = e-1$ if and only if, none of the inequalities on the left in the proof of the (2.6.10) is strict. So

$$e > \text{length } (m^n/m^{n+1}) \qquad (n=1,2,\ldots \nu-1),$$

never holds ie. if and only if $\nu - 1 < 1$ or $\nu \lesssim 1$.

(2.6.10.2) Corollary 2. The maximal ideal of Q can be generated by two elements if and only if $\rho = \frac{1}{2}e(e-1)$. When this occurs $\nu = e-1$.

Proof. Suppose, the maximal ideal m of Q generated by two elements then by corollary 20 of [4] $\rho = \frac{1}{2}e(e-1)$. Suppose now that $\rho = \frac{1}{2}e(e-1)$ then none of the right hand inequalities (2.6.10)

$$\text{length}(m^n/m^{n+1}) \gtrsim n+1 \qquad n = 1, \ldots \nu - 1$$

$$\text{length}(m^n/m^{n+1}) > n+1 \qquad n = \nu, \ldots e - 2$$

can be strict. So $e-2 < \nu$, which together with $\nu \lesssim e-1$ gives $\nu = e-1$. Also $\text{length}(m^n/m^{n+1}) = n+1$ for $n = 1,\ldots \nu-1$. Therefore either $\nu - 1 < 1$ and $\text{length}(m/m^2) = e = \nu + 1 \lesssim 2$ or $\nu - 1 \gtrsim 1$ and $\text{length}(m/m^2) = 2$, thus, in either case, $\text{length}(m/m^2) \lesssim 2$ and the maximal ideal m can be generated by two elements.

(2.6.10.3) Corollary 3. If $\rho = e$, then $\text{length}(m/m^2) = e-1$ and $\nu = 2$.

Proof. The difference $\rho-(e-1)$ is the sum of the positive difference $e-\text{length}(m^n/m^{n+1})$ with $n = 1,\ldots \nu - 1$. Therefore, if $\rho = e$, there is one positive difference and it is equal to 1. So $\nu = 2$ and $e-\text{length}(m/m^2) = 1$.

(2.6.10.4) Corollary 4. If $\rho = \frac{1}{2}(e-2)(e+1)$, then $\text{length}(m/m^2) = 3$ and $\text{length}(m^n/m^{n+1}) = n+1$ for $n = 2, \ldots e-2$; furthermore $\nu = e - 1$ when $e \geq 4$, and $\nu = 1$ when $e = 3$.

Proof. The difference $\frac{1}{2}e(e-1) - \rho$ is the sum of positive differences $\text{length}(m^n/m^{n+1}) - (n+1)$ for $n = 1, \ldots, e-2$ now suppose that, $\rho = \frac{1}{2}(e-2)(e+1) = \frac{1}{2}e(e-1)-1$ therefore there is one positive difference and it is equal to 1. However $\text{length}(m/m^2) \geq 3$ for, otherwise $\rho = \frac{1}{2}e(e-1)$ by corollary 2. Consequently $\text{length}(m/m^2) = 3$ and $\text{length}(m^n/m^{n+1}) = n+1$ for $n = 2, \ldots e-2$.

Further, for $e \geq 4$ $\text{length}(m^{e-2}/m^{e-1}) = e-1$ but $\text{length}(m^{e-1}/m^e) = e$ therefore $\nu = e-1$, and, for $e = 3$ $\text{length}(Q/m)=1$ but $\text{length}(m/m^2) = 3 = e$ consequently $\nu = 1$.

(2.6.10.5) Corollary 5. $\rho = 0$ if and only if $e = 1$.

Proof. If $e = 1$ then $0 \leq \rho \leq 0$ or $\rho = 0$. Now if $\rho = 0$ then $e - 1 \leq 0$ and $e(e-1) \geq 0$. But $e > 0$, so $e = 1$.

(2.6.10.6) Corollary 6. $\rho = 1$ if and only if $e = 2$.

Proof. If $e = 2$, then $1 \leq \rho \leq 1$ or $\rho = 1$. Now if $\rho = 1$ $e-1 \leq 1$ and $(e+1)(e-2) = e(e-1)-2 \geq 0$. But $e + 1 > 0$, so $e = 2$.

Chapter III

"A lattice of extension rings for a local ring"

(3.1) Introduction. Throughout this chapter, Q is local ring and m is its maximal ideal. The work of this chapter was motivated in the first place by Northcott's theory of dilations for one-dimensional local rings (see, for example, [10] and [13]). This produces a tree of local rings as in [13] which corresponds in the abstract case to the branching sequence of infinitely-near multiple points on an algebroid curve. From the algebraic point of view it seems more natural to characterize such one-dimensional local rings Q by means of the set of rings which arise by blowing up all ideals Q which are primary for the maximal ideal m of Q. This set of rings forms a lattice $\mathcal{L}(Q)$, ordered by inclusion, each ring S of which is a finite Q-module Moreover the length of the Q-module S/Q is just the reduction number of the corresponding ideal Q (c.f. Theorem 1 of Northcott [12]). Thus the lattice $\mathcal{L}(Q)$ provides a finer classification of the rings Q than does the set of reduction numbers (c.f. Kirby [2]).

In section (3.2) we include some of Northcotts work [10] on the first neighbourhood ring.

In section (3.3) we introduce the lattice $\mathcal{L}(Q)$ of extension rings which are also fractionary ideals of Q, and show how $\mathcal{L}(Q)$ provides an equivalence relation on a certain set I of ideals of Q. The ideals in I are those which when blown up produce the rings of $\mathcal{L}(Q)$.

(3.2) The first neighbourhood ring.

Throughout this section, Q will denote a one-dimensional local ring with maximal ideal m, and residue field $K = Q/m$. It will be assumed that not every element of m is a zero-divisor or (equivalently) that all the prime ideals belonging to the zero-ideal are of dimension unity. One consequence of this assumption is that an ideal $I \neq (1)$ is m-primary if and only if it contains at least one element which is not a zero-divisor.

We recall some of the notations of chapter (I) section two, when $q = m$.

Let us suppose that $(u_0, u_1, \ldots, u_d)$ be a fixed but otherwise arbitrary set of generators for the maximal ideal m, so that in particular there may be elements which are superfluous among the u_i. Let N denote the form ideal of the zero-ideal of Q constructed with respect to this base; then $\bar{N}$ is the homogeneous ideal in $K[x_0, x_1, \ldots, x_d]$ generated by the leading forms of the zero element and its affine dimension is unity.

Further, when ϕ is a form then $\bar{\phi}$ will be used to denote the same form read modulo m. Thus to give one example of the use of these conventions, a form ϕ of degree s, will satisfy $\bar{\phi} \in \bar{N}$ if and only if

$$\phi(u) \equiv 0 \pmod{m^{s+1}}$$

It will be convenient to denote by $\bar{N}_0$ the isolated component of $\bar{N}$ determined by its one-dimensional prime ideals.

(3.2.1) Proposition. Let ω belong to m^s. Then ω is superficial element of degree s if and only if $R_1\omega = R_1 m^s$, where R_1 is the first neighbourhood ring of Q.

Proof. First suppose that ω is a superficial element of degree s, then $m^s \subseteq R_1\omega$ by (2.6.1) and $\omega \in R_1 m^s$. Therefore $R_1\omega = R_1 m^s$.

Now assume that $R_1\omega = R_1 m^s$, for this let us suppose that $p(x)$ is a power-product of the $x_0, x_1, \ldots, x_d$, of degree s, and also write ω as $\psi(u)$, where ψ is a form of degree s. Since $p(u) \in R_1 m^s$,

$$p(u) = \frac{\phi_0(u)}{\psi_0(u)} \psi(u)$$

where ϕ_0, ψ_0 are forms of the same degree and by (Theorem 1 of [10]) $\bar{N}_0 : (\bar{\psi}_0) = \bar{N}_0$. Let ϕ be an arbitrary form such that $\bar{\phi} \in \bar{N}_0 : (\bar{\psi})$, then $\bar{\phi}\,\bar{\psi} \in \bar{N}_0$ and,

$$p(x)\bar{\psi}_0 - \bar{\phi}_0\psi \in \bar{N} \subseteq \bar{N}_0$$

consequently $p(x)\bar{\psi}_0\bar{\phi} \in \bar{N}_0$ and therefore $p(x)\bar{\phi} \in \bar{N}_0$, it follows that,

$$(x_0, x_1, \ldots, x_d)^s \bar{\phi} \subseteq \bar{N}_0 ,$$

and for this reason $\bar{\phi} \in \bar{N}_0$. This shows that

$$\bar{N}_0 : (\bar{\psi}) = \bar{N}_0 ,$$

and, thus ω is a superficial element of degree s.

(3.2.2) Proposition. The first neighbourhood ring R_1 is a finite Q-module.

Proof. Let us suppose that z be an element of the first neighbourhood ring R_1 of Q, it is clear that the form of z is $\frac{v}{\omega}$ where, for a suitable integer s, $v \in m^s$ and ω is superficial

element of degree s by ((ii) of Theorem 1 of [10]) we can choose an integer r such that $\omega m^r = m^{r+s}$. Hence if

$$m^r = (\lambda_1, \lambda_2, \ldots, \lambda_t) \quad ,$$

then $v\lambda_i \in m^{r+s} = \omega m^r$, for this it follows immediately that

$v\lambda_i = \sum_{j=1}^{t} \omega q_{ij}\lambda_j$ where $q_{ij} \in Q$. It is obvious that if δ_{ij} is the usual Kronecker symbol and Δ is the determinant $|z\delta_{ij} - q_{ij}|$, then $\Delta\lambda_i = 0$ for $1 \leq i \leq t$. In this circumstance $\Delta m^r = 0$ and since m^r is not composed exclusively of zero-divisors, so $\Delta = 0$ and from this point z is integral with respect to Q.

Let x be a fixed superficial element of degree σ, so $xm^\rho = m^{\rho+\sigma}$ say. Choose $\tau \geq {}^{\rho}/_{\sigma}$ so

$$xm^{\sigma\tau} = m^{\sigma(\tau+1)}$$

We prove $R_1 = \left({}^{1}/_{x^\tau}\right) m^{\sigma\tau}$ from which the proposition follows as $m^{\sigma\tau}$ is a finitely generated ideal of Q. $R_1 \supseteq \left({}^{1}/_{x^\tau}\right) m^{\sigma\tau}$ is clear.

Let $z = {}^{v}/_{\omega} \in R_1$, where $v, \omega \in m^s$ and ω is superficial of degree s, so $\omega m^r = m^{r+s}$ say. Let $t \geq \max\left(\tau, {}^{r}/_{\sigma}\right)$ then

$$v x^t \in m^{s+\sigma t} = \omega m^{\sigma t} = \omega m^{\sigma\tau} x^{(t-\tau)}$$

or

$$v x^\tau \in \omega m^{\sigma\tau}$$

as x is not a zero-divisor. Hence

$$z = {}^{v}/_{\omega} \in \left({}^{1}/_{x^\tau}\right) m^{\sigma\tau} \quad \text{and}$$

$$R_1 \subseteq \left({}^{1}/_{x^\tau}\right) m^{\sigma\tau}$$

as required.

(3.2.3) Proposition. The first neighbourhood ring R_1 coincides with Q if and only if Q is regular.

Proof. By (2.6.10.5) we have

$$\text{length}(R_1/Q) = \rho(m)$$

So $R_1 = Q$ if and only if $\rho(m) = 0$.
By (2.6.6) we have, $\rho(m) = 0$ if and only if Q is a discrete valuation ring. i.e. a one-dimensional regular local ring.

Now suppose that Q is regular local ring, in particular, it is clear that, Q is an integrally closed integral domain, for this reason by (3.2.2) Q and R_1 must coincide.

Again assume that $Q = R_1$ by (Theorem 2 of [10]) we can find a superficial element ω of positive degree s (say) and therefore we can write

$$Qm^s = R_1 m^s = R_1\omega = Q\omega$$

so m^s is a principal ideal and consequently Q is a regular local ring.

(3.2.4) Remarks. Let us suppose that Q is a one-dimensional local ring and m is the maximal ideal of Q, and then suppose R_1 is the first neighbourhood ring of Q the notion of which is due to Northcott, in fact he produces the tree of the neighbourhood rings by localizing R_1 at its maximal ideals and resolving again. We prefer to generalize Q and so produce a lattice of finite extension rings of Q.

(3.3) The lattice $\mathcal{L}(Q)$.

Let Q be a local ring, and let $T(Q)$ be its total quotient ring. Let $\mathcal{L}(Q)$ denote the set of rings which are finite

Q-modules containing Q so its obvious all these rings are also fractionary ideals. Conversely if $Q \subseteq S \subseteq T(Q)$, and the ring S is a fractionary ideal i.e. $S \subseteq Q.1/d$, then $A = dS$ is an ideal of Q and $S = (1/d)A$ is finitely generated as Q is Noetherian. For this reasoning for each element S belonging to $\mathcal{L}(Q)$, we can write

$$Q \subseteq S \subseteq T(Q)$$

and there exists an element $d \in Q$, such that $dS \subseteq Q$ and d is not a zero-divisor. Clearly $\mathcal{L}(Q)$ is partially ordered by inclusion. Now suppose that S_i be an element of $\mathcal{L}(Q)$ and that $d_i S_i \subseteq Q$, where d_i is not a zero-divisor for $i = 1,2$ then $d_1(S_1 \cap S_2) \subseteq Q$, and $d_1 d_2 S_1 S_2 \subseteq Q$. Therefore $\mathcal{L}(Q)$ is a lattice with intersection and product, the lattice operations $\wedge$ and $\vee$. Every non-empty set of elements of $\mathcal{L}(Q)$ has an infinum, the intersection, but not necessarily a supremum. Thus $\mathcal{L}(Q)$ may not be complete. Since each ring $S \in \mathcal{L}(Q)$ is a finitely generated Q-module. S is an integral extension of Q ([17] p254).

Conversely, if $x \in T(Q)$ is integral over Q, then $Q[x]$ belongs to the lattice, thus, in particular, the integral closure $\hat{Q}$ of Q in its total quotient ring T(Q) is the union of all the rings of the lattice $\mathcal{L}(Q)$.

The rings of $\mathcal{L}(Q)$ can be constructed by blowing up certain ideals of Q.

(3.3.1) Let I denote the set of ideals A of Q such that,

(i) $0:A = 0$

(ii) There exists integers $m,n(\geq 1)$ and $\alpha \in A^n$ such that $A^{m+n} = \alpha A^m$.

For each $A \in I$ we denote the set of α as in (ii) by $\sum_n (A)$.

(3.3.1.1) Remark. Condition (i) ensures that no element of $\sum_n (A)$ is a zero-divisor.

(3.3.2) Proposition.

(a) I contains all principal ideals, whose generators are not zero-divisors.

(b) I is multiplicatively closed.

Proof. (a). is immediate.

(b). follows from the observation that

$$\alpha \in \sum_n (A) \quad , \quad \beta \in \sum_p (B)$$

then

$$\alpha^p \beta^n \in \sum_{np} (AB)$$

(3.3.3) Definition.

For each ideal $A \in I$ we denote by $S(A)$ the subset of the total quotient ring $T(Q)$ such that, $S(A)$ is the set of all elements ~~such that~~ β/α where, there exists $n \geq 1$ with $\beta \in A^n$ and $\alpha \in \sum_n (A)$.

(3.3.4) Remark. If Q has dimension one, and its maximal ideal m does not consist entirely of zero-diviors, then $\sum_n (m)$ is the set of superficial elements of degree n for m. Consequently $S(m)$ is none other than the first neighbourhood ring R_1 of Q. Thus the rings $S(A)$ are generalizations of the first neighbourhood ring in the case $\dim Q = 1$. We show next that the rings $S(A)$ are just the rings of $\mathcal{L}(Q)$.

(3.3.5) Proposition. $S(A) \in \mathcal{L}(Q)$ for all $A \in I$.

Proof. Let $\alpha \in \sum_n (A)$, $\alpha' \in \sum_{n'} (A)$, therefore

$$A^{m+n} = \alpha A^m \quad , \quad A^{m+n'} = \alpha' A^m$$

for some m,

Hence $$A^{m+n+n'} = \alpha\alpha' A^m \text{ and } \alpha\alpha' \in \sum_{n+n'} (A)$$

Therefore the denominators occuring in the definition of $S(A)$ form a multiplicatively closed set and it follows that $S(A)$ is a ring containing Q.

Choose an integer $r \geq 1$ such that $rn \geq m$, put $s = rn$ and $\alpha_1 = \alpha^r$. Then $A^{2s} = \alpha_1 A^s$.

Consider, now $\beta'/\alpha' \in S(A)$ with $\beta' \in A^{n'}$, $\alpha' \in \sum_{n'} (A)$, so $A^{m'+n'} = \alpha' A^{m'}$ say. Then

$$\alpha_1(\beta'/\alpha') = \alpha_1^{m'+1} \beta'/\alpha_1^{m'}\alpha'$$

and $$\alpha_1^{m'+1} \beta' \in A^{s(m'+1)+n'} = \alpha' A^{s(m'+1)} = \alpha'\alpha_1^{m'} A^s$$

consequently $$\alpha_1(\beta'/\alpha') A^s \subseteq Q$$

and $$\alpha_1 S(A) \subseteq Q .$$

So $S(A)$ is a fractionary ideal, and is in $\mathcal{L}(Q)$.

(3.3.5.1) Corollary. If $A \in I$, $n \geq 1$ and $\alpha \in \sum_n (A)$, then there exists $r \geq 1$ such that $A^{2nr} = \alpha^r A^{nr}$, and this implies

$$S(A) = (1/\alpha^r) A^{nr}$$

(3.3.6) Proposition. If $S \in \mathcal{L}(Q)$ and $d \in Q$, satisfies $dS \subseteq Q$ and is not a zero-divisor, then $dS \in I$ and $S = S(dS)$.

Proof. Suppose $d \in Q$ is not a zero-divisor. We have $0:d = 0$ which implies $0:dS = 0$ as $1 \in S$. Also $(dS)^2 = d(dS^2) = d(dS)$ which implies $dS \in I$, and $d \in \sum_1(dS)$. It also implies $S(dS) = (1/d)dS = S$ by corollary (3.3.5.1)

(3.3.7) Definition. For each ideal $A \in I$ we denote by $c\ell(A)$ the set of $B \in I$ such that $S(A) = S(B)$, and by $\mathcal{L}'(Q)$ the set of $c\ell(A)$.

The relation $S(A) = S(B)$ is clearly an equivalence relation on I, and proposition (3.3.5) and (3.3.6) shows that there is a bijection between $\mathcal{L}(Q)$ and $\mathcal{L}'(Q)$ this bijection is used to turn $\mathcal{L}'(Q)$ into a lattice and we use the symbol $\lesssim$ to denote its order relation. For each principal ideal A as in propostion (3.3.2), (a), $S(A) = S(Q) = Q$, thus $c\ell(Q)$ is the least element of $\mathcal{L}'(Q)$. Indeed it is not difficult to show that $c\ell(Q)$ consists of ideals of I some power of which is principal.

Next we interpret the structure of $\mathcal{L}'(Q)$ in ideal theoretic terms.

(3.3.8) Proposition. Let $A,B \in I$, $c\ell(A) \lesssim c\ell(B)$ if, and only if there exists $\alpha \in \sum_m(A)$ such that $A^mB^n = \alpha B^n$ for some n.

Proof. Suppose $\alpha \in \sum_m(A)$ and $A^mB^n = \alpha B^n$, choose an integer r in accordance with (3.3.5.1) so

$$S(A) = (1/\alpha^r)\, A^{mr}$$

Let $\beta \in \sum_s(B)$ with $s \geq n$ then

$$A^{mr}\ \beta \subseteq A^{mr}B^{s} = \alpha^{r}B^{s}$$

and $$S(A) = (1/\alpha^{r})\ A^{mr} \subseteq (1/\beta)B^{s} \subseteq S(B)$$

or $$c\ell(A) \lesssim c\ell(B).$$

Conversely, suppose $c\ell(A) \lesssim c\ell(B)$. By (3.3.5.1) we can choose $\alpha \in \sum_{m}(A)$ and $\beta \in \sum_{n}(B)$ such that

$$A^{2m} = \alpha A^{m}, \quad B^{2n} = \beta B^{n}.$$

Then $$(1/\alpha)A^{m} = S(A) \subseteq S(B) = (1/\beta)B^{n}$$

and $$A^{m}\ B^{2n} \subseteq A^{m}\ \beta B^{n} \subseteq \alpha B^{2n} \subseteq A^{m}\ B^{2n}$$ so $\alpha B^{2n} = A^{m}B^{2n}$.

An immediate consequence of the above proposition is that $c\ell(A) \lesssim c\ell(AB)$ when $A, AB \in I$. When both $A,\ B \in I$ we have a stronger result.

(3.3.9) Proposition. If $A,B \in I$, then $c\ell(A) \vee c\ell(B) = c\ell(AB)$.

Proof. In terms of the resolved rings we must prove

$$S(AB) = S(A)\ S(B).$$

by (3.3.5.1) we can choose $\alpha \in \sum_{m}(A)$, $\beta \in \sum_{n}(B)$

such that $$A^{2m} = \alpha A^{m}, \quad B^{2n} = \beta B^{n}$$

then $$(AB)^{2mn} = A^{2mn}\ B^{2nm} = \alpha^{n}\ \beta^{m}(AB)^{mn}$$

and $$\alpha^{n}\ \beta^{m} \in \sum_{mn}(AB).$$

Again by (3.3.5.1)

$$S(AB) = (1/_{\alpha^{n}\beta^{m}})(AB)^{mn} = \left((1/\alpha)A^{m}\right)^{n}\left((1/\beta)B^{n}\right)^{m} = S(A)S(B).$$

The infimum of two elements of $\mathcal{L}'(Q)$ is less easily described in terms of ideals.

(3.3.10) Proposition. If $A,B \in I$, $\alpha \in \sum_m(A)$ and $\beta \in \sum_n(B)$, then $\beta^s A^{rm} \cap \alpha^r B^{sn} \in I$ and

$$c\ell(A) \wedge c\ell(B) = c\ell(\beta^s A^{rm} \cap \alpha^r B^{sn})$$

for both r,s sufficiently large.

Proof. Let $A^{m+t} = \alpha A^t$ for $t \geq t_0$ and $B^{n+t} = \beta B^t$ for $t \geq t_1$. Consider $r \geq t_0/m$ and $s \geq t_1/n$ so $A^{2rm} = \alpha^r A^{rm}$ and $B^{2sn} = \beta^s B^{sn}$, it is clear that $\alpha^r\beta^s \in \beta^s A^{rm} \cap \alpha^r B^{sn}$ is not zero-divisor.

So $\alpha^r\beta^s(\beta^s A^{rm} \cap \alpha^r B^{sn}) \subseteq (\beta^s A^{rm} \cap \alpha^r B^{sn})^2 \subseteq \beta^{2s} A^{2rm} \cap \alpha^{2r} B^{2sn}$

$$= \beta^{2s}\alpha^r A^{rm} \cap \alpha^{2r}\beta^s B^{sn} = \alpha^r\beta^s(\beta^s A^{rm} \cap \alpha^r B^{sn}),$$

and $\beta^s A^{rm} \cap \alpha^r B^{sn} \in I$ with $\alpha^r B^s \in \sum_1(B^s A^{rm} \cap \alpha^r B^{sn})$.

Hence by (3.3.5.1)

$$S(\beta^s A^{rm} \cap \alpha^r B^{sn}) = (1/\alpha^r\beta^s)(\beta^s A^{rm} \cap \alpha^r B^{sn}) =$$

$$= (1/\alpha^r)A^{rm} \cap (1/\beta^s)B^{sn}$$

$$= S(A) \cap S(B).$$

Chapter IV

One-dimensional local rings of multiplicity two.

(4.1) Introduction. Throughout this chapter Q is a one-dimensional local ring of multiplicity two and m is its maximal ideal.

Our aim in this chapter is to find the lattice $\mathcal{L}(Q)$. Our work depends on that of Matlis [4], Matlis shows that if the local ring Q has multiplicity two, then every ideal of Q can be generated by two elements, and Q has a superficial element of degree one belonging to m. We introduce the equation $y^2 - \alpha xy - \beta x^2 = 0$ for suitable $\alpha, \beta \in Q$, (x,y in generators of m).

If $\alpha^2 + 4\beta \notin m$, then the first neighbourhood ring R_1, of Q is $\hat{Q}$ the integral closure of Q.

If $\alpha^2 + 4\beta \in m$, then the first neighbourhood ring R_1 of Q is again a local ring, as a consequence the lattice of finite extension rings $\mathcal{L}(Q)$ will either be finite.

$$R_0 \subset R_1 \subset \cdots\cdots \subset R_n ,$$

where R_n is $\hat{Q}$,

or

$$R_0 \subset R_1 \subset \cdots\cdots \subset R_i \subset \cdots\cdots ,$$

where each R_i is a local ring with multiplicity two.

(4.2) Local ring of multiplicity two.

Now, let Q be a one-dimensional local ring and let m, the maximal ideal of Q, not consist entirely of zero-divisors, and let the multiplicity of the local ring Q be $e(Q) = 2$. By (2.6.7),

every m-primary ideal of Q can be generated by two elements, in particular $m = (x,y)$ (say), also Q has a superficial element x (say) of degree one belonging to m.

We may assume the superficial element x of Q by proposition 13 of [4] (which is not a zero-divisor) satisfies $m^2 = mx$, and in particular

$$y^2 - \alpha xy - \beta x^2 = 0$$

for suitable $\alpha,\beta \in Q$.

(4.2.1) Remark. (3.3) implies that $S(m)$ which is the first neighbourhood ring R_1 is $(1/x)m = Q + Q.\frac{y}{x} = Q\left[\frac{y}{x}\right]$.

(4.2.2) Proposition. Every element $(\neq 0)$ of Q is either of the form unit $\times x^r$ (some $r \geq 0$) or of the form unit $\times x^r(y - \lambda x)$ (some $\lambda \in Q$, and $r \geq 0$)

Proof. Suppose $z \neq 0$ is an element of Q which satisfies $z \in m^r$ and $z \notin m^{r+1}$ $(r \geq 0)$.

In fact with previous notations $m^2 = xm$, where x is superficial element of degree one. Thus, either $r = 0$ or $r > 0$ and $z \in x^{r-1}m$, $z \notin x^r m$, that is

$$z = x^{r-1}(\bar{\alpha}x - \bar{\beta}y) \quad \text{for some } \bar{\alpha},\bar{\beta} \text{ not both}$$

in m. In this case either $\bar{\alpha} \notin m$ and $\bar{\beta} \in m$ which implies $z = \lambda x^r$ where λ is unit and $r \geq 0$, or $\bar{\beta} \notin m$, in this circumstance

$$z = \text{unit} \times x^{r-1}(y - \lambda x)$$

where $\lambda \in Q$ and $r-1 \geq 0$.

(4.2.3) Proposition. Every element of the quotient ring $\bar{R}$ of Q is of the form $\frac{q}{x^r}$ for some $r \geq 0$, and $q \in Q$.

Proof. Let ~~suppose that~~ $\bar{z} = \frac{\bar{q}}{p}$ be an element of the quotient ring $\bar{R}$ of Q, where $\bar{q}$ and p belong to Q, and p is not a zero-divisor. By (4.2.2) every element of Q is of the form, either unit $\times x^r$ or unit $\times x^r(y-\lambda x)$ where $\lambda \in Q$ and some $r \geq 0$.

(i) Suppose $\bar{z} = \frac{\bar{q}}{p}$ where $p = \text{unit} \times x^r$. In this circumstance $\bar{z} = \frac{\bar{q}}{\text{unit} \times x^r}$ and the proposition is clear.

(ii) Suppose that $\bar{z} = \frac{\bar{q}}{p}$, where $p = \text{unit} \times x^r(y-\lambda x)$ in this case $\bar{z} = \frac{\bar{q}}{\text{unit} \times x^r(y-\lambda x)}$

Now put $y-\lambda x = Y$. From this it follows immediately that $y = Y + \lambda x$, and Y is not zero-divisor, so from the equation $y^2 - \alpha xy - \beta x^2 = 0$, we deduce

$$Y^2 - (\alpha - 2\lambda)xY - (\beta + \alpha\lambda - \lambda^2)x^2 = 0$$

For simplification we denote $(\alpha - 2\lambda)$ by A and $(\beta + \alpha\lambda - \lambda^2)$ by B, so

$$Y^2 - AxY - Bx^2 = 0 \qquad (4.1)$$

Now we have two different possibilities:

(a) Suppose that $B \in QY$, then it will imply that $B = B'Y$. So the equation (4.1) will give

$$Y = Ax + B'x^2$$

i.e. $Y \in Qx$ or $m = Qx$ this is a contradiction to $e(Q) = 2$.

(b) Assume that $B \notin QY$, then we can choose an integer t such that

$$\begin{cases} B \in QY + Qx^{t} \\ B \notin QY + Qx^{t+1} \end{cases}$$

therefore the form of B is $\xi Y + \eta x^{t}$ where η is a unit.

It is clear that the equation (4.1) will be

$$Y^2 - (\alpha - 2\lambda + \xi x)xY - \eta x^{t+2} = 0 \qquad (4.2)$$

We multiply numerator and denominator of $\bar{z}$ by

$$(Y - (\alpha - 2\lambda + \xi x)x) = (y - \lambda' x) \quad \text{(say)}$$

It is clear that $y - \lambda' x$ is not zero-divisor, because x is not zero-divisor, consequently

$$\bar{z} = \frac{\bar{q}(y - \lambda' x)}{\text{unit} \times x^{s}.Y(Y - (\alpha - 2\lambda + \xi x)x)}$$

and from equation (4.2) we deduce

$$\bar{z} = \frac{\bar{q}(y - \lambda' x)}{\text{unit} \times x^{s}.\eta\, x^{t+2}}$$

For simplification we denote $q = \bar{q}(y - \lambda' x)$ and $(s + t + 2)$ by r, then $\bar{z} = \dfrac{q}{\text{unit} \times x^{r}}$, this completes the proof.

(4.2.4) Proposition. Every ideal is either principal or has two generators of the form $(x^{r}(y - \lambda x), x^{s})$ with $r < s$.

Proof. Let I be an ideal, it has two generators say z_1, z_2. It is obvious by (4.2.2) we will have three cases,

(a) The ideal I has two generators such that

$$I = (x^r, x^s)$$

From this it follows immediately that the ideal I is principal

(b) The ideal I has two generators such that

$$I = (x^r(y - \lambda x), x^s)$$

If $s > r$ then it has the required form

If $s \leq r$ then the ideal I has one-generator x^s and it is obvious the ideal I is principal.

(c) The ideal I generated by

$$(x^r(y - \lambda x) , x^t(y - \lambda' x))$$

Suppose that $t \geq r$ then

$$I = (x^r(y - \lambda x), x^t(y - \lambda' x))$$

$$= (x^r(y - \lambda x), x^{t+1}(\lambda - \lambda'))$$

and $$Qx^r(y - \lambda x) \subseteq I \subseteq Qx^r(y - \lambda x) + Qx^{r+1}$$

In fact by Krull's intersection theorem either

$$Qx^r(y - \lambda x) = I$$

and the ideal I is principal or there exists an integer $s > r$ such that

$$Qx^r(y - \lambda x) \subseteq I \subseteq Qx^r(y - \lambda x) + Qx^s$$

$$I \not\subseteq Qx^r(y - \lambda x) + Qx^{s+1} .$$

In this case, as $mx^s = x^s(y - \lambda x, x) \subseteq Qx^r(y-\lambda x) + Qx^{s+1}$,

we have $I \not\subseteq Qx^r(y - \lambda x) + \mathfrak{m}x^s$.

So I contains an element of the form

$$a\, x^r(y - \lambda x) + b\, x^s ,$$

where b is a unit, and therefore I contains x^s.

Hence $Qx^r(y - \lambda x) + Qx^s \subseteq I \subseteq Qx^r(y-\lambda x) + Qx^s$,

and $(x^r(y - \lambda x)\ ,\ x^s)$, with $r < s$, are generators of I.

(4.3) Proposition. If $\bar{z} \in \bar{R}$ and $\bar{z} \notin Q$, where $\bar{R}$ is the quotient ring of Q, then $\frac{y}{x} \in Q[\bar{z}]$

(Note that $\frac{y}{x}$ we prove belongs to module $Q.1 + Q.\bar{z}$)

Proof. Let $\bar{z}$ be an element of the quotient ring $\bar{R}$ of Q and suppose $\bar{z} = \frac{q}{p}$ where q and p belong to Q and p is not zero-divisor, by (4.2.3) we will have $\bar{z} = \frac{q}{x^r}$ for some $r \geq 0$ and $q \in Q$ and also by (4.2.2) we have two different cases.

(a) Assume that $q = \text{unit} \times x^s$ $(s \geq 0)$. With assumption $\bar{z} \notin Q$, then $\bar{z} = \text{unit} \times x^{s-r}$ and $r > s$, therefore we can write $x^{r-s-1}.\ \bar{z}.y = \frac{y}{x} \times \text{unit}$ consequently $\frac{y}{x}$ belongs to $Q[\bar{z}]$

(b) Now suppose that $q = \text{unit} \times x^s(y - \lambda x)$ for some $\lambda \in Q$ and $s \geq 0$, therefore $\bar{z} = \text{unit} \times x^{s-r}(y-\lambda x)$ where $r > s$, as $\bar{z}$ does not belong to Q, then it is obvious that $x^{r-s-1}.\bar{z} = \text{unit}\left(\frac{y}{x} - \lambda\right)$ therefore $\frac{y}{x} - \lambda \in Q[\bar{z}]$, consequently $\frac{y}{x} \in Q[\bar{z}]$ which completes the proof.

(4.3.1) Proposition. Every proper extension S of Q in the total quotient ring $\bar{R}$ of Q contains $R_m = R_1$ where R_1 is the first neighbourhood ring of Q.

Proof. Suppose that $\bar{z}$ is an element of the proper extension S of Q, and that it does not belong to Q, then $S \supseteq Q[\bar{z}]$, but by (4.3), $\frac{y}{x}$ belongs to $Q[\bar{z}]$, consequently by (4.2.1) $S \supseteq Q[\frac{y}{x}] = R_1$ which completes the proof.

(4.4) Proposition. If $\alpha^2 + 4\beta$ is a unit, then the first neighbourhood ring R_1 of Q is $\hat{Q}$, the integral closure of Q.

Proof. By assumption we must prove $R_1 \supseteq \hat{Q}$ as the opposition inclusion is obvious.

Let z be an element of $\hat{Q}$, it is clear that there is an ideal I of Q which contains a non-zero-divisor such that $zI \subseteq I$, see the condition (c") of (§1, chapter V of vol(I)[17]).

As we saw in the previous propositions, every ideal I of Q is either principal or has two generators of the form $\left(x^s(y - \lambda x), x^{r+s}\right)$ and also $y^2 - \alpha xy - \beta x^2 = 0$.

First suppose that the ideal I has two generators such that $I = x^s\left((y - \lambda x), x^r\right)$ where $r \geq 1$, with assumption $\alpha^2 + 4\beta \notin m$, so we can write

$$\begin{cases} zx^r = a\,x^r + b(y - \lambda x) \\ z(y - \lambda x) = c\,x^r + d(y - \lambda x), \end{cases}$$

where x is not a zero-divisor and $a,b,c,d \in Q$.

For simplification we denote

$$\begin{cases} y - \lambda x = t \\ \bar{z} = z - d \end{cases} \quad \text{and} \quad \begin{cases} \bar{a} = a - d \\ \bar{t} = y + (\lambda - \alpha)x \end{cases}$$

Therefore, from this it follows immediately that

$$\begin{cases} \bar{z}x^r = \bar{a}x^r + bt & (4.3) \\ \bar{z}t = cx^r & (4.4) \end{cases}$$

$$t^2 + (2\lambda - \alpha)xt + (\lambda^2 - \alpha\lambda - \beta)x^2 = 0$$

(i) If $(\lambda^2 - \alpha\lambda - \beta) \notin m$, then $x^2 \in mt$, therefore $m^3 = x^2 m \subseteq t\ m^2 \subseteq m^3$. i.e. $t\ m^2 = m^3$. Consequently t is superficial element of degree one and

$$\bar{z} = z - d = \frac{cx^r}{t} \in R_1$$

So, z belongs to the first neighbourhood ring R_1 of Q.

(ii) If $(\lambda^2 - \alpha\lambda - \beta) \in m$, in this circumstance

$$\begin{cases} \text{multiply (4.3) by } (\bar{t} + \mu x^2) \text{ where } \mu \in Q \text{ is yet to be determined} \\ \text{multiply (4.4) by } x^r \quad \text{where } r \geq 0 \end{cases}$$

then

$$\bar{z}\, x^r\left[(\bar{t} + \mu x^2) + t\right] = \bar{a}\, x^r(\bar{t} + \mu x^2) + cx^{2r} + bt\,(\bar{t} + \mu x^2)$$

It is obvious that

$$t(\bar{t} + \mu x^2) = y^2 - \alpha xy - \beta x^2 - (\lambda^2 - \alpha\lambda - \beta)x^2 + \mu x^2 y - \lambda\mu x^3 \qquad (4.5)$$

Now we have two different cases.

(a) Let us suppose that

$$\begin{cases} (\lambda^2 - \alpha\lambda - \beta) \in Qt + Qx^s \\ (\lambda^2 - \alpha\lambda - \beta) \notin Qt + Qx^{s+1} \end{cases} \quad \text{where} \quad (0 \leq s \leq r-2)$$

So, $(\lambda^2 - \alpha\lambda - \beta) = bt + c'x^s$ where c' = unit, now choose $\mu = 0$ in (4.5) then $c'x^{s+2} + bt\,x^2 = -t\bar{t}$

i.e. $x^{s+2} = d't$ where $d' \in Q$.

Consequently $z - d = \bar{z} = \dfrac{cx^r}{t} = \dfrac{cd'x^r}{x^{s+2}} \in Q$

So $\bar{z} \in R_1$ and $z = \bar{z} + d \in R_1$, as required.

(b) Now suppose that

$$(\lambda^2 - \alpha\lambda - \beta) \in Qt + Qx^{r-1} \quad \text{in this case}$$

$$\lambda^2 - \alpha\lambda - \beta = \xi t + \eta x^{r-1} \quad \text{where } \xi, \eta \in Q. \text{ Considering}$$

$\bar{z}x^r((\bar{t} + \mu x^2) + t)$, as $y^2 - \alpha xy - \beta x^2 = 0$, we have

$$\bar{z}x^r\left((\bar{t} + \mu x^2) + t\right) = \bar{a}x^r(\bar{t} + \mu x^2) + cx^{2r} + bt(\bar{t} + \mu x^2)$$

But $$t(\bar{t} + \mu x^2) = -(\lambda^2 - \alpha\lambda - \beta)x^2 + \mu x^2 t$$

$$= -x^2\left((\xi - \mu)t + \eta\, x^{r-1}\right)$$

Now choose $\xi = \mu$, then

$$t(\bar{t} + \mu x^2) = -\eta x^{r+1}$$

consequently $$\bar{z}x^r\left((\bar{t} + \mu x^2) + t\right) \in m^{r+1}$$

In fact

$$\left((\bar{t} + \mu x^2) + t\right)^2 = 4y^2 - 4\alpha xy + \alpha^2 x^2 + \mu^2 x^4 + 4\mu x^2 y - 2\alpha\mu x^3$$

$$= (4\beta + \alpha^2)x^2 + \mu^2 x^4 + 4\mu x^2 y - 2\alpha\mu x^3 = \text{unit} \times x^2$$

Therefore $x^2 \in Q\left((\bar{t} + \mu x^2) + t\right)^2$ and

$$m^3 = mx^2 \subseteq m\left((\bar{t} + \mu x^2) + t\right)^2 \subseteq m^3$$

i.e. $m^3 = m\left((\bar{t} + \mu x^2) + t\right)^2$ which means

$\left((\bar{t} + \mu x^2) + t\right)^2$ is a superficial element of degree two and

$x^r\left((\bar{t} + \mu x^2) + t\right)^2$ is a superficial element of degree $r + 2$

From this it follows immediately that

$$\bar{z}\, x^r\left((\bar{t} + \mu x^2) + t\right)^2 \in m^{r+2}$$

and $\bar{z} \in R_1$, thus $z = \bar{z} + d \in R_1$ as required.

Now let the ideal I of Q have only one-generator where I contains a non-zero-divisor.

From this it follows immediately that the relation $z\, I \subseteq Q\, I$ implies that $z \in Q \subseteq R_1$.

(4.5) So far we know the first neighbourhood ring R_1 of Q is the set of all the form $\frac{z}{x}$ where x is a superficial element of degree one, and $z \in m$, so $z = rx + sy$, where $r,s \in Q$.

(4.5.1) Proposition. $\frac{\alpha}{x}$ is a unit of R_1 if and only if α is superficial element of degree one.

Proof. Let us suppose that α is a superficial element of degree one, then $\frac{x}{\alpha}$, the inverse of $\frac{\alpha}{x}$ is in R_1. Hence $\frac{\alpha}{x}$ is a unit of R_1.

Now let us suppose that $\frac{\alpha}{x}$ is a unit in R_1, then $\frac{\alpha}{x} \cdot \frac{\beta}{x} = 1$ for some $\beta \in m$, or $x^2 \in m\alpha$, thus

$$m^2x = mx^2 \subseteq m^2\alpha = mx\alpha$$

So $m^2 = m\alpha$ as x is not a zero-divisor. Hence α is a superficial element of degree one.

(4.6) Proposition. $\alpha \in m$ is a superficial element of degree one, if and only if either $\alpha = \text{unit} \times x$ or $\alpha = \text{unit} \times (y - \lambda x)$ where $\lambda^2 - \alpha\lambda - \beta \notin m$.

Proof. Consider $\alpha \in m$. When $\alpha \in Qx$, it is clear that α is superficial of degree one if, and only if, $\alpha \in Qx \setminus mx$. Otherwise $\alpha = ax + by$ with $b \notin m$, i.e. $\alpha = \text{unit} \times (y - \lambda x)$. So we must show that $Y = y - \lambda x$ is superficial of degree one if and only if $\lambda^2 - \alpha\lambda - \beta \notin m$.

As $y^2 - \alpha xy - \beta x^2 = 0$ we have

$$Y^2 - (\alpha - 2\lambda)xY + (\lambda^2 - \alpha\lambda - \beta)x^2 = 0$$

If $\lambda^2 - \alpha\lambda - \beta \notin m$, then $x^2 \in mY$ and

$$m^3 \supseteq m^2 Y \supseteq mx^2 = m^3 ,$$

Thus $m^3 = m^2Y$ and Y is a superficial element of degree one for m.

Conversely if Y is superficial of degree one, then $m^{r+1} = m^rY$ for some $r \geq 1$. But $m^2 = mx$ and x is not a zero-divisor, so $x^2 \in m^2 = mY$ or $x^2 = \mu Y$ for some $\mu \in m$. Thus Y is not a zero-divisor, so

$$(\lambda^2 - \alpha\lambda - \beta)\mu Y = (\lambda^2 - \alpha\lambda - \beta)x^2 = ((\alpha-2\lambda)x-Y)Y$$

gives $\quad Y = y-\lambda x \in Qx + m(\lambda^2 - \alpha\lambda - \beta)$.

$\lambda^2 - \alpha\lambda - \beta \in m$ would imply $y \in Qx + m^2 = Qx$, contrary to $e(Q) = 2$. So $\lambda^2 - \alpha\lambda - \beta \notin m$ as required.

(4.7) Theorem. If $\alpha^2 + 4\beta$ belongs to m, then the first neighbourhood ring R_1 is a local ring.

Proof. All elements of R_1 are of the form $\frac{z}{x}$, and so the first neighbourhood ring R_1 is just,

$$R_1 = Q \cup \left\{u\left(\frac{y-\lambda x}{x}\right)\right\},$$

where λ ranges through Q and u through the units of Q. But the local ring Q itself is the union of $Q-m$ and m in which $Q-m$ are units in Q and m are non-units in Q.

Again $\left\{u\left(\frac{y-\lambda x}{x}\right)\right\}$ is the union of the $u \times \frac{y-\lambda x}{x}$ where $\lambda^2 - \alpha\lambda - \beta \notin m$ which is a unit in R_1 by (4.6) and (4.5.1) and $u \times \frac{y-\lambda x}{x}$ where $\lambda^2 - \alpha\lambda - \beta \in m$ which is a non-unit in R_1.

Therefore, R_1 = units $\cup$ non-units

- $Q-m$, unit $\times \frac{y-\lambda x}{x}$ where $y-\lambda x$ is superficial element of degree one
- m, unit $\times \frac{y-\lambda x}{x}$ where $y-\lambda x$ is not superficial element of degree one

Now we must show that, the set of non-units of R_1 form an ideal. For this

(4.7.1)(a). The non-units of R_1 is closed for product by elements of R_1 .

Proof. For this, multiply the non-unit t of R_1 by $r \in R_1$. If tr is a unit of R_1, then there is another element $s \in R_1$ such that $trs = 1$, which implies t is a unit, a contradiction.

(4.7.2)(b) The non-units of R_1 is closed for sums.

Proof. For the proof of this part we have three different possibilities

(4.7.2)(i) Suppose that the two components are in m.

Proof. It is obvious that if the two components are in m , then the sum of them is a non-unit.

(4.7.2.2)(ii) Suppose that, one of components is in m and the other is in the form $u\left(\frac{y-\lambda x}{x}\right)$ where $y-\lambda x$ is not a superficial element of degree one and x is a unit of Q.

Proof. For this, we can write

$$m - u\left(\frac{y-\lambda x}{x}\right) = - u\left(\frac{y-(\lambda+u^{-1}m)x}{x}\right)$$

and $(\lambda+u^{-1}m)^2 - \alpha(\lambda+u^{-1}m) - \beta = \lambda^2 - \alpha\lambda - \beta+m(2\lambda u^{-1} + u^{-2}m - \alpha u^{-1}) \in m$.

Consequently this is again a non-unit of R_1 by (4.6)

(4.7.2.3)(iii). Suppose that the two components are both of the form unit $\times \frac{y-\lambda x}{x}$ where, each $y-\lambda x$ is not a superficial element of degree one.

Proof. For this, we show

$$u_1\left(\frac{y-\lambda_1 x}{x}\right) - u_2\left(\frac{y-\lambda_2 x}{x}\right) \text{ is a non-unit of } R_1 .$$

As we mentioned $y - \lambda x$ is not a superficial element of degree one if and only if $\lambda^2 - \alpha\lambda - \beta \in m$,

So $\lambda_1^2 - \alpha\lambda_1 - \beta \in m$ and $\lambda_2^2 - \alpha\lambda_2 - \beta \in m$

This implies that $(\lambda_1 - \lambda_2)(\lambda_1 + \lambda_2 - \alpha) \in m$.

Therefore $\lambda_1 - \lambda_2 \in m$ or $\lambda_1 + \lambda_2 - \alpha \in m$.

Now $\lambda_1 + \lambda_2 - \alpha \in m$ and $\lambda_1^2 - \alpha\lambda_1 - \beta \in m$

imply that $\lambda_1\lambda_2 + \beta = \lambda_1(\lambda_1+\lambda_2-\alpha) - (\lambda_1^2-\alpha\lambda_1-\beta) \in m$

With the assumption that $\alpha^2 + 4\beta \in m$, we have

$$(\lambda_1-\lambda_2)^2 = (\lambda_1+\lambda_2)^2 - 4\lambda_1\lambda_2 = \alpha^2+4\beta = 0 \bmod m$$

From this it follows immediately that $\lambda_1-\lambda_2 \in m$

Thus $$u_1\left(\frac{y-\lambda_1 x}{x}\right) - u_1\left(\frac{y-\lambda_2 x}{x}\right) = u_1\left(\frac{y-\lambda x}{x}\right) - u_2\left(\frac{y-\lambda x}{x}\right) + m$$

$$= (u_1-u_2)\left(\frac{y-\lambda x}{x}\right) + m$$

which is again a non-unit of R_1 by (i) if $u_1-u_2 \in m$ and by (ii) if $(u_1-u_2) \notin m$.

In fact the maximal ideal M_1 of R_1 will be generated by $\left(x, \frac{y-\lambda x}{x}\right)$ where $y-\lambda x$ is not superficial element, which is true if and only if $\lambda^2 - \alpha\lambda - \beta \in m$.

Note that if $2 \notin m$, $\lambda^2 - \alpha\lambda - \beta = \left(\lambda - \frac{\alpha}{2}\right)^2 - \frac{1}{4}(\alpha^2 + 4\beta)$.

So $y-\lambda x$ is superficial of degree one if and only if $\lambda = \frac{\alpha}{2} \bmod m$.

In this case the maximal ideal M_1 of R_1 will be generated by $\left(x, \frac{2y-\alpha x}{x}\right)$.

(4.8.1) Proposition. Let $\alpha^2 + 4\beta \in m$ and let $\lambda^2 - \alpha\lambda - \beta \in m$ have no solution for λ, then the first neighbourhood ring R_1 of Q is a one-dimensional regular local ring.

Proof. If $\lambda^2 - \alpha\lambda - \beta$ belongs to m and has no solution for λ, then the maximal ideal M_1 of R_1 is generated by a single element x. So R_1 is a one-dimensional regular local ring.

Note that this case can only occur when $2 \in m$.

(4.8.2) Proposition. Let $\alpha^2 + 4\beta \in m$ and let $\lambda^2 - \alpha\lambda - \beta \in m$ be a superficial element of m of degree one, then R_1 is a one-dimensional regular local ring.

Proof. With previous notation and assumption the maximal ideal M_1 of R_1 is generated by $\left(\frac{y-\lambda x}{x}\right)$ because, we can write

$$-(\lambda^2-\alpha\lambda-\beta)x^2 = -(\lambda^2-\alpha\lambda)x^2 + (y^2-\alpha xy)$$

$$= (y-\lambda x)(y + \lambda x - \alpha x)$$

So $$x = -\frac{y-\lambda x}{x} \cdot \frac{y+(\lambda-\alpha)x}{(\lambda^2-\alpha\lambda-\beta)} \in R_1\left(\frac{y-\lambda x}{x}\right)$$

consequently R_1 is a one-dimensional regular local ring.

(4.8.3) Proposition. Let $\alpha^2 + 4\beta \in m$ and let $\lambda^2-\alpha\lambda-\beta \in m$ not be a superficial element of m of degree one, then the first neighbourhood ring R_1 of Q is local ring of multiplicity two and x is a superficial element of degree one belonging to M_1.

Proof. By (4.7) the first neighbourhood ring R_1 of Q is a local ring and by the proof of (4.8.2) we can write

$$-(\lambda^2 - \alpha\lambda - \beta)x^2 = (y-\lambda x)(y + \lambda x - \alpha x)$$

From this it follows immediately that

$$\left(\frac{y-\lambda x}{x}\right)^2 + (2\lambda-\alpha)\left(\frac{y-\lambda x}{x}\right) + (\lambda^2 - \alpha\lambda - \beta) = 0$$

But $(2\lambda-\alpha)^2 = 4\lambda^2 - 4\lambda\alpha + \alpha^2 = 4\beta + \alpha^2 \pmod m$

$= 0 \pmod m$

i.e. $2\lambda - \alpha \in m$

So $\left(\frac{y-\lambda x}{x}\right)^2 = -x\left(\frac{2\lambda-\alpha}{x}\right).\left(\frac{y-\lambda x}{x}\right) - x\,\frac{\lambda^2-\alpha\lambda-\beta}{x} \in x M_1$

therefore $\left(\frac{y-\lambda x}{x}\right)^2 \in xM_1$ which implies that $M_1^2 = xM_1$

so x is superficial element of degree one for M_1.

Turning our attention to the other assertion

by Prop 1 of [4] $\text{length}_{R_1}(R_1/xR_1) = e(R_1)$

It is clear that the multiplicity of the first neighbourhood ring R_1 is $\text{length}_{R_1}(R_1/M_1) + \text{length}_{R_1}(M_1/xR_1)$. We know

$\text{Length}_{R_1}(R_1/M_1) = 1$

therefore $e(R_1) = 1 + \text{length}_{R_1}\left(x, \frac{y-\lambda x}{x}/(x)\right)$

or $e(R_1) = 1 + \text{length}_{R_1}\left(\frac{y-\lambda x}{x} / (x) \cap (\frac{y-\lambda x}{x})\right)$

But $(x) \cap (\frac{y-\lambda x}{x}) \supseteq M_1(\frac{y-\lambda x}{x})$

and $\frac{y-\lambda x}{x} \in R_1 x$ would imply $y-\lambda x \in mx$. i.e. $y \in Qx$ contrary to $e(Q) = 2$. Therefore $(x) \cap (\frac{y-\lambda x}{x}) = M_1 \frac{y-\lambda x}{x}$. Consequently

$e(R_1) = 1 + \text{length}_{R_1}(R_1/M_1) = 1 + 1 = 2$ which completes the proof.

(4.9) It will now be convenient to introduce some more notations

Let Q be a one-dimensional local ring, with maximal ideal m, and let the multiplicity of Q be $e(Q) = 2$, then the first neighbourhood ring is R_1 ~~which~~ is either, an integrally closed ring, in this circumstance the tree of neighbourhood rings is only $Q = R_o \subset R_m = R_1$. Or a local ring, with multiplicity two.

Again if the first neighbourhood ring R_1 of R_0 is local ring with multiplicity two, with previous propositions, the second neighbourhood ring is either an integrally closed ring, in this case the tree of neighbourhood rings is only $R_0 \subset R_1 \subset R_2$ or a local ring with multiplicity two, so that if we repeat this procedure we will have

$$R_0 \subset R_1 \subset R_2 \subset \ldots\ldots \subset R_n$$

or

$$R_0 \subset R_1 \subset R_2 \subset \ldots\ldots \subset R_i \subset \ldots\ldots\ldots$$

From this it follows that, the tree of neighbourhood rings is linearly ordered.

(4.9.1) Definition. Let $R_0 = Q, R_1 = R_m$ and let $R_{i+1} = (R_i)_{m_i}$ where m_i is the maximal ideal of R_i and $i \geq 0$, if R_i is defined and not integrally closed. Otherwise R_{i+1} is not defined.

The theorem follows at once that,

(4.10) Theorem. If S belongs to the lattice $\mathcal{L}(Q)$ of finite extension rings of Q, then $S = R_i$ for some $i \geq 0$.

Proof. Let S belong to the lattice, we know S is a finite R_1-module, ($\supseteq Q$), and that

$$\text{length}(R_1/Q) = \rho$$

(see theorem 1 of [12])

Now, suppose that t be the largest integer such that $S \supseteq R_t$, the existance of such an integer is guaranteed by the following statement.

If $S \supseteq R_t$ for all t and R_t defined for all t then we have

$$\text{length}(S/Q) \geq \text{length}(R_t/Q) \geq t \quad \text{(for all } t\text{)}$$

this, however, is a contradiction, because the

length(S/Q) is finite

Now either $S = R_t$ as required

or $S \supset R_t$

and in this last circumstance R_t is not integrally closed, so R_{t+1} is defined and $S \supseteq R_{t+1}\left(= (R_t)_{m_t}\right)$ by (4.3.1) this is contrary to definition of t.

Example 1.

Let $Q = K[[t^2, t^{2m+1}]]$ (where $m \geq 1$) be a local ring, then the finite lattice of finite extension rings is

$$K[[t^2,t^{2m+1}]] \subset K[[t^2,t^{2m-1}]] \subset K[[t^2,t^{2m-3}]] \subset \ldots \subset K[[t^2,t]]=K[[t]]$$

which is integrally closed.

Example 2.

Let $Q = K[[x,y]]/(y^2)$ be a local ring, then

$R_1 = K[[x,y/x]]/((y/x)^2)$ which is isomorphic with Q.

So $K[[x,y]]/(y^2) \subset K[[x,y/x]] / (y/x)^2) \subset \ldots\ldots\ldots \simeq Q$

therefore the lattice of finite extension rings is infinite.

References

1. Kirby, D. "A note on superficial elements of an ideal in local ring"(Qurt.J.Math.(Oxf) (2),14(1963),21-28)

2. Kirby, D. "The defect of a one-dimensional local ring" (Mathematika, 6(1959), 91-97)

3. Kirby, D. "The reduction number of a one-dimensional local ring" (J.Lond.Math.Soc.(2),10(1975), 471-488)

4. Mathis, E. "The multiplicity and reduction number of a one-dimensional local ring" (Proc.Lond.Math.Soc., 26(1973), 273-288

5. Nagata, M. "Local rings (Interscience, New York 1962)

6. Narita, M. "A note on the coefficients of Hilbert characteristic function in semi-regular local rings" (Proc. Camb.Phil.Soc. (1963), 59, 269-275)

7. Northcott, D.G. "Hilbert's function in a local ring" (Quart. J.Of Math.(Oxford)(2), 4(1953), 67-80)

8. Northcott, D.G. "Ideal theory," Cambridge Tract No.42 (Cambridge University Press 1953)

9. Northcott, D.G. "On the algebraic foundations of the theory of local dilatations" (Proc.Lond.Math.Soc.(3),6(1956), 267-285).

10. Northcott, D.G. "On the notion of a first neighbourhood ring with an application to the AF + BΦ theorem". (Proc.Cambridge Phil.Soc. 53(1957) 43-56)

11. Northcott, D.G. "The coefficients of the abstract Hilbert functions". (J.Lond.Math.Soc. 35(1960), 209-214)

12. Northcott, D.G. "The reduction number of a one-dimensional local ring". (Mathematika.6 (1959) 87-90)

13. Northcott, D.G. "The neighbourhoods of a local ring". (J.Lond.Math.Soc. 30(1955), 360-375).

14. Rees, D. "Two classical theorems of ideal theory (ibid, 52 (1956), 155-157).

15. Samuel, P. "Algébre locale." (Mémor.Sci.Math.123 (1953)).

16. Samuel, P. "La notion de multiplicité en algèbre et en géométrie" (Thesis, paris, 1951).

17. Zariski, O. and Samuel, P. "Commutative algebra". Vol.I and II (Van Nostrand, Princeton,New Jersey 1960).