CHAPTER 6. IDEAL THEORY IN COMMUTATIVE NOETHERIAN RINGS

CHAPTER 7. DEDEKIND RINGS

Comments:

These chapters and those following were written by Peter May and Lutz Bungart. They are based in part on lectures presented in 1960-1961 in connection with my course. These lectures were partly presented by various people who attended the course. In addition to the preceding, May and Bungart have made some additions which were not covered in the lectures presented.

John C. Moore

CHAPTER 6

IDEAL THEORY IN COMMUTATIVE NOETHERIAN RINGS

In this chapter we develop further some of the results of primary decompositions of ideals obtained in chapters 1 and 2 and develop briefly the ideal theory of local rings. The results obtained will be used in the next chapter for the characterization of Dedekind rings. The results on regular local rings will be amplified later by the use of homological methods.

In this chapter Λ will denote a commutative Noetherian ring.

1. Preliminaries (Krull's theorem).

We begin by restating some of the results of chapters 1 and 2 as applied to ideal theory.

Proposition 1.1: Any ideal I in Λ has a reduced primary decomposition.

Proof: This is immediate from Theorem 2.9 of chapter 1.

Notations 1.2: An associated prime ideal of an ideal I is said to belong to I. An ideal I will be called P-primary if I is primary and $P = \sqrt{I}$. $I(M) = \{k/k \in \Lambda , mk \in I$ for some $m \in M\}$, where M is a monoid, is called the M-component of I.

Proposition 1.3: The set of ideals belonging to I is uniquely determined by I.

Proof: This follows from theorem 2.11 of chapter 1.

Proposition 1.4: Let I be an ideal and P a prime ideal minimal among the prime ideals containing I. Then P belongs to I and in any reduced primary decomposition of I, the P-primary factor is uniquely determined as $I(\Lambda - P)$.

Proof: This follows from proposition 1.6 of chapter 2.

Definition 1.5: Let P be a prime ideal. P is certainly a minimal prime belonging to P^N , $N \geq 1$. $P^{(N)} = P^N(\Lambda - P)$, the P-primary factor of P^N , is called the Nth symbolic prime power of P . If P is maximal, then P^N is primary, $P^{(N)} = P^N$.

Lemma 1.6: Let $J = \bigcap_N I^N$; then $IJ = J$.

Proof: This follows from proposition 2.16 of chapter 1.

Lemma 1.7: Let I and J be ideals such that $IJ = J$. Then there exists $z \in I$ such that $(1 - z)J = (0)$.

Proof: Let $J = (x_1,\ldots,x_N)$. Define $J_i = (x_i,\ldots,x_N)$, $J_{N+1} = (0)$. By induction on i , we prove that there exists $z_i \in I$ such that $(1 - z_i)J \subset J_i$. $z = z_{N+1}$ will then be as desired. For $i = 1$, $z_1 = 0$ suffices. Now assume we have z_i with $(1 - z_i)J \subset J_i$; $J = IJ$, so $(1 - z_i)J \subset I(1 - z_i)J \subset IJ_i$. $(1 - z_i)x_i = \sum_{j=i}^{N} z_{ij} x_j$, $z_{ij} \in I$. $(1 - z_i - z_{ii})x_i \in J_{i+1}$. Then $1 - z_{i+1} = (1 - z_i)(1 - z_i - z_{ii})$ defines a suitable z_{i+1} .

Corollary 1.8: $J = \bigcap_N I^N$ is the $(1 - I)$ -component of (0),

$(1 - I = \{1 - a/a \in I\})$.

Proof: There exists $z \in I$ with $(1 - z)J = (0)$, so $J \subset (0)(1 - I)$. But if $(1 - x)y = 0$, $x \in I$, then $y = xy = x^2y = \cdots$ and $y \in J$, so $J = (0)(1 - I)$.

Proposition 1.9: $\bigcap_N I^N = (0)$ if and only if $1 - I$ contains no zero divisors [Krull's theorem].

Proof: $1 - I$ contains no zero divisors means that the $(1 - I)$-component of (0) is (0).

Corollary 1.10: If Λ is a local ring with maximal ideal M , then $\bigcap_N M^N = (0)$.

Proof: Every element of $1 - M$ is a unit.

Corollary 1.11: If Λ is a local ring with maximal ideal M , then $\bigcap_N (I + M^N) = I$, where I is a proper ideal.

Proof: Λ/I is a local ring with maximal ideal $\bar{M} = \text{im}\ (M)$. $\bigcap_N \bar{M}^N = (0)$ implies $\bigcap_N (I + M^N) = I$.

Corollary 1.12: Let $P \subset \Lambda$ be a prime ideal. Then $\cap P^{(N)}$ is the $(\Lambda - P)$-component of (0) .

Proof: Let $\pi\colon \Lambda \longrightarrow \Lambda_p$ be the localization of Λ at P . $\ker(\pi)$ is the $(\Lambda - P)$-component of (0) . $P^{(N)}$ is the $(\Lambda - P)$-component of P^N , which is $P_p^N \cap \Lambda$. $\bigcap_N P^{(N)} = (\bigcap_N P_p^N) \cap \Lambda = (0) \cap \Lambda = \ker(\pi)$.

We conclude this section with the useful

Proposition 1.13: Let Λ be a commutative ring. Let I be an ideal and $P_1,\ldots,P_N$ prime ideals none of which contains I . Then there exists $a \in I$ such that a belongs to none of the P_i .

Proof: We use induction of N , the case $N = 1$ being trivial. Assume the result holds for any set of $N - 1$ prime ideals: For each $i(1 \leq i \leq N)$ choose $a_i \in I$ such that a_i does not belong to any of $P_1,\ldots,P_{i-1},P_{i+1},\ldots,P_N$. If for any i , $a_i \notin P_i$ the result holds. Assume then that each $a_i \in P_i$. Let $a = \sum_{i=1}^{N} (a_1 \ldots a_{i-1}\ a_{i+1} \ldots a_N)$. The jth term of the sum is not in P_j while all the other terms are in P_j . Hence a is as desired.

2. Residual division of modules and ideals.

Let B be a fixed Λ-module.

Definition 2.1: Let A be a submodule of B and I an ideal; define $A: I = \{x | x \in B , x I \subset A\}$.

Lemma 2.2: Let Q be a primary submodule of B with associated prime ideal P and let I be an ideal not contained in P . Then $Q: I = Q$.

Proof: By definition $I(Q : I) \subset Q$; $I \not\subset P$, so $Q: I \subset Q$. $Q: I \supset Q$ is obvious, so $Q: I = Q$.

Proposition 2.3: Let A be a proper submodule of B and let I be an ideal. Then $A: I = A$ if and only if I is not contained in any associated prime ideal of A in B .

Proof: Let $A = Q_1 \cap \ldots \cap Q_N$ be a reduced primary decomposition of A in B and let P_i be the associated prime ideal of Q_i . Assume no P_i contains I . By the lemma, $Q_i: I = Q_i$ for all i . Then $A: I = (\bigcap_i Q_i): I = \bigcap_i (Q_i : I) = \bigcap_i Q_i = A$. Now assume that $A: I = A$. Observe that if J and K are ideals, $(A : J): K = A: JK$. $A = A: I = A: I^2$, and $A = A: I^r$ for all r . Choose r such that $P_i^r \subset \text{ann} ({}^B/Q_i)$ for all i . If $I \subset P_i$ for any i , $Q_i: I^r = B$, while if $I \not\subset P_i$ then $Q_i: I^r = Q_i$, by the lemma. Thus $I \subset P_i$ for any i would contradict the choice of $Q_i \cap \ldots \cap Q_N$ as a reduced primary decomposition of A in B .

Corollary 2.4: Let I be an ideal such that $(0): I = (0)$. Then I contains an element a which is not a zero divisor for B (i.e., $ab = 0$, $b \varepsilon B$ implies $b = 0$).

Proof: I is not contained in any of the prime ideals P_i associated with (0). Choose $a \varepsilon I$ such that $a \notin P_i$ for any P_i associated with (0). Then $(0): (a) = (0)$, and this means that a is not a zero divisor in B.

3. Composition series, rank and dimension

Definition 3.1: Let Q be a P-primary ideal. A chain $P = Q_1 \supset Q_2 \supset \dots \supset Q_N = Q$ of primary ideals, where the inclusions are strict, is called a composition series if it has no proper refinements.

Theorem 3.2: Let Q be P-primary. Then there exists at least one composition series for Q, any two such series have the same number of terms, and every primary chain from P to Q can be refined to a composition series for Q.

Proof: i) By propositions 2.10 and theorem 2.13 of chapter 2, there is a 1 - 1 length preserving correspondence between primary chains from P to Q in Λ and in Λ_P, so we may assume that Λ is a local ring with maximal ideal P.

ii) Let $Q \subset I \subset P$; then there exists N with $P^N \subset I \subset P$. I is P-primary since if $P' \supset I$, $P' = P$, and P is the only prime ideal belonging to I . Thus any chain of ideals is a primary chain.

iii) P is the only prime ideal containing Q , and chains are preserved in Λ/Q so we may assume that Λ is primary (Λ is commutative and Noetherian with exactly one proper prime ideal), and Q is the zero ideal. Since Q is P-primary, there exists ℓ such that $P^\ell = (0)$.

iv) For $N \geq 1$ P^N/P^{N+1} is a vector space of dim d_N , say, over Λ/P . Thus there is a composition series of length d_{N+1} between P^N and P^{N+1} and combining these from $N = 1$ to $N = \ell - 1$, we obtain a series from P to (0) .

v) If $P = I_r \supset \ldots \supset I_0 = (0)$ is a chain, and $P = J_N \supset \ldots \supset J_0 = (0)$ is a composition series, then $r \leq N$: $J_1 \not\subset I_0$. Let k be such that $J_1 \not\subset I_k$, $J_1 \subset I_{k+1}$. We will show that

$J_1 + I_k \supset J_1 + I_{k-1} \supset \ldots \supset J_1 + I_0 = J_1$ is a primary chain: Let $0 \leq j < k$; choose $a_{j+1} \in I_{j+1}$, $a_{j+1} \notin I_j$. Then $a_{j+1} \notin I_j + J_1$: since $J_1 \not\subset I_{j+1}$, $J_1 \cap I_{j+1} \subset J_1$ (strict) and $J_1 \cap I_{j+1} = (0)$. If $a_{j+1} \in I_j + J_1$, $a_{j+1} = a_j + b$, $a_{j+1} - a_j = b \in J_1 \cap I_{j+1}$, $a_{j+1} = a_j \in I_j$, a contradiction. Now $P = I_r \supset \ldots \supset I_{k+1} \supseteq I_k + J_1 \supset \ldots \supset I_0 + J_1 = J_1 \supset (0)$ has at least $r + 1$ terms and ends with J_1 , (0) . Arguing similarly in Λ/J_1 , using the original composition series and the new primary chain, and returning to Λ , there is a primary chain from P to (0) ending in J_2, J_1, (0) with at least $r + 1$ terms. Inductively, there is a chain from P to (0) with at least $r + 1$ terms ending with $J_N, \ldots, (0)$, so $r \leq N$.

vi) By symmetric use of v), any two composition series have the same length. Finally, any longest possible refinement of a chain will be a composition series, and the proof is complete.

Definition 3.3: If Q is primary, the number of terms in a composition series for Q will be called the length of Q.

Definition 3.4: A proper prime ideal P is said to be of rank r if there exists a descending chain of r prime ideals all strictly contained in P and no chain with $r + 1$ terms; P is said to be of dimension d if there exists an ascending chain of d prime ideals all strictly containing P, and no chain with $d + 1$ terms. If I is any proper ideal, define rank (I) $= \min_i$ rank (P_i) and $\dim (I) = \max \dim (P_i)$, where $P_1, \ldots, P_N$ are the prime ideals belonging to I. An ideal I is said to be unmixed of rank N if rank $(P_i) = N$ for all primes P_i belonging to I.

Note that in determining rank (I) and $\dim (I)$ we may restrict ourselves to the minimal primes belonging to I. Also, if I is unmixed, then all primes belonging to I are minimal, and I has a unique reduced primary decomposition.

Proposition 3.5: Let b be a non-unit and P a minimal prime belonging to (b). Then rank $(P) \leq 1$.

Proof: Assume $P \supset P_1 \supset P_2$, $P \neq P_1$. We will prove $P_1 = P_2$. Localizing at P , we may assume that Λ is local with maximal ideal P ; (b) is P-primary, and every ideal between P and (b) is P-primary. Let $P_1^{(r)}$ be the rth symbolic prime power of P_1 . The number of terms in $P_1^{(1)} + (b) \supset P_1^{(2)} + (b) \supset \ldots$ is finite, being bounded by the length of (b) , so for some S , $P_1^{(S)} + (b) = P_1^{(S+1)} + (b) = \ldots$. We assert that for $M \geq S$, $P_1^{(M)} \subset (b)P_1^{(M)} + P_1^{(M+1)}$: let $x \varepsilon P_1^{(M)} \subset (b) + P_1^{(M+1)}$; $x = y + \lambda b$, $y \varepsilon P_1^{(M+1)}$, $\lambda \varepsilon \Lambda$; $x - y = \lambda b \varepsilon P_1^{(M)}$, $b \notin P_1$, so $\lambda \varepsilon P_1^{(M)}$, $x = y + \lambda b \varepsilon (b)P_1^{(M)} + P_1^{(M+1)}$. Then $P_1^{(M)} \subset PP_1^{(M)} + P_1^{(M+1)}$, $P_1^{(M)}/P_1^{(M+1)} = P(P_1^{(M)}/P_1^{(M+1)})$, $P_1^{(M)}/P_1^{(M+1)} = 0$, by proposition 4.1 of chapter 5, and $P_1^{(M)} = P_1^{(M+1)}$ for all $M \geq S$. Thus $P_1^S \subset P_1^{(S)} \subset \bigcap_N P_1^{(N)}$, which is the $(\Lambda - P_1)$ -component of (0) by corollary 1.15. Let $x \varepsilon P_1$; there exists $M \varepsilon \Lambda - P_1$ such that $Mx^S = 0$; $M \notin P_2$ since $P_1 \supset P_2$, so $x^s \varepsilon P_2$, $x \varepsilon P_2$, $P_1 \subset P_2$, $P_1 = P_2$. This completes the proof.

Proposition 3.6: Let $P \supset P_1 \supset P_o$ be a chain of proper prime ideals. Let $P_1', \ldots, P_k'$ be any finite set of prime ideals none of which contains P . Then there exists P^* not contained in any P_i' such that $P \supset P^* \supset P_o$ is a chain of prime ideals.

Proof: Choose $a \varepsilon P$ such that a does not belong to P_o or to any of the P_i' . $(a) + P_o \subset P$; let P^* be a minimal prime of $(a) + P_o$ contained in P . $P^* \supset P_o$ and P^* is not contained in any of the P'_i . If $P = P^*$, P/P_o is a minimal prime of $(\bar{a})$ in ${}^{\Lambda}/P_o$ and ${}^{P}/P_o \supset {}^{P}o/P_o \supset {}^{P}o/P_o$, contradicting proposition 3.5. Hence $P \supset P^* \supset P_o$ is a chain as desired.

Corollary 3.7: Let $P = P_\ell \supset \dots \supset P_1 \supset P_o$ be a chain of proper prime ideals. Let $P'_1,\dots,P'_k$ be any finite set of prime ideals none of which contains P . Then there is a chain of length ℓ from P to P_o with P_1 not contained in any P'_i .

Proof: If $\ell = 1$, the result is trivial. If $\ell \geq 2$, we apply the proposition to P_ℓ and $P_{\ell-2}$, then to $P_{\ell-3}$ and the new $P_{\ell-1}$ and so on until we obtain the result.

Theorem 3.8: Let $I = (a_1,\dots,a_M)$ be a proper ideal and let P be a minimal prime ideal belonging to I . Then rank $(P) \leq M$.

Proof: If $M = 1$, proposition 3.5 gives the result. Assume $M > 2$ and the result holds for $M - 1$ generators. Let $P'_1,\dots,P'_k$ be the minimal prime ideals of $(a_2,\dots,a_M)$. Rank $(P'_i) \leq M - 1$, so we may assume that P is not contained in any of the P'_i . Let $P = P_\ell \supset \dots \supset P_1 \supset P_o$ be a chain of prime ideals. We will show that $\ell \leq M$. By corollary 3.7, we may assume that P_1 is not contained in any of the P'_i . Choose $b \in P_1$ such that b is not in any of the P'_i . $(b, a_2,\dots,a_M) \subset P$, so there is a minimal prime ideal P^* belonging to $(b, a_2,\dots,a_M)$ such that $P^* \subset P$. $P^* \supset (a_2,\dots,a_M)$ so $P^* \supset P'_i$ for some i . By construction, $P^* \neq P'_i$. $P \supset P^* \supset P'_i$, but $P/(a_2,\dots,a_M)$ is a minimal prime of $\bar{a}_1$ in $\Lambda/(a_2,\dots,a_M)$, so $P = P^*$.

Thus P is a minimal prime of $(b, a_2, \dots, a_M)$, and $P/(b)$ is a minimal prime of $(\bar{a}_2, \dots, \bar{a}_M)$, in $\Lambda/(b)$. Rank $({}^P/(b)) \leq M - 1$ and ${}^P/(b) = {}^P\ell/(b) \supset \dots \supset {}^P1/(b)$ is a chain. Therefore $\ell - 1 \leq M - 1$, $\ell \leq M$.

Theorem 3.9: Let I be a proper ideal with rank $(I) = r \geq 1$. Then there exist r elements $a_1, \dots, a_r$ of I such that for $1 \leq i \leq r$, rank $(a_1, \dots, a_i) = i$.

Proof: We proceed inductively, The prime ideals of rank 0 are just the minimal primes belonging to (0) , hence are finite in number, and none contain I since rank $(I) \geq 1$. Choose $a_1 \varepsilon I$ so that a_1 is not in any prime ideal of rank 0 . Rank $(a_1) \geq 1$, so by proposition 3.5 rank $(a_1) = 1$. Now assume we have found $a_1, \dots, a_j$ as desired, $j < r$. Let $P_1, \dots, P_h$ be the prime ideals of $(a_1, \dots, a_j)$ of rank j , $P_{b+1}, \dots, P_k$ those of higher rank. Since rank $(I) = r > j$, I is not contained in any of $P_1, \dots, P_h$. Choose $a_{j+1} \varepsilon I$ such that $a_{j+1} \notin P_i$, $i = 1, \dots, h$. Let P be any minimal prime ideal of $(a_1, \dots, a_{j+1})$. $P \supset P_\mu$ for some $\mu \leq k$. If $\mu > h$, rank $(P) \geq$ rank $(P_\mu) \geq j+1$. If $\mu \leq b$, $P \neq P_\mu$ by construction and rank $(P) \geq$ rank $(P_\mu) + 1 = j + 1$. Thus rank $(P) \geq j + 1$. By Theorem 3.8, rank $(a_1, \dots, a_{j+1}) \leq j + 1$, so rank $(a_1, \dots, a_{j+1}) = j + 1$. This completes the proof.

4. Polynomial rings

To facilitate the discussion of local rings in the succeeding sections, we introduce some auxilary results concerning ideals in polynomial rings.

Let $\Lambda^* = \Lambda[x_1,\ldots,x_N]$ be the polynomial ring in N indeterminates over Λ . Λ^* is Noetherian by theorem 3.9 of chapter 1. An element of Λ^* will be written as $\phi(x_1,\ldots,x_N)$ or, for brevity, as $\phi(x)$. I, J, etc. will denote ideals in Λ , $I^* = \Lambda^*I$, $J^* = \Lambda^*J$, etc. their extensions to Λ^* .

Lemma 4.1: $\phi(x) \varepsilon I^*$ if and only if all the coefficients of $\phi(x)$ to I .

Corollary 4.2: $I^* \cap \Lambda = I$.

Corollary 4.3: If $I = J_1 \cap \ldots \cap J_r$, then $I^* = J_1^* \cap \ldots \cap J_r^*$.

Proposition 4.4: If Q is P-primary, then P^* is prime and Q^* is P^*-primary.

Proof: We may assume Λ^* is the polynomial ring in one indeterminate by proposition 3.4 of chapter 1. Assume $\phi(x) \notin P^*$, $\psi(x) \notin P^*$. If $\phi(x) = a_o + a_1 x + \ldots + a_s x^s$, $\psi(x) = b_o + b_1 c + \ldots + b_r x^r$, and a_ℓ and b_M are the first coefficients not in P , then $c = \sum_{i+j=\ell+m} a_i b_j$ is not in P and $\phi(x)\psi(x)$ is not in P^* . Thus P^* is prime. Let $P' \subset \Lambda^*$ belong to Q^* . $P' \cap \Lambda \supset Q^* \cap \Lambda = Q, P' \cap \Lambda$ is prime, hence $P \subset P' \cap \Lambda$, $P^* \subset P'$.

We will show that $P' = P^*$. Suppowe $\phi(x) = a_h x^h + \ldots + a_k x^k \in P'$. By proposition 2.3, $Q^*: \phi \nsubseteq Q^*$. Choose $\psi(x) = b_r x^r + \ldots + b_s x^s$ such that $\phi(x)\,\psi(x) \in Q^*$, $\psi(x) \notin Q^*$. We may assume $b_r \notin Q$; $a_h b_r \in Q$, so $a_h \in P$. $\phi(x) - a_h x^h \in P' + P^*$, $P' = P^*$, and Q^* is P^*-primary.

Corollary 4.5: If $I = Q_1 \cap \ldots \cap Q_N$ where Q_i is P_i-primary, then $I^* = Q_1^* \cap \ldots \cap Q_N^*$ where Q_i^* is P_i^*-primary, and if the first decomposition is reduced, then so is the second.

Proposition 4.6: If $\phi(x)$ is a zero division in Λ^* , then we can find $c \neq 0$ in Λ such that $c\,\phi(x) = 0$.

Proof: $(0): \phi(x) \neq (0)$, so $\phi(x) \in P^*$ where P^* is some prime ideal belonging to (0) in Λ^* , by proposition 2.3. P^* is the extension of a prime ideal P belonging to (0) in Λ . By lemma 4.1, all the coefficients of $\phi(x)$ are in P . $(0): P \neq (0)$, so there exists $c \neq 0$ such that $c \in (0): P$. Then $\phi(x) = 0$.

Proposition 4.7: If P is a prime ideal in Λ , then $\text{rank}\,(P) = \text{rank}\,(P^*)$.

Proof: We may assume Λ^* is a polynomial ring in one indeterminate. By corollaries 4.2 and 4.5, if P is a minimal prime ideal of an ideal I , then P^* is a minimal prime of I^* . Let rank $(P) = r$, rank $(P^*) = s$. If $r = 0$, P is a minimal prime of (0) , P^* is a minimal prime of (0) in Λ^* and $s = 0$. Suppose $r \geq 1$. Let $P \supset P_1 \supset \ldots \supset P_r$ be a chain. Then $P \supset P_1^* \supset \ldots \supset P_r^*$

is a chain and $s \geq r$. By theorem 3.9, there exist r elements $a_1,\ldots,a_r$ of P such that $(a_1,\ldots,a_r)$ is of rank r ; hence P^* must be a minimal prime ideal of $\Lambda^*a_1 + \ldots + \Lambda^*a_r$. By theorem 3.8, rank $(P^*) \leq r$. Therefore $r = s$.

5. Local rings; systems of parameters.

For the remainder of this chapter, a local ring will mean a Noetherian commutative ring with one maximal ideal. Q will denote such a ring. M its maximal ideal. By $\dim Q$ we shall mean the dimension of the zero ideal, $\dim Q = \operatorname{rank} M$. A local ring of dimension zero is a primary ring.

Proposition 5.1: $\dim Q$ is equal to the smallest number of non-zero elements required to generate an M-primary ideal.

Proof: Let $\dim Q = d$. If $d = 0$, (0) is an M-primary ideal, and the result is trivial. Suppose $d \geq 1$ and $(a_1,\ldots,a_s)$ is an M-primary ideal. By theorem 3.8, $d = \operatorname{rank}(M) \leq s$. By theorem 3.9 there exist elements $b_1,\ldots,b_d$ in M such that $(b_1,\ldots,b_d)$ has rank d . Since M is the only prime ideal of rank $\geq d$, $(b_1,\ldots,b_d)$ is M-primary. This completes the proof.

Definition 5.2: If $\dim Q = d \geq 1$, a set of d elements which qenerates an M-primary ideal is called a system of parameters in Q.

Proposition 5.3: Let $I = (a_1,\ldots,a_s)$ be a proper ideal in Q, and let $Q' = {}^{Q}/I$. Then $\dim Q \geq \dim Q' \geq \dim Q - s$. Also, $\dim Q' = \dim Q - s$ if and only if $a_1,\ldots,a_s$ is a subset of a system of parameters.

Proof: Let $\dim Q' = t$. If $t = 0$, (0) of Q' is M'-primary, so I is M-primary, $\dim Q \leq s$, $\dim Q - s \leq 0 = \dim Q'$. If $t \geq 1$, choose $b_1,\ldots,b_t$ in Q such that there residues mod I generate an M'-primary ideal. Then $(a_1,\ldots,a_s,b_1,\ldots,b_t)$ will be M-primary. By theorem 3.8, rank $M \leq s + t$, $\dim Q' \geq \dim Q - s$. If $\dim Q' = \dim Q - s$, then $s + t = \dim Q$, and $(a_1,\ldots,a_s,b_1,\ldots,b_t)$ is a system of parameters. Finally, if $(a_1,\ldots,a_s,c_1,\ldots,c_r)$ is a system of parameters, the residues of $c_1,\ldots,c_r$ mod I generate an M'-primary ideal, $\dim Q' \leq r = \dim Q - s$, $\dim Q' = \dim Q - s$.

Corollary 5.4: If I is a proper ideal in Q containing an element which is not a zero divisor, then $\dim {}^{Q}/I < \dim Q$. If $b \in Q$ is neither a unit nor a zero divisor, then $\dim {}^{Q}/(b) = \dim Q - 1$.

Proof: Any minimal prime P of I has rank ≥ 1, since otherwise $(0){:}\,P \neq (0)$, $(0){:}\,I \neq (0)$. Hence $\dim P <$ rank M, $\dim {}^{Q}/I = \dim I <$ rank $M = \dim Q$. Setting $I = (b)$, $\dim {}^{Q}/(b) \leq \dim Q - 1$, and the opposite inequality follows from the proposition.

Definitions 5.5: Let $Q^* = Q[x_1,\ldots,x_N]$. A homogeneous polynomial of degree s will be called a form of degree s . Let $t_1,\ldots,t_N$ be elements of M . The t_i will be called analytically independent if $\phi(t_1,\ldots,t_N) = 0$ implies that $\phi \,\varepsilon\, M^* = Q^*M$, where ϕ is a form of arbitrary degree.

If $t_1,\ldots,t_N$ are analytically independent and $\psi \not\varepsilon M^*$ is a form of degree s , then $\psi(t_1,\ldots,t_N) \not\varepsilon M(t_1,\ldots,t_N)^s$: otherwise $\psi(t) = \psi_o(t)$, $\psi_o(t) \,\varepsilon\, M(t_1,\ldots,t_N)^s$; $\phi(t) = \psi(t) - \psi_o(t) = 0$, and $\phi \,\varepsilon\, M^*$; hence $\psi = \phi + \psi_o$ would belong to M^* , a contradiction. This property will be of use in characterizing regular local rings. We prove now

Proposition 5.6: If $t_1,\ldots,t_d$ is a system of parameters, then the t_i are analytically independent.

Proof: i) Let $\phi(t) = \phi(t_1,\ldots,t_d) = 0$, where ϕ is a form of degree s . We first show that the coefficient a of t_1^s is in M . $at_1^s \,\varepsilon\, (t_2,\ldots,t_d)$; if $a \not\varepsilon M$, a is a unit, $t_1^s \,\varepsilon (t_2,\ldots,t_d)$, $(t_1,\ldots,t_d)^s \subset (t_2,\ldots,t_d)$ and since $(t_1,\ldots,t_d)$ is M-primary, so is $(t_2,\ldots,t_d)$. This contradicts the minimality of d , so $a \,\varepsilon\, M$.

ii) We now reduce the problem to the part already proven. Let $Q^* = Q[x_{ij}]$, $M^* = Q^*M$, where $x_{ij}(1 \leq i \leq d \, , 1 \leq j \leq d)$ are d^2 indeterminates. M^* is prime by proposition 4.4. Let π: $Q^* \longrightarrow Q'$ be the localization of Q^* at M^* . If

If $\psi \varepsilon Q^* - M^*$, ψ has a coefficient not in M , so by proposition 4.6, ψ is not a zero divisor in Q^* . Hence $\ker(\pi) = (0)$. Let $M' = Q'M^* = Q'M$. rank M' = rank M by proposition 4.7, and $Q't_1 + \cdots + Q't_d$ is M'-primary by proposition 4.4. Hence $t_1, \ldots, t_d$ is a system of parameters in Q' . Consider the determinant $|x_{ij}|$. $|x_{ij}| \notin M^*$, so $|x_{ij}|$ is a unit in Q'. Define $u_1, \ldots, u_d$ by $t_i = \sum_{j=1}^{d} x_{ij} u_j$. $Q'u_1 + \cdots + Q'u_d = Q't_1 + \cdots + Q't_d$ so $u_1, \ldots, u_d$ is a system of parameters in Q'. Define $f(u) = \phi(\sum_j x_{1j}u_j, \ldots, \sum_j x_{dj}u_j) = \phi(t) = 0$. By part i) the coefficient of u_1^s in $f(u)$ is in M'. But this coefficient is $\phi(x_{11}, x_{21}, \ldots, x_{d1})$, which therefore is in $M' \cap Q^* = M^*$. This completes the proof.

6. Regular local rings.

We need one more preliminary result:

Proposition 6.1: Let A be a finitely generated Q-module and let $a_1, \ldots, a_N$ be in A . Let $\bar{a}_i \equiv a_i \bmod MA$. Then the a_i generate A if and only if the $\bar{a}_i$ generate ${}^{A}/MA$ over $K = {}^{A}/M$.

Proof: Assume ${}^{A}/MA = K\bar{a}_1 + \ldots + K\bar{a}_s$. Let $a \varepsilon A$, $\bar{a} = q_1\bar{a}_1 + \ldots + q_N\bar{a}_N$, $q_i \varepsilon Q$. $a \varepsilon (a_1, \ldots, a_N) + MA$, $A \subset (a_1, \ldots, a_N) + MA$, ${}^{A}/(a_1, \ldots, a_N) = {}^{MA}/(a_1, \ldots, a_N)$, hence ${}^{A}/(a_1, \ldots, a_N) = 0$, $A = (a_1, \ldots, a_N)$. The converse is obvious.

Corollary 6.2: $\{a_1,\ldots,a_N\}$ is a minimal generating set of A if and only if $\{\bar{a}_1,\ldots,\bar{a}_N\}$ is a basis for the vector space ${}^{A}/MA$ over K. The length N of a minimal generating set for A is equal to $\dim_K {}^{A}/MA$.

Definition 6.3: Let Q be a local ring with maximal ideal M generated by a minimal set of N elements $u_1,\ldots,u_N$ and let $K = {}^{Q}/M$. By proposition 5.1 and corollary 6.2, $\dim Q \leq N = \dim_k {}^{M}/M^2$. A local ring for which $\dim\ Q = N$ is said to be regular.

Note that if $\dim Q = 0$ and Q is regular, $M = M^2$, so $M = M^N$ for all N; since $\bigcap_N M^N = (0)$, $M = (0)$. Thus a regular local ring of dimension zero is the same as a field.

If Q is a local ring and $M = (u_1,\ldots,u_N)$, the u_i form a system of parameters if and only if Q is regular. By proposition 5.6, if Q is regular, the u_i are analytically independent. We will prove the converse, and simultaneously obtain some fundamental properties of regular local rings. For the next two lemmas, assume that Q is local, $u_1,\ldots,u_N$ form a minimal set of generators for M, and the u_i are analytically independent.

Lemma 6.4: Let $a \in M^h$, $a \notin M^{h+1}$, $b \in M^k$, $b \notin M^{k+1}$ where h and k are non-negative integers. Then $ab \notin M^{h+k+1}$.

Proof: $a \in M^h = (u_1,\ldots,u_N)^h$, so $a = \phi(u_1,\ldots,u_N) = \phi(u)$ where ϕ is a form of degree h not all of whose coefficients are in M (since $a \notin M^{h+1}$). Similarly, $b = \psi(u_1,\ldots,u_N) = \psi(u)$ where

ψ is a form of degree k not all of whose coefficients are in M . If $Q^* = Q[x_1,\ldots,x_N] = Q[x]$, $\phi(x) \notin M^*$, $\psi(x) \notin M^*$, so $\phi(x)\,\psi(x) \notin M^*$. Since the u_i are analytically independent, $ab = \phi(u)\,\psi(u) \notin M^{h+k+1}$ (by the comment after definition 5.5).

Corollary 6.5: Q is an integral domain.

Proof: If $a \neq 0$, $b \neq 0$, $ab \notin M^s$ for some $s > 0$, so $ab \neq 0$.

Lemma 6.6: Suppose $N \geq 2$. Let $Q' = Q/(u_1)$, $\bar{u}_i \equiv u_i \bmod (u_1)(2 \leq i \leq N)$. Then $(\bar{u}_2,\ldots,\bar{u}_N)$ is a minimal base for M' and $\bar{u}_2,\ldots,\bar{u}_N$ are analytically independent.

Proof: It is obvious that the $\bar{u}_i$, $(2 \leq i \leq N)$ form a mimimal base for M' . Let $\phi'(\bar{u}_2,\ldots,\bar{u}_N) = 0$ where ϕ' is a form of degree s . Let ϕ be the form obtained from ϕ' by replacing each coefficient by a representative in Q . It suffices to show that all the coefficients of ϕ are in M . Assume not. Then $\phi(u_2,\ldots,u_N) \in (u_1)$, say $\phi(u_2,\ldots,u_N) = au_1$; $a \neq 0$ since $\phi(u_2,\ldots,u_N) \notin M^{s+1}$. Let h be such that $a \in M^h$, $a \notin M^{h+1}$, say $a = \psi(u_1,\ldots,u_N)$ where ψ is a form of degree h not all of whose coefficients are in M. $au_1 = u_1\,\psi(u_1,\ldots,u_N) \in M^{h+1}$ but not to M^{h+2} ; so $h + 1 = s$. The form X of degree s defined by $X(x_1,\ldots,x_N) = \phi(x_1,\ldots,x_N) - x_1\psi(x_1,\ldots,x_N)$ is such that not all its coefficients are in M ; hence, since the u_i are analytically independent, $X(u_1,\ldots,u_N) \notin M^{s+1}$. Since $X(u_1,\ldots,u_N) = 0$ this is a contradiction.

Corollary 6.7: The ideals (0), $(u_1),\ldots,(u_1,u_z,\ldots,u_N)$ are all prime.

Proof: (0) is prime by corollary 6.5. By the lemma, $Q/(u_1)$ satisifes the hypotheses on Q, hence is an integral domain and (u_1) is prime.

Inductively, the result is obtained.

Corollary 6.8: Q is regular.

Proof: $\dim Q \leq N$. But by the previous corollary, $\dim Q \geq N$.

Definition 6.9: Let A be a Q-module, $q_1,\ldots,q_p$ a sequence of elements of Q. If q_i all belong to M and for each i, $1 \leq i \leq p$, q_i is not a zero division for ${}^{A}/(q_1,\ldots,q_{i-1})\ A$, then the sequence is said to be a normal A-sequence.

We collect results in

Theorem 6.10: Let Q be a local ring and let $\{u_1,\ldots,u_N\}$ be a minimal set of generators for M. Then

i) Q is regular if and only if the u_i are analytically independent.

ii) If Q is regular, Q is an integral domain.

iii) If Q is regular, $(0) \subset (u_1) \subset \cdots \subset (u_1,\ldots,u_N)$ is a chain of prime ideals and the sequence $u_1,\ldots,u_N$ is a normal Q-sequence.

iv) If Q is regular, ${}^{Q}/(u_1,\ldots,u_1)$ is a regular local ring of dimension $N - i$.

Proof: i) folows from proposition 5.6 and corollary 6.8.

ii) follows from i) and corollary 6.5

iii) follows from corollary 6.7 and the fact that $q \varepsilon Q$, $qu_{i+1} \varepsilon (u_1,\dots,u_i)$ implies $q \varepsilon (u_1,\dots,u_i)$.

iv) Let $Q' = {}^{Q}/(u_1,\dots,u_i)$. By proposition 5.3, $\dim Q' = N - i$; but $M' = (u_1,\dots,u_N)/(u_1,\dots,u_i)$ has a minimal base of $N - i$ elements.

We conclude this section with

Proposition 6.11: Let Q be a regular local ring of dimension one. Let I be a proper ideal in Q . Then there exists $N \geq 0$ such that $I = M^N$.

Proof: M is primcipal, say $M = (u)$. Choose $N \geq 0$ such that $I \subset M^N$, $I \not\subset M^{N+1}$. Let $a \varepsilon I$, $a \notin M^{N+1}$. $a \varepsilon (u^N)$, say $a = gu^N$; $g \notin M$, hence is a unit. Thus $M^N = (u^N) = (a) \subset I \subset M^N$.

We will later show that this result means that Q is a local Dedekind ring.

7. Integral closure; divisor.

Definitions 7.1: If A is a subring of a ring B , an element $x \varepsilon B$ is said to be integral over A if it satisfies a monic polynomial with coefficients in A . The elements of B which are integral over A form a ring which contains A : if x and y are integral over A , x and y are contained in a finitely generated algebra $M \subset B$ over A, say $M = \Sigma Ax_i$. Now $zx_i = \Sigma \lambda_{ij}x_j$, $\Sigma(z \delta_{ij} - \lambda_{ij})x_j = 0$ for $z \in B$, hence $\Delta B = 0$, $\Delta = 0$, where $\Delta = \det(z \delta_{ij} - \lambda_{ij})$. $\Delta = 0$ is an equation of integral dependence for z over A . — The ring so obtained is called the integral closure of A in B . Let B be the full quotient ring of A (the ring of fractions of A with respect to the monoid of non-zero-divisors); A is said to be integrally closed if A is equal to its integral closure in B .

In the remainder of this sections, Λ will denote an integrally closed, Noetherian, commutative ring, R its full quotient ring.

Definition 7.2: A prime ideal P of Λ is called relevant if P is of rank one and contains at least one non zero-divisor.

Theorem 7.3: Let $a \varepsilon \Lambda$ be neither a unit nor a zero divisor. Then (a) is unmixed of rank one and the localization of Λ at P is a regular local ring of dimension one for any P belonging to (a) .

Proof: i) Let P belong to (a) . $(a) \neq (a) : P$ by proposition 2.3. Choose $b \varepsilon (a) : P$, $b \notin (a)$. Let $c = {}^{b}/a \varepsilon R$; $c \notin \Lambda$. $bP \subset (a)$, so $cP \subset \Lambda$. If $cP \subset P$ and $P = (u_1, \ldots, u_N)$, then $cu_i = \sum_j \lambda_{ij} u_j$, $\sum_j (c\ \delta_{ij} - \lambda_{ij}) u_j = 0$, $\Delta P = 0$ where $\Delta = \det\ (c\ \delta_{ij} - \lambda_{ij})$, $\Delta a = 0$, $\Delta = 0$. This means that c is integral over Λ , $c \varepsilon \Lambda$, a contradiction. Hence $cP \not\subset P$. Choose $p \varepsilon P$ such that $d = cp \notin P$. $ad = bp$, $d \notin P$.

ii) We now consider $\pi: \Lambda \longrightarrow \Lambda_p = Q$, the localization of Λ at P . $\ker (\pi)$ is the $(\Lambda - P)$-component of (0) . Let $\pi(a) = a'$, etc. $a'd' = b'p'$, $(a'd') = (b'p') \subset b'M$, where $M = P'$ is the maximal ideal of Q . $d \notin P$, so $d' \notin P'$, hence d' is a unit in Q , $(a') = (a'd') \subset b'M$. Conversely,

$bP \subset (a)$, $b'M \subset (a')$, hence $b'M = (a')$. Choose $m \varepsilon M$ such that $b'm = a'$, $b'M = (b'm)$. We will prove that b' is not a zero divisor in Q , so that $M = (m)$. It suffices to show that b' is not a zero divisor in $\pi(\Lambda)$. Let $b'\lambda' = 0$, $\lambda \varepsilon \Lambda$. Then $b \lambda \varepsilon \ker(\pi)$ so there exists $\gamma \varepsilon \Lambda - P$ with $\gamma b \lambda = 0$. $bp = ad$, $0 = \gamma \lambda bp = \gamma \lambda ad$, $0 = \gamma \lambda d$, since a is not a zero divisor. $d \notin P$, $\gamma \notin P$ so $\gamma d \notin P$, $\lambda \varepsilon \ker(\pi)$, $\lambda' = 0$.

iii) We now have that $M = (m)$. $a \varepsilon P$, $(0): P = (0)$, so by proposition 2.3, P does not belong to (0) . Hence rank $P \geq 1$, dim Q = rank M = rank $P \geq 1$. By theorem 3.8, rank $M \leq 1$. Thus rank $P = 1$, dim Q = rank $M = 1$, and Q is regular.

Corollary 7.4: If P is a relevant prime ideal of Λ , then Λ_p is a regular local ring of dimension one.

Proof: If $b \varepsilon P$ is not a zero divisor , P belongs to (b) .

Corollary 7.5: Let P be a relevant prime ideal of Λ . Then every P-primary ideal is a symbolic prime power of P .

Proof: Let I be P-primary and let $Q = \Lambda_p$, $M = P_p$. $I_p = M^N$ for some $N > 0$ by proposition 6.11. Then $I = I_p \cap \Lambda = M^N \cap \Lambda = P^{(N)}$.

Corollary 7.6: Let $b \varepsilon \Lambda$ be neither a unit nor a zero divisor and let $P_1,\ldots,P_N$ be the prime ideals which belong to (b) . Then the P_i are precisely the relevant prime ideals which contain b , and all of them are minimal prime ideals of (b) . (b) has exactly one reduced primary decomposition and this is of the form $(b) = P_1^{(r_1)} \cap \ldots \cap P_N^{(r_N)}$.

Proof: This follows from proposition 1.4, the theorem, and the previous corollary.

Definition 7.7: By a divisor will be meant a member of the free Abelian group (written additively) generated by the relevant prime ideals of Λ ; that is, if the relevant prime ideals are indexed by a set I , a divisor is a formal sum $\sum_{i \varepsilon I} s_i P_i$, $s_1 \varepsilon Z$, $s_i \neq 0$ for at most a finite number of i . If $s_i \geq 0$ for all $i \varepsilon I$, $\sum_{i \varepsilon I} s_i P_i$ is said to be an integral divisor. If $s_i = 0$ for all i , $\sum_{i \varepsilon I} s_i P_i$ is called the null divisor.

Let $b \varepsilon \Lambda$ be an element which is not a zero divisor and let P be a relevant prime ideal. Define ord $p(b)$ as the symbolic power to which P occurs in the reduced primary decomposition of (b) , where $P^{(0)}$ is defined as Λ so that $\text{ord}_p(b) = 0$ if P does not belong to (b) . Writing $s_i(b) = \text{ord } p_i(b)$, we obtain a unique integral divisor corresponding to b . If $a \varepsilon R$ and is not a zero divisor, say $a = {}^b/c$, define $s_i(a) = s_i(b) - s_i(c)$. This extends the order function to the non-zero divisors of R .

Proposition 7.8: Let a and b be elements of R which are not zero divisors. Then:

i) $\text{ord}_{p_i} a \geq N \geq 0$ if and only if $a \varepsilon P^{(N)}$

ii) $\text{ord}_{p_i} ab = \text{ord}_{p_i} a + \text{ord}_{p_i} b$.

iii) If $a + b$ is not a zero divisor, then

$\text{ord}_{P_i}(a + b) \geq \min(\text{ord}_{P_i} a, \text{ord}_{P_i} b)$ with equality if

$\text{ord}_{P_i} a \neq \text{ord}_{P_i} b$.

Proof: It suffices to prove the proposition for a , $b \in \Lambda$. Let

$Q = \Lambda_p$ have maximal ideal M . Let $\text{ord}_p a = r$, $\text{ord}_p b = s$.

$P^{(r)} = Q(a) \cap \Lambda$ so $Q(a) = M^r$; similarly $Q(b) = M^s$.

i) If $r \geq N$, $a \in P^{(r)} \subset P^{(N)}$; if $a \in P^{(N)}$, $M^r = Q(a) \subset QP^{(N)} = M^N$, and $r \geq N$.

ii) $Q(ab) = Q(a)Q(b) = M^{r+s}$ and the result follows from i).

iii) If $r \leq s$, $P^{(s)} \subseteq P^{(r)}$, $a + b \in P^{(r)} + P^{(s)} = P^{(r)}$ while if $r < s$, $a \notin P^{(r+1)}$, $b \in P^{(s)} \subset P^{(r+1)} \subset P^{(r)}$, and $a + b \in P^{(r)}$, $a + b \notin P^{(r+1)}$; the result follows from i).

Corollary 7.9: Let a and b be non-zero divisors in R with corresponding divisors $\sum_{i \in I} r_i P_i$ and $\sum_{i \in I} s_i P_i$, written $a \Leftrightarrow \sum_{i \in I} r_i P_i$, $b \Leftrightarrow \sum_{i \in I} s_i P_i$. Then

i) $ab \Leftrightarrow \sum_{i \in I} (r_i + s_i)P_i$; $a/b \Leftrightarrow \sum_{i \in I} (r_i - s_i)P_i$.

ii) $a \in \Lambda$ if and only if its divisor is integral.

iii) a and b have the same divisor if and only if a/b is a unit in Λ .

Proof: i) and ii) are obvious. iii) follows from ii) since a/b has null divisor if and only if b/a has, and then both are in Λ .

For the remainder of this section we assume that Λ is an integrally closed Noetherian integral domain, R its field of quotients. The relevant prime ideals are now the minimal non-zero prime ideals

Lemma 7.10: Let I_o be a finite subset of I and let $i \in I - I_o$. Then there exists $b \in \Lambda$ such that $\text{ord}_{p_i} b = 1$, $\text{ord}_{p_j} b = 0$ for all $j \in I_o$.

Proof: Choose $x \in P_i$, $x \notin P_i^{(2)}$. Let $I_o = I_1 + I_2$ where $x \in P_j$ if $j \in I_1$ $x \notin P_k$ if $k \in I_2$. Since $P_j \not\supset P_i^{(2)} \cap (\bigcap_{k \in I_2} P_k)$ if $j \in I_1$ (since all relevant primes are minimal), we may choose $y \in P_i^{(2)} \cap (\bigcap_{k \in I_2} P_k)$ and $y \notin P_j$ for $j \in I_1$. Put $b = x + y$. $b \in P_i + P_i^{(2)} = P_i$ but $b \notin P_i^{(2)}$ so $\text{ord}\, p_i\, b = 1$. If $j \in I_1$, $x \in P_j$ and $y \notin P_j$; if $k \in I_2$, $x \notin P_k$, $y \in P_k$. Thus $b \notin P_j$ if $j \in I_o$, $\text{ord}_{p_j} b = 0$ for all $j \in I_o$.

Theorem 7.11: Let I_o be a finite subset of I and let $s_i \in Z$ be given for each $i \in I_o$. Then there exists $a \in R$ such that $\text{ord}_{p_i} a = s_i$ for $i \in I_o$ and $\text{ord}_{p_i} a \geq 0$ for $j \in I - I_o$.

Proof: For each $i \in I_o$, choose $b_i \in \Lambda$ such that $\text{ord}_{p_i} b_i = 1$, $\text{ord}_{p_j} b_i = 0$ for $j \in I_o - i$. Let $\beta = \prod_{i \in I_o} b_i^{s_i}$. $\text{ord}_{p_i} \beta = s_i$ for all $i \in I_o$. Let $I,$ be a finite subset of $I - I_o$ such that $\text{ord}_{p_k} \beta = 0$ if $k \in I - (I_o + I_1)$. For each $h \in I_1$, choose $c_j \in \Lambda$ such that $\text{ord}_{p_j} c_j = 1$, $\text{ord}_{p_i} c_j = 0$ for $I \in I_o$. Let $\gamma = \prod_{j \in I_1} c_j$. $\gamma \in A$. Consider $\beta\,\gamma^N$ where $N > 0$ is an integer. If $i \in I_o$, $\text{ord}_{p_i} \beta\,\gamma^N = \text{ord}_{p_i} \beta + N\,\text{ord}_{p_j} \gamma = s_i$.

If $j \varepsilon I_1$, $\text{ord}_{p_j} \beta \gamma^N = \text{ord}_{p_j} \beta + N \, \text{ord}_{p_j} \gamma \geq \text{ord}_{p_j} \beta + N \, \text{ord}_{p_j} c_j$, so $\text{ord}_{p_j} \beta \gamma^N \geq \text{ord}_{p_j} \beta + N \geq 0$ for N sufficiently large. If $k \varepsilon I - (I_o + I_1)$, $\text{ord}_{p_k} \beta \gamma^N \geq \text{ord}_{p_k} \beta = 0$. Thus $\alpha = \beta \gamma^N$ has the desired properties if N is sufficiently large.

Note that the proof of the theorem used only the lemma and the fact that any element of R corresponds to a unique divisor. This result will be useful in the study of Dedekind rings.