A Course In Commutative Algebra

Robert B. Ash

Preface

This is a text for a basic course in commutative algebra, written in accordance with the following objectives.

The course should be accessible to those who have studied algebra at the beginning graduate level. For general algebraic background, see my online text "Abstract Algebra: The Basic Graduate Year", which can be downloaded from my web site

www.math.uiuc.edu/~ r-ash

This text will be referred to as TBGY.

The idea is to help the student reach an advanced level as quickly and efficiently as possible. In Chapter 1, the theory of primary decomposition is developed so as to apply to modules as well as ideals. In Chapter 2, integral extensions are treated in detail, including the lying over, going up and going down theorems. The proof of the going down theorem does not require advanced field theory. Valuation rings are studied in Chapter 3, and the characterization theorem for discrete valuation rings is proved. Chapter 4 discusses completion, and covers the Artin-Rees lemma and the Krull intersection theorem. Chapter 5 begins with a brief digression into the calculus of finite differences, which clarifies some of the manipulations involving Hilbert and Hilbert-Samuel polynomials. The main result is the dimension theorem for finitely generated modules over Noetherian local rings. A corollary is Krull's principal ideal theorem. Some connections with algebraic geometry are established via the study of affine algebras. Chapter 6 introduces the fundamental notions of depth, systems of parameters, and M-sequences. Chapter 7 develops enough homological algebra to prove, under approprate hypotheses, that all maximal M-sequences have the same length. The brief Chapter 8 develops enough theory to prove that a regular local ring is an integral domain as well as a Cohen-Macaulay ring. After completing the course, the student should be equipped to meet the Koszul complex, the Auslander-Buchsbaum theorems, and further properties of Cohen-Macaulay rings in a more advanced course.

Bibliography

Atiyah, M.F. and Macdonald, I.G., Introduction to Commtative Algebra, Addison-Wesley 1969

Balcerzyk, S. and Jozefiak, T., Commutative Noetherian and Krull Rings, Wiley 1989

Balcerzyk, S. and Jozefiak, T., Commutative Rings: Dimension, Multiplicity and Homological Methods, Wiley 1989

Eisenbud, D., Commutative Algebra with a view toward algebraic geometry, Springer-Verlag 1995

Gopalakrishnan, N.S., Commutatilve Algebra, Oxonian Press (New Delhi) 1984

Kaplansky, I., Commutative Rings, Allyn and Bacon 1970

Kunz, E., Introduction to Commutative Algebra and Algebraic Geometry, Birkhäuser 1985
Matsumura, H., Commutatlive Ring Theory, Cambridge 1986
Raghavan, S., Singh, B., and Sridharan, S., Homological Methods in Commutative Algebra, Oxford 1975
Serre, J-P., Local Albegra, Springer-Verlag 2000
Sharp, R.Y., Steps in Commutative Algebra, Cambridge 2000

Table of Contents

Chapter 5 Dimension Theory

Chapter 6 Depth

Chapter 7 Homological Methods

Chapter 8 Regular Local Rings

Exercises

Solutions

Chapter 0

Ring Theory Background

We collect here some useful results that might not be covered in a basic graduate algebra course.

0.1 Prime Avoidance

Let $P_1, P_2, \dots, P_s$, $s \geq 2$, be ideals in a ring R, with P_1 and P_2 not necessarily prime, but $P_3, \dots, P_s$ prime (if $s \geq 3$). Let I be any ideal of R. The idea is that if we can avoid the P_j individually, in other words, for each j we can find an element in I but not in P_j, then we can avoid all the P_j simultaneously, that is, we can find a single element in I that is in none of the P_j. We will state and prove the contrapositive.

0.1.1 Prime Avoidance Lemma

With I and the P_i as above, if $I \subseteq \cup_{i=1}^{s} P_i$, then for some i we have $I \subseteq P_i$.

Proof. Suppose the result is false. We may assume that I is not contained in the union of any collection of $s-1$ of the P_i's. (If so, we can simply replace s by $s-1$.) Thus for each i we can find an element $a_i \in I$ with $a_i \notin P_1 \cup \cdots \cup P_{i-1} \cup P_{i+1} \cup \cdots \cup P_s$. By hypothesis, I is contained in the union of all the P's, so $a_i \in P_i$. First assume $s = 2$, with $I \not\subseteq P_1$ and $I \not\subseteq P_2$. Then $a_1 \in P_1$, $a_2 \notin P_1$, so $a_1 + a_2 \notin P_1$. Similarly, $a_1 \notin P_2$, $a_2 \in P_2$, so $a_1 + a_2 \notin P_2$. Thus $a_1 + a_2 \notin I \subseteq P_1 \cup P_2$, contradicting $a_1, a_2 \in I$. Note that P_1 and P_2 need not be prime for this argument to work. Now assume $s > 2$, and observe that $a_1 a_2 \cdots a_{s-1} \in P_1 \cap \cdots \cap P_{s-1}$, but $a_s \notin P_1 \cup \cdots \cup P_{s-1}$. Let $a = (a_1 \cdots a_{s-1}) + a_s$, which does not belong to $P_1 \cup \cdots \cup P_{s-1}$, else a_s would belong to this set. Now for all $i = 1, \dots, s-1$ we have $a_i \notin P_s$, hence $a_1 \cdots a_{s-1} \notin P_s$ because P_s is prime. But $a_s \in P_s$, so a cannot be in P_s. Thus $a \in I$ and $a \notin P_1 \cup \cdots \cup P_s$, contradicting the hypothesis. ♣

It may appear that we only used the primeness of P_s, but after the preliminary reduction (see the beginning of the proof), it may very well happen that one of the other P_i's now occupies the slot that previously housed P_s.

0.2 Jacobson Radicals, Local Rings, and Other Miscellaneous Results

0.2.1 Lemma

Let $J(R)$ be the Jacobson radical of the ring R, that is, the intersection of all maximal ideals of R. Then $a \in J(R)$ iff $1 + ax$ is a unit for every $x \in R$.

Proof. Assume $a \in J(R)$. If $1 + ax$ is not a unit, then it generates a proper ideal, hence $1+ax$ belongs to some maximal ideal $\mathcal{M}$. But then $a \in \mathcal{M}$, hence $ax \in \mathcal{M}$, and therefore $1 \in \mathcal{M}$, a contradiction. Conversely, if a fails to belong to a maximal ideal $\mathcal{M}$, then $\mathcal{M} + Ra = R$. Thus for some $b \in \mathcal{M}$ and $y \in R$ we have $b + ay = 1$. If $x = -y$, then $1 + ax = b \in \mathcal{M}$, so $1 + ax$ cannot be a unit (else $1 \in \mathcal{M}$). ♣

0.2.2 Lemma

Let $\mathcal{M}$ be a maximal ideal of the ring R. Then R is a *local ring* (a ring with a unique maximal ideal, necessarily $\mathcal{M}$) if and only if every element of $1 + \mathcal{M}$ is a unit.

Proof. Suppose R is a local ring, and let $a \in \mathcal{M}$. If $1 + a$ is not a unit, then it must belong to $\mathcal{M}$, which is the ideal of nonunits. But then $1 \in \mathcal{M}$, a contradiction. Conversely, assume that every element of $1+\mathcal{M}$ is a unit. We claim that $\mathcal{M} \subseteq J(R)$, hence $\mathcal{M} = J(R)$. If $a \in \mathcal{M}$, then $ax \in \mathcal{M}$ for every $x \in R$, so $1+ax$ is a unit. By (0.2.1), $a \in J(R)$, proving the claim. If $\mathcal{N}$ is another maximal ideal, then $\mathcal{M} = J(R) \subseteq \mathcal{M} \cap \mathcal{N}$. Thus $\mathcal{M} \subseteq \mathcal{N}$, and since both ideals are maximal, they must be equal. Therefore R is a local ring. ♣

0.2.3 Lemma

Let S be any subset of R, and let I be the ideal generated by S. Then $I = R$ iff for every maximal ideal $\mathcal{M}$, there is an element $x \in S \setminus \mathcal{M}$.

Proof. We have $I \subset R$ iff I, equivalently S, is contained in some maximal ideal $\mathcal{M}$. In other words, $I \subset R$ iff $\exists \mathcal{M}$ such that $\forall x \in S$ we have $x \in \mathcal{M}$. The contrapositive says that $I = R$ iff $\forall \mathcal{M}\ \exists x \in S$ such that $x \notin \mathcal{M}$. ♣

0.2.4 Lemma

Let I and J be ideals of the ring R. Then $I + J = R$ iff $\sqrt{I} + \sqrt{J} = R$.

Proof. The "only if" part holds because any ideal is contained in its radical. Thus assume that $1 = a + b$ with $a^m \in I$ and $b^n \in J$. Then

$$1 = (a + b)^{m+n} = \sum_{i+j=m+n} \binom{m+n}{i} a^i b^j.$$

Now if $i + j = m + n$, then either $i \geq m$ or $j \geq n$. Thus every term in the sum belongs either to I or to J, hence to $I + J$. Consequently, $1 \in I + J$. ♣

0.3 Nakayama's Lemma

First, we give an example of the *determinant trick*; see (2.1.2) for another illustration.

0.3.1 Theorem

Let M be a finitely generated R-module, and I an ideal of R such that $IM = M$. Then there exists $a \in I$ such that $(1+a)M = 0$.

Proof. Let $x_1, \dots, x_n$ generate M. Since $IM = M$, we have equations of the form $x_i = \sum_{j=1}^n a_{ij}x_j$, with $a_{ij} \in I$. The equations may be written as $\sum_{j=1}^n (\delta_{ij} - a_{ij})x_j = 0$. If I_n is the n by n identity matrix, we have $(I_n - A)x = 0$, where $A = (a_{ij})$ and x is a column vector whose coefficients are the x_i. Premultiplying by the adjoint of $(I_n - A)$, we obtain $\Delta x = 0$, where Δ is the determinant of $(I_n - A)$. Thus $\Delta x_i = 0$ for all i, hence $\Delta M = 0$. But if we look at the determinant of $I_n - A$, we see that it is of the form $1 + a$ for some element $a \in I$. ♣

Here is a generalization of a familiar property of linear transformations on finite-dimensional vector spaces.

0.3.2 Theorem

If M is a finitely generated R-module and $f : M \to M$ is a surjective homomorphism, then f is an isomorphism.

Proof. We can make M into an $R[X]$-module via $Xx = f(x)$, $x \in M$. (Thus $X^2x = f(f(x))$, etc.) Let $I = (X)$; we claim that $IM = M$. For if $m \in M$, then by the hypothesis that f is surjective, $m = f(x)$ for some $x \in M$, and therefore $Xx = f(x) = m$. But $X \in I$, so $m \in IM$. By (0.3.1), there exists $g = g(X) \in I$ such that $(1+g)M = 0$. But by definition of I, g must be of the form $Xh(X)$ with $h(X) \in R[X]$. Thus $(1+g)M = [1 + Xh(X)]M = 0$.

We can now prove that f is injective. Suppose that $x \in M$ and $f(x) = 0$. Then

$$0 = [1 + Xh(X)]x = [1 + h(X)X]x = x + h(X)f(x) = x + 0 = x. \quad ♣$$

In (0.3.2), we cannot replace "surjective" by "injective". For example, let $f(x) = nx$ on the integers. If $n \geq 2$, then f is injective but not surjective.

The next result is usually referred to as Nakayama's lemma. Sometimes, Akizuki and Krull are given some credit, and as a result, a popular abbreviation for the lemma is NAK.

0.3.3 NAK

(a) If M is a finitely generated R-module, I an ideal of R contained in the Jacobson radical $J(R)$, and $IM = M$, then $M = 0$.

(b) If N is a submodule of the finitely generated R-module M, I an ideal of R contained in the Jacobson radical $J(R)$, and $M = N + IM$, then $M = N$.

Proof.
(a) By (0.3.1), $(1+a)M = 0$ for some $a \in I$. Since $I \subseteq J(R)$, $1+a$ is a unit by (0.2.1). Multiplying the equation $(1+a)M = 0$ by the inverse of $1+a$, we get $M = 0$.

(b) By hypothesis, $M/N = I(M/N)$, and the result follows from (a). ♣

Here is an application of NAK.

0.3.4 Proposition

Let R be a local ring with maximal ideal J. Let M be a finitely generated R-module, and let $V = M/JM$. Then
(i) V is a finite-dimensional vector space over the *residue field* $k = R/J$.
(ii) If $\{x_1 + JM, \dots, x_n + JM\}$ is a basis for V over k, then $\{x_1, \dots, x_n\}$ is a minimal set of generators for M.
(iii) Any two minimal generating sets for M have the same cardinality.

Proof.
(i) Since J annihilates M/JM, V is a k-module, that is, a vector space over k. Since M is finitely generated over R, V is a finite-dimensional vector space over k.
(ii) Let $N = \sum_{i=1}^n Rx_i$. Since the $x_i + JM$ generate $V = M/JM$, we have $M = N + JM$. By NAK, $M = N$, so the x_i generate M. If a proper subset of the x_i were to generate M, then the corresponding subset of the $x_i + JM$ would generate V, contradicting the assumption that V is n-dimensional.
(iii) A generating set S for M with more than n elements determines a spanning set for V, which must contain a basis with exactly n elements. By (ii), S cannot be minimal. ♣

0.4 Localization

Let S be a subset of the ring R, and assume that S is *multiplicative*, in other words, $0 \notin S$, $1 \in S$, and if a and b belong to S, so does ab. In the case of interest to us, S will be the complement of a prime ideal. We would like to divide elements of R by elements of S to form the *localized ring* $S^{-1}R$, also called the *ring of fractions* of R by S. There is no difficulty when R is an integral domain, because in this case all division takes place in the fraction field of R. We will sketch the general construction for arbitrary rings R. For full details, see TBGY, Section 2.8.

0.4.1 Construction of the Localized Ring

If S is a multiplicative subset of the ring R, we define an equivalence relation on $R \times S$ by $(a,b) \sim (c,d)$ iff for some $s \in S$ we have $s(ad - bc) = 0$. If $a \in R$ and $b \in S$, we define the fraction a/b as the equivalence class of (a,b). We make the set of fractions into a ring in a natural way. The sum of a/b and c/d is defined as $(ad+bc)/bd$, and the product of a/b and c/d is defined as ac/bd. The additive identity is $0/1$, which coincides with $0/s$ for every $s \in S$. The additive inverse of a/b is $-(a/b) = (-a)/b$. The multiplicative identity is $1/1$, which coincides with s/s for every $s \in S$. To summarize:

$S^{-1}R$ is a ring. If R is an integral domain, so is $S^{-1}R$. If R is an integral domain and $S = R \setminus \{0\}$, then $S^{-1}R$ is a field, the *fraction field* of R.

There is a natural ring homomorphism $h : R \to S^{-1}R$ given by $h(a) = a/1$. If S has no zero-divisors, then h is a monomorphism, so R can be embedded in $S^{-1}R$. In particular, a ring R can be embedded in its *full ring of fractions* $S^{-1}R$, where S consists of all non-divisors of 0 in R. An integral domain can be embedded in its fraction field.

Our goal is to study the relation between prime ideals of R and prime ideals of $S^{-1}R$.

0.4.2 Lemma

If X is any subset of R, define $S^{-1}X = \{x/s : x \in X, s \in S\}$. If I is an ideal of R, then $S^{-1}I$ is an ideal of $S^{-1}R$. If J is another ideal of R, then
(i) $S^{-1}(I+J) = S^{-1}I + S^{-1}J$;
(ii) $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$;
(iii) $S^{-1}(I \cap J) = (S^{-1}I) \cap (S^{-1}J)$;
(iv) $S^{-1}I$ is a proper ideal iff $S \cap I = \emptyset$.

Proof. The definitions of addition and multiplication in $S^{-1}R$ imply that $S^{-1}R$ is an ideal, and that in (i), (ii) and (iii), the left side is contained in the right side. The reverse inclusions in (i) and (ii) follow from

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}, \quad \frac{a}{s}\frac{b}{t} = \frac{ab}{st}.$$

To prove (iii), let $a/s = b/t$, where $a \in I,\ b \in J,\ s,t \in S$. There exists $u \in S$ such that $u(at - bs) = 0$. Then $a/s = uat/ust = ubs/ust \in S^{-1}(I \cap J)$.

Finally, if $s \in S \cap I$, then $1/1 = s/s \in S^{-1}I$, so $S^{-1}I = S^{-1}R$. Conversely, if $S^{-1}I = S^{-1}R$, then $1/1 = a/s$ for some $a \in I,\ s \in S$. There exists $t \in S$ such that $t(s-a) = 0$, so $at = st \in S \cap I$. ♣

Ideals in $S^{-1}R$ must be of a special form.

0.4.3 Lemma

Let h be the natural homomorphism from R to $S^{-1}R$ [see (0.4.1)]. If J is an ideal of $S^{-1}R$ and $I = h^{-1}(J)$, then I is an ideal of R and $S^{-1}I = J$.

Proof. I is an ideal by the basic properties of preimages of sets. Let $a/s \in S^{-1}I$, with $a \in I$ and $s \in S$. Then $a/1 = h(a) \in J$, so $a/s = (a/1)(1/s) \in J$. Conversely, let $a/s \in J$, with $a \in R, s \in S$. Then $h(a) = a/1 = (a/s)(s/1) \in J$, so $a \in I$ and $a/s \in S^{-1}I$. ♣

Prime ideals yield sharper results.

0.4.4 Lemma

If I is any ideal of R, then $I \subseteq h^{-1}(S^{-1}I)$. There will be equality if I is prime and disjoint from S.

Proof. If $a \in I$, then $h(a) = a/1 \in S^{-1}I$. Thus assume that I is prime and disjoint from S, and let $a \in h^{-1}(S^{-1}I)$. Then $h(a) = a/1 \in S^{-1}I$, so $a/1 = b/s$ for some $b \in I, s \in S$. There exists $t \in S$ such that $t(as - b) = 0$. Thus $ast = bt \in I$, with $st \notin I$ because $S \cap I = \emptyset$. Since I is prime, we have $a \in I$. ♣

0.4.5 Lemma

If I is a prime ideal of R disjoint from S, then $S^{-1}I$ is a prime ideal of $S^{-1}R$.

Proof. By part (iv) of (0.4.2), $S^{-1}I$ is a proper ideal. Let $(a/s)(b/t) = ab/st \in S^{-1}I$, with $a, b \in R, s, t \in S$. Then $ab/st = c/u$ for some $c \in I, u \in S$. There exists $v \in S$ such that $v(abu - cst) = 0$. Thus $abuv = cstv \in I$, and $uv \notin I$ because $S \cap I = \emptyset$. Since I is prime, $ab \in I$, hence $a \in I$ or $b \in I$. Therefore either a/s or b/t belongs to $S^{-1}I$. ♣

The sequence of lemmas can be assembled to give a precise conclusion.

0.4.6 Theorem

There is a one-to-one correspondence between prime ideals P of R that are disjoint from S and prime ideals Q of $S^{-1}R$, given by

$$P \to S^{-1}P \text{ and } Q \to h^{-1}(Q).$$

Proof. By (0.4.3), $S^{-1}(h^{-1}(Q)) = Q$, and by (0.4.4), $h^{-1}(S^{-1}P) = P$. By (0.4.5), $S^{-1}P$ is a prime ideal, and $h^{-1}(Q)$ is a prime ideal by the basic properties of preimages of sets. If $h^{-1}(Q)$ meets S, then by (0.4.2) part (iv), $Q = S^{-1}(h^{-1}(Q)) = S^{-1}R$, a contradiction. Thus the maps $P \to S^{-1}P$ and $Q \to h^{-1}(Q)$ are inverses of each other, and the result follows. ♣

0.4.7 Definitions and Comments

If P is a prime ideal of R, then $S = R \setminus P$ is a multiplicative set. In this case, we write R_P for $S^{-1}R$, and call it the *localization* of R at P. We are going to show that R_P is a local ring, that is, a ring with a unique maximal ideal. First, we give some conditions equivalent to the definition of a local ring.

0.4.8 Proposition

For a ring R, the following conditions are equivalent.

(i) R is a local ring;
(ii) There is a proper ideal I of R that contains all nonunits of R;
(iii) The set of nonunits of R is an ideal.

Proof.
(i) implies (ii): If a is a nonunit, then (a) is a proper ideal, hence is contained in the unique maximal ideal I.
(ii) implies (iii): If a and b are nonunits, so are $a + b$ and ra. If not, then I contains a unit, so $I = R$, contradicting the hypothesis.
(iii) implies (i): If I is the ideal of nonunits, then I is maximal, because any larger ideal J would have to contain a unit, so $J = R$. If H is any proper ideal, then H cannot contain a unit, so $H \subseteq I$. Therefore I is the unique maximal ideal. ♣

0.4.9 Theorem

R_P is a local ring.

Proof. Let Q be a maximal ideal of R_P. Then Q is prime, so by (0.4.6), $Q = S^{-1}I$ for some prime ideal I of R that is disjoint from $S = R \setminus P$. In other words, $I \subseteq P$. Consequently, $Q = S^{-1}I \subseteq S^{-1}P$. If $S^{-1}P = R_P = S^{-1}R$, then by (0.4.2) part (iv), P is not disjoint from $S = R \setminus P$, which is impossible. Therefore $S^{-1}P$ is a proper ideal containing every maximal ideal, so it must be the unique maximal ideal. ♣

0.4.10 Remark

It is convenient to write the ideal $S^{-1}I$ as IR_P. There is no ambiguity, because the product of an element of I and an arbitrary element of R belongs to I.

0.4.11 Localization of Modules

If M is an R-module and S a multiplicative subset of R, we can essentially repeat the construction of (0.4.1) to form the localization of M by S, and thereby divide elements of M by elements of S. If $x, y \in M$ and $s, t \in S$, we call (x, s) and (y, t) equivalent if for some $u \in S$, we have $u(tx - sy) = 0$. The equivalence class of (x, s) is denoted by x/s, and addition is defined by

$$\frac{x}{s} + \frac{y}{t} = \frac{tx + sy}{st}.$$

If $a/s \in S^{-1}R$ and $x/t \in S^{-1}M$, we define

$$\frac{a}{s}\frac{x}{t} = \frac{ax}{st}.$$

In this way, $S^{-1}M$ becomes an $S^{-1}R$-module. Exactly as in (0.4.2), if M and N are submodules of an R-module L, then

$$S^{-1}(M + N) = S^{-1}M + S^{-1}N \text{ and } S^{-1}(M \cap N) = (S^{-1}M) \cap (S^{-1}N).$$

Chapter 1

Primary Decomposition and Associated Primes

1.1 Primary Submodules and Ideals

1.1.1 Definitions and Comments

If N is a submodule of the R-module M, and $a \in R$, let $\lambda_a : M/N \to M/N$ be multiplication by a. We say that N is a *primary submodule* of M if N is proper and for every a, λ_a is either injective or nilpotent. Injectivity means that for all $x \in M$, we have $ax \in N \Rightarrow x \in N$. Nilpotence means that for some positive integer n, $a^n M \subseteq N$, that is, a^n belongs to the annihilator of M/N, denoted by $\text{ann}(M/N)$. Equivalently, a belongs to the radical of the annihilator of M/N, denoted by $r_M(N)$.

Note that λ_a cannot be both injective and nilpotent. If so, nilpotence gives $a^n M = a(a^{n-1}M) \subseteq N$, and injectivity gives $a^{n-1}M \subseteq N$. Inductively, $M \subseteq N$, so $M = N$, contradicting the assumption that N is proper. Thus if N is a primary submodule of M, then $r_M(N)$ is the set of all $a \in R$ such that λ_a is not injective. Since $r_M(N)$ is the radical of an ideal, it is an ideal of R, and in fact it is a prime ideal. For if λ_a and λ_b fail to be injective, so does $\lambda_{ab} = \lambda_a \circ \lambda_b$. (Note that $r_M(N)$ is proper because λ_1 is injective.) If $P = r_M(N)$, we say that N is *P-primary*.

If I is any ideal of R, then $r_R(I) = \sqrt{I}$, because $\text{ann}(R/I) = I$. (Note that $a \in \text{ann}(R/I)$ iff $aR \subseteq I$ iff $a = a1 \in I$.)

Specializing to $M = R$ and replacing a by y, we define a *primary ideal* in a ring R as a proper ideal Q such that if $xy \in Q$, then either $x \in Q$ or $y^n \in Q$ for some $n \geq 1$. Equivalently, $R/Q \neq 0$ and every zero-divisor in R/Q is nilpotent.

A useful observation is that if P is a prime ideal, then $\sqrt{P^n} = P$ for all $n \geq 1$. (The radical of P^n is the intersection of all prime ideals containing P^n, one of which is P. Thus $\sqrt{P^n} \subseteq P$. Conversely, if $x \in P$, then $x^n \in P^n$, so $x \in \sqrt{P^n}$.)

1.1.2 Lemma

If $\sqrt{I}$ is a maximal ideal $\mathcal{M}$, then I is $\mathcal{M}$-primary.

Proof. Suppose that $ab \in I$ and b does not belong to $\sqrt{I} = \mathcal{M}$. Then by maximality of $\mathcal{M}$, it follows that $\mathcal{M} + Rb = R$, so for some $m \in \mathcal{M}$ and $r \in R$ we have $m + rb = 1$. Now $m \in \mathcal{M} = \sqrt{I}$, hence $m^k \in I$ for some $k \geq 1$. Thus $1 = 1^k = (m + rb)^k = m^k + sb$ for some $s \in R$. Multiply by a to get $a = am^k + sab \in I$. ♣

1.1.3 Corollary

If $\mathcal{M}$ is a maximal ideal, then $\mathcal{M}^n$ is $\mathcal{M}$-primary for every $n \geq 1$.

Proof. As we observed in (1.1.1), $\sqrt{\mathcal{M}^n} = \mathcal{M}$, and the result follows from (1.1.2). ♣

1.2 Primary Decomposition

1.2.1 Definitions and Comments

A *primary decomposition* of the submodule N of M is given by $N = \cap_{i=1}^r N_i$, where the N_i are P_i-primary submodules. The decomposition is *reduced* if the P_i are distinct and N cannot be expressed as the intersection of a proper subcollection of the N_i.

We can always extract a reduced primary decomposition from an unreduced one, by discarding those N_i that contain $\cap_{j \neq i} N_j$ and intersecting those N_i that are P-primary for the same P. The following result justifies this process.

1.2.2 Lemma

If $N_1, \dots, N_k$ are P-primary, then $\cap_{i=1}^k N_i$ is P-primary.

Proof. We may assume that $k = 2$; an induction argument takes care of larger values. Let $N = N_1 \cap N_2$ and $r_M(N_1) = r_M(N_2) = P$. Assume for the moment that $r_M(N) = P$. If $a \in R$, $x \in M, ax \in N$, and $a \notin r_M(N)$, then since N_1 and N_2 are P-primary, we have $x \in N_1 \cap N_2 = N$. It remains to show that $r_M(N) = P$. If $a \in P$, then there are positive integers n_1 and n_2 such that $a^{n_1}M \subseteq N_1$ and $a^{n_2}M \subseteq N_2$. Therefore $a^{n_1+n_2}M \subseteq N$, so $a \in r_M(N)$. Conversely, if $a \in r_M(N)$ then a belongs to $r_M(N_i)$ for $i = 1, 2$, and therefore $a \in P$. ♣

We now prepare to prove that every submodule of a Noetherian module has a primary decomposition.

1.2.3 Definition

The proper submodule N of M is *irreducible* if N cannot be expressed as $N_1 \cap N_2$ with N properly contained in the submodules $N_i, i = 1, 2$.

1.2.4 Proposition

If N is an irreducible submodule of the Noetherian module M, then N is primary.

Proof. If not, then for some $a \in R$, $\lambda_a : M/N \to M/N$ is neither injective nor nilpotent. The chain $\ker \lambda_a \subseteq \ker \lambda_a^2 \subseteq \ker \lambda_a^3 \subseteq \cdots$ terminates by the ascending chain condition, say at $\ker \lambda_a^i$. Let $\varphi = \lambda_a^i$; then $\ker \varphi = \ker \varphi^2$ and we claim that $\ker \varphi \cap \operatorname{im} \varphi = 0$. Suppose $x \in \ker \varphi \cap \operatorname{im} \varphi$, and let $x = \varphi(y)$. Then $0 = \varphi(x) = \varphi^2(y)$, so $y \in \ker \varphi^2 = \ker \varphi$, so $x = \varphi(y) = 0$.

Now λ_a is not injective, so $\ker \varphi \neq 0$, and λ_a is not nilpotent, so λ_a^i can't be 0 (because $a^i M \not\subseteq N$). Consequently, $\operatorname{im} \varphi \neq 0$.

Let $p : M \to M/N$ be the canonical epimorphism, and set $N_1 = p^{-1}(\ker \varphi)$, $N_2 = p^{-1}(\operatorname{im} \varphi)$. We will prove that $N = N_1 \cap N_2$. If $x \in N_1 \cap N_2$, then $p(x)$ belongs to both $\ker \varphi$ and $\operatorname{im} \varphi$, so $p(x) = 0$, in other words, $x \in N$. Conversely, if $x \in N$, then $p(x) = 0 \in \ker \varphi \cap \operatorname{im} \varphi$, so $x \in N_1 \cap N_2$.

Finally, we will show that N is properly contained in both N_1 and N_2, so N is reducible, a contradiction. Choose a nonzero element $y \in \ker \varphi$. Since p is surjective, there exists $x \in M$ such that $p(x) = y$. Thus $x \in p^{-1}(\ker \varphi) = N_1$ (because $y = p(x) \in \ker \varphi$), but $x \notin N$ (because $p(x) = y \neq 0$). Similarly, $N \subset N_2$ (with $0 \neq y \in \operatorname{im} \varphi$), and the result follows. ♣

1.2.5 Theorem

If N is a proper submodule of the Noetherian module M, then N has a primary decomposition, hence a reduced primary decomposition.

Proof. We will show that N can be expressed as a finite intersection of irreducible submodules of M, so that (1.2.4) applies. Let $\mathcal{S}$ be the collection of all submodules of M that cannot be expressed in this form. If $\mathcal{S}$ is nonempty, then $\mathcal{S}$ has a maximal element N (because M is Noetherian). By definition of $\mathcal{S}$, N must be reducible, so we can write $N = N_1 \cap N_2$, $N \subset N_1$, $N \subset N_2$. By maximality of N, N_1 and N_2 can be expressed as finite intersections of irreducible submodules, hence so can N, contradicting $N \in \mathcal{S}$. Thus $\mathcal{S}$ is empty. ♣

1.3 Associated Primes

1.3.1 Definitions and Comments

Let M be an R-module, and P a prime ideal of R. We say that P is an *associated prime* of M (or that P is *associated* to M) if P is the annihilator of some nonzero $x \in M$. The set of associated primes of M is denoted by $\mathrm{AP}(M)$. (The standard notation is Ass(M). Please do not use this regrettable terminology.)

Here is a useful characterization of associated primes.

1.3.2 Proposition

The prime ideal P is associated to M if and only if there is an injective R-module homomorphism from R/P to M. Therefore if N is a submodule of M, then $\mathrm{AP}(N) \subseteq \mathrm{AP}(M)$.

Proof. If P is the annihilator of $x \neq 0$, the desired homomorphism is given by $r+P \to rx$. Conversely, if an injective R-homomorphism from R/P to M exists, let x be the image of $1+P$, which is nonzero in R/P. By injectivity, $x \neq 0$. We will show that $P = \operatorname{ann}_R(x)$, the set of elements $r \in R$ such that $rx = 0$. If $r \in P$, then $r + P = 0$, so $rx = 0$, and therefore $r \in \operatorname{ann}_R(x)$. If $rx = 0$, then by injectivity, $r + P = 0$, so $r \in P$. ♣

Associated primes exist under wide conditions, and are sometimes unique.

1.3.3 Proposition

If $M = 0$, then $\operatorname{AP}(M)$ is empty. The converse holds if R is a Noetherian ring.

Proof. There are no nonzero elements in the zero module, hence no associated primes. Assuming that $M \neq 0$ and R is Noetherian, there is a maximal element $I = \operatorname{ann}_R x$ in the collection of all annihilators of nonzero elements of M. The ideal I must be proper, for if $I = R$, then $x = 1x = 0$, a contradiction. If we can show that I is prime, we have $I \in \operatorname{AP}(M)$, as desired. Let $ab \in I$ with $a \notin I$. Then $abx = 0$ but $ax \neq 0$, so $b \in \operatorname{ann}(ax)$. But $I = \operatorname{ann} x \subseteq \operatorname{ann}(ax)$, and the maximality of I gives $I = \operatorname{ann}(ax)$. Consequently, $b \in I$. ♣

1.3.4 Proposition

For any prime ideal P, $\operatorname{AP}(R/P) = \{P\}$.

Proof. By (1.3.2), P is an associated prime of R/P because there certainly is an R-monomorphism from R/P to itself. If $Q \in \operatorname{AP}(R/P)$, we must show that $Q = P$. Suppose that $Q = \operatorname{ann}(r + P)$ with $r \notin P$. Then $s \in Q$ iff $sr \in P$ iff $s \in P$ (because P is prime). ♣

1.3.5 Remark

Proposition 1.3.4 shows that the annihilator of any nonzero element of R/P is P.

The next result gives us considerable information about the elements that belong to associated primes.

1.3.6 Theorem

Let $z(M)$ be the set of zero-divisors of M, that is, the set of all $r \in R$ such that $rx = 0$ for some nonzero $x \in M$. Then $\cup\{P : P \in \operatorname{AP}(M)\} \subseteq z(M)$, with equality if R is Noetherian.

Proof. The inclusion follows from the definition of associated prime; see (1.3.1). Thus assume $a \in z(M)$, with $ax = 0$, $x \in M$, $x \neq 0$. Then $Rx \neq 0$, so by (1.3.3) [assuming R Noetherian], Rx has an associated prime $P = \operatorname{ann}(bx)$. Since $ax = 0$ we have $abx = 0$, so $a \in P$. But $P \in \operatorname{AP}(Rx) \subseteq \operatorname{AP}(M)$ by (1.3.2). Therefore $a \in \cup\{P : P \in \operatorname{AP}(M)\}$. ♣

Now we prove a companion result to (1.3.2).

1.3.7 Proposition

If N is a submodule of M, then $\mathrm{AP}(M) \subseteq \mathrm{AP}(N) \cup \mathrm{AP}(M/N)$.

Proof. Let $P \in \mathrm{AP}(M)$, and let $h : R/P \to M$ be a monomorphism. Set $H = h(R/P)$ and $L = H \cap N$.
Case 1: $L = 0$. Then the map from H to M/N given by $h(r + P) \to h(r + P) + N$ is a monomorphism. (If $h(r + P)$ belongs to N, it must belong to $H \cap N = 0$.) Thus H is isomorphic to a submodule of M/N, so by definition of H, there is a monomorphism from R/P to M/N. Thus $P \in \mathrm{AP}(M/N)$.
Case 2: $L \neq 0$. If L has a nonzero element x, then x must belong to both H and N, and H is isomorphic to R/P via h. Thus $x \in N$ and the annihilator of x coincides with the annihilator of some nonzero element of R/P. By (1.3.5), $\operatorname{ann} x = P$, so $P \in \mathrm{AP}(N)$. ♣

1.3.8 Corollary

$$\mathrm{AP}(\bigoplus_{j \in J} M_j = \bigcup_{j \in J} \mathrm{AP}(M_j).$$

Proof. By (1.3.2), the right side is contained in the left side. The result follows from (1.3.7) when the index set is finite. For example,

$$\begin{aligned} \mathrm{AP}(M_1 \oplus M_2 \oplus M_3) &\subseteq \mathrm{AP}(M_1) \cup \mathrm{AP}(M/M_1) \\ &= \mathrm{AP}(M_1) \cup \mathrm{AP}(M_2 \oplus M_3) \\ &\subseteq \mathrm{AP}(M_1) \cup \mathrm{AP}(M_2) \cup \mathrm{AP}(M_3). \end{aligned}$$

In general, if P is an associated prime of the direct sum, then there is a monomorphism from R/P to $\oplus M_j$. The image of the monomorphism is contained in the direct sum of finitely many components, as R/P is generated as an R-module by the single element $1 + P$. This takes us back to the finite case. ♣

We now establish the connection between associated primes and primary decomposition, and show that under wide conditions, there are only finitely many associated primes.

1.3.9 Theorem

Let M be a nonzero finitely generated module over the Noetherian ring R, so that by (1.2.5), every proper submodule of M has a reduced primary decomposition. In particular, the zero module can be expressed as $\cap_{i=1}^{r} N_i$, where N_i is P_i-primary. Then $\mathrm{AP}(M) = \{P_1, \dots, P_r\}$, a finite set.

Proof. Let P be an associated prime of M, so that $P = \operatorname{ann}(x),\ x \neq 0,\ x \in M$. Renumber the N_i so that $x \notin N_i$ for $1 \le i \le j$ and $x \in N_i$ for $j + 1 \le i \le r$. Since N_i is P_i-primary, we have $P_i = r_M(N_i)$ (see (1.1.1)). Since P_i is finitely generated, $P_i^{n_i} M \subseteq N_i$ for some $n_i \ge 1$. Therefore

$$(\bigcap_{i=1}^{j} P_i^{n_i})x \ \subseteq\ \bigcap_{i=1}^{r} N_i = (0)$$

so $\cap_{i=1}^{j} P_i^{n_i} \subseteq \operatorname{ann}(x) = P$. (By our renumbering, there is a j rather than an r on the left side of the inclusion.) Since P is prime, $P_i \subseteq P$ for some $i \le j$. We claim that $P_i = P$, so that every associated prime must be one of the P_i. To verify this, let $a \in P$. Then $ax = 0$ and $x \notin N_i$, so λ_a is not injective and therefore must be nilpotent. Consequently, $a \in r_M(N_i) = P_i$, as claimed.

Conversely, we show that each P_i is an associated prime. Without loss of generality, we may take $i = 1$. Since the decomposition is reduced, N_1 does not contain the intersection of the other N_i's, so we can choose $x \in N_2 \cap \cdots \cap N_r$ with $x \notin N_1$. Now N_1 is P_1-primary, so as in the preceding paragraph, for some $n \ge 1$ we have $P_1^n x \subseteq N_1$ but $P_1^{n-1} x \not\subseteq N_1$. (Take $P_1^0 x = Rx$ and recall that $x \notin N_1$.) If we choose $y \in P_1^{n-1} x \setminus N_1$ (hence $y \ne 0$), the proof will be complete upon showing that P_1 is the annihilator of y. We have $P_1 y \subseteq P_1^n x \subseteq N_1$ and $x \in \cap_{i=2}^{r} N_i$, so $P_1^n x \subseteq \cap_{i=2}^{r} N_i$. Thus $P_1 y \subseteq \cap_{i=1}^{r} N_i = (0)$, so $P_1 \subseteq \operatorname{ann} y$. On the other hand, if $a \in R$ and $ay = 0$, then $ay \in N_1$ but $y \notin N_1$, so $\lambda_a : M/N_1 \to M/N_1$ is not injective and is therefore nilpotent. Thus $a \in r_M(N_1) = P_1$. ♣

We can now say something about uniqueness in primary decompositions.

1.3.10 First Uniqueness Theorem

Let M be a finitely generated module over the Noetherian ring R. If $N = \cap_{i=1}^{r} N_i$ is a reduced primary decomposition of the submodule N, and N_i is P_i-primary, $i = 1, \dots, r$, then (regarding M and R as fixed) the P_i are uniquely determined by N.

Proof. By the correspondence theorem, a reduced primary decomposition of (0) in M/N is given by $(0) = \cap_{i=1}^{r} N_i/N$, and N_i/N is P_i-primary, $1 \le i \le r$. By (1.3.9),

$$\operatorname{AP}(M/N) = \{P_1, \dots, P_r\}.$$

But [see (1.3.1)] the associated primes of M/N are determined by N. ♣

1.3.11 Corollary

Let N be a submodule of M (finitely generated over the Noetherian ring R). Then N is P-primary iff $\operatorname{AP}(M/N) = \{P\}$.

Proof. The "only if" part follows from the displayed equation above. Conversely, if P is the only associated prime of M/N, then N coincides with a P-primary submodule N', and hence $N (= N')$ is P-primary. ♣

1.3.12 Definitions and Comments

Let $N = \cap_{i=1}^{r} N_i$ be a reduced primary decomposition, with associated primes $P_1, \dots, P_r$. We say that N_i is an *isolated* (or *minimal*) component if P_i is minimal, that is P_i does not properly contain any P_j, $j \ne i$. Otherwise, N_i is an *embedded* component (see Exercise 5 for an example). Embedded components arise in algebraic geometry in situations where one irreducible algebraic set is properly contained in another.

1.4 Associated Primes and Localization

To get more information about uniqueness in primary decompositions, we need to look at associated primes in localized rings and modules. In this section, S will be a multiplicative subset of the Noetherian ring R, R_S the localization of R by S, and M_S the localization of the R-module M by S. Recall that $P \to P_S = PR_S$ is a bijection of C, the set of prime ideals of R not meeting S, and the set of all prime ideals of R_S.

The set of associated primes of the R-module M will be denoted by $\mathrm{AP}_R(M)$. We need a subscript to distinguish this set from $\mathrm{AP}_{R_S}(M_S)$, the set of associated primes of the R_S-module M_S.

1.4.1 Lemma

Let P be a prime ideal not meeting S. If $P \in \mathrm{AP}_R(M)$, then $P_S = PR_S \in \mathrm{AP}_{R_S}(M_S)$. (By the above discussion, the map $P \to P_S$ is the restriction of a bijection and therefore must be injective.)

Proof. If P is the annihilator of the nonzero element $x \in M$, then P_S is the annihilator of the nonzero element $x/1 \in M_S$. (By (1.3.6), no element of S can be a zero-divisor, so $x/1$ is indeed nonzero.) For if $a \in P$ and $a/s \in P_S$, then $(a/s)(x/1) = ax/s = 0$. Conversely, if $(a/s)(x/1) = 0$, then there exists $t \in S$ such that $tax = 0$, and it follows that $a/s = at/st \in P_S$. ♣

1.4.2 Lemma

The map of (1.4.1) is surjective, hence is a bijection of $\mathrm{AP}_R(M) \cap C$ and $\mathrm{AP}_{R_S}(M_S)$.

Proof. Let P be generated by $a_1, \dots, a_n$. Suppose that P_S is the annihilator of the nonzero element $x/t \in M_S$. Then $(a_i/1)(x/t) = 0,\ 1 \le i \le n$. For each i there exists $s_i \in S$ such that $s_i a_i x = 0$. If s is the product of the s_i, then $sa_i x = 0$ for all i, hence $sax = 0$ for all $a \in P$. Thus $P \subseteq \mathrm{ann}(sx)$. On the other hand, suppose b annihilates sx. Then $(b/1)(x/t) = bsx/st = 0$, so $b/1 \in P_S$, and consequently $b/1 = b'/s'$ for some $b' \in P$ and $s' \in S$. This means that for some $u \in S$ we have $u(bs' - b') = 0$. Now b', hence ub', belongs to P, and therefore so does ubs'. But $us' \notin P$ (because $S \cap P = \emptyset$). We conclude that $b \in P$, so $P = \mathrm{ann}(sx)$. As in (1.4.1), s cannot be a zero-divisor, so $sx \ne 0$ and the proof is complete. ♣

1.4.3 Lemma

Let M be a finitely generated module over the Noetherian ring R, and N a P-primary submodule of M. Let P' be any prime ideal of R, and set $M' = M_{P'},\ N' = N_{P'}$. If $P \not\subseteq P'$, then $N' = M'$.

Proof. By (1.4.1) and (1.4.2), there is a bijection between $\mathrm{AP}_{R_{P'}}(M/N)_{P'}$ (which coincides with $\mathrm{AP}_{R_{P'}}(M'/N')$) and the intersection $\mathrm{AP}_R(M/N) \cap C$, where C is the set of prime ideals contained in P' (in other words, not meeting $S = R \setminus P'$). By (1.3.11), there is only one associated prime of M/N over R, namely P, which is not contained in P' by hypothesis. Thus $\mathrm{AP}_R(M/N) \cap C$ is empty, so by (1.3.3), $M'/N' = 0$, and the result follows. ♣

At the beginning of the proof of (1.4.3), we have taken advantage of the isomorphism between $(M/N)_{P'}$ and M'/N'. The result comes from the exactness of the localization functor. If this is unfamiliar, look ahead to the proof of (1.5.3), where the technique is spelled out. See also TBGY, Section 8.5, Problem 5.

1.4.4 Lemma

In (1.4.3), if $P \subseteq P'$, then $N = f^{-1}(N')$, where f is the natural map from M to M'.

Proof. As in (1.4.3), $\mathrm{AP}_R(M/N) = \{P\}$. Since $P \subseteq P'$, we have $R \setminus P' \subseteq R \setminus P$. By (1.3.6), $R \setminus P'$ contains no zero-divisors of M/N, because all such zero-divisors belong to P. Thus the natural map $g : x \to x/1$ of M/N to $(M/N)_{P'} \cong M'/N'$ is injective. (If $x/1 = 0$, then $sx = 0$ for some $s \in S = R \setminus P'$, and since s is not a zero-divisor, we have $x = 0$.)

If $x \in N$, then $f(x) \in N'$ by definition of f, so assume $x \in f^{-1}(N')$. Then $f(x) \in N'$, so $f(x)+N'$ is 0 in M'/N'. By injectivity of g, $x+N$ is 0 in M/N, in other words, $x \in N$, and the result follows. ♣

1.4.5 Second Uniqueness Theorem

Let M be a finitely generated module over the Noetherian ring R. Suppose that $N = \cap_{i=1}^r N_i$ is a reduced primary decomposition of the submodule N, and N_i is P_i-primary, $i = 1, \dots, r$. If P_i is minimal, then (regarding M and R as fixed) N_i is uniquely determined by N.

Proof. Suppose that P_1 is minimal, so that $P_1 \not\supseteq P_i$, $i > 1$. By (1.4.3) with $P = P_i$, $P' = P_1$, we have $(N_i)_{P_1} = M_{P_1}$ for $i > 1$. By (1.4.4) with $P = P' = P_1$, we have $N_1 = f^{-1}[(N_1)_{P_1}]$, where f is the natural map from M to M_{P_1}. Now

$$N_{P_1} = (N_1)_{P_1} \cap \cap_{i=2}^r (N_i)_{P_1} = (N_1)_{P_1} \cap M_{P_1} = (N_1)_{P_1}.$$

Thus $N_1 = f^{-1}[(N_1)_{P_1}] = f^{-1}(N_{P_1})$ depends only on N and P_1, and since P_1 depends on the fixed ring R, it follows that N_1 depends only on N. ♣

1.5 The Support of a Module

The support of a module M is closely related to the set of associated primes of M. We will need the following result in order to proceed.

1.5.1 Proposition

M is the zero module if and only if $M_P = 0$ for every prime ideal P, if and only if $M_{\mathcal{M}} = 0$ for every maximal ideal $\mathcal{M}$.

Proof. It suffices to show that if $M_{\mathcal{M}} = 0$ for all maximal ideals $\mathcal{M}$, then $M = 0$. Choose a nonzero element $x \in M$, and let I be the annihilator of x. Then $1 \notin I$ (because $1x = x \neq 0$), so I is a proper ideal and is therefore contained in a maximal ideal $\mathcal{M}$. By hypothesis, $x/1$ is 0 in $M_{\mathcal{M}}$, hence there exists $a \notin \mathcal{M}$ (so $a \notin I$) such that $ax = 0$. But then by definition of I we have $a \in I$, a contradiction. ♣

1.5.2 Definitions and Comments

The *support* of an R-module M (notation $\operatorname{Supp} M$) is the set of prime ideals P of R such that $M_P \neq 0$. Thus $\operatorname{Supp} M = \emptyset$ iff $M_P = 0$ for all prime ideals P. By (1.5.1), this is equivalent to $M = 0$.

If I is any ideal of R, we define $V(I)$ as the set of prime ideals containing I. In algebraic geometry, the *Zariski topology* on $\operatorname{Spec} R$ has the sets $V(I)$ as its closed sets.

1.5.3 Proposition

$\operatorname{Supp} R/I = V(I)$.

Proof. We apply the localization functor to the exact sequence $0 \to I \to R \to R/I \to 0$ to get the exact sequence $0 \to I_P \to R_P \to (R/I)_P \to 0$. Consequently, $(R/I)_P \cong R_P/I_P$. Thus $P \in \operatorname{Supp} R/I$ iff $R_P \supset I_P$ iff I_P is contained in a maximal ideal, necessarily PR_P. But this is equivalent to $I \subseteq P$. To see this, suppose $a \in I$, with $a/1 \in I_P \subseteq PR_P$. Then $a/1 = b/s$ for some $b \in P$, $s \notin P$. There exists $c \notin P$ such that $c(as - b) = 0$. We have $cas = cb \in P$, a prime ideal, and $cs \notin P$. We conclude that $a \in P$. ♣

1.5.4 Proposition

Let $0 \to M' \to M \to M'' \to 0$ be exact, hence $0 \to M'_P \to M_P \to M''_P \to 0$ is exact. Then

$$\operatorname{Supp} M = \operatorname{Supp} M' \cup \operatorname{Supp} M''.$$

Proof. Let P belong to $\operatorname{Supp} M \setminus \operatorname{Supp} M'$. Then $M'_P = 0$, so the map $M_P \to M''_P$ is injective as well as surjective, hence is an isomorphism. But $M_P \neq 0$ by assumption, so $M''_P \neq 0$, and therefore $P \in \operatorname{Supp} M''$. On the other hand, since M'_P is isomorphic to a submodule of M_P, it follows that $\operatorname{Supp} M' \subseteq \operatorname{Supp} M$. If $M_P = 0$, then $M''_P = 0$ (because $M_P \to M''_P$ is surjective). Thus $\operatorname{Supp} M'' \subseteq \operatorname{Supp} M$. ♣

Supports and annihilators are connected by the following basic result.

1.5.5 Theorem

If M is a finitely generated R-module, then $\operatorname{Supp} M = V(\operatorname{ann} M)$.

Proof. Let $M = Rx_1 + \cdots + Rx_n$, so that $M_P = (Rx_1)_P + \cdots + (Rx_n)_P$. Then $\operatorname{Supp} M = \cup_{i=1}^n \operatorname{Supp} Rx_i$, and by the first isomorphism theorem, $Rx_i \cong R/\operatorname{ann} x_i$. By (1.5.3), $\operatorname{Supp} Rx_i = V(\operatorname{ann} x_i)$. Therefore $\operatorname{Supp} M = \cup_{i=1}^n V(\operatorname{ann} x_i) = V(\operatorname{ann} M)$. To justify the last equality, note that if $P \in V(\operatorname{ann} x_i)$, then $P \supseteq \operatorname{ann} x_i \supseteq \operatorname{ann} M$. Conversely, if $P \supseteq \operatorname{ann} M = \cap_{i=1}^n \operatorname{ann} x_i$, then $P \supseteq \operatorname{ann} x_i$ for some i. ♣

And now we connect associated primes and annihilators.

1.5.6 Proposition

If M is a finitely generated module over the Noetherian ring R, then

$$\bigcap_{P\in \mathrm{AP}(M)} P = \sqrt{\operatorname{ann} M}.$$

Proof. If $M = 0$, then by (1.3.3), $\mathrm{AP}(M) = \emptyset$, and the result to be proved is $R = R$. Thus assume $M \neq 0$, so that (0) is a proper submodule. By (1.2.5) and (1.3.9), there is a reduced primary decomposition $(0) = \cap_{i=1}^{r} N_i$, where for each i, N_i is P_i-primary and $\mathrm{AP}(M) = \{P_1, \dots , P_r\}$.

If $a \in \sqrt{\operatorname{ann} M}$, then for some $n \geq 1$ we have $a^n M = 0$. Thus for each i, $\lambda_a : M/N_i \to M/N_i$ is nilpotent [see (1.1.1)]. Consequently, $a \in \cap_{i=1}^{r} r_M(N_i) = \cap_{i=1}^{r} P_i$. Conversely, if a belongs to this intersection, then for all i there exists $n_i \geq 1$ such that $a^{n_i} M \subseteq N_i$. If $n = \max n_i$, then $a^n M = 0$, so $a \in \sqrt{\operatorname{ann} M}$. ♣

1.5.7 Corollary

If R is a Noetherian ring, then the nilradical of R is the intersection of all associated primes of R.

Proof. Take $M = R$ in (1.5.6). Since $\operatorname{ann} R = 0$, $\sqrt{\operatorname{ann} R}$ is the nilradical. ♣

And now, a connection between supports, associated primes and annihilators.

1.5.8 Proposition

Let M be a finitely generated module over the Noetherian ring R, and let P be any prime ideal of R. The following conditions are equivalent:

(1) $P \in \operatorname{Supp} M$;
(2) $P \supseteq P'$ for some $P' \in \mathrm{AP}(M)$;
(3) $P \supseteq \operatorname{ann} M$.

Proof. Conditions (1) and (3) are equivalent by (1.5.5). To prove that (1) implies (2), let $P \in \operatorname{Supp} M$. If P does not contain any associated prime of M, then P does not contain the intersection of all associated primes (because P is prime). By (1.5.6), P does not contain $\sqrt{\operatorname{ann} M}$, hence P cannot contain the smaller ideal $\operatorname{ann} M$. This contradicts (1.5.5). To prove that (2) implies (3), let Q be the intersection of all associated primes. Then $P \supseteq P' \supseteq Q =$ [by (1.5.6)] $\sqrt{\operatorname{ann} M} \supseteq \operatorname{ann} M$. ♣

Here is the most important connection between supports and associated primes.

1.5.9 Theorem

Let M be a finitely generated module over the Noetherian ring R. Then $\mathrm{AP}(M) \subseteq \operatorname{Supp} M$, and the minimal elements of $\mathrm{AP}(M)$ and $\operatorname{Supp} M$ are the same.

Proof. We have $\mathrm{AP}(M) \subseteq \operatorname{Supp} M$ by (2) implies (1) in (1.5.8), with $P = P'$. If P is minimal in $\operatorname{Supp} M$, then by (1) implies (2) in (1.5.8), P contains some $P' \in \mathrm{AP}(M) \subseteq$

Supp M. By minimality, $P = P'$. Thus $P \in \mathrm{AP}(M)$, and in fact, P must be a minimal associated prime. Otherwise, $P \supset Q \in \mathrm{AP}(M) \subseteq \operatorname{Supp} M$, so that P is not minimal in $\operatorname{Supp} M$, a contradiction. Finally, let P be minimal among associated primes but not minimal in $\operatorname{Supp} M$. If $P \supset Q \in \operatorname{Supp} M$, then by (1) implies (2) in (1.5.8), $Q \supseteq P' \in \mathrm{AP}(M)$. By minimality, $P = P'$, contradicting $P \supset Q \supseteq P'$. ♣

Here is another way to show that there are only finitely many associated primes.

1.5.10 Theorem

Let M be a nonzero finitely generated module over the Noetherian ring R. Then there is a chain of submodules $0 = M_0 < M_1 < \cdots < M_n = M$ such that for each $j = 1, \dots, n$, $M_j/M_{j-1} \cong R/P_j$, where the P_j are prime ideals of R. For any such chain, $\mathrm{AP}(M) \subseteq \{P_1, \dots, P_n\}$.

Proof. By (1.3.3), M has an associated prime $P_1 = \operatorname{ann} x_1$, with x_1 a nonzero element of M. Take $M_1 = Rx_1 \cong R/P_1$ (apply the first isomorphism theorem). If $M \neq M_1$, then the quotient module M/M_1 is nonzero, hence [again by (1.3.3)] has an associated prime $P_2 = \operatorname{ann}(x_2 + M_1)$, $x_2 \notin M_1$. Let $M_2 = M_1 + Rx_2$. Now map R onto M_2/M_1 by $r \to rx_2 + M_1$. By the first isomorphism theorem, $M_2/M_1 \cong R/P_2$. Continue inductively to produce the desired chain. (Since M is Noetherian, the process terminates in a finite number of steps.) For each $j = 1, \dots, n$, we have $\mathrm{AP}(M_j) \subseteq \mathrm{AP}(M_{j-1}) \cup \{P_j\}$ by (1.3.4) and (1.3.7). Another inductive argument shows that $\mathrm{AP}(M) \subseteq \{P_1, \dots, P_n\}$. ♣

1.5.11 Proposition

In (1.5.10), each P_j belongs to $\operatorname{Supp} M$. Thus (replacing $\mathrm{AP}(M)$ by $\{P_1, \dots, P_n\}$ in the proof of (1.5.9)), the minimal elements of all three sets $\mathrm{AP}(M)$, $\{P_1, \dots, P_n\}$ and $\operatorname{Supp} M$ are the same.

Proof. By (1.3.4) and (1.5.9), $P_j \in \operatorname{Supp} R/P_j$, so by (1.5.10), $P_j \in \operatorname{Supp} M_j/M_{j-1}$. By (1.5.4), $\operatorname{Supp} M_j/M_{j-1} \subseteq \operatorname{Supp} M_j$, and finally $\operatorname{Supp} M_j \subseteq \operatorname{Supp} M$ because $M_j \subseteq M$. ♣

1.6 Artinian Rings

1.6.1 Definitions and Comments

Recall that an R-module is Artinian if it satisfies the descending chain condition on submodules. If the ring R is Artinian as a module over itself, in other words, R satisfies the dcc on ideals, then R is said to be an *Artinian ring*. Note that $\mathbb{Z}$ is a Noetherian ring that is not Artinian. Any finite ring, for example $\mathbb{Z}_n$, is both Noetherian and Artinian, and in fact we will prove later in the section that an Artinian ring must be Noetherian. The theory of associated primes and supports will help us to analyze Artinian rings.

1.6.2 Lemma

If I is an ideal in the Artinian ring R, then R/I is an Artinian ring.

Proof. Since R/I is a quotient of an Artinian R-module, it is also an Artinian R-module. In fact it is an R/I module via $(r+I)(x+I) = rx + I$, and the R-submodules are identical to the R/I-submodules. Thus R/I is an Artinian R/I-module, in other words, an Artinian ring. ♣

1.6.3 Lemma

An Artinian integral domain is a field.

Proof. Let a be a nonzero element of the Artinian domain R. We must produce a multiplicative inverse of a. The chain of ideals $(a) \supseteq (a^2) \supseteq (a^3) \supseteq \cdots$ stabilizes, so for some t we have $(a^t) = (a^{t+1})$. If $a^t = ba^{t+1}$, then since R is a domain, $ba = 1$. ♣

1.6.4 Proposition

If R is an Artinian ring, then every prime ideal of R is maximal. Therefore, the nilradical $N(R)$ coincides with the Jacobson radical $J(R)$.

Proof. Let P be a prime ideal of R, so that R/I is an integral domain, Artinian by (1.6.2). By (1.6.3), R/P is a field, hence P is maximal. ♣

One gets the impression that the Artinian property puts strong constraints on a ring. The following two results reinforce this conclusion.

1.6.5 Proposition

An Artinian ring has only finitely many maximal ideals.

Proof. Let Σ be the collection of all finite intersections of maximal ideals. Then Σ is nonempty and has a minimal element $I = \mathcal{M}_1 \cap \cdots \cap \mathcal{M}_r$ (by the Artinian property). If $\mathcal{M}$ is any maximal ideal, then $\mathcal{M} \supseteq \mathcal{M} \cap I \in \Sigma$, so by minimality of I we have $\mathcal{M} \cap I = I$. But then $\mathcal{M}$ must contain one of the $\mathcal{M}_i$ (because $\mathcal{M}$ is prime), hence $\mathcal{M} = \mathcal{M}_i$ (because $\mathcal{M}$ and $\mathcal{M}_i$ are maximal). ♣

1.6.6 Proposition

If R is Artinian, then the nilradical $N(R)$ is nilpotent, hence by (1.6.4), the Jacobson radical $J(R)$ is nilpotent.

Proof. Let $I = N(R)$. The chain $I \supseteq I^2 \supseteq I^3 \supseteq \cdots$ stabilizes, so for some i we have $I^i = I^{i+1} = \cdots = L$. If $L = 0$ we are finished, so assume $L \neq 0$. Let Σ be the collection of all ideals K of R such that $KL \neq 0$. Then Σ is nonempty, since L (as well as R) belongs to Σ. Let K_0 be a minimal element of Σ, and choose $a \in K_0$ such that $aL \neq 0$. Then $Ra \subseteq K_0$ (because K_0 is an ideal), and $RaL = aL \neq 0$, hence $Ra \in \Sigma$. By minimality of K_0 we have $Ra = K_0$.

We will show that the principal ideal $(a) = Ra$ coincides with aL. We have $aL \subseteq Ra = K_0$, and $(aL)L = aL^2 = aL \neq 0$, so $aL \in \Sigma$. By minimality of K_0 we have $aL = K_0 = Ra$.

From $(a) = aL$ we get $a = ab$ for some $b \in L \subseteq N(R)$, so $b^n = 0$ for some $n \geq 1$. Therefore $a = ab = (ab)b = ab^2 = \cdots = ab^n = 0$, contradicting our choice of a. Since the assumption $L \neq 0$ has led to a contradiction, we must have $L = 0$. But L is a power of the nilradical I, and the result follows. ♣

We now prove a fundamental structure theorem for Artinian rings.

1.6.7 Theorem

Every Artinian ring R is isomorphic to a finite direct product of Artinian local rings R_i.

Proof. By (1.6.5), R has only finitely many maximal ideals $\mathcal{M}_1, \dots, \mathcal{M}_r$. The intersection of the $\mathcal{M}_i$ is the Jacobson radical $J(R)$, which is nilpotent by (1.6.6). By the Chinese remainder theorem, the intersection of the $\mathcal{M}_i$ coincides with their product. Thus for some $k \geq 1$ we have $(\prod_1^r \mathcal{M}_i)^k = \prod_1^r \mathcal{M}_i^k = 0$. Powers of the $\mathcal{M}_i$ still satisfy the hypothesis of the Chinese remainder theorem, so the natural map from R to $\prod_1^r R/\mathcal{M}_i^k$ is an isomorphism. By (1.6.2), $R/\mathcal{M}_i^k$ is Artinian, and we must show that it is local. A maximal ideal of $R/\mathcal{M}_i^k$ corresponds to a maximal ideal $\mathcal{M}$ of R with $\mathcal{M} \supseteq \mathcal{M}_i^k$, hence $\mathcal{M} \supseteq \mathcal{M}_i$ (because $\mathcal{M}$ is prime). By maximality, $\mathcal{M} = \mathcal{M}_i$. Thus the unique maximal ideal of $R/\mathcal{M}_i^k$ is $\mathcal{M}_i/\mathcal{M}_i^k$. ♣

1.6.8 Remarks

A finite direct product of Artinian rings, in particular, a finite direct product of fields, is Artinian. To see this, project a descending chain of ideals onto one of the coordinate rings. At some point, all projections will stabilize, so the original chain will stabilize. A sequence of exercises will establish the uniqueness of the Artinian local rings in the decomposition (1.6.7).

It is a standard result that an R-module M has finite length $l_R(M)$ if and only if M is both Artinian and Noetherian. We can relate this condition to associated primes and supports.

1.6.9 Proposition

Let M be a finitely generated module over the Noetherian ring R. The following conditions are equivalent:
(1) $l_R(M) < \infty$;
(2) Every associated prime ideal of M is maximal;
(3) Every prime ideal in the support of M is maximal.

Proof.
(1) $\Rightarrow$ (2): As in (1.5.10), there is a chain of submodules $0 = M_0 < \cdots < M_n = M$, with $M_i/M_{i-1} \cong R/P_i$. Since M_i/M_{i-1} is a submodule of a quotient M/M_{i-1} of M, the hypothesis (1) implies that R/P_i has finite length for all i. Thus R/P_i is an Artinian R-module, hence an Artinian R/P_i-module (note that P_i annihilates R/P_i). In other words, R/P_i is an Artinian ring. But P_i is prime, so R/P_i is an integral domain, hence a field by (1.6.3). Therefore each P_i is a maximal ideal. Since every associated prime is one of the P_i's [see (1.5.10)], the result follows.

(2) $\Rightarrow$ (3): If $P \in \operatorname{Supp} M$, then by (1.5.8), P contains some associated prime Q. By hypothesis, Q is maximal, hence so is P.

(3) $\Rightarrow$ (1): By (1.5.11) and the hypothesis (3), every P_i is maximal, so R/P_i is a field. Consequently, $l_R(M_i/M_{i-1}) = l_R(R/P_i) = 1$ for all i. But length is additive, that is, if N is a submodule of M, then $l(M) = l(N) + l(M/N)$. Summing on i from 1 to n, we get $l_R(M) = n < \infty$. ♣

1.6.10 Corollary

Let M be finitely generated over the Noetherian ring R. If $l_R(M) < \infty$, then $\operatorname{AP}(M) = \operatorname{Supp} M$.

Proof. By (1.5.9), $\operatorname{AP}(M) \subseteq \operatorname{Supp} M$, so let $P \in \operatorname{Supp} M$. By (1.5.8), $P \supseteq P'$ for some $P' \in \operatorname{AP}(M)$. By (1.6.9), P and P' are both maximal, so $P = P' \in \operatorname{AP}(M)$. ♣

We can now characterize Artinian rings in several ways.

1.6.11 Theorem

Let R be a Noetherian ring. The following conditions are equivalent:
(1) R is Artinian;
(2) Every prime ideal of R is maximal;
(3) Every associated prime ideal of R is maximal.

Proof. (1) implies (2) by (1.6.4), and (2) implies (3) is immediate. To prove that (3) implies (1), note that by (1.6.9), $l_R(R) < \infty$, hence R is Artinian. ♣

1.6.12 Theorem

The ring R is Artinian if and only if $l_R(R) < \infty$.

Proof. The "if" part follows because any module of finite length is Artinian and Noetherian. Thus assume R Artinian. As in (1.6.7), the zero ideal is a finite product $\mathcal{M}_1 \cdots \mathcal{M}_k$ of not necessarily distinct maximal ideals. Now consider the chain

$$R = \mathcal{M}_0 \supseteq \mathcal{M}_1 \supseteq \mathcal{M}_1\mathcal{M}_2 \supseteq \cdots \supseteq \mathcal{M}_1 \cdots \mathcal{M}_{k-1} \supseteq \mathcal{M}_1 \cdots \mathcal{M}_k = 0.$$

Since any submodule or quotient module of an Artinian module is Artinian, it follows that $T_i = \mathcal{M}_1 \cdots \mathcal{M}_{i-1}/\mathcal{M}_1 \cdots \mathcal{M}_i$ is an Artinian R-module, hence an Artinian $R/\mathcal{M}_i$-module. (Note that $\mathcal{M}_i$ annihilates $\mathcal{M}_1 \cdots \mathcal{M}_{i-1}/\mathcal{M}_1 \cdots \mathcal{M}_i$.) Thus T_i is a vector space over the field $R/\mathcal{M}_i$, and this vector space is finite-dimensional by the descending chain condition. Thus T_i has finite length as an $R/\mathcal{M}_i$-module, hence as an R-module. By additivity of length [as in (3) implies (1) in (1.6.9)], we conclude that $l_R(R) < \infty$. ♣

1.6.13 Theorem

The ring R is Artinian if and only if R is Noetherian and every prime ideal of R is maximal.

Proof. The "if" part follows from (1.6.11). If R is Artinian, then $l_R(R) < \infty$ by (1.6.12), hence R is Noetherian. By (1.6.4) or (1.6.11), every prime ideal of R is maximal. ♣

1.6.14 Corollary

Let M be finitely generated over the Artinian ring R. Then $l_R(M) < \infty$.

Proof. By (1.6.13), R is Noetherian, hence the module M is both Artinian and Noetherian. Consequently, M has finite length. ♣

Chapter 2

Integral Extensions

2.1 Integral Elements

2.1.1 Definitions and Comments

Let R be a subring of the ring S, and let $\alpha \in S$. We say that α is *integral* over R if α is a root of a *monic* polynomial with coefficients in R. If R is a field and S an extension field of R, then α is integral over R iff α is algebraic over R, so we are generalizing a familiar notion. If α is a complex number that is integral over $\mathbb{Z}$, then α is said to be an *algebraic integer* For example, if d is any integer, then $\sqrt{d}$ is an algebraic integer, because it is a root of $x^2 - d$. Notice that $2/3$ is a root of the polynomial $f(x) = 3x - 2$, but f is not monic, so we cannot conclude that $2/3$ is an algebraic integer. In a first course in algebraic number theory, one proves that a rational number that is an algebraic integer must belong to $\mathbb{Z}$, so $2/3$ is not an algebraic integer.

There are several conditions equivalent to integrality of α over R, and a key step is the following result, sometimes called the *determinant trick*.

2.1.2 Lemma

Let R, S and α be as above, and recall that a module is *faithful* if its annihilator is 0. Let M be a finitely generated R-module that is faithful as an $R[\alpha]$-module. Let I be an ideal of R such that $\alpha M \subseteq IM$. Then α is a root of a monic polynomial with coefficients in I.

Proof. let $x_1, \dots, x_n$ generate M over R. Then $\alpha x_i \in IM$, so we may write $\alpha x_i = \sum_{j=1}^n c_{ij} x_j$ with $c_{ij} \in I$. Thus

$$\sum_{j=1}^{n} (\delta_{ij}\alpha - c_{ij})x_j = 0, \ 1 \leq i \leq n.$$

In matrix form, we have $Ax = 0$, where A is a matrix with entries $\alpha - c_{ii}$ on the main diagonal, and $-c_{ij}$ elsewhere. Multiplying on the left by the adjoint matrix, we get $\Delta x_i = 0$ for all i, where Δ is the determinant of A. But then Δ annihilates all of M, so $\Delta = 0$. Expanding the determinant yields the desired monic polynomial. ♣

2.1.3 Remark

If $\alpha M \subseteq IM$, then in particular, α *stabilizes* M, in other words, $\alpha M \subseteq M$.

2.1.4 Theorem

Let R be a subring of S, with $\alpha \in S$. The following conditions are equivalent:
(1) α is integral over R;
(2) $R[\alpha]$ is a finitely generated R-module;
(3) $R[\alpha]$ is contained in a subring R' of S that is a finitely generated R-module;
(4) There is a faithful $R[\alpha]$-module M that is finitely generated as an R-module.

Proof.
(1) implies (2): If α is a root of a monic polynomial over R of degree n, then α^n and all higher powers of α can be expressed as linear combinations of lower powers of α. Thus $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ generate $R[\alpha]$ over R.

(2) implies (3): Take $R' = R[\alpha]$.

(3) implies (4): Take $M = R'$. If $y \in R[\alpha]$ and $yM = 0$, then $y = y1 = 0$.

(4) implies (1): Apply (2.1.2) with $I = R$. ♣

We are going to prove a transitivity property for integral extensions, and the following result will be helpful.

2.1.5 Lemma

Let R be a subring of S, with $\alpha_1, \dots, \alpha_n \in S$. If α_1 is integral over R, α_2 is integral over $R[\alpha_1], \dots,$ and α_n is integral over $R[\alpha_1, \dots, \alpha_{n-1}]$, then $R[\alpha_1, \dots, \alpha_n]$ is a finitely generated R-module.

Proof. The $n = 1$ case follows from (2.1.4), part (2). Going from $n-1$ to n amounts to proving that if A, B and C are rings, with C a finitely generated B-module and B a finitely generated A-module, then C is a finitely generated A-module. This follows by a brief computation:

$$C = \sum_{j=1}^{r} By_j, \; B = \sum_{k=1}^{s} Ax_k, \text{ so } C = \sum_{j=1}^{r}\sum_{k=1}^{s} Ay_jx_k. \; ♣$$

2.1.6 Transitivity of Integral Extensions

Let A, B and C be subrings of R. If C is integral over B, that is, every element of C is integral over B, and B is integral over A, then C is integral over A.

Proof. Let $x \in C$, with $x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0 = 0$. Then x is integral over $A[b_0, \dots, b_{n-1}]$. Each b_i is integral over A, hence over $A[b_0, \dots, b_{i-1}]$. By (2.1.5), $A[b_0, \dots, b_{n-1}, x]$ is a finitely generated A-module. By (2.1.4), part (3), x is integral over A. ♣

2.1.7 Definitions and Comments

If R is a subring of S, the *integral closure* of R in S is the set R_c of elements of S that are integral over R. Note that $R \subseteq R_c$ because each $a \in R$ is a root of $x - a$. We say that R is *integrally closed* in S if $R_c = R$. If we simply say that R is *integrally closed* without reference to S, we assume that R is an integral domain with fraction field K, and R is integrally closed in K.

If the elements x and y of S are integral over R, then just as in the proof of (2.1.6), it follows from (2.1.5) that $R[x, y]$ is a finitely generated R-module. Since $x + y, x - y$ and xy belong to this module, they are integral over R by (2.1.4), part (3). The important conclusion is that

$$R_c \text{ is a subring of } S \text{ containing } R.$$

If we take the integral closure of the integral closure, we get nothing new.

2.1.8 Proposition

The integral closure R_c of R in S is integrally closed in S.

Proof. By definition, $R_c \subseteq (R_c)_c$. Thus let $x \in (R_c)_c$, so that x is integral over R_c. As in the proof of (2.1.6), x is integral over R. Thus $x \in R_c$. ♣

We can identify a large class of integrally closed rings.

2.1.9 Proposition

If R is a UFD, then R is integrally closed.

Proof. Let x belong to the fraction field K of R. Write $x = a/b$ where $a, b \in R$ and a and b are relatively prime. If x is integral over R, there is an equation of the form

$$(a/b)^n + a_{n-1}(a/b)^{n-1} + \cdots + a_1(a/b) + a_0 = 0$$

with $a_i \in R$. Multiplying by b^n, we have $a^n + bc = 0$, with $c \in R$. Thus b divides a^n, which cannot happen for relatively prime a and b unless b has no prime factors at all, in other words, b is a unit. But then $x = ab^{-1} \in R$. ♣

A domain that is an integral extension of a field must be a field, as the next result shows.

2.1.10 Proposition

Let R be a subring of the integral domain S, with S integral over R. Then R is a field if and only if S is a field.

Proof. Assume that S is a field, and let a be a nonzero element of R. Since $a^{-1} \in S$, there is an equation of the form

$$(a^{-1})^n + c_{n-1}(a^{-1})^{n-1} + \cdots + c_1 a^{-1} + c_0 = 0$$

with $c_i \in R$. Multiply the equation by a^{n-1} to get

$$a^{-1} = -(c_{n-1} + \cdots + c_1 a^{n-2} + c_0 a^{n-1}) \in R.$$

Now assume that R is a field, and let b be a nonzero element of S. By (2.1.4) part (2), $R[b]$ is a finite-dimensional vector space over R. Let f be the R-linear transformation on this vector space given by multiplication by b, in other words, $f(z) = bz,\ z \in R[b]$. Since $R[b]$ is a subring of S, it is an integral domain. Thus if $bz = 0$ (with $b \neq 0$ by choice of b), we have $z = 0$ and f is injective. But any linear transformation on a finite-dimensional vector space is injective iff it is surjective. Therefore if $b \in S$ and $b \neq 0$, there is an element $c \in R[b] \subseteq S$ such that $bc = 1$. Consequently, S is a field. ♣

2.1.11 Preview

Let S be integral over the subring R. We will analyze in great detail the relation between prime ideals of R and those of S. Suppose that Q is a prime ideal of S, and let $P = Q \cap R$. (We say that Q *lies over* P.) Then P is a prime ideal of R, because it is the preimage of Q under the inclusion map from R into S. The map $a + P \to a + Q$ is a well-defined injection of R/P into S/Q, because $P = Q \cap R$. Thus we can regard R/P as a subring of S/Q. Moreover, S/Q is integral over R/P. To see this, let $b + Q \in S/Q$. Then b satisfies an equation of the form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

with $a_i \in R$. But $b + Q$ satisfies the same equation with a_i replaced by $a_i + P$ for all i, proving integrality of S/Q over R/P. We can now invoke (2.1.10) to prove the following result.

2.1.12 Proposition

Let S be integral over the subring R, and let Q be a prime ideal of S, lying over the prime ideal $P = Q \cap R$ of R. Then P is a maximal ideal of R if and only if Q is a maximal ideal of S.

Proof. By (2.1.10), R/P is a field iff S/Q is a field. ♣

2.1.13 Remarks

Some results discussed in (2.1.11) work for arbitrary ideals, not necessarily prime. If R is a subring of S and J is an ideal of S, then $I = J \cap R$ is an ideal of R. As in (2.1.11), R/I can be regarded as a subring of S/J, and if S is integral over R, then S/J is integral over R/I. Similarly, if S is integral over R and T is a multiplicative subset of R, then S_T is integral over R_T. To prove this, let $\alpha/t \in S_T$, with $\alpha \in S, t \in T$. Then there is an equation of the form $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0$, with $c_i \in R$. Thus

$$(\frac{\alpha}{t})^n + (\frac{c_{n-1}}{t})(\frac{\alpha}{t})^{n-1} + \cdots + (\frac{c_1}{t^{n-1}})\frac{\alpha}{t} + \frac{c_0}{t^n} = 0$$

with $c_{n-j}/t^j \in R_T$.

2.2 Integrality and Localization

Results that hold for maximal ideals can sometimes be extended to prime ideals by the technique of localization. A good illustration follows.

2.2.1 Proposition

Let S be integral over the subring R, and let P_1 and P_2 be prime ideals of S that lie over the prime ideal P of R, that is, $P_1 \cap R = P_2 \cap R = P$. If $P_1 \subseteq P_2$, then $P_1 = P_2$.

Proof. If P is maximal, then by (2.1.12), so are P_1 and P_2, and the result follows. In the general case, we localize with respect to P. Let $T = R \backslash P$, a multiplicative subset of $R \subseteq S$. The prime ideals P_i , $i = 1, 2$, do not meet T, because if $x \in T \cap P_i$, then $x \in R \cap P_i = P$, contradicting the definition of T. By the basic correspondence between prime ideals in a ring and prime ideals in its localization, it suffices to show that $P_1 S_T = P_2 S_T$. We claim that

$$PR_T \subseteq (P_1 S_T) \cap R_T \subset R_T.$$

The first inclusion holds because $P \subseteq P_1$ and $R_T \subseteq S_T$. The second inclusion is proper, for otherwise $R_T \subseteq P_1 S_T$ and therefore $1 \in P_1 S_T$, contradicting the fact that $P_1 S_T$ is a prime ideal.

But PR_T is a maximal ideal of R_T, so by the above claim,

$$(P_1 S_T) \cap R_T = PR_T, \text{ and similarly } (P_2 S_T) \cap R_T = PR_T.$$

Thus $P_1 S_T$ and $P_2 S_T$ lie over PR_T. By (2.1.13), S_T is integral over R_T. As at the beginning of the proof, $P_1 S_T$ and $P_2 S_T$ are maximal by (2.1.12), hence $P_1 S_T = P_2 S_T$. ♣

If S/R is an integral extension, then prime ideals of R can be lifted to prime ideals of S, as the next result demonstrates. Theorem 2.2.2 is also a good example of localization technique.

2.2.2 Lying Over Theorem

If S is integral over R and P is a prime ideal of R, there is a prime ideal Q of S such that $Q \cap R = P$.

Proof. First assume that R is a local ring with unique maximal ideal P. If Q is any maximal ideal of S, then $Q \cap R$ is maximal by (2.1.12), so $Q \cap R$ must be P. In general, let T be the multiplicative set $R \setminus P$. We have the following commutative diagram.

$$\begin{array}{ccc} R & \longrightarrow & S \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g} \\ R_T & \longrightarrow & S_T \end{array}$$

The horizontal maps are inclusions, and the vertical maps are canonical ($f(r) = r/1$ and $g(s) = s/1$). Recall that S_T is integral over R_T by (2.1.13). If Q' is any maximal ideal of S_T, then as at the beginning of the proof, $Q' \cap R_T$ must be the unique maximal ideal of R_T, namely PR_T. By commutativity of the diagram, $f^{-1}(Q' \cap R_T) = g^{-1}(Q') \cap R$. (Note that if $r \in R$, then $f(r) \in Q' \cap R_T$ iff $g(r) \in Q'$.) If $Q = g^{-1}(Q')$, we have $f^{-1}(PR_T) = Q \cap R$. By the basic localization correspondence [cf.(2.2.1)], $f^{-1}(PR_T) = P$, and the result follows. ♣

2.2.3 Going Up Theorem

Let S be integral over R, and suppose we have a chain of prime ideals $P_1 \subseteq \cdots \subseteq P_n$ of R, and a chain of prime ideals $Q_1 \subseteq \cdots \subseteq Q_m$ of S, where $m < n$. If Q_i lies over P_i for $i = 1, \dots, m$, then there are prime ideals $Q_{m+1}, \dots, Q_n$ of S such that $Q_m \subseteq Q_{m+1} \subseteq \cdots \subseteq Q_n$ and Q_i lies over P_i for every $i = 1, \dots, n$.

Proof. By induction, it suffices to consider the case $n = 2, m = 1$. Thus assume $P_1 \subseteq P_2$ and $Q_1 \cap R = P_1$. By (2.1.11), S/Q_1 is integral over R/P_1. Since P_2/P_1 is a prime ideal of R/P_1, we may apply the lying over theorem (2.2.2) to produce a prime ideal Q_2/Q_1 of S/Q_1 such that

$$(Q_2/Q_1) \cap R/P_1 = P_2/P_1,$$

where Q_2 is a prime ideal of S and $Q_1 \subseteq Q_2$. We claim that $Q_2 \cap R = P_2$, which gives the desired extension of the Q-chain. To verify this, let $x_2 \in Q_2 \cap R$. By (2.1.11), we have an embedding of R/P_1 into S/Q_1, so $x_2 + P_1 = x_2 + Q_1 \in (Q_2/Q_1) \cap R/P_1 = P_2/P_1$. Thus $x_2 + P_1 = y_2 + P_1$ for some $y_2 \in P_2$, so $x_2 - y_2 \in P_1 \subseteq P_2$. Consequently, $x_2 \in P_2$. Conversely, if $x_2 \in P_2$ then $x_2 + P_1 \in Q_2/Q_1$, hence $x_2 + P_1 = y_2 + Q_1$ for some $y_2 \in Q_2$. But as above, $x_2 + P_1 = x_2 + Q_1$, so $x_2 - y_2 \in Q_1$, and therefore $x_2 \in Q_2$. ♣

It is a standard result of field theory that an embedding of a field F in an algebraically closed field can be extended to an algebraic extension of F. There is an analogous result for ring extensions.

2.2.4 Theorem

Let S be integral over R, and let f be a ring homomorphism from R into an algebraically closed field C. Then f can be extended to a ring homomorphism $g : S \to C$.

Proof. Let P be the kernel of f. Since f maps into a field, P is a prime ideal of R. By (2.2.2), there is a prime ideal Q of S such that $Q \cap R = P$. By the factor theorem, f induces an injective ring homomorphism $\overline{f} : R/P \to C$, which extends in the natural way to the fraction field K of R/P. Let L be the fraction field of S/Q. By (2.1.11), S/Q is integral over R/P, hence L is an algebraic extension of K. Since C is algebraically closed, $\overline{f}$ extends to a monomorphism $\overline{g} : L \to C$. If $p : S \to S/Q$ is the canonical epimorphism and $g = \overline{g} \circ p$, then g is the desired extension of f, because $\overline{g}$ extends $\overline{f}$ and $\overline{f} \circ p|_R = f$. ♣

In the next section, we will prove the companion result to (2.2.3), the going down theorem. There will be extra hypotheses, including the assumption that R is integrally closed. So it will be useful to get some practice with the idea of integral closure.

2.2.5 Lemma

Let R be a subring of S, and denote by $\overline{R}$ the integral closure of R in S. If T is a multiplicative subset of R, then $(\overline{R})_T$ is the integral closure of R_T in S_T.

Proof. Since $\overline{R}$ is integral over R, it follows from (2.1.13) that $(\overline{R})_T$ is integral over R_T. If $\alpha/t \in S_T$ $(\alpha \in S, t \in T)$ and α/t is integral over R_T, we must show that $\alpha/t \in (\overline{R})_T$. There is an equation of the form

$$(\frac{\alpha}{t})^n + (\frac{a_1}{t_1})(\frac{\alpha}{t})^{n-1} + \cdots + \frac{a_n}{t_n} = 0$$

with $a_i \in R$ and $t_i, t \in T$. Let $t_0 = \prod_{i=1}^n t_i$, and multiply the equation by $(tt_0)^n$ to conclude that $t_0\alpha$ is integral over R. Therefore $t_0\alpha \in \overline{R}$, so $\alpha/t = t_0\alpha/t_0t \in (\overline{R})_T$. ♣

2.2.6 Corollary

If T is a multiplicative subset of the integrally closed domain R, then R_T is integrally closed.

Proof. Apply (2.2.5) with $\overline{R} = R$ and $S = K$, the fraction field of R (and of R_T). Then R_T is the integral closure of R_T in S_T. But $S_T = K$, so R_T is integrally closed. ♣

Additional results on localization and integral closure will be developed in the exercises. The following result will be useful. (The same result was proved in (1.5.1), but a slightly different proof is given here.)

2.2.7 Proposition

The following conditions are equivalent, for an arbitrary R-module M.
(1) $M = 0$;
(2) $M_P = 0$ for all prime ideals P of R;
(3) $M_P = 0$ for all maximal ideals P of R.

Proof. It is immediate that (1) $\Rightarrow$ (2) $\Rightarrow$ (3). To prove that (3) $\Rightarrow$ (1), let $m \in M$. If P is a maximal ideal of R, then $m/1$ is 0 in M_P, so there exists $r_P \in R \setminus P$ such that $r_P m = 0$ in M. Let $I(m)$ be the ideal generated by the r_P. Then $I(m)$ cannot be contained in any maximal ideal $\mathcal{M}$, because $r_{\mathcal{M}} \notin \mathcal{M}$ by construction. Thus $I(m)$ must be R, and in particular, $1 \in I(m)$. Thus 1 can be written as a finite sum $\sum_P a_P r_P$ where P is a maximal ideal of R and $a_P \in R$. Consequently,

$$m = 1m = \sum_P a_P r_P m = 0. \quad ♣$$

2.3 Going Down

We will prove a companion result to the going up theorem (2.2.3), but additional hypotheses will be needed and the analysis is more complicated.

2.3.1 Lemma

Let S be integral over the subring R, with I an ideal of R. Then $\sqrt{IS}$ is the set of all $s \in S$ satisfying an equation of integral dependence $s^m + r_{m-1}s^{m-1} + \cdots + r_1 s + r_0 = 0$ with the $r_i \in I$.

Proof. If s satisfies such an equation, then $s^m \in IS$, so $s \in \sqrt{IS}$. Conversely, let $s^n \in IS$, $n \geq 1$, so that $s^n = \sum_{i=1}^k r_i s_i$ for some $r_i \in I$ and $s_i \in S$. Then $S_1 = R[s_1, \dots, s_k]$ is a subring of S, and is also a finitely generated R-module by (2.1.5). Now

$$s^n S_1 = \sum_{i=1}^k r_i s_i S_1 \subseteq \sum_{i=1}^k r_i S_1 \subseteq IS_1.$$

Moreover, S_1 is a faithful $R[s^n]$-module, because an element that annihilates S_1 annihilates 1 and is therefore 0. By (2.1.2), s^n, hence s, satisfies an equation of integral dependence with coefficients in I. ♣

2.3.2 Lemma

Let R be an integral domain with fraction field K, and assume that R is integrally closed. Let f and g be monic polynomials in $K[x]$. If $fg \in R[x]$, then both f and g are in $R[x]$.

Proof. In a splitting field containing K, we have $f(x) = \prod_i (x - a_i)$ and $g(x) = \prod_j (x - b_j)$. Since the a_i and b_j are roots of the monic polynomial $fg \in R[x]$, they are integral over R. The coefficients of f and g are in K and are symmetric polynomials in the roots, hence are integral over R as well. But R is integrally closed, and the result follows. ♣

2.3.3 Proposition

Let S be integral over the subring R, where R is an integrally closed domain. Assume that no nonzero element of R is a zero-divisor of S. (This is automatic if S itself is an integral domain.) If $s \in S$, define a homomorphism $h_s : R[x] \to S$ by $h_s(f) = f(s)$; thus h_s is just evaluation at s. Then the kernel I of h_s is a principal ideal generated by a monic polynomial.

Proof. If K is the fraction field of R, then $IK[x]$ is an ideal of the PID $K[x]$, and $IK[x] \neq 0$ because s is integral over R. (If this is unclear, see the argument in Step 1 below.) Thus $IK[x]$ is generated by a monic polynomial f.

Step 1: $f \in R[x]$.

By hypothesis, s is integral over R, so there is a monic polynomial $h \in R[x]$ such that $h(s) = 0$. Then $h \in I \subseteq IK[x]$, hence h is a multiple of f, say $h = fg$, with g monic in $K[x]$. Since R is integrally closed, we may invoke (2.3.2) to conclude that f and g belong to $R[x]$.

Step 2: $f \in I$.

Since $f \in IK[x]$, we may clear denominators to produce a nonzero element $r \in R$ such that $rf \in IR[x] = I$. By definition of I we have $rf(s) = 0$, and by hypothesis, r is not a zero-divisor of S. Therefore $f(s) = 0$, so $f \in I$.

Step 3: f generates I.

Let $q \in I \subseteq IK[x]$. Since f generates $IK[x]$, we can take a common denominator and write $q = q_1 f/r_1$ with $0 \neq r_1 \in R$ and $q_1 \in R[x]$. Thus $r_1 q = q_1 f$, and if we pass to residue classes in the polynomial ring $(R/Rr_1)[x]$, we have $\overline{q_1}\,\overline{f} = 0$. Since $\overline{f}$ is monic, the leading coefficient of $\overline{q_1}$ must be 0, which means that $\overline{q_1}$ itself must be 0. Consequently, r_1 divides every coefficient of q_1, so $q_1/r_1 \in R[x]$. Thus f divides q in $R[x]$. ♣

2.3.4 Going Down Theorem

Let the integral domain S be integral over the integrally closed domain R. Suppose we have a chain of prime ideals $P_1 \subseteq \cdots \subseteq P_n$ of R and a chain of prime ideals $Q_m \subseteq \cdots \subseteq Q_n$ of S, with $1 < m \leq n$. If Q_i lies over P_i for $i = m, \dots, n$, then there are prime ideals $Q_1, \dots, Q_{m-1}$ such that $Q_1 \subseteq \cdots \subseteq Q_m$ and Q_i lies over P_i for every $i = 1, \dots, n$.

Proof. By induction, it suffices to consider $n = m = 2$. Let T be the subset of S consisting of all products $rt,\ r \in R \setminus P_1,\ t \in S \setminus Q_2$. In checking that T is a multiplicative set, we must make sure that it does not contain 0. If $rt = 0$ for some $r \notin P_1$ (hence $r \neq 0$) and $t \notin Q_2$, then the hypothesis that r is not a zero-divisor of S gives $t = 0$, which is a contradiction (because $0 \in Q_2$). Note that $R \setminus P_1 \subseteq T$ (take $t = 1$), and $S \setminus Q_2 \subseteq T$ (take $r = 1$).

First we prove the theorem under the assumption that $T \cap P_1 S = \emptyset$. Now $P_1 S_T$ is a proper ideal of S_T, else 1 would belong to $T \cap P_1 S$. Therefore $P_1 S_T$ is contained in a maximal ideal $\mathcal{M}$. By basic localization theory, $\mathcal{M}$ corresponds to a prime ideal Q_1 of S that is disjoint from T. Explicitly, $s \in Q_1$ iff $s/1 \in \mathcal{M}$. We refer to Q_1 as the *contraction* of $\mathcal{M}$ to S; it is the preimage of $\mathcal{M}$ under the canonical map $s \to s/1$. With the aid of the note at the end of the last paragraph, we have $(R \setminus P_1) \cap Q_1 = (S \setminus Q_2) \cap Q_1 = \emptyset$. Thus $Q_1 \cap R \subseteq P_1$ and $Q_1 = Q_1 \cap S \subseteq Q_2$. We must show that $P_1 \subseteq Q_1 \cap R$. We do this by taking the contraction of both sides of the inclusion $P_1 S_T \subseteq \mathcal{M}$. Since the contraction of $P_1 S_T$ to S is $P_1 S$, we have $P_1 S \subseteq Q_1$, so $P_1 \subseteq (P_1 S) \cap R \subseteq Q_1 \cap R$, as desired.

Finally, we show that $T \cap P_1 S$ is empty. If not, then by definition of T, $T \cap P_1 S$ contains an element rt with $r \in R \setminus P_1$ and $t \in S \setminus Q_2$. We apply (2.3.1), with $I = P_1$ and s replaced by rt, to produce a monic polynomial $f(x) = x^m + r_{m-1}x^{m-1} + \cdots + r_1 x + r_0$ with coefficients in P_1 such that $f(rt) = 0$. Define

$$v(x) = r^m x^m + r_{m-1} r^{m-1} x^{m-1} + \cdots + r_1 r x + r_0.$$

Then $v(x) \in R[x]$ and $v(t) = 0$. By (2.3.3), there is a monic polynomial $g \in R[x]$ that generates the kernel of the evaluation map $h_t : R[x] \to S$. Therefore $v = ug$ for some $u \in R[x]$. Passing to residue classes in the polynomial ring $(R/P_1)[x]$, we have $\overline{v} = \overline{u}\,\overline{g}$. Since $r_i \in P_1$ for all $i = 0, \dots, m-1$, we have $\overline{v} = \overline{r}^m x^m$. Since R/P_1 is an integral domain and g, hence $\overline{g}$, is monic, we must have $\overline{g} = x^j$ for some j with $0 \leq j \leq m$. (Note that $r \notin P_1$, so $\overline{v}$ is not the zero polynomial.) Consequently,

$$g(x) = x^j + a_{j-1}x^{j-1} + \cdots + a_1 x + a_0$$

with $a_i \in P_1, i = 0, \dots, j-1$. But $g \in \ker h_t$, so $g(t) = 0$. By (2.3.1), t belongs to the radical of $P_1 S$, so for some positive integer l, we have $t^l \in P_1 S \subseteq P_2 S \subseteq Q_2 S = Q_2$, so $t \in Q_2$. This contradicts our choice of t (recall that $t \in S \setminus Q_2$). ♣

Chapter 3

Valuation Rings

The results of this chapter come into play when analyzing the behavior of a rational function defined in the neighborhood of a point on an algebraic curve.

3.1 Extension Theorems

In Theorem 2.2.4, we generalized a result about field extensions to rings. Here is another variation.

3.1.1 Theorem

Let R be a subring of the field K, and $h : R \to C$ a ring homomorphism from R into an algebraically closed field C. If α is a nonzero element of K, then either h can be extended to a ring homomorphism $\overline{h} : R[\alpha] \to C$, or h can be extended to a ring homomorphism $\overline{h} : R[\alpha^{-1}] \to C$.

Proof. Without loss of generality, we may assume that R is a local ring and $F = h(R)$ is a subfield of C. To see this, let P be the kernel of h. Then P is a prime ideal, and we can extend h to $g : R_P \to C$ via $g(a/b) = h(a)/h(b),\ h(b) \neq 0$. The kernel of g is PR_P, so by the first isomorphism theorem, $g(R_P) \cong R_P/PR_P$, a field (because PR_P is a maximal ideal). Thus we may replace (R, h) by (R_P, g).

Our first step is to extend h to a homomorphism of polynomial rings. If $f \in R[x]$ with $f(x) = \sum a_i x^i$, we take $h(f) = \sum h(a_i)x^i \in F[x]$. Let $I = \{f \in R[x] : f(\alpha) = 0\}$. Then $J = h(I)$ is an ideal of $F[x]$, necessarily principal. Say $J = (j(x))$. If j is nonconstant, it must have a root β in the algebraically closed field C. We can then extend h to $\overline{h} : R[\alpha] \to C$ via $\overline{h}(\alpha) = \beta$, as desired. To verify that $\overline{h}$ is well-defined, suppose $f \in I$, so that $f(\alpha) = 0$. Then $h(f) \in J$, hence $h(f)$ is a multiple of j, and therefore $h(f)(\beta) = 0$. Thus we may assume that j is constant. If the constant is zero, then we may extend h exactly as above, with β arbitrary. So we can assume that $j \neq 0$, and it follows that $1 \in J$. Consequently, there exists $f \in I$ such that $h(f) = 1$.

This gives a relation of the form

$$\sum_{i=0}^{r} a_i\alpha^i = 0 \text{ with } a_i \in R \text{ and } \overline{a}_i = h(a_i) = \begin{cases} 1, & i = 0 \\ 0, & i > 0 \end{cases} \tag{1}$$

Choose r as small as possible. We then carry out the same analysis with α replaced by α^{-1}. Assuming that h has no extension to $R[\alpha^{-1}]$, we have

$$\sum_{i=0}^{s} b_i\alpha^{-i} = 0 \text{ with } b_i \in R \text{ and } \overline{b}_i = h(b_i) = \begin{cases} 1, & i = 0 \\ 0, & i > 0 \end{cases} \tag{2}$$

Take s minimal, and assume (without loss of generality) that $r \geq s$. Since $h(b_0) = 1 = h(1)$, it follows that $b_0 - 1 \in \ker h \subseteq \mathcal{M}$, the unique maximal ideal of the local ring R. Thus $b_0 \notin \mathcal{M}$ (else $1 \in \mathcal{M}$), so b_0 is a unit. It is therefore legal to multiply (2) by $b_0^{-1}\alpha^s$ to get

$$\alpha^s + b_0^{-1}b_1\alpha^{s-1} + \cdots + b_0^{-1}b_s = 0 \tag{3}$$

Finally, we multiply (3) by $a_r\alpha^{r-s}$ and subtract the result from (1) to contradict the minimality of r. (The result of multiplying (3) by $a_r\alpha^{r-s}$ cannot be a copy of (1). If so, $r = s$ (hence $\alpha^{r-s} = 1$)and $a_0 = a_r b_0^{-1}b_s$. But $h(a_0) = 1$ and $h(a_r b_0^{-1}b_s) = 0$.) ♣

It is natural to try to extend h to a larger domain, and this is where valuation rings enter the picture.

3.1.2 Definition

A subring R of a field K is a *valuation ring* of K if for every nonzero $\alpha \in K$, either α or α^{-1} belongs to R.

3.1.3 Examples

The field K is a valuation ring of K, but there are more interesting examples.

1. Let $K = \mathbb{Q}$, with p a fixed prime. Take R to be the set of all rationals of the form $p^r m/n$, where $r \geq 0$ and p divides neither m nor n.

2. Let $K = k(x)$, where k is any field. Take R to be the set of all rational functions $p^r m/n$, where $r \geq 0$, p is a fixed polynomial that is irreducible over k and m and n are arbitrary polynomials in $k[x]$ not divisible by p. This is essentially the same as the previous example.

3. Let $K = k(x)$, and let R be the set of all rational functions $f/g \in k(x)$ such that $\deg f \leq \deg g$.

4. Let K be the field of formal *Laurent series* over k. Thus a nonzero element of K looks like $f = \sum_{i=r}^{\infty} a_i x^i$ with $a_i \in k$, $r \in \mathbb{Z}$, and $a_r \neq 0$. We may write $f = a_r x^r g$, where g belongs to the ring $R = k[[x]]$ of formal power series over k. Moreover, the constant term of g is 1, and therefore g, hence f, can be inverted (by long division). Thus R is a valuation ring of K.

We now return to the extension problem.

3.1.4 Theorem

Let R be a subring of the field K, and $h : R \to C$ a ring homomorphism from R into an algebraically closed field C. Then h has maximal extension $(V, \overline{h})$. In other words, V is a subring of K containing R, $\overline{h}$ is an extension of h, and there is no extension to a strictly larger subring. In addition, for any maximal extension, V is a valuation ring of K.

Proof. Let $\mathcal{S}$ be the set of all (R_i, h_i), where R_i is a subring of K containing R and h_i is an extension of h to R_i. Partially order $\mathcal{S}$ by $(R_i, h_i) \leq (R_j, h_j)$ if and only if R_i is a subring of R_j and h_j restricted to R_i coincides with h_i. A standard application of Zorn's lemma produces a maximal extension $(V, \overline{h})$. If α is a nonzero element of K, then by (3.1.1), $\overline{h}$ has an extension to either $V[\alpha]$ or $V[\alpha^{-1}]$. By maximality, either $V[\alpha] = V$ or $V[\alpha^{-1}] = V$. Therefore $\alpha \in V$ or $\alpha^{-1} \in V$. ♣

3.2 Properties of Valuation Rings

We have a long list of properties to verify, and the statement of each property will be followed immediately by its proof. The end of proof symbol will only appear at the very end. Throughout, V is a valuation ring of the field K.

1. The fraction field of V is K.

This follows because a nonzero element α of K can be written as $\alpha/1$ or as $1/\alpha^{-1}$.

2. Any subring of K containing V is a valuation ring of K.

This follows from the definition of a valuation ring.

3. V is a local ring.

We will show that the set $\mathcal{M}$ of nonunits of V is an ideal. If a and b are nonzero nonunits, then either a/b or b/a belongs to V. If $a/b \in V$, then $a + b = b(1 + a/b) \in \mathcal{M}$ (because if $b(1 + a/b)$ were a unit, then b would be a unit as well). Similarly, if $b/a \in V$, then $a + b \in \mathcal{M}$. If $r \in V$ and $a \in \mathcal{M}$, then $ra \in \mathcal{M}$, else a would be a unit. Thus $\mathcal{M}$ is an ideal.

4. V is integrally closed.

Let α be a nonzero element of K, with α integral over V. Then there is an equation of the form

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0$$

with the c_i in V. We must show that $\alpha \in V$. If not, then $\alpha^{-1} \in V$, and if we multiply the above equation of integral dependence by $\alpha^{-(n-1)}$, we get

$$\alpha = -c_{n-1} - c_{n-2}\alpha^{-1} - \cdots - c_1\alpha^{n-2} - c_0\alpha^{n-1} \in V.$$

5. If I and J are ideals of V, then either $I \subseteq J$ or $J \subseteq I$. Thus the ideals of V are totally ordered by inclusion.

Suppose that I is not contained in J, and pick $a \in I \setminus J$ (hence $a \neq 0$). If $b \in J$, we must show that $b \in I$. If $b = 0$ we are finished, so assume $b \neq 0$. We have $b/a \in V$ (else $a/b \in V$, so $a = (a/b)b \in J$, a contradiction). Therefore $b = (b/a)a \in I$.

6. Conversely, let V be an integral domain with fraction field K. If the ideals of V are partially ordered by inclusion, then V is a valuation ring of K.

If α is a nonzero element of K, then $\alpha = a/b$ with a and b nonzero elements of V. By hypothesis, either $(a) \subseteq (b)$, in which case $a/b \in V$, or $(b) \subseteq (a)$, in which case $b/a \in V$.

7. If P is a prime ideal of the valuation ring V, then V_P and V/P are valuation rings.

First note that if K is the fraction field of V, it is also the fraction field of V_P. Also, V/P is an integral domain, hence has a fraction field. Now by Property 5, the ideals of V are totally ordered by inclusion, so the same is true of V_P and V/P. The result follows from Property 6.

8. If V is a Noetherian valuation ring, then V is a PID. Moreover, for some prime $p \in V$, every ideal is of the form (p^m), $m \geq 0$. For any such p, $\cap_{m=1}^{\infty}(p^m) = 0$.

Since V is Noetherian, an ideal I of V is finitely generated, say by $a_1, \dots, a_n$. By Property 5, we may renumber the a_i so that $(a_1) \subseteq (a_2) \cdots \subseteq (a_n)$. But then $I \subseteq (a_n) \subseteq I$, so $I = (a_n)$. In particular, the maximal ideal $\mathcal{M}$ of V is (p) for some p, and p is prime because $\mathcal{M}$ is a prime ideal. If (a) is an arbitrary ideal, then $(a) = V$ if a is a unit, so assume a is a nonunit, that is, $a \in \mathcal{M}$. But then p divides a, so $a = pb$. If b is a nonunit, then p divides b, and we get $a = p^2c$. Continuing inductively and using the fact that V is a PID, hence a UFD, we have $a = p^m u$ for some positive integer m and unit u. Thus $(a) = (p^m)$. Finally, if a belongs to (p^m) for every $m \geq 1$, then p^m divides a for all $m \geq 1$. Again using unique factorization, we must have $a = 0$. (Note that if a is a unit, so is p, a contradiction.)

9. Let R be a subring of the field K. The integral closure $\overline{R}$ of R in K is the intersection of all valuation rings V of K such that $V \supseteq R$.

If $a \in \overline{R}$, then a is integral over R, hence over any valuation ring $V \supseteq R$. But V is integrally closed by Property 4, so $a \in V$. Conversely, assume $a \notin \overline{R}$. Then a fails to belong to the ring $R' = R[a^{-1}]$. (If a is a polynomial in a^{-1}, multiply by a sufficiently high power of a to get a monic equation satisfied by a.) Thus a^{-1} cannot be a unit in R'. (If $ba^{-1} = 1$ with $b \in R'$, then $a = a1 = aa^{-1}b = b \in R'$, a contradiction.) It follows that a^{-1} belongs to a maximal ideal $\mathcal{M}'$ of R'. Let C be an algebraic closure of the field $k = R'/\mathcal{M}'$, and let h be the composition of the canonical map $R' \to R'/\mathcal{M}' = k$ and the inclusion $k \to C$. By (3.1.4), h has a maximal extension to $\overline{h} : V \to C$ for some valuation ring V of K containing $R' \supseteq R$. Now $\overline{h}(a^{-1}) = h(a^{-1})$ since $a^{-1} \in \mathcal{M}' \subseteq R'$, and $h(a^{-1}) = 0$ by definition of h. Consequently $a \notin V$, for if $a \in V$, then

$$1 = \overline{h}(1) = \overline{h}(aa^{-1}) = \overline{h}(a)\overline{h}(a^{-1}) = 0,$$

a contradiction. The result follows.

10. Let R be an integral domain with fraction field K. Then R is integrally closed if and only if $R = \cap_\alpha V_\alpha$, the intersection of some (not necessarily all) valuation rings of K.

The "only if" part follows from Property 9. For the "if" part, note that each V_α is integrally closed by Property 4, hence so is R. (If a is integral over R, then a is integral over each V_α, hence a belongs to each V_α, so $a \in R$.) ♣

3.3 Discrete Valuation Rings

3.3.1 Definitions and Comments

An *absolute value* on a field K is a mapping $x \to |x|$ from K to the real numbers, such that for every $x, y \in K$,
1. $|x| \geq 0$, with equality if and only if $x = 0$;
2. $|xy| = |x|\,|y|$;
3. $|x + y| \leq |x| + |y|$.

The absolute value is *nonarchimedean* if the third condition is replaced by a stronger version:
$3'$. $|x + y| \leq \max(|x|, |y|)$.
As expected, *archimedean* means not nonarchimedean.

The familiar absolute values on the reals and the complex numbers are archimedean. However, our interest will be in nonarchimedean absolute values. Here is where most of them come from.

A *discrete valuation* on K is a surjective map $v : K \to \mathbb{Z} \cup \{\infty\}$, such that for every $x, y \in K$,
(a) $v(x) = \infty$ if and only if $x = 0$;
(b) $v(xy) = v(x) + v(y)$;
(c) $v(x + y) \geq \min(v(x), v(y))$.

A discrete valuation induces a nonarchimedean absolute value via $|x| = c^{v(x)}$, where c is a constant with $0 < c < 1$.

3.3.2 Examples

We can place a discrete valuation on all of the fields of Subsection 3.1.3. In Examples 1 and 2, we take $v(p^r m/n) = r$. In Example 3, $v(f/g) = \deg g - \deg f$. In Example 4, $v(\sum_{i=r}^{\infty} a_i x^i) = r$ (if $a_r \neq 0$).

3.3.3 Proposition

If v is a discrete valuation on the field K, then $V = \{a \in K : v(a) \geq 0\}$ is a valuation ring with maximal ideal $\mathcal{M} = \{a \in K : v(a) \geq 1\}$.

Proof. The defining properties (a), (b) and (c) of 3.3.1 show that V is a ring. If $a \notin V$, then $v(a) < 0$, so $v(a^{-1}) = v(1) - v(a) = 0 - v(a) > 0$, so $a^{-1} \in V$, proving that V is a valuation ring. Since a is a unit of V iff both a and a^{-1} belong to V iff $v(a) = 0$, $\mathcal{M}$ is the ideal of nonunits and is therefore the maximal ideal of the valuation ring V. ♣

3.3.4 Definitions and Comments

Discrete valuations do not determine all valuation rings. An arbitrary valuation ring corresponds to a generalized absolute value mapping into an ordered group rather than the real numbers. We will not consider the general situation, as discrete valuations will be entirely adequate for us. A valuation ring V arising from a discrete valuation v as in

(3.3.3) is said to be a *discrete valuation ring*, abbreviated DVR. An element $t \in V$ with $v(t) = 1$ is called a *uniformizer* or *prime element*. A uniformizer tells us a lot about the DVR V and the field K.

3.3.5 Proposition

Let t be a uniformizer in the discrete valuation ring V. Then t generates the maximal ideal $\mathcal{M}$ of V, in particular, $\mathcal{M}$ is principal. Conversely, if t' is any generator of $\mathcal{M}$, then t' is a uniformizer.

Proof. Since $\mathcal{M}$ is the unique maximal ideal, $(t) \subseteq \mathcal{M}$. If $a \in \mathcal{M}$, then $v(a) \geq 1$, so $v(at^{-1}) = v(a) - v(t) \geq 1 - 1 = 0$, so $at^{-1} \in V$, and consequently $a \in (t)$. Now suppose $\mathcal{M} = (t')$. Since $t \in \mathcal{M}$, we have $t = ct'$ for some $c \in V$. Thus

$$1 = v(t) = v(c) + v(t') \geq 0 + 1 = 1,$$

which forces $v(t') = 1$. ♣

3.3.6 Proposition

If t is a uniformizer, then every nonzero element $a \in K$ can be expressed uniquely as $a = ut^n$ where u is a unit of V and $n \in \mathbb{Z}$. Also, $K = V_t$, that is, $K = S^{-1}V$ where $S = \{1, t, t^2, \dots\}$.

Proof. Let $n = v(a)$, so that $v(at^{-n}) = 0$ and therefore at^{-n} is a unit u. To prove uniqueness, note that if $a = ut^n$, then $v(a) = v(u) + nv(t) = 0 + n = n$, so that n, and hence u, is determined by a. The last statement follows by Property 1 of Section 3.2 and the observation that the elements of V are those with valuation $n \geq 0$. ♣

A similar result holds for ideals.

3.3.7 Proposition

Every nonzero ideal I of the DVR V is of the form $\mathcal{M}^n$, where $\mathcal{M}$ is the maximal ideal of V and n is a unique nonnegative integer. We write $v(I) = n$; by convention, $\mathcal{M}^0 = V$.

Proof. Choose $a \in I$ such that $n = v(a)$ is as small as possible. By (3.3.6), $a = ut^n$, so $t^n = u^{-1}a \in I$. By (3.3.5), $\mathcal{M} = (t)$, and therefore $\mathcal{M}^n \subseteq I$. Conversely, let $b \in I$, with $v(b) = k \geq n$ by minimality of n. As in the proof of (3.3.6), bt^{-k} is a unit u', so $b = u't^k$. Since $k \geq n$ we have $b \in (t^n) = \mathcal{M}^n$, proving that $I \subseteq \mathcal{M}^n$. The uniqueness of n is a consequence of Nakayama's lemma. If $\mathcal{M}^r = \mathcal{M}^s$ with $r < s$, then $\mathcal{M}^r = \mathcal{M}^{r+1} = \mathcal{M}\mathcal{M}^r$. Thus $\mathcal{M}^r$, hence $\mathcal{M}$, is 0, contradicting the hypothesis that I is nonzero. ♣

We may interpret $v(I)$ as the length of a composition series.

3.3.8 Proposition

Let I be a nonzero ideal of the discrete valuation ring R. Then $v(I) = l_R(R/I)$, the composition length of the R-module R/I.

Proof. By (3.3.7), we have $R \supset \mathcal{M} \supset \mathcal{M}^2 \supset \cdots \supset \mathcal{M}^n = I$, hence

$$R/I \supset \mathcal{M}/I \supset \mathcal{M}^2/I \supset \cdots \supset \mathcal{M}^n/I = 0.$$

By basic properties of composition length, we have, with $l = l_R$,

$$l(R/I) = l(\frac{R/I}{\mathcal{M}/I}) + l(\mathcal{M}/I) = l(R/\mathcal{M}) + l(\frac{\mathcal{M}/I}{\mathcal{M}^2/I}) + l(\mathcal{M}^2/I).$$

Continuing in this fashion, we get

$$l(R/I) = \sum_{i=0}^{n-1} l(\mathcal{M}^i/\mathcal{M}^{i+1}).$$

Since $\mathcal{M}$ is generated by a uniformizer t, it follows that $t^i + \mathcal{M}^{i+1}$ generates $\mathcal{M}^i/\mathcal{M}^{i+1}$. Since $\mathcal{M}^i/\mathcal{M}^{i+1}$ is annihilated by $\mathcal{M}$, it is an $R/\mathcal{M}$-module, that is, a vector space, over the field $R/\mathcal{M}$. The vector space is one-dimensional because the $\mathcal{M}^i$, $i = 0, 1, \dots, n$, are distinct [see the proof of (3.3.7)]. Consequently, $l(R/I) = n$. ♣

We are going to prove a characterization theorem for DVR's, and some preliminary results will be needed.

3.3.9 Proposition

Let I be an ideal of the Noetherian ring R. Then for some positive integer m, we have $(\sqrt{I})^m \subseteq I$. In particular (take $I = 0$), the nilradical of R is nilpotent.

Proof. Since R is Noetherian, $\sqrt{I}$ is finitely generated, say by $a_1, \dots, a_t$, with $a_i^{n_i} \in I$. Then $(\sqrt{I})^m$ is generated by all products $a_1^{r_1} \cdots a_t^{r_t}$ with $\sum_{i=1}^t r_i = m$. Our choice of m is

$$m = 1 + \sum_{i=1}^{t}(n_i - 1).$$

We claim that $r_i \geq n_i$ for some i. If not, then $r_i \leq n_i - 1$ for all i, and

$$m = \sum_{i=1}^{t} r_i < 1 + \sum_{i=1}^{t}(n_i - 1) = m,$$

a contradiction. But then each product $a_1^{r_1} \cdots a_t^{r_t}$ is in I, hence $(\sqrt{I})^m \subseteq I$. ♣

3.3.10 Proposition

Let $\mathcal{M}$ be a maximal ideal of the Noetherian ring R, and let Q be any ideal of R. The following conditions are equivalent:

1. Q is $\mathcal{M}$-primary.
2. $\sqrt{Q} = \mathcal{M}$.
3. For some positive integer n, we have $\mathcal{M}^n \subseteq Q \subseteq \mathcal{M}$.

Proof. We have (1) implies (2) by definition of $\mathcal{M}$-primary; see (1.1.1). The implication (2) $\Rightarrow$ (1) follows from (1.1.2). To prove that (2) implies (3), apply (3.3.9) with $I = Q$ to get, for some positive integer n,

$$\mathcal{M}^n \subseteq Q \subseteq \sqrt{Q} = \mathcal{M}.$$

To prove that (3) implies (2), observe that by (1.1.1),

$$\mathcal{M} = \sqrt{\mathcal{M}^n} \subseteq \sqrt{Q} \subseteq \sqrt{\mathcal{M}} = \mathcal{M}. \clubsuit$$

Now we can characterize discrete valuation rings.

3.3.11 Theorem

Let R be a Noetherian local domain with fraction field K and unique maximal ideal $\mathcal{M} \neq 0$. (Thus R is not a field.) The following conditions are equivalent:
1. R is a discrete valuation ring.
2. R is a principal ideal domain.
3. $\mathcal{M}$ is principal.
4. R is integrally closed and every nonzero prime ideal is maximal.
5. Every nonzero ideal is a power of $\mathcal{M}$.
6. The dimension of $\mathcal{M}/\mathcal{M}^2$ as a vector space over $R/\mathcal{M}$ is 1.

Proof.

(1) $\Rightarrow$ (2): This follows from (3.3.7) and (3.3.5).
(2) $\Rightarrow$ (4): This holds because a PID is integrally closed, and a PID is a UFD in which every nonzero prime ideal is maximal.
(4) $\Rightarrow$ (3): Let t be a nonzero element of $\mathcal{M}$. By hypothesis, $\mathcal{M}$ is the only nonzero prime ideal, so the radical of (t), which is the intersection of all prime ideals containing t, coincides with $\mathcal{M}$. By (3.3.10), for some $n \geq 1$ we have $\mathcal{M}^n \subseteq (t) \subseteq \mathcal{M}$, and we may assume that $(t) \subset \mathcal{M}$, for otherwise we are finished. Thus for some $n \geq 2$ we have $\mathcal{M}^n \subseteq (t)$ but $\mathcal{M}^{n-1} \not\subseteq (t)$. Choose $a \in \mathcal{M}^{n-1}$ with $a \notin (t)$, and let $\beta = t/a \in K$. If $\beta^{-1} = a/t \in R$, then $a \in Rt = (t)$, contradicting the choice of a. Therefore $\beta^{-1} \notin R$. Since R is integrally closed, β^{-1} is not integral over R. But then $\beta^{-1}\mathcal{M} \not\subseteq \mathcal{M}$, for if $\beta^{-1}\mathcal{M} \subseteq \mathcal{M}$, then β^{-1} stabilizes a finitely generated R-module, and we conclude from the implication (4) $\Rightarrow$ (1) in (2.1.4) that β^{-1} is integral over R, a contradiction.

Now $\beta^{-1}\mathcal{M} \subseteq R$, because $\beta^{-1}\mathcal{M} = (a/t)\mathcal{M} \subseteq (1/t)\mathcal{M}^n \subseteq R$. (Note that $a \in \mathcal{M}^{n-1}$ and $\mathcal{M}^n \subseteq (t)$.) Thus $\beta^{-1}\mathcal{M}$ is an ideal of R, and if it were proper, it would be contained in $\mathcal{M}$, contradicting $\beta^{-1}\mathcal{M} \not\subseteq \mathcal{M}$. Consequently, $\beta^{-1}\mathcal{M} = R$, hence $\mathcal{M}$ is the principal ideal (β).
(3) $\Rightarrow$ (2): By hypothesis, $\mathcal{M}$ is a principal ideal (t), and we claim that $\cap_{n=0}^{\infty}\mathcal{M}^n = 0$. Suppose that a belongs to $\mathcal{M}^n$ for all n, with $a = b_n t^n$ for some $b_n \in R$. Then $b_n t^n = b_{n+1}t^{n+1}$, hence $b_n = b_{n+1}t$. Thus $(b_n) \subseteq (b_{n+1})$ for all n, and in fact $(b_n) = (b_{n+1})$ for sufficiently large n because R is Noetherian. Therefore $b_n = b_{n+1}t = ctb_n$ for some $c \in R$, so $(1 - ct)b_n = 0$. But $t \in \mathcal{M}$, so t is not a unit, and consequently $ct \neq 1$. Thus b_n must be 0, and we have $a = b_n t^n = 0$, proving the claim.

Now let I be any nonzero ideal of R. Then $I \subseteq \mathcal{M}$, but by the above claim we have $I \not\subseteq \cap_{n=0}\mathcal{M}^n$. Thus there exists $n \geq 0$ such that $I \subseteq \mathcal{M}^n$ and $I \not\subseteq \mathcal{M}^{n+1}$. Choose

$a \in I \setminus \mathcal{M}^{n+1}$; since $\mathcal{M}^n = (t)^n = (t^n)$, we have $a = ut^n$ with $u \notin \mathcal{M}$ (because $a \notin \mathcal{M}^{n+1}$). But then u is a unit, so $t^n = u^{-1}a \in I$. To summarize, $I \subseteq \mathcal{M}^n = (t^n) \subseteq I$, proving that I is principal.

(2) $\Rightarrow$ (1): By hypothesis, $\mathcal{M}$ is a principal ideal (t), and by the proof of (3) $\Rightarrow$ (2), $\cap_{n=0}^{\infty} \mathcal{M}^n = 0$. Let a be any nonzero element of R. Then $(a) \subseteq \mathcal{M}$, and since $\cap_{n=0}^{\infty} \mathcal{M}^n = 0$, we will have $a \in (t^n)$ but $a \notin (t^{n+1})$ for some n. Thus $a = ut^n$ with $u \notin \mathcal{M}$, in other words, u is a unit. For fixed a, both u and n are unique (because t, a member of $\mathcal{M}$, is a nonunit). It follows that if β is a nonzero element of the fraction field K, then $\beta = ut^m$ uniquely, where u is a unit of R and m is an integer, possibly negative. If we define $v(\beta) = m$, then v is a discrete valuation on K with valuation ring R.

(1) $\Rightarrow$ (5): This follows from (3.3.7).

(5) $\Rightarrow$ (3): As in the proof of (3.3.7), $\mathcal{M} \neq \mathcal{M}^2$. Choose $t \in \mathcal{M} \setminus \mathcal{M}^2$. By hypothesis, $(t) = \mathcal{M}^n$ for some $n \geq 0$. We cannot have $n = 0$ because $(t) \subseteq \mathcal{M} \subset R$, and we cannot have $n \geq 2$ by choice of t. The only possibility is $n = 1$, hence $\mathcal{M} = (t)$.

(1) $\Rightarrow$ (6): This follows from the proof of (3.3.8).

(6) $\Rightarrow$ (3): By hypothesis, $\mathcal{M} \neq \mathcal{M}^2$, so we may choose $t \in \mathcal{M} \setminus \mathcal{M}^2$. But then $t + \mathcal{M}^2$ is a generator of the vector space $\mathcal{M}/\mathcal{M}^2$ over the field $R/\mathcal{M}$. Thus $R(t+\mathcal{M}^2)/\mathcal{M}^2 = \mathcal{M}/\mathcal{M}^2$. By the correspondence theorem, $t + \mathcal{M}^2 = \mathcal{M}$. Now $\mathcal{M}(\mathcal{M}/(t)) = (\mathcal{M}^2 + (t))/(t) = \mathcal{M}/(t)$, so by NAK, $\mathcal{M}/(t) = 0$, that is, $\mathcal{M} = (t)$. ♣.

Let us agree to exclude the *trivial valuation* $v(a) = 0$ for every $a \neq 0$.

3.3.12 Corollary

The ring R is a discrete valuation ring if and only if R is a local PID that is not a field. In particular, since R is a PID, it is Noetherian.

Proof. The "if" part follows from (2) implies (1) in (3.3.11). For the "only if" part, note that a discrete valuation ring R is a PID by (1) implies (2) of (3.3.11); the Noetherian hypothesis is not used here. Moreover, R is a local ring by Property 3 of Section 3.2. If R is a field, then every nonzero element $a \in R$ is a unit, hence $v(a) = 0$. Thus the valuation v is trivial, contradicting our convention. ♣

3.3.13 Corollary

Let R be a DVR with maximal ideal $\mathcal{M}$. If $t \in \mathcal{M} \setminus \mathcal{M}^2$, then t is a uniformizer.

Proof. This follows from the proof of (5) implies (3) in (3.3.11). ♣

Chapter 4

Completion

The set $\mathbb{R}$ of real numbers is a complete metric space in which the set $\mathbb{Q}$ of rationals is dense. In fact any metric space can be embedded as a dense subset of a complete metric space. The construction is a familiar one involving equivalence classes of Cauchy sequences. We will see that under appropriate conditions, this procedure can be generalized to modules.

4.1 Graded Rings and Modules

4.1.1 Definitions and Comments

A *graded ring* is a ring R that is expressible as $\oplus_{n\geq 0} R_n$ where the R_n are additive subgroups such that $R_m R_n \subseteq R_{m+n}$. Sometimes, R_n is referred to as the n^{th} *graded piece* and elements of R_n are said to be *homogeneous of degree* n. The prototype is a polynomial ring in several variables, with R_d consisting of all homogeneous polynomials of degree d (along with the zero polynomial). A *graded module* over a graded ring R is a module M expressible as $\oplus_{n\geq 0} M_n$, where $R_m M_n \subseteq M_{m+n}$.

Note that the identity element of a graded ring R must belong to R_0. For if 1 has a component a of maximum degree $n > 0$, then $1a = a$ forces the degree of a to exceed n, a contradiction.

Now suppose that $\{R_n\}$ is a *filtration* of the ring R, in other words, the R_n are additive subgroups such that

$$R = R_0 \supseteq R_1 \supseteq \cdots \supseteq R_n \supseteq \cdots$$

with $R_m R_n \subseteq R_{m+n}$. We call R a *filtered ring.* A *filtered module*

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq \cdots$$

over the filtered ring R may be defined similarly. In this case, each M_n is a submodule and we require that $R_m M_n \subseteq M_{m+n}$.

If I is an ideal of the ring R and M is an R-module, we will be interested in the I*-adic filtrations* of R and of M, given respectively by $R_n = I^n$ and $M_n = I^n M$. (Take $I^0 = R$, so that $M_0 = M$.)

4.1.2 Associated Graded Rings and Modules

If $\{R_n\}$ is a filtration of R, the *associated graded ring* of R is defined as

$$\mathrm{gr}(R) = \bigoplus_{n \geq 0} \mathrm{gr}_n(R)$$

where $\mathrm{gr}_n(R) = R_n/R_{n+1}$. We must be careful in defining multiplication in $\mathrm{gr}(R)$. If $a \in R_m$ and $b \in R_n$, then $a + R_{m+1} \in R_m/R_{m+1}$ and $b + R_{n+1} \in R_n/R_{n+1}$. We take

$$(a + R_{m+1})(b + R_{n+1}) = ab + R_{m+n+1}$$

so that the product of an element of $\mathrm{gr}_m(R)$ and an element of $\mathrm{gr}_n(R)$ will belong to $\mathrm{gr}_{m+n}(R)$. If $a \in R_{m+1}$ and $b \in R_n$, then $ab \in R_{m+n+1}$, so multiplication is well-defined.

If M is a filtered module over a filtered ring R, we define the *associated graded module* of M as

$$\mathrm{gr}(M) = \bigoplus_{n \geq 0} \mathrm{gr}_n(M)$$

where $\mathrm{gr}_n(M) = M_n/M_{n+1}$. If $a \in R_m$ and $x \in M_n$, we define scalar multiplication by

$$(a + R_{m+1})(x + M_{n+1}) = ax + M_{m+n+1}$$

and it follows that

$$(R_m/R_{m+1})(M_n/M_{n+1}) \subseteq M_{m+n}/M_{m+n+1}.$$

Thus $\mathrm{gr}(M)$ is a graded module over the graded ring $\mathrm{gr}(R)$.

It is natural to ask for conditions under which a graded ring will be Noetherian, and the behavior of the subring R_0 is critical.

4.1.3 Proposition

Let $R = \oplus_{d \geq 0} R_d$ be a graded ring. Then R is Noetherian if and only if R_0 is Noetherian and R is a finitely generated R_0-algebra.

Proof. If the condition on R_0 holds, then R is a quotient of a polynomial ring $R_0[X_1, \dots, X_n]$, hence R is Noetherian by the Hilbert Basis Theorem. Conversely, if R is Noetherian, then so is R_0, because $R_0 \cong R/I$ where I is the ideal $\oplus_{d \geq 1} R_d$. By hypothesis, I is finitely generated, say by homogeneous elements $a_1, \dots, a_r$ of degree $n_1, \dots, n_r$ respectively. Let $R' = R_0[a_1, \dots, a_r]$ be the R_0-subalgebra of R generated by the a_i. It suffices to show that $R_n \subseteq R'$ for all $n \geq 0$ (and therefore $R = R'$). We have $R_0 \subseteq R'$ by definition of R', so assume as an induction hypothesis that $R_d \subseteq R'$ for $d \leq n-1$, where $n > 0$. If $a \in R_n$, then a can be expressed as $c_1 a_1 + \cdots + c_r a_r$, where c_i $(i = 1, \dots, r)$ must be a homogeneous element of degree $n - n_i < n = \deg a$. By induction hypothesis, $c_i \in R'$, and since $a_i \in R'$ we have $a \in R'$. ♣

We now prepare for the basic Artin-Rees lemma.

4.1.4 Definitions and Comments

Let M be a filtered R-module with filtration $\{M_n\}$, I an ideal of R. We say that $\{M_n\}$ is an *I-filtration* if $IM_n \subseteq M_{n+1}$ for all n. An I-filtration with $IM_n = M_{n+1}$ for all sufficiently large n is said to be *I-stable*. Note that the I-adic filtration is I-stable.

4.1.5 Proposition

Let M be a finitely generated module over a Noetherian ring R, and suppose that $\{M_n\}$ is an I-filtration of M. The following conditions are equivalent.

1. $\{M_n\}$ is I-stable.
2. Define a graded ring R^* and a graded R^*-module M^* by

$$R^* = \bigoplus_{n\geq 0} I^n, \quad M^* = \bigoplus_{n\geq 0} M_n.$$

   Then M^* is finitely generated.

Proof. Let $N_n = \oplus_{i=0}^n M_i$, and define

$$M_n^* = M_0 \oplus \cdots \oplus M_n \oplus IM_n \oplus I^2 M_n \oplus \cdots$$

Since N_n is finitely generated over R, it follows that M_n^* is a finitely generated R^*-module. By definition, M^* is the union of the M_n^* over all $n \geq 0$. Therefore M^* is finitely generated over R^* if and only if $M^* = M_m^*$ for some m, in other words, $M_{m+k} = I^k M_m$ for all $k \geq 1$. Equivalently, the filtration $\{M_n\}$ is I-stable. ♣

4.1.6 Induced Filtrations

If $\{M_n\}$ is a filtration of the R-module M, and N is a submodule of M, then we have filtrations induced on N and M/N, given by $N_n = N \cap M_n$ and $(M/N)_n = (M_n + N)/N$ respectively.

4.1.7 Artin-Rees Lemma

Let M be a finitely generated module over the Noetherian ring R, and assume that M has an I-stable filtration $\{M_n\}$, where I is an ideal of R. Let N be a submodule of M. Then the filtration $\{N_n = N \cap M_n\}$ induced by M on N is also I-stable.

Proof. As in (4.1.5), let $R^* = \oplus_{n\geq 0} I^n$, $\quad M^* = \oplus_{n\geq 0} M_n$, $\quad$ and $N^* = \oplus_{n\geq 0} N_n$. Since R is Noetherian, I is finitely generated, so R^* is a finitely generated R-algebra. (Elements of R^* can be expressed as polynomials in a finite set of generators of I.) By (4.1.3), R^* is a Noetherian ring. Now by hypothesis, M is finitely generated over the Noetherian ring R and $\{M_n\}$ is I-stable, so by (4.1.5), M^* is finitely generated over R^*. Therefore the submodule N^* is also finitely generated over R^*. Again using (4.1.5), we conclude that $\{N_n\}$ is I-stable. ♣

4.1.8 Applications

Let M be a finitely generated module over the Noetherian ring R, with N a submodule of M. The filtration on N induced by the I-adic filtration on M is given by $N_m = (I^m M) \cap N$. By Artin-Rees, for large enough m we have

$$I^k((I^m M) \cap N) = (I^{m+k} M) \cap N$$

for all $k \geq 0$.

There is a basic topological interpretation of this result. We can make M into a topological abelian group in which the module operations are continuous. The sets $I^m M$ are a base for the neighborhoods of 0, and the translations $x + I^m M$ form a basis for the neighborhoods of an arbitrary point $x \in M$. The resulting topology is called the *I-adic topology* on M. The above equation says that the I-adic topology on N coincides with the topology induced on N by the I-adic topology on M.

4.2 Completion of a Module

4.2.1 Inverse Limits

Suppose we have countably many R-modules $M_0, M_1, \dots,$ with R-module homomorphisms $\theta_n : M_n \to M_{n-1}, n \geq 1$. (We are restricting to the countable case to simplify the notation, but the ideas carry over to an arbitrary family of modules, indexed by a directed set. If $i \leq j$, we have a homomorphism f_{ij} from M_j to M_i. We assume that the maps can be composed consistently, in other words, if $i \leq j \leq k$, then $f_{ij} \circ f_{jk} = f_{ik}$.)The collection of modules and maps is called an *inverse system*.

A sequence (x_i) in the direct product $\prod M_i$ is said to be *coherent* if it respects the maps θ_n in the sense that for every i we have $\theta_{i+1}(x_{i+1}) = x_i$. The collection M of all coherent sequences is called the *inverse limit* of the inverse system. The inverse limit is denoted by

$$\varprojlim M_n.$$

Note that M becomes an R-module with componentwise addition and scalar multiplication of coherent sequences, in other words, $(x_i) + (y_i) = (x_i + y_i)$ and $r(x_i) = (rx_i)$.

Now suppose that we have homomorphisms g_i from an R-module M' to $M_i, i = 0, 1, \dots$. Call the g_i *coherent* if $\theta_{i+1} \circ g_{i+1} = g_i$ for all i. Then the g_i can be lifted to a homomorphism g from M' to M. Explicitly, $g(x) = (g_i(x))$, and the coherence of the g_i forces the sequence $(g_i(x))$ to be coherent.

An inverse limit of an inverse system of rings can be constructed in a similar fashion, as coherent sequences can be multiplied componentwise, that is, $(x_i)(y_i) = (x_i y_i)$.

4.2.2 Examples

1. Take $R = \mathbb{Z}$, and let I be the ideal (p) where p is a fixed prime. Take $M_n = \mathbb{Z}/I^n$ and $\theta_{n+1}(a + I^{n+1}) = a + I^n$. The inverse limit of the M_n is the ring $\mathbb{Z}_p$ of p-adic integers.

2. Let $R = A[x_1, \dots, x_n]$ be a polynomial ring in n variables, and I the maximal ideal $(x_1, \dots, x_n)$. Let $M_n = R/I^n$ and $\theta_n(f + I^n) = f + I^{n-1}, n = 1, 2, \dots$. An element of M_n is represented by a polynomial f of degree at most $n-1$. (We take the degree of f to be the maximum degree of a monomial in f.) The image of f in I^{n-1} is represented by the same polynomial with the terms of degree $n-1$ deleted. Thus the inverse limit can be identified with the ring $A[[x_1, \dots, x_n]]$ of formal power series.

Now let M be a filtered R-module with filtration $\{M_n\}$. The filtration determines a topology on M as in (4.1.8), with the M_n forming a base for the neighborhoods of 0. We have the following result.

4.2.3 Proposition

If N is a submodule of M, then the closure of N is given by $\overline{N} = \cap_{n=0}^{\infty}(N + M_n)$.

Proof. Let x be an element of M. Then x fails to belong to $\overline{N}$ iff some neighborhood of x is disjoint from N, in other words, $(x+M_n) \cap N = \emptyset$ for some n. Equivalently, $x \notin N + M_n$ for some n, and the result follows. To justify the last step, note that if $x \in N + M_n$, then $x = y + z$, $y \in N$, $z \in M_n$. Thus $y = x - z \in (x + M_n) \cap N$. Conversely, if $y \in (x + M_n) \cap N$, then for some $z \in M_n$ we have $y = x - z$, so $x = y + z \in N + M_n$. ♣

4.2.4 Corollary

The topology is Hausdorff if and only if $\cap_{n=0}^{\infty} M_n = \{0\}$.

Proof. By (4.2.3), $\cap_{n=0}^{\infty} M_n = \overline{\{0\}}$, so we are asserting that the Hausdorff property is equivalent to points being closed, that is, the T_1 condition. This holds because separating distinct points x and y by disjoint open sets is equivalent to separating $x - y$ from 0. ♣

4.2.5 Definition of the Completion

Let $\{M_n\}$ be a filtration of the R-module M. Recalling the construction of the reals from the rationals, or the process of completing an arbitrary metric space, let us try to come up with something similar in this case. If we go far out in a Cauchy sequence, the difference between terms becomes small. Thus we can define a *Cauchy sequence* $\{x_n\}$ *in* M by the requirement that for every positive integer r there is a positive integer N such that $x_n - x_m \in M_r$ for $n, m \geq N$. We identify the Cauchy sequences $\{x_n\}$ and $\{y_n\}$ if they get close to each other for large n. More precisely, given a positive integer r there exists a positive integer N such that $x_n - y_n \in M_r$ for all $n \geq N$. Notice that the condition $x_n - x_m \in M_r$ is equivalent to $x_n + M_r = x_m + M_r$. This suggests that the essential feature of the Cauchy condition is that the sequence is coherent with respect to the maps $\theta_n : M/M_n \to M/M_{n-1}$. Motivated by this observation, we define the *completion* of M as

$$\hat{M} = \varprojlim (M/M_n).$$

The functor that assigns the inverse limit to an inverse system of modules is left exact, and becomes exact under certain conditions.

4.2.6 Theorem

Let $\{M'_n, \theta'_n\}$, $\{M_n, \theta_n\}$, and $\{M''_n, \theta''_n\}$ be inverse systems of modules, and assume that the diagram below is commutative with exact rows.

$$\begin{tikzcd}
0 \arrow[r] & M'_{n+1} \arrow[r, "f_{n+1}"] \arrow[d, "\theta'_{n+1}"] & M_{n+1} \arrow[r, "g_{n+1}"] \arrow[d, "\theta_{n+1}"] & M''_{n+1} \arrow[r] \arrow[d, "\theta''_{n+1}"] & 0 \\
0 \arrow[r] & M'_n \arrow[r, "f_n"] & M_n \arrow[r, "g_n"] & M''_n \arrow[r] & 0
\end{tikzcd}$$

Then the sequence

$$0 \to \varprojlim M'_n \to \varprojlim M_n \to \varprojlim M''_n$$

is exact. If θ'_n is surjective for all n, then

$$0 \to \varprojlim M'_n \to \varprojlim M_n \to \varprojlim M''_n \to 0$$

is exact.

Proof. Let $M = \prod M_n$ and define an R- homomorphism $d_M : M \to M$ by $d_M(x_n) = (x_n - \theta_{n+1}(x_{n+1}))$. The kernel of d_M is the inverse limit of the M_n. Now the maps (f_n) and (g_n) induce $f = \prod f_n : M' = \prod M'_n \to M$ and $g = \prod g_n : M \to M'' = \prod M''_n$. We have the following commutative diagram with exact rows.

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "f"] \arrow[d, "d_{M'}"'] & M \arrow[r, "g"] \arrow[d, "d_M"] & M'' \arrow[r] \arrow[d, "d_{M''}"] & 0 \\
0 \arrow[r] & M' \arrow[r, "f"] & M \arrow[r, "g"] & M'' \arrow[r] & 0
\end{tikzcd}$$

We now apply the snake lemma, which is discussed in detail in TBGY (Section S2 of the supplement). The result is an exact sequence

$$0 \to \ker d_{M'} \to \ker d_M \to \ker d_{M''} \to \text{coker } d_{M'},$$

proving the first assertion. If θ'_n is surjective for all n, then $d_{M'}$ is surjective, and consequently the cokernel of $d_{M'}$ is 0. The second assertion follows. ♣

4.2.7 Corollary

Suppose that the sequence

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "f"] & M \arrow[r, "g"] & M'' \arrow[r] & 0
\end{tikzcd}$$

is exact. Let $\{M_n\}$ be a filtration of M, so that $\{M_n\}$ induces filtrations $\{M' \cap f^{-1}(M_n)\}$ and $\{g(M_n)\}$ on M' and M'' respectively. Then the sequence

$$0 \to (M')\hat{} \to \hat{M} \to (M'')\hat{} \to 0$$

is exact.

Proof. Exactness of the given sequence implies that the diagram below is commutative with exact rows.

$$\begin{tikzcd}
0 \arrow[r] & M'/(M' \cap f^{-1}(M_{n+1})) \arrow[r] \arrow[d, "\theta'_{n+1}"] & M/M_{n+1} \arrow[r] \arrow[d, "\theta_{n+1}"] & M''/g(M_{n+1}) \arrow[r] \arrow[d, "\theta''_{n+1}"] & 0 \\
0 \arrow[r] & M'/(M' \cap f^{-1}(M_n)) \arrow[r] & M/M_n \arrow[r] & M''/g(M_n) \arrow[r] & 0
\end{tikzcd}$$

Since θ_n is surjective for all n, (4.2.6) allows us to pass to the inverse limit. ♣

4.2.8 Remark

A filtration $\{M_n\}$ of an R-module M induces in a natural way a filtration $\{N \cap M_n\}$ on a given submodule N, and a filtration $\{(N + M_n)/N\}$ on the quotient module M/N. We have already noted this in (4.2.7) (with f the inclusion map and g the canonical epimorphism), but the point is worth emphasizing.

4.2.9 Corollary

Let $\{M_n\}$ be a filtration of the R-module M. Let $\hat{M}_n$ be the completion of M_n with respect to the induced filtration on M_n [see (4.2.8)]. Then $\hat{M}_n$ is a submodule of $\hat{M}$ and $\hat{M}/\hat{M}_n \cong M/M_n$ for all n.

Proof. We apply (4.2.7) with $M' = M_n$ and $M'' = M/M_n$, to obtain the exact sequence

$$0 \to \hat{M}_n \to \hat{M} \to (M/M_n)\hat{} \to 0.$$

Thus we may identify $\hat{M}_n$ with a submodule of $\hat{M}$, and

$$\hat{M}/\hat{M}_n \cong (M/M_n)\hat{} = (M'')\hat{}.$$

Now the m^{th} term of the induced filtration on M'' is

$$M''_m = (M_n + M_m)/M_n = M_n/M_n = 0$$

for $m \geq n$. Thus M'' has the discrete topology, so Cauchy sequences (and coherent sequences) can be identified with single points. Therefore M'' is isomorphic to its completion, and we have $\hat{M}/\hat{M}_n \cong M/M_n$ for every n. ♣

4.2.10 Remarks

Two filtrations $\{M_n\}$ and $\{M'_n\}$ of a given R-module are said to be *equivalent* if they induce the same topology. For example, under the hypothesis of (4.1.8), the filtrations $\{I^nN\}$ and $\{N \cap I^nM\}$ of the submodule N are equivalent (Problem 5). Since equivalent filtrations give rise to the same set of Cauchy sequences, it follows that completions of a given module with respect to equivalent filtrations are isomorphic.

4.3 The Krull Intersection Theorem

4.3.1 Definitions and Comments

Recall from (4.1.1) and (4.1.8) that the I-adic topology on the R-module M is the topology induced on M by the I-adic filtration $M_n = I^nM$. The completion of M with respect to the I-adic filtration is called the *I-adic completion*.

There is a natural map from a filtered module M to its completion $\hat{M}$ given by $x \to \{x + M_n\}$. The kernel of this map is $\cap_{n=0}^{\infty} M_n$, which is $\cap_{n=0}^{\infty} I^nM$ if the filtration is I-adic. The Krull intersection theorem (4.3.2) gives precise information about this kernel.

4.3.2 Theorem

Let M be a finitely generated module over the Noetherian ring R, I an ideal of R, and $\hat{M}$ the I-adic completion of M. Let N be the kernel of the natural map $M \to \hat{M}$. Then N is the set of elements $x \in M$ such that x is annihilated by some element of $1 + I$. In fact, we can find a single element of $1 + I$ that works for the entire kernel.

Proof. Suppose that $a \in I$, $x \in M$, and $(1 + a)x = 0$. Then

$$x = -ax = -a(-ax) = a^2x = a^2(-ax) = -a^3x = a^4x = \cdots ,$$

hence $x \in I^nM$ for all $n \geq 0$. Conversely, we must show that for some $a \in I$, $1 + a$ annihilates everything in the kernel N. By (4.1.8), for some n we have, for all $k \geq 0$,

$$I^k((I^nM) \cap N) = (I^{n+k}M) \cap N.$$

Set $k = 1$ to get

$$I((I^nM) \cap N) = (I^{n+1}M) \cap N.$$

But $N \subseteq I^{n+1}M \subseteq I^nM$, so the above equation says that $IN = N$. By (0.3.1), there exists $a \in I$ such that $(1 + a)N = 0$. ♣

4.3.3 Corollary

If I is a proper ideal of the Noetherian integral domain R, then $\cap_{n=0}^{\infty} I^n = 0$.

Proof. The intersection of the I^n is the kernel N of the natural map from R to $\hat{R}$. By (4.3.2), $1 + a$ annihilates N for some $a \in I$. If $0 \neq x \in N$ then $(1 + a)x = 0$, and since R is a domain, $1 + a = 0$. But then -1, hence 1, belongs to I, contradicting the hypothesis that I is proper. ♣

4.3.4 Corollary

Let M be a finitely generated module over the Noetherian ring R. If the ideal I of R is contained in the Jacobson radical $J(R)$, then $\cap_{n=0}^{\infty} I^nM = 0$. Thus by (4.2.4), the I-adic topology on M is Hausdorff.

Proof. Let $a \in I \subseteq J(R)$ be such that $(1 + a)$ annihilates the kernel $N = \cap_{n=0}^{\infty} I^nM$ of the natural map from M to $\hat{M}$. By (0.2.1), $1 + a$ is a unit of R, so if $x \in N$ (hence $(1 + a)x = 0$), we have $x = 0$. ♣

4.3.5 Corollary

Let R be a Noetherian local ring with maximal ideal $\mathcal{M}$. If M is a finitely generated R-module, then $\cap_{n=0}^{\infty}\mathcal{M}^n M = 0$. Thus the $\mathcal{M}$-adic topology on M, in particular the $\mathcal{M}$-adic topology on R, is Hausdorff.

Proof. Since $\mathcal{M} = J(R)$, this follows from (4.3.4). ♣

4.4 Hensel's Lemma

Let A be a local ring with maximal ideal P, and let $k = A/P$ be the residue field. Assume that A is complete with respect to the P-adic topology, in other words, every Cauchy sequence converges. In algebraic number theory, where this result is most often applied, A is a discrete valuation ring of a local field. But the statement and proof of the algebraic number theory result can be copied, as follows.

If $a \in A$, then the coset $a + P \in k$ will be denoted by $\overline{a}$. If f is a polynomial in $A[X]$, then reduction of the coefficients of f mod P yields a polynomial $\overline{f}$ in $k[X]$. Thus

$$f(X) = \sum_{i=0}^{d} a_i X^i \in A[X],\ \overline{f}(X) = \sum_{i=0}^{d} \overline{a}_i X^i \in k[X].$$

Hensel's lemma is about lifting a factorization of $\overline{f}$ from $k[X]$ to $A[X]$. Here is the precise statement.

4.4.1 Hensel's Lemma

Assume that f is a monic polynomial of degree d in $A[X]$, and that the corresponding polynomial $F = \overline{f}$ factors as the product of relatively prime monic polynomials G and H in $k[X]$. Then there are monic polynomials g and h in $A[X]$ such that $\overline{g} = G$, $\overline{h} = H$ and $f = gh$.

Proof. Let r be the degree of G, so that $\deg H = d - r$. We will inductively construct $g_n, h_n \in A[X], n = 1, 2, \dots,$ such that $\deg g_n = r$, $\deg h_n = d - r$, $\overline{g}_n = G$, $\overline{h}_n = H$, and

$$f(X) - g_n(X)h_n(X) \in P^n[X].$$

Thus the coefficients of $f - g_n h_n$ belong to P^n.

The basis step: Let $n = 1$. Choose monic $g_1, h_1 \in A[X]$ such that $\overline{g}_1 = G$ and $\overline{h}_1 = H$. Then $\deg g_1 = r$ and $\deg h_1 = d - r$. Since $\overline{f} = \overline{g}_1\overline{h}_1$, we have $f - g_1h_1 \in P[X]$.

The inductive step: Assume that g_n and h_n have been constructed. Let $f(X)-g_n(X)h_n(X) = \sum_{i=0}^{d} c_i X^i$ with the $c_i \in P^n$. Since $G = \overline{g}_n$ and $H = \overline{h}_n$ are relatively prime, for each $i = 0, \dots, d$ there are polynomials $\overline{v}_i$ and $\overline{w}_i$ in $k[X]$ such that

$$X^i = \overline{v}_i(X)\overline{g}_n(X) + \overline{w}_i(X)\overline{h}_n(X).$$

Since $\overline{g}_n$ has degree r, the degree of $\overline{v}_i$ is at most $d - r$, and similarly the degree of $\overline{w}_i$ is at most r. Moreover,

$$X^i - v_i(X)g_n(X) - w_i(X)h_n(X) \in P[X]. \qquad (1)$$

We define

$$g_{n+1}(X) = g_n(X) + \sum_{i=0}^{d} c_i w_i(X),\ h_{n+1}(X) = h_n(X) + \sum_{i=0}^{d} c_i v_i(X).$$

Since the c_i belong to $P^n \subseteq P$, it follows that $\overline{g}_{n+1} = \overline{g}_n = G$ and $\overline{h}_{n+1} = \overline{h}_n = H$. Since the degree of g_{n+1} is at most r, it must be exactly r, and similarly the degree of h_{n+1} is $d-r$. To check the remaining condition,

$$f - g_{n+1}h_{n+1} = f - (g_n + \sum_i c_i w_i)(h_n + \sum_i c_i v_i)$$

$$= (f - g_n h_n - \sum_i c_i X^i) + \sum_i c_i(X^i - g_n v_i - h_n w_i) - \sum_{i,j} c_i c_j w_i v_j.$$

By the induction hypothesis, the first grouped term on the right is zero, and, with the aid of Equation (1) above, the second grouped term belongs to $P^n P[X] = P^{n+1}[X]$. The final term belongs to $P^{2n}[X] \subseteq P^{n+1}[X]$, completing the induction.

Finishing the proof. By definition of g_{n+1}, we have $g_{n+1} - g_n \in P^n[X]$, so for any fixed i, the sequence of coefficients of X^i in $g_n(X)$ is Cauchy and therefore converges. To simplify the notation we write $g_n(X) \to g(X)$, and similarly $h_n(X) \to h(X)$, with $g(X), h(X) \in A[X]$. By construction, $f - g_n h_n \in P^n[X]$, and we may let $n \to \infty$ to get $f = gh$. Since $\overline{g}_n = G$ and $\overline{h}_n = H$ for all n, we must have $\overline{g} = G$ and $\overline{h} = H$. Since f, G and H are monic, the highest degree terms of g and h are of the form $(1+a)X^r$ and $(1+a)^{-1}X^{d-r}$ respectively, with $a \in P$. (Note that $1+a$ must reduce to 1 mod P.) By replacing g and h by $(1+a)^{-1}g$ and $(1+a)h$, respectively, we can make g and h monic without disturbing the other conditions. The proof is complete. ♣

Chapter 5

Dimension Theory

The geometric notion of the dimension of an affine algebraic variety V is closely related to algebraic properties of the coordinate ring of the variety, that is, the ring of polynomial functions on V. This relationship suggests that we look for various ways of defining the dimension of an arbitrary commutative ring. We will see that under appropriate hypotheses, several concepts of dimension are equivalent. Later, we will connect the algebraic and geometric ideas.

5.1 The Calculus of Finite Differences

Regrettably, this charming subject is rarely taught these days, except in actuarial programs. It turns out to be needed in studying Hilbert and Hilbert-Samuel polynomials in the next section.

5.1.1 Lemma

Let g and G be real-valued functions on the nonnegative integers, and assume that $\Delta G = g$, that is, $G(k+1) - G(k) = g(k)$ for all $k \geq 0$. (We call ΔG the *difference* of G.) Then

$$\sum_{k=a}^{b} g(k) = G(k)|_a^{b+1} = G(b+1) - G(a).$$

Proof. Add the equations $G(a+1) - G(a) = g(a)$, $G(a+2) - G(a+1) = g(a+1)$, $\dots$, $G(b+1) - G(b) = g(b)$. ♣

5.1.2 Lemma

If r is a positive integer, define $k^{(r)} = k(k-1)(k-2)\cdots(k-r+1)$. Then $\Delta k^{(r)} = rk^{(r-1)}$.

Proof. Just compute:

$$\begin{aligned}\Delta k^{(r)} &= (k+1)^{(r)} - k^{(r)} = (k+1)k(k-1)\cdots(k-r+2) - k(k-1)\cdots(k-r+1)\\ &= k(k-1)\cdots(k-r+2)[k+1-(k-r+1)] = rk^{(r-1)}. \ ♣\end{aligned}$$

5.1.3 Examples

$\Delta k^{(2)} = 2k^{(1)}$, so $\sum_{k=1}^{n} k = [k^{(2)}/2]|_1^{n+1} = (n+1)n/2$.
$k^2 = k(k-1) + k = k^{(2)} + k^{(1)}$, so

$$\begin{aligned}\sum_{k=1}^{n} k^2 &= [k^{(3)}/3]|_1^{n+1} + (n+1)n/2 = (n+1)n(n-1)/3 + (n+1)n/2 \\ &= n(n+1)(2n+1)/6.\end{aligned}$$

$k^{(3)} = k(k-1)(k-2) = k^3 - 3k^2 + 2k$, so $k^3 = k^{(3)} + 3k^2 - 2k$. Therefore

$$\sum_{k=1}^{n} k^3 = [k^{(4)}/4]|_1^{n+1} + 3n(n+1)(2n+1)/6 - 2n(n+1)/2.$$

The first term on the right is $(n+1)n(n-1)(n-2)/4$, so the sum of the first n cubes is

$$[n(n+1)/4][n^2 - 3n + 2 + 2(2n+1) - 4]$$

which simplifies to $[n(n+1)/2]^2$.

In a similar fashion we can find $\sum_{k=1}^{n} k^s$ for any positive integer s.

5.1.4 Definitions and Comments

A *polynomial-like function* is a function f from the natural numbers (nonnegative integers) $\mathbb{N}$ to the rational numbers $\mathbb{Q}$, such that f eventually agrees with a polynomial $g \in \mathbb{Q}[X]$. In other words, $f(n) = g(n)$ for all sufficiently large n (abbreviated $n >> 0$). The *degree* of f is taken to be the degree of g.

5.1.5 Lemma

Let $f : \mathbb{N} \to \mathbb{Q}$. Then f is a polynomial-like function of degree r if and only if Δf is a polynomial-like function of degree $r - 1$. (We can allow $r = 0$ if we take the degree of the zero polynomial to be -1.)

Proof. This follows from (5.1.1) and (5.1.2), along with the observation that a function whose difference is zero is constant. (The analogous result from differential calculus that a function with zero derivative is constant is harder to prove, and is usually accomplished via the mean value theorem.) ♣

5.2 Hilbert and Hilbert-Samuel Polynomials

There will be two polynomial-like functions of interest, and we begin preparing for their arrival.

5.2.1 Proposition

Let $R = \oplus_{n\geq 0} R_n$ be a graded ring. Assume that R_0 is Artinian and R is finitely generated as an algebra over R_0. If $M = \oplus_{n\geq 0} M_n$ is a finitely generated graded R-module, then each M_n is a finitely generated R_0-module.

Proof. By (4.1.3) and (1.6.13), R is a Noetherian ring, hence M is a Noetherian R-module. Let N_n be the direct sum of the $M_m, m \geq n$. Since M is Noetherian, N_n is finitely generated over R, say by $x_1, \ldots, x_t$. Since $N_n = M_n \oplus \oplus_{m>n} M_m$, we can write $x_i = y_i + z_i$ with $y_i \in M_n$ and $z_i \in \oplus_{m>n} M_m$. It suffices to prove that $y_1, \ldots, y_t$ generate M_n over R_0. If $y \in M_n$, then y is of the form $\sum_{i=1}^t a_i x_i$ with $a_i \in R$. But just as we decomposed x_i above, we can write $a_i = b_i + c_i$ where $b_i \in R_0$ and $c_i \in \oplus_{j>0} R_j$. Thus

$$y = \sum_{i=1}^t (b_i + c_i)(y_i + z_i) = \sum_{i=1}^t b_i y_i$$

because the elements $b_i z_i, c_i y_i$ and $c_i z_i$ must belong to $\oplus_{m>n} M_m$. ♣

5.2.2 Corollary

In (5.2.1), the length $l_{R_o}(M_n)$ of the R_0-module M_n is finite for all $n \geq 0$.

Proof. Apply (5.2.1) and (1.6.14). ♣

We will need the following basic property of composition length.

5.2.3 Additivity of Length

Suppose we have an exact sequence of R-modules $0 \to A_1 \to A_2 \to \cdots \to A_n \to 0$, all with finite length. Then we have *additivity of length*, that is,

$$l(A_1) - l(A_2) + \cdots + (-1)^{n-1} l(A_n) = 0.$$

This is probably familiar for a short exact sequence $0 \to N \to M \to M/N \to 0$, where the additivity property can be expressed as $l(M) = l(N) + l(M/N)$. (See TBGY, Section 7.5, Problem 5.) The general result is accomplished by decomposing a long exact sequence into short exact sequences. ("Long" means longer than short.) To see how the process works, consider an exact sequence

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \xrightarrow{i} E \longrightarrow 0.$$

Our first short exact sequence is

$$0 \to A \to B \to \operatorname{coker} f \to 0.$$

Now $\operatorname{coker} f = B/\operatorname{im} f = B/\ker g \cong \operatorname{im} g$ ($= \ker h$), so our second short exact sequence is

$$0 \to \operatorname{im} g \to C \to \operatorname{coker} g \to 0.$$

As above, $\operatorname{coker} g \cong \operatorname{im} h$ ($= \ker i$), so the third short exact sequence is

$$0 \to \operatorname{im} h \to D \to \operatorname{coker} h \to 0.$$

But $\operatorname{coker} h \cong \operatorname{im} i = E$, so we may replace the third short exact sequence by

$$0 \to \operatorname{im} h \to D \to E \to 0.$$

Applying additivity for short exact sequences, we have

$$l(A) - l(B) + l(\operatorname{coker} f) - l(\operatorname{im} g) + l(C) - l(\operatorname{coker} g) + l(\operatorname{im} h) - l(D) + l(E) = 0.$$

After cancellation, this becomes

$$l(A) - l(B) + l(C) - l(D) + l(E) = 0$$

as desired.

5.2.4 Theorem

Let $R = \oplus_{n \geq 0} R_n$ be a graded ring. Assume that R_0 is Artinian and R is finitely generated as an algebra over R_0, with all generators $a_1, \dots, a_r$ belonging to R_1. If M is a finitely generated graded R-module, define $h(M,n) = l_{R_0}(M_n), n \in \mathbb{N}$. Then h, as a function of n with M fixed, is polynomial-like of degree at most $r-1$. Using slightly loose language, we call h the *Hilbert polynomial* of M.

Proof. We argue by induction on r. If $r = 0$, then $R = R_0$. Choose a finite set of homogeneous generators for M over R. If d is the maximum of the degrees of the generators, then $M_n = 0$ for $n > d$, and therefore $h(M,n) = 0$ for $n >> 0$. Now assume $r > 0$, and let λ_r be the endomorphism of M given by multiplication by a_r. By hypothesis, $a_r \in R_1$, so $\lambda_r(M_n) \subseteq M_{n+1}$. if K_n is the kernel, and C_n the cokernel, of $\lambda_r : M_n \to M_{n+1}$, we have the exact sequence

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{\lambda_r} M_{n+1} \longrightarrow C_n \longrightarrow 0.$$

Let K be the direct sum of the K_n and C the direct sum of the C_n, $n \geq 0$. Then K is a submodule of M and C a quotient of M. Thus K and C are finitely generated Noetherian graded R-modules, so by (5.2.1) and (5.2.2), $h(K,n)$ and $h(C,n)$ are defined and finite. By (5.2.3),

$$h(K,n) - h(M,n) + h(M,n+1) - h(C,n) = 0$$

hence $\Delta h(M,n) = h(C,n) - h(K,n)$. Now a_r annihilates K and C, so K and C are finitely generated T-modules, where T is the graded subring of R generated over R_0 by $a_1, \dots, a_{r-1}$. (If an ideal I annihilates an R-module M, then M is an R/I-module; see TBGY, Section 4.2, Problem 6.) By induction hypothesis, $h(K,n)$ and $h(C,n)$ are polynomial-like of degree at most $r-2$, hence so is $\Delta h(M,n)$. By (5.1.5), $h(M,n)$ is polynomial-like of degree at most $r-1$. ♣

5.2.5 Definitions and Comments

Let R be any Noetherian local ring with maximal ideal $\mathcal{M}$. An ideal I of R is said to be an *ideal of definition* if $\mathcal{M}^n \subseteq I \subseteq \mathcal{M}$ for some $n \geq 1$. Equivalently, R/I is an Artinian ring. [See (3.3.10), and note that $\sqrt{I} = \mathcal{M}$ if and only if every prime ideal containing I is maximal, so (1.6.11) applies.]

5.2.6 The Hilbert-Samuel Polynomial

Let I be an ideal of definition of the Noetherian local ring R. If M is a finitely generated R-module, then M/IM is a finitely generated module over the Artinian ring R/I. Thus M/IM is Artinian (as well as Noetherian), hence has finite length over R/I. With the I-adic filtrations on R and M, the associated graded ring and the associated graded module [see (4.1.2)] are given by

$$\mathrm{gr}_I(R) = \oplus_{n\geq 0}(I^n/I^{n+1}), \quad \mathrm{gr}_I(M) = \oplus_{n\geq 0}(I^nM/I^{n+1}M).$$

If I is generated over R by $a_1, \ldots, a_r$, then the images $\overline{a}_1, \ldots, \overline{a}_r$ in I/I^2 generate $\mathrm{gr}_I(R)$ over R/I. (Note that by definition of a graded ring, $R_iR_j \subseteq R_{i+j}$, which allows us to produce elements in R_t for arbitrarily large t.) By (5.2.4),

$$h(\mathrm{gr}_I(M), n) = l_{R/I}(I^nM/I^{n+1}M) < \infty.$$

Again recall that if N is an R-module and the ideal I annihilates N, then N becomes an R/I-module via $(a+I)x = ax$. It follows that we may replace $l_{R/I}$ by l_R in the above formula. We define the *Hilbert-Samuel polynomial* by

$$s_I(M, n) = l_R(M/I^nM).$$

Now the sequence

$$0 \to I^nM/I^{n+1}M \to M/I^{n+1}M \to M/I^nM \to 0$$

is exact by the third isomorphism theorem. An induction argument using additivity of length shows that $s_I(M, n)$ is finite. Consequently

$$\Delta s_I(M, n) = s_I(M, n+1) - s_I(M, n) = h(\mathrm{gr}_I(M), n).$$

By (5.2.4), $h(\mathrm{gr}_I(M), n)$ is polynomial-like of degree at most $r-1$, so by (5.1.5), $s_I(M, n)$ is polynomial like of degree at most r.

The Hilbert-Samuel polynomial $s_I(M, n)$ depends on the particular ideal of definition I, but the degree $d(M)$ of $s_I(M, n)$ is the same for all possible choices. To see this, let t be a positive integer such that $\mathcal{M}^t \subseteq I \subseteq \mathcal{M}$. Then for every $n \geq 1$ we have $\mathcal{M}^{tn} \subseteq I^n \subseteq \mathcal{M}^n$, so $s_{\mathcal{M}}(M, tn) \geq s_I(M, n) \geq s_{\mathcal{M}}(M, n)$. If the degrees of these polynomial are, from right to left, d_1, d_2 and d_3, we have $O(d_1^n) \leq O(d_2^n) \leq O(d_3^n)$, with $d_3 = d_1$. Therefore all three degrees coincide.

The Hilbert-Samuel polynomial satisfies a property analogous to (4.1.7), the additivity of length.

5.2.7 Theorem

Let I be an ideal of definition of the Noetherian local ring R, and suppose we have an exact sequence $0 \to M' \to M \to M'' \to 0$ of finitely generated R-modules. Then

$$s_I(M', n) + s_I(M'', n) = s_I(M, n) + r(n)$$

where $r(n)$ is polynomial-like of degree less than $d(M)$, and the leading coefficient of $r(n)$ is nonnegative.

Proof. The following sequence is exact:

$$0 \to M'/(M' \cap I^n M) \to M/I^n M \to M''/I^n M'' \to 0.$$

Set $M'_n = M' \cap I^n M$. Then by additivity of length,

$$s_I(M,n) - s_I(M'',n) = l_R(M'/M'_n)$$

hence $l_R(M'/M'_n)$ is polynomial-like. By the Artin-Rees lemma (4.1.7), the filtration $\{M'_n\}$ is I-stable, so $IM'_n = M'_{n+1}$ for sufficiently large n, say, $n \geq m$. Thus for every $n \geq 0$ we have $M'_{n+m} = M' \cap I^{n+m}M \supseteq I^{n+m}M'$, and consequently

$$I^{n+m}M' \subseteq M'_{n+m} = I^n M'_m \subseteq I^n M',$$

which implies that

$$l_R(M'/I^{n+m}M') \geq l_R(M'/M'_{n+m}) \geq l_R(M'/I^n M').$$

The left and right hand terms of this inequality are $s_I(M', n+m)$ and $s_I(M',n)$ respectively, and it follows that $s_I(M',n)$ and $l_R(M'/M'_n)$ have the same degree and the same leading coefficient. Moreover, $s_I(M',n) - l_R(M'/M'_n) = r(n)$ is polynomial-like of degree less than $\deg l_R(M'/M'_n) \leq \deg s_I(M,n)$, as well as nonnegative for $n >> 0$. The result now follows upon adding the equations

$$s_I(M,n) - s_I(M'',n) = l_R(M'/M'_n)$$

and

$$r(n) = s_I(M',n) - l_R(M'/M'_n). \quad \clubsuit$$

5.2.8 Corollary

Let M' be a submodule of M, where M is a finitely generated module over the Noetherian local ring R. Then $d(M') \leq d(M)$.

Proof. Apply (5.2.7), noting that we can ignore $r(n)$ because it is of lower degree than $s_I(M,n)$. $\clubsuit$

5.3 The Dimension Theorem

5.3.1 Definitions and Comments

The *dimension* of a ring R, denoted by $\dim R$, will be taken as its *Krull dimension*, the maximum length n of a chain $P_0 \subset P_1 \subset \cdots \subset P_n$ of prime ideals of R. If there is no upper bound on the length of such a chain, we take $n = \infty$. An example of an infinite-dimensional ring is the non-Noetherian ring $k[X_1, X_2, \dots]$, where k is a field. We have the infinite chain of prime ideals $(X_1) \subset (X_1, X_2) \subset (X_1, X_2, X_3) \subset \cdots$. At the other extreme, a field, and more generally an Artinian ring, has dimension 0 by (1.6.4).

A *Dedekind domain* is a Noetherian, integrally closed integral domain in which every nonzero prime ideal is maximal. A Dedekind domain that is not a field has dimension 1. Algebraic number theory provides many examples, because the ring of algebraic integers of a number field is a Dedekind domain.

There are several other ideas that arise from the study of chains of prime ideals. We define the *height* of a prime ideal P (notation $\operatorname{ht} P$) as the maximum length n of a chain of prime ideals $P_0 \subset P_1 \subset \cdots \subset P_n = P$. By (0.4.6), the height of P is the dimension of the localized ring R_P.

The *coheight* of the prime ideal P (notation $\operatorname{coht} P$) is the maximum length n of a chain of prime ideals $P = P_0 \subset P_1 \subset \cdots \subset P_n$. It follows from the correspondence theorem and the third isomorphism theorem that the coheight of P is the dimension of the quotient ring R/P. (If I and J are ideals of R with $I \subseteq J$, and $S = (R/I)/(J/I)$, then $S \cong R/J$, so S is an integral domain iff R/J is an integral domain, and J/I is a prime ideal of R/I iff J is a prime ideal of R.)

If I is an arbitrary ideal of R, we define the height of I as the infimum of the heights of prime ideals $P \supseteq I$, and the coheight of I as the supremum of the coheights of prime ideals $P \supseteq I$.

5.3.2 The Dimension of a Module

Intuitively, the *dimension* of an R-module M, denoted by $\dim M$, will be measured by length of chains of prime ideals, provided that the prime ideals in the chain contribute to M in the sense that they belong to the support of M. Formally, we define $\dim M = \dim(R/\operatorname{ann} M)$ if $M \neq 0$, and we take the dimension of the zero module to be -1.

We now assume that M is nonzero and finitely generated over the Noetherian ring R. By (1.3.3), M has at least one associated prime. By (1.5.5), $P \supseteq \operatorname{ann} M$ iff $P \in \operatorname{Supp} M$, and by (1.5.9), the minimal elements of $\operatorname{AP}(M)$ and $\operatorname{Supp} M$ are the same. Thus

$$\dim M = \sup\{\operatorname{coht} P : P \in \operatorname{Supp} M\} = \sup\{\operatorname{coht} P : P \in \operatorname{AP}(M)\}.$$

By (1.6.9), the following conditions are equivalent.

1. $\dim M = 0$;
2. Every prime ideal in $\operatorname{Supp} M$ is maximal;
3. Every associated prime ideal of M is maximal;
4. The length of M as an R-module is finite.

We make the additional assumption that R is a local ring with maximal ideal $\mathcal{M}$. Then by (1.5.5),

$$\operatorname{Supp}(M/\mathcal{M}M) = V(\operatorname{ann}(M/\mathcal{M}M))$$

which coincides with $\{\mathcal{M}\}$ by Problem 2. By the above equivalent conditions, $l_R(M/\mathcal{M}M)$ is finite. Since $\mathcal{M}$ is finitely generated, we can assert that there is a smallest positive integer r, called the *Chevalley dimension* $\delta(M)$, such that for some elements $a_1, \dots, a_r$ belonging to $\mathcal{M}$ we have $l_R(M/(a_1, \dots, a_r)M < \infty$. If $M = 0$ we take $\delta(M) = -1$.

5.3.3 Dimension Theorem

Let M be a finitely generated module over the Noetherian local ring R. The following quantities are equal:
1. The dimension $\dim M$ of the module M;
2. The degree $d(M)$ of the Hilbert-Samuel polynomial $s_I(M,n)$, where I is any ideal of definition of R. (For convenience we take $I=\mathcal{M}$, the maximal ideal of R, and we specify that the degree of the zero polynomial is -1.);
3. The Chevalley dimension $\delta(M)$.

Proof. We divide the proof into three parts.

1. $\dim M \le d(M)$, hence $\dim M$ is finite.

If $d(M)=-1$, then $s_{\mathcal{M}}(M,n)=l_R(M/\mathcal{M}^nM)=0$ for $n>>0$. By NAK, $M=0$ so $\dim M=-1$. Thus assume $d(M)\ge 0$. By (1.3.9) or (1.5.10), M has only finitely many associated primes. It follows from (5.3.2) and (5.3.1) that for some associated prime P we have $\dim M = \operatorname{coht} P = \dim R/P$. By (1.3.2) there is an injective homomorphism from R/P to M, so by (5.2.8) we have $d(R/P)\le d(M)$. If we can show that $\dim R/P \le d(R/P)$, it will follow that $\dim M = \dim R/P \le d(R/P) \le d(M)$.

It suffices to show that for any chain of prime ideals $P=P_0\subset\cdots\subset P_t$ in R, the length t of the chain is at most $d(R/P)$. If $t=0$, then $R/P\neq 0$ (because P is prime), hence $d(R/P)\neq -1$ and we are finished. Thus assume $t\ge 1$, and assume that the result holds up to $t-1$. Choose $a\in P_1\setminus P$, and consider prime ideals Q such that $Ra+P\subseteq Q\subseteq P_1$. We can pick a Q belonging to $\operatorname{AP}(R/(Ra+P))$. [Since $Ra+P\subseteq Q$, we have $(R/(Ra+P))_Q\neq 0$; see Problem 3. Then choose Q to be a minimal element in the support of $R/(Ra+P)$, and apply (1.5.9).] By (1.3.2) there is an injective homomorphism from R/Q to $R/(Ra+P)$, so by (5.2.8) we have $d(R/Q)\le d(R/(Ra+P))$. Since the chain $Q\subset P_2\subset\cdots\subset Q_r$ is of length $t-1$, the induction hypothesis implies that $t-1\le d(R/Q)$, hence $t-1\le d(R/(Ra+P))$. Now the sequence

$$0\to R/P\to R/P\to R/(Ra+P)\to 0$$

is exact, where the map from R/P to itself is multiplication by a. (The image of the map is $Ra+P$.) By (5.2.7),

$$s_{\mathcal{M}}(R/P,n)+s_{\mathcal{M}}(R/(Ra+P),n)=s_{\mathcal{M}}(R/P,n)+r(n)$$

where $r(n)$ is polynomial-like of degree less than $d(R/P)$. Thus $d(R/(Ra+P))<d(R/P)$, and consequently $t-1<d(R/P)$. Therefore $t\le d(R/P)$, as desired.

2. $d(M)\le\delta(M)$.

If $\delta(M)=-1$, then $M=0$ and $d(M)=-1$. Assume $M\neq 0$ and $r=\delta(M)\ge 0$, and let $a_1,\dots,a_r$ be elements of $\mathcal{M}$ such that $M/(a_1,\dots,a_r)M$ has finite length. Let I be the ideal $(a_1,\dots,a_r)$ and let P be the annihilator of M; set $Q=I+P$.

We claim that the support of R/Q is $\{\mathcal{M}\}$. To prove this, first note that $M/IM\cong M\otimes_R R/I$. (TBGY, subsection S7.1 of the supplement.) By Problem 9 of Chapter 1, $\operatorname{Supp} M/IM = \operatorname{Supp} M\cap\operatorname{Supp} R/I$, which by (1.5.5) is $V(P)\cap V(I)=V(Q)=\operatorname{Supp} R/Q$. (Note that the annihilator of R/I is I and the annihilator of R/Q is Q.) But the support of M/IM is $\{\mathcal{M}\}$ by (1.6.9), proving the claim. (If $M/IM = 0$, then $M = 0$ by NAK, contradicting our assumption.)

Again by (1.6.9), $\operatorname{AP}(R/Q) = \{\mathcal{M}\}$, so by (1.3.11), Q is $\mathcal{M}$-primary. By (5.2.5) and (3.3.10), Q is an ideal of definition of R.

Let $\overline{R} = R/P$, $\overline{Q} = Q/P$, and consider M as an $\overline{R}$-module. Then $\overline{R}$ is a Noetherian local ring and $\overline{Q}$ is an ideal of definition of $\overline{R}$ generated by $\overline{a}_1, \dots, \overline{a}_r$, where $\overline{a}_i = a_i + P$. By (5.2.6), the degree of the Hilbert-Samuel polynomial $s_{\overline{Q}}(M,n)$ is at most r. But by the correspondence theorem, $l_{\overline{R}}(M/\overline{Q}^n M) = l_R(M/Q^n M)$, hence $s_{\overline{Q}}(M,n) = s_Q(M,n)$. It follows that $d(M) \le r$.

3. $\delta(M) \le \dim M$.

If $\dim M = -1$ then $M = 0$ and $\delta(M) = -1$, so assume $M \ne 0$. If $\dim M = 0$, then by (5.3.2), M has finite length, so $\delta(M) = 0$.

Now assume $\dim M > 0$. (We have already noted in part 1 that $\dim M$ is finite.) Let $P_1, \dots, P_t$ be the associated primes of M whose coheight is as large as it can be, that is, $\operatorname{coht} P_i = \dim M$ for all $i = 1, \dots, t$. Since the dimension of M is greater than 0, $P_i \subset \mathcal{M}$ for every i, so by the prime avoidance lemma (0.1.1),

$$\mathcal{M} \not\subseteq \cup_{1 \le i \le t} P_i.$$

Choose an element a in $\mathcal{M}$ such a belongs to none of the P_i, and let $N = M/aM$. Then

$$\operatorname{Supp} N \subseteq \operatorname{Supp} M \setminus \{P_1, \dots, P_t\}.$$

To see this, note that if $N_P \ne 0$, then $M_P \ne 0$; also, $N_{P_i} = 0$ for all i because $a \notin P_i$, hence division by a is allowed. Thus $\dim N < \dim M$, because $\dim M = \operatorname{coht} P_i$ and we are removing all the P_i. Let $r = \delta(N)$, and let $a_1, \dots, a_r$ be elements of $\mathcal{M}$ such that $N/(a_1, \dots, a_r)N$ has finite length. But

$$M/(a, a_1, \dots, a_r)M \cong N/(a_1, \dots, a_r)N$$

(apply the first isomorphism theorem) , so $M/(a, a_1, \dots, a_r)M$ also has finite length. Thus $\delta(M) \le r + 1$. By the induction hypothesis, $\delta(N) \le \dim N$. In summary,

$$\delta(M) \le r + 1 = \delta(N) + 1 \le \dim N + 1 \le \dim M. \ \clubsuit$$

5.4 Consequences of the Dimension Theorem

In this section we will see many applications of the dimension theorem (5.3.3).

5.4.1 Proposition

Let R be a Noetherian local ring with maximal ideal $\mathcal{M}$. If M is a finitely generated R-module, then $\dim M < \infty$; in particular, $\dim R < \infty$. Moreover, the dimension of R is the minimum, over all ideals I of definition of R, of the number of generators of I.

Proof. Finiteness of dimension follows from (5.3.3). The last assertion follows from the definition of Chevalley dimension in (5.3.2). In more detail, R/I has finite length iff (by the Noetherian hypothesis) R/I is Artinian iff [by (5.2.5)] I is an ideal of definition. ♣

5.4.2 Proposition

Let R be a Noetherian local ring with maximal ideal $\mathcal{M}$ and residue field $k = R/\mathcal{M}$. Then $\dim R \le \dim_k(\mathcal{M}/\mathcal{M}^2)$.

Proof. Let $a_1, \dots, a_r$ be elements of $\mathcal{M}$ such that $\overline{a}_1, \dots, \overline{a}_r$ form a k-basis of $\mathcal{M}/\mathcal{M}^2$, where $\overline{a}_i = a_i + \mathcal{M}$. Then by (0.3.4), $a_1, \dots, a_r$ generate $\mathcal{M}$. Since $\mathcal{M}$ itself is an ideal of definition (see (5.2.5)), we have $\dim R \le r$ by (5.4.1). (Alternatively, by (5.4.5), the height of $\mathcal{M}$ is at most r. Since ht $\mathcal{M} = \dim R$, the result follows.) ♣

5.4.3 Proposition

Let R be Noetherian local ring with maximal ideal $\mathcal{M}$, and $\hat{R}$ its $\mathcal{M}$-adic completion. Then $\dim R = \dim \hat{R}$.

Proof. By (4.2.9), $R/\mathcal{M}^n \cong \hat{R}/\hat{\mathcal{M}}^n$. By (5.2.6), $s_{\mathcal{M}}(R, n) = s_{\hat{\mathcal{M}}}(\hat{R}, n)$. In particular, the two Hilbert-Samuel polynomials must have the same degree. Therefore $d(R) = d(\hat{R})$, and the result follows from (5.3.3). ♣

5.4.4 Theorem

If R is a Noetherian ring, then the prime ideals of R satisfy the descending chain condition.

Proof. We may assume without loss of generality that R is a local ring. Explicitly, if P_0 is a prime ideal of R, let A be the localized ring R_{P_0}. Then the chain $P_0 \supset P_1 \supset P_2 \supset \dots$ of prime ideals of R will stabilize if and only if the chain $AP_0 \supset AP_1 \supset AP_2 \supset \cdots$ of prime ideals of A stabilizes. But if R is local as well as Noetherian, the result is immediate because $\dim R < \infty$. ♣

5.4.5 Generalization of Krull's Principal Ideal Theorem

Let P be a prime ideal of the Noetherian ring R. The following conditions are equivalent:
(a) ht $P \le n$;
(b) There is an ideal I of R that is generated by n elements, such that P is a minimal prime ideal over I. (In other words, P is minimal subject to $P \supseteq I$.)

Proof. If (b) holds, then IR_P is an ideal of definition of R_P that is generated by n elements. (See (3.3.10), and note that if P is minimal over I iff $\sqrt{I} = P$.) By (5.3.1) and (5.4.1), ht $P = \dim R_P \le n$. Conversely, if (a) holds then $\dim R_P \le n$, so by (5.4.1) there is an ideal of definition J of R_P generated by n elements $a_1/s, \dots, a_n/s$ with $s \in R \setminus P$. The elements a_i must belong to P, else the a_i/s will generate R_P, which is a contradiction because J must be proper; see (5.2.5). Take I to be the ideal of R generated by $a_1, \dots, a_n$. Invoking (3.3.10) as in the first part of the proof, we conclude that I satisfies (b). ♣

5.4.6 Krull's Principal Ideal Theorem

Let a be a nonzero element of the Noetherian ring R. If a is neither a unit nor a zero-divisor, then every minimal prime ideal P over (a) has height 1.

Proof. It follows from (5.4.5) that ht $P \leq 1$. Thus assume ht $P = \dim R_P = 0$. We claim that $R_P \neq 0$, hence $P \in \operatorname{Supp} R$. For if $a/1 = 0$, then for some $s \in R \setminus P$ we have $sa = 0$, which contradicts the hypothesis that a is not a zero-divisor. We may assume that P is minimal in the support of R, because otherwise P has height 1 and we are finished. By (1.5.9), P is an associated prime of R, so by (1.3.6), P consists entirely of zero-divisors, a contradiction. ♣

The hypothesis that a is not a unit is never used, but nothing is gained by dropping it. If a is a unit, then a cannot belong to the prime ideal P and the theorem is vacuously true.

5.4.7 Theorem

Let R be a Noetherian local ring with maximal ideal $\mathcal{M}$, and let $a \in \mathcal{M}$ be a non zero-divisor. Then $\dim R/(a) = \dim R - 1$.

Proof. We have $\dim R > 0$, for if $\dim R = 0$, then $\mathcal{M}$ is the only prime ideal, and as in the proof of (5.4.6), $\mathcal{M}$ consists entirely of zero-divisors, a contradiction. In the proof of part 3 of the dimension theorem (5.3.3), take $M = R$ and $N = R/(a)$ to conclude that $\dim R/(a) < \dim R$, hence $\dim R/(a) \leq \dim R - 1$. To prove equality, we appeal to part 2 of the proof of (5.3.3). This allows us to find elements $a_1, \dots, a_s \in \mathcal{M}$, with $s = \dim R/(a)$, such that the images $\overline{a}_i$ in $R/(a)$ generate an $\mathcal{M}/(a)$-primary ideal of $R/(a)$. Then $a, a_1, \dots, a_s$ generate an $\mathcal{M}$-primary ideal of R, so by (5.4.1) and (3.3.10), $\dim R \leq 1 + s = 1 + \dim R/(a)$. ♣

5.4.8 Corollary

Let a be a non zero-divisor belonging to the prime ideal P of the Noetherian ring R. Then ht $P/(a) =$ ht $P - 1$.

Proof. In (5.4.7), replace R by R_P and $R/(a)$ by $(R_P)_Q$, where Q is a minimal prime ideal over (a). ♣

5.4.9 Theorem

Let $R = k[[X_1, \dots, X_n]]$ be a formal power series ring in n variables over the field k. Then $\dim R = n$.

Proof. The unique maximal ideal is $(X_1, \dots, X_n)$, so the dimension of R is at most n. On the other hand, the dimension is at least n because of the chain

$$(0) \subset (X_1) \subset (X_1, X_2) \subset \cdots \subset (X_1, \dots, X_n)$$

of prime ideals. ♣

5.5 Strengthening of Noether's Normalization Lemma

5.5.1 Definition

An *affine k-algebra* is an integral domain that is also a finite-dimensional algebra over a field k.

Affine algebras are of great interest in algebraic geometry because they are the coordinate rings of affine algebraic varieties. To study them we will need a stronger version of Noether's normalization lemma. In this section we will give the statement and proof, following Serre's Local Algebra, page 42.

5.5.2 Theorem

Let A be a finitely generated k-algebra, and $I_1 \subset \cdots \subset I_r$ a chain of nonzero proper ideals of A. There exists a nonnegative integer n and elements $x_1, \ldots, x_n \in A$ algebraically independent over k such that the following conditions are satisfied.

1. A is integral over $B = k[x_1, \ldots, x_n]$. (This is the standard normalization lemma.)

2. For each $i = 1, \ldots, r$, there is a positive integer $h(i)$ such that $I_i \cap B$ is generated (as an ideal of B) by $x_1, \ldots, x_{h(i)}$.

Proof. It suffices to let A be a polynomial ring $k[Y_1, \ldots, Y_m]$. For we may write $A = A'/I'_0$ where $A' = k[Y_1, \ldots, Y_m]$. If I'_i is the preimage of I_i under the canonical map $A' \to A'/I'_0$, and we find elements $x'_1, \ldots, x'_n \in A'$, relative to the ideals $I'_0 \subset I'_1 \subset \cdots \subset I'_r$, then the images of $x'_{i-h(0)}$ in A, $i > h(0)$, satisfy the required conditions. The proof is by induction on r.

Assume $r = 1$. We first consider the case in which I_1 is a principal ideal $(x_1) = x_1 A$ with $x_1 \notin k$. By our assumption that A is a polynomial ring, we have $x_1 = g(Y_1, \ldots, Y_m)$ for some nonconstant polynomial g with coefficients in k. We claim that there are positive integers $r_i (i = 2, \ldots, m)$ such that A is integral over $B = k[x_1, \ldots, x_m]$, where

$$x_i = Y_i - Y_1^{r_i}, \quad i = 2, \ldots, m.$$

If we can show that Y_1 is integral over B, then (since the x_i belong to B, hence are integral over B) all Y_i are integral over B, and therefore A is integral over B. Now Y_1 satisfies the equation $x_1 = g(Y_1, \ldots, Y_m)$, so

$$g(Y_1, x_2 + Y_1^{r_2}, \ldots, x_m + Y_1^{r_m}) - x_1 = 0.$$

If we write the polynomial g as a sum of monomials $\sum c_\alpha Y^\alpha, \alpha = (a_1, \ldots, a_m), c_\alpha \neq 0$, the above equation becomes

$$\sum c_\alpha Y_1^{a_1} (x_2 + Y_1^{r_2})^{a_2} \cdots (x_m + Y_1^{r_m})^{a_m} - x_1 = 0.$$

To produce the desired r_i, let $f(\alpha) = a_1 + a_2 r_2 + \cdots + a_m r_m$, and pick the r_i so that all the $f(\alpha)$ are distinct. For example, take $r_i = s^i$, where s is greater than the maximum of the a_j. Then there will be a unique α that maximizes f, say $\alpha = \beta$, and we have

$$c_\beta Y_1^{f(\beta)} + \sum_{j < f(\beta)} p_j(x_1, \ldots, x_m) Y_1^j = 0$$

so Y_1 is integral over B, and as we noted above, $A = k[Y_1, \dots, Y_m]$ is integral over $B = k[x_1, \dots, x_m]$. Since A has transcendence degree m over k and an integral extension must be algebraic, it follows that $x_1, \dots, x_m$ are algebraically independent over k. Thus the first assertion of the theorem holds (in this first case, where I_1 is principal). If we can show that $I_1 \cap B = (x_1) = x_1B$, the second assertion will also hold. The right-to-left inclusion follows from our assumptions about x_1, so let t belong to $I_1 \cap B$. Then $t = x_1u$ with $u \in A$, hence, dividing by x_1, $u \in A \cap k(x_1, \dots, x_m)$. Since B is isomorphic to a polynomial ring, it is a unique factorization domain and therefore integrally closed. Since A is integral over B, we have $u \in B$. Thus $x_1A \cap B = x_1B$, and the proof of the first case is complete. Note that we have also shown that $A \cap k(x_1, \dots, x_m) = B = k[x_1, \dots, x_m]$.

Still assuming $r = 1$, we now consider the general case by induction on m. If $m = 0$ there is nothing to prove, and we have already taken care of $m = 1$ (because A is then a PID). Let x_1 be a nonzero element of I_1, and note that $x_1 \notin k$ because I_1 is proper. By what we have just proved, there are elements $t_2, \dots, t_m \in A$ such that $x_1, t_2, \dots, t_m$ are algebraically independent over k, A is integral over the polynomial ring $C = k[x_1, t_2, \dots, t_m]$, and $x_1A \cap C = x_1C$. By the induction hypothesis, there are elements $x_2, \dots, x_m$ satisfying the conditions of the theorem for $k[t_2, \dots, t_m]$ and the ideal $I_1 \cap k[t_2, \dots, t_m]$. Then $x_1, \dots, x_m$ satisfy the desired conditions.

Finally, we take the inductive step from $r-1$ to r. let $t_1, \dots, t_m$ satisfy the conditions of the theorem for the chain of ideals $I_1 \subset \cdots \subset I_{r-1}$, and let $s = h(r-1)$. By the argument of the previous paragraph, there are elements $x_{s+1}, \dots, x_m \in k[t_{s+1}, \dots, t_m]$ satisfying the conditions for the ideal $I_r \cap k[t_{s+1}, \dots, t_m]$. Take $x_i = t_i$ for $1 \le i \le s$. ♣

5.6 Properties of Affine k-algebras

We will look at height, coheight and dimension of affine algebras.

5.6.1 Proposition

Let $S = R[X]$ where R is an arbitrary ring. If $Q \subset Q'$, where Q and Q' are prime ideals of S both lying above the same prime ideal P of R, then $Q = PS$.

Proof. Since R/P can be regarded as a subring of S/Q, we may assume without loss of generality that $P = 0$. By localizing with respect to the multiplicative set $R \setminus \{0\}$, we may assume that R is a field. But then every nonzero prime ideal of S is maximal, hence $Q = 0$. Since PS is also 0, the result follows. ♣

5.6.2 Corollary

Let I be an ideal of the Noetherian ring R, and let P be a prime ideal of R with $I \subseteq P$. Let S be the polynomial ring $R[X]$, and take $J = IS$ and $Q = PS$. If P is a minimal prime ideal over I, then Q is a minimal prime ideal over J.

Proof. To verify that Q is prime, note that $R[X]/PR[X] \cong R[X]/P[X] \cong (R/P)[X]$, an integral domain. By modding out I, we may assume that $I = 0$. Suppose that the prime ideal Q_1 of S is properly contained in Q. Then $Q_1 \cap R \subseteq Q \cap R = PS \cap R = P$. (A polynomial belonging to R coincides with its constant term.) By minimality, $Q_1 \cap R = P$. By (5.6.1), $Q_1 = PS = Q$, a contradiction. ♣

5.6.3 Proposition

As above, let $S = R[X]$, R Noetherian, P a prime ideal of R, $Q = PS$. Then $\operatorname{ht} P = \operatorname{ht} Q$.

Proof. Let n be the height of P. By the generalized Krull principal ideal theorem (5.4.5), there is an ideal I of R generated by n elements such that P is a minimal prime ideal over I. By (5.6.2), $Q = PS$ is a minimal prime ideal over $J = IS$. But J is also generated over S by n elements, so again by (5.4.5), $\operatorname{ht} Q \leq \operatorname{ht} P$. Conversely, if $P_0 \subset P_1 \subset \cdots \subset P_n = P \subset R$ and $Q_i = P_i[X]$, then $Q_0 \subset Q_1 \subset \cdots \subset Q_n = Q$, so $\operatorname{ht} Q \geq \operatorname{ht} P$. ♣

We may now prove a major result on the dimension of a polynomial ring.

5.6.4 Theorem

Let $S = R[X]$, where R is a Noetherian ring. Then $\dim S = 1 + \dim R$.

Proof. Let $P_0 \subset P_1 \subset \cdots \subset P_n$ be a chain of prime ideals of R. If $Q_n = P_n S$, then by (5.6.3), $\operatorname{ht} Q_n = \operatorname{ht} P_n$. But the Q sequence can be extended via $Q_n \subset Q_{n+1} = Q_n + (X)$. (Note that X cannot belong to Q_n because $1 \notin P_n$.) It follows that $\dim S \geq 1 + \dim R$. Now consider a chain $Q_0 \subset Q_1 \subset \cdots \subset Q_n$ of prime ideals of S, and let $P_i = Q_i \cap R$ for every $i = 0, 1, \dots, n$. We may assume that the P_i are not all distinct (otherwise $\dim R \geq \dim S \geq \dim S - 1$). Let j be the largest index i such that $P_i = P_{i+1}$. By (5.6.1), $Q_j = P_j S$, and by (5.6.3), $\operatorname{ht} P_j = \operatorname{ht} Q_j \geq j$. But by choice of j,

$$P_j = P_{j+1} \subset P_{j+2} \subset \cdots \subset P_n$$

so $\operatorname{ht} P_j + n - j - 1 \leq \dim R$. Since the height of P_j is at least j, we have $n - 1 \leq \dim R$, hence $\dim S \leq 1 + \dim R$. ♣

5.6.5 Corollary

If R is a Noetherian ring, then $\dim R[X_1, \dots, X_n] = n + \dim R$. In particular, if K is a field then $\dim K[X_1, \dots, X_n] = n$.

Proof. This follows from (5.6.4) by induction. ♣

5.6.6 Corollary

Let $R = K[X_1, \dots, X_n]$, where K is a field. Then $\operatorname{ht}(X_1, \dots, X_i) = i,\ 1 \leq i \leq n$.

Proof. First consider $i = n$. The height of $(X_1, \dots, X_n)$ is at most n, the dimension of R, and in fact the height is n, in view of the chain $(X_1) \subset (X_1, X_2) \subset \cdots \subset (X_1, \dots, X_n)$. The general result now follows by induction, using (5.4.8). ♣

If X is an affine algebraic variety over the field k, its (geometric) dimension is the transcendence degree over k of the function field (the fraction field of the coordinate ring). We now show that the geometric dimension coincides with the algebraic (Krull) dimension. We abbreviate transcendence degree by tr deg.

5.6.7 Theorem

If R is an affine k-algebra, then $\dim R = \text{tr deg}_k \text{ Frac } R$.

Proof. By Noether's normalization lemma, there are elements $x_1, \dots, x_n \in R$, algebraically independent over k, such that R is integral over $k[x_1, \dots, x_n]$. Since an integral extension cannot increase dimension (see Problem 4), $\dim R = \dim k[x_1, \dots, x_n] = n$ by (5.6.5). Let $F = \text{Frac } R$ and $L = \text{Frac } k[x_1, \dots, x_n]$. Then F is an algebraic extension of L, and since an algebraic extension cannot increase transcendence degree, we therefore have $\text{tr deg}_k F = \text{tr deg}_k L = n = \dim R$. ♣

It follows from the definitions that if P is a prime ideal of R, then $\text{ht}\, P + \text{coht}\, P \leq \dim R$. If R is an affine k-algebra, there is equality.

5.6.8 Theorem

If P is a prime ideal of the affine k-algebra R, then $\text{ht}\, P + \text{coht}\, P = \dim R$.

Proof. By Noether's normalization lemma, R is integral over a polynomial algebra. We can assume that $R = k[X_1, \dots, X_n]$ with $\text{ht}\, P = h$. (See Problems 4,5 and 6. An integral extension preserves dimension and coheight, and does not increase height. So if height plus coheight equals dimension in the larger ring, the same must be true in the smaller ring.) By the strong form (5.5.2) of Noether's normalization lemma, along with (5.6.6), there are elements $y_1, \dots, y_n$ algebraically independent over k such that R is integral over $k[y_1, \dots, y_n]$ and $Q = P \cap k[y_1, \dots, y_n] = (y_1, \dots, y_h)$ Since $k[y_1, \dots, y_n]/Q \cong k[y_{h+1}, \dots, y_n]$, it follows from (5.3.1) and (5.6.5) that $\text{coht}\, Q = \dim k[y_{h+1}, \dots, y_n] = n - h$. But $\text{coht}\, Q = \text{coht}\, P$ (Problem 5), so $\text{ht}\, P + \text{coht}\, P = h + (n - h) = n = \dim R$. ♣

Chapter 6

Depth

6.1 Systems of Parameters

We prepare for the study of regular local rings, which play an important role in algebraic geometry.

6.1.1 Definition

Let R be a Noetherian local ring with maximal ideal $\mathcal{M}$, and let M be a finitely generated R-module of dimension n. A *system of parameters* for M is a set $\{a_1, \ldots, a_n\}$ of elements of $\mathcal{M}$ such that $M/(a_1, \ldots, a_n)M$ has finite length. The finiteness of the Chevalley dimension (see (5.3.2) and (5.3.3) guarantees the existence of such a system.

6.1.2 Example

Let R be a Noetherian local ring of dimension d. Then any set $\{a_1, \ldots, a_d\}$ that generates an ideal of definition is a system of parameters for R, by (5.4.1). In particular, if $R = k[[X_1, \ldots, X_n]]$ is a formal power series ring over a field, then $X_1, \ldots, X_n$ form a system of parameters, since they generate the maximal ideal.

6.1.3 Proposition

Let M be finitely generated and of dimension n over the Noetherian local ring R, and let $a_1, \ldots, a_t$ be arbitrary elements of the maximal ideal $\mathcal{M}$. Then $\dim(M/(a_1, \ldots, a_t)M) \geq n - t$, with equality if and only if the a_i can be extended to a system of parameters for M.

Proof. Let a be any element of $\mathcal{M}$, and let $N = M/aM$. Choose $b_1, \ldots, b_r \in \mathcal{M}$ such that $N/(b_1, \ldots, b_r)N$ has finite length, with r as small as possible. Then $M/(a, b_1, \ldots, b_r)M$ also has finite length, because

$$(M/aM)/(b_1, \ldots, b_r)(M/aM) \cong M/(a, b_1, \ldots, b_r)M.$$

It follows that the Chevalley dimension of M is at most $r+1$, in other words,

$$\delta(M/aM) \geq \delta(M) - 1.$$

The proof will be by induction on t, and we have just taken care of $t = 1$ as well as the key step in the induction, namely

$$\dim(M/(a_1, \dots, a_t)M) = \dim(N/a_1N)$$

where $N = M/(a_2, \dots, a_t)M$. By the $t = 1$ case and the induction hypothesis,

$$\dim(N/a_1N) \geq \dim N - 1 \geq \dim M - (t-1) - 1 = \dim M - t$$

as asserted. If $\dim(M/(a_1, \dots, a_t)M) = n - t$ with $n = \dim M$, then we can choose a system of parameters $a_{t+1}, \dots, a_n$ for $N = M/(a_1, \dots, a_t)M$. Then

$$N/(a_{t+1}, \dots, a_n)N \cong M/(a_1, \dots, a_t, a_{t+1}, \dots, a_n)M$$

has finite length. Thus $a_1, \dots, a_n$ form a system of parameters for M. Conversely, if $a_1, \dots, a_t$ can be extended to a system of parameters $a_1, \dots, a_n$ for M, define $N = M/(a_1, \dots, a_t)M$. Then $N/(a_{t+1}, \dots, a_n)N \cong M/(a_1, \dots, a_n)M$ has finite length, hence $\dim N \leq n - t$. But $\dim N \geq n - t$ by the main assertion, and the proof is complete. ♣

6.2 Regular Sequences

We introduce sequences that are guaranteed to be extendable to a system of parameters.

6.2.1 Definition

Let M be an R-module. The sequence $a_1, \dots, a_t$ of nonzero elements of R is an *M-sequence*, also called a *regular sequence for M* or an *M-regular sequence*, if $(a_1, \dots, a_t)M \neq M$ and for each $i = 1, \dots, t$, a_i is not a zero-divisor of $M/(a_1, \dots, a_{i-1})M$.

6.2.2 Comments and Examples

We interpret the case $i = 1$ as saying that a_1 is not a zero-divisor of M, that is, if $x \in M$ and $a_1x = 0$, then $x = 0$. Since $(a_1, \dots, a_t)M \neq M$, $M \neq 0$ and the a_i are nonunits.

It follows from the definition that the elements $a_1, \dots, a_t$ form an M-sequence if and only if for all $i = 1, \dots, t$, $a_1, \dots, a_i$ is an M-sequence and $a_{i+1}, \dots, a_t$ is an $M/(a_1, \dots, a_i)M$-sequence.

1. If $R = k[X_1, \dots, X_n]$ with k a field, then $X_1, \dots, X_n$ is an R-sequence.

2. (A tricky point) A permutation of a regular sequence need not be regular. For example, let $R = k[X, Y, Z]$, where k is a field. Then $X, Y(1-X), Z(1-X)$ is an R-sequence, but $Y(1-X), Z(1-X), X$ is not, because the image of $Z(1-X)Y$ is zero in $R/(Y(1-X))$.

6.2.3 Theorem

Let M be a finitely generated module over the Noetherian local ring R. If $a_1, \dots, a_t$ is an M-sequence, then $\{a_1, \dots, a_t\}$ can be extended to a system of parameters for M.

Proof. We argue by induction on t. Since a_1 is not a zero-divisor of M, we have $\dim M/a_1M = \dim M - 1$ by (5.4.7). (Remember that the a_i are nonunits (see (6.2.2)) and therefore belong to the maximal ideal of R.) By (6.1.3), a_1 is part of a system of parameters for M. If $t > 1$, the induction hypothesis says that $a_1, \dots, a_{t-1}$ is part of a system of parameters for M. By (6.1.3), $\dim M/(a_1, \dots, a_{t-1})M = n - (t-1)$, where $n = \dim M$. Since a_t is not a zero-divisor of $N = M/(a_1, \dots, a_{t-1})M$, we have, as in the $t = 1$ case, $\dim N/a_tN = \dim N - 1$. But, as in the proof of (6.1.3),

$$N/a_tN \cong M/(a_1, \dots, a_t)M,$$

hence

$$\dim M/(a_1, \dots, a_t)M = \dim N/a_tN = \dim N - 1 = n - (t-1) - 1 = n - t.$$

By (6.1.3), $a_1, \dots, a_t$ extend to a system of parameters for M. ♣

6.2.4 Corollary

If R is a Noetherian local ring, then every R-sequence can be extended to a system of parameters for R.

Proof. Take $M = R$ in (6.2.3). ♣

6.2.5 Definition

Let M be a nonzero finitely generated module over the Noetherian local ring R. The *depth* of M over R, written $\operatorname{depth}_R M$ or simply depth M, is the maximum length of an M-sequence. We will see in the next chapter that any two maximal M-sequences have the same length.

6.2.6 Theorem

Let M be a nonzero finitely generated module over the Noetherian local ring R. Then depth $M \le \dim M$.

Proof. Since $\dim M$ is the number of elements in a system of parameters, the result follows from (6.2.3). ♣

6.2.7 Proposition

Let M be a finitely generated module over the Noetherian ring R, and let $a_1, \dots, a_n$ be an M-sequence with all a_i belonging to the Jacobson radical $J(R)$. Then any permutation of the a_i is also an M-sequence.

Proof. It suffices to consider the transposition that interchanges a_1 and a_2. First let us show that a_1 is not a zero-divisor of M/a_2M. Suppose $a_1\overline{x} = 0$, where $\overline{x}$ belongs to M/a_2M. Then a_1x belongs to a_2M, so we may write $a_1x = a_2y$ with $y \in M$. By hypothesis, a_2 is not a zero-divisor of M/a_1M, so y belongs to a_1M. Therefore $y = a_1z$ for some $z \in M$. Then $a_1x = a_2y = a_2a_1z$. By hypothesis, a_1 is not a zero-divisor of M, so $x = a_2z$, and consequently $\overline{x} = 0$.

To complete the proof, we must show that a_2 is not a zero-divisor of M. If N is the submodule of M annihilated by a_2, we will show that $N = a_1N$. Since $a_1 \in J(R)$, we can invoke NAK (0.3.3) to conclude that $N = 0$, as desired. It suffices to show that $N \subseteq a_1N$, so let $x \in N$. By definition of N we have $a_2x = 0$. Since a_2 is not a zero-divisor of M/a_1M, x must belong to a_1M, say $x = a_1y$ with $y \in M$. Thus $a_2x = a_2a_1y = 0$. But a_1 is not a zero-divisor of M, hence $a_2y = 0$ and therefore $y \in N$. But $x = a_1y$, so $x \in a_1N$, and we are finished. ♣

6.2.8 Corollary

Let M be a finitely generated module over the Noetherian local ring R. Then any permutation of an M-sequence is also an M-sequence.

Proof. By (6.2.2), the members of the sequence are nonunits, hence they belong to the maximal ideal, which coincides with the Jacobson radical. ♣

6.2.9 Definitions and Comments

Let M be a nonzero finitely generated module over a Noetherian local ring R. If the depth of M coincides with its dimension, we call M a *Cohen-Macaulay module*. We say that R is a *Cohen-Macaulay ring* if it is a Cohen-Macaulay module over itself. To study these rings and modules, we need some results from homological algebra. The required tools will be developed in Chapter 7.

Chapter 7

Homological Methods

We now begin to apply homological algebra to commutative ring theory. We assume as background some exposure to derived functors and basic properties of Ext and Tor. In addition, we will use standard properties of projective and injective modules. Everything we need is covered in TBGY, Chapter 10 and the supplement.

7.1 Homological Dimension: Projective and Global

Our goal is to construct a theory of dimension of a module M based on possible lengths of projective and injective resolutions of M.

7.1.1 Definitions and Comments

A projective resolution $0 \to X_n \to \cdots \to X_0 \to M \to 0$ of the R-module M is said to be of *length* n. The largest such n is called the *projective dimension* of M, denoted by $\operatorname{pd}_R M$. (If M has no finite projective resolution, we set $\operatorname{pd}_R M = \infty$.)

7.1.2 Lemma

The projective dimension of M is 0 if and only if M is projective.

Proof. If M is projective, then $0 \to X_0 = M \to M \to 0$ is a projective resolution, where the map from M to M is the identity. Conversely, if $0 \to X_0 \to M \to 0$ is a projective resolution, then $M \cong X_0$, hence M is projective. ♣

7.1.3 Lemma

If R is a PID, then for every R-module M, $\operatorname{pd}_R M \leq 1$. If M is an abelian group whose torsion subgroup is nontrivial, then $\operatorname{pd}_R M = 1$.

Proof. There is an exact sequence $0 \to X_1 \to X_0 \to M \to 0$ with X_0 free and X_1, a submodule of a free module over a PID, also free. Thus $\operatorname{pd}_R M \leq 1$. If $\operatorname{pd}_R M = 0$, then by (7.1.2), M is projective, hence free because R is a PID. Since a free module has zero torsion, the second assertion follows. ♣

7.1.4 Definition

The *global dimension* of a ring R, denoted by $\operatorname{gldim} R$, is the least upper bound of $\operatorname{pd}_R M$ as M ranges over all R-modules.

7.1.5 Remarks

If R is a field, then every R-module is free, so $\operatorname{gldim} R = 0$. By (7.1.3), a PID has global dimension at most 1. Since an abelian group with nonzero torsion has projective dimension 1, $\operatorname{gldim} \mathbb{Z} = 1$.

We will need the following result from homological algebra; for a proof, see TBGY, subsection S5.7.

7.1.6 Proposition

If M is an R-module, the following conditions are equivalent.

(i) M is projective;

(ii) $\operatorname{Ext}^n_R(M, N) = 0$ for all $n \geq 1$ and all R-modules N;

(iii) $\operatorname{Ext}^1_R(M, N) = 0$ for all R-modules N.

We can now characterize projective dimension in terms of the Ext functor.

7.1.7 Theorem

If M is an R-module and n is a positive integer, the following conditions are equivalent.

1. $\operatorname{pd}_R M \leq n$.
2. $\operatorname{Ext}^i_R(M, N) = 0$ for all $i > n$ and every R-module N.
3. $\operatorname{Ext}^{n+1}_R(M, N) = 0$ for every R-module N.
4. If $0 \to K_{n-1} \to X_{n-1} \to \cdots \to X_0 \to M \to 0$ is an exact sequence with all X_i projective, then K_{n-1} is projective.

Proof. To show that (1) implies (2), observe that by hypothesis, there is a projective resolution $0 \to X_n \to \cdots \to X_0 \to M \to 0$. Use this resolution to compute Ext, and conclude that (2) holds. Since (3) is a special case of (2), we have (2) implies (3). If (4) holds, construct a projective resolution of M in the usual way, but pause at X_{n-1} and terminate the sequence with $0 \to K_{n-1} \to X_{n-1}$. By hypothesis, K_{n-1} is projective, and this gives (4) implies (1). The main effort goes into proving that (3) implies (4). We break the exact sequence given in (4) into short exact sequences. The procedure is a bit different from the decomposition of (5.2.3). Here we are proceeding from right to left, and our first short exact sequence is

$$0 \longrightarrow K_0 \xrightarrow{i_0} X_0 \xrightarrow{\epsilon} M \longrightarrow 0$$

where K_0 is the kernel of ϵ. The induced long exact sequence is

$$\cdots \to \operatorname{Ext}^n_R(X_0, N) \to \operatorname{Ext}^n_R(K_0, N) \to \operatorname{Ext}^{n+1}_R(M, N) \to \operatorname{Ext}^{n+1}_R(X_0, N) \to \cdots$$

Now if every third term in an exact sequence is 0, then the maps in the middle are both injective and surjective, hence isomorphisms. This is precisely what we have here, because X_0 is projective and (7.1.6) applies. Thus $\mathrm{Ext}_R^{n+1}(M,N) \cong \mathrm{Ext}_R^n(K_0,N)$, so as we slide from right to left through the exact sequence, the upper index decreases by 1. This technique is referred to as **dimension shifting**.

Now the second short exact sequence is

$$0 \longrightarrow K_1 \xrightarrow{i_1} X_1 \xrightarrow{d_1} K_0 \longrightarrow 0.$$

We can replace X_0 by K_0 because $\operatorname{im} d_1 = \ker \epsilon = K_0$. The associated long exact sequence is

$$\cdots \to \mathrm{Ext}_R^n(X_1,N) \to \mathrm{Ext}_R^n(K_1,N) \to \mathrm{Ext}_R^{n+1}(K_0,N) \to \mathrm{Ext}_R^{n+1}(X_1,N) \to \cdots$$

and dimension shifting gives $\mathrm{Ext}_R^n(K_0,N) \cong \mathrm{Ext}_R^{n-1}(K_1,N)$. Iterating this procedure, we get $\mathrm{Ext}_R^{n+1}(M,N) \cong \mathrm{Ext}_R^1(K_{n-1},N)$, hence by the hypothesis of (3), $\mathrm{Ext}_R^1(K_{n-1},N) = 0$. By (7.1.6), K_{n-1} is projective. ♣

7.1.8 Corollary

gldim $R \le n$ if and only if $\mathrm{Ext}_R^{n+1}(M,N) = 0$ for all R-modules M and N.

Proof. By the definition (7.1.4) of global dimension, gldim $R \le n$ iff $\mathrm{pd}_R\, M$ for all M iff (by (1) implies (3) of (7.1.7)) $\mathrm{Ext}_R^{n+1}(M,N) = 0$ for all M and N. ♣

7.2 Injective Dimension

As you might expect, projective dimension has a dual notion. To develop it, we will need the analog of (7.1.6) for injective modules. A proof is given in TBGY, subsection S5.8.

7.2.1 Proposition

If N is an R-module, the following conditions are equivalent.

(i) N is injective;

(ii) $\mathrm{Ext}_R^n(M,N) = 0$ for all $n \ge 1$ and all R-modules M;

(iii) $\mathrm{Ext}_R^1(M,N) = 0$ for all R-modules M.

We are going to dualize (7.1.7), and the technique of **dimension shifting** is again useful.

7.2.2 Proposition

Let $0 \to M' \to E \to M'' \to 0$ be an exact sequence, with E injective. Then for all $n \ge 1$ and all R-modules M, we have $\mathrm{Ext}_R^{n+1}(M,M') \cong \mathrm{Ext}_R^n(M,M'')$. Thus as we slide through the exact sequence from left to right, the index of Ext drops by 1.

Proof. The given short exact sequence induces the following long exact sequence:

$$\cdots \to \mathrm{Ext}_R^n(M,E) \to \mathrm{Ext}_R^n(M,M'') \to \mathrm{Ext}_R^{n+1}(M,M') \to \mathrm{Ext}_R^{n+1}(M,E) \to \cdots$$

By (7.2.1), the outer terms are 0 for $n \ge 1$, hence as in the proof of (7.1.7), the map in the middle is an isomorphism. ♣

7.2.3 Definitions and Comments

An injective resolution $0 \to N \to X_0 \to \cdots \to \cdots X_n \to 0$ of the R-module N is said to be of *length* n. The largest such n is called the *injective dimension* of M, denoted by $\operatorname{id}_R M$. (If N has no finite injective resolution, we set $\operatorname{id}_R M = \infty$.) Just as in (7.1.2), $\operatorname{id}_R N = 0$ if and only if N is injective.

7.2.4 Proposition

If N is an R-module and n is a positive integer, the following conditions are equivalent.

1. $\operatorname{id}_R N \le n$.
2. $\operatorname{Ext}^i_R(M, N) = 0$ for all $i > n$ and every R-module M.
3. $\operatorname{Ext}^{n+1}_R(M, N) = 0$ for every R-module M.
4. If $0 \to N \to X_0 \to \cdots \to X_{n-1} \to C_{n-1} \to 0$ is an exact sequence with all X_i injective, then C_{n-1} is injective.

Proof. If (1) is satisfied, we have an exact sequence $0 \to N \to X_0 \to \cdots \to X_n \to 0$, with the X_i injective. Use this sequence to compute Ext, and conclude that (2) holds. If we have (2), then we have the special case (3). If (4) holds, construct an injective resolution of N, but pause at step $n-1$ and terminate the sequence by $X_{n-1} \to C_{n-1} \to 0$. By hypothesis, C_{n-1} is injective, proving that (4) implies (1). To prove that (3) implies (4), we decompose the exact sequence of (4) into short exact sequences. The process is similar to that of (5.2.3), but with emphasis on kernels rather than cokernels. The decomposition is given below.

$$0 \to N \to X_0 \to K_0 \to 0, \quad 0 \to K_0 \to X_1 \to K_1 \to 0, \dots ,$$

$$0 \to K_{n-2} \to X_{n-1} \to C_{n-1} \to 0$$

We now apply the dimension shifting result (7.2.2) to each short exact sequence. If the index of Ext starts at $n+1$, it drops by 1 as we go through each of the n sequences, and it ends at 1. More precisely,

$$\operatorname{Ext}^{n+1}_R(M, N) \cong \operatorname{Ext}^1_R(M, C_{n-1})$$

for any M. The left side is 0 by hypothesis, so the right side is also 0. By (7.2.1), C_{n-1} is injective. ♣

7.2.5 Corollary

The global dimension of R is the least upper bound of $\operatorname{id}_R N$ over all R-modules N.

Proof. By the definition (7.1.4) of global dimension, gldim $R \le n$ iff $\operatorname{pd}_R M \le n$ for all M. Equivalently, by (7.1.7), $\operatorname{Ext}^{n+1}_R(M, N) = 0$ for all M and N. By (7.2.4), this happens iff $\operatorname{id}_R N \le n$ for all N. ♣

7.3 Tor and Dimension

We have observed the interaction between homological dimension and the Ext functor, and this suggests that it would be profitable to bring in the Tor functor as well. We will need the following result, which is proved in TBGY, subsection S5.6.

7.3.1 Proposition

If M is an R-module, the following conditions are equivalent.

(i) M is flat.

(ii) $\operatorname{Tor}_n^R(M,N)=0$ for all $n \geq 1$ and all R-modules N.

(iii) $\operatorname{Tor}_1^R(M,N)=0$ for all R-modules N.

In addition, if R is a Noetherian local ring and M is finitely generated over R, then M is free if and only if M is projective, if and only if M is flat. See Problems 3-6 for all the details.

7.3.2 Proposition

Let R be Noetherian local ring with maximal ideal $\mathcal{M}$ and residue field k. Let M be a finitely generated R-module. Then M is free ($\Longleftrightarrow$ projective $\Longleftrightarrow$ flat) if and only if $\operatorname{Tor}_1^R(M,k)=0$.

Proof. The "only if" part follows from (7.3.1). To prove the "if" part, let $\{x_1,\dots,x_n\}$ be a minimal set of generators for M. Take a free module F with basis $\{e_1,\dots,e_n\}$ and define an R-module homomorphism $f: F \to M$ via $f(e_i)=x_i, i=1,\dots,n$. If K is the kernel of f, we have the short exact sequence $0 \to K \to F \to M \to 0$. Since $\operatorname{Tor}_1^R(M,k)=0$, we can truncate the associated long exact sequence:

$$0=\operatorname{Tor}_1^R(M,k) \to K \otimes_R k \to F \otimes_R k \to M \otimes_R k \to 0$$

where the map $\overline{f}: F \otimes_R k \to M \otimes_R k$ is induced by f. Now $\overline{f}$ is surjective by construction, and is injective by minimality of the generating set [see (0.3.4) and the base change device below]. Thus $K \otimes_R k = \ker \overline{f} = 0$. But (TBGY, subsection S7.1)

$$K \otimes_R k = K \otimes_R (R/\mathcal{M}) \cong K/\mathcal{M}K$$

so $K=\mathcal{M}K$. By NAK, $K=0$. Therefore f is an isomorphism of F and M, hence M is free. ♣

7.3.3 Theorem

Let R be a Noetherian local ring with maximal ideal $\mathcal{M}$ and residue field k. If M is a finitely generated R-module, the following conditions are equivalent.

(i) $\operatorname{pd}_R M \leq n$.

(ii) $\operatorname{Tor}_i^R(M,N)=0$ for all $i>n$ and every R-module N.

(iii) $\mathrm{Tor}_{n+1}^R(M,N)=0$ for every R-module N.

(iv) $\mathrm{Tor}_{n+1}^R(M,k)=0$.

Proof. If (i) holds, then M has a projective resolution of length n, and if we use this resolution to compute Tor, we get (ii). There is no difficulty with (ii) $\Longrightarrow$ (iii) $\Longrightarrow$ (iv), so it remains to prove (iv) $\Longrightarrow$ (i). Let $0 \to K_{n-1} \to X_{n-1} \to \cdots \to X_0 \to M \to 0$ be an exact sequence with all X_i projective. By (7.1.7), it suffices to show that K_{n-1} is projective. Now we apply dimension shifting as in the proof of (7.1.7). For example, the short exact sequence $0 \to K_1 \to X_1 \to K_0 \to 0$ [see(7.1.7)] induces the long exact sequence $\cdots \to \mathrm{Tor}_n^R(X_1,k) \to \mathrm{Tor}_n^R(K_0,k) \to \mathrm{Tor}_{n-1}^R(K_1,k) \to \mathrm{Tor}_{n-1}^R(X_1,k) \to \cdots$ and as before, the outer terms are 0, which implies that the map in the middle is an isomorphism. Iterating, we have $\mathrm{Tor}_1^R(K_{n-1},k) \cong \mathrm{Tor}_{n+1}^R(M,k)=0$ by hypothesis. By (7.3.2), K_{n-1} is projective. ♣

7.3.4 Corollary

Let R be a Noetherian local ring with maximal ideal $\mathcal{M}$ and residue field k. For any positive integer n, the following conditions are equivalent.

(1) $\operatorname{gldim} R \le n$.

(2) $\mathrm{Tor}_{n+1}^R(M,N)=0$ for all finitely generated R-modules M and N.

(3) $\mathrm{Tor}_{n+1}^R(k,k)=0$.

Proof. If (1) holds, then $\mathrm{pd}_R\, M \le n$ for all M, and (2) follows from (7.3.3). Since (3) is a special case of (2), it remains to prove that (3) implies (1). Assuming (3), (7.3.3) gives $\mathrm{Tor}_{n+1}^R(k,N)=\mathrm{Tor}_{n+1}^R(N,k)=0$ for all R-modules N. Again by (7.3.3), the projective dimension of any R-module N is at most n, hence $\operatorname{gldim} R \le n$. ♣

7.4 Application

As promised in (6.2.5), we will prove that under a mild hypothesis, all maximal M-sequences have the same length.

7.4.1 Lemma

Let M and N be R-modules, and let $a_1,\dots,a_n$ be an M-sequence. If a_n annihilates N, then the only R-homomorphism h from N to $M'=M/(a_1,\dots,a_{n-1})M$ is the zero map.

Proof. If x is any element of N, then $a_n h(x)=h(a_n x)=h(0)=0$. Since a_n is not a zero-divisor of M', the result follows. ♣

7.4.2 Proposition

Strengthen the hypothesis of (7.4.1) so that each $a_i, i=1,\dots,n$ annihilates N. Then $\mathrm{Ext}_R^n(N,M) \cong \hom_R(N, M/(a_1,\dots,a_n)M)$.

Proof. The short exact sequence $0 \to M \to M \to M/a_1M \to 0$, with the map from M to M given by multiplication by a_1, induces the following long exact sequence:

$$\operatorname{Ext}_R^{n-1}(N,M) \longrightarrow \operatorname{Ext}_R^{n-1}(N,M/a_1M) \xrightarrow{\delta} \operatorname{Ext}_R^n(N,M) \xrightarrow{a_1} \operatorname{Ext}_R^n(N,M)$$

where the label a_1 indicates multiplication by a_1. In fact this map is zero, because a_1 annihilates N; hence δ is surjective. By induction hypothesis, $\operatorname{Ext}_R^{n-1}(N,M)$ is isomorphic to $\hom_R(N, M/(a_1,\dots,a_{n-1})M = 0$ by (7.4.1). (The result is vacuously true for $n=1$.) Thus δ is injective, hence an isomorphism. Consequently, if $\overline{M} = M/a_1M$, we have $\operatorname{Ext}_R^{n-1}(N,\overline{M}) \cong \operatorname{Ext}_R^n(N,M)$. Again using the induction hypothesis, we have $\operatorname{Ext}_R^{n-1}(N,\overline{M}) \cong \hom_R(N, \overline{M}/(a_2,\dots,a_n)\overline{M} = \hom_R(N, M/(a_1,\dots,a_n)M)$. ♣

We prove a technical lemma to prepare for the main theorem.

7.4.3 Lemma

Let M_0 be an R-module, and I an ideal of R. Then $\hom_R(R/I, M_0) \neq 0$ if and only if there is a nonzero element of M_0 annihilated by I. Equivalently, by (1.3.1), I is contained in some associated prime of M_0. (If there are only finitely many associated primes, for example if R is Noetherian [see (1.3.9)], then by (0.1.1), another equivalent condition is that I is contained in the union of the associated primes of M_0.)

Proof. If there is a nonzero homomorphism from R/I to M_0, it will map $1+I$ to a nonzero element $x \in M_0$. If $a \in I$, then $a+I$ is mapped to ax. But $a+I = 0+I$ since $a \in I$, so ax must be 0. Conversely, if x is a nonzero element of M_0 annihilated by I, then we can construct a nonzero homomorphism by mapping $1+I$ to x, and in general, $r+I$ to rx. We must check that the map is well defined, but this follows because I annihilates x. ♣

7.4.4 Theorem

Let M be a finitely generated module over the Noetherian ring R, and I an ideal of R such that $IM \neq M$. Then any two maximal M-sequences in I have the same length, namely the smallest nonnegative integer n such that $\operatorname{Ext}_R^n(R/I, M) \neq 0$.

Proof. In (7.4.2), take $N = R/I$ and let $\{a_1,\dots,a_n\}$ be a set of generators of I. Then

$$\operatorname{Ext}_R^n(R/I, M) \cong \hom_R(R/I, M_0)$$

where $M_0 = M/(a_1,\dots,a_n)M$. By (7.4.3), $\operatorname{Ext}_R^n(R/I,M) = 0$ if and only if I is not contained in the union of all associated primes of M_0. In view of (1.3.6), this says that if $a_1,\dots,a_n$ is an M-sequence in I, it can be extended to some $a_{n+1} \in I$ as long as $\operatorname{Ext}_R^n(R/I,M) = 0$. This is precisely the statement of the theorem. ♣

7.4.5 Remarks

Under the hypothesis of (7.4.4), we call the maximum length of an M-sequence in I the *grade of I on M*. If R is a Noetherian local ring with maximal ideal $\mathcal{M}$, then by (6.2.2), the elements a_i of an M-sequence are nonunits, hence belong to $\mathcal{M}$. Thus the depth of M, as defined in (6.2.5), coincides with the grade of $\mathcal{M}$ on M.

Again let M be finitely generated over the Noetherian local ring R. By (7.4.4), the depth of M is 0 if and only if $\hom_R(R/\mathcal{M}, M) \neq 0$. By (7.4.3) and the maximality of $\mathcal{M}$, this happens iff $\mathcal{M}$ is an associated prime of M. Note also that by (6.1.1) and (6.2.3), if $a_1, \ldots, a_r$ is an M-sequence of maximal length, then the module $M/(a_1, \ldots, a_r)M$ has finite length.

Chapter 8

Regular Local Rings

In algebraic geometry, the local ring of an affine algebraic variety V at a point P is the set $\mathcal{O}(P, V)$ of rational functions on V that are defined at P. Then P will be a nonsingular point of V if and only if $\mathcal{O}(P, V)$ is a regular local ring.

8.1 Basic Definitions and Examples

8.1.1 Definitions and Comments

Let $(R, \mathcal{M}, k)$ be a Noetherian local ring. (The notation means that the maximal ideal is $\mathcal{M}$ and the residue field is $k = R/\mathcal{M}$.) If d is the dimension of R, then by the dimension theorem [see (5.4.1)], every generating set of $\mathcal{M}$ has at least d elements. If $\mathcal{M}$ does in fact have a generating set S of d elements, we say that R is *regular* and that S is a *regular system of parameters*. (Check the definition (6.1.1) to verify that S is indeed a system of parameters.)

8.1.2 Examples

1. If R has dimension 0, then R is regular iff $\{0\}$ is a maximal ideal, in other words, iff R is a field.

2. If R has dimension 1, then by (3.3.11), condition (3), R is regular iff R is a discrete valuation ring. Note that (3.3.11) assumes that R is an integral domain, but this is not a problem because we will prove shortly that every regular local ring is a domain.

3. Let $R = K[[X_1, \dots, X_d]]$, where K is a field. By (5.4.9), $\dim R = d$, hence R is regular and $\{X_1, \dots, X_d\}$ is a regular system of parameters.

4. Let K be a field whose characteristic is not 2 or 3, and let $R = K[X, Y]/(X^3 - Y^2)$, localized at the maximal ideal $\mathcal{M} = \{\overline{X} - 1, \overline{Y} - 1\}$. (The overbars indicate calculations mod $(X^3 - Y^2)$.) It appears that $\{\overline{X} - 1, \overline{Y} - 1\}$ is a minimal generating set for $\mathcal{M}$, but this is not the case (see Problem 1). In fact $\mathcal{M}$ is principal, hence $\dim R = 1$ and R is regular. (See Example 2 above, and note that R is a domain because $X^3 - Y^2$ is irreducible, so $(X^3 - Y^2)$ is a prime ideal.)

5. Let R be as in Example 4, except that we localize at $\mathcal{M} = (\overline{X}, \overline{Y})$ and drop the restriction on the characteristic of K. Now it takes two elements to generate $\mathcal{M}$, but $\dim R = 1$ (Problem 2). Thus R is not regular.

Here is a convenient way to express regularity.

8.1.3 Proposition

Let $(R, \mathcal{M}, k)$ be a Noetherian local ring. Then R is regular if and only if the dimension of R coincides with $\dim_k \mathcal{M}/\mathcal{M}^2$, the dimension of $\mathcal{M}/\mathcal{M}^2$ as a vector space over k. (See (3.3.11), condition (6), for a prior appearance of this vector space.)

Proof. Let d be the dimension of R. If R is regular and $a_1, \dots, a_d$ generate $\mathcal{M}$, then the $a_i + \mathcal{M}^2$ span $\mathcal{M}/\mathcal{M}^2$, so $\dim_k \mathcal{M}/\mathcal{M}^2 \le d$. But the opposite inequality always holds (even if R is not regular), by (5.4.2). Conversely, if $\{a_1 + \mathcal{M}^2, \dots, a_d + \mathcal{M}^2\}$ is a basis for $\mathcal{M}/\mathcal{M}^2$, then the a_i generate $\mathcal{M}$. (Apply (0.3.4) with $J = M = \mathcal{M}$.) Thus R is regular. ♣

8.1.4 Theorem

A regular local ring is an integral domain.

Proof. The proof of (8.1.3) shows that the associated graded ring of R, with the $\mathcal{M}$-adic filtration [see (4.1.2)], is isomorphic to the polynomial ring $k[X_1, \dots, X_d]$, and is therefore a domain. The isomorphism identifies a_i with X_i, $i = 1, \dots, d$. By the Krull intersection theorem, $\cap_{n=0}^{\infty} \mathcal{M}^n = 0$. (Apply (4.3.4) with $M = R$ and $I = \mathcal{M}$.) Now let a and b be nonzero elements of R, and choose m and n such that $a \in \mathcal{M}^m \setminus \mathcal{M}^{m+1}$ and $b \in \mathcal{M}^n \setminus \mathcal{M}^{n+1}$. Let $\overline{a}$ be the image of a in $\mathcal{M}^m/\mathcal{M}^{m+1}$ and let $\overline{b}$ be the image of b in $\mathcal{M}^n/\mathcal{M}^{n+1}$. Then $\overline{a}$ and $\overline{b}$ are nonzero, hence $\overline{a}\,\overline{b} \neq 0$ (because the associated graded ring is a domain). But $\overline{a}\,\overline{b} = \overline{ab}$, the image of ab in $\mathcal{M}^{m+n+1}$, and it follows that ab cannot be 0. ♣

We now examine when a sequence can be extended to a regular system of parameters.

8.1.5 Proposition

Let $(R, \mathcal{M}, k)$ be a regular local ring of dimension d, and let $a_1, \dots, a_t \in \mathcal{M}$, where $1 \le t \le d$. The following conditions are equivalent.

(1) $a_1, \dots, a_t$ can be extended to a regular system of parameters for R.
(2) $\overline{a}_1, \dots, \overline{a}_t$ are linearly independent over k, where $\overline{a}_i = a_i \mod \mathcal{M}^2$.
(3) $R/(a_1, \dots, a_t)$ is a regular local ring of dimension $d - t$.

Proof. The proof of (8.1.3) shows that (1) and (2) are equivalent. Specifically, the a_i extend to a regular system of parameters iff the $\overline{a}_i$ extend to a k-basis of $\mathcal{M}/\mathcal{M}^2$. To prove that (1) implies (3), assume that $a_1, \dots, a_t, a_{t+1}, \dots, a_d$ is a regular system of parameters for R. By (6.1.3), the dimension of $\overline{R} = R/(a_1, \dots, a_t)$ is $d - t$. But the $d - t$ elements $\overline{a}_i, i = t + 1, \dots, d$, generate $\overline{\mathcal{M}} = \mathcal{M}/(a_1, \dots, a_t)$, hence $\overline{R}$ is regular.

Now assume (3), and let $a_{t+1}, \dots, a_d$ be elements of $\mathcal{M}$ whose images in $\overline{\mathcal{M}}$ form a regular system of parameters for $\overline{R}$. If $x \in \mathcal{M}$, then modulo $I = (a_1, \dots, a_t)$, we have

$x - \sum_{t+1}^{d} c_i a_i = 0$ for some $c_i \in R$. In other words, $x - \sum_{t+1}^{d} c_i a_i \in I$. It follows that $a_1, \dots, a_t, a_{t+1}, \dots, a_d$ generate $\mathcal{M}$. Thus R is regular (which we already know by hypothesis) and $a_1, \dots, a_t$ extend to a regular system of parameters for R. ♣

8.1.6 Theorem

Let $(R, \mathcal{M}, k)$ be a Noetherian local ring. Then R is regular if and only if $\mathcal{M}$ can be generated by an R-sequence. The length of any such R-sequence is the dimension of R.

Proof. Assume that R is regular, with a regular system of parameters $a_1, \dots, a_d$. If $1 \le t \le d$, then by (8.1.5), $\overline{R} = R/(a_1, \dots, a_t)$ is regular and has dimension $d - t$. The maximal ideal $\overline{\mathcal{M}}$ of $\overline{R}$ can be generated by $\overline{a}_{t+1}, \dots, \overline{a}_d$, so these elements form a regular system of parameters for $\overline{R}$. By (8.1.4), $\overline{a}_{t+1}$ is not a zero-divisor of $\overline{R}$, in other words, a_{t+1} is not a zero-divisor of $R/(a_1, \dots, a_t)$. By induction, $a_1, \dots, a_d$ is an R-sequence. (To start the induction, set $t = 0$ and take $(a_1, \dots, a_t)$ to be the zero ideal.)

Now assume that $\mathcal{M}$ is generated by the R-sequence $a_1, \dots, a_d$. By repeated applicaion of (5.4.7), we have $\dim R/\mathcal{M} = \dim R - d$. But $R/\mathcal{M}$ is the residue field k, which has dimension 0. It follows that $\dim R = d$, so R is regular. ♣

8.1.7 Corollary

A regular local ring is Cohen-Macaulay.

Proof. By (8.1.6), the maximal ideal $\mathcal{M}$ of the regular local ring R can be generated by an R-sequence $a_1, \dots, a_d$, with (necessarily) $d = \dim R$. By definition of depth [see(6.2.5)], $d \le$ depth R. But by (6.2.6), depth $R \le \dim R$. Since $\dim R = d$, it follows that depth$R = \dim R$. ♣

List of Symbols

Index

Exercises

Chapter 1

1. What are the primary ideals of $\mathbb{Z}$?
2. Let $R = k[x, y]$ where k is a field. Show that $Q = (x, y^2)$ is P-primary, and identify P.
3. Continuing Problem 2, show that Q is not a power of a prime ideal.
4. Let $R = k[x, y, z]/I$ where $I = (xy - z^2)$. Let $\overline{x} = x + I,\ \overline{y} = y + I,\ \overline{z} = z + I$. If $\overline{P} = (\overline{x}, \overline{z})$, show that $\overline{P}^2$ is a power of a prime ideal and its radical is prime, but it is not primary.
5. Let $R = k[x, y]$ where k is a field, and let $P_1 = (x),\ P_2 = (x, y),\ Q = (x^2, y),\ I = (x^2, xy)$. Show that $I = P_1 \cap P_2^2$ and $I = P_1 \cap Q$ are both primary decompositions of I.
6. Let M and N be finitely generated modules over a local ring R. Show that $M \otimes_R N = 0$ if and only if either M or N is 0.
7. Continuing Problem 6, show that the result fails to hold if R is not local.
8. Let S be a multiplicative subset of R, and $M_S = S^{-1}M$. Use base change formulas in the tensor product to show that $(M \otimes_R N)_S \cong M_S \otimes_{R_S} N_S$ as R_S-modules.
9. If M and N are finitely generated R-modules, show that $\operatorname{Supp}(M \otimes_R N) = \operatorname{Supp} M \cap \operatorname{Supp} N$.

   In Problems 10-13, we consider uniqueness in the structure theorem (1.6.7) for Artinian rings.

10. Let $R = \prod_1^r R_i$, where the R_i are Artinian local rings, and let π_i be the projection of R on R_i. Show that each R_i has a unique prime ideal P_i, which is nilpotent. Then show that $\mathcal{M}_i = \pi_i^{-1}(P_i)$ is a maximal ideal of R.
11. Let $I_i = \ker \pi_i, i = 1, \dots, r$. Show that $\sqrt{I_i} = \mathcal{M}_i$, so by (1.1.2), I_i is $\mathcal{M}_i$-primary.
12. Show that $\cap_1^r I_i$ is a reduced primary decomposition of the zero ideal.
13. Show that in (1.6.7), the R_i are unique up to isomorphism.
14. Let M be finitely generated over the Noetherian ring R, and let P be a prime ideal in the support of M. Show that $l_{R_P}(M_P) < \infty$ if and only if P is a minimal element of $\operatorname{AP}(M)$.

Chapter 2

1. Let $R = \mathbb{Z}$ and $S = \mathbb{Z}[i]$, the Gaussian integers. Give an example of two prime ideals of S lying above the same prime ideal of R. (By (2.2.1), there cannot be an inclusion relation between the prime ideals of S.)
2. Let $R = k[X,Y]/I$, where k is a field and I is the prime ideal $(X^2 - Y^3)$. Write the coset $X + I$ simply as x, and $Y + I$ as y. Show that $\alpha = x/y$ is integral over R, but $\alpha \notin R$. Thus R is not integrally closed.
3. Suppose we have a diagram of R-modules

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

with $\operatorname{im} f \subseteq \ker g$. Show that the following conditions are equivalent.

(a) The given sequence is exact.

(b) The sequence

$$M'_P \xrightarrow{f_P} M_P \xrightarrow{g_P} M''_P$$

is exact for every prime ideal P.

(c) The localized sequence of (b) is exact for every maximal ideal P.

4. Let $f : M \to N$ be an R-module homomorphism. Show that f is injective [resp. surjective] if and only if f_P is injective [resp. surjective] for every prime, equivalently for every maximal, ideal P.
5. Let R be an integral domain with fraction field K. We may regard all localized rings R_P as subsets of K. Let M be the intersection of all R_P for maximal ideals P. If S is any multiplicative subset of R, show that

$$S^{-1}M \subseteq \bigcap_{P \in \max R} S^{-1}R_P$$

where $\max R$ is the set of maximal ideals of R.

6. Continuing Problem 5, if Q is any maximal ideal of R, show that $M_Q \subseteq R_Q$.
7. Continuing Problem 6, show that the intersection of all R_P, P prime, coincides with the intersection of all R_P, P maximal, and in fact both intersections coincide with R.
8. If R is an integral domain, show that the following conditions are equivalent:

(a) R is integrally closed;

(b) R_P is integrally closed for every prime ideal P;

(c) R_Q is integrally closed for every maximal ideal Q.

9. Let P be a prime ideal of R. Show that the fields R_P/PR_P and $\operatorname{Frac} R/P$ are isomorphic. Each is referred to as the *residue field* at P.

Chapter 3

Let R and S be local subrings of the field K, with maximal ideals $\mathcal{M}_R$ and $\mathcal{M}_S$ respectively. We say that S *dominates* R, and write $(R, \mathcal{M}_R) \leq (S, \mathcal{M}_S)$, if R is a subring of S and $R \cap \mathcal{M}_S = \mathcal{M}_R$.

1. If V is a valuation ring of K, show that $(V, \mathcal{M}_V)$ is maximal with respect to the partial ordering induced by domination.

   Conversely, we will show in Problems 2 and 3 that if $(V, \mathcal{M}_V)$ is maximal, then V is a valuation ring. Let k be the residue field $V/\mathcal{M}_V$, and let C be an algebraic closure of k. We define a homomorphism $h : V \to C$, by following the canonical map from V to k by the inclusion map of k into C. By (3.1.4), it suffices to show that (V, h) is a maximal extension. As in (3.1.1), if (R_1, h_1) is an extension of (V, h), we may assume R_1 local and $h_1(R_1)$ a subfield of C. Then $\ker h_1$ is the unique maximal ideal $\mathcal{M}_{R_1}$.

2. Show that $(R_1, \mathcal{M}_{R_1})$ dominates $(V, \mathcal{M}_V)$.
3. Complete the proof by showing that (V, h) is a maximal extension.
4. Show that every local subring of a field K is dominated by at least one valuation ring of K.

Chapter 4

1. Let R be the formal power series ring $k[[X_1, \ldots, X_n]]$, where k is a field. Put the I-adic filtration on R, where I is the unique maximal ideal $(X_1, \ldots, X_n)$. Show that the associated graded ring of R is the polynomial ring $k[X_1, \ldots, X_n]$.
2. Let M and N be filtered modules over the filtered ring R. The R-homomorphism $f : M \to N$ is said to be a *homomorphism of filtered modules* if $f(M_n) \subseteq N_n$ for all $n \geq 0$. For each n, f induces a homomorphism $\overline{f}_n : M_n/M_{n+1} \to N_n/N_{n+1}$ via $\overline{f}_n(x + M_{n+1}) = f(x) + N_{n+1}$. We write $\mathrm{gr}_n(f)$ instead of $\overline{f}_n$. The $\mathrm{gr}_n(f)$ extend to a homomorphism of graded $\mathrm{gr}(R)$-modules, call it $\mathrm{gr}(f) : \mathrm{gr}(M) \to \mathrm{gr}(N)$. We write

   $$\mathrm{gr}(f) = \bigoplus_{n \geq 0} \mathrm{gr}_n(f).$$

   For the remainder of this problem and in Problems 3 and 4, we assume that $\mathrm{gr}(f)$ is injective. Show that $M_n \cap f^{-1}(N_{n+1}) \subseteq M_{n+1}$ for all $n \geq 0$.
3. Continuing Problem 2, show that $f^{-1}(N_n) \subseteq M_n$ for all $n \geq 0$.
4. Continuing Problem 3, show that if in addition we have $\cap_{n=0}^{\infty} M_n = 0$, then f is injective.
5. Show that in (4.2.10), the two filtrations $\{I^n N\}$ and $\{N \cap I^n M\}$ are equivalent.
6. If we reverse the arrows in the definition of an inverse system [see (4.2.1)], so that maps go from M_n to M_{n+1}, we get a *direct system*. The *direct limit* of such a system is the disjoint union $\coprod M_n$, with sequences x and y identified if they agree sufficiently far out in the ordering. In other words, $\theta_n(x_n) = \theta_n(y_n)$ for all sufficiently large n.

   In (4.2.6) we proved that the inverse limit functor is left exact, and exact under an additional assumption. Show that the direct limit functor is always exact. Thus if $M_n' \xrightarrow{f_n} M_n \xrightarrow{g_n} M_n''$ is exact for all n, and

   $$M = \varinjlim M_n$$

is the direct limit of the M_n (similarly for M' and M''), then the sequence

$M' \xrightarrow{f} M \xrightarrow{g} M''$ is exact. (The maps f and g are induced by the f_n and g_n.)

7. Let M be an R-module, and let $\hat{M}$ [resp. $\hat{R}$] be the I-adic completion of M [resp. R]. Note that $\hat{M}$ is an $\hat{R}$-module via $\overline{\{a_n\}}\ \overline{\{x_n\}} = \overline{\{a_n x_n\}}$. Define an R-module homomorphism $h_M : \hat{R} \otimes_R M \to \hat{M}$ by $(\overline{r}, m) \to \overline{r}\ m$. If M is finitely generated over R, show that h_M is surjective.
8. In Problem 7, if in addition R is Noetherian, show that h_M is an isomorphism. Thus if R is complete ($R \cong \hat{R}$), then M is complete ($M \cong \hat{M}$).
9. Show that the completion of M is always complete, that is, $\hat{\hat{M}} \cong \hat{M}$.
10. Let $\hat{R}$ be the I-adic completion of the Noetherian ring R. Show that $\hat{R}$ is a flat R-module.
11. If M is complete with respect to the filtration $\{M_n\}$, show that the topology induced on M by $\{M_n\}$ must be Hausdorff.

In Problems 12-16, $\hat{R}$ is the I-adic completion of the ring R. In Problems 12-14, R is assumed Noetherian.

12. Show that $\hat{I} \cong \hat{R} \otimes_R I \cong \hat{R}I$.
13. Show that $(\hat{I})^n \cong (I^n)\hat{}$.
14. Show that $I^n/I^{n+1} \cong (\hat{I})^n/(\hat{I})^{n+1}$.
15. Show that $\hat{I}$ is contained in the Jacobson radical $J(\hat{R})$.
16. Let R be a local ring with maximal ideal $\mathcal{M}$. If $\hat{R}$ is the $\mathcal{M}$-adic completion of R, show that $\hat{R}$ is a local ring with maximal ideal $\hat{\mathcal{M}}$.

Chapter 5

1. In differential calculus, the exponential function e^x is its own derivative. What is the analogous statement in the calculus of finite differences?
2. Let M be nonzero and finitely generated over the local ring R with maximal ideal $\mathcal{M}$. Show that $V(\operatorname{ann}(M/\mathcal{M}M)) = \{\mathcal{M}\}$.
3. If I is an arbitrary ideal and P a prime ideal of R, show that $(R/I)_P \neq 0$ iff $P \supseteq I$.

In Problems 4-7, the ring S is integral over the subring R, J is an ideal of S, and $I = J \cap R$. Establish the following.

4. $\dim R = \dim S$.
5. coht $I =$ coht J.
6. ht $J \leq$ ht I.
7. If R and S are integral domains with R integrally closed, then ht $J =$ ht I.

If P is a prime ideal of R, then by definition of height, coheight and dimension, we have ht $P+$ coht $P \leq \dim R$. In Problems 8 and 9 we show that the inequality can be strict, even if R is Noetherian. Let $S = k[[X,Y,Z)]]$ be a formal power series ring over the field k, and let $R = S/I$ where $I = (XY, XZ)$. Define $\overline{X} = X + I$, $\overline{Y} = Y + I$, $\overline{Z} = Z + I$.

8. Show that the dimension of R is 2.
9. Let P be the prime ideal $(\overline{Y}, \overline{Z})$ of R. Show that P has height 0 and coheight 1, so that ht $P+$ coht $P < \dim R$.

Chapter 6

1. Let R be a Noetherian local ring with maximal ideal $\mathcal{M}$, and suppose that the elements $a_1, \dots, a_t$ are part of a system of parameters for R. If the ideal $P = (a_1, \dots, a_t)$ is prime and has height t, show that $\operatorname{ht} P + \operatorname{coht} P = \dim R$.
2. let $S = k[[X,Y,Z]]$ be a formal power series ring over the field k, and let $R = S/I$, where $I = (XY, XZ)$. Use an overbar to denote cosets mod I, for example, $\overline{X} = X + I \in R$. Show that $\{\overline{Z}, \overline{X} + \overline{Y}\}$ is a system of parameters, but $\overline{Z}$ is a zero-divisor. On the other hand, members of a regular sequence (Section 6.2) cannot be zero-divisors.

Chapter 7

1. Let $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$, a free $\mathbb{Z}_4$-module. Define $f : \mathbb{Z}_4 \to \mathbb{Z}_4$ by $0 \to 0, 1 \to 2, 2 \to 0, 3 \to 2$, i.e., $f(x) = 2x \mod 4$. Let $M = 2\mathbb{Z}_4 \cong \mathbb{Z}_2$ (also a $\mathbb{Z}_4$-module), and define $g : \mathbb{Z}_4 \to M$ by $0 \to 0, 1 \to 1, 2 \to 0, 3 \to 1$, i.e., $g(x) = x \mod 2$. Show that $\cdots \longrightarrow \mathbb{Z}_4 \xrightarrow{f} \mathbb{Z}_4 \xrightarrow{f} \mathbb{Z}_4 \xrightarrow{f} \mathbb{Z}_4 \xrightarrow{g} M \longrightarrow 0$ is a free, hence projective, resolution of M of infinite length.
2. Given an exact sequence

$$\cdots \longrightarrow C_{n+1} \xrightarrow{\partial_{n+1}} A_n \xrightarrow{f_n} B_n \xrightarrow{g_n} C_n \xrightarrow{\partial_n} A_{n-1} \xrightarrow{f_{n-1}} B_{n-1} \xrightarrow{g_{n-1}} C_{n-1} \longrightarrow \cdots$$

Show that if the maps f_n are all isomorphisms, then $C_n = 0$ for all n.

Let R be a Noetherian local ring with maximal ideal $\mathcal{M}$ and residue field $k = R/\mathcal{M}$. Let M be a finitely generated R-module, and define $u_M : \mathcal{M} \otimes_R M \to M$ via $u_M(a \otimes x) = ax, a \in \mathcal{M}, x \in M$. We are going to show in Problems 3,4 and 5 that if u_M is injective, then M is free. If M is generated by $x_1, \dots, x_n$, let F be a free R-module with basis $e_1, \dots, e_n$. Define a homomorphism $g : F \to M$ via $e_i \to x_i, 1 \le i \le n$. We have an exact sequence $0 \to K \to F \to M \to 0$, where $f : K \to F, g : F \to M$, and $K = \ker g$. The following diagram is commutative, with exact rows.

$$\begin{array}{ccccccc}
 & & \mathcal{M} \otimes K & \longrightarrow & \mathcal{M} \otimes F & \longrightarrow & \mathcal{M} \otimes M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle u_K} & & \downarrow{\scriptstyle u_F} & & \downarrow{\scriptstyle u_M} & & \\
0 & \longrightarrow & K & \longrightarrow & F & \longrightarrow & M & &
\end{array}$$

Applying the snake lemma, we have an exact sequence

$$\ker u_M \xrightarrow{\delta} \operatorname{coker} u_K \xrightarrow{f^*} \operatorname{coker} u_F \xrightarrow{g^*} \operatorname{coker} u_M.$$

3. Show that $\operatorname{coker} u_M \cong k \otimes_R M$, and similarly $\operatorname{coker} u_F \cong k \otimes_R F$.
4. Show that $\operatorname{coker} u_K = 0$.
5. Show that g is injective. Since g is surjective by definition, it is an isomorphism, hence $M \cong F$, and M is free.
6. Let M be a finitely generated module over the Noetherian local ring R. Show that M is free if and only if M is projective, if and only if M is flat.
7. Show that in (7.2.1), M can be replaced by R/I, I an arbitrary ideal of R.
8. Show that the global dimension of a ring R is the least upper bound of $\operatorname{pd}_R(R/I)$, where I ranges over all ideals of R.
9. Let $f : R \to S$ be a ring homomorphism, and let M be an R-module. Prove that the following conditions are equivalent.
   (a) $\operatorname{Tor}_1^R(M, N) = 0$ for all S-modules N.
   (b) $\operatorname{Tor}_1^R(M, S) = 0$ and $M \otimes_R S$ is a flat S-module.

Chapter 8

1. In (8.1.2), Example 4, show that $\overline{X} - 1$ and $\overline{Y} - 1$ are associates.
2. Justify the assertions made in Example 5 of (8.1.2).

   Let $(R, \mathcal{M}, k)$ be a Noetherian local ring, and let $\operatorname{gr}_{\mathcal{M}}(R)$ be the associated graded ring with respect to the $\mathcal{M}$-adic filtration [see(4.1.2)]. We can define a homomorphism of graded k-algebras $\varphi : k[X_1, \dots, X_r] \to \operatorname{gr}_{\mathcal{M}}(R)$ via $\varphi(X_i) = a_i + \mathcal{M}^2$, where the a_i generate $\mathcal{M}$. (See Chapter 4, Problem 2 for terminology.) In Problems 3-5, we are going to show that φ is an isomorphism if and only if the Hilbert polynomial $h(n) = h(\operatorname{gr}_{\mathcal{M}}(R), n)$ has degree $r - 1$. Equivalently, the Hilbert-Samuel polynomial $s_{\mathcal{M}}(R, n)$ has degree r.
3. Assume that φ is an isomorphism, and let A_n be the set of homogeneous polynomials of degree n in $k[X_1, \dots, X_r]$. Then A_n is isomorphic as a k-vector space to $I = (X_1, \dots, X_r)$. Compute the Hilbert polynomial of $\operatorname{gr}_{\mathcal{M}}(R)$ and show that it has degree $r - 1$.
4. Now assume that φ is not an isomorphism, so that its kernel B is nonzero. Then B becomes a graded ring $\oplus_{n \geq 0} B_n$ with a grading inherited from the polynomial ring $A = k[X_1, \dots, X_r]$. We have an exact sequence
   $$0 \to B_n \to A_n \to \mathcal{M}^n/\mathcal{M}^{n+1} \to 0.$$
   Show that
   $$h(n) = \binom{n + r - 1}{r - 1} - l_k(B_n).$$
5. Show that the polynomial-like functions on the right side of the above equation for $h(n)$ have the same degree and the same leading coefficient. It follows that the Hilbert polynomial has degree less than $r - 1$, completing the proof.

6. Let $(R, \mathcal{M}, k)$ be a Noetherian local ring of dimension d. Show that R is regular if and only if the associated graded ring $\mathrm{gr}_{\mathcal{M}}(R)$ is isomorphic as a graded k-algebra to $k[X_1, \dots, X_d]$.

Solutions to Problems

Chapter 1

1. The primary ideals are (0) and (p^n), p prime.
2. $R/Q \cong k[y]/(y^2)$, and zero-divisors in this ring are of the form $cy + (y^2)$, $c \in k$, so they are nilpotent. Thus Q is primary. Since $r(Q) = P = (x, y)$, Q is P-primary.
3. If $Q = P_0^n$ with P_0 prime, then $\sqrt{Q} = P_0$, so by Problem 2, $P_0 = (x, y)$. But $x \in Q$ and $x \notin P_0^n$ for $n \geq 2$, so $Q \neq P_0^n$ for $n \geq 2$. Since $y \in P_0$ but $y \notin Q$, we have $Q \neq P_0$ and we reach a contradiction.
4. $\overline{P}$ is prime since $R/\overline{P} \cong k[y]$, an integral domain. Thus $\overline{P}^2$ is a prime power and its radical is the prime ideal $\overline{P}$. But it is not primary, because $\overline{x}\,\overline{y} = \overline{z}^2 \in \overline{P}^2$, $\overline{x} \notin \overline{P}^2$, $\overline{y} \notin \overline{P}$.
5. We have $I \subseteq P_1 \cap P_2^2$ and $I \subseteq P_1 \cap Q$ by definition of the ideals involved. For the reverse inclusions, note that if $f(x, y)x = g(x, y)y^2$ (or $f(x, y)x = g(x, y)y$), then $g(x, y)$ must involve x and $f(x, y)$ must involve y, so $f(x, y)$ is a polynomial multiple of xy.

   Now P_1 is prime (because $R/P_1 \cong k[y]$, a domain), hence P_1 is P_1-primary. P_2 is maximal and $\sqrt{P_2^2} = \sqrt{Q} = P_2$. Thus P_2^2 and Q are P_2-primary. [See (1.1.1) and (1.1.2). Note also that the results are consistent with the first uniqueness theorem.]
6. Let $\mathcal{M}$ be the maximal ideal of R, and $k = R/\mathcal{M}$ the residue field. Let $M_k = k \otimes_R M = (R/\mathcal{M}) \otimes_R M \cong M/\mathcal{M}M$. Assume $M \otimes_R N = 0$. Then $M_k \otimes_k N_k = (k \otimes_R M) \otimes_k (k \otimes_R N) = [(k \otimes_R M) \otimes_k k] \otimes_R N = (k \otimes_R M) \otimes_R N = k \otimes_R (M \otimes_R N) = 0$. Since M_k and N_k are finite-dimensional vector spaces over a field, one of them must be 0. [$k^r \otimes_k k^s = (k \otimes_k k^s)^r$ because tensor product commutes with direct sum, and this equals $(k^s)^r = k^{rs}$.] If $M_k = 0$, then $M = \mathcal{M}M$, so by NAK, $M = 0$. Similarly, $N_k = 0$ implies $N = 0$.
7. We have $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/(n, m)\mathbb{Z}$, which is 0 if n and m are relatively prime.
8. $(M \otimes_R N)_S \cong R_S \otimes_R (M \otimes_R N) \cong (R_S \otimes_R M) \otimes_R N \cong M_S \otimes_R N \cong (M_S \otimes_{R_S} R_S) \otimes_R N \cong M_S \otimes_{R_S} (R_S \otimes_R N) \cong M_S \otimes_{R_S} N_S$.
9. By Problem 8, $(M \otimes_R N)_P \cong M_P \otimes_{R_P} N_P$ as R_P-modules. Thus $P \notin \operatorname{Supp}(M \otimes_R N)$ iff $M_P \otimes_{R_P} N_P = 0$. By Problem 6, this happens iff $M_P = 0$ or $N_P = 0$, that is, $P \notin \operatorname{Supp} M$ or $P \notin \operatorname{Supp} N$.

10. The first assertion follows from (1.6.4) and (1.6.6). Since the preimage of a prime ideal under a ring homomorphism is prime, the second assertion follows from (1.6.4).
11. Say $P_i^n = 0$. Then $x \in \mathcal{M}_i$ iff $\pi_i(x) \in P_i$ iff $\pi_i(x^n) = 0$ iff $x^n \in I_i$, and the result follows.
12. Since I_i consists of those elements that are 0 in the i^{th} coordinate, the zero ideal is the intersection of the I_i, and $I_i \not\supseteq \cap_{j \neq i} I_j$. By Problem 11, the decomposition is primary. Now $I_i \subseteq \sqrt{I_i} = \mathcal{M}_i$, and $I_i + I_j = R$ for $i \neq j$. Thus $\mathcal{M}_i + \mathcal{M}_j = R$, so the $\mathcal{M}_i$ are distinct and the decomposition is reduced.
13. By Problem 12, the $\mathcal{M}_i$ are distinct and hence minimal. By the second uniqueness theorem (1.4.5), the I_i are unique (for a given R). Since $R_i \cong R/I_i$, the R_i are unique up to isomorphism.
14. By (1.6.9), the length $l_{R_P}(M_P)$ will be finite iff every element of $\mathrm{AP}_{R_P}(M_P)$ is maximal. Now R_P is a local ring with maximal ideal PR_P. By the bijection of (1.4.2), $l_{R_P}(M_P) < \infty$ iff there is no $Q \in \mathrm{AP}(M)$ such that $Q \subset P$. By hypothesis, $P \in \operatorname{Supp} M$, so by (1.5.8), P contains some $P' \in \mathrm{AP}(M)$, and under the assumption that $l_{R_P}(M_P)$ is finite, P must coincide with P'. The result follows.

Chapter 2

1. Let $Q_1 = (2+i), \quad Q_2 = (2-i)$. An integer divisible by $2+i$ must also be divisible by the complex conjugate $2-i$, hence divisible by $(2+i)(2-i) = 5$. Thus $Q_1 \cap \mathbb{Z} = (5)$, and similarly $Q_2 \cap \mathbb{Z} = (5)$.
2. We have $x^2 = y^3$, hence $(x/y)^2 = y$. Thus $\alpha^2 - y = 0$, so α is integral over R. If $\alpha \in R$, then $\alpha = x/y = f(x,y)$ for some polynomial f in two variables with coefficients in k, Thus $x = yf(x,y)$. Written out longhand, this is $X + I = Yf(X,Y) + I$, and consequently $X - Yf(X,Y) \in I = (X^2, Y^3)$. This is impossible because there is no way that a linear combination $g(X,Y)X^2 + h(X,Y)Y^3$ can produce X.
3. Since the localization functor is exact, we have (a) implies (b), and (b) implies (c) is immediate. To prove that (c) implies (a), consider the exact sequence

$$0 \longrightarrow \operatorname{im} f \xrightarrow{i} \ker g \xrightarrow{\pi} \ker g / \operatorname{im} f \longrightarrow 0$$

Applying the localization functor, we get the exact sequence

$$0 \longrightarrow (\operatorname{im} f)_P \xrightarrow{i_P} (\ker g)_P \xrightarrow{\pi_P} (\ker g / \operatorname{im} f)_P \longrightarrow 0$$

for every prime ideal P. But by basic properties of localization,

$$(\ker g / \operatorname{im} f)_P = (\ker g)_P / (\operatorname{im} f)_P = \ker g_P / \operatorname{im} f_P,$$

which is 0 for every prime ideal P, by (c). By (1.5.1), $\ker g / \operatorname{im} f = 0$, in other words, $\ker g = \operatorname{im} f$, proving (a).
4. In the injective case, apply Problem 3 to the sequence

$$0 \longrightarrow M \xrightarrow{f} N,$$

and in the surjective case, apply Problem 3 to the sequence

$$M \xrightarrow{f} N \longrightarrow 0.$$

5. This follows because $S^{-1}(\cap A_i) \subseteq \cap_i S^{-1}(A_i)$ for arbitrary rings (or modules) A_i.
6. Taking $S = R \setminus Q$ and applying Problem 5, we have the following chain of inclusions, where P ranges over all maximal ideals of R:

$$M_Q = (\cap_P R_P)_Q \subseteq \cap_P (R_P)_Q \subseteq (R_Q)_Q = R_Q.$$

7. Since R is contained in every R_P, we have $R \subseteq M$, hence $R_Q \subseteq M_Q$ for every maximal ideal Q. Let $i : R \to M$ and $i_Q : R_Q \to M_Q$ be inclusion maps. By Problem 6, $R_Q = M_Q$, in particular, i_Q is surjective. Since Q is an arbitrary maximal ideal, i is surjective by Problem 4, so $R = M$. But $R \subseteq \cap_{P\text{prime}} R_P \subseteq M$, and the result follows.
8. The implication (a) implies (b) follows from (2.2.6), and (b) immediately implies (c). To prove that (c) implies (a), note that if for every i, K is the fraction field of A_i, where the A_i are domains that are integrally closed in K, then $\cap_i A_i$ is integrally closed. It follows from Problem 7 that R is the intersection of the R_Q, each of which is integrally closed (in the same fraction field K). Thus R is integrally closed.
9. The elements of the first field are $a/f + PR_P$ and the elements of the second field are $(a+P)/(f+P)$, where in both cases, $a, f \in R, f \notin P$. This tells you exactly how to construct the desired isomorphism.

Chapter 3

1. Assume that $(V, \mathcal{M}_V) \le (R, \mathcal{M}_R)$, and let α be a nonzero element of R. Then either α or α^{-1} belongs to V. If $\alpha \in V$ we are finished, so assume $\alpha \notin V$, hence $\alpha^{-1} \in V \subseteq R$. Just as in the proof of Property 9 of Section 3.2, α^{-1} is not a unit of V. (If $b \in V$ and $b\alpha^{-1} = 1$, then $\alpha = \alpha\alpha^{-1}b = b \in V$.) Thus $\alpha^{-1} \in \mathcal{M}_V = \mathcal{M}_R \cap V$, so α^{-1} is not a unit of R. This is a contradiction, as α and its inverse both belong to R.
2. 2. By definition of h, $\ker h = \mathcal{M}_V$. Since h_1 extends h, $\ker h = (\ker h_1) \cap V$, that is, $\mathcal{M}_V = \mathcal{M}_{R_1} \cap V$. Since $R_1 \supseteq V$, the result follows.
3. By hypothesis, $(V, \mathcal{M}_V)$ is maximal with respect to domination, so $(V, \mathcal{M}_V) = (R_1, \mathcal{M}_{R_1})$. Therefore $V = R_1$, and the proof is complete.
4. If $(R, \mathcal{M}_R)$ is not dominated in this way, then it is a maximal element in the domination ordering, hence R itself is a valuation ring.

Chapter 4

1. We have $f \in I^d$ iff all terms of f have degree at least d, so if we identify terms of degree at least $d+1$ with 0, we get an isomorphism between I^d/I^{d+1} and the homogeneous polynomials of degree d. Take the direct sum over all $d \ge 0$ to get the desired result.
2. If $x \in M_n$ and $f(x) \in N_{n+1}$, then $f(x) + N_{n+1} = 0$, so $x \in M_{n+1}$.

3. The result holds for $n = 0$ because $M_0 = M$ and $N_0 = N$. If it is true for n, let $x \in f^{-1}(N_{n+1})$. Since $N_{n+1} \subseteq N_n$, it follows that x belongs to $f^{-1}(N_n)$, which is contained in M_n by the induction hypothesis. By Problem 2, the result is true for $n+1$.

4. Using the additional hypothesis and Problem 3, we have $f^{-1}(0) \subseteq f^{-1}(\cap N_n) = \cap f^{-1}(N_n) \subseteq \cap M_n = 0$.

5. By (4.1.8) we have

$$(I^{m+k}M) \cap N = I^k((I^m) \cap N) \subseteq I^k N \subseteq (I^k M) \cap N.$$

6. Since $g_n \circ f_n = 0$ for all n, we have $g \circ f = 0$. If $g(y) = 0$, then y is represented by a sequence $\{y_n\}$ with $y_n \in M_n$ and $g_n(y_n) = 0$ for sufficiently large n. Thus for some $x_n \in M'_n$ we have $y_n = f_n(x_n)$. The elements x_n determine $x \in M'$ such that $y = f(x)$, proving exactness.

7. Since $\hat{R} \otimes_R R \cong \hat{R}$ and tensor product commutes with direct sum, h_M is an isomorphism when M is free of finite rank. In general, we have an exact sequence $0 \longrightarrow N \xrightarrow{f} F \xrightarrow{g} M \longrightarrow 0$ with F free of finite rank. Thus the following diagram is commutative, with exact rows.

$$\begin{array}{ccccccccc}
 & & \hat{R} \otimes_R N & \longrightarrow & \hat{R} \otimes_R F & \longrightarrow & \hat{R} \otimes_R M & \longrightarrow & 0 \\
 & & \downarrow h_N & & \downarrow h_F & & \downarrow h_M & & \\
0 & \longrightarrow & \hat{N} & \xrightarrow[\hat{f}]{} & \hat{F} & \xrightarrow[\hat{g}]{} & \hat{M} & \longrightarrow & 0
\end{array}$$

See (4.2.7) for the last row. Since $\hat{g}$ is surjective and h_F is an isomorphism, it follows that h_M is surjective.

8. By hypothesis, N is finitely generated, so by Problem 8, h_N is surjective. Since h_F is an isomorphism, h_M is injective by the four lemma. (See TBGY, 4.7.2, part (ii).)

9. Take inverse limits in (4.2.9).

10. Consider the diagram for Problem 7, with M finitely generated. No generality is lost; see TBGY, (10.8.1). Then all vertical maps are isomorphisms, so if we augment the first row by attaching $0 \to$ on the left, the first row remains exact. Thus the functor $\hat{R} \otimes_R$ — is exact, proving that $\hat{R}$ is flat.

11. Since M is isomorphic to its completion, we may regard $\hat{M}$ as the set of constant sequences in M. If x belongs to M_n for every n, then x converges to 0, hence x and 0 are identified in $\hat{M}$. By (4.2.4), the topology is Hausdorff.

12. I is finitely generated, so by Problem 8, $h_I : \hat{R} \otimes_R I \to \hat{I}$ is an isomorphism. Since $\hat{R}$ is flat over R by Problem 10, $\hat{R} \otimes_R I \to \hat{R} \otimes_R R \cong \hat{R}$ is injective, and the image of this map is $\hat{R}I$.

13. By Problem 12, $(I^n)\hat{} \cong \hat{R}I^n = (\hat{R}I)^n \cong (\hat{I})^n$.

14. The following diagram is commutative, with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I^n/I^{n+1} & \longrightarrow & R/I^{n+1} & \longrightarrow & R/I^n & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & (\hat{I})^n/(\hat{I})^{n+1} & \longrightarrow & \hat{R}/(\hat{I})^{n+1} & \longrightarrow & \hat{R}/(\hat{I})^n & \longrightarrow & 0 \end{array}$$

The second and third vertical maps are isomorphisms by (4.2.9), so the first vertical map is an isomorphism by the short five lemma.

15. By (4.2.9) and Problem 9, $\hat{R}$ is complete with respect to the $\hat{I}$-adic topology. Suppose that $a \in \hat{I}$. Since $a^n + a^{n+1} + \cdots + a^m \in (\hat{I})^n$ for all n, the series $1 + a + a^2 + \cdots + a^n$ converges to some $b \in \hat{R}$. Now $(1-a)(1+a+a^2+\cdots+a^n) = 1 - a^{n+1}$, and we can let n approach infinity to get $(1-a)b = 1$. Thus $a \in \hat{I} \Rightarrow 1 - a$ is a unit in $\hat{R}$. Since ax belongs to $\hat{I}$ for every $x \in \hat{R}$, $1 + ax$ is also a unit. By (0.2.1), $a \in J(\hat{R})$.

16. By (4.2.9), $R/\mathcal{M} \cong \hat{R}/\hat{\mathcal{M}}$, so $\hat{R}/\hat{\mathcal{M}}$ is a field, hence $\hat{\mathcal{M}}$ is a maximal ideal. By Problem 15, $\hat{\mathcal{M}}$ is contained in every maximal ideal, and it follows that $\hat{\mathcal{M}}$ is the unique maximal ideal of $\hat{R}$.

Chapter 5

1. The function 2^n is its own difference.

2. If P is a prime ideal containing $\operatorname{ann}(M/\mathcal{M}M)$, then $P \supseteq \mathcal{M}$, hence $P = \mathcal{M}$ by maximality of $\mathcal{M}$. Conversely, we must show that $\mathcal{M} \supseteq \operatorname{ann}(M/\mathcal{M}M)$. This will be true unless $\operatorname{ann}(M/\mathcal{M}M) = R$. In this case, 1 annihilates $M/\mathcal{M}M$, so $\mathcal{M}M = M$. By NAK, $M = 0$, contradicting the hypothesis.

3. Let $S = R \setminus P$. Then $(R/I)_P = 0$ iff $S^{-1}(R/I) = 0$ iff $S^{-1}R = S^{-1}I$ iff $1 \in S^{-1}I$ iff $1 = a/s$ for some $a \in I$ and $s \in S$ iff $I \cap S \neq 0$ iff I is not a subset of P.

4. By Going Up [see (2.2.3)], any chain of distinct prime ideals of R can be lifted to a chain of distinct prime ideals of S, so $\dim S \geq \dim R$. A chain of distinct prime ideals of S contracts to a chain of prime ideals of R, distinct by (2.2.1). Thus $\dim R \geq \dim S$.

5. Since S/J is integral over the subring R/I, it follows from (5.3.1) and Problem 4 that coht $I = \dim R/I = \dim S/J =$ coht J.

6. If J is a prime ideal of S, then $I = J \cap R$ is a prime ideal of R. The contraction of a chain of prime ideals of S contained in J is a chain of prime ideals of R contained in R, and distinctness is preserved by (2.2.1). Thus ht $J \leq$ ht I. Now let J be any ideal of S, and let P be a prime ideal of R such that $P \supseteq I$ and ht $P =$ ht I. (If the height of I is infinite, there is nothing to prove.) As in the previous problem, S/J is integral over R/I, so by Lying Over [see (2.2.2)] there is a prime ideal Q containing J that lies over P. Thus with the aid of the above proof for J prime, we have ht $J \leq$ ht $Q \leq$ ht $P =$ ht I.

7. First assume J is a prime ideal of S, hence I is a prime ideal of R. A descending chain of distinct prime ideals of R starting from I can be lifted to a descending chain of distinct prime ideals of S starting from J, by Going Down [see (2.3.4)]. Thus ht $J \geq$ ht I. For any ideal J, let Q be a prime ideal of S with $Q \supseteq J$. Then $P = Q \cap R \supseteq I$.

By what we have just proved, ht $Q \geq$ ht P, and ht $P \geq$ ht I by definition of height. Taking the infimum over Q, we have ht $J \geq$ ht I. By Problem 6, ht $J =$ ht I.

8. The chain of prime ideals $(\overline{X}) \subset (\overline{X}, \overline{Y}) \subset (\overline{X}, \overline{Y}, \overline{Z})$ gives $\dim R \geq 2$. Since XY (or equally well XZ), belongs to the maximal ideal (X, Y, Z) and is not a zero-divisor, we have $\dim R \leq \dim S/(XY) = \dim S - 1 = 2$ by (5.4.7) and (5.4.9).
9. The height of P is 0 because the ideals $(\overline{Y})$ and $(\overline{Z})$ are not prime. For example, $\overline{X} \notin (\overline{Y})$ and $\overline{Z} \notin (\overline{Y})$, but $\overline{X}\ \overline{Z} = \overline{0} \in (\overline{Y})$. Since $R/P \cong k[[X]]$ has dimension 1, P has coheight 1 by (5.3.1).

Chapter 6

1. By (6.1.3), $\dim R/P = \dim R - t = \dim R - \operatorname{ht} P$. By (5.3.1), $\dim R/P = \operatorname{coht} P$, and the result follows.
2. Let J be the ideal $(\overline{Z},\ \overline{X} + \overline{Y})$. If $\mathcal{M} = (X, Y, Z)$ is the unique maximal ideal of S, then $\overline{\mathcal{M}}^2 = (\overline{X}^2, \overline{Y}^2, \overline{Z}^2, \overline{Y}\ \overline{Z}) \subseteq J \subseteq \mathcal{M}$, so J is an ideal of definition. (Note that $\overline{X}\ \overline{Y} = \overline{X}\ \overline{Z} = 0$, $\overline{X}(\overline{X} + \overline{Y}) = \overline{X}^2$, and $\overline{Y}(\overline{X} + \overline{Y}) = \overline{Y}^2$.) By (6.1.2), $\{\overline{Z},\ \overline{X} + \overline{Y}\}$ is a system of parameters. Since $\overline{Z}\ \overline{X} = 0$, $\overline{Z}$ is a zero-divisor.

Chapter 7

1. Note that $\ker f, \operatorname{im} f$, and $\ker g$ are all equal to $\{0, 2\}$.
2. We have $\operatorname{im} \partial_n = \ker f_{n-1} = 0$ and $\ker g_n = \operatorname{im} f_n = B_n$. Thus g_n is the zero map, so $\ker \partial_n = \operatorname{im} g_n = 0$. Therefore ∂_n is an injective zero map, which forces $C_n = 0$.
3. This follows from the base change formula $R/I \otimes_R M \cong M/IM$ with $I = \mathcal{M}$ (see TBGY, S7.1).
4. We have $g^* : 1 \otimes e_i \to 1 \otimes x_i$, which is an isomorphism. (The inverse is $1 \otimes x_i \to 1 \otimes e_i$.) Thus $\operatorname{im} f^* = \ker g^* = 0$. Since f^* is the zero map, δ is surjective. But $\ker u_M$ is 0 by hypothesis, so $\delta = 0$. This forces coker $u_K = 0$.
5. By Problem 4, $K = \mathcal{M}K$. Since M is a Noetherian R-module, K is finitely generated, so by NAK we have $K = 0$. Thus $0 = \operatorname{im} f = \ker g$, so g is injective.
6. Since free implies projective implies flat always, it suffices to show that flat implies free. If M is flat, then the functor $N \to N \otimes_R M$ is exact. If $\mathcal{M}$ is the maximal ideal of R, then the map $\mathcal{M} \otimes_R M \to R \otimes_R M \cong M$ via $a \otimes x \to ax$ is injective. But this map is just u_M, and the result follows from Problems 3-5.
7. We have the short exact sequence $0 \to I \to R \to R/I \to 0$, which induces, for any R-module N, the exact sequence

$$\operatorname{Hom}_R(R/I, N) \to \operatorname{Hom}_R(R, N) \to \operatorname{Hom}_R(I, N) \to \operatorname{Ext}^1_R(R/I, N).$$

The last term is 0 by hypothesis, hence the map $i^* : \operatorname{Hom}_R(R, N) \to \operatorname{Hom}_R(I, N)$ is surjective. This says, by Baer's criterion (TBGY 10.6.4), that N is injective.

8. The left side is at least equal to the right side, so assuming that the right side is at most n, it suffices to show that $\text{id}_R N \le n$ for all N. Given an exact sequence as in (7.2.4) part 4, dimension shifting yields $\text{Ext}_R^{n+1}(R/I, N) \cong \text{Ext}_R^1(R/I, C_{n-1})$. By (7.1.7), $\text{Ext}_R^1(R/I, C_{n-1}) = 0$, so by (7.2.1) and Problem 7, C_{n-1} is injective. By (7.2.4), $\text{id}_R N \le n$.
9. If (a) holds, only the second assertion of (b) requires proof. Apply Tor to the exact sequence $0 \to N' \to N \to N'' \to 0$ to get the exact sequence

$$0 = \text{Tor}_1^R(M, N'') \to M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0.$$

We may replace $M \otimes_R N$ by $(M \otimes_R S) \otimes_S N$, and similarly for the other two tensor products. By exactness, $M \otimes_R S$ is flat. Now assuming (b), we have $\text{Tor}_1^R(M, F) = 0$ for every free S-module F, because Tor commutes with direct sums. If N is an arbitrary S-module, we have a short exact sequence $0 \to K \to F \to N \to 0$ with F free. The corresponding (truncated) long exact sequence is

$$0 = \text{Tor}_1^R(M, F) \to \text{Tor}_1^R(M, N) \to M \otimes_R K \to M \otimes_R F \to M \otimes_R N \to 0.$$

As before, we replace $M \otimes_R K$ by $(M \otimes_R S) \otimes_S K$, and similarly for the other two tensor products. The map whose domain is $(M \otimes_R S) \otimes_S K$ is induced by the inclusion of K into F, and is therefore injective, because $M \otimes_R S$ is a flat S-module by hypothesis. Thus the kernel of the map, namely $\text{Tor}_1^R(M, N)$, is zero.

Chapter 8

1. To ease the notation we will omit all the overbars and adopt the convention that all calculations are mod $(X^3 - Y^2)$. We have $(X^2 + X + 1)(X - 1) = X^3 - 1 = Y^2 - 1 = (Y - 1)(Y + 1)$. Now $X^2 + X + 1$ and $Y + 1$ are units in R because they do not vanish when $X = Y = 1$, assuming that the characteristic of K is not 2 or 3. Thus $X - 1$ and $Y - 1$ are associates.
2. The maximal ideal is not principal because $\overline{X}$ and $\overline{Y}$ cannot both be multiples of a single polynomial. To show that $\dim R = 1$, we use (5.6.7). Since $K(Y)$ has transcendence degree 1 over K and $K(X, Y)/(X^3 - Y^2)$ is algebraic over $K(Y)$, (we are adjoining a root of $X^3 - Y^2$), it follows that the dimension of $K[X, Y]/(X^3 - Y^2)$ is 1. By (5.3.1), the coheight of $(X^3 - Y^2)$ is 1, and the corresponding sequence of prime ideals is $(X^3 - Y^2), (X, Y)$. Thus localization at $(\overline{X}, \overline{Y})$ has no effect on dimension, so $\dim R = 1$. (In general, prime ideals of a localized ring A_P correspond to prime ideals of A that are contained in P, so localization may reduce the dimension.)
3. By definition, the Hilbert polynomial is the composition length $l_k(I^n/I^{n+1})$. Since monomials of degree n in r variables form a basis for the polynomials of degree n, we must count the number of such monomials, which is

$$\binom{n+r-1}{r-1} = \frac{(n+r-1)(n+r-2)\cdots(n+2)(n+1)}{(r-1)!}$$

This is a polynomial of degree $r - 1$ in the variable n.

4. This follows from Problem 3 and additivity of length (5.2.3).
5. Fix a nonzero element $b \in B_d$. (Frequently, b is referred to as a homogeneous element of degree d.) By definition of a graded ring, we have $bA_n \subseteq B_{n+d}$ for $n \geq 0$. Then

$$l_k(B_{n+d}) \geq l_k(bA_n) = l_k(A_n) \geq l_k(B_n).$$

Since $l_k(A_n) = \binom{n+r-1}{r-1}$, the result follows.
6. If R is regular, we may define the graded k-algebra homomorphism φ of Problems 3-5 with $r = d$. Since the Hilbert polynomial has degree d, φ is an isomorphism. Conversely, an isomorphism of graded k-algebras induces an isomorphism of first components, in other words,

$$(k[X_1, \dots, X_d])_1 \cong \mathcal{M}/\mathcal{M}^2.$$

But the k-vector space on the left has a basis consisting of all monomials of degree 1. Since there are exactly d of these, we have $\dim_k \mathcal{M}/\mathcal{M}^2 = d$. By (8.1.3), R is regular.