PRIMARY DECOMPOSITION OF MODULES

SUDHIR R. GHORPADE AND JUGAL K. VERMA

Department of Mathematics, Indian Institute of Technology, Mumbai 400076, India
E-Mail: {srg, jkv}@math.iitb.ac.in

Abstract. Basics of the theory of primary decomposition of modules are outlined here. The notions of graded rings and modules are also introduced, and then the special features of primary decomposition in the case of graded modules are discussed.

Contents

Date: November 23, 2000.

This is a slightly revised version of the second chapter of the Lecture Notes of the NBHM sponsored Instructional Conference on Combinatorial Topology and Algebra, held at IIT Bombay in December 1993. As such, these notes may be viewed as a continuation of [Gh], which was a revised version of the first chapter.

Introduction

In the first two sections, we will discuss an extension of the notions of associated primes and primary decomposition to the case of modules. The classical case of ideals I in (noetherian) rings A corresponds, in this general set-up, to the case of A–modules A/I; remembering this may be helpful in understanding some of the concepts and results below. Later, in Section 3, we describe the notion of graded rings and graded modules and prove some basic results concerning them. Finally, in Section 4 we discuss some special properties of primary decomposition in the case of graded modules over graded rings.

1. Associated Primes

Taking into consideration the modern viewpoint that the notion of associated primes is more fundamental than primary decomposition, we shall derive in this section basic results about associated primes without mentioning primary submodules or primary decomposition.

Throughout this section, we let A denote a ring and M an A–module. By $\operatorname{Spec} A$ we shall denote the set of all prime ideals of A; $\operatorname{Spec} A$ is sometimes called the *spectrum*[1] of A.

Definition: A prime ideal $\mathfrak{p}$ of A is called an *associated prime* of M if $\mathfrak{p} = (0 : x)$ for some $x \in M$. The set of all associated primes of M is denoted by $\operatorname{Ass}_A(M)$, or simply by $\operatorname{Ass}(M)$. Minimal elements of $\operatorname{Ass}(M)$ are called the *minimal primes* of M, and the remaining elements of $\operatorname{Ass}(M)$ are called the *embedded primes* of M.

Note that if $\mathfrak{p} = (0 : x) \in \operatorname{Ass}(M)$, then the map $a \mapsto ax$ of $A \to M$ defines an embedding (i.e., an injective A–module homomorphism) $A/\mathfrak{p} \hookrightarrow M$. Conversely, if for $\mathfrak{p} \in \operatorname{Spec} A$, we have an embedding $A/\mathfrak{p} \hookrightarrow M$, then clearly $\mathfrak{p} \in \operatorname{Ass}(M)$. It may also be noted that if M is isomorphic to some A–module M', then $\operatorname{Ass}(M) = \operatorname{Ass}(M')$.

(1.1) Lemma. *Any maximal element of* $\{(0 : y) : y \in M,\ y \neq 0\}$ *is a prime ideal. In particular, if A is noetherian, then* $\operatorname{Ass}(M) \neq \emptyset$ *iff* $M \neq 0$.

Proof: Suppose $(0 : x)$ is a maximal element of $\{(0 : y) : y \in M,\ y \neq 0\}$. Then $(0 : x) \neq A$ since $x \neq 0$. Moreover, if $a, b \in A$ are such that $ab \in (0 : x)$ and $a \notin (0 : x)$, then $ax \neq 0$ and $b \in (0 : ax) \subseteq (0 : x)$. Since $(0 : x)$ is maximal, $(0 : ax) = (0 : x)$. Thus $b \in (0 : x)$. Thus $(0 : x)$ is a prime ideal. The last assertion is evident. $\square$

Definition: An element $a \in A$ is said to be a *zerodivisor* of M if $(0 : a)_M \neq 0$, i.e., if $ax = 0$ for some $x \in M$ with $x \neq 0$. The set of all zerodivisors of M is denoted by $\mathcal{Z}(M)$.

(1.2) Exercise: Check that the above definition of $\mathcal{Z}(M)$ is consistent with that in (2.4) of [Gh]. Show that if A is noetherian, then $\mathcal{Z}(M) = \displaystyle\bigcup_{\mathfrak{p} \in \operatorname{Ass}(M)} \mathfrak{p}$.

[1] For an explanation of this terminology, see the article [Ta] by Taylor.

(1.3) Lemma. *For any submodule N of M,* $\mathrm{Ass}(N) \subseteq \mathrm{Ass}(M) \subseteq \mathrm{Ass}(N) \cup \mathrm{Ass}(M/N)$. *More generally, if $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ is any chain of submodules of M, then* $\mathrm{Ass}(M) \subseteq \cup_{i=1}^{n} \mathrm{Ass}(M_i/M_{i-1})$.

Proof: The inclusion $\mathrm{Ass}(N) \subseteq \mathrm{Ass}(M)$ is obvious. Let $x \in M$ be such that $(0 : x) \in \mathrm{Ass}(M)$. If $(0 : x) \notin \mathrm{Ass}(N)$, then we claim that $(0 : x) = (0 : \bar{x}) \in \mathrm{Ass}(M/N)$, where $\bar{x}$ denotes the image of x in M/N. To see this, note that $(0 : x) \subseteq (0 : \bar{x})$ and if $a \in A$ is such that $a\bar{x} = 0 \neq ax$, then $ax \in N$ and $a \notin (0 : x)$, and since $(0 : x)$ is prime, we have $b \in (0 : ax) \Leftrightarrow ba \in (0 : x) \Leftrightarrow b \in (0 : x)$; consequently, $(0 : x) = (0 : ax) \in \mathrm{Ass}(N)$, which is a contradiction. Thus $\mathrm{Ass}(M) \subseteq \mathrm{Ass}(N) \cup \mathrm{Ass}(M/N)$. The last assertion follows from this by induction on n. $\square$

The inclusions $\mathrm{Ass}(N) \subseteq \mathrm{Ass}(M)$ and $\mathrm{Ass}(M) \subseteq \mathrm{Ass}(N) \cup \mathrm{Ass}(M/N)$ in the above Lemma are, in general, proper. This may be seen, for instance, when A is a domain and $M = A$ by taking $N = 0$ and $N =$ a nonzero prime ideal of A, respectively.

(1.4) Corollary. *Suppose $M_1, \ldots, M_h$ are A–modules such that $M \simeq \oplus_{i=1}^{h} M_i$. Then* $\mathrm{Ass}(M) = \cup_{i=1}^{h} \mathrm{Ass}(M_i)$.

Proof: Follows using induction on h by noting that the case of $h = 2$ is a consequence of the first assertion in (1.3). $\square$

Example: Let G be a finite abelian group of order n. Suppose $n = p_1^{e_1} \ldots p_h^{e_h}$, where $p_1, \ldots, p_h$ are distinct prime numbers and $e_1, \ldots, e_h$ are positive integers. Then G is a $\mathbb{Z}$–module, and the p_i–Sylow subgroups P_i, $1 \leq i \leq h$, are $\mathbb{Z}$–submodules of G such that $G \simeq P_1 \oplus \cdots \oplus P_h$. Clearly, $\mathrm{Ass}(P_i) = p_i\mathbb{Z}$ [indeed, if y is any nonzero element of P_i of order p_i^e, then elements of $(0 : y)$ are multiples of p_i^e, and if $x = p_i^{e-1}y$, then $(0 : x) = p_i\mathbb{Z}$]. Thus by (1.4), $\mathrm{Ass}(G) = \{p_1\mathbb{Z}, \ldots, p_h\mathbb{Z}\}$. More generally, if M is a finitely generated abelian group, then $M = \mathbb{Z}^r \oplus T$ for some $r \geq 0$ and some finite abelian group T, and it follows from (1.4) that if $r > 0$ then $\mathrm{Ass}(M) = \{l_0\mathbb{Z}, l_1\mathbb{Z}, \ldots, l_s\mathbb{Z}\}$, where $l_0 = 0$ and $l_1, \ldots l_s$ are the prime numbers dividing the order of T.

Having discussed some properties of associated primes of quotient modules, we now describe what happens to associated prime upon localisation. Before that, let us recall that if S is m. c. subset of A, then the map $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ gives a one-to-one correspondence of $\{\mathfrak{p} \in \operatorname{Spec} A : \mathfrak{p} \cap S = \emptyset\}$ onto $\operatorname{Spec} S^{-1}A$.

(1.5) Lemma. *Suppose A is noetherian and S is a* m. c. *subset of A. Then*

$$\mathrm{Ass}_{S^{-1}A}(S^{-1}M) = \{S^{-1}\mathfrak{p} : \mathfrak{p} \in \mathrm{Ass}(M) \text{ and } \mathfrak{p} \cap S = \emptyset\}$$

Proof: If $\mathfrak{p} \in \mathrm{Ass}(M)$ and $S \cap \mathfrak{p} = \emptyset$, then we have an embedding $A/\mathfrak{p} \hookrightarrow M$, which, in view of (1.2) of [Gh], induces an embedding $S^{-1}A/S^{-1}\mathfrak{p} \hookrightarrow S^{-1}M$. And $S^{-1}\mathfrak{p} \in \operatorname{Spec} S^{-1}A$ since $S \cap \mathfrak{p} = \emptyset$. Thus $S^{-1}\mathfrak{p} \in \mathrm{Ass}_{S^{-1}A}(S^{-1}M)$. On the other hand, if $\mathfrak{p}' \in \mathrm{Ass}_{S^{-1}A}(S^{-1}M)$, then $\mathfrak{p}' = S^{-1}\mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Spec} A$ with $\mathfrak{p} \cap S = \emptyset$, and $\mathfrak{p}' = (0 : \frac{x}{1})$ for some $x \in M$. Write $\mathfrak{p} = (a_1, \ldots, a_n)$. Now $\frac{a_i}{1} \cdot \frac{x}{1} = 0$ in $S^{-1}M$ for $1 \leq i \leq n$, and thus there exists $t \in S$ such that $ta_ix = 0$ for $1 \leq i \leq n$. This implies that $\mathfrak{p} \subseteq (0 : tx)$. Further, if $a \in (0 : tx)$, then $\frac{a}{1} \in (0 : \frac{x}{1}) = S^{-1}\mathfrak{p}$ so that $sa \in \mathfrak{p}$ for some $s \in S$, and hence $a \in \mathfrak{p}$. Thus $\mathfrak{p} \in \mathrm{Ass}(M)$. $\square$

Note that the above result implies that if $\mathfrak{p} \in \mathrm{Ass}(M)$, then $\mathfrak{p}A_{\mathfrak{p}} \in \mathrm{Ass}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}})$. So, in particular, $M_{\mathfrak{p}} \neq 0$.

Definition: The set $\{\mathfrak{p} \in \operatorname{Spec} A : M_{\mathfrak{p}} \neq 0\}$ is called the *support* of M and is denoted by $\operatorname{Supp}(M)$.

(1.6) Lemma. $\operatorname{Supp}(M) \subseteq \{\mathfrak{p} \in \operatorname{Spec} A : \mathfrak{p} \supseteq \mathrm{Ann}(M)\}$. *Moreover, if M is* f. g., *then these two sets are equal.*

Proof: If $\mathfrak{p} \in \operatorname{Spec} A$ and $M_{\mathfrak{p}} \neq 0$, then there is $x \in M$ such that $\frac{x}{1} \neq 0$ in $M_{\mathfrak{p}}$. Now $a \in \mathrm{Ann}(M) \Rightarrow ax = 0 \Rightarrow a \notin A \setminus \mathfrak{p} \Rightarrow a \in \mathfrak{p}$. Thus $\mathfrak{p} \supseteq \mathrm{Ann}(M)$. Next, suppose M is f. g. and $\mathfrak{p} \in \operatorname{Spec} A$ contains $\mathrm{Ann}(M)$. Write $M = Ax_1 + \cdots + Ax_n$. If $M_{\mathfrak{p}} = 0$, we can find $a \in A \setminus \mathfrak{p}$ such that $ax_i = 0$ for $1 \leq i \leq n$. But then $aM = 0$, i.e., $a \in \mathrm{Ann}(M)$, which is a contradiction. □

(1.7) Theorem. *Suppose A is noetherian and M is finitely generated. Then there exists a chain $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ of submodules of M such that $M_i/M_{i-1} \simeq A/\mathfrak{p}_i$, for some $\mathfrak{p}_i \in \operatorname{Spec} A$ $(1 \leq i \leq n)$. Moreover, for any such chain of submodules, we have* $\mathrm{Ass}(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subseteq \operatorname{Supp}(M)$*; furthermore, the minimal elements of these three sets coincide.*

Proof: The case of $M = 0$ is trivial. If $M \neq 0$, then there exists $\mathfrak{p}_1 \in \operatorname{Spec} A$ such that $A/\mathfrak{p}_1$ is isomorphic to a submodule M_1 of M. If $M_1 \neq M$, we apply the same argument to M/M_1 to find $\mathfrak{p}_2 \in \operatorname{Spec} A$, and a submodule M_2 of M such that $M_2 \supseteq M_1$ and $A/\mathfrak{p}_2 \simeq M_2/M_1$. By (3.1), M has no strictly ascending chain of submodules, and therefore the above process must terminate. This yields the first assertion. Moreover, $\mathrm{Ass}(M_i/M_{i-1}) = \mathrm{Ass}(A/\mathfrak{p}_i) = \{\mathfrak{p}_i\}$, and so by (1.3), we see that $\mathrm{Ass}(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. Also, in view of (1.2) of [Gh], we have $(M_i/M_{i-1})_{\mathfrak{p}_i} \simeq A_{\mathfrak{p}_i}/\mathfrak{p}_i A_{\mathfrak{p}_i} \neq 0$. Hence $(M_i)_{\mathfrak{p}_i} \neq 0$. Thus $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subseteq \operatorname{Supp}(M)$. Lastly, if $\mathfrak{p} \in \operatorname{Supp}(M)$, then $M_{\mathfrak{p}} \neq 0$ and so $\mathrm{Ass}_{A_{\mathfrak{p}}}(M_{\mathfrak{p}}) \neq \emptyset$. Now (1.5) shows that there exists $\mathfrak{q} \in \mathrm{Ass}(M)$ with $\mathfrak{q} \cap (A \setminus \mathfrak{p}) = \emptyset$, i.e., $\mathfrak{q} \subseteq \mathfrak{p}$. This implies the last assertion. □

(1.8) Corollary. *If A is noetherian and M is* f. g., *then* $\mathrm{Ass}(M)$ *is finite. Furthermore, the minimal primes of M are precisely the minimal elements among the prime ideals of A containing* $\mathrm{Ann}(M)$.

Proof: Follows from (1.7) in view of (1.6). □

Remark: A chain $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ of submodules of M is sometimes called a *filtration* of M. Using a filtration as in (1.7), it is often possible to reduce questions about modules to questions about integral domains.

(1.9) Exercise: Show that if A is noetherian, M is f. g., and I is an ideal of A consisting only of zerodivisors of M, then there exists some $x \in M$ such that $x \neq 0$ and $Ix = 0$.

(1.10) Exercise: Show that if A is noetherian and M is f. g., then

$$\sqrt{\mathrm{Ann}(M)} = \bigcap_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \operatorname{Supp}(M)} \mathfrak{p} = \bigcap_{\substack{\mathfrak{p} \text{ a minimal} \\ \text{prime of } M}} \mathfrak{p}.$$

2. Primary Decomposition

We continue to let A denote a ring and M an A–module. As in the case of ideals, the primary decomposition of modules into primary submodules will be achieved using the auxiliary notion of irreducible submodules. To compare the notions and results discussed in this section to those in the classical case, you may substitute A for M.

Definition: Let Q be a submodule of M. We say that Q is *primary* if $Q \neq M$ and for any $a \in A$ and $x \in M$, we have

$$ax \in Q \text{ and } x \notin Q \Longrightarrow a^n M \subseteq Q \quad \text{for some } n \geq 1.$$

We say that Q is *irreducible* if $Q \neq M$ and for any submodules N_1 and N_2 of M we have

$$Q = N_1 \cap N_2 \Longrightarrow Q = N_1 \text{ or } Q = N_2.$$

Clearly, a submodule Q of M is primary iff every zerodivisor of M/Q is nilpotent for M/Q. [An element $a \in A$ is said to be *nilpotent* for M if $a^n M = 0$ for some $n \geq 1$. In other words, a is nilpotent for M iff $a \in \sqrt{\text{Ann}(M)}$.] If Q is a primary submodule of M and $\mathfrak{p} = \sqrt{\text{Ann}(M/Q)}$, we say that Q is $\mathfrak{p}$*–primary.*

(2.1) Exercise: Given any submodule Q of M, show that

$$\mathcal{Z}(M/Q) = \sqrt{\text{Ann}(M/Q)} \iff Q \text{ is primary } \Longrightarrow \text{Ann}(M/Q) \text{ is a primary ideal of } A$$

Use (1.2), (1.8) and (1.10) to deduce the following characterization.

$$\text{If } A \text{ is noetherian and } M \text{ is f. g., then: } Q \text{ is primary} \iff \text{Ass}(M/Q) \text{ is singleton.}$$

And also the following characterization.

$$\text{If } A \text{ is noetherian and } M \text{ is f. g., then: } Q \text{ is } \mathfrak{p}\text{–primary} \iff \text{Ass}(M/Q) = \{p\}.$$

As we shall see in the sequel, the above characterization of primary submodules [of f. g. modules over noetherian rings] is extremely useful. For this reason perhaps, it is sometimes taken as a definition of primary submodules [of arbitrary modules]. At any rate, we may tacitly use the above characterizations of primary and $\mathfrak{p}$–primary submodules in several of the proofs below.

(2.2) Lemma. *Suppose A is noetherian, M is f. g., and $Q_1, \ldots, Q_r$ are $\mathfrak{p}$–primary submodules of M, where r is a positive integer. Then $Q_1 \cap \cdots \cap Q_r$ is also $\mathfrak{p}$–primary.*

Proof: Clearly, $Q_1 \cap \cdots \cap Q_r \neq M$. Moreover, there is a natural injective homomorphism of $M/Q_1 \cap \cdots \cap Q_r$ into $M/Q_1 \oplus \cdots \oplus M/Q_r$. Therefore, in view of (1.1), (1.3) and (1.4), we see that

$$\emptyset \neq \text{Ass}(M/Q_1 \cap \cdots \cap Q_r) \subseteq \text{Ass}\left(\oplus_{i=1}^r M/Q_i\right) = \cup_{i=1}^r \text{Ass}(M/Q_i) = \{\mathfrak{p}\}.$$

Thus it follows from (2.1) that $Q_1 \cap \cdots \cap Q_r$ is $\mathfrak{p}$–primary. $\square$

(2.3) Lemma. *If M is noetherian, then every submodule of M is a finite intersection of irreducible submodules of M.*

Proof: Assume the contrary. Then we can find a maximal element, say Q, among the submodules of M which aren't finite intersections of irreducible submodules of M. Now Q can't be irreducible. Also $Q \neq M$ (because M is the intersection of the empty family of irreducible submodules of M). Hence $Q = N_1 \cap N_2$ for some submodules N_1 and N_2 of M with $N_1 \neq Q$ and $N_2 \neq Q$. By maximality of Q, both N_1 and N_2 are finite intersections of irreducible submodules of M. But then so is Q, which is a contradiction. $\square$

(2.4) Lemma. *Suppose A is noetherian, M is* f. g.*, and Q is an irreducible submodule of M. Then Q is primary.*

Proof: Since $Q \neq M$, $\operatorname{Ass}(M/Q) \neq \emptyset$. Suppose $\operatorname{Ass}(M/Q)$ contains two distinct prime ideals $\mathfrak{p}_1 = (0 : \bar{x}_1)$ and $\mathfrak{p}_2 = (0 : \bar{x}_2)$, where $\bar{x}_1, \bar{x}_2$ denote the images in M/Q of some elements x_1, x_2 of M. Clearly $\bar{x}_1$ and $\bar{x}_2$ are nonzero elements of M/Q. We claim that $A\bar{x}_1 \cap A\bar{x}_2 = \{0\}$ Indeed, if $a\bar{x}_1 = b\bar{x}_2$, with $a, b \in A$, is nonzero, then $a \notin (0 : \bar{x}_1)$ and $b \notin (0 : \bar{x}_2)$. Since $(0 : \bar{x}_1)$ is prime, we find that $(0 : \bar{x}_1) = (0 : a\bar{x}_1)$ (check!). Similarly, $(0 : \bar{x}_2) = (0 : b\bar{x}_2)$. This gives $\mathfrak{p}_1 = \mathfrak{p}_2$, which is a contradiction. Now if $y \in (Q + Ax_1) \cap (Q + Ax_2)$, then $y = y_1 + ax_1 = y_2 + bx_2$ for some $y_1, y_2 \in Q$ and $a, b \in A$. But then $a\bar{x}_1 = b\bar{x}_2$ in M/Q and thus $y \in Q$. It follows that $Q = (Q + Ax_1) \cap (Q + Ax_2)$. Also since $\bar{x}_1 \neq 0 \neq \bar{x}_2$, we have $(Q + Ax_1) \neq Q \neq (Q + Ax_2)$. This contradicts the irreducibility of Q. Thus $\operatorname{Ass}(M/Q)$ is singleton so that Q is primary. $\square$

(2.5) Lemma. *Suppose A is noetherian, M is* f. g.*, Q is a $\mathfrak{p}$–primary submodule of M. Then the inverse image of $Q_{\mathfrak{p}}$ under the natural map $M \to M_{\mathfrak{p}}$ (given by $x \mapsto \frac{x}{1}$) is Q.*

Proof: Suppose $x \in M$ is such that $\frac{x}{1} \in Q_{\mathfrak{p}}$. Then $tx \in Q$ for some $t \in A \setminus \mathfrak{p}$. If $x \notin Q$, then $\bar{x}$, the image of x in M/Q, is nonzero, and thus $t \in \mathcal{Z}(M/Q)$. Hence from (2.1), we see that $t \in \mathfrak{p}$, which is a contradiction. $\square$

(2.6) Remark: Given any $\mathfrak{p} \in \operatorname{Spec} A$ and a submodule Q' of $M_{\mathfrak{p}}$, the inverse image of Q' under the natural map $M \to M_{\mathfrak{p}}$ is often denoted by $Q' \cap M$. Thus (2.5) can be expressed by saying that if Q is a $\mathfrak{p}$–primary submodule of M, then $Q_{\mathfrak{p}} \cap M = Q$. Note that we have been tacitly using the fact that if Q is any submodule of M and S is any m. c. subset of A, then $S^{-1}Q$ can be regarded as a submodule of $S^{-1}M$.

(2.7) Theorem. *Suppose A is noetherian, M is* f. g.*, and N is any submodule of M. Then we have*

- (i) *There exist primary submodules $Q_1, \dots, Q_h$ of M such that $N = Q_1 \cap \cdots \cap Q_h$.*
- (ii) *In* (i) *above, $Q_1, \dots, Q_h$ can be chosen such that $Q_i \not\supseteq \cap_{j \neq i} Q_j$ for $1 \leq i \leq h$, and $\mathfrak{p}_1, \dots, \mathfrak{p}_h$ are distinct, where $\mathfrak{p}_i = \sqrt{\operatorname{Ann}(M/Q_i)}$.*
- (iii) *If Q_i and $\mathfrak{p}_i$ are as in* (ii) *above, then $\mathfrak{p}_1, \dots, \mathfrak{p}_h$ are unique; in fact, $\{\mathfrak{p}_1, \dots, \mathfrak{p}_h\} = \operatorname{Ass}(M/N)$. Moreover, if $\mathfrak{p}_i$ is minimal among $\mathfrak{p}_1, \dots, \mathfrak{p}_h$, i.e. $\mathfrak{p}_i \not\supseteq \mathfrak{p}_j$ for $j \neq i$, then the corresponding primary submodule Q_i is also unique; in fact, $Q_i = N_{\mathfrak{p}_i} \cap M$.*

Proof: Clearly, (i) is a direct consequence of (2.3) and (2.4). Given a decomposition as in (i), we can use (2.2) to reduce it by grouping together the primary submodules having the same associated prime so as to ensure that the associated primes become distinct. Then we can successively remove the primary submodules contained in the intersections of the remaining submodules. This yields (ii). Now let $Q_1, \dots, Q_h$ be as in (ii). Fix some i with $1 \le i \le h$. Let $P_i = \cap_{j \ne i} Q_i$. Clearly, $N \subset P_i$ and $N \ne P_i$. Thus we have $0 \ne P_i/N = P_i/P_i \cap Q_i \simeq P_i + Q_i/Q_i \hookrightarrow M/Q_i$, and hence, in view of (1.1) and (1.3), we find that $\emptyset \ne \operatorname{Ass}(P_i/N) \subseteq \operatorname{Ass}(M/Q_i) = \{\mathfrak{p}_i\}$. Thus $\{\mathfrak{p}_i\} = \operatorname{Ass}(P_i/N) \subseteq \operatorname{Ass}(M/N)$. On the other hand, since $N = Q_1 \cap \dots \cap Q_h$, M/N is isomorphic to a submodule of $\oplus_{j=1}^h M/Q_j$, and so by (1.4), $\operatorname{Ass}(M/N) \subseteq \cup_{j=1}^h \operatorname{Ass}(M/Q_j) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_h\}$. This proves that $\operatorname{Ass}(M/N) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_h\}$. In particular, $\mathfrak{p}_1, \dots, \mathfrak{p}_h$ are unique. Now suppose, without loss of generality, that $\mathfrak{p}_1$ is minimal among $\mathfrak{p}_1, \dots, \mathfrak{p}_h$. Then for $j > 1$, $\mathfrak{p}_1 \not\supseteq \mathfrak{p}_j$, i.e., $(A \setminus \mathfrak{p}_1) \cap \mathfrak{p}_j \ne \emptyset$, and hence by (1.5), we find that $\operatorname{Ass}_{A_{\mathfrak{p}_1}}((M/Q_j)_{\mathfrak{p}_1}) = \emptyset$; thus by (1.3), $(M/Q_j)_{\mathfrak{p}_1} = 0$, i.e., $M_{\mathfrak{p}_1} = (Q_j)_{\mathfrak{p}_1}$. It follows that $N_{\mathfrak{p}_1} = (Q_1)_{\mathfrak{p}_1} \cap \dots \cap (Q_h)_{\mathfrak{p}_1} = (Q_1)_{\mathfrak{p}_1}$, and, in view of (2.5) and (2.6), we obtain that $Q_1 = (Q_1)_{\mathfrak{p}_1} \cap M = N_{\mathfrak{p}_1} \cap M$. This proves (iii). □

Definition: A decomposition $N = Q_1 \cap \dots \cap Q_h$, as in (i) above is called a *primary decomposition* of N. If $Q_1, \dots, Q_h$ satisfy the conditions in (ii), then it is called an *irredundant (primary) decomposition* of N.

Example: Let G be a finite abelian group of order n. Let the notation be as in the Example preceding (1.5). For $1 \le i \le h$, let $Q_i = P_1 + \dots + P_{i-1} + P_{i+1} + \dots + P_h$. Then $G/Q_i \simeq P_i$, and thus Q_i is $p_i\mathbb{Z}$–primary. Observe that $(0) = Q_1 \cap \dots \cap Q_h$ is an irredundant primary decomposition of (0); in fact, this decomposition is unique because each of the associated primes $p_1\mathbb{Z}, \dots, p_h\mathbb{Z}$ is clearly minimal. In general, if N is a subgroup, i.e., a $\mathbb{Z}$–submodule, of G, and $\Lambda = \{i : 1 \le i \le h \text{ and } N + Q_i \ne G\}$, then $N = \cap_{i \in \Lambda}(N + Q_i)$ is an irredundant primary decomposition of N, and this too is unique. Verify!

It may be remarked that the examples of primary ideals, primary decomposition of ideals, etc., discussed in the last chapter, constitute examples in this general set–up as well. Thus the pathologies which arise in the case of ideals [see, for instance, the Remark and the Example preceding (2.3) of Ch. 1] continue to exist for f. g. modules over noetherian rings.

3. Graded Rings and Modules

In this section, we shall study some basic facts about graded rings and modules. This will allow us to discuss, in the next section, some special properties of associated primes and primary decomposition in the graded situation.

The prototype of a graded ring is the polynomial ring $A[X_1, \dots, X_n]$ over a ring A. Before giving the general definition, we point out that the set of all nonnegative integers is denoted by $\mathbb{N}$.

Definition: A ring R is said to be $\mathbb{N}$–*graded*, or simply *graded*, if it has additive subgroups R_d, for $d \in \mathbb{N}$, such that $R = \oplus_{d \in \mathbb{N}} R_d$ and $R_d R_e \subseteq R_{d+e}$, for all $d, e \in \mathbb{N}$. The family $\{R_d\}_{d \in \mathbb{N}}$ is called an $\mathbb{N}$–*grading* of R, and the subgroup R_d is called the d^{th} *graded component* of R.

Let $R = \oplus_{d \in \mathbb{N}} R_d$ be a graded ring. Elements of R_d are said to be *homogeneous* of degree d. Every $a \in R$ can be uniquely written as $a = \sum_{d \in \mathbb{N}} a_d$ with $a_d \in R_d$ such that all except finitely many a_d's are 0; we call a_d's to be the *homogeneous components* of a. Given a homogeneous element $b \in R$, we sometimes write $\deg(b)$ to denote its degree. An ideal of R generated by homogeneous elements is called a *homogeneous ideal*. Note that an ideal is homogeneous iff it contains the homogeneous components of each of its elements. If I is a homogeneous ideal of R, then R/I has the induced $\mathbb{N}$–grading given by $(R/I)_d = R_d/(I \cap R_d)$. A subring S of R is said to be *graded* if $S = \oplus_{d\in\mathbb{N}}(S \cap R_d)$. Note that R_0 is a graded subring of R and each R_d is an R_0–module. If $R' = \oplus_{d\in\mathbb{N}} R'_d$ is any graded ring, then a homomorphism $\phi : R \to R'$ is called a *graded ring homomorphism*, or a *homomorphism of graded rings*, if $\phi(R_d) \subseteq R'_d$ for all $d \in \mathbb{N}$; note that in this case the kernel of ϕ is a homogeneous ideal of R and the image of ϕ is a graded subring of R'.

Examples: 1. Let A be a ring and I be a homogeneous ideal of $A[X_1, \ldots, X_n]$. Then $R = A[X_1, \ldots, X_n]/I$ is a graded ring, with its d^{th} graded component being given by $R_d = A[X_1, \ldots, X_n]_d/I_d$, where $I_d = I \cap A[X_1, \ldots, X_n]_d$. Note that in this case R as well as R_d are f. g. A–algebras, and in particular, A–modules. Graded rings of this type are usually called *graded A–algebras*.

2. Let A be a ring and I be any ideal of A such that $I \neq A$. Then $\mathrm{gr}_I(A) \stackrel{\text{def}}{=} \oplus_{d\in\mathbb{N}} I^d/I^{d+1}$ is a graded ring. It is called the *associated graded ring* of A w.r.t. I.

(3.1) Exercise: Let $R = \oplus_{d\in\mathbb{N}} R_d$ be a graded ring, and I, J be homogeneous ideals of R. Then show that $I + J$, IJ, $I \cap J$, $(I : J)$ and $\sqrt{I}$ are homogeneous ideals.

(3.2) Exercise: Let $R = \oplus_{d\in\mathbb{N}} R_d$ be a graded ring, and I be a homogeneous ideal of R. Show that I is prime iff I is prime in the graded sense, that is, $I \neq R$ and

$$a, b \text{ homogeneous elements of } R \text{ and } ab \in I \Rightarrow a \in I \text{ or } b \in I.$$

Given an ideal I of a graded ring $R = \oplus_{d\in\mathbb{N}} R_d$, we shall denote by I^* the largest homogeneous ideal contained in I. Note that I^* is precisely the ideal generated by the homogeneous elements in I.

(3.3) Lemma. *If $R = \oplus_{d\in\mathbb{N}} R_d$ is a graded ring and $\mathfrak{p}$ is a prime ideal of R, then $\mathfrak{p}^*$ is a prime ideal of R.*

Proof: Follows from (3.2). $\square$

(3.4) Lemma. *Let $R = \oplus_{d\in\mathbb{N}} R_d$ be a graded ring. Then $1 \in R_0$.*

Proof: Write $1 = \sum_{d\in\mathbb{N}} a_d$ with $a_d \in R_d$. Then for any $b \in R_e$, $b = \sum_{d\in\mathbb{N}} ba_d$. Equating the degree e components, we find $b = ba_0$. This implies that $ca_0 = 1$ for all $c \in R$. Hence $1 = a_0 \in R_0$. $\square$

Given a graded ring $R = \oplus_{d\in\mathbb{N}} R_d$, we define $R_+ = \oplus_{d>0} R_d$. Note that R_+ is a homogeneous ideal of R and $R/R_+ \simeq R_0$. Thus if R_0 is a field, then R_+ is a *homogeneous maximal ideal* of R; moreover, R_+ is also maximal among all homogeneous ideals of R other than R, and so it is the *maximal homogeneous ideal* of R.

(3.5) Lemma. *Let $R = \oplus_{d\in\mathbb{N}} R_d$ be a graded ring and $x_1, \ldots, x_n$ be any homogeneous elements of positive degree in R. Then $R_+ = (x_1, \ldots, x_n)$ iff $R = R_0[x_1, \ldots, x_n]$. In particular, R is noetherian iff R_0 is noetherian and R is a* f. g. *R_0–algebra.*

Proof: Suppose $R_+ = (x_1, \ldots, x_n)$. We show by induction on d that each $x \in R_d$ is in $R_0[x_1, \ldots, x_n]$. The case of $d = 0$ is clear. Suppose $d > 0$. Write $x = a_1x_1 + \cdots + a_nx_n$, where $a_1, \ldots, a_n \in R$. Since x is homogeneous, we may assume, without loss of generality, that each a_i is homogeneous. Then for $1 \leq i \leq n$, we must have $\deg(a_i) = d - \deg(x_i) < d$, and so, by induction hypothesis, $a_i \in R_0[x_1, \ldots, x_n]$. It follows that $R = R_0[x_1, \ldots, x_n]$. Conversely, if $R = R_0[x_1, \ldots, x_n]$, then it is evident that $R_+ = (x_1, \ldots, x_n)$. The second assertion in the Lemma follows from the first one by noting that f. g. algebras over noetherian rings are noetherian. $\square$

(3.6) Exercise: Let $R = \oplus_{d\in\mathbb{N}} R_d$ be a graded ring. Show that R is noetherian iff it satisfies a.c.c. on homogeneous ideals.

(3.7) Exercise: Let A be a ring and $I = (a_1, \ldots, a_r)$. If $\bar{a}_1, \ldots, \bar{a}_r$ denote the images of $a_1, \ldots, a_r$ mod I^2, then show that $\mathrm{gr}_I(A) = (A/I)[\bar{a}_1, \ldots, \bar{a}_r] \simeq (A/I)[X_1, \ldots, X_r]/J$, for some homogeneous ideal J of $(A/I)[X_1, \ldots, X_r]$. Deduce that if (A/I) is noetherian and I is f. g., then $\mathrm{gr}_I(A)$ is noetherian.

(3.8) Graded Noether Normalisation Lemma. *Let k be an infinite field and $R = k[x_1, \ldots, x_n]$ be a graded k–algebra such that $R_0 = k$ and $\deg(x_i) = m$ for $1 \leq i \leq n$. Then there exist homogeneous elements $\theta_1, \ldots, \theta_d$ of degree m in R such that $\theta_1, \ldots, \theta_d$ are algebraically independent over k and R is integral over the graded subring $k[\theta_1, \ldots, \theta_d]$. In particular, R is a finite $k[\theta_1, \ldots, \theta_d]$–module.*

Proof: If k is an infinite field, then in (4.13) of [Gh], the elements $\theta_1, \ldots, \theta_d$ can be chosen to be k–linear combinations of $x_1, \ldots, x_n$. The result follows. $\square$

Now let us turn to modules.

Definition: Let $R = \oplus_{d\in\mathbb{N}} R_d$ be a graded ring, and M be an R–module. Then M is said to be $\mathbb{N}$–*graded* or simply, *graded*, if it contains additive subgroups M_d, for $d \in \mathbb{N}$, such that $M = \oplus_{d\in\mathbb{N}} M_d$, and $R_d M_e \subseteq M_{d+e}$, for all $d, e \in \mathbb{N}$. Such a family $\{M_d\}_{d\in\mathbb{N}}$ is called an $\mathbb{N}$–*grading* of M, and M_d the d^{th} *graded component* of M.

Let $R = \oplus_{d\in\mathbb{N}} R_d$ be a graded ring and $M = \oplus_{d\in\mathbb{N}} M_d$ be a graded R–module. By a *graded submodule* of M we mean a submodule N of M such that $N = \oplus_{d\in\mathbb{N}}(N \cap M_d)$. Note that if N is a graded submodule of M, then M/N is a graded R–module with the induced grading given by $(M/N)_d = M_d/(N \cap M_d)$. If $M' = \oplus_{d\in\mathbb{N}} M'_d$ is any graded R–module, then by *graded module homomorphism*, or a *homomorphism of graded modules*, we mean a R–module homomorphism $\phi : M \to M'$ such that $\phi(M_d) \subseteq M'_d$, for all $d \in \mathbb{N}$. For any such ϕ, the kernel of ϕ and the image of ϕ are graded submodules of M and M' respectively.

Examples: 1. Let $R = A[X_1, \ldots, X_n]$ and I be a homogeneous ideal of R. Then $M = R/I$ is a graded R–module. In this example, the graded components M_d are finite A–modules.

2. Let A be a ring and I be an ideal of A. If M is any A–module, then $\mathrm{gr}_I(M) = \oplus_{d\in\mathbb{N}} I^d M/I^{d+1}M$ is a graded $\mathrm{gr}_I(A)$–module. It is called the *associated graded module* of M w.r.t. I.

(3.9) Exercise: Let the notation be as in (3.7). Let M be an A–module. Suppose $M = Ax_1 + \cdots + Ax_m$, and $\bar{x}_1, \ldots, \bar{x}_m$ denote the images of $x_1, \ldots, x_m$ in M/IM, then show that $\operatorname{gr}_I(M) = \operatorname{gr}_I(A)\bar{x}_1 + \cdots + \operatorname{gr}_I(A)\bar{x}_m$. Deduce that if A is noetherian and M is f. g., then $\operatorname{gr}_I(M)$ is a noetherian $\operatorname{gr}_I(A)$–module.

(3.10) Graded Nakayama's Lemma. *Let $R = \oplus_{d\in\mathbb{N}} R_d$ be a graded ring and $M = \oplus_{d\in\mathbb{N}} M_d$ be a graded R–module. If $R_+M = M$, then $M = 0$.*

Proof: If $M \neq 0$, we can find a nonzero element x of least degree in M. Now the assumption $x \in R_+M$ leads to a contradiction. □

(3.11) Artin-Rees Lemma. *Let A be a noetherian ring, I an ideal of A and M a f.g. A-module. Suppose $M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$ is a chain of submodules of M such that $IM_n \subseteq M_{n+1}$ for all $n \geq 0$ with equality for $n \geq r$ (for some r). Then for any submodule M' of M, there exists $s \geq 0$ such that $IM'_n = M'_{n+1}$ for all $n \geq s$, where M'_i denotes $M' \cap M_i$.*

Proof: Let t be an indeterminate over A and let R be the subring of $A[t]$ defined by $R = \oplus_{n\geq 0} I^n t^n = A \oplus It \oplus I^2t^2 \oplus \cdots$. If $I = (a_1, \ldots, a_m)$, then $R = A[a_1t, \ldots, a_mt]$ and so R is a f.g. graded A-algebra [called the *Rees algebra* of I]. Thus by (3.5), R is noetherian. Moreover, $L = \oplus_{n\geq 0} M_n t^n$ is naturally a graded R-module. Now clearly $IM'_n \subseteq M' \cap IM_n \subseteq M'_{n+1}$, and hence $L' = \oplus_{n\geq 0} M'_n t^n$ is an R-submodule of L. By (3.1) of [Gh], each M_n is a f.g. A-module, and hence so is $\widetilde{M_n} = M_0 \oplus M_1 t \oplus \cdots \oplus M_n t^n$. Consequently, the R-module $\tilde{L}_n = M_0 \oplus M_1 t \oplus \cdots \oplus M_n t^n \oplus IM_n t^{n+1} \oplus I^2 M_n t^{n+2} \oplus \cdots$, generated by $\widetilde{M_n}$, is f.g. Since $IM_n = M_{n+1}$ for $n \geq r$, it follows that $L = \tilde{L}_n$ for $n \geq r$, and so L is a noetherian R-module. Hence the chain $\tilde{L}'_0 \subseteq \tilde{L}'_1 \subseteq \tilde{L}'_2 \subseteq \cdots$ of R-submodules of L terminates, i.e., there exists $s \geq 0$ such that $\tilde{L}'_n = \tilde{L}'_s$ for $n \geq s$. It follows that $IM'_n = M'_{n+1}$ for $n \geq s$. □

Remark: By taking $M'_n = I^n M$ in (3.11), we get $M' \cap I^n M = I^n \left(M' \cap I^{n-s} M\right)$ for $n \geq s$. This, or the particular case when $M = A$ and $M' = J$, an ideal of A, is often the version of Artin-Rees Lemma used in practise. For example, putting $M' = \cap_{n\geq 0} I^n M$ and using Nakayama's Lemma, we get a proof of Krull's Intersection Theorem [viz., (3.3) of Ch. 1]. Artin-Rees Lemma is most useful in the theory of completions. For more on completions, which may be regarded as the fourth fundamental process, one may refer to [AM, Ch. 10].

Sometimes, it is useful to consider gradings which are more general than $\mathbb{N}$–grading.

Definition: Let R be a ring and s be a positive integer. By a $\mathbb{Z}^s$*–grading* on R we mean a family $\{R_\alpha\}_{\alpha\in\mathbb{Z}^s}$ of additive subgroups of R such that $R = \oplus_{\alpha\in\mathbb{Z}^s} R_\alpha$ and $R_\alpha R_\beta \subseteq R_{\alpha+\beta}$, for all $\alpha, \beta \in \mathbb{Z}^s$. Elements of R_α are said to be *homogeneous* of degree α. A ring with a $\mathbb{Z}^s$–grading is called a $\mathbb{Z}^s$*–graded ring.*

The definitions of graded subring, homogeneous ideal, graded ring homomorphism, in the context of $\mathbb{Z}^s$–graded rings, are exactly similar to those in the case of $\mathbb{N}$–graded rings. If $R = \oplus_{\alpha\in\mathbb{Z}^s} R_\alpha$ is a $\mathbb{Z}^s$–graded rings, and M is an R-module, then M is said to be $\mathbb{Z}^s$*–graded* if it contains additive subgroups M_α, for $\alpha \in \mathbb{Z}^s$, such that $M = \oplus_{\alpha\in\mathbb{Z}^s} M_\alpha$ and $R_\alpha M_\beta \subseteq M_{\alpha+\beta}$, for all $\alpha, \beta \in \mathbb{Z}^s$. Corresponding notions of homogeneous element, graded submodule, and graded module isomorphism, etc. are defined in a similar fashion.

If $\{R_\alpha\}_{\alpha\in\mathbb{Z}^s}$ is a $\mathbb{Z}^s$–grading on a ring R such that $R_\alpha = 0$ for all $\alpha = (\alpha_1, \ldots, \alpha_s) \in \mathbb{Z}^s$ with $\alpha_i < 0$ for some i, then it is called an $\mathbb{N}^s$*–grading*; note that in this case $R = \oplus_{\alpha\in\mathbb{N}^s} R_\alpha$. Similarly, one has the notion of $\mathbb{N}^s$–gradings for modules.

Examples: 1. Let A be a ring and $R = A[X_1, \ldots, X_n]$. Then R has a $\mathbb{Z}^n$–grading $\{R_\alpha\}_{\alpha\in\mathbb{Z}^s}$ given by $R_\alpha = A\,X^\alpha$, where for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$, X^α denotes the monomial $X_1^{\alpha_1}\cdots X_n^{\alpha_n}$ if $\alpha \in \mathbb{N}^s$ and $X^\alpha = 0$ if $\alpha \notin \mathbb{N}^s$. Note that if $A = k$, a field, then the homogeneous ideals of R, w.r.t. the above grading, are precisely the monomial ideals of $k[X_1, \ldots, X_n]$.

2. Let A be a ring and $R = A[X_1, \ldots, X_n]$. Let $d_1, \ldots, d_n$ be any integers. For $d \in \mathbb{Z}$, let R_d be the A–submodule of R generated by the monomials $X_1^{\alpha_1}\cdots X_n^{\alpha_n}$ for which $d_1\alpha_1 + \cdots + d_n\alpha_n = d$. Then $\{R_d\}_{d\in\mathbb{Z}}$ defines a $\mathbb{Z}$–grading on R which is an $\mathbb{N}$–grading iff $d_i = \deg(X_i) \geq 0$ for $1 \leq i \leq n$. The corresponding homogeneous polynomials and homogeneous ideals are sometimes called *weighted homogeneous polynomials* and *weighted homogeneous ideals* respectively.

The notion of $\mathbb{Z}$–gradings permits us to define the following simple but useful operation on graded rings. If $R = \oplus_{d\in\mathbb{N}} R_d$ is a graded ring and m is any integer, then we define $R(m)$ to be the graded R–module obtained from R by *shifting*, or by *twisting*, the grading by m, i.e., $R(m)_d = R_{m+d}$ for $d \in \mathbb{Z}$ and $R(m) = \oplus_{d\in\mathbb{Z}} R(m)_d$. Further, if $M = \oplus_{d\in\mathbb{N}} M_d$ is a graded R–module, then we define $M(m) = \oplus_{d\in\mathbb{Z}} M(m)_d$, where $M(m)_d = M_{m+d}$. Note that $M(m)$ is a graded R–module.

Remark: Most of the results proved earlier in this section extend to $\mathbb{Z}^s$–graded rings and $\mathbb{Z}^s$–graded modules over them. The notion of grading can also be extended by replacing $\mathbb{Z}^s$ by a monoid; most results extend to this case as well provided the monoid is assumed to be torsionfree. See [B] or [N] for more on this.

4. Primary Decomposition in Graded Modules

Throughout this section, $R = \oplus_{d\in\mathbb{N}} R_d$ denotes a graded ring and $M = \oplus_{d\in\mathbb{N}} M_d$ a graded R–module. Given a submodule N of M, by N^* we denote the largest graded submodule of N, i.e., N^* is the submodule generated by the homogeneous elements in N.

(4.1) Lemma. *Every associated prime of M is a homogeneous prime ideal and the annihilator of some homogeneous element of M.*

Proof: Suppose $\mathfrak{p} \in \operatorname{Ass}(M)$ and $\mathfrak{p} = (0 : x)$ for some $x \in M$. Then $x \neq 0$, and we can write $x = x_e + x_{e+1} + \cdots + x_d$ with $x_j \in M_j$ and $x_e \neq 0$. Now for any $a \in \mathfrak{p}$ with $a = a_r + a_{r+1} + \cdots + a_s$ and $a_i \in R_i$, the equation $ax = 0$ yields the equations

$$a_r x_e = 0,\ a_r x_{e+1} + a_{r+1} x_e = 0,\ a_r x_{e+2} + a_{r+1} x_{e+1} + a_{r+2} x_e = 0, \ldots$$

which imply that $a_r x_e = a_r^2 x_{e+1} = a_r^3 x_{e+2} = \cdots = a_r^{d-e+1} x_d = 0$. Hence $a_r^{d-e+1} x = 0$, i.e., $a_r \in \sqrt{(0 : x)}$. Since $\mathfrak{p} = (0 : x)$ is prime, we have $a_r \in \mathfrak{p}$. Now $(a - a_r)x = 0$ and using arguments similar to those above, we find that $a_{r+1} \in \mathfrak{p}$. Proceeding in this manner, we see that $a_i \in \mathfrak{p}$ for $r \leq i \leq s$. This proves that $\mathfrak{p}$ is homogeneous. Moreover, if we let $I_j = (0 : x_j)$, then we have $\mathfrak{p} \subseteq I_j$ for $e \leq j \leq d$ and $\cap_{j=e}^{d} I_j \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is prime, we have $I_j \subseteq \mathfrak{p}$ for some j and thus $\mathfrak{p} = (0 : x_j)$. $\square$

(4.2) Corollary. *Given any $\mathfrak{p} \in \mathrm{Ass}(M)$, there exists an integer m and a graded ring isomorphism of $(R/\mathfrak{p})(-m)$ onto a graded submodule of M.*

Proof: Write $\mathfrak{p} = (0 : x)$ for some homogeneous element x of M. Let $m = \deg(x)$. The map $a \mapsto ax$ of $R \to M$ is a homomorphism with $\mathfrak{p}$ as its kernel and it maps R_d into M_{m+d}. Hence it induces a desired graded ring isomorphism of $(R/\mathfrak{p})(-m)$. □

(4.3) Exercise: Show that if $\mathfrak{p} \in \mathrm{Supp}\,(M)$, then $\mathfrak{p}^* \in \mathrm{Supp}\,(M)$.

(4.4) Theorem. *If R is noetherian and M is* f. g., *then there exists a chain $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ of graded submodules of M, homogeneous prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of R and integers $m_1, \ldots, m_n$ such that $M_i/M_{i-1} \simeq (R/\mathfrak{p}_i)(-m_i)$, the isomorphism being that of graded modules.*

Proof: Similar to the proof of (1.7) in view of (4.1) and (4.2) above. □

Now let us turn to primary submodules of M.

(4.5) Lemma. *Let N be a graded submodule of M such that $N \neq M$ and for any homogeneous elements $b \in R$ and $y \in N$ we have*

$$by \in N \text{ and } y \notin N \Longrightarrow b^n M \subseteq N \text{ for some } n \geq 1.$$

Then N is a primary submodule of M.

Proof: Let $a \in R$ and $x \in M$ be any elements such that $ax \in N$ and $x \notin N$. Then we can write $x = x' + x_e + x_{e+1} + \cdots + x_d$ with $x' \in N$, $x_j \in M_j$ and $x_e \notin N$. Let $a = a_r + a_{r+1} + \cdots + a_s$ where $a_i \in R_i$. Now $a(x_e + x_{e+1} + \cdots + x_d) \in N$, and since N is graded, we find that $a_r x_e \in N$. By assumption, there exists $n_1 \geq 1$ with $a_r^{n_1} M \subseteq N$. Now $(a - a_r)^{n_1}(x_e + x_{e+1} + \cdots + x_d) \in N$, and hence there exists $n_2 \geq 1$ with $a_{r+1}^{n_1 n_2} M \subseteq N$. Proceeding in this manner, we can find $n_0 \geq 1$ such that $a_i^{n_0} M \subseteq N$ for $r \leq i \leq s$. Therefore, we can find $n \geq 1$ [e.g., $n = n_0(s-r+1)$] such that $a^n M \subseteq N$. Thus N is primary. □

(4.6) Lemma. *If Q is a $\mathfrak{p}$–primary submodule of M, then Q^* is $\mathfrak{p}^*$–primary.*

Proof: Since the homogeneous elements of Q (resp: $\mathfrak{p}$) are elements of Q^* (resp: $\mathfrak{p}^*$), it follows from (4.5) that Q^* is a primary submodule. Further, if a is any homogeneous element of $\mathfrak{p} = \sqrt{\mathrm{Ann}(M/Q)}$, then $a^n M \subseteq Q$ for some $n \geq 1$, and since M is graded, $a^n M \subseteq Q^*$. It follows that $\mathfrak{p}^* \subseteq \sqrt{\mathrm{Ann}(M/Q^*)}$. On the other hand, since M/Q^* is graded and $\mathrm{Ann}(M/Q^*) \subseteq \mathrm{Ann}(M/Q)$, we see that $\sqrt{\mathrm{Ann}(M/Q^*)}$ is a homogeneous ideal contained in $\mathfrak{p}$, and hence $\sqrt{\mathrm{Ann}(M/Q^*)} \subseteq \mathfrak{p}^*$. Thus Q^* is $\mathfrak{p}^*$–primary. □

(4.7) Theorem. *Suppose A is noetherian, M is* f. g., *and N is a graded submodule of M. Let $N = Q_1 \cap \cdots \cap Q_h$ be a primary decomposition of N, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_h$ be the associated primes corresponding to $Q_1, \ldots, Q_h$, respectively. Then we have*

(i) $\mathfrak{p}_i = \mathfrak{p}_i^*$, *$Q_i^*$ is $\mathfrak{p}_i$–primary for $1 \leq i \leq h$ and $N = Q_1^* \cap \cdots \cap Q_h^*$.*
(ii) *If the primary decomposition $N = Q_1 \cap \cdots \cap Q_h$ is irredundant, then so is the primary decomposition $N = Q_1^* \cap \cdots \cap Q_h^*$.*

(iii) *If $\mathfrak{p}_i$ is minimal among $\mathfrak{p}_1, \dots, \mathfrak{p}_h$, then Q_i is a graded submodule of N.*

Proof: Applying (4.1) to M/N, we get $\mathfrak{p}_i = \mathfrak{p}_i^*$. So by (4.6), we find that Q_i^* is $\mathfrak{p}_i$–primary. Since N is graded and $N \subseteq Q_i$, we have $N \subseteq Q_i^*$. Thus $N \subseteq Q_1^* \cap \cdots \cap Q_h^* \subseteq Q_1 \cap \cdots \cap Q_h = N$, which proves (i). If $N = Q_1 \cap \cdots \cap Q_h$ is an irredundant primary decomposition, then $\mathfrak{p}_1, \dots, \mathfrak{p}_h$ are distinct, and $\mathrm{Ass}(M/N) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_h\}$. Thus the associated primes corresponding to $Q_1^*, \dots, Q_h^*$ are distinct. Moreover, if the decomposition $N = Q_1^* \cap \cdots \cap Q_h^*$ can be shortened, then $\mathrm{Ass}(M/N)$ would have less than h elements, which is a contradiction. This proves (ii). Finally, if $\mathfrak{p}_i$ is minimal among $\mathfrak{p}_1, \dots, \mathfrak{p}_h$, then the corresponding primary component Q_i is unique. Hence from (i), we obtain $Q_i = Q_i^*$, i.e., Q_i is graded. $\square$

Remark: As a special case of the results of this section, we obtain some useful results about ideals in graded rings. You may find it instructive to write these down explicitly.

(4.8) Exercise: Show that all the results of this section remain valid if R is replaced by a $\mathbb{Z}^s$–graded ring and M by a $\mathbb{Z}^s$–graded module over it. Deduce from this that if I is a monomial ideal in $k[X_1, \dots, X_n]$, then the associated primes of I are monomial ideals and that I has a primary decomposition such that each of the primary ideals occurring in it is a monomial ideal.

The following exercise indicates a constructive method to obtain primary decompositions of monomial ideals.

(4.9) Exercise: Let J be a monomial ideal of $k[X_1, \dots, X_n]$ and u, v be relatively prime monomials in $k[X_1, \dots, X_n]$. Show that $(J, uv) = (J, u) \cap (J, v)$. Also show that if $e_1, \dots, e_n$ are positive integers, then the ideal $(X_1^{e_1}, \dots, X_n^{e_n})$ is $(X_1, \dots, X_n)$–primary. Use these facts to determine the associated primes and a primary decomposition of the ideal $I = (X^2YZ, Y^2Z, YZ^3)$ of $k[X, Y, Z]$.

References

[Ab] S. S. Abhyankar, *Algebraic Geometry for Scientists and Engineers*, American Math. Society, 1990.
[AM] M. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison–Wesley, 1969.
[Bo] N. Bourbaki, *Commutative Algebra*, Hermann, 1972.
[BH] W. Bruns and J. Herzog, *Cohen-Macaulay Rings*, Cambridge University Press, 1993.
[Ei] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer–Verlag, 1995.
[Gh] S. R. Ghorpade, *A Quick Review of Commutative Algebra*, Unpublished lecture notes, 2000.
[Ka] I. Kaplansky, *Commutative Rings*, The University of Chicago Press, 1974.
[KS] A. I. Kostrikin and I. R. Shafarevich (Eds), *Algebra I : Basic Notions of Algebra*, Springer–Verlag, 1990.
[Ku] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, 1985.
[M1] H. Matsumura, *Commutative Algebra*, Benjamin, 1970.
[M2] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, 1986.
[N1] D. G. Northcott, *Ideal Theory*, Cambridge University Press, 1953.
[N2] D. G. Northcott, *Lessons on Rings, Modules and Multiplicities*, Cambridge University Press, 1968.
[Sh] R. Y. Sharp, *Steps in Commutative Algebra*, Cambridge University Press, 1990.
[Ta] D. E. Taylor, From rainbows to rings: a history of the idea of the spectrum, in: *Fourier techniques and applications* (Kensington, 1983), pp. 221-224, Plenum Press, 1985.
[ZS] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. 1, Van Nostrand, 1958.