Introduction to Commutative Algebra

M. F. ATIYAH   I. G. MACDONALD

January 1, 1980

Contents

Introduction

Commutative algebra is essentially the study of commutative rings. Roughly speaking, it has developed from two sources: (1) algebraic geometry and (2) algebraic number theory. In (1) the prototype of the rings studied is the ring $k[x_1, \cdots, x_n]$ of polynomials in several variables over a field k; in (2) it is the ring $\mathbf{Z}$ of rational integers. Of these two the algebro-geometric case is the more far-reaching and, in its modern development by Grothendieck, it embraces much of algebraic number theory. Commutative algebra is now one of the foundation stones of this new algebraic geometry. It provides the complete local tools for the subject in much the same way as differential analysis provides the tools for differential geometry.

This book grew out of a course of lectures given to third year under- graduates at Oxford University and it has the modest aim of providing a rapid introduction to the subject. It is designed to be read by students who have had a first elementary course in general algebra. On the other hand, it is not intended as a substitute for the more voluminous tracts on commutative algebra such as Zariski-Samuel [4] or Bourbaki [1]. We have concentrated on certain central topics, and large areas, such as field theory, are not touched. In content we cover rather more ground than Northcott [3] and our treatment is substantially different in that, following the modern trend, we put more emphasis on modules and localization.

The central notion in commutative algebra is that of a prime ideal. This provides a common generalization of the primes of arithmetic and the points of geometry. The geometric notion of concentrating attention "near a point" has as its algebraic analogue the important process of localizing a ring at a prime ideal. It is not surprising, therefore, that results about localization can usefully be thought of in geometric terms. This is done methodically in Grothendieck's theory of schemes and, partly as an introduction to Grothendieck's work [2], and partly because of the geometric insight it provides, we have added schematic versions of many results in the form of exercises and remarks.

The lecture-note origin of this book accounts for the rather terse style with little general padding, and for the condensed account of many proofs. We have resisted the temptation to expand it in the hope that the brevity of our presentation will make clearer the mathematical structure of what is by now an elegant and attractive theory. Our philosophy has been to build up to the main theorems in a succession of simple steps and to omit routine verifications.

Anyone writing now on commutative algebra faces a dilemma in connection with homological algebra, which plays such an important part in modern developments. A proper treatment of homological algebra is impossible within the confines of a small book: on the other hand, it is hardly sensible to ignore it completely. The compromise we have adopted is to use elementary homological methods-exact sequences, diagrams, etc.-but to stop short of any results requiring a deep study of homology. In this way we hope to prepare the ground for a systematic course on homological algebra which the reader should undertake if he wishes to pursue algebraic geometry in any depth.

We have provided a substantial number of exercises at the end of each chapter. Some of them are easy and some of them are hard. Usually we have provided hints, and sometimes complete solutions, to the hard ones. We are indebted to Mr. R. Y. Sharp, who worked through them all and saved us from error more than once.

We have made no attempt to describe the contributions of the many mathematicians who have helped to develop the theory as expounded in this book. We would, however, like to put on record our indebtedness to J.-P. Serre and J. Tate from whom we learnt the subject, and whose influence was the determining factor in our choice of material and mode of presentation.

References

[1] N Bourbaki. "Algèbre commutative, Hermann". In: *Paris, 1961–65* (1961).

[2] A Grothendieck and J Dieudonné. "Éléments de Géométrie algébrique". In: *Publications Mathématiques de l'Institut des Hautes Études Scientifiques* 4.1 (1960), pp. 5–214.

[3] D. G. Northcott. *Ideal Theory*. Cambridge University Press, 1953.

[4] Oscar Zariski and Pierre Samuel. *Commutative algebra I, II*. Vol. 1. 1958, 1960.

Notation and Terminology

Rings and modules are denoted by capital italic letters, elements of them by small italic letters. A field is often denoted by k. Ideals are denoted by small German characters. **Z**, **Q**, **R**, **C** denote respectively the ring of rational integers, the field of rational numbers, the field of real numbers and the field of complex numbers.

Mappings are consistently written on the *left*, thus the image of an element x under a mapping f is written $f(x)$ and not $(x)f$. The composition of mappings $f : X \to Y, g : Y \to Z$ is therefore $g \circ f$, not $f \circ g$. A mapping $f : X \to Y$ is *injective* if $f(x_1) = f(x_2)$ implies $x_1 = x_2$; surjective if $f(X) = Y$; bijective if both injective and surjective.

The end of a proof (or absence of proof) is marked thus $\square$·

Inclusion of sets is denoted by the sign $\subseteq$. We reserve the sign $\subset$ for strict inclusion. Thus $A \subset B$ means that A is contained in B and is not equal to B.

Chapter 1

Rings and Ideals

Chapter 2

Modules

Chapter 3

Rings and Modules of Fractions

Chapter 4

Primary Decomposition

The decomposition of an ideal into primary ideals is a traditional pillar of ideal theory. It provides the algebraic foundation for decomposing an algebraic variety into its irreducible components—although it is only fair to point out that the algebraic picture is more complicated than naïve geometry would suggest. From another point of view primary decomposition provides a generalization of the factorization of an integer as a product of prime-powers. In the modern treatment, with its emphasis on localization, primary decomposition is no longer such a central tool in the theory. It is still, however, of interest in itself and in this chapter we establish the classical uniqueness theorems.

The prototypes of commutative rings are $\mathbf{Z}$ and the ring of polynomials $k[x_1, \cdots, x_n]$ where k is a field; both these are unique factorization domains. This is not true of arbitrary commutative rings, even if they are integral domains (the classical example is the ring $\mathbf{Z}[\sqrt{-5}]$, in which the element 6 has two essentially distinct factorizations, $2 \cdot 3$ and $(1 + \sqrt{-5})(1 - \sqrt{-5})$. However, there is a generalized form of "unique factorization" of *ideals* (not of elements) in a wide class of rings (the Noetherian rings).

A prime ideal in a ring A is in some sense a generalization of a prime number. The corresponding generalization of a power of a prime number is a primary ideal. An ideal $\mathfrak{q}$ in a ring A is *primary* if $\mathfrak{q} \neq A$ and if

$$xy \in \mathfrak{q} \implies \text{either } x \in \mathfrak{q} \text{ or } y^n \in \mathfrak{q} \text{ for some } n > 0.$$

In other words,

$$\mathfrak{q} \text{ is primary} \iff A/\mathfrak{q} \neq 0 \text{ and every zero-divisor in } A/\mathfrak{q} \text{ is nilpotent.}$$

Clearly every prime ideal is primary. Also the contraction of a primary ideal is primary, for if $f : A \to B$ and if $\mathfrak{q}$ is a primary ideal in B , then $A/\mathfrak{q}^c$ is isomorphic to a subring of $B/\mathfrak{q}$.

Proposition 4.1. *Let $\mathfrak{q}$ be a primary ideal in a ring A. Then $r(\mathfrak{q})$ is the smallest prime ideal containing $\mathfrak{q}$.*

Proof. By (1.8) it is enough to show that $\mathfrak{p} = r(\mathfrak{q})$ is prime. Let $xy \in r(\mathfrak{q})$, then $(xy)^m \in \mathfrak{q}$ for some $m > 0$, and therefore either $x^m \in \mathfrak{q}$ or $y^{mn} \in \mathfrak{q}$ for some $n > 0$; i.e., either $x \in r(\mathfrak{q})$ or $y \in r(\mathfrak{q})$. □

If $\mathfrak{p} = r(\mathfrak{q})$, then $\mathfrak{q}$ is said to be $\mathfrak{p}$-primary.

Example. 1. *The primary ideals in* $\mathbf{Z}$ *are* (0) *and* (p^n)*, where* p *is prime. For these are the only ideals in* $\mathbf{Z}$ *with prime radical, and it is immediately checked that they are primary.*

2. *Let* $A = k[x, y]$, $\mathfrak{q} = (x, y^2)$*. Then* $A/\mathfrak{q} \simeq k[y]/(y^2)$*, in which the zero-divisors are all the multiples of* y*, hence are nilpotent. Hence* $\mathfrak{q}$ *is primary, and its radical* $\mathfrak{p}$ *is* (x, y)*. We have* $\mathfrak{p}^2 \subset \mathfrak{q} \subset \mathfrak{p}$ *(strict inclusions), so that a primary ideal is not necessarily a prime-power.*

3. *Conversely, a prime power* $\mathfrak{p}^n$ *is not necessarily primary, although its radical is the prime ideal* $\mathfrak{p}$*. For example, let* $A = k[x, y, z]/(xy - z^2)$ *and let* $\bar{x}, \bar{y}, \bar{z}$ *denote the images of* x, y, z *respectively in* A*. Then* $\mathfrak{p} = (\bar{x}, \bar{z})$ *is prime (since* $A/\mathfrak{p} \simeq k[y]$*, an integral domain); we have* $\bar{x}\bar{y} = \bar{z}^2 \in \mathfrak{p}^2$ *but* $x \notin \mathfrak{p}^2$ *and* $y \notin r(\mathfrak{p}^2) = \mathfrak{p}$*; hence* $\mathfrak{p}^2$ *is not primary. However, there is the following result:*

Proposition 4.2. *If* $r(\mathfrak{a})$ *is maximal, then* $\mathfrak{a}$ *is primary. In particular, the powers of a maximal ideal* $\mathfrak{m}$ *are* $\mathfrak{m}$*-primary.*

Proof. Let $r(\mathfrak{a}) = \mathfrak{m}$. The image of $\mathfrak{m}$ in $A/\mathfrak{a}$ is the nilradical of $A/\mathfrak{a}$, hence $A/\mathfrak{a}$ has only one prime ideal, by (1.8). Hence every element of $A/\mathfrak{a}$ is either a unit or nilpotent, and so every zero-divisor in $A/\mathfrak{a}$ is nilpotent. □

We are going to study presentations of an ideal as an intersection of primary ideals. First, a couple of lemmas:

lemma 4.3. *If* $\mathfrak{q}_i$, $(1 \le i \le n)$ *are* $\mathfrak{p}$*-primary, then* $\mathfrak{q} = \bigcap_{i=1}^n \mathfrak{q}_i$ *is* $\mathfrak{p}$*-primary.*

Proof. $r(\mathfrak{q}) = r(\bigcap_{i=1}^n \mathfrak{q}_i) = \cap r(\mathfrak{q}_i) = \mathfrak{p}$. Let $xy \in \mathfrak{q}$, $y \notin \mathfrak{q}$. Then for some i we have $xy \in \mathfrak{q}_i$ and $y \notin \mathfrak{q}_i$ hence $x \in \mathfrak{p}$. since $\mathfrak{q}_i$ is primary. □

lemma 4.4. *Let* q *be a* $\mathfrak{p}$*-primary ideal,* x *an element of* A*. Then*

1. *if* $x \in \mathfrak{q}$ *then* $(\mathfrak{q} : x) = (1)$*;*

2. *if* $x \notin \mathfrak{q}$ *then* $(\mathfrak{q} : x)$ *is* $\mathfrak{p}$*-primary, and therefore* $r(\mathfrak{q} : x) = \mathfrak{p}$*;*

3. *if* $x \notin \mathfrak{p}$ *then* $(\mathfrak{q} : x) = \mathfrak{q}$*.*

Proof. i) and iii) follow immediately from the definitions. ii): if $y \in (\mathfrak{q} : x)$ then $xy \in \mathfrak{q}$, hence (as $x \notin \mathfrak{q}$) we have $y \in \mathfrak{p}$ Hence $\mathfrak{q} \subseteq (\mathfrak{q} : x) \subseteq \mathfrak{p}$;taking radicals, we get $r(\mathfrak{q} : x) = \mathfrak{p}$. Let $yz \in (\mathfrak{q} : x)$ with $y \notin \mathfrak{p}$; then $xyz \in \mathfrak{q}$, hence $xz \in \mathfrak{q}$, hence $z \in (\mathfrak{q} : x)$. □

A primary decomposition of an ideal a in A is an expression of a as a finite intersection of primary ideals, say

$$a = \bigcap_{i=1}^{n} \mathfrak{q}_i \tag{4.1}$$

(In general such a primary decomposition need not exist; in this chapter we shall restrict our attention to ideals which have a primary decomposition.) If moreover (i) the $r(\mathfrak{q}_i)$ are all distinct, and (ii) we have $\mathfrak{q}_t \neq \bigcap_{j\neq i} \mathfrak{q}_j (2 \leqslant i \leqslant n)$ the primary decomposition (4.1) is said to be minimal (or irredundant, or reduced, or normal, ...). By Lemma 4.3 we can achieve (i) and then we can omit any superfluous terms to achieve (ii); thus any primary decomposition can be reduced to a minimal one. We shall say that $\mathfrak{a}$ is *decomposable* if it has a primary decomposition.

Theorem 4.5 (1st uniqueness theorem)**.** *Let* $\mathfrak{a}$ *be a decomposable ideal and let* $\mathfrak{a} = \bigcap_{\mathrm{i}=1}^{\mathrm{n}} \mathfrak{q}_i$ *be a minimal primary decomposition of* $\mathfrak{a}$*. Let* $\mathfrak{p}_i = r(\mathfrak{q}_i)$ *(*$1 \leq i \leq n$*). Then the* $\mathfrak{p}_1$ *are precisely the prime ideals which occur in the set of ideals* $r(\mathfrak{a} : x)$ *(*$x \in A$*), and hence are independent of the particular decomposition of* $\mathfrak{a}$*.*

Proof. For any $x \in A$ we have $(\mathfrak{a} : x) = (\cap \mathfrak{q}_i : x) = \bigcap (\mathfrak{q}_i : x)$, hence $r(\mathfrak{a} : x) = \bigcap_{i=1}^{n} r(\mathfrak{q}_i : x) = \bigcap_{x \notin q_j} \mathfrak{p}_j$ by Lemma 4.4. Suppose $r(a : x)$ is prime; then by (1.11) we have $r(\mathfrak{a} : x) = \mathfrak{p}_j$ for some j. Hence every prime ideal of the form $r(\mathfrak{a} : x)$ is one of the $\mathfrak{p}_j$. Conversely, for each i there exists $x_i \notin \mathfrak{q}_i, x_i \in \bigcap_{j\neq i} \mathfrak{q}_j$, since the decomposition is minimal; and we have $r(\mathfrak{a} : x_{\mathrm{i}}) = \mathfrak{p}_i$.

□

Remark. 1. The above proof, coupled with the last part of Lemma 4.4, shows that for each i there exists x_i in A such that $(\mathfrak{a} : x_i)$ is $\mathfrak{p}_i$-primary.

2. Considering $A/\mathfrak{a}$ as an A-module, Theorem 4.5 is equivalent to saying that the $\mathfrak{p}_i$ are precisely the prime ideals which occur as radicals of annihilators of elements of $A/\mathfrak{a}$

Example. Let $\mathfrak{a} = (x^2, xy)$ in $A = k[x, y]$. Then $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2^2$ where $\mathfrak{p}_1 = (x)$, $\mathfrak{p}_2 = (x, y)$. The ideal $\mathfrak{p}_2^2$ is primary by (4.2). So the prime ideals are $\mathfrak{p}_1, \mathfrak{p}_2$. In this example $\mathfrak{p}_1 \subset \mathfrak{p}_2$; we have $r(\mathfrak{a}) = \mathfrak{p}_1 \cap \mathfrak{p}_2 = \mathfrak{p}_1$, but $\mathfrak{a}$ is not a primary ideal.

The prime ideals $\mathfrak{p}_1$ in (4.5) are said to belong to $\mathfrak{a}$, or to be associated with a. The ideal a is primary if and only if it has only one associated prime ideal. The minimal elements of the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ are called the minimal or isolated prime ideals belonging to a. The others are called embedded prime ideals. In the example above, $\mathfrak{p}_2 = (x, y)$ is embedded.

Proposition 4.6. Let a be a decomposable ideal. Then any prime ideal $\mathfrak{p} \supseteq a$ contains a minimal prime ideal belonging to a, and thus the minimal prime ideals of $\mathfrak{a}$ are precisely the minimal elements in the set of all prime ideals containing a.

Proof. If $\mathfrak{p} \supseteq \mathfrak{a} = \bigcap_{\mathrm{i}-1}^{\pi} \mathfrak{q}_{\mathfrak{s}}$, then $\mathfrak{p} = r(\mathfrak{p}) \supseteq \bigcap r(\mathfrak{q}_{\mathfrak{k}}) = \bigcap \mathfrak{p}_{\mathfrak{k}}$. Hence by (1.11) we have $\mathfrak{p} \supseteq \mathfrak{p}_i$ for some i; hence $\mathfrak{p}$ contains a minimal prime ideal of $\mathfrak{a}$.

Remarks. 1) The names isolated and embedded come from geometry. Thus if $A = k[x_1, \ldots, x_n]$ where k is a field, the ideal a gives rise to a variety $X \subseteq k^n$ (see Chapter 1, Exercise 25). The minimal primes $\mathfrak{p}_i$ correspond to the irreducible components of X, and the embedded primes correspond to subvarieties of these, i.e., varieties embedded in the irreducible components. Thus in the example before (4.6) the variety defined by a is the line $x = 0$, and the embedded ideal $\mathfrak{p}_2 = (x, y)$ corresponds to the origin $(0, 0)$.

2. It is not true that all the primary components are independent of the decomposition. For example $\left(x^2, xy\right) = (x) \cap (x, y)^2 = (x) \cap \left(x^2, y\right)$ are two distinct minimal primary decompositions. However, there are some uniqueness properties: see (4.10).

Proposition 4.7. Let $\mathfrak{a}$ be a decomposable ideal, let $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_\mathrm{i}$ be a minimal primary decomposition, and let $r(\mathfrak{q}_\mathrm{i}) = \mathfrak{p}_\mathrm{i}$. Then

$$\bigcup_{i=1}^n \mathfrak{p}_i = \{x \in A : (\mathfrak{a} : x) \neq \mathfrak{a}\}.$$

In particular, if the zero ideal is decomposable, the set D of zero-divisors of A is the union of the prime ideals belonging to 0.

Proof. If a is decomposable, then 0 is decomposable in A/a : namely $0 = \bigcap \bar{q}_1$ where $\bar{q}_1$ is the image of q_1 in $A/\mathfrak{a}$, and is primary. Hence it is enough to prove the last statement of (4.7). By (1.15) we have $D = \bigcup_{x \neq 0} r(0 : x)$; from the proof of (4.5), we have $r(0 : x) = \bigcap_{x \xi q_1} \mathfrak{p}_j \subseteq \mathfrak{p}_j$ for some j, hence $D \subseteq \bigcup_{i-1}^n \mathfrak{p}_i$. But also from (4.5) each p_i is of the form $r(0 : x)$ for some $x \in A$, hence $\cup p_1 \subseteq D$.

Thus (the zero ideal being decomposabie)

$$\begin{aligned} D &= \text{ set of zero-divisors} \\ &= \bigcup \text{ of all prime ideals belonging to 0;} \\ \mathfrak{R} &= \text{ set of nilpotent elements} \\ &= \bigcap \text{ of all minimal primes belonging to 0.} \end{aligned}$$

Next we investigate the behavior of primary ideals under localization.

Proposition 4.8. Let S be a multiplicatively closed subset of A, and let $\mathfrak{q}$ be a p-primary ideal.

i) If $S \cap \mathfrak{p} \neq \emptyset$, then $S^{-1}\mathfrak{q} = S^{-1}A$.

ii) If $S \cap \mathfrak{p} = \emptyset$, then $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$-primary and its contraction in A is $\mathfrak{q}$. Hence primary ideals correspond to primary ideals in the correspondence (3.11) between ideals in $S^{-1}A$ and contracted ideals in A.

Proof. i) If $s \in S \cap \mathfrak{p}$, then $s^n \in S \cap \mathfrak{q}$ for some $n > 0$; hence $S^{-1}\mathfrak{q}$ contains $s^n/1$, which is a unit in $S^{-1}A$.

ii) If $S \cap \mathfrak{p} = \emptyset$, then $s \in S$ and $as \in \mathfrak{q}$ imply $a \in \mathfrak{q}$, hence $q^{ec} = \mathfrak{q}$ by (3.11). Also from (3.11) we have $r(\mathfrak{q}^e) = r\left(S^{-1}\mathfrak{q}\right) = S^{-1}r(\mathfrak{q}) = S^{-1}\mathfrak{p}$. The verification that $S^{-1}q$ is primary is straightforward. Finally, the contraction of a primary ideal is primary.

For any ideal $\mathfrak{a}$ and any multiplicatively closed subset S in A, the contraction in A of the ideal $S^{-1}\mathfrak{a}$ is denoted by $S(\mathfrak{a})$. Proposition 4.9. Let S be a multiplicatively closed subset of A and let $\mathfrak{a}$ be a decomposable ideal. Let $\mathfrak{a} = \bigcap_{i=1}^{n} q_i$ be a minimal primary decomposition of $\mathfrak{a}$. Let $\mathfrak{p}_i = r(\mathfrak{q}_\mathrm{i})$ and suppose the $\mathfrak{q}_i$ numbered so that S meets $\mathfrak{p}_{m+1}, \ldots, \mathfrak{p}_n$ but not $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Then

$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} S^{-1}\mathfrak{a}_i, \quad S(\mathfrak{a}) = \bigcap_{i=1}^{m} a_\mathrm{i},$$

and these are minimal primary decompositions.

Proof. $S^{-1}\mathfrak{a} = \bigcap_{i=1}^{n} S^{-1}q_i$ by (3.11) $= \bigcap_{i=1}^{m} S^{-1}q_i$ by (4.8), and $S^{-1}q_i$ is $S^{-1}\mathfrak{p}_i$-primary for $i = 1, \ldots, m$. Since the $\mathfrak{p}_i$ are distinct, so are the $S^{-1}\mathfrak{p}_i$ $(1 \leqslant i \leqslant m)$, hence we have a minimal primary decomposition. Contracting both sides, we get

$$S(\mathfrak{a}) = \left(S^{-1}\mathfrak{a}\right)^{\mathfrak{c}} = \bigcap_{i=1}^{m} \left(S^{-1}a_i\right)^{\mathfrak{c}} = \bigcap_{i=1}^{m} a_i$$

by (4.8) again.

A set Σ of prime ideals belonging to $\mathfrak{a}$ is said to be isolated if it satisfies the following condition: if $\mathfrak{p}'$ is a prime ideal belonging to $\mathfrak{a}$ and $\mathfrak{p}' \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$, then $\mathfrak{p}' \in \Sigma$.

Let Σ be an isolated set of prime ideals belonging to a, and let $S = A - U_{\text{per}}\, \mathfrak{p}$. Then S is multiplicatively closed and, for any prime ideal $\mathfrak{p}'$ belonging to $\mathfrak{a}$, we have

$$\mathfrak{p}' \in \Sigma \Rightarrow \mathfrak{p}' \cap S = \emptyset;$$
$$\mathfrak{p}' \notin \Sigma \Rightarrow \mathfrak{p}' \neq \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}(\text{ by } (1.11)) \Rightarrow \mathfrak{p}' \cap S \neq \emptyset.$$

Hence, from (4.9), we deduce

Theorem 4.10. (2nd uniqueness theorem). Let $\mathfrak{a}$ be a decomposable ideal, let $\mathfrak{a} = \bigcap_{\mathrm{i}=1}^{\mathrm{m}} \mathfrak{q}_\mathrm{i}$ be a minimal primary decomposition of $\mathfrak{a}$, and let $\left\{\mathfrak{p}_{1_2}, \ldots, \mathfrak{p}_{\mathrm{i}_m}\right\}$ be an isolated set of prime ideals of $\mathfrak{a}$. Then $a_{i_1} \cap \ldots \cap a_{i_m}$ is independent of the decomposition.

In particular:

Corollary 4.11. The isolated primary components (i.e., the primary components q_i corresponding to minimal prime ideals $\mathfrak{p}_\mathrm{i}$) are uniquely determined by a.

Proof of (4.10). We have $q_{i_2} \cap \cdots \cap q_{i_m} = S(\mathfrak{a})$ where $S = \bar{A} - \mathfrak{p}_{i_2} \cup \cdots \cup \mathfrak{p}_{i_m}$, hence depends only on a (since the $\mathfrak{p}_\mathfrak{l}$ depend only on $\mathfrak{a}$)

Remark. On the other hand, the embedded primary components are in general not uniquely determined by a. If A is a Noetherian ring, there are in fact infinitely many choices for each embedded component (see Chapter 8, Exercise 1).

4.1 EXERCISES

1. If an ideal $\mathfrak{a}$ has a primary decomposition, then $\operatorname{Spec}(A/\mathfrak{a})$ has only finitely many irreducible components.

2. If $\mathfrak{a} = r(\mathfrak{a})$, then $\mathfrak{a}$ has no embedded prime ideals.

3. If A is absolutely flat, every primary ideal is maximal.

4. In the polynomial ring $Z[t]$, the ideal $m = (2, t)$ is maximal and the ideal $q = (4, t)$ is m-primary, but is not a power of m.

5. In the polynomial ring $K[x, y, z]$ where K is a field and x, y, z are independent indeterminates, let $\mathfrak{p}_1 = (x, y), \mathfrak{p}_2 = (x, z), \mathfrak{m} = (x, y, z)$; $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime, and $\mathfrak{m}$ is maximal. Let $a = \mathfrak{p}_1\mathfrak{p}_2$. Show that $a = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ is a reduced primary decomposition of $\mathfrak{a}$. Which components are isolated and which are embedded?

6. Let X be an infinite compact Hausdorff space, $C(X)$ the ring of real-valued continuous functions on X (Chapter 1, Exercise 26). Is the zero ideal decomposable in this ring?

7. Let A be a ring and let $A[x]$ denote the ring of polynomials in one indeterminate over A. For each ideal $\mathfrak{a}$ of A, let $\mathfrak{a}[x]$ denote the set of all polynomials in $A[x]$ with coefficients in $\mathfrak{a}$.

i) $\mathfrak{a}[x]$ is the extension of $\mathfrak{a}$ to $A[x]$.
ii) If $\mathfrak{p}$ is a prime ideal in A, then $\mathfrak{p}[x]$ is a prime ideal in $A[x]$.
iii) If $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal in A, then $\mathfrak{q}[x]$ is a $\mathfrak{p}[x]$-primary ideal in $A[x]$. [Use Chapter 1, Exercise 2.]
iv) If $a = \bigcap_{1=1}^{n} \mathfrak{q}_t$ is a minimal primary decomposition in A, then $\mathfrak{a}[x] = \cap_{i=1}^{n} \mathfrak{q}_i[x]$ is a minimal primary decomposition in $A[x]$.
v) If $\mathfrak{p}$ is a minimal prime ideal of $\mathfrak{a}$, then $\mathfrak{p}[x]$ is a minimal prime ideal of $\mathfrak{a}[x]$.

8. Let k be a field. Show that in the polynomial ring $k[x_1, \ldots, x_n]$ the ideals $p_i = (x_1, \ldots, x_i)$ $(1 \leqslant i \leqslant n)$ are prime and all their powers are primary. [Use Exercise 7.]

9. In a ring A, let $D(A)$ denote the set of prime ideals $\mathfrak{p}$ which satisfy the following condition: there exists $a \in A$ such that $\mathfrak{p}$ is minimal in the set of prime ideals containing (0:a). Show that $x \in A$ is a zero divisor $\Leftrightarrow x \in \mathfrak{p}$ for some $\mathfrak{p} \in D(A)$.

Let S be a multiplicatively closed subset of A, and identify Spec $\left(S^{-1}A\right)$ with its image in Spec (A) (Chapter 3, Exercise 21). Show that

$$D\left(S^{-1}A\right) = D(A) \cap \operatorname{Spec}\left(S^{-1}A\right).$$

If the zero ideal has a primary decomposition, show that $D(A)$ is the set of associated prime ideals of 0 .

10. For any prime ideal $\mathfrak{p}$ in a ring A, let $S_{\mathfrak{p}}(0)$ denote the kernel of the homomorphism $A \rightarrow A_p$. Prove that

i) $S_{\mathfrak{p}}(0) \subseteq \mathfrak{p}$.
ii) $r\left(S_{\mathfrak{p}}(0)\right)=\mathfrak{p} \Leftrightarrow \mathfrak{p}$ is a minimal prime ideal of A.
iii) If $\mathfrak{p} \supseteq \mathfrak{p}'$, then $S_{\mathfrak{p}}(0) \subseteq S_{\mathfrak{p}}, (0)$.
iv) $\bigcap_{\mathfrak{D} \in D(A)} S_{\mathfrak{p}}(0) = 0$, where $D(A)$ is defined in Exercise 9. 11. If $\mathfrak{p}$ is a minimal prime ideal of a ring A, show that $S_{\downarrow}(0)$ (Exercise 10) is the smallest p-primary ideal.

Let a be the intersection of the ideals $S_{\mathfrak{p}}(0)$ as $\mathfrak{p}$ runs through the minimal prime ideals of A. Show that $\mathfrak{a}$ is contained in the nilradical of A.

Suppose that the zero ideal is decomposable. Prove that $\mathfrak{a}=0$ if and only if every prime ideal of 0 is isolated.

12. Let A be a ring, S a multiplicatively closed subset of A. For any ideal a, let $S(\mathfrak{a})$ denote the contraction of $S^{-1}\mathfrak{a}$ in A. The ideal $S(\mathfrak{a})$ is called the saturation of a with respect to S. Prove that

i) $S(\mathfrak{a}) \cap S(\mathfrak{b})=S(\mathfrak{a} \cap \mathfrak{b})$
ii) $S(r(\mathfrak{a}))=r(S(\mathfrak{a}))$
iii) $S(\mathfrak{a})=(1) \Leftrightarrow a$ meets S
iv) $S_1\left(S_2(\mathfrak{a})\right)=\left(S_1 S_2\right)(\mathfrak{a})$.

If $\mathfrak{a}$ has a primary decomposition, prove that the set of ideals $S(\mathfrak{a})$ (where S runs through all multiplicatively closed subsets of A) is finite.

13. Let A be a ring and $\mathfrak{p}$ a prime ideal of A. The *nth* symbolic power of $\mathfrak{p}$ is defined to be the ideal (in the notation of Exercise 12)

$$\mathfrak{p}^{(n)}=S_{\mathfrak{p}}\left(\mathfrak{p}^n\right)$$

where $S_{\mathfrak{p}}=A-\mathfrak{p}$. Show that
i) $\mathfrak{p}^{(n)}$ is a $\mathfrak{p}$-primary ideal;
ii) if $\mathfrak{p}^n$ has a primary decomposition, then $\mathfrak{p}^{(n)}$ is its $\mathfrak{p}$-primary component;
iii) if $\mathfrak{p}^{(m)} \mathfrak{p}^{(n)}$ has a primary decomposition, then $\mathfrak{p}^{(m+n)}$ is its $\mathfrak{p}$-primary component;
iv) $\mathfrak{p}^{(n)}=\mathfrak{p}^n \Leftrightarrow \mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary.

14. Let a be a decomposable ideal in a ring A and let p be a maximal element of the set of ideals ($\mathfrak{a}: x$), where $x \in A$ and $x \notin \mathfrak{a}$. Show that $\mathfrak{p}$ is a prime ideal belonging to $\mathfrak{a}$.

15. Let a be a decomposable ideal in a ring A, let Σ be an isolated set of prime ideals belonging to a, and let q_{Σ} be the intersection of the corresponding primary components. Let f be an element of A such that, for each prime ideal $\mathfrak{p}$ belonging to a, we have $f \in \mathfrak{p} \Leftrightarrow \mathfrak{p} \notin \Sigma$, and let S_f be the set of all powers of f. Show that $q_{\Sigma}=S_f(a)=\left(a: f^n\right)$ for all large n.

16. If A is a ring in which every ideal has a primary decomposition, show that every ring of fractions $S^{-1}A$ has the same property.

17. Let A be a ring with the following property.

(L1) For every ideal $\mathfrak{a} \neq (1)$ in A and every prime ideal $\mathfrak{p}$, there exists $x \notin \mathfrak{p}$ such that $S_{\mathfrak{p}}(\mathfrak{a}) = (\mathfrak{a} : x)$, where $S_{\mathfrak{p}} = A - \mathfrak{p}$.

Then every ideal in A is an intersection of (possibly infinitely many) primary ideals.

[Let a be an ideal $\neq (1)$ in A, and let p_1 be a minimal element of the set of prime ideals containing $\mathfrak{a}$. Then $\mathfrak{q}_1 = S_{\mathfrak{p}_1}(\mathfrak{a})$ is $\mathfrak{p}_1$-primary (by Exercise 11), and $q_1 = (\mathfrak{a} : x)$ for some $x \notin \mathfrak{p}_1$. Show that $\mathfrak{a} = \mathfrak{q}_1 \cap (\mathfrak{a} + (x))$.

Now let a_1 be a maximal element of the set of ideals $\mathfrak{b} \supseteq \mathfrak{a}$ such that $a_1 \cap \mathfrak{b} = a$, and choose a_1 so that $x \in \mathfrak{a}_1$, and therefore $a_1 \not\subseteq \mathfrak{p}_1$. Repeat the construction starting with $\mathfrak{a}_1$, and so on. At the nth stage we have $a = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n \cap \mathfrak{a}_n$ where the $\mathfrak{q}_{\mathfrak{t}}$ are primary ideals, $\mathfrak{a}_n$ is maximal among the ideals $\mathfrak{b}$ containing $\mathfrak{a}_{n-1} = \mathfrak{a}_n \cap \mathfrak{q}_n$ such that $\mathfrak{a} = q_{\mathfrak{z}} \cap \cdots \cap \mathfrak{q}_n \cap \mathfrak{b}$, and $\mathfrak{a}_n \not\subseteq \mathfrak{p}_n$. If at any stage we have $\mathfrak{a}_n = (1)$, the process stops, and $\mathfrak{a}$ is a finite intersection of primary ideals. If not, continue by transfinite induction, observing that each $\mathfrak{a}_n$ strictly contains a_{n-1}.]

18. Consider the following condition on a ring A :

(L2) Given an ideal a and a descending chain $S_1 \supseteq S_2 \supseteq \cdots \geq S_n \supseteq \cdots$ of multiplicatively closed subsets of A, there exists an integer n such that $S_n(\mathfrak{a}) = S_{n+1}(\mathfrak{a}) = \cdots$. Prove that the following are equivalent:

i) Every ideal in A has a primary decomposition;

ii) A satisfies (L1) and (L2).

[For i) $\Rightarrow$ ii), use Exercises 12 and 15 . For ii) $\Rightarrow$ i) show, with the notation of the proof of Exercise 17, that if $S_n = S_{\mathfrak{p}_1} \cap \cdots \cap S_{\mathfrak{p}_n}$ then S_n meets $\mathfrak{a}_n$, hence $S_n\left(\mathfrak{a}_n\right) = (1)$, and therefore $S_n(\mathfrak{a}) = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$. Now use (L2) to show that the construction must terminate after a finite number of steps.]

19. Let A be a ring and $\mathfrak{p}$ a prime ideal of A. Show that every p-primary ideal contains $S_{\mathfrak{p}}(0)$, the kernel of the canonical homomorphism $A \rightarrow A_{\mathfrak{p}}$.

Suppose that A satisfies the following condition: for every prime ideal p, the intersection of all $\mathfrak{p}$-primary ideals of A is equal to $S_{\mathfrak{p}}(0)$. (Noetherian rings satisfy this condition: see Chapter 10.) Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be distinct prime ideals, none of which is a minimal prime ideal of A. Then there exists an ideal a in A whose associated prime ideals are $p_1, \ldots, p_n$.

[Proof by induction on n. The case $n = 1$ is trivial (take $a = \mathfrak{p}_1$). Suppose $n > 1$ and let $\mathfrak{p}_n$ be maximal in the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. By the inductive hypothesis there exists an ideal $\mathfrak{b}$ and a minimal primary decomposition $\mathfrak{b} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{n-1}$, where each $\mathfrak{q}_t$ is $\mathfrak{p}_{\mathfrak{t}}$-primary. If $\mathfrak{b} \subseteq S_{\mathfrak{p}_n}(0)$, let $\mathfrak{p}$ be a minimal prime ideal of A contained in $\mathfrak{p}_n$. Then $S_{\mathfrak{p}_n}(0) \subseteq S_{\mathfrak{p}}(0)$, hence $\mathfrak{b} \subseteq S_{\mathfrak{p}}(0)$. Taking radicals and using Exercise 10 , we have $\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_{n-1} \subseteq \mathfrak{p}$, hence some $\mathfrak{p}_{\mathfrak{t}} \subseteq \mathfrak{p}$, hence

$\mathfrak{p}_t = \mathfrak{p}$ since $\mathfrak{p}$ is minimal. This is a contradiction since no $\mathfrak{p}_t$ is minimal. Hence $\mathfrak{b} \not\subseteq S_{\mathfrak{p}_n}(0)$ and therefore there exists a $\mathfrak{p}_n$-primary ideal q_n such that $\mathfrak{b} \not\subseteq \mathfrak{q}_n$. Show that $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ has the required properties.]

4.2 Primary decomposition of modules

Practically the whole of this chapter can be transposed to the context of modules over a ring A. The following exercises indicate how this is done.

20. Let M be a fixed A-module, N a submodule of M. The radical of N in M is defined to be

$$r_M(N) = \{x \in A : x^q M \subseteq N \text{ for some } q > 0\}.$$

Show that $r_M(N) = r(N : M) = r(\text{ Ann } (M/N))$. In particular, $r_M(N)$ is an ideal.

State and prove the formulas for r_M analogous to (1.13).

21. An element $x \in A$ defines an endomorphism ϕ_x of M, namely $m \mapsto xm$. The element x is said to be a zero-divisor (resp. nilpotent) in M if ϕ_x is not injective (resp. is nilpotent). A submodule Q of M is primary in M if $Q \neq M$ and every zero-divisor in M/Q is nilpotent.

Show that if Q is primary in M, then $(Q : M)$ is a primary ideal and hence $r_M(Q)$ is a prime ideal $\mathfrak{p}$. We say that Q is $\mathfrak{p}$-primary (in M).

Prove the analogues of (4.3) and (4.4).

22. A primary decomposition of N in M is a representation of N as an intersection

$$N = Q_1 \cap \cdots \cap Q_n$$

of primary submodules of M; it is a minimal primary decomposition if the ideals $\mathfrak{p}_i = r_M(Q_i)$ are all distinct and if none of the components Q_i can be omitted from the intersection, that is if $Q_t¥\bigcap_{t\neq 1} Q_1 (1 \leqslant i \leqslant n)$.

Prove the analogue of (4.5), that the prime ideals $\mathfrak{p}_1$ depend only on N (and M). They are called the prime ideals belonging to N in M. Show that they are also the prime ideals belonging to 0 in M/N.

23. State and prove the analogues of (4.6)-(4.11) inclusive. (There is no loss of generality in taking $N = 0$.)

Chapter 5

Integral Dependence and Valuations

Chapter 6

Chain Conditions

Chapter 7

Noetherian Rings

Chapter 8

Artin Rings

Chapter 9

Discrete Valuation Rings and Dedekind Domains

Chapter 10

Completions

Chapter 11

Dimension Theory

Index