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 $k[x_1, \ldots, x_n]$ 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

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

In other words,

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

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*.

Examples. 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 $A/\mathfrak{q} \cong k[y]/(y^2)$, 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 $A/\mathfrak{p} \cong k[y]$, an integral domain); we have $\bar{x}\bar{y} = \bar{z}^2 \in \mathfrak{p}^2$ but $\bar{x} \notin \mathfrak{p}^2$ and $\bar{y} \notin r(\mathfrak{p}^2) = \mathfrak{p}$; 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 $\mathfrak{q}_i$ $(1 \leqslant i \leqslant n)$ are $\mathfrak{p}$-primary, then $\mathfrak{q} = \bigcap_{i=1}^n \mathfrak{q}_i$ is $\mathfrak{p}$-primary.*

Proof. $r(\mathfrak{q}) = r(\bigcap_{i=1}^n \mathfrak{q}_i) = \bigcap r(\mathfrak{q}_i) = \mathfrak{p}$. 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 $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal, x an element of A. Then*

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

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

iii) *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 $\mathfrak{a}$ in A is an expression of $\mathfrak{a}$ as a finite intersection of primary ideals, say

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

(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 more-

over (i) the $r(\mathfrak{q}_i)$ are all distinct, and (ii) we have $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$ $(1 \leqslant i \leqslant n)$ the primary decomposition (1) is said to be *minimal* (or irredundant, or reduced, or normal, . . .). By (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 $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ be a minimal primary decomposition of $\mathfrak{a}$. Let $\mathfrak{p}_i = r(\mathfrak{q}_i)$ $(1 \leqslant i \leqslant n)$. Then the $\mathfrak{p}_i$ 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 $(\mathfrak{a}:x) = (\bigcap \mathfrak{q}_i:x) = \bigcap (\mathfrak{q}_i:x)$, hence $r(\mathfrak{a}:x) = \bigcap_{i=1}^{n} r(\mathfrak{q}_i:x) = \bigcap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j$ by (4.4). Suppose $r(\mathfrak{a}:x)$ 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 $r(\mathfrak{a}:x_i) = \mathfrak{p}_i$. ∎

Remarks. 1) The above proof, coupled with the last part of (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, (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 $\mathfrak{p}_i$ in (4.5) are said to *belong* to $\mathfrak{a}$, or to be *associated* with $\mathfrak{a}$. The ideal $\mathfrak{a}$ 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 $\mathfrak{a}$. The others are called *embedded* prime ideals. In the example above, $\mathfrak{p}_2 = (x, y)$ is embedded.

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

Proof. If $\mathfrak{p} \supseteq \mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$, then $\mathfrak{p} = r(\mathfrak{p}) \supseteq \bigcap r(\mathfrak{q}_i) = \bigcap \mathfrak{p}_i$. 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 $\mathfrak{a}$ 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 $\mathfrak{a}$ 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 $(x^2, xy) = (x) \cap (x, y)^2 = (x) \cap (x^2, y)$ 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 $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ be a minimal primary decomposition, and let $r(\mathfrak{q}_i) = \mathfrak{p}_i$. 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 $\mathfrak{a}$ is decomposable, then 0 is decomposable in $A/\mathfrak{a}$: namely $0 = \bigcap \bar{\mathfrak{q}}_i$ where $\bar{\mathfrak{q}}_i$ is the image of $\mathfrak{q}_i$ 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 $r(0:x) = \bigcap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j \subseteq \mathfrak{p}_j$ for some j, hence $D \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$. But also from (4.5) each $\mathfrak{p}_i$ is of the form $r(0:x)$ for some $x \in A$, hence $\bigcup \mathfrak{p}_i \subseteq D$. ∎

Thus (the zero ideal being decomposable)

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

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 $\mathfrak{p}$-primary ideal.*

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

ii) *If $S \cap \mathfrak{p} = \varnothing$, 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 $S \cap \mathfrak{p} = \varnothing$, then $s \in S$ and $as \in \mathfrak{q}$ imply $a \in \mathfrak{q}$, hence $\mathfrak{q}^{ec} = \mathfrak{q}$ by (3.11). Also from (3.11) we have $r(\mathfrak{q}^e) = r(S^{-1}\mathfrak{q}) = S^{-1}r(\mathfrak{q}) = S^{-1}\mathfrak{p}$. The verification that $S^{-1}\mathfrak{q}$ 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 $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ be a minimal primary decomposition of $\mathfrak{a}$. Let $\mathfrak{p}_i = r(\mathfrak{q}_i)$ 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*

$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i, \qquad S(\mathfrak{a}) = \bigcap_{i=1}^{m} \mathfrak{q}_i,$$

and these are minimal primary decompositions.

Proof. $S^{-1}\mathfrak{a} = \bigcap_{i=1}^{n} S^{-1}\mathfrak{q}_i$ by (3.11) $= \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i$ by (4.8), and $S^{-1}\mathfrak{q}_i$ 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

$$S(\mathfrak{a}) = (S^{-1}\mathfrak{a})^c = \bigcap_{i=1}^{m} (S^{-1}\mathfrak{q}_i)^c = \bigcap_{i=1}^{m} \mathfrak{q}_i$$

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 $\mathfrak{a}$, and let $S = A - \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}$. Then S is multiplicatively closed and, for any prime ideal $\mathfrak{p}'$ belonging to $\mathfrak{a}$, we have

$$\mathfrak{p}' \in \Sigma \Rightarrow \mathfrak{p}' \cap S = \varnothing;$$

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

Hence, from (4.9), we deduce

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

In particular:

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

Proof of (4.10). We have $\mathfrak{q}_{i_1} \cap \cdots \cap \mathfrak{q}_{i_m} = S(\mathfrak{a})$ where $S = A - \mathfrak{p}_{i_1} \cup \cdots \cup \mathfrak{p}_{i_m}$, hence depends only on $\mathfrak{a}$ (since the $\mathfrak{p}_i$ depend only on $\mathfrak{a}$). ■

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

7

Noetherian Rings

We recall that a ring A is said to be *Noetherian* if it satisfies the following three equivalent conditions:

1) Every non-empty set of ideals in A has a maximal element.
2) Every ascending chain of ideals in A is stationary.
3) Every ideal in A is finitely generated.

(The equivalence of these conditions was proved in (6.1) and (6.2).)

Noetherian rings are by far the most important class of rings in commutative algebra: we have seen some examples already in Chapter 6. In this chapter we shall first show that Noetherian rings reproduce themselves under various familiar operations—in particular we prove the famous basis theorem of Hilbert. We then proceed to make a number of important deductions from the Noetherian condition, including the existence of primary decompositions.

Proposition 7.1. *If A is Noetherian and ϕ is a homomorphism of A onto a ring B, then B is Noetherian.*

Proof. This follows from (6.6), since $B \cong A/\mathfrak{a}$, where $\mathfrak{a} = \mathrm{Ker}(\phi)$. ■

Proposition 7.2. *Let A be a subring of B; suppose that A is Noetherian and that B is finitely generated as an A-module. Then B is Noetherian (as a ring).*

Proof. By (6.5) B is Noetherian as an A-module, hence also as a B-module. ■

Example. $B = \mathbf{Z}[i]$, the ring of Gaussian integers. By (7.2) B is Noetherian. More generally, the ring of integers in any algebraic number field is Noetherian.

Proposition 7.3. *If A is Noetherian and S is any multiplicatively closed subset of A, then $S^{-1}A$ is Noetherian.*

Proof. By (3.11—i) and (1.17—iii) the ideals of $S^{-1}A$ are in one-to-one order-preserving correspondence with the contracted ideals of A, hence satisfy the maximal condition. (Alternative proof: if $\mathfrak{a}$ is any ideal of A, then $\mathfrak{a}$ has a finite set of generators, say $x_1, \ldots, x_n$, and it is clear that $S^{-1}\mathfrak{a}$ is generated by $x_1/1, \ldots, x_n/1$.) ■

Corollary 7.4. *If A is Noetherian and $\mathfrak{p}$ is a prime ideal of A, then $A_{\mathfrak{p}}$ is Noetherian.* ■

Theorem 7.5. (Hilbert's Basis Theorem). *If A is Noetherian, then the polynomial ring $A[x]$ is Noetherian.*

Proof. Let $\mathfrak{a}$ be an ideal in $A[x]$. The leading coefficients of the polynomials in $\mathfrak{a}$ form an ideal $\mathfrak{l}$ in A. Since A is Noetherian, $\mathfrak{l}$ is finitely generated, say by $a_1, \ldots, a_n$. For each $i = 1, \ldots, n$ there is a polynomial $f_i \in A[x]$ of the form $f_i = a_i x^{r_i} +$ (lower terms). Let $r = \max_{i=1}^{n} r_i$. The f_i generate an ideal $\mathfrak{a}' \subseteq \mathfrak{a}$ in $A[x]$.

Let $f = ax^m +$ (lower terms) be any element of $\mathfrak{a}$; we have $a \in \mathfrak{l}$. If $m \geqslant r$, write $a = \sum_{i=1}^{n} u_i a_i$, where $u_i \in A$; then $f - \sum u_i f_i x^{m-r_i}$ is in $\mathfrak{a}$ and has degree $< m$. Proceeding in this way, we can go on subtracting elements of $\mathfrak{a}'$ from f until we get a polynomial g, say, of degree $< r$; that is, we have $f = g + h$, where $h \in \mathfrak{a}'$.

Let M be the A-module generated by $1, x, \ldots, x^{r-1}$; then what we have proved is that $\mathfrak{a} = (\mathfrak{a} \cap M) + \mathfrak{a}'$. Now M is a finitely generated A-module, hence is Noetherian by (6.5), hence $\mathfrak{a} \cap M$ is finitely generated (as an A-module) by (6.2). If $g_1, \ldots, g_m$ generate $\mathfrak{a} \cap M$ it is clear that the f_i and the g_j generate $\mathfrak{a}$. Hence $\mathfrak{a}$ is finitely generated and so $A[x]$ is Noetherian. ∎

Remark. It is also true that A Noetherian $\Rightarrow$ $A[[x]]$ Noetherian ($A[[x]]$ being the ring of formal power series in x with coefficients in A). The proof runs almost parallel to that of (7.5) except that one starts with the terms of *lowest* degree in the power series belonging to $\mathfrak{a}$. See also (10.27).

Corollary 7.6. *If A is Noetherian so is $A[x_1, \ldots, x_n]$.*

Proof. By induction on n from (7.5). ∎

Corollary 7.7. *Let B be a finitely-generated A-algebra. If A is Noetherian, then so is B.*

In particular, every finitely-generated ring, and every finitely generated algebra over a field, is Noetherian.

Proof. B is a homomorphic image of a polynomial ring $A[x_1, \ldots, x_n]$, which is Noetherian by (7.6). ∎

Proposition 7.8. *Let $A \subseteq B \subseteq C$ be rings. Suppose that A is Noetherian, that C is finitely generated as an A-algebra and that C is either* (i) *finitely generated as a B-module or* (ii) *integral over B. Then B is finitely generated as an A-algebra.*

Proof. It follows from (5.1) and (5.2) that the conditions (i) and (ii) are equivalent in this situation. So we may concentrate on (i).

Let $x_1, \ldots, x_m$ generate C as an A-algebra, and let $y_1, \ldots, y_n$ generate C as a B-module. Then there exist expressions of the form

$$x_i = \sum_j b_{ij} y_j \qquad (b_{ij} \in B) \tag{1}$$

$$y_i y_j = \sum_k b_{ijk} y_k \qquad (b_{ijk} \in B). \tag{2}$$

Let B_0 be the algebra generated over A by the b_{ij} and the b_{ijk}. Since A is Noetherian, so is B_0 by (7.7), and $A \subseteq B_0 \subseteq B$.

Any element of C is a polynomial in the x_i with coefficients in A. Substituting (1) and making repeated use of (2) shows that each element of C is a linear combination of the y_j with coefficients in B_0, and hence C is finitely generated as a B_0-module. Since B_0 is Noetherian, and B is a submodule of C, it follows (by (6.5) and (6.2)) that B is finitely generated as a B_0-module. Since B_0 is finitely generated as an A-algebra, it follows that B is finitely-generated as an A-algebra. ∎

Proposition 7.9. *Let k be a field, E a finitely generated k-algebra. If E is a field then it is a finite algebraic extension of k.*

Proof. Let $E = k[x_1, \ldots, x_n]$. If E is not algebraic over k then we can renumber the x_i so that $x_1, \ldots, x_r$ are algebraically independent over k, where $r \geqslant 1$, and each of $x_{r+1}, \ldots, x_n$ is algebraic over the field $F = k(x_1, \ldots, x_r)$. Hence E is a finite algebraic extension of F and therefore finitely generated as an F-module. Applying (7.8) to $k \subseteq F \subseteq E$, it follows that F is a finitely generated k-algebra, say $F = k[y_1, \ldots, y_s]$. Each y_j is of the form f_j/g_j, where f_j and g_j are polynomials in $x_1, \ldots, x_r$.

Now there are infinitely many irreducible polynomials in the ring $k[x_1, \ldots, x_r]$ (adapt Euclid's proof of the existence of infinitely many prime numbers). Hence there is an irreducible polynomial h which is prime to each of the g_j (for example, $h = g_1 g_2 \cdots g_s + 1$ would do) and the element h^{-1} of F could not be a polynomial in the y_j. This is a contradiction. Hence E is algebraic over k, and therefore finite algebraic. ∎

Corollary 7.10. *Let k be a field, A a finitely generated k-algebra. Let $\mathfrak{m}$ be a maximal ideal of A. Then the field $A/\mathfrak{m}$ is a finite algebraic extension of k. In particular, if k is algebraically closed then $A/\mathfrak{m} \cong k$.*

Proof. Take $E = A/\mathfrak{m}$ in (7.9). ∎

(7.10) is the so-called "weak" version of Hilbert's Nullstellensatz (= theorem of the zeros). The proof given here is due to Artin and Tate. For its geometrical meaning, and the "strong" form of the theorem, see the Exercises at the end of this chapter.

PRIMARY DECOMPOSITION IN NOETHERIAN RINGS

The next two lemmas show that every ideal $\neq (1)$ in a Noetherian ring has a primary decomposition.

An ideal $\mathfrak{a}$ is said to be *irreducible* if

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \Rightarrow (\mathfrak{a} = \mathfrak{b} \text{ or } \mathfrak{a} = \mathfrak{c}).$$

Lemma 7.11. *In a Noetherian ring A every ideal is a finite intersection of irreducible ideals.*

Proof. Suppose not; then the set of ideals in A for which the lemma is false is not empty, hence has a maximal element $\mathfrak{a}$. Since $\mathfrak{a}$ is reducible, we have $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ where $\mathfrak{b} \supset \mathfrak{a}$ and $\mathfrak{c} \supset \mathfrak{a}$. Hence each of $\mathfrak{b}$, $\mathfrak{c}$ is a finite intersection of irreducible ideals and therefore so is $\mathfrak{a}$: contradiction. ■

Lemma 7.12. *In a Noetherian ring every irreducible ideal is primary.*

Proof. By passing to the quotient ring, it is enough to show that if the zero ideal is irreducible then it is primary. Let $xy = 0$ with $y \neq 0$, and consider the chain of ideals $\mathrm{Ann}(x) \subseteq \mathrm{Ann}(x^2) \subseteq \cdots$. By the a.c.c., this chain is stationary, i.e., we have $\mathrm{Ann}(x^n) = \mathrm{Ann}(x^{n+1}) = \cdots$ for some n. It follows that $(x^n) \cap (y) = 0$; for if $a \in (y)$ then $ax = 0$, and if $a \in (x^n)$ then $a = bx^n$, hence $bx^{n+1} = 0$, hence $b \in \mathrm{Ann}(x^{n+1}) = \mathrm{Ann}(x^n)$, hence $bx^n = 0$; that is, $a = 0$. Since (0) is irreducible and $(y) \neq 0$ we must therefore have $x^n = 0$, and this shows that (0) is primary. ■

From these two lemmas we have at once

Theorem 7.13. *In a Noetherian ring A every ideal has a primary decomposition.* ■

Hence all the results of Chapter 4 apply to Noetherian rings.

Proposition 7.14. *In a Noetherian ring A, every ideal $\mathfrak{a}$ contains a power of its radical.*

Proof. Let $x_1, \ldots, x_k$ generate $r(\mathfrak{a})$: say $x_i^{n_i} \in \mathfrak{a}$ $(1 \leqslant i \leqslant k)$. Let $m = \sum_{i=1}^{k} (n_i - 1) + 1$. Then $r(\mathfrak{a})^m$ is generated by the products $x_1^{r_1} \cdots x_k^{r_k}$ with $\sum r_i = m$; from the definition of m we must have $r_i \geqslant n_i$ for at least one index i, hence each such monomial lies in $\mathfrak{a}$, and therefore $r(\mathfrak{a})^m \subseteq \mathfrak{a}$. ■

Corollary 7.15. *In a Noetherian ring the nilradical is nilpotent.*

Proof. Take $\mathfrak{a} = (0)$ in (7.14). ■

Corollary 7.16. *Let A be a Noetherian ring, $\mathfrak{m}$ a maximal ideal of A, $\mathfrak{q}$ any ideal of A. Then the following are equivalent:*

i) *$\mathfrak{q}$ is $\mathfrak{m}$-primary;*

ii) *$r(\mathfrak{q}) = \mathfrak{m}$;*

iii) *$\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ for some $n > 0$.*

Proof. i) $\Rightarrow$ ii) is clear; ii) $\Rightarrow$ i) from (4.2); ii) $\Rightarrow$ iii) from (7.14); iii) $\Rightarrow$ ii) by taking radicals: $\mathfrak{m} = r(\mathfrak{m}^n) \subseteq r(\mathfrak{q}) \subseteq r(\mathfrak{m}) = \mathfrak{m}$. ■

Proposition 7.17. *Let $\mathfrak{a} \neq (1)$ be an ideal in a Noetherian ring. Then the prime ideals which belong to $\mathfrak{a}$ are precisely the prime ideals which occur in the set of ideals $(\mathfrak{a}:x)$ $(x \in A)$.*

Proof. By passing to $A/\mathfrak{a}$ we may assume that $\mathfrak{a} = 0$. Let $\bigcap_{i=1}^{n} \mathfrak{q}_i = 0$ be a minimal primary decomposition of the zero ideal, and let $\mathfrak{p}_i$ be the radical of $\mathfrak{q}_i$.

Let $\mathfrak{a}_i = \bigcap_{j \neq i} \mathfrak{q}_j \neq 0$. Then from the proof of (4.5) we have $r(\mathrm{Ann}(x)) = \mathfrak{p}_i$ for any $x \neq 0$ in $\mathfrak{a}_i$, so that $\mathrm{Ann}(x) \subseteq \mathfrak{p}_i$.

Since $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary, by (7.14) there exists an integer m such that $\mathfrak{p}_i^m \subseteq \mathfrak{q}_i$, and therefore $\mathfrak{a}_i\mathfrak{p}_i^m \subseteq \mathfrak{a}_i \cap \mathfrak{p}_i^m \subseteq \mathfrak{a}_i \cap \mathfrak{q}_i = 0$. Let $m \geqslant 1$ be the smallest integer such that $\mathfrak{a}_i\mathfrak{p}_i^m = 0$, and let x be a non-zero element in $\mathfrak{a}_i\mathfrak{p}_i^{m-1}$. Then $\mathfrak{p}_i x = 0$, therefore for such an x we have $\mathrm{Ann}(x) \supseteq \mathfrak{p}_i$, and hence $\mathrm{Ann}(x) = \mathfrak{p}_i$.

Conversely, if $\mathrm{Ann}(x)$ is a prime ideal $\mathfrak{p}$, then $r(\mathrm{Ann}(x)) = \mathfrak{p}$ and so by (4.5) $\mathfrak{p}$ is a prime ideal belonging to 0. ∎

EXERCISES

1. Let A be a non-Noetherian ring and let Σ be the set of ideals in A which are not finitely generated. Show that Σ has maximal elements and that the maximal elements of Σ are prime ideals.
   [Let $\mathfrak{a}$ be a maximal element of Σ, and suppose that there exist $x, y \in A$ such that $x \notin \mathfrak{a}$ and $y \notin \mathfrak{a}$ and $xy \in \mathfrak{a}$. Show that there exists a finitely generated ideal $\mathfrak{a}_0 \subseteq \mathfrak{a}$ such that $\mathfrak{a}_0 + (x) = \mathfrak{a} + (x)$, and that $\mathfrak{a} = \mathfrak{a}_0 + x\cdot(\mathfrak{a}:x)$. Since $(\mathfrak{a}:x)$ strictly contains $\mathfrak{a}$, it is finitely generated and therefore so is $\mathfrak{a}$.]
   Hence a ring in which every prime ideal is finitely generated is Noetherian (I. S. Cohen).

2. Let A be a Noetherian ring and let $f = \sum_{n=0}^{\infty} a_n x^n \in A[[x]]$. Prove that f is nilpotent if and only if each a_n is nilpotent.

3. Let $\mathfrak{a}$ be an irreducible ideal in a ring A. Then the following are equivalent:
   i) $\mathfrak{a}$ is primary;
   ii) for every multiplicatively closed subset S of A we have $(S^{-1}\mathfrak{a})^c = (\mathfrak{a}:x)$ for some $x \in S$;
   iii) the sequence $(\mathfrak{a}:x^n)$ is stationary, for every $x \in A$.

4. Which of the following rings are Noetherian?
   i) The ring of rational functions of z having no pole on the circle $|z| = 1$.
   ii) The ring of power series in z with a positive radius of convergence.
   iii) The ring of power series in z with an infinite radius of convergence.
   iv) The ring of polynomials in z whose first k derivatives vanish at the origin (k being a fixed integer).
   v) The ring of polynomials in z, w all of whose partial derivatives with respect to w vanish for $z = 0$.
   In all cases the coefficients are complex numbers.

5. Let A be a Noetherian ring, B a finitely generated A-algebra, G a finite group of A-automorphisms of B, and B^G the set of all elements of B which are left fixed by every element of G. Show that B^G is a finitely generated A-algebra.

6. If a finitely generated ring K is a field, it is a finite field.
   [If K has characteristic 0, we have $\mathbf{Z} \subset \mathbf{Q} \subseteq K$. Since K is finitely generated over $\mathbf{Z}$ it is finitely generated over $\mathbf{Q}$, hence by (7.9) is a finitely generated $\mathbf{Q}$-