be irreducible since it is the intersection of the ideals $(x) + (x, y)^2 = (x, y^2)$ and $(y)+(x, y)^2 = (y, x^2)$. In a Noetherian ring, however, irreducible ideals are necessarily primary:

Proposition 20. Let R be a Noetherian ring. Then

(1) every irreducible ideal is primary, and

(2) every proper ideal in R is a finite intersection of irreducible ideals.

Proof: To prove (1) let Q be an irreducible ideal and suppose that $ab \in Q$ and $b \notin Q$. It is easy to check that for any fixed n the set of elements $x \in R$ with $a^n x \in Q$ is an ideal, A_n, in R. Clearly $A_1 \subseteq A_2 \subseteq \dots$ and since R is Noetherian this ascending chain of ideals must stabilize, i.e., $A_n = A_{n+1} = \dots$ for some $n > 0$. Consider the two ideals $I = (a^n) + Q$ and $J = (b) + Q$ of R, each containing Q. If $y \in I \cap J$ then $y = a^n z + q$ for some $z \in R$ and $q \in Q$. Since $ab \in Q$, it follows that $aJ \subseteq Q$, and in particular $ay \in Q$. Then $a^{n+1}z = ay - aq \in Q$, so $z \in A_{n+1} = A_n$. But $z \in A_n$ means that $a^n z \in Q$, so $y \in Q$. It follows that $I \cap J = Q$. Since Q is irreducible and $(b) + Q \neq Q$ (since $b \notin Q$), we must have $a^n \in Q$, which shows that Q is primary.

The proof of (2) is the same as the proof of the second statement in Proposition 17. Let $\mathcal{S}$ be the collection of ideals of R that cannot be written as a finite intersection of irreducible ideals. If $\mathcal{S}$ is not empty, then since R is Noetherian, there is a maximal element I in $\mathcal{S}$. Then I is not itself irreducible, so $I = J \cap K$ for some ideals J and K distinct from I. Then $I \subset J$ and $I \subset K$ and the maximality of I implies that neither J nor K is in $\mathcal{S}$. But this means that both J and K can be written as finite intersections of irreducible ideals, hence the same would be true for I. This is a contradiction, so $\mathcal{S} = \emptyset$, which completes the proof of the proposition.

It is immediate from the previous proposition that in a Noetherian ring every proper ideal has a primary decomposition. If any of the primary ideals in this decomposition contains the intersection of the remaining primary ideals, then we may simply remove this ideal since this will not change the intersection. Hence we may assume the decomposition satisfies (a) in the definition of a minimal decomposition. Since a finite intersection of P-primary ideals is again P-primary (Exercise 31), replacing the primary ideals in the decomposition with the intersections of all those primary ideals belonging to the same prime, we may also assume the decomposition satisfies (b) in the definition of a minimal decomposition. This proves the first statement of the following:

Theorem 21. *(Primary Decomposition Theorem)* Let R be a Noetherian ring. Then every proper ideal I in R has a minimal primary decomposition. If

$$I = \bigcap_{i=1}^{m} Q_i = \bigcap_{i=1}^{n} Q'_i$$

are two minimal primary decompositions for I then the sets of associated primes in the two decompositions are the same:

$$\{\operatorname{rad} Q_1, \operatorname{rad} Q_2, \dots, \operatorname{rad} Q_m\} = \{\operatorname{rad} Q'_1, \operatorname{rad} Q'_2, \dots, \operatorname{rad} Q'_n\}.$$

Moreover, the primary components Q_i belonging to the minimal elements in this set of associated primes are uniquely determined by I.

Proof: The proof of the uniqueness of the set of associated primes is outlined in the exercises, and the proof of the uniqueness of the primary components associated to the minimal primes will be given in Section 4.

Definition. If I is an ideal in the Noetherian ring R then the associated prime ideals in any primary decomposition of I are called the *associated prime ideals of* I. If an associated prime ideal P of I does not contain any other associated prime ideal of I then P is called an *isolated prime ideal*; the remaining associated prime ideals of I are called *embedded prime ideals*.

The prime ideals associated to an ideal I provide a great deal of information about the ideal I (cf. for example Exercises 41 and 43):

Corollary 22. Let I be a proper ideal in the Noetherian ring R.

(1) A prime ideal P contains the ideal I if and only if P contains one of the associated primes of I, hence if and only if P contains one of the isolated primes of I, i.e., the isolated primes of I are precisely the minimal elements in the set of all prime ideals containing I. In particular, there are only finitely many minimal elements among the prime ideals containing I.

(2) The radical of I is the intersection of the associated primes of I, hence also the intersection of the isolated primes of I.

(3) There are prime ideals $P_1, \dots, P_n$ (not necessarily distinct) containing I such that $P_1 P_2 \cdots P_n \subseteq I$.

Proof: The first statement in (1) is an exercise (cf. Exercise 37), and the remainder of (1) follows. Then (2) follows from (1) and Proposition 12, and (3) follows from (2) and Proposition 14.

The last statement in Theorem 21 states that not only the isolated primes, but also the primary components belonging to the isolated primes, are uniquely determined by I. In general the primary decomposition of an ideal I is itself not unique.

Examples

(1) Let $I = (x^2, xy)$ in $\mathbb{R}[x, y]$. Then

$$(x^2, xy) = (x) \cap (x, y)^2 = (x) \cap (x^2, y)$$

are two minimal primary decompositions for I. The associated primes for I are (x) and $\operatorname{rad}((x, y)^2) = \operatorname{rad}((x^2, y)) = (x, y)$. The prime (x) is the only isolated prime since $(x) \subset (x, y)$, and (x, y) is an embedded prime. A prime ideal P contains I if and only if P contains (x). The (x)-primary component of I corresponding to this isolated prime is just (x) and occurs in both primary decompositions; the (x, y)-primary component of I corresponding to this embedded prime is not uniquely determined — it is $(x, y)^2$ in the first decomposition and is (x^2, y) in the second. The radical of I is the isolated prime (x).

This example illustrates the origin of the terminology: in general the irreducible components of the algebraic space $\mathcal{Z}(I)$ defined by I are the zero sets of the isolated primes for I, and the zero sets of the embedded primes are irreducible subspaces of these components (so are "embedded" in the irreducible components). In this example, $\mathcal{Z}(I)$ is the set of points with $x^2 = xy = 0$, which is just the y-axis in $\mathbb{R}^2$. There is only one irreducible component of this algebraic space (namely the y-axis), which is the locus for the isolated prime (x). The locus for the embedded prime (x, y) is the origin (0. 0), which is an irreducible subspace embedded in the y-axis.

(2) Suppose R is a U.F.D. If $a = p_1{}^{e_1} \cdots p_m{}^{e_m}$ is the unique factorization into distinct prime powers of the element $a \in R$, then $(a) = (p_1)^{e_1} \cap \cdots \cap (p_m)^{e_m}$ is the minimal primary decomposition of the principal ideal (a). The associated primes to (a) are $(p_1), \ldots, (p_m)$ and are all isolated. The primary decomposition of ideals is a generalization of the factorization of elements into prime powers. See also Exercise 44 for a characterization of U.F.D.s in terms of minimal primary decompositions.

For any Noetherian ring, an ideal I is radical if and only if the primary components of a minimal primary decomposition of I are all *prime* ideals (in which case this primary decomposition is unique), cf. Exercise 43. This generalizes the observation made previously that Proposition 17 together with Hilbert's Nullstellensatz shows that any radical ideal in $k[\mathbb{A}^n]$ may be written uniquely as a finite intersection of prime ideals when the field k is algebraically closed — this is the algebraic statement that an algebraic set can be decomposed uniquely into the union of irreducible algebraic sets.

EXERCISES

1. Prove (3) of Corollary 22 directly by considering the collection $\mathcal{S}$ of ideals that do not contain a finite product of prime ideals. [If I is a maximal element in $\mathcal{S}$, show that since I is not prime there are ideals J, K properly containing I (hence not in $\mathcal{S}$) with $JK \subseteq I$.]

2. Let I and J be ideals in the ring R. Prove the following statements:

(a) If $I^k \subseteq J$ for some $k \geq 1$ then $\operatorname{rad} I \subseteq \operatorname{rad} J$.

(b) If $I^k \subseteq J \subseteq I$ for some $k \geq 1$ then $\operatorname{rad} I = \operatorname{rad} J$.

(c) $\operatorname{rad}(IJ) = \operatorname{rad}(I \cap J) = \operatorname{rad} I \cap \operatorname{rad} J$.

(d) $\operatorname{rad}(\operatorname{rad} I) = \operatorname{rad} I$.

(e) $\operatorname{rad} I + \operatorname{rad} J \subseteq \operatorname{rad}(I + J)$ and $\operatorname{rad}(I + J) = \operatorname{rad}(\operatorname{rad} I + \operatorname{rad} J)$.

3. Prove that the intersection of two radical ideals is again a radical ideal.

4. Let $I = \mathfrak{m}_1\mathfrak{m}_2$ be the product of the ideals $\mathfrak{m}_1 = (x, y)$ and $\mathfrak{m}_2 = (x-1, y-1)$ in $\mathbb{F}_2[x, y]$. Prove that I is a radical ideal. Prove that the ideal $(x^3 - y^2)$ is a radical ideal in $\mathbb{F}_2[x, y]$.

5. If $I = (xy, (x - y)z) \subset k[x, y, z]$ prove that $\operatorname{rad} I = (xy, xz, yz)$. For this ideal prove directly that $\mathcal{Z}(I) = \mathcal{Z}(\operatorname{rad} I)$, that $\mathcal{Z}(I)$ is not irreducible, and that $\operatorname{rad} I$ is not prime.

6. Give an example to show that over a field k that is not algebraically closed the containment $I \subseteq \mathcal{I}(\mathcal{Z}(I))$ can be proper even when I is a radical ideal.

7. Suppose R and S are rings and $\varphi : R \to S$ is a ring homomorphism. If I is an ideal of R show that $\varphi(\operatorname{rad} I) \subseteq \operatorname{rad}(\varphi(I))$. If in addition φ is surjective and I contains the kernel of φ show that $\varphi(\operatorname{rad} I) = \operatorname{rad}(\varphi(I))$.

8. Suppose the prime ideal P contains the ideal I. Prove that P contains the radical of I.

9. Prove that for any field k the map $\mathcal{Z}$ in the Nullstellensatz is always surjective and the map $\mathcal{I}$ in the Nullstellensatz is always injective. [Use property (10) of the maps $\mathcal{Z}$ and $\mathcal{I}$ in Section 1.] Give examples (over a field k that is not algebraically closed) where $\mathcal{Z}$ is not injective and $\mathcal{I}$ is not surjective.