an element $r \in R$, $r \notin P$ with $rm = 0$. Deduce that $P \in \text{Supp}(M)$ if and only if P contains the annihilator of m in R (cf. Exercise 10 in Section 10.1).

(b) If $M = Rm_1 + \cdots + Rm_n$ is a finitely generated R-module prove that $P \in \text{Supp}(M)$ if and only if P is contained in $\text{Supp}(Rm_i)$ for some $i = 1, \ldots, n$. [Use Proposition 42.] Deduce that $P \in \text{Supp}(M)$ if and only if P contains the annihilator $\text{Ann}(M)$ of M in R. [Note $\text{Ann}(M) = \cap_{i=1}^{n} \text{Ann}(Rm_i)$, then use (a) and Exercise 11 of Section 7.4.]

35. Suppose P is a prime ideal of R with $P \cap D = \emptyset$. Prove that if $P \in \text{Ass}_R(M)$ then $D^{-1}P \in \text{Ass}_{D^{-1}R}(D^{-1}M)$. [Use Proposition 38(3) and Proposition 42.]

36. Suppose $D^{-1}P \in \text{Ass}_{D^{-1}R}(D^{-1}M)$ where $P = (a_1, \ldots, a_n)$ is a finitely generated prime ideal in R with $P \cap D = \emptyset$.

(a) Suppose $m/d \in D^{-1}M$ has annihilator $D^{-1}P$ in $D^{-1}R$. Show that $d_i a_i m = 0 \in R$ for some $d_1, \ldots, d_n \in D$.

(b) Let $d' = d_1 d_2 \ldots d_n$. Show that $P = \text{Ann}(d'm)$ and conclude that $P \in \text{Ass}_R(M)$. [The inclusion $P \subseteq \text{Ann}(d'm)$ is immediate. For the reverse inclusion, show that $b \in \text{Ann}(d'm)$ implies that $b/1$ annihilates m/d in $D^{-1}M$, hence $b/1 \in D^{-1}P$, and conclude $b \in P$.]

37. Suppose M is a module over the Noetherian ring R. Use the previous two exercises to show that under the bijection of Proposition 38(3) the prime ideals P of $\text{Ass}_R(M)$ with $P \cap D = \emptyset$ correspond bijectively with the prime ideals of $\text{Ass}_{D^{-1}R}(D^{-1}M)$.

38. Suppose M is a module over the Noetherian ring R and D is a multiplicatively closed subset of R. Let $\mathcal{S}$ be the subset of prime ideals P in $\text{Ass}_R(M)$ with $P \cap D \neq \emptyset$. This exercise proves that the kernel N of the localization map $M \to D^{-1}M$ is the unique submodule N of M with $\text{Ass}_R(N) = \mathcal{S}$ and $\text{Ass}_R(M/N) = \text{Ass}_R(M) - \mathcal{S}$.

(a) If N' is a submodule of M with $\text{Ass}_R(N') = \mathcal{S}$ and $\text{Ass}_R(M/N') = \text{Ass}_R(M) - \mathcal{S}$ as in Exercise 35 in Section 1, prove that the diagram

$$\begin{array}{ccc} M & \xrightarrow{\pi} & M/N' \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi'} \\ D^{-1}M & \xrightarrow{\pi'} & D^{-1}(M/N') \end{array}$$

is commutative, where π and π' are the natural projections (cf. Proposition 42(6)) and φ, φ' are the localization homomorphisms.

(b) Show that $\text{Ass}_{D^{-1}R}(D^{-1}N') = \emptyset$ and conclude that $D^{-1}N' = 0$ and that π' is injective. [Use the previous exercise, the definition of $\mathcal{S}$, and Exercise 34 in Section 1.]

(c) If x is the kernel K of φ' show that $\text{Ann}(x) \cap D \neq \emptyset$ and that $\text{Ass}_R(K) \subseteq \mathcal{S}$. Show that $\text{Ass}_R(K) \subseteq \text{Ass}_R(M/N')$ implies that $\text{Ass}_R(K) = \emptyset$, and deduce that $K = 0$.

(d) Prove φ and π have the same kernel, i.e., $N = N'$, and this submodule of M is unique.

The next two exercises establish a fundamental relation between the sets $\text{Ass}_R(M)$ and $\text{Supp}(M)$ of prime ideals related to the R-module M.

39. Prove that $\text{Ass}_R(M) \subseteq \text{Supp}(M)$. [If $Rm \cong R/P$ use Proposition 42(4) and Proposition 46(1) to show that $0 \neq (Rm)_P \subseteq M_P$.]

40. Suppose that R is Noetherian and M is an R-module.

(a) If $P \in \text{Supp}(M)$ prove that P contains a prime ideal Q with $Q \in \text{Ass}_R(M)$.

(b) If P is a minimal prime in $\text{Supp}(M)$, show that $P \in \text{Ass}_R(M)$. [Use Exercise 33 in Section 1 to show that $\text{Ass}_{R_P}(M_P) \neq \emptyset$ and then use Exercise 37.]

(c) Conclude that $\text{Ass}_R(M) \subseteq \text{Supp}(M)$ and that these two sets have the same minimal elements.

15.5 THE PRIME SPECTRUM OF A RING

Throughout this section the term "ring" will mean commutative ring with 1 and all ring homomorphisms $\varphi : R \to S$ will be assumed to map 1_R to 1_S.

We have seen that most of the geometric properties of affine algebraic sets V over k can be translated into algebraic properties of the associated coordinate rings $k[V]$ of k-valued functions on V. For example, the morphisms from V to W correspond to k-algebra ring homomorphisms from $k[W]$ to $k[V]$. When the field k is an algebraically closed field this translation is particularly precise: Hilbert's Nullstellensatz establishes a bijection between the points v of V and the maximal ideals $M = \mathcal{I}(v)$ of $k[V]$, and if $\varphi : V \to W$ is a morphism then $\varphi(v) \in W$ corresponds to the maximal ideal $\widetilde{\varphi}^{-1}(M)$ in $k[W]$. In this development we have generally started with geometric properties of the affine algebraic sets and then seen that many of the algebraic properties common to the associated coordinate rings can be defined for arbitrary commutative rings. Suppose now we try to reverse this, namely start with a general commutative ring as the algebraic object and attempt to define a corresponding "geometric" object by analogy with $k[V]$ and V.

Given a commutative ring R, perhaps the most natural analogy with $k[V]$ and V would suggest defining the collection of maximal ideals M of R as the "points" of the associated geometric object. Under this definition, if $\widetilde{\varphi} : R' \to R$ is a ring homomorphism, then $\widetilde{\varphi}^{-1}(M)$ should correspond to the maximal ideal M. Unfortunately, the inverse image of a maximal ideal by a ring homomorphism in general need not be a maximal ideal. Since the inverse image of a *prime* ideal under a ring homomorphism (that maps 1 to 1) *is* prime, this suggests that a better definition might include the prime ideals of R. This leads to the following:

Definition. Let R be a commutative ring with 1. The *spectrum* or *prime spectrum* of R, denoted Spec R, is the set of all prime ideals of R. The set of all maximal ideals of R, denoted mSpec R, is called the *maximal spectrum* of R.

Examples

(1) If R is a field then $\operatorname{Spec} R = \operatorname{mSpec} R = \{(0)\}$.

(2) The points in $\operatorname{Spec}\mathbb{Z}$ are the prime ideal (0) and the prime ideals (p) where $p > 0$ is a prime, and $\operatorname{mSpec}\mathbb{Z}$ consists of all the prime ideals of $\operatorname{Spec}\mathbb{Z}$ except (0).

(3) The elements of $\operatorname{Spec}\mathbb{Z}[x]$ are the following:

- **(a)** (0)
- **(b)** (p) where p is a prime in $\mathbb{Z}$
- **(c)** (f) where $f \neq 1$ is a polynomial of content 1 (i.e., the g.c.d. of its coefficients is equal to 1) that is irreducible in $\mathbb{Q}[x]$
- **(d)** (p, g) where p is a prime in $\mathbb{Z}$ and g is a monic polynomial that is irreducible mod p.

The elements of $\operatorname{mSpec}\mathbb{Z}[x]$ are the primes in (d) above.

In the analogy with $k[V]$ and V when k is algebraically closed, the elements $f \in k[V]$ are functions on V with values in k, obtained by evaluating f at the point v in V. Note that "evaluation at v" defines a homomorphism from $k[V]$ to k with kernel $\mathcal{I}(v)$, and that the value of f at v is the element of k representing f in the quotient

$k[V]/\mathcal{I}(v) \cong k$. Put another way, the value of $f \in k[V]$ at $v \in V$ can be viewed as the element $\bar{f} \in k[V]/\mathcal{I}(v) \cong k$. A similar definition can be made in general:

Definition. If $f \in R$ then the *value* of f at the point $P \in \operatorname{Spec} R$ is the element $f(P) = \bar{f} \in R/P$.

Note that the values of f at different points P in general lie in *different* integral domains. Note also that in general $f \in R$ is not uniquely determined by its values, rather f is determined only up to an element in the nilradical of R (cf. Exercise 3).

There are analogues of the maps $\mathcal{Z}$ and $\mathcal{I}$ and also for the Zariski topology. For any subset A of R define

$$\mathcal{Z}(A) = \{P \in X \mid A \subseteq P\} \subseteq \operatorname{Spec} R,$$

the collection of prime ideals containing A. It is immediate that $\mathcal{Z}(A) = \mathcal{Z}(I)$, where $I = (A)$ is the ideal generated by A so there is no loss simply in considering $\mathcal{Z}(I)$ where I is an ideal of R. Note that, by definition, $P \in \mathcal{Z}(I)$ if and only if $I \subseteq P$, which occurs if and only if $f \in P$ for every $f \in I$. Viewing $f \in R$ as a function on $\operatorname{Spec} R$ as above, this says that $P \in \mathcal{Z}(I)$ if and only if $f(P) = f \bmod P = 0 \in R/P$ for all $f \in I$. In this sense, $\mathcal{Z}(I)$ consists of the points in $\operatorname{Spec} R$ at which all the functions in I have the value 0.

For any subset Y of $\operatorname{Spec} R$ define

$$\mathcal{I}(Y) = \bigcap_{P \in Y} P,$$

the intersection of the prime ideals in Y.

Proposition 53. Let R be a commutative ring with 1. The maps $\mathcal{Z}$ and $\mathcal{I}$ between R and $\operatorname{Spec} R$ defined above satisfy

(1) for any ideal I of R, $\mathcal{Z}(I) = \mathcal{Z}(\operatorname{rad}(I)) = \mathcal{Z}(\mathcal{I}(\mathcal{Z}(I)))$, and $\mathcal{I}(\mathcal{Z}(I)) = \operatorname{rad} I$,
(2) for any ideals I, J of R, $\mathcal{Z}(I \cap J) = \mathcal{Z}(IJ) = \mathcal{Z}(I) \cup \mathcal{Z}(J)$, and
(3) if $\{I_j\}$ is an arbitrary collection of ideals of R, then $\mathcal{Z}(\cup I_j) = \cap \mathcal{Z}(I_j)$.

Proof: If P is a prime ideal containing the ideal I then P contains $\operatorname{rad} I$ (Exercise 8, Section 2), which implies $\mathcal{Z}(I) = \mathcal{Z}(\operatorname{rad}(I))$. Since $\operatorname{rad} I$ is the intersection of all the prime ideals containing I (Proposition 12), the definition of $\mathcal{I}(I)$ gives $\mathcal{Z}(\operatorname{rad}(I)) = \mathcal{Z}(\mathcal{I}(I))$. Similarly,

$$\mathcal{I}(\mathcal{Z}(I)) = \bigcap_{P \in \mathcal{Z}(I)} P = \bigcap_{I \subseteq P} P = \operatorname{rad} I,$$

which completes the proof of (1). It is immediate that $\mathcal{Z}(I \cap J) = \mathcal{Z}(I) \cup \mathcal{Z}(J)$. Suppose the prime ideal P contains IJ. If P does not contain I then there is some element $i \in I$ with $i \notin P$. Since $iJ \subseteq P$, it follows that $J \subseteq P$. This proves $\mathcal{Z}(IJ) = \mathcal{Z}(I) \cup \mathcal{Z}(J)$ and completes the proof of (2). The proof of (3) is immediate.

The first statement in the proposition shows that every set $\mathcal{Z}(I)$ in $\operatorname{Spec} R$ occurs for some *radical* ideal I, and since $\mathcal{I}(\mathcal{Z}(I)) = \operatorname{rad} I$, this radical ideal is unique.