(a) Prove that if the collection of ideals of R that are not finitely generated is nonempty, then it contains a maximal element I, and that R/I is a Noetherian ring.

(b) Prove that there are finitely generated ideals J_1 and J_2 containing I with $J_1 J_2 \subseteq I$ and that $J_1 J_2$ is finitely generated. [Observe that I is not a prime ideal.]

(c) Prove that $I/J_1 J_2$ is a finitely generated R/I-submodule of $J_1/J_1 J_2$. [Use Exercise 8.]

(d) Show that (c) implies the contradiction that I would be finitely generated over R and deduce that R is Noetherian.

12. Suppose R is a Noetherian ring and S is a finitely generated R-algebra. If $T \subseteq S$ is an R-algebra such that S is a finitely generated T-*module*, prove that T is a finitely generated R-algebra. [If $s_1, \dots, s_n$ generate S as an R-algebra, and $s'_1, \dots, s'_m$ generate S as a T-module, show that the elements s_i and $s'_j s'_k$ can be written as finite T-linear combinations of the s'_i. If T_0 is the R-subalgebra generated by the coefficients of these linear combinations, show S (hence T_0) is finitely generated (by the s'_i) as a T_0-module, and conclude that T is finitely generated as an R-algebra.]

13. Verify properties (1) to (10) of the maps $\mathcal{Z}$ and $\mathcal{I}$.

14. Show that the affine algebraic sets in $\mathbb{A}^1$ over any field k are $\emptyset$, k, and finite subsets of k.

15. If $k = \mathbb{F}_2$ and $V = \{(0,0), (1,1)\} \subset \mathbb{A}^2$, show that $\mathcal{I}(V)$ is the product ideal $\mathfrak{m}_1\mathfrak{m}_2$ where $\mathfrak{m}_1 = (x, y)$ and $\mathfrak{m}_2 = (x-1, y-1)$.

16. Suppose that V is a finite algebraic set in $\mathbb{A}^n$. If V has m points, prove that $k[V]$ is isomorphic as a k-algebra to k^m. [Use the Chinese Remainder Theorem.]

17. If k is a finite field show that every subset of $\mathbb{A}^n$ is an affine algebraic set.

18. If $k = \mathbb{F}_q$ is the finite field with q elements show that $\mathcal{I}(\mathbb{A}^1) = (x^q - x) \subset k[x]$.

19. For each nonconstant $f \in k[x]$ describe $\mathcal{Z}(f) \subseteq \mathbb{A}^1$ in terms of the unique factorization of f in $k[x]$, and then use this to describe $\mathcal{I}(\mathcal{Z}(f))$. Deduce that $\mathcal{I}(\mathcal{Z}(f)) = (f)$ if and only if f is the product of distinct linear factors in $k[x]$.

20. If f and g are irreducible polynomials in $k[x, y]$ that are not associates (do not divide each other), show that $\mathcal{Z}((f, g))$ is either $\emptyset$ or a finite set in $\mathbb{A}^2$. [If $(f, g) \neq (1)$, show (f, g) contains a nonzero polynomial in $k[x]$ (and similarly a nonzero polynomial in $k[y]$) by letting $R = k[x]$, $F = k(x)$, and applying Gauss's Lemma to show f and g are relatively prime in $F[y]$.]

21. Identify each 2×2 matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with entries from k with the point (a, b, c, d) in $\mathbb{A}^4$. Show that the group $SL_2(k)$ of matrices of determinant 1 is an algebraic set in $\mathbb{A}^4$.

22. Prove that $SL_n(k)$ is an affine algebraic set in $\mathbb{A}^{n^2}$. [Generalize the preceding exercise.]

23. Let V be any line in $\mathbb{R}^2$ (the zero set of any nonzero linear polynomial $ax + by - c$). Prove that $\mathbb{R}[V]$ is isomorphic as an $\mathbb{R}$-algebra to the polynomial ring $\mathbb{R}[x]$, and give the corresponding isomorphism from $\mathbb{A}^1$ to V.

24. Let $V = \mathcal{Z}(xy - z) \subseteq \mathbb{A}^3$. Prove that V is isomorphic to $\mathbb{A}^2$ and provide an explicit isomorphism φ and associated k-algebra isomorphism $\widetilde{\varphi}$ from $k[V]$ to $k[\mathbb{A}^2]$, along with their inverses. Is $V = \mathcal{Z}(xy - z^2)$ isomorphic to $\mathbb{A}^2$?

25. Suppose $V \subseteq \mathbb{A}^n$ is an affine algebraic set and $f \in k[V]$. The *graph* of f is the collection of points $\{(a_1, \dots, a_n, f(a_1, \dots, a_n))\}$ in $\mathbb{A}^{n+1}$. Prove that the graph of f is an affine algebraic set isomorphic to V. [The morphism in one direction maps $(a_1, \dots, a_n)$ to $(a_1, \dots, a_n, f(a_1, \dots, a_n))$.]

26. Let $V = \mathcal{Z}(xz - y^2, yz - x^3, z^2 - x^2y) \subseteq \mathbb{A}^3$.

(a) Prove that the map $\varphi : \mathbb{A}^1 \to V$ defined by $\varphi(t) = (t^3, t^4, t^5)$ is a surjective morphism. [For the surjectivity, if $(x, y, z) \neq (0, 0, 0)$, let $t = y/x$.]

(b) Describe the corresponding k-algebra homomorphism $\widetilde{\varphi} : k[V] \to k[\mathbb{A}^1]$ explicitly.

(c) Prove that φ is not an isomorphism.

27. Suppose $\varphi : V \to W$ is a morphism of affine algebraic sets. If W' is an affine algebraic subset of W prove that the preimage $V' = \varphi^{-1}(W')$ of W' in V is an affine algebraic subset of V. If $W' = \mathcal{Z}(I)$ show that $V' = \mathcal{Z}(\widetilde{\varphi}(I))$ for the corresponding morphism $\widetilde{\varphi} : k[W] \to k[V]$.

28. Prove that if V and W are affine algebraic sets, then so is $V \times W$ and $k[V \times W] \cong k[V] \otimes_k k[W]$.

The following seven exercises introduce the notion of the *associated primes* of an R-module M. Cf. also Exercises 30–40 in Section 4 and Exercises 25–30 in Section 5.

Definition. A prime ideal P of R is said to be *associated* to the R-module M (sometimes called an *assassin* for M) if P is the annihilator of some element m of M, i.e., if M contains a submodule Rm isomorphic to R/P. The collection of associated primes for M is denoted $\mathrm{Ass}_R(M)$.

When $M = I$ is an ideal in R, it is customary to abuse the terminology and refer instead to the elements of $\mathrm{Ass}_R(R/I)$ (rather than the less interesting collection $\mathrm{Ass}_R(I)$) as the *primes associated to* I. (Cf. Exercises 28–29 in Section 5.)

29. If $R = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$, show that $\mathrm{Ass}_R(M)$ consists of the prime ideals (p) for the prime divisors p of n.

30. If M is the union of some collection of submodules M_i, prove that $\mathrm{Ass}_R(M)$ is the union of the collection $\mathrm{Ass}_R(M_i)$.

31. Suppose that $\mathrm{Ann}(m) = P$, i.e., that $Rm \cong R/P$. Prove that if $0 \neq m' \in Rm$ then $\mathrm{Ann}(m') = P$. Deduce that $\mathrm{Ass}_R(R/P) = \{P\}$. [Observe that R/P is an integral domain.]

32. Suppose that M is an R-module and that P is a maximal element in the collection of ideals of the form $\mathrm{Ann}(m)$, for $m \in M$. Prove that P is a prime ideal. [If $P = \mathrm{Ann}(m)$ and $ab \in P$, show that $bm \neq 0$ implies $\mathrm{Ann}(m) \subseteq \mathrm{Ann}(bm)$ and use the maximality of P to deduce that $a \in \mathrm{Ann}(bm) = P$.]

33. Suppose R is a Noetherian ring and $M \neq 0$ is an R-module. Prove that $\mathrm{Ass}_R(M) \neq \emptyset$. [Use Exercise 32.]

34. If L is a submodule of M with quotient $N \cong M/L$, prove that there are containments $\mathrm{Ass}_R(N) \subseteq \mathrm{Ass}_R(M) \subseteq \mathrm{Ass}_R(L) \cup \mathrm{Ass}_R(N)$, and show that both containments can be proper. [If $Rm \cong R/P$, show that $Rm \cap L = 0$ implies $P \in \mathrm{Ass}_R(N)$ and if $Rm \cap L \neq 0$ then $P \in \mathrm{Ass}_R(L)$ (by Exercise 31). For the second statement, consider $n\mathbb{Z} \subset \mathbb{Z}$.]

35. Suppose M is an R-module and let $\mathcal{S}$ be a subset of the prime ideals in $\mathrm{Ass}_R(M)$. Prove there is a submodule N of M with $\mathrm{Ass}_R(N) = \mathcal{S}$ and $\mathrm{Ass}_R(M/N) = \mathrm{Ass}_R(M) - \mathcal{S}$. [Consider the collection of submodules N' of M with $\mathrm{Ass}_R(N') \subseteq \mathcal{S}$. Use Exercise 30 and Zorn's Lemma to show that there is a maximal submodule N subject to $\mathrm{Ass}_R(N) \subseteq \mathcal{S}$. If $P \in \mathrm{Ass}_R(M/N)$, there is a submodule $M'/N \cong R/P$. Use the previous exercise to show that $\mathrm{Ass}_R(M') \subseteq \mathrm{Ass}_R(N) \cup \{P\}$ and then use maximality of N to show $P \in \mathrm{Ass}_R(M) - \mathcal{S}$, so that $\mathrm{Ass}_R(M/N) \subseteq \mathrm{Ass}_R(M) - \mathcal{S}$ and $\mathrm{Ass}_R(N) \subseteq \mathcal{S}$. Use the previous exercise again to conclude that equality holds in each.]

Suppose M is a finitely generated module over the commutative ring R with generators $m_1, \ldots, m_n$. The *Fitting ideal* $\mathcal{F}_R(M)$ (of level 0) of M (also called a *determinant ideal*) is the ideal in R generated by the determinants of all $n \times n$ matrices $A = (r_{ij})$ where $r_{ij} \in R$ and $r_{i1}m_1 + \cdots + r_{in}m_n = 0$ in M, i.e., the rows of A consist of the coefficients in R of relations among the generators m_i (A is called an $n \times n$ "relations matrix" for M). The following five exercises outline some of the properties of the Fitting ideal.

36. **(a)** Show that the Fitting ideal of M is also the ideal in R generated by all the $n \times n$ minors of all $p \times n$ matrices $A = (r_{ij})$ for $p \geq 1$ whose rows consist of the coefficients in R of relations among the generators m_i.

(b) Let A be a fixed $p \times n$ matrix as in (a) and let A' be a $p \times n$ matrix obtained from A by any elementary row or column operation. Show that the ideal in R generated by all the $n \times n$ minors of A is the same as the ideal in R generated by all the $n \times n$ minors of A'.

37. Suppose $m_1, \ldots, m_n$ and $m'_1, \ldots, m'_{n'}$ are two sets of R-module generators for M. Let $\mathcal{F}$ denote the Fitting ideal for M computed using the generators $m_1, \ldots, m_n$ and let $\mathcal{F}'$ denote the Fitting ideal for M computed using the generators $m_1, \ldots, m_n, m'_1, \ldots, m'_{n'}$.

(a) Show that $m'_s = a_{s'1}m_1 + \cdots + a_{s'n}m_n$ for some $a_{s'1}, \ldots, a_{s'n} \in R$, and deduce that $(-a_{s'1}, \ldots, -a_{s'n}, 0, \ldots, 0, 1, 0, \ldots 0)$ is a relation among $m_1, \ldots, m_n, m'_1, \ldots, m'_{n'}$.

(b) If $A = (r_{ij})$ is an $n \times n$ matrix whose rows are the coefficients of relations among $m_1, \ldots, m_n$ show that $\det A = \det A'$ where A' is an $(n+n') \times (n+n')$ matrix whose rows are the coefficients of relations among $m_1, \ldots, m_n, m'_1, \ldots m'_{n'}$. Deduce that $\mathcal{F} \subseteq \mathcal{F}'$. [Use (a) to find a block upper triangular A' having A in the upper left block and the $n' \times n'$ identity matrix in the lower right block.]

(c) Prove that $\mathcal{F}' \subseteq \mathcal{F}$ and conclude that $\mathcal{F}' = \mathcal{F}$. [Use the previous exercise.]

(d) Deduce from (c) that the Fitting ideal $\mathcal{F}_R(M)$ of M is an invariant of M that does not depend on the choice of generators for M used to compute it.

38. All modules in this exercise are assumed finitely generated.

(a) If M can be generated by n elements prove that $\mathrm{Ann}(M)^n \subseteq \mathcal{F}_R(M) \subseteq \mathrm{Ann}(M)$, where $\mathrm{Ann}(M)$ is the annihilator of M in R. [If A is an $n \times n$ relations matrix for M, then $AX = 0$, where X is the column matrix whose entries are $m_1, \ldots, m_n$. Multiply by the adjoint of A to deduce that $\det A$ annihilates M.]

(b) If $M = M_1 \times M_2$ is the direct product of the R-modules M_1 and M_2 prove that $\mathcal{F}_R(M) = \mathcal{F}_R(M_1)\mathcal{F}_R(M_2)$.

(c) If $M = (R/I_1) \times \cdots \times (R/I_n)$ is the direct product of cyclic R-modules for ideals I_i in R prove that $\mathcal{F}_R(M) = I_1 I_2 \ldots I_n$.

(d) If $R = \mathbb{Z}$ and M is a finitely generated abelian group show that $\mathcal{F}_{\mathbb{Z}}(M) = 0$ if M is infinite and $\mathcal{F}_{\mathbb{Z}}(M) = |M|\mathbb{Z}$ if M is finite.

(e) If I is an ideal in R prove that the image of $\mathcal{F}_R(M)$ in the quotient R/I is $\mathcal{F}_{R/I}(M/IM)$.

(f) Prove that $\mathcal{F}_R(M/IM) \subseteq (\mathcal{F}_R(M), I) \subseteq R$.

(g) If $\varphi : M \to M'$ is a surjective R-module homomorphism prove $\mathcal{F}_R(M) \subseteq \mathcal{F}_R(M')$.

(h) If $0 \to L \to M \to N \to 0$ is a short exact sequence of R-modules, prove that $\mathcal{F}_R(L)\mathcal{F}_R(N) \subseteq \mathcal{F}_R(M)$.

(i) Suppose R is the polynomial ring $k[x, y, z]$ over the field k. Let $M = R/(x, y^2, yz, z^2)$ and let L be the submodule $(x, y, z)/(x, y^2, yz, z^2)$ of M. Prove that $\mathcal{F}_R(M)$ is (x, y^2, yz, z^2) and $\mathcal{F}_R(L)$ is $(x, y, z)^2$. (This shows that in general the Fitting ideal of a submodule L of M need not contain the Fitting ideal for M.)

39. Suppose M is an R-module and that $\varphi : R^n \to M$ is a surjective R-module homomorphism (i.e., M can be generated by n elements). Let $L = \ker \varphi$. Prove that the image of the