

nents of a minimal primary decomposition are all prime ideals, and conclude that in this case the minimal primary decomposition is unique. [If $I = Q_1 \cap \cdots \cap Q_m$ is radical with Q_i a P_i -primary component of a minimal decomposition, show that if $a \in P_1 \cap \cdots \cap P_m$ then some power of a is in I , hence $a \in I$ since I is radical. Deduce that $I = P_1 \cap \cdots \cap P_m$ and show that this is also a minimal primary decomposition, i.e., for any i there exists b with $b \notin P_i$, but $b \in P_j$ for $j \neq i$. If $a \in P_i$, show that $ab \in Q_i$, and that $a \in Q_i$. Conclude that $Q_i = P_i$.]

44. Prove that a Noetherian integral domain R is a U.F.D. if and only if for every $a \in R$ the isolated primes associated to the principal ideal (a) are principal ideals. [See Example 2 following Corollary 22. To prove R is a U.F.D., show that an irreducible $a \in R$ is prime and then follow the proof of Theorem 14 in Section 8.3.]
45. Let R be the ring of all real valued functions on the open interval $(-1, 1)$ that have derivatives of all orders (the ring of C^∞ functions). Let

$$F(x) = \begin{cases} e^{-1/x^4} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

(you may assume $F \in R$ and $F^{(n)}(0) = 0$ for all $n \geq 0$). Let (F) be the principal ideal generated by F and let $A = \text{rad}((F))$. Let M be the (maximal) ideal of all functions in R that are zero at $x = 0$ and let $P = \bigcap_{n=1}^{\infty} M^n$.

- (a) Prove that $M = (x)$ is the ideal generated by the function x in R and that $M^n = (x^n)$ consists of the functions whose first $n - 1$ derivatives vanish at the origin.
- (b) Prove that R is not Noetherian (compare Exercise 33 in Section 7.4). [One approach is the following: Let $G(x)$ be the function that is 0 for $x < 0$ and is equal to $F(x)$ for $x \geq 0$. Let I_n be the ideal of functions in R vanishing for all $x \leq 1/n$. Use translates of $G(x)$ to show that $I_1 \subset I_2 \subset I_3 \subset \cdots$ is an infinite ascending chain.]
- (c) Prove that P consists of the functions all of whose derivatives are zero at $x = 0$ (i.e., the functions whose associated Taylor series at $x = 0$ is identically zero), and that P is a prime ideal.
- (d) Prove that $F \in P$ and deduce that $A \subseteq P$.
- (e) Prove that $A \neq P$. [Let $G(x) = e^{-1/x^2}$ when $x \neq 0$ and $G(0) = 0$. Show that $G \in P$ but $G \notin A$.]
- (f) Show that there is a prime ideal Q containing (F) with $Q \neq P, M$. Prove that $Q \subset P$ i.e., there are nonzero prime ideals properly contained in P .
46. Let \mathcal{A} be any ideal in $R = k[x_1, \dots, x_n, y_1, \dots, y_m]$.
- (a) Show that $\text{rad}(\mathcal{A} \cap k[y_1, \dots, y_m]) = \text{rad } \mathcal{A} \cap k[y_1, \dots, y_m]$.
- (b) Suppose (f_1, \dots, f_s) is an ideal in $k[x_1, \dots, x_n]$. Let F_1, \dots, F_t be generators for the radical of (f_1, \dots, f_s) , computed in $k[x_1, \dots, x_n]$. Suppose J is an ideal in R and let $\mathcal{A} = J + (f_1, \dots, f_s)$, $\mathcal{B} = J + (F_1, \dots, F_t)$ as ideals in R . Prove that $\text{rad } \mathcal{A} = \text{rad } \mathcal{B}$.
- (c) Conclude from (a) and (b) that $\mathcal{A} = (y_1 - x_1, \dots, y_m - x_m, f_1, \dots, f_s) \cap k[y_1, \dots, y_m]$ and $\mathcal{B} = (y_1 - x_1, \dots, y_m - x_m, F_1, \dots, F_t) \cap k[y_1, \dots, y_m]$ have the same zero sets over an algebraically closed field k . [Use Hilbert's Nullstellensatz.]
47. Determine the Zariski closure in \mathbb{C}^3 of the points on the curve $\{(a^2, a^3, a^4) \mid a \in \mathbb{C}\}$.
48. Show that $\mathcal{Z}(x^3 - xyz + z^2)$ is the smallest algebraic set in \mathbb{R}^3 containing the points $\{(st, s + t, s^2t) \mid s, t \in \mathbb{R}\}$.
49. Show that $\mathcal{Z}(x^3z^2 - 3xy^2z^2 - y^6 - z^4)$ is the smallest algebraic set in \mathbb{R}^3 containing the points $\{(s^2 + t^2, st, s^3) \mid s, t \in \mathbb{R}\}$.

50. Find equations defining the Zariski closure of the set of points $\{(s^4, s^3t, st^3, t^4) \mid s, t \in \mathbb{R}\}$.
51. Show that $V = \mathcal{Z}(x^2 - y^2z)$ (the *Whitney umbrella surface*) is the smallest algebraic set in \mathbb{R}^3 containing the points $S = \{(st, s, t^2) \mid s, t \in \mathbb{R}\}$. Show that S is not Zariski closed in V (the missing points explain the name for the surface). Do the same over \mathbb{C} , but show that in this case $S = V$ is closed.
52. Let $V = \mathcal{Z}(xz^2 - w^3, xw^2 - y^4, y^4z^2 - w^5) \subset \mathbb{C}^4$. Determine the Zariski closure of the image of V under the projection $\pi((x, y, z, w)) = (x, y, z)$.
53. Let $V = \mathcal{Z}(xy - 1)$ in \mathbb{A}^2 and let S be the projection of V onto the x -axis in \mathbb{A}^1 .
- (a) If $k = \mathbb{R}$, show that $\mathcal{I}(V) = (xy - 1) \subset \mathbb{R}[x, y]$ and that $(u - x, xy - 1) \cap \mathbb{R}[u] = 0$ in $\mathbb{R}[x, y, u]$. Use Propositions 8 and 16 to conclude that the Zariski closure of S is \mathbb{A}^1 and show that S is not itself closed.
 - (b) If $k = \mathbb{F}_3$, show that $\mathcal{I}(V) = (xy - 1, x^3 - x, y^3 - y) \subset \mathbb{F}_3[x, y]$ and that $(u - x, xy - 1, x^3 - x, y^3 - y) \cap \mathbb{F}_3[u] = (u^2 - 1)$ in $\mathbb{F}_3[x, y, u]$. Use Propositions 8 and 16 to conclude that S is Zariski closed in \mathbb{A}^1 .
54. Recall the *ideal quotient* $(I : J) = \{r \in R \mid rJ \in I\}$ of two ideals I, J in a ring R (cf. Exercise 34 ff. in Section 9.6). Clearly $I \subseteq (I : J)$.
- (a) Show that $\mathcal{Z}(I) - \mathcal{Z}(J)$, the set of elements of $\mathcal{Z}(I)$ not lying in $\mathcal{Z}(J)$, is contained in $\mathcal{Z}((I : J))$ and conclude that the Zariski closure of $\mathcal{Z}(I) - \mathcal{Z}(J)$ is contained in $\mathcal{Z}((I : J))$.
 - (b) Show that if k is algebraically closed and I is a radical ideal then $\mathcal{Z}((I : J))$ is precisely the Zariski closure of $\mathcal{Z}(I) - \mathcal{Z}(J)$.
 - (c) Show that if V and W are affine algebraic sets then $(\mathcal{I}(V) : \mathcal{I}(W)) = \mathcal{I}(V - W)$.

15.3 INTEGRAL EXTENSIONS AND HILBERT'S NULLSTELLENSATZ

In this section we consider the important concept of an integral extension of rings, which is a generalization to rings of algebraic extensions of fields. This leads to the definition of the “integers” in finite extensions of \mathbb{Q} (the basic subject of the branch of mathematics called algebraic number theory) and is also related to the existence of tangent lines for algebraic curves.

Definition. Suppose R is a subring of the commutative ring S with $1 = 1_S \in R$.

- (1) An element $s \in S$ is *integral over R* if s is the root of a monic polynomial in $R[x]$.
- (2) The ring S is an *integral extension of R* or just *integral over R* if every $s \in S$ is integral over R .
- (3) The *integral closure* of R in S is the set of elements of S that are integral over R .
- (4) The ring R is said to be *integrally closed in S* if R is equal to its integral closure in S . The integral closure of an integral domain R in its field of fractions is called the *normalization of R* . An integral domain is called *integrally closed* or *normal* if it is integrally closed in its field of fractions.

Before giving some examples of integral extensions we prove some basic properties of integral elements analogous to those of algebraic elements over fields.

Proposition 23. Let R be a subring of the commutative ring S with $1 \in R$ and let $s \in S$. Then the following are equivalent:

- (1) s is integral over R ,
- (2) $R[s]$ is a finitely generated R -module (where $R[s]$ is the ring of all R -linear combinations of powers of s), and
- (3) $s \in T$ for some subring T , $R \subseteq T \subseteq S$, that is a finitely generated R -module.

Proof: Suppose first that (1) holds and let s be a root of the monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$. Then

$$s^n = -(a_{n-1}s^{n-1} + a_{n-2}s^{n-2} + \cdots + a_0)$$

and so s^n , and then all higher powers of s , can be expressed as R -linear combinations of $s^{n-1}, \dots, s, 1$. Hence $R[s] = R \cdot 1 + Rs + \cdots + Rs^{n-1}$ is finitely generated as an R -module, which gives (2).

If (2) holds, then (3) holds with $T = R[s]$.

Suppose that (3) holds and let v_1, v_2, \dots, v_n be a finite generating set for T . Then for $i = 1, 2, \dots, n$ the element sv_i is an element of T since T is a ring, and so can be written as R -linear combinations of v_1, \dots, v_n :

$$sv_i = \sum_{j=1}^n a_{ij}v_j,$$

i.e.,

$$0 = \sum_{j=1}^n (\delta_{ij}s - a_{ij})v_j \quad i = 1, 2, \dots, n$$

where δ_{ij} is the Kronecker delta. If B is the $n \times n$ matrix whose i, j entry is $\delta_{ij}s - a_{ij}$, and v is the $n \times 1$ column vector whose entries are v_1, \dots, v_n , then these equations are simply $Bv = 0$. It follows from Cramer's Rule that $(\det B)v_i = 0$ for all i (cf. Exercise 3, Section 11.4). Since $1 \in T$ is an R -linear combination of v_1, \dots, v_n , it follows that $\det B = 0$. But $B = sI - A$, where A is the matrix (a_{ij}) . Thus s is a root of the monic polynomial $\det(xI - A) \in R[x]$ (the characteristic polynomial of A), and so s is a root of a monic polynomial with coefficients in R , which gives (1), completing the proof.

Corollary 24. Let $R \subseteq S$ be as in Proposition 23 and let $s, t \in S$.

- (1) If s and t are integral over R then so are $s \pm t$ and st .
- (2) The integral closure of R in S is a subring of S containing R .
- (3) Integrality is transitive: let S be a subring of T ; if T is integral over S and S is integral over R , then T is integral over R .

Proof: Let s and t be integral over R . By Proposition 23 both $R[s]$ and $R[t]$ are finitely generated R -modules, say

$$R[s] = Rs_1 + Rs_2 + \cdots + Rs_n$$

$$R[t] = Rt_1 + Rt_2 + \cdots + Rt_m.$$