R-module homomorphism from $\bigwedge^n(L) \to \bigwedge^n(R^n) \cong R$ induced by the inclusion of L in R^n is the Fitting ideal $\mathcal{F}_R(M)$.

40. Suppose R and S are commutative rings, $\varphi : R \to S$ is a ring homomorphism, M is a finitely generated R-module, and $M' = S \otimes_R M$ is the S-module obtained by extending scalars from R to S. Prove that the Fitting ideal $\mathcal{F}_S(M')$ for M' over S is the extension to S of the Fitting ideal $\mathcal{F}_R(M)$ for M over R.

The following two exercises indicate how the remainder in Theorem 23 of Chapter 9 can be used to effect computations in quotients of polynomial rings.

41. Suppose $\{g_1, \ldots, g_m\}$ is a Gröbner basis for the ideal I in $k[x_1, \ldots, x_n]$. Prove that the monomials m not divisible by any $LT(g_i)$, $1 \le i \le m$, give a k-vector space basis for the quotient $k[x_1, \ldots, x_n]/I$.

42. Let $I = (x^3y - xy^2 + 1, x^2y^2 - y^3 - 1)$ as in Example 1 following Proposition 9.26.

(a) Use the previous exercise to show that $\{1, y, y^2, y^3\}$ is a basis for the k-vector space $k[x, y]/I$.

(b) Compute the 4×4 multiplication table for the basis vectors in (a).

43. Suppose $K[x_1, \ldots, x_n]$ is a polynomial ring in n variables over a field K and k is a subfield of K. If I is an ideal in $k[x_1, \ldots, x_n]$, let I' be the ideal generated by I in $K[x_1, \ldots, x_n]$.

(a) If G is a Gröbner basis for the ideal I in $k[x_1, \ldots, x_n]$ with respect to some monomial ordering, show that G is also a Gröbner basis for the ideal I' in $K[x_1, \ldots, x_n]$ with respect to the same monomial ordering. [Use Buchberger's Criterion.]

(b) Prove that the dimension of the quotient $k[x_1, \ldots, x_n]/I$ as a vector space over k is the same as the dimension of the quotient $K[x_1, \ldots, x_n]/I'$ as a vector space over K. [One method: use (a) and Exercise 41.]

(c) Prove that $I = k[x_1, \ldots, x_n]$ if and only if $I' = K[x_1, \ldots, x_n]$.

44. Let $V = \mathcal{Z}(x^3 - x^2z - y^2z)$ and $W = \mathcal{Z}(x^2 + y^2 - z^2)$ in $\mathbb{C}^3$. Then $\mathcal{I}(V) = (x^3 - x^2z - y^2z)$ and $\mathcal{I}(W) = (x^2 + y^2 - z^2)$ in $\mathbb{C}[x, y, z]$ (cf. Exercise 23 in Section 3). Show that $\varphi((a, b, c)) = (a^2c - b^2c, 2abc, -a^3)$ defines a morphism from V to W.

45. Let $V = \mathcal{Z}(x^3 + y^3 + 7z^3) \subset \mathbb{C}^3$. Then $\mathcal{I}(V) = (x^3 + y^3 + 7z^3)$ in $\mathbb{C}[x, y, z]$ (cf. Exercise 24 in Section 3).

(a) Show that

$$\widetilde{\varphi}(x) = x(y^3 - 7z^3), \qquad \widetilde{\varphi}(y) = y(7z^3 - x^3), \qquad \widetilde{\varphi}(z) = z(x^3 - y^3)$$

defines a $\mathbb{C}$-algebra homomorphism from $k[V]$ to itself.

(b) Let $\varphi : V \to V$ be the morphism corresponding to $\widetilde{\varphi}$. Observe that $(-2, 1, 1) \in V$ and compute $\varphi((-2, 1, 1)) \in V$.

(c) Prove there are infinitely many points (a, b, c) on V with $a, b, c \in \mathbb{Z}$ and the greatest common divisor of a, b, and c is 1.

46. Let $V = \mathcal{Z}(xz + y^2 + z^2, xy - xz + yz - 2z^2) \subset \mathbb{C}^3$ and $W = \mathcal{Z}(u^3 - uv^2 + v^3) \subset \mathbb{C}^2$ as in Example 2 following Corollary 9. Show that the map $\varphi((a, b)) = (-2a^2 + ab, ab - b^2, a^2 - ab)$ defines a morphism from W to V. Show the corresponding $\mathbb{C}$-algebra homomorphism from $k[V]$ to $k[W]$ has a kernel generated by $x^2 - 3y^2 + yz$.

47. Define $\Phi : \mathbb{Q}[u, v, w] \to \mathbb{Q}[x, y]$ by $\Phi(u) = x^2 + y$, $\Phi(v) = x + y^2$, and $\Phi(w) = x - y$. Show that neither x nor y is in the image of Φ. Show that $f = 2x^3 - 4xy - 2y^3 - 4y$ is in the image of Φ and find a polynomial in $\mathbb{Q}[u, v, w]$ mapping to f. Show that $\ker \Phi$ is the ideal generated by

$$u^2 - 2uv - 2uw^2 + 4uw + v^2 - 2vw^2 - 4vw + w^4 + 3w^2.$$

48. Suppose α is a root of the irreducible polynomial $p(x) \in k[x]$ and $\beta = f(\alpha)/g(\alpha)$ with polynomials $f(x), g(x) \in k[x]$ where $g(\alpha) \neq 0$.

(a) Show $ag + bp = 1$ for some polynomials $a, b \in k[x]$ and show $\beta = h(\alpha)$ where $h = af$.

(b) Show that the ideals $(p, y - h)$ and $(p, gy - f)$ are equal in $k[x, y]$.

(c) Conclude that the minimal polynomial for β is the monic polynomial in $G \cap k[y]$ where G is the reduced Gröbner basis for the ideal $(p, gy - f)$ in $k[x, y]$ for the lexicographic monomial ordering $x > y$.

(d) Find the minimal polynomial over $\mathbb{Q}$ of $(3 - \sqrt[3]{2} + \sqrt[3]{4})/(1 + 3\sqrt[3]{2} - 3\sqrt[3]{4})$.

15.2 RADICALS AND AFFINE VARIETIES

Since the zeros of a polynomial f are the same as the zeros of the powers $f^2, f^3, \ldots$ in general there are many different ideals in the ring $k[x_1, x_2, \ldots, x_n]$ whose zero locus define the same algebraic set V in affine n-space. This leads to the notion of the radical of an ideal, which can be defined in any commutative ring:

Definition. Let I be an ideal in a commutative ring R.

(1) The *radical* of I, denoted by $\operatorname{rad} I$, is the collection of elements in R some power of which lie in I, i.e.,

$$\operatorname{rad} I = \{a \in R \mid a^k \in I \text{ for some } k \geq 1\}.$$

(2) The radical of the zero ideal is called the *nilradical* of R.

(3) An ideal I is called a *radical* ideal if $I = \operatorname{rad} I$.

Note that $a \in R$ is in the nilradical of R if and only if some power of a is 0, so the nilradical of R is the set of all nilpotent elements of R.

Proposition 11. Let I be an ideal in the commutative ring R. Then $\operatorname{rad} I$ is an ideal containing I, and $(\operatorname{rad} I)/I$ is the nilradical of R/I. In particular, R/I has no nilpotent elements if and only if $I = \operatorname{rad} I$ is a radical ideal.

Proof: It is clear that $I \subseteq \operatorname{rad} I$. By definition, the nilradical of R/I consists of the elements in the quotient some power of which is 0. Under the Lattice Isomorphism Theorem for rings this collection of elements corresponds to the elements of R some power of which lie in I, i.e., $\operatorname{rad} I$. It is therefore sufficient to prove that the nilradical N of any commutative ring R is an ideal. Since $0 \in N$, $N \neq \emptyset$. If $a \in N$ and $r \in R$, then since $a^n = 0$ for some $n \geq 1$, the commutativity of R implies that $(ra)^n = r^n a^n = 0$, so $ra \in N$. It remains to see that if $a, b \in N$ then $a + b \in N$. Suppose $a^n = 0$ and $b^m = 0$. Since the Binomial Theorem holds in the commutative ring R (cf. Exercise 25 in Section 7.3),

$$(a + b)^{n+m} = \sum_{i=0}^{n+m} r_i a^i b^{n+m-i}$$

for some ring elements r_i (the binomial coefficients in R). For each term in this sum either $i \geq n$ (in which case $a^i = 0$) or $n + m - i \geq m$, (in which case $b^{n+m-i} = 0$). Hence $(a + b)^{n+m} = 0$, which shows that $a + b$ is nilpotent, i.e., $a + b \in N$.

Proposition 12. The radical of a proper ideal I is the intersection of all prime ideals containing I. In particular, the nilradical is the intersection of all the prime ideals in R.

Proof: Passing to R/I, Proposition 11 shows that it suffices to prove this result for $I = 0$, and in this case the statement is that the nilradical N of R is the intersection of all the prime ideals in R. Let N' denote the intersection of all the prime ideals in R.

Let a be any nilpotent element in R and let P be any prime ideal. Since $a^k = 0$ for some k, there is a smallest positive power n such that $a^n \in P$. Then the product $a^{n-1}a \in P$, and since P is prime, either $a^{n-1} \in P$ or $a \in P$. The former contradicts the minimality of n, and so $a \in P$. Since P was arbitrary, $a \in N'$, which shows that $N \subseteq N'$.

We prove the reverse containment $N' \subseteq N$ by showing that if $a \notin N$, then $a \notin N'$. If a is an element of R not contained in N, let $\mathcal{S}$ be the family of all proper ideals not containing any positive power of a. The collection $\mathcal{S}$ is not empty since $0 \in \mathcal{S}$. Also, if a^k is not contained in any ideal in the chain $I_1 \subseteq I_2 \subseteq \cdots$, then a^k is also not contained in the union of these ideals, which shows that chains in $\mathcal{S}$ have upper bounds. By Zorn's Lemma, $\mathcal{S}$ has a maximal element, P. The ideal P must in fact be a prime ideal, as follows. Suppose for some x and y not contained in P, the product xy is an element of P. By the maximality of P, $a^n \in (x) + P$ and $a^m \in (y) + P$ for some positive integers n and m. Then $a^{n+m} \in (xy) + P = P$ contradicting the fact that P is an element of $\mathcal{S}$. This shows that P is indeed a prime ideal not containing a, and hence $a \notin N'$, completing the proof.

Note that in Noetherian rings, Theorem 2 can be used to circumvent the appeal to Zorn's Lemma in the preceding proof.

Corollary 13. Prime (and hence also maximal) ideals are radical.

Proof: If P is a prime ideal, then P is clearly the intersection of all the prime ideals containing P, so $P = \text{rad } P$ by the proposition.

Examples

(1) In the ring of integers $\mathbb{Z}$, the ideal (a) is a radical ideal if and only if a is square-free or zero. More generally, if $a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ with $a_i \geq 1$ for all i, is the prime factorization of the positive integer a, then $\text{rad}(a) = (p_1 p_2 \cdots p_r)$. For instance, $\text{rad}(180) = (30)$. Note that $(p_1), (p_2), \ldots, (p_r)$ are precisely the prime ideals containing the ideal (a) and that their intersection is the ideal $(p_1 p_2 \cdots p_r)$. More generally, in any U.F.D. R, $\text{rad}(a) = (p_1 p_2 \cdots p_r)$ if $a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ is the unique factorization of a into distinct irreducibles.

(2) The ideal $(x^3 - y^2)$ in $k[x, y]$ is a prime ideal (Exercise 14, Section 9.1), hence is radical.

(3) If $l_1, \ldots, l_m$ are linear polynomials in $k[x_1, x_2, \ldots, x_n]$ then $I = (l_1, \ldots, l_m)$ is either $k[x_1, x_2, \ldots, x_n]$ or a prime ideal, hence I is a radical ideal.

Proposition 14. If R is a Noetherian ring then for any ideal I some positive power of $\text{rad } I$ is contained in I. In particular, the nilradical, N, of a Noetherian ring is a nilpotent ideal: $N^k = 0$ for some $k \geq 1$.