Noether's Normalization Lemma and Hilbert's Nullstellensatz

We now apply some of the techniques from the algebraic theory of integral ring extensions to affine geometry.

Definition. If k is a field the elements $y_1, y_2, \ldots, y_q$ in some k-algebra are called *algebraically independent* over k if there is no nonzero polynomial p in q variables over k such that $p(y_1, y_2, \ldots, y_q) = 0$.

Thus $y_1, y_2, \ldots, y_q$ are algebraically independent if and only if the k-algebra homomorphism from the polynomial ring $k[x_1, \ldots, x_q]$ to $k[y_1, \ldots, y_q]$ defined by $x_i \mapsto y_i$ is an isomorphism. Elements in a field extension of k are algebraically independent if and only if they are independent transcendentals over k.

Theorem 30. *(Noether's Normalization Lemma)* Let k be a field and suppose that $A = k[r_1, r_2, \ldots, r_m]$ is a finitely generated k-algebra. Then for some q, $0 \leq q \leq m$, there are algebraically independent elements $y_1, y_2, \ldots, y_q \in A$ such that A is integral over $k[y_1, y_2, \ldots, y_q]$.

Proof: Proceed by induction on m. If $r_1, \ldots, r_m$ are algebraically independent over k then take $y_i = r_i$, $i = 1, \ldots, m$. Otherwise, there exists $f(x_1, \ldots, x_m) \in k[x_1, \ldots, x_m]$ such that $f(r_1, \ldots, r_m) = 0$. The polynomial f is a sum of monomials of the form $ax_1^{e_1}x_2^{e_2} \cdots x_m^{e_m}$, where the degree of this monomial is $e_1 + \cdots + e_m$ and the degree, d, of f is the maximum of the degrees of its monomials. Renumbering the variables if necessary, we may assume that f is a nonconstant polynomial in x_m with coefficients in the ring $k[x_1, x_2, \ldots, x_{m-1}]$. We now perform a change of variables that transforms (or "normalizes") f into a *monic* polynomial in x_m with coefficients from a subring of A which is generated over k by $m - 1$ elements, at which point we shall be able to apply induction.

Define integers $\alpha_i = (1 + d)^i$ and new variables $X_i = x_i - x_m^{\alpha_i}$ for $1 \leq i \leq m - 1$. Let

$$g(X_1, X_2, \ldots, X_{m-1}, x_m) = f(X_1 + x_m^{\alpha_1}, X_2 + x_m^{\alpha_2}, \ldots, X_{m-1} + x_m^{\alpha_{m-1}}, x_m),$$

so $g \in k[X_1, \ldots, X_{m-1}, x_m]$. Each monomial term of f contributes a single term of the form a constant times x_m^e to g. It is also easy to check that the choice of α_i ensures that distinct monomials in f give different values of e (for example by viewing the degrees of the monomials in the new variables as integers expressed in base $b = d + 1$). If N is the highest power of x_m that occurs, then it follows that

$$g = cx_m^N + \sum_{i=0}^{N-1} h_i(X_1, \ldots, X_{m-1})x_m^i$$

for some nonzero $c \in k$. If now $s_i = r_i - r_m^{\alpha_i}$ then

$$\frac{1}{c}g(s_1, s_2, \ldots, s_{m-1}, r_m) = \frac{1}{c}f(r_1, r_2, \ldots, r_{m-1}, r_m) = 0,$$

which shows that r_m is integral over $B = k[s_1, \ldots, s_{m-1}]$. Each r_i for $1 \leq i \leq m - 1$ is integral over $B[r_m]$ since r_i is a root of the monic polynomial $x - s_i - r_m^{\alpha_i}$, so A is

integral over $B[r_m]$. By transitivity of integrality, A is therefore integral over B. Since B is a k-algebra generated by $m-1$ elements, induction completes the proof.

A more "geometric" interpretation of Noether's Normalization Lemma is indicated in Exercise 15. We next use the Normalization Lemma to prove that if k is an algebraically closed field then the maximal ideals of the polynomial ring $k[x_1, x_2, \ldots, x_n]$ are of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for some $a_1, \ldots, a_n \in k$. Viewing $k[x_1, x_2, \ldots, x_n]$ as the ring of polynomial functions on $\mathbb{A}^n$, this says that the maximal ideals correspond to the kernels of evaluation maps at points of $\mathbb{A}^n$ — similar to the corresponding result for rings of continuous functions on a compact set (cf. Exercises 33, 34 in Section 7.4).

Theorem 31. *(Hilbert's Nullstellensatz — Weak Form)* Let k be an algebraically closed field. Then M is a maximal ideal in the polynomial ring $k[x_1, x_2, \ldots, x_n]$ if and only if $M = (x_1 - a_1, \ldots, x_n - a_n)$ for some $a_1, \ldots, a_n \in k$. Equivalently, the maps $\mathcal{Z}$ and $\mathcal{I}$ give a bijective correspondence

$$\{\text{points in } \mathbb{A}^n\} \underset{\mathcal{Z}}{\overset{\mathcal{I}}{\rightleftarrows}} \{\text{maximal ideals in } k[\mathbb{A}^n]\}.$$

Moreover, if I is any proper ideal in $k[x_1, x_2, \ldots, x_n]$ then $\mathcal{Z}(I) \neq \emptyset$.

Proof: Certainly $(x_1 - a_1, \ldots, x_n - a_n)$ is a maximal ideal in $k[x_1, x_2, \ldots, x_n]$. Conversely, for any maximal ideal M in $k[x_1, x_2, \ldots, x_n]$, let $E = k[x_1, x_2, \ldots, x_n]/M$. Then E is a field containing k that is finitely generated over k (by $\bar{x}_i, \ldots, \bar{x}_n$). By Noether's Normalization Lemma, E is integral over a polynomial ring $k[y_1, \ldots, y_q]$. Then $k[y_1, \ldots, y_q]$ is a field by Theorem 26(1), and since a polynomial ring in one or more variables is never a field, it follows that $q = 0$. Hence E is integral over k, so E is algebraic over k. Because k is algebraically closed, $E = k$, i.e., $\bar{x}_i \in k$ for $1 \leq i \leq n$. Hence for $i = 1, \ldots, n$ there is some $a_i \in k$ such that $x_i - a_i \in M$. This means that the maximal ideal $(x_1 - a_1, \ldots, x_n - a_n)$ is contained in M, so $M = (x_1 - a_1, \ldots, x_n - a_n)$. Finally, if I is any nonzero ideal in $k[x_1, x_2, \ldots, x_n]$ then I is contained in a maximal ideal $M = (x_1 - a_1, \ldots, x_n - a_n)$, and so $(a_1, \ldots, a_n) \in \mathcal{Z}(I)$.

Theorem 32. *(Hilbert's Nullstellensatz)* Let k be an algebraically closed field. Then $\mathcal{I}(\mathcal{Z}(I)) = \operatorname{rad} I$ for every ideal I of $k[x_1, x_2, \ldots, x_n]$. Moreover, the maps $\mathcal{Z}$ and $\mathcal{I}$ define inverse bijections

$$\{\text{affine algebraic sets}\} \underset{\mathcal{Z}}{\overset{\mathcal{I}}{\rightleftarrows}} \{\text{radical ideals}\}.$$

Proof: Since $\operatorname{rad} I \subseteq \mathcal{I}(\mathcal{Z}(I))$ it remains to prove the reverse inclusion. By Hilbert's Basis Theorem, $I = (f_1, f_2, \ldots, f_m)$. Let $g \in \mathcal{I}(\mathcal{Z}(I))$. Introduce a new variable x_{n+1} and consider the ideal I' generated by $f_1, \ldots, f_m$ and $x_{n+1}g - 1$ in $k[x_1, \ldots, x_n, x_{n+1}]$. At any point of $\mathbb{A}^{n+1}$ where $f_1, \ldots, f_m$ vanish the polynomial g also vanishes since $g \in \mathcal{I}(\mathcal{Z}(I))$, so that $x_{n+1}g - 1$ is nonzero. Hence $\mathcal{Z}(I') = \emptyset$ in $\mathbb{A}^{n+1}$. By the Weak Form of the Nullstellensatz, I' cannot be a proper ideal, i.e., $1 \in I'$. Write

$$1 = a_1 f_1 + \cdots + a_m f_m + a_{m+1}(x_{n+1}g - 1) \qquad \text{for some } a_i \in k[x_1, \ldots, x_{n+1}].$$

Letting $y = 1/x_{n+1}$ and multiplying by a high power of y in this equation shows that

$$y^N = c_1 f_1 + \cdots + c_m f_m + c_{m+1}(g - y) \qquad \text{for some } c_i \in k[x_1, \ldots, x_n, y].$$

Substituting g for y in this polynomial equation shows that $g^N \in I$ (in $k[x_1, \ldots, x_n]$), i.e., $g \in \operatorname{rad} I$. Hence $\mathcal{I}(\mathcal{Z}(I)) \subseteq \operatorname{rad} I$ and so $\mathcal{I}(\mathcal{Z}(I)) = \operatorname{rad} I$, completing the proof.

It follows directly from Proposition 12 and Theorem 26(2) that if S is an integral extension of R with $1 \in R$ and if I is an ideal of R, then

$$(\operatorname{rad}_S IS) \cap R = \operatorname{rad}_R I$$

where IS is the ideal generated by I in S, and the subscript indicates the ring in which the radicals are being computed. This has the following geometric interpretation.

Corollary 33. *(Variant of Hilbert's Nullstellensatz)* If k is any field with algebraic closure $\bar{k}$ and I is an ideal in $k[x_1, x_2, \ldots, x_n]$, then $\mathcal{I}_k(\mathcal{Z}_{\bar{k}}(I)) = \operatorname{rad} I$, where $\mathcal{Z}_{\bar{k}}(I)$ is the zero set in $\bar{k}^n$ of the polynomials in I and $\mathcal{I}_k(\mathcal{Z}_{\bar{k}}(I))$ is the ideal of polynomials in $k[x_1, x_2, \ldots, x_n]$ vanishing at all the points in $\mathcal{Z}_{\bar{k}}(I)$. In particular, $I = (1)$ if and only if there are no common zeros in $\bar{k}^n$ of the polynomials in I.

Proof: Since $\bar{k}[x_1, x_2, \ldots, x_n]$ is an integral extension of $k[x_1, x_2, \ldots, x_n]$ (generated by the integral elements $\bar{k}$), the corollary follows immediately from Theorem 32 and the remarks on radicals above.

From the Nullstellensatz we now have a dictionary between geometric and ring-theoretic objects over the algebraically closed field k:

Geometry	Algebra
affine algebraic set V	coordinate ring $k[V]$
points of V	maximal ideals of $k[V]$
affine algebraic subsets in V	radical ideals of $k[V]$
subvarieties in V	prime ideals in $k[V]$
morphism $\varphi : V \to W$	k-algebra homomorphism $\tilde{\varphi} : k[W] \to k[V]$

Computing Radicals

There are algorithms for computing radicals and primary decompositions in polynomial rings using Gröbner bases. While they are relatively elementary, they are somewhat technical and so we limit our discussion here to some preliminary results.

For hypersurfaces $V = \mathcal{Z}(f)$ defined by a single polynomial $f \in k[x_1, \ldots, x_n]$, determining $\mathcal{I}(V) = \operatorname{rad}(f)$ is straightforward. Since $k[x_1, \ldots, x_n]$ is a U.F.D., f factors uniquely as the product of powers of nonassociate irreducibles: $f = p_1^{a_1} \cdots p_s^{a_s}$ and then $\operatorname{rad}(f)$ is generated by $p_1 \cdots p_s$ (the 'squarefree part' of f).

Example

Suppose $W = \mathcal{Z}(J)$ with $J = (u^3 - uv^2 + v^3) \in \mathbb{Q}[u, v]$. The polynomial $x^3 - x + 1$ is irreducible over $\mathbb{Q}$, so $f = u^3 - uv^2 + v^3$ is irreducible in $\mathbb{Q}[u, v]$. Hence $\operatorname{rad} J = J$ and $\mathcal{I}(W) = J$.

For nonprincipal ideals I, determining $\operatorname{rad} I$ is more complicated. The following proposition (based on Hilbert's Nullstellensatz) gives a criterion determining when an element is contained in $\operatorname{rad} I$.

Proposition 34. Suppose k is any field. If $I = (f_1, \ldots, f_s)$ is a proper ideal in $k[x_1, \ldots, x_n]$, then $f \in \operatorname{rad} I$ if and only if $(f_1, \ldots, f_s, 1 - yf) = k[x_1, \ldots, x_n, y]$.

Proof: By Corollary 33, $(f_1, \ldots, f_s, 1 - yf) = k[x_1, \ldots, x_n, y]$ if and only if the equations

$$1 - yf(x_1, \ldots, x_n) = 0, \quad f_1(x_1, \ldots, x_n) = 0, \quad \ldots, \quad f_s(x_1, \ldots, x_n) = 0$$

have no common zero over the algebraic closure $\bar{k}$ of k. For a given $(a_1, \ldots, a_n) \in \bar{k}^n$, the equation $1 - yf(a_1, \ldots, a_n) = 0$ has a solution y unless $f(a_1, \ldots, a_n) = 0$. Hence, the system of equations has no common zero if and only if for every $(a_1, \ldots, a_n) \in \bar{k}^n$ with $f_1(a_1, \ldots, a_n) = \cdots = f_s(a_1, \ldots, a_n) = 0$ we also have $f(a_1, \ldots, a_n) = 0$. Equivalently, if $(a_1, \ldots, a_n) \in \mathcal{Z}_{\bar{k}}(I)$, then also $f(a_1, \ldots, a_n) = 0$, i.e., we have $f \in \mathcal{I}_k(\mathcal{Z}_{\bar{k}}(I)) = \operatorname{rad} I$, by Corollary 33.

Since the reduced Gröbner basis (with respect to any fixed monomial ordering) for an ideal is unique, we immediately obtain the following algorithmic method for determining when a polynomial lies in the radical of an ideal.

Corollary 35. Suppose $I = (f_1, \ldots, f_s)$ in $k[x_1, \ldots, x_n]$. Then $f \in \operatorname{rad} I$ if and only if $\{1\}$ is the reduced Gröbner basis for the ideal $(f_1, \ldots, f_s, 1 - yf)$ in $k[x_1, \ldots, x_n, y]$ with respect to any monomial ordering.

Example

Consider $I = (x^2 - y^2, xy)$ in $k[x, y]$. The reduced Gröbner basis for $(x^2 - y^2, xy, 1 - tx)$ in $k[x, y, t]$ with respect to the order $x > y > t$ is $\{1\}$, showing $x \in \operatorname{rad}(I)$. To determine the smallest power of x lying in I, we find that the ideal $(x^2 - y^2, xy, x^3)$ in $k[x, y]$ has the same reduced Gröbner basis as I (namely $\{x^2 - y^2, xy, y^3\}$), but $(x^2 - y^2, x^2, xy)$ has basis $\{x^2, xy, y^2\}$. It follows that $x^3 \in I$ and $x^2 \notin I$ (alternatively, x^3 leaves a nonzero remainder after general polynomial division by $\{x^2 - y^2, xy, y^3\}$, but x^3 has a remainder of 0). By a similar computation (or by symmetry), $y \in \operatorname{rad} I$, with $y^3 \in I$ but $y^2 \notin I$. Since $(x, y) \subseteq \operatorname{rad} I$, it follows that $\operatorname{rad} I = (x, y)$.

Some additional results for computing radicals are presented in the exercises.