8. Hilbert's Nullstellensatz

8.1 Theorem: *(Hilbert's Weak Nullstellensatz) Let* $\mathbf{F}$ *be an algebraically closed field, and let* $A \subsetneqq \mathbf{F}[x_1, \cdots, x_n]$ *be a proper ideal. Then* $V(A) \neq \emptyset$.

Proof: Using Zorn's Lemma, we can choose a maximal ideal $M \subseteq \mathbf{F}[x_1, \cdots, x_n]$ with $A \subseteq M$. Note that $V(M) \subseteq V(A)$ so it suffices to show that $V(M) \neq \emptyset$.

Let $\mathbf{L} = \mathbf{F}[x_1, \cdots, x_n]/M$, and note that $\mathbf{L}$ is a field since M is maximal. Let ϕ be the natural projection $\phi : \mathbf{F}[x_1, \cdots, x_n] \to \mathbf{L}$, which is given by $\phi(f) = f + M$. Notice that $\mathbf{F} \cap M = \{0\}$ since if we had $0 \neq a \in \mathbf{F} \cap M$ then we would also have $1 = \frac{1}{a}\, a \in M$ so M would not be maximal. This implies that the restriction of ϕ to $\mathbf{F}$ is injective, since for $a \in \mathbf{F}$ we have $\phi(a) = 0 \implies a \in M \implies a \in \mathbf{F} \cap M \implies a = 0$. Let us write $\mathbf{K} = \phi(\mathbf{F})$. Then $\phi : \mathbf{F} \to \mathbf{K}$ is an isomorphism of fields. In particular, $\mathbf{K}$ is also algebraically closed.

Now for $i = 1, \cdots, n$, write $u_i = \phi(x_i) = x_i + M$. Then we have $\mathbf{L} = \mathbf{K}[u_1, \cdots, u_n]$. We claim that the fact that $\mathbf{L} = \mathbf{K}[u_1, \cdots, u_n]$ is a field implies that each u_i must be algebraic over $\mathbf{K}$. Suppose, for a contradiction, that the u_i are not all algebraic over $\mathbf{K}$. Then, writing $r = \text{trans}_{\mathbf{K}}\mathbf{K}[u_1, \cdots, u_n]$, we have $r \geq 1$. By Noether's Normalization Lemma we can choose an algebraically independent set $\{v_1, \cdots, v_r\} \subseteq \mathbf{K}[u_1, \cdots, u_n]$ such that $\mathbf{K}[u_1, \cdots, u_n]$ is integral over $\mathbf{K}[v_1, \cdots, v_r]$. But since $\{v_1, \cdots, v_r\}$ is algebraically independent over $\mathbf{K}$, so that we can identify $\mathbf{K}[v_1, \cdots, v_r]$ as the ring of polynomials in the variables $v_1, \cdots, v_r$, the ideal $\langle v_1, \cdots, v_r \rangle$ is maximal in $\mathbf{K}[v_1, \cdots, v_r]$. By the Lying Over Theorem there must be a maximal ideal $N \subseteq \mathbf{L}$ which lies over it. But since $\mathbf{L}$ is a field, $\{0\}$ is the only maximal ideal in $\mathbf{L}$, and $\{0\}$ certainly does not lie over $\langle v_1, \cdots, v_r \rangle$. This gives the required contradiction.

Since each u_i is algebraic over $\mathbf{K} = \phi(\mathbf{F})$, which is algebraically closed, we have $u_i \in \mathbf{K}$ for all i. For each $i = 1, \cdots, n$, choose $a_i \in \mathbf{F}$ so that $\phi(a_i) = u_i$, that is $\phi(a_i) = \phi(x_i)$, and set $a = (a_1, \cdots, a_n) \in \mathbf{F}^n$. We claim that $a \in V(M)$ so that $V(M) \neq \emptyset$. Indeed, for $f \in M$ we have $\phi(f) = 0$, so if we write $f = \sum c_{i_1, \cdots, i_n} {x_1}^{i_1} \cdots {x_n}^{i_n}$ then we have $\phi(f(a)) = \sum \phi\big(c_{i_1, \cdots, i_n}\big)\phi(a_1)^{i_1} \cdots \phi(a_n)^{i_n} = \sum \phi\big(c_{i_1, \cdots, i_n}\big)\phi(x_1)^{i_1} \cdots \phi(x_n)^{i_n} = \phi(f) = 0$, and hence $f(a) = 0$ since the restriction of ϕ to $\mathbf{F}$ is injective.

8.2 Example: If $\mathbf{F}$ is not algebraically closed, then it is certainly possible to find a proper ideal $A \subsetneqq \mathbf{F}[x_1, \cdots, x_n]$ with $V(A) = \emptyset$. Indeed for any non-constant polynomial $f \in \mathbf{F}[x_1, \cdots, x_n]$ with no roots, we have $\langle f \rangle \subsetneqq \mathbf{F}[x_1, \cdots, x_n]$ but $V(\langle f \rangle) = \emptyset$.

8.3 Definition: Let R be a commutative ring. The **radical** of an ideal A is the ideal

$$\sqrt{A} = \big\{ r \in R \big| r^n \in A \text{ for some } n \in \mathbf{N} \big\} .$$

Note that $\sqrt{A}$ is an ideal since for $r \in R$ and $a, b \in \sqrt{A}$ with $a^n \in A$ and $b^m \in A$, we have $(ar)^n = a^n r^n \in A$ and we have $(a+b)^{n+m} = a^{n+m} + \cdots + a^n b^m + \cdots + b^{n+m} \in A$. Also note that $A \subseteq \sqrt{A}$. A **radical ideal** is an ideal in R of the form $\sqrt{A}$ for some ideal A.

8.4 Note: For any ideal A in a commutative ring R, A is radical $\iff$ $A = \sqrt{A}$.

Proof: If $A = \sqrt{A}$ then A is radical by definition. Coversely, suppose that A is radical, say $A = \sqrt{B}$. We have $A \subseteq \sqrt{A}$, so we only need to show that $\sqrt{A} \subseteq A$. Let $a \in \sqrt{A}$, say $a^n \in A = \sqrt{B}$. Choose $m \in \mathbf{N}$ such that $(a^n)^m \in B$. Then $a^{nm} \in B$ so $a \in \sqrt{B} = A$.

8.5 Example: In a commutative ring, every prime ideal is a radical ideal.

8.6 Example: In $\mathbf{Z}$, if $n = {p_1}^{k_1}{p_2}^{k_2}\cdots{p_l}^{k_l}$ where the p_i are distinct primes, then we have $\sqrt{\langle n\rangle} = \langle p_1p_2\cdots p_l\rangle$. Similarly, if $f \in \mathbf{F}[x_1,\cdots,x_n]$ factors into irreducible polynomials as $f = {f_1}^{k_1}{f_2}^{k_2}\cdots{f_l}^{k_l}$, then $\sqrt{\langle f\rangle} = \langle f_1f_2\cdots f_l\rangle$.

8.7 Note: Let A be any ideal in $\mathbf{F}[x_1,\cdots,x_n]$. Then $V(A) = V(\sqrt{A})$, and $\sqrt{A} \subseteq \overline{A}$, and if A is closed then A must be radical.

Proof: Since $A \subseteq \sqrt{A}$, we have $V(\sqrt{A}) \subseteq V(A)$. Let $a \in V(A)$. Let $f \in \sqrt{A}$. Choose $n \in \mathbf{N}$ so that $f^n \in A$. Then since $a \in V(A)$, we have $f^n(a) = 0$, and so $f(a) = 0$. Since $f \in \sqrt{A}$ was arbitrary, we have $f(a) = 0$ for every $f \in \sqrt{A}$, and so $a \in V(\sqrt{A})$. Thus $V(A) = V(\sqrt{A})$. Since $V(A) = V(\sqrt{A})$, we have $\sqrt{A} \subseteq \overline{\sqrt{A}} = I(V(\sqrt{A})) = I(V(A)) = \overline{A}$. And finally, if A is closed then we have $\sqrt{A} \subseteq \overline{A} = A$.

8.8 Theorem: *(Hilbert's Nullstellensatz) Let $\mathbf{F}$ be an algebraically closed field and let A be an ideal in $\mathbf{F}[x_1,\cdots,x_n]$. Then $\overline{A} = \sqrt{A}$.*

Proof: We have seen that $\sqrt{A} \subseteq I(V(A))$, so we must show that $I(V(A)) \subseteq \sqrt{A}$. Let $f \in I(V(A)) \subseteq \mathbf{F}[x_1,\cdots,x_n]$. Write $x = (x_1,\cdots,x_n)$, let $g(x,y) = y\,f(x) - 1 \in \mathbf{F}[x_1,\cdots,x_n,y]$ and let B be the ideal generated by $A \cup \{g\}$ in $\mathbf{F}[x_1,\cdots,x_n,y]$. We claim that $V(B) = \emptyset$. Indeed, suppose for a contradiction that $(a,b) \in V(B)$, where $a \in \mathbf{F}^n$ and $b \in \mathbf{F}$. Then for every $h(x) \in A$, we also have $h(x) \in B$ so $h(a) = 0$, and so we have $a \in V(A) \subseteq \mathbf{F}^n$. Since $f \in I(V(A))$, we have $f(a) = 0$. Also, $g(x,y) \in B$ so we have $0 = g(a,b) = b\,f(a) - 1 = -1$, giving a contradiction, so $V(B) = \emptyset$, as claimed. By Hilbert's Weak Nullstellensatz, we must have $B = \mathbf{F}[x_1,\cdots,x_n,y]$. In particular, we have $1 \in B = \langle A \cup \{g\}\rangle$, so we can write

$$1 = \sum_{i=1}^{k-1} f_i(x)g_i(x,y) + (yf(x) - 1)g_k(x,y) \ \in \mathbf{F}[x_1,\cdots,x_n,y]$$

where each $f_i(x) \in A$ and each $g_i(x,y) \in \mathbf{F}[x_1,\cdots,x_n,y]$. Setting $y = \frac{1}{f(x)} \in \mathbf{F}(x_1,\cdots,x_n)$ we have

$$1 = \sum_{i=1}^{k} f_i(x)g_i\big(x, \tfrac{1}{f(x)}\big) \ \in \mathbf{F}(x_1,\cdots,x_n)\,.$$

Multiplying by $f^N(x)$, where N is the maximum of the degrees in y of the polynomials $g_i(x,y)$, we obtain

$$f^N(x) = \sum_{i=1}^{k} f_i(x)h_i(x) \ \in A \subseteq \mathbf{F}[x_1,\cdots,x_n]$$

where $h_i(x) = f^N(x)g_i\big(x, \frac{1}{f(x)}\big) \in \mathbf{F}[x_1,\cdots,x_n]$. Since $f^N \in A$ for some N, we have $f \in \sqrt{A}$ as required.

8.9 Example: If $\mathbf{F}$ is not algebraically closed, then we can find ideals $A \subseteq \mathbf{F}[x_1,\cdots,x_n]$ such that $\sqrt{A} \subsetneqq \overline{A}$. For example, if f is any irreducible polynomial in $\mathbf{F}[x_1,\cdots,x_n]$ with no roots, then we have $\sqrt{\langle f\rangle} = \langle f\rangle \subsetneqq \mathbf{F}[x_1,\cdots,x_n] = \overline{\langle f\rangle}$

8.10 Corollary: *If $\mathbf{F}$ is an algebraically closed field, then the maps $A \mapsto V(A)$ and $X \mapsto I(X)$ give a bijective order-reversing correspondence between the set of all radical ideals $A \subseteq \mathbf{F}[x_1,\cdots,x_n]$ and the set of all varieties $X \subseteq \mathbf{F}^n$. Under this correspondence, every maximal ideal M corresponds to a point, and every prime ideal P corresponds to an irreducible variety.*

8.11 Corollary: *If* $\mathbf{F}$ *is an algebraically closed field and* $X \subseteq \mathbf{F}^n$ *is an irreducible variety and* $\phi : \mathbf{F}[x_1, \cdots, x_n] \to \mathbf{F}[x_1, \cdots, x_n]/I(X) = A(X)$ *is the natural projection, then the maps* $B \mapsto V\big(\phi^{-1}(B)\big)$ *and* $Y \mapsto \phi\big(I(Y)\big)$ *give a bijective order-reversing correspondence between the set of all radical ideals* $B \subseteq A(X)$ *and the set of all varieties* $Y \subseteq X$*. Under this correspondence, every maximal ideal* $M \subseteq A(X)$ *corresponds to a point in* X*, and every prime ideal* $P \subseteq A(X)$ *corresponds to an irreducible variety* $Y \subseteq X$*.*

Proof: This follows from the previous corollary together with the fact that, when R is a commutative ring and $I \subseteq R$ is an ideal and $\phi : R \to R/I$ is the natural projection, the maps $A \mapsto \phi(A)$ and $B \mapsto \phi^{-1}(B)$ give a bijective correspondence between the set of ideals $A \subseteq R$ with $I \subseteq A$ and the set of all ideals $B \subseteq R/I$ and that, under this correspondence, radical and prime and maximal ideals $A \subseteq R$ with $I \subseteq A$ correspond to radical and prime and maximal ideals $B \subseteq R/I$.

8.12 Corollary: *If* $\mathbf{F}$ *is an algebraically closed field and* $X \subseteq \mathbf{F}^n$ *is a variety, then every radical ideal* $A \subseteq A(X)$ *can be decomposed uniquely (up to order) as* $A = P_1 \cap P_2 \cap \cdots \cap P_l$ *for some prime ideals* $P_i \subseteq A(X)$ *with no* P_i *contained in any other* P_j*.*

8.13 Corollary: *If* $\mathbf{F}$ *is algebraically closed, and if* $f \in \mathbf{F}[x_1, \cdots, x_n]$ *is an irreducible polynomial, then* $X = V(f) \subseteq \mathbf{F}^n$ *is an irreducible variety with* $I(X) = \langle f \rangle$*. More generally, if* $f \in \mathbf{F}[x_1, \cdots, x_n]$ *decomposes into irreducible factors as* $f = {f_1}^{k_1} {f_2}^{k_2} \cdots {f_l}^{k_l}$*, then the irreducible components of the variety* $X = V(f)$ *are the varieties* $V(f_i)$*.*

8.14 Example: In $\mathbf{C}[x, y]$, the polynomial $f(x, y) = y^2 + x^2(x-1)^2$ factors into irreducibles as $f(x, y) = \big(y + i\,x(x-1)\big)\big(y - i\,x(x-1)\big)$, and so the irreducible components of the variety $V(f) \subseteq \mathbf{C}^2$ are the varieties $V(y + i\,x(x-1))$ and $V(y - i\,x(x-1))$. On the other hand, the same polynomial $f(x, y)$ is irreducible in $\mathbf{R}[x, y]$, and in $\mathbf{R}^2$ we have $V(f) = \{(0, 0), (1, 0)\}$ which is a reducible variety.

8.15 Corollary: *If* $\mathbf{F}$ *is algebraically closed and* R *is an integral domain which is finitely generated over* $\mathbf{F}$*, then there exists an irreducible affine variety* X *with* $A(X) \cong R$*.*

Proof: Let $u_1, \cdots, u_n$ be generators for R over $\mathbf{F}$ so that we have $R = \mathbf{F}[u_1, \cdots, u_n]$. Let $\phi : \mathbf{F}[x_1, \cdots, x_n] \to R$ be the $\mathbf{F}$-algebra homomorphism given by $\phi(x_k) = u_k$ for $1 \le k \le n$. Let $P = \ker \phi$. Then P is an ideal and $R = \mathbf{F}[u_1, \cdots, u_n] \cong \mathbf{F}[x_1, \cdots, x_n]\big/P$. Since R is an integral domain, it follows that P is prime, hence radical. Since $\mathbf{F}$ is algebraically closed, it follows that P is closed. Thus for the variety $X = V(P) \subseteq \mathbf{F}^n$, we have $I(X) = P$. Since $I(X) = P$ and P is prime, it follows that $A(X) \cong R$ and X is irreducible.

8.16 Corollary: *If* $\mathbf{F}$ *is algebraically closed, and* $X \subseteq \mathbf{F}^n$ *and* $Y \subseteq \mathbf{F}^m$ *are irreducible varieties, and* $f : X \to Y$ *is a rational map with domain* X*, then* f *is a polynomial map.*

Proof: Suppose $f : X \to Y$ is well-defined at every point $a \in X$. For each $a \in X$ choose $p_a \in \mathbf{F}[x_1, \cdots, x_n]^m$ and $q_a \in \mathbf{F}[x_1, \cdots, x_n]$ such that $f = \frac{p_a}{q_a}$ and $q_a(a) \ne 0$. Let $A = \langle S \rangle$ where $S = \{q_a \big| a \in X\}$. By Hilbert's Basis Theorem, we can choose points $a_1, \cdots, a_\ell \in X$ such that $A = \big\langle q_{a_1}, \cdots, q_{a_\ell} \big\rangle$. Note that $V(A) = \emptyset$ because for all $a \in X$ we have $q_a \in A$ and $q_a(a) \ne 0$. By Hilbert's Weak Nullstellensatz, we must have $A = \mathbf{F}[x_1, \cdots, x_n]$. In particular, we have $1 \in A = \big\langle q_{a_1}, \cdots, q_{a_\ell} \big\rangle$ so we can write $1 = \sum\limits_{k=1}^{\ell} g_k q_{a_k}$ for some $g_k \in \mathbf{F}[x_1, \cdots, x_n]$. Then $f = 1 \cdot f = \sum\limits_{k=1}^{\ell} g_k q_{a_k} f = \sum\limits_{k=1}^{\ell} g_k p_{a_k}$, which is a polynomial map.

8.17 Example: In $\mathbf{R}[x]$ the rational map $f(x) = \frac{1}{x^2+1}$ is not a polynomial map.

8.18 Corollary: *Let* $\mathbf{F}$ *be algebraically closed, and let* $X \subseteq \mathbf{F}^n$ *and* $Y \subseteq \mathbf{F}^m$ *be irreducible varieties, Let* $f : Y \to X$ *is a dominant polynomial map and note that* $f^* : A(X) \to A(Y)$ *is injective so that* $A(X) \cong f^*\big(A(X)\big) \subseteq A(Y)$. *If* $A(Y)$ *is integral over* $f^*\big(A(X)\big)$ *then* f *is surjective.*

Proof: Let $a \in X$ and let $M \subseteq A(X)$ be the maximal ideal corresponding to a. Let $N = f^*(M)$. Since f is dominant so that f^* is injective, N is maximal in $f^*(A(X))$. By the Lying Over Theorem, since $A(Y)$ is integral over $f^*(A(X))$, we can choose a maximal ideal $N \subseteq A(Y)$ such that $N \cap f^*(A(X)) = f^*(M)$. Let $b \in Y$ be the element which corresponds to the maximal ideal N. We claim that $f(b) = a$. Let $g \in M$. Then $f^*(g) \in f^*(M) \subseteq N$. Since $f^*(g) \in N$ we have $f^*(g)(b) = 0$, that is $g(f(b)) = 0$. In particular, taking $g = x_k - a_k \in M$ we obtain $f_k(b) = a_k$ so that $f(b) = a$, as claimed.

8.19 Example: For $X = \mathbf{R}$ and $Y = V(y - x^2) \subseteq \mathbf{R}^2$, the projection map $f : Y \to X$ given by $f(x, y) = y$ is a dominant polynomial map, and $A(Y)$ is integral over $f^*\big(A(X)\big)$, but f is not surjective.