STRONG NULLSTELLENSATZ: Let K be an algebraically closed field, and $R = K[X_1, \dots, X_n]$ be a polynomial ring. Let $I \subseteq R$ be an ideal and $f \in R$ a polynomial. Then

$$f \text{ vanishes at every point of } \mathcal{Z}(I) \text{ if and only if } f \in \sqrt{I}.$$

DEFINITION: Let K be a field and $R = K[X_1, \dots, X_n]$. A **subvariety** of K^n is a set of the form $\mathcal{Z}(S)$ for some set of polynomials $S \subseteq R$; i.e., a solution set of some system of polynomial equations.

COROLLARY: Let K be an algebraically closed field. There is a bijection

$$\{\text{radical ideals in } K[X_1, \dots, X_n]\} \longleftrightarrow \{\text{subvarieties of } K^n\}.$$

(1) Proof of Strong Nullstellensatz:

(a) Show that $\mathcal{Z}(I) = \mathcal{Z}(\sqrt{I})$, and deduce the ($\Leftarrow$) direction.

(b) Let Y be an extra indeterminate. Show that f vanishes on $\mathcal{Z}(I)$ implies that

$$\mathcal{Z}\big(I + (Yf - 1)\big) = \varnothing \quad \text{in } K^{n+1}.$$

(c) What does the Nullstellensatz have to say about that?

(d) Apply the R-algebra homomorphism $\phi : R[Y] \to \mathrm{frac}(R)$ given by $\phi(Y) = \frac{1}{f}$ and clear denominators.

(a) Since $I \subseteq \sqrt{I}$, we have $\mathcal{Z}(\sqrt{I}) \subseteq \mathcal{Z}(I)$. On the other hand, if $\alpha \in \mathcal{Z}(I)$ and $f^n \in I$, then $f^n(\alpha) = 0$, so $f(\alpha) = 0$, so $\alpha \in \mathcal{Z}(\sqrt{I})$. In particular, the ($\Leftarrow$) direction of the statement holds.

(b) If there was a solution (α, a), this would mean $\alpha \in \mathcal{Z}(I)$ and $af(\alpha) - -1 = 0$, so $f(\alpha) \neq 0$, contradicting that $\alpha \in \mathcal{Z}(f)$.

(c) We can write $1 = \sum_i r_i(\underline{X}, Y) g_i(\underline{X}) + s(\underline{X}, Y)(Yf(\underline{X}) - 1)$ for some $r_i, s \in R[Y]$ and $g_i \in I$.

(d) We get $1 = \sum_i r_i(\underline{X}, 1/f) g_i(\underline{X}) + s(\underline{X}, 1/f)(1/f \cdot f(\underline{X}) - 1)$. The last term dies so $1 = \sum_i r_i(\underline{X}, 1/f) g_i(\underline{X})$. We can clear denominators to get $f^n = \sum r_i'(\underline{X}) g_i(\underline{X})$ in R, so $f^n \in I$.

(2) Strong Nullstellensatz warmup:

(a) Consider the ideal $I = (X^2 + Y^2) \in \mathbb{R}[X, Y]$ and $f = X$. Discuss the hypotheses and conclusion of Strong Nullstellensatz in this example.

(b) Show that[1] no power of $F = X^2 + Y^2 + Z^2$ is in the ideal

$$I = (X^3 - Y^2 Z, Y^7 - XZ^3, 3X^5 - XYZ - 2Z^{19}) \quad \text{in the ring} \quad \mathbb{C}[X, Y, Z].$$

(a) $\mathcal{Z}(I) = \{(0,0)\}$ and X vanishes along $\mathcal{Z}(I)$, but $(X^2 + Y^2)$ is prime and hence radical. The conclusion of Strong Nullstellensatz fails. Of course, $\mathbb{R}$ is not algebraically closed.

(b) $F(1,1,1) = 3 \neq 0$ but $(1,1,1) \in \mathcal{Z}(I)$, since it is in the zero-set of each generator.

(3) Prove the Corollary.

[1] Hint: You just need to find one point. *One*, *one*, *one*...

We have a map from radical ideals to subvarieities given by $I \mapsto \mathcal{Z}(I)$. This is surjective by definition and the first part of the proof of Strong Nullstellensatz. It is injective too: if I and J are distinct radical ideals, without loss of generality there is some $f \in J$ such that $f \notin \sqrt{I}$; then $f(\alpha) \neq 0$ for some $\alpha \in \mathcal{Z}(I)$, so $\mathcal{Z}(I) \not\subseteq \mathcal{Z}(J)$.

(4) Let $R = \mathbb{C}[T]$ be a polynomial ring. In this problem, we will show that the ideal of $\mathbb{C}$-algebraic relations on the elements $\{T^2, T^3, T^4\}$ is $I = (X_1^2 - X_3, X_2^2 - X_1 X_3)$.

(a) Let $\phi : \mathbb{C}[X_1, X_2, X_3] \to \mathbb{C}[T]$ be the $\mathbb{C}$-algebra map $X_1 \mapsto T^2, X_2 \mapsto T^3, X_3 \mapsto T^4$. Show that $I \subseteq \ker(\phi)$.

(b) Show that $\mathcal{Z}(I) \subseteq \{(\lambda^2, \lambda^3, \lambda^4) \in \mathbb{C}^3 \mid \lambda \in \mathbb{C})\} \subseteq \mathcal{Z}(\ker(\phi))$, and deduce that $\ker(\phi) \subseteq \sqrt{I}$.

(c) Show that I is prime[2], and complete the proof.

(a) The generators map to 0 under ϕ.

(b) For the first containment, let $(\alpha, \beta, \gamma) \in \mathcal{Z}(I)$. From the first equation, we can write $\gamma = \alpha^2$. From the second, we have $\beta^2 = \alpha^3$. If $\alpha = 0$, we must have $(0,0,0)$. Otherwise, α has two square roots. Take λ to be one of these. Then $\alpha = \lambda^2$ and $\beta^2 = \lambda^6$. This means $\beta = \pm\lambda^3$. If $\beta = -\lambda^3$, replace λ by $-\lambda$; this does not change $\alpha = \lambda^2$ or $\gamma = \lambda^4$. So, we obtain λ such that $(\alpha, \beta, \gamma) = (\lambda^2, \lambda^3, \lambda^4)$.

For the second, if $F(X_1, X_2, X_3) \in \ker(\phi)$, then $F(T^2, T^3, T^4) = 0$, so $F(\lambda^2, \lambda^3, \lambda^4) = 0$.

(c) Using the first relation and an isomorphism theorem, $\mathbb{C}[X_1, X_2, X_3]/I \cong \mathbb{C}[X_1, X_2]/(X_2^2 - X_1^3)$. The element $X_2^2 - X_1^3$ is irreducible by Eisenstein's criterion, so I is prime.

(5) Let K be an algebraically closed field and $R = K\begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix}$ be a polynomial ring. Use the Strong Nullstellensatz to show that any polynomial $F(X_{11}, X_{12}, X_{21}, X_{22})$ that vanishes on every matrix of rank at most one is a multiple of $\det \begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix}$.

(6) We say that a subvariety of K^n is **irreducible** if it cannot be written as a union of two proper subvarities. Show that the bijection from the Corollary restricts to a bijection

$$\{\text{prime ideals in } K[X_1, \dots, X_n]\} \longleftrightarrow \{\text{irreducible subvarieties of } K^n\}.$$

Let I be a radical ideal. We need to show that $\mathcal{Z}(I)$ is irreducible if and only if I is prime.

Suppose that I is not prime, so one has $f, g \notin I$ with $fg \in I$. Since I is radical, $f, g \notin \sqrt{I}$, so $\mathcal{Z}(f), \mathcal{Z}(g) \not\supseteq \mathcal{Z}(I)$. This means that $\mathcal{Z}(I + (f))$ and $\mathcal{Z}(I + (g))$ are proper subvarieties of $\mathcal{Z}(I)$. But $\alpha \in \mathcal{Z}(I)$ and $fg \in I$ implies $f(\alpha)g(\alpha) = 0$ so $f(\alpha) = 0$ or $g(\alpha) = 0$, which means $\mathcal{Z}(I) = \mathcal{Z}(I + (f)) \cup \mathcal{Z}(I + (g))$.

Conversely, suppose that $\mathcal{Z}(I) = \mathcal{Z}(J_1) \cup \mathcal{Z}(J_2)$, with J_1, J_2 radical and not equal to I. Since $\mathcal{Z}(I) \supseteq \mathcal{Z}(J_i)$ we have $J_i \supsetneq I$. We can take $f \in J_1 \setminus J_2$ and $g \in J_2 \setminus J_1$. Since $f(\alpha) = 0$ for all $\alpha \in \mathcal{Z}(J_1)$, $g(\alpha) = 0$ for all $\alpha \in \mathcal{Z}(J_2)$, and $\mathcal{Z}(I) = \mathcal{Z}(J_1) \cup \mathcal{Z}(J_2)$, we have $fg(\alpha) = 0$ for all $\alpha \in \mathcal{Z}(I)$, so $fg \in I$, and I is not prime.

[2] Show $\mathbb{C}[X_1, X_2, X_3]/I$ is a domain by simplifying the quotient.

(7) Use the Strong Nullstellensatz to show that, in a finitely generated algebra over an algebrically closed field, every radical ideal can be written as an intersection of maximal ideals.