# §4.16: NULLSTELLENSATZ

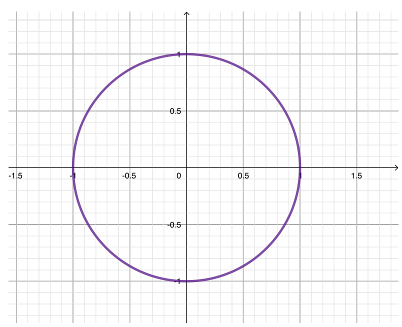
DEFINITION: Let $K$ be a field and $R = K[X_1, \dots, X_n]$. For a set of polynomials $S \subseteq R$, we define the **zero-set** of **solution set** of $S$ to be

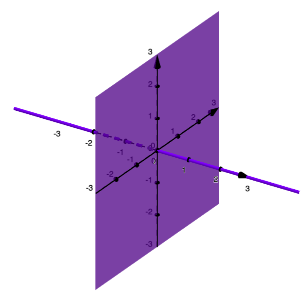
$$\mathcal{Z}(S) := \{(a_1, \dots, a_n) \in K^n \mid F(a_1, \dots, a_n) = 0 \text{ for all } F \in S\}.$$

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. Then $\mathcal{Z}(I) = \varnothing$ if and only if $I = R$ is the unit ideal.
Put another way, a set $S$ of multivariate polynomials has a common zero unless there is a "certificate of infeasibility" consisting of $f_1, \dots, f_t \in S$ and $r_1, \dots, r_t \in R$ such that $\sum_i r_i s_i = 1$.

PROPOSITION: Let $K$ be an algebraically closed field, and $R = K[X_1, \dots, X_n]$ be a polynomial ring. Every maximal ideal of $R$ is of the form $\mathfrak{m}_\alpha = (X_1 - a_1, \dots, X_n - a_n)$ for some point $\alpha = (a_1 \dots, a_n) \in K^n$.

**(1)** Draw the "real parts" of $\mathcal{Z}(X^2 + Y^2 - 1)$ and of $\mathcal{Z}(XY, XZ)$.





**(2)** Explain why the Nullstellensatz is definitely false if $K$ is assumed to *not* be algebraically closed.

To not be algebraically closed means that there is a nonconstant polynomial in one variable that has empty solution set; such a polynomial generates a proper ideal.

**(3)** Basics of $\mathcal{Z}$: Let $R = K[X_1, \dots, X_n]$ be a polynomial ring.

**(a)** Explain why, for any system of polynomial equations $F_1 = G_1, \dots, F_m = G_m$, the solution set can be written in the form $\mathcal{Z}(S)$ for some set $S$.

**(b)** Let $S \subseteq T$ be two sets of polynomials. Show that $\mathcal{Z}(S) \supseteq \mathcal{Z}(T)$.

**(c)** Let $I = (S)$. Show that $\mathcal{Z}(I) = \mathcal{Z}(S)$. Thus, every solution set system of any polynomial equations can be written as $\mathcal{Z}$ of some ideal.

**(d)** Explain the following: every system of equations over a polynomial ring is equivalent to a *finite* system of equations.

**(e)** Given a system of polynomial equations and inequations

$$(\star) \qquad F_1 = 0, \dots, F_m = 0 \qquad G_1 \neq 0, \dots, G_\ell \neq 0$$

come up with a system[1] of equations $(\dagger)$ such that $(\star)$ has a solution if and only if $(\dagger)$ has a solution. Thus every equation-and-inequation feasibility problem is equivalent to a question of the form $\mathcal{Z}(I) \stackrel{?}{=} \varnothing$.

[1]Hint: $\lambda \in K$ is nonzero if and only if there is some $\mu$ such that $\lambda\mu = 1$. You can use more variables if you want!

**(a)** Take $S = \{F_1 - G_1, \dots, F_m - G_m\}$.
**(b)** $\alpha \in \mathcal{Z}(T)$ implies $F(\alpha) = 0$ for all $F \in T$ implies $F(\alpha) = 0$ for all $F \in S$ implies $\alpha \in \mathcal{Z}(S)$.
**(c)** Since $S \subseteq I$ we have $\mathcal{Z}(S) \supseteq \mathcal{Z}(I)$. On the other hand, if $\alpha \in \mathcal{Z}(S)$ and $F \in I$, then $F = \sum_i r_i s_i$ with $s_i \in S$, and $F(\alpha) = \sum_i r_i(\alpha) s_i(\alpha) = \sum_i r_i(\alpha) \cdot 0 = 0$. Thus $\alpha \in \mathcal{Z}(I)$.
**(d)** We can write any system as $\mathcal{Z}(I)$. By the Hilbert Basis Theorem, $I = (f_1, \dots, f_m)$, and $\mathcal{Z}(I) = \mathcal{Z}(f_1, \dots, f_m)$, which is equivalent to the system $f_1 = 0, \dots, f_m = 0$.
**(e)** We can take $F_1 = 0, \dots, F_m = 0, G_1 G_2 \dots G_\ell Y - 1 = 0$: a solution of this must consist of a solution of $(\star)$ for the $X$'s and the inverse of the product of the $G_i(X)$ for $Y$.

**(4)** Proof of Proposition and Nullstellensatz: Let $K$ be an algebraically closed field, and $R = K[X_1, \dots, X_n]$ be a polynomial ring.
  **(a)** Use Zariski's Lemma to show that for every maximal ideal $\mathfrak{m} \subseteq R$, we have $R/\mathfrak{m} \cong K$.
  **(b)** Reuse some old work to deduce the Proposition.
  **(c)** Deduce the Nullstellensatz from the Proposition.
  **(d)** Convince yourself that the "certificate of infeasibility" version follows from the other one.

**(a)** The ring $R/\mathfrak{m}$ is a finitely generated $K$-algebra and a field, so $K \subseteq R/\mathfrak{m}$ is module-finite by Zariski's Lemma. Since $K$ is algebraically closed, we must have $K \cong R/\mathfrak{m}$.
**(b)** From worksheet #2, we know that any maximal ideal in a polynomial ring with $R/\mathfrak{m} \cong K$ is of the form $\mathfrak{m}_\alpha$ for some $\alpha$.
**(c)** If $I$ is a proper ideal, then $I \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, and from above $I \subseteq \mathfrak{m}_\alpha$ for some $\alpha$. Then $\mathcal{Z}(I) \supseteq \mathcal{Z}(\mathfrak{m}_\alpha) = \{\alpha\}$ is nonempty!
**(d)** This is just unpackaging what it means for $(S)$ to be the unit ideal.

(5) Show that any system of multivariate polynomial equations (or equations and inequations) over a field $K$ has a solution in some extension field of $L$ if and only if it has a solution over $\overline{K}$.

(6) Let $K$ be a field and $R = K[X_1, \dots, X_n]$. Let $L \supseteq K$ and $S = L[X_1, \dots, X_n]$.
  (a) Find some $f$ that is irreducible in $R$ but reducible in $S$ for some choice of $K \subseteq L$.
  (b) Show that if $K$ is algebraically closed and $f \in R$ is irreducible, then it is irreducible in $S$.
  (c) Show that if $K$ is algebraically closed and $I \subseteq R$ is prime, then $IS$ is prime.

(7) Show that the statement of the Nullstellensatz holds for the ring of continuous functions from $[0, 1]$ to $\mathbb{R}$.