

## §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** or **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  $\mathcal{Z}(I) = \emptyset$  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.
- (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.
- (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.

- (5)** Given a system of polynomial equations and inequations

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

come up with a system<sup>1</sup> of equations  $(\dagger)$  *in one extra variable* 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  $\mathcal{Z}(I) \stackrel{?}{=} \emptyset$ .

<sup>1</sup>Hint:  $\lambda \in K$  is nonzero if and only if there is some  $\mu$  such that  $\lambda\mu = 1$ .

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