Lesson 23 – Three Nullstellensatz Theorems

Disclaimer: In these notes, I am trying to convey a general understanding of the Nullstellensatz Theorems. In an attempt to convey ideas without getting too bogged down in the details, I have decided to concentrate on the single-variable situation *when providing full proofs.* Please read the detailed proofs for the multivariate situation in your textbook – particularly for the Weak Nullstellensatz.

Today we will discuss three (equivalent) Nullstellensatz Theorems: *The Weak Nullstellensatz Theorem*, *Hilbert's Nullstellensatz Theorem*, and *The Strong Nullstellensatz Theorem*.

I. The Weak Nullstellensatz Theorem

Let $f_1(x), f_2(x), \ldots, f_m(x) \in \mathbb{C}[x]$. When do we know that the polynomial equations

$$f_1(x) = f_2(x) = \cdots = f_m(x) = 0$$

do NOT have a complex solution? That is, when is $\mathbf{V}(f_1, f_2, \ldots, f_m) = \phi$? A guarantee for an empty solution set is the existence of polynomials $q_1(x), q_2(x), \ldots, q_m(x) \in \mathbb{C}[x]$ such that

$$q_1(x)f_1(x) + q_2(x)f_2(x) + \cdots + q_m(x)f_m(x) = 1$$

Example Consider the polynomial system in $\mathbb{C}[x]$:

$$\begin{aligned} f_1(x) &= 1 + x^2 \\ f_2(x) &= 1 + x^2 + x^4 \end{aligned}$$

Exercise 1 Show that $\mathbf{V}(f_1, f_2) = \phi$.

Lemma (Weak Nullstellensatz in one variable). Let $f_1(x), f_2(x), \ldots, f_m(x) \in k[x]$, where k is an algebraically closed field. Then $\mathbf{V}(f_1, f_2, \ldots, f_m) = \phi$ if and only if there exists $q_1(x), q_2(x), \ldots, q_m(x) \in k[x]$ such that

$$q_1(x)f_1(x) + q_2(x)f_2(x) + \cdots + q_m(x)f_m(x) = 1$$

Proof.

The result generalizes to ideals of multivariate polynomials...

Theorem 1 (The Weak Nullstellensatz). Let k be an algebraically closed field and let $I \subseteq k[x_1, x_2, \dots, x_n]$. Then $\mathbf{V}(I) = \phi$ if and only if $I = k[x_1, x_2, \dots, x_n]$.

See the textbook for this proof. One direction is trivial. Clearly, if $I = k[x_1, x_2, \dots, x_n]$, then $1 \in I$ and $\mathbf{V}(I) = \phi$. The reverse direction is proved by induction on the number of variables. The base case was proved in the previous lemma.

So the weak Nullstellensatz tells us precisely when $\mathbf{V}(f_1, f_2, \dots, f_m) = \phi$, that is, when a system of polynomial equations has no solution. Since $I = k[x_1, x_2, \dots, x_n]$ if and only if $1 \in I$, the Weak Nullstellensatz gives us the "The Consistency Theorem", which allows us to use Groebner bases to determine if a system of polynomial equations has a solution.

The Consistency Theorem. Let k be an algebraically closed field and let $I \subseteq k[x_1, x_2, \dots, x_n]$. Then the following are equivalent:

- $I = k[x_1, x_2, \dots, x_n]$
- $1 \in I$
- $\mathbf{V}(f_1, f_2, \dots, f_m) = \phi$
- I has the reduced Groebner basis $G = \{1\}$.

Exercise 2 Explain why the last bulleted statement is equivalent to the rest.

Exercise 3. Show that the Weak Nullstellensatz Theorem holds if <u>and only if</u> k is an algebraically closed field.

Question: The Nullstellensatz theorems[1] are sometimes described as a generalization of the Fundamental Theorem of Algebra. Why?

---

[1] Incidentally, the name "Nullstellensatz" is German for "zero locus theorem" (Null = zero, stellen = places, satz = theorem).

II. Hilbert's Nullstellensatz

Now suppose $\mathbf{V}(f_1, f_2, \dots, f_m) \neq \phi$. How do we know when a particular f vanishes at all points in $\mathbf{V}(f_1, f_2, \dots, f_m)$?

Theorem (Hilbert's Nullstellensatz in one variable). Let $f_1(x), f_2(x), \dots, f_s(x) \in k[x]$, where k is an algebraically closed field. Then $f \in \mathbf{I}(\mathbf{V}(f_1, f_2, \dots, f_s))$ if and only if there exists an integer $m \geq 1$ and $q_1(x), q_2(x), \dots, q_s(x) \in k[x]$ such that

$$f(x)^m = q_1(x)f_1(x) + q_2(x)f_2(x) + \cdots + q_s(x)f_s(x)$$

i.e. iff $f^m \in I = \langle f_1, f_2, \dots, f_s \rangle$.

Proof. As your text states, the proof makes use of an "ingenious trick" which involves introducing an additional variable, y. (We have used this trick before. Do you remember when?)

Consider the system of polynomial equations in $k[x, y]$:

$$f_1(x) = f_2(x) = \cdots = f_s(x) = 0$$

$$1 - yf(x) = 0$$

Exercise 4 Show that if $x \in \mathbf{V}(f_1, f_2, \dots, f_s)$ then $1 \in \langle f_1, f_2, \dots, f_s, 1 - yf \rangle$.

Exercise 5 By the previous exercise, there exist polynomials $Q_1(x, y), \dots, Q_s(x, y), Q(x, y)$ $\in$ $k[x, y]$ such that

$$Q_1(x, y)f_1(x) + Q_2(x, y)f_2(x) + \cdots + Q_s(x, y)f_s(x) + Q(x, y)(1 - yf(x)) = 1.$$

Show that there exists an $m \in \mathbb{N}$ such that $f^m(x) \in I = \langle f_1, f_2, \dots, f_s \rangle$. This completes the forward direction of the theorem.

Exercise 6 The converse requires no ingenuity, but let's prove it for the sake of completion.

Theorem (The full-blown Hilbert Nullstellensatz) Let k be an algebraically closed field and let $I = \langle f_1, f_2, \dots, f_s \rangle \subseteq k[x_1, x_2, \dots, x_n]$. If $f \in k[x_1, x_2, \dots, x_n]$, then $f \in \mathbf{I}(\mathbf{V}(f_1, f_2, \dots, f_s))$ if and only if there exists an integer $m \geq 1$ such that $f^m \in I$.

Proof. Again, this proof is very similar to the single-variable case. See pages 173-174 in your textbook.

Exercise 7 Give an example of a polynomial $f \in k[x, y]$, with k algebraically closed, and an ideal $I = \langle f_1, f_2, \dots, f_s \rangle \subseteq k[x, y]$ satisfying $f \in \mathbf{I}(\mathbf{V}(f_1, f_2, \dots, f_s))$ but $f \notin I = \langle f_1, f_2, \dots, f_s \rangle$.

III. The Strong Nullstellensatz Theorem

The key to the relation between an ideal I and the ideal $\mathbf{I}(\mathbf{V}(I))$ is illustrated in Exercise 5. Whereas I may contain some polynomial power f^m, the ideal of the variety then contains f itself. This motivates the notion of a *radical ideal*.

Definition An ideal I is called **radical** if whenever $f^m \in I$ for some $m \geq 1$, then $f \in I$.

It is clear that for any variety V, the $\mathbf{I}(V)$ is radical.

Definition Let $I \subseteq k[x_1, x_2, \dots, x_n]$ be an ideal. Its radical, $\sqrt{I}$, is the set

$$\sqrt{I} = \{f \in k[x_1, x_2, \dots, x_n] : f^m \in I \text{ for some } m \geq 1\}.$$

Exercise 8 Consider the ideal $I = \langle x + y, (x - y)^2 \rangle$. Show that $x \in \sqrt{I}$.

It is an easy exercise to prove that $\sqrt{I}$ is itself an ideal, and of course, radical. Moreover, $\mathbf{V}(I) = \mathbf{V}(\sqrt{I})$.

Theorem (The Strong Nullstellensatz Theorem). Let k be an algebraically closed field and let $I \subseteq k[x_1, x_2, \ldots, x_n]$ be an ideal. Then

$$\mathbf{I}\big(\mathbf{V}(I)\big) = \sqrt{I}.$$

Proof.