HILBERT'S NULLSTELLENSATZ

Reference: Section 1.7 "Algebraic curves" Fulton.

In the previous classes we have seen that we have a correspondence between algebraic sets $V \subseteq \mathbb{A}^n(k)$ and ideals $I \subseteq k[x_1, \dots, x_n]$.

$$\left\{ \begin{array}{c} \text{Algebraic sets} \\ V \subseteq \mathbb{A}^n(k) \end{array} \right\} \qquad \left\{ \begin{array}{c} \text{Ideals} \\ I \subseteq k[x_1, \dots, x_n] \end{array} \right\}$$

$$V \longmapsto I(V)$$

$$V(I) \longleftarrow\!\!\shortmid \; I$$

Neverthless this correspondence is not one-to-one: in particular the map $V \longmapsto I(V)$ is not surjective, since we have seen that it covers only radical ideals of $k[x_1, \dots, x_n]$.

We will see that, for k an algebraically closed field, if we replace the set of ideals of $k[x_1, \dots, x_n]$ with the set of radical ideals of $k[x_1, \dots, x_n]$, then the map $I \longmapsto V(I)$ becomes injective and we get a one-to-one correspondence.

The Hilbert's Nullstellensatz or Zeros-theorem represents the basis of algebraic geometry, because it tell us this exact relationship between ideals and algebraic sets.

HILBERT'S NULLSTELLENSATZ

Let k be an algebraically closed field.

If I is an ideal of $k[x_1, \dots, x_n]$, then.

$$I(V(I)) = \mathrm{Rad}(I).$$

The reason of the name "nullstellensatz" (from German literally "zero-locus-theorem") is clearer when we look at a somewhat weaker form of the previous theorem:

WEAK NULLSTELLENSATZ

Let k be an algebraically closed field.
If $I \subsetneq k[x_1, \dots, x_n]$ is a proper ideal, then $V(I) \neq \emptyset$.

We will first prove the Weak Nullstellensatz and then deduce the the main theorem from it.

We will need the following result:

Zariski's lemma: If K is a field and A is a finitely generated K-algebra, then for all maximal ideals $M \subsetneq A$ $\frac{A}{I}$ is a finite extension of K.

Proof (Weak Nullstellensatz)

We can assume I maximal. Indeed, for every proper ideal $I \subsetneq K[x_1,\dots,x_n]$ there exists a maximal ideal $M \subseteq K[x_1,\dots,x_n]$ such that $I \subseteq M \Rightarrow V(I) \supseteq V(M)$. So if we show that $V(M) \neq \emptyset$, then we have also $V(I) \neq \emptyset$.

If I is maximal then $\frac{K[x_1,\dots,x_n]}{I}$ is a field.

Moreover, the map:

$$\begin{aligned} K &\longrightarrow \frac{K[x_1,\dots,x_n]}{I} \\ a &\longmapsto \bar{a} = a + I \end{aligned}$$

is injective: if $\bar{a} = 0 \Rightarrow a \in I \Rightarrow a = 0$, since a can not be a unit.

Then we have that $K \subseteq \frac{K[x_1,\dots,x_n]}{I}$ is a field extension.

Moreover, by the Zariski's lemma, $\frac{K[x_1,\dots,x_n]}{I}$ is a finite extension of K.

Since K is algebraically closed, this implies

$$\frac{K[x_1,\dots,x_n]}{I} \approx K.$$

Let φ be an isomorphism between $\frac{K[x_1,\dots,x_n]}{I}$ and K:

$$\begin{aligned} \varphi : \frac{K[x_1,\dots,x_n]}{I} &\xrightarrow{\sim} K \\ \bar{x}_1 &\longmapsto a_1 \\ &\vdots \\ \bar{x}_n &\longmapsto a_n \\ \bar{a} &\longmapsto a \end{aligned}$$

So $\forall i \ \varphi(\overline{x_i}) = \varphi(\overline{a_i}) \overset{\varphi \text{ injective}}{\Longrightarrow} \forall i \ \ \overline{x_i} = \overline{a_i} \Rightarrow \forall i \ \ x_i - a_i \in I$

$\Rightarrow (x_1 - a_1, \dots, x_n - a_n) \subseteq I \underset{\substack{(x_1-a_1,\dots,x_n-a_n) \\ \text{maximal ideal}}}{\Longrightarrow} I = (x_1-a_1,\dots,x_n-a_n) \Rightarrow$

$\Rightarrow V(I) = \{(a_1,\dots,a_n)\} \neq \emptyset$

$\square$

<u>Remark</u>: Note that in the Weak Nullstellensatz the hypothesis for k to be algebraically closed can not be removed:

If in $\mathbb{R}[x]$ we consider the ideal $I = (x^2+1)$, we have $V(I) = \emptyset$ and $I \subsetneq \mathbb{R}[x]$.

<u>Proof</u> (Hilbert's Nullstellensatz)

We want to show that if $I \subseteq k[x_1,\dots,x_n]$ then

$$\mathrm{Rad}(I) = I(V(I))$$

($\subseteq$) We have

$$I \subseteq I(V(I))$$
$$\Downarrow$$
$$\mathrm{Rad}(I) \subseteq \mathrm{Rad}(I(V(I))) \underset{\substack{I(V(I)) \text{ is a} \\ \text{radical ideal}}}{=} I(V(I))$$

✓

($\supseteq$) For this part of the proof we will used the so called "Rabinowitsch trick".

Since $k[x_1,\dots,x_n]$ is Noetherian, then there exist $F_1,\dots,F_r \in$ $\in k[x_1,\dots,x_n]$ such that:

$$I = (F_1,\dots,F_r).$$

Let $G \in I(V(I))$. We want to show that $G \in \mathrm{Rad}(I)$, ie. $\exists N > 0$ such that $G^N \in I$.

Let us consider the following ideal:

$$J = (F_1,\dots,F_r, x_{n+1}G - 1) \subseteq k[x_1,\dots,x_n,x_{n+1}].$$

Note that $V(J) = V(I) \cap V(x_{n+1}G - 1) \underset{G \in I(V(I))}{=} \emptyset \subseteq \mathbb{A}^{n+1}(k)$.

Then, by the Weak Nullstellensatz, we get $J = K[X_1, \dots, X_{n+1}]$, i.e. $1 \in J$.

So $\exists\ A_i(X_1, \dots, X_{n+1}),\ B(X_1, \dots, X_{n+1}) \in K[X_1, \dots, X_{n+1}]$ such that:

$$1 = \sum_{i=1}^{r} A_i(X_1, \dots, X_{n+1}) F_i + B(X_1, \dots, X_{n+1})(X_{n+1} \cdot G - 1)$$

In particular, if we replace $X_{n+1} = \frac{1}{G}$ and we clear the denominators by multiplying by a suitable power of G, we get:

$$G^N \cdot 1 = \sum_{i=1}^{r} A_i\left(X_1, \dots, \frac{1}{G}\right) \cdot G^N \cdot F_i + B\left(X_1, \dots, \frac{1}{G}\right)\left(\frac{1}{G} G - 1\right) \cdot G^N$$

$$\Downarrow$$

$$G^N = \sum_{i=1}^{r} \tilde{A}_i(X_1, \dots, X_n) \cdot F_i + 0.$$

$$\Downarrow$$

$$G^N = \sum_{i=1}^{r} \underbrace{\tilde{A}_i(X_1, \dots, X_n)}_{\in K[X_1, \dots, X_n]} \cdot F_i \in (F_1, \dots, F_r) = I.$$

$\square$

We can easily deduce some corollaries from the Hilbert's Nullstellensatz, which hold if and only if K is alg. closed.

Corollary 1: If $I \subseteq K[X_1, \dots, X_n]$ is radical, then $I(V(I)) = I$

There is a one-to-one correspondence between radical ideals of $K[X_1, \dots, X_n]$ and algebraic sets of $\mathbb{A}^n(K)$.

Corollary 2: If $I \subseteq K[X_1, \dots, X_n]$ is a prime ideal then $V(I)$ is irreducible.

There is a one-to-one correspondence between prime ideals of $K[X_1, \dots, X_n]$ and irreducible algebraic sets of $\mathbb{A}^n(K)$.

The maximal ideals correspond to points.

Proof (Corollary 2)

Note, first, that if I is prime, then I is radical.

Indeed, if $F \in K[X_1, \dots, X_n]$ is such that $F^n \in I$, $n > 0$ $\Rightarrow$ $\xRightarrow{I \text{ prime}}$ $F \in I$.

Recall that $V(I)$ is irreducible if and only if $I(V(I))$ is prime. We have:

$$I(V(I)) \underset{\substack{\uparrow \\ \text{Hilbert's Null.}}}{=} \operatorname{Rad}(I) \underset{\substack{\uparrow \\ I \text{ is} \\ \text{radical}}}{=} I$$, which is prime by hypothesis.

Corollary 3: Let F be a non constant polynomial in $K[x_1, \dots, x_n]$ with a decomposition into irreducible factors given by:

$$F = F_1^{n_1} \cdots F_r^{n_r}, \quad F_i \text{ irreducible}.$$

Then

$$V(F) = V(F_1) \cup \cdots \cup V(F_r)$$

is the decomposition into irreducible components and

$$I(V(F)) = (F_1 \cdots F_r)$$

Remarks: From corollary 3 we get that any hypersurface in $\mathbb{A}^n(K)$ is uniquely defined by a polynomial whose factorization into irreducible components has no multiple factors (up to a constant multiple).

We had already proved this result in the particular case of algebraic plane curves.

K algebraically closed

Corollary 1: $\{\text{Algebraic sets} \subseteq \mathbb{A}^n(K)\} \longleftrightarrow \{\text{radical ideals} \subseteq K[x_1, \dots, x_n]\}$

Corollary 2:

$\{\text{Irreducible algebraic sets} \subseteq \mathbb{A}^n(K)\} \longleftrightarrow \{\text{prime ideals} \subseteq K[x_1, \dots, x_n]\}$

$\{\text{points} \in \mathbb{A}^n(K)\} \longleftrightarrow \{\text{maximal ideals} \subseteq K[x_1, \dots, x_n]\}$

Corollary 3: $\{\text{irreducible hypersurfaces} \subseteq \mathbb{A}^n(K)\} \longleftrightarrow \{\text{irreducible polynomials} \in K[x_1, \dots, x_n] \text{ up to constant multiple}\}$