Hilbert's Nullstellensatz

Recall the relationships we know so far between ideals and algebraic sets.

We have a map $V: \{\text{ideals in } k[x_1,\dots,x_n]\} \to \{\text{alg. sets in } \mathbb{A}^n_k\}$

- map is inclusion-reversing: $I \subseteq J \Rightarrow V(J) \subseteq V(I)$.
- surjective (by def)
- If X is algebraic, $V(I(X)) = X$, so I is a right inverse.
- $V(x^2) = V(x)$, so it's not injective.
- However, $V(I) = V(\sqrt{I})$.

If we restrict our attention to radical ideals, is V a bijection?

Note that this is not true over e.g. $\mathbb{R}$:
x^2+y^2 is irreducible, thus (x^2+y^2) and (x,y) are both prime and thus radical over $\mathbb{R}$. However, the zero set of each is $(0,0)$.

The Nullstellensatz says that if k is algebraically closed, we do get a bijection:

Hilbert's Nullstellensatz: Let k be algebraically closed and

$I \subseteq k[x_1, \dots, x_n]$ an ideal. Then $I(V(I)) = \sqrt{I}$.

(Thus I is a left inverse when V is restricted to radical ideals)

In order to prove this, we first need the following.

Weak Nullstellensatz: If k is algebraically closed and $I \subsetneq k[x_1, \dots, x_n]$ a proper ideal, then $V(I) \neq \emptyset$.

Pf: Find a maximal ideal $m \supset I$. Then $V(m) \subseteq V(I)$.

> Claim: Any maximal ideal $m \subseteq k[x_1, \dots, x_n]$ is of the form $(x_1 - a_1, \dots, x_n - a_n)$, $a_i \in k$.
> (we'll prove this next time.)

So $V(m) = \{(a_1, \dots, a_n)\}$. In particular, $V(I) \neq \emptyset$. $\square$

Proof of Nullstellensatz: We know $\sqrt{I} \subseteq I(V(I))$.

Let $I = (f_1, \dots, f_r)$. Suppose $g \in I(V(I))$.

Let $R = k[x_1, \dots, x_n]$ and $S = k[x_1, \dots, x_{n+1}]$.

Define $J = (f_1, \dots, f_r, x_{n+1} g - 1) \subseteq S$.

What is $V(J) \subseteq \mathbb{A}^{n+1}$? If $P \in V(J)$ then $f_i(P) = 0 \ \forall \ i$, so $g(P) = 0$.

Thus, $x_{n+1}g-1$ evaluated at P is not 0. $\Rightarrow V(J)=\emptyset$.

The weak Nullstellensatz implies that $J=S$, so $1\in J$.

$$\Rightarrow \sum a_i f_i + b(x_{n+1}g-1) = 1 \quad \text{for some} \quad a_1,\dots,a_r,b\in S.$$

Let N be the highest power of x_{n+1} appearing in the equation, and set $y=\frac{1}{x_{n+1}}$

Multiplying both sides of the equation by y^N and cancelling all the x_{n+1}'s yields

$$\sum \tilde{a}_i f_i + \tilde{b}(g-y) = y^N, \quad \text{where} \quad \tilde{a}_1,\dots,\tilde{a}_r,\tilde{b}\in k[x_1,\dots,x_n,y].$$

Substituting $\underbrace{g}_{\text{do you see why we're allowed to do this?}}$ for y, we get $g^N = F + 0$ where $F\in I$,

so $g\in\sqrt{I}$. $\square$

Cor: We now have the beginnings of a dictionary between commutative algebra and algebraic geometry. Let $S=k[x_1,\dots,x_n]$.

Algebraic geometry		Commutative algebra
Algebraic sets in $\mathbb{A}^n$	$\longleftrightarrow$	radical ideals in S
Irreducible algebraic sets	$\longleftrightarrow$	prime ideals of S

points in $\mathbb{A}^n$ $(a_1, \dots, a_n)$ $\longleftrightarrow$ maximal ideals in S $(x_1 - a_1, \dots, x_n - a_n)$

$\emptyset \longleftrightarrow (1) = S$

$\mathbb{A}^n \longleftrightarrow (0)$

Inclusion of algebraic sets $\longleftrightarrow$ (reverse) inclusion of ideals

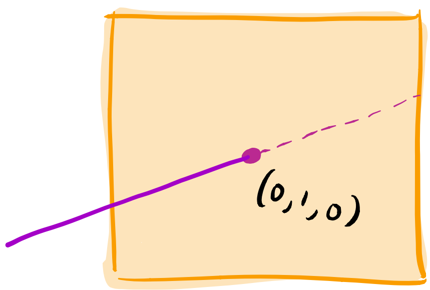
irreducible hypersurfaces $\longleftrightarrow$ irreducible polynomials (up to scaling)

algebraic subsets of $V(I)$ $\longleftrightarrow$ Radical ideals in S/I ($\longleftrightarrow$ radical ideals in S containing I) See HW#2

Ex: Consider $I = (x(y-1), xz^2) \subseteq \mathbb{C}[x,y,z]$

$$= (x)(y-1, z^2) \Rightarrow \sqrt{I} = (x)(y-1, z)$$

$V(I) = V(x) \cup V(y-1, z)$.



Irreducible algebraic subsets of $V(I)$
$= \{\text{irr. subsets of } V(x)\} \cup \{\text{irr. subsets of } V(y-1, z)\}$

$\mathbb{C}[x,y,z]/(x) \cong \mathbb{C}[y,z]$ so the algebraic subsets correspond to those in the plane.

$\mathbb{C}[x,y,z]/(y-1,z) \cong \mathbb{C}[x]$, so the proper alg. subsets are just points and $\emptyset$.

Cor: k algebraically closed, $I \subseteq k[x_1, \dots, x_n] = S$ an ideal. Then

$V(I)$ is finite $\iff$ S/I is a finite dimensional k-vector space.

Ex: 1.) $k[x]$ has k-basis $1, x, x^2, \dots$ and $V(0) = \mathbb{A}^1$, which is infinite.

2.) In $k[x,y]/(x^2-y)$, $\bar{y} = \bar{x}^2$, so it has k-basis $1, \bar{x}, \bar{x}^2, \dots$, and $V(x^2-y)$ is infinite.

3.) $k[x,y]/(x^2,y)$ has k-basis $1, \bar{x}$, so dimension 2, and $V(x^2, y) = \{(0,0)\}$, finite.

4.) $k[x,y]/(y, x(x-1))$ also has k-basis $1, \bar{x}$, and dim 2, but $V(y, x(x-1)) = \{(0,0), (1,0)\}$

5.) If $f \in k[x]$ is a polynomial of deg $d > 0$, then in $k[x]/(f)$, $\bar{x}^n$ is a k-linear combination of lower degree terms, so $\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}$ forms a basis.

Note: This dimension $\dim_k(S/I)$ is called the "length" of the corresponding "scheme". Even though $V(x^2, y) = V(x,y)$, the two ideals define different schemes.

$\bullet\!\!\to$ versus $\bullet$

We'll come back to this in a few weeks.

Pf of corollary: First assume $\dim_k(S/I) < \infty$. Let $P_1, \dots, P_r \in V(I)$.

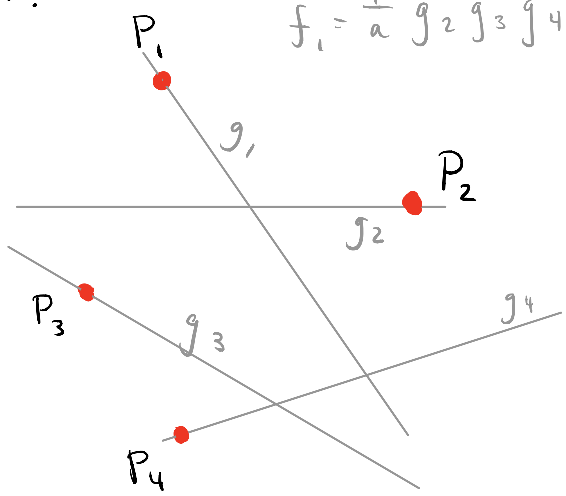
Claim: We can find $f_1, \dots, f_r \in S$ s.t. $f_i(P_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$

Sketch of Pf of Claim: For each i find g_i linear s.t. $g_i(P_i) = 0$ but $g_i(P_j) \neq 0$ for $j \neq i$ (i.e. a hyperplane avoiding P_j).

$f_1 = \frac{1}{a} g_2 g_3 g_4$

Set $f_j = \frac{1}{a} g_1 g_2 \cdots \hat{g_j} \cdots g_r$

with a = product of g_i eval at P_j. □



We want to show that the $\overline{f_i}$'s are linearly independent in S/I.

Let $\lambda_1, \dots, \lambda_r \in k$ s.t. $\sum \lambda_i \overline{f_i} = 0$. Then $\sum \lambda_i f_i \in I$.

Since $P_j \in V(I)$, $0 = \sum \lambda_i f_i(P_j) = \lambda_j$, so $\lambda_i = 0$ for all i.

Thus, $\overline{f_1}, \dots, \overline{f_r}$ are linearly independent so $r \leq \dim_k(S/I) < \infty \Rightarrow V(I)$ finite.

Now assume $V(I) = \{P_1, \dots, P_r\}$, i.e. $V(I)$ is finite.

For each $j \in \{1, \dots, n\}$, define $f_j = (x_j - a_{1j})(x_j - a_{2j}) \dots (x_j - a_{rj})$

where $a_{ij} = j^{th}$ coordinate of P_i.

Then $f_j(P_i) = 0$ $\forall i, j$, so $f_j \in I(V(I)) = \sqrt{I}$.

Thus, $\exists\ N >> 0$ s.t. $f_j^N \in I\ \forall j$.

$\Rightarrow \bar{f}_j^N = 0$, so $\bar{x}_j^{Nr}$ is a k-linear combination of smaller powers

$\Rightarrow$ we can generate S/I as a vector space by finitely many monomials. $\Rightarrow \dim_k (S/I) < \infty$. $\square$

Effective Nullstellensatz

Let $I = (f_1, \dots, f_r) \subseteq k[x_1, \dots, x_n]$.

If $g(P) = 0$ for all $P \in V(I)$, then since $\sqrt{I} = I(V(I))$, $g^N \in I$ for some $N > 0$.

Question: Is there an upper bound on the minimum N that works?

Thm: (Kollár, 1988) If f_i are homogeneous of deg $d_i > 2$, then $g \in \sqrt{I} \Leftrightarrow g^N \in I$ for some $N \leq \prod_{i=1}^{r} d_i$.

If $r < n$, no smaller N will work in general.