Ideals and subsets of k^n

Let k be an algebraically closed field. An element $f \in k[x_1, \ldots, x_n]$ can be evaluated at an n-tuple $\alpha = (\alpha_1, \ldots, \alpha_n) \in k^n$ to give

$$f(\alpha) = f(\alpha_1, \ldots, \alpha_n) \in k,$$

and so f can be considered as a function $f\colon k^n \to k$.

Definition. The **vanishing locus** (or zero locus) of f is the set

$$V(f) = \{\alpha \in k^n \mid f(\alpha) = 0\}.$$

Given polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$, their joint vanishing locus is

$$V(f_1, \ldots, f_m) = \{\alpha \in k^n \mid f_i(\alpha) = 0 \text{ for } i = 1, \ldots, m\} = V(f_1) \cap \cdots \cap V(f_m) \subseteq k^n$$

Example. If $f \in k[x]$, then $V(f) \subseteq k$ is the set of roots of f.

Example. If $f = x^2 + y^2 - 1 \in \mathbb{C}[x]$, then $V(f) \cap \mathbb{R}^2 \subseteq \mathbb{C}^2$ is the set $(\alpha, \beta) \in \mathbb{R}^2$ such that $\alpha^2 + \beta^2 = 1$, i.e. a circle.

Algebraic geometry is essentially the study of the geometry of such sets (or more general sets obtained by "gluing" different such sets together). The goal of this lecture is to explain a correspondence between these subsets of k^n and ideals of $k[x_1, \ldots, x_n]$.

Recall first Hilbert's (weak) nullstellensatz, which says that there is a bijection

$$k^n \leftrightarrow \{\text{maximal ideals in } k[x_1, \ldots, x_n]\}$$
$$\alpha = (\alpha_i)_{i=1}^n \mapsto \mathfrak{m}_\alpha = (x_1 - \alpha_1, \ldots, x_n - \alpha_n).$$

Consider the evaluation homomorphism

$$\phi_\alpha\colon k[x_1, \ldots, x_n] \to k$$
$$\phi_\alpha(f) = f(\alpha).$$

Then clearly $x_i - \alpha_i \in \ker \phi_\alpha$ for all i, and so $\mathfrak{m}_\alpha \subseteq \ker \phi_\alpha$. As $\mathfrak{m}_\alpha$ is maximal, we have $\ker \phi_\alpha = \mathfrak{m}_\alpha$. It follows that if $\alpha \in k^n$ and $f \in k[x_1, \ldots, x_n]$, then

$$\alpha \in V(f) \Leftrightarrow f \in \mathfrak{m}_\alpha.$$

From ideals to subsets.

Definition. Given an ideal $I \subseteq k[x_1, \ldots, x_n]$, define $V(I) \subseteq k^n$ by

$$V(I) = \{\alpha \in k^n \mid \text{ for all } f \in I, f(\alpha) = 0\} = \cap_{f \in I} V(f).$$

A subset of k^n which can be written as $V(I)$ for some ideal I is called **algebraic**.

Lemma. *We have $\alpha \in V(I)$ if and only if $I \subseteq \mathfrak{m}_\alpha$.*

Proof. If $I \subseteq \mathfrak{m}_\alpha$, then for every $f \in I$ we have $f \in \mathfrak{m}_\alpha$, and so $\alpha \in V(f)$. Conversely, if $I \not\subseteq \mathfrak{m}_\alpha$, there is some $f \in I$ such that $f \notin \mathfrak{m}_\alpha$, hence $\alpha \notin V(f)$. □

Example. If $f \in k[x_1, \ldots, x_n]$, then

$$V((f)) = V(f).$$

Proof. We have

$$\alpha \in V((f)) \Leftrightarrow (f) \subseteq \mathfrak{m}_\alpha \Leftrightarrow f \in \mathfrak{m}_\alpha \Leftrightarrow \alpha \in V(f).$$

□

Proposition. *Let $I, J \subseteq k[x_1, \ldots, x_n]$ be ideals.*

(1) $V((0))) = k^n$.
(2) $V((1)) = \varnothing$
(3) *If $I \subseteq J$, then $V(J) \subseteq V(I)$.*
(4) $V(I + J) = V(I) \cap V(J)$.
(5) $V(IJ) = V(I \cap J) = V(I) \cup V(J)$.
(6) $V(\sqrt{I}) = V(I)$.

Proof. (1): $(0) \subseteq \mathfrak{m}_\alpha$ for every $\alpha \in k^n$.
(2): $(1) \not\subseteq \mathfrak{m}_\alpha$ for every $\alpha \in k^n$.
(3): If $\alpha \in V(J)$, then $I \subseteq J \subseteq \mathfrak{m}_\alpha$, so $\alpha \in V(I)$.
(4): We have $\alpha \in V(I + J)$ if and only if $I + J \subseteq \mathfrak{m}_\alpha$ which is if and only if $I \subseteq \mathfrak{m}_\alpha$ and $J \subseteq \mathfrak{m}_\alpha$, which is if and only if $\alpha \in V(I) \cap V(J)$.
(5): The inclusions $IJ \subseteq I \cap J \subseteq I, J$ give

$$V(I) \cup V(J) \subseteq V(I \cap J) \subseteq V(IJ).$$

Let now $\alpha \in V(IJ)$. Then $IJ \subseteq \mathfrak{m}_\alpha$. If neither I nor J are contained in $\mathfrak{m}_\alpha$, then there is an $f \in I \setminus \mathfrak{m}_\alpha$ and a $g \in J \setminus \mathfrak{m}_\alpha$ giving $fg \in IJ \setminus \mathfrak{m}_\alpha$, which is a contradiction. Hence either $I \subseteq \mathfrak{m}_\alpha$ or $J \subseteq \mathfrak{m}_\alpha$, so $\alpha \in V(I) \cup V(J)$. This proves the inclusions in the chain above are equalities.
(6): Since $I \subseteq \sqrt{I}$, we have $V(\sqrt{I}) \subseteq V(I)$. If $\alpha \in V(I)$, then $I \subseteq \mathfrak{m}_\alpha$, and so $\sqrt{I} \subseteq \sqrt{\mathfrak{m}_\alpha} = \mathfrak{m}_\alpha$, so $\alpha \in V(\sqrt{\alpha})$. □

Example. Every ideal $I \subseteq k[x_1, \ldots, x_n]$ is finitely generated, since $k[x_1, \ldots, x_n]$ is Noetherian. We can choose generators and write $I = (f_1, \ldots, f_m)$. Then

$$V(I) = V((f_1) + \cdots + (f_m)) = V((f_1)) \cap \cdots \cap V((f_m)) = V(f_1, \ldots, f_m).$$

Example. Let $I, J \subseteq k[x_1, \ldots, x_n]$ be ideals. Then I and J are coprime if and only if there is no maximal ideal containing $\mathfrak{m}_\alpha$ containing both I and J, i.e. if and only if $V(I) \cap V(J) = \varnothing$.

From subsets to ideals.

Definition. Let $S \subseteq k^n$, and define

$$I(S) = \{f \in k[x_1, \ldots, x_n] \mid \forall \alpha \in S, f(\alpha) = 0\}.$$

Example. If $S = \{\alpha\}$ for some $\alpha \in k^n$, we have $I(S) = \mathfrak{m}_\alpha$.

Lemma. *The set $I(S) \subseteq k[x_1, \ldots, x_n]$ is an ideal.*

Proof. We have

$$I(S) = \cap_{\alpha \in S} I(\{\alpha\}) = \cap_{\alpha \in S} I(\{\alpha\}) = \cap_{\alpha \in S} \mathfrak{m}_\alpha,$$

which is an ideal. □

Proposition. *Let $R, S \subseteq k^n$. We have*

(1) $I(\varnothing) = (1)$.
(2) $I(k^n) = (0)$.
(3) *If $R \subseteq S \subseteq k^n$, then $I(S) \subseteq I(R)$.*
(4) $I(R \cup S) = I(R) \cap I(S)$.

Proof. (1), (3) and (4) are obvious from the definitions.

(2): We have

$$I(k^n) = \cap_{\alpha \in k^n} \mathfrak{m}_\alpha.$$

If $f \in \cap_{\alpha \in k^n} \mathfrak{m}_\alpha$ then $1 + f$ lies in no maximal ideal, hence $1 + f$ is a unit. But the units of $k[x_1, \ldots, x_n]$ are constants, and so f must itself be constant. Then clearly $f = 0$, so $I(k^n) = (0)$. □

Subsets and radical ideals.

Proposition (Strong nullstellensatz)**.** *Let $J \subseteq k[x_1, \ldots, x_n]$ be an ideal. Then*

$$I(V(J)) = \sqrt{J}.$$

Proof. For the containment $\supseteq$, if $f \in \sqrt{J}$, then $V(f) \supseteq V(\sqrt{J}) = V(J)$, so $f \in I(V(J))$.

The other is trickier, and we omit the proof (see suggested exercise this week). □

Remark. A concrete reformulation (close to Hilbert's original) of the above statement is as follows. Let polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ be given. If every $\alpha \in k^n$ which satisfies $f_1(\alpha) = \cdots = f_m(\alpha) = 0$ also satisfies $f(\alpha) = 0$, then there exists an $N \geq 0$ and $g_1, \ldots, g_m \in k[x_1, \ldots, x_n]$ such that

$$f^N = \sum_{i=1}^{m} f_i g_i.$$

Definition. We say an ideal I is **radical** if $\sqrt{I} = I$.

Corollary. *The operations $S \mapsto I(S)$ and $I \mapsto V(I)$ define an order-reversing bijection*

$$\{\textit{radical ideals of } k[x_1, \ldots, x_n]\} \leftrightarrow \{\textit{algebraic subsets of } k^n\}.$$

Proof. If $S \subseteq k^n$ is algebraic, then we have $S = V(I)$ for some ideal I, and so $S = V(I) = V(\sqrt{I})$, so V is surjective. If J is a radical ideal, then $I(V(J)) = \sqrt{J} = J$, so V is injective, and the inverse is given by I. □

Definition. Let $V = V(I) \subseteq k^n$ be an algebraic subset. We say that V is **reducible** if we can write $V(I)$ as the union of two strictly smaller algebraic subsets, and **irreducible** if it is not reducible.

Example. The algebraic subset $V(xy) = V(x) \cup V(y)$ is reducible, while $V(x)$ and $V(y)$ are irreducible.

Proposition. *If J is a radical ideal, then $V(J)$ is irreducible if and only if J is prime.*

Proof. Let J be a radical ideal.

Then $V(J)$ is reducible if and only if we can find radical ideals J_1, J_2 with $V(J_1), V(J_2) \subsetneq V(J)$ and $V(J) = V(J_1) \cup V(J_2)$. The first condition means that $J \subsetneq J_1, J_2$, and the second gives, since $V(J_1 \cup J_2) = V(J_1 \cap J_2)$ and $J_1 \cap J_2$ is radical, that $J = J_1 \cap J_2$.

Now if J is prime and $J \subsetneq J_1, J_2$, we can find $f_i \in J_i \setminus J$, and then $f_1 f_2 \in J_1 \cap J_2 \setminus J$, which shows that $J_1 \cap J_2 \neq J$. Hence $V(J)$ is irreducible.

If J is not prime, then we can find $f_1, f_2 \notin J$ with $f_1 f_2 \in J$. Take $J_i = \sqrt{J + (f_i)}$, and then

$$J \subseteq J_1 \cap J_2 = \sqrt{J_1} \cap \sqrt{J_2} = \sqrt{J_1 J_2} \subseteq J,$$

proving J is reducible. $\square$

Example. If $f \in k[x_1, \ldots, x_n]$ is an irreducible polynomial, then as (f) is prime, we have $V(f)$ is irreducible.