C3.4 Algebraic Geometry

Lecture 2: The ideal-variety correspondence

Balázs Szendrői, University of Oxford, Michaelmas 2020

The Zariski topology on general affine varieties

Recall that the Zariski topology on $\mathbb{A}^n = k^n$ is defined by declaring that the closed sets are the sets of the form $\mathbb{V}(I)$ for ideals $I \lhd R = k[x_1, \ldots, x_n]$.

Let $X = \mathbb{V}(I)$ be a vanishing set defined by an ideal $I \lhd R$.

Definition The **Zariski topology** on $X \subset \mathbb{A}^n$ is the subspace topology inherited from $\mathbb{A}^n$.

A vanishing set $X = \mathbb{V}(I) \subset \mathbb{A}^n$ together with its Zariski topology is called an **affine variety**.

Note that thus the closed sets in X are $\mathbb{V}(I + J) = X \cap \mathbb{V}(J)$ for any ideal $J \subset R$, or equivalently, $\mathbb{V}(S)$ for ideals $I \subset S \subset R$.

Definition An **affine subvariety** $Y \subset X$ is a closed subset of X.

Vanishing ideal

For any subset $X \subset \mathbb{A}^n$, let

$$\mathbb{I}(X) = \{f \in R : f(a) = 0 \text{ for all } a \in X\}.$$

Examples

1. $\mathbb{I}(\{a\}) = \mathfrak{m}_a = \{f \in R : f(a) = 0\}$.
2. $\mathbb{I}(\mathbb{V}(x^2)) = (x) \subset k[x]$, so $\mathbb{I}(\mathbb{V}(I)) \neq I$ in general.

Easy properties of the vanishing ideal

1. $X \subset Y \Rightarrow \mathbb{I}(X) \supset \mathbb{I}(Y)$.
2. $I \subset \mathbb{I}(\mathbb{V}(I))$.

Lemma $\mathbb{V}(\mathbb{I}(\mathbb{V}(I))) = \mathbb{V}(I)$.

Corollary $\mathbb{V}(\mathbb{I}(X)) = X$ for any affine variety X.

Dictionary between ideals and affine varieties

What we are doing here is building up a dictionary between ideals

$$I \lhd R = k[x_1, \ldots, x_n]$$

and affine varieties $X \subset \mathbb{A}^n$.

- From ideals to varieties: $I \mapsto \mathbb{V}(I)$.
- From varieties to ideals: $X \mapsto \mathbb{I}(X)$.
- One-sided inverse: $\mathbb{V}(\mathbb{I}(X)) = X$ for any affine variety X.
- The mappings are inclusion-reversing: subvarieties $Y \subset X$ correspond to over-ideals $J \supset I$.
- Maximal ideals $\mathfrak{m} \lhd R$ correspond to minimal (closed) subvarieties: points $p \in \mathbb{A}^n$.

Reducible and irreducible varieties

An affine variety X is **reducible** if $X = X_1 \cup X_2$ for proper closed subsets X_i ($X_i \subsetneq X$). Otherwise, we call X **irreducible**.

Examples and properties

1. $\mathbb{V}(x_1 x_2) = \mathbb{V}(x_1) \cup \mathbb{V}(x_2)$ is reducible.
2. If X irreducible, then any non-empty open subset is dense. (Exercise)
3. If X irreducible, then any two non-empty open subsets intersect. (Exercise)

Theorem An affine variety $X = \mathbb{V}(I) \neq \emptyset$ is irreducible if and only if its ideal $\mathbb{I}(X) \subset R$ is a **prime ideal**.

Note this is a statement about the ideal $\mathbb{I}(X) \subset R$, not about I that was used to define X on the left hand side!

Think about the example $I = \langle x^2 \rangle \lhd k[x]$ above.

Irreducible varieties and prime ideals

Theorem An affine variety $X = \mathbb{V}(I) \neq \emptyset$ is irreducible if and only if its ideal $\mathbb{I}(X) \subset R$ is a prime ideal.

Proof If $\mathbb{I}(X)$ is not prime, then pick f_1, f_2 satisfying $f_1 \notin \mathbb{I}(X)$, $f_2 \notin \mathbb{I}(X)$, $f_1 f_2 \in \mathbb{I}(X)$. Then

$$X \subset \mathbb{V}(f_1 f_2) = \mathbb{V}(f_1) \cup \mathbb{V}(f_2)$$

so take $X_i = X \cap \mathbb{V}(f_i) \neq X$ (since $f_i \notin \mathbb{I}(X)$).

Conversely, if X is not irreducible, $X = X_1 \cup X_2$, $X_i \neq X$, so there are $f_i \in \mathbb{I}(X_i) \setminus \mathbb{I}(X)$ but $f_1 f_2 \in \mathbb{I}(X)$, so $\mathbb{I}(X)$ is not prime. (Here we used $\mathbb{V}(\mathbb{I}(X)) = X$ for X_i). $\square$

Irreducible varieties: some examples

Here are some examples of irreducible varieties.

1. The variety $\mathbb{A}^n$ itself is irreducible. Proof: it corresponds to the zero ideal $I = 0$, which is prime since R is an integral domain.
2. $\mathbb{V}(\langle x_n \rangle) \subset \mathbb{A}^n$ is irreducible, since $I = \langle x_n \rangle$ is a prime ideal, as
$$R/I \cong k[x_1, \ldots, x_{n-1}]$$
is an integral domain.
3. More generally, if f is an irreducible polynomial in R, then $V_f = \mathbb{V}(\langle f \rangle)$ is an irreducible variety. Indeed, $I = \langle f \rangle$ is a principal ideal in the UFD $k[x_1, \ldots, x_n]$ and as f is irreducible, it generates a prime ideal inside it.

Extending the dictionary between ideals and affine varieties

Dictionary between ideals $I \lhd R = k[x_1, \ldots, x_n]$ and affine varieties $X \subset \mathbb{A}^n$.

- Maps: $I \mapsto \mathbb{V}(I)$ and $X \mapsto \mathbb{I}(X)$.
- One-sided inverse: $\mathbb{V}(\mathbb{I}(X)) = X$ for any affine variety X.
- Inclusion-reversing: subvarieties $Y \subset X$ correspond to over-ideals $J \supset I$.
- Maximal ideals $\mathfrak{m} \lhd R$ correspond to points $p \in \mathbb{A}^n$.
- Prime ideals $I \lhd R$ correspond to irreducible subvarieties $X \subset \mathbb{A}^n$.

Decomposition into irreducible components

Theorem An affine variety $X \subset \mathbb{A}^n$ can be decomposed into **irreducible components**: there exists a decomposition

$$X = X_1 \cup X_2 \cup \cdots \cup X_N,$$

where $X_i \subset \mathbb{A}^n$ are irreducible affine varieties, and the decomposition is unique up to reordering if we ensure $X_i \not\subset X_j$ for all $i \neq j$.

Proof We show existence of the decomposition.
Suppose X is not irreducible. Then we can write $X = Y_1 \cup Y_1'$ for proper subvarieties Y_1, Y_1'. Suppose one of these is not irreducible, say $Y_1 = Y_2 \cup Y_2'$. Keep going, assume that the process does not end in a finite number of steps. We obtain a sequence $X \supsetneq Y_1 \supsetneq Y_2 \supsetneq \cdots$. But then

$$\mathbb{I}(X) \subsetneq \mathbb{I}(Y_1) \subsetneq \mathbb{I}(Y_2) \subsetneq \cdots$$

This contradicts the ACC on ideals of R.
Proof of uniqueness: see notes. $\square$

An example

Consider $I = \langle xy, xz \rangle \lhd k[x, y, z]$. Let us work out the irreducible decomposition of $X = \mathbb{V}(I)$.

We have $I = \langle x \rangle . \langle y, z \rangle$.

This means that if we let $I_1 = \langle x \rangle$, $I_2 = \langle y, z \rangle$ and $X_i = \mathbb{V}(I_i)$ then

$$X = X_1 \cup X_2.$$

Clearly X_1, X_2 are not contained in each other. Also both X_i are irreducible, since $k[x, y, z]/I_i$ are both integral domains (easy check).

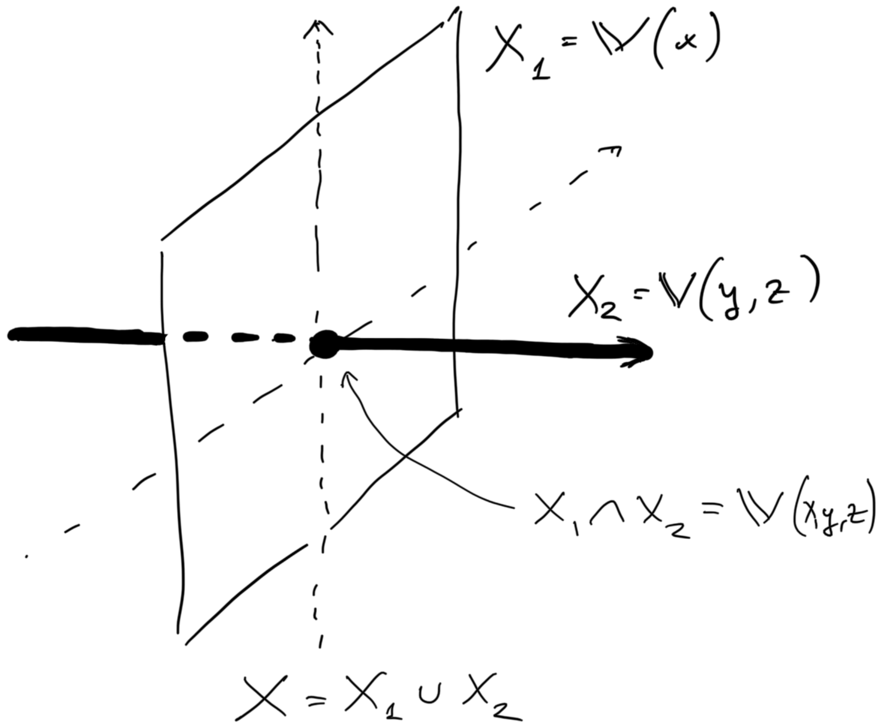
So this is an irreducible decomposition of X.

Geometrically:

- X_1 is the (y, z) plane $\{x = 0\}$.
- X_2 is the x-axis $\{y = z = 0\}$.
- $X_1 \cap X_2 = X_3$ is given by the ideal $I_3 = I_1 + I_2 = \langle x, y, z \rangle$: the origin.

An example

Here $I = \langle xy, xz \rangle \lhd k[x, y, z]$ and $X = \mathbb{V}(I)$.



Another example

Consider $J = \langle x^2 - 4 \rangle \lhd k[x, y]$. Let us work out the irreducible decomposition of $Y = \mathbb{V}(J)$.

This polynomial is reducible, so we have $J = \langle x - 2 \rangle . \langle x + 2 \rangle$. So if we let $J_1 = \langle x - 2 \rangle$, $J_2 = \langle x + 2 \rangle$ and $Y_i = \mathbb{V}(I_i)$ then

$$Y = Y_1 \cup Y_2$$

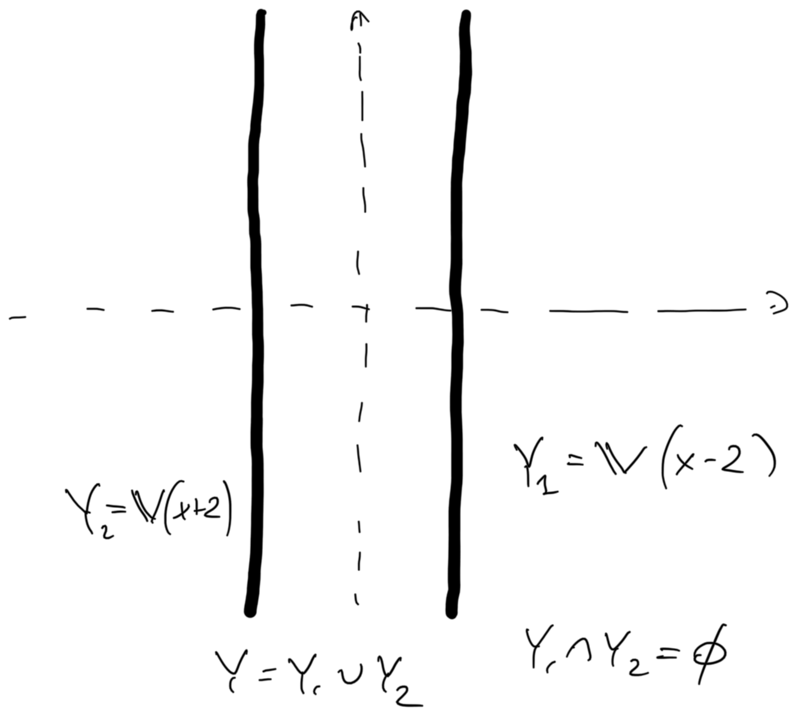
a union of two lines in $\mathbb{A}^2$. Indeed, both components are irreducible, as the corresponding ideals are prime (check!).

In this case, the intersection is given by the ideal $J_3 = J_1 + J_2 = \langle 1 \rangle = R$, so

$$Y_3 = Y_1 \cap Y_2 = \emptyset.$$

Another example

Here $J = \langle x^2 - 4 \rangle \lhd k[x, y]$ and $Y = \mathbb{V}(J)$.



Ideals and varieties: completing the dictionary

We have our dictionary between ideals $I \lhd R = k[x_1, \ldots, x_n]$ and affine varieties $X \subset \mathbb{A}^n$. Maps: $I \mapsto \mathbb{V}(I)$ and $X \mapsto \mathbb{I}(X)$, and

$$\mathbb{V}(\mathbb{I}(X)) = X.$$

We also know that $\mathbb{I}(\mathbb{V}(I))$ may be different from I. Example: $I = \langle x^2 \rangle$.

Key observation: for any $X \subset \mathbb{A}^n$, $\mathbb{I}(X)$ has the property that if $f^m \in \mathbb{I}(X)$ then $f \in \mathbb{I}(X)$, as $\mathbb{I}(X)$ is defined by a **vanishing condition**.

Definition An ideal $I \lhd R$ of a ring is called a **radical ideal**, if $r^m \in I$ for some $m \geq 1$ implies $r \in I$.

Given any ideal $I \lhd R$, its **radical** is the set

$$\sqrt{I} = \{f \in R : f^m \in I \text{ for some } m \geq 1\}.$$

Radicals and radical ideals

Easy Lemma

1. $\sqrt{I} \lhd R$ is an ideal of R.
2. $I \subset R$ is radical if and only if the quotient R/I has no nilpotent elements.
3. $\mathbb{V}(I) = \mathbb{V}(\sqrt{I})$.
4. For any $X \subset \mathbb{A}^n$, $\mathbb{I}(X) \lhd R$ is a radical ideal.

Example $\sqrt{\langle x^2 \rangle} = \langle x \rangle$.

Expectation: we can only hope for $\mathbb{I}(\mathbb{V}(I)) = I$ if the right hand side is radical, since the left hand side is.

Caveat: condition still not sufficient!

Example Let $k = \mathbb{R}$, and $I = \langle x^2 + 1 \rangle \lhd \mathbb{R}[x]$. Then $\mathbb{V}(I) = \emptyset$, so $\mathbb{I}(\mathbb{V}(I)) = \mathbb{R}[x]$ still does not equal I.

The strong Nullstellensatz and the completion of the dictionary

Theorem (Hilbert's Nullstellensatz) Assume that k **is algebraically closed**. For any ideal $I \lhd R = k[x_1, \ldots, x_n]$, we have

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

In particular, if I is radical then $\mathbb{I}(\mathbb{V}(I)) = I$.

Corollary There are order-reversing bijections between affine varieties $X \subset \mathbb{A}^n$ and radical ideals $I \lhd R = k[x_1, \ldots, x_n]$.

$$\begin{array}{rcl} X & \mapsto & \mathbb{I}(X) \\ \mathbb{V}(I) & \leftarrow\!\shortmid & I \\ \{\text{varieties}\} & \leftrightarrow & \{\text{radical ideals}\} \\ \{\text{irreducible varieties}\} & \leftrightarrow & \{\text{prime ideals}\} \\ \{\text{points}\} & \leftrightarrow & \{\text{maximal ideals}\} \end{array}$$

Towards proof of the Strong Nullstellensatz

We are going to assume the Weak Nullstellensatz, and deduce the strong version. Let us start with

Lemma For any proper ideal $I \lhd R$, we have $\mathbb{V}(I) \neq \emptyset$.

Proof Pick a maximal ideal $I \subset \mathfrak{m} \subset R$.
By the Weak Nullstellensatz, $\mathfrak{m} = \mathfrak{m}_a = (x_1 - a_1, \ldots, x_n - a_n)$ for some $a \in k^n$.
Hence $\mathbb{V}(I) \supset \mathbb{V}(\mathfrak{m}_a) = \{a\} \supset \mathbb{V}(R) = \emptyset$.

Remember this statement already needs k algebraically closed; otherwise it is false.

Proof of NSZ, easy direction
We showed above that $\mathbb{I}(\mathbb{V}(I))$ is always radical, also $I \subset \mathbb{I}(\mathbb{V}(I))$, so

$$\sqrt{I} \subset \mathbb{I}(\mathbb{V}(I)).$$

Conclusion of the proof of the Strong Nullstellensatz

We want to show $\mathbb{I}(\mathbb{V}(I)) \subset \sqrt{I}$. Let $I = \langle f_1, \ldots, f_N \rangle$, and take $g \in \mathbb{I}(\mathbb{V}(I))$.
Trick: let $I' = \langle I, yg - 1 \rangle \subset k[x_1, \ldots, x_n, y]$.
Observe that $\mathbb{V}(I') = \emptyset \subset \mathbb{A}^{n+1}$.
By Lemma on previous page, $I' = k[x_1, \ldots, x_n, y]$.
So $1 \in I'$, giving an equality

$$1 = G_0(x_1, \ldots, x_n, y) \cdot (yg - 1) + \sum G_i(x_1, \ldots, x_n, y) \cdot f_i$$

for some polynomials G_j.
Multiplying this with a large power of g, for some large ℓ we can turn this into

$$g^\ell = F_0(x_1, \ldots, x_n, gy) \cdot (yg - 1) + \sum F_i(x_1, \ldots, x_n, gy) \cdot f_i$$

for some polynomials F_j.
Finally substitute gy by 1 here, to get

$$g^\ell = \sum F_i(x_1, \ldots, x_n, 1) \cdot f_i \in I.$$

So $g \in \sqrt{I}$ as required. $\square$