Algebraic Geometry, Lecture 6

Frank-Olaf Schreyer

Saarland University, Perugia 2021

Overview

Today we will discuss the algebra-geometry dictionary.

1. Vanishing ideals of subsets of $\mathbb{A}^n$
2. The Zariski topology
3. Radical ideals and the strong Nullstellensatz
4. Trick of Rabinowitch
5. Prime ideal, maximal ideals and varieties
6. Coordinate ring
7. Morphisms between algebraic sets and varieties

Vanishing loci and vanishing ideals

Let K be an algebraically closed field. For any ideal $J \subset K[x_1, \ldots, x_n]$ we have defined its **vanishing loci** as

$$V(J) = \{a \in \mathbb{A}^n \mid f(a) = 0 \; \forall f \in J\}.$$

Conversely for $A \subset \mathbb{A}^n$ an arbitrary subset we define the **vanishing ideal** as

$$\mathrm{I}(A) = \{f \in K[x_1, \ldots, x_n] \mid f(a) = 0 \; \forall a \in A\}.$$

Example. Consider the set $C = \{(t, t^2, t^3) \in \mathbb{A}^3 \mid t \in \mathbb{A}^1\}$. The vanishing ideal of C is the kernel of the ring homomorphism

$$\varphi : K[x, y, z] \to K[t], x \mapsto t, y \mapsto t^2, z \mapsto t^3$$

Claim. $\mathrm{I}(C) = \ker \varphi = (y - x^2, z - x^3)$.

Twisted cubic curve

Proof of the Claim. $(y - x^2, z - x^3) \subset \mathrm{I}(C)$ is clear. For the converse pick a global monomial order such that $\mathrm{Lt}(y - x^2) = y$ and $\mathrm{Lt}(z - x^3)$. Let $f \in \ker\varphi$. Division with remainder gives

$$f = g_1(y - x^2) + g_2(z - x^3) + h$$

with no term of h divisible by y or z, i.e., $h \in K[x] \subset K[x, y, z]$. From $0 = f(t, t^2, t^3) = h(t)$ we deduce that h is the zero polynomial. Hence $f \in (y - x^2, z - x^3)$. $\square$

$$C = \{(t, t^2, t^3) \in \mathbb{A}^3 \mid t \in \mathbb{A}^1\}$$

is called the twisted cubic curve.

Basic properties of the correspondence V

Today we will study the correspondences

$$\{ \text{ ideals of } K[x_1, \ldots, x_n]\} \underset{\mathrm{I}}{\overset{V}{\longleftrightarrow}} \{\text{subsets of } \mathbb{A}^n\}$$

$$J \mapsto V(J), \quad \mathrm{I}(A) \leftarrow A.$$

Proposition. *Let $S = K[x_1, \ldots, x_n]$ and let $I, J, I_\lambda \subset S$ be ideals.*

1) $V(0) = \mathbb{A}^n$ *and* $V(1) = \emptyset$.
2) $I \subset J \implies V(I) \supset V(J)$.
3) $V(I) \cup V(J) = V(I \cap J) = V(I \cdot J)$.
4) $\bigcap_\lambda V(I_\lambda) = V(\sum_\lambda I_\lambda)$.
5) $V(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\}$

Proof. Only 3) needs an argument. Since $I \cdot J \subset I \cap J \subset J$ the inclusions $V(J) \subset V(I \cap J) \subset V(I \cdot J)$ follow by property 2. For the converse let $a \in V(I \cdot J)$ be a point not contained in $V(J)$. By assumption $\exists g \in J$ with $g(a) \neq 0$. Let $f \in I$ be arbitrarily. Since $f \cdot g \in I \cdot J$, we have $f(a)g(a) = 0$. Since $g(a) \neq 0$, we deduce $f(a) = 0$. Hence $a \in V(I)$. $\square$

The Zariski topology

Definition. An algebraic subset $A \subset \mathbb{A}^n$ is a subset of the form $A = V(J)$.

Conditions 1), 3) and 4) of the proposition can be rephrased by saying that the collection of algebraic subsets of $\mathbb{A}^n$ form the closed sets of a topology on $\mathbb{A}^n$. We call the complement $U = \mathbb{A}^n \setminus A$ of an algebraic set **Zariski open**.

Recall, a topology on a set X is a subset $\mathcal{T} \subset 2^X$ satisfying

1) $\emptyset \in \mathcal{T}$, $X \in \mathcal{T}$,
3) $U_1, U_2 \in \mathcal{T} \implies U_1 \cap U_2$, and
4) $U_\lambda \in \mathcal{T} \implies \bigcup_\lambda U_\lambda \in \mathcal{T}$.

The elements $U \in \mathcal{T}$ are called the open sets of the topology, and their complements $A = X \setminus U$ are called the closed sets of the topology. The closure of an arbitrary subset $Y \subset X$ is

$$\overline{Y} = \bigcap_{\substack{A \supset Y \\ \text{closed}}} A.$$

This is the smallest closed set containing Y.

Basic properties of the correspondence I

Proposition. *Let $S = K[x_1, \ldots, x_n]$ and let $A, B \subset \mathbb{A}^n$.*

1) $\mathrm{I}(\emptyset) = (1)$ *and* $\mathrm{I}(\mathbb{A}^n) = (0)$.
2) $A \subset B \implies \mathrm{I}(A) \supset \mathrm{I}(B)$.
3) $\mathrm{I}(A \cup B) = \mathrm{I}(A) \cap \mathrm{I}(B)$.
4) $V(\mathrm{I}(A)) \supset A$ *and equality holds if A is an algebraic subset.*

$$V(\mathrm{I}(A)) = \overline{A}$$

holds always.

5) $\mathrm{I}(\{(a_1, \ldots, a_n)\}) = (x_1 - a_1, \ldots, x_n - a_n)$.

Remark. If $\mathbb{F}_q \subset K$ is a finite subfield, then the set of $\mathbb{F}_q$-rational points $\mathbb{A}^n(\mathbb{F}_q)$ is algebraic since it is a finite union of q^n points.

$$\mathrm{I}(\mathbb{A}^n(\mathbb{F}_q)) = (x_1^q - x_1, \ldots, x_n^q - x_n)$$

is defined over the prime field $\mathbb{F}_p$ where $p = \operatorname{char} K$ and $q = p^r$.

Our next goal is to describe $\mathrm{I}(V(J))$.

The strong version of Hilbert's Nullstellensatz

Definition. Let R be a ring and $J \subset R$ an ideal. The **radical** of I is the ideal

$$\text{rad}(J) = \{f \in R \mid \exists n \in \mathbb{N} \text{ such that } f^n \in J\}.$$

To see that this is indeed an ideal we use

$$f^n \in J \text{ and } g^m \in J \implies (f+g)^{n+m-1} \in J.$$

Theorem. *Let K be an algebraically closed field and let $J \subset K[x_1, \ldots, x_n]$ be an ideal. Then*

$$\mathrm{I}(V(J)) = \text{rad}(J).$$

The inclusion $\text{rad}(J) \subset \mathrm{I}(V(J))$ is elementary:

$$\begin{aligned} f \in \text{rad}(J) &\implies f^N \in J \text{ for some } N \in \mathbb{N} \\ &\implies 0 = f^N(a) = (f(a))^N \ \forall a \in V(J) \\ &\implies f(a) = 0 \ \forall a \in V(J) \\ &\implies f \in \mathrm{I}(V(J)). \end{aligned}$$

The trick of Rabinowitch

Let $J = (f_1, \ldots, f_r)$ and $f \in \mathrm{I}(V(J))$. We have to show that

$$f^m \in (f_1, \ldots, f_r)$$

for a suitable $m \in \mathbb{N}$.
Consider an additional variable y and the ideal

$$(f_1, \ldots, f_r, yf - 1) \subset K[x_1, \ldots, x_n, y].$$

If $(a, b) \in \mathbb{A}^n \times \mathbb{A}^1 = \mathbb{A}^{n+1}$ lies in $V(f_1, \ldots, f_r, yf - 1)$, then $f_1(a) = 0, \ldots, f_r(a) = 0$. Thus $a \in V(J)$. Hence $f(a) = 0$ and the last polynomal $(fy - 1)(a, b) = f(a)b - 1 = -1 \neq 0$. Thus $V(f_1, \ldots, f_r, yf - 1) = \emptyset$ and the weak version of the Nullstellensatz implies

$$1 = g_1 f_1 + \ldots + g_r f_r + g_{r-1}(yf - 1)$$

for suitable polynomials $g_1, \ldots, g_{r+1} \in K[x_1, \ldots, x_n, y]$.

The trick of Rabinowitch 2

Let m be the maximal power in which y occurs in $g_1, \ldots, g_r$. Then

$$f^m \equiv \tilde{g}_1 f_1 + \ldots + \tilde{g}_r f_r \mod (yf - 1)$$

for polynomials $\tilde{g}_1, \ldots, \tilde{g}_r \in K[x_1, \ldots, x_n]$ since we can remove the appearance of y using $fy \equiv 1 \mod (yf - 1)$.
Since $K[x_1, \ldots, x_n]$ is a subring of $K[x_1, \ldots, x_n, y]/(yf - 1)$, we obtain

$$f^m = \tilde{g}_1 f_1 + \ldots + \tilde{g}_r f_r \in K[x_1, \ldots, x_n].$$

Thus $f \in \mathrm{rad}(J)$. $\square$

The coordinate ring

Thus for an algebraically closed field K the correspondences V and I induce bijections

$$\{\text{ radical ideals of } K[x_1, \ldots, x_n]\} \underset{\mathrm{I}}{\overset{V}{\longleftrightarrow}} \{\text{algebraic subsets of } \mathbb{A}^n\}$$

$$J \mapsto V(J), \quad \mathrm{I}(A) \leftarrow A.$$

A radical ideal in a ring R is an ideal J satisfying $\mathrm{rad}(J) = J$. Note that $\mathrm{rad}(\mathrm{rad}(I)) = \mathrm{rad}(I)$ always holds. Hence the radical of an ideal is always a radical ideal.

Definition. The **coordinate ring** of an algebraic set $A \subset \mathbb{A}^n$ is the residue ring

$$K[A] = K[x_1, \ldots, x_n]/\,\mathrm{I}(A).$$

This can be regarded as a subring of the ring $K^A = \{f : A \to K\}$ of K-valued functions on A. It is the K-subalgebra generated by the coordinate functions $x_j|_A$ of x_j restricted to A.

Prime ideals and maximal ideals

Definition. An ideal $\mathfrak{p} \subset R$ in ring R is called a **prime ideal** if

$$ab \in \mathfrak{p} \implies a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}$$

holds for all $a, b \in R$, equivalently, $R/\mathfrak{p}$ is an integral domain.
A **maximal ideal** $\mathfrak{m} \subsetneq R$ is an ideal which is maximal with respect to inclusion for proper ideals, i.e.,

$$\mathfrak{m} \subset I \subsetneq R \implies \mathfrak{m} = I$$

holds for all proper ideals $I \subsetneq R$. An equivalent condition is that $R/\mathfrak{m}$ is a field.
In the ring $K[x_1, \ldots, x_n]$ these types of ideals have a geometric interpretation.

Irreducible algebraic sets

Definition. An algebraic set $A \subset \mathbb{A}^n$ satisfying

$$A = A_1 \cup A_2 \implies A = A_1 \text{ or } A = A_2$$

for all **algebraic** subsets A_1, A_2 is called **irreducible**. Irreducible algebraic sets are also called **varieties**

Example.

$$V(xy, yz) = V(y) \cup V(x, z)$$

is a reducible algebraic set.

Irreducible algebra sets 2

Proposition. *An algebraic subset $A \subset \mathbb{A}^n$ is irreducible iff $\mathrm{I}(A) \subset K[x_1, \ldots, x_n]$ is a prime ideal.*

Proof. Suppose $A = A_1 \cup A_2$ with $A \supsetneq A_j$ for $j = 1, 2$. Consider $f_j \in \mathrm{I}(A_j) \setminus \mathrm{I}(A)$. Then $f_1 f_2 \in \mathrm{I}(A)$ with both factors not in $\mathrm{I}(A)$. So $\mathrm{I}(A)$ is not prime. Conversely if $\mathrm{I}(A)$ is not prime and $fg \in \mathrm{I}(A)$ a product whose factors are not in $\mathrm{I}(A)$, then

$$A = V(\mathrm{I}(A)) = V((fg) + \mathrm{I}(A)) = V((f) + \mathrm{I}(A)) \cup V((g) + \mathrm{I}(A))$$

shows that A is not irreducible. $\square$

Example. $V(y)$ and $V(x, z)$ are irreducible because $K[x, y, z]/(y) \cong K[x, z]$ and $K[x, y, z]/(x, z) \cong K[y]$ are integral domains. Thus

$$V(xy, yz) = V(y) \cup V(x, z)$$

is a decomposition into irreducible algebraic sets.

The algebra-geometry dictionary

Theorem. *Let K be an algebraically closed field. The correspondences V and I induce bijections*

$$\begin{array}{ccc}
\{\textit{radical ideals of } K[x_1,\dots,x_n]\} & \leftrightarrow & \{\textit{algebraic subsets of } \mathbb{A}^n\} \\
\cup & & \cup \\
\{\textit{prime ideals of } K[x_1,\dots,x_n]\} & \leftrightarrow & \{\textit{irreducible alg. subsets of } \mathbb{A}^n\} \\
\cup & & \cup \\
\{\textit{maximal ideals of } K[x_1,\dots,x_n]\} & \leftrightarrow & \{\textit{points of } \mathbb{A}^n\}
\end{array}$$

The last bijection still needs a proof. If $\mathfrak{m} \subset K[x_1,\dots,x_n]$ is a maximal ideal, then $V(\mathfrak{m}) \neq \emptyset$ by the Nullstellensatz. If $a = (a_1,\dots,a_n) \in V(\mathfrak{m})$, then

$$\mathfrak{m} \subset (x_1 - a_1, \dots x_n - a_n)$$

and the maximality of $\mathfrak{m}$ implies that equality holds.

part 3

Morphism between algebraic sets

Definition. Let $A \subset \mathbb{A}^n$ and $B \subset \mathbb{A}^m$ be algebraic sets. A **morphism**

$$\Phi : A \to \mathbb{A}^m, a \mapsto \Phi(a) = (\overline{f}_1(a), \ldots, \overline{f}_m(a))$$

is a map given by an m-tupel of functions $\overline{f}_1, \ldots, \overline{f}_m \in K[A]$. A **morphism**

$$\varphi : A \to B$$

is given by a morphism $\Phi : A \to \mathbb{A}^m$ such that $\Phi(a) \in B \ \forall a \in A$.

Thus for a morphism $\varphi : A \to B$ we always have a diagram

Algebra side of a morphism

A morphism $\Phi : A \to \mathbb{A}^m$ specifies a ring homomorphism

$$\Phi^* \colon K[y_1, \dots, y_m] \to K[A],\ y_j \mapsto \overline{f}_j,$$

and conversely any K-algebra homomorphism Φ^* induces a morphism $\Phi : A \to \mathbb{A}^m$.
A morphism $\varphi : A \to B$ corresponds to a ring homomorphism

$$\varphi^* : K[B] \to K[A].$$

While Φ is easy to specify, morphisms $\varphi : A \to B$ are difficult to find: The tupel $(\overline{f}_1, \dots, \overline{f}_m)$ has to satisfy

$$F(\overline{f}_1, \dots, \overline{f}_m) = 0 \in K[A]$$

for all equations $F(y_1, \dots, y_m) \in \mathrm{I}(B) \subset K[y_1, \dots, y_m]$.

Isomorphisms

Thus we have

$$Mor(A,B) \cong \mathrm{Hom}_{K-\mathrm{algebra}}(K[B],K[A]), \quad \varphi \mapsto \varphi^*.$$

Definition. A morphism $\varphi : A \to B$ is an **isomorphism** if there exists a morphism $\psi : B \to A$ with

$$\psi \circ \varphi = id_A \text{ and } \varphi \circ \psi = id_B.$$

Proposition. *A and B are isomorphic iff $K[A] \cong K[B]$.*

Example. $A = V(y - x^2) \subset \mathbb{A}^2$ and $\mathbb{A}^1$ are isomorphic because

$$K[x] \to K[x,y]/(y - x^2)$$

is an isomorphism.

Examples of morphisms

1) The $K[x] \hookrightarrow K[x, x^{-1}] \cong K[x, y]/(xy - 1)$ defines a morphism of the hyperbola $A = V(xy - 1)$ to $\mathbb{A}^1$. This corresponds to the projection onto the x-axis.

In particular we see that the image of a morphism is not necessarily again an algebraic set.

Examples of morphisms

2)
$$\mathbb{A}^1 \to B = V(z^2 - y^3) \subset \mathbb{A}^2, x \mapsto (x^2, x^3)$$
is a morphism because $(x^3)^2 - (x^2)^3 = 0$.

Although this is a bijection as a map of sets, this is not an isomorphism because
$$K[y,z]/(z^2 - y^3) \cong K[x^2, x^3] \hookrightarrow K[x]$$
is not surjective.