Session I

10/10/22

Contents

1. Zariski Topology

Throughout, let $\Bbbk$ be an algebraically closed field.

Definition 1.1. We call a subset $V \subseteq \Bbbk^n$ an *affine algebraic set* oif there is a $M \subseteq \Bbbk[X_1, \ldots, X_n]$ such that

$$V = \mathrm{V}(M) \coloneqq \{(x_1, \ldots, x_n) \in \Bbbk^n \mid \forall f \in M : f(x_1, \ldots, x_n) = 0\}.$$

In the above definition, we only required that M is some subset of the polynomial ring. As it turns out, there are various restrictions we can impose on M, the more straight-forward ones being:

Proposition 1.2. Let $M \subseteq \Bbbk[X_1, \ldots, X_n]$ be any subset.

(i) Denote by $\mathfrak{a} \coloneqq \langle M \rangle$ the ideal generated by M. Then $\mathrm{V}(\mathfrak{a}) = \mathrm{V}(M)$.
(ii) There are finitely many $f_1, \ldots, f_m \in \Bbbk[X_1, \ldots, X_n]$ such that $\mathrm{V}(M) = \mathrm{V}(\{f_1, \ldots, f_m\})$.

We also have good compatibility of $\mathrm{V}(-)$ with the lattice of subsets of $\Bbbk[X_1, \ldots, X_n]$:

Proposition 1.3. Let I be an index set and $(M_i)_{i \in I}$ a collection of subsets index by I. Then $\mathrm{V}(\bigcup M_i) = \bigcap \mathrm{V}(M_i)$. Moreover, for $M \subseteq M' \subseteq \Bbbk[X_1, \ldots, X_n]$, it holds that $\mathrm{V}(M) \supseteq \mathrm{V}(M')$.

Now, let's look at some examples:

Example 1.4.

(i) Somewhat trivally, we have $\mathrm{V}(\emptyset) = \Bbbk^n$ and $\mathrm{V}(\Bbbk[X_1, \ldots, X_N) = \emptyset$.
(ii) Consider the case $n = 1$, so $\Bbbk[X]$ is a principal ideal domain. In particular, we are reduced to understanding $\mathrm{V}(f)$ for a single polynomial f. As we assume $\Bbbk$ to be algebraically closed, f factors as $f = \prod_{i=1}^{n}(X - \lambda_i)$ for some $\lambda_i \in \Bbbk$. In particular, we have that

$$\mathrm{V}(f) = \{\lambda_1, \ldots, \lambda_n\}.$$

The second part of the above example is a special instance of the following, more general statement:

Proposition 1.5. Let $M_1, M_2 \subseteq \Bbbk[X_1, \ldots, X_n]$ be subsets. Then

$$\mathrm{V}(M_1) \cup \mathrm{V}(M_2) = \mathrm{V}(M_1 M_2).$$

Commit: 2022-10-15, a69bc59.

Example 1.6. As a special instance of this, we see that for any ideal $\mathfrak{a}$, the equality

$$\mathrm{V}(\mathfrak{a}) = \mathrm{V}(\mathfrak{a}^i)$$

holds for all $i \geqslant 1$.

So we see that the subsets of $\Bbbk^n$ that are of the form $\mathrm{V}(M)$ for some M satisfy the conditions imposed on the closed subsets of a topology.

Definition 1.7. This topology on $\Bbbk^n$ is called the *Zariski topology.* If we consider $\Bbbk^n$ as a topological space with the Zariski topology, we also write $\mathbb{A}^n$.*

Example 1.8. We have just seen that for $n = 1$, the closed subsets of $\mathbb{A}^1$ are given by finite unions of points. For $n \geqslant 2$, there will be many more closed subsets in general. I drew a bunch of pictures in the tutorial, but this takes too much time on the computer rn.

2. Hilbert's Nullstellensatz

By definition, every closed subset of $\mathbb{A}^n$ is of the form $\mathrm{V}(\mathfrak{a})$ for some ideal $\mathfrak{a}$. A "natural" question is now dependent the subset is on the "presentation" by a particular ideal. We have already seen above that taking powers of the ideal doesn't change the associated closed subset. But this actually all that can go wrong. To make this more precise, we need the following defintion from commutative algebra:

Definition 2.1. Let R be a ring and $\mathfrak{a} \subseteq R$ an ideal. Then the *radical* of $\mathfrak{a}$ is defined as

$$\mathrm{rad}(\mathfrak{a}) = \{x \in R \mid \exists n \geqslant 1 : x^n \in \mathfrak{a}.\}$$

We say that $\mathfrak{a}$ is a *radical ideal* if $\mathrm{rad}(\mathfrak{a}) = \mathfrak{a}$ holds.

Let us quickly collect some properties of radicals:

Lemma 2.2.

(i) An ideal $\mathfrak{a} \subseteq R$ is radical if and only if $R/\mathfrak{a}$ is a *reduced ring* (i.e. does not contain a non-trivial nilpotent element).
(ii) Every prime ideal is a radical ideal.
(iii) For all ideals $\mathfrak{a}, \mathfrak{b} \subseteq R$, it holds that $\mathrm{rad}(\mathfrak{a}\mathfrak{b}) = \mathrm{rad}(\mathfrak{a}) \cap \mathrm{rad}(\mathfrak{b})$.
(iv) For every ideal $\mathfrak{a} \subseteq R$, it holds that $\mathrm{rad}(\mathfrak{a}) = \mathrm{rad}(\mathfrak{a}^n)$ for all $n \geqslant 1$.
(v) Assume $R = \Bbbk[X_1, \ldots, X_n]$. Then $\mathrm{V}(\mathfrak{a}) = \mathrm{V}(\mathrm{rad}(\mathfrak{a}))$ for all ideals $\mathfrak{a} \subseteq R$.

With this out of the way, we can formulate the main theorem of today:

Theorem 2.3 (Hilbert's Nullstellensatz)**.** *The map* $\mathrm{V}(-)$ *induces an inclusion-reversing bijection*

$$\mathrm{V}(-)\colon \{\textit{radical ideals in } \Bbbk[X_1, \ldots, X_n]\} \xrightarrow{\sim} \{\textit{closed subsets of } \mathbb{A}^n\},$$

with an inverse given by

$$\mathrm{I}(-)\colon Z \longmapsto \{f \in k[X_1, \ldots, X_n] \mid \forall x \in Z : f(x) = 0\}.$$

Before we prove the Nullstellensatz, let us note that it implies that $\Bbbk^n$ is still "'algebraically closed'"†:

Corollary 2.4 (Weak Nullstellensatz)**.** Let $\mathfrak{a} \subsetneq \Bbbk[X_1, \ldots, X_n]$ be a proper ideal. Then there is a $x \in \Bbbk^n$ such that $f(x) = 0$ for all $f \in \mathfrak{a}$.

*Depending on the context, people sometimes add the ground field to the notation, e.g. $\mathbb{A}^n_k$, but since we don't switch the ground field today, we can safely omit it.

†This makes not too much sense but still is the best way I know of thinking about this

Deducing the WNS from the HNS. As $\mathfrak{a}$ is proper, so is $\operatorname{rad}(\mathfrak{a})$. By the bijection from the Nullstellensatz, this implies in particular that

$$\mathrm{V}(\mathfrak{a}) = \mathrm{V}(\operatorname{rad}(\mathfrak{a}) \supsetneq \emptyset,$$

yielding the desired root. □

Proof of HNS. We will blackbox a lot of commutative algebra for the proof; in particular, we don't appeal to Noether normalization directly but hide it in the following fact:

Fact. Let R be a non-zero, finitely generated $\Bbbk$-algebra. There there is a (non-zero) $\Bbbk$-algebra homomorphism $R \to \Bbbk$.

Now, the main challenge is to show that for any ideal $\mathfrak{a} \subseteq \Bbbk[X_1, \dots, X_n]$, the equality

$$\operatorname{rad}(\mathfrak{a}) = \mathrm{I}(\mathrm{V}(\mathfrak{a}))$$

holds. To get the inclusion $\operatorname{rad}(\mathfrak{a}) \subseteq \mathrm{I}(\mathrm{V}(\mathfrak{a}))$, consider a $f \in \operatorname{rad}(\mathfrak{a})$ and $x \in \mathrm{V}(\mathfrak{a})$. Since $f \in \operatorname{rad}(\mathfrak{a})$, we have $f^m \in \mathfrak{a}$ for some $m \geqslant 1$. In particular, $f^m(x) = 0$, and thus $f(x) = 0$, i.e. $f \in \mathrm{I}(\mathrm{V}(\mathfrak{a}))$.

Conversely, let $f \notin \operatorname{rad}(\mathfrak{a})$. We now need to produce an element $x \in \mathrm{V}(\mathfrak{a})$ such that $f(x) \neq 0$. To that end, we want to apply the fact to the $\Bbbk$-algebra

$$R = \Bbbk[X_1, \dots, X_n, Y]/(fY - 1, \mathfrak{a}) = (\Bbbk[X_1, \dots, X_n]/\mathfrak{a}) \left[\tfrac{1}{f}\right].$$

So first of all, we need to check that R is indeed non-zero! Here we will need our assumption: namely, $R = 0$ if and only if f is nilpotent in $\Bbbk[X_1, \dots, X_n]/\mathfrak{a}$, if and only if $f^m \in \mathfrak{a}$ for some $m \geqslant 1$, so iff $f \in \operatorname{rad}(\mathfrak{a})$, which we assumed to be false. Hence R is non-zero, and the fact gives us a non-zero, k-linear ring map $\varphi\colon R \to \Bbbk$. If we write $x_i \coloneqq \varphi(X_i)$ and $y \coloneqq \varphi(Y)$, then the fact that $fy = 1$ holds in R implies that

$$f(x_1, \dots, x_n)y = 1$$

holds in $\Bbbk$; moreover, since we're taking the quotient by $\mathfrak{a}$ in the construction of R, we have necessarily $x \in \mathrm{V}(\mathfrak{a})$. □

3. Irreducible subsets

Many of the topological spaces we will encounter in this course are irreducible:

Definition 3.1. Let Y be a topological space. Then Y is *irreducible* if cannot be written as $Y = Y_1 \cup Y_2$ for proper, closed subsets $Y_1, Y_2 \subseteq Y$.

Note that we do not require these two subsets to be disjoint! So every irreducible space is in particular connected, but the former condition is striclty stronger:

Lemma 3.2.

(i) Let Y be a topological space. Then Y is irreducible if and only if every pair of open subsets of Y has non-empty intersection.

(ii) Let Y be an irreducible Hausdorff space. Then Y is irreducible if and only if Y contains at most one point.

Proof. Part (i) is a good exercise in general point-set topology. For part (ii), note that by definition, any distinct points of a Hausdorff space can be seperated by disjoint open sets, violating part (i). □

Coming back to the Zariski-topology, we now remark the following:

Proposition 3.3. Let $\mathfrak{a} \subseteq \Bbbk[X_1, \dots, X_n]$ be a radical ideal. Then $\mathfrak{a}$ is prime if and only if $\mathrm{V}(\mathfrak{a}) \subseteq \mathbb{A}^n$ is irreducible (when endowed with the subspace topology).

Proof. One first verifies that for $Z \subseteq \mathbb{A}^n$ closed, the ideal $\mathrm{I}(Z)$ is prime if and only if Z is irreducible (this can be done directly). Then the Nullstellensatz implies the claim. $\square$

In particular, the Nullstellensatz restricts to a bijection

$$\mathrm{V}(-)\colon \{\text{prime ideals in } \Bbbk[X_1, \dots, X_n]\} \xrightarrow{\sim} \{\text{irreducible subsets of } \mathbb{A}^n\}.$$

We will say more about how to extend such notions to ideals that aren't radical, like $\langle X^2 \rangle$, once we know what (affine) schemes are.

Email address: `s6aawild@uni-bonn.de`