LECTURE 8

YIHANG ZHU

1. A brief introduction to Algebraic Geometry: Affine algebraic sets

What is Algebraic Geometry? Roughly speaking, it is the study of zero loci of polynomials. To formulate the problem, let R be a commutative ring and $\{f_i\}$ a collection of polynomials in $R[X_1, \cdots, X_n]$. We would like to define and study the common zero locus of the f_i's. However, the naive definition below is simply not good enough.

$$\{(x_1, \cdots, x_n) \in R^n | f_i(x_1, \cdots, x_n) = 0, \forall i\}$$

For example, if we take the single polynomial $f(X) = X^2 + 1$, then the above set is empty if we take $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$. But that does not mean $f(X)$ is not interesting to study in this case. One strategy of fixing the situation is just to look at the ring $A = R[X_1, \cdots, X_n]/(f_i)$, where (f_i) means the ideal of $R[X]$ generated by the $f_i's$. This R-algebra A always makes sense, no matter whether the f_i's have common solutions in R or not. We may just view A as the fundamental object of study, which sort of captures the geometric properties of the "common zero locus of the f_i's". This strategy works for general rings R, and is of the flavor of scheme theory. However for our purposes we need only treat the case where R is a perfect field. In this case there is a much more straightforward and also classical approach, which we describe below. Simply put, we look at the set of solutions in the algebraic closure $\bar{R}$ of R, while remembering the Galois action everywhere.

From now on we fix a perfect field k, with algebraic closure $\bar{k}$ and absolute Galois group $G_k = \mathrm{Gal}(\bar{k}/k)$.

Definition 1.1. The affine n-space over k is $\mathbb{A}^n_k := \left\{(x_1, \cdots, x_n) \in \bar{k}^n\right\}$. The Galois group G_k acts on $\mathbb{A}^n_k$ coordinate-wise. Let $k \subset l \subset \bar{k}$, define $\mathbb{A}^n_k(l) = \{x \in \mathbb{A}^n_k | x_i \in l\}$. It is the subset of $\mathbb{A}^n_k$ fixed by G_k.

Remark 1.2. We write $\mathbb{A}^n_k$ instead of $\bar{k}^n$ for two reasons. Firstly we want to emphasize that we remember the action of G_k, and the field $\bar{k}$ contains a preferred subfield k. Secondly we want to emphasize that we do not view $\mathbb{A}^n_k$ as a vector space, but rather an affine space on the vector space $\bar{k}^n$. (Namely it is a "vector space without origin.")

From now on we will use the multi-variable notation, when n is understood from the context.

Let I be a subset of $\bar{k}[X] = \bar{K}[X_1, \cdots, X_n]$. Define the locus of I to be

$$V(I) := \{x \in \mathbb{A}^n_k | f(x) = 0, \forall f \in I\}.$$

Note that we are looking at solutions inside $\bar{k}$. Observe: if we replace I by the ideal generated by I inside $\bar{k}[X]$, the set $V(I)$ remains to be the same. Conversely, if $I \subset \bar{k}[X]$ is an ideal, then $V(I) = V(I')$, if I' is a set of generators of the ideal I.

Remark 1.3. By Hilbert' basis theorem, any ideal $I \subset \bar{k}[X]$ is finitely generated.

Definition 1.4. A subset of $\mathbb{A}^n_k$ of the form $V(I)$ for some subset $I \subset \bar{k}[X]$ is called an affine algebraic set. It is also called a Zariski closed subset of $\mathbb{A}^n_k$.

We also have a construction that produces an ideal of $\bar{k}[X]$ out of an arbitrary subset $V \subset \mathbb{A}^n_k$. Define $I(V) := \left\{ f \in \bar{k}[X] | f(x) = 0, \forall x \in V \right\}$. One easily checks that this is an ideal. Observe: if an ideal I of $\bar{k}[X]$ arises in this way, then I is radical, i.e.

$$I = \sqrt{I} := \left\{ f \in \bar{k}[X] | f^n \in I \text{ for some } n \right\}.$$

Theorem 1.5 (Hilbert's Nullstellensatz)**.** *Let I be an ideal of $\bar{k}[X]$. Then $I(V(I)) = \sqrt{I}$.*

Corollary 1.6. *Any maximal ideal of $\bar{k}[X]$ is of the form $(X_1 - a_1, \cdots, X_n - a_n)$, for some $(a_1, \cdots, a_n) \in \mathbb{A}^n_k$.*

Proof. First note that an ideal of the form $(X_1 - a_1, \cdots, X_n - a_n)$ is indeed maximal. Conversely, let $I \subset \bar{k}[X]$ be a maximal ideal. Then $I = \sqrt{I}$. By the above theorem $I = I(V)$ for some subset $V \subset \mathbb{A}^n_k$. If $V = \emptyset$ then $I(V) = (1)$, contradiction. Let $a = (a_1, \cdots, a_n) \in V$. Then $I = I(V) \subset I(\{a\})$. We also have $(X_1 - a_1, \cdots, X_n - a_n) \subset I(\{a\})$. Since both I and $(X_1 - a_1, \cdots, X_n - a_n)$ are maximal ideals and $I(a) \neq (1)$, we conclude that $I = I(\{a\}) = (X_1 - a_1, \cdots, X_n - a_n)$. □

Corollary 1.7. *We have a bijection*

$$\left\{ \text{radical ideals } I \subset \bar{k}[X] \right\} \longleftrightarrow \text{ affine algebraic sets in } \mathbb{A}^n_k$$
$$I \mapsto V(I)$$
$$I(V) \leftarrow\!\shortmid V.$$

This bijection is inclusion reversing. In particular, the maximal ideals of $\bar{k}[X]$ corresponds to points in $\mathbb{A}^n_k$, as seen in the previous corollary, the ideal (0) corresponds to $\mathbb{A}^n_k$, and the ideal (1) corresponds to $\emptyset$.

Definition 1.8. An affine algebraic variety in $\mathbb{A}^n_k$ is an affine algebraic set V such that $I(V)$ is a prime ideal.

Corollary 1.9. *We have a bijection*

$$\left\{ \text{prime ideals } I \subset \bar{k}[X] \right\} \longleftrightarrow \text{ affine algebraic varieties in } \mathbb{A}^n_k$$

Example 1.10. Let $I = (X^2 Y) \subset \bar{k}[X, Y]$. Consider $V = V(I) \subset \mathbb{A}^2_k$. Then $V = \{(x, y) | x = 0 \text{ or } y = 0\}$. $I(V) = (xy) = \sqrt{I}$. We see $I(V)$ is not prime, so V is not a variety. However, V is equal to the union $\{(x, 0)\} \cup \{(0, y)\}$, both of which are affine algebraic varieties, with ideals (x) and (y) respectively. Algebraically speaking, (x) and (y) are the two ideals that are minimal among the prime ideals containing $I(V)$.

Fact 1.11. *In general, any affine algebraic set V can be uniquely written as a union $V = V_1 \cup \cdots \cup U_k$, with each U_i an affine algebraic variety, and $V_i \not\subset V_i, i \neq j$. The ideals $I(V_i)$ are the minimal ideals among the prime ideals containing $I(V)$. The V_i's are called the irreducible components of V.*

Definition 1.12. Let $V \subset \mathbb{A}^n_k$ be an affine algebraic set. Let $I(V/k) := I(V) \cap k[X]$. This is an ideal of $k[X]$. It is a prime ideal if V is a variety. We say V is defined over k, if it is of the form $V(J)$ where $J \subset k[X]$, or equivalently, if $I(V/k)\bar{k}[X] = I(V)$.

Exercise 1.13. Prove the equivalence asserted in the definition.

Example 1.14. $k = \mathbb{R}, \bar{k} = \mathbb{C}$. $V = V(x^2+1) = \{\pm i\} \subset \mathbb{A}^1_{\bar{k}}$ is an affine algebraic set, not a variety, defined over $\mathbb{R}$. $V' = V(x-i) = \{i\} \subset \mathbb{A}^1_{\bar{k}}$ is an affine algebraic variety, not defined over $\mathbb{R}$. In fact $I(V'/k) = (x^2+1)$, and $I(V'/k)\mathbb{C}[X] \subsetneq I(V') = (X-i)\mathbb{C}[X]$.

Proposition 1.15. *Let $V \subset \mathbb{A}^n_{\bar{k}}$ be an affine algebraic set. It is defined over k if and only if $\forall \sigma \in G_k$, $\sigma(V) = V$.*

Proof. Suppose V is defined over k, then $V = V(J)$ for a subset $J \subset k[X]$. Note that for $f \in k[X]$ and $x \in \mathbb{A}^n_{\bar{k}}$, $f(x) = 0 \Leftrightarrow f(\sigma(x)) = 0, \forall \sigma \in G_k$, since the coefficients of f are fixed by σ. Thus we see that $\sigma(V) = V$.

Conversely, suppose $\sigma(V) = V, \forall \sigma \in G_k$. Then $\sigma(I(V)) = I(V)$. Suppose there exists $f \in I(V) - I(V/k)\bar{k}[X]$. Assume the degree of f is minimal among such f's. Let $l \subset \bar{k}$ be a finite extension of k containing all the coefficients of f. By scaling by $\bar{k}^\times$, we may assume the leading coefficient of f is $a \in l$ with $\operatorname{Tr}_{l/k} a \neq 0$. Look at $g = \operatorname{Tr}_{l/k} f = \sum_{\sigma \in \operatorname{Gal}(l/k)} \sigma(f)$. Then $g \in I(V/k)$, and g has the same degree as f. But then $f - \lambda g$ has strictly smaller degree than f, for some $\lambda \in \bar{k}$, and $f - \lambda g \in I(V) - I(V/k)\bar{k}[X]$, contradiction. □

Definition 1.16. Let $V \subset \mathbb{A}^n_{\bar{k}}$ be an affine algebraic variety defined over k. Define

$$\begin{aligned} k[V] &= k[X]/I(V/k), \\ k(V) &= \operatorname{Frac}(k[V]), \\ \bar{k}[V] &= \bar{k}[X]/I(V), \\ \bar{k}(V) &= \operatorname{Frac}(\bar{k}[V]). \end{aligned}$$

We have $\bar{k}[V] = k[V] \otimes_k \bar{k}, \bar{k}(V) = k(V) \otimes_k \bar{k}$. For $k \subset l \subset \bar{k}$, we also define the set of l-rational points of V to be $V(l) := V \cap \mathbb{A}^n_{\bar{k}}(l)$. Recall G_k acts on V, and $V(l) = V^H$, where $H = \operatorname{Gal}(\bar{k}/H) \subset G_k$.

Remark 1.17. Given an element f in $\bar{k}[V]$, resp. $k[V]$, we get a function from V to $\bar{k}$, resp. k, by evaluating f on the points in V. Similarly, given an element $f/g \in \bar{k}(V)$, resp. $k(V)$, we get a function with values in $\bar{k}$, resp. k, defined everywhere on V except where g vanishes. Note that by definition g does not vanish on the whole of V.

Remark 1.18. Even if V is not defined over k the definition $V(l) = V \cap \mathbb{A}^n_{\bar{k}} \cap V$ still makes sense, but we will never talk about this set exclusively when V is defined over some subfield of l.

Example 1.19. Consider the algebraic set $V = V(X^n + Y^n - 1) \subset \mathbb{A}^n_{\bar{\mathbb{Q}}}$. It is defined over $\mathbb{Q}$, and it is a variety (see the exercise below). Fermat's Last Theorem states that for $n \geq 3$, we have

$$V(\mathbb{Q}) = \begin{cases} \{(1,0),(0,1)\}, & n \text{ odd} \\ \{(\pm 1,0),(0,\pm 1)\}, & n \text{ even} \end{cases}.$$

Exercise 1.20. Let $f \in \bar{K}[X]$. Show that $V = V(f)$ is a variety if and only if f is irreducible. Show that $f(X,Y) = X^n + Y^n - 1$ is irreducible.

Corollary 1.21. *Let $V \subset \mathbb{A}^n_{\bar{k}}$ be an algebraic variety. Then as a set V is in bijection with the maximal ideals of $\bar{k}[V]$. Concretely, a point $p \in V$ corresponds to the maximal ideal $\mathfrak{m}_p := \{f \in \bar{k}[V] | f(p) = 0\}$.*