602: Algebra II

Nir Elber

Spring 2025

Contents

How strange to actually have to see the path of your journey in order to make it.

—Neal Shusterman, [Shu16]

Theme 1
Introduction

1.1 January 30

I missed the first class due to an interview. Hopefully I have some idea of what is going on. This class has a grader, named Chuhuan Huang; his email is `chuaun@jh.edu`.

1.1.1 Algebraic Sets

Today we will continue talking about algebraic sets. Our exposition follows [Lan02, Section 11.2]. We recall the definition.

Definition 1.1 (algebraic)**.** Fix a field k. An *algebraic set* is a subset $A \subseteq k^n$ for which there is an ideal $I \subseteq k[x_1, \dots, x_n]$ for which

$$A = \{x \in k^n : f(x) = 0 \text{ for all } f \in I\}.$$

We may say that A is the zero set $Z(I)$ for the polynomials f.

Remark 1.2. One may replace the ideal I with a general subset $S \subseteq k[x_1, \dots, x_n]$. This does not increase the generality because the subset $Z(S) \subseteq k^n$ of zeroes of S is the same as the subset $Z(I)$ where I is the ideal generated by S.

Algebraic sets form some classical version of algebraic geometry, which encodes a certain communication between geometry and algebra. For example, the affine space $k^n = \mathbb{A}_k^n$ and the algebra $k[x_1, \dots, x_n]$.

Last time, we stated the nullstellensatz. This requires the notion of the radical.

Definition 1.3 (radical)**.** An ideal I of a ring R is *radical* if and only if any $a \in R$ for which there is $n \geq 0$ such that $a^n \in I$ satisfies $a \in I$. Given any ideal I of a ring R, one can define the radical ideal $\sqrt{I}$ as

$$\{a \in R : a^n \in I \text{ for some } n \geq 0\}.$$

Example 1.4. Given an algebraic set $A \subseteq \mathbb{A}_k^n$, one can check that the ideal

$$I(A) \coloneqq \{f \in k[x_1, \dots, x_n] : f(x) = 0 \text{ for all } x \in A\}$$

is a radical ideal.

And here is our statement.

Theorem 1.5 (Nullstellensatz)**.** Fix an algebraically closed field k and a positive integer n. Then there is a bijection between the set of algebraic subsets of an affine space $\mathbb{A}_k^n$ and the radical ideals $I \subseteq k[x_1, \dots, x_n]$. This bijection is given by the constructions $I \mapsto Z(I)$ and $A \mapsto I(A)$.

Proof. This theorem is rather hard, so we will not attempt to prove it now. ■

Remark 1.6. One can check that the bijections in Theorem 1.5 are inclusion-reversing. For example, an inclusion $A \subseteq B$ of algebraic sets induces an inclusion of ideals $I(B) \subseteq I(A)$.

This is remarkable because it will let us play algebraic intuition and geometric intuition off of each other, which each have their own strengths.

As a sort of example of this interplay, we recall the notion of Noetherian.

Definition 1.7 (Noetherian)**.** A ring R is *Noetherian* if and only if any ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq \cdots$$

eventually stabilizes; i.e., there should exist some N such that $I_n = I_m$ for any $n, m > N$.

As such, the bijection of Theorem 1.5 tells us that algebraic sets satisfies some kind of descending chain condition: any descending chain

$$A_1 \supseteq A_2 \supseteq \cdots$$

of algebraic sets must stabilize in the sense there is N for which $A_n = A_m$ whenever $n, m > N$.

As another example, we note that there are natural geometric operations of union and intersection of algebraic sets. Here are the corresponding operations on ideals.

Lemma 1.8. Fix two ideals I and J of a ring R.

(a) The intersection $I \cap J$ is an ideal of R.

(b) The sum $I + J = \{a + b : a \in I \text{ and } b \in J\}$ is an ideal of R.

Proof. Omitted. The idea is to unravel the definition of ideals everywhere. ■

The point is that, for algebraic sets A and B, one can check that $I(A \cup B) = I(A) \cap I(B)$ and $I(A \cap B) = \sqrt{I(A) + I(B)}$. For example, to check that $I(A \cup B) = I(A) \cap I(B)$, we must check that some $f \in k[x_1, \dots, x_n]$ vanishes on $A \cup B$ if and only if it vanishes on both A and B. Similarly, to check $I(A \cap B) = \sqrt{I(A) + I(B)}$, Theorem 1.5 allows us to check that $A \cap B$ is cut out by $I(A) + I(B)$, which can be done after some effort.

1.1.2 Irreducible Algebraic Sets

On the geometric side, one often finds that our algebraic sets can be decomposed into smaller pieces.

Example 1.9. The algebraic set $x_1 x_2 = 0$ inside $\mathbb{A}_k^2$ is the union of the two lines $x_1 = 0$ and $x_2 = 0$.

To prevent this sort of thing from happening, we introduce irreducibility.

Definition 1.10 (irreducible)**.** Fix an algebraically closed field k. An algebraic set $A \subseteq \mathbb{A}_k^n$ is *irreducible* if and only if any decomposition $A = A_1 \cup A_2$ into algebraic subsets has $A = A_1$ or $A = A_2$.

This allows us to define the notion of variety.

Definition 1.11 (variety)**.** Fix an algebraically closed field k. An *affine algebraic variety* over k is an irreducible algebraic set.

Of course, with a notion of irreducibility, we would like to know that we can always break down algebraic sets into irreducible ones.

Proposition 1.12. Fix an algebraically closed field k.

(a) For any algebraic set $A \subseteq \mathbb{A}_k^n$, there are irreducible algebraic subsets $V_1, \dots, V_n$ such that

$$A = V_1 \cup \cdots \cup V_n.$$

(b) The decomposition in (a) is unique up to permutation and inclusions.

(c) Fix irreducible algebraic subsets $W, V_1, \dots, V_n$ such that $W \subseteq V_1 \cup \cdots \cup V_n$. Then $W \subseteq V_i$ for some i.

Proof. Here we go.

(a) This is an example of "Noetherian induction." If A is irreducible, then we are done. Otherwise, we may write A as a union of proper algebraic subsets $A_1 \cup A_2$. If A_1 and A_2 are irreducible, then we are done. Otherwise, we can continue decomposing them. Note that this process must eventually terminate by the descending chain condition described above.

(b) Suppose that we have two equal unions

$$V_1 \cup \cdots \cup V_n = W_1 \cup \cdots \cup W_m$$

of irreducible algebraic sets. It is enough to check that each V_i is included in some W_j, for then one finds that the decompositions must be the same up to permutation and inclusion. This last claim follows from (c), which we prove next (and independently).

(c) Note that

$$W = (W \cap V_1) \cup \cdots \cup (W \cap V_n).$$

Thus, we have decomposed W into a union of algebraic sets, so we must have $W = W \cap V_i$ for some i. The result follows. ∎

Corollary 1.13. Fix an algebraically closed field k. Then an algebraic set $A \subseteq \mathbb{A}_k^n$ is irreducible if and only if $I(A)$ is a prime ideal.

Proof. We show our two implications separately. Set $I \coloneqq I(A)$ for brevity.

- Suppose that I is not prime, and we will show that A is not irreducible. Well, because I is not prime, we are granted $f, g \notin I$ such that $fg \in I$. Then define $A_1 \coloneqq Z(I + (f))$ and $A_2 \coloneqq Z(I + (g))$ so that A_1 and A_2 are proper subsets of A. We finish by claiming that $A = A_1 \cup A_2$. Well, $x \in A$ will have $(fg)(x) = 0$, so $f(x) = 0$ or $g(x) = 0$, so $x \in A_1$ or $x \in A_2$.

- Suppose that A is not irreducible, and we will show that I is not prime. Well, we are granted a decomposition $A = A_1 \cup A_2$ of A into proper algebraic subsets, and write $I_1 = I(A_1)$ and $I_2 = I(A_2)$. Then Theorem 1.5 tells us that there must be $f \in I_1 \setminus I$ and $g \in I_2 \setminus I$. But then fg can be checked to vanish on $A_1 \cup A_2$, so $fg \in I$, and we are done. ∎

1.1.3 Asides

A key benefit of geometry is that one expects to have some topological structure. However, for an arbitrary field k, it is not so obvious how to do this. The solution is the Zariski topology.

Definition 1.14 (Zariski topology)**.** Fix a field k. Then we define the *Zariski topology* on $\mathbb{A}_k^n$ as given by requiring that the closed sets are exactly the algebraic sets.

Remark 1.15. Let's check that the Zariski topology is actually a topology.

- Note that $\varnothing$ is an algebraic set cut out by $k[x_1, \dots, x_n]$, and $\mathbb{A}_k^n$ is an algebraic set cut out by (0).
- For two algebraic sets A and B, the union $A \cup B$ is still algebraic by Lemma 1.8.
- For a collection $\{A_i\}$ of closed sets, the intersection must go down to a finite intersection by the descending chain condition, which is then algebraic by Lemma 1.8.

As a quick aside, let's gesture towards algebraic geometry. For example, there is an irreducible decomposition for general rings, even working for rings which are not radical; this is known as the primary decomposition. For example, the algebraic set cut out by (x^2y) should be expanded as $(x^2) \cap (y)$, and even though (x^2) is not radical! This is the realm of scheme theory.

In our classical language above, we see that closed points of $\mathbb{A}_k^n$ correspond to maximal ideals $\mathfrak{m} \subseteq k[x_1, \dots, x_n]$: simply send $(a_1, \dots, a_n) \in \mathbb{A}_k^n$ to the ideal

$$(x_1 - a_1, \dots, x_n - a_n)$$

which cuts out this point. When moving to scheme theory, maximal ideals will produce points, but we will have other points; maximal ideals will correspond precisely to the closed points.

Remark 1.16. If k fails to be algebraically closed, field, we note that the bijection between n-tuples in $\mathbb{A}_k^n$ and maximal ideals breaks down. For example, if $k = \mathbb{R}$, then the ideal $(x^2 + 1) \subseteq \mathbb{R}[x]$ is maximal, but it cuts out no points in $\mathbb{A}_{\mathbb{R}}^1$; similarly, $(x^2 + y^2 + 1) \subseteq \mathbb{R}[x, y]$ is maximal! We may say that these maximal ideals cut out a closed point "of degree 2" because they are generated by a polynomial of degree 2. It turns out that all closed points in $\mathbb{A}_{\mathbb{R}}^n$ have degree 1 or 2; this boils down to a classification of the maximal ideals in $\mathbb{R}[x_1, \dots, x_n]$.

Remark 1.17 (Pappus)**.** It is possible to detect the commutativity of the field k using geometry. This is a configuration due to Pappus. In short, one considers two pairs of collinear points (P_1, P_5, P_3) and (P_4, P_2, P_6). It turns out that the collinearity of the intersections $\overline{P_1P_2} \cap \overline{P_4P_5}$ and $\overline{P_5P_6} \cap \overline{P_2P_3}$ and $\overline{P_1P_6} \cap \overline{P_3P_4}$ exactly corresponds to an algebraic equation which detects commutativity of k. To be slightly more formal, one can write out what the collinearity means in terms of an algebraic equation in terms of elements of k, and this equation is always satisfied in elements of k if and only if k is commutative.

1.1.4 Kummer Theory

Our exposition follows [Lan02, Theorems 8.1–8.2]. Similar to Galois theory, Kummer theory is interested in a duality between fields and groups. However, Kummer theory will work only with abelian extensions and pay special attention to cyclic extensions. In this sense, Kummer theory is more related to class field theory (in number theory) than Galois theory.

For this discussion, we fix a field k (probably not algebraically closed) and a positive integer m, and we assume for simplicity that $\operatorname{char} k \nmid m$. We are interested in Galois extensions K of k with abelian Galois group of exponent m. Intuitively, this means that $\operatorname{Gal}(K/k)$ is sum of cyclic groups whose sizes divide m. The key assumption of Kummer theory is that $\mu_m \subseteq k$, where μ_m means the set of mth roots of unity.

Example 1.18. The extensions of $\mathbb{Q}$ which are Galois with Galois group of exponent 2 are called "multi-quadratic." It turns out that they can also be described as being generated by square roots of elements of $\mathbb{Q}$. This is possible, from the perspective of Kummer theory, because $\mu_2 = \{\pm 1\}$ is contained in $\mathbb{Q}$.

Remark 1.19. Relaxing the condition $\mu_m \subseteq k$ dives into class field theory. Relaxing the condition that our extensions are abelian leads towards the Langlands program.

Here is the main theorem, which extends the above example.

Theorem 1.20 (Kummer)**.** Fix a field k and a positive integer m. Suppose that $\operatorname{char} k \nmid m$ and $\mu_m \subseteq k$.

(a) There is a map sending subgroups B between $k^{\times m}$ and $k^\times$ to abelian extensions K/k of exponent m. This map sends B to the extension $K = k(B^{1/m})$ of k generated by the mth roots of B.

(b) The map in (a) is an inclusion-reversing bijection.

(c) Given some such B, the extension K_B/k is finite if and only if the index $[B : k^{\times m}]$ is finite.

We will prove this next time. The key input is some Kummer pairing. (We will stay away from any modern cohomological point of view.)

BIBLIOGRAPHY

[Lan02] Serge Lang. *Algebra / Serge Lang.* eng. Revised Third Edition. Graduate texts in mathematics ; 211. New York: Springer, 2002. ISBN: 038795385X.

[Shu16] Neal Shusterman. *Scythe*. Arc of a Scythe. Simon & Schuster, 2016.

List of Definitions