Intro to Algebraic Geometry - Nir Avni

Raz Slutsky

Abstract

Notes for a course on Algebraic Geometry given by Prof. Nir Avni at the Weizmann Institute of Science, Fall 2019.
This course is going to present some of the fundamental theorems and notions. The price we pay for that is that we're going to work with some more basic (that is, old) definitions of the objects we deal with. The course is divided into two parts. Every lecture will be divided into two parts. The first one on Algebraic curves (that is, algebraic geometry in one dimension), and the second part will be more general algebraic geometry.

1 Lecture 1 - Part 1

Definition 1.1. Let $f \in \mathbb{C}[x, y]$. Then the locus of f, denoted by

$$Z(f) = \{(a, b) \in \mathbb{C}^2 \mid f(a, b) = 0\}$$

is called an **affine algebraic curve**.

We work over $\mathbb{C}$ because it turns out to be easier, and many times will imply the real case. An easy property is the following-

- $Z(f \cdot g) = Z(f) \cup Z(g)$

$f \in \mathbb{C}[x, y]$ is called irreducible if it is not a product of two lower degree polynomials.

Theorem 1.2. *If $f, g \in \mathbb{C}[x, y]$ are irreducible and not co-linear then $|Z(f) \cap Z(g)| < \infty$*

Remark 1.3. Note that this implies the real case as well.

For the we will need the following lemma.

Lemma 1.4. *If $f \in \mathbb{Q}[x,y]$ is irreducible, then $f(\pi,y) \in \mathbb{Q}(\pi)[y]$ is irreducible.*

Proof. Assume the contrary, that is, $f(\pi,y) = A(y)B(y)$. Multiply by the common denominator of the coefficients of A and B, so we get

$$d(\pi) \cdot f(\pi,y) = a(\pi,y) \cdot b(\pi,y)$$

for some $d \in \mathbb{Q}[x]$ and $a, b \in \mathbb{Q}[x,y]$.

Looking at the coefficients of the LHS and RHS, we get polynomials with rational coefficients that agree on π. But π is transcendental, so this means every coefficient in the LHS is the same as the coefficient in the RHS, and so the polynomials are the same.

Now look at a complex root, α, of d. Let's plug it in the previous equality instead of x. We get that the LHS is zero, and so either $a(\alpha,y) = 0$ or $b(\alpha,y) = 0$ (The zero polynomial). If $a(\alpha,y) = 0$ then for $a(x,y) = a_0(x) + a_1(x)y + ...$ this means that $a_i(\alpha) = 0$ for all i, and so $(x-\alpha)$ divides $a(x,y)$. We can thus divide both sides of the previous equation by $(x-\alpha)$ and get a lower degree equation. Continue until $\deg(d) = 0$, and then we get $f(x,y) = a(x,y) \cdot b(x,y)$. A contradiction. □

Remark 1.5. Formally, to make sure that when we divide by $(x-\alpha)$ we still get rational polynomials, we need to divide by all Galois conjugates of α.

Proof of Theorem. We start with the case where $f, g \in \mathbb{Q}[x,y]$.

By the Lemma, $f(\pi,y), g(\pi,y)$ are irreducible and (prove at home) they are not co-linear. Therefore, $gcd(f(\pi,y), g(\pi,y)) = 1$, therefore there are polynomials $A, B \in \mathbb{Q}(\pi)[y]$ such tha t $A(y) \cdot f(\pi,y) + B(y) \cdot g(\pi,y) = 1$. Multiply by the denominators of the coefficients of A, B and get

$$a(\pi,y) \cdot f(\pi,y) + b(\pi,y) \cdot g(\pi,y) = d(\pi)$$

where all polynomials are now over the rationals. As before, since we have equality at π, we have equality everywhere, that is, $a(x,y) \cdot f(x,y) + b(x,y) \cdot g(x,y) = d(x)$. Now, if $(\alpha,\beta) \in Z(f) \cap Z(g)$ then $d(\alpha) = 0$, but d has only finitely many roots. Similarly, β has only finitely many possibilities.

□

In general, this argument works the same, the only special thing about $\mathbb{Q}$ and π is that π is transcendental over $\mathbb{Q}$. Given f, g we let $k \subset \mathbb{C}$ be the field generated by the coefficients of f, g over $\mathbb{Q}$. Pick $\theta \in \mathbb{C}$, a transcendental element over k and run the same argument.

Alternatively, work with $\mathbb{C}(x), x$ instead of $\mathbb{Q}, \pi$.

1.1 Takeaways from the proof

- The first idea was to take a polynomial and plug into the first variable some number, so we reduced the problem from a two variable problem to a one variable problem. In general,

$$Z(f(x,y)) = \bigcup_{\alpha \in \mathbb{C}} Z(f(\alpha, y))$$

  Geometrically, we look at the projection to the $x-$axis and think about $Z(f)$ as the union of the fibres of this projection. In other words, affine curves are families of finite sets varying with parameter in $\mathbb{C}$.

- What we showed is that over a generic point, π, the curves don't intersect, and we found out algebraically, that at almost all other points they also don't intersect. In other words, the behaviour of equations at a generic parameter controls the behaviour over almost all parameters. This method is called the generic point method.

Corollary 1.6.
- *$C[x,y]$ is a unique factorization domain. If f is irreducible, then if f divides $g \cdot h$ then f divides g or f divides h, because the zero locus of f is contained in the union of the loci of g, h. But one of them must be infinite, so f mus be co-linear with one of them.*
- *If $Z(f) = Z(g)$ then f, g have the same irreducible factors. In other words, f divides g^n or g divides f^n for n large enough.*
- *Every affine curve has a canonical (up to scalar) equation.*

2 Lecture 1 - Part 2

Definition 2.1. Let $S \subset \mathbb{C}[x_1, ..., x_n]$. The common zero locus of S,

$$Z(S) = \{\alpha \in \mathbb{C}^n \mid f(\alpha) = 0 \; \forall f \in S\}$$

is called an **Algebraic Set**.

Remark 2.2. $Z(S) = Z((S))$ where (S) is the ideal generated by S.

Theorem 2.3 (Hilbert Basis Theorem)**.** *Any ideal in* $\mathbb{C}[x_1, ..., x_n]$ *is generated by a finite set*

Corollary 2.4. *Any system of polynomial equations is equivalent to a finite system of equations*

Proof.

Lemma 2.5. *If* $V \subset \mathbb{C}[x]^n$ *is a* $\mathbb{C}[x]$*-submodule, then* V *is finitely generated*

Proof. Induction on n: for $n = 1$ a sub-module just means an ideal, and ideals are finitely generated.

For the induction step, $n+1$, look at $\pi : V \to \mathbb{C}[x]$, the projection to the last coordinate. We have the short exact sequence

$$0 \to \ker(\pi) \to V \to \pi(V) \to 0$$

And the kernel is contained in $\mathbb{C}[x]^{n-1}$ so it is finitely generated. An extension of f.g. modules is finitely generated. □

Look at $I \lhd \mathbb{C}[x, y]$. For $f \in I$ we can write $f(x, y) = a_0^f(x) + a_1(x) \cdot y + ... + a_m^f(x) \cdot y^m$. Where the leading coefficient is non-zero, that is, $a_f := a_m^f(x) \neq 0$. Consider the ideal $J \lhd \mathbb{C}[x, y]$ generated by all $a_f, f \in I$. By induction, J is finitely generated, so $J = (a_{f_1}, ..., a_{f_n})$. Exercise: $J = \{a_f \mid f \in I\}$. Let d be the maximal $y-$degree of $f_1, ..., f_n$. We claim that if $g \in I$, then there are $h_1, ..., h_n$ such that $g - \sum h_i f_i$ has $y-$degree less than d. Given the claim, I is generated by $f_1, ..., f_n$ and generators of the module $I \cap \{$ polynomials of $y -$ degree $< d\} \cong I \cap \mathbb{C}[x]^d$. □

Example 2.6.

- Every affine curve is an algebraic set
- $Z(\{1\}) = \emptyset, Z(\{0\}) = \mathbb{C}^n$ are algebraic sets.
- $Z(\cup_i S_i) = \cap_i Z(S_i)$
- $Z(S_1) \cup Z(S_2) = Z(S_1 \cdot S_2)$.

Remark 2.7. These properties say that the collection of algebraic subsets of $\mathbb{C}^n$ defines a topology called "Zariski Topology" where algebraic sets are the basic closed sets.

Algebraic sets in $\mathbb{C}$ are either $\mathbb{C}$ or finite sets (that is, the Zariski topology on $\mathbb{C}$ is the co-fonite topology).

Any Zariski open set in $\mathbb{C}^n$ is open, dense, connected in the usual topology.

Proof. Let's prove that it is connected. If U is a Zariski open set, and $p, q \in U$, let l be the complex line incident to p, q. Then we have that $\mathbb{C} \cong l \supset l \cap U$ is a non-empty Zariski open subset of $\mathbb{C}$, so it is co-finite. Hence there is a path in $U \cap l$ between p and q. □

Theorem 2.8 (Hilbert's Nullstellensatz)**.** *If a system of equations S has a solution in some field extension of $\mathbb{C}$, then it has a solution in $\mathbb{C}$.*

Proof. W.L.O.G we can assume that S is finite. Let $k \subset \mathbb{C}$ be the field generated by the coefficients of the elements in S. Let α be a solution in L^n where $L \supset \mathbb{C}$. Consider $K(\alpha_1, ..., \alpha_n) \subset L$. By induction on n, we will show that there is a homomorphism $\theta : k(\alpha_1, ..., \alpha_n) \to \mathbb{C}$ such that $\theta|_k = id$.

$n = 0$ is clear. Let's do $n = 1$. Look at $k(\alpha_1)$. There are two options:

- either α_1 is algebraic over k, and so α_1 solves an equation $f(x) = 0$. Since $\mathbb{C}$ is algebraically closed, there is $\beta \in \mathbb{C}$ solving the same equation. Now the map $\alpha_1 \mapsto \beta$ extends to a homomorphism of $k(\alpha_1) \hookrightarrow \mathbb{C}$
- α_1 is transcendental over k. Now we take $\beta \in \mathbb{C}$ a transcendental element over k, and map $\alpha_1 \mapsto \beta$.

Now $\theta(\alpha_1, ..., \alpha_n) \in \mathbb{C}^n$ is a solution of S, since

$$0 = \theta(f(\alpha_1, ..., \alpha_n)) = f(\theta(\alpha_1), ..., \theta(\alpha_n))$$

□

Another version of the theorem is that $Z(S) = \emptyset \iff (S) = \mathbb{C}[x_1, ..., x_n] \iff 1 \in (S)$.

Proof. Assume that (S) is a proper ideal. Choose $\mathfrak{m}$ a maximal ideal containing (S). Look at the field $L = \mathbb{C}[x_1, ..., x_n]/\mathfrak{m}$. We have a solution there since $(x_1 + \mathfrak{m}, ..., x_n + \mathfrak{m})$ is a solution of S, and for $f \in S$ we have $f(\overline{x_1}, \overline{x_2}, ..., \overline{x_n}) = \overline{f(x_1, ..., x_n)} = 0$. □

An even fancier version is the following: f vanishes on $Z(S) \iff f^n \in (S)$ for some $n > 0$.

Rabinowitz Trick. f vanishes on $Z(S) \iff \{f(x_1, ..., x_n) \cdot y - 1\} \cup S$ has no solution. But this implies by Hilbert's Nullstellensatz that $1 \in \{f(x_1, ..., x_n) \cdot y - 1\} \cup S$ and so

$$1 = h(f(x_1, ..., x_n) \cdot y - 1) + h_1 f_1 + ...h_m f_m$$

for some $f_1, ..., f_m \in S$ and $h, h_1, ..., h_m \in \mathbb{C}[x_1, ..., x_n, y]$. If we plug $y = \frac{1}{f(x_1,...,x_n)}$ we get

$$1 = h_1(x_1, ..., x_n, \frac{1}{f}) \cdot f_1 + ... + h_m(x_1, ..., x_n, \frac{1}{f}) \cdot f_m$$

Where this equation is in the ring $\mathbb{C}[x_1, ..., x_n][\frac{1}{f}]$. Now multiply by f^n for $n > 0$ big enough. So we get that $f^n = H(x_1, ..., x_m)f_1 + ... + H_m(x_1, ..., x_m)f_m$ where now this equality can be considered in $\mathbb{C}[x_1, ..., x_n]$. □

Definition 2.9. $I \lhd \mathbb{C}[x_1, ..., x_n]$. Define

$$\sqrt{I} = \{f \in \mathbb{C}[x_1, ..., x_n] \mid f^m \in I \text{ for some } m > 0\}$$

Corollary 2.10. $Z(I_1) = Z(I_2) \iff \sqrt{I_1} = \sqrt{I_2}$

Proof. If $f \in \sqrt{I_1}$ then f vanishes on $Z(I_1) = Z(I_2)$. By the fancier version, $f^m \in I_2$ for some $m > 0$, *i.e.* $f \in \sqrt{I_2}$. The other direction is due to the fact that $Z(I) = Z(\sqrt{I})$. □

References