Geometria Algébrica I

lecture 3: Strong Nullstellensatz

Misha Verbitsky

IMPA, sala 232

August 21, 2018

REMINDER: Affine varieties and finitely generated rings

DEFINITION: Category of affine varieties over $\mathbb{C}$: its objects are algebraic subsets in $\mathbb{C}^n$, morphisms – polynomial maps.

DEFINITION: Finitely generated ring over $\mathbb{C}$ is a quotient of $\mathbb{C}[t_1, ..., t_n]$ by an ideal.

DEFINITION: Let R be a ring. An element $x \in R$ is called **nilpotent** if $x^n = 0$ for some $n \in \mathbb{Z}^{>0}$.

Theorem 1: Let $\mathcal{C}_R$ be a category of finitely generated rings over $\mathbb{C}$ without non-zero nilpotents and $\mathcal{A}ff$ – category of affine varieties. Consider the functor $\Phi : \mathcal{A}ff \longrightarrow \mathcal{C}_R^{op}$ mapping an algebraic variety X to the ring of polynomial functions on X. **Then Φ is an equivalence of categories.**

Proof: Later in this lecture.

Strong Nullstellensatz

DEFINITION: Let $I \subset \mathbb{C}[t_1, ..., t_n]$ be an ideal. Denote the **set of common zeros** for I by $V(I)$, with

$$V(I) = \{(z_1, ..., z_n) \in \mathbb{C}^n \ \ | \ \ f(z_1, ..., z_n) = 0 \forall f \in I\}.$$

For $Z \subset \mathbb{C}^n$ an algebraic subset, denote by $\operatorname{Ann}(A)$ the set of all polynomials $P(t_1, ..., t_n)$ vanishing in Z.

THEOREM: (strong Nullstellensatz). For any ideal $I \subset \mathbb{C}[t_1, ..., t_n]$ such that $\mathbb{C}[t_1, ..., t_n]/I$ has no nilpotents, **one has** $\operatorname{Ann}(V(I)) = I$**.**

Proof: Later in this lecture.

REMARK: "Weak Nullstellensatz" claims that $V(I)$ is never empty for any non-trivial ideal I; "Strong Nullstellensatz" claims that I is uniquely determined by $V(I)$ when R/I has no nilpotents.

Strong Nullstellensatz and equivalence of categories

THEOREM: (strong Nullstellensatz). For any ideal $I \subset \mathbb{C}[t_1, ..., t_n]$ such that $\mathbb{C}[t_1, ..., t_n]/I$ has no nilpotents, **one has** $\operatorname{Ann}(V(I)) = I$**.**

Now we deduce Theorem 1 from Strong Nullstellensatz. This would require us to construct a functor $\Psi : \mathcal{C}_R^{op} \longrightarrow \mathcal{A}ff$. Since any object $R \in \mathcal{O}b(\mathcal{C}_R)$ is given as $R = \mathbb{C}[t_1, ..., t_n]/I$, we define Ψ as $\Psi(R) := V(I)$; the functor $\Phi : \mathcal{A}ff \longrightarrow \mathcal{C}_R^{op}$ was defined as $Z \longrightarrow \operatorname{Ann}(Z)$.

Strong Nullstellensatz gives $\operatorname{Ann}(V(I)) = I$, hence $\Phi(\Psi(R)) = R$ **for any finitely generated ring.** It remains to prove $V(\operatorname{Ann}(Z)) = Z$.

Clearly, $V(\operatorname{Ann}(Z)) \supset Z$: any point $z \in Z$ belongs to the set of common zeros of $\operatorname{Ann}(Z)$. On the other hand, Z is a set of common zeros of a system $\mathcal{P}$ of polynomial equations, giving $Z = V(\mathcal{P}) \supset V(\operatorname{Ann}(Z))$.

Localization

DEFINITION: Localization $R(F))$ of a ring R with respect to $F \in R$ is a ring $R[F^{-1}]$, which is formally generated by the elements of form a/F^n and relations $a/F^n \cdot b/F^m = ab/F^{n+m}$, $a/F^n + b/F^m = \frac{aF^m + bF^n}{F^{n+m}}$, and $aF^k/F^{k+n} = a/F^n$.

REMARK: Clearly, $R(F) = R[t]/(tF - 1)$.

EXAMPLE: $\mathbb{Z}[2^{-1}]$, the ring of rational numbers with denominators 2^k.
EXAMPLE: $\mathbb{C}[t, t^{-1}]$, the ring of Laurent polynomials.

EXERCISE: Let R be a finitely generated ring over a field k. **Prove that $R[F^{-1}]$ is a finitely generated ring over k.**

CLAIM 1: Suppose that $R[F^{-1}] = 0$, where $F \in R$. **Then F is nilpotent.**

Proof. Step 1: $R(F) = R[t]/(tF - 1)$. **Therefore, $1 = 0$ implies $1 = (Ft - 1)P$, for some $P \in R[t]$.**

Step 2: Let $P(t) = \sum a_i t^i$, where $a_i \in R$. **Then $1 = (Ft - 1)P$ implies $a_i = a_{i-1}F$ for all $i > 0$, and $a_0 = 1$.**

Step 3: This gives $P = \sum F^i t^i$, and $F^{n+1} = 0$. ■

Spectrum and localization

DEFINITION: Spectrum of a ring R is the set $\operatorname{Spec} R$ if its prime ideals.

EXERCISE: Let $R \xrightarrow{\varphi} R_1$ be a ring homomorphism. Prove that $\varphi^{-1}(\mathfrak{p})$ is a prime ideal, for any $\mathfrak{p} \in \operatorname{Spec} R_1$.

PROPOSITION: In other words, any morphism $R \longrightarrow R_1$ **gives an injective map of spectra** $\operatorname{Spec} R[f^{-1}] \hookrightarrow \operatorname{Spec} R$.

Proof: Suppose that $\mathfrak{p}_f, \mathfrak{q}_f \in \operatorname{Spec} R(f)$, and $\mathfrak{p} = \mathfrak{q}$ are their images in $\operatorname{Spec} R$. Then for each $p \in \mathfrak{p}_f$, we have $f^N p \in \mathfrak{q} \subset \mathfrak{q}_f$; since $\mathfrak{q}$ is prime, this implies that $p \in \mathfrak{q}$. ■

DEFINITION: Nilradical of a ring R is the set $\operatorname{Nil}(R)$ of all nilpotent elements of R.

THEOREM: Interesection P of all prime ideals of R is equal to $\operatorname{Nil}(R)$.

Proof: Clearly, $P \supset \operatorname{Nil}(R)$. Assume that, conversely, $x \notin \operatorname{Nil}(R)$. Then $R[x^{-1}] \neq 0$, **hence $R[x^{-1}]$ contains a prime ideal** (the maximal one), and its image in $\operatorname{Spec} R$ does not contaim x. ■

Rabinowitz trick

DEFINITION: Let $I \subset \mathbb{C}[t_1, ..., t_n]$ be an ideal. Recall that the set of common zeros of I is denoted by $V(I)$ **("vanishing set", "null-set", "zero set"),** and the set of all polynomials vanishing in $Z \subset \mathbb{C}^n$ is denoted $\operatorname{Ann}(Z)$ **("annihilator").**

Theorem 1: Let $I \subset \mathbb{C}[t_1, ..., t_n]$ be an ideal, and f a polynomial function, vanishing on $V(I)$. **Then $f^N \in I$ for some $N \in \mathbb{Z}^{>0}$.**

Proof. Step 1: Consider an ideal $I_1 \subset \mathbb{C}[t_1, ..., t_{n+1}]$ generated by $I \subset \mathbb{C}[t_1, ..., t_n]$ and $ft_{n+1} - 1$. **Since the submodule of R generated by $\langle ft_{n+1} - 1, I\rangle$ has no common zeros, I_1 contains 1** by (weak) Nullstellensatz.

Step 2: Let $R := \mathbb{C}[t_1, ..., t_n]/I$. Consider the map $\zeta : \mathbb{C}[t_1, ..., t_{n+1}] \longrightarrow R[f^{-1}]$ which is identity on $t_1, ..., t_n$ and mapping t_{n+1} to f^{-1}. Since $\zeta(I_1) = 0$, and $1 \in I_1$, one has $1 = 0$ in $R[f^{-1}]$, giving $R[f^{-1}] = 0$. **By Claim 1, f is nilpotent in R.** ■

COROLLARY: (Strong Nullstellensatz)
Suppose that $R := \mathbb{C}[t_1, ..., t_n]/I$ is a ring without nilpotents. **Then $I = \operatorname{Ann}(V_I))$.**

Proof: If $a \in \operatorname{Ann}(V_I))$, then $a^n \in I$ by Theorem 1. ■

Smooth points

DEFINITION: Let $A \subset \mathbb{C}^n$ is an algebraic subset. A point $a \in A$ is called **smooth**, if there exists a neighbourhood U of $a \in \mathbb{C}^n$ (in usual topology) such that $A \cap U$ is a smooth $2k$-dimensional real submanifold. A point is called **singular** if such diffeomorphism does not exist. A variety is called **smooth** if it has no singularities, and **singular** otherwise.

PROPOSITION: For any algebraic variety A and any smooth point $a \in A$, a diffeomorphism between a neighbourhood of a and an open ball **can be chosen polynomial**.

Proof. Step 1: Inverse function theorem. Let $a \in M$ be a point on a smooth k-dimensional manifold and $f_1, ..., f_k$ functions on M such that their differentials $df_1, ..., df_k$ are linearly independent in a. Then $f_1, ..., f_k$ **define a coordinate system in a neighbourhood of a, giving a diffeomorphism of this neighbourhood to an open ball.**

Step 2: If $a \in A \subset \mathbb{C}^n$ is a smooth point of a k-dimensional embedded manifold, **there exists k complex linear functions on $\mathbb{C}^n$ which are linearly independent on $T_a A$.**

Step 3: These function define **diffeomorphism from a neighbourhood of A to an open subset of $\mathbb{C}^k$.** ■

Maximal ideal of a smooth point

REMARK: The set of smooth points of A is open.

CLAIM: Let $\mathfrak{m}_x$ be a maximal ideal of a smooth point of a k-dimensional manifold M. **Then $\dim_{\mathbb{C}} \mathfrak{m}_x/\mathfrak{m}_x^2 = k$.**

Proof: Consider a map $d_x : \mathfrak{m}_x \longrightarrow T_x^*M$ mapping a function f to $df|_x$. Clearly, d_x is surjective, and satisfies $\ker d_x = \mathfrak{m}_x^2$ **(prove it!)** ■

CLAIM: A manifold $A \subset \mathbb{C}^2$ given by equation $xy = 0$ **is not smooth in $a := (0,0)$.**

Proof. Step 1: $\mathfrak{m}_a/\mathfrak{m}_a^2$ is the quotient of the space of all polynomials, vanishing in a, that is, degree $\geqslant 1$, by all polynomials of degree $\geqslant 2$, hence it is 2-dimensional.

Step 2: Therefore, if a is smooth point of A, A is 2-dimensional in a neighbourhood of $(0,0)$. **However, outside if a, A is a line, hence 1-dimensional:** contradiction. ■

Hard to prove, but intiutively obvious observations

EXERCISE: Prove that **the set of smooth points of an affine variety is constructible**, that is, obtained as a complement of an algebraic set to an algebraic set.

Really hard exercise: Prove that **any affine variety over $\mathbb{C}$ contains a smooth point.**

EXERCISE: Using these two exercises, **prove that the set of smooth points of A is dense in A.**

Irreducible varietiees

DEFINITION: A affine manifold A is called **reducible** if it can be expressed as a union $A = A_1 \cup A_2$ of affine varieties, such that $A_1 \not\subset A_2$ and $A_2 \not\subset A_1$. If such a decomposition is impossible, A is called **irreducible**.

CLAIM: An affine variety A is **irreducible** if and only if its ring of polynomial functions $\mathcal{O}_A$ **has no zero divizors.**

Proof: If $A = A_1 \cup A_2$ is a decomposition of A into a non-trivial union of subvarieties, choose a non-zero function $f \in \mathcal{O}_A$ vanishing at A_1 and g vanishing at A_2. The product of these non-zero functions vanishes in $A = A_1 \cup A_2$, **hence $fg = 0$ in $\mathcal{O}_A$.** Conversely, **if $fg = 0$, we decompose $A = V_f \cup V_g$.** ■

Irreducibility for smooth varieties

EXERCISE: Let M be an algebraic variety which is smooth and connected. **Prove that it is irreducible.**

COROLLARY: Let A be an affine manifold such that its set A_0 of smooth points is dense in A and connected. **Then A is irreducible.**

Proof: If f and g are non-zero function such that $fg = 0$, the ring of polynomial functions on A_0 contains zero divizors. However, **on a smooth, connected complex manifold the ring of polynomial functions has no zero divisors by analytic continuity principle.** ■

EXERCISE: Let $X \longrightarrow Y$ be a morphism of affine manifols, where X is irreducible, and its image in Y is dense. **Prove that Y is also irreducible.**

Noetherian rings and irreducible components

DEFINITION: A ring is called **Noetherian** if any increasing chain of ideals stabilizes: for any chain $I_1 \subset I_2 \subset I_3 \subset ...$ one has $I_n = I_{n+1} = I_{n+2} = ...$

THEOREM: (Hilbert basis theorem)
Any finitely generated ring is Noetherian.

DEFINITION: **An irreducible component** of an algebraic set A is an irreducible algebraic subset $A' \subset A$ such that $A = A' \cup A''$, and $A' \not\subset A''$.

Remark 1: Let $A_1 \supset A_2 \supset ... \supset A_n \supset ...$ be a decreasing chain of algebraic subsets in an algebraic variety. **Then the corresponding ideals form an increasing chain of ideals:** $\operatorname{Ann}(A_1) \subset \operatorname{Ann}(A_2) \subset \operatorname{Ann}(A_3) \subset ...$

THEOREM: Let A be an affine variety, and $\mathcal{O}_A$ its ring of polynomial functions. Assume that $\mathcal{O}_A$ is Noetherian. Then A **is a union of its irreducible components, which are finitely many.**

Proof: See the next slide ■

Remark 2: From the noetherianity and Remark 1 it follows that A **cannot contain a strictly decreasing infinite chain of algebraic subvarieties.**

Noetherian rings and irreducible components (2)

THEOREM: Let A be an affine variety, and $\mathcal{O}_A$ its ring of polynomial functions. Assume that $\mathcal{O}_A$ is Noetherian. Then A **is a union of its irreducible components, which are finitely many.**

Proof. Step1: Each point $a \in A$ belongs to a certain irreducible component. Indeed, suppose that such a component does not exist. Then for each decomposition $A = A_1 \cup A_2$ of A onto algebraic sets, the set A_i containing a can be split non-trivially onto a union of algebraic sets, the component containing a can also be split, and so on, *ad infinitum*. This gives a strictly decreasing infinity sequence, a contradiction (Remark 2).

Step 2: We proved existence of an irreducible decomposition, and **it remains only to show that number of irreducible components of A is finite.** Let $A = \bigcup A_i$ be an irreducible decomposition. Then each A_i is not contained in the union of the rest of A_i.

Step 3: Let **algebraic closure** of a set $X \subset \mathbb{C}^n$ be the intersection of all algebraic subsets containing X. Clearly, it is algebraic **(prove it!)** Since $A = A_i \cup \bigcup_{j\neq i} A_j$, the algebraic closure B_i of $A \backslash A_i$ does not contain A_i. and **the sequence $B_1 \supset B_1 \cap B_2 \supset B_1 \cap B_2 \cap B_3 \subset ...$ decreases strictly, unless there are only finitely many irreducible components.** Applying Remark 2 again, we obtain that the number of B_i is finite. ■