Geometria Algébrica I

lecture 1: Hilbert's Nullstellensatz

Misha Verbitsky

IMPA, sala 232

August 13, 2018

The Plan.

1. Algebraic sets.

2. Ideals; existence of maximal ideals.

3. Hilbert's Nullstellensatz.

4. Continuum-dimensional spaces and the proof of Nullstellensatz.

Preliminaries: I assume knowledge of **groups**, **rings**, **fields**, **vector spaces**, basic set theory (surjective, injective, bijective maps, cardinals, equivalence classes), **topological spaces**, and **Hausdorff spaces**. It is possible that at a later point we shall need **implicit map theorem**. For today's lecture (and only) we use advanced set theory, such as Zorn lemma.

Algebraic sets in $\mathbb{C}^n$

REMARK: In most situations, you can replace your ground field $\mathbb{C}$ by any other field. However, there are cases when chosing $\mathbb{C}$ as a ground field simplifies the situation. Moreover, **using $\mathbb{C}$ is essentially the only way to apply topological arguments which help us to develop the geometric intuition.**

DEFINITION: A subset $Z \subset \mathbb{C}^n$ is called **an algebraic set** if it can be goven as a set of solutions of a system of polynomial equations $P_1(z_1, ..., z_n) = P_2(z_1, ..., z_n) = ... = P_k(z_1, ..., z_n) = 0$, where $P_i(z_1, ..., z_n) \in \mathbb{C}[z_1, ..., z_n]$ are polynomials.

EXERCISE: Prove that **finite unions and finite intersections of algebraic sets are again algebraic sets.**

DEFINITION: Let $A \subset \mathbb{C}^m, A' \subset \mathbb{C}^n$ be algebraic sets. An **polynomial map** $\varphi: A \longrightarrow A'$ is a map from A to A' which is given in coordinates by a set of polynomial functions $\varphi_1, ..., \varphi_n: \mathbb{C}^m \longrightarrow \mathbb{C}$.

Algebraic geometry is (roughly speaking) the study of algebraic sets and polynomial maps between algebraic sets.

Affine varieties

DEFINITION: Algebraic function on an algebraic set $Z \subset \mathbb{C}^n$ is a restriction of a polynomial function to Z. An algebraic set with a ring of algebraic functions on it is called **an affine variety**.

DEFINITION: Two affine varieties A, A' are **isomorphic** if there exists a bijective polynomial map $A \longrightarrow A'$ such that its inverse is also polynomial.

REMARK: The cornerstone observation of algebraic geometry (essentially due to Hilbert and Emmy Noether): **an affine variety is determined, up to an isomorphism, by its ring of polynomial functions**.

To explain this, I would need to introduce some notions of commutative algebra.

Maximal ideals

REMARK: All rings are assumed to be commutative and with unity.

DEFINITION: An ideal I in a ring R is a subset $I \subsetneq R$ closed under addition, and such that for all $a \in I, f \in R$, the product fa sits in I.

REMARK: The quotient group R/I is equipped with a structure of a ring, called **the quotient ring**.

DEFINITION: A maximal ideal is an ideal $I \subset R$ such that for any other ideal $I' \supset I$, one has $I = I'$.

EXERCISE: Let $a \in R$ be an element of a ring which is not invertible. Prove that a **is contained in an ideal** $I \subset R$**.**

Using this exercise, one obtains the following statement.

EXERCISE: Prove that **an ideal** $I \subset R$ **is maximal if and only if** R/I **is a field.**

Existence of maximal ideals

THEOREM: Let $I \subset R$ be an ideal in a ring. **Then I is contained in a maximal ideal.**

Proof: One applies the Zorn lemma to the set of all ideals, partially ordered by inclusion. ■

CLAIM: Let A be an affine variety, $\mathcal{O}_A$ the ring of polynomial functions on A, $a \in A$ a point, and $I_a \subset \mathcal{O}_A$ an ideal of all functions vanishing in a. **Then I_a is a maximal ideal.**

Proof: For any $f \in \mathcal{O}_A$, the function $f - f(a)$ belongs to I_a, hence **the quotient $\mathcal{O}_A/I$ is isomorphic to $\mathbb{C}$.** ■

DEFINITION: The ideal I_a is called **the (maximal) ideal of the point $a \in A$.**

Basis for an infinite-dimensional space

THEOREM: (Hilbert's Nullstellensatz)
Let A be an affine variety, and $\mathcal{O}_A$ the ring of polynomial functions on A. **Then every maximal ideal in A is an ideal of a point $a \in A$: $I = I_a$.**

The proof **(which works only over $\mathbb{C}$)** is based on the following concept.

DEFINITION: Let V be a vector space (possibly, infinite-dimensional). **Basis** (in the sence of Hamel) of V is a set of vectors S in V such that any finite subset $S_0 \subset S$ is linearly independent, and any vector in V is expressed as a linear combination of some vectors in S.

EXERCISE: Using Zorn lemma, prove that **any vector space admits a basis.**

EXERCISE: Let S, S' be two basises (bases) in V. **Then S and S' have the same cardinality;** in particular, one of them is countable when another is countable.

DEFINITION: Dimension of an infinite-dimensional space V is cardinality of its basis.

Hilbert's Nullstellensatz

THEOREM: (Hilbert's Nullstellensatz)
Let $A \subset \mathbb{C}^n$ be an affine variety, and $\mathcal{O}_A$ the ring of polynomial functions on A. **Then every maximal ideal in A is an ideal of a point $a \in A$: $I = I_a$.**

Proof. Step 1: For an ideal $I \subset \mathcal{O}_A$, consider **the set of common zeros of I**:

$$V(I) := \{a \in A \quad | \quad \forall f \in I, f(a) = 0\}.$$

If $V(I)$ contains $a \in A$, one has $I \subset I_a$. This means that for any maximal ideal $I \subset \mathcal{O}_A$, the set $V(I)$ is empty, or contains precisely one point; in the second case, one has $I = I_a$. Therefore, **to prove the Nullstellensatz, one needs only to show that $V(I)$ is non-empty.**

Idea of a proof: The quotient $k := \mathcal{O}_A/I$ is countably-dimensional, but **there are no countably-dimensional fields over $\mathbb{C}$ except $\mathbb{C}$ itself.** In the later case, existence of common zeros is essentially a tautology.

Digression: dimension of the field of rational functions.

Lemma 1: Let $\mathbb{C}(t)$ be the field of rational functions (fraction field of the rings of polynomials). **Then $\mathbb{C}(t)$ is continuum-dimensional over $\mathbb{C}$.**

Proof: For any set $a_1, ..., a_k \in \mathbb{C}$ of pairwise distinct points, **the rational functions $\left\{\frac{1}{t-a_i}\right\} \in \mathbb{C}(t)$ are linearly independent over $\mathbb{C}$.** Indeed, if $\sum_{i=1}^k \frac{\lambda_i}{t-a_i} = 0$, one has

$$\frac{\sum_{i=1}^k \lambda_i (t-a_1)(t-a_2)\dots\widehat{(t-a_i)}\dots(t-a_n)}{(\prod_{i=1}^k (t-a_i))} = 0.$$

(we denote by $\widehat{(t-a_i)}$ a multiplier which is omitted), and this gives

$$P(t) := \sum_{i=1}^k \lambda_i (t-a_1)(t-a_2)\dots\widehat{(t-a_i)}\dots(t-a_n) = 0.$$

However, $P(a_1) = \lambda_1(a_1-a_2)(a_1-a_3)\dots(a_1-a_n) \neq 0$, hence $P(t) \neq 0$.

This implies that $\mathbb{C}(t)$ contains a continuous, linearly independent family of rational functions, and its dimension is at least continuum. It is at most continuum, because cardinality of $\mathbb{C}(t)$ is continuum **(prove it).** ■

Hilbert's Nullstellensatz (2)

THEOREM: (Hilbert's Nullstellensatz)
Let $A \subset \mathbb{C}^n$ be an affine variety, and $\mathcal{O}_A$ the ring of polynomial functions on A. **Then every maximal ideal in A is an ideal of a point $a \in A$: $I = I_a$.**

(Step 1:) Need only to show that the set of common zeros of I is non-empty.

Step 2: The quotient $k := \mathcal{O}_A/I$ is a field, because I is maximal. Also, it contains $\mathbb{C}$ (the field of constant functions). Since $\mathbb{C}$ is algebraically closed, **any element $t \in k \backslash \mathbb{C}$ is transcendental over $\mathbb{C}$.** This means that $\mathbb{C} = k$ or $k \subset \mathbb{C}(t)$, where $\mathbb{C}(t)$ denotes the field of rational functions.

Step 3: Since $\mathcal{O}_A$ is generated by coordinate monomials, **$\mathcal{O}_A$ is countably-dimensional over $\mathbb{C}$.** Clearly, the same is true for $k = \mathcal{O}_A/I$.

Step 4: By Lemma 1, k cannot contain the field of rational functions. Therefore, $k = \mathbb{C}$.

Hilbert's Nullstellensatz (2)

THEOREM: (Hilbert's Nullstellensatz)
Let $A \subset \mathbb{C}^n$ be an affine variety, and $\mathcal{O}_A$ the ring of polynomial functions on A. **Then every maximal ideal in A is an ideal of a point $a \in A$: $I = I_a$.**

(Step 1:) Need only to show that the set of common zeros of I is non-empty.

(Step 2-4:) We have shown that $k = \mathcal{O}_A/I = \mathbb{C}$.

Step 5: It remains to produce a point $a = (a_1, ..., a_n) \in A$ such that $a \in V(I)$. Consider the homomorphism $\varphi: \mathcal{O}_A \longrightarrow \mathcal{O}_A/I = \mathbb{C}$ constructed above, and let $a_1 = \varphi(z_1), ..., a_n = \varphi(z_n)$, where z_i are coordinate functions. For any polynomial $P(z_1, ..., z_n) \in I$, one has

$$0 = \varphi(P) = P(\varphi(z_1), \varphi(z_2), ..., \varphi(z_n)) = P(a).$$

Therefore, **all functions $P \in I$ satisfy $P(a) = 0$.** ■