Commutative algebra

lecture 1: Hilbert's Nullstellensatz

Misha Verbitsky

IMPA, sala 232

January 2, 2022, 15:00

Commutative algebra

Commutative algebra deals with **commutative rings** (or **commutative algebras** over a field), **ideals**, and **modules** over commutative rings.

It is used mostly to advance **algebraic geometry**, but it is also used in **number theory**, **complex analysis** and **homological algebra**.

Preliminaries: I assume knowledge of **groups**, **rings**, **fields**, **vector spaces**, and basic set theory (surjective, injective, bijective maps, cardinals, equivalence classes). For today's lecture (and only for it) we use the more advanced set theory, such as the Zorn lemma.

Further on, **all rings are assumed to be commutative and with unity**.

The Plan for today's lecture.

1. Algebraic sets.

2. Ideals; existence of maximal ideals.

3. Hilbert's Nullstellensatz.

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

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 choosing $\mathbb{C}$ 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 given 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 $\varphi_1, ..., \varphi_n : \mathbb{C}^m \longrightarrow \mathbb{C}$.

Affine varieties

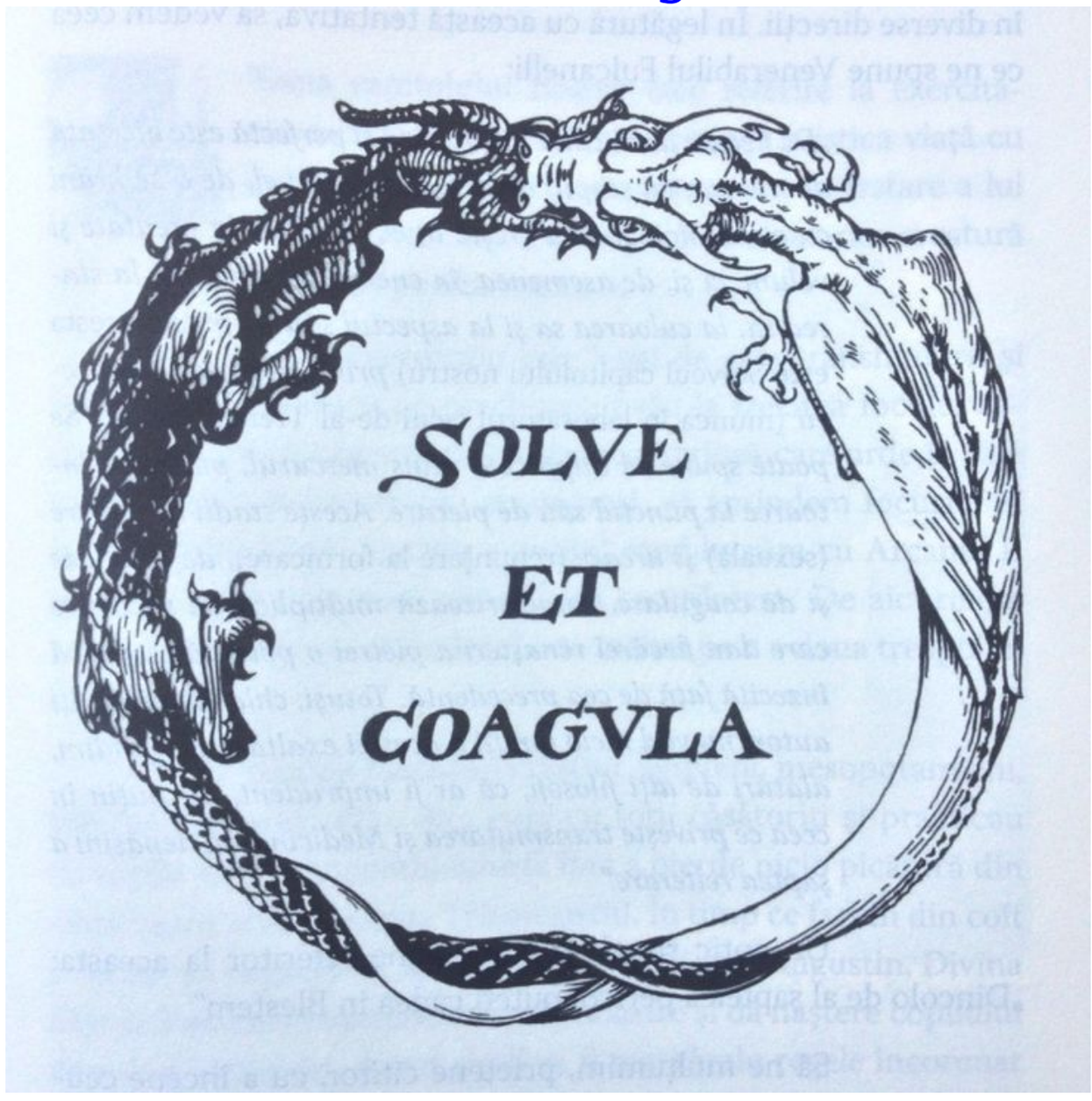
DEFINITION: Algebraic function on an algebraic set $Z \subset \mathbb{C}^n$ is a restriction of a polynomial function to Z. An algebraic set with a ring of algebraic functions on it is called **an affine variety**.

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**.

This allows one *to solve problems of geometry algebraically, and to solve the problems of algebra using the geometric intuition.*

Solve et coagula



Geometry and 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.**

Zorn lemma

DEFINITION: Partial order is a relation $x \prec y$, which is **transitive** (if $x \prec y$ and $y \prec z$ then $x \prec z$) and **non-reflexive** ($z \prec z$ does not hold for any z). A set with partial order is called **partially ordered set**, or **poset**.

DEFINITION: Let $(S, \prec)$ be a poset. An element $x \in S$ is called **maximal** if there is no $y \in S$ such that $x \prec y$. For a subset $S_1 \subset S$ and $x \in S$, we write $S_1 \prec x$ if $\xi \prec x$ for all $\xi \in S_1$.

DEFINITION: A partial order on S is called **linear order**, or **total order** if for all $x \neq y$ either $x \prec y$ or $y \prec x$.

Zorn lemma: Let $(S, \prec)$ be a poset such that for any linearly ordered subset $S_1 \subset S$ there exists $x \in S_1$ such that $S_1 \backslash \{x\} \prec x$. **Then S has a maximal element**.

Existence of a basis

DEFINITION: Let V be a vector space over a field k. A subset $S \subset V$ is **linearly independent** if for any linear combination $\sum_{i=1}^n a_i s_i$ where s_i are distinct elements of S, and $a_i \in k$, $\sum_{i=1}^n a_i s_i = 0$ implies that all $a_i = 0$. A linearly independent subset **is a basis** in V if any $v \in V$ can be represented as a linear combination $v = \sum_{i=1}^n a_i s_i$.

EXERCISE: Prove that a linearly independent subset S is a basis **if and only if it is maximal,** that is, for any linearly independent $S' \supset S$, one has $S = S'$.

CLAIM: Every vector space V has a basis.

Proof: Let $\mathfrak{S}$ be the set of all linearly independent subsets of V, ordered by inclusion. A union of an increasing chain of linearly independent subsets is linearly independent **(prove it).** Therefore, Zorn lemma can be applied to $\mathfrak{S}$, yielding a maximal linearly independent subset S, that is, a basis. ■

EXERCISE: Let S, S' be two basises for a vector space V. **Prove that S and S' have the same cardinality,** that is, there exists a bijective map $S \longrightarrow S'$.

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

Existence of maximal ideals

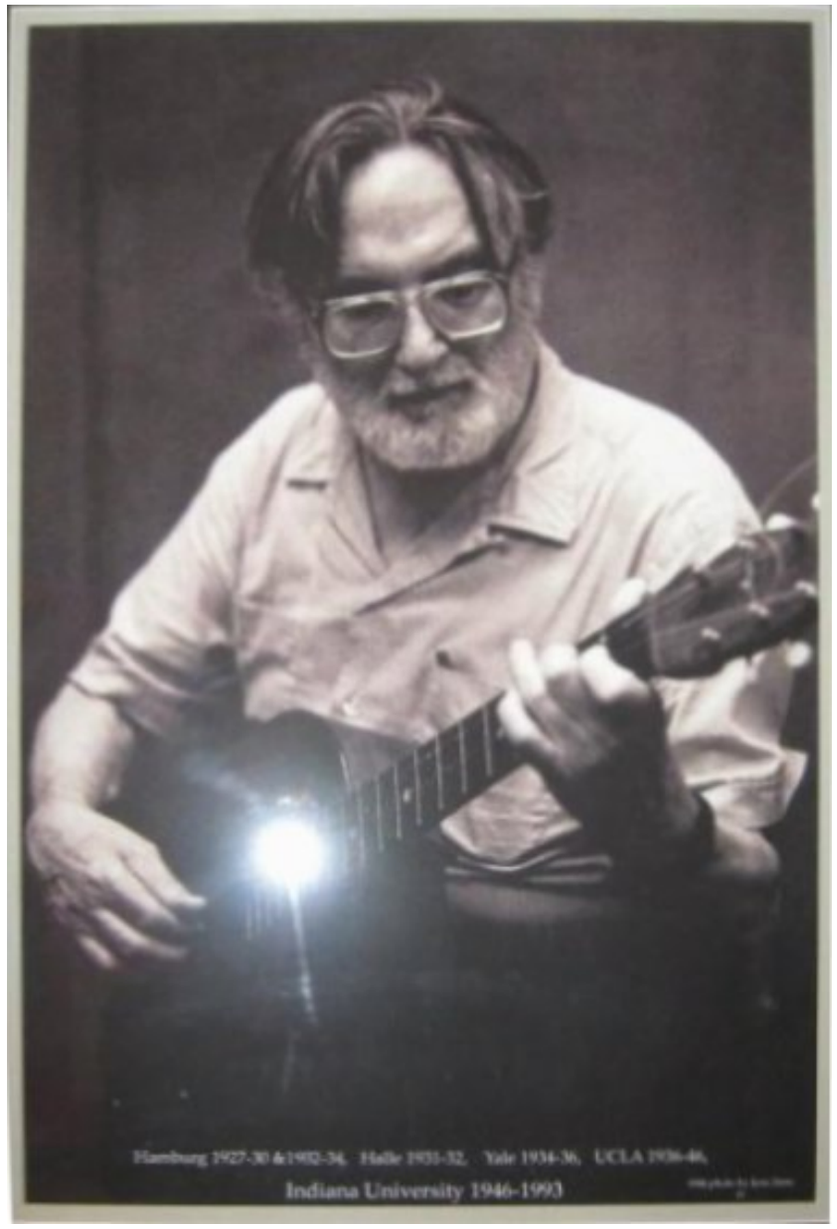
THEOREM: Let $I \subset R$ be an ideal in a ring. **Then I is contained in a maximal ideal.**

Proof: A union of an increasing chain of ideals is an ideal **(prove it).** Therefore, we can apply Zorn lemma to the set of all ideals, partially ordered by inclusion, and obtain a maximal ideal. ■

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** $a \in A$.



Max August Zorn (1906 - 1993)

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:

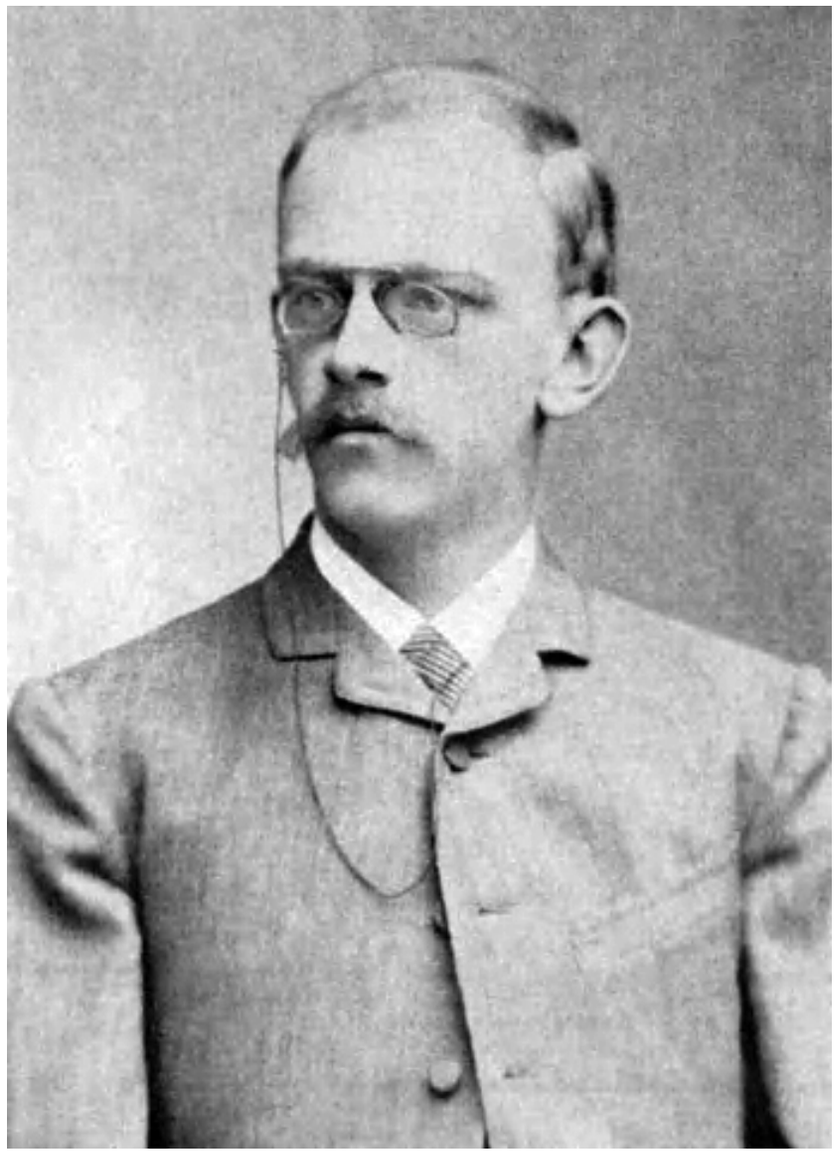
$$V(I) := \{a \in A \ \mid \ \forall f \in I, f(a) = 0\}.$$

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 for any ideal $I \in \mathcal{O}_A$.**

David Hilbert, Ueber die vollen Invariantensysteme, Mathematische Annalen, Band 42, 1893, S. 313-337

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.

David Hilbert (1862-1943)



Hilbert in 1886

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 linearly independent family of rational functions $\{\frac{1}{t-a}\}$, parametrized by $a \in \mathbb{C}$. Clearly, **its dimension is at least continual.** It is at most continual, because cardinality of $\mathbb{C}(t)$ is continuum. ■

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 $P(a) = 0$.** ■