Geometria Algébrica I

lecture 2: Hilbert's Nullstellensatz and categories

Misha Verbitsky

IMPA, sala 232

August 17, 2018

Field extensions

DEFINITION: Let $k \subset K$ be a field contained in a field. In this case, we say that k is **a subfield** of K, and K is **extension** of k. An element $x \in K$ is called **algebraic** over K if x is a root of a non-zero polynomial with coefficients in k. An element which is not algebraic is called **transcendental**.

CLAIM: Let $k \subset K$ be a subfield. An element $x \in K$ is algebraic over k **if and only if the subring $k[x] \subset K$ generated by x is finite-dimensional over k.**

Proof: If $P(x) = 0$, one has $x^n = \sum_{i=0}^{n-1} a_i x^i$, $a_i \in k$, hence all x^N for $N \geqslant n$ are linear combinations of $1, x, ..., x^{n-1}$. Conversely, if $k[x] \subset K$ is finite-dimensional, there is a linear relation $\sum_{i=0}^{n} a_i x^i$, , $a_i \in k$, giving a polynomial. ■

EXERCISE: Prove that **the sum and the product of algebraic elements in $K \subset k$ are algebraic.**

DEFINITION: A field extension $K \supset k$ is called **algebraic** if all elements of K are algebraic over k. A field k is called **algebraically closed** if all algebraic extensions of k are trivial.

Finite-dimensional algebras without zero divisors

CLAIM: Let $k \subset K$ be a subfield, and $x \in K$ an algebraic element. **Then the subring $k[x] \subset K$ generated by x is a subfield.**

Proof: We need to prove that any non-zero $y \in k[x]$ is invertible, that is, there exists $z \in k[x]$ such that $zy = 1$. However, the operator $L_y : k[x] \longrightarrow k[x]$ has no kernel because K has no zero divisors. **A linear endomorphism of a finite-dimensional space is surjective if it has no kernel.** Therefore, there exists $z \in k[x]$ such that $L_y(z) = 1$. ■

REMARK: The same argument proves the following assertion. Let $A \supset k$ be a commutative, finite-dimensional algebra over k. Suppose that A has no zero divisors. **Then A is a field.**

Algebraically closed fields

CLAIM: A field k **is algebraically closed if and only if any if any polynomial $P(t) \in k[t]$ of positive degree has a root in k.**

Proof. Step1: Suppose, from absurd, that k is algebraically closed, and $P(t)$ a polynomial with no roots in k. Decomposing $P(t)$ onto multipliers if necessary, we may assume that $P(t)$ is irreducible. Then the ideal $(P) \subset k[t]$ is prime, and the algebra $k[t]/(P)$ has no zero divisors. As we have shown, a finite-dimensional commutative algebra over k without zero divisors is a field. Then $k[t]/(P)$ is a finite-dimensional extension of k, which is impossible, because $\dim_k k[t]/(P) = \deg P$.

Step 2: Suppose, conversely, that any polynomial $P(t) \in k[t]$ of positive degree has a root in k. Then any k-algebra of form $k[t]/(P)$ has zero divisors. However, any algebraic elements generates an algebra of such form. Therefore, for any field extension $K \supset k$, an any algebraic element $x \in K$, we have $x \in k$. ■

Complex numbers are algebraicaly closed

COROLLARY: The field $\mathbb{C}$ of complex numbers is algebraically closed.

COROLLARY: Any non-trivial field extension of $\mathbb{C}$ contains a transcendental element t.

REMARK: Suppose $K \supsetneq \mathbb{C}$ is a field extension, and $t \in K$ a transcendental element. Then K contains fractions of all polynomials $P(t)$, hence **it contains the field $k(t)$ of rational functions.**

Basis for an infinite-dimensional space

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.

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 continual, linearly independent family of rational functions, and its dimension is at least continuum. ■

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 $a \in A$: $I = I_a$.**

Step 1: 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 2: 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 3: By Lemma 1, k cannot contain the field of rational functions. Therefore, $k = \mathbb{C}$.

Step 4: 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 $P(a) = 0$.** ■

Categories

DEFINITION: A category $\mathcal{C}$ is a collection of data called "objects" and "morphisms between objects" which satisfies the axioms below.

DATA.

Objects: A class $\mathcal{O}b(\mathcal{C})$ of **objects** of $\mathcal{C}$.

Morphisms: For each $X, Y \in \mathcal{O}b(\mathcal{C})$, one has a set $\mathcal{M}or(X,Y)$ of **morphisms from** X **to** Y.

Composition of morphisms: For each $\varphi \in \mathcal{M}or(X,Y), \psi \in \mathcal{M}or(Y,Z)$ there exists **the composition** $\varphi \circ \psi \in \mathcal{M}or(X,Z)$

Identity morphism: For each $A \in \mathcal{O}b(\mathcal{C})$ there exists a morphism $\mathrm{Id}_A \in \mathcal{M}or(A,A)$.

AXIOMS.

Associativity of composition: $\varphi_1 \circ (\varphi_2 \circ \varphi_3) = (\varphi_1 \circ \varphi_2) \circ \varphi_3$.

Properties of identity morphism: For each $\varphi \in \mathcal{M}or(X,Y)$, one has $\mathrm{Id}_x \circ \varphi = \varphi = \varphi \circ \mathrm{Id}_Y$

Categories (2)

DEFINITION: Let $X, Y \in \mathcal{O}b(\mathcal{C})$ – objects of $\mathcal{C}$. A morphism $\varphi \in \mathcal{M}or(X,Y)$ is called **an isomorphism** if there exists $\psi \in \mathcal{M}or(Y,X)$ such that $\varphi \circ \psi = \mathrm{Id}_X$ and $\psi \circ \varphi = \mathrm{Id}_Y$. In this case, the objects X and Y are called **isomorphic**.

Examples of categories:
Category of sets: its morphisms are arbitrary maps.
Category of vector spaces: its morphisms are linear maps.
Categories of rings, groups, fields: morphisms are homomorphisms.
Category of topological spaces: morphisms are continuous maps.
Category of smooth manifolds: morphisms are smooth maps.

Functors

DEFINITION: Let $\mathcal{C}_1, \mathcal{C}_2$ be two categories. A **covariant functor** from $\mathcal{C}_1$ to $\mathcal{C}_2$ is the following set of data.

1. **A map** $F: \mathcal{O}b(\mathcal{C}_1) \longrightarrow \mathcal{O}b(\mathcal{C}_2)$.

2. **A map** $F: \mathcal{M}or(X,Y) \longrightarrow \mathcal{M}or(F(X),F(Y))$ **defined for any pair of objects** $X, Y \in \mathcal{O}b(\mathcal{C}_1)$.

These data define a functor if they are **compatible with compositions,** that is, satisfy $F(\varphi) \circ F(\psi) = F(\varphi \circ \psi)$ for any $\varphi \in \mathcal{M}or(X,Y)$ and $\psi \in \mathcal{M}or(Y,Z)$, and **map identity morphism to identity** morphism.

Small categories

REMARK: This way, one could speak of **category of all categories**, with categories as objects and functors as morphisms.

A caution To avoid set-theoretic complications, Grothendieck added another axiom to set theory, "universum axiom", postulating existence of "universum", a very big set, and worked with "small categories" – categories where the set of all objects and sets of morphisms belong to the universum. In this sense, "category of all categories" is not a "small category", because the set of its object (being comparable to the set of all subsets of the universum) is too big to fit in the universum.

In practice, mathematicians say "category" when they mean "small category", tacitly assuming that any given category is "small". This is why not many people call "category of all categories" a category: nobody wants to deal with set-theoretic complications.

Example of functors

A "natural operation" on mathematical objects is usually a functor.
Examples:

1. A map $X \longrightarrow 2^X$ from the set X to the set of all subsets of X is a functor from the category $\mathcal{S}ets$ of sets to itself.

2. A map $M \longrightarrow M^2$ mapping a topological space to its product with itself is a functor on topological spaces.

3. A map $V \longrightarrow V \oplus V$ is a functor on vector spaces; same for a map $V \longrightarrow V \otimes V$ or $V \longrightarrow (V \oplus V) \otimes V$.

4. **Identity functor** from any category to itself.

5. A map from topological spaces to $\mathcal{S}ets$, putting a topological space to the set of its connected components.

EXERCISE: Prove that it is a functor.

Contravariant functors

DEFINITION: Let $\mathcal{C}$ be a category. Define the **opposite category** $\mathcal{C}^{op}$ with the same set of objects, and $\mathcal{M}or_{\mathcal{C}^{op}}(A,B) = \mathcal{M}or_{\mathcal{C}}(B,A)$. The composition $\varphi \circ \psi$ in $\mathcal{C}$ gives the composition $\psi^{op} \circ \varphi^{op}$ in $\mathcal{C}^{op}$.

DEFINITION: A **contravariant functor** from $\mathcal{C}_1$ to $\mathcal{C}_2$ is the usual ("covariant") functor from $\mathcal{C}_1$ to $\mathcal{C}_2^{op}$.

EXAMPLE: A map from the category of topological spaces to category of rings mapping a space to a ring of continuous functions on it gives a contravariant functor.

EXAMPLE: Let $X \in \mathcal{O}b(\mathcal{C})$ be an object of $\mathcal{C}$. A map $Y \longrightarrow \mathcal{M}or(X,Y)$ defines a covariant functor from $\mathcal{C}$ to the category $\mathcal{S}ets$ of sets. A map $Y \longrightarrow \mathcal{M}or(Y,X)$ defines a contravariant functor from $\mathcal{C}$ to $\mathcal{S}ets$. Such functors to $\mathcal{S}ets$ are called **representable**.

Equivalence of functors

DEFINITION: Let $X, Y \in \mathcal{O}b(\mathcal{C})$ be objects of a category $\mathcal{C}$. A mprphism $\varphi \in \mathcal{M}or(X,Y)$ is called **an isomorphism** if there exists $\psi \in \mathcal{M}or(Y,X)$ such that $\varphi \circ \psi = \mathrm{Id}_X$ and $\psi \circ \varphi = \mathrm{Id}_Y$. In this case X and Y are called **isomorphic**.

DEFINITION: Two functors $F, G: \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ are called **equivalent** if for any $X \in \mathcal{O}b(\mathcal{C}_1)$ we are given an isomorphism $\Psi_X: F(X) \longrightarrow G(X)$, in such a way that for any $\varphi \in \mathcal{M}or(X,Y)$, one has $F(\varphi) \circ \Psi_Y = \Psi_X \circ G(\varphi)$.

REMARK: Such commutation relations are usually expressed by **commutative diagrams**. For example, the condition $F(\varphi) \circ \Psi_Y = \Psi_X \circ G(\varphi)$ is expressed by a commutative diagram

$$\begin{array}{ccc} F(X) & \xrightarrow{F(\varphi)} & F(Y) \\ {\scriptstyle \Psi_X}\downarrow & & \downarrow{\scriptstyle \Psi_Y} \\ G(X) & \xrightarrow{G(\varphi)} & G(Y) \end{array}$$

Equivalence of categories

DEFINITION: A functor $F: \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ is called **equivalence of categories** if there exists a functor $G: \mathcal{C}_2 \longrightarrow \mathcal{C}_1$ such that the compositions $G \circ F$ and $G \circ F$ are equivaleent to the identity functors $\mathrm{Id}_{\mathcal{C}_1}$, $\mathrm{Id}_{\mathcal{C}_2}$.

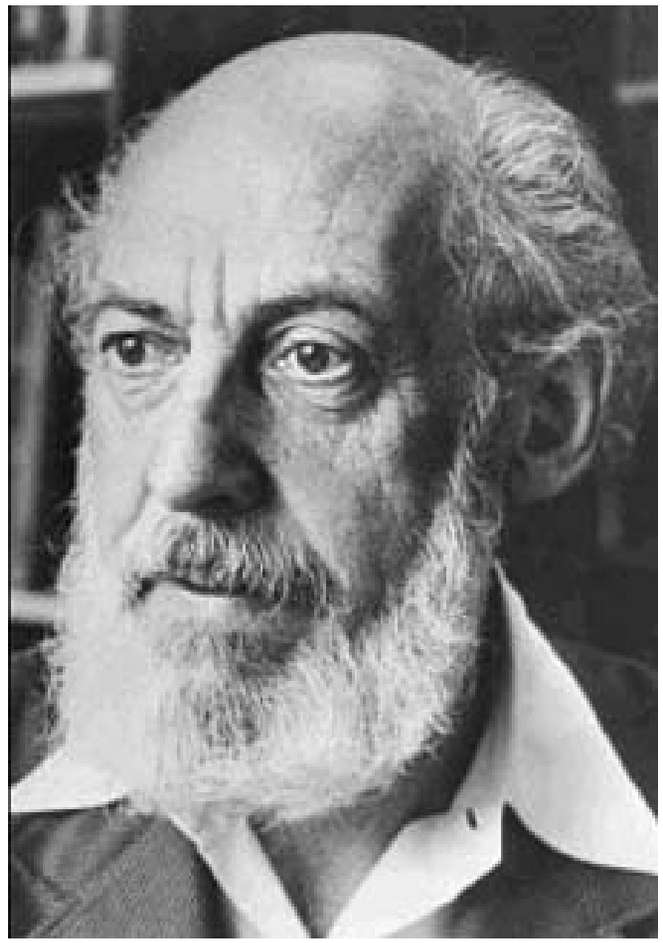
REMARK: It is possible to show that this is equivalent to the following conditions: F **defines a bijection on the set of isomorphism classes of objects of** $\mathcal{C}_1$ **and** $\mathcal{C}_2$**, and a bijection**

$$\mathcal{M}or(X,Y) \longrightarrow \mathcal{M}or(F(X),F(Y)).$$

for each $X, Y \in \mathcal{O}b(\mathcal{C}_1)$.

REMARK: From the point of view of category theory, **equivalent categories are two instances of the same category** (even if the cardinality of corresponding sets of objects is different).

Saunders Mac Lane
(1909-2005)



Samuel Eilenberg
(1913-1998)

Alexander Grothendieck
(28.03.1928 - 13.11.2014)

Category of affine varieties and category of 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: Next lecture.