Commutative algebra

lecture 2: Strong Nullstellensatz and eqiuvalence of categories

Misha Verbitsky

IMPA, sala 236
March 20, 2026, 17:00

http://verbit.ru/IMPA/CA-2026/

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 $\operatorname{Id}_A \in \mathcal{M}or(A,A)$.

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 $\operatorname{Id}_x \circ \varphi = \varphi = \varphi \circ \operatorname{Id}_Y$

Categories (2)

DEFINITION: Let $X, Y \in \mathcal{Ob}(\mathcal{C})$ be objects of $\mathcal{C}$. A morphism $\varphi \in \mathcal{Mor}(X,Y)$ is called **an isomorphism** if there exists $\psi \in \mathcal{Mor}(Y,X)$ such that $\varphi \circ \psi = \operatorname{Id}_X$ and $\psi \circ \varphi = \operatorname{Id}_Y$. 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.

However, a category of categories where all objects are indexed by a set which belongs to the universum is a "small category" and can be considered set-theoretically.

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 morphism $\varphi \in \mathcal{M}or(X,Y)$ is called **an isomorphism** if there exists $\psi \in \mathcal{M}or(Y,X)$ such that $\varphi \circ \psi = \operatorname{Id}_X$ and $\psi \circ \varphi = \operatorname{Id}_Y$. 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 $\operatorname{Id}_{\mathcal{C}_1}$, $\operatorname{Id}_{\mathcal{C}_2}$.

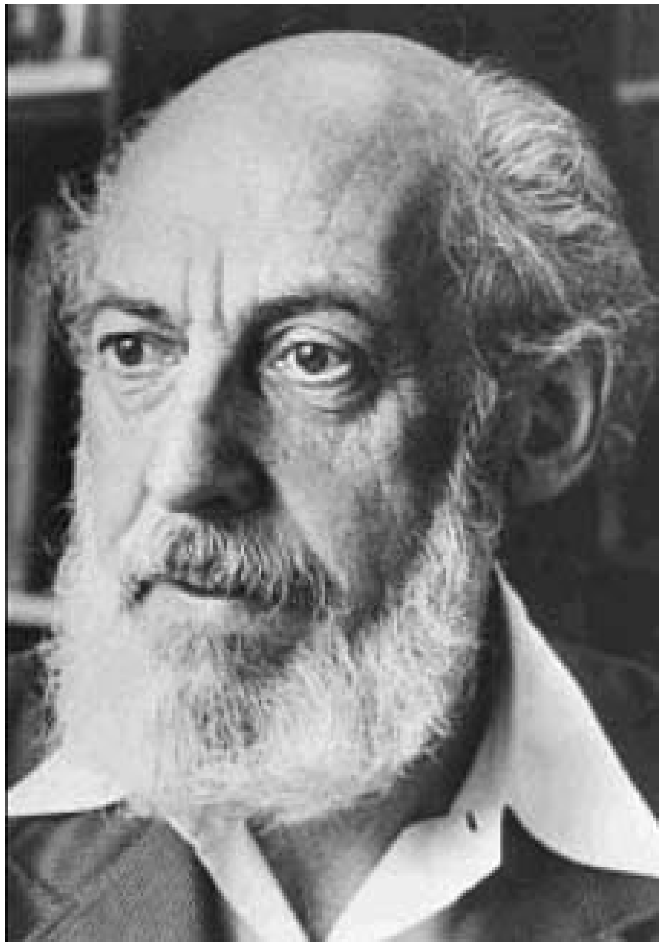
REMARK: It is possible to show that this is equivalent to the following conditions: F **defines a bijection on the set of isomorphism classes of objects of $\mathcal{C}_1$ and $\mathcal{C}_2$, and a bijection**

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

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 Aff – category of affine varieties. Consider the functor $\Phi:$ Aff $\longrightarrow \mathcal{C}_R^{op}$ mapping an algebraic variety X to the ring of polynomial functions on X. **Then Φ is an equivalence of categories.**

Proof: Later today

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

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

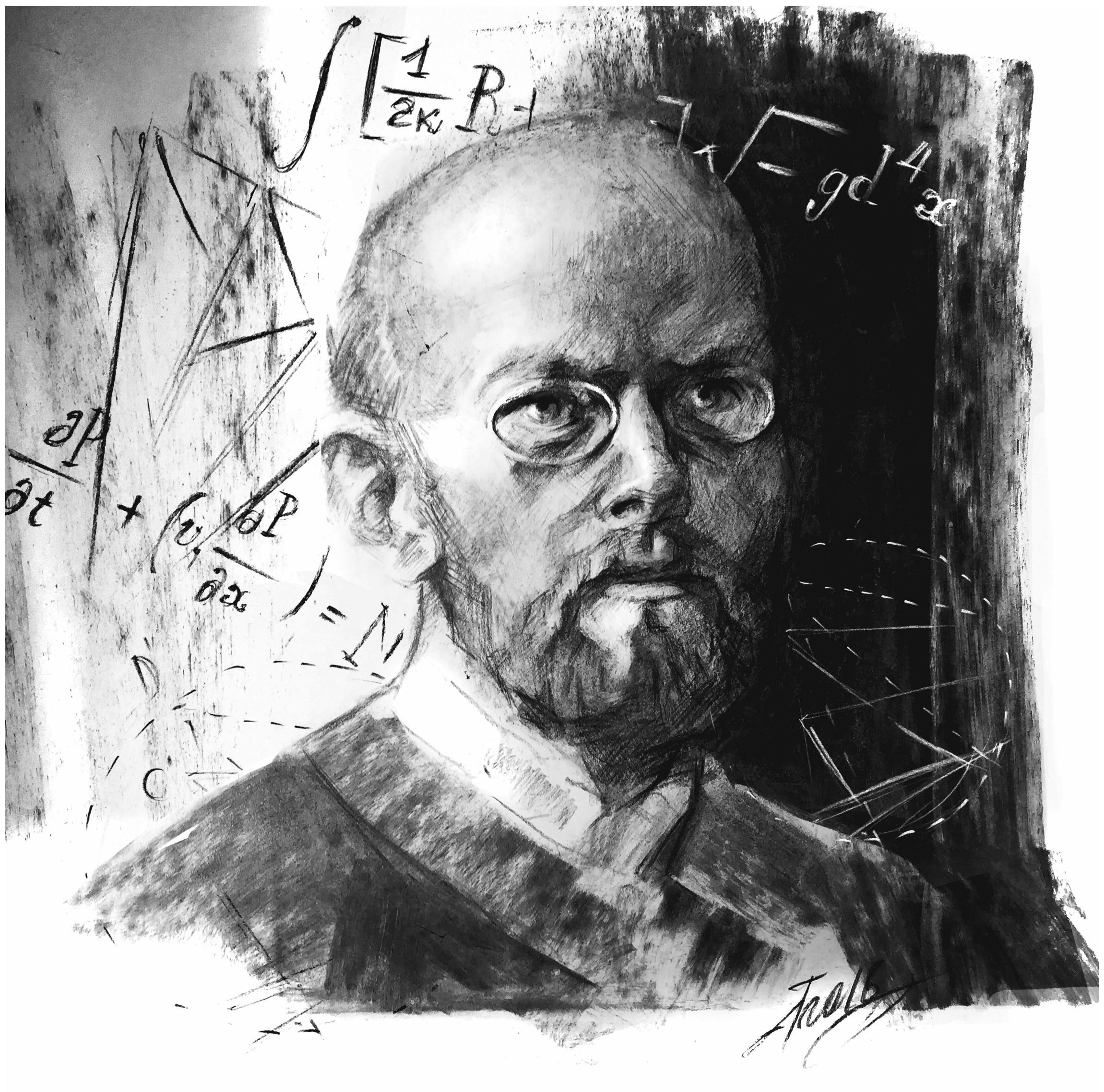
For $Z \subset \mathbb{C}^n$ an algebraic subset, denote by $\operatorname{Ann}(A)$ the set of all polynomials $P(t_1, ..., t_n)$ vanishing in Z.

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 ideal I; "Strong Nullstellensatz" claims that I is uniquely determined by $V(I)$ when R/I has no nilpotents.

David Hilbert (1862-1943)



David Hilbert (Anna Gorban, 2018)

Strong Nullstellensatz (2)

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 $\Psi : \mathcal{C}_R^{op} \longrightarrow \mathrm{Aff}$. Since any finitely-generated ring R is obtained as $R = \mathbb{C}[t_1, ..., t_n]/I$, we define Ψ as $\Psi(R) := V(I)$; the functor $\Phi :$ Aff $\longrightarrow \mathcal{C}_R^{op}$ 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 the 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 (denoted $R(F)$ or $R[F^{-1}]$) of a ring R with respect to an element $F \in R$ is the 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 **("dyadic rational numbers").**
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**.**

DEFINITION: $a \in R$ is called **nilpotent** if $a^n = 0$ for some $n > 0$.

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** $1 = (1 - Ft)P$ **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 $\mathfrak{p} \in \operatorname{Spec} R_1$.

REMARK: The kernel of the natural map $R \longrightarrow R[f^{-1}]$ **is the set of all $a \in G$ such that $f^k a = 0$ for some k.**

PROPOSITION: The morphism $R \longrightarrow R[f^{-1}]$ **gives an injective map of spectra $\operatorname{Spec} R[f^{-1}] \hookrightarrow \operatorname{Spec} R$.**
Proof: Suppose that $\mathfrak{p}_f$, $\mathfrak{q}_f \in \operatorname{Spec} R[f^{-1}]$, 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 and $F \notin \mathfrak{q}$, 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. ■

Rabinowitsch 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 Ann(Z) **("annihilator").**

Theorem 2: 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 surjective map $\zeta: \mathbb{C}[t_1, ..., t_{n+1}] \longrightarrow R[f^{-1}]$ taking $t_1, ..., t_n$ to their images in R 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 $I =$ Ann(V_I)).**

Proof: If $a \in$ Ann(V_I)), then $a^n \in I$ by Theorem 2. ■

Zum Hilbertschen Nullstellensatz

The first time Hilbert Nullstellensatz was called by this name.

Zum Hilbertschen Nullstellensatz.

Von

J. L. Rabinowitsch in Moskau.

Satz. *Verschwindet das Polynom* $f(x_1, x_2, \ldots, x_n)$ *in allen Nullstellen — im algebraisch abgeschlossenen Körper — eines Polynomideals* $\mathfrak{a}$, *so gibt es eine Potenz* f^ϱ *von* f, *die zu* $\mathfrak{a}$ *gehört.*

Beweis. Es sei $\mathfrak{a} = (f_1, f_2, \ldots, f_r)$, wo f_i die Variablen $x_1, \ldots, x_n$ enthalten. x_0 sei eine Hilfsvariable. Wir bilden das Ideal $\bar{\mathfrak{a}} = (f_1, f_2, \ldots, f_r, x_0 f - 1)$. Da der Voraussetzung nach $f = 0$ ist, sobald alle f_i verschwinden, so hat das Ideal $\bar{\mathfrak{a}}$ keine Nullstellen.

Folglich muß $\bar{\mathfrak{a}}$ mit dem Einheitsideal zusammenfallen. (Vgl. etwa bei K. Hentzelt, „Eigentliche Eliminationstheorie", § 6, Math. Annalen 88[1].) Ist also $1 = \sum_{i=1}^{i=r} F_i(x_0, x_1, \ldots, x_n) f_i + F_0 \cdot (x_0 f - 1)$ und setzen wir in dieser Identität $x_0 = \frac{1}{f}$, so ergibt sich:

$$1 = \sum_{i=1}^{i=r} F_i\left(\frac{1}{f}, x_1, \ldots, x_n\right) f_i = \frac{\sum_{i=1}^{i=r} \bar{F}_i f_i}{f^\varrho}.$$

Folglich ist $f^\varrho = 0\,(\mathfrak{a})$, w. z. b. w.

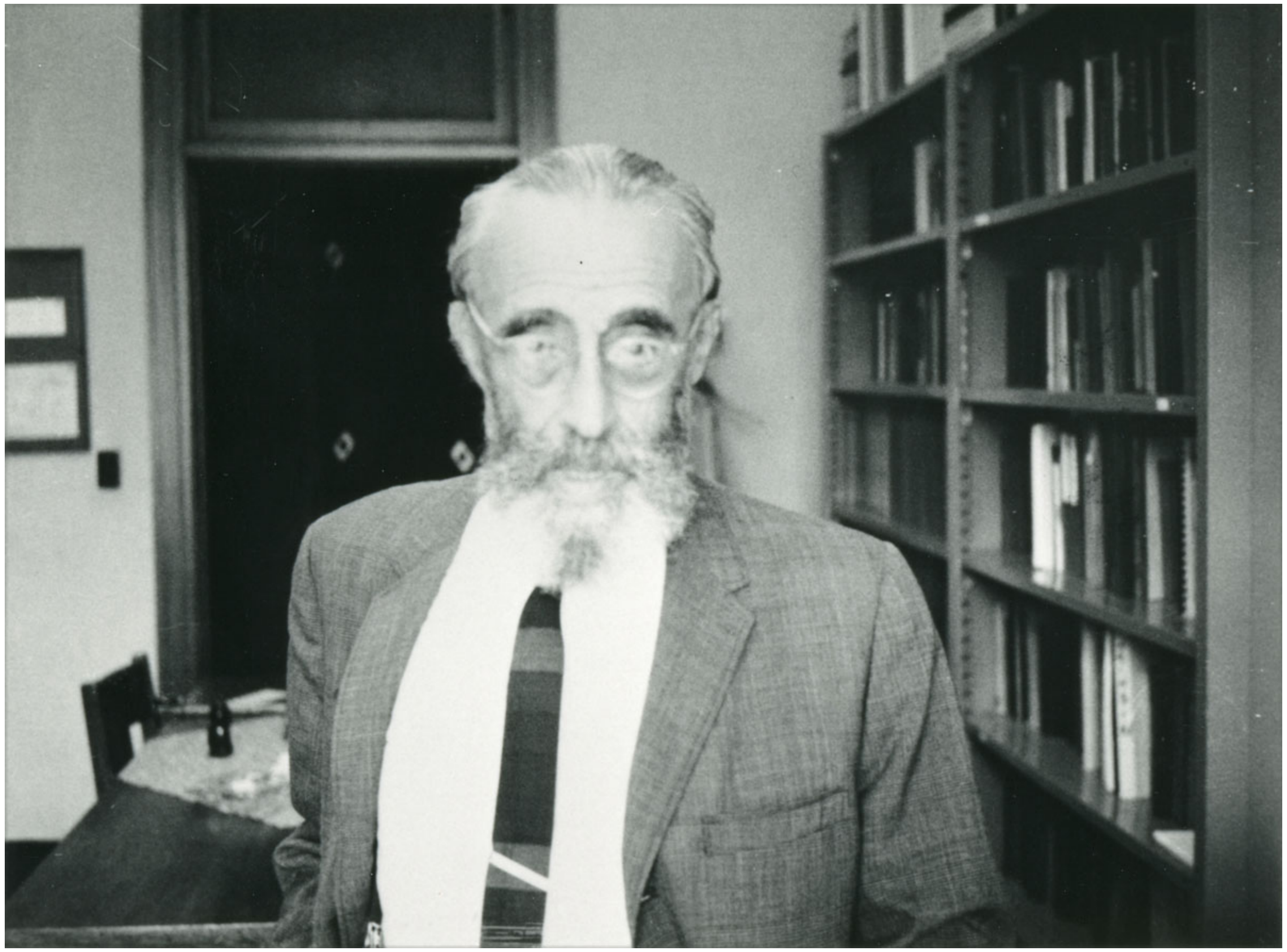
[1]) Folgt auch schon aus der Kroneckerschen Eliminationstheorie.

(Eingegangen am 8. 5. 1929.)

J. L. Rabinowitsch, *Zum Hilbertschen Nullstellensatz,* Mathematische Annalen (1930), 102, p. 520-520

George Rainich

George Yuri Rainich (Rabinovich), 1886-1968.



Photograph by Paul R. Halmosh, 1964, Ann Arbor.

Since 2022, *it is no longer accepted that J. L. Rabinowitsch is George Yuri Rainich.*

Hilbert Nullstellensatz as equivalence of categories

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

Proof: Let $R = \mathbb{C}[t_1, ..., t_n]/I$. The functor $\Psi: \mathcal{C}_R^{op} \longrightarrow \text{Aff}$ takes R to V_I (the zero set of I). Then $\Psi \circ \Phi$ takes R to the ring of polynomial functions on V_I, which is equal to $\frac{\mathbb{C}[t_1,...,t_n]}{\text{Ann}(V_I)}$. Since $\text{Ann}(V_I) = I$, this functor takes R to itself.

For another direction, $\Phi \circ \Psi$ takes an algebraic set A to the common zeros of the ideal $\text{Ann}(A)$, which is the same as A, because $A = V_{\text{Ann}(A)}$, by definition of an algebraic set. ■