The Nullstellensatz for algebraic structures I

Vladimir Remeslennikov

Omsk Division of the Sobolev Institute of Mathematics of the SB RAS

October, Montreal

Let G be an algebraic system (e.g. group, ring, etc)

Motto

Systematic study of a structure G in first-order language $=$ systematic study of all H which are universally equivalent to G (limit structures over G).

There are two main obstacles to achieve this goal.

- Does there exist a good procedure to compute the radical for systems of equations over G (Nullstellensatz)?
- Can one prove projection theorems for definable sets over G?

Formal definition of a projection theorem for subsets from $G^n = G \times \cdots \times G$ that possess property Φ:

If $M \subseteq G^n$ has property Φ, then $proj(M)$ also has property Φ.

Typical examples

1. $P = NP$?
2. Is the projection of an algebraic set again algebraic?

Structure of the talk

1. Algebraic sets

Let k be a field, $k[x]$ be the ring of polynomials in x and $S : x^3 = 0$ an equation over k.

$V(S) = \{0\}$ - the set of solutions of the system S = the algebraic set defined by S.

2. Ring of functions on $V(S)$ (the coordinate ring)

Introduce a V-equivalence on $k[x]$:

$$f(x) \sim_V g(x) \leftrightarrow f(p) = g(p) \text{ for all } p \in V(S).$$

Set

$$\mathrm{Rad}(S) = f(x) \in k[x] \mid f(x) \sim_V 0,\ I = \mathrm{id}\langle S \rangle = \mathrm{id}\langle x^3 \rangle.$$

We have $I \subseteq \mathrm{Rad}(S)$ and $\mathrm{Rad}(S)$ is an ideal. Then

$$\Gamma(S) \simeq k[x]/\mathrm{Rad}(S)$$

is the coordinate ring (k-algebra) of S.

Structure of the talk

3. Nullstellensatz

Any procedure that allows for a transition from I to $\mathrm{Rad}(S)$ or any theorem which describes $\mathrm{Rad}(S)$ will be called Nullstellensatz

Why?

Hilbert's Nullstellensatz [1893]

Let $S \subset \mathbb{C}[x_1, \ldots, x_n]$ be a system of equations and I the ideal of the ring $\mathbb{C}[x_1, \ldots, x_n]$ generated by the set S. Then

$$\mathrm{Rad}(S) = \sqrt{I} = \{f \in \mathbb{C}[x_1, \ldots, x_n] \mid \exists r \in \mathbb{N} \;\; f^r \in I\}.$$

$$\mathrm{Rad}(S) = \{f \in \mathbb{C}[x_1, \ldots, x_n] \mid$$
$$\forall\, (a_1, \ldots, a_n) \in \mathbb{C}^n \quad S(a_1, \ldots, a_n) = 0 \;\longrightarrow\; f(a_1, \ldots, a_n) = 0\}$$

Let $\mathcal{A} = \langle A \mid \mathtt{L} \rangle$ be an algebraic structure in a language $\mathtt{L}$.

Problem of the Nullstellensatz type

For a system of equations S over $\mathcal{A}$ find the radical $\mathrm{Rad}(S)$.

Algebraic geometry over algebraic structures


G. Baumslag, A. Myasnikov, V. Remeslennikov
Algebraic geometry over groups I: Algebraic sets and ideal theory
Journal of Algebra, **219**, 16–79, 1999.


A. Myasnikov, V. Remeslennikov
Algebraic geometry over groups II: Logical foundations
Journal of Algebra, **234**, 225–276, 2000.


B. I. Plotkin
Some notions of algebraic geometry in universal algebra
Algebra and Analysis, **9 (4)**, 224–248, 1997.


B. I. Plotkin
Algebras with the same (algebraic) geometry
Proc. Steklov Inst. Math., **242**, 165–196, 2003.


O. Kharlampovich, A. Myasnikov, 1998, 1998, 2005.

Universal algebraic geometry


E. Daniyarova, A. Myasnikov, V. Remeslennikov
Unification theorems in algebraic geometry
Algebra and Discrete Mathematics, **1**, 80–112, 2008,
arXiv:0808.2522v1 [math.AG].


E. Daniyarova, A. Myasnikov, V. Remeslennikov
Algebraic geometry over algebraic structures II: Foundations
arXiv:1002.3562v2 [math.AG].

Unification Theorem A

Let $\mathcal{A}$ be an equationally Noetherian algebra in a language $\mathtt{L}$ (with no predicates). Then for a finitely generated algebra $\mathcal{C}$ of $\mathtt{L}$ the following conditions are equivalent:

1. $\mathrm{Th}_\forall(\mathcal{A}) \subseteq \mathrm{Th}_\forall(\mathcal{C})$, i.e., $\mathcal{C} \in \mathbf{Ucl}(\mathcal{A})$;
2. $\mathrm{Th}_\exists(\mathcal{A}) \supseteq \mathrm{Th}_\exists(\mathcal{C})$;
3. $\mathcal{C}$ embeds into an ultrapower of $\mathcal{A}$;
4. $\mathcal{C}$ is discriminated by $\mathcal{A}$;
5. $\mathcal{C}$ is a limit algebra over $\mathcal{A}$;
6. $\mathcal{C}$ is an algebra defined by a complete atomic type in the theory $\mathrm{Th}_\forall(\mathcal{A})$ in $\mathtt{L}$;
7. $\mathcal{C}$ is the coordinate algebra of an irreducible algebraic set over $\mathcal{A}$ defined by a system of equations in the language $\mathtt{L}$.

Unification Theorem C

Let $\mathcal{A}$ be an equationally Noetherian algebra in a language $\mathtt{L}$ (with no predicates). Then for a finitely generated algebra $\mathcal{C}$ of $\mathtt{L}$ the following conditions are equivalent:

1. $\mathcal{C} \in \mathbf{Qvar}(\mathcal{A})$, i.e., $\mathrm{Th}_{\mathrm{qi}}(\mathcal{A}) \subseteq \mathrm{Th}_{\mathrm{qi}}(\mathcal{C})$;
2. $\mathcal{C} \in \mathbf{Pvar}(\mathcal{A})$;
3. $\mathcal{C}$ embeds into a direct power of $\mathcal{A}$;
4. $\mathcal{C}$ is separated by $\mathcal{A}$;
5. $\mathcal{C}$ is a subdirect product of finitely many limit algebras over $\mathcal{A}$;
6. $\mathcal{C}$ is an algebra defined by a complete atomic type in the theory $\mathrm{Th}_{\mathrm{qi}}(\mathcal{A})$ in $\mathtt{L}$;
7. $\mathcal{C}$ is the coordinate algebra of an algebraic set over $\mathcal{A}$ defined by a system of equations in the language $\mathtt{L}$.

The Nullstellensatz

for algebraically closed fields

Let k be an algebraically closed field.

Hilbert's Nullstellensatz [1893]

Let $S \subset k[x_1, \ldots, x_n]$ be a system of equations and I the ideal of the ring $k[x_1, \ldots, x_n]$ generated by the set S. Then

$$\mathrm{Rad}(S) = \sqrt{I} = \{f \in k[x_1, \ldots, x_n] \mid \exists r \in \mathbb{N} \;\; f^r \in I\}.$$

There exists one-to-one correspondence between algebraic sets in k^n and radical ideals of the ring $k[x_1, \ldots, x_n]$.

Inconsistent systems

Corollary 1 (inconsistent systems)

A system of equations $\{f_1 = 0, \ldots, f_m = 0\}$, $f_i \in k[x_1, \ldots, x_n]$, has no solutions in k if and only if there exist polynomials $h_1, \ldots, h_m \in k[x_1, \ldots, x_n]$ with

$$\sum_{i=1}^{m} h_i f_i = 1.$$

Corollary 2 (irreducible coordinate rings)

A k-algebra A is the coordinate ring of an irreducible algebraic set over k if and only if A is finitely generated (as a k-algebra) and has no zero-divisors.

Corollary 3 (coordinate rings)

A k-algebra A is the coordinate ring of an algebraic set over f k if and only if A is finitely generated (as a k-algebra) and has no non-zero nilpotent elements.

Let $\mathrm{L}_{\mathrm{ring}k} = \{+, -, \cdot, \alpha, \alpha \in k\}$ be the extended language of rings.

Corollary 4

Axioms for **Qvar**(k):

(I) axioms of commutative associative k-algebras with 1;

(II) $\forall x\ (x^n = 0 \longrightarrow x = 0)$, $n \in \mathbb{N}$.

Axioms for **Ucl**(k):

(III) $\forall x, y\ (xy = 0 \longrightarrow [x = 0 \vee y = 0])$.

Unification Theorem A

Let $\mathcal{A}$ be an equationally Noetherian algebra in a language $\mathtt{L}$ (with no predicates). Then for a finitely generated algebra $\mathcal{C}$ of $\mathtt{L}$ the following conditions are equivalent:

- $\mathcal{C} \in \mathbf{Ucl}(\mathcal{A})$;
- ...
- $\mathcal{C}$ is the coordinate algebra of an irreducible algebraic set over $\mathcal{A}$ defined by a system of equations in the language $\mathtt{L}$.

Unification Theorem C

- $\mathcal{C} \in \mathbf{Qvar}(\mathcal{A})$;
- ...
- $\mathcal{C}$ is the coordinate algebra of an algebraic set over $\mathcal{A}$ defined by a system of equations in the language $\mathtt{L}$.

Choice of a language

We use $\mathrm{L}_{\mathrm{ring}} = \{+, -, \cdot, 1\}$ to study systems of coefficient-free equations over k.

We use $\mathrm{L}_{\mathrm{ring}k} = \{+, -, \cdot, \alpha, \alpha \in k\}$ to study systems of equations with coefficients in k.

Universal formulas and quasi-identities

A universal formula is a formula of the type

$$\forall x_1 \ldots \forall x_n \quad \left(\bigwedge_{i=1}^{m} \bigvee_{j=1}^{s_i} f_{ij}(x_1, \ldots, x_n) \neq\!\!\!| \; 0 \right),$$

where $f_{ij} \in k[x_1, \ldots, x_n]$.

A quasi-identity is a universal formula of the type

$$\forall x_1 \ldots \forall x_n \quad \left(\bigwedge_{i=1}^{m} f_i(x_1, \ldots, x_n) = 0 \quad \longrightarrow \quad g(x_1, \ldots, x_n) = 0 \right),$$

where $f_i, g \in k[x_1, \ldots, x_n]$.

Universal closure and quasivariety

Denote by $\mathfrak{U}$ the set of all universal formulas in the language

$$\mathrm{L}_{\mathrm{ring}k} = \{+, -, \cdot, \alpha, \alpha \in k\}$$

that are true in k;
and by $\mathfrak{Q}$ the set of all quasi-identities that hold in k.

The universal closure $\mathbf{Ucl}(k) =$ the class of all rings that satisfy all the formulas from $\mathfrak{U}$.

The quasi-identical closure $\mathbf{Qvar}(k) =$ the class of all rings that satisfy all the formulas from $\mathfrak{Q}$.

$$\mathbf{Ucl}(k) \subseteq \mathbf{Qvar}(k)$$

Let $\mathrm{L}_{\mathrm{ring}k} = \{+, -, \cdot, \alpha, \alpha \in k\}$ be the extended language of rings.

Corollary 4

Axioms for **Qvar**(k):

(I) axioms of commutative associative k-algebras with 1;

(II) $\forall x\ (x^n = 0 \longrightarrow x = 0)$, $n \in \mathbb{N}$.

Axioms for **Ucl**(k):

(III) $\forall x, y\ (xy = 0 \longrightarrow [x = 0 \vee y = 0])$.

The Nullstellensatz

for the field of real numbers

A. Prestel

Lectures on formally real fields

Lecture Notes in Math., **1093**, Springer-Verlag, Berlin, 1984.

Formally real fields

Axioms:

(1) axioms of linear order;

(2) $x \leqslant y \longrightarrow x + z \leqslant y + z$;

(3) $x \leqslant y \wedge z \geqslant 0 \longrightarrow xz \leqslant yz$.

A field (ring) F with predicate "$\leqslant$", satisfying axioms (1), (2), and (3), is called a linearly ordered field $(F, \leqslant)$.
A field, that admits at least one linear ordering, is called formally real.

The characterization of formally real fields

Artin-Schreier theory:

(i) -1 is not a sum of squares in F;

(ii) every equation of the form $x_1^2 + \ldots + x_n^2 = 0$ $(n \in \mathbb{N})$ has no non-trivial solutions in F.

Theorem

A field $F \supset \mathbb{R}$ is formally real if and only if $\mathbf{Ucl}(F) = \mathbf{Ucl}(\mathbb{R})$ in the language $\mathrm{L}_{\mathrm{ring}\mathbb{R}}$.

Axioms for Qvar($\mathbb{R}$) and Ucl($\mathbb{R}$) in the language $\mathrm{L}_{\mathrm{ring}\mathbb{R}}$

Axioms for **Qvar**($\mathbb{R}$):

(I) axioms of commutative associative $\mathbb{R}$-algebra with 1;

(II) order and no nilpotent elements:

$$\forall x_1, \ldots, x_n \quad \left(x_1^{2m_1} + \ldots + x_n^{2m_n} = 0 \longrightarrow \bigwedge_{i=1}^{n} (x_i = 0) \right),$$

$$n,\ m_1, \ldots, m_n \in \mathbb{N}.$$

Axioms for **Ucl**($\mathbb{R}$):

(III) no zero-divisors:

$$\forall x, y\ (xy = 0 \to [x = 0 \vee y = 0]).$$

Corollaries

Corollary 1

A commutative associative $\mathbb{R}$-algebra A with 1 belongs to $\mathbf{Ucl}(\mathbb{R})$ if and only if A is an orderable domain.

Corollary 2

A commutative associative ring A is the coordinate ring of an (irreducible) algebraic set over $\mathbb{R}$ if and only if A is a finitely generated orderable $\mathbb{R}$-algebra with no nilpotent elements (zero-divisors).

17^{th} Hilbert's problem

Let $\mathcal{S} = \mathcal{S}_{\mathbb{R}[x_1,\ldots,x_n]}(\mathbb{R}^+)$ be the set of all non-negative definite functions:

$$f \in \mathcal{S} \quad \longleftrightarrow \quad f(a_1,\ldots,a_n) \geqslant 0 \quad \forall\, (a_1,\ldots,a_n) \in \mathbb{R}^n.$$

E. Artin, 1927

A function $f \in \mathbb{R}[x_1,\ldots,x_n]$ is non-negative definite if and only if it can be written as a sum of squares of functions from $\mathbb{R}[x_1,\ldots,x_n]$.

The Real Nullstellensatz

Theorem 1 (The Real Nullstellensatz)

Let $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$ and $I = \mathrm{id}\langle f_1, \ldots, f_m \rangle$. Then the radical of the system of equations $\{f_1 = 0, \ldots, f_m = 0\}$ is the following ideal of the ring $\mathbb{R}[x_1, \ldots, x_n]$:

$$\mathrm{Rad}(I) = \{f \in \mathbb{R}[x_1, \ldots, x_n] \mid \exists m \in \mathbb{N}, s \in \mathcal{S} \;\; f^{2m} + s \in I\}.$$

Theorem 2 (on consistence)

A system of equations $\{f_1 = 0, \ldots, f_m = 0\}$ is consistent over $\mathbb{R}$ if and only if $(1 + \mathcal{S}) \cap I = \emptyset$.
A system of equations $\{f_1 = 0, \ldots, f_m = 0\}$ is inconsistent over $\mathbb{R}$ if and only if there exist $s \in \mathcal{S}$ and $h_1, \ldots, h_m \in \mathbb{R}[x_1, \ldots, x_n]$ with $\sum_{i=1}^{m} h_i f_h = 1 + s$.

The Nullstellensatz for finite fields

The Nullstellensatz

for the field of p-adic numbers

A. Prestel, P. Roquette
Formally p-adic fields
Lecture Notes in Math., **1050**, SpringerVerlag, Berlin, 1984.

Ax-Kochen's, Ershov's Theory

Let F be a field (or a domain) and $x \mid_p y$ (or simply, $x \mid y$) be a binary predicate on F.

d_1: $x \mid x$;

d_2: $x \mid y$ and $y \mid z \longrightarrow x \mid z$;

d_3: $x \mid y$ or $y \mid x$;

d_4: $x \mid y \longrightarrow xz \mid yz$;

d_5: $1 \mid x$ or $1 \mid y \longrightarrow 1 \mid (x + y)$;

d_6: $p \nmid 1$;

d_7: $1 \mid x \longrightarrow p \mid (x - 1)$ or $\ldots$ or $p \mid (x - p)$;

d_8: $1 \mid x$ and $x \mid p \longrightarrow p \mid x$ or $x \mid 1$.

If $\langle F; \mathrm{L}_{\mathrm{ring}} \cup \{x \mid_p y\}\rangle$ satisfies axioms $d_1 - d_7$, then the field F is called formally p-adic.

Examples of formally p-adic fields

1. The field of p-adic numbers $\mathbb{Q}_p$ is formally p-adic.
2. $\langle \mathbb{Q};\ x \mid_p y \rangle$, where $x \mid_p y$ is defined as follows:
   if $x = p^{\alpha}\frac{r_1}{s_1}$, $y = p^{\beta}\frac{r_2}{s_2}$,
   $(p, r_1) = (p, s_1) = (p, r_2) = (p, s_2) = 1$, then

$$x \mid_p y \ \longleftrightarrow\ \alpha \leqslant \beta.$$

3. The ring $\langle \mathbb{Z};\ x \mid_p y \rangle$ is formally p-adic.

Theorem

A field $F \supset \mathbb{Q}_p$ is formally p-adic, and satisfies the axiom d_8, if and only if $\mathbf{Ucl}(F) = \mathbf{Ucl}(\mathbb{Q}_p)$ in the language $\mathrm{L}_{\mathrm{ring}\mathbb{Q}_p}$.

Fact

Let F be a formally p-adic field. Let $R_v = \{a \in F \mid 1 \mid a\}$ and $\mathfrak{m}_v = \{a \in R_v \mid p \mid a\}$. Then R_v is a local ring with the maximal ideal $\mathfrak{m}_v$. The ring R_v is called the valuation ring.

Definition

A rational function $f \in \mathbb{Q}_p(x_1, \ldots, x_n) : \mathbb{Q}_p^n \to \mathbb{Q}_p$ is called regular if it is everywhere defined. The set of all regular functions is a ring. It is denoted by $\mathrm{O}(\mathbb{Q}_p^n)$.

A family of all regular functions $f \in \mathrm{O}(\mathbb{Q}_p^n) : \mathbb{Q}_p^n \to \mathbb{Q}_p$ with images in the valuation ring R_v form the so-called Kochen ring. Understanding the structure of the Kochen ring helps describe the whole ring of regular functions $\mathrm{O}(\mathbb{Q}_p^n)$.

The p-adic Nullstellensatz

Theorem 1 (the p-adic Nullstellensatz)

A polynomial $g(\bar{x})$ is a consequence of a system of equations $\{f_1(\bar{x}) = 0, \ldots, f_m(\bar{x}) = 0\}$ over $\mathbb{Q}_p$ if and only if there exists a power g^r that admits a presentation

$$g^r = h_1 f_1 + \ldots + h_m f_m, \quad h_i \in \mathrm{O}(\mathbb{Q}_p^n).$$

Theorem 2

A ring A is the coordinate ring of an irreducible algebraic set over $\mathbb{Q}_p$ if and only if A is a finitely generated formally p-adic algebra over $\mathbb{Q}_p$ with no zero-divisors and satisfies axiom d_8.

Axioms for Ucl($\mathbb{Q}_p$) in the language $\mathrm{L}_{\mathrm{ring}\mathbb{Q}_p} \cup \{x \mid_p y\}$

1. Axioms of commutative associative algebras with 1 over $\mathbb{Q}_p$;
2. $\mathbb{Q}_p$ is a domain;
3. $d_1 - d_8$.

To be continued...