The Nullstellensatz for algebraic structures II

Vladimir Remeslennikov

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

October, Montreal

Nullstellensatz for finite fields

Let F_q be a finite field of order $q = p^n$.

Nullstellensatz for F_q

Let $\bar{x} = (x_1, \ldots, x_n)$, and let $S : \{f_1(\bar{x}), \ldots, f_m(\bar{x})\}$ be a system of equations over F_q. Then

$$\mathrm{Rad}(S) = \mathrm{id}\langle f_1, \ldots, f_m, x_1^q - x_1, \ldots, x_n^q - x_n \rangle$$

The resolvent problem

Example: quadratic equations over $\mathbb{R}$

$$s: \ ax^2 + bx + c = 0, \text{ where } a, b, c \text{ are parameters.}$$

Let T be a transformation so that $T(s) = s'$,

$$s': \ y^2 = d, \text{ where } d \text{ is the discriminant.}$$

Then T induces an isomorphism

$$T^* : \mathbb{R}[x]/\mathrm{Rad}(s) \to \mathbb{R}[x]/\mathrm{Rad}(s')$$

$$R = \{\text{the set of resolvents for } s\} = \{r_0 : 0 = 1; r_1 : x = \sqrt{d}; r_2 : x = -\sqrt{d}\},$$

note that $c(r_i) < c(s)$.

Example: quadratic equations over $\mathbb{R}$

$d < 0$ Then s is inconsistent, $\mathrm{Rad}(s) = R[x]$. The corresponding universal formula is

$$\Phi(a, b, c) : \forall x(ax^2 + bx + c = 0 \to 0 = 1).$$

This formula holds in $\mathbb{R}$ iff $d = b^2 - 4ac < 0$.

$d \geq 0$

$$\Phi(a, b, c) : \forall x(ax^2 + bx + c = 0 \to x = \sqrt{d} \vee x = -\sqrt{d}).$$

We have

$$V(S) \subseteq V(r_1) \cup V(r_2).$$

Formal definition of the resolvent method

Let S be a finite system of equations with parameters over $\mathcal{A}$ (over a field) in variables $X = \{x_1, \ldots, x_n\}$.
Let $c(S)$ be complexity of systems of equations. We will say that for the system S there is a resolvent R if

1. $R = \{R_1, \ldots, R_m\}$, $c(R_i) < c(S)$;
2. $V(R) \subseteq \bigcup_{i=1}^{m} R_i$; There exists finitely many universal formulas

$$\phi_i : \forall x(S(X) = 0 \to \bigvee_{j_1 \in J \subseteq \{1,\ldots,m\}} R_{j_1}(X),$$

$$\ldots$$

$$\phi_k : \forall x(S(X) = 0 \to \bigvee_{j_k \in J \subseteq \{1,\ldots,m\}} R_{j_k}(X).$$

If such R exists, then we say that S has a solution of the resolvent problem.
Similar for systems of equations with parameters.

Definable predicate for inconsistent systems

Let $S(X, p_1, \ldots, p_m)$ be a finite system of equations with parameters

$$\Phi(p_1, \ldots, p_m) = \forall \bar{x} S(\bar{x}, p_1, \ldots p_m) = 0 \to 0 = 1)$$

Note that

$\Phi(p_1, \ldots, p_m)$ is true $\Leftrightarrow S(\bar{x}, p_1, \ldots, p_m) = 0$ is inconsistent.

Questions and open problems

1. The resolvent problem for systems of equations in one variable for finitely generated t.f. nilpotent groups.
2. Romanovskii and R.: solution of the resolvent problem for one-variable equations over some finitely generated metabelian groups.
3. The resolvent problem for free associative, Lie and anti-commutative algebras.

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 algebraic structures

Terms and atomic formulas

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

$$\mathrm{L} = \{\text{set of const symbols}\} \cup \{\text{set of functional symbols}\}.$$

Terms in the language L in variables $X = \{x_1, \ldots, x_n\}$ are formal expressions defined recursively as follows:

- variables $x_1, x_2, \ldots, x_n$ and constants from L are terms;
- if $t_1, \ldots, t_n$ are terms and $F(x_1, \ldots, x_n) \in \mathrm{L}$ is a function then $F(t_1, \ldots, t_n)$ is a term.

Atomic formulas are formulas of the form

$$(t = s),$$

where t, s are terms.

Denote by $\mathrm{At}_{\mathrm{L}}(X)$ the set of all atomic formulas in the language L with variables in X.

Elements of algebraic geometry

- Any subset $S \subseteq \mathrm{At}_{\mathrm{L}}(X)$ is called a system of equations in the language L.
- The set

$$\mathrm{V}(S) = \{\ (a_1, \ldots, a_n) \in A^n \ \mid \\ t(a_1, \ldots, a_n) = s(a_1, \ldots, a_n) \quad \forall\, (t = s) \in S\ \},$$

  is called algebraic set over $\mathcal{A}$.
- The radical $\mathrm{Rad}(S)$ of S over $\mathcal{A}$ is the set of all consequences of S over $\mathcal{A}$.
- An equation $(t' = s') \in \mathrm{At}_{\mathrm{L}}$ is called a consequence of S over $\mathcal{A}$ if $\mathcal{A}$ satisfies the (infinite) quasi-identity

$$\forall\, x_1, \ldots, x_n \quad \left(\bigwedge_{(t=s)\in S} t(\bar{x}) = s(\bar{x}) \ \longrightarrow\ t'(\bar{x}) = s'(\bar{x}) \right).$$

The Nullstellensatz for algebraic structure $\mathcal{A}$ is ...

- ... a procedure for constructing the $\mathrm{Rad}(S)$ of a system of equations S;
- ... a theorem about the structure of the radical $\mathrm{Rad}(S)$ of a system of equations S;
- ... a procedure for constructing a system of equations S' with the Nullstellensatz property and so that $\mathrm{V}(S') = \mathrm{V}(S)$.

Definition

A system of equations S' is called a system with Nullstellensatz property if $\mathrm{Rad}(S') = [S']$, where $[S']$ is the congruence closure of S' (e.g., normal subgroup, ideal).

Equationally Noetherian algebraic structures

Definition

An algebraic structure $\mathcal{A}$ is called equationally Noetherian if for any positive integer n and any system of equations $S(x_1, \ldots, x_n)$ there exists a finite subsystem $S_0 \subseteq S$ such that $\mathrm{V}(S) = \mathrm{V}(S_0)$.

Equationally Noetherian $=$ every chain

$$\mathrm{Rad}(S_1) \subseteq \mathrm{Rad}(S_2) \subseteq \ldots \subseteq \mathrm{Rad}(S_m) \subseteq \ldots$$

stabilizes.

Definition

An algebraic structure $\mathcal{A}$ is called Noetherian (with respect to congruences) if ...

The Nullstellensatz for equationally Noetherian algebraic structures

Suppose that $\mathcal{A}$ is an equationally Noetherian algebraic structure and S a system of equations.

Then $\mathrm{Rad}(S)$ = the set of all equations $(t' = s')$ such that the quasi-identity

$$\forall\, x_1, \ldots, x_n \quad \left(\bigwedge_{(t=s)\in S} t(\bar{x}) = s(\bar{x}) \;\longrightarrow\; t'(\bar{x}) = s'(\bar{x}) \right)$$

holds in $\mathcal{A}$.

But, as usual, we don't know all quasi-identities that hold in $\mathcal{A}$.

Suppose, we know only axioms of **Qvar**$(\mathcal{A})$. How can we realize the Nullstellensatz procedure in this case?

The Nullstellensatz procedure for equationally Noetherian groups

Let G be a group and $\mathfrak{Q}$ a "good" set of axioms for $\mathbf{Qvar}(G)$.

$$G[X] = G * F\langle x_1, \ldots, x_n \rangle.$$

Equations $=$ expressions of the type $s = 1$, where $s \in G[X]$.

To solve the Nullstellensatz problem it suffices to compute radicals in $G[X]$.

The Nullstellensatz procedure for equationally Noetherian groups

A procedure for constructing $\mathrm{Rad}(S)$, S - finite:

$$S_0 = S \quad \subseteq \quad S_1 = \mathrm{ncl}\langle S_0 \rangle \quad \subset \quad \ldots \quad \subset \quad S_{i-1} \quad \subset \quad S_i \quad \subset \quad \ldots$$

Here:

- $S_i = \mathrm{ncl}\langle S_{i-1} \cup h_i \rangle$, $h_i \notin S_{i-1}$;
- $h_i = \mathbf{s}\,(w_1(x_1, \ldots, x_n), \ldots, w_r(x_1, \ldots, x_n))$, where
- $w_1(x_1, \ldots, x_n), \ldots, w_r(x_1, \ldots, x_n) \in G[X]$ and
- there exists a quasi-identity from $\mathfrak{Q}$

$$\forall\, x_1, \ldots, x_r \quad \left(\bigwedge_{j=1}^{m} \mathbf{s_j}\,(\bar{x}) = 1 \longrightarrow \mathbf{s}\,(\bar{x}) = 1 \right);$$

- such that $\mathbf{s_j}\,(w_1(x_1, \ldots, x_n), \ldots, w_r(x_1, \ldots, x_n)) \in S_{i-1}$ for all $j = 1, \ldots, m$.

We have $\mathrm{Rad}(S) = \bigcup_i S_i$. If G is Noetherian wrt congruences (normal subgroups), then $\mathrm{Rad}(S) = S_i$ for some $i \in \mathbb{N}$.

The Nullstellensatz procedure for equationally Noetherian groups

A procedure for constructing the radical $\mathrm{Rad}(S)$ for a finite system of equations S:

$$S_0 = S \quad \subseteq \quad S_1 = \mathrm{ncl}\langle S_0 \rangle \quad \subset \quad \ldots \quad \subset \quad S_{i-1} \quad \subset \quad S_i \quad \subset \quad \ldots$$

Here:

- $S_i = \mathrm{ncl}\langle S_{i-1} \cup \{\text{all } h_i\} \rangle$, $h_i \notin S_{i-1}$;
- $h_i = \mathbf{s}\,(w_1(x_1, \ldots, x_n), \ldots, w_r(x_1, \ldots, x_n))$, where
- $w_1(x_1, \ldots, x_n), \ldots, w_r(x_1, \ldots, x_n) \in G[X]$ and
- there exists a quasi-identity from $\mathfrak{Q}$

$$\forall\, x_1, \ldots, x_r \quad \left(\bigwedge_{j=1}^{m} \mathbf{s_j}\,(\bar{x}) = 1 \;\longrightarrow\; \mathbf{s}\,(\bar{x}) = 1 \right);$$

- such that $\mathbf{s_j}\,(w_1(x_1, \ldots, x_n), \ldots, w_r(x_1, \ldots, x_n)) \in S_{i-1}$ for all $j = 1, \ldots, m$.

If G is equationally Noetherian, then $\mathrm{Rad}(S) = S_i$ for some $i \in \mathbb{N}$.

Irreducible algebraic sets

Fact

Every algebraic set Y over an equationally Noetherian algebraic structure $\mathcal{A}$ can be expressed as a finite union of irreducible algebraic sets (irreducible components):

$$Y = Y_1 \cup Y_2 \cup \ldots \cup Y_m.$$

Furthermore, this decomposition is unique up to permutation and omission of superfluous irreducible components.

Irreducible = can not be expressed as a finite union of proper algebraic subsets.

Statement of the problem

The irreducible Nullstellensatz:

For a system of equations S

- find systems of equations $S_1, \ldots, S_m$, such that

$$\mathrm{V}(S) = \mathrm{V}(S_1) \cup \ldots \cup \mathrm{V}(S_m)$$

  and $\mathrm{V}(S_i)$'s are irreducible,
- and compute the radicals $\mathrm{Rad}(S_1), \ldots, \mathrm{Rad}(S_m)$.

Let G be an equationally Noetherian group and $S(X) \subseteq G * F(X)$ a finite system of equations over G. Suppose that we have a good system of axioms for $\mathbf{Ucl}(G)$ by formulas of the form:

$$\forall x_1, \ldots, x_n \left(\bigwedge_{i=1}^{m} u_i(X) = 1 \rightarrow \bigvee_{j=1}^{r} v_i(X) = 1 \right)$$

Let $S_1 = \mathrm{ncl}\langle S \rangle \lhd G[X]$. If $S_1 = \mathrm{Rad}(S)$, then the process ends and we say that S has Nullstellensatz.
It is well-known that majority of quadratic equations have Nullstellensatz.

The Nullstellensatz

for torsion-free abelian groups

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

Let A be a torsion-free abelian group and $\mathrm{L}_{\mathrm{gr}} = \{+, -, 0\}$ the language of abelian groups.

Axioms for **Qvar**(A) in the extended language $\mathrm{L}_{\mathrm{gr}A}$:

(I) axioms of abelian groups;

(II) torsion-free: $\forall\, x\, (nx = 0 \longrightarrow x = 0)$, $n \in \mathbb{N}$;

(III) $\forall\, x\, (p^n x = a \longrightarrow x = 0)$
for all natural numbers n, all prime numbers p, and all $a \in A$, such that the equation $p^n x = a$ has no solutions in A.

The Nullstellensatz procedure

Let $S = \{s_1 = 0, \ldots, s_m = 0\}$ be a system of equations over A.

1. If the system S is inconsistent, then, using the Euclidean algorithm, one can use S to produce an equation of the type $p^n x = a$ with no solutions in A. In this case $\mathrm{Rad}(S) = A[\bar{x}]$.
2. If the system S is consistent, then $\mathrm{Rad}(S) = \mathrm{Is}\langle S \rangle$.

The Nullstellensatz

for free metabelian groups

O. Chapuis

∀-free metabelian groups

J. Symbolic Logic, **62**, 159–174, 1997.

V. Remeslennikov, R. Stöhr

On the quasivariety generated by a non-cyclic free metabelian group

Algebra Colloq., **11**, 191–214, 2004.

Elementary properties of free metabelian groups

The metabelian identity:

$$\forall\, x, y, z, t \quad [[x, y], [z, t]] = 1.$$

Let F_n be a free metabelian group of a rank $n \geqslant 2$.

1. The compatibility problem of systems of equations with coefficients in F_n is algorithmically undecidable (V. A. Roman'kov).
2. The compatibility problem of coefficient-free systems of equations over F_n is algorithmically decidable (O. Chapuis).

Fact

$\mathbf{Ucl}(F_n) = \mathbf{Ucl}(F_m)$ and $\mathbf{Qvar}(F_n) = \mathbf{Qvar}(F_m)$, $n, m \geqslant 2$, in the language L_{gr}. Therefore, we may talk about universal (quasi-equational) theory of a free non-abelian metabelian group and write $\mathbf{Ucl}(F)$ ($\mathbf{Qvar}(F)$).

Axioms for Ucl(F) in the language L_{gr}

V. Remeslennikov, R. Stöhr:

1. $\forall\, x, y, z, t \quad [[x, y], [z, t]] = 1$;
2. $\forall\, x \quad (x^n = 1 \longrightarrow x = 1),\ n \in \mathbb{N}$;
3. $\forall\, x_1 \ldots, x_n,\ y, z \quad ([y, z]^\alpha = 1 \longrightarrow [y, z] = 1),$
   $\alpha \in R_n, \varepsilon(\alpha) \neq 0$;
4. $\forall\, x_1 \ldots, x_n,\ y, z \quad ([y, z]^\alpha = 1 \longrightarrow [y, z]^{\prod(1-x_i)} = 1),$
   $\alpha \in R_n, \varepsilon(\alpha) = 0$;
5. CT-axiom:
   $\forall\, x, y, z \quad (x \neq 1 \wedge [x, y] = 1 \wedge [x, z] = 1 \longrightarrow [y, z] = 1) \sim$
   $\forall\, x, y, z \quad ([x, y] = 1 \wedge [x, z] = 1 \longrightarrow [y, z] = 1 \vee x = 1).$

Axioms for Qvar(F) in the language $\mathrm{L_{gr}}$

V. Remeslennikov, R. Stöhr:

6.1 $\forall\, x, y, z, t \quad [[x, y], [z, t]] = 1;$

6.2 $\forall\, x \quad (x^n = 1 \longrightarrow x = 1),\ n \in \mathbb{N};$

6.3 $\forall\, x, y \quad ([x, y, x] = 1 \wedge [x, y, y] = 1 \longrightarrow [x, y] = 1);$

6.4 $\forall\, x, y \quad ([x^n, (x^n)^y] = 1 \longrightarrow [x, x^y] = 1),\ n \in \mathbb{N};$

6.5 $\forall\, x_1 \ldots, x_n,\ y, z \quad ([y, z]^\alpha = 1 \longrightarrow [y, z] = 1),$
$\alpha \in R_n, \varepsilon(\alpha) \neq 0;$

6.6 $\forall\, x_1 \ldots, x_n,\ y, z \quad ([y, z]^\alpha = 1 \longrightarrow [y, z]^{\prod(1-x_i)} = 1),$
$\alpha \in R_n, \varepsilon(\alpha) = 0;$

6.7 $\forall\, x_1 \ldots, x_n,\ y, z \quad ([y, z]^\alpha = 1 \longrightarrow [y, z]^{\beta_i} = 1),$
$\mathrm{Rad}(\alpha) = \langle \beta_1, \ldots, \beta_q \rangle;$

6.8 $\forall\, x_1 \ldots, x_n,\ y_1, \ldots, y_n,\ z$
$(z = \prod [x_i, y_i] \wedge \bigwedge_{i=1}^{n} [z, x_i] = [z, y_i] = 1 \longrightarrow z = 1).$

Proposition 3.2

There exists an algorithm to compute the radical $\mathrm{Rad}(S)$ of a finite coefficient-free system of equations S over a free finitely generated non-abelian metabelian group.

O. Chapuis's Theorem

For any finitely generated group G the following conditions are equivalent:

- G is a subgroup of a wreath product $W_{r,s}$, $r, s \in \mathbb{N}$;
- $G \in \mathbf{Ucl}(F)$;
- G satisfies 6.1, 6.2, 6.5, 6.6, and CT;
- G is an s-group.

Questions and problems

Open questions

1. Does there exist a satisfactory system of axioms for $\mathbf{Ucl}(\mathbb{Q}_p)$ and $\mathbf{Qvar}(\mathbb{Q}_p)$ in the language $\mathrm{L}_{\mathrm{ring}\mathbb{Q}_p}$? And for $\mathbf{Qvar}(\mathbb{Q}_p)$ in the language $\mathrm{L}_{\mathrm{ring}} \cup \{x \mid_p y\}$?
2. Let F be a free solvable group of class $r > 2$. Does there exist a recursive system of axioms for $\mathbf{Ucl}(F)$ and $\mathbf{Qvar}(F)$ in the language L_{gr}? In other languages?
3. Nullstellensatz for free metabelian (free solvable) group in the extended language
   - in dimension 1,
   - for semigroup equations.