Equations in groups and rings

Alexei Miasnikov
Stevens Institute

(Diablerets , March 10th, 2016)

Outline

- Groups
  - Equations and Diophantine problems
  - Commutative rings with decidable/undecidable DP Groups and rings with decidable/undecidable DP
  - Nilpotent groups
  - Particular equations
- Free associative and Lie algebras

Equations in rings

- Equations in associative commutative rings R are the classical polynomial equations in R:

$$p(x_1, \ldots, x_n) = 0, \quad \textit{where} \quad p \in R[x_1, \ldots, x_n]$$

Solutions:

$$x_1 \to a_1, \ldots, x_n \to a_n \quad (a_i \in R)$$

such that

$$p(a_1, \ldots, a_n) = 0 \quad \textit{in} \quad R.$$

- Similar for systems of equations in variables $x_1, \ldots, x_n$. If R is Noetherian it suffices to consider only finite systems of equations.

Equations in rings

- Equations in associative commutative rings R are the classical polynomial equations in R:

$$p(x_1, \ldots, x_n) = 0, \quad \textit{where} \quad p \in R[x_1, \ldots, x_n]$$

Solutions:

$$x_1 \to a_1, \ldots, x_n \to a_n \quad (a_i \in R)$$

such that

$$p(a_1, \ldots, a_n) = 0 \quad \textit{in} \quad R.$$

- Similar for systems of equations in variables $x_1, \ldots, x_n$. If R is Noetherian it suffices to consider only finite systems of equations.

Diophantine problems

Diophantine problems for a given ring R: if there exists an algorithm that decides whether or not a given equation (finite system of equations) in R has a solution in R.

Diophantine problem = decidability of equations = generalized tenth Hilbert problem

For an integral domain R finite systems of equations are equivalent to single equations provided the field of fractions of R is not algebraically closed.

Remark: to consider Diophantine problems in R the coefficients of the polynomial equations must be "constructible" or "computable", say integers, or elements from a computable subring $R_0 \leq R$.

Diophantine problems

Diophantine problems for a given ring R: if there exists an algorithm that decides whether or not a given equation (finite system of equations) in R has a solution in R.

Diophantine problem = decidability of equations = generalized tenth Hilbert problem

For an integral domain R finite systems of equations are equivalent to single equations provided the field of fractions of R is not algebraically closed.

Remark: to consider Diophantine problems in R the coefficients of the polynomial equations must be "constructible" or "computable", say integers, or elements from a computable subring $R_0 \leq R$.

Diophantine problems

Diophantine problems for a given ring R: if there exists an algorithm that decides whether or not a given equation (finite system of equations) in R has a solution in R.

Diophantine problem = decidability of equations = generalized tenth Hilbert problem

For an integral domain R finite systems of equations are equivalent to single equations provided the field of fractions of R is not algebraically closed.

Remark: to consider Diophantine problems in R the coefficients of the polynomial equations must be "constructible" or "computable", say integers, or elements from a computable subring $R_0 \leq R$.

Examples: decidable DP

For the following fields Diophantine problem is decidable:

- $\mathbb{C}$, coefficients in $\bar{\mathbb{Q}}$. In fact, $Th(\mathbb{C})$ is decidable.
- $\mathbb{R}$, coefficients are computable reals. $Th(\mathbb{R})$ is decidable.
- $\mathbb{Q}_p$, coefficients are computable p-adics. $Th(\mathbb{Q}_p)$ is decidable.

By the way, there are rings where equations are decidable, but the elementary theory is not.

Examples: decidable DP

For the following fields Diophantine problem is decidable:

- $\mathbb{C}$, coefficients in $\bar{\mathbb{Q}}$. In fact, $Th(\mathbb{C})$ is decidable.
- $\mathbb{R}$, coefficients are computable reals. $Th(\mathbb{R})$ is decidable.
- $\mathbb{Q}_p$, coefficients are computable p-adics. $Th(\mathbb{Q}_p)$ is decidable.

By the way, there are rings where equations are decidable, but the elementary theory is not.

Examples: decidable DP

For the following fields Diophantine problem is decidable:

- $\mathbb{C}$, coefficients in $\bar{\mathbb{Q}}$. In fact, $Th(\mathbb{C})$ is decidable.
- $\mathbb{R}$, coefficients are computable reals. $Th(\mathbb{R})$ is decidable.
- $\mathbb{Q}_p$, coefficients are computable p-adics. $Th(\mathbb{Q}_p)$ is decidable.

By the way, there are rings where equations are decidable, but the elementary theory is not.

Examples: decidable DP

For the following fields Diophantine problem is decidable:

- $\mathbb{C}$, coefficients in $\bar{\mathbb{Q}}$. In fact, $Th(\mathbb{C})$ is decidable.
- $\mathbb{R}$, coefficients are computable reals. $Th(\mathbb{R})$ is decidable.
- $\mathbb{Q}_p$, coefficients are computable p-adics. $Th(\mathbb{Q}_p)$ is decidable.

By the way, there are rings where equations are decidable, but the elementary theory is not.

Examples: decidable DP

For the following fields Diophantine problem is decidable:

- $\mathbb{C}$, coefficients in $\bar{\mathbb{Q}}$. In fact, $Th(\mathbb{C})$ is decidable.
- $\mathbb{R}$, coefficients are computable reals. $Th(\mathbb{R})$ is decidable.
- $\mathbb{Q}_p$, coefficients are computable p-adics. $Th(\mathbb{Q}_p)$ is decidable.

By the way, there are rings where equations are decidable, but the elementary theory is not.

Examples: decidable DP

For the following fields Diophantine problem is decidable:

- $\mathbb{C}$, coefficients in $\bar{\mathbb{Q}}$. In fact, $Th(\mathbb{C})$ is decidable.
- $\mathbb{R}$, coefficients are computable reals. $Th(\mathbb{R})$ is decidable.
- $\mathbb{Q}_p$, coefficients are computable p-adics. $Th(\mathbb{Q}_p)$ is decidable.

By the way, there are rings where equations are decidable, but the elementary theory is not.

Tenth Hilbert Problem

Matiyasevich, 1970

Diophantine problem for $\mathbb{Z}$ is undecidable.

This truly fundamental result is the combined work of Martin Davis, Yuri Matiyasevich, Hilary Putnam and Julia Robinson which spans 21 years.

Diophantine problem for $\mathbb{Q}$

Tenth Hilbert Problem for $\mathbb{Q}$

Diophantine problem for $\mathbb{Q}$ is a major open problem in number theory.

J. Robinson showed that $\mathbb{Z}$ is definable in $\mathbb{Q}$ by some first order formulas. But all attempts to define to define this $\mathbb{Z}$ by equations failed so far.

All known examples of algebraic varieties over $\mathbb{Q}$ have the property that the real topological closure of the Zariski closure of their rational points has finitely many connected components. Barry Mazur has conjectured that this holds for any variety over the $\mathbb{Q}$.

If true Mazur's conjecture implies that the integers are not Diophantine over the rationals.

Diophantine problem for $\mathbb{Q}$

Tenth Hilbert Problem for $\mathbb{Q}$

Diophantine problem for $\mathbb{Q}$ is a major open problem in number theory.

J. Robinson showed that $\mathbb{Z}$ is definable in $\mathbb{Q}$ by some first order formulas. But all attempts to define to define this $\mathbb{Z}$ by equations failed so far.

All known examples of algebraic varieties over $\mathbb{Q}$ have the property that the real topological closure of the Zariski closure of their rational points has finitely many connected components. Barry Mazur has conjectured that this holds for any variety over the $\mathbb{Q}$.

If true Mazur's conjecture implies that the integers are not Diophantine over the rationals.

Diophantine problem for $\mathbb{Q}$

Tenth Hilbert Problem for $\mathbb{Q}$

Diophantine problem for $\mathbb{Q}$ is a major open problem in number theory.

J. Robinson showed that $\mathbb{Z}$ is definable in $\mathbb{Q}$ by some first order formulas. But all attempts to define to define this $\mathbb{Z}$ by equations failed so far.

All known examples of algebraic varieties over $\mathbb{Q}$ have the property that the real topological closure of the Zariski closure of their rational points has finitely many connected components. Barry Mazur has conjectured that this holds for any variety over the $\mathbb{Q}$.

If true Mazur's conjecture implies that the integers are not Diophantine over the rationals.

Diophantine problem for $\mathbb{Q}$

Tenth Hilbert Problem for $\mathbb{Q}$

Diophantine problem for $\mathbb{Q}$ is a major open problem in number theory.

J. Robinson showed that $\mathbb{Z}$ is definable in $\mathbb{Q}$ by some first order formulas. But all attempts to define to define this $\mathbb{Z}$ by equations failed so far.

All known examples of algebraic varieties over $\mathbb{Q}$ have the property that the real topological closure of the Zariski closure of their rational points has finitely many connected components. Barry Mazur has conjectured that this holds for any variety over the $\mathbb{Q}$.

If true Mazur's conjecture implies that the integers are not Diophantine over the rationals.

Diophantine problem for $\mathbb{Q}$

Another approach is to interprete $\mathbb{Z}$ in $\mathbb{Q}$ using elliptic curves or abelian varieties over $\mathbb{Q}$.

In any case, common believe is that the Diophantine problem over $\mathbb{Q}$ is undecidable.

Diophantine problem for number fields and their algebraic integers

Conjectures

- Diophantine problem in a ring of algebraic integers is undecidable.
- Diophantine problem in a finite extension of $\mathbb{Q}$ is undecidable.

Further results

Theorem (Denef, 78)

Let R be an integral domain of characteristic zero. Then the diophantine problem for $R[t]$ with coefficients in $\mathbb{Z}[t]$ is undecidable.

Theorem (Pappas, 85)

Let R be an integral domain of characteristic zero. Then the diophantine problem for $R[t, t^{-1}]$ with coefficients in $\mathbb{Z}[t]$ is undecidable.

Equations in groups

A group equation in variables X and constants from a group G is a formal expression of the type

$$w(x_1, \ldots, x_n, g_1, \ldots, g_m) = 1,$$

where w is a group word in X and constants from G.

Solutions:

$$x_1 \to u_1, \ldots, x_n \to u_n \quad (u_i \in G)$$

such that $w(u_1, \ldots, u_n, g_1, \ldots, g_m) = 1$ in G.

Systems of equations, etc.

Equations in other structures

Let $\mathcal{M}$ be an arbitrary structure in a language L.

An equation in $\mathcal{M}$ is equality of two terms in L with constants from $\mathcal{M}$:

$$t(x_1, \ldots, x_n, a_1, \ldots, a_m) = s(x_1, \ldots, x_n, b_1, \ldots, b_m).$$

So one can consider equations in semigroups, associative or Lie algebras, etc.

Principal questions

The principal questions on equations in $\mathcal{M}$:

- Decidability of single equations and finite systems (Diophantine problems).
- Is every infinite system of equations in finite number of variables and constants from $\mathcal{M}$ equivalent in $\mathcal{M}$ to some finite subsystem of this system? In this case $\mathcal{M}$ is called Equationally Noetherian.
- Description of solution sets of finite systems of equations.
- Algebraic geometry over $\mathcal{M}$.
- Algebraically (existentially) closed objects related to $\mathcal{M}$.

Principal questions

The principal questions on equations in $\mathcal{M}$:

- Decidability of single equations and finite systems (Diophantine problems).
- Is every infinite system of equations in finite number of variables and constants from $\mathcal{M}$ equivalent in $\mathcal{M}$ to some finite subsystem of this system? In this case $\mathcal{M}$ is called Equationally Noetherian.
- Description of solution sets of finite systems of equations.
- Algebraic geometry over $\mathcal{M}$.
- Algebraically (existentially) closed objects related to $\mathcal{M}$.

Principal questions

The principal questions on equations in $\mathcal{M}$:

- Decidability of single equations and finite systems (Diophantine problems).
- Is every infinite system of equations in finite number of variables and constants from $\mathcal{M}$ equivalent in $\mathcal{M}$ to some finite subsystem of this system? In this case $\mathcal{M}$ is called Equationally Noetherian.
- Description of solution sets of finite systems of equations.
- Algebraic geometry over $\mathcal{M}$.
- Algebraically (existentially) closed objects related to $\mathcal{M}$.

Principal questions

The principal questions on equations in $\mathcal{M}$:

- Decidability of single equations and finite systems (Diophantine problems).
- Is every infinite system of equations in finite number of variables and constants from $\mathcal{M}$ equivalent in $\mathcal{M}$ to some finite subsystem of this system? In this case $\mathcal{M}$ is called Equationally Noetherian.
- Description of solution sets of finite systems of equations.
- Algebraic geometry over $\mathcal{M}$.
- Algebraically (existentially) closed objects related to $\mathcal{M}$.

Principal questions

The principal questions on equations in $\mathcal{M}$:

- Decidability of single equations and finite systems (Diophantine problems).
- Is every infinite system of equations in finite number of variables and constants from $\mathcal{M}$ equivalent in $\mathcal{M}$ to some finite subsystem of this system? In this case $\mathcal{M}$ is called Equationally Noetherian.
- Description of solution sets of finite systems of equations.
- Algebraic geometry over $\mathcal{M}$.
- Algebraically (existentially) closed objects related to $\mathcal{M}$.

Developing the theory

- Algebraic geometry over $\mathcal{M}$.
- Algebraically (existentially) closed objects related to $\mathcal{M}$.

Developing the theory

- Algebraic geometry over $\mathcal{M}$.
- Algebraically (existentially) closed objects related to $\mathcal{M}$.

Equations in groups

The principal questions are solved in the following groups:

- Abelian (linear systems of equations).
- Free groups (Makanin-Razborov, Kharlampovich-M.)
- Hyperbolic and toral relatively hyperbolic groups (Rips-Sela, Dahmani-Groves)
- Right angled Artin groups (Diekert-Muscholl, Casals-Ruiz-Kazachkov)
- Free products of groups (Casals-Ruiz-Kazachkov)

Equations in groups

The principal questions are solved in the following groups:

- Abelian (linear systems of equations).
- Free groups (Makanin-Razborov, Kharlampovich-M.)
- Hyperbolic and toral relatively hyperbolic groups (Rips-Sela, Dahmani-Groves)
- Right angled Artin groups (Diekert-Muscholl, Casals-Ruiz-Kazachkov)
- Free products of groups (Casals-Ruiz-Kazachkov)

Complexity questions

If Diophantine problems are decidable in a group G the next fundamental algorithmic question is on complexity of the decision algorithms.
Initial Makanin's algorithm was evaluated as non-elementary. At present, due to brilliant "compression" ideas introduced by Plamdowski and Jeh,
It seems the current space complexity estimate is $NSPACE(n \log n)$.

Major open problem

Are the Diophantine problems in free groups decidable in non-deterministic polynomial time?

Kharlampovch, Lysenok, M., and Touikan showed that decidability of quadratic equations in a given free group is NP-complete.

Complexity questions

If Diophantine problems are decidable in a group G the next fundamental algorithmic question is on complexity of the decision algorithms.
Initial Makanin's algorithm was evaluated as non-elementary. At present, due to brilliant "compression" ideas introduced by Plamdowski and Jeh,
It seems the current space complexity estimate is $NSPACE(n \log n)$.

Major open problem

Are the Diophantine problems in free groups decidable in non-deterministic polynomial time?

Kharlampovch, Lysenok, M., and Touikan showed that decidability of quadratic equations in a given free group is NP-complete.

Good descriptions of solution sets

- Makanin-Razborov diagrams (process, not the description)
- Ciobanu-Diekert-Elder (no cancellation, EDT0L)
- Kharlampovich-Miasnikov (algebraic geometry)

Good descriptions of solution sets

- Makanin-Razborov diagrams (process, not the description)
- Ciobanu-Diekert-Elder (no cancellation, EDT0L)
- Kharlampovich-Miasnikov (algebraic geometry)

Good descriptions of solution sets

- Makanin-Razborov diagrams (process, not the description)
- Ciobanu-Diekert-Elder (no cancellation, EDT0L)
- Kharlampovich-Miasnikov (algebraic geometry)

Good descriptions of solution sets

- Makanin-Razborov diagrams (process, not the description)
- Ciobanu-Diekert-Elder (no cancellation, EDT0L)
- Kharlampovich-Miasnikov (algebraic geometry)

Good descriptions of solution sets

- Makanin-Razborov diagrams (process, not the description)
- Ciobanu-Diekert-Elder (no cancellation, EDT0L)
- Kharlampovich-Miasnikov (algebraic geometry)

Triangular quasi-quadratic (TQ) system is a finite system that has the following form

$$S_1(X_1, X_2, \ldots, X_n, A) = 1,$$
$$S_2(X_2, \ldots, X_n, A) = 1,$$
$$\ldots$$
$$S_n(X_n, A) = 1$$

where either $S_i = 1$ is quadratic in variables X_i, or $S_i = 1$ is a system $[x_j, x_k] = 1$ and, in addition, equations $[x, u] = 1$ for all $x, x_j, x_k \in X_i$ and some $u \in F_{R(S_{i+1},\ldots,S_n)}$ or S_i is empty.
A TQ system above is non-degenerate (NTQ) if for every i, $S_i(X_i, \ldots, X_n, A) = 1$ has a solution in the coordinate group $G_i = F_{R(S_{i+1},\ldots,S_n)}$, where $G_n = F$ (or $G_n = \Gamma$).

Description of solution sets of equations

Theorem

For a system of equations

$$S(X, A) = 1$$

over F one can find finitely many NTQ systems

$$U_1(Y_1, A) = 1, \ldots, U_m(Y_m, A) = 1$$

such that

$$V_F(S) = P_1(V(U_1)) \cup \ldots \cup P_m(V(U_m))$$

for some word mappings $P_1, \ldots, P_m$. (P_i maps a tuple $\bar{Y}_i \in V(U_i)$ to a tuple $\bar{X} \in V_F(S)$.

Similarly one can effectively describe the solution set of a system over a torsion-free hyperbolic group Γ.

Groups with undecidable word and conjugacy problems

Especially constructed finitely presented groups:

- with undecidable word problem,
- with undecidable conjugacy problem

The main tool: simulating Turing or Minski machines in the groups.

Nilpotent and solvable groups

Two crucial results:

- (Romankov) Single equations are undecidable in free nilpotent groups of sufficiently large rank and nilpotency class.
- (Romankov) Single equations are undecidable in free metabelian groups of sufficiently large rank

The main tool: interpreting arithmetic in the groups.

Nilpotent and solvable groups

Two crucial results:

- (Romankov) Single equations are undecidable in free nilpotent groups of sufficiently large rank and nilpotency class.
- (Romankov) Single equations are undecidable in free metabelian groups of sufficiently large rank

The main tool: interpreting arithmetic in the groups.

Systems of equations in Nilpotent groups

Theorem [Moon Duchin, Hao Liang, Michael Shapiro]

The following hold:

- Single equations are decidable in $UT(3, \mathbb{Z})$;
- Finite systems of equations are undecidable in all non-abelian free nilpotent groups.

Finite systems of equations are not equivalent to single equations in $UT(3, \mathbb{Z})$.
The main tool: interpreting arithmetic in the groups.

Systems of equations in Nilpotent groups

Theorem [Moon Duchin, Hao Liang, Michael Shapiro]

The following hold:

- Single equations are decidable in $UT(3, \mathbb{Z})$;
- Finite systems of equations are undecidable in all non-abelian free nilpotent groups.

Finite systems of equations are not equivalent to single equations in $UT(3, \mathbb{Z})$.

The main tool: interpreting arithmetic in the groups.

Systems of equations in Nilpotent groups

Theorem [Moon Duchin, Hao Liang, Michael Shapiro]

The following hold:

- Single equations are decidable in $UT(3, \mathbb{Z})$;
- Finite systems of equations are undecidable in all non-abelian free nilpotent groups.

Finite systems of equations are not equivalent to single equations in $UT(3, \mathbb{Z})$.
The main tool: interpreting arithmetic in the groups.

Interpretations by equations.

E-definable sets.

$A \subset \mathcal{M}^n$ is called e-definable in $\mathcal{M}$ if there exists a finite system of equations $\Sigma(x_1, \ldots, x_n, \bar{y})$ such that

$(a_1, \ldots, a_n)$ is in A iff $\Sigma(a_1, \ldots, a_n, \bar{y})$ has a solution in $\bar{y}$.

Examples

- Positive numbers in $\mathbb{R}$: $x = y^2$;
- Natural numbers $\mathbb{N}$ in integers $\mathbb{Z}$:

$$x \in \mathbb{N} \Longleftrightarrow \exists y_1, \ldots, y_4 (x = y_1^2 + \ldots y_4^2)$$

- Center of a f.g. group G;
- G' if it has a finite width : $x = [y_1, y_2] \cdots, [y_{2k-1}, y_{2k}]$;

Interpretations by equations.

E-interpretation or Diophantine interpretation

Let A and $\mathcal{M}$ be algebraic structures. A map $\phi : X \subset \mathcal{M}^n \to A$ is called an e-interpretation of A in $\mathcal{M}$ if

- ϕ is onto;
- X is e-definable in $\mathcal{M}$;
- Preimage of " $=$ " in A is e-definable:
- Preimage of the graph of every function in $\mathcal{A}$ is e-definable;

Encoding equations.

Reduction of equations.

there is an effective procedure that given an e-enterpretation $\phi : X \subset \mathcal{M}^n \to \mathcal{A}$ and a finite system of equations over $\mathcal{A}$ constructs an equivalent system of equations over $\mathcal{M}$.

- Negative direction;
- Positive direction.

Examples

- $Z(G)$ for any finitely generated group G; G' for any polycyclic group G. They are e-interpretable as groups!
- $G/Z(G)$ for any finitely generated group G;
- For a commutative associative ring R (f.g. additive group), nillradical of R.

Sytems of equations in nilpotent groups

Main theorem [Albert Garreta Fontelles, M., Denis Ovchinnikov]

For every finitely generated non-virtually abelian nilpotent group G there exists (and can be effectively computed) a ring of algebraic integers $O(G)$ which e-interpretable in G. Hence, the Diophantine problem in $O(G)$ reduces to the Diophantine problem in G.

Corollary The Diophantine problem in the class of torsion-free finitely generated nilpotent groups of class 2 (or higher) is equivalent to the Diophantine problem in the rings of algebraic integers: $G \to O(G)$, $O \to UT(3, O)$.

Probably, it is undecidable.

Main theorem [Albert Garreta Fontelles, M., Denis Ovchinnikov]

For every finitely generated non-virtually abelian nilpotent group G there exists (and can be effectively computed) a ring of algebraic integers $O(G)$ which e-interpretable in G. Hence, the Diophantine problem in $O(G)$ reduces to the Diophantine problem in G.

Corollary The Diophantine problem in the class of torsion-free finitely generated nilpotent groups of class 2 (or higher) is equivalent to the Diophantine problem in the rings of algebraic integers: $G \to O(G)$, $O \to UT(3, O)$.

Probably, it is undecidable.

Corrolaries

Polycyclic groups

For any polycyclic group G that contains at least one non virtually abelian nilpotent subgroup, the analogue of the last theorem holds. In particular any non virtually metabelian nilpotent subgroup is like this.

Arithmetic groups

For any arithmetic group that contains a non virtually nilpotent subgroup, the analogue of the last result holds.

The elements a and b are said to be *in general position* in a 2-nilpotent group G if $[a, b] \neq 1$ and the only solutions to the system

$$\begin{aligned} [a, x] &= 1, \\ [b, y] &= 1, \\ [a, y] &= [x, b]. \end{aligned} \tag{1}$$

in G have the following form:

$$x = b^t \, mod \; Z(G), \quad y = a^t \, mod \; Z(G),$$

for t any integer.

Theorem

If a 2-nilpotent group G has a pair of elements in a general position then $O(G) = \mathbb{Z}$. Hence the Diophantine problem in G is undecidable.

Many 2-nilpotent finitely generated groups have elements in a general position.

Theorem

If a 2-nilpotent group G has a pair of elements in a general position then $O(G) = \mathbb{Z}$. Hence the Diophantine problem in G is undecidable.

Many 2-nilpotent finitely generated groups have elements in a general position.

The commutator equation in Nilpotent groups

The commutator problem in a group G: Is there an algorithm that decides if a given element $g \in G$ is a commutator or not?

Decidability of commutator equations $[x, y] = g$ in G.

Common intuition: The commutator equations are decidable in most "reasonable groups".

The commutator equation in Nilpotent groups

The commutator problem in a group G: Is there an algorithm that decides if a given element $g \in G$ is a commutator or not?

Decidability of commutator equations $[x, y] = g$ in G.

Common intuition: The commutator equations are decidable in most "reasonable groups".

A surprising result

Theorem [Romankov, 2015]

There is a finitely generated 2-nilpotent group G with undecidable Commutator Problem.

Endomorphism Problem

The Endomorphism Problem in a group G: given two elements $u, v \in G$ decide whether there is an endomorphism $\phi \in End(G)$ such that $\phi(u) = v$.

Corollary of Romankov's theorem

There is a finitely generated 2-nilpotent group H with undecidable Endomorphism Problem.

Proof:
Let G be the group from Romankov's theorem. Put

$$H = G \times N_{2,2},$$

where $N_{2,2}$ has basis $\{x, y\}$. Then an element $g \in G$ is an endomorphic image of $[x, y]$ if and only if g is a commutator in G.

Endomorphism Problem

The Endomorphism Problem in a group G: given two elements $u, v \in G$ decide whether there is an endomorphism $\phi \in End(G)$ such that $\phi(u) = v$.

Corollary of Romankov's theorem

There is a finitely generated 2-nilpotent group H with undecidable Endomorphism Problem.

Proof:
Let G be the group from Romankov's theorem. Put

$$H = G \times N_{2,2},$$

where $N_{2,2}$ has basis $\{x, y\}$. Then an element $g \in G$ is an endomorphic image of $[x, y]$ if and only if g is a commutator in G.

Retract Problem

The Retract Problem in a group G: given a finitely generated subgroup H of G decide if H is a retract of G or not.

Corollary of Romankov's theorem

There is no (uniform) algorithm to solve Retract Problem in all finitely generated 2-nilpotent groups.

Proof:
Let $H = G \times_{[x,y]=g} N_{2,2}$. Then there is a retraction $\varphi : H \to G$ if and only if g is a commutator in G.

Retract Problem

The Retract Problem in a group G: given a finitely generated subgroup H of G decide if H is a retract of G or not.

Corollary of Romankov's theorem

There is no (uniform) algorithm to solve Retract Problem in all finitely generated 2-nilpotent groups.

Proof:
Let $H = G \times_{[x,y]=g} N_{2,2}$. Then there is a retraction $\varphi : H \to G$ if and only if g is a commutator in G.

Let $\mathbb{A}_K(A)$ be a free associative algebra with basis X over field K.

An equation with variables in $X = \{x_1, \ldots, x_n\}$ and constants from $\mathbb{A}_K(A)$ is an expression

$$P(X, A) = 0$$

where $P(X, A)$ is an element from $\mathbb{A}_K(A \cup X)$.

Solutions are maps $x_i \to u_i \in \mathbb{A}_K(A)$ such that $P(u_1, \ldots, u_n, A) = 0$ in $\mathbb{A}_K(A)$.

Diophantine problem in $\mathbb{A}_K(A)$

Diophantine problem in $\mathbb{A}_K(A)$

Is it true that there is an algorithm which given an equation in $\mathbb{A}_K(A)$ decides if the equation has a solution in $\mathbb{A}_K(A)$ or not for an algebraically closed field $\mathbb{K}$? A finite field $\mathbb{K}$?

Solutions of bounded degree

We assume that the Diophantine problem in K is decidable.

Theorem

For each $m \in \mathbb{N}$ there exists an algorithm which given a finite system of equations in $\mathbb{A}_K(A)$ decides whether there is a solution of degree $\leq m$ of the system (and if it exists the algorithm finds one). Hence the Bounded Diophantine Problem in $\mathbb{A}_K(A)$ is decidable.

The result follows from the decidability of the Diophantine problem in K.

Solutions of bounded degree

width $width(f)$ of a polynomial f = the number of monomials in f.

Theorem

Assume that the Diophantine problem in K is decidable. Then for each $m \in \mathbb{N}$ there exists an algorithm which given a finite system of equations in $\mathbb{A}_K(A)$ decides whether there is a solution of degree $\leq m$ of the system (and if it exists the algorithm finds one). Hence the Bounded Diophantine Problem in $\mathbb{A}_K(A)$ is decidable.

The result follows from Makanin's result on the decidability of the systems of equations in a free semigroup.

Conjecture

Let K be a field with decidable Diophantine problem and $\mathbb{A}_K(A)$ a free associative algbera of finite rank. Then there is a computable function $c : \mathbb{N} \to \mathbb{N}$ such that if an equation $P = 0$ has a solution in $\mathbb{A}_K(A)$ then it has a solution of width at most $f(degP)$.

If the conjecture holds then the Diophantine problem would be

Solutions of bounded degree

width $width(f)$ of a polynomial f = the number of monomials in f.

Theorem

Assume that the Diophantine problem in K is decidable. Then for each $m \in \mathbb{N}$ there exists an algorithm which given a finite system of equations in $\mathbb{A}_K(A)$ decides whether there is a solution of degree $\leq m$ of the system (and if it exists the algorithm finds one). Hence the Bounded Diophantine Problem in $\mathbb{A}_K(A)$ is decidable.

The result follows from Makanin's result on the decidability of the systems of equations in a free semigroup.

Conjecture

Let K be a field with decidable Diophantine problem and $\mathbb{A}_K(A)$ a free associative algbera of finite rank. Then there is a computable function $c : \mathbb{N} \to \mathbb{N}$ such that if an equation $P = 0$ has a solution in $\mathbb{A}_K(A)$ then it has a solution of width at most $f(degP)$.

If the conjecture holds then the Diophantine problem would be

Pell equation In $R[t]$

Pell equation in $R[t]$ for an integral domain R of char 0:

$$X^2 - (t^2 - 1)Y^2 = 1.$$

The solution set P of the Pell equation in $R[t]$ (the Pell curve) is precisely the set of pairs

$$P = (\pm X_n, \pm Y_{n-1}), \quad n \in \mathbb{N},$$

where $X_n, Y_n \in \mathbb{Z}[t]$ are Chebyshev's polynomials.

Recall that:

- $deg Y_n = n$
- $Y_n(1) = n + 1$, so $\{Y_n(1) \mid n = 0, 1, 2, \ldots\} = \mathbb{Z}$.

Pell equation In $R[t]$

Pell equation in $R[t]$ for an integral domain R of char 0:

$$X^2 - (t^2 - 1)Y^2 = 1.$$

The solution set P of the Pell equation in $R[t]$ (the Pell curve) is precisely the set of pairs

$$P = (\pm X_n, \pm Y_{n-1}), \quad n \in \mathbb{N},$$

where $X_n, Y_n \in \mathbb{Z}[t]$ are Chebyshev's polynomials.

Recall that:

- $deg Y_n = n$
- $Y_n(1) = n + 1$, so $\{Y_n(1) \mid n = 0, 1, 2, \ldots\} = \mathbb{Z}$.

Undecidability of the Diophantine problem in $R[t]$

Notice that for $f, g \in \mathbb{Z}[t]$ one has

$$f(1) = g(1) \Longleftrightarrow \exists h(f - g = h(t-1))$$

So the equivalence relation $f \sim g \Longleftrightarrow f(1) = g(1)$ is definable by equations in $\mathbb{Z}[t]$. Hence

$$\mathbb{Z} = \{Y_n \mid n = 0, 1, 2, \ldots\}/\sim$$

and the standard operation $+$ and $\times$ on $\mathbb{Z}$ are interpretable by equations on the Pell curve:

$$m + n = k \Longleftrightarrow Y_m + Y_n \sim Y_k,$$

$$m \times n = k \Longleftrightarrow Y_m \times Y_n \sim Y_k.$$

Degrees of minimal solutions are unbounded

Theorem

Arithmetic $\mathbb{Z}$ is interpretable by equations on the Pell curve in $R[t]$. In particular, the Tenth Hilbert Problem reduces to decidability of equations on the Pell curve in $R[t]$.

From undecidability of THP for $\mathbb{Z}$ follows that the least positive solution of a Diophantine equation $P = 0$ in $\mathbb{Z}$ is not bounded by a computable function on the size of P.

Hence the degrees of minimal solutions of polynomial equations on the Pell curve are not bounded by any computable function.

Diophantine problem in $\mathbb{A}_K(A)$

Theorem

Let $\mathbb{A}_K(X)$ be a free associative algebra over K. Then for any field K of characteristic zero the Diophantine problem for $\mathbb{A}_K(X)$ is undecidable.

Diophantine problem in group rings

Theorem

Let G be a torsion-free hyperbolic group. Then for any field K of characteristic zero the Diophantine problem for $K(G)$ is undecidable.

Zelmanov's question

Towards Dehn functions

Given elements $r, r_1, \ldots, r_n \in \mathbb{A}_K(A)$, decide whether there exist elements $y_1, z_1, \ldots, y_n, z_n \in \mathbb{A}_K(A)$ such that $r = \Sigma_{i=1}^{n} y_i r_i z_i$.

Solution to this problem would clarify the algorithmic nature of Dehn's functions in finitely generated associative algebras.

Observe, that existence of finitely presented algebras with undecidable word problem does not imply undecidability of the quadratic equations above.

Zelmanov's question

Towards Dehn functions

Given elements $r, r_1, \ldots, r_n \in \mathbb{A}_K(A)$, decide whether there exist elements $y_1, z_1, \ldots, y_n, z_n \in \mathbb{A}_K(A)$ such that $r = \Sigma_{i=1}^{n} y_i r_i z_i$.

Solution to this problem would clarify the algorithmic nature of Dehn's functions in finitely generated associative algebras.

Observe, that existence of finitely presented algebras with undecidable word problem does not imply undecidability of the quadratic equations above.

Open questions

Interesting topic

Study elliptic curves in $\mathbb{A}_K(A)$.

Interesting topic

Is the algebra $\mathbb{A}_K(A)$ equationally Noetherian?.

Open questions

Interesting topic

Study elliptic curves in $\mathbb{A}_K(A)$.

Interesting topic

Is the algebra $\mathbb{A}_K(A)$ equationally Noetherian?.

Equations in free Lie algebras

Let $\mathcal{L}_K(X)$ be a free Lie algebra over a field K with basis X ($|X| \geq 2$).

General question

Is Diophantine problem in $\mathcal{L}_K(X)$ decidable?

Theorem

If DP is undecidable in K then it is undecidable in $\mathcal{L}_K(X)$.

Based on a result that the field K is interpretable by equations in $\mathcal{L}_K(X)$.

Equations in free Lie algebras

Let $\mathcal{L}_K(X)$ be a free Lie algebra over a field K with basis X ($|X| \geq 2$).

General question

Is Diophantine problem in $\mathcal{L}_K(X)$ decidable?

Theorem

If DP is undecidable in K then it is undecidable in $\mathcal{L}_K(X)$.

Based on a result that the field K is interpretable by equations in $\mathcal{L}_K(X)$.

Equations in free Lie algebras

Interesting question

Is the Diophantine problem decidable in free Lie algebras over an algebraically closed fields?

Question

Is there an analog of Pell equation in $\mathcal{L}_K(X)$?

Interesting topic

Is the algebra $\mathbb{A}_K(A)$ equationally Noetherian?.

Equations in free Lie algebras

Interesting question

Is the Diophantine problem decidable in free Lie algebras over an algebraically closed fields?

Question

Is there an analog of Pell equation in $\mathcal{L}_K(X)$?

Interesting topic

Is the algebra $\mathbb{A}_K(A)$ equationally Noetherian?.

Equations in free Lie algebras

Interesting question

Is the Diophantine problem decidable in free Lie algebras over an algebraically closed fields?

Question

Is there an analog of Pell equation in $\mathcal{L}_K(X)$?

Interesting topic

Is the algebra $\mathbb{A}_K(A)$ equationally Noetherian?.