Systems of Equations in Nilpotent Groups

Albert Garreta
(joint results with Alexei Miasnikov and Denis Ovchinnikov)

University of the Basque Country

Napoli, May 2016

Diophantine problem

- $\mathscr{D}(A)$ denotes the *Diophantine problem* over a structure A (e.g. a group or a ring).

Diophantine problem

- $\mathscr{D}(A)$ denotes the *Diophantine problem* over a structure A (e.g. a group or a ring).
- $\mathscr{D}(A)$ is *decidable* or *undecidable*.

Diophantine problem

- $\mathscr{D}(A)$ denotes the *Diophantine problem* over a structure A (e.g. a group or a ring).
- $\mathscr{D}(A)$ is *decidable* or *undecidable*.
- *Hilbert's 10th Problem*: $\mathscr{D}(\mathbb{Z}, +, \cdot)$ is undecidable (Davis, Matiyasevich, Putnam, Robinson, 1970).

Diophantine problem

- $\mathscr{D}(A)$ denotes the *Diophantine problem* over a structure A (e.g. a group or a ring).
- $\mathscr{D}(A)$ is *decidable* or *undecidable*.
- *Hilbert's 10th Problem*: $\mathscr{D}(\mathbb{Z}, +, \cdot)$ is undecidable (Davis, Matiyasevich, Putnam, Robinson, 1970).
- $\mathscr{D}(F, \cdot)$ is decidable (Makanin, 1983).

Diophantine problem

- $\mathscr{D}(A)$ denotes the *Diophantine problem* over a structure A (e.g. a group or a ring).
- $\mathscr{D}(A)$ is *decidable* or *undecidable*.
- *Hilbert's 10th Problem*: $\mathscr{D}(\mathbb{Z}, +, \cdot)$ is undecidable (Davis, Matiyasevich, Putnam, Robinson, 1970).
- $\mathscr{D}(F, \cdot)$ is decidable (Makanin, 1983).
- Decidability of $\mathscr{D}(\mathbb{Q}, +, \cdot)$ is an open problem.

Diophantine problem

- $\mathscr{D}(A)$ denotes the *Diophantine problem* over a structure A (e.g. a group or a ring).
- $\mathscr{D}(A)$ is *decidable* or *undecidable*.
- *Hilbert's 10th Problem*: $\mathscr{D}(\mathbb{Z}, +, \cdot)$ is undecidable (Davis, Matiyasevich, Putnam, Robinson, 1970).
- $\mathscr{D}(F, \cdot)$ is decidable (Makanin, 1983).
- Decidability of $\mathscr{D}(\mathbb{Q}, +, \cdot)$ is an open problem.

Initial question

When is $\mathscr{D}(G)$ decidable, for G nilpotent?

Nilpotent groups

- Let G be a group. Define $[x, y] = x^{-1}y^{-1}xy$.

Nilpotent groups

- Let G be a group. Define $[x, y] = x^{-1}y^{-1}xy$.
- $G_1(G) = G$, $G_2 = [G, G]$, $\ldots$, $G_k = [G_{k-1}, G]$.

Nilpotent groups

- Let G be a group. Define $[x, y] = x^{-1}y^{-1}xy$.
- $G_1(G) = G$, $G_2 = [G, G]$, ..., $G_k = [G_{k-1}, G]$.
- G is *nilpotent* if $G_k = 1$ for some k.

Nilpotent groups

- Let G be a group. Define $[x,y] = x^{-1}y^{-1}xy$.
- $G_1(G) = G$, $G_2 = [G,G]$, ..., $G_k = [G_{k-1}, G]$.
- G is *nilpotent* if $G_k = 1$ for some k.
- That is, for some k, all commutators of length k, $[g_1, \overset{k}{\ldots}, g_k] = [\ldots[[[g_1, g_2], g_3], g_4] \ldots, g_k]$ are trivial.

Equations in nilpotent groups - known results

- There exists a 4-nilpotent group G such that $\mathscr{D}(G)$ is undecidable (Roman'kov, 1974).

Equations in nilpotent groups - known results

- There exists a 4-nilpotent group G such that $\mathscr{D}(G)$ is undecidable (Roman'kov, 1974).
- $\mathscr{D}(G)$ is undecidable in any free nonabelian nilpotent group G. (Duchin, Liang, Shapiro, 2014).

Equations in nilpotent groups - known results

- There exists a 4-nilpotent group G such that $\mathscr{D}(G)$ is undecidable (Roman'kov, 1974).
- $\mathscr{D}(G)$ is undecidable in any free nonabelian nilpotent group G. (Duchin, Liang, Shapiro, 2014).

Single equations:

- Single equations are decidable in any free 2-step nilpotent group. (Duchin, Liang, Shapiro, 2014).

Equations in nilpotent groups - known results

- There exists a 4-nilpotent group G such that $\mathscr{D}(G)$ is undecidable (Roman'kov, 1974).
- $\mathscr{D}(G)$ is undecidable in any free nonabelian nilpotent group G. (Duchin, Liang, Shapiro, 2014).

Single equations:

- Single equations are decidable in any free 2-step nilpotent group. (Duchin, Liang, Shapiro, 2014).
- Hence single equations and systems of equations are 'essentially different' in nilpotent groups. This is not the case for $(\mathbb{Z}, +, \cdot)$, for example.

E-definable sets

- Let $x \in \mathbb{R}$. Then $x \in \mathbb{R}_{\geq 0}$ iff $x = y^2$ for some $y \in \mathbb{R}$.

E-definable sets

- Let $x \in \mathbb{R}$. Then $x \in \mathbb{R}_{\geq 0}$ iff $x = y^2$ for some $y \in \mathbb{R}$.
- Let $x \in \mathbb{Z}$. Then $x \in \mathbb{N}$ iff $x = y_1^2 + \cdots + y_4^2$ for some $y_i \in \mathbb{Z}$.

E-definable sets

- Let $x \in \mathbb{R}$. Then $x \in \mathbb{R}_{\geq 0}$ iff $x = y^2$ for some $y \in \mathbb{R}$.
- Let $x \in \mathbb{Z}$. Then $x \in \mathbb{N}$ iff $x = y_1^2 + \cdots + y_4^2$ for some $y_i \in \mathbb{Z}$.

Definition

- $R \subseteq G$ (or $\subseteq G^n$) is *e-definable in* G if "$g \in R$" can be expressed as a system over G:

$$g \in R \;\Leftrightarrow\; \exists \vec{y}\; S(g, \vec{y}) = 1.$$

E-definable sets

- Let $x \in \mathbb{R}$. Then $x \in \mathbb{R}_{\geq 0}$ iff $x = y^2$ for some $y \in \mathbb{R}$.
- Let $x \in \mathbb{Z}$. Then $x \in \mathbb{N}$ iff $x = y_1^2 + \cdots + y_4^2$ for some $y_i \in \mathbb{Z}$.

Definition

- $R \subseteq G$ (or $\subseteq G^n$) is *e-definable in* G if "$g \in R$" can be expressed as a system over G:

$$g \in R \;\Leftrightarrow\; \exists \vec{y}\; S(g, \vec{y}) = 1.$$

- An operation $\odot$ in R is *e-definable* in G if "$\vec{z} = \vec{x} \odot \vec{y}$," can be expressed as a system over G.

Definable and interpretable structures

Definition

- A ring $(R, +, \cdot)$ (or a structure) is *e-definable in G* if $R \subseteq G^n$, and $R, +, \cdot$ are e-definable in G.

Definable and interpretable structures

Definition

- A ring $(R, +, \cdot)$ (or a structure) is *e-definable in G* if $R \subseteq G^n$, and $R, +, \cdot$ are e-definable in G.
- If $(R, +, \cdot)$ is e-definable in G up to an e-definable equivalence relation, then $(R, +, \cdot)$ is *e-interpretable* in G.

Definable and interpretable structures

Definition

- A ring $(R, +, \cdot)$ (or a structure) is *e-definable in G* if $R \subseteq G^n$, and $R, +, \cdot$ are e-definable in G.
- If $(R, +, \cdot)$ is e-definable in G up to an e-definable equivalence relation, then $(R, +, \cdot)$ is *e-interpretable* in G.

In both cases:

- $\mathscr{D}(R, +, \cdot)$ is reducible to $\mathscr{D}(G)$.

Definable and interpretable structures

Definition

- A ring $(R, +, \cdot)$ (or a structure) is *e-definable in G* if $R \subseteq G^n$, and $R, +, \cdot$ are e-definable in G.
- If $(R, +, \cdot)$ is e-definable in G up to an e-definable equivalence relation, then $(R, +, \cdot)$ is *e-interpretable* in G.

In both cases:

- $\mathscr{D}(R, +, \cdot)$ is reducible to $\mathscr{D}(G)$.
- If $R = \mathbb{Z}$, then $\mathscr{D}(G)$ is undecidable, by the negative answer to Hilbert's 10th problem.

Rings of algebraic integers

Theorem (G., Miasnikov, Ovchinnikov)

Let G be a f.g. non-virtually abelian nilpotent group. Then there exists a ring of algebraic integers O that is e-interpretable in G.

Rings of algebraic integers

Theorem (G., Miasnikov, Ovchinnikov)

Let G be a f.g. non-virtually abelian nilpotent group. Then there exists a ring of algebraic integers O that is e-interpretable in G.

- *Generalized Hilbert's 10th problem*: Determine whether $\mathscr{D}(O)$ is decidable. It is conjectured it is not. Open problem in number theory.

Rings of algebraic integers

Theorem (G., Miasnikov, Ovchinnikov)

Let G be a f.g. non-virtually abelian nilpotent group. Then there exists a ring of algebraic integers O that is e-interpretable in G.

- *Generalized Hilbert's 10th problem*: Determine whether $\mathscr{D}(O)$ is decidable. It is conjectured it is not. Open problem in number theory.

Conjecture

$\mathscr{D}(G)$ is undecidable for any f.g. non-virtually abelian nilpotent group G.

Where does the ring $\mathcal{O}$ come from?

- The following is a bilinear map between abelian groups:

$$\begin{aligned}[\cdot,\cdot] : G/G' \times G/G' &\to G'/G_3 \\ [gG', hG'] &\mapsto [g,h]G_3\end{aligned}$$

Where does the ring $\mathcal{O}$ come from?

- The following is a bilinear map between abelian groups:

$$\begin{aligned} [\cdot,\cdot] : G/G' \times G/G' &\rightarrow G'/G_3 \\ [gG', hG'] &\mapsto [g,h]G_3 \end{aligned}$$

- The set of endomorphisms $End(A)$ of an abelian group A, with the operations $+$ and $\circ$, forms a non-commutative ring.

Where does the ring $\mathcal{O}$ come from?

- The following is a bilinear map between abelian groups:

$$\begin{aligned}[\cdot,\cdot] : G/G' \times G/G' &\to G'/G_3 \\ [gG', hG'] &\mapsto [g,h]G_3\end{aligned}$$

- The set of endomorphisms $End(A)$ of an abelian group A, with the operations $+$ and $\circ$, forms a non-commutative ring.
- $\mathcal{O}$ is constructed using subrings of $End(G/G')$ and $End(G'/G_3)$.

Where does the ring $\mathcal{O}$ come from?

- $[\cdot,\cdot] : G/G' \times G/G' \to G'/G_3$, $[gG', hG'] \mapsto [g,h]G_3$.

Where does the ring $\mathcal{O}$ come from?

- $[\cdot,\cdot] : G/G' \times G/G' \to G'/G_3$, $[gG', hG'] \mapsto [g,h]G_3$.
- One finds a certain subring R of both $End(G/G')$ and $End(G'/G_3)$. It is called the *maximal ring of scalars of* $[\cdot,\cdot]$.

Where does the ring $\mathcal{O}$ come from?

- $[\cdot,\cdot] : G/G' \times G/G' \to G'/G_3$, $[gG', hG'] \mapsto [g,h]G_3$.
- One finds a certain subring R of both $End(G/G')$ and $End(G'/G_3)$. It is called the *maximal ring of scalars of* $[\cdot,\cdot]$.

Definition

A *ring of scalars* of a bilinear map $f : N \times N \to M$ between abelian groups is an integral domain R such that:

Where does the ring $\mathcal{O}$ come from?

- $[\cdot,\cdot] : G/G' \times G/G' \to G'/G_3$, $[gG', hG'] \mapsto [g,h]G_3$.
- One finds a certain subring R of both $End(G/G')$ and $End(G'/G_3)$. It is called the *maximal ring of scalars of* $[\cdot,\cdot]$.

Definition

A *ring of scalars* of a bilinear map $f : N \times N \to M$ between abelian groups is an integral domain R such that:

- R embeds in $End(N)$ and in $End(M)$.

Where does the ring $\mathcal{O}$ come from?

- $[\cdot,\cdot] : G/G' \times G/G' \to G'/G_3$, $[gG', hG'] \mapsto [g,h]G_3$.
- One finds a certain subring R of both $End(G/G')$ and $End(G'/G_3)$. It is called the *maximal ring of scalars of* $[\cdot,\cdot]$.

Definition

A *ring of scalars* of a bilinear map $f : N \times N \to M$ between abelian groups is an integral domain R such that:

- R embeds in $End(N)$ and in $End(M)$.
- $f(\alpha x, y) = f(x, \alpha y) = \alpha f(x,y)$ for all $x, y \in N$, $\alpha \in R$.

Where does the ring $\mathcal{O}$ come from?

- $[\cdot,\cdot] : G/G' \times G/G' \to G'/G_3$, $[gG', hG'] \mapsto [g,h]G_3$.
- One finds a certain subring R of both $End(G/G')$ and $End(G'/G_3)$. It is called the *maximal ring of scalars of* $[\cdot,\cdot]$.

Definition

A *ring of scalars* of a bilinear map $f : N \times N \to M$ between abelian groups is an integral domain R such that:

- R embeds in $End(N)$ and in $End(M)$.
- $f(\alpha x, y) = f(x, \alpha y) = \alpha f(x,y)$ for all $x, y \in N$, $\alpha \in R$.

- $\mathbb{Z}$ is always a ring of scalars of f.

Where does the ring $\mathcal{O}$ come from?

- $[\cdot,\cdot] : G/G' \times G/G' \to G'/G_3$, $[gG', hG'] \mapsto [g,h]G_3$.
- One finds a certain subring R of both $End(G/G')$ and $End(G'/G_3)$. It is called the *maximal ring of scalars of* $[\cdot,\cdot]$.

Definition

A *ring of scalars* of a bilinear map $f : N \times N \to M$ between abelian groups is an integral domain R such that:

- R embeds in $End(N)$ and in $End(M)$.
- $f(\alpha x, y) = f(x, \alpha y) = \alpha f(x,y)$ for all $x, y \in N$, $\alpha \in R$.

- $\mathbb{Z}$ is always a ring of scalars of f.
- $\mathscr{O}$ is constructed using R.

Applications

- Groups where one can e-interpret a f.g. non-virtually abelian nilpotent group.

Applications

- Groups where one can e-interpret a f.g. non-virtually abelian nilpotent group.
- Example: F.g. metabelian groups G such that G/G_3 is non-virtually abelian.

Applications

- Groups where one can e-interpret a f.g. non-virtually abelian nilpotent group.
- Example: F.g. metabelian groups G such that G/G_3 is non-virtually abelian.
- Groups G that satisfy one of the following equivalent conditions:

Applications

- Groups where one can e-interpret a f.g. non-virtually abelian nilpotent group.
- Example: F.g. metabelian groups G such that G/G_3 is non-virtually abelian.
- Groups G that satisfy one of the following equivalent conditions:
    - Any set of nilpotent subgroups of class c has a maximal element.

Applications

- Groups where one can e-interpret a f.g. non-virtually abelian nilpotent group.
- Example: F.g. metabelian groups G such that G/G_3 is non-virtually abelian.
- Groups G that satisfy one of the following equivalent conditions:
  - Any set of nilpotent subgroups of class c has a maximal element.
  - All abelian subgroups are finitely generated.

Applications

- Groups where one can e-interpret a f.g. non-virtually abelian nilpotent group.
- Example: F.g. metabelian groups G such that G/G_3 is non-virtually abelian.
- Groups G that satisfy one of the following equivalent conditions:
  - Any set of nilpotent subgroups of class c has a maximal element.
  - All abelian subgroups are finitely generated.
  - All solvable subgroups are polycyclic.

Applications

- Groups where one can e-interpret a f.g. non-virtually abelian nilpotent group.
- Example: F.g. metabelian groups G such that G/G_3 is non-virtually abelian.
- Groups G that satisfy one of the following equivalent conditions:
  - Any set of nilpotent subgroups of class c has a maximal element.
  - All abelian subgroups are finitely generated.
  - All solvable subgroups are polycyclic.

  Additionally, G must contain a f.g. non-virtually abelian nilpotent group,

Applications

- Groups where one can e-interpret a f.g. non-virtually abelian nilpotent group.
- Example: F.g. metabelian groups G such that G/G_3 is non-virtually abelian.
- Groups G that satisfy one of the following equivalent conditions:
  - Any set of nilpotent subgroups of class c has a maximal element.
  - All abelian subgroups are finitely generated.
  - All solvable subgroups are polycyclic.

  Additionally, G must contain a f.g. non-virtually abelian nilpotent group,
- Examples: Subgroups of $GL(n, K)$ for K a ring of algebraic integers. Discrete solvable subgroups of $GL(n, \mathbb{R})$.

Grazie per l'attenzione!

Mila esker!

CS