Topological methods to solve equations over groups

Andreas Thom
TU Dresden, Germany

July 26, 2016 in Buenos Aires
XXI Coloquio Latinoamericano de Álgebra

How to solve a polynomial equation?

How to solve a polynomial equation?

Even though not every non-constant polynomial $p(t) \in \mathbb{Q}[t]$ has a root in $\mathbb{Q}$, there always exists a finite field extension $\mathbb{Q} \subset K$, such that $p(t) = 0$ can be solved in K,

How to solve a polynomial equation?

Even though not every non-constant polynomial $p(t) \in \mathbb{Q}[t]$ has a root in $\mathbb{Q}$, there always exists a finite field extension $\mathbb{Q} \subset K$, such that $p(t) = 0$ can be solved in K, i.e., there exists $\alpha \in K$ with $p(\alpha) = 0$.

How to solve a polynomial equation?

Even though not every non-constant polynomial $p(t) \in \mathbb{Q}[t]$ has a root in $\mathbb{Q}$, there always exists a finite field extension $\mathbb{Q} \subset K$, such that $p(t) = 0$ can be solved in K, i.e., there exists $\alpha \in K$ with $p(\alpha) = 0$.

1. Consider a simple quotient $\mathbb{Q}[t]/\langle p(t)\rangle \twoheadrightarrow K$ and and convince yourself that $\mathbb{Q} \subset K$. The image α of t will solve the equation $p(t) = 0$ in K.

How to solve a polynomial equation?

Even though not every non-constant polynomial $p(t) \in \mathbb{Q}[t]$ has a root in $\mathbb{Q}$, there always exists a finite field extension $\mathbb{Q} \subset K$, such that $p(t) = 0$ can be solved in K, i.e., there exists $\alpha \in K$ with $p(\alpha) = 0$.

1. Consider a simple quotient $\mathbb{Q}[t]/\langle p(t) \rangle \twoheadrightarrow K$ and and convince yourself that $\mathbb{Q} \subset K$. The image α of t will solve the equation $p(t) = 0$ in K.
2. Embed $\mathbb{Q} \subset \mathbb{C}$, study the continuous map $p\colon \mathbb{C} \to \mathbb{C}$, and use a topological argument to see that there exists $\alpha \in \mathbb{C}$, such that $p(\alpha) = 0$.

How to solve a polynomial equation?

Even though not every non-constant polynomial $p(t) \in \mathbb{Q}[t]$ has a root in $\mathbb{Q}$, there always exists a finite field extension $\mathbb{Q} \subset K$, such that $p(t) = 0$ can be solved in K, i.e., there exists $\alpha \in K$ with $p(\alpha) = 0$.

1. Consider a simple quotient $\mathbb{Q}[t]/\langle p(t) \rangle \twoheadrightarrow K$ and and convince yourself that $\mathbb{Q} \subset K$. The image α of t will solve the equation $p(t) = 0$ in K.
2. Embed $\mathbb{Q} \subset \mathbb{C}$, study the continuous map $p\colon \mathbb{C} \to \mathbb{C}$, and use a topological argument to see that there exists $\alpha \in \mathbb{C}$, such that $p(\alpha) = 0$.

The second argument was essentially already present in Gauss' first proof in 1799.

How to solve a polynomial equation?

Even though not every non-constant polynomial $p(t) \in \mathbb{Q}[t]$ has a root in $\mathbb{Q}$, there always exists a finite field extension $\mathbb{Q} \subset K$, such that $p(t) = 0$ can be solved in K, i.e., there exists $\alpha \in K$ with $p(\alpha) = 0$.

1. Consider a simple quotient $\mathbb{Q}[t]/\langle p(t) \rangle \twoheadrightarrow K$ and and convince yourself that $\mathbb{Q} \subset K$. The image α of t will solve the equation $p(t) = 0$ in K.
2. Embed $\mathbb{Q} \subset \mathbb{C}$, study the continuous map $p \colon \mathbb{C} \to \mathbb{C}$, and use a topological argument to see that there exists $\alpha \in \mathbb{C}$, such that $p(\alpha) = 0$.

The second argument was essentially already present in Gauss' first proof in 1799. However, the right language was not developed until 1930.

Equations over groups

Equations over groups

Definition

Let Γ be a group and let $g_1, \ldots, g_n \in \Gamma$, $\varepsilon_1, \ldots, \varepsilon_n \in \mathbb{Z}$.

Equations over groups

Definition

Let Γ be a group and let $g_1, \dots, g_n \in \Gamma$, $\varepsilon_1, \dots, \varepsilon_n \in \mathbb{Z}$. We say that the equation

$$w(t) = g_1 t^{\varepsilon_1} g_2 t^{\varepsilon_2} g_3 \dots g_n t^{\varepsilon_n}$$

has a solution **in** Γ if there exists $h \in \Gamma$ such that $w(h) = e$.

Equations over groups

Definition

Let Γ be a group and let $g_1, \ldots, g_n \in \Gamma$, $\varepsilon_1, \ldots, \varepsilon_n \in \mathbb{Z}$. We say that the equation

$$w(t) = g_1 t^{\varepsilon_1} g_2 t^{\varepsilon_2} g_3 \ldots g_n t^{\varepsilon_n}$$

has a solution **in** Γ if there exists $h \in \Gamma$ such that $w(h) = e$.

The equation has a solution **over** Γ if there is an extension $\Gamma \leq \Lambda$ and there is some $h \in \Lambda$ such that $w(h) = e$ in Λ.

Equations over groups

Definition

Let Γ be a group and let $g_1, \ldots, g_n \in \Gamma$, $\varepsilon_1, \ldots, \varepsilon_n \in \mathbb{Z}$. We say that the equation

$$w(t) = g_1 t^{\varepsilon_1} g_2 t^{\varepsilon_2} g_3 \ldots g_n t^{\varepsilon_n}$$

has a solution **in** Γ if there exists $h \in \Gamma$ such that $w(h) = e$.

The equation has a solution **over** Γ if there is an extension $\Gamma \leq \Lambda$ and there is some $h \in \Lambda$ such that $w(h) = e$ in Λ.

The study of equations like this goes back to:

Bernhard H. Neumann, *Adjunction of elements to groups*, J. London Math. Soc. 18 (1943), 411.

Example

If $a, b \in \Gamma$, then $w(t) = atbt^{-1}$ cannot be solved over Γ unless the orders of a and b agree.

Example

If $a, b \in \Gamma$, then $w(t) = atbt^{-1}$ cannot be solved over Γ unless the orders of a and b agree.

Indeed, if such a t exists, then

$$a^{-1} = tbt^{-1}.$$

Example

If $a, b \in \Gamma$, then $w(t) = atbt^{-1}$ cannot be solved over Γ unless the orders of a and b agree.

Indeed, if such a t exists, then

$$a^{-1} = tbt^{-1}.$$

Example

The equation $w(t) = tat^{-1}ata^{-1}t^{-1}a^{-2}$ cannot be solved over $\mathbb{Z}/p\mathbb{Z} = \langle a \rangle$.

Example

If $a, b \in \Gamma$, then $w(t) = atbt^{-1}$ cannot be solved over Γ unless the orders of a and b agree.

Indeed, if such a t exists, then

$$a^{-1} = tbt^{-1}.$$

Example

The equation $w(t) = tat^{-1}ata^{-1}t^{-1}a^{-2}$ cannot be solved over $\mathbb{Z}/p\mathbb{Z} = \langle a \rangle$.

Indeed, if $w(t) = 1$, then

$$a^2 = (tat^{-1})a(tat^{-1})^{-1}$$

and a conjugate of a (namely tat^{-1}) would conjugate a to a^2.

Example

If $a, b \in \Gamma$, then $w(t) = atbt^{-1}$ cannot be solved over Γ unless the orders of a and b agree.

Indeed, if such a t exists, then

$$a^{-1} = tbt^{-1}.$$

Example

The equation $w(t) = tat^{-1}ata^{-1}t^{-1}a^{-2}$ cannot be solved over $\mathbb{Z}/p\mathbb{Z} = \langle a \rangle$.

Indeed, if $w(t) = 1$, then

$$a^2 = (tat^{-1})a(tat^{-1})^{-1}$$

and a conjugate of a (namely tat^{-1}) would conjugate a to a^2. But the automorphism of $\mathbb{Z}/p\mathbb{Z}$ which sends 1 to 2 has order dividing $p-1$ and hence the order is co-prime to p.

Definition

We say that the equation $w(t) = g_1 t^{\varepsilon_1} g_2 t^{\varepsilon_2} g_3 \ldots g_n t^{\varepsilon_n}$ is non-singular if $\sum_{i=1}^{n} \varepsilon_i \neq 0$.

Definition

We say that the equation $w(t) = g_1 t^{\varepsilon_1} g_2 t^{\varepsilon_2} g_3 \dots g_n t^{\varepsilon_n}$ is non-singular if $\sum_{i=1}^{n} \varepsilon_i \neq 0$. It is called non-trivial if it is not conjugate to $w(t) = g \neq 1$.

Definition

We say that the equation $w(t) = g_1 t^{\varepsilon_1} g_2 t^{\varepsilon_2} g_3 \dots g_n t^{\varepsilon_n}$ is non-singular if $\sum_{i=1}^{n} \varepsilon_i \neq 0$. It is called non-trivial if it is not conjugate to $w(t) = g \neq 1$.

Conjecture (Levin)

Any non-trivial equation can be solved over Γ, if Γ is torsionfree.

Definition

We say that the equation $w(t) = g_1 t^{\varepsilon_1} g_2 t^{\varepsilon_2} g_3 \ldots g_n t^{\varepsilon_n}$ is non-singular if $\sum_{i=1}^{n} \varepsilon_i \neq 0$. It is called non-trivial if it is not conjugate to $w(t) = g \neq 1$.

Conjecture (Levin)

Any non-trivial equation can be solved over Γ, if Γ is torsionfree.

Conjecture (Kervaire-Laudenbach)

If $w(t)$ is non-singular, then $w(t)$ has a solution over Γ.

Definition

We say that the equation $w(t) = g_1 t^{\varepsilon_1} g_2 t^{\varepsilon_2} g_3 \dots g_n t^{\varepsilon_n}$ is non-singular if $\sum_{i=1}^{n} \varepsilon_i \neq 0$. It is called non-trivial if it is not conjugate to $w(t) = g \neq 1$.

Conjecture (Levin)

Any non-trivial equation can be solved over Γ, if Γ is torsionfree.

Conjecture (Kervaire-Laudenbach)

If $w(t)$ is non-singular, then $w(t)$ has a solution over Γ.

Theorem (Klyachko)

If Γ is torsionfree **and** *$w(t)$ is non-singular, then $w(t)$ can be solved over Γ.*

Anton A. Klyachko, *A funny property of sphere and equations over groups*, Comm. Algebra 21 (1993), no. 7, 2555–2575.

Definition

We say that the equation $w(t) = g_1 t^{\varepsilon_1} g_2 t^{\varepsilon_2} g_3 \ldots g_n t^{\varepsilon_n}$ is non-singular if $\sum_{i=1}^{n} \varepsilon_i \neq 0$. It is called non-trivial if it is not conjugate to $w(t) = g \neq 1$.

Conjecture (Levin)

Any non-trivial equation can be solved over Γ, if Γ is torsionfree.

Conjecture (Kervaire-Laudenbach)

If $w(t)$ is non-singular, then $w(t)$ has a solution over Γ.

Theorem (Klyachko)

If Γ is torsionfree **and** *$w(t)$ is non-singular, then $w(t)$ can be solved over Γ.*

Anton A. Klyachko, *A funny property of sphere and equations over groups*, Comm. Algebra 21 (1993), no. 7, 2555–2575.

We will focus on the second conjecture.

The algebraic/combinatorial approach

Why is this complicated?

The algebraic/combinatorial approach

Why is this complicated? Just consider:

$$\Gamma \to \frac{\Gamma * \langle t \rangle}{\langle\langle w(t) \rangle\rangle}.$$

The algebraic/combinatorial approach

Why is this complicated? Just consider:

$$\Gamma \to \frac{\Gamma * \langle t \rangle}{\langle\langle w(t) \rangle\rangle}.$$

But nobody can show easily that this homomorphism is injective.

The algebraic/combinatorial approach

Why is this complicated? Just consider:

$$\Gamma \to \frac{\Gamma * \langle t \rangle}{\langle\langle w(t) \rangle\rangle}.$$

But nobody can show easily that this homomorphism is injective. In fact, injectivity is equivalent to existence of a solution over Γ.

The algebraic/combinatorial approach

Why is this complicated? Just consider:

$$\Gamma \to \frac{\Gamma * \langle t \rangle}{\langle\langle w(t) \rangle\rangle}.$$

But nobody can show easily that this homomorphism is injective. In fact, injectivity is equivalent to existence of a solution over Γ.

The Kervaire-Laudenbach conjecture was motivated originally from 3-dimensional topology, where certain geometric operations on knot complements amount to the attachment of an "arc" and a "disc".

The algebraic/combinatorial approach

Why is this complicated? Just consider:

$$\Gamma \to \frac{\Gamma * \langle t \rangle}{\langle\langle w(t) \rangle\rangle}.$$

But nobody can show easily that this homomorphism is injective. In fact, injectivity is equivalent to existence of a solution over Γ.

The Kervaire-Laudenbach conjecture was motivated originally from 3-dimensional topology, where certain geometric operations on knot complements amount to the attachment of an "arc" and a "disc".

The resulting effect on fundamental groups is exactly

$$\Gamma \rightsquigarrow \frac{\Gamma * \langle t \rangle}{\langle\langle w(t) \rangle\rangle}.$$

Topological methods

Theorem (Gerstenhaber-Rothaus, 1962)

Any non-singular equation in $U(n)$ can be solved in $U(n)$.

Topological methods

Theorem (Gerstenhaber-Rothaus, 1962)

Any non-singular equation in $U(n)$ can be solved in $U(n)$.

Proof.

Consider the word map $w\colon U(n) \to U(n)$, $w(t) = g_1 t^{\varepsilon_1} \dots g_n t^{\varepsilon_n}$.

Topological methods

Theorem (Gerstenhaber-Rothaus, 1962)

Any non-singular equation in $U(n)$ can be solved in $U(n)$.

Proof.

Consider the word map $w\colon U(n) \to U(n)$, $w(t) = g_1 t^{\varepsilon_1} \dots g_n t^{\varepsilon_n}$.
Since $U(n)$ is connected, each g_i can be moved continuously to 1_n.

Topological methods

Theorem (Gerstenhaber-Rothaus, 1962)

Any non-singular equation in $U(n)$ can be solved in $U(n)$.

Proof.

Consider the word map $w\colon U(n) \to U(n)$, $w(t) = g_1 t^{\varepsilon_1} \dots g_n t^{\varepsilon_n}$.
Since $U(n)$ is connected, each g_i can be moved continuously to 1_n.
Thus, this map is homotopic to $t \mapsto t^{\sum_i \varepsilon_i}$,

Topological methods

Theorem (Gerstenhaber-Rothaus, 1962)

Any non-singular equation in $U(n)$ can be solved in $U(n)$.

Proof.

Consider the word map $w\colon U(n) \to U(n)$, $w(t) = g_1 t^{\varepsilon_1} \dots g_n t^{\varepsilon_n}$. Since $U(n)$ is connected, each g_i can be moved continuously to 1_n. Thus, this map is homotopic to $t \mapsto t^{\sum_i \varepsilon_i}$, which has non-trivial degree as a map of topological manifolds.

Topological methods

Theorem (Gerstenhaber-Rothaus, 1962)

Any non-singular equation in $U(n)$ can be solved in $U(n)$.

Proof.

Consider the word map $w\colon U(n) \to U(n)$, $w(t) = g_1 t^{\varepsilon_1} \dots g_n t^{\varepsilon_n}$. Since $U(n)$ is connected, each g_i can be moved continuously to 1_n. Thus, this map is homotopic to $t \mapsto t^{\sum_i \varepsilon_i}$, which has non-trivial degree as a map of topological manifolds. Indeed, a generic matrix has exactly d^n preimages with $d := |\sum_i \varepsilon_i|$.

Topological methods

Theorem (Gerstenhaber-Rothaus, 1962)

Any non-singular equation in $U(n)$ can be solved in $U(n)$.

Proof.

Consider the word map $w\colon U(n) \to U(n)$, $w(t) = g_1 t^{\varepsilon_1} \dots g_n t^{\varepsilon_n}$. Since $U(n)$ is connected, each g_i can be moved continuously to 1_n. Thus, this map is homotopic to $t \mapsto t^{\sum_i \varepsilon_i}$, which has non-trivial degree as a map of topological manifolds. Indeed, a generic matrix has exactly d^n preimages with $d := |\sum_i \varepsilon_i|$. Hence, the map w must be surjective.

Topological methods

Theorem (Gerstenhaber-Rothaus, 1962)

Any non-singular equation in $U(n)$ can be solved in $U(n)$.

Proof.

Consider the word map $w\colon U(n) \to U(n)$, $w(t) = g_1 t^{\varepsilon_1} \dots g_n t^{\varepsilon_n}$. Since $U(n)$ is connected, each g_i can be moved continuously to 1_n. Thus, this map is homotopic to $t \mapsto t^{\sum_i \varepsilon_i}$, which has non-trivial degree as a map of topological manifolds. Indeed, a generic matrix has exactly d^n preimages with $d := |\sum_i \varepsilon_i|$. Hence, the map w must be surjective. Each pre-image of 1_n gives a solution of the equation $w(t) = 1_n$. □

Corollary

Any non-singular equation with coefficients in a finite group Γ can be solved over Γ.

Corollary

Any non-singular equation with coefficients in a finite group Γ can be solved over Γ. In fact, they can be solved in a finite extension $\Gamma \leq \Lambda$.

Corollary

Any non-singular equation with coefficients in a finite group Γ can be solved over Γ. In fact, they can be solved in a finite extension $\Gamma \leq \Lambda$.

Proof.

Embed Γ in $U(n)$, solve the equation there to get a solution u.

Corollary

Any non-singular equation with coefficients in a finite group Γ can be solved over Γ. In fact, they can be solved in a finite extension $\Gamma \leq \Lambda$.

Proof.

Embed Γ in $U(n)$, solve the equation there to get a solution u. Now, $\Lambda = \langle \Gamma, u \rangle \subset U(n)$ is residually finite my Mal'cev's theorem. Thus, there exists a finite quotient of Λ which contains Γ. □

Corollary

Any non-singular equation with coefficients in a finite group Γ can be solved over Γ. In fact, they can be solved in a finite extension $\Gamma \leq \Lambda$.

Proof.

Embed Γ in $U(n)$, solve the equation there to get a solution u. Now, $\Lambda = \langle \Gamma, u \rangle \subset U(n)$ is residually finite my Mal'cev's theorem. Thus, there exists a finite quotient of Λ which contains Γ. □

The same holds for locally residually finite groups, but the general situation remained unclear back in the 60s.

Corollary

Any non-singular equation with coefficients in a finite group Γ *can be solved over* Γ*. In fact, they can be solved in a finite extension* $\Gamma \leq \Lambda$*.*

Proof.

Embed Γ in $U(n)$, solve the equation there to get a solution u. Now, $\Lambda = \langle \Gamma, u \rangle \subset U(n)$ is residually finite my Mal'cev's theorem. Thus, there exists a finite quotient of Λ which contains Γ. □

The same holds for locally residually finite groups, but the general situation remained unclear back in the 60s.

Definition

We say that Γ is algebraically closed if any non-singular equation has a solution in Γ.

Definition

We say that Γ is algebraically closed if any non-singular equation has a solution in Γ.

Proposition

The class of algebraically closed groups is closed under products and quotients.

Definition

We say that Γ is algebraically closed if any non-singular equation has a solution in Γ.

Proposition

The class of algebraically closed groups is closed under products and quotients.

Corollary (Pestov)

Any group Γ that embeds into an abstract quotient of $\prod_n U(n)$ (these are called **hyperlinear***) satisfies Kervaire's Conjecture.*

Definition

We say that Γ is algebraically closed if any non-singular equation has a solution in Γ.

Proposition

The class of algebraically closed groups is closed under products and quotients.

Corollary (Pestov)

Any group Γ that embeds into an abstract quotient of $\prod_n U(n)$ (these are called **hyperlinear***) satisfies Kervaire's Conjecture.*

Remark

Every **sofic** *group can be embedded into a quotient of $\prod_n U(n)$.*

Sofic groups – Definition

Let $\mathrm{Sym}(n)$ be the permutation group on n letters. We set:

$$d(\sigma, \tau) = \frac{1}{n} \cdot |\{i \in \{0, ..., n\} \mid \sigma(i) \neq \tau(i)\}|$$

to be the normalized Hamming distance on permutations $\sigma, \tau \in \mathrm{Sym}(n)$.

Sofic groups – Definition

Let $\mathrm{Sym}(n)$ be the permutation group on n letters. We set:

$$d(\sigma, \tau) = \frac{1}{n} \cdot |\{i \in \{0, ..., n\} \mid \sigma(i) \neq \tau(i)\}|$$

to be the normalized Hamming distance on permutations $\sigma, \tau \in \mathrm{Sym}(n)$.

Definition

A group Γ is called **sofic**, if for every finite subset $F \subset \Gamma$ and every $\epsilon \in (0, 1)$ there exists $n \in \mathbb{N}$ and a map $\phi \colon \Gamma \to \mathrm{Sym}(n)$, such that:

Sofic groups – Definition

Let $\mathrm{Sym}(n)$ be the permutation group on n letters. We set:

$$d(\sigma, \tau) = \frac{1}{n} \cdot |\{i \in \{0, ..., n\} \mid \sigma(i) \neq \tau(i)\}|$$

to be the normalized Hamming distance on permutations $\sigma, \tau \in \mathrm{Sym}(n)$.

Definition

A group Γ is called **sofic**, if for every finite subset $F \subset \Gamma$ and every $\epsilon \in (0, 1)$ there exists $n \in \mathbb{N}$ and a map $\phi\colon \Gamma \to \mathrm{Sym}(n)$, such that:

1. $d(\phi(gh), \phi(g)\phi(h)) \leq \epsilon, \quad \forall g, h \in F$,

Sofic groups – Definition

Let $\mathrm{Sym}(n)$ be the permutation group on n letters. We set:

$$d(\sigma, \tau) = \frac{1}{n} \cdot |\{i \in \{0, ..., n\} \mid \sigma(i) \neq \tau(i)\}|$$

to be the normalized Hamming distance on permutations $\sigma, \tau \in \mathrm{Sym}(n)$.

Definition

A group Γ is called **sofic**, if for every finite subset $F \subset \Gamma$ and every $\epsilon \in (0, 1)$ there exists $n \in \mathbb{N}$ and a map $\phi \colon \Gamma \to \mathrm{Sym}(n)$, such that:

1. $d(\phi(gh), \phi(g)\phi(h)) \leq \epsilon, \quad \forall g, h \in F$,
2. $d(1_n, \phi(g)) \geq 1/2, \qquad \forall g \in F \setminus \{e\}$.

Sofic groups – Examples

Examples of sofic groups:

- residually finite groups,

Sofic groups – Examples

Examples of sofic groups:

- residually finite groups,
  - free groups are residually finite,
  - Theorem (Mal'cev): Every finitely generated subgroup of $GL_n\mathbb{C}$ is residually finite.

Sofic groups – Examples

Examples of sofic groups:

- residually finite groups,
  - free groups are residually finite,
  - Theorem (Mal'cev): Every finitely generated subgroup of $GL_n\mathbb{C}$ is residually finite.
- amenable groups,

Sofic groups – Examples

Examples of sofic groups:

- residually finite groups,
  - free groups are residually finite,
  - Theorem (Mal'cev): Every finitely generated subgroup of $GL_n\mathbb{C}$ is residually finite.
- amenable groups,
- inverse and direct limits of sofic groups,

Sofic groups – Examples

Examples of sofic groups:

- residually finite groups,
  - free groups are residually finite,
  - Theorem (Mal'cev): Every finitely generated subgroup of $GL_n\mathbb{C}$ is residually finite.
- amenable groups,
- inverse and direct limits of sofic groups,
- free and direct products of sofic groups,

Sofic groups – Examples

Examples of sofic groups:

- residually finite groups,
  - free groups are residually finite,
  - Theorem (Mal'cev): Every finitely generated subgroup of $GL_n\mathbb{C}$ is residually finite.
- amenable groups,
- inverse and direct limits of sofic groups,
- free and direct products of sofic groups,
- subgroups of sofic groups,

Sofic groups – Examples

Examples of sofic groups:

- residually finite groups,
  - free groups are residually finite,
  - Theorem (Mal'cev): Every finitely generated subgroup of $GL_n\mathbb{C}$ is residually finite.
- amenable groups,
- inverse and direct limits of sofic groups,
- free and direct products of sofic groups,
- subgroups of sofic groups,
- extension with sofic normal subgroup and amenable quotient.

Sofic groups – Examples

Examples of sofic groups:

- residually finite groups,
  - free groups are residually finite,
  - Theorem (Mal'cev): Every finitely generated subgroup of $GL_n\mathbb{C}$ is residually finite.
- amenable groups,
- inverse and direct limits of sofic groups,
- free and direct products of sofic groups,
- subgroups of sofic groups,
- extension with sofic normal subgroup and amenable quotient.

Remark

There is no group known to be non-sofic.

Now, $\mathrm{Sym}(n) \subset U(n)$ and one easily sees that a sofic group Γ is a subgroup of the quotient group

$$\frac{\prod_n U(n)}{N},$$

Now, $\mathrm{Sym}(n) \subset U(n)$ and one easily sees that a sofic group Γ is a subgroup of the quotient group

$$\frac{\prod_n U(n)}{N},$$

where

$$N = \left\{ (u_n)_n \in \prod_n U(n) \mid \lim_{n \to \omega} \frac{1}{n} \sum_{i,j=1}^{n} |\delta_{ij} - u_{ij}|^2 = 0 \right\}$$

for some suitable ultrafilter $\omega \in \beta\mathbb{N}$.

Now, $\mathrm{Sym}(n) \subset U(n)$ and one easily sees that a sofic group Γ is a subgroup of the quotient group

$$\frac{\prod_n U(n)}{N},$$

where

$$N = \left\{ (u_n)_n \in \prod_n U(n) \mid \lim_{n \to \omega} \frac{1}{n} \sum_{i,j=1}^{n} |\delta_{ij} - u_{ij}|^2 = 0 \right\}$$

for some suitable ultrafilter $\omega \in \beta\mathbb{N}$.

Remark

Connes' Embedding Conjecture also implies that every group has such an embedding.

More "Magical realism" with sofic groups

More "Magical realism" with sofic groups

... uses fantastical and unreal elements. Miracles happen naturally.

More "Magical realism" with sofic groups

... uses fantastical and unreal elements. Miracles happen naturally.

Conjecture (Kaplansky)

Let Γ be a group and k be a field. If $a, b \in k\Gamma$ satisfy $ab = 1$, then also $ba = 1$.

More "Magical realism" with sofic groups

... uses fantastical and unreal elements. Miracles happen naturally.

Conjecture (Kaplansky)

Let Γ be a group and k be a field. If $a, b \in k\Gamma$ satisfy $ab = 1$, then also $ba = 1$.

- Known to hold if $\mathrm{char}(k) = 0$.

More "Magical realism" with sofic groups

... uses fantastical and unreal elements. Miracles happen naturally.

Conjecture (Kaplansky)

Let Γ *be a group and* k *be a field. If* $a, b \in k\Gamma$ *satisfy* $ab = 1$*, then also* $ba = 1$*.*

- Known to hold if $\mathrm{char}(k) = 0$.
- Known for any field if Γ is sofic. (Elek-Szabo)

More "Magical realism" with sofic groups

... uses fantastical and unreal elements. Miracles happen naturally.

Conjecture (Kaplansky)

Let Γ be a group and k be a field. If $a, b \in k\Gamma$ satisfy $ab = 1$, then also $ba = 1$.

- Known to hold if $\mathrm{char}(k) = 0$.
- Known for any field if Γ is sofic. (Elek-Szabo)

Idea: If Γ can be modelled by permutations, then $k\Gamma$ can be modelled by $M_n(k)$. Hence, $ab = 1$ implies $ba = 1$.

More variables

More variables

Question

Can you solve the equation

$$w(s,t) = g_1 s g_2 t g_3 s^{-1} g_4 t^{-1} = 1$$

over some group?

More variables

Question

Can you solve the equation

$$w(s,t) = g_1 s g_2 t g_3 s^{-1} g_4 t^{-1} = 1$$

over some group?

Consider the augmentation $\varepsilon\colon \Gamma * \mathbb{F}_n \to \mathbb{F}_n$. An equation $w \in \Gamma * \mathbb{F}_n$ is non-singular, if $\varepsilon(w) \neq 1$.

More variables

Question

Can you solve the equation

$$w(s,t) = g_1 s g_2 t g_3 s^{-1} g_4 t^{-1} = 1$$

over some group?

Consider the augmentation $\varepsilon\colon \Gamma * \mathbb{F}_n \to \mathbb{F}_n$. An equation $w \in \Gamma * \mathbb{F}_n$ is non-singular, if $\varepsilon(w) \neq 1$.

Conjecture

If $w \in \Gamma * \mathbb{F}_n$ is non-singular, then w has a solution over Γ.

More variables

Question

Can you solve the equation

$$w(s,t) = g_1 s g_2 t g_3 s^{-1} g_4 t^{-1} = 1$$

over some group?

Consider the augmentation $\varepsilon\colon \Gamma * \mathbb{F}_n \to \mathbb{F}_n$. An equation $w \in \Gamma * \mathbb{F}_n$ is non-singular, if $\varepsilon(w) \neq 1$.

Conjecture

If $w \in \Gamma * \mathbb{F}_n$ is non-singular, then w has a solution over Γ.

Theorem (with Anton Klyachko)

If $w \in \Gamma * \mathbb{F}_2$ satisfies $\varepsilon(w) \notin [[\mathbb{F}_2, \mathbb{F}_2], \mathbb{F}_2]$ and Γ is hyperlinear, then w has a solution over Γ.

Theorem (with Klyachko)

Let p be prime. Any $w \in SU(p) * \mathbb{F}_2$ with $\varepsilon(w) \notin \mathbb{F}_2^p[[\mathbb{F}_2, \mathbb{F}_2], \mathbb{F}_2]$ can be solved in $SU(p)$.

Theorem (with Klyachko)

Let p be prime. Any $w \in SU(p) * \mathbb{F}_2$ *with* $\varepsilon(w) \notin \mathbb{F}_2^p[[\mathbb{F}_2, \mathbb{F}_2], \mathbb{F}_2]$ *can be solved in* $SU(p)$*.*

Instead of degree theory, we are making use of the cohomology ring of $SU(p)$ and $PU(p)$.

Theorem (with Klyachko)

Let p be prime. Any $w \in SU(p) * \mathbb{F}_2$ with $\varepsilon(w) \notin \mathbb{F}_2^p[[\mathbb{F}_2, \mathbb{F}_2], \mathbb{F}_2]$ can be solved in $SU(p)$.

Instead of degree theory, we are making use of the cohomology ring of $SU(p)$ and $PU(p)$. The key insight is:

1. The commutator map $c\colon PU(p)^{\times 2} \to PU(p)$ lifts to $SU(p)$.

Theorem (with Klyachko)

Let p be prime. Any $w \in SU(p) * \mathbb{F}_2$ with $\varepsilon(w) \notin \mathbb{F}_2^p[[\mathbb{F}_2, \mathbb{F}_2], \mathbb{F}_2]$ can be solved in $SU(p)$.

Instead of degree theory, we are making use of the cohomology ring of $SU(p)$ and $PU(p)$. The key insight is:

1. The commutator map $c\colon PU(p)^{\times 2} \to PU(p)$ lifts to $SU(p)$. (Indeed, the analogous commutator map $c\colon SU(p)^{\times 2} \to SU(p)$ factorized through $PU(p)^{\times 2}$.)

Theorem (with Klyachko)

Let p be prime. Any $w \in SU(p) * \mathbb{F}_2$ with $\varepsilon(w) \notin \mathbb{F}_2^p[[\mathbb{F}_2, \mathbb{F}_2], \mathbb{F}_2]$ can be solved in $SU(p)$.

Instead of degree theory, we are making use of the cohomology ring of $SU(p)$ and $PU(p)$. The key insight is:

1. The commutator map $c \colon PU(p)^{\times 2} \to PU(p)$ lifts to $SU(p)$. (Indeed, the analogous commutator map $c \colon SU(p)^{\times 2} \to SU(p)$ factorized through $PU(p)^{\times 2}$.)
2. The generator of the top-dimensional cohomology group $H^*(SU(p), \mathbb{Z}/p\mathbb{Z})$ is mapped non-trivially to

   $H^*(PU(p)^{\times 2}, \mathbb{Z}/p\mathbb{Z})$

Theorem (with Klyachko)

Let p be prime. Any $w \in SU(p) * \mathbb{F}_2$ with $\varepsilon(w) \notin \mathbb{F}_2^p[[\mathbb{F}_2, \mathbb{F}_2], \mathbb{F}_2]$ can be solved in $SU(p)$.

Instead of degree theory, we are making use of the cohomology ring of $SU(p)$ and $PU(p)$. The key insight is:

1. The commutator map $c\colon PU(p)^{\times 2} \to PU(p)$ lifts to $SU(p)$. (Indeed, the analogous commutator map $c\colon SU(p)^{\times 2} \to SU(p)$ factorized through $PU(p)^{\times 2}$.)
2. The generator of the top-dimensional cohomology group $H^*(SU(p), \mathbb{Z}/p\mathbb{Z})$ is mapped non-trivially to

$$H^*(PU(p)^{\times 2}, \mathbb{Z}/p\mathbb{Z}) \cong H^*(PU(p), \mathbb{Z}/p\mathbb{Z}) \otimes H^*(PU(p), \mathbb{Z}/p\mathbb{Z}).$$

Theorem (with Klyachko)

Let p be prime. Any $w \in SU(p) * \mathbb{F}_2$ with $\varepsilon(w) \notin \mathbb{F}_2^p[[\mathbb{F}_2, \mathbb{F}_2], \mathbb{F}_2]$ can be solved in $SU(p)$.

Instead of degree theory, we are making use of the cohomology ring of $SU(p)$ and $PU(p)$. The key insight is:

1. The commutator map $c\colon PU(p)^{\times 2} \to PU(p)$ lifts to $SU(p)$. (Indeed, the analogous commutator map $c\colon SU(p)^{\times 2} \to SU(p)$ factorized through $PU(p)^{\times 2}$.)
2. The generator of the top-dimensional cohomology group $H^*(SU(p), \mathbb{Z}/p\mathbb{Z})$ is mapped non-trivially to

   $$H^*(PU(p)^{\times 2}, \mathbb{Z}/p\mathbb{Z}) \cong H^*(PU(p), \mathbb{Z}/p\mathbb{Z}) \otimes H^*(PU(p), \mathbb{Z}/p\mathbb{Z}).$$

3. Thus, $c\colon PU(p)^{\times 2} \to SU(p)$ is not homotopic to a non-surjective map.

Theorem (Borel)

$$H^*(SU(n), \mathbb{Z}/p\mathbb{Z}) = \Lambda^*_{\mathbb{Z}/p\mathbb{Z}}(x_2, x_3, \ldots, x_n)$$

with $|x_i| = 2i - 1$ *and*

Theorem (Borel)

$$H^*(SU(n), \mathbb{Z}/p\mathbb{Z}) = \Lambda^*_{\mathbb{Z}/p\mathbb{Z}}(x_2, x_3, \ldots, x_n)$$

with $|x_i| = 2i - 1$ *and*

$$\Delta(x_i) = x_i \otimes 1 + 1 \otimes x_i.$$

Theorem (Baum-Browder)

Let p be an odd prime number. Then,

$$H^*(PU(p), \mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})[y]/(y^p) \otimes_{\mathbb{Z}} \Lambda^*_{\mathbb{Z}/p\mathbb{Z}}(y_1, y_2, \ldots, y_{p-1})$$

with $|y| = 2$, $|y_i| = 2i - 1$.

Theorem (Baum-Browder)

Let p be an odd prime number. Then,

$$H^*(PU(p), \mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})[y]/(y^p) \otimes_{\mathbb{Z}} \Lambda^*_{\mathbb{Z}/p\mathbb{Z}}(y_1, y_2, \ldots, y_{p-1})$$

with $|y| = 2$, $|y_i| = 2i - 1$. *The co-multiplication takes the form*

$$\Delta(y) = y \otimes 1 + 1 \otimes y,$$

and

Theorem (Baum-Browder)

Let p be an odd prime number. Then,

$$H^*(PU(p), \mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})[y]/(y^p) \otimes_{\mathbb{Z}} \Lambda^*_{\mathbb{Z}/p\mathbb{Z}}(y_1, y_2, \ldots, y_{p-1})$$

with $|y| = 2$, $|y_i| = 2i - 1$. *The co-multiplication takes the form*

$$\Delta(y) = y \otimes 1 + 1 \otimes y,$$

and

$$\Delta(y_i) = y_i \otimes 1 + 1 \otimes y_i + \sum_{j=1}^{i-1} \binom{j-1}{i-1} \cdot y_j \otimes y^{i-j}.$$

Theorem (Baum-Browder)

Let p be an odd prime number. Then,

$$H^*(PU(p), \mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})[y]/(y^p) \otimes_{\mathbb{Z}} \Lambda^*_{\mathbb{Z}/p\mathbb{Z}}(y_1, y_2, \ldots, y_{p-1})$$

with $|y| = 2$, $|y_i| = 2i - 1$. *The co-multiplication takes the form*

$$\Delta(y) = y \otimes 1 + 1 \otimes y,$$

and

$$\Delta(y_i) = y_i \otimes 1 + 1 \otimes y_i + \sum_{j=1}^{i-1} \binom{j-1}{i-1} \cdot y_j \otimes y^{i-j}.$$

In particular, the co-multiplication is not co-commutative.

Larsen's Conjecture

For $w \in F_2 \setminus \{1\}$, what about the equation

$$w(s,t) = g \quad ?$$

Larsen's Conjecture

For $w \in F_2 \setminus \{1\}$, what about the equation

$$w(s,t) = g \quad ?$$

It can always be solved **over** Γ, but can it be solved **in** $PU(n)$ or $SU(n)$?

Larsen's Conjecture

For $w \in F_2 \setminus \{1\}$, what about the equation

$$w(s,t) = g \quad ?$$

It can always be solved **over** Γ, but can it be solved **in** $PU(n)$ or $SU(n)$?

Conjecture (Larsen)

Let $w \in \mathbb{F}_2$. If $n \geq N_w$, then the word map $w\colon PU(n)^{\times 2} \to PU(n)$ is surjective.

Larsen's Conjecture

For $w \in F_2 \setminus \{1\}$, what about the equation

$$w(s,t) = g \quad ?$$

It can always be solved **over** Γ, but can it be solved **in** $PU(n)$ or $SU(n)$?

Conjecture (Larsen)

Let $w \in \mathbb{F}_2$. If $n \geq N_w$, then the word map $w\colon PU(n)^{\times 2} \to PU(n)$ is surjective.

Theorem (with Abdul Elkasapy)

If $w \notin [[\mathbb{F}_2, \mathbb{F}_2], [\mathbb{F}_2, \mathbb{F}_2]]$ and n is not divisible a prime in some finite set P_w, then Larsen's Conjecture holds for w.

Larsen's Conjecture

For $w \in F_2 \setminus \{1\}$, what about the equation

$$w(s,t) = g \quad ?$$

It can always be solved **over** Γ, but can it be solved **in** $PU(n)$ or $SU(n)$?

Conjecture (Larsen)

Let $w \in \mathbb{F}_2$. If $n \geq N_w$, then the word map $w\colon PU(n)^{\times 2} \to PU(n)$ is surjective.

Theorem (with Abdul Elkasapy)

If $w \notin [[\mathbb{F}_2, \mathbb{F}_2], [\mathbb{F}_2, \mathbb{F}_2]]$ and n is not divisible a prime in some finite set P_w, then Larsen's Conjecture holds for w.

Corollary

Engel words $w(s,t) = [...[[s,t],t],...,t]$ are always surjective on groups $PU(n)$.

Remark

Maybe, for fixed $w \in F_2 \setminus \{1\}$ *and* n *large enough,*

$$w\colon PU(n)^{\times 2} \to PU(n)$$

is not even homotopic to a non-surjective map?

Remark

Maybe, for fixed $w \in F_2 \setminus \{1\}$ *and* n *large enough,*

$$w \colon PU(n)^{\times 2} \to PU(n)$$

is not even homotopic to a non-surjective map? Maybe at least not homotopically trivial?

Remark

Maybe, for fixed $w \in F_2 \setminus \{1\}$ and n large enough,

$$w\colon PU(n)^{\times 2} \to PU(n)$$

is not even homotopic to a non-surjective map? Maybe at least not homotopically trivial?

Theorem

For any $n \in \mathbb{N}, \varepsilon > 0$, there exists a word $w \in \mathbb{F}_2 \setminus \{1\}$ such that

$$\|w(u,v) - 1_n\| \leq \varepsilon, \quad \forall u, v \in U(n).$$

This solved a longstanding open problem in non-commutative harmonic analysis in the negative.

Thank you for your attention!