# The complexity of the equation solvability and equivalence problems over finite groups

Attila Földvári

BLAST 2019

March 23, 2019

# Equivalence problem

- given: finite algebra $\mathcal{A}$
- input: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials
- question:

$$p(x_1, \ldots, x_n) \stackrel{?}{\equiv} q(x_1, \ldots, x_n)$$

$$\Updownarrow$$

every $a_1, \ldots, a_n \in \mathcal{A}$ : $p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$

# Equivalence problem

- given: finite algebra $\mathcal{A}$
- input: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials
- question:

$$p(x_1, \ldots, x_n) \stackrel{?}{\equiv} q(x_1, \ldots, x_n)$$

$$\Updownarrow$$

every $a_1, \ldots, a_n \in \mathcal{A}$ : $p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$

## Example

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$:

$$x^{11} \cdot y^4 + x^2 \cdot y + \alpha \cdot x \cdot y^2 \cdot z + z^6 + 1 \stackrel{?}{\equiv} 0$$

# Equivalence problem

- given: finite algebra $\mathcal{A}$
- input: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials
- question:

$$p(x_1, \ldots, x_n) \stackrel{?}{\equiv} q(x_1, \ldots, x_n)$$

$$\Updownarrow$$

every $a_1, \ldots, a_n \in \mathcal{A}$ : $p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$

## Example

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$: $u \in \mathbb{F}_4 \Longrightarrow u^4 = u$

$$x^{11} \cdot y^4 + x^2 \cdot y + \alpha \cdot x \cdot y^2 \cdot z + z^6 + 1 \stackrel{?}{\equiv} 0$$

# Equivalence problem

- given: finite algebra $\mathcal{A}$
- input: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials
- question:

$$p(x_1, \ldots, x_n) \stackrel{?}{\equiv} q(x_1, \ldots, x_n)$$

$$\Updownarrow$$

every $a_1, \ldots, a_n \in \mathcal{A}$ : $p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$

## Example

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$: $u \in \mathbb{F}_4 \Longrightarrow u^4 = u$

$$x^{11} \cdot y^4 + x^2 \cdot y + \alpha \cdot x \cdot y^2 \cdot z + z^6 + 1 \stackrel{?}{\equiv} 0$$

$$x^2 \cdot y^1 + x^2 \cdot y + \alpha \cdot x \cdot y^2 \cdot z + z^3 + 1 \stackrel{?}{\equiv} 0$$

# Equivalence problem

- given: finite algebra $\mathcal{A}$
- input: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials
- question:

$$p(x_1, \ldots, x_n) \stackrel{?}{\equiv} q(x_1, \ldots, x_n)$$

$$\Updownarrow$$

every $a_1, \ldots, a_n \in \mathcal{A}$ : $p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$

## Example

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$: $u \in \mathbb{F}_4 \Longrightarrow u^4 = u$

$$x^{11} \cdot y^4 + x^2 \cdot y + \alpha \cdot x \cdot y^2 \cdot z + z^6 + 1 \stackrel{?}{\equiv} 0$$

$$x^2 \cdot y^1 + x^2 \cdot y + \alpha \cdot x \cdot y^2 \cdot z + z^3 + 1 \stackrel{?}{\equiv} 0$$

$$\alpha \cdot x \cdot y^2 \cdot z + z^3 + 1 \stackrel{?}{\equiv} 0$$

# Equivalence problem

- given: finite algebra $\mathcal{A}$
- input: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials
- question:

$$p(x_1, \ldots, x_n) \stackrel{?}{\equiv} q(x_1, \ldots, x_n)$$

$$\Updownarrow$$

every $a_1, \ldots, a_n \in \mathcal{A}$ : $p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$

## Example

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$: $u \in \mathbb{F}_4 \Longrightarrow u^4 = u$

$$x^{11} \cdot y^4 + x^2 \cdot y + \alpha \cdot x \cdot y^2 \cdot z + z^6 + 1 \not\equiv 0$$

$$x^2 \cdot y^1 + x^2 \cdot y + \alpha \cdot x \cdot y^2 \cdot z + z^3 + 1 \not\equiv 0$$

$$\alpha \cdot x \cdot y^2 \cdot z + z^3 + 1 \not\equiv 0$$

# Equation solvability problem

- given: finite algebra $\mathcal{A}$
- input: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials
- question:

$$p(x_1, \ldots, x_n) \stackrel{?}{=} q(x_1, \ldots, x_n)$$

$$\Updownarrow$$

$$\text{exists } a_1, \ldots, a_n \in \mathcal{A} : p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$$

# Equation solvability problem

- given: finite algebra $\mathcal{A}$
- input: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials
- question:

$$p(x_1, \ldots, x_n) \stackrel{?}{=} q(x_1, \ldots, x_n)$$

$$\Updownarrow$$

$$\text{exists } a_1, \ldots, a_n \in \mathcal{A} : p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$$

## Example

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ :

$$x^4 \cdot y \cdot z^3 + x^2 \cdot z + \alpha^2 \cdot y^4 \cdot z^5 + 1 \stackrel{?}{=} 0$$

# Equation solvability problem

- given: finite algebra $\mathcal{A}$
- input: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials
- question:

$$p(x_1, \ldots, x_n) \stackrel{?}{=} q(x_1, \ldots, x_n)$$

$$\Updownarrow$$

$$\text{exists } a_1, \ldots, a_n \in \mathcal{A} : p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$$

## Example

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\} : u \in \mathbb{F}_4 \Longrightarrow u^3 \in \{0, 1\}$

$$x^4 \cdot y \cdot z^3 + x^2 \cdot z + \alpha^2 \cdot y^4 \cdot z^5 + 1 \quad \stackrel{?}{=} 0$$

# Equation solvability problem

- given: finite algebra $\mathcal{A}$
- input: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials
- question:

$$p(x_1, \ldots, x_n) \stackrel{?}{=} q(x_1, \ldots, x_n)$$

$$\Updownarrow$$

$$\text{exists } a_1, \ldots, a_n \in \mathcal{A} : p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$$

## Example

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\} : u \in \mathbb{F}_4 \Longrightarrow u^3 \in \{0, 1\}$

$$x^4 \cdot y \cdot z^3 + x^2 \cdot z + \alpha^2 \cdot y^4 \cdot z^5 + 1 \stackrel{?}{=} 0$$

$$(x^4 \cdot y \cdot z^3 + x^2 \cdot z + \alpha^2 \cdot y^4 \cdot z^5 + 1)^3$$

# Equation solvability problem

- given: finite algebra $\mathcal{A}$
- input: $p(x_1, \ldots, x_n), q(x_1, \ldots, x_n)$ polynomials
- question:

$$p(x_1, \ldots, x_n) \stackrel{?}{=} q(x_1, \ldots, x_n)$$

$$\Updownarrow$$

$$\text{exists } a_1, \ldots, a_n \in \mathcal{A} : p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$$

## Example

$\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\} : u \in \mathbb{F}_4 \Longrightarrow u^3 \in \{0, 1\}$

$$x^4 \cdot y \cdot z^3 + x^2 \cdot z + \alpha^2 \cdot y^4 \cdot z^5 + 1 \stackrel{?}{=} 0$$

$$(x^4 \cdot y \cdot z^3 + x^2 \cdot z + \alpha^2 \cdot y^4 \cdot z^5 + 1)^3 \stackrel{?}{\neq} 1$$

# Complexity

- always decidable
- what is the complexity?

# Complexity

- always decidable
- what is the complexity?
- equation solvability always in NP

# Complexity

- always decidable
- what is the complexity?
- equation solvability always in NP
- equivalence always in coNP

# Complexity

$\mathcal{A}$ a group/ring: solvability is in P $\Longrightarrow$ equivalence is in P

# Complexity

$\mathcal{A}$ a group/ring: solvability is in P $\Longrightarrow$ equivalence is in P

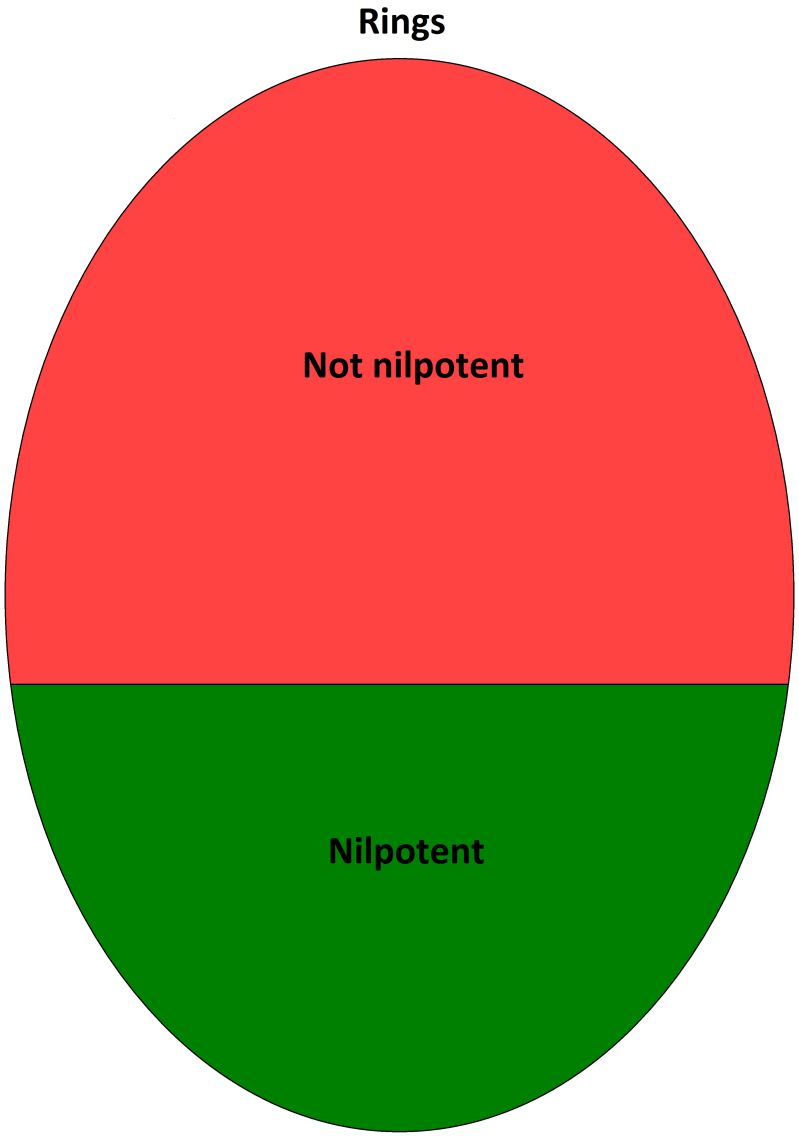
## Example

$$S, T \in \mathbf{G}[x_1, \ldots, x_n]: \qquad S \stackrel{?}{\equiv} T$$

$$S \cdot T^{-1} \stackrel{?}{\equiv} \mathrm{id}$$

*every* $g \in \mathbf{G} \setminus \{\mathrm{id}\}$: $\qquad S \cdot T^{-1} \stackrel{?}{\neq} g$

# Rings




Theorem (Burris, Lawrence (1993), Horváth (2011))

$\mathcal{R}$ *not nilpotent* $\Longrightarrow$ *NP-complete*

$\mathcal{R}$ *nilpotent* $\Longrightarrow$ *in P*

# Sigma problem

## Example

$$\underbrace{(x_1 + y_1) \cdot \ldots \cdot (x_n + y_n)}_{n \text{ factors}} = \underbrace{x_1 \cdot \ldots \cdot x_n + \cdots + y_1 \cdot \ldots \cdot y_n}_{2^n \text{ summands}}$$

# Sigma problem

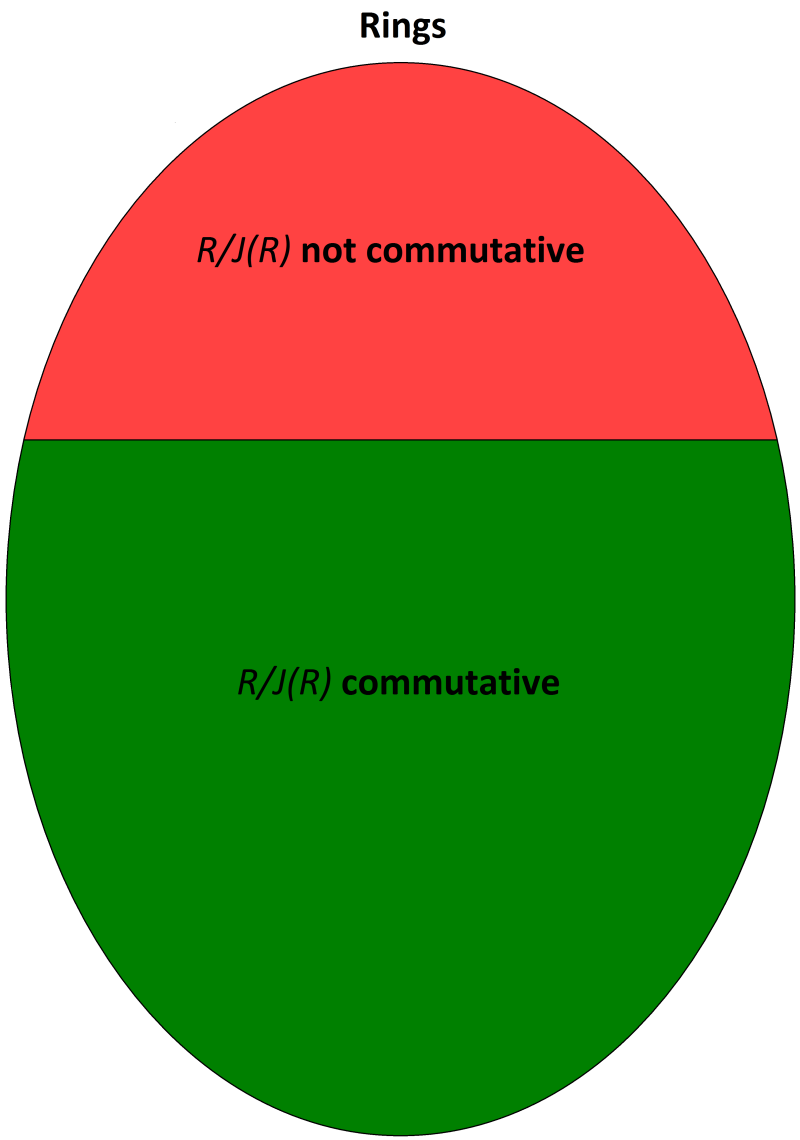
## Example

$$\underbrace{(x_1 + y_1) \cdot \ldots \cdot (x_n + y_n)}_{n \text{ factors}} = \underbrace{x_1 \cdot \ldots \cdot x_n + \cdots + y_1 \cdot \ldots \cdot y_n}_{2^n \text{ summands}}$$

## Lawrence, Willard:

sigma equivalence, sigma solvability:
inputs are given as sums of monomials

# Rings

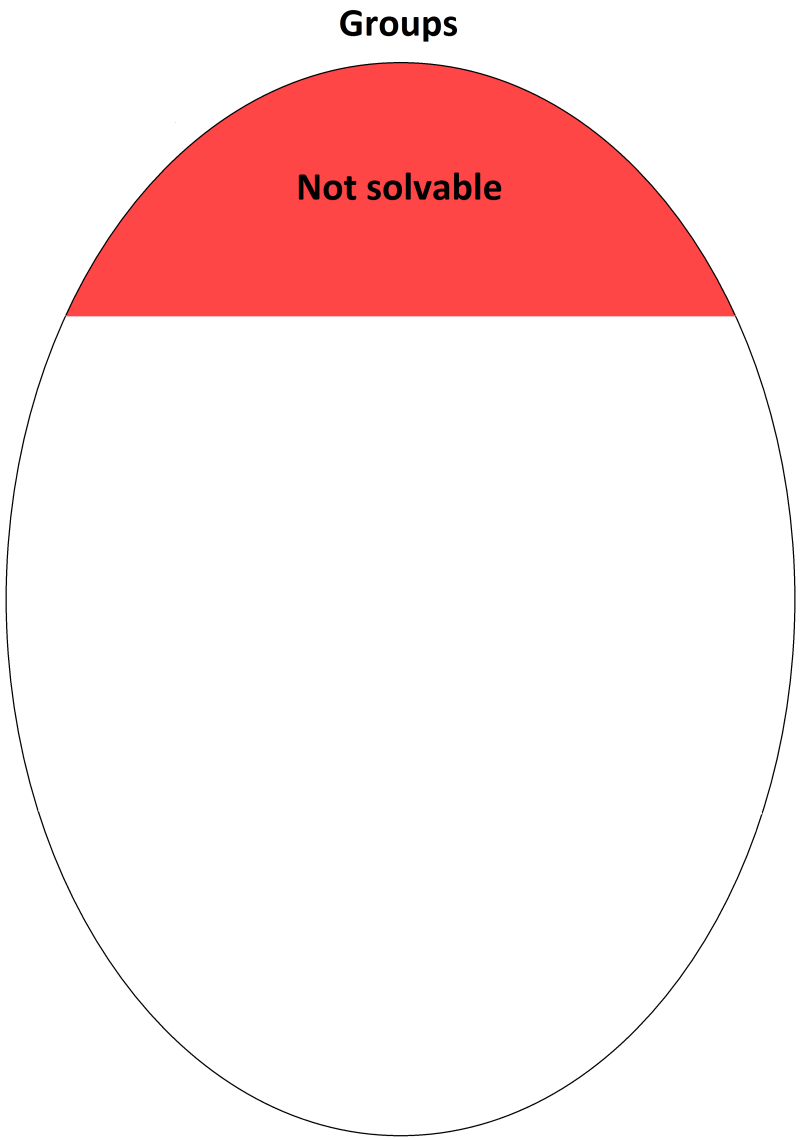



Theorem (Szabó, Vértesi (2011), Horváth, Lawrence, Willard)

$\mathcal{R}/\mathcal{J}(\mathcal{R})$ *not comm.* $\Longrightarrow$ *sigma problem is NP-complete*

$\mathcal{R}/\mathcal{J}(\mathcal{R})$ *comm.* $\Longrightarrow$ *sigma problem is in P*

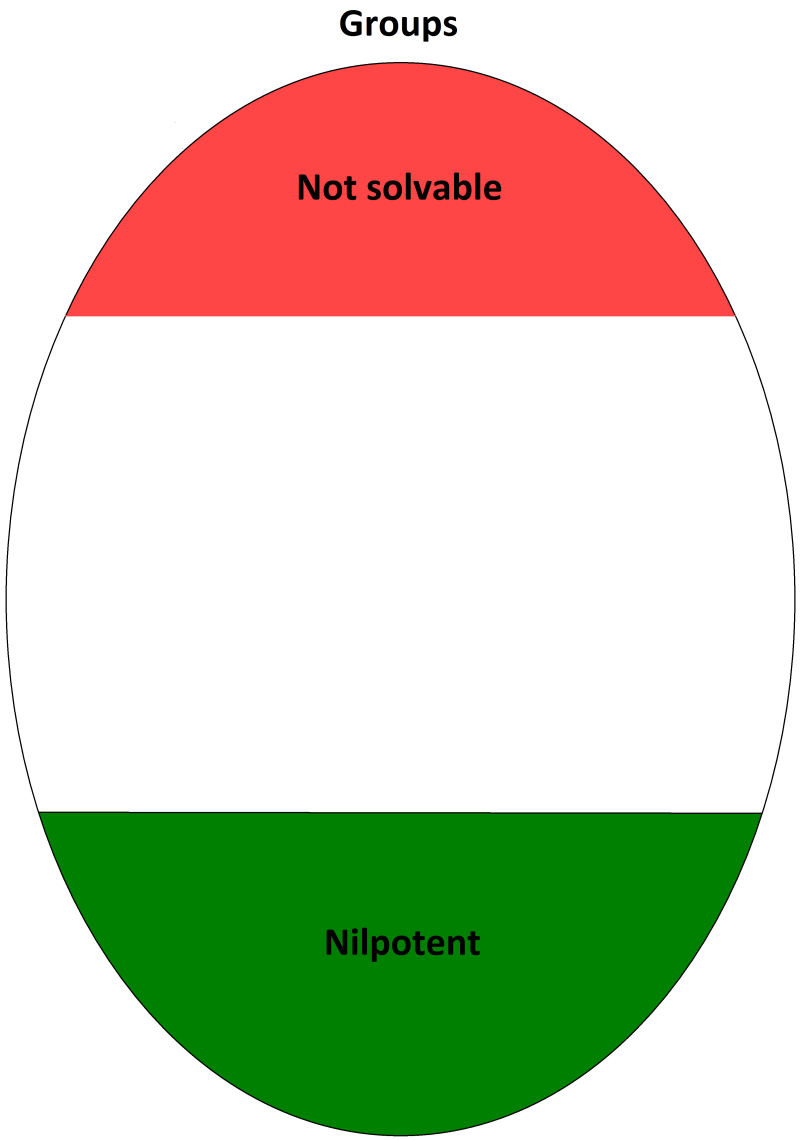
# Solvability over groups




## Theorem

- *not solvable (Goldmann, Russell (1999)): NP-complete*

# Solvability over groups



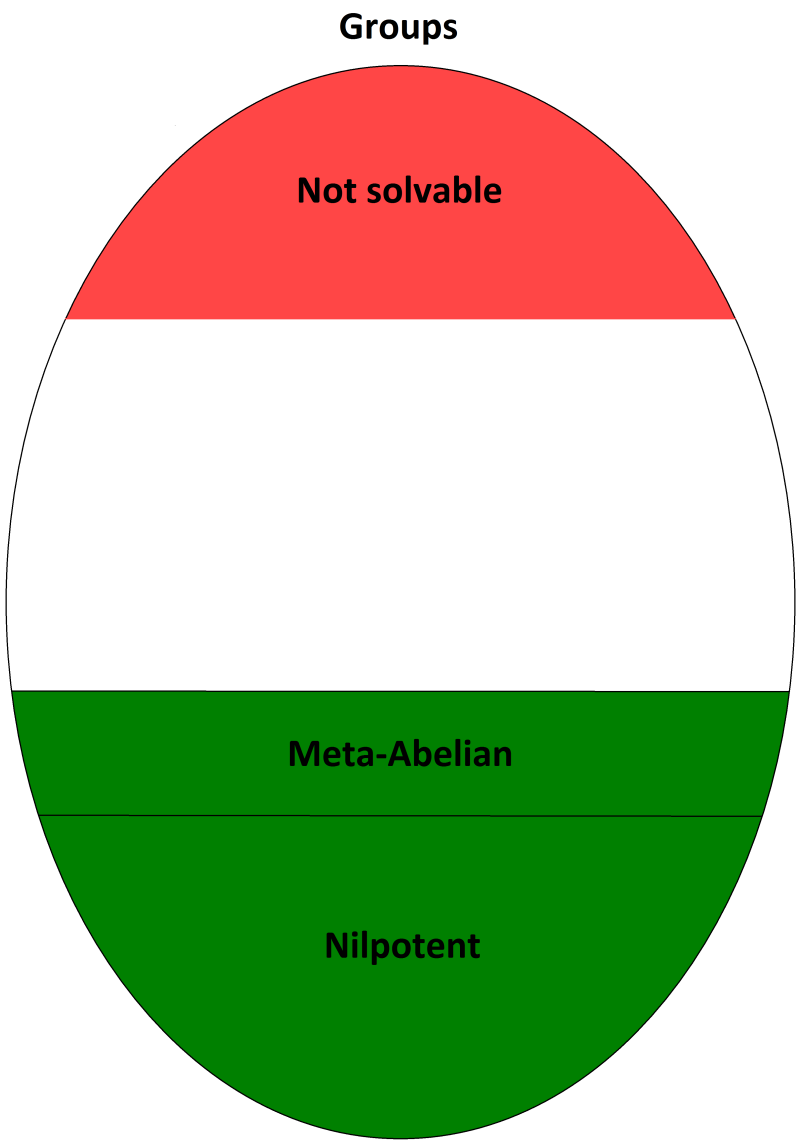

## Theorem

- *not solvable (Goldmann, Russell (1999)): NP-complete*

- *nilpotent (Goldmann, Russell (1999)): in P*

  $Ramsey \Longrightarrow O\left(n^{|\mathbf{G}|^{\cdots^{|\mathbf{G}|}}}\right)$

# Solvability over groups



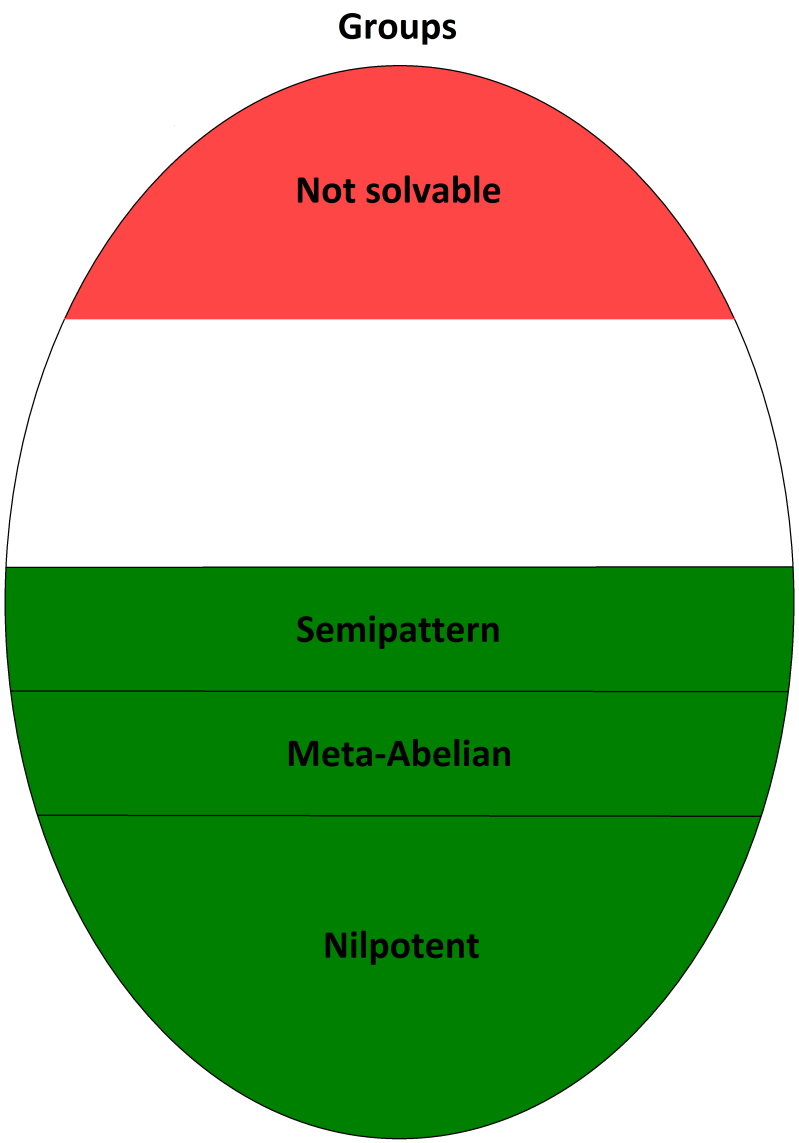

## Theorem

- *not solvable (Goldmann, Russell (1999)): NP-complete*

- *meta-Abelien (Horváth (2015)): in P*
- *nilpotent (Goldmann, Russell (1999)): in P*

  *Ramsey* $\Longrightarrow O\left(n^{|\mathbf{G}|^{\cdots^{|\mathbf{G}|}}}\right)$

# Solvability over groups

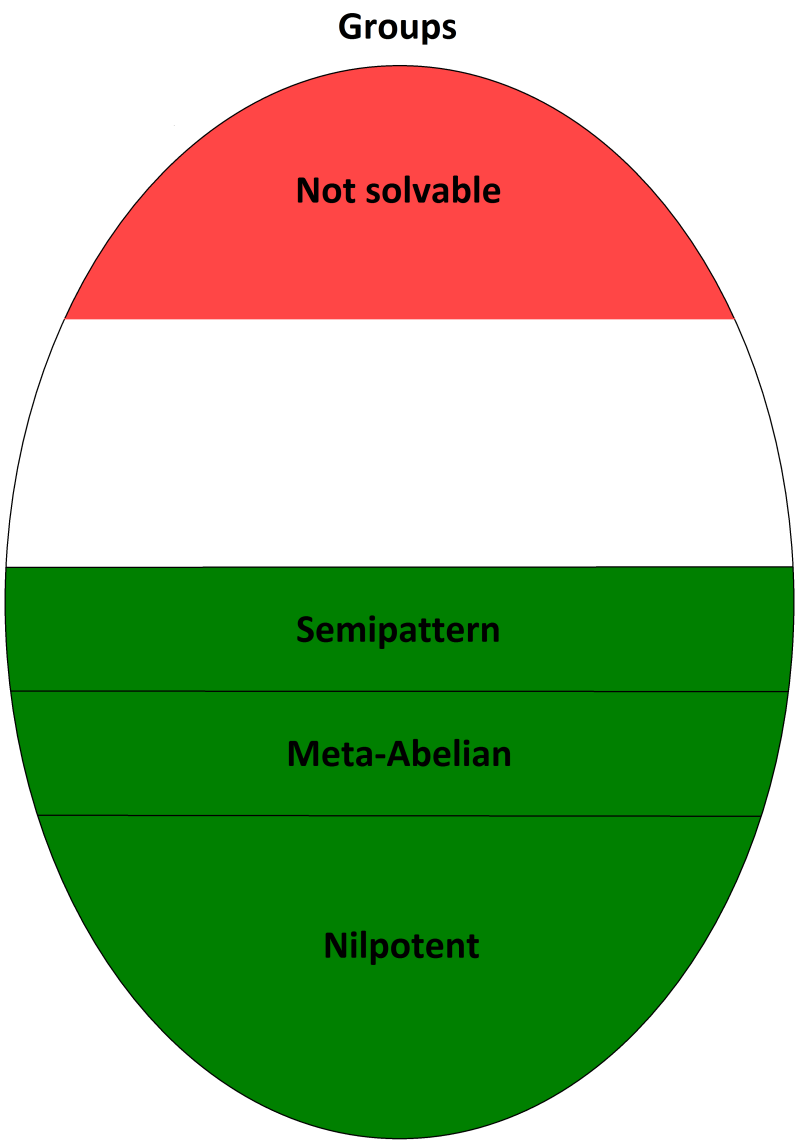



## Theorem

- *not solvable (Goldmann, Russell (1999)): NP-complete*
- *semmipattern (Földvári (2016)): in P*
- *meta-Abelien (Horváth (2015)): in P*
- *nilpotent (Goldmann, Russell (1999)): in P*

$$\textit{Ramsey} \Longrightarrow O\left(n^{|\mathbf{G}|^{\cdots^{|\mathbf{G}|}}}\right)$$

# Solvability over groups




## Theorem

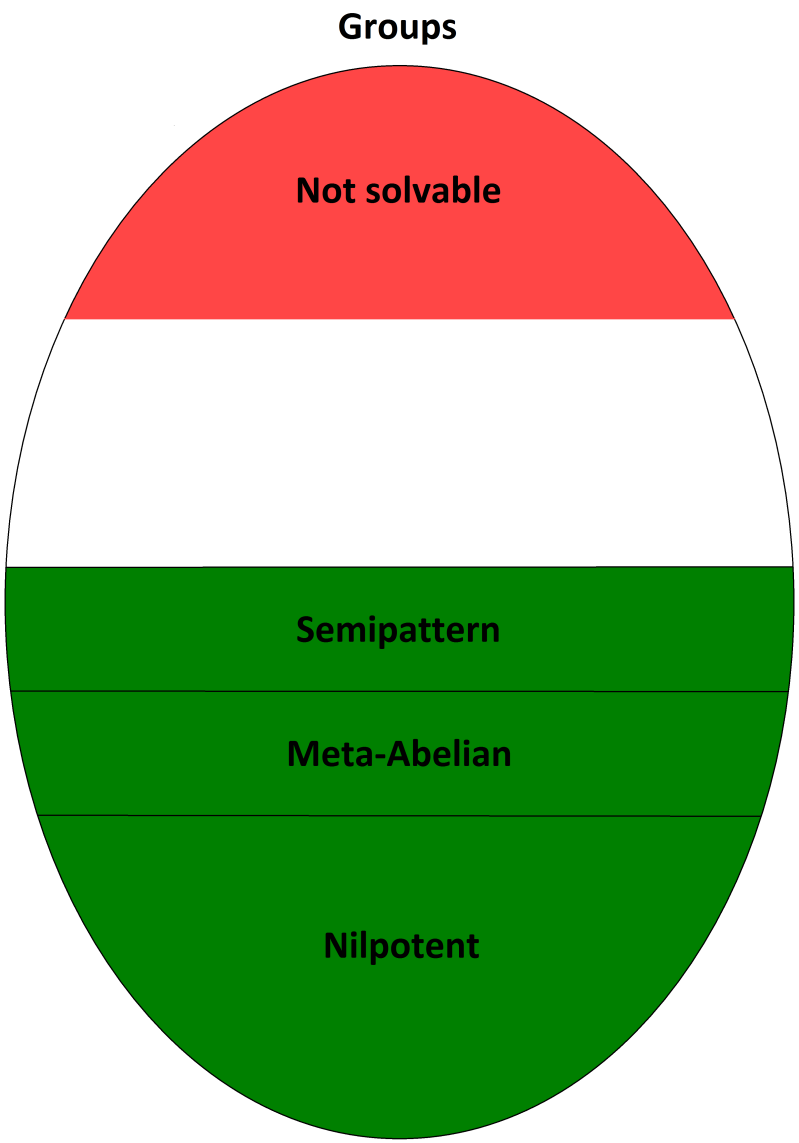
- *not solvable (Goldmann, Russell (1999)): NP-complete*
- *semmipattern (Földvári (2016)): in P*
- *meta-Abelien (Horváth (2015)): in P*
- *nilpotent (Goldmann, Russell (1999)): in P*

  $Ramsey \Longrightarrow O\left(n^{|\mathbf{G}|^{\cdots^{|\mathbf{G}|}}}\right)$

## Question:

$\mathbf{S}_4$, $\mathbf{SL}(2, \mathbb{Z}_3)$

# Solvability over groups




## Theorem

- *not solvable (Goldmann, Russell (1999)): NP-complete*
- *semmipattern (Földvári (2016)): in P*
- *meta-Abelien (Horváth (2015)): in P*
- *nilpotent (Goldmann, Russell (1999)): in P*

  $Ramsey \Longrightarrow O\left(n^{|\mathbf{G}|^{\cdots^{|\mathbf{G}|}}}\right)$

## Question:

$\mathbf{S}_4$, $\mathbf{SL}(2, \mathbb{Z}_3)$

# The group $\mathbf{SL}(2, \mathbb{Z}_3)$

$$\mathbf{SL}(2, \mathbb{Z}_3) \cong \mathbf{Q} \rtimes \mathbf{C}_3$$

$$\mathbf{Q} = \{1, -1, i, -i, j, -j, k, -k\},\ \mathbf{C}_3 = \{1, \alpha, \alpha^2\}:$$

$$i^\alpha = j \qquad j^\alpha = k \qquad k^\alpha = i$$

# Multiplication in the group $\mathbf{Q}$

## Polycyclic generating system

$u \in \mathbf{Q} \Rightarrow \exists!\, x, y, z \in \{0,1\} : u = (-1)^x \cdot i^y \cdot j^z$

# Multiplication in the group $\mathbf{Q}$

## Polycyclic generating system

$u \in \mathbf{Q} \Rightarrow \exists!\, x, y, z \in \{0,1\} : u = (-1)^x \cdot i^y \cdot j^z$

## Product of 2 elements

$u_1 \cdot u_2 = (-1)^{x_1} \cdot i^{y_1} \cdot j^{z_1} \cdot (-1)^{x_2} \cdot i^{y_2} \cdot j^{z_2} =$

# Multiplication in the group $\mathbf{Q}$

## Polycyclic generating system

$u \in \mathbf{Q} \Rightarrow \exists!\, x, y, z \in \{0,1\} : u = (-1)^x \cdot i^y \cdot j^z$

## Product of 2 elements

$$u_1 \cdot u_2 = (-1)^{x_1} \cdot i^{y_1} \cdot j^{z_1} \cdot (-1)^{x_2} \cdot i^{y_2} \cdot j^{z_2} =$$
$$= (-1)^{f_1(\dots)} \cdot i^{f_2(\dots)} \cdot j^{f_3(\dots)}$$

$$f_1, f_2, f_3 \in \mathbb{Z}_2[x_1, y_1, z_1, y_2, x_2, z_2]$$

$$f_1(\dots) = x_1 + x_2 + y_1 \cdot y_2 + z_1 \cdot z_2 + z_1 \cdot y_2$$

$$f_2(\dots) = y_1 + y_2$$

$$f_3(\dots) = z_1 + z_2$$

# Multiplication in the group $\mathbf{Q}$

## Polycyclic generating system

$u \in \mathbf{Q} \Rightarrow \exists!\, x, y, z \in \{0,1\} : u = (-1)^x \cdot i^y \cdot j^z$

## Product of $n$ elements

$$u_1 \cdot \ldots \cdot u_n = (-1)^{x_1} \cdot i^{y_1} \cdot j^{z_1} \cdot \ldots \cdot (-1)^{x_n} \cdot i^{y_n} \cdot j^{z_n} = \\ = (-1)^{F_1(\ldots)} \cdot i^{F_2(\ldots)} \cdot j^{F_3(\ldots)}$$

$$F_1, F_2, F_3 \in \mathbb{Z}_2[x_1, y_1, z_1, \ldots, x_n, y_n, z_n]$$

$$F_1(\ldots) = \sum_{k=1}^{n} x_k + \sum_{l=2}^{n} \sum_{k=1}^{l-1} y_k y_l + \sum_{l=2}^{n} \sum_{k=1}^{l-1} z_k z_l + \sum_{l=2}^{n} \sum_{k=1}^{l-1} z_k y_l$$

$$F_2(\ldots) = \sum_{k=1}^{n} y_k$$

$$F_3(\ldots) = \sum_{k=1}^{n} z_k$$

# Multiplication in the group $\mathbf{Q}$

## Polycyclic generating system

$u \in \mathbf{Q} \Rightarrow \exists!\, x, y, z \in \{0,1\} : u = (-1)^x \cdot i^y \cdot j^z$

## Product of $n$ elements

$$u_1 \cdot \ldots \cdot u_n = (-1)^{x_1} \cdot i^{y_1} \cdot j^{z_1} \cdot \ldots \cdot (-1)^{x_n} \cdot i^{y_n} \cdot j^{z_n} = \\ = (-1)^{F_1(\ldots)} \cdot i^{F_2(\ldots)} \cdot j^{F_3(\ldots)}$$

$$F_1, F_2, F_3 \in \mathbb{Z}_2[x_1, y_1, z_1, \ldots, x_n, y_n, z_n]$$

$$F_1(\ldots) = \sum_{k=1}^{n} x_k + \sum_{l=2}^{n} \sum_{k=1}^{l-1} y_k y_l + \sum_{l=2}^{n} \sum_{k=1}^{l-1} z_k z_l + \sum_{l=2}^{n} \sum_{k=1}^{l-1} z_k y_l$$

$$F_2(\ldots) = \sum_{k=1}^{n} y_k$$

$$F_3(\ldots) = \sum_{k=1}^{n} z_k$$

# Multiplication in the group $\mathbf{SL}(2, \mathbb{Z}_3)$

- $\mathbf{SL}(2, \mathbb{Z}_3) \cong \mathbf{Q} \rtimes \mathbf{C}_3$

$$g \in \mathbf{SL}(2, \mathbb{Z}_3) \implies \exists!\, u \in \mathbf{Q}, h \in \mathbf{C}_3 : \; g = (u, h)$$

# Multiplication in the group $\mathbf{SL}(2, \mathbb{Z}_3)$

- $\mathbf{SL}(2, \mathbb{Z}_3) \cong \mathbf{Q} \rtimes \mathbf{C}_3$

$$g \in \mathbf{SL}(2, \mathbb{Z}_3) \implies \exists!\, u \in \mathbf{Q}, h \in \mathbf{C}_3 : \; g = (u, h)$$

- the rule for multiplication:

$$g_1 \cdot g_2 = (u_1, h_1) \cdot (u_2, h_2) = (u_1 \cdot u_2^{h_1}, h_1 \cdot h_2)$$

# Multiplication in the group $\mathbf{SL}(2, \mathbb{Z}_3)$

- $\mathbf{SL}(2, \mathbb{Z}_3) \cong \mathbf{Q} \rtimes \mathbf{C}_3$

$$g \in \mathbf{SL}(2, \mathbb{Z}_3) \implies \exists!\, u \in \mathbf{Q}, h \in \mathbf{C}_3 : \; g = (u, h)$$

- the rule for multiplication:

$$g_1 \cdot g_2 = (u_1, h_1) \cdot (u_2, h_2) = (u_1 \cdot u_2^{h_1}, h_1 \cdot h_2)$$

# Multiplication in the group $\mathbf{SL}(2,\mathbb{Z}_3)$

- $\mathbf{SL}(2,\mathbb{Z}_3) \cong \mathbf{Q} \rtimes \mathbf{C}_3$

$$g \in \mathbf{SL}(2,\mathbb{Z}_3) \implies \exists!\, u \in \mathbf{Q}, h \in \mathbf{C}_3 :\ g = (u,h)$$

- the rule for multiplication:

$$g_1 \cdot g_2 = (u_1,h_1)\cdot(u_2,h_2) = (u_1 \cdot u_2^{h_1}, h_1 \cdot h_2)$$

- conjugation:

$$\begin{array}{ll} u \in \mathbf{Q} & \implies \quad \exists!\, x,y,z \in \mathbb{Z}_2 :\ u = (-1)^x \cdot i^y \cdot j^z \\ h \in \mathbf{C}_3 & \end{array}$$

basis form:

$$\phi_1, \phi_2, \phi_3 \in \mathbb{F}_q[x,y,z,h]$$

$$u^h = ((-1)^x \cdot i^y \cdot j^z)^h = (-1)^{\phi_1(\dots)} \cdot i^{\phi_2(\dots)} \cdot j^{\phi_3(\dots)}$$

# Multiplication in the group $\mathbf{SL}(2,\mathbb{Z}_3)$

- $\mathbf{SL}(2,\mathbb{Z}_3) \cong \mathbf{Q} \rtimes \mathbf{C}_3$

$$g \in \mathbf{SL}(2,\mathbb{Z}_3) \implies \exists!\, u \in \mathbf{Q}, h \in \mathbf{C}_3 :\ g = (u,h)$$

- the rule for multiplication:

$$g_1 \cdot g_2 = (u_1,h_1)\cdot(u_2,h_2) = (u_1 \cdot u_2^{h_1}, h_1 \cdot h_2)$$

- conjugation:

$$u \in \mathbf{Q} \implies \exists!\, x,y,z \in \mathbb{Z}_2 :\ u = (-1)^x \cdot i^y \cdot j^z$$
$$h \in \mathbf{C}_3 \leq \mathbb{F}_q^\times$$

basis form:

$$\phi_1,\phi_2,\phi_3 \in \mathbb{F}_q[x,y,z,h]$$
$$u^h = ((-1)^x \cdot i^y \cdot j^z)^h = (-1)^{\phi_1(\dots)} \cdot i^{\phi_2(\dots)} \cdot j^{\phi_3(\dots)}$$

# Multiplication in the group $\mathbf{SL}(2,\mathbb{Z}_3)$

- $\mathbf{SL}(2,\mathbb{Z}_3) \cong \mathbf{Q} \rtimes \mathbf{C}_3$

$$g \in \mathbf{SL}(2,\mathbb{Z}_3) \implies \exists!\, u \in \mathbf{Q}, h \in \mathbf{C}_3 :\ g = (u,h)$$

- the rule for multiplication:

$$g_1 \cdot g_2 = (u_1,h_1)\cdot(u_2,h_2) = (u_1 \cdot u_2^{h_1}, h_1 \cdot h_2)$$

- conjugation:

$$u \in \mathbf{Q} \implies \exists!\, x,y,z \in \mathbb{Z}_2 :\ u = (-1)^x \cdot i^y \cdot j^z$$
$$h \in \mathbf{C}_3 \cong \mathbb{F}_4^\times$$

basis form:

$$\phi_1,\phi_2,\phi_3 \in \mathbb{F}_4[x,y,z,h]$$
$$u^h = ((-1)^x \cdot i^y \cdot j^z)^h = (-1)^{\phi_1(\dots)} \cdot i^{\phi_2(\dots)} \cdot j^{\phi_3(\dots)}$$

# Equation solvability problem over $\mathbf{SL}(2, \mathbb{Z}_3)$

- question: $T = t_1 \cdot t_2 \cdot \ldots \cdot t_n \stackrel{?}{=} \mathrm{id}$

# Equation solvability problem over $\mathbf{SL}(2, \mathbb{Z}_3)$

- question: $T = t_1 \cdot t_2 \cdot \ldots \cdot t_n \stackrel{?}{=} \mathrm{id}$
- semidirect product: $t_k = (u_k, h_k)$

  $T = (u_1, h_1) \cdot (u_2, h_2) \cdots (u_n, h_n) = (T_{\mathbf{Q}}, T_{\mathbf{C}_3})$

  $T_{\mathbf{Q}} = u_1 \cdot u_2^{h_1} \cdot u_3^{h_1 \cdot h_2} \cdot \ldots \cdot u_n^{h_1 \cdot h_2 \cdot \ldots \cdot h_{n-1}}$

  $T_{\mathbf{C}_3} = h_1 \cdot h_2 \cdot \ldots \cdot h_n$

# Equation solvability problem over $\mathbf{SL}(2, \mathbb{Z}_3)$

- question: $T = t_1 \cdot t_2 \cdot \ldots \cdot t_n \stackrel{?}{=} \mathrm{id}$
- semidirect product: $t_k = (u_k, h_k)$

  $T = (u_1, h_1) \cdot (u_2, h_2) \cdots (u_n, h_n) = (T_{\mathbf{Q}}, T_{\mathbf{C}_3})$

  $T_{\mathbf{Q}} = u_1 \cdot u_2^{h_1} \cdot u_3^{h_1 \cdot h_2} \cdot \ldots \cdot u_n^{h_1 \cdot h_2 \cdot \ldots \cdot h_{n-1}}$

  $T_{\mathbf{C}_3} = h_1 \cdot h_2 \cdot \ldots \cdot h_n$
- conjugation: $\exists\ \phi_1, \phi_2, \phi_3 \in \mathbb{F}_4[\ldots]$ :

  $u^h = (-1)^{\phi_1(\ldots)} i^{\phi_2(\ldots)} j^{\phi_3(\ldots)}$

# Equation solvability problem over $\mathbf{SL}(2, \mathbb{Z}_3)$

- question: $T = t_1 \cdot t_2 \cdot \ldots \cdot t_n \stackrel{?}{=} \mathrm{id}$
- semidirect product: $t_k = (u_k, h_k)$

  $T = (u_1, h_1) \cdot (u_2, h_2) \cdots (u_n, h_n) = (T_{\mathbf{Q}}, T_{\mathbf{C}_3})$

  $T_{\mathbf{Q}} = u_1 \cdot u_2^{h_1} \cdot u_3^{h_1 \cdot h_2} \cdot \ldots \cdot u_n^{h_1 \cdot h_2 \cdot \ldots \cdot h_{n-1}}$

  $T_{\mathbf{C}_3} = h_1 \cdot h_2 \cdot \ldots \cdot h_n$
- conjugation: $\exists\ \phi_1, \phi_2, \phi_3 \in \mathbb{F}_4[\ldots]$ :

  $u^h = (-1)^{\phi_1(\ldots)} i^{\phi_2(\ldots)} j^{\phi_3(\ldots)}$
- multiplication in $\mathbf{Q}$: $\exists\ F_1, F_2, F_3 \in \mathbb{Z}_2[\ldots]$ :

  $u_1 \cdot \ldots \cdot u_n = (-1)^{F_1(\ldots)} \cdot i^{F_2(\ldots)} \cdot j^{F_2(\ldots)}$

# Equation solvability problem over $\mathbf{SL}(2, \mathbb{Z}_3)$

- question: $T = t_1 \cdot t_2 \cdot \ldots \cdot t_n \stackrel{?}{=} \mathrm{id}$
- semidirect product: $t_k = (u_k, h_k)$

  $T = (u_1, h_1) \cdot (u_2, h_2) \cdots (u_n, h_n) = (T_{\mathbf{Q}}, T_{\mathbf{C}_3})$

  $T_{\mathbf{Q}} = u_1 \cdot u_2^{h_1} \cdot u_3^{h_1 \cdot h_2} \cdot \ldots \cdot u_n^{h_1 \cdot h_2 \cdot \ldots \cdot h_{n-1}}$

  $T_{\mathbf{C}_3} = h_1 \cdot h_2 \cdot \ldots \cdot h_n$
- conjugation: $\exists\ \phi_1, \phi_2, \phi_3 \in \mathbb{F}_4[\ldots]$:

  $$u^h = (-1)^{\phi_1(\ldots)} i^{\phi_2(\ldots)} j^{\phi_3(\ldots)}$$
- multiplication in $\mathbf{Q}$: $\exists\ F_1, F_2, F_3 \in \mathbb{Z}_2[\ldots]$:

  $$u_1 \cdot \ldots \cdot u_n = (-1)^{F_1(\ldots)} \cdot i^{F_2(\ldots)} \cdot j^{F_2(\ldots)}$$
- $\exists\ \Phi_1, \Phi_2, \Phi_3 \in \mathbb{F}_4[\ldots]$:

  $\Phi_i = F_i(\ldots, \phi_1, \phi_2, \phi_3, \ldots)$, $\Phi_i$ is a sum of monomials,

  $$T_{\mathbf{Q}} = (-1)^{\Phi_1} \cdot i^{\Phi_2} \cdot j^{\Phi_3}$$

# Equation solvability problem over $\mathbf{SL}(2,\mathbb{Z}_3)$

- question: $T = t_1 \cdot t_2 \cdot \ldots \cdot t_n \stackrel{?}{=} \mathrm{id}$
- semidirect product: $t_k = (u_k, h_k)$

  $T = (u_1, h_1) \cdot (u_2, h_2) \cdots (u_n, h_n) = (T_{\mathbf{Q}}, T_{\mathbf{C}_3})$

  $T_{\mathbf{Q}} = u_1 \cdot u_2^{h_1} \cdot u_3^{h_1 \cdot h_2} \cdot \ldots \cdot u_n^{h_1 \cdot h_2 \cdot \ldots \cdot h_{n-1}} \stackrel{?}{=} \mathrm{id}_{\mathbf{Q}}$

  $T_{\mathbf{C}_3} = h_1 \cdot h_2 \cdot \ldots \cdot h_n \stackrel{?}{=} \mathrm{id}_{\mathbf{C}_3}$
- conjugation: $\exists\ \phi_1, \phi_2, \phi_3 \in \mathbb{F}_4[\ldots]$ :

  $u^h = (-1)^{\phi_1(\ldots)} i^{\phi_2(\ldots)} j^{\phi_3(\ldots)}$
- multiplication in $\mathbf{Q}$: $\exists\ F_1, F_2, F_3 \in \mathbb{Z}_2[\ldots]$ :

  $u_1 \cdot \ldots \cdot u_n = (-1)^{F_1(\ldots)} \cdot i^{F_2(\ldots)} \cdot j^{F_2(\ldots)}$
- $\exists\ \Phi_1, \Phi_2, \Phi_3 \in \mathbb{F}_4[\ldots]$ :

  $\Phi_i = F_i(\ldots, \phi_1, \phi_2, \phi_3, \ldots)$, $\Phi_i$ is a sum of monomials,

  $T_{\mathbf{Q}} = (-1)^{\Phi_1} \cdot i^{\Phi_2} \cdot j^{\Phi_3} \stackrel{?}{=} (-1)^0 \cdot i^0 \cdot j^0$

# Equation solvability problem over $\mathbf{SL}(2,\mathbb{Z}_3)$

- question: $T = t_1 \cdot t_2 \cdot \ldots \cdot t_n \stackrel{?}{=} \mathrm{id}$
- semidirect product: $t_k = (u_k, h_k)$

  $T = (u_1, h_1) \cdot (u_2, h_2) \cdots (u_n, h_n) = (T_{\mathbf{Q}}, T_{\mathbf{C}_3})$

  $T_{\mathbf{Q}} = u_1 \cdot u_2^{h_1} \cdot u_3^{h_1 \cdot h_2} \cdot \ldots \cdot u_n^{h_1 \cdot h_2 \cdot \ldots \cdot h_{n-1}} \stackrel{?}{=} \mathrm{id}_{\mathbf{Q}}$

  $T_{\mathbf{C}_3} = h_1 \cdot h_2 \cdot \ldots \cdot h_n \stackrel{?}{=} \mathrm{id}_{\mathbf{C}_3}$
- conjugation: $\exists\, \phi_1, \phi_2, \phi_3 \in \mathbb{F}_4[\ldots]$:

  $u^h = (-1)^{\phi_1(\ldots)} i^{\phi_2(\ldots)} j^{\phi_3(\ldots)}$
- multiplication in $\mathbf{Q}$: $\exists\, F_1, F_2, F_3 \in \mathbb{Z}_2[\ldots]$:

  $u_1 \cdot \ldots \cdot u_n = (-1)^{F_1(\ldots)} \cdot i^{F_2(\ldots)} \cdot j^{F_2(\ldots)}$
- $\exists\, \Phi_1, \Phi_2, \Phi_3 \in \mathbb{F}_4[\ldots]$:

  $\Phi_i = F_i(\ldots, \phi_1, \phi_2, \phi_3, \ldots)$, $\Phi_i$ is a sum of monomials,

  $T_{\mathbf{Q}} = (-1)^{\Phi_1} \cdot i^{\Phi_2} \cdot j^{\Phi_3} \stackrel{?}{=} (-1)^0 \cdot i^0 \cdot j^0$
- system of equations over $\mathbb{F}_4$:

  $\Phi_1 \stackrel{?}{=} 0 \qquad \Phi_2 \stackrel{?}{=} 0 \qquad \Phi_3 \stackrel{?}{=} 0 \qquad h_1 \cdot h_2 \cdot \ldots \cdot h_n \stackrel{?}{=} 1$

# Main ideas

- semidirect product: $\mathbf{N} \rtimes \mathbf{H}$

# Main ideas

- semidirect product: $\mathbf{N} \rtimes \mathbf{H} \Longrightarrow$
  an equation over $\mathbf{N}$ + an equation over $\mathbf{H}$

# Main ideas

- semidirect product: $\mathbf{N} \rtimes \mathbf{H} \Longrightarrow$
  an equation over $\mathbf{N}$ + an equation over $\mathbf{H}$
- polycyclic generating system of $\mathbf{N} \Longrightarrow$
  characterization the multiplication of $\mathbf{N}$ with the **suitable** polynomials over $\mathbb{Z}_p$

# Main ideas

- semidirect product: $\mathbf{N} \rtimes \mathbf{H} \Longrightarrow$
  an equation over $\mathbf{N}$ + an equation over $\mathbf{H}$
- $\mathbf{N}$ is a p-group $\Longrightarrow$ polycyclic generating system of $\mathbf{N} \Longrightarrow$
  characterization the multiplication of $\mathbf{N}$ with the **suitable** polynomials over $\mathbb{Z}_p$

# Main ideas

- semidirect product: $\mathbf{N} \rtimes \mathbf{H} \Longrightarrow$
  an equation over $\mathbf{N}$ + an equation over $\mathbf{H}$
- $\mathbf{N}$ is a p-group $\Longrightarrow$ polycyclic generating system of $\mathbf{N} \Longrightarrow$
  characterization the multiplication of $\mathbf{N}$ with the **suitable** polynomials over $\mathbb{Z}_p$
- a field $\mathbb{F}_q$: $\mathbf{H} \leq \mathbb{F}_q^\times$ and $\mathbb{Z}_p \leq \mathbb{F}_q \Longrightarrow$
  characterization the conjugation with polynomials over $\mathbb{F}_q$

# Main ideas

- semidirect product: $\mathbf{N} \rtimes \mathbf{H} \Longrightarrow$
  an equation over $\mathbf{N}$ + an equation over $\mathbf{H}$
- $\mathbf{N}$ is a p-group $\Longrightarrow$ polycyclic generating system of $\mathbf{N} \Longrightarrow$
  characterization the multiplication of $\mathbf{N}$ with the **suitable** polynomials over $\mathbb{Z}_p$
- $\mathbf{H}$ Abelian, $p \nmid |\mathbf{H}| \Longrightarrow$ a field $\mathbb{F}_q$: $\mathbf{H} \leq \mathbb{F}_q^\times$ and $\mathbb{Z}_p \leq \mathbb{F}_q \Longrightarrow$
  characterization the conjugation with polynomials over $\mathbb{F}_q$

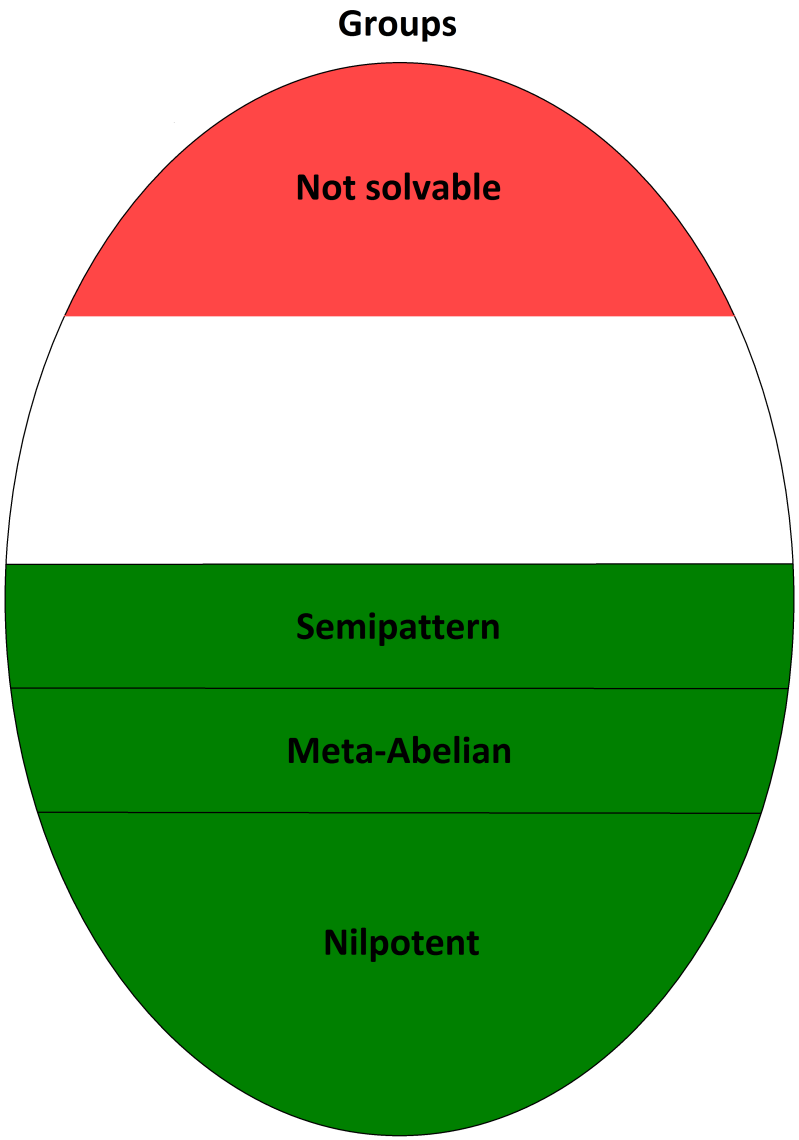
# Main ideas

- semidirect product: $\mathbf{N} \rtimes \mathbf{H} \Longrightarrow$
  an equation over $\mathbf{N}$ + an equation over $\mathbf{H}$
- $\mathbf{N}$ is a p-group $\Longrightarrow$ polycyclic generating system of $\mathbf{N} \Longrightarrow$
  characterization the multiplication of $\mathbf{N}$ with the **suitable** polynomials over $\mathbb{Z}_p$
- $\mathbf{H}$ Abelian, $p \nmid |\mathbf{H}| \Longrightarrow$ a field $\mathbb{F}_q$: $\mathbf{H} \leq \mathbb{F}_q^\times$ and $\mathbb{Z}_p \leq \mathbb{F}_q \Longrightarrow$
  characterization the conjugation with polynomials over $\mathbb{F}_q$

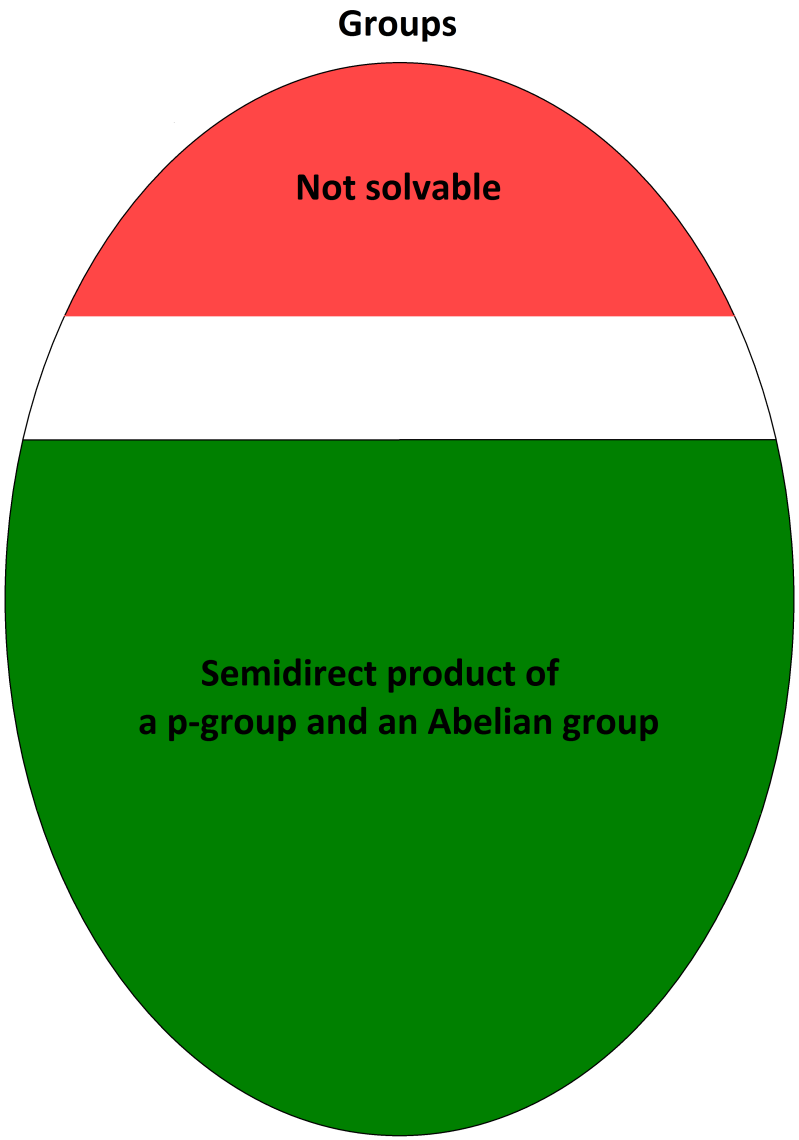
# Main ideas

- semidirect product: $\mathbf{N} \rtimes \mathbf{H} \Longrightarrow$
  an equation over $\mathbf{N}$ + an equation over $\mathbf{H}$
- $\mathbf{N}$ is a p-group $\Longrightarrow$ polycyclic generating system of $\mathbf{N} \Longrightarrow$
  characterization the multiplication of $\mathbf{N}$ with the **suitable** polynomials over $\mathbb{Z}_p$
- $\mathbf{H}$ Abelian, $p \nmid |\mathbf{H}| \Longrightarrow$ a field $\mathbb{F}_q$: $\mathbf{H} \leq \mathbb{F}_q^\times$ and $\mathbb{Z}_p \leq \mathbb{F}_q \Longrightarrow$
  characterization the conjugation with polynomials over $\mathbb{F}_q$
- solvability over $\mathbf{N} \rtimes \mathbf{H} \Longrightarrow$ system of equation over $\mathbb{F}_q$ is in P

# Results



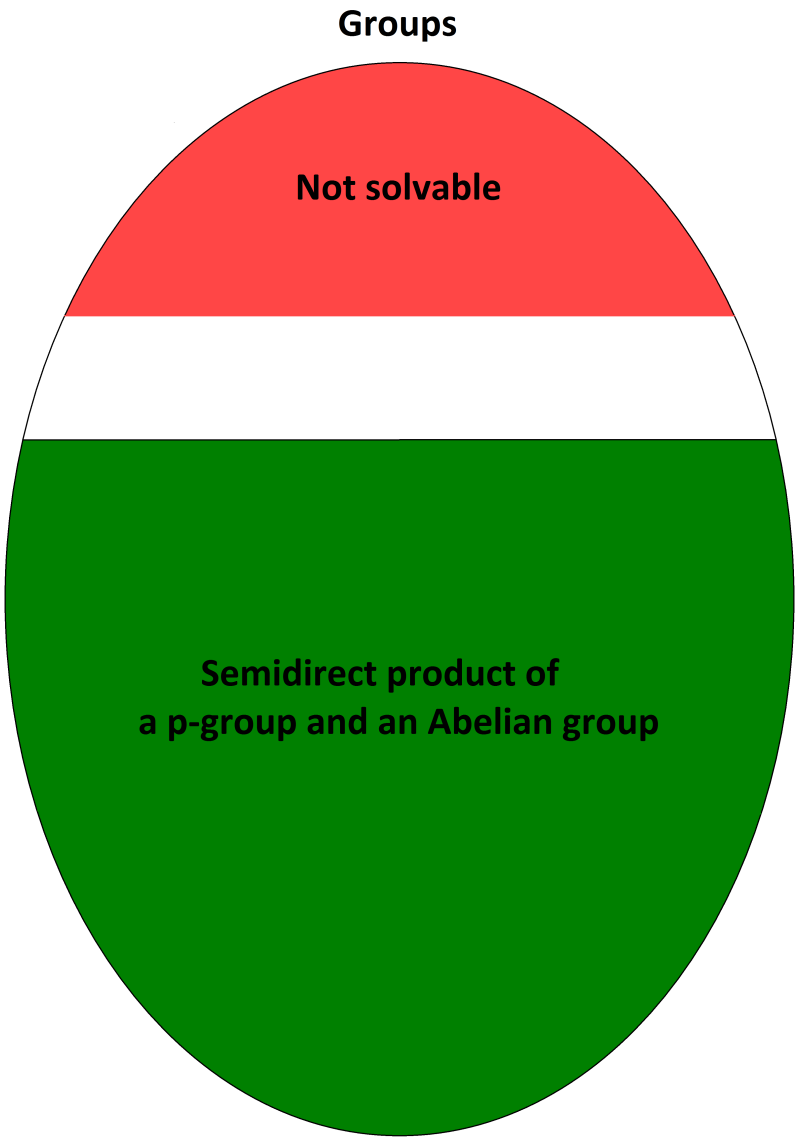
# Results




## Theorem (Földvári,Horváth)

$\mathbf{G} \cong \mathbf{P} \rtimes \mathbf{A} \Rightarrow$ *equation solvability in* $P$

# Results



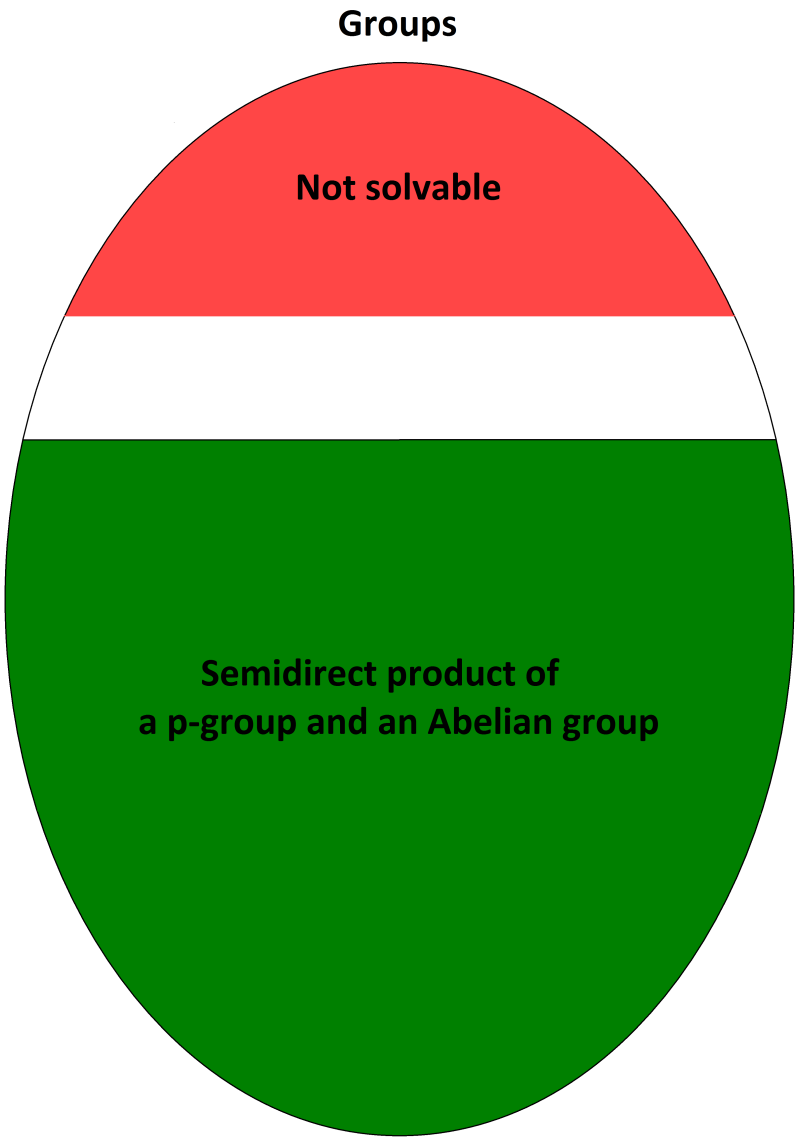

## Theorem (Földvári,Horváth)

$\mathbf{G} \cong \mathbf{P} \rtimes \mathbf{A} \Rightarrow$ *equation solvability in* $P$

## Corollary (Földvári)

$\mathbf{G}$ *nilpotent: solvability deciding in* $O\left(n^{|\mathbf{G}|^2 \log |\mathbf{G}|}\right)$ *time*

# Results




## Theorem (Földvári,Horváth)

$\mathbf{G} \cong \mathbf{P} \rtimes \mathbf{A} \Rightarrow$ *equation solvability in* $P$

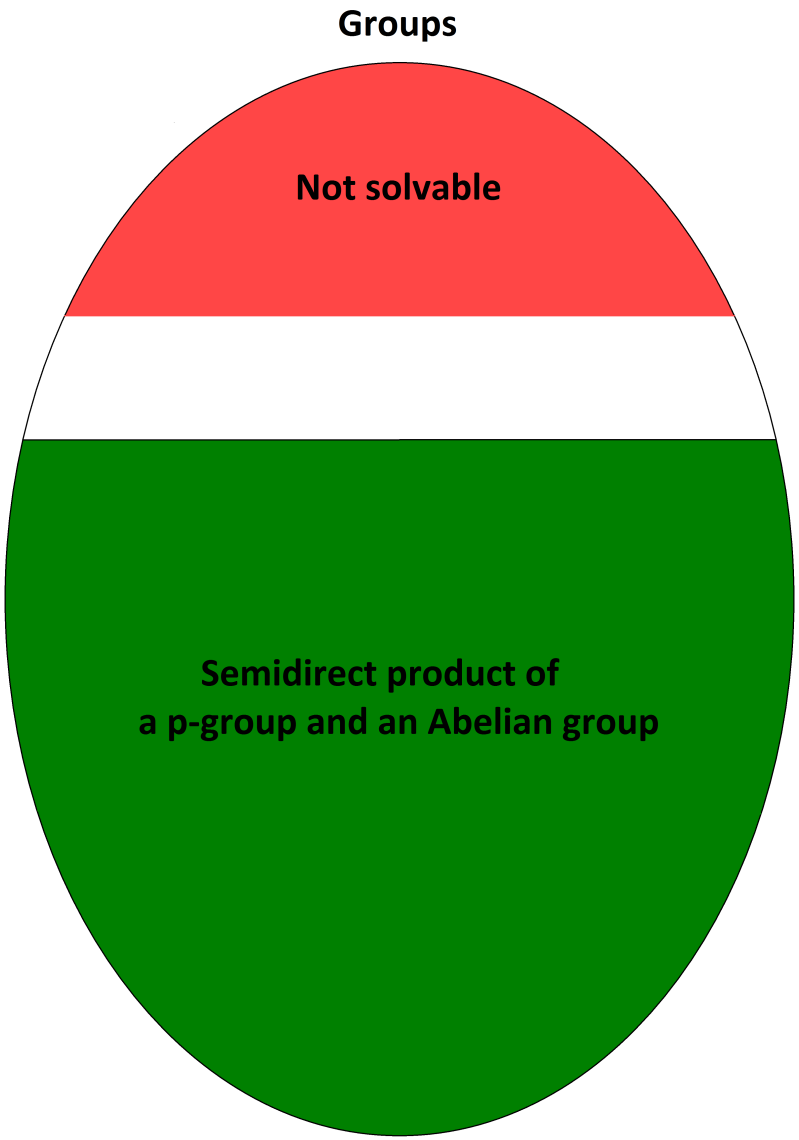
## Corollary (Földvári)

$\mathbf{G}$ *nilpotent: solvability deciding in* $O\left(n^{|\mathbf{G}|^2 \log |\mathbf{G}|}\right)$ *time*

## Question:

$\mathbf{S}_4$?

# Results




## Theorem (Földvári,Horváth)

$\mathbf{G} \cong \mathbf{P} \rtimes \mathbf{A} \Rightarrow$ *equation solvability in* $P$

## Corollary (Földvári)

$\mathbf{G}$ *nilpotent: solvability deciding in* $O\left(n^{|\mathbf{G}|^2 \log |\mathbf{G}|}\right)$ *time*

## Question:

$\mathbf{S}_4$?

## Thank you for your attention!

# The group $\mathbf{S}_4$

$\mathbf{S}_4$ is solvable $\implies$ $\mathbf{S}_4$ has a bases:

$$a = (1\ 2)(3\ 4), \quad b = (1\ 3)(2\ 4), \quad c = (1\ 2\ 4), \quad d = (2\ 4)$$

$$g \in \mathbf{S}_4 \implies \exists! x, y, u \in \{0,1\},\ z \in \{0,1,2\} : \quad g = a^x \cdot b^y \cdot c^z \cdot d^u$$

# The group $\mathbf{S}_4$

$\mathbf{S}_4$ is solvable $\implies$ $\mathbf{S}_4$ has a bases:

$$a = (1\ 2)(3\ 4), \quad b = (1\ 3)(2\ 4), \quad c = (1\ 2\ 4), \quad d = (2\ 4)$$

$$g \in \mathbf{S}_4 \implies \exists! x, y, u \in \{0,1\},\ z \in \{0,1,2\} : \quad g = a^x \cdot b^y \cdot c^z \cdot d^u$$

$$\begin{aligned} g_1 \cdots g_n &= a^{x_1} b^{y_1} c^{z_1} d^{u_1} \cdots a^{x_n} b^{y_n} c^{z_n} d^{u_n} = \\ &= a^{f_1(\dots)} \cdot b^{f_2(\dots)} \cdot c^{f_3(\dots)} \cdot d^{f_4(\dots)} \\ f_1, f_2, f_4 &\in \mathbb{F}_{2^\alpha}[x_1, y_1, z_1, u_1, \dots, x_n, y_n, z_n, u_n] \\ f_3 &\in \mathbb{F}_{3^\beta}[x_1, y_1, z_1, u_1, \dots, x_n, y_n, z_n, u_n] \end{aligned}$$

$\implies$ the lengths of $f_1(\dots)$ and $f_2(\dots)$ is exponential in $n$