Definability of linear equation systems over groups and rings

A. Dawar, E. Grädel, B. Holm, E. Kopczynski, W. Pakusa

University of Cambridge, University of Warsaw, RWTH Aachen University

AlMoTh, Ilmenau, 17 February 2012
A logic for polynomial time

Atserias, Bulatov, Dawar

\[ \text{Slv}(G) \notin \text{FP} + \text{C} \]

Dawar, Grohe, Holm, Laubner

\[ \text{FP} + \text{C} \preceq \text{FP} + \text{rk} \preceq \text{PTIME} \]
A logic for polynomial time

Atserias, Bulatov, Dawar \[ \text{Slv}(G) \not\in \text{FP} + C \]

Dawar, Grohe, Holm, Laubner \[ \text{FP} + C \not\subseteq \text{FP} + \text{rk} \leq \text{PTIME} \]

Matrix rank and linear equation systems

\textbf{Fields} \[ A \cdot x = b \text{ solvable iff } \text{rk}(A) = \text{rk}(A|b) : \]

If \( r = \text{rk}(A) \), then \( a_1 \cdot c_1 + \cdots + a_r \cdot c_r + a \cdot b = 0 \)
A logic for polynomial time

Atserias, Bulatov, Dawar \quad \text{S}lv(G) \notin \text{FP}+C

Dawar, Grohe, Holm, Laubner \quad \text{FP}+C \subseteq \text{FP}+rk \leq \text{PTIME}

Matrix rank and linear equation systems

**Fields** \( A \cdot x = b \) solvable iff \( \text{rk}(A) = \text{rk}(A|b) \):

If \( r = \text{rk}(A) \), then \( a_1 \cdot c_1 + \cdots + a_r \cdot c_r + a \cdot b = 0 \)

**Rings** Many notions (linear dependence, McCoy, inner rank, ...), unknown complexity, above characterisation fails

**Groups** Undefined
A logic for polynomial time

Atserias, Bulatov, Dawar \( \text{Slv}(G) \notin FP+C \)

Dawar, Grohe, Holm, Laubner \( FP+C \nsubseteq FP+rk \leq PTIME \)

Matrix rank and linear equation systems

**Fields** \( A \cdot x = b \) solvable iff \( rk(A) = rk(A|b) \):

If \( r = rk(A) \), then \( a_1 \cdot c_1 + \cdots + a_r \cdot c_r + a \cdot b = 0 \)

**Rings** Many notions (linear dependence, McCoy, inner rank, ...), unknown complexity, above characterisation fails

**Groups** Undefined

**Question:** Is \( \text{Slv}(G) \in FP+rk? \)
A systematic study of solvability

Inter-definability: \( \sim \) natural domain for Slv
A systematic study of solvability

Inter-definability: $\leadsto$ natural domain for $\text{Slv}$

**Theorem**

$k$-ideal rings $\overset{\text{FP-red.}}{\Longrightarrow}$ cyclic groups of prime power order.
A systematic study of solvability

Inter-definability: \(\sim\) natural domain for \(\text{Slv}\)

**Theorem**

\(k\)-ideal rings \(\overset{\text{FP-red.}}{\Longrightarrow}\) cyclic groups of prime power order.

Intra-definability: \(\sim\) FO extended by \(\text{Slv}_F\)
A systematic study of solvability

Inter-definability: $\leadsto$ natural domain for $\text{Slv}$

**Theorem**

$k$-ideal rings $\xrightarrow{\text{FP-red.}}$ cyclic groups of prime power order.

Intra-definability: $\leadsto$ FO extended by $\text{Slv}_F$

**Theorem**

Normal form for FO+$\text{slv}_F$. 
Inter-definability: a natural class for solvability

\( \text{Slv}(\mathbf{CG}) \): Cyclic groups \((\mathbb{Z}_p^e)\)
\( \text{Slv}(\mathbf{I}_k \mathbf{R}) \): \(k\)-gen. ideal rings \((I \leq R \Rightarrow I = \pi_1 R + \cdots + \pi_k R)\)
Inter-definability: a natural class for solvability

\[ \text{Slv}(\mathbf{CG}): \text{ Cyclic groups } (\mathbb{Z}_{p^e}) \]
\[ \text{Slv}(\mathbf{I_kR}): \text{ k-gen. ideal rings } (I \leq R \Rightarrow I = \pi_1 R + \cdots + \pi_k R) \]
Inter-definability: a natural class for solvability

\( \text{Slv}(\text{CG}) \): Cyclic groups (\( \mathbb{Z}_{p^e} \))
\( \text{Slv}(I_k R) \): \( k \)-gen. ideal rings (\( I \leq R \Rightarrow I = \pi_1 R + \cdots + \pi_k R \))
Inter-definability: a natural class for solvability

\( \text{Slv}(\text{CG}) \): Cyclic groups \( (\mathbb{Z}_p^e) \)

\( \text{Slv}(I_k R) \): \( k \)-gen. ideal rings \( (I \leq R \Rightarrow I = \pi_1 R + \cdots + \pi_k R) \)

- \( R \) local iff \( R \setminus R^* \leq R \)
Inter-definability: a natural class for solvability

\( \text{Slv}(\text{CG}) \): Cyclic groups \((\mathbb{Z}_{p^e})\)
\( \text{Slv}(I_k R) \): k-gen. ideal rings \((I \leq R \Rightarrow I = \pi_1 R + \cdots + \pi_k R)\)

\( \text{Slv}(I_k R) \)
\( \text{Slv}(\text{local-}I_k R) \)

\( R \) local iff \( R \setminus R^* \leq R \)

\( \mathbb{Z}_m \) local iff \( m = p^e \)

\( \text{Slv}(\text{CG}) \)
\( \text{Slv}(R_\prec) \)
Inter-definability: a natural class for solvability

\( \text{Slv}(\mathbb{Z}_p^e) \): Cyclic groups

\( \text{Slv}(I_k \mathbb{R}) \): k-gen. ideal rings (\( I \trianglelefteq R \Rightarrow I = \pi_1 R + \cdots + \pi_k R \))

\[ R = \bigoplus_{e \in \mathcal{E}} e \mathbb{R}, \ e \mathbb{R} \text{ local} \]

\( \text{Slv}(I_k \mathbb{R}) \xrightarrow{\text{R}} \text{Slv(local-I}_k \mathbb{R}) \)

\( \text{Slv}(\mathbb{C} \mathbb{G}) \)

\( \text{Slv}(\mathbb{R}_<) \)
Inter-definability: a natural class for solvability

\( \text{Slv}(CG) \): Cyclic groups \((\mathbb{Z}_p^e)\)
\( \text{Slv}(I_kR) \): \(k\)-gen. ideal rings \((I \subseteq R \Rightarrow I = \pi_1 R + \cdots + \pi_k R)\)

\[
\text{Slv}(I_kR) \xrightarrow{R = \bigoplus_{e \in \varphi} eR, \ eR \text{ local}} \text{Slv(local-I}_kR\text{)}
\]

\[
m = R \setminus R^* \subseteq R
\]

\[
\text{Slv}(CG) \text{ Slv}(R<)
\]
Inter-definability: a natural class for solvability

\( \text{Slv}(\text{CG}) \): Cyclic groups \( (\mathbb{Z}_{p^e}) \)

\( \text{Slv}(I_k R) \): k-gen. ideal rings \( (I \subseteq R \Rightarrow I = \pi_1 R + \cdots + \pi_k R) \)

\[
R = \bigoplus_{e \in \varnothing} eR, \ eR \text{ local}
\]

\[
\text{Slv}(I_k R) \quad \xrightarrow{\text{Slv}(\text{local-}I_k R)} \quad \text{Slv}(\Gamma(R) = \{ \alpha : \alpha^{\mid R/m\mid} = \alpha \})
\]

\[
\text{Slv}(\text{CG}) \quad \xrightarrow{\text{Slv}(\text{local-}I_k R)} \quad \text{Slv}(R_{<})
\]
Inter-definability: a natural class for solvability

**Slv**(CG): Cyclic groups ($\mathbb{Z}_p^e$)

**Slv**(IₖR): k-gen. ideal rings ($I \leq R \Rightarrow I = \pi_1 R + \cdots + \pi_k R$)

\[ R = \bigoplus_{e \in \varphi} eR, \ eR \text{ local} \]

\[ \text{Slv}(I_k R) \xrightarrow{\text{isom}} \text{Slv}(\text{local-}I_k R) \]

\[ m = R \setminus R^* \leq R \]

\[ \Gamma(R) = \{ a : a^{[R/m]} = a \} \]

\[ \Gamma(R) \tilde{\to} R/m, r \mapsto r + m \]

**Slv**(R<)
Inter-definability: a natural class for solvability

\( \text{Slv}(\mathbb{C}G) \): Cyclic groups \((\mathbb{Z}_p^e)\)
\( \text{Slv}(I_k R) \): \(k\)-gen. ideal rings \((I \trianglelefteq R \Rightarrow I = \pi_1 R + \cdots + \pi_k R)\)

\[
\text{Slv}(I_k R) \quad R = \bigoplus_{e \in \varphi} eR, eR \text{ local} \quad \text{Slv}(\text{local-}I_k R)
\]

\[
\begin{align*}
\text{Slv}(\mathbb{C}G) & \quad \text{Slv}(R_<) \\
\end{align*}
\]

\[
\begin{align*}
\text{Slv}(I_k R) \quad m = R \setminus R^* \trianglelefteq R \\
\Gamma(R) & = \{ a : a^{R/m} = a \} \\
\Gamma(R) \xrightarrow{\sim} & R/m, r \mapsto r + m \\
r & \mapsto \sum_{\epsilon \in \Gamma(R)} a_{i_1\cdots i_k} \pi_1^{i_1} \cdots \pi_k^{i_k}
\end{align*}
\]
Inter-definability: a natural class for solvability

\[ \text{Slv}(\mathbf{CG}): \text{Cyclic groups } (\mathbb{Z}_p^e) \]
\[ \text{Slv}(\mathbf{I}_k \mathbf{R}): \text{k-gen. ideal rings } (I \trianglelefteq R \Rightarrow I = \pi_1 R + \cdots + \pi_k R) \]

\[ R = \bigoplus_{e \in \varphi} eR, \ eR \text{ local} \]

\[ \text{Slv}(\mathbf{I}_k \mathbf{R}) \xrightarrow{R = \bigoplus_{e \in \varphi} eR, \ eR \text{ local}} \text{Slv(\text{local-}I_k \mathbf{R})} \]

\[ (\mathbf{R}, +) = \bigoplus_{g \in \psi} \langle g \rangle \]
\[ (A, b) \mapsto (A_1, b_1), \ldots, (A_k, b_k) \]

\[ \text{Slv}(\mathbf{CG}) \xleftarrow{\text{Slv}(\mathbf{R}_<)} \text{Slv}(\mathbf{R}_<) \]

\[ m = R \setminus R^* \trianglelefteq R \]
\[ \Gamma(R) = \{ a : a|^{R/m|} = a \} \]
\[ \Gamma(R) \xrightarrow{\sim} R/m, \ r \mapsto r + m \]
\[ r \mapsto \sum_{e \in \Gamma(R)} a_{i_1 \cdots i_k} \pi_1^{i_1} \cdots \pi_k^{i_k} \]
Inter-definability: a natural class for solvability

\( \text{Slv}(CG) \): Cyclic groups \((\mathbb{Z}_{p^e})\)
\( \text{Slv}(I_kR) \): \(k\)-gen. ideal rings \((I \trianglelefteq R \Rightarrow I = \pi_1 R + \cdots + \pi_k R)\)

\[
\text{Slv}(I_kR) \xrightarrow{R = \bigoplus_{e \in \varphi} eR, \text{ eR local}} \text{Slv(local-I}_k\text{R)}
\]

\[
\text{Slv}(CG) \xleftarrow{\text{Theorem}} \text{Slv}(R_<)
\]

\[
\text{m} = R \setminus R^* \trianglelefteq R
\]
\[
\Gamma(R) = \{a : a^{\lfloor R/m \rfloor} = a\}
\]
\[
\Gamma(R) \sim R/m, \ r \mapsto r + m
\]
\[
\sum_{a_{i_1} \ldots i_k} \pi_1^{i_1} \ldots \pi_k^{i_k}
\]

\[
\text{Theorem} \quad \text{Slv}(I_kR) \leq_{FP} \text{Slv}(CG)
\]
Intra-definability: solvability as a logical operator

\[ \text{slv}(\bar{x}, \bar{y}, \bar{r}_i).[\varphi_M(\bar{x}, \bar{y}, \bar{r}), \varphi_b(\bar{x}, \bar{r}), (\varphi_R, \varphi_+, \varphi.)(\bar{r}_1, \bar{r}_2, \bar{r}_3)] \]

- coefficient matrix
- solution vector
- finite ring
Intra-definability: solvability as a logical operator

$$\text{slv}(\bar{x}, \bar{y}, \bar{r}_i).[\varphi_M(\bar{x}, \bar{y}, \bar{r}), \varphi_b(\bar{x}, \bar{r}), (\varphi_R, \varphi_+, \varphi.)(\bar{r}_1, \bar{r}_2, \bar{r}_3)]$$

- coefficient matrix
- solution vector
- finite ring

$$\downarrow$$

**FO + slv**: First-order logic closed under solvability quantifier

**FO + slv$_F$**: Solvability quantifier over a fixed finite field $F$
Intra-definability: solvability as a logical operator

Theorem
Every FO+slv\textsubscript{F}-formula equivalent to an FO+slv\textsubscript{F}-formula

\[ \text{solv}(\bar{x}, \bar{y}).[\varphi_{\text{M}}(\bar{x}, \bar{y}), 1], \text{ with } \varphi_{\text{M}} \text{ quantifier-free.} \]
Intra-definability: solvability as a logical operator

Theorem
Every FO+slv\textsubscript{F}-formula equivalent to an FO+slv\textsubscript{F}-formula

\[ \text{slv}(\bar{x}, \bar{y}).[\varphi_M(\bar{x}, \bar{y}), 1], \text{ with } \varphi_M \text{ quantifier-free}. \]

Proof illustration: (negation)

\[ \neg \text{slv}(\bar{x}, \bar{y}).[\varphi, 1] \]

Non-solvability \equiv \neg \exists x : Mx = b \equiv \exists y : M'y = b' \equiv \text{Solvability}
Intra-definability: solvability as a logical operator

Theorem
Every FO+\text{slv}_F\text{-formula equivalent to an FO+}\text{slv}_F\text{-formula}

\[
\text{slv} (\tilde{x}, \tilde{y}). [\varphi_M (\tilde{x}, \tilde{y}), 1], \text{ with } \varphi_M \text{ quantifier-free.}
\]

Proof illustration: (negation)

\[
\neg \text{slv} (\tilde{x}, \tilde{y}). [\varphi, 1]
\]

Non-solvability \equiv \neg \exists x : Mx = b \equiv \exists y : M'y = b' \equiv \text{Solvability}

Gaussian elimination implies:

\[
\neg \exists x : Mx = b \equiv \exists y : y(M|b) = (0, \ldots, 0|1).
\]
Intra-definability: solvability as a logical operator

Theorem
Every FO+$\text{slv}_F$-formula equivalent to an FO+$\text{slv}_F$-formula

$$\text{slv}(\bar{x}, \bar{y}).[\varphi_M(\bar{x}, \bar{y}), 1], \text{ with } \varphi_M \text{ quantifier-free.}$$

Proof illustration: (conjunction)

$$\text{slv}(\bar{x}, \bar{y}).[\varphi, 1] \land \text{slv}(\bar{x}, \bar{y}).[\psi, 1]$$

\[
\begin{align*}
\varphi & \cdot \nu_y = 1 \\
\psi & \cdot \nu_y = 1
\end{align*}
\]
Intra-definability: solvability as a logical operator

Theorem
Every FO+slv_F-formula equivalent to an FO+slv_F-formula

\[ \text{solv}(\bar{x}, \bar{y}).[\varphi_M(\bar{x}, \bar{y}), 1], \text{ with } \varphi_M \text{ quantifier-free.} \]

Proof illustration: (conjunction)

\[ \text{solv}(\bar{x}, \bar{y}).[\varphi, 1] \land \text{solv}(\bar{x}, \bar{y}).[\psi, 1] \]
Intra-definability: solvability as a logical operator

**Theorem**
Every FO+slv\(_F\)-formula equivalent to an FO+slv\(_F\)-formula

\[ \text{slv}(\bar{x}, \bar{y}).[\varphi_M(\bar{x}, \bar{y}), 1], \text{ with } \varphi_M \text{ quantifier-free.} \]

**Proof illustration: (universal quantification)**

\[ \forall z (\text{slv}(\bar{x}, \bar{y}).[\varphi(\bar{x}, \bar{y}, z), 1]) \]

\[ \varphi(z_1) \cdot \mathbf{v_y} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \]

\[ \varphi(z_n) \cdot \mathbf{v_y} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \]
Intra-definability: solvability as a logical operator

Theorem
Every FO$+$slv$_F$-formula equivalent to an FO$+$slv$_F$-formula

\[ \text{slv}(\bar{x}, \bar{y}).[\varphi_M(\bar{x}, \bar{y}), 1], \text{ with } \varphi_M \text{ quantifier-free.} \]

Proof illustration: (universal quantification)

\[ \forall z (\text{slv}(\bar{x}, \bar{y}).[\varphi(\bar{x}, \bar{y}, z), 1]) \]

\[ \varphi(z_1) \cdot \mathbf{v}_y = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \quad \sim \quad \varphi(z_1) \cdot \mathbf{v}_y = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \]

\[ \varphi(z_n) \cdot \mathbf{v}_y = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \quad \sim \quad \varphi(z_n) \cdot \mathbf{v}_y = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \]
**Intra-definability: solvability as a logical operator**

**Theorem**
Every FO+$\slv_F$-formula equivalent to an FO+$\slv_F$-formula

$$\slv(\bar{x}, \bar{y}).[\varphi_M(\bar{x}, \bar{y}), 1], \text{ with } \varphi_M \text{ quantifier-free.}$$

**Proof illustration: (nesting of solvability)**

$$\slv(\bar{r}, \bar{s}).[\slv(\bar{x}, \bar{y}).[\varphi(\bar{r}, \bar{s}, \bar{x}, \bar{y}), 1], 1]$$

**Outer system: S**

**Inner system: I[\bar{r}, \bar{s}]**
Intra-definability: solvability as a logical operator

Proof illustration: (nesting of solvability)

\[
\text{solv}(\bar{\rho}, \bar{s}).[\text{solv}(\bar{x}, \bar{y}).[\varphi(\bar{\rho}, \bar{s}, \bar{x}, \bar{y}), 1], 1]
\]
Intra-definability: solvability as a logical operator

Proof illustration: (nesting of solvability)

\[
\text{slv}(\bar{r}, \bar{s}).[\text{slv}(\bar{x}, \bar{y}).[\varphi(\bar{r}, \bar{s}, \bar{x}, \bar{y}), 1], 1]
\]

For \( \bar{r} \): \( \sum_{\bar{s}} \alpha[\bar{r}, \bar{s}] \cdot v_{\bar{s}} = 1 \)
Intra-definability: solvability as a logical operator

Proof illustration: (nesting of solvability)

\[ \text{slv}(\bar{r}, \bar{s}).[\text{slv}(\bar{x}, \bar{y}).[\varphi(\bar{r}, \bar{s}, \bar{x}, \bar{y}), 1], 1] \]

For \( \bar{r} \): \( \sum_{\bar{s}} a[\bar{r}, \bar{s}] \cdot v_{\bar{s}} = 1 \)

\[ \downarrow \]

For \( \bar{r} \): \( \sum_{\bar{s}} 1 \cdot v[\bar{r}, \bar{s}] = 1 \)
Intra-definability: solvability as a logical operator

Proof illustration: (nesting of solvability)

\[ \text{slv}(\bar{r}, \bar{s}).[\text{slv}(\bar{x}, \bar{y}).[\varphi(\bar{r}, \bar{s}, \bar{x}, \bar{y}), 1], 1] \]

For \( \bar{r} \): \( \sum_{\bar{s}} a[\bar{r}, \bar{s}] \cdot \nu_{\bar{s}} = 1 \)

Consistency conditions:

\( \nu[\bar{r}, \bar{s}] = 1 \Rightarrow a[\bar{r}, \bar{s}] = 1 \)

\( \nu[\bar{r}, \bar{s}] \neq \nu[\bar{r}', \bar{s}] \Rightarrow a[\bar{r}, \bar{s}] \neq a[\bar{r}', \bar{s}] \)

For \( \bar{r} \): \( \sum_{\bar{s}} 1 \cdot \nu[\bar{r}, \bar{s}] = 1 \)
Intra-definability: solvability as a logical operator

Proof illustration: (nesting of solvability)

\[ \text{slv}(\bar{r}, \bar{s}).[\text{slv}(\bar{x}, \bar{y}).[\varphi(\bar{r}, \bar{s}, \bar{x}, \bar{y}), 1], 1] \]

For \( \bar{r} \): \( \sum_{\bar{s}} a[\bar{r}, \bar{s}] \cdot v_{\bar{s}} = 1 \)

Consistency conditions:

\[ v[\bar{r}, \bar{s}] = 1 \Rightarrow a[\bar{r}, \bar{s}] = 1 \]

\[ v[\bar{r}, \bar{s}] \neq v[\bar{r}', \bar{s}] \Rightarrow a[\bar{r}, \bar{s}] \neq a[\bar{r}', \bar{s}] \]

For \( \bar{r} \): \( \sum_{\bar{s}} 1 \cdot v[\bar{r}, \bar{s}] = 1 \)

How to formalise: “If \( v = 1 \) then \( A \cdot x = 1 \) solvable”
Intra-definability: solvability as a logical operator

Proof illustration: (nesting of solvability)

\[ \text{slv}(\bar{r}, \bar{s}).[\text{slv}(\bar{x}, \bar{y}).[\varphi(\bar{r}, \bar{s}, \bar{x}, \bar{y}), 1], 1] \]

For \( \bar{r} \): \( \sum_{\bar{s}} a[\bar{r}, \bar{s}] \cdot v[\bar{s}] = 1 \)

Consistency conditions:

- \( v[\bar{r}, \bar{s}] = 1 \Rightarrow a[\bar{r}, \bar{s}] = 1 \)
- \( v[\bar{r}, \bar{s}] \neq v[\bar{r}', \bar{s}] \Rightarrow a[\bar{r}, \bar{s}] \neq a[\bar{r}', \bar{s}] \)

For \( \bar{r} \): \( \sum_{\bar{s}} 1 \cdot v[\bar{r}, \bar{s}] = 1 \)

How to formalise: “If \( v = 1 \) then \( A \cdot x = 1 \) solvable”
Conclusion and outlook

Theorem
Every FO+slv\(_F\)-formula is equivalent to an FO+slv\(_F\)-formula

\[ \text{slv}(\bar{x}, \bar{y}).[\varphi_M, 1], \text{ with } \varphi_M \text{ quantifier-free.} \]

Theorem
\(k\)-ideal rings \(\xrightarrow{\text{FP-red.}}\) cyclic groups of prime power order.
Conclusion and outlook

Theorem
Every FO+$\text{slv}_F$-formula is equivalent to an FO+$\text{slv}_F$-formula

$$\text{slv}(\bar{x}, \bar{y}).[\varphi_M, 1], \text{ with } \varphi_M \text{ quantifier-free}.$$  

Theorem
$k$-ideal rings $\xrightarrow{\text{FP-red.}}$ cyclic groups of prime power order.

Outlook: Permutation group membership (GM)

Given: Permutations $\pi_1, \ldots, \pi_k$ and $\pi$ on a set $A$

Question: Is $\pi \in \langle \pi_1, \ldots, \pi_l \rangle \leq S_A$?
Conclusion and outlook

Theorem
Every FO+slv\textsubscript{F}-formula is equivalent to an FO+slv\textsubscript{F}-formula

\[ \text{slv}(\overline{x}, \overline{y}).[\varphi_M, 1], \text{ with } \varphi_M \text{ quantifier-free.} \]

Theorem
\(k\)-ideal rings FP-red. \(\iff\) cyclic groups of prime power order.

Outlook: Permutation group membership (GM)

**Given:** Permutations \(\pi_1, \ldots, \pi_k\) and \(\pi\) on a set \(A\)

**Question:** Is \(\pi \in \langle \pi_1, \ldots, \pi_k \rangle \leq S_A\)?

\[ \text{Slv}(D) \overset{\text{FO-reduction}}{\leftrightarrow} \text{GM} \quad (\text{Cayley’s theorem}) \]