Abelianess and Solvability

David Stanovský

Charles University, Prague, Czech Republic
stanovsk@karlin.mff.cuni.cz

joint work with Petr Vojtěchovský, University of Denver

September 2013
What is a solvable algebra?

Theorem (Galois 1830s)

\[ \text{Gal}(f) \text{ is solvable (as a group) iff } f \text{ is solvable (in radicals).} \]
In groups

A group $G$ is **solvable** iff

- there are $N_i \trianglelefteq G$ such that $1 = N_0 \leq N_1 \leq \ldots \leq N_k = G$ and $N_{i+1}/N_i$ are abelian groups
- there are abelian groups $A_i$ s.t. $G \simeq A_1 : (A_2 : \ldots (A_{k-1} : A_k))$

A group $G$ is **nilpotent** iff

- there are $N_i \trianglelefteq G$ such that $1 = N_0 \leq N_1 \leq \ldots \leq N_k = G$ and $N_{i+1}/N_i \leq Z(G/N_i)$
- there are abelian groups $A_i$ s.t. $G \simeq A_1 :c (A_2 :c \ldots (A_{k-1} :c A_k))$

$G = A : F$ is an **(abelian) extension**: $A \trianglelefteq G$ is abelian, $G/A \simeq F$ and

$$(a, x)(b, y) = (\varphi_{x,y}(a) + \psi_{x,y}(b) + \theta_{x,y}, xy), \quad \varphi_{x,y}, \psi_{x,y} \in \text{Aut}(A)$$

... **central extension** iff $\varphi = \psi = id$
In finite groups

Structural theorems, e.g.,

- $p$-groups are nilpotent
- finite nilpotent groups are direct products of $p$-groups
- (Feit, Thompson) groups of odd order are solvable

Characterizations, e.g.,

- Galois’ theorem
- a finite group is solvable iff it is not Boolean complete

$BC = \text{there is a polynomial subreduct isomorphic to 2-elt Boolean a.}$

Computational problems, e.g.,

- equation solving: nilpotent $\Rightarrow$ P, not solvable $\Rightarrow$ NP-complete
- identity checking: nilpotent $\Rightarrow$ P, not solvable $\Rightarrow$ coNP-complete
- circuit evaluation: solvable $\Rightarrow$ ACC$^1$, not solvable $\Rightarrow$ P-complete
In universal algebra

A is **solvable** if there are $\alpha_i \in \text{Con}(A)$ such that
$0_A = \alpha_0 \leq \alpha_1 \leq ... \leq \alpha_k = 1_A$ and $\alpha_{i+1}/\alpha_i$ is an abelian congr. in $A/\alpha_i$

A is **nilpotent** if there are $\alpha_i \in \text{Con}(A)$ such that
$0_A = \alpha_0 \leq \alpha_1 \leq ... \leq \alpha_k = 1_A$ and $\alpha_{i+1}/\alpha_i \leq \zeta(A/\alpha_i)$

A is **abelian** if dtto with $k = 1$

$\alpha$ abelian in $A$ iff (TC) for every term $t$ and every $x\alpha y$, $u_i \alpha v_i$

$\alpha \in \zeta(A)$ iff (TC) for every term $t$ and every $x\alpha y$ and $u_i, v_i$ arbitrary

(TC)

$t(x, u_1, ..., u_n) = t(x, v_1, ..., v_n) \Rightarrow t(y, u_1, ..., u_n) = t(y, v_1, ..., v_n)$
In universal algebra

A is **solvable** if there are \( \alpha_i \in \text{Con}(A) \) such that

\[
0_A = \alpha_0 \leq \alpha_1 \leq \ldots \leq \alpha_k = 1_A \text{ and } \alpha_{i+1}/\alpha_i \text{ is an abelian congr. in } A/\alpha_i
\]

A is **nilpotent** if there are \( \alpha_i \in \text{Con}(A) \) such that

\[
0_A = \alpha_0 \leq \alpha_1 \leq \ldots \leq \alpha_k = 1_A \text{ and } \alpha_{i+1}/\alpha_i \leq \zeta(A/\alpha_i)
\]

A is **abelian** if dtto with \( k = 1 \)

\( \alpha \) **abelian in** \( A \) iff (TC) for every term \( t \) and every \( x \alpha y, u_i \alpha v_i \)

\( \alpha \in \zeta(A) \) iff (TC) for every term \( t \) and every \( x \alpha y \) and \( u_i, v_i \) arbitrary

(TC)

\[
t(x, u_1, \ldots, u_n) = t(x, v_1, \ldots, v_n) \Rightarrow t(y, u_1, \ldots, u_n) = t(y, v_1, \ldots, v_n)
\]

Abelian extensions?
Other nice properties?

**TCT:** type 3 \( \Rightarrow \) BC; no type 3 \( \Rightarrow \) ???
In algebras with a Mal’tsev term

\[ m(x, x, y) = m(y, x, x) = y \]

**Fact** (Gumm-Smith):
An algebra with a Mal’tsev term is *abelian* iff it is poly. equiv. to a *module*.

But abelian congruences / extensions are less clear.
In algebras with a Mal’tsev term

\[ m(x, x, y) = m(y, x, x) = y \]

**Fact** (Gumm-Smith): An algebra with a Mal’tsev term is *abelian* iff it is poly. equiv. to a *module*. But abelian congruences / extensions are less clear.

So are generalizations of many group theory results. Nevertheless:

**TCT**: no type 3 ⇒ solvable ⇔ no 2-snags ⇒ not BC
Hence, ”solvable iff not BC” for algebras with a Mal’tsev term

(Horváth) identity checking, equation solving as in groups
In loops

A loop is an algebra \((L, \cdot, \setminus, 1)\) such that
- \(1x = x1 = x\)
- \(\forall x, y \) there are unique \(u = x \setminus y\), \(v = y / x\) such that \(xu = y\), \(vx = y\)

Mal’tsev term: \(m(x, y, z) = (x/y)z\)

\[
\text{Mlt}(L) = \langle L_a, R_a : a \in L \rangle \\
\text{Inn}(L) = \text{Mlt}(L)_1 = \langle L_{a,b}, R_{a,b}, T_a : a, b \in L \rangle
\]

\[
L_{a,b} = L_{ab}^{-1}L_aL_b \\
L_{a,b} = R_{ba}^{-1}R_aR_b \\
T_a = L_a^{-1}R_a
\]

Normal subloops \(\leftrightarrow\) congruences
- = kernels of a homomorphisms
- = subloops invariant with respect to \(\text{Inn}(L)\)
In loops

Fact: A loop is **abelian** iff it is an abelian group

Fact: \( Z(L) = \{ a \in L : ax = xa, a(xy) = (ax)y, (xa)y = x(ay) \ \forall \ x, y \in L \} \)

Hence \( L \) is **nilpotent** if there are \( N_i \leq L \) such that
\[ 1 = N_0 \leq N_1 \leq \ldots \leq N_k = L \ \text{and} \ \frac{N_{i+1}}{N_i} \leq Z(L/N_i) \]

Fact: TFAE

- \( A \leq Z(L) \)
- \( \varphi_{r,s}(a) = 1 \) for every \( a \in A, \ r, s \in L, \ \varphi \in \{ L, R, T \} \)
- \( L \cong A : c \ F \) where \( A \) is an abelian group, with operation
  \[ (a, x)(b, y) = (a + b + \theta_{x,y}, xy) \]
In loops

Fact: A loop is **abelian** iff it is an abelian group

Fact: \( Z(L) = \{ a \in L : ax = xa, a(xy) = (ax)y, (xa)y = x(ay) \, \forall \, x, y \in L \} \)

Hence \( L \) is **nilpotent** if there are \( N_i \sqsubseteq L \) such that
\[
1 = N_0 \leq N_1 \leq \ldots \leq N_k = L \text{ and } N_{i+1}/N_i \leq Z(L/N_i)
\]

Fact: TFAE

- \( A \leq Z(L) \)
- \( \varphi_{r,s}(a) = 1 \) for every \( a \in A, \, r, s \in L, \, \varphi \in \{ L, R, T \} \)
- \( L \simeq A :_c F \) where \( A \) is an abelian group, with operation
\[
(a, x)(b, y) = (a + b + \theta_{x,y}, xy)
\]

!!! \( A \trianglelefteq L \) is an abelian group \( \not\Rightarrow \) the corresp. congr. is abelian in \( L \) !!!
In loops

Main Theorem (S., Vojtěchovský)

$L$ loop, $A \trianglelefteq L$ then the following are equivalent:

- $A$ is abelian in $L$
- $\varphi_{r,s}(a) = \varphi_{u,v}(a)$ for every $a, r/u, s/v \in A, \varphi \in \{L, R, T\}$
- $L \simeq A : F$ where $A$ is an abelian group, with operation

$$(a, x)(b, y) = (\varphi_{x,y}(a) + \psi_{x,y}(b) + \theta_{x,y}, xy)$$

where $\varphi_{x,y}, \psi_{x,y} \in \text{Aut}(A), \theta_{x,y} \in A$ with $\varphi_{x,1} = \psi_{1,x} = 1, \theta_{x,1} = \theta_{1,x} = 0$.

Compare:

- $A \leq Z(L)$
- $\varphi_{r,s}(a) = a$ for every $a \in A, r, s \in L, \varphi \in \{L, R, T\}$
- $L \simeq A : c F$ with $(a, x)(b, y) = (a + b + \theta_{x,y}, xy)$
Loops and their associated groups

\begin{center}
\begin{tikzpicture}
\node (Q) at (0,0) {$Q$};
\node (MltQ) at (2,0) {$\text{Mlt } Q$};
\node (InnQ) at (4,0) {$\text{Inn } Q$};
\node (abelian) at (-2,-2) {abelian};
\node (supernilpotent) at (-2,-4) {supernilpotent};
\node (centrally-nilpotent) at (-2,-6) {(centrally) nilpotent};
\node (congruence-solvable) at (-2,-8) {congruence-solvable};
\node (Bruck-solvable) at (-2,-10) {Bruck-solvable};
\node (Bruck) at (0,-2) {$\text{Bruck}$};
\node (Wright) at (2,-2) {$\text{Wright}$};
\node (Niemennmaa) at (4,-2) {$\text{Niemennmaa}$};
\node (Vesanen) at (2,-4) {$\text{Vesanen}$};
\draw (Q) -- (MltQ);
\draw (MltQ) -- (InnQ);
\draw (abelian) -- (supernilpotent);
\draw (supernilpotent) -- (centrally-nilpotent);
\draw (centrally-nilpotent) -- (congruence-solvable);
\draw (congruence-solvable) -- (Bruck-solvable);
\draw (abelian) -- (Bruck);
\draw (abelian) -- (Wright);
\draw (abelian) -- (Niemennmaa);
\draw (abelian) -- (Vesanen);
\end{tikzpicture}
\end{center}
Feit-Thompson theorem

**Theorem (Feit-Thompson 1962)**

*Groups of odd order are solvable.*

**Theorem (Glauberman 1964/68)**

*Moufang loops of odd order are weakly solvable.*

$L$ is *weakly solvable* if there are $H_i \leq L$ such that

$1 = H_0 \triangleleft H_1 \triangleleft \ldots \triangleleft H_k = L$ and $H_{i+1}/H_i$ are abelian groups

**Problem**

*Are Moufang loops of odd order solvable?*

*Are other loops of ??? ???? solvable?*
WOW, WHAT A GREAT AUDIENCE!