Classical solvability and congruence solvability in Moufang loops

Petr Vojtěchovský (joint work with Aleš Drápal)

UNIVERSITY OF DENVER

Loops '23
July 1, 2023
IMPAN Bedlewo, Poland

Commutator of congruences

In 1978, Freese and McKenzie developed commutator theory for congruence modular varieties.

Definition

Let A be an algebra and α, β, δ congruences of A. Then α **centralizes** β **over** δ if

$$t(\vec{x}, \vec{u})\delta t(\vec{x}, \vec{v}) \;\Rightarrow\; t(\vec{y}, \vec{u})\delta t(\vec{y}, \vec{v})$$

whenever t is a term, $x_i \alpha y_i$ and $u_i \beta v_i$.

Definition

The **commutator** $[\alpha, \beta]$ **of congruences** is the smallest congruence δ such that α centralizes β over δ.

Solvability in general

Let $0_A = \{(a, a) : a \in A\}$ and $1_A = A \times A$.

An algebra A is **solvable** if the "derived series"

$$\gamma^0 = 1_A, \quad \gamma^{i+1} = [\gamma^i, \gamma^i]$$

reaches 0_A in finitely many steps.

Congruence commutators in groups and loops

Normal subloops $=$ congruence classes containing 1.

Deviations from commutativity and associativity:

$$T_a(x) = ax/a, \quad L_{a,b}(x) = (ab)\backslash(a(bx)), \quad R_{a,b}(x) = ((xa)b)/(ab).$$

Theorem (Stanovský + V 2014, improved by Barnes 2021)

Let α, β be congruences of a loop Q. Then $[\alpha, \beta]$ is the congruence generated by

$$(T_{u_1}(a), T_{v_1}(a)),\ (L_{u_1,u_2}(a), L_{v_1,v_2}(a)),\ (R_{u_1,u_2}(a), R_{v_1,v_2}(a)),$$

where $1 \alpha a$ and $u_i \beta v_i$.

Classical solvability vs. congruence solvability for loops

Classical solvability: (Bruck, Glauberman)
$1 = Q_0 \leq Q_1 \leq \cdots \leq Q_n = Q$, where each factor Q_{i+1}/Q_i is an abelian group.

A normal subloop X of Q **induces an abelian congruence** if $[X, X]_Q = 1$.

Congruence solvability:
$1 = Q_0 \leq Q_1 \leq \cdots \leq Q_n = Q$, where each factor Q_{i+1}/Q_i *induces an abelian congruence* of Q/Q_i.

Open problems

- For which varieties of loops the two solvability theories coincide?
- In which varieties of loops does every abelian normal subloop $X \trianglelefteq Q$ induce an abelian congruence of Q?
- Moufang loops do not satisfy the second property, but *might* satisfy the first.

Abelian extensions

Definition

Let $(X, +)$ be an abelian group and $(F, \cdot)$ a loop. Then $Q = (F \times X, *)$ is an **abelian extension of X by F** if

$$(r, x) * (s, y) = (rs, \varphi_{r,s}(x) + \psi_{r,s}(y) + \theta_{r,s}),$$

where $\varphi_{r,s}, \psi_{r,s} \in \mathrm{Aut}(X)$, $\theta_{r,s} \in X$ and $\varphi_{r,1} = \psi_{1,r} = \mathrm{id}_X$, $\theta_{r,1} = \theta_{1,r} = 0$.

Theorem (Stanovský + V)

Let X be an abelian group, $X \trianglelefteq Q$. Then $[X, X]_Q = 1$ iff Q is an abelian extension of X by Q/X. A loop is congruence solvable iff it is an iterated abelian extension.

Abelian extensions in groups

Lemma

Let G be a group and X an abelian normal subgroup of Q. Then $[X, X]_Q = 1$.

Proof.

Internal version of abelian extension: $X \trianglelefteq Q$, U a left transversal to X in Q and

$$rx \cdot sy = u_{r,s} \cdot \varphi_{r,s}(x)\psi_{r,s}(y)\theta_{r,s},$$

where $u_{r,s} \in U \cap (rs)X$.

Here we have

$$rx \cdot sy = rss^{-1}xsy = u_{r,s}(u_{r,s}^{-1}rs)(s^{-1}xs)y = u_{r,s}(s^{-1}xs)y(u_{r,s}^{-1}rs),$$

so it suffices to take $\varphi_{r,s} = T_s^{-1}|_X$, $\psi_{r,s} = \mathrm{id}_X$ and $\theta_{r,s} = u_{r,s}^{-1}rs$. □

Nuclear case

The next result follows nearly as easily as the group case:

Lemma

Let X be an abelian normal subloop of Q such that $X \leq \mathrm{Nuc}_m(Q) \cap \mathrm{Nuc}_r(Q)$. Then $[X, X]_Q = 1$.

We will greatly generalize this result for **Moufang loops**, that is, loops satisfying one of the identities

$$x(y(xz)) = ((xy)x)z,$$
$$x(y(zy)) = ((xy)z)y,$$
$$(xy)(zx) = (x(yz))x,$$
$$(xy)(zx) = x((yz)x).$$

A construction for $[X, X]_Q \neq 1$ in Moufang loops

- $W = (W, +)$ be a commutative group with subgroups $F \leq B \leq W$ (specialize to $F = B$ at first reading)
- $F = \{0, 1\}$ and $\overline{W} = W/B$ an elementary abelian 2-group,
- $\overline{q} : \overline{W} \to F$ a quadratic form with associated bilinear form $\overline{h} : \overline{W} \times \overline{W} \to F$,
- $q : W \to F$ and $h : W \times W \to F$ defined by $q(u) = \overline{q}(\overline{u})$ and $h(u, v) = \overline{h}(\overline{u}, \overline{v})$,
- define multiplication on $Q = F \times W$ by

$$(i, u) \cdot (j, v) = (i + j,\ u + v + jq(u) + ih(u, v)).$$

A construction for $[X, X]_Q \neq 1$ in Moufang loops

Then:

- Q is a centrally nilpotent loop, a central extension of the commutative group B by the elementary abelian 2-group $F \times \overline{W}$,
- Q is congruence solvable and hence classically solvable,
- Q is a Moufang loop,
- Q is a group if and only if the quadratic form $\overline{q}$ is linear,
- $X = 0 \times W$ is an abelian normal subloop of Q,
- if Q is not a group, then the congruence of Q induced by X is not abelian.

Results of Bruck (more or less)

From now on let Q be a Moufang loop.

- every inner mapping is a pseudoautomorphism, that is, $cf(x) \cdot f(y) = cf(xy)$ for a suitable c,
- every pseudoautomorphism is a semiautomorphism, that is, $f(xyx) = f(x)f(y)f(x)$ and $f(1) = 1$,
- semiautomorphisms satisfy $f(x^n) = f(x)^n$

Lemma

Let X be a 2-divisible abelian group. Then every semiautomorphism of X is an automorphism of X.

Proof.

$f(xy)=f(u^2y)=f(uyu)=f(u)f(y)f(u)=f(u)^2f(y)=f(u^2)f(y)=f(x)f(y)$. □

Results of Bruck (more or less)

Corollary

Let Q be a Moufang loop and X an abelian normal subloop of Q that is 2-divisible. Then every inner mapping of Q restricts to an automorphism of X.

Results of Gagola

Theorem

Suppose that $Q = \langle S \rangle$ is a Moufang loop such that every element of S is a cube. Then $\mathrm{Inn}(Q) = \langle T_u : u \in Q \rangle$.

Theorem

Let Q be a Moufang loop and $x, y, u \in Q$. Then

$$u^{3i}x \cdot u^{3j}y = u^{3(i+j)}T_u^{-i-2j}(T_u^{i-j}(x)T_u^{i-j}(y))$$

for all $i, j \in \mathbb{Z}$.

Abelian extensions again

Suppose that Q is a 3-divisible Moufang loop with a 2-divisible abelian normal subgroup X. Let's calculate:

$rx \cdot sy = rx \cdot sys^{-1}s = rx \cdot T_s(y)s$
and T_s restricts to an automorphism of X since X is 2-divisible

$rx \cdot T_s(y)s = (s \cdot (s^{-1}r)f(x)) \cdot T_s(y)s = s \cdot ((s^{-1}r)f(x) \cdot T_s(y)) \cdot s$
with the inner mapping $f = L^{-1}_{s^{-1}r} L^{-1}_s L_r$

rewrite as $s(uv \cdot w)s = s(u(vu^{-1} \cdot uw)s) = su \cdot (vu^{-1} \cdot uw)s$
using Moufang identities

$vu^{-1} \cdot uw = va^{-3} \cdot a^3 w = T_a^{-1}(T_a(v)T_a(w)) = vw$
by 3-divisibility and Gagola

get $su \cdot (vw)s$, etc, bring it to the desired form.

The 6-divisible case

Theorem (D+V)

Let Q be a 3-divisible Moufang loop and X a 2-divisible abelian normal subgroup of Q. Then $[X, X]_Q = 1$.

Corollary (D+V)

Let Q be a 6-divisible Moufang loop. Then Q is congruence solvable iff it is classically solvable.

Characterizing $[X, X]_Q = 1$

Theorem (D+V)

Let Q be a Moufang loop and X a normal subloop of Q. Then $[X, X]_Q = 1$ (in particular, X is an abelian group) iff every inner mapping of Q restricts to an automorphism of X and $u \cdot xy = uy \cdot x$ for all $u \in Q$ and $x, y \in X$.

Characterizing $[X, X]_Q = 1$ when Q is 3-divisible

Theorem (D+V)

Let Q be a 3-divisible Moufang loop and X a normal subloop of Q. Then $[X, X]_Q = 1$ iff $u \cdot xy = uy \cdot x$ for all $u \in Q$ and $x, y \in X$.

Proof.

By Gagola, it suffices to check that $T_u|_X$ is an automorphism of X. By the second result of Gagola, we have

$$u^3 \cdot xy = u^3 \cdot yx = u^3 x \cdot y = u^3 T_u^{-1}(T_u(x) T_u(y)).$$

□

The main result here

After much additional work and using this result of Aleš:

Theorem (Drápal)

Let Q be a finite Moufang loop, p a prime and S a p-subloop of Q. Then $\mathrm{Mlt}_Q(S) = \langle L_s, R_s : s \in S \rangle$ is a p-group.

... we proved

Theorem (D+V)

Let Q be a finite 3-divisible Moufang loop. Then Q is congruence solvable iff it is classically solvable.

Results of Glauberman and Csörgő

We wish to strengthen the following result:

Theorem (Glauberman)

Every Moufang loop of odd order is classically solvable.

We will use:

Theorem (Csörgő)

Every nontrivial Moufang loop of odd order has a nontrivial nucleus.

The final result

Theorem (D+V)

Every Moufang loop of odd order is congruence solvable.

- let Q be a smallest counterexample
- clearly $1 < Q$, so $1 < N = \mathrm{Nuc}(Q)$ by Csörgő
- we can assume $N < Q$ else we are done by Feit-Thompson
- let X be a minimal characteristic subgroup of N and $f \in \mathrm{Inn}(Q)$
- since $X \leq N$ and $X \trianglelefteq Q$, we have $f|_X \in \mathrm{Aut}(X)$
- standard group theory argument implies that X is an abelian group
- thus $[X, X]_Q = 1$
- since Q/X is congruence solvable by minimality, Q is an iterated abelian extension

Thank you!


A.A. Albert, *Quasigroups. II.*, Trans. Amer. Math. Soc. **55** (1944), 401–419.


R.H. Bruck, *Contributions to the theory of loops*, Trans. Amer. Math. Soc. **60** (1946), 245–354.


P. Csörgő, *Every Moufang loop of odd order has nontrivial nucleus*, J. Algebra **603** (2022), 89–117.


A. Drápal and P. Vojtěchovský, *Abelian congruences and solvability in Moufang loops*, to appear in J. Algebra.


A. Drápal and P. Vojtěchovský, *Congruence solvability in finite Moufang loops of order coprime to three*, submitted.


R. Freese and R. McKenzie, *Commutator theory for congruence modular varieties*, London Mathematical Society Lecture Note Series **125**, Cambridge University Press, Cambridge, 1987.


G. Glauberman, *On loops of odd order. II.*, J. Algebra **8** (1968), 393–414.


D. Stanovský and P. Vojtěchovský, *Commutator theory for loops*, J. Algebra **399** (2014), 290–322.


D. Stanovský and P. Vojtěchovský, *Abelian extensions and solvable loops*, Results Math. **66** (2014), 367–384.