

# Solvability and supernilpotence in varieties close to groups

Petr Vojtěchovský (joint work with Aleš Drápal and David Stanovský)



Panglobal Algebra and Logic Seminar  
October 3, 2023  
University of Colorado Boulder

## Commutator of congruences

In 1987, Freese and McKenzie developed commutator theory for congruence modular varieties.

### Definition

Let  $A$  be an algebra and  $\alpha, \beta, \delta$  congruences of  $A$ . Then  $\alpha$  **centralizes**  $\beta$  **over**  $\delta$  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  $\delta$  such that  $\alpha$  centralizes  $\beta$  over  $\delta$ .

## 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.

# Loops

A *loop* is an algebra  $(Q, \cdot, \backslash, /, 1)$  such that

$$1 \cdot x = x \cdot 1 = x,$$

$$x \cdot (x \backslash y) = y = x \backslash (x \cdot y),$$

$$(x \cdot y) / y = x = (x / y) \cdot y.$$

Note:

- the left translations  $L_x$  and the right translations  $R_x$  are bijections of  $Q$  and they generate the **multiplication group**  $\text{Mlt}(Q) = \langle L_x, R_x : x \in Q \rangle$ ,
- in the finite case the multiplication table of  $Q$  is a normalized latin square,
- unlike in groups, there need not be two-sided inverses and associativity does not necessarily hold.

## Congruence commutators in groups and loops

Normal subloops = congruence classes containing  $1$ .

Deviations from commutativity and associativity:

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

These are **inner mappings** and they generate the **inner mapping group**  $\text{Inn}(Q)$ .

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

Let  $\alpha, \beta$  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

An algebra  $A$  is **abelian** if  $[1_A, 1_A] = 0_A$ .

Abelian loops = abelian groups.

*Classical solvability:* (Bruck, Glauberman)

$1 = Q_0 \leq Q_1 \leq \dots \leq Q_n = Q$ , where each factor  $Q_{i+1}/Q_i$  is an abelian group.

A normal subloop  $X$  of  $Q$  **induces an abelian congruence** if  $[X, X]_Q = 1$ , that is, the commutator of the congruence induced by  $X$  in  $Q$  is trivial.

*Congruence solvability:*

$1 = Q_0 \leq Q_1 \leq \dots \leq Q_n = Q$ , 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  $Q$ ?
- The second property implies the first but not vice versa.
- There are easy examples of loops of order 8 that are classically solvable but not congruence solvable.
- A **Bol loop** is a loop satisfying  $x(y(xz)) = (x(yx))z$ . (Fairly close to groups.) There is a Bol loop of order 16 that is classically solvable but not congruence solvable.

# 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

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

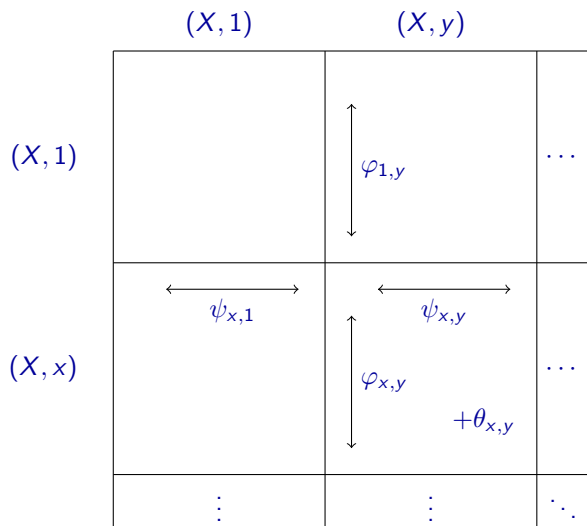
where  $\varphi_{r,s}, \psi_{r,s} \in \text{Aut}(X)$ ,  $\theta_{r,s} \in X$  and  $\varphi_{r,1} = \psi_{1,r} = \text{id}_X$ ,  $\theta_{r,1} = \theta_{1,r} = 0$ .

## 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.



## An abelian extension visualized



# 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  $\varphi_{r,s} = T_s^{-1}|_X$ ,  $\psi_{r,s} = \text{id}_X$  and  $\theta_{r,s} = u_{r,s}^{-1}rs$ . □

## Nuclear case

For a loop  $Q$  we have

$$\text{Nuc}_\ell(Q) = \{x \in Q : x(yz) = (xy)z \text{ for all } y, z \in Q\},$$

$$\text{Nuc}_m(Q) = \{x \in Q : y(xz) = (yx)z \text{ for all } y, z \in Q\},$$

$$\text{Nuc}_r(Q) = \{x \in Q : y(zx) = (yz)x \text{ for all } y, z \in Q\},$$

$$\text{Nuc}(Q) = \text{Nuc}_\ell(Q) \cap \text{Nuc}_m(Q) \cap \text{Nuc}_r(Q).$$

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

### Lemma

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

# Moufang loops

We will greatly generalize this result for **Moufang loops**, that is, loops satisfying the identity

$$x(y(xz)) = ((xy)x)z.$$

- Think octonions but there are many other examples.
- Very close to groups. Are **diassociative**, that is,  $\langle x, y \rangle$  is a group.
- All four nuclei coincide.
- Smallest Moufang non-group is of order 12 obtained by “doubling”  $S_3$ .

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

An abelian normal subloop of a Moufang loop need not induce an abelian congruence:

- $W = (W, +)$  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,
- $\overline{q} : \overline{W} \rightarrow F$  a quadratic form with associated bilinear form  $\overline{h} : \overline{W} \times \overline{W} \rightarrow F$ ,
- $q : W \rightarrow F$  and  $h : W \times W \rightarrow F$  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 congruence solvable (in fact nilpotent, see later) and hence classically solvable,
- $Q$  is a Moufang loop,
- $Q$  is a group if and only if the quadratic form  $\bar{q}$  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)

For a while 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.

$$f(xy) = f(u^2y) = f(uyu) = f(u)f(y)f(u) = f(u)^2f(y) = f(u^2)f(y) = f(x)f(y). \quad \square$$

## 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  $\text{Inn}(Q) = \langle T_u : u \in Q \rangle$ .

## 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  $f = L_{s^{-1}r}^{-1}L_s^{-1}L_r$

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

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

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  $[X, X]_Q = 1$  iff  $u \cdot xy = uy \cdot x$  for all  $u \in Q$  and  $x, y \in X$ .

## The 3-divisible case

After much additional work and using this result of Drápal:

### Theorem (Drápal)

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

Her basic setup:

- $L_Q = \{L_x : x \in Q\}$  and  $R_Q$  are transversals to  $\text{Inn}(Q)$  in  $\text{Mlt}(Q)$ , in fact, transversals to every conjugate of  $\text{Inn}(Q)$  in  $\text{Mlt}(Q)$ ,
- $[L_Q, R_Q] \subseteq \text{Inn}(Q)$  (standard group commutator of subsets),
- $\text{core}_{\text{Mlt}(Q)}(\text{Inn}(Q)) = 1$ .

## The odd order theorem

### Theorem (D+V)

*Every Moufang loop of odd order is congruence solvable.*

- let  $Q$  be a smallest counterexample
- clearly  $1 < Q$ , so  $1 < N = \text{Nuc}(Q)$  by Csörgő
- we can assume  $N < Q$  else we are done by Feit-Thompson
- let  $X$  be a minimal characteristic subgroup of  $N$  and  $f \in \text{Inn}(Q)$
- since  $X \leq N$  and  $X \trianglelefteq Q$ , we have  $f|_X \in \text{Aut}(X)$
- 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

## The newest result

### Theorem (D+V 2023)

*A finite Moufang loop is classically solvable iff it is congruence solvable.*

One ingredient that comes into play are **groups with triality**, that is, groups that admit automorphisms  $\rho, \sigma$  such that  $\langle \rho, \sigma \rangle \cong S_3$  and

$$[x, x^\sigma][x, x^\sigma]^\rho[x, x^\sigma]^{\rho^2} = 1.$$

In Moufang loops with trivial nucleus one can consider  $G = \text{Mlt}(Q) = \langle L_x, R_x : x \in Q \rangle$  and

$$\begin{aligned}\sigma : L_x &\mapsto R_x^{-1}, & R_x &\mapsto L_x^{-1}, \\ \rho : L_x &\mapsto R_x, & R_x &\mapsto L_x^{-1}R_x^{-1}.\end{aligned}$$

(See Jonathan Hall's volume of Memoirs of AMS.)



## Nilpotence in general

With the commutators as before, define the “lower central series”

$$\gamma_0 = [1_A, 1_A], \quad \gamma_{i+1} = [1_A, \gamma_i].$$

Then  $A$  is **nilpotent** if the series reaches  $0_A$  in finitely many steps.

The **center** is the largest congruence  $\zeta$  such that  $\zeta$  centralizes  $1_A$  over  $0_A$ .

## Nilpotence in loops

The concept of nilpotence in loops behaves as in groups. We have

$$Z(Q) = \text{Nuc}(Q) \cap \{x \in Q : xy = yx \text{ for all } y\}$$

and the corresponding notion of upper central series.

But even simple questions about nilpotence can be very difficult.

## An open problem concerning nilpotence

Recall the following theorem from a first course on group theory:

### Theorem

Let  $G$  be a group. Then  $G/Z(G) \cong \text{Inn}(G)$ . In particular,  $\text{cl}(G) \leq 2$  iff  $\text{Inn}(G)$  is abelian.

Bruck showed:

### Theorem (Bruck)

Let  $Q$  be a loop. If  $\text{cl}(Q) \leq 2$  then  $\text{Inn}(Q)$  is abelian.

What about the converse?

## An open problem concerning nilpotence

- Csörgő constructed a loop  $Q$  such that  $\text{Inn}(Q)$  is abelian and  $\text{cl}(Q) = 3$ .
- Nagy and V constructed a Moufang loop with the same property.
- After approximately ten years of effort and using automated deduction on massive scale, Kinyon and Veroff proved that if  $\text{Inn}(Q)$  is abelian then  $\text{cl}(Q) \leq 3$ . Some of their proofs are among the longest ever obtained by automated deduction (100k deductive steps).
- But we don't know, for instance, if there is a commutative loop  $Q$  with  $\text{Inn}(Q)$  abelian and  $\text{cl}(Q) = 3$ .

## Decomposition theorem

The most important theorem about finite nilpotent groups is of course:

### Theorem (Decomposition Theorem)

*A finite group is nilpotent iff it is a direct product of  $p$ -groups.*

It turns out that (universal algebraic) nilpotence is too weak to furnish the analog of the Decomposition Theorem. There exist finite nilpotent algebraic structures very close to groups that are not direct products of algebras of prime power orders.

In 2010, Aichinger and Mudrinski identified a concept stronger than nilpotence, so-called **supernilpotence**, that precisely guarantees the Decomposition Theorem in reasonable varieties.

## Mal'cev term and permutable congruences

A variety  $V$  is **congruence permutable** if  $\alpha\beta = \beta\alpha$  for any  $A \in V$  and any congruences  $\alpha, \beta$  of  $A$ .

### Theorem (Mal'cev 1954)

*A variety is congruence permutable iff it contains a **Mal'cev term**, a term satisfying  $m(x, y, y) = x = m(y, y, x)$ .*

In groups, we can take  $m(x, y, z) = xy^{-1}z$ .

In loops, we can take  $m(x, y, z) = x(y \setminus z)$ .

# Supernilpotence

A **polynomial** is a term with constants.

## Definition

Let  $A$  be an algebra,  $p(x_1, \dots, x_n)$  a polynomial,  $(e_1, \dots, e_n) \in A^n$  and  $e \in A$ . Then  $p$  is **absorbing at  $(e_1, \dots, e_n)$  into  $e$**  if whenever  $a_i = e_i$  for some  $i$  then  $p(a_1, \dots, a_n) = e$ .

## Definition

An algebra  $A$  is  **$k$ -supernilpotent** if every polynomial of arity  $n > k$  that is absorbing at some  $(e_1, \dots, e_n) \in A^n$  into some  $e \in A$  is constant. An algebra is **supernilpotent** if it is  $k$ -supernilpotent for some  $k$ .

## Theorem (Aichinger+Mudrinski 2010)

*Let  $V$  be a congruence permutable variety. Then a finite algebra in  $V$  is supernilpotent iff it is a direct product of nilpotent algebras of prime power order.*

# Absorption in groups

In groups:

- it suffices to consider absorption at  $(1, \dots, 1)$  into 1:  
replace  $p(x_1, \dots, x_n)$  with  $p(x_1^{-1}e_1, \dots, x_n^{-1}e_n)e^{-1}$ ,
- the commutator  $[x, y] = x^{-1}y^{-1}xy$  and all complex commutators are prototypical absorbing terms.



# Nilpotence vs. supernilpotence in groups

Theorem (Aichinger+Mudrinski, Moorhead)

*In general,  $k$ -supernilpotence implies  $k$ -nilpotence. But nilpotence (even 2-nilpotence) does not imply supernilpotence.*

Theorem (Shaw 2008 PhD thesis, A+M, S+V gave a conceptually simpler proof in 2023)

*A group is  $k$ -nilpotent iff it is  $k$ -supernilpotent.*

## Main idea of the group proof

- If  $G$  is  $k$ -supernilpotent then the absorbing commutator

$$[x_1, [x_2, [\dots, [x_k, x_{k+1}] \dots ]]]$$

is constant (thus trivial), and  $G$  is  $k$ -nilpotent from upper central series considerations.

- The other direction is more complicated (about 3 pages now).
- Use a 1934 result of Phillip Hall: *In a  $k$ -nilpotent group all complex commutators of weight  $k + 1$  vanish.*
- Rewrite any absorbing polynomial, attempting to order commutators first by their support and then by complexity. This will succeed, using the fact that  $(\mathbb{N}^m, \leq_{\text{lex}})$  has no infinite descending chains and commutators of weight  $> k$  vanish.
- Apply a technical result (next page).

## A technical result

### Lemma

Let  $(A, \cdot, 1, \dots)$  be an algebra such that  $1$  is the identity element with respect to the binary operation  $\cdot$ . Let  $p$  be an  $n$ -ary polynomial on  $A$  with support  $\{x_1, \dots, x_n\}$  that is absorbing at  $(e_1, \dots, e_n)$  into  $1$ . Assume that  $p$  is equivalent to

$$\prod_{S \in \mathcal{S}} p_S,$$

where the product (in some order and in some parenthesizing) ranges over a subset  $\mathcal{S}$  of proper subsets of  $\{1, \dots, n\}$ , and where every  $p_S$  is a polynomial with support  $\{x_i : i \in S\}$  that is absorbing at  $(e_i : i \in S)$  into  $1$ . Then  $p$  is constant.

## Commutators and associators

In a loop, these are uniquely determined elements  $[x, y]$ ,  $[x, y, z]$  such that

$$yx = (xy)[x, y], \quad x(yz) = ((xy)z)[x, y, z].$$

Note that as terms they are absorbing.

## $k$ -supernilpotent loops for $k = 1, 2$

### Theorem

*For  $k \in \{1, 2\}$ , a loop is  $k$ -supernilpotent iff it is a  $k$ -nilpotent group.*

There exists a 2-nilpotent loop (of order 8) that is not supernilpotent.

So, in loops,  $k$ -nilpotence and  $k$ -supernilpotence diverge already at  $k = 2$ .

## 3-supernilpotent loops

### Theorem (S+V 2023)

A loop is 3-supernilpotent iff the following identities hold:

$$1 = [x, [y, u, v]],$$

$$1 = [x, y, [u, v, w]] = [x, [u, v, w], y] = [[u, v, w], x, y],$$

$$1 = [x, y, [u, v]] = [x, [u, v], y] = [[u, v], x, y],$$

$$1 = [x, [y, [u, v]]] = [x, [[u, v], y]],$$

$$1 = [[y, [u, v]], x] = [[[u, v], y], x],$$

$$1 = [[x, y], [u, v]],$$

$$[xy, u, v] = [x, u, v] [y, u, v],$$

$$[u, xy, v] = [u, x, v] [u, y, v],$$

$$[u, v, xy] = [u, v, x] [u, v, y].$$

## $k$ -supernilpotent loops with $k > 3$ ?

The general theory guarantees that there is an equational basis for  $k$ -supernilpotent algebras  $V_k$  in a given variety  $V$ , constructed from an equational basis for  $V$ .

If  $V$  is finitely based, it is not clear if  $V_k$  is finitely based.










### Conjecture

*$k$ -supernilpotent loops are finitely based.*

That should not be too hard to prove. Finding a small basis will be hard.

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.