Supernilpotent loops

Žaneta Semanišinová[1]
with David Stanovský[2]

[1]Institute of Algebra
TU Dresden

[2]Department of Algebra
Charles University, Prague

International Seminar, 15.10.2021

Outline

Definition of a loop

- a loop is an algebra $(Q, \cdot, 1)$, where multiplication table of $\cdot$ is a latin square (possibly infinite) and 1 is a neutral element of $\cdot$
- alternatively, loop can be defined as a universal algebra:

Definition (loop)

A loop is an algebra $(Q, \cdot, \backslash, /, 1)$ satisfying the following identities:

$$x\backslash(x \cdot y) = y, \quad x \cdot (x\backslash y) = y,$$
$$(y \cdot x)/x = y, \quad (y/x) \cdot x = y,$$
$$x \cdot 1 = x = 1 \cdot x.$$

Example: $(\mathbb{Z}_{p^2}, *, 0)$, where p is an odd prime and $*$ is defined by

$$x * y = x + y + px^2y \bmod p^2$$

Properties of loops

- loops have Mal'tsev term $x \cdot (y \backslash z)$ (satisfies $x \cdot (x \backslash y) = y = y \cdot (x \backslash x)$)

Definition (multiplication group)

Let Q be a loop. For every $x \in Q$, let $L_x, R_x : Q \to Q$ be defined by

$$L_x(y) = xy, \qquad R_x(y) = yx.$$

and called left and right translations resp. The group generated by $\{L_x, R_x : x \in Q\}$ is called the multiplication group of Q and denoted $\mathrm{Mlt}(Q)$.

- observe that $L_x^{-1}(y) = x \backslash y$ and $R_x^{-1}(y) = y/x$

Nilpotence in loops and groups

Groups:

- the center $Z(G)$ is the set of all elements that commute with all of G
- define $Z_0(G) = 1$ and for $i \geq 0$ define $Z_{i+1}(G)$ as a preimage of $Z(G/Z_i(G))$ under the projection of G to $G/Z_i(G)$
- G is k-nilpotent if $Z_k(G) = G$ for some $k \geq 0$
- could be equivalently defined via commutator of two subgroups

Nilpotence in loops and groups

Groups:

- the center $Z(G)$ is the set of all elements that commute with all of G
- define $Z_0(G) = 1$ and for $i \geq 0$ define $Z_{i+1}(G)$ as a preimage of $Z(G/Z_i(G))$ under the projection of G to $G/Z_i(G)$
- G is k-nilpotent if $Z_k(G) = G$ for some $k \geq 0$
- could be equivalently defined via commutator of two subgroups

Loops:

- the center $Z(Q)$ is the set of all elements that commute and associate with all of Q
- we define $Z_i(Q)$, $i \geq 0$ and k-nilpotence as in groups

Nilpotence in loops and groups

- a finite group is nilpotent iff it is a direct product of groups of prime power order
- this is not true for finite loops:
  - every non-associative loop of prime order is not nilpotent, since $|Z(Q)|$ divides $|Q|$
  - there is a directly indecomposable nilpotent loop of order 6

Nilpotence in loops and groups

- a finite group is nilpotent iff it is a direct product of groups of prime power order
- this is not true for finite loops:
  - every non-associative loop of prime order is not nilpotent, since $|Z(Q)|$ divides $|Q|$
  - there is a directly indecomposable nilpotent loop of order 6

Theorem (Wright, 1969)

A finite loop Q is a direct product of nilpotent loops of prime power order if and only if $\mathrm{Mlt}(Q)$ is nilpotent.

Binary commutator

Definition (binary commutator)

Let A be an algebra and let α, β, $\delta \in \mathrm{Con}(A)$. We say that α centralizes β modulo δ if for every term operation t and for all tuples $\mathbf{a}\,\alpha\,\mathbf{b}$ and $\mathbf{u}\,\beta\,\mathbf{v}$

$$t(\mathbf{a},\mathbf{u})\,\delta\,t(\mathbf{a},\mathbf{v})$$
$$\Downarrow$$
$$t(\mathbf{b},\mathbf{u})\,\delta\,t(\mathbf{b},\mathbf{v})$$

The binary commutator $[\alpha,\beta]$ is the smallest congruence δ of A such that α centralize β modulo δ.

Binary commutator in groups

- observe that in abelian groups 1_G centralizes 1_G modulo 0_G since every term is of the form

$$t(\mathbf{z}, \mathbf{w}) = \sum_i k_i \cdot z_i + \sum_j l_j \cdot w_j,$$

so we have

$$t(\mathbf{a}, \mathbf{u}) = t(\mathbf{a}, \mathbf{v}) \Rightarrow t(\mathbf{b}, \mathbf{u}) = t(\mathbf{b}, \mathbf{v})$$

- hence in abelian groups $[1_G, 1_G] = 0_G$
- more generally, if $A, B \trianglelefteq G$ and α, β are the corresponding congruences then $[\alpha, \beta]$ corresponds to $[A, B]$

Bulatov's definition of higher commutator

Definition (higher commutator; Bulatov, 2001)

Let A be an algebra, $\alpha_1, \ldots, \alpha_n$, β, $\delta \in \mathrm{Con}(A)$. We say that $\alpha_1, \ldots, \alpha_n$ centralize β modulo δ if, for every term operation t and all pairs of tuples $\mathbf{a}_i \, \alpha_i \, \mathbf{b}_i$, $\mathbf{u} \, \beta \, \mathbf{v}$,

$$\begin{gathered}\forall(\mathbf{x}_1, \ldots, \mathbf{x}_n) \in \{\mathbf{a}_1, \mathbf{b}_1\} \times \ldots \times \{\mathbf{a}_n, \mathbf{b}_n\} \setminus \{(\mathbf{b}_1, \ldots, \mathbf{b}_n)\} \\ t(\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{u}) \, \delta \, t(\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{v}) \\ \Downarrow \\ t(\mathbf{b}_1, \ldots, \mathbf{b}_n, \mathbf{u}) \, \delta \, t(\mathbf{b}_1, \ldots, \mathbf{b}_n, \mathbf{v}).\end{gathered}$$

The $(n+1)$-ary commutator $[\alpha_1, \ldots, \alpha_n, \beta]$ is the smallest congruence δ of A such that $\alpha_1, \ldots, \alpha_n$ centralize β modulo δ.

Nilpotence and supernilpotence

Definition (nilpotence)

An algebra A is said to be k-nilpotent if

$$\underbrace{[1_A, [1_A, [..., [1_A, 1_A] \dots]]]}_{k+1} = 0_A.$$

- in groups and loops this definition yields the same nilpotence

Definition (supernilpotence)

An algebra A is said to be k-supernilpotent if

$$[\underbrace{1_A, ..., 1_A}_{k+1}] = 0_A.$$

Supernilpotence vs. nilpotence

- $\mathrm{cl_n}(A)$ - class of nilpotence of A
- $\mathrm{cl_{sn}}(A)$ - class of supernilpotence of A
- $\mathrm{cl_m}(Q)$ - class of nilpotence of $\mathrm{Mlt}(Q)$ for a loop Q
- if an algebra is not (super)nilpotent, we say that the class is ∞

Theorem (Aichinger, Mudrinski, 2010)

If A is a Mal'tsev algebra, then $\mathrm{cl_n}(A) \leq \mathrm{cl_{sn}}(A)$.

Theorem (Aichinger, Ecker, 2006)

If G is a group, then $\mathrm{cl_n}(G) = \mathrm{cl_{sn}}(G) = \mathrm{cl_m}(G)$.

Supernilpotence vs. nilpotence in loops

Theorem (Bruck, 1946)

If Q is a loop, then $\mathrm{cl_n}(Q) \le \mathrm{cl_m}(Q)$.

Theorem (Aichinger, Mudrinski, 2010; Wright, 1969)

If Q is a finite loop then $\mathrm{cl_{sn}}(Q) < \infty$ iff $\mathrm{cl_m}(Q) < \infty$ iff it is a direct product of loops Q_i of prime power size, $\mathrm{cl_n}(Q_i) < \infty$.

Theorem (Ž.S., D.S.)

Let Q be a loop, then $\mathrm{cl_m}(Q) \le \mathrm{cl_{sn}}(Q)$.

- we found algorithmically 8-element supernilpotent loops Q such that

$$\mathrm{cl_n}(Q) < \mathrm{cl_m}(Q) < \mathrm{cl_{sn}}(Q)$$

Proof of the theorem

Theorem

Let Q be a loop, then $\mathrm{cl}_{\mathrm{m}}(Q) \leq \mathrm{cl}_{\mathrm{sn}}(Q)$.

Proof by example.

- 2-supernilpotent loop Q, $a, b, c \in Q$,
- a group term $t(x_1, x_2, x_3) = x_2 x_3 x_1^{-1}$,
- $f_1 = L_a L_b$, $g_1 = L_b = L_1 L_b$,
- $f_2 = R_c L_a^{-1} = R_c L_a^{-1} R_1^{-1}$, $g_2 = R_b R_a^{-1} = R_b L_1^{-1} R_a^{-1}$,
- $u = R_c^{-1} = R_c^{-1} R_1$, $v = R_b = R_1^{-1} R_b$.

Define term t' as

$$t'(x_1^1, x_1^2, x_2^1, x_2^2, x_2^3, x_3^1, x_3^2) = x_2^1 x_2^2 x_2^3 x_3^1 x_3^2 (x_1^1 x_1^2)^{-1}.$$

Proof of the theorem

The following are equivalent:

$$t(f_1, f_2, u) = t(f_1, f_2, v)$$
$$t(L_aL_b, R_cL_a^{-1}R_1^{-1}, R_c^{-1}R_1) = t(L_aL_b, R_cL_a^{-1}R_1^{-1}, R_1^{-1}R_b)$$
$$t'(L_a, L_b, R_c, L_a^{-1}, R_1^{-1}, R_c^{-1}, R_1) = t'(L_a, L_b, R_c, L_a^{-1}, R_1^{-1}, R_1^{-1}, R_b)$$
$$R_cL_a^{-1}R_1^{-1}R_c^{-1}R_1L_b^{-1}L_a^{-1} = R_cL_a^{-1}R_1^{-1}R_1^{-1}R_bL_b^{-1}L_a^{-1}$$
$$R_cL_a^{-1}R_1^{-1}R_c^{-1}R_1R_1L_b^{-1}L_a^{-1}(q) = R_cL_a^{-1}R_1^{-1}R_1^{-1}R_bR_aL_b^{-1}L_a^{-1}(q)$$
$$s(a, b, c, a, 1, c, 1, 1, q) = s(a, b, c, a, 1, 1, b, a, q)$$

for all $q \in Q$ and a suitable loop term s.
The other equations are translated similarly. By 2-supernilpotence of Q, we derive the equation $t(g_1, g_2, u) = t(g_1, g_2, v)$ first in Q and then translate it to $\mathrm{Mlt}(Q)$.

□

Absorbing polynomials

Definition (absorbing polynomial)

Let A be an algebra, $\mathbf{a}, e \in A$. A polynomial operation f of A is called absorbing at $\mathbf{a}$ into e if $f(\mathbf{u}) = e$ whenever there is i such that $u_i = a_i$.

- in loops it is enough to consider $\mathbf{a} = \mathbf{1}$ and $e = 1$

Theorem (Aichinger, Mudrinski, 2010)

A Mal'tsev algebra is k-supernilpotent iff every absorbing polynomial of arity $k+1$ is constant.

Identities defining supernilpotence

The following mappings generate the group $\mathrm{Inn}(Q) = \mathrm{Mlt}(Q)_1$:

$$L_{x,y} = L_{xy}^{-1} L_x L_y, \quad R_{x,y} = R_{yx}^{-1} R_x R_y, \quad T_x = R_x^{-1} L_x.$$

Using absorbing polynomials, we can derive the following:

Proposition (Ž.S., D.S.)

1. *A loop is 1-supernilpotent if and only if it is an abelian group.*
2. *A loop is 2-supernilpotent if and only if it is a 2-nilpotent group.*
3. *In a 3-supernilpotent loop Q, for every $x, y, u, v \in Q$ the following is true:*
    - $L_{x,y}$, $R_{x,y}$ *and* $[L_x, R_y]$ *are automorphisms of* Q,
    - $[L_{x,y}, L_{u,v}] = [L_{x,y}, R_{u,v}] = [R_{x,y}, R_{u,v}] = [L_{x,y}, T_u] = [R_{x,y}, T_u] = 1.$

Proof sketch

Proof sketch.

- supernilpotence implies nilpotence in loops, hence ($\Leftarrow$) in (1) and (2)

Proof sketch

Proof sketch.

- supernilpotence implies nilpotence in loops, hence ($\Leftarrow$) in (1) and (2)

(1) ($\Rightarrow$)

- terms $T_x(y)/y = ((xy)/x)/y$ and $L_{x,y}(z)/z = (xy\backslash(x(yz)))/z$ are absorbing, therefore constant
- hence a 1-supernilpotent loop needs to be commutative and associative – abelian group

Proof sketch

Proof sketch.

- supernilpotence implies nilpotence in loops, hence ($\Leftarrow$) in (1) and (2)

(1) ($\Rightarrow$)

- terms $T_x(y)/y = ((xy)/x)/y$ and $L_{x,y}(z)/z = (xy\backslash(x(yz)))/z$ are absorbing, therefore constant
- hence a 1-supernilpotent loop needs to be commutative and associative – abelian group

(2) ($\Rightarrow$)

- the second term from (1) is constant, hence 2-supernilpotent loops are associative – 2-nilpotent groups

Proof sketch

Proof sketch.

- supernilpotence implies nilpotence in loops, hence ($\Leftarrow$) in (1) and (2)

(1) ($\Rightarrow$)

- terms $T_x(y)/y = ((xy)/x)/y$ and $L_{x,y}(z)/z = (xy\backslash(x(yz)))/z$ are absorbing, therefore constant
- hence a 1-supernilpotent loop needs to be commutative and associative – abelian group

(2) ($\Rightarrow$)

- the second term from (1) is constant, hence 2-supernilpotent loops are associative – 2-nilpotent groups

(3)

- as in (1), (2) we show that appropriate terms are absorbing and hence constant, e.g. $L_{x,y}(uv)/(L_{x,y}(u)L_{x,y}(v))$

□

Relational description of the commutator

- original definition of supernilpotence does not provide a natural algorithm
- there is an equivalent relational description by Opršal using a certain relation $\Delta(\underbrace{1_A, \ldots, 1_A}_{k+1}) \leq A^{2^{k+1}}$ given by its generators

Example

$\Delta(1_A, 1_A, 1_A)$ is generated by the tuples of the form (a, b, a, b, a, b, a, b), (a, a, b, b, a, a, b, b) or (a, a, a, a, b, b, b, b).

Relational description of the commutator

- original definition of supernilpotence does not provide a natural algorithm
- there is an equivalent relational description by Opršal using a certain relation $\Delta(\underbrace{1_A, \ldots, 1_A}_{k+1}) \leq A^{2^{k+1}}$ given by its generators

Example

$\Delta(1_A, 1_A, 1_A)$ is generated by the tuples of the form (a, b, a, b, a, b, a, b), (a, a, b, b, a, a, b, b) or (a, a, a, a, b, b, b, b).

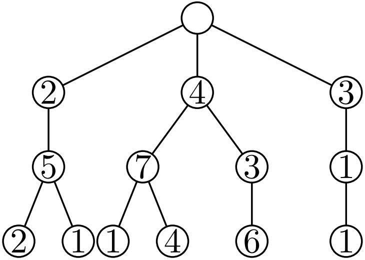
Theorem (Opršal, 2016)

A Mal'tsev algebra A is k-supernilpotent if and only if Δ contains no non-trivial fork in the last coordinate, that is, a pair of tuples of the form

$$(u_1, \ldots, u_{2^{k+1}-1}, a), (u_1, \ldots, u_{2^{k+1}-1}, b), \quad a \neq b.$$

Algorithmic testing of supernilpotence

- for finite loops Q and $k \in \mathbb{N}$ we generated Δ and checked existence of non-trivial forks
- we represented collections of tuples as rooted trees to make the check for forks and duplicates faster
- this allows us to perform the check in $O(|Q| \cdot 2^{k+1})$
- in the straightforward list representation it takes $O(2^{k+1}s)$, where s is the size of the collection (bounded by $|Q|^{2^{k+1}}$)



Results of tests

- we tested 3-supernilpotence in non-associative loops Q, where:
  - $|Q| = 8$, $\mathrm{cl_m}(Q) = 3$
  - $|Q| = 9$ (they have $\mathrm{cl_m}(Q) = 3$)
- we found 8-element supernilpotent loops where $2 = \mathrm{cl_n}(Q) < 3 = \mathrm{cl_m}(Q) < \mathrm{cl_{sn}}(Q)$
- we were unable to confirm 3-supernilpotence of any of the tested loops (some tests were running for > 3 hrs)

New results

- D. Stanovský and P. Vojtěchovský characterized 3-supernilpotent loops by finitely many identities using commutator and associator terms
- might be possible to generalize the characterization to k-supernilpotence
- allows to test 3-supernilpotence in finite loops very fast
- 8-element loops:
  - confirmed the previous results (loops that are not 3-supernilpotent)
  - showed the rest to be 3-supernilpotent
- 9-element loops:
  - just part of the loops is 3-supernilpotent
  - the former algorithm was not fast enough to find forks

Open problems

Problem

Let Q be a supernilpotent loop. Find a function

1. *f such that* $\mathrm{cl}_{\mathrm{sn}}(Q) \leq f(\mathrm{cl}_{\mathrm{n}}(Q))$*, or*
2. *g such that* $\mathrm{cl}_{\mathrm{sn}}(Q) \leq g(\mathrm{cl}_{\mathrm{m}}(Q))$

or prove that no such function exists.

Open problems

Problem

Let Q be a supernilpotent loop. Find a function

1. *f such that* $\mathrm{cl}_{\mathrm{sn}}(Q) \leq f(\mathrm{cl}_{\mathrm{n}}(Q))$, *or*
2. *g such that* $\mathrm{cl}_{\mathrm{sn}}(Q) \leq g(\mathrm{cl}_{\mathrm{m}}(Q))$

or prove that no such function exists.

Problem

Does the equivalence

$$\mathrm{cl}_{\mathrm{sn}}(Q) < \infty \Leftrightarrow \mathrm{cl}_{\mathrm{m}}(Q) < \infty$$

hold for every loop Q?

Thank you for your attention