Results Math (2023) 78:119

1422-6383/23/040001-15
published online April 7, 2023
https://doi.org/10.1007/s00025-023-01882-x

Results in Mathematics

Three Concepts of Nilpotence in Loops

Žaneta Semanišinová and David Stanovský

Abstract. We introduce the abstract concept of supernilpotence in loop theory, and relate it to existing concepts, namely, central nilpotence and nilpotence of the multiplication group. We prove that the class of supernilpotence is greater or equal than the class of nilpotence of the multiplication group, and combining existing results, we show that a finite loop is supernilpotent if and only if its multiplication group is nilpotent. We also provide a new exposition of a classical result and crucial ingredient, that loops with a nilpotent multiplication group are centrally nilpotent and admit a prime decomposition.

Mathematics Subject Classification. 20N05, 20F18.

Keywords. Loops, multiplication groups of loops, nilpotence, supernilpotence.

1. Introduction

Loops generalize groups by dropping the axiom of associativity [6,17], so, naturally, many concepts in early loop theory were developed in direct analogy to group theory. For example, the center of a loop is defined as the set of all elements that commute *and associate* with every other element, and subsequently we obtain the concept of central series and of *central nilpotence*.

Groups of prime power order are nilpotent and finite nilpotent groups admit a prime decomposition, i.e., they decompose as a direct product of groups of prime power order. Both statements generalize to Moufang loops [9, 10] (the proofs are much harder!), but neither statement holds in general: every non-associative loop of prime order is not centrally nilpotent (since the order of the center divides the order of the loop) and there is a directly indecomposable nilpotent loop of order 6.

The path towards a loop theoretic concept of nilpotence is certainly not unique. For example, one could consider *nilpotence of the multiplication group*. Bruck [5] proved that every loop with a nilpotent multiplication group is centrally nilpotent, but the converse fails. Wright [23] proved that a finite loop with a nilpotent multiplication group admits a prime decomposition, i.e., it is a direct product of nilpotent loops of prime power order.

In late 1970s, universal algebra established an abstract concept of the commutator of congruences, and subsequently of nilpotence and solvability of general algebraic structures [8,11,19]. Applied to loop theory, it is not difficult to verify that the universal algebraic concept of nilpotence coincides with central nilpotence, although the two notions solvability are quite different [20,21].

Over the last decade, universal algebra introduced a stronger concept of nilpotence, called *supernilpotence* [2,7], which, under certain assumptions met by groups and loops, implies prime decomposition. The purpose of the present note is to introduce the concept of supernilpotence into loop theory and to make initial observations on the relationship of the three concepts of nilpotence.

Formal definitions will be presented in subsequent sections. To state the main theorem, let us introduce the following notation: for a loop Q, let

- $\mathrm{cl}_{cn}(Q)$ denote the class of central nilpotence of Q,
- $\mathrm{cl}_{m}(Q)$ denote the class of nilpotence of $\mathrm{Mlt}(Q)$,
- $\mathrm{cl}_{sn}(Q)$ denote the class of supernilpotence of Q.

If Q fails to be centrally nilpotent, we will denote $\mathrm{cl}_{cn}(Q) = \infty$, *et cetera* for the other properties.

Theorem 1.1. *Let Q be a loop. Then*

$$\mathrm{cl}_{sn}(Q) \geq \mathrm{cl}_{m}(Q) \geq \mathrm{cl}_{cn}(Q).$$

Moreover, if Q finite, then $\mathrm{cl}_{sn}(Q) < \infty$ if and only if $\mathrm{cl}_{m}(Q) < \infty$.

The first inequality is a new result, the second inequality is due to Bruck [5, p. 282, Corollary III to Theorem 8B] (he states it for finite loops, however, this assumption is never used in the proof), and the last part is a combination of a loop theoretic result of Wright [23, Theorem 1] and universal algebraic results based on works of Kearnes [12] and Aichinger and Mudrinski [2, Section 7]. It is an open problem whether the assumption of finiteness is necessary.

For a group G, $\mathrm{cl}_{sn}(G) = \mathrm{cl}_{cn}(G)$, and thus the three classes of nilpotence coincide [1,22]. For loops, the classes may be different: there is a loop Q such that

- $|Q| = 6$, $\mathrm{cl}_{cn}(Q) = 2$, $\mathrm{cl}_{m}(Q) = \infty$ (Example 3.2).
- $|Q| = 8$, $\mathrm{cl}_{cn}(Q) = 2$, $\mathrm{cl}_{m}(Q) = 3$, $\mathrm{cl}_{sn}(Q) \geq 4$ (Example 3.5).

The structure of the paper is as follows. In Sect. 2, we introduce the abstract concepts of nilpotence and supernilpotence. In Sect. 3, we explain how these concepts are realized in loops. In Sect. 4, we prove Theorem 1.1.

Although two of the three parts of the theorem are not new, we present a complete proof, since parts of the original proofs are scattered around several old papers written in a somewhat outdated style, and they are omitted in recent surveys such as [15,17].

2. (Super)nilpotence in Universal Algebra

For a general background in universal algebra, we refer to the textbook [4]. We will focus on the the abstract notions of nilpotence and supernilpotence.

By a *polynomial operation* on an algebraic structure (shortly, *algebra*) A we mean a term operation of the algebra A enhanced with constants for every element of A. If no confusion arises, we will just use the noun *polynomial*.

We are mostly interested in algebras with a *Mal'tsev term*, i.e., a term m satisfying the identities $m(x, y, y) = m(y, y, x) = x$. Groups and loops always have a Mal'tsev term, $m(x, y, z) = xy^{-1}z$ and $m(x, y, z) = (x/y)z$, respectively. Algebras with a Mal'tsev term will be called shortly *Mal'tsev algebras*.

2.1. Nilpotence

The abstract commutator theory for congruence modular varieties was developed by Freese and McKenzie [8], building upon earlier works of Smith [19] and Hagemann and Herrmann [11]. In particular, they defined the center of an algebra, and subsequently, they define the abstract notion of nilpotence.

Definition 2.1. The *center* of an algebra A is the largest congruence ζ_A such that for every polynomial operation p, all pairs $a\,\zeta_A\,b$ and all tuples $\boldsymbol{u}, \boldsymbol{v}$ of elements of A

$$p(a, \boldsymbol{u}) = p(a, \boldsymbol{v})$$
$$\Downarrow$$
$$p(b, \boldsymbol{u}) = p(b, \boldsymbol{v})$$

An algebra A is called k-*nilpotent* if it possesses a central series of congruences of length k, i.e., a series of congruences $0_A = \alpha_0 \leq \alpha_1 \leq \ldots \leq \alpha_k = 1_A$ such that $\alpha_{i+1}/\alpha_i \leq \zeta_{A/\alpha_i}$. The *class of nilpotence*, $\mathrm{cl}_n(A)$, is the smallest k such that A is k-nilpotent.

(Equivalently, we could have defined the commutator of two congruences and subsequently, the lower and upper central series.)

It is not difficult to prove that the center of a group in the present sense is the congruence corresponding to the standard center. Consequently, the two concepts of nilpotence are equivalent for groups.

2.2. Supernilpotence

The theory of higher commutators was introduced by Bulatov [7] and developed mainly by Aichinger and Mudrinski [2] for Mal'tsev varieties and by Moorhead [13] for congruence modular varieties. The outcome of the theory is a new, stronger notion of nilpotence, called *supernilpotence*. Under mild universal algebraic assumptions (existence of a Taylor term), k-supernilpotence implies k-nilpotence [13].

Definition 2.2. An algebra A is called *k-supernilpotent* if for every polynomial operation p and all pairs of tuples $\boldsymbol{a}_1 \neq \boldsymbol{b}_1, \ldots, \boldsymbol{a}_k \neq \boldsymbol{b}_k$ and $\boldsymbol{u}, \boldsymbol{v}$ of elements of A

$$p(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k, \boldsymbol{u}) = p(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k, \boldsymbol{v}) \qquad \forall (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k) \in \{\boldsymbol{a}_1, \boldsymbol{b}_1\} \times \ldots \times \{\boldsymbol{a}_k, \boldsymbol{b}_k\} \smallsetminus \{(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k)\}$$

$$\Downarrow$$

$$p(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k, \boldsymbol{u}) = p(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k, \boldsymbol{v}).$$

The *class of supernilpotence*, $\mathrm{cl}_{sn}(A)$, is the smallest k such that A is k-supernilpotent.

Note that 1-nilpotence and 1-supernilpotence are exactly the same conditions. Such algebras are called *abelian*.

A k-ary operation p is called *absorbing at $a_1, \ldots, a_k$ into e* if $p(u_1, \ldots, u_k) = e$ whenever there is i such that $u_i = a_i$. More generally, an operation p is called *k-batch-absorbing at $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ into e* if $p(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k) = e$ whenever there is i such that $\boldsymbol{u}_i = \boldsymbol{a}_i$.

Lemma 2.3. *Let A be a k-supernilpotent algebra. Then, for every $l > k$, all l-batch-absorbing polynomial operations are constant. In particular, all absorbing polynomial operations of arity $> k$ are constant.*

Proof. Let p be a $(k+1)$-batch-absorbing polynomial at $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{k+1}$ into e. Let $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k+1}$ be tuples of elements of A. We will prove that $p(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k+1}) = e$. Let $\boldsymbol{u} = \boldsymbol{a}_{k+1}$ and $\boldsymbol{v} = \boldsymbol{b}_{k+1}$. Indeed, p satisfies the assumptions of the implication from Definition 2.2, since $\boldsymbol{x}_i = \boldsymbol{a}_i$ for at least one i. The conclusion then reads $p(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k, \boldsymbol{b}_{k+1}) = p(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k, \boldsymbol{a}_{k+1}) = e$ by absorption.

Let p be an l-batch-absorbing polynomial at $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_l$, with $l > k+1$. Let $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_l$ be tuples of elements of A. To prove that $p(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_l) = e$, consider the polynomial $q(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{k+1}) = p(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_{k+1}, \boldsymbol{b}_{k+2}, \ldots, \boldsymbol{b}_l)$, observe that it is $(k+1)$-batch-absorbing at $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{k+1}$, and thus constant onto e. ☐

It follows from the second part of the proof that if all absorbing polynomials of arity $k+1$ are constant, then this holds for every arity $> k$, and similarly for batch-absorption.

For Mal'tsev algebras, the converse implication in Lemma 2.3 also holds, although the proof is not so simple. Also, for Mal'tsev algebras, we can replace tuples by single elements in Definition 2.2. Theorem 2.4 collects several equivalent definitions of supernilpotence in Mal'tsev algebras. Condition (4) provides an algorithm to check k-supernilpotence. Condition (4) implies that k-supernilpotent algebras in a variety $\mathcal{V}$ form a subvariety.

To state condition (3), we need the following technical definitions. A *fork* in a relation $R \subseteq A^n$ is a pair $(\boldsymbol{u}, \boldsymbol{v}) \in R^2$ satisfying $u_n \neq v_n$ and $u_i = v_i$ for all $i < n$. For a positive integer k, let $k(i)$ denote the i-th digit from the right of the binary expansion of k. For a pair (a, b), denote $(a, b)_{(0)} = a$, $(a, b)_{(1)} = b$ and define $c_i^n(a, b) = ((a, b)_{(k(i))} : k = 0, \ldots, 2^n - 1) \in A^{2^n}$.

To state condition (4), we need a sequence of terms q_n in $2^n - 1$ variables (using a Mal'tsev term m as a parameter) defined inductivily as follows:

$$q_2 = m(y, x, z), \qquad q_{n+1} = m(x_{2^n}, q_n(x_1, \ldots, x_{2^n-1}), q_n(x_{2^n+1}, \ldots, x_{2^{n+1}-1})).$$

Theorem 2.4 [2,3,16]. *Let A be a Mal'tsev algebra. The following conditions are equivalent:*

(1) *A is k-supernilpotent.*

(1*) *For every $(k+1)$-ary polynomial operation p and all $a_1 \neq b_1, \ldots, a_k \neq b_k$ and u, v from A,*

$$p(x_1, \ldots, x_k, u) = p(x_1, \ldots, x_k, v) \quad \forall (x_1, \ldots, x_k) \in \{a_1, b_1\} \times \ldots \times \{a_k, b_k\} \setminus \{(b_1, \ldots, b_k)\}$$
$$\Downarrow$$
$$p(b_1, \ldots, b_k, u) = p(b_1, \ldots, b_k, v).$$

(2) *Every l-batch-absorbing polynomial operation, $l > k$, is constant.*

(2*) *Every absorbing polynomial operation of arity $> k$ is constant.*

(3) *The subalgebra of $A^{2^{k+1}}$ generated by $\{c_i^{k+1}(a, b) : a, b \in A,\ i = 1, \ldots, k+1\}$ contains no fork.*

(4) *For every term t and all pairs of tuples $\boldsymbol{a}_1, \boldsymbol{b}_1, \ldots, \boldsymbol{a}_{k+1}, \boldsymbol{b}_{k+1}$ of elements of A,*

$$q_{k+1}(t(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{k+1}), t(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k, \boldsymbol{b}_{k+1}), \ldots, t(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k, \boldsymbol{a}_{k+1})) = t(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{k+1})$$

(the parameters of t on the left hand side are all combinations of $\boldsymbol{a}$'s and $\boldsymbol{b}$'s except the one on the right hand side).

Equivalence of conditions (1),(1*),(2*) is proved in [2], equivalence of condition (2) follows from Lemma 2.3, condition (3) appears in [16], condition (4) appears in [3].

Finite supernilpotent Mal'tsev algebras admit prime decomposition. This result can be found in [2, Section 7] although a major part of the proof is based on results of Kearnes [12].

Theorem 2.5 [2]. *Let A be a finite Mal'tsev algebra. Then A is k-supernilpotent for some k if and only if A is a direct product of nilpotent algebras of prime power size.*

3. (Super)nilpotence in Loops

3.1. Loops

Let $(Q, \cdot, \backslash, /, 1)$ be a loop, i.e., $\cdot$ is a binary operation, 1 is its unit element, $a\backslash b$ is the unique solution to the equation $a * x = b$ and dually for $/$. We denote $L_x(y) = xy$, $R_x(y) = yx$ the *left* and *right translations*. The *multiplication group* of Q is the permutation group generated by the translations, $\mathrm{Mlt}(Q) = \langle L_x, R_x : x \in Q\rangle$. The stabilizer of the unit element is called the *inner mapping group*, $\mathrm{Inn}(Q) = \mathrm{Mlt}(Q)_1$. The inner mapping group is generated by the mappings

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

A subloop of Q invariant with respect to the action of $\mathrm{Inn}(Q)$ is called *normal*. Normal subloops are precisely the kernels of homomorphisms. If N is a normal subloop of Q, then $|N|$ divides $|Q|$. If M, N are normal subloops of Q such that $M \cap N = 1$, then $|MN| = |M| \cdot |N|$.

For a general background in loops, we refer to the textbook [17].

3.2. Nilpotence

The theory of nilpotent loops has been developed since the very beginnings of loop theory, with definitions taken in direct analogy to group theory (for details, see the survey article [15]).

Fix any commutator term $[x, y]$, i.e., a term such that $[x, y] = 1$ if and only if $xy = yx$. Fix any associator term $[x, y, z]$, i.e., a term such that $[x, y, z] = 1$ if and only if $x(yz) = (xy)z$. The following definition is a straightforward generalization from group theory.

Definition 3.1. The *center of a loop* Q is defined by

$$Z(Q) = \{a \in Q : [a, x] = [a, x, y] = [x, a, y] = [x, y, a] = 1 \text{ for all } x, y \in Q\}.$$

A loop Q is called *k-centrally-nilpotent* if there is a series of normal subloops $1 = N_0 \le N_1 \le \ldots \le N_k = Q$ such that $N_{i+1}/N_i \le Z(Q/N_i)$. The *class of central nilpotence*, $\mathrm{cl}_{cn}(Q)$, is the smallest k such that A is k-centrally-nilpotent.

Note that $a \in Z(Q)$ if and only if $f(a) = a$ for every $f \in \mathrm{Inn}(Q)$.

We define the *upper central series* of Q as the series of normal subloops $Z_i(Q)$, $i = 0, 1, \ldots$ such that $Z_0(Q) = 1$ and $Z_{i+1}(Q)/Z_i(Q) = Z(Q/Z_i(Q))$. Clearly, if $Z_k(Q) = Q$, then Q is k-centrally-nilpotent, as witnessed by the series of iterated centers. The converse implication is also true, and not difficult to prove.

A loop is centrally nilpotent if and only if it is nilpotent in the sense of Sect. 2, see [20, Section 10] for a proof and [21] for a further discussion.

As noted earlier, loops of prime power order need not be nilpotent (since $|Z(Q)|$ divides $|Q|$, any non-associative loop of prime order fails to be nilpotent) and nilpotent loops generally do not admit a prime decomposition.

Example 3.2. The following multiplication table shows a loop Q of order 6 such that $\mathrm{cl}_{cn}(Q) = 2$, but it is directly indecomposable.

Q	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	4	5	6	1	2
4	4	3	6	5	2	1
5	5	6	2	1	3	4
6	6	5	1	2	4	3

The center is $Z(Q) = \{1, 2\}$, the factor $Q/Z(Q)$ is a cyclic group of order 3, hence $\mathrm{cl}_{cn}(Q) = 2$. It is the only proper normal subloop of Q, hence direct indecomposability.

3.3. Nilpotence of the Multiplication Group

The *multiplication group* $\mathrm{Mlt}(Q)$ of a loop Q is the subgroup of the symmetric group S_Q generated by all left and right translations (i.e., the mappings $x \mapsto ax$ and $x \mapsto xa$, for every $a \in Q$). The loop Q from Example 3.2 is 2-centrally-nilpotent, however, $\mathrm{Mlt}(Q)$ is a non-nilpotent group of order 24.

Bruck [5] proved that loops with a nilpotent multiplication group are centrally nilpotent, and Wright [23] proved that finite loops with a nilpotent multiplication group admit a prime decomposition. We present both proofs in Sect. 4.

3.4. Supernilpotence

Loops are Mal'tsev algebras, therefore, we can define supernilpotence by any of the equivalent conditions of Theorem 2.4. In our opinion, the absorption conditions (2) and (2*) are the most natural ones. We will use them in our proof of Theorem 1.1, and also in the subsequent paper [22].

We start with an observation that in loops, without loss of generality, we can consider only absorbing polynomials at $(1, \ldots, 1)$ into 1.

Observation 3.3. *Let Q be a loop. Then Q is k-supernilpotent if and only if all polynomials of arity $> k$ absorbing at* $(1, \ldots, 1)$ *into 1 are constant.*

Proof. ($\Rightarrow$) follows from Lemma 2.3. ($\Leftarrow$) Let $p(x_1, \ldots, x_n)$ be a polynomial absorbing at $\boldsymbol{a}$ into e. Let $q(x_1, \ldots, x_n) = p(x_1a_1, \ldots, x_na_n)/e$. Then q is absorbing at $(1, \ldots, 1)$ into 1, thus constant. Consequently, $p(x_1, \ldots, x_n) = q(x_1/a_1, \ldots, x_n/a_n)e$ is constant onto e. □

In the rest of the paper, all absorbing polynomials are implicitly understood to be absorbing $(1, \ldots, 1)$ into 1. A similar statement applies to batch-absorption.

Note that any commutator or associator term is absorbing. Therefore, 2-supernilpotent loops are associative and 1-supernilpotent loops are also commutative. Since in groups the classes of nilpotence and supernilpotence coincide, we obtain that

- A loop is 1-supernilpotent if and only if it is an abelian group,
- A loop is 2-supernilpotent if and only if it is a 2-nilpotent group.

For central nilpotence, we have $\mathrm{cl}_{cn}(Q/Z(Q)) = \mathrm{cl}_{cn}(Q) - 1$. For supernilpotence, the difference may be greater than 1. We will show that it is at least 1.

Proposition 3.4. *Let Q be a supernilpotent loop. Then $\mathrm{cl}_{sn}(Q/Z(Q)) < \mathrm{cl}_{sn}(Q)$.*

Proof. Let p be a k-ary absorbing polynomial on $Q/Z(Q)$. Let q result from p by replacing every constant $aZ(Q)$ by a. Then q is a polynomial on Q such that $q(a_1,\dots,a_k) \in Z(Q)$ whenever $a_i \in Z(Q)$ for some i. Let

$$\begin{aligned} r(y, x_1,\dots,x_k) &= [y, q(x_1,\dots,x_k)],\\ r_1(y,z,x_1,\dots,x_k) &= [y,z,q(x_1,\dots,x_k)],\\ r_2(y,z,x_1,\dots,x_k) &= [y,q(x_1,\dots,x_k),z],\\ r_3(y,z,x_1,\dots,x_k) &= [q(x_1,\dots,x_k),y,z]. \end{aligned}$$

Then r, r_1, r_2, r_3 are absorbing polynomials on Q of arity $> k$, hence constant on Q. Consequently, $q(a_1,\dots,a_k) \in Z(Q)$ for all $a_1,\dots,a_k \in Q$, and thus $p(a_1Z(Q),\dots,a_kZ(Q)) = 1Z(Q)$ in $Q/Z(Q)$. □

(This proposition actually holds for every Mal'tsev algebra A: if A is k-supernilpotent, then, using inequality (HC8) of [2], $[[1_A,\dots,1_A]_k, 1_A] \le [1_A,\dots,1_A]_{k+1} = 0_A$, which implies that $[1,\dots,1]_k$ is contained in the center ζ_A of A, and so A/ζ_A is $(k-1)$-supernilpotent. However note that the loop theoretic proof is rather elementary, not relying on the inequality (HC8).)

Condition (3) of Theorem 2.4 suggests an algorithmic procedure for checking supernilpotence. Subalgebra generation is efficient with respect to the subalgebra size, and searching for a fork is a simple task. Nevertheless, the subalgebra of A^{2^k} described in the condition may be (and often is) very large, even for small k and $|A|$. Storing the elements of the power in a tree data structure allows to identify forks instantly. With some optimization, we were able to find forks for certain loops of size 8, thus proving that they are not 3-supernilpotent.

Example 3.5. There are 134 non-associative nilpotent loops of order 8, listed in the `loops` package for the computer system `GAP` [14]. All of them have $\mathrm{cl}_{cn} = 2$ and $\mathrm{cl}_m \in \{3,4\}$.

There are 62 nilpotent loops of order 8 with $\mathrm{cl}_m = 3$. For 34 of them, we calculated that $\mathrm{cl}_{sn} > 3$. We expect that the remaining 28 loops have $\mathrm{cl}_{sn} = 3$, but we have no tool to prove so.

A detailed report on the computational experiments, including a description of the algorithm, can be found in [18].

4. Proof of Theorem 1.1

4.1. Proof of $\mathbf{cl}_m(Q) \leq \mathbf{cl}_{sn}(Q)$

First, let us formally introduce a correspondence between words in the multiplication group and terms of the loop.

Fix a set of variables X. An *m-word* of length l is a formal expression of the form $(U^{(1)}_{x_1})^{k_1}\dots(U^{(l)}_{x_l})^{k_l}$ where $U^{(i)} \in \{L, R\}$, $x_1, \dots, x_l \in X$ and $k_1, \dots, k_l \in \{\pm 1\}$. Expressions using group commutators will be also understood as m-words, for example, the expression $[L_x, R_y^{-1}]$ shall be understood as the m-word $L_x^{-1}R_yL_xR_y^{-1}$.

An m-word W containing variables $x_1, \dots, x_n \in X$ can be converted naturally into a loop term $t_W(x_1, \dots, x_n, z)$. For example, for $W = L_yR_x^{-1}$ we have $t_W(x, y, z) = y(z/x)$, interpreting the expression $L_yR_x^{-1}(z)$ as a term. Formally, we define t_W recursively: let $t_{l+1} = z$; for $i = l, \dots, 1$ we define $t_i = x_it_{i+1}$ if $U^{(i)} = L$ and $k_i = 1$, $t_i = x_i\backslash t_{i+1}$ if $U^{(i)} = L$ and $k_i = -1$, $t_i = t_{i+1}x_i$ if $U^{(i)} = R$ and $k_i = 1$, $t_i = t_{i+1}/x_i$ if $U^{(i)} = R$ and $k_i = -1$; finally, let $t_W = t_1$.

Observe that for every $f \in \mathrm{Mlt}(Q)$ there is an m-word W and $a_1, \dots, a_n \in Q$ such that $f(q) = t_W(a_1, \dots, a_n, q)$ for every $q \in Q$.

Proof. Assume that Q is k-supernilpotent. To prove that $\mathrm{Mlt}(Q)$ is k-nilpotent, we will show that

$$[f_1, [\dots, [f_k, f_{k+1}]]] = id$$

for all $f_1, \dots, f_{k+1} \in \mathrm{Mlt}(Q)$. This is equivalent to proving that Q satisfies every identity

$$t_W(\boldsymbol{x}_1, \dots, \boldsymbol{x}_{k+1}, z) = z$$

where

$$W = [W_1, [\dots, [W_k, W_{k+1}]]]$$

and $W_1(\boldsymbol{x}_1), \dots, W_{k+1}(\boldsymbol{x}_{k+1})$ are arbitrary m-words. Note that $t_W(\boldsymbol{u}_1, \dots, \boldsymbol{u}_{k+1}, q) = q$ whenever there is i such that $\boldsymbol{u}_i = (1, \dots, 1)$. Therefore, the polynomial

$$p(\boldsymbol{x}_1, \dots, \boldsymbol{x}_{k+1}) = t_W(\boldsymbol{x}_1, \dots, \boldsymbol{x}_{k+1}, q)/q$$

is $(k+1)$-batch-absorbing, thus constant onto 1, and $t_W(\boldsymbol{u}_1, \dots, \boldsymbol{u}_{k+1}, q) = q$ for every $\boldsymbol{u}_1, \dots, \boldsymbol{u}_{k+1}$ and q. □

4.2. Proof of $\mathbf{cl}_{cn}(Q) \leq \mathbf{cl}_m(Q)$

Let Q be a loop. We define a series $\mathcal{N}_0 \leq \mathcal{N}_1 \leq \dots$ of subgroups of $\mathrm{Mlt}(Q)$ inductively: let $\mathcal{N}_0 = \mathrm{Inn}(Q)$ and let $\mathcal{N}_{i+1}$ be the normalizer of $\mathcal{N}_i$ in $\mathrm{Mlt}(Q)$.

Lemma 4.1. *Let Q be a loop and $\mathcal{Z}_0 \leq \mathcal{Z}_1 \leq \dots$ the upper central series of* $\mathrm{Mlt}(Q)$*. Then $\mathcal{N}_i \geq \mathcal{Z}_i$ for every i.*

Proof. We proceed by induction on i. For $i = 0$, we have $\mathrm{Inn}(Q) = \mathcal{N}_0 \geq \mathcal{Z}_0 = 1$.

Suppose that $\mathcal{N}_i \geq \mathcal{Z}_i$ and let $f \in \mathcal{Z}_{i+1}$. By definition, $f\mathcal{Z}_i \in Z(\mathrm{Mlt}(Q)/\mathcal{Z}_i)$. For every $g \in \mathcal{N}_i$, $fgf^{-1}\mathcal{Z}_i = g\mathcal{Z}_i$, and thus, by the induction assumption, $fgf^{-1}\mathcal{N}_i = g\mathcal{N}_i = \mathcal{N}_i$, that is, $fgf^{-1} \in \mathcal{N}_i$. It follows that f is in the normalizer of $\mathcal{N}_i$, which is $\mathcal{N}_{i+1}$. □

Observe that, for every $t \in \mathrm{Mlt}(Q)$, we have $t = R_{t(1)}h$ for some $h \in \mathrm{Inn}(Q)$.

Lemma 4.2. *Let Q be a loop and $Z_0 \leq Z_1 \leq \ldots$ its upper central series. Then, for every i,*

$$\mathcal{N}_i = \{R_a f : \ a \in Z_i, f \in \mathrm{Inn}(Q)\}.$$

In particular, Q is k-nilpotent if and only if $\mathcal{N}_k = \mathrm{Mlt}(Q)$.

Proof. We prove the claim by induction on i. The case $i = 0$ is obvious, so suppose that the claim holds for some i and we prove it for $i + 1$.

($\subseteq$) Let $t = R_{t(1)}h \in N_{i+1}$. It is sufficient to show that $t(1) \in Z_{i+1}$. That is, $t(1)Z_i = Z(Q/Z_i)$, which means $f(t(1))Z_i = t(1)Z_i$ for every $f \in \mathrm{Inn}(Q)$.

Let $f \in \mathrm{Inn}(Q)$. Since t is in the normalizer of $\mathcal{N}_i$, for every $a \in Z_i$ we have $(R_a f)t = t(R_b g)$ for some $b \in Z_i$, $g \in \mathrm{Inn}(Q)$. Applying the equality on the unit element, we obtain

$$f(t(1))a = t(g(1)b) = t(b) = h(b)t(1),$$

and thus $f(t(1))Z_i = Z_i t(1) = t(1)Z_i$ which we wanted to prove.

($\supseteq$) Let $t = R_x h$, $h \in \mathrm{Inn}(Q)$, $x \in Z_{i+1}$, we prove that it normalizes every element of $\mathcal{N}_i$. By the induction assumption, consider the element $R_a f$ where $a \in Z_i$, $f \in \mathrm{Inn}(Q)$. Then $R_a ft = R_y h_1$, where $h_1 \in \mathrm{Inn}(Q)$ and $y = R_a ft(1) = f(x) \cdot a$. Since $x \in Z_{i+1}$, we have $f(x)Z_i = xZ_i = Z_i x$. Therefore, $y = f(x) \cdot a = cx$ for some $c \in Z_i$. Now, let $h_2 = R_c^{-1} R_x^{-1} R_{cx} h_1 \in \mathrm{Inn}(Q)$ and calculate

$$R_a ft = R_{cx}h_1 = R_x R_c h_2 = (R_x h)(h^{-1} R_c h_2) = (R_x h)(R_b g) = t(R_b g),$$

for $b = h^{-1}(c) \in Z_i$ and some $g \in \mathrm{Inn}(Q)$. It follows that $t \in \mathcal{N}_{i+1}$.

The last claim follows from the fact that $\{R_a : a \in Q\}$ is a transversal of $\mathrm{Inn}(Q)$ in $\mathrm{Mlt}(Q)$. □

The inequality $\mathrm{cl}_{cn}(Q) \leq \mathrm{cl}_m(Q)$ immediately follows, since, by Lemma 4.1, the series $\mathcal{N}_i$ terminates not later than the series $\mathcal{Z}_i$.

4.3. Proof of $\mathrm{cl}_m(Q) < \infty \Rightarrow \mathrm{cl}_{sn}(Q) < \infty$

For every loop Q, there is a (covariant) Galois correspondence (cf. [4, Section 2.5]) between normal subloops of Q and normal subgroups of $\mathrm{Mlt}(Q)$, given by

$$\begin{aligned} \mathrm{NSub}(Q) &\leftrightarrow \mathrm{NSub}(\mathrm{Mlt}(Q)) \\ N &\rightarrowtail N^* = \{f \in \mathrm{Mlt}(Q):\ f(x)/x \in N \text{ for all } x \in Q\} \\ G(1) = \{g(1) : g \in G\} &\leftarrowtail G \end{aligned}$$

Checking all the properties is routine. In our proof, we will use the following two of them:

(G1) $G(1)$ *is a normal subloop of* Q, since, for every $f \in \mathrm{Inn}(Q)$ and $g \in G$, we have $fgf^{-1} \in G$ and thus $f(g(1)) = fgf^{-1}(f(1)) = fgf^{-1}(1) \in G(1)$;
(G2) $G \subseteq G(1)^*$, since, for every $g \in G$ and $x \in Q$, we have $R_x^{-1} g R_x \in G$ and thus $g(x)/x = R_x^{-1} g R_x(1) \in G(1)$.

Furthermore, observe that

(G3) $|G(1)|$ *divides* $|G|$, since $|G(1)| = [G : G_1]$ (the orbit size equals the index of the stabilizer);
(G4) *if* N *is a normal subloop of* Q, *then* $\mathrm{Mlt}(Q/N) \simeq \mathrm{Mlt}(Q)/N^*$: consider the homomorphism $\mathrm{Mlt}(Q) \to \mathrm{Mlt}(Q/N)$, $f \mapsto (xN \mapsto f(x)N)$, calculate its kernel $\{f : f(x)N = xN \text{ for all } x \in Q\} = N^*$ and use the first isomorphism theorem.

Proposition 4.3 ([6, Lemma 2.2 of Section VI.2]). *Let* Q *be a finite loop and* p *a prime. Then* Q *is nilpotent of order* p^k *if and only if* $\mathrm{Mlt}(Q)$ *is a* p*-group.*

Proof. ($\Leftarrow$) Since p-groups are nilpotent, Q is nilpotent by the result of the previous section. If m divides $|Q|$, then m also divides $|\mathrm{Mlt}(Q)| = |Q|\cdot|\mathrm{Inn}(Q)|$, hence the only prime divisor of $|Q|$ is p.

($\Rightarrow$) We will proceed by induction on $\mathrm{cl}_{cn}(Q)$. If Q is an abelian group, then $\mathrm{Mlt}(Q) \simeq Q$ and we are done. In the induction step, consider the factor $Q/Z(Q)$. Its nilpotence class is smaller, hence $\mathrm{Mlt}(Q/Z(Q))$ is a p-group. Using (G4), we obtain $|\mathrm{Mlt}(Q)| = |\mathrm{Mlt}(Q/Z(Q))| \cdot |Z(Q)^*|$, hence it remains to show that $Z(Q)^*$ is a p-group.

For f in $Z(Q)^*$, consider the mapping $\varphi_f(x) = f(x)/x$. By definition of $Z(Q)^*$, the mapping φ_f maps Q into $Z(Q)$, thus it belongs to the direct power $Z(Q)^Q$. The mapping $Z(Q)^* \to Z(Q)^Q$, $f \mapsto \varphi_f$ is clearly injective, and we show that it is a group homomorphism: for every $x \in Q$,

$$\varphi_{fg}(x) = f(g(x))/x = f((g(x)/x) \cdot x)/x = (f(x)/x)(g(x)/x) = \varphi_f(x)\varphi_g(x),$$

where the crucial equality follows from the observation that $h(zx) = zh(x) = h(x)z$ for every $x \in Q$, $z \in Z(Q)$ and $h \in \mathrm{Mlt}(Q)$. Consequently, $Z(Q)^*$ is isomorphic to a subgroup of $Z(Q)^Q$, which is an abelian p-group. □

Proof (Proof of $\mathrm{cl}_m(Q) < \infty \Rightarrow \mathrm{cl}_{sn}(Q) < \infty$). Let Q be a finite loop such that $\mathrm{Mlt}(Q)$ is nilpotent. In particular, Q is also nilpotent, as we proved earlier, and so are all subloops of Q. If we prove that Q admits a prime decomposition, then supernilpotence follows from Theorem 2.5.

We find the prime decomposition by induction on $|Q|$. If Q is trivial or $|Q|$ is a prime power, it admits trivial prime decomposition. So assume that $|Q| = p^e r$ where p is prime, $e \geq 1$, $p \nmid r \neq 1$.

Under the assumptions, $\mathrm{Mlt}(Q)$ is not a p-group, otherwise violating Proposition 4.3. Let $\mathrm{Mlt}(Q) = PR$ be an internal direct product where P is the Sylow p-subgroup (it exists, since $\mathrm{Mlt}(Q)$ is nilpotent). By (G1), both $P(1)$ and $R(1)$ are normal subloops of Q, and (G3) implies that $|P(1)|$ is a power of p, and p does not divide $|R(1)|$. By the Lagrange property of normal subloops, $P(1) \cap R(1) = 1$. We will show that $Q = P(1)R(1)$.

By (G2), $\mathrm{Mlt}(Q) = PR \subseteq P(1)^* R(1)^*$, hence $P(1)^* R(1)^* = \mathrm{Mlt}(Q)$. We also have $P(1)^* \cap R(1)^* = 1$, since, if $f \in P(1)^* \cap R(1)^*$, then $f(x)/x \in P(1) \cap R(1) = 1$ for every $x \in Q$. Therefore, $\mathrm{Mlt}(Q) = P(1)^* R(1)^*$ is also an internal direct decomposition, and comparing the numbers of elements, we obtain that $P(1)^* = P$ and $R(1)^* = R$. Using (G4),

$$\mathrm{Mlt}(Q/R(1)) \simeq \mathrm{Mlt}(Q)/R(1)^* = \mathrm{Mlt}(Q)/R \simeq P,$$

which is a p-group, hence $|Q/R(1)|$ is a power of p by Proposition 4.3, and thus r divides $R(1)$. Using (G4) again,

$$\mathrm{Mlt}(Q/P(1)) \simeq \mathrm{Mlt}(Q)/P(1)^* = \mathrm{Mlt}(Q)/P \simeq R,$$

a nilpotent group, hence we can apply the induction assumption, obtain a direct decomposition $Q/P(1) \simeq \prod Q_{p_i}$, hence also a direct decomposition $R \simeq \mathrm{Mlt}(Q/P(1)) \simeq \prod \mathrm{Mlt}(Q_{p_i})$, and we see from Proposition 4.3 that none of p_i equals p. Therefore, p does not divide $Q/P(1)$, and thus $|P(1)| = p^e$ (we already know that $|P(1)|$ is a power of p). Consequently, $|P(1)R(1)| = |P(1)| \cdot |R(1)| \geq p^e r = |Q|$ (the first equality follows from $P(1) \cap R(1) = 1$), and thus $Q = P(1)R(1)$.

Consequently, $Q \simeq P(1) \times R(1)$ is a direct decomposition, $|P(1)| = p^e$, $|R(1)| = r < |Q|$. Applying the induction assumption on $R(1) \simeq Q/P(1)$, we obtain a prime decomposition of Q. $\square$

5. Open Problems

Problem 1. Does the equivalence

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

hold for every loop Q? Stated differently, is every loop Q with nilpotent multiplication group supernilpotent?

Problem 2. (1) Find a function f such that $\mathrm{cl}_{sn}(Q) \leq f(\mathrm{cl}_{cn}(Q))$ for every supernilpotent loop Q, or prove that no such function exists.

(2) Find a function g such that $\mathrm{cl}_{sn}(Q) \leq g(\mathrm{cl}_m(Q))$ for every supernilpotent loop Q, or prove that no such function exists.

Examples of loops Q with small $\mathrm{cl}_{cn}(Q)$ or $\mathrm{cl}_m(Q)$ and large $\mathrm{cl}_{sn}(Q)$ are also of interest, since they provide lower bounds for f, g.

Funding Open access publishing supported by the National Technical Library in Prague. Ž. Semanišinová partially supported by the DFG grant 467967530. D. Stanovský partially supported by the GAČR grant 18-20123S and by the cooperation grant LTAUSA19070.

Data Availibility Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose.

References

[1] Aichinger, E., Ecker, J.: Every $(k+1)$-affine complete nilpotent group of class k is affine complete. Internat J. Algebra Comput. **16**(2), 259–274 (2006)

[2] Aichinger, E., Mudrinski, N.: Some applications of higher commutators in Mal'cev algebras. Algebra Universalis **63**(4), 367–403 (2010)

[3] Aichinger, E., Mudrinski, N., Opršal, J.: Complexity of term representations of finitary functions. Internat J. Algebra Comput. **28**(6), 1101–1118 (2018)

[4] Bergman, C.: Universal Algebra: Fundamentals and Selected Topics. Chapman & Hall/CRC Press (2011)

[5] Bruck, R.H.: Contributions to the theory of loops. Trans. Am. Math. Soc. **60**, 245–354 (1946)

[6] Bruck, R.H.: A Survey of Binary Systems. Ergebnisse der Mathematik und ihrer Grenzgebiete, 3rd edn. Springer (1971)

[7] Bulatov, A.: On the number of finite Mal'tsev algebras. Contrib. Gener. Algebra **13**, 41–54 (2001)

[8] Freese, R., McKenzie, R.: Commutator Theory for Congruence Modular Varieties. London Mathematical Society Lecture Note Series 125, Cambridge University Press, Cambridge (1987)

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

[10] Glauberman, G., Wright, C.R.B.: Nilpotence of finite Moufang 2-loops. J. Algebra **8**, 415–417 (1968)

[11] Hagemann, J., Herrmann, C.: A concrete ideal multiplication for algebraic systems and its relations to congruence distributivity. Arch. Math. **32**, 234–245 (1979)

[12] Kearnes, K.A.: Congruence modular varieties with small free spectra. Algebra Universalis **42**, 165–181 (1999)

[13] Moorhead, A.: Higher commutator theory for congruence modular varieties. J. Algebra **513**, 133–158 (2018)

[14] Nagy, G. P., Vojtěchovský, P.: LOOPS: computing with quasigroups and loops in GAP, version 2.2.0, available at https://science.du.edu/math/loops

[15] Niemenmaa, M., Rytty, M.: Centrally nilpotent finite loops. Quasigroups Relat. Syst. **19**(1), 123–132 (2011)

[16] Opršal, J.: A relational description of higher commutators in Mal'cev varieties. Algebra Universalis **76**(3), 367–383 (2016)

[17] Pflugfelder, H.O.: Quasigroups and Loops: Introduction. Heldermann Verlag, Berlin (1990)

[18] Semanišinová, Ž: Higher commutators in loop theory. Master Thesis, Charles University, Prague (2021)

[19] Smith, J. D. H.: Mal'cev Varieties. Lecture Notes in Math. 554, Springer, Berlin (1976)

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

[21] Stanovský, D., Vojtěchovský, P.: Abelian extensions and solvable loops. Results Math. **66**(3–4), 367–384 (2014)

[22] Stanovský, D., Vojtěchovský, P.: Supernilpotent groups and 3-supernilpotent loops, to appear. J. Algebra Appl.

[23] Wright, C.R.B.: On the multiplication group of a loop. Illinois J. Math. **13**, 660–673 (1969)

Žaneta Semanišinová
Faculty of Mathematics, Institute of Algebra
Technische Universität Dresden
Dresden
Germany
e-mail: `zaneta.semanisinova@tu-dresden.de`

David Stanovský
Department of Algebra, Faculty of Mathematics and Physics
Charles University
Prague
Czechia
e-mail: `stanovsk@karlin.mff.cuni.cz`

Received: August 5, 2022.
Accepted: March 4, 2023.