COMMUTATOR THEORY FOR LOOPS

DAVID STANOVSKÝ AND PETR VOJTĚCHOVSKÝ

Abstract. Using the Freese-McKenzie commutator theory for congruence modular varieties as the starting point, we develop commutator theory for the variety of loops. The fundamental theorem of congruence commutators for loops relates generators of the congruence commutator to generators of the total inner mapping group. We specialize the fundamental theorem into several varieties of loops, and also discuss the commutator of two normal subloops.

Consequently, we argue that some standard definitions of loop theory, such as elementwise commutators and associators, should be revised and linked more closely to inner mappings. Using the new definitions, we prove several natural properties of loops that could not be so elegantly stated with the standard definitions of loop theory. For instance, we show that the subloop generated by the new associators defined here is automatically normal. We conclude with a preliminary discussion of abelianess and solvability in loops.

1. Introduction

The two primary influences on modern loop theory come from group theory and universal algebra, a fact that is reflected already in the definition of a loop. Using the group-theoretical approach, a *loop* is a nonempty set Q with identity element 1 and with binary operation $\cdot$ such that for every a, $b \in Q$ the equations $a \cdot x = b$, $y \cdot a = b$ have unique solutions x, $y \in Q$. The implied presence of divisions is made explicit in the equivalent universal algebraic definition due to Evans [11]: a *loop* is a universal algebra $(Q, 1, \cdot, \backslash, /)$ satisfying the identities

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

It is not difficult to see that associative loops are precisely groups, where we write $x^{-1}y$ and xy^{-1} in place of $x\backslash y$ and x/y, respectively.

The most influential text on loop theory in the English-speaking world is the book of Bruck [5]. Although its title "A survey of binary systems" and its opening chapters are rather encompassing, it focuses on and culminates in the study of Moufang loops, a variety of loops with properties close to groups. It is therefore natural that Bruck's definitions are rooted mostly in group theory. For instance, a subloop N of a loop Q is said to be *normal* in Q if

$$xN = Nx, \quad x(yN) = (xy)N, \quad N(xy) = (Nx)y$$

for every x, $y \in Q$, the *center* $Z(Q)$ of Q is defined as

$$Z(Q) = \{a \in Q;\ ax{=}xa,\ a(xy){=}(ax)y,\ x(ay){=}(xa)y,\ x(ya){=}(xy)a \text{ for every } x, y \in Q\},$$

2000 *Mathematics Subject Classification.* Primary: 08B10, 20N05. Secondary: 08A30.

Key words and phrases. Commutator theory, congruence commutator, loop, commutator of normal subloops, commutator, associator, associator subloop, derived subloop, inner mapping, inner mapping group, total inner mapping group.

Research partially supported by the Simons Foundation Collaboration Grant 210176 to Petr Vojtěchovský.

and the elementwise *commutator* $[x, y]$ and *associator* $[x, y, z]$ are defined as the unique solutions to the equations

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

respectively. The *associator subloop* $A(Q)$ of Q is the smallest normal subloop of Q such that $Q/A(Q)$ is a group, or, equivalently, the smallest normal subloop of Q containing all associators $[x, y, z]$ of Q. The *derived subloop* Q' of Q is the smallest normal subloop of Q such that Q/Q' is an abelian group, or, equivalently, the smallest normal subloop of Q containing all commutators $[x, y]$ and all associators $[x, y, z]$ of Q. With $Q^{[0]} = Q$, $Q^{[i+1]} = (Q^{[i]})'$, a loop is called *solvable* if $Q^{[n]} = 1$ for some n.

It is easy to see that in groups the above concepts specialize to the usual group-theoretical notions (the associator and the associator subloop being void). Bruck's deep results [5] showed that the group-theoretical definitions are sensible in Moufang loops, as did Glauberman's extension of the Feit-Thompson Odd Order Theorem to Moufang loops [17].

As it turns out, the normality, the center and the derived notion of central nilpotency are the correct concepts for loops even from the universal algebraic point of view. (For normality this was known already to Bruck. For the center and central nilpotency this is probably folklore, but since we were not able to find a proof in the literature, we present it at the end of this paper for the convenience of the reader.) It is therefore not surprising that central nilpotency played a prominent role in the development of loop theory, as witnessed by the 42 papers listed in MathSciNet under primary classification 20N05 and with one of the words "nilpotent", "nilpotency" or "nilpotence" in the title. We mention [8, 9, 17, 18, 21, 25, 29, 30, 32, 33, 37] as a representative sample.

But the commutators and associators did not fare as well, and neither did the concept of solvability. The inadequacies of the elementwise associators were first pointed out by Leong [24]; see below for more details. There is no established notion of commutator of two normal subloops and, in contrast to nilpotency, there are only 9 papers on MathSciNet under 20N05 and with one of the words "solvable", "solvability", "soluble" or "solubility" in the title.

We maintain that this is not a coincidence, but rather a consequence of the fact that the elementwise associators, the commutator theory and solvability were not well conceived in loop theory. This is somewhat surprising, since loops are known to be congruence modular (they possess a Mal'tsev term), the general commutator theory for congruence modular varieties [12] has been developed more than 25 years ago, and, furthermore, the original impetus for the commutator theory came from an important work of Smith [36], who set out to understand abelianess (or, centrality, in his terms) in quasigroups, a variety closely related to loops. For more historical details concerning commutator theory, see [12].

The Freese-McKenzie commutator theory has proved useful in so many applications (see [28] for a survey) that we have little doubt it is the correct setting for loops, too. In this paper we derive the commutator theory for loops, with the congruence commutators at its core. The results are summarized in Section 2.

Standard references to loop theory include [2, 5, 34]. See [4, 6] for an introduction to universal algebra and [28] for an introduction to congruence commutators.

2. Summary of results

Inner mappings. Let Q be a loop with identity element 1. For every $x \in Q$ let L_x, R_x, $M_x : Q \to Q$ be the bijections defined by

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

The mappings L_x, R_x are traditionally called *left* and *right translations*. The mappings $y \mapsto x\backslash y$ and $y \mapsto y/x$ are the respective inverses of L_x and R_x. The mapping $y \mapsto x/y$ is the inverse of M_x, because $z = y\backslash x$ iff $yz = x$ iff $y = x/z$.

Following the conventional definitions of loop theory, the left and right translations generate the *multiplication group* $\mathrm{Mlt}(Q)$ of Q, i.e.,

$$\mathrm{Mlt}(Q) = \langle L_x, R_x;\ x \in Q\rangle.$$

The *inner mapping group* $\mathrm{Inn}(Q)$ of Q is the stabilizer of 1 in $\mathrm{Mlt}(Q)$.

To bring the mappings M_x into play, we introduce the *total multiplication group* $\mathrm{TMlt}(Q)$ of Q as

$$\mathrm{TMlt}(Q) = \langle L_x, R_x, M_x;\ x \in Q\rangle.$$

The *total inner mapping group* $\mathrm{TInn}(Q)$ of Q is the stabilizer of 1 in $\mathrm{TMlt}(Q)$. (Belousov [3] was probably the first to ever consider total multiplication groups and total inner mapping groups.)

Although we will carefully distinguish between $\mathrm{Inn}(Q)$ and $\mathrm{TInn}(Q)$, we will call elements of both $\mathrm{Inn}(Q)$ and $\mathrm{TInn}(Q)$ *inner mappings*. Note that, unlike in groups, $\mathrm{Inn}(Q)$ is not necessarily a subgroup of the automorphism group $\mathrm{Aut}(Q)$. (Loops where $\mathrm{TInn}(Q) \leq \mathrm{Aut}(Q)$ were investigated in [3].)

In Section 3.2, we calculate two small sets of generators for $\mathrm{TInn}(Q)$, namely

$$\mathrm{TInn}(Q) = \langle L_{x,y},\, R_{x,y},\, M_{x,y},\, T_x,\, U_x;\ x,\, y \in Q\rangle = \langle A^{\cdot}_{x,y},\, B^{\cdot}_{x,y},\, A^{\backslash}_{x,y};\ x,\, y \in Q\rangle,$$

where

$$L_{x,y} = L_{xy}^{-1}L_xL_y, \quad R_{x,y} = R_{yx}^{-1}R_xR_y, \quad M_{x,y} = M_{y\backslash x}^{-1}M_xM_y, \quad T_x = R_x^{-1}L_x, \quad U_x = R_x^{-1}M_x,$$

and

$$(z \cdot x) \circ y = A^{\circ}_{x,y}(z) \cdot (x \circ y), \qquad y \circ (z \cdot x) = B^{\circ}_{x,y}(z) \cdot (y \circ x).$$

for $\circ \in \{\cdot, \backslash, /\}$. Each of these generating sets is an example of a *set of words* that *generates total inner mapping groups* in all loops, a concept that is formally defined in Section 3.3. Informally, the above mappings, applied to an argument z, can be seen as loop terms in variables x, y, z which yield a generating set of $\mathrm{TInn}(Q)$ for any loop Q upon substituting all elements of Q for x and y.

The commutator. Let $\mathbf{A}$ be a universal algebra. The congruences of $\mathbf{A}$ form a lattice with largest element $1_{\mathbf{A}} = \mathbf{A} \times \mathbf{A}$ and smallest element $0_{\mathbf{A}} = \{(a, a);\ a \in \mathbf{A}\}$.

Let α, β, δ be congruences of $\mathbf{A}$. We say that α *centralizes* β *over* δ, and write $C(\alpha, \beta; \delta)$, if for every $(n+1)$-ary term operation t, every pair $a\,\alpha\,b$ and every $u_1\,\beta\,v_1$, …, $u_n\,\beta\,v_n$ we have

$$t(a, u_1, \ldots, u_n)\,\delta\,t(a, v_1, \ldots, v_n) \quad \text{implies} \quad t(b, u_1, \ldots, u_n)\,\delta\,t(b, v_1, \ldots, v_n).$$

This implication is referred to as the *term condition* for t, or $\mathrm{TC}(t, \alpha, \beta, \delta)$.[1]

[1] From now on, we will use the word "term" for both term operations and terms.

The *commutator* of α, β, denoted by $[\alpha, \beta]$, is the smallest congruence δ such that $C(\alpha, \beta; \delta)$. The Freese-McKenzie monograph [12] developed the theory and applications of this congruence operation in congruence modular varieties.

It is not easy to work with $C(\alpha, \beta; \delta)$ because the term condition must be tested for every term. It is therefore by no means straightforward to specialize the theory of [12] into a particular variety. The fundamental result of our paper is a description of the commutator $[\alpha, \beta]$ in loops, involving only a few special terms, namely the terms resulting from any set of words that generates total inner mapping groups. We will write $\mathrm{Cg}(X)$ for the congruence generated by X, and we will denote by $\bar{u}$ the n-tuple $u_1, \ldots, u_n$, where we intentionally omit the usual enclosing parentheses. We also write $\bar{u}\,\beta\,\bar{v}$ instead of $u_1\,\beta\,v_1,\ \ldots,\ u_n\,\beta\,v_n$.

Theorem 2.1 (Fundamental Theorem of Commutator Theory in Loops)**.** *Let $\boldsymbol{V}$ be a variety of loops and $\mathcal{W}$ a set of words that generates total inner mapping groups in $\boldsymbol{V}$. Then*

$$[\alpha, \beta] = \mathrm{Cg}(\ (W_{\bar{u}}(a), W_{\bar{v}}(a));\ W \in \mathcal{W},\ 1\,\alpha\,a,\ \bar{u}\,\beta\,\bar{v}\ )$$

for any congruences α, β of any $Q \in \boldsymbol{V}$.

A particular generating set for $[\alpha, \beta]$ is obtained anytime a suitable generating set $\mathcal{W}$ is given, for instance the above-mentioned set $\mathcal{W} = \{L_{x,y},\ R_{x,y},\ T_x,\ M_{x,y},\ U_x\}$ for the variety $\boldsymbol{V}$ of all loops. See Example 3.12 for other options.

Notice that the definition of the commutator is asymmetric, and so is the generating set from Theorem 2.1. Nevertheless, $[\alpha, \beta] = [\beta, \alpha]$ for any congruences α, β in any algebra in a congruence modular variety [12]. This is an important property, although we do not need it in the present paper.

The proof of Theorem 2.1 is presented in Section 4, and it is based on the words $A^{\circ}_{x,y}$, $B^{\circ}_{x,y}$. Note that the words $A^{\circ}_{x,y}$ resemble associators and the words $B^{\circ}_{x,y}$ look like a combination of commutators and associators, except that the element z is absorbed into both $A^{\circ}_{x,y}(z)$ and $B^{\circ}_{x,y}(z)$.

The machinery of Theorem 2.1 can be used to obtain numerous descriptions of the commutator $[\alpha, \beta]$. Theorem 4.4 strengthens Theorem 2.1 in loops satisfying a finiteness condition. More efficient generating sets $\mathcal{W}$ for Theorem 2.1 are investigated in Section 5, with the results summarized in Corollary 5.2. Generating sets in terms of elementwise associators and commutators, a traditional approach of group theory and loop theory, are given in Corollary 6.3. The normal subloop corresponding to the congruence commutator is studied in Section 7.

Further simplifications are possible in specific classes of loops—throughout the paper we focus on inverse property loops, commutative loops and groups. In Section 9 we illustrate how Theorem 2.1 and its corollaries can be used to calculate the commutator in concrete loops. We also provide examples that witness that our results are optimal in certain ways.

Elementwise associators and commutators. Leong [24] noticed that, indeed, the associator $[x, y, z]$ corrects for the lack of associativity in the equation $(xy)z = x(yz)$, but so do many other associators, for instance the associator $a^L(x, y, z)$ defined by

$$(xy)z = (a^L(x, y, z)x)(yz),$$

or the associator $b^L(x, y, z)$ defined by

$$x(yz) = ((b^L(x, y, z)x)y)z.$$

The advantage of these new associators is that they relate to inner mappings, namely, $a^L(x,y,z) = R_{z,y}(x)/x$, and $b^L(x,y,z) = R^{-1}_{z,y}(x)/x$. Leong proved that in every loop Q the subloop $\langle a^L(x,y,z), b^L(x,y,z);\ x,y,z \in Q\rangle$ is normal, and hence equal to $A(Q)$. He also showed that if Q is a Moufang loop then $A(Q) = \langle [x,y,z];\ x,y,z \in Q\rangle$. Covalschi and Sandu [7] recently introduced similar associators that can be used to generate Q'.

The difficulty lies in deciding which associators should be used. Our approach is systematic and is based on the idea that elementwise associators and commutators should follow naturally from the commutator theory for congruences. Upon separating the roles of commutators and associators, we present a systematic definition of all possible associators and commutators in any loop, the result being summarized in Table 1. Importantly, all these associators and commutators are associated with certain inner mappings (they evaluate to 1 when $x = 1$ is substituted), and thus can be used to obtain a generating set of the congruence commutator; see Corollary 6.3.

In Section 8, we make a case for our commutators and associators. First, we show that Q' is the subloop generated by a choice of associators and commutators whenever the corresponding inner mappings generate $\mathrm{Inn}(Q)$; see Theorem 8.2. Then, imitating the proof of Leong, we show that certain associators generate $A(Q)$; see Theorem 8.4.

The commutator of normal subloops. It is well known that a subloop of a loop Q is normal iff it is a kernel of some homomorphism from Q to another loop. Equivalently, normal subloops are precisely the blocks of congruences on Q containing the identity element 1, or subloops closed under all inner mappings from $\mathrm{Inn}(Q)$. In Proposition 3.7, we show that normal subloops are closed under all inner mappings from $\mathrm{TInn}(Q)$, too.

There exists an order-preserving correspondence between the lattice of normal subloops of Q and the lattice of congruences of Q. If N is a normal subloop of Q, let γ_N be the congruence on Q defined by

$$a\,\gamma_N\,b \text{ iff } a/b \in N,$$

or, equivalently, iff $b\backslash a \in N$, $b/a \in N$, or $a\backslash b \in N$. If α is a congruence of Q, let N_α be the normal subloop of Q defined by

$$N_\alpha = \{a \in Q;\ a\,\alpha\,1\}.$$

For two normal subloops A, B of Q, define the *commutator* of A and B in Q by

$$[A,B]_Q = N_{[\gamma_A,\gamma_B]}.$$

The above correspondence allows us to immediately translate Theorem 2.1 from the language of congruences to the language of normal subloops. We will write $\mathrm{Ng}(X)$ for the smallest normal subloop containing the set X, and $\bar{u}/\bar{v} \in B$ as a shorthand for $u_1/v_1 \in B$, ..., $u_n/v_n \in B$.

Theorem 2.2. *Let $\boldsymbol{V}$ be a variety of loops and $\mathcal{W}$ a set of words that generates total inner mapping groups in $\boldsymbol{V}$. Then*

$$[A,B]_Q = \mathrm{Ng}(\ W_{\bar{u}}(a)/W_{\bar{v}}(a);\ W \in \mathcal{W},\ a \in A,\ \bar{u}/\bar{v} \in B\ )$$

for any normal subloops A, B of any $Q \in \boldsymbol{V}$.

Using the ideas of Section 6, we can choose $\mathcal{W}$ so that we can interpret the generating set of $[A,B]_Q$ as quotients of associators and commutators.

In Section 7, we explore simplifications of the generating set. It so happens that in groups the normal closure is not needed and the quotients can be reduced, i.e.,

$$[A, B]_Q = \langle [a, u]/[a, v];\ a \in A,\ u/v \in B \rangle = \langle [a, b];\ a \in A,\ b \in B \rangle.$$

Neither of these properties holds in general loops, as illustrated by examples in Section 9. The normal closure can be avoided in all *automorphic loops*, that is, loops Q with $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$; see Proposition 7.3. Some types of quotients can be reduced in all loops; see Corollary 7.5.

Center and nilpotency, abelianess and solvability. The general commutator theory for universal algebras offers more than just the commutator of two congruences. An algebra $\mathbf{A}$ is called *nilpotent*, if $\gamma_{(n)} = 0_{\mathbf{A}}$ for some n, where

$$\gamma_{(0)} = 1_{\mathbf{A}}, \qquad \gamma_{(i+1)} = [\gamma_{(i)}, 1_{\mathbf{A}}].$$

An algebra $\mathbf{A}$ is called *solvable*, if $\gamma^{(n)} = 0_{\mathbf{A}}$ for some n, where

$$\gamma^{(0)} = 1_{\mathbf{A}}, \qquad \gamma^{(i+1)} = [\gamma^{(i)}, \gamma^{(i)}].$$

Notice that both definitions use a special type of commutators: nilpotency requires only commutators $[\alpha, 1_{\mathbf{A}}]$, while solvability requires only commutators $[\alpha, \alpha]$. Both of these types of commutators can be defined using specialized concepts: center and abelianess.

Let $\mathbf{A}$ be an algebra. The *center* of $\mathbf{A}$, denoted by $\zeta(\mathbf{A})$, is the largest congruence of $\mathbf{A}$ such that $C(\zeta(\mathbf{A}), 1_{\mathbf{A}}; 0_{\mathbf{A}})$. It is easy to show that $[\alpha, 1_{\mathbf{A}}]$ is the smallest congruence δ such that $\alpha/\delta \leq \zeta(\mathbf{A}/\delta)$.

A congruence α of an algebra $\mathbf{A}$ is called *abelian* if $C(\alpha, \alpha; 0_{\mathbf{A}})$. It is easy to show that $[\alpha, \alpha]$ is the smallest congruence δ such that α/δ is an abelian congruence of $\mathbf{A}/\delta$. An algebra $\mathbf{A}$ is called *abelian* if $\zeta(\mathbf{A}) = 1_{\mathbf{A}}$, or, equivalently, if the congruence $1_{\mathbf{A}}$ is abelian.

An argument similar to the one in group theory shows that $\mathbf{A}$ is nilpotent (resp. solvable) if and only if there is a chain of congruences

$$1_{\mathbf{A}} = \alpha_0 \geq \alpha_1 \geq \ldots \geq \alpha_n = 0_{\mathbf{A}}$$

such that $\alpha_i/\alpha_{i+1} \leq \zeta(\mathbf{A}/\alpha_{i+1})$ (resp. such that α_i/α_{i+1} is an abelian congruence of $\mathbf{A}/\alpha_{i+1}$) for all $i \in \{0, 1, \ldots, n-1\}$.

Now, let Q be a loop. One can quickly show (and it follows from Theorem 10.1) that a loop is abelian if and only if it is a commutative group. With respect to nilpotency and solvability, there are good news and bad news.

Fortunately, the center $\zeta(Q)$ as defined in universal algebra, and the center $Z(Q)$ as defined in loop theory agree, i.e., $N_{\zeta(Q)} = Z(Q)$; see Theorem 10.1. Consequently, nilpotency based on the commutator theory is the same concept as central nilpotency traditionally used in loop theory. In our opinion, this explains why central nilpotency has been playing a prominent role in loop theory.

Unfortunately, Bruck's concept of solvability derived from group theory does not agree with the universal algebraic solvability. The commutator theory suggests there is a difference between *abelianess* of an algebra and *abelianess in an algebra*. This is inherent in the congruence approach, since congruences carry over the universe of the original algebra, so the congruence commutator $[\alpha, \alpha]$ automatically takes place in the underlying algebra $\mathbf{A}$. In loops, we have to be careful. Upon translating the concept of abelianess from congruences to normal subloops, we note that a normal subloop N of Q is *abelian* if $[1_N, 1_N] = 0_N$. However,

N is *abelian in* Q if $[\gamma_N, \gamma_N] = 0_Q$, a stronger property in general. Examples of an abelian loop $N \trianglelefteq Q$ that is not abelian in Q were known already to Freese and McKenzie; see [12, Chapter 5, Exercise 10] or our Example 9.3.

In our opinion, this explains why there are relatively few results on solvable loops, and why most existing results deal with varieties of loops that are close to groups. For instance, the Feit-Thompson Odd Order Theorem [14] has been extended from groups to Moufang loops in [17], and to automorphic loops in [22], Hall's theorem for Moufang loops can be found in [17] and in [15]. A notable exception is the general result of Vesanen [38]: if the group $\mathrm{Mlt}(Q)$ is solvable then Q itself is solvable in the group-theoretical sense. But hardly anything is known in the other direction, starting with the assumption that Q is solvable. Could this be so because the traditional definition of solvability in loops is too weak?

We propose to call a loop Q *congruence solvable* if there is a chain $1 = Q_0 \leq Q_1 \leq \cdots \leq Q_n = Q$ of normal subloops Q_i of Q such that every factor Q_{i+1}/Q_i is abelian in Q/Q_i. Does congruence solvability of Q relate to the structure of the total multiplication group $\mathrm{TMlt}(Q)$? Is group-theoretical solvability equivalent to congruence solvability in classes of loops close to groups? These questions and related problems are subject of an ongoing investigation of the authors. Here we at least show that while every congruence solvable loop is indeed solvable, the converse is not true; see Example 9.3.

Section 10 explains in more detail how the center, central nilpotency, abelianess and solvability specialize from universal algebras to loops, and from loops to groups. We also provide references to other alternative approaches to nilpotency and solvability in loops and other classes of algebras.

Auxiliary definitions. Let Q be a loop with *two-sided inverses*, that is, a loop in which for every $x \in Q$ there is $x^{-1} \in Q$ such that $xx^{-1} = x^{-1}x = 1$. We then define the inversion mapping

$$J : Q \to Q, \qquad J(x) = x^{-1}.$$

Note that $(x^{-1})^{-1} = x$, and hence J is involutory.

We say that Q has the *anti-automorphic inverse property* (AAIP) if $(xy)^{-1} = y^{-1}x^{-1}$ for every $x, y \in Q$, or, equivalently, if the mapping J is an anti-automorphism. We say that Q has the *inverse property* if $x^{-1}(xy) = y = (yx)x^{-1}$ holds for every x, $y \in Q$. Then $x\backslash y$ can be replaced by $x^{-1}y$ and x/y by xy^{-1}, as in groups. Note that inverse property loops have the AAIP: $(xy) \cdot (xy)^{-1}x = x = (xy)y^{-1}$, so $(xy)^{-1}x = y^{-1}$, and using the inverse property again, $(xy)^{-1} = y^{-1}x^{-1}$. Many highly structured varieties of loops have the inverse property, most notably groups and Moufang loops.

3. Inner mappings

3.1. **Inner mapping groups.** Let Q be a loop. Recall that $\mathrm{Mlt}(Q) = \langle L_x, R_x;\ x \in Q \rangle$ and $\mathrm{Inn}(Q) = \mathrm{Mlt}(Q)_1 = \{f \in \mathrm{Mlt}(Q);\ f(1) = 1\}$. One possible generating set of $\mathrm{Inn}(Q)$ is described in the well known Proposition 3.2, which is in turn based on a variation of a result of O. Schreier about generators of stabilizers.

Lemma 3.1 (O. Schreier)**.** *Let G be a transitive permutation group on a set X and let $c \in X$. For $y \in X$ let $g_y \in G$ be such that $g_y(c) = y$, where we choose $g_c = 1$. If $G = \langle H \rangle$ then $G_c = \langle g_{h(y)}^{-1} h g_y;\ h \in H,\ y \in X \rangle$.*

Proof. Let $g \in G_c$. Since $G = \langle H \rangle$, there are $h_1, \ldots, h_n \in H \cup H^{-1}$ such that $g = h_1 \cdots h_n$. We thus have

$$g = g_{h_1 \cdots h_n(c)}(g^{-1}_{h_1 \cdots h_n(c)} h_1 g_{h_2 \cdots h_n(c)}) \cdots (g^{-1}_{h_{n-1} h_n(c)} h_{n-1} g_{h_n(c)})(g^{-1}_{h_n(c)} h_n g_c) g_c^{-1}.$$

Note that $g_{h_1 \cdots h_n(c)} = g_{g(c)} = g_c = 1$, so g is a product of elements of the form $g^{-1}_{h(y)} h g_y$, where $h \in H \cup H^{-1}$. The identity

$$(g^{-1}_{h(y)} h g_y)^{-1} = g_y^{-1} h^{-1} g_{h(y)} = g^{-1}_{h^{-1}h(y)} h^{-1} g_{h(y)}$$

shows that generators of the form $g^{-1}_{h(y)} h g_y$ with $h \in H$ suffice. □

Recall the mappings $A^{\cdot}_{x,y} = R^{-1}_{xy} R_y R_x$ and $B^{\cdot}_{x,y} = R^{-1}_{yx} L_y R_x$ introduced in Section 2.

Proposition 3.2. *Let Q be a loop. Then*

$$\mathrm{Inn}(Q) = \langle L_{x,y},\ R_{x,y},\ T_x;\ x, y \in Q \rangle = \langle A^{\cdot}_{x,y}, B^{\cdot}_{x,y};\ x, y \in Q \rangle.$$

Proof. The multiplication group $G = \mathrm{Mlt}(Q)$ acts transitively on $X = Q$. Upon applying Lemma 3.1 with $c = 1$, $g_y = R_y$ and $H = \{L_x,\ R_x;\ x \in Q\}$, we conclude that $G_1 = \mathrm{Inn}(Q)$ is generated by $\{R^{-1}_{L_x(y)} L_x R_y,\ R^{-1}_{R_x(y)} R_x R_y;\ x,\ y \in Q\} = \{B^{\cdot}_{y,x},\ A^{\cdot}_{y,x};\ x, y \in Q\}$. Now note that $A^{\cdot}_{y,x} = R_{x,y}$ and $B^{\cdot}_{y,x} = R^{-1}_{L_x(y)} L_x R_y = (R^{-1}_{xy} L_{xy})(L^{-1}_{xy} L_x L_y)(L_y^{-1} R_y) = T_{xy} L_{x,y} T_y^{-1}$. □

An immediate corollary of Proposition 3.2 is the observation that $\mathrm{Inn}(Q) = 1$ if and only if Q is an abelian group. We will need this fact in Section 8.

The significance of $\mathrm{Inn}(Q)$ is that it can be used to characterize normal subloops, just as in the case of groups.

Proposition 3.3. *Let N be a subloop of Q. Then the following conditions are equivalent:*

(i) *N is normal in Q, that is, $xN = Nx$, $x(yN) = (xy)N$, $N(xy) = (Nx)y$ holds for every x, $y \in Q$.*
(ii) *$f(N) = N$ for every $f \in \mathrm{Inn}(Q)$.*
(iii) *N is the kernel of some loop homomorphism.*
(iv) *N is the block containing 1 of some congruence on Q.*

Proof. This is folklore. See [34, Section I.7] for the equivalence of (i)–(iii), or [10]. □

3.2. **Total inner mapping groups.** In this subsection, we partly follow Belousov and Shcherbakov [3, 35]. Recall that $\mathrm{TMlt}(Q) = \langle L_x, R_x, M_x;\ x \in Q \rangle$, where $M_x(y) = y \backslash x$, and $\mathrm{TInn}(Q) = \mathrm{TMlt}(Q)_1$. Also recall the mappings

$$M_{x,y} = M^{-1}_{y \backslash x} M_x M_y \quad \text{and} \quad U_x = R_x^{-1} M_x$$

and note that $M_{x,y}$, $U_x \in \mathrm{TInn}(Q)$ thanks to $M_{x,y}(1) = (y \backslash x)/((1 \backslash y) \backslash x) = 1$ and $U_x(1) = (1 \backslash x)/x = 1$. Finally, the mappings $A^{\circ}_{x,y}$, $B^{\circ}_{x,y}$ can be written as

$$\begin{aligned}
A^{\cdot}_{x,y} &= R^{-1}_{xy} R_y R_x, & B^{\cdot}_{x,y} &= R^{-1}_{yx} L_y R_x,\\
A^{\backslash}_{x,y} &= R^{-1}_{x \backslash y} M_y R_x, & B^{\backslash}_{x,y} &= R^{-1}_{y \backslash x} L_y^{-1} R_x,\\
A^{/}_{x,y} &= R^{-1}_{x/y} R_y^{-1} R_x, & B^{/}_{x,y} &= R^{-1}_{y/x} M_y^{-1} R_x,
\end{aligned}$$

and we note that $A^{/}_{x,y} = (A^{\cdot}_{x/y,y})^{-1}$, $B^{\backslash}_{x,y} = (B^{\cdot}_{y \backslash x,y})^{-1}$ and $B^{/}_{x,y} = (A^{\backslash}_{y/x,y})^{-1}$. All these mappings fix the identity element 1 and hence are inner mappings.

Proposition 3.4. *Let Q be a loop. Then*

$$\mathrm{TInn}(Q) = \langle L_{x,y},\, R_{x,y},\, M_{x,y},\, T_x,\, U_x;\ x, y \in Q\rangle = \langle A^{\cdot}_{x,y},\, B^{\cdot}_{x,y},\, A^{\backslash}_{x,y};\ x, y \in Q\rangle.$$

Proof. Let us apply Lemma 3.1 to the transitive group $G = \mathrm{TMlt}(Q)$ with $X = Q$, $c = 1$, $g_y = R_y$ and $H = \{L_x,\, R_x,\, M_x;\ x \in Q\}$. We conclude that $G_1 = \mathrm{TInn}(Q) = \langle R^{-1}_{L_x(y)} L_x R_y,\, R^{-1}_{R_x(y)} R_x R_y,\, R^{-1}_{M_x(y)} M_x R_y;\ x, y \in Q\rangle = \langle B^{\cdot}_{y,x},\, A^{\cdot}_{y,x},\, A^{\backslash}_{y,x};\ x, y \in Q\rangle$. By Proposition 3.2, $\mathrm{Inn}(Q) = \langle A^{\cdot}_{x,y},\, B^{\cdot}_{x,y};\ x, y \in Q\rangle = \langle L_{x,y},\, R_{x,y},\, T_x;\ x, y \in Q\rangle$. We finish with $A^{\backslash}_{y,x} = R^{-1}_{y\backslash x} M_x R_y = (R^{-1}_{y\backslash x} M_{y\backslash x})(M^{-1}_{y\backslash x} M_x M_y)(M^{-1}_y R_y) = U_{y\backslash x} M_{x,y} U^{-1}_y$. □

Problem 3.5. *Are the generating sets from Proposition 3.4 minimal, in the sense that none of the five (respectively three) types of mappings can be removed? Is there a generating set for* $\mathrm{TMlt}(Q)$ *with only two types of inner mappings?*

Example 3.6. Consider the loops Q_1, Q_2, Q_3, Q_4 with multiplication tables

Q_1	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	2	1
4	4	6	2	5	1	3
5	5	3	6	1	4	2
6	6	5	1	2	3	4

Q_3	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	5	6	3
3	3	4	5	6	1	2
4	4	5	6	3	2	1
5	5	6	1	2	3	4
6	6	3	2	1	4	5

Q_2	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	7	8	5	6
3	3	4	1	2	6	5	8	7
4	4	3	2	1	8	7	6	5
5	5	6	7	8	1	2	3	4
6	6	8	5	7	3	1	4	2
7	7	5	8	6	2	4	1	3
8	8	7	6	5	4	3	2	1

Q_4	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	1	2	7	8	5	6
4	4	3	2	1	8	7	6	5
5	5	6	7	8	1	2	4	3
6	6	5	8	7	2	1	3	4
7	7	8	5	6	4	3	1	2
8	8	7	6	5	3	4	2	1

In the `GAP` package `LOOPS`, these are the loops with catalog numbers $Q_1 =$ `SmallLoop(6,8)`, $Q_2 =$ `LeftBolLoop(8,1)`, $Q_3 =$ `SmallLoop(6,47)` and $Q_4 =$ `AutomorphicLoop(8,1)`. Then it can be verified in `GAP` that

$$\langle L_{x,y},\, R_{x,y},\, M_{x,y},\, U_x;\ x, y \in Q\rangle \neq \mathrm{TMlt}(Q)$$

for $Q = Q_1, Q_2$, and

$$\langle L_{x,y},\, R_{x,y},\, M_{x,y},\, T_x;\ x, y \in Q\rangle \neq \mathrm{TMlt}(Q) \neq \langle A^{\cdot}_{x,y},\, B^{\cdot}_{x,y};\ x,\, y \in Q\rangle$$

for $Q = Q_3, Q_4$. Hence neither of the mappings T_x, U_x, $A^{\backslash}_{x,y}$ can be removed in general from the generating sets of $\mathrm{TInn}(Q)$ (cf. Proposition 3.4), even in some highly structured varieties of loops.

We now observe that $\mathrm{TInn}(Q)$ can also be used to characterize normal subloops, hence adding another equivalent condition to Proposition 3.3.

Proposition 3.7 ([3])**.** *Let N be a subloop of Q. Then N is normal in Q if and only if $f(N) = N$ for every $f \in \mathrm{TInn}(Q)$.*

Proof. In view of Propositions 3.3 and 3.4, it only remains to show that if $N \trianglelefteq Q$, then $U_x(a) = (a\backslash x)/x \in N$ and $M_{x,y}(a) = (y\backslash x)/((a\backslash y)\backslash x) \in N$ for every $x,\ y \in Q$ and $a \in N$. Let φ be a homomorphism from Q to another loop such that $N = \ker(\varphi)$. Then $\varphi(U_x(a)) = (\varphi(a)\backslash\varphi(x))/\varphi(x) = U_{\varphi(x)}(\varphi(a)) = U_{\varphi(x)}(1) = 1$, and, similarly, $\varphi(M_{x,y}(a)) = M_{\varphi(x),\varphi(y)}(\varphi(a)) = M_{\varphi(x),\varphi(y)}(1) = 1$. □

We now focus on an important special case, the class of inverse property loops (see also [35]).

Proposition 3.8. *Let Q be an inverse property loop. Then*

(i) $\mathrm{TMlt}(Q) = \langle L_x,\ J;\ x \in Q\rangle = \langle M_x;\ x \in Q\rangle$.
(ii) $\mathrm{TInn}(Q) = \langle L_{x,y},\ T_x,\ J;\ x, y \in Q\rangle = \langle M_{x,y};\ x, y \in Q\rangle$.

Proof. (i) Clearly, $J \in \mathrm{TMlt}(Q)$, since $J = M_1$. To show that L_x, J generate $\mathrm{TMlt}(Q)$, observe that $R_x = JL_x^{-1}J$ and $M_x = JL_x^{-1}$. To show that M_x generate $\mathrm{TMlt}(Q)$, observe again that $J = M_1$ and $L_x = M_x^{-1}J$.

(ii) For the first assertion, apply Lemma 3.1 to the transitive group $G = \mathrm{TMlt}(Q)$ with $X = Q$, $c = 1$, $g_y = L_y$ and $H = \{L_x,\ J;\ x \in Q\}$. We conclude that $G_1 = \mathrm{TInn}(Q) = \langle L_yJL_y,\ L_{xy}^{-1}L_xL_y;\ x, y \in Q\rangle = \langle JT_y,\ L_{x,y};\ x, y \in Q\rangle = \langle L_{x,y},\ T_x,\ J;\ x, y \in Q\rangle$, because $J = JT_1$.

For the second assertion, apply Lemma 3.1 to the transitive group $G = \mathrm{TMlt}(Q)$ with $X = Q$, $c = 1$, $g_y = R_y$ and $H = \{M_x,;\ x \in Q\}$. We conclude that $G_1 = \mathrm{TInn}(Q) = \langle R_{y\backslash x}^{-1}M_xR_y;\ x, y \in Q\rangle = \langle JM_{x,y}J;\ x, y \in Q\rangle = \langle M_{x,y};\ x, y \in Q\rangle$, because $J = M_{1,1}$ and $JM_{1,1}J = J^3 = J$. □

We finish this subsection with a side remark. It is well known that the multiplication group $\mathrm{Mlt}(G)$ of a group G is isomorphic to $(G \times G)/\{(a, a);\ a \in Z(G)\}$. Here is an analogous description of $\mathrm{TMlt}(G)$:

Proposition 3.9. *Let G be a group.*

(i) *If G is not an elementary abelian 2-group then* $\mathrm{TMlt}(G)$ *is isomorphic to*

$$((G \times G) \rtimes \mathbb{Z}_2)/\{(a, a, 0);\ a \in Z(G)\},$$

where $\mathbb{Z}_2$ acts on $G \times G$ by transposing the two coordinates in the direct product.
(ii) *If G is an elementary abelian 2-group then* $\mathrm{TMlt}(G) = \mathrm{Mlt}(G)$ *is isomorphic to G.*

Proof. Note that $\mathrm{TMlt}(G) = \langle L_x, R_x, J;\ x \in G\rangle$. If G is an elementary abelian 2-group then J is the identity mapping, $L_x = R_x$ for every $x \in G$, and hence $\mathrm{TMlt}(G) = \{L_x;\ x \in G\}$ is isomorphic to G according to Cayley's left regular representation. For the rest of the proof assume that G is not an elementary abelian 2-group.

With the action from the statement of the proposition, the multiplication in $(G \times G) \rtimes \mathbb{Z}_2$ is given by

$$(a, b, u)(c, d, v) = \begin{cases} (ac, bd, v), & \text{if } u = 0, \\ (ad, bc, 1 + v), & \text{if } u = 1. \end{cases}$$

Define $\varphi : (G \times G) \rtimes \mathbb{Z}_2 \to \mathrm{TMlt}(G)$ by $\varphi(a, b, u) = L_aR_b^{-1}J^u$. To check that φ is a homomorphism, take $\varphi(a, b, u)\varphi(c, d, v)(x) = L_aR_b^{-1}J^uL_cR_d^{-1}J^v(x)$ and consider two cases. If $u = 0$, the above element is equal to $acJ^v(x)d^{-1}b^{-1} = L_{ac}R_{bd}^{-1}J^v(x) = \varphi(ac, bd, v)(x) =$

$\varphi((a,b,0)(c,d,v))(x)$. If $u=1$, we calculate $a(cJ^v(x)d^{-1})^{-1}b^{-1} = adJ^{1+v}(x)c^{-1}b^{-1} = L_{ad}R_{bc}^{-1}J^{1+v}(x) = \varphi(ad,bc,1+v)(x) = \varphi((a,b,1)(c,d,v))(x)$.

Since the image of φ contains all generators of $\mathrm{TMlt}(G)$, we see that φ is onto $\mathrm{TMlt}(G)$. The kernel of φ consists of all (a,b,u) such that $L_aR_b^{-1}J^u$ is the identity mapping, which means $aJ^u(x)b^{-1} = x$ for every $x \in G$. If $x=1$, we obtain $a=b$, hence the kernel only contains triples (a,a,u) such that $aJ^u(x)a^{-1} = x$ for every $x \in G$, or, equivalently, $a^{-1}xa = J^u(x)$ for every $x \in G$. If $u=0$, this is equivalent to $a \in Z(G)$. If $u=1$, the left hand side defines an automorphism of G, but J is an automorphism only if G is abelian. When G is abelian, the condition $x = a^{-1}xa = J(x) = x^{-1}$ says that G is an elementary abelian 2-group, a contradiction. Hence $\ker(\varphi) = \{(a,a,0);\ a \in Z(G)\}$. □

3.3. **Generating inner mappings uniformly.** Propositions 3.2, 3.4 and 3.8 establish small sets of inner mappings generating $\mathrm{Inn}(Q)$ and $\mathrm{TInn}(Q)$ for a loop Q in certain varieties (of all loops, and all IP loops). Interestingly, these sets generate the respective groups *uniformly*, independently of Q within a given variety. In the rest of the section, we will formalize this idea, to be used in the proof of Theorem 2.1.

Formally, a *word* $W = W_{\bar{x}}$ is an element of the free group generated by letters K_t, where $K \in \{L,R,M\}$ and t is a term over $\bar{x}$. Equivalently, it is a formal expression of the form $K^1_{t_1(\bar{x})}\dots K^k_{t_k(\bar{x})}$ where $K^1,\dots,K^k$ are letters from $\{L,R,M,L^{-1},R^{-1},M^{-1}\}$ and $t_1,\dots,t_k$ are arbitrary loop terms. Every word induces a mapping

$$W_{\bar{x}} : Q^n \to \mathrm{TMlt}(Q), \qquad \bar{a} \mapsto W_{\bar{a}},$$

where $W_{\bar{a}}$ is the mapping obtained by replacing every $K^i_{t_i(\bar{a})}$ with the actual translation on Q by $t_i(\bar{a})$. We can thus write $W_{\bar{a}}(b) \in Q$ for the result of the mapping $W_{\bar{a}}$ on $b \in Q$. Every word W also induces a term: given another variable y, we can consider $W_{\bar{x}}(y)$ as a term, resulting by evaluating the mapping $W_{\bar{x}}$ in the free loop of terms over $x_1,\dots,x_n,y$. The following examples should make this clear.

Example 3.10. The expression $L_{x,y}$ defined by $L_{xy}^{-1}L_xL_y$ is a word. Then $L_{x,y}(z)$ denotes the term $(xy)\backslash(x(yz))$, and for every loop Q and every $a,b \in Q$, $L_{a,b}$ denotes the inner mapping $L_{ab}^{-1}L_aL_b$. Note that J is also a word, with no parameters, defined by $J = M_1$, where 1 is a term with no parameters.

Let $\boldsymbol{V}$ be a variety of loops. We say that a word W is *inner* for $\boldsymbol{V}$, if $W_{\bar{a}} \in \mathrm{TInn}(Q)$ for every $Q \in \boldsymbol{V}$ and every $a_1,\dots,a_n \in Q$. Note that this is equivalent to saying that $W_{\bar{x}}(1) = 1$ is a valid identity in the variety $\boldsymbol{V}$. Again, let us clarify the idea with an example.

Example 3.11. The word $L_{x,y}$ is inner for the variety of all loops. The word J is inner for the variety of all inverse property loops. The word $W = L_xL_x$ is inner for the variety of all loops satisfying the identity $x^2 = 1$, since $L_aL_a(1) = a^2 = 1$, but it is not inner for the variety of all loops.

Let $\boldsymbol{V}$ be a variety of loops, and let $\mathcal{W}$ be a set of inner words for $\boldsymbol{V}$. We say that $\mathcal{W}$ *generates inner mapping groups* in $\boldsymbol{V}$ if for every $Q \in \boldsymbol{V}$ we have

$$\mathrm{Inn}(Q) = \langle W_{\bar{a}};\ W \in \mathcal{W},\ a_1,\dots,a_n \in Q\rangle,$$

and it *generates total inner mapping groups* in $\boldsymbol{V}$ if for every $Q \in \boldsymbol{V}$ we have

$$\mathrm{TInn}(Q) = \langle W_{\bar{a}};\ W \in \mathcal{W},\ a_1,\dots,a_n \in Q\rangle.$$

Example 3.12. Using Propositions 3.2, 3.4, 3.8, and some trivial observations, we have:

- Let $\boldsymbol{V}$ be a variety of loops. Then $\{L_{x,y},\, R_{x,y},\, T_x\}$ generates inner mapping groups in $\boldsymbol{V}$, $\{L_{x,y},\, R_{x,y},\, T_x,\, M_{x,y},\, U_x\}$ generates total inner mapping groups in $\boldsymbol{V}$, $\{A^{\cdot}_{x,y},\, B^{\cdot}_{x,y}\}$ generates inner mapping groups in $\boldsymbol{V}$, and $\{A^{\cdot}_{x,y},\, B^{\cdot}_{x,y},\, A^{\backslash}_{x,y}\}$ generates total inner mapping groups in $\boldsymbol{V}$.
- Let $\boldsymbol{V}$ be a variety of commutative loops. Then $\{L_{x,y}\}$ generates inner mapping groups in $\boldsymbol{V}$, $\{L_{x,y},\, M_{x,y},\, U_x\}$ generates total inner mapping groups in $\boldsymbol{V}$, and $\{A^{\cdot}_{x,y},\, A^{\backslash}_{x,y}\}$ generates total inner mapping groups in $\boldsymbol{V}$.
- Let $\boldsymbol{V}$ be a variety of inverse property loops. Then $\{L_{x,y},\, T_x,\, J\}$ generates total inner mapping groups in $\boldsymbol{V}$.
- Let $\boldsymbol{V}$ be a variety of groups. Then $\{T_x\}$ generates inner mapping groups in $\boldsymbol{V}$, and $\{T_x,\, J\}$ generates total inner mapping groups in $\boldsymbol{V}$.

The following lemma explains how (total) inner mapping groups can be generated uniformly. We will write $\mathcal{W}^{\pm 1}$ for $\{W,\, W^{-1};\ W \in \mathcal{W}\}$, where W^{-1} is the word obtained by formally inverting W.

Lemma 3.13. *Let $\boldsymbol{V}$ be a variety of loops, $\mathcal{W}$ a set generating (total) inner mapping groups in $\boldsymbol{V}$ and V an inner word for $\boldsymbol{V}$. Then there exist $W^i \in \mathcal{W}^{\pm 1}$ and terms t^i_j such that*

$$V_{\bar{a}} = W^1_{t^1_1(\bar{a}),\dots,t^1_{r_1}(\bar{a})} \dots W^k_{t^k_1(\bar{a}),\dots,t^k_{r_k}(\bar{a})}$$

for every $Q \in \boldsymbol{V}$ and every $a_1, \dots, a_n \in Q$.

Proof. We will write down the case of inner mapping groups. For total inner mapping groups, replace every reference to $\mathrm{Inn}(Q)$ by $\mathrm{TInn}(Q)$.

Let F be the free loop in $\boldsymbol{V}$ on n generators $x_1, \dots, x_n$. We know that $V_{\bar{x}} \in \mathrm{Inn}(F)$ (as it does for any $Q \in \boldsymbol{V}$ and every choice of parameters from Q). Since $\mathrm{Inn}(F)$ is generated by all $W_{\bar{t}}$ such that $W \in \mathcal{W}$ and $t_1, \dots, t_n \in F$ (as so does $\mathrm{Inn}(Q)$ for every $Q \in \boldsymbol{V}$), there exist words $W^1, \dots, W^k \in \mathcal{W}^{\pm 1}$ and parameters $t^i_j \in F$ such that

$$V_{\bar{x}} = W^1_{t^1_1,\dots,t^1_{r_1}} \dots W^k_{t^k_1,\dots,t^k_{r_k}}.$$

Notice that elements of F are just terms in variables $x_1, \dots, x_k$, and inner mappings in F can be considered as inner words for $\boldsymbol{V}$, since the equality $V(1) = 1$ in F becomes an identity true in $\boldsymbol{V}$.

The whole situation easily maps into every loop in $\boldsymbol{V}$. Given $Q \in \boldsymbol{V}$ and $a_1 \dots, a_n \in Q$, let $f : F \to Q$ be the homomorphism induced by $x_1 \mapsto a_1, \dots, x_n \mapsto a_n$. Upon applying the homomorphism, we obtain the equality in the statement of the lemma. □

Assuming the notation of Lemma 3.13, we say that, in the variety $\boldsymbol{V}$, the mappings induced by V are *uniformly generated* using the words W^i and the terms t^i_j. Since the statement of Lemma 3.13 is a bit technical, we again make it clear with an example:

Example 3.14. Let Q be an arbitrary loop, $a \in Q$, and consider the mapping f_a defined by $f_a(z) = (z\backslash a)\backslash a$. Then $f_a \in \mathrm{TMlt}(Q)$, because $f_a = M_a M_a$. It is an inner mapping because $f_a(1) = 1$. Consequently, Proposition 3.4 says that f_a is a product of mappings $A^{\cdot}_{x,y}$, $B^{\cdot}_{x,y}$, $A^{\backslash}_{x,y}$ and their inverses, for some choice of parameters x, $y \in Q$.

But what if we choose a different $b \in Q$, or if we work in a different loop? Do we get an analogous generating word for f_b? Lemma 3.13 guarantees that there is a uniform way of generating f_a in every loop for every choice of a, because f_a is induced by the inner word $M_x M_x$.

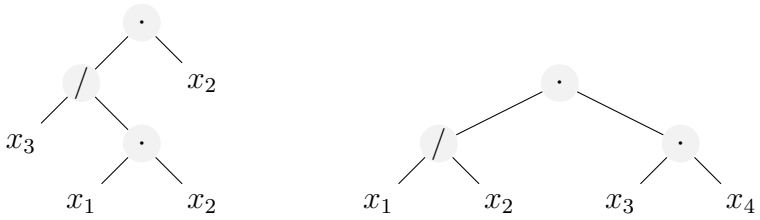
Note, however, that the proof of Lemma 3.13 is not constructive, so it is not at all clear how to generate a particular inner mapping from a set of words that generates (total) inner mapping groups.

4. Proof of the fundamental theorem

4.1. **Auxiliary lemmas.** The principal difficulty with the proof of Theorem 2.1 is the fact that to establish centrality, one has to consider the term condition TC for all terms. Lemma 4.1 below reduces the set of terms that need to be considered.

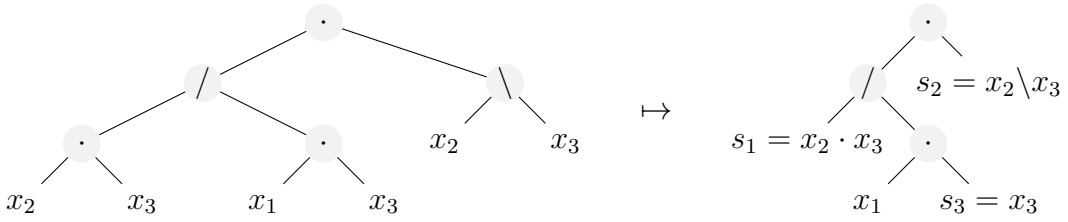
A term $t(x_1, \dots, x_n)$ is called *slim with respect to* x_1, if there is only one occurrence of x_1 in t, if this occurrence is in the lowest level of t, and if every node of t has at most one branch of length greater than 1.

For example, the term on the left is slim with respect to x_1 but not with respect to the other variables, and the term on the right is not slim with respect to any variables:



Lemma 4.1. *Let* $\mathbf{A}$ *be an algebra and* α, β, δ *its congruences. If* $\mathrm{TC}(t, \alpha, \beta, \delta)$ *holds for every term* t *that is slim with respect to the first variable, then* $C(\alpha, \beta; \delta)$ *holds.*

Proof. We prove the lemma in two steps. First, we show that $\mathrm{TC}(t, \alpha, \beta, \delta)$ holds for every term t, not necessarily slim, with only one occurrence of the first variable. Let $t = t(x_1, \dots, x_{n+1})$ be such a term. Define a new term, $s(x_1, y_1, \dots, y_k)$, by replacing each maximal subterm $s_i(x_2, \dots, x_n)$ of t not containing x_1 by a new variable y_i. Then s is slim with respect to x_1, and $t(x_1, \dots, x_{n+1}) = s(x_1, s_1, \dots, s_k)$, as illustrated below:



Let $a \,\alpha\, b$, $\bar{u} \,\beta\, \bar{v}$. Then indeed $s_i(u_1, \dots, u_n) \,\beta\, s_i(v_1, \dots, v_n)$ for every i, because β is a congruence. Suppose that $t(a, u_1, \dots, u_n) \,\delta\, t(a, v_1, \dots, v_n)$, which we can restate as

$$s(a, s_1(u_1, \dots, u_n), \dots, s_k(u_1, \dots, u_n)) \,\delta\, s(a, s_1(v_1, \dots, v_n), \dots, s_k(v_1, \dots, v_n)).$$

Using $\mathrm{TC}(s, \alpha, \beta, \delta)$, we deduce

$$s(b, s_1(u_1, \dots, u_n), \dots, s_k(u_1, \dots, u_n)) \,\delta\, s(b, s_1(v_1, \dots, v_n), \dots, s_k(v_1, \dots, v_n)),$$

which means $t(b,u_1,\dots,u_n)\,\delta\,t(b,v_1,\dots,v_n)$. Hence $\mathrm{TC}(t,\alpha,\beta,\delta)$ holds for every term t with a single occurrence of the first variable.

In the second step, consider a general term $t=t(x_1,\dots,x_{n+1})$ with k occurrences of x_1. Define a new term, $s(y_1,\dots,y_k,x_2,\dots,x_{n+1})$, by replacing every occurrence of x_1 by a unique new variable y_1, …, y_k. We will use $\mathrm{TC}(s,\alpha,\beta,\delta)$ repeatedly, once for each of the variables y_1, …, y_k, starting with $t(a,u_1,\dots,u_n)\,\delta\,t(a,v_1,\dots,v_n)$, i.e., with

$$s(a,\dots,a,u_1,\dots,u_n)\,\delta\,s(a,\dots,a,v_1,\dots,v_n).$$

Then

$$\begin{gathered}s(b,a,\dots,a,u_1,\dots,u_n)\,\delta\,s(b,a,\dots,a,v_1,\dots,v_n),\\ s(b,b,a,\dots,a,u_1,\dots,u_n)\,\delta\,s(b,b,a,\dots,a,v_1,\dots,v_n),\\ \vdots\\ s(b,\dots,b,u_1,\dots,u_n)\,\delta\,s(b,\dots,b,v_1,\dots,v_n),\end{gathered}$$

which translates into $t(b,u_1,\dots,u_n)\,\delta\,t(b,v_1,\dots,v_n)$, and we are through. □

The following lemma is more general than we need in the proof of Theorem 2.1, but it is readily available using Lemma 3.13.

Lemma 4.2. *Let $\boldsymbol{V}$ be a variety of loops, $\mathcal{W}$ a set of words that generates total inner mapping groups in $\boldsymbol{V}$, $Q\in\boldsymbol{V}$ and α, β congruences of Q. Put*

$$\delta=\mathrm{Cg}(\ (W_{\bar u}(a),W_{\bar v}(a));\ W\in\mathcal{W},\ 1\,\alpha\,a,\ \bar u\,\beta\,\bar v\ ).$$

Then $(V_{\bar u}(a),V_{\bar v}(a))\in\delta$ for every word V that is inner for $\boldsymbol{V}$ and for every $1\,\alpha\,a$, $\bar u\,\beta\,\bar v$.

Proof. We first note that $W_{\bar u}^{-1}(a)\,\delta\,W_{\bar v}^{-1}(a)$ for every $W\in\mathcal{W}$, $1\,\alpha\,a$ and $\bar u\,\beta\,\bar v$. Indeed, since $1=W_{\bar u}^{-1}(1)\,\alpha\,W_{\bar u}^{-1}(a)$, we get $a=W_{\bar u}(W_{\bar u}^{-1}(a))\,\delta\,W_{\bar v}(W_{\bar u}^{-1}(a))$, and thus $W_{\bar u}^{-1}(a)\,\delta\,W_{\bar v}^{-1}(a)$.

According to Lemma 3.13, there exist $W^1,\dots,W^k\in\mathcal{W}^{\pm1}$ and terms t_i^j such that they uniformly generate the mappings induced by V. To keep our notation simple, we will use the shorthand $W^i_{\bar t(\bar z)}$ for the mapping $W^i_{t_1^i(\bar z),\dots,t_{r_i}^i(\bar z)}$. Notice that if $x\,\delta\,y$, then $W^i_{\bar t(\bar z)}(x)\,\delta\,W^i_{\bar t(\bar z)}(y)$ for every $\bar z\in Q$.

Fix $a\,\alpha\,1$. An easy induction shows the result: for $i=k$, we have $W^k_{\bar t(\bar u)}(a)\,\delta\,W^k_{\bar t(\bar v)}(a)$ by the definition of δ, and if $W^{i+1}_{\bar t(\bar u)}\dots W^k_{\bar t(\bar u)}(a)\,\delta\,W^{i+1}_{\bar t(\bar v)}\dots W^k_{\bar t(\bar v)}(a)$, then

$$W^i_{\bar t(\bar u)}W^{i+1}_{\bar t(\bar u)}\dots W^k_{\bar t(\bar u)}(a)\,\delta\,W^i_{\bar t(\bar u)}W^{i+1}_{\bar t(\bar v)}\dots W^k_{\bar t(\bar v)}(a)\,\delta\,W^i_{\bar t(\bar v)}W^{i+1}_{\bar t(\bar v)}\dots W^k_{\bar t(\bar v)}(a),$$

where the former equivalence follows from the induction assumption, and the latter one follows from the definition of δ, because $W^{i+1}_{\bar t(\bar v)}\dots W^k_{\bar t(\bar v)}$ is an inner mapping, and thus $1=W^{i+1}_{\bar t(\bar v)}\dots W^k_{\bar t(\bar v)}(1)\,\alpha\,W^{i+1}_{\bar t(\bar v)}\dots W^k_{\bar t(\bar v)}(a)$. □

4.2. **Proof of the fundamental theorem.** We are ready to prove Theorem 2.1:

Proof of Theorem 2.1. Let $\delta=\mathrm{Cg}(\ (W_{\bar u}(a),W_{\bar v}(a));\ W\in\mathcal{W},\ 1\,\alpha\,a,\ \bar u\,\beta\,\bar v\ )$ and $A=N_\alpha$.

First we show $[\alpha,\beta]\supseteq\delta$. We only need to check that $W_{\bar u}(a)\,[\alpha,\beta]\,W_{\bar v}(a)$ whenever W is inner, $a\in A$ and $\bar u\,\beta\,\bar v$. Note that $W_{\bar u}(1)=1=W_{\bar v}(1)$ because W is an inner word. In particular $W_{\bar u}(1)\,[\alpha,\beta]\,W_{\bar v}(1)$ and the term condition $C(\alpha,\beta;[\alpha,\beta])$ for $t(\bar x,y)=W_{\bar x}(y)$ gives $W_{\bar u}(a)\,[\alpha,\beta]\,W_{\bar v}(a)$.

Now we show $[\alpha,\beta]\subseteq\delta$. Recall that $[\alpha,\beta]$ is the smallest congruence with $C(\alpha,\beta;[\alpha,\beta])$. In order to show $[\alpha,\beta]\subseteq\delta$, it is sufficient to check that $C(\alpha,\beta;\delta)$. We will write $x\equiv y$ if $x\,\delta\,y$.

According to Lemma 4.1, we need to check the term condition $\mathrm{TC}(t,\alpha,\beta,\delta)$ for every term t that is slim in the first coordinate. Consider such a term t, $a\,\alpha\,b$, $\bar{u}\,\beta\,\bar{v}$ and assume $t(a,u_1,\dots,u_n)\equiv t(a,v_1,\dots,v_n)$. We will show that $t(b,u_1,\dots,u_n)\equiv t(b,v_1,\dots,v_n)$.

Let d be the depth of the (unique) occurrence of x_1 in t. We will construct a sequence of $(n+2)$-ary terms $s_0,\dots,s_d$ and elements $a_0,\dots,a_d\in A$ and $a'_0,\dots,a'_d\in A$ satisfying the following conditions for every $i=0,\dots,d$:

(1) s_i has a single occurrence of x_1 at depth $d+1-i$, and it appears in a subterm of the form $x_1\cdot s$ for some term s,
(2) $s_i(1,x_1,\dots,x_{n+1})=t(x_1,\dots,x_{n+1})$,
(3) $s_i(a_i,b,u_1,\dots,u_n)\equiv s_i(a'_i,b,v_1,\dots,v_n)$,
(4) $a_i\equiv a'_i$ and $a_i,a'_i\in A$.

Assuming existence of the sequences, it is easy to finish the proof of the theorem: it follows from (1) and (2) that $s_d(x_1,\dots,x_{n+2})=x_1\cdot t(x_2,\dots,x_{n+2})$, and using (3),

$$a_d\cdot t(b,u_1,\dots,u_n)=s_d(a_d,b,u_1,\dots,u_n)\equiv s_d(a'_d,b,v_1,\dots,v_n)=a'_d\cdot t(b,v_1,\dots,v_n).$$

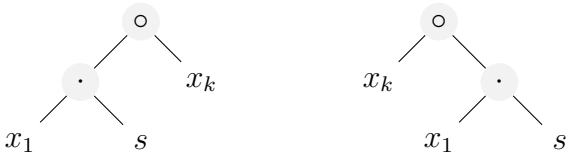
According to (4), $a_d\equiv a'_d$, so we can cancel in Q/δ and get $t(b,u_1,\dots,u_n)\equiv t(b,v_1,\dots,v_n)$.

Now we will construct the sequences. In the initial step, take

$$s_0(x_1,\dots,x_{n+2})=t(x_1\cdot x_2,x_3,\dots,x_{n+2}),$$

and let $a_0=a'_0=a/b$. It is readily seen that the conditions (1), (2), (4) are satisfied, and (3) follows from the assumption that $t(a,u_1,\dots,u_n)\equiv t(a,v_1,\dots,v_n)$.

Induction step: given s_i,a_i,a'_i satisfying the conditions, we will construct s_{i+1},a_{i+1},a'_{i+1}. Since t is slim, one of the following configurations takes place near the occurrence of x_1 in s_i, for some variable x_k, some term $s(x_2,\dots,x_{n+2})$ and some operation $\circ\in\{\cdot,\backslash,/\}$:



Let $W_{x,y}=A^{\circ}_{x,y}$ in the former case and $W_{x,y}=B^{\circ}_{x,y}$ in the latter case. (Recall that $(z\cdot x)\circ y=A^{\circ}_{x,y}(z)\cdot(x\circ y)$ and $y\circ(z\cdot x)=B^{\circ}_{x,y}(z)\cdot(y\circ x)$.) Define

$$a_{i+1}=W_{s(b,u_1,\dots,u_n),u_{k-2}}(a_i),\qquad a'_{i+1}=W_{s(b,v_1,\dots,v_n),v_{k-2}}(a'_i),$$

and let s_{i+1} result from s_i by replacing the subterm $(x_1\cdot s)\circ x_k$ by $x_1\cdot(s\circ x_k)$, or $x_k\circ(x_1\cdot s)$ by $x_1\cdot(x_k\circ s)$, respectively. Graphically, the configuration near the occurrence of x_1 in s_{i+1} becomes one of the following:

It is readily seen that the conditions (1), (2) hold for s_{i+1} too.

Let us verify condition (3). Suppose that we are in the former case. Then near x_1 the evaluated term $s_i(a_i, b, u_1, \dots, u_n)$ gives $(a_i \cdot s(b, u_1, \dots, u_n)) \circ u_{k-2}$, which is equal to $A^{\circ}_{s(b,u_1,\dots,u_n),u_{k-2}}(a_i) \cdot (s(b, u_1, \dots, u_n) \circ u_{k-2}) = a_{i+1} \cdot (s(b, u_1, \dots, u_n) \circ u_{k-2})$, which is how the evaluated term $s_{i+1}(a_{i+1}, b, u_1, \dots, u_n)$ looks near x_1. In other words, $s_i(a_i, b, u_1, \dots, u_n) = s_{i+1}(a_{i+1}, b, u_1, \dots, u_n)$. Similarly, $s_i(a'_i, b, v_1, \dots, v_n) = s_{i+1}(a'_{i+1}, b, v_1, \dots, v_n)$. Then we can use (3) for s_i to conclude that

$$s_{i+1}(a_{i+1}, b, u_1, \dots, u_n) = s_i(a_i, b, u_1, \dots, u_n) \equiv s_i(a'_i, b, v_1, \dots, v_n) = s_{i+1}(a'_{i+1}, b, v_1, \dots, v_n),$$

so that (3) holds for s_{i+1}. Similarly in the latter case.

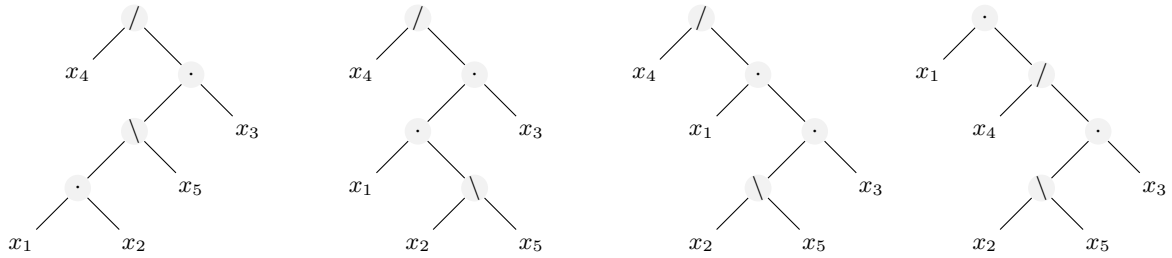
To check condition (4), observe that $a_{i+1}, a'_{i+1} \in A$ because the normal subloop A is closed under inner mappings by Proposition 3.7, and that

$$a_{i+1} = W_{s(b,u_1,\dots,u_n),u_{k-2}}(a_i) \equiv W_{s(b,u_1,\dots,u_n),u_{k-2}}(a'_i) \equiv W_{s(b,v_1,\dots,v_n),v_{k-2}}(a'_i) = a'_{i+1},$$

where the former equivalence follows from the fact that $a_i \equiv a'_i$ and $\equiv$ is a congruence, and the latter one follows from Lemma 4.2. □

The following example illustrates the inductive algorithm used in the proof of Theorem 2.1.

Example 4.3. Let $t(x_1, x_2, x_3, x_4) = x_3/((x_1\backslash x_4) \cdot x_2)$. The sequence s_0, s_1, s_2, s_3 is depicted below. Notice the occurrence of x_1 "climbing the tree" to the top level, while the structure of the rest of the tree remains intact. Also notice that $s_3(x_1, \dots, x_5) = x_1 \cdot t(x_2, \dots, x_5)$.



4.3. **The fundamental theorem in loops with a finiteness condition.** Assume that Q has a bound on the order of all left and right translations, i.e., there is an integer $n > 0$ such that $L_x^n = R_x^n = 1$ for every $x \in Q$. (This is certainly true in every finite loop.) Then the theory developed so far simplifies considerably, because we can avoid the division operations: we have

$$x\backslash y = L_x^{-1}(y) = L_x^{n-1}(y) = \underbrace{x(\dots(x(x}_{n-1}\, y))\dots),$$

and dually for the right division. Hence, for every loop term t, there is a *multiplicative* term s (i.e., a term in the language of multiplication) such that $t = s$ is a valid identity in every loop where $L_x^n = R_x^n = 1$ for every x. So, in the term condition $\mathrm{TC}(t, \alpha, \beta, \delta)$ verified in the proof of Theorem 2.1, we only need to consider *multiplicative slim terms*. Hence, later in the proof, we only need to use the words $A^{\cdot}_{x,y}$ and $B^{\cdot}_{x,y}$, which always induce mappings from $\mathrm{Inn}(Q)$ (while the other options may induce mappings from $\mathrm{TInn}(Q)$). It means that we only need a weaker version of Lemma 4.2, for inner words from $\mathrm{Inn}(Q)$, and thus we can choose a weaker $\mathcal{W}$, a set of words that generates inner mapping groups (not necessarily total inner mapping groups) in $\boldsymbol{V}$. We have proved:

Theorem 4.4. *Let $\boldsymbol{V}$ be a variety of loops and $\mathcal{W}$ a set of words that generates inner mapping groups in $\boldsymbol{V}$. If for $Q \in \boldsymbol{V}$ there is $n > 0$ such that $L_x^n = R_x^n = 1$ for every $x \in Q$, then*

$$[\alpha, \beta] = \mathrm{Cg}(\ (W_{\bar{u}}(a), W_{\bar{v}}(a));\ W \in \mathcal{W},\ 1\,\alpha\,a,\ \bar{u}\,\beta\,\bar{v}\ )$$

for any congruences α, β of Q.

5. Pruning the generating sets

Assume the notation of Theorem 2.1, that is, let $\boldsymbol{V}$ be a variety of loops and $\mathcal{W}$ a set of words that generates inner mapping groups in $\boldsymbol{V}$. For $Q \in \boldsymbol{V}$ and congruences α, β of Q call $\mathrm{Cg}(\ (W_{\bar{u}}(a), W_{\bar{v}}(a));\ W \in \mathcal{W},\ 1\,\alpha\,a,\ \bar{u}\,\beta\,\bar{v}\ )$ the *congruence induced by* $\mathcal{W}$. In some cases, a word can be removed from $\mathcal{W}$ with no effect on the congruences induced by $\mathcal{W}$. Formally, we say that a word W is *removable* from a set $\mathcal{W}$, if for every loop $Q \in \boldsymbol{V}$ and every congruences α, β of Q the congruence induced by $\mathcal{W}$ and the congruence induced by $\mathcal{W} \setminus \{W\}$ are equal.

Proposition 5.1. *Let $\boldsymbol{V}$ be a variety of loops, $\mathcal{W}$ be a set of inner words, $W \in \mathcal{W}$, and $\equiv$ the congruence induced by $\mathcal{W} \setminus \{W\}$.*

(i) *If W has no parameters, it is removable from $\mathcal{W}$.*
(ii) *The word $W = U_x$ is removable from $\mathcal{W}$, provided that $[a, x, b] \equiv 1$ for every loop $Q \in \boldsymbol{V}$, every congruences α, β of Q, and every $1\,\alpha\,a$, $1\,\beta\,b$, $x \in Q$.*
(iii) *The word $W = T_x$ is removable from $\mathcal{W}$, provided that $[a, b] \equiv 1$, $[a, b, x] \equiv 1$, $[b, a, x] \equiv 1$ and $[x, b, a] \equiv 1$ for every loop $Q \in \boldsymbol{V}$, every congruences α, β of Q, and every $1\,\alpha\,a$, $1\,\beta\,b$, $x \in Q$.*

Proof. (i) The diagonal element $(W(a), W(a))$ belongs to every congruence.

(ii) The assumption $[a, x, b] \equiv 1$ can be written as

$$ax \cdot b \equiv a \cdot xb, \quad \text{i.e.,} \quad R_b R_x(a) \equiv R_{xb}(a). \tag{5.1}$$

Upon replacing x with $a\backslash x$, and dividing both sides by a, we get

$$a\backslash(xb) \equiv (a\backslash x)b, \quad \text{i.e.,} \quad M_{xb}(a) \equiv R_b M_x(a) \tag{5.2}$$

for every $1\,\alpha\,a$, $1\,\beta\,b$, $x \in Q$. Suppose that $1\,\alpha\,a$ and $u\,\beta\,v$, thus $1 = M_v^{-1}R_v(1)\,\alpha\,M_v^{-1}R_v(a)$ and $(v\backslash u)\,\beta\,1$. Then

$$\begin{aligned} U_u U_v^{-1}(a) &= R_u^{-1} M_u M_v^{-1} R_v(a) = R_u^{-1} M_{v(v\backslash u)} M_v^{-1} R_v(a) \\ &\equiv R_u^{-1} R_{v\backslash u} M_v M_v^{-1} R_v(a) = R_u^{-1} R_{v\backslash u} R_v(a) && \text{by (5.2) with } M_v^{-1}R_v(a)\,\alpha\,1 \\ &\equiv R_u^{-1} R_{v(v\backslash u)}(a) = R_u^{-1} R_u(a) = a && \text{by (5.1).} \end{aligned}$$

Upon replacing a with $U_v(a)$, we obtain $U_u(a) \equiv U_v(a)$.

(iii) The assumptions can be written as

$$\begin{aligned} ab \equiv ba, &\quad \text{i.e.,} \quad L_b(a) \equiv R_b(a), \\ a \cdot bx \equiv ab \cdot x, &\quad \text{i.e.,} \quad R_{bx}(a) \equiv R_x R_b(a), \\ b \cdot ax \equiv ba \cdot x, &\quad \text{i.e.,} \quad L_b R_x(a) \equiv R_x L_b(a), \\ x \cdot ba \equiv xb \cdot a, &\quad \text{i.e.,} \quad L_x L_b(a) \equiv L_{xb}(a), \end{aligned}$$

for every $1 \,\alpha\, a$, $1 \,\beta\, b$, $x \in Q$. Suppose that $1 \,\alpha\, a$ and $u \,\beta\, v$, thus $1 = L_v^{-1}R_v(1) \,\alpha\, L_v^{-1}R_v(a)$ and $(u/v) \,\beta\, 1$. Then

$$\begin{aligned}
T_uT_v^{-1}(a) &= R_u^{-1}L_uL_v^{-1}R_v(a) = R_u^{-1}L_{(u/v)v}L_v^{-1}R_v(a) \\
&\equiv R_u^{-1}L_{u/v}L_vL_v^{-1}R_v(a) = R_u^{-1}L_{u/v}R_v(a) && \text{by } [u/v, v, L_v^{-1}R_v(a)] \equiv 1 \\
&\equiv R_u^{-1}R_vL_{u/v}(a) && \text{by } [u/v, a, v] \equiv 1 \\
&\equiv R_u^{-1}R_vR_{u/v}(a) && \text{by } [a, u/v] \equiv 1 \\
&\equiv R_u^{-1}R_{(u/v)v}(a) = R_u^{-1}R_u(a) = a && \text{by } [a, u/v, v] \equiv 1.
\end{aligned}$$

Upon replacing a with $T_v(a)$, we obtain $T_u(a) \equiv T_v(a)$. □

Item (i) of Proposition 5.1 applies, for example, to the inverse mapping J in inverse property loops, or more generally, to the mapping M_1 in every loop. The assumptions of (ii) are satisfied, for example, if $R_{x,y} \in \mathcal{W}$; then $R_{b,x}(a) \equiv R_{1,x}(a) = 1$ whenever $1 \,\alpha\, a$, $1 \,\beta\, b$ and $x \in Q$, and thus $[a, x, b] \equiv 1$. Using (iii) is less straightforward; we will do so in Corollary 7.5.

The full power of Theorems 2.1 and 4.4 is realized only in combination with the results of Section 3, as summarized in Example 3.12.

Corollary 5.2. *Let Q be a loop and α, β congruences of Q. Let $\mathcal{W}$ be defined as follows:*

(i) *If Q is a loop, let $\mathcal{W} = \{L_{x,y}, R_{x,y}, T_x, M_{x,y}\}$ or $\mathcal{W} = \{A^{\cdot}_{x,y}, B^{\cdot}_{x,y}, A^{\backslash}_{x,y}\}$.*

(ii) *If Q is an inverse property loop, let $\mathcal{W} = \{L_{x,y}, T_x\}$ or $\mathcal{W} = \{M_{x,y}\}$.*

(iii) *If Q is a group, let $\mathcal{W} = \{T_x\}$.*

(iv) *If Q is a commutative loop, let $\mathcal{W} = \{L_{x,y}, M_{x,y}\}$ or $\mathcal{W} = \{A^{\cdot}_{x,y}, A^{\backslash}_{x,y}\}$.*

Then

$$[\alpha, \beta] = \mathrm{Cg}(\ (W_{\bar{u}}(a), W_{\bar{v}}(a));\ W \in \mathcal{W},\ 1 \,\alpha\, a,\ \bar{u} \,\beta\, \bar{v}\ )$$

for any congruences α, β of Q.

Proof. Apply Theorem 2.1 to the generating sets from Example 3.12, and use the pruning principles of Proposition 5.1. □

It follows from Theorem 4.4 that for loops with a finiteness condition we can remove $M_{x,y}$ and $A^{\backslash}_{x,y}$ from the sets $\mathcal{W}$ in Corollary 5.2 (i,iv).

Problem 5.3. *Find additional small generating sets for Corollary 5.2.*

Proposition 5.1 is an ad hoc argument designed specifically to prune the standard generating sets. We therefore ask:

Problem 5.4. *Describe systematically when a word is removable from a set of inner words.*

Given a set of words $\mathcal{W}$, we now show a simple trick that decreases the size of the generating set of the commutator, useful for computational purposes. Suppose that some two-parameter inner word $W_{x,y}$ is used in $\mathcal{W}$. We claim that

$$\begin{aligned}
&\mathrm{Cg}(\ (W_{u_1,u_2}(a), W_{v_1,v_2}(a));\ 1 \,\alpha\, a,\ \bar{u} \,\beta\, \bar{v}\ ) \\
&\qquad = \mathrm{Cg}(\ (W_{u,c}(a), W_{v,c}(a)),\ (W_{c,u}(a), W_{c,v}(a));\ 1 \,\alpha\, a,\ u \,\beta\, v,\ c \in Q\ ).
\end{aligned}$$

Indeed, choosing $u_2 = v_2 = c$ (so surely $u_2 \,\beta\, v_2$) or $u_1 = v_1 = c$ shows that the second congruence is a subset of the first. Conversely, if the generators of the second congruence are

available then $W_{u_1,u_2}(a)$ is congruent to $W_{u_1,v_2}(a)$, which is in turn congruent to $W_{v_1,v_2}(a)$. Of course, a similar observation holds for inner terms with an arbitrary number of parameters. Note that the second generating set is generally smaller than the first, but it is more cumbersome to write down.

6. Elementwise commutators and associators

6.1. **Commutators and associators as inner mappings.** We have seen that the words $A^\circ_{x,y}$, $B^\circ_{x,y}$ form a set that generates total inner mapping groups in all loops, and thus can be used to generate congruence commutators. Can these words be replaced by terms that resemble elementwise commutators and associators?

The standard commutator $[x, y]$ defined by $xy = (yx)[x, y]$ will not work, since the terms $t_x(y) = [x, y] = s_y(x)$ do not preserve normality in the variety of loops, in the sense that there exists a loop Q with normal subloop N and $x, y \in Q$, $a \in N$ such that neither of $[x, a]$, $[a, y]$ is in N. The standard associator $[x, y, z]$ is similarly flawed.

With Leong's associator $xy \cdot z = a^L(x, y, z)x \cdot yz$, we can write $A^L_{y,z}(x) = a^L(x, y, z)x$, so that $xy \cdot z = A^L_{y,z}(x) \cdot yz$, and we notice that $A^L_{y,z} = R^{-1}_{yz} R_z R_y$ is an inner mapping. (This is the most important feature of the associator $a^L(x, y, z)$, which seems to have gone unnoticed in [24].) Consequently, $a^L(N, Q, Q) \subseteq N$ for every $N \trianglelefteq Q$.

We will now define commutators and associators systematically. Let $\boldsymbol{V}$ be the variety of all loops. A loop term $a(x, y, z)$ is an *associator* if we have $*$, $\circ$, $\circledast$, $\circledcirc \in \{\cdot, \backslash, /\}$ such that the following hold:

(a) $(x * y) \circ z = (a(x, y, z)x) \circledast (y \circledcirc z)$ in $\boldsymbol{V}$ or $z * (y \circ x) = (z \circledast y) \circledcirc (xa(x, y, z))$ in $\boldsymbol{V}$,
(b) $a(1, y, z) = 1$ in $\boldsymbol{V}$ (thus the associators give rise to inner mappings),
(c) $a(x, y, z) = 1$ on all abelian groups in $\boldsymbol{V}$.

A loop term $c(x, y)$ is a *commutator* if we have $*$, $\circledast \in \{\cdot, \backslash, /\}$ such that the following hold:

(a) $x * y = y \circledast xc(x, y)$ in $\boldsymbol{V}$ or $y * x = c(x, y)x \circledast y$ in $\boldsymbol{V}$,
(b) $c(1, y) = 1$ in $\boldsymbol{V}$ (thus the commutators give rise to inner mappings),
(c) $c(x, y) = 1$ on all abelian groups in $\boldsymbol{V}$.

For instance, given the loop operations $* = \cdot$, $\circ = /$, can we find loop operations $\circledast$, $\circledcirc$ such that $a^{\cdot/}(x, y, z)$ defined by $(x \cdot y)/z = (a^{\cdot/}(x, y, z)x) \circledast (y \circledcirc z)$ fulfills (b) and (c)? We can equivalently study $A^{\cdot/}_{y,z}(x)$ defined by $A^{\cdot/}_{y,z}(x) = a^{\cdot/}(x, y, z)x$. To make the identity $(x \cdot y)/z = x \circledast (y \circledcirc z)$ valid in abelian groups, we must choose $(x \cdot y)/z = x \cdot (y/z)$ or $(x \cdot y)/z = x/(y \backslash z)$. But only the first choice gives a valid loop identity when $x = 1$. Equivalently, only the first choice gives rise to an inner mapping $A^{\cdot/}_{y,z}$, namely to $A^{\cdot/}_{y,z} = R^{-1}_{y/z} R^{-1}_z R_y$. Note that the answer is therefore unique here.

The following lemma can be proved by similar arguments. We omit the straightforward proof.

Lemma 6.1.

(i) *Let $*$, $\circ$ be loop operations such that $* \neq /$. Then*
- *there are uniquely determined loop operations $\circledast$, $\circledcirc$ such that $(x * y) \circ z = x \circledast (y \circledcirc z)$ is an identity in all abelian groups, and such that $(1 * y) \circ z = 1 \circledast (y \circledcirc z)$ is an identity in all loops;*

- *there is a uniquely determined loop operation $\circledast$ such that $x * y = y \circledast x$ is an identity in all abelian groups, and such that $1 * y = y \circledast 1$ is an identity in all loops.*

(ii) *Let $*$, $\circ$ be loop operations such that $\circ \neq \backslash$. Then*

- *there are uniquely determined loop operations $\circledast$, $\circledcirc$ such that $z * (y \circ x) = z \circledast (y \circledcirc x)$ is an identity in all abelian groups, and such that $z * (y \circ 1) = z \circledast (y \circledcirc 1)$ is an identity in all loops;*
- *there is a uniquely determined loop operation $\circledast$ such that $y \circ x = x \circledast y$ is an identity in all abelian groups, and such that $y \circ 1 = 1 \circledast y$ is an identity in all loops.*

The cases excluded in Lemma 6.1 do not have a solution. For instance, with $* = /$ and $\circ = \cdot$, the only choices of $\circledast$, $\circledcirc \in \{\cdot, /, \backslash\}$ that make $(x * y) \circ z = x \circledast (y \circledcirc z)$ valid in all abelian groups are $(x/y) \cdot z = x \cdot (y\backslash z)$ and $(x/y) \cdot z = x/(y/z)$, and with $x = 1$ these identities become $(1/y) \cdot z = y\backslash z$ and $(1/y) \cdot z = 1/(y/z)$. But the first identity is not valid in all loops (take $z = 1$ to get $1/y = y\backslash 1$), and neither is the second identity (take $y = 1$ to get $z = 1/(1/z)$, i.e., $1/z = z\backslash 1$).

We therefore obtain 12 associators and 4 commutators, summarized in Table 1. The associators and commutators are presented in the form of inner mappings and also as actual elementwise associators and commutators. The a-associators of Table 1 are dual to the b-associators, and the c-commutators are dual to the d-commutators, in the order listed in the table. For instance, $a^{\cdot/}(x, y, z)$ is dual to $b^{\backslash\cdot}(x, y, z)$.

It is interesting to point out that the multiplicative associators and commutators correspond to the standard generating set for the inner mapping groups:

$$A^{\cdot\cdot}_{y,z} = R_{z,y}, \quad B^{\cdot\cdot}_{y,z} = L_{z,y}, \quad C^{\cdot}_{y} = T^{-1}_{y}, \quad D^{\cdot}_{y} = T_y.$$

The following discussion will be important with respect to the choice of associators and commutors that generate the derived subloops and the associator subloops.

Lemma 6.2. *Let Q be a loop and $N \trianglelefteq Q$.*

(i) *Let a denote one of the associators $a^{\cdot\cdot}$, $a^{\cdot/}$, $a^{\backslash\cdot}$, $a^{\backslash/}$, $b^{\cdot\cdot}$, $b^{\backslash\cdot}$, $b^{\cdot/}$, $b^{\backslash/}$. Then Q/N is a group if and only if $\{a(x, y, z);\ x, y, z \in Q\} \subseteq N$.*

(ii) *Let a denote one of the associators $a^{\cdot\backslash}$, $a^{\backslash\backslash}$, $b^{/\cdot}$, $b^{//}$. Then Q/N is an abelian group if and only if $\{a(x, y, z);\ x, y, z \in Q\} \subseteq N$.*

Proof. We will give the proof for two cases and leave the remaining ten to the reader.

Let $a = a^{\cdot\cdot}$. Suppose that $a(x, y, z) \in N$ for every x, y, $z \in N$. In Q/N, $a(x, y, z) = 1$, hence $(xy)z = (a(x, y, z)x)(yz) = x(yz)$. Conversely, if Q/N is a group then, in Q/N, $x(yz) = (xy)z = (a(x, y, z)x)(yz)$, and $a(x, y, z) = 1$ (or $a(x, y, z) \in N$) follows by cancelation in Q/N.

Let $a = a^{\cdot\backslash}$. Suppose that $a(x, y, z) \in N$ for every x, y, $z \in N$. In Q/N, $a(x, y, z) = 1$, hence $(xy)\backslash z = (a(x, y, z)x)\backslash(y\backslash z) = x\backslash(y\backslash z)$, so $y(x((xy)\backslash z)) = z$. Substituting $z = xy$, we obtain commutativity. Substituting $z = xy \cdot u$ and using commutativity, we obtain associativity. Conversely, if Q/N is an abelian group then, in Q/N, $x^{-1}(y^{-1}z) = (xy)^{-1}z = (xy)\backslash z = (a(x, y, z)x)\backslash(y\backslash z) = (a(x, y, z)x)^{-1}(y^{-1}z)$, and $a(x, y, z) = 1$ (or $a(x, y, z) \in N$) follows by cancelation in Q/N. $\square$

defining identity	as an inner mapping	as an associator/commutator
$(x\cdot y)\cdot z = A^{\cdot\cdot}_{y,z}(x)\cdot(y\cdot z)$	$A^{\cdot\cdot}_{y,z} = R^{-1}_{yz}R_zR_y$	$a^{\cdot\cdot}(x,y,z) = A^{\cdot\cdot}_{y,z}(x)/x$
$(x\cdot y)\backslash z = A^{\cdot\backslash}_{y,z}(x)\backslash(y\backslash z)$	$A^{\cdot\backslash}_{y,z} = M^{-1}_{y\backslash z}M_zR_y$	$a^{\cdot\backslash}(x,y,z) = A^{\cdot\backslash}_{y,z}(x)/x$
$(x\cdot y)/z = A^{\cdot/}_{y,z}(x)\cdot(y/z)$	$A^{\cdot/}_{y,z} = R^{-1}_{y/z}R^{-1}_zR_y$	$a^{\cdot/}(x,y,z) = A^{\cdot/}_{y,z}(x)/x$
$(x\backslash y)\cdot z = A^{\backslash\cdot}_{y,z}(x)\backslash(y\cdot z)$	$A^{\backslash\cdot}_{y,z} = M^{-1}_{yz}R_zM_y$	$a^{\backslash\cdot}(x,y,z) = A^{\backslash\cdot}_{y,z}(x)/x$
$(x\backslash y)\backslash z = A^{\backslash\backslash}_{y,z}(x)\cdot(y\backslash z)$	$A^{\backslash\backslash}_{y,z} = R^{-1}_{y\backslash z}M_zM_y$	$a^{\backslash\backslash}(x,y,z) = A^{\backslash\backslash}_{y,z}(x)/x$
$(x\backslash y)/z = A^{\backslash/}_{y,z}(x)\backslash(y/z)$	$A^{\backslash/}_{y,z} = M^{-1}_{y/z}R^{-1}_zM_y$	$a^{\backslash/}(x,y,z) = A^{\backslash/}_{y,z}(x)/x$
$z\cdot(y\cdot x) = (z\cdot y)\cdot B^{\cdot\cdot}_{y,z}(x)$	$B^{\cdot\cdot}_{y,z} = L^{-1}_{zy}L_zL_y$	$b^{\cdot\cdot}(x,y,z) = x\backslash B^{\cdot\cdot}_{y,z}(x)$
$z/(y\cdot x) = (z/y)/B^{/\cdot}_{y,z}(x)$	$B^{/\cdot}_{y,z} = M^{-1}_{z/y}M^{-1}_zL_y$	$b^{/\cdot}(x,y,z) = x\backslash B^{/\cdot}_{y,z}(x)$
$z\backslash(y\cdot x) = (z\backslash y)\cdot B^{\backslash\cdot}_{y,z}(x)$	$B^{\backslash\cdot}_{y,z} = L^{-1}_{z\backslash y}L^{-1}_zL_y$	$b^{\backslash\cdot}(x,y,z) = x\backslash B^{\backslash\cdot}_{y,z}(x)$
$z\cdot(y/x) = (z\cdot y)/B^{\cdot/}_{y,z}(x)$	$B^{\cdot/}_{y,z} = M_{z\cdot y}L_zM^{-1}_y$	$b^{\cdot/}(x,y,z) = x\backslash B^{\cdot/}_{y,z}(x)$
$z/(y/x) = (z/y)\cdot B^{//}_{y,z}(x)$	$B^{//}_{y,z} = L^{-1}_{z/y}M^{-1}_zM^{-1}_y$	$b^{//}(x,y,z) = x\backslash B^{//}_{y,z}(x)$
$z\backslash(y/x) = (z\backslash y)/B^{\backslash/}_{y,z}(x)$	$B^{\backslash/}_{y,z} = M_{z\backslash y}L^{-1}_zM^{-1}_y$	$b^{\backslash/}(x,y,z) = x\backslash B^{\backslash/}_{y,z}(x)$
$x\cdot y = y\cdot C^{\cdot}_y(x)$	$C^{\cdot}_y = L^{-1}_yR_y$	$c^{\cdot}(x,y) = x\backslash C^{\cdot}_y(x)$
$x\backslash y = y/C^{\backslash}_y(x)$	$C^{\backslash}_y = M_yM_y$	$c^{\backslash}(x,y) = x\backslash C^{\backslash}_y(x)$
$y\cdot x = D^{\cdot}_y(x)\cdot y$	$D^{\cdot}_y = R^{-1}_yL_y$	$d^{\cdot}(x,y) = D^{\cdot}_y(x)/x$
$y/x = d^{/}_y(x)\backslash y$	$D^{/}_y = M^{-1}_yM^{-1}_y$	$d^{/}(x,y) = D^{/}_y(x)/x$

TABLE 1. Commutators and associators that yield inner mappings in loops.

6.2. **The fundamental theorem in terms of commutators and associators.** The machinery of Theorem 2.1 can now be applied to various subsets of the commutators and associators in Table 1.

Whether we work with the inner mappings or with the elementwise commutators and associators is irrelevant. Indeed, for trivial reasons, the two elements $A^{\cdot\cdot}_{y_1,z_1}(x)$, $A^{\cdot\cdot}_{y_2,z_2}(x)$ are congruent if and only if the two elements $a^{\cdot\cdot}(x,y_1,z_1) = A^{\cdot\cdot}_{y_1,z_1}(x)/x$, $a^{\cdot\cdot}(x,y_2,z_2) = A^{\cdot\cdot}_{y_2,z_2}(x)/x$ are congruent; and similarly for all other commutators/associators.[2]

Using the operations from Table 1, we can reformulate Corollary 5.2 as follows:

Corollary 6.3. *Let Q be a loop and α, β congruences of Q. Let $\mathcal{W}$ be defined as follows:*

(i) *If Q is a loop, let $\mathcal{W} = \{A^{\cdot\cdot}_{x,y},\ B^{\cdot\cdot}_{x,y},\ A^{\cdot\backslash}_{x,y},\ C^{\cdot}_x\}$.*
(ii) *If Q is an inverse property loop, let $\mathcal{W} = \{A^{\cdot\cdot}_{x,y},\ C^{\cdot}_x\}$.*
(iii) *If Q is a group, let $\mathcal{W} = \{C^{\cdot}_x\}$.*
(iv) *If Q is a commutative loop, let $\mathcal{W} = \{A^{\cdot\cdot}_{x,y},\ A^{\cdot\backslash}_{x,y}\}$.*

Then

$$[\alpha,\beta] = \mathrm{Cg}(\ (W_{\bar u}(a), W_{\bar v}(a));\ W\in\mathcal{W},\ 1\,\alpha\,a,\ \bar u\,\beta\,\bar v\ ).$$

Proof. Note that $R_{x,y} = A^{\cdot\cdot}_{y,x}$, $L_{x,y} = B^{\cdot\cdot}_{y,x}$, $T_x = (C^{\cdot}_x)^{-1}$ and $M_{x,y} = A^{\cdot\backslash}_{y,x}U_x$, so $\mathcal{W}\cup\{U_x\}$ does the job, by Corollary 5.2. We can remove U_x by Proposition 5.1. □

[2]However, inner mappings can be composed to form a group while commutators and associators cannot be composed. This is why Theorem 2.1 is stated in terms of inner mappings.

It follows from Theorem 4.4 that for loops with a finiteness condition we can remove $A^{\backslash}_{x,y}$ from the sets $\mathcal{W}$ of Corollary 6.3.

Problem 6.4. *Find all minimal subsets of the* 12 *associators and* 4 *commutators that, together with* M_1*, generate total inner mapping groups in all loops.*

7. The commutator of normal subloops

The correspondence $\alpha \mapsto N_\alpha$, $N \mapsto \gamma_N$ between loop congruences and normal subloops allows us to restate Theorem 2.1 and all its corollaries in terms of normal subloops, rather than in terms of congruences.

Lemma 7.1. *Let* Q *be a loop.*

(i) *If* $X \subseteq Q \times Q$ *and* $\alpha = \mathrm{Cg}(X)$*, then* $N_\alpha = \mathrm{Ng}(\ x/y;\ (x,y) \in X\ )$.
(ii) *If* $X \subseteq Q$ *and* $N = \mathrm{Ng}(X)$*, then* $\gamma_N = \mathrm{Cg}(\ (x,1);\ x \in X\ )$.

Proof. (i) Let $N = \mathrm{Ng}(\ x/y;\ (x,y) \in X\ )$. Since $(x,y) \in X \subseteq \alpha$, we immediately get $N \subseteq N_\alpha$. On the other hand, since $(x/y, 1) \in \gamma_N$ for every $(x,y) \in X$, we also get $(x,y) \in \gamma_N$ for every $(x,y) \in X$, hence $\alpha \leq \gamma_N$. Part (ii) is similar. □

Applying this observation to Theorem 2.1, we immediately get a generating set for the commutator of two normal subloops, as described in Theorem 2.2, stating that

$$[A,B]_Q = \mathrm{Ng}(\ W_{\bar{u}}(a)/W_{\bar{v}}(a);\ W \in \mathcal{W},\ a \in A,\ \bar{u}/\bar{v} \in B\ )$$

for any normal subloops A, B of any loop Q in a variety $\boldsymbol{V}$, where $\mathcal{W}$ is a set of words that generates total inner mapping groups in $\boldsymbol{V}$. Of course, in loops with a finiteness condition we only need $\mathcal{W}$ that generates inner mapping groups. Using Corollary 6.3, we obtain generating sets consisting of quotients of certain associators and commutators. Let us discuss the case of groups first.

Let Q be a group and A, $B \trianglelefteq Q$. Note that $C^{\cdot}_y(x) = y^{-1}xy$ and $c^{\cdot}(x,y) = x^{-1}y^{-1}xy = [x,y]$. Corollary 6.3 therefore yields

$$[A,B]_Q = \mathrm{Ng}(\ [a,u]/[a,v];\ a \in A,\ u/v \in B\ ).$$

From this it is not difficult to recover the standard group-theoretical result

$$[A,B]_Q = \langle [a,b];\ a \in A,\ b \in B \rangle.$$

Namely, let $N_1 = \mathrm{Ng}(\ [a,u]/[a,v];\ a \in A,\ u/v \in B\ )$ and $N_2 = \langle [a,b];\ a \in A,\ b \in B \rangle$. First notice that N_2 is a normal subgroup, since $\mathrm{Inn}(Q) = \langle T_x;\ x \in Q \rangle \leq \mathrm{Aut}(Q)$ and thus $T_x([a,b]) = [T_x(a), T_x(b)]$ and $T_x(a) \in A$, $T_x(b) \in B$ for every $a \in A$, $b \in B$. Taking $u = b \in B$ and $v = 1$, we obtain $[a,b] = [a,u]/[a,v]$ with $u/v \in B$, hence $N_2 \subseteq N_1$. Conversely, calculating in Q/N_2, we get $[a,u]/[a,v] = a^{-1}u^{-1}auv^{-1}a^{-1}va = 1$, since we can commute $uv^{-1} \in B$ with $a \in A$ and cancel; this shows $N_1 \subseteq N_2$.

The discussion of the group case raises two natural questions for general loops. First, is the subloop generated by the quotients always normal? Second, can we dispose of the quotients in the generating set of $[A,B]_Q$?

Let us first answer the first question. In general, normality fails, as the following example and Corollary 5.2 illustrate:

Example 7.2. Let Q be the commutative loop

	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	1	0	6	7	4	5
3	3	2	0	1	7	6	5	4
4	4	5	6	7	3	0	1	2
5	5	4	7	6	0	3	2	1
6	6	7	4	5	1	2	3	0
7	7	6	5	4	2	1	0	3

Then $A = \{0, 1, 2, 3\}$ is a normal subloop of Q. But $\langle L_{u_1,u_2}(a)/L_{v_1,v_2}(a);\ a \in A,\ \bar{u}/\bar{v} \in A\rangle = \{0, 1\}$ is not a normal subloop of Q.

On the other hand, in many loops, the answer is positive. The gist of the proof for groups was the fact that inner mappings of groups are automorphisms. Recall that a loop Q is said to be automorphic if $\mathrm{Inn}(Q) \leq \mathrm{Aut}(Q)$.

Proposition 7.3. *Let $\boldsymbol{V}$ be a variety of automorphic loops and $\mathcal{W}$ a set of words that generates total inner mapping groups in $\boldsymbol{V}$. Then*

$$[A, B]_Q = \langle W_{\bar{u}}(a)/W_{\bar{v}}(a);\ W \in \mathcal{W},\ a \in A,\ \bar{u}/\bar{v} \in B\rangle$$

for any normal subloops A, B of any $Q \in \boldsymbol{V}$.

Proof. Denote the right hand side subloop by N. In view of Theorem 2.2, we only need to check that N is normal in Q. Since inner mappings are automorphisms, we only need to check that the generators of N are preserved by inner mappings. Let F be any of the words $L_{x,y}, R_{x,y}, T_x$, and let $W \in \mathcal{W}$. Then the composition FW is also an inner word. Hence, by Lemma 4.2, $(F_{\bar{x}}W_{\bar{u}}(a), F_{\bar{x}}W_{\bar{v}}(a)) \in [\gamma_A, \gamma_B]$ for every tuple $\bar{x}$ over Q, $a \in A$ and tuples $\bar{u}$, $\bar{v}$ over Q such that $\bar{u}/\bar{v} \in B$. Thus $F_{\bar{x}}(W_{\bar{u}}(a)/W_{\bar{v}}(a)) = F_{\bar{x}}W_{\bar{u}}(a)/F_{\bar{x}}W_{\bar{v}}(a) \in [A, B]_Q$. □

Problem 7.4. *Characterize loops Q such that (with the notation of Theorem 2.2) the subloop $\langle W_{\bar{u}}(a)/W_{\bar{v}}(a);\ W \in \mathcal{W},\ a \in A,\ \bar{u}/\bar{v} \in B\rangle$ is normal for all subloops A, $B \trianglelefteq Q$.*

The second question, whether quotients can be reduced, is also tricky. Example 9.2 shows that it is not possible to get rid of quotients in the standard generating set, or in the generating set resulting from elementwise associators and commutators. (It might be possible to get rid of all quotients in different generating sets.) On the other hand, Proposition 5.1 says that some quotients can be removed: words without parameters for good, and the words U_x and T_x can be replaced by certain associators and commutators.

Corollary 7.5. *Let Q be a loop and A, B normal subloops of Q.*

(i) *Then*

$$[A, B]_Q = \mathrm{Ng}(\ [a, b], [b, a, x],\ W_{u_1,u_2}(a)/W_{v_1,v_2}(a);\\ W \in \{L, R, M\},\ a \in A,\ b \in B,\ x \in Q,\ \bar{u}/\bar{v} \in B\ ).$$

(ii) *If Q is an inverse property loop, then*

$$[A, B]_Q = \mathrm{Ng}(\ [a, b],\ L_{u_1,u_2}(a)/L_{v_1,v_2}(a);\ a \in A,\ b \in B,\ \bar{u}/\bar{v} \in B\ ).$$

(iii) *If Q is a group, then*

$$[A,B]_Q = \langle [a,b];\ a \in A,\ b \in B \rangle.$$

(iv) *If Q is a commutative loop, then*

$$[A,B]_Q = \mathrm{Ng}(\ W_{u_1,u_2}(a)/W_{v_1,v_2}(a);\ W \in \{L,M\},\ a \in A,\ \bar{u}/\bar{v} \in B\ ).$$

Proof. Corollary 5.2 can be translated via Lemma 7.1 in the same way that we have translated Theorem 2.1 into Theorem 2.2. We will use the translation of Corollary 5.2 without reference. In all cases, let N denote the subloop on the right hand side.

(i) We check that N satisfies the assumptions of conditions (ii), (iii) of Proposition 5.1. We will calculate in Q/N. For every $a \in A$, $b \in B$, $x \in Q$, we have $R_{x,b}(a) = R_{x,1}(a) = a$, so $[a,x,b] = 1$, and $R_{x,b}(a) = R_{x,1}(a) = a$, so $[a,b,x] = 1$, and also $L_{x,b}(a) = L_{x,1}(a) = a$, so $[x,b,a] = 1$.

(ii) Following the proof of case (i), we only need to show that $[b,a,x] \in N$ for every $a \in A$, $b \in B$, $x \in Q$. The following statements, universally quantified with $a \in A$, $b \in B$, $x \in Q$, are equivalent: $b \cdot ax = ba \cdot x$, $ax = b^{-1}(ba \cdot x)$, (use substitution $x \mapsto (ba)^{-1}x$) $a \cdot (ba)^{-1}x = b^{-1}x$, $(ba)^{-1}x = a^{-1} \cdot b^{-1}x$, (use the AAIP) $[a^{-1}, b^{-1}, x] = 1$.

(iii) This follows from case (ii) once we realize that $L_{x,y} = 1$. Proposition 7.3 applies.

(iv) This is merely a restatement of Corollary 5.2(iv). □

In loops with a finiteness condition we can omit the mappings $M_{x,y}$ from the sets $\mathcal{W}$ of Corollary 7.5.

In the proof, we rely on the ad hoc arguments of Proposition 5.1. We therefore ask:

Problem 7.6. *Describe systematically when quotients of inner mappings can be reduced, analogously to Corollary 7.5.*

8. The derived subloop and the associator subloop

Recall that the derived subloop Q' of Q is the smallest normal subloop of Q such that Q/Q' is an abelian group, and the associator subloop $A(Q)$ of a loop Q is the smallest normal subloop of Q such that $Q/A(Q)$ is a group. It is clear that

$$Q' = \mathrm{Ng}(\ [x,y,z],\ [x,y];\ x,y,z \in Q\ ) \quad \text{and} \quad A(Q) = \mathrm{Ng}(\ [x,y,z];\ x,y,z \in Q\ ).$$

Alternatively, we can use the associators and commutators defined in Section 6, along the guidelines given by Lemma 6.2.

As in groups, it was shown by Bruck [5, p. 13] that, in fact, $Q' = \langle [x,y,z],\ [x,y];\ x,y,z \in Q \rangle$. However, the case of $A(Q)$ is more complicated: $\langle [x,y,z];\ x,y,z \in Q \rangle$ needs not be normal in Q; one has to consider its normal closure. We are going to see that the normal closure is not needed upon replacing the traditional associators/commutators with our associators/commutators.

Lemma 8.1. *Let $\boldsymbol{V}$ be a variety of loops, $\mathcal{W}$ a set of words generating inner mapping groups in $\boldsymbol{V}$, and $N \trianglelefteq Q \in \boldsymbol{V}$. The following two conditions are equivalent:*

(i) *Q/N is an abelian group.*

(ii) *$W_{\bar{x}}(z)/z \in N$ for every $W \in \mathcal{W}$, $\bar{x}$ a tuple over Q, and $z \in Q$.*

Proof. Condition (ii) says that, in Q/N, $W_{\bar{x}} = 1$ for every $W \in \mathcal{W}$ and $x_1, \dots, x_n \in Q/N$. Since the mappings $W_{\bar{x}}$ generate $\mathrm{Inn}(Q/N)$, this is equivalent to the fact that $\mathrm{Inn}(Q/N) = 1$. This is equivalent to Q/N being an abelian group, i.e., (i). □

Theorem 8.2. *Let $\boldsymbol{V}$ be a variety of loops, $\mathcal{W}$ a set of words generating inner mapping groups in $\boldsymbol{V}$, and $Q \in \boldsymbol{V}$. Then*

$$Q' = \langle W_{\bar{x}}(z)/z;\ W \in \mathcal{W},\ \bar{x} \text{ a tuple over } Q,\ z \in Q \rangle.$$

Proof. Let H denote the subloop on the right hand side. In view of Lemma 8.1, it suffices to show that $H \trianglelefteq Q$. Using Proposition 3.3(ii), we only need to check that $W_{\bar{x}}(H) = H$ for every $W \in \mathcal{W}$ and every tuple $\bar{x}$ over Q. For $a \in H$, we have $W_{\bar{x}}(a)/a \in H$ by definition, so $W_{\bar{x}}(a) = (W_{\bar{x}}(a)/a) \cdot a \in H$. □

Any choice of associators and commutators such that the set of the corresponding inner words generates inner mapping groups will provide a generating set for Q'. Here is such a choice, corresponding to the standard generating set of $\mathrm{Inn}(Q)$. (The facts of Corollary 8.3 were observed by Covalschi and Sandu in [7].)

Corollary 8.3.

(i) *Let Q be a loop. Then*

$$\begin{aligned} Q' &= \langle L_{x,y}(z)/z,\ R_{x,y}(z)/z,\ T_x(z)/z;\ x, y, z \in Q \rangle \\ &= \langle a^{\cdot\cdot}(x,y,z),\ b^{\cdot\cdot}(x,y,z),\ c^{\cdot}(x,y);\ x, y, z \in Q \rangle. \end{aligned}$$

(ii) *Let Q be an inverse property loop. Then*

$$Q' = \langle L_{x,y}(z)/z,\ T_x(z)/z;\ x, y, z \in Q \rangle = \langle a^{\cdot\cdot}(x,y,z),\ c^{\cdot}(x,y);\ x, y, z \in Q \rangle.$$

(iii) *Let Q be a group. Then*

$$Q' = \langle T_x(y)/y;\ x, y \in Q \rangle = \langle [x,y];\ x, y \in Q \rangle.$$

Proof. Note that if $N \trianglelefteq Q$ then $a/b \in N$ iff $a\backslash b \in N$. It is therefore irrelevant on which side of the inner mappings $W(z)$ we divide by z. □

Notice that we have just recovered the classical result of group theory that Q' is the subgroup generated by all commutators.

The case of the associator subloop is more difficult. A similar trick as above allows us to show that the subloop is preserved by the inner mappings $L_{x,y}$ and $R_{x,y}$, but it cannot be used for T_x, because $A(Q)$ does not contain commutators. The idea behind the proof of Theorem 8.4 comes from Leong [24], who proved a similar result with a different choice of associators, described in Section 2. We will imitate his proof with our associators.

Theorem 8.4. *Let Q be a loop. Then $A(Q) = \langle a^{\cdot\cdot}(x,y,z),\ b^{\cdot\cdot}(x,y,z);\ x, y, z \in Q \rangle$.*

Proof. Write a instead of $a^{\cdot\cdot}$, b instead of $b^{\cdot\cdot}$, and let H be the subloop on the right hand side. By Lemma 6.2, it suffices to show that $H \trianglelefteq Q$.

For $h \in H$ we have $(hx)y = a(h,x,y)h \cdot xy \in H \cdot xy$ and $x \cdot yh = xy \cdot hb(h,y,x) \in xy \cdot H$, so

$$Hx \cdot y \subseteq H \cdot xy \quad \text{and} \quad x \cdot yH \subseteq xy \cdot H.$$

We will use these inclusions freely.

We claim that

$$(H/x)/y = H/(yx). \tag{8.1}$$

Let $h \in H$. For one inclusion, we need to show that $((h/x)/y)\cdot yx \in H$. Now, $((h/x)/y)\cdot yx = ((h/x)/y)y \cdot xb((h/x)/y, y, x) \in ((h/x)/y)y \cdot xH = (h/x) \cdot xH \subseteq (h/x \cdot x)H = hH = H$. For the other inclusion, we need to show that $(h/(yx))y \cdot x \in H$. Now, $(h/(yx))y \cdot x = a(h/(yx), y, x)(h/(yx)) \cdot yx \in (H \cdot h/(yx)) \cdot yx \subseteq H((h/(yx)) \cdot yx) = Hh = H$. We will use (8.1) freely.

Let $X = \{H/x;\ x \in Q\}$. For $x \in Q$ define $\alpha_x \in \mathrm{Sym}(X)$ by

$$\alpha_x(H/y) = (H/y)/x = H/(xy).$$

If $H/y = H/z$ then $(H/y)/x = (H/z)/x$, so α_x is a well-defined mapping into X. If $(H/y)/x = (H/z)/x$ then $H/y = H/z$, so α_x is one-to-one. Finally, for any $y \in Q$ we have $\alpha_x(H/(x\backslash y)) = H/(x \cdot x\backslash y) = H/y$, so α_x is onto X.

Note that $y \cdot zx \in yz \cdot xH \subseteq (yz \cdot x)H$, so there is $h \in H$ such that $y \cdot zx = (yz \cdot x)h$. Consequently, $H/(y \cdot zx) = H/((yz \cdot x)h) = (H/h)/(yz \cdot x) = H/(yz \cdot x)$. Define

$$\alpha : Q \to \mathrm{Sym}(X), \quad x \mapsto \alpha_x.$$

Then $\alpha_{yz}(H/x) = H/(yz \cdot x) = H/(y \cdot zx) = (H/(zx))/y = ((H/x)/z)/y = \alpha_y\alpha_z(H/x)$, so α is a homomorphism into a group. Let $K = \ker(\alpha)$. Then $Q/K \cong \mathrm{Img}(\alpha)$ is a group, and so $H \subseteq K$ by Lemma 6.2. Given $x \in K$, we have $(H/y)/x = H/y$ for every $y \in Q$, in particular, with $y = 1$ we get $H/x = H$, so $x \in H$, proving $K \subseteq H$. This means that $H = K \trianglelefteq Q$. □

Corollary 8.5. *Suppose that Q is a finite loop, or an inverse property loop, or a commutative loop. Then*

$$A(Q) = \langle a^{\cdot\cdot}(x, y, z);\ x, y, z \in Q\rangle = \langle b^{\cdot\cdot}(x, y, z);\ x, y, z \in Q\rangle.$$

Proof. If Q is an inverse property loop, observe that $a^{\cdot\cdot}(x, y, z)^{-1} = b^{\cdot\cdot}(x^{-1}, y^{-1}, z^{-1})$. If Q is commutative, we have $a^{\cdot\cdot}(x, y, z) = b^{\cdot\cdot}(x, y, z)$. In either case, we are done by Theorem 8.4.

Now suppose that Q is a finite loop, and let us focus on the associator $b = b^{\cdot\cdot}$. Let $H = \langle b(x, y, z);\ x, y, z \in Q\rangle$. As in the proof of Theorem 8.4, we have $x \cdot yH \subseteq xy \cdot H$. Since the two sets have the same cardinality, we have $x \cdot yH = xy \cdot H$ by finiteness. Using this inclusion with $h \in H$, we have $((h/x)/y) \cdot yx \in ((h/x)/y)y \cdot xH = (h/x) \cdot xH \subseteq (h/x \cdot x)H = hH = H$, so $(H/x)/y \subseteq H/(yx)$, and thus $(H/x)/y = H/(yx)$ by finiteness. Then the last two paragraphs of the proof of Theorem 8.4 go through word for word. □

Our choice of associators and commutators for Theorem 8.4 is certainly not the only choice; in the end, Leong used a different associator b.

Problem 8.6. *Determine all minimal subsets $\mathcal{A}$ of the eight types of associators of Lemma 6.2(i) such that for every loop Q we have $A(Q) = \langle a(x, y, z);\ a \in \mathcal{A},\ x,\ y,\ z \in Q\rangle$.*

Just like in group theory, it is reasonable to consider the smallest normal subloop N such that Q/N is a commutative loop. Clearly, $N = \mathrm{Ng}(\ [x, y];\ x, y \in Q\ )$. Can we possibly avoid the normal closure? Let

$$\mathrm{Comm}(Q) = \langle c^{\cdot}(x, y),\ d^{\cdot}(x, y),\ c^{\backslash}(x, y),\ d^{/}(x, y);\ x, y \in Q\rangle.$$

It is easy to check that $c^{\backslash}(x,y) = c^{\cdot}(x, x\backslash y)$ and $d^{/}(x,y) = d^{\cdot}(x, y/x)$, hence, in fact, $\mathrm{Comm}(Q) = \langle c^{\cdot}(x,y),\ d^{\cdot}(x,y);\ x,y \in Q\rangle$. Unfortunately, $\mathrm{Comm}(Q)$ is not necessarily normal in Q, as witnessed by Example 9.5.

Problem 8.7. *Is there a loop Q such that $\langle a^{\cdot\cdot}(x,y,z);\ x,y,z \in Q\rangle \neq \langle b^{\cdot\cdot}(x,y,z);\ x,y,z \in Q\rangle$? Is there a loop Q such that $\langle c^{\cdot}(x,y);\ x,y \in Q\rangle \neq \langle d^{\cdot}(x,y);\ x,y \in Q\rangle$?*

9. Examples and counterexamples

All examples in this section will be based on a general construction, inspired by the example in [12, Chapter 5, Exercise 10].

Construction 9.1. Let $(G,+)$ be an abelian group and let $(G,\oplus)$ be a quasigroup. We define $Q = G[\oplus]$ to be the loop on $G \times \mathbb{Z}_2$ with multiplication

$$(x,a)(y,b) = \begin{cases} (x+y, a+b) & \text{if } a = 0 \text{ or } b = 0, \\ (x \oplus y, 0) & \text{otherwise.} \end{cases}$$

Properties. The set $H = G \times \{0\}$ forms a normal subloop isomorphic to $(G,+)$, since it is the kernel of the projection $Q \to \mathbb{Z}_2$, $(x,a) \mapsto a$. Hence Q possesses a chain of normal subloops $0 \leq H \leq Q$ such that each factor is an abelian group. Consequently, $Q' \leq H$ and Q is solvable (in the sense of Bruck).

Notational remarks. For $x \in Q$, we will implicitly assume $x = (x_0, x_1)$. For brevity, for $a \in H$ and $k \in \mathbb{N}$, let $ka = (ka_0, 0)$. The division operations with respect to $\oplus$ will be denoted by $\oslash$ and $\odot$. The identity element $(0,0)$ of Q will be denoted by 0.

Inner mappings. Since $Q' \subseteq H$, to determine congruence solvability and nilpotency we will need to calculate commutators $[A,B]_Q$ for $A,\ B \trianglelefteq Q$ such that $A \subseteq H$. Hence, we need to determine the values of inner mappings on the elements of H. For every $a,b \in H$, $x,y \in Q \setminus H$ and every $z \in Q$, we get

$$\begin{aligned} T_z(a) &= a \quad \text{and} \quad U_z(a) = -a, \\ L_{b,z}(a) &= L_{z,b}(a) = R_{b,z}(a) = R_{z,b}(a) = a \quad \text{and} \quad M_{z,b}(a) = M_{x,z}(a) = -a, \\ L_{x,y}(a) &= ((x_0 \oplus (y_0 + a_0)) - (x_0 \oplus y_0), 0), \\ R_{x,y}(a) &= (((y_0 + a_0) \oplus x_0) - (y_0 \oplus x_0), 0), \\ M_{b,x}(a) &= ((x_0 \oslash b_0) - ((x_0 - a_0) \oslash b_0), 0). \end{aligned}$$

It follows from Theorem 2.2 and Proposition 3.4 that

$$[A,B]_Q = \mathrm{Ng}(\ W_{u_1,u_2}(a)/W_{v_1,v_2}(a);\ W \in \{L,R,M\},\ a \in A,\ \bar{u}/\bar{v} \in B\ )$$

for every $A,\ B \trianglelefteq Q$ such that $A \subseteq H$.

Also note that $c^{\cdot}(z,a) = 1$ and $a^{\cdot\cdot}(a,b,z) = a^{\cdot\cdot}(a,z,b) = b^{\cdot\cdot}(a,b,z) = b^{\cdot\cdot}(a,z,b) = 1$ whenever $a,b \in H$ and $z \in Q$.

The next three examples show how to use our theory to efficiently calculate commutators and derived subloops, and also illustrate the variety of options that Construction 9.1 offers. Imitating the notation for congruences, set

$$Q^{(0)} = Q_{(0)} = Q, \qquad Q_{(i+1)} = [Q_{(i)}, Q]_Q, \qquad Q^{(i+1)} = [Q^{(i)}, Q^{(i)}]_Q.$$

Note that $Q^{(1)} = Q_{(1)} = Q'$. A loop Q is called *centrally nilpotent* if $Q_{(n)} = 1$ for some n, and it is called *congruence solvable* if $Q^{(n)} = 1$ for some n.

Example 9.2. Let $(G,+)$ be an abelian group. Consider the loop $Q = G[-]$, i.e., $x \oplus y = x - y$, the subtraction in G. In general we obtain a non-commutative non-associative loop. It is easy to check that $x \oslash y = x - y$ and $x \oslash y = x + y$. For $n \in \mathbb{N}$, let $H_n = 2^n G \times \{0\}$, where $mG = \{mg;\ g \in G\}$, and notice that this is a subloop of Q.

Let $a, b \in H$ and $x, y \in Q \setminus H$. Using the general expressions above, we see that $L_{x,y}(a) = ((x_0 - (y_0 + a_0)) - (x_0 - y_0), 0) = (-a_0, 0) = -a$, and thus also $L^{-1}_{x,y}(a) = -a$. Similar computations yield $R_{x,y}(a) = a$ and $M_{b,x}(a) = a$, and the remaining inner mappings are also identical or inverse mappings on H. Consequently, every subloop of H is normal in Q (in particular, $H_n \trianglelefteq Q$), and

$$[A, B]_Q = \mathrm{Ng}(\ L_{u_1,u_2}(a)/L_{v_1,v_2}(a);\ \ a \in A,\ \bar{u}/\bar{v} \in B\ )$$

for every $A, B \trianglelefteq Q$ such that $A \subseteq H$.

Let us calculate the derived subloop of $Q = G[-]$. Note that $a^{\cdot\cdot}(x,y,z)$, $b^{\cdot\cdot}(x,y,z)$, and $c^{\cdot}(x,y)$, evaluated in Q, are expressions with an even number of occurences of x_0, y_0, z_0, each with a positive or negative sign. For example,

$$c^{\cdot}((x_0,1),(y_0,1)) = ((y_0 \oslash (x_0 \oplus y_0)) - x_0, 0) = ((y_0 - (x_0 - y_0)) - x_0, 0) = (2y_0 - 2x_0, 0).$$

Consequently, the result is always in $H_1 = 2G \times \{0\}$. On the other hand, every element $2a \in H_1$ can be expressed, for example, by $2a = (2a_0, 0) = c^{\cdot}((a,1),(0,1))$. We see that $Q' = H_1$.

Now, let us have a look at the commutator. If both $A, B \subseteq H$, then $[A,B]_Q \subseteq [H,H]_Q$. But $[H,H]_Q = 0$: if $u_i/v_i \in H$, then $u_i \in H$ iff $v_i \in H$, hence either $L_{u_1,u_2}(a)/L_{v_1,v_2}(a) = a/a = 0$, or $L_{u_1,u_2}(a)/L_{v_1,v_2}(a) = (-a)/(-a) = 0$. In particular, $Q^{(2)} = 0$ and Q is congruence solvable.

On the other hand, $[A,Q]_Q$ may not vanish, since $L_{(0,1),(0,1)}(a)/L_{(0,0),(0,0)}(a) = (-a)/a = -2a$, hence $[A,Q]_Q = 2A$. Consequently, we have $Q_{(n)} = H_n$ for every $n \geq 1$. If $|G|$ is odd, we have $Q_{(n)} = H$ for every n, and Q is not centrally nilpotent. If $G = \mathbb{Z}$, for instance, we obtain a strictly decreasing chain with trivial intersection, hence Q is not centrally nilpotent (this situation is sometimes refered to as transfinite nilpotency). If $|G|$ is a power of two, then $2^n G = 0$ for some n, and thus Q is centrally nilpotent.

Example 9.2 also shows an obstacle to removing quotients from the generating set of the commutator, as described in Corollary 7.5. Let $A, B \trianglelefteq G[\oplus]$ be such that $A \subseteq H$. On one hand, all associators and commutators with at least one parameter from A and one parameter from B vanish. On the other hand, associators with one parameter in A (or B) and other parameters arbitrary may not belong to $[A,B]_Q$. For instance, in $G[-]$ with $A = B = H$, we have $[H,H]_Q = 0$, but $b^{\cdot\cdot}(a,x,y) = a \backslash L_{y,x}(a) = -2a$, for every $a \in H$ and $x, y \in Q \setminus H$.

The next two examples show a particular choice of G and $\oplus$ such that the subloop H, which itself is an abelian group, is not abelian in $G[\oplus]$. In Example 9.3, $G[\oplus]$ is not congruence solvable. This is a rather typical situation, resulting from most combinations of G and $\oplus$. In Example 9.4, $G[\oplus]$ is congruence solvable.

Example 9.3. Consider the loop $Q = \mathbb{Z}_4[\oplus]$, where the operation $\oplus$ is given by the following multiplication table:

	0	1	2	3
0	0	1	2	3
1	1	3	0	2
2	2	0	3	1
3	3	2	1	0

Notice that $(\{0,1,2,3\},\oplus) \cong \mathbb{Z}_4$. We will show that $Q' = H$ and that $Q^{(2)} = Q_{(2)} = H$, hence Q is not congruence solvable.

Observe that $L_{(0,1),(0,1)}((1,0)) = (1,0)$ and $L_{(1,1),(0,1)}((1,0)) = (2,0)$. It follows that $b^{\cdot\cdot}((1,0),(0,1),(1,1)) = (1,0)\backslash L_{(1,1),(0,1)}((1,0)) = (1,0) \in Q'$, and thus $H = \langle(1,0)\rangle \subseteq Q' \subseteq H$, hence $Q' = H$. Furthermore, $L_{(1,1),(0,1)}((1,0))/L_{(0,1),(0,1)}((1,0)) = (1,0) \in [H,H]_Q$, hence $H = \langle(1,0)\rangle \subseteq [H,H]_Q \subseteq [H,Q]_Q \subseteq H$, so $[H,H]_Q = [H,Q]_Q = H$.

According to `GAP`, the total multiplication group $\mathrm{TMlt}(Q)$ is solvable. Hence, Vesanen's theorem [38] does not strengthen to congruence solvability.

Example 9.4. Consider the loop $Q = \mathbb{Z}_4[\oplus]$, where the operation $\oplus$ is given by the following multiplication table:

	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Notice that $(\{0,1,2,3\},\oplus) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ and that

$$r \oplus s = \begin{cases} r+s+2 & \text{if } r,s \in \{1,3\}, \\ r+s & \text{otherwise.} \end{cases}$$

Consequently, we can write $r \oplus s = r + s + \varepsilon$ where $\varepsilon \in \{0,2\}$, where $\varepsilon = 2$ iff r, $s \in \{1,3\}$, and similarly for the division operations $\oslash$, $\oslash$. Let $K = \{0,2\} \times \{0\}$. We will show that $Q' = [H,H]_Q = K$, and that $Q^{(2)} = Q_{(2)} = 0$. Hence, Q is centrally nilpotent, although H is not abelian in Q.

Q is finite and commutative, so we can focus on $L_{x,y}$. For $a \in H$ and $x, y \in Q \setminus H$, we have

$$L_{x,y}(a) = ((x_0 \oplus (y_0 + a)) - (x_0 \oplus y_0), 0) = (x + (y + a) + \varepsilon_1 - (x + y + \varepsilon_2), 0) = (\varepsilon_1 - \varepsilon_2, 0) \in K.$$

We immediately see that K is normal in Q and that $[H,H]_Q \subseteq K$. Since

$$L_{(1,1),(0,1)}(1,0)/L_{(0,1),(0,1)}(1,0) = (3,0)/(1,0) = (2,0) \in [H,H]_Q,$$

we obtain $[H,H]_Q = K$. Furthermore, if $a \in K$, then $\varepsilon_1 = \varepsilon_2$, and thus $[K,K]_Q \subseteq [K,Q]_Q = 0$. To show that $Q' = K$, calculate the associator $a^{\cdot\cdot}(x,y,z) = ((xy \cdot z)/(yz))/x = ((((x_0 + y_0 + \varepsilon_1) + z_0 + \varepsilon_2) - (y_0 + z_0 + \varepsilon_3) + \varepsilon_4) - x + \varepsilon_5, 0) = (\varepsilon_1 + \varepsilon_2 - \varepsilon_3 + \varepsilon_4 + \varepsilon_5, 0) \in K$, so $Q' \subseteq K$. Since Q is not associative, we get $Q' = K$.

The distinction between "abelianess" and "abelianess in Q" persists even in varieties of loops that are very close to groups. For instance, let Q be the left Bol loop of order 8 from Example 3.6 (catalog number `LeftBolLoop(8,1)` in the `LOOPS` package for `GAP`), and let $N = \{1,2,3,4\}$. Then $N \trianglelefteq Q$, N is an abelian group, but $[N,N]_Q = Z(Q) = \{1,2\}$, so N is

not abelian in Q. Nevertheless, Q is congruence solvable. A similar situation occurs in the Moufang loop of order 16 with catalog number `MoufangLoop(16,4)` for one of its normal subloops isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Finally, we present an example of a loop where $\mathrm{Comm}(Q)$ is not normal.

Example 9.5. Consider the loop $Q = \mathbb{Z}_4[\oplus]$, where the operation $\oplus$ is given by

$\oplus$	0	1	2	3
0	0	2	3	1
1	1	0	2	3
2	3	1	0	2
3	2	3	1	0

One can check that $\mathrm{Comm}(Q) = \{(0,0),(2,0)\}$, which is not a normal subloop of Q.

10. Center and nilpotency, abelianess and solvability

The purpose of this section is to supply details for the exposition in Section 2.

Recall the definitions of the commutator $[\alpha,\beta]$, the center $\zeta(\mathbf{A})$ and abelianess in $\mathbf{A}$. First, we show how $[\alpha, 1_{\mathbf{A}}]$ relates to the center, and how $[\alpha,\alpha]$ relates to abelianess.

Let α be a congruence of an algebra $\mathbf{A}$. By definition, $[\alpha, 1_{\mathbf{A}}]$ is the smallest congruence δ such that $C(\alpha, 1_{\mathbf{A}}; \delta)$ in $\mathbf{A}$, or equivalently, $C(\alpha/\delta, 1_{\mathbf{A}/\delta}; 0_{\mathbf{A}/\delta})$ in $\mathbf{A}/\delta$. The definition of the center says $C(\xi, 1_{\mathbf{B}}; 0_{\mathbf{B}})$ in $\mathbf{B}$ iff $\xi \leq \zeta(\mathbf{B})$. Applied to $\mathbf{B} = \mathbf{A}/\delta$, we see that $[\alpha, 1_{\mathbf{A}}]$ is the smallest δ such that $\alpha/\delta \leq \zeta(\mathbf{A}/\delta)$.

By definition, $[\alpha,\alpha]$ is the smallest congruence δ such that $C(\alpha,\alpha;\delta)$ in $\mathbf{A}$, or equivalently, $C(\alpha/\delta, \alpha/\delta; 0_{\mathbf{A}/\delta})$ in $\mathbf{A}/\delta$. The latter says that the congruence α/δ is abelian in $\mathbf{A}/\delta$.

10.1. **In loops.** Recall that the center $Z(Q)$ of a loop Q is defined in loop theory as

$$Z(Q) = \{a \in Q;\ ax{=}xa,\ a(xy){=}(ax)y,\ x(ay){=}(xa)y,\ x(ya){=}(xy)a \text{ for every } x, y \in Q\}.$$

Theorem 10.1 shows that $Z(Q)$ and $\zeta(Q)$ define the same concept. For groups, the proof can be found in [6, Section II.13], for instance, and it easily extends to loops. For the sake of completeness (and because we are not aware of a proof in the literature), we present a complete proof here. It is instructive to read the proof to become accustomed to the universal algebraic approach to loop theory.

Theorem 10.1. *If Q is a loop, then $Z(Q) = N_{\zeta(Q)}$.*

Proof. We will prove two inclusions: $\gamma_{Z(Q)} \subseteq \zeta(Q)$ and $N_{\zeta(Q)} \subseteq Z(Q)$.

Let $a\,\gamma_{Z(Q)}\,b$. We want to show $a\,\zeta(Q)\,b$. Since $\zeta(Q)$ is the largest congruence such that $C(\zeta(Q), 1_Q; 0_Q)$, it is sufficient to show that (the congruence generated by) the pair (a,b) centralizes 1_Q over 0_Q. Let t be a term and $u_1,\dots,u_n$, $v_1,\dots,v_n$ two tuples over Q. Assuming $t(a,u_1,\dots,u_n) = t(a,v_1,\dots,v_n)$, we get

$$\begin{aligned} t(b,u_1,\dots,u_n) &= t(b/a\cdot a, u_1,\dots,u_n) = b/a\cdot t(a,u_1,\dots,u_n) \\ &= b/a\cdot t(a,v_1,\dots,v_n) = t(b/a\cdot a, v_1,\dots,v_n) = t(b,v_1,\dots,v_n), \end{aligned}$$

where the second and the fourth equalities follow form the fact that $b/a \in Z(Q)$, i.e., b/a commutes and associates with everything.

Conversely, let $a \in N_{\zeta(Q)}$, i.e., $a\,\zeta(Q)\,1$. We want to show that $a \in Z(Q)$. It actually suffices to show that $ab = ba$, $a(bc) = (ab)c$ and $b(ca) = (bc)a$ for every b, $c \in Q$, since

then $b(ac) = b(ca) = (bc)a = a(bc) = (ab)c = (ba)c$, too. We will use $C(\zeta(Q), 1_Q; 0_Q)$ freely, noting that the equivalence modulo 0_Q is merely the equality.

For $ab = ba$, consider the term $t(x, y, z) = x(yz)$. Then $t(1, 1, b) = b = t(b, 1, 1)$, and upon replacing the middle argument 1 with a, we conclude that $ab = t(1, a, b) = t(b, a, 1) = ba$. For $a(bc) = (ab)c$, consider the auxiliary term $m(x, y, z) = x(y\backslash z)$. (This is in fact a Mal'tsev term for loops.) Then $m(1, a, a)m(b, 1, c) = bc = m(1, 1, b)m(c, c, c)$, and replacing the first argument 1 with a yields $a(bc) = m(a, a, a)m(b, 1, c) = m(a, 1, b)m(c, c, c) = (ab)c$. For $b(ca) = (bc)a$, we proceed dually and consider the auxiliary term $m'(x, y, z) = (x/y)z$. Then $m'(b, b, b)m'(c, 1, 1) = bc = m'(b, 1, c)m'(a, a, 1)$, and replacing the last argument 1 with a yields $b(ca) = m'(b, b, b)m'(c, 1, a) = m'(b, 1, c)m'(a, a, a) = (bc)a$. □

Corollary 10.2. *A loop is abelian if and only if it is a commutative group.*

Proof. $\zeta(Q) = 1_Q$ iff $Z(Q) = Q$ iff Q is commutative and associative. □

Using the observations at the beginning of the section, this finishes the proof that universal algebraic nilpotency is the same notion as central nilpotency.

We want to point out that abelian groups and nilpotent loops are important classes of algebras in the abstract structure theory of universal algebra. Let A be an algebra with a Mal'tsev term m. Choose an arbitrary element $e \in A$ and define $a + b = m(a, e, b)$. The fundamental theorem of abelian algebras [12, Section 5] says that if A is abelian, then $(A, +)$ is an abelian group with unit e (it actually states a stronger property: A is polynomially equivalent to a module, whose group reduct is $(A, +)$). According to [12, Section 7], if A is nilpotent, then $(A, +)$ is a nilpotent loop with unit e (no polynomial equivalence in this case).

10.2. **In groups.** It is instructive to look at how the commutator theory from universal algebra applies to groups. Unlike in loops, the standard commutator in groups is in accordance with the commutator theory. In fact, the situation in groups (and also in rings) gave rise to the general commutator theory. Nevertheless, an elementary proof that the two commutators agree in groups is not obvious, and the reader might want to look at one, for instance, in [28].

In groups, unlike in loops, if A is a normal subgroup of G and A itself is an abelian group, then A is abelian in G. It is interesting to see why. The following chain of equivalent conditions settles it: A is abelian in G, $[\gamma_A, \gamma_A] = 0_G$ (by definition), $[A, A]_G = 1$ (*because the two commutators agree*), A is a commutative group (by definition of the commutator in groups), $Z(A) = A$ (by definition of the center in groups), $\zeta(A) = 1_A$ (because the two centers agree), $[1_A, 1_A] = 0_A$, A is abelian (by definition). This explains why it is safe to call commutative groups by the traditional name abelian groups, and why it is not necessary to distinguish between normal subgroups that are abelian and normal subgroups that are abelian *in* the enveloping group.

Problem 10.3. *Investigate the commutator in varieties of loops close to groups, e.g., Moufang loops, Bruck loops or automorphic loops. Describe what does it mean for a subloop of Q to be abelian in Q. Is congruence solvability equivalent to solvability here?*

10.3. **Alternative approaches to commutators, nilpotency and solvability.** Each of the following four paragraphs presents an alternative to what we have done here.

Recent discussions in the universal algebraic community seem to lead to a conclusion that the notion of nilpotency coming from the Freese-McKenzie commutator theory is too weak. A new approach, called *supernilpotency*, based on Bulatov's higher commutators, has been promoted recently by Aichinger and Mudrinski [1]. An important property of supernilpotency, reflecting the situation in finite groups, is the following. A finite algebra with a Mal'tsev term (a finite loop in particular) is supernilpotent if and only if it is a direct product of nilpotent algebras of prime power size. Wright [39] proved that a loop Q satisfies the latter property if and only if $\mathrm{Mlt}(Q)$ is nilpotent. A characterization of infinite supernilpotent loops, and more generally, calculation of higher commutators in the variety of loops, is an interesting open problem.

Yet another approach to nilpotency has been proposed by Mostovoy [26], using so-called *commutator-associator filtration*. The relation between the commutator-associator filtrations and the universal algebraic approach is not clear.

Solvability in loops has been tackled by Lemieux et al. [23] in connection with the question whether algebras can express arbitrary Boolean functions. They introduced the notion of *polyabelianess*, a property of loops strictly between nilpotency and solvability (in the Bruck sense), and proved that a finite loop is polyabelian if and only it is *not* able to express Boolean functions. It follows easily from the tame congruence theory [20] that, for finite algebras with a Mal'tsev term (finite loops in particular), solvability in the sense of commutator theory is equivalent to inability to express Boolean functions in the sense of [23]. Hence, for finite loops, polyabelianess is the same as congruence solvability. The relation of the two notions in the infinite case is under investigation.

Finally, let us mention that in category theory, an alternative commutator theory, called the *Huq commutator*, has been proposed. For groups, the two commutators agree. For loops, they do not [19]. Translating the Huq commutator into loop theory might identify important structural features in loops.

Acknowledgment

The proof of Proposition 3.2 was suggested to us by A. Drápal. We acknowledge the assistance of the model builder `mace4` [27], the Universal Algebra Calculator [13], and the `LOOPS` [31] package for `GAP` [16]—we used them to construct several examples and counterexamples. We thank an anonymous referee of an earlier version of the paper for many useful comments and suggestions for further research. We also thank an anonymous referee of this version for a thorough survey of related literature.

References

[1] E. Aichinger and N. Mudrinski, *Some applications of higher commutators in Mal'cev algebras*, Algebra Universalis **63** (2010), no. **4** , 367-403.

[2] V.D. Belousov, *Osnovy teorii kvazigrupp i lup* (Russian), Izdat. "Nauka", Moscow, 1967.

[3] V.D. Belousov, *The group associated with a quasigroup* (Russian), Mat. Issled. **4**/3 (1969), 21-39.

[4] C. Bergman, *Universal algebra: Fundamentals and selected topics*, Chapman & Hall/CRC Press, 2011.

[5] R.H. Bruck, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer Verlag, Berlin-Göttingen-Heidelberg, 1958.

[6] S. Burris and H.P. Sankappanavar, *A course in universal algebra*, Graduate Texts in Mathematics **78**, Springer-Verlag, New York-Berlin, 1981.

[7] A.V. Covalschi, N.I. Sandu, *On the generalized nilpotent and generalized solvable loops*, ROMAI J. **7/1** (2011), 39–62.

[8] P. Csörgő, *Abelian inner mappings and nilpotency class greater than two*, European J. Combin. **28** (2007), no. **3**, 858–867.
[9] P. Csörgő and A. Drápal, *Left conjugacy closed loops of nilpotency class two*, Results Math. **47** (2005), no. **3**–**4**, 242–265.
[10] A. Drápal, M. Kinyon and P. Vojtěchovský, *Loop Theory*, textbook, in preparation.
[11] T. Evans, *Homomorphisms of non-associative systems*, J. London Math. Soc. **24** (1949), 254–260.
[12] R. Freese and R. McKenzie, *Commutator theory for congruence modular varieties*, London Mathematical Society Lecture Note Series **125**, Cambridge University Press, Cambridge, 1987.
[13] R. Freese, E. Kiss and M. Valeriote, *Universal Algebra Calculator*, 2011. Available at: `www.uacalc.org`.
[14] W. Feit and J.G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775–1029.
[15] S.M. Gagola III, *How and why Moufang loops behave like groups*, Quasigroups Related Systems **19** (2011), no. **1**, 1–22.
[16] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.5.5; 2012. (http://www.gap-system.org)
[17] G. Glauberman, *On loops of odd order II*, J. Algebra **8** (1968), 393–414.
[18] G. Glauberman and C.R.B. Wright, *Nilpotence of finite Moufang 2-loops*, J. Algebra **8** (1968), 415–417.
[19] M. Hartl and T. Van der Linden, *The ternary commutator obstruction for internal crossed modules*, Adv. Math. **232** (2013), 571-607.
[20] D. Hobby and R. McKenzie, *The structure of finite algebras*, Contemporary Mathematics **76**, American Mathematical Society, Providence, RI, 1988.
[21] P. Jedlička, M. Kinyon and P. Vojtěchovský, *Nilpotency in automorphic loops of prime power order*, J. Algebra **350** (2012), 64–76.
[22] M. Kinyon, K. Kunen, J.D. Phillips and P. Vojtěchovský, *The structure of automorphic loops*, to appear in Trans. Amer. Math. Soc.
[23] F. Lemieux, C. Moore and D. Thérien, *Polyabelian loops and Boolean completeness*, Comment. Math. Univ. Carolin. **41** (2000), no. **4**, 671-686.
[24] F. Leong, *The devil and the angel of loops*, Proc. Amer. Math. Soc. **54** (1976), 32–34.
[25] M. Mazur, *Connected transversals to nilpotent groups*, J. Group Theory **10** (2007), no. **2**, 195–203.
[26] J. Mostovoy, *Nilpotency and dimension series for loops*, Comm. Algebra **36** (2008), no. **4**, 1565–1579.
[27] W. McCune, `mace4`, finite model builder, available at `http://www.cs.unm.edu/~mccune/mace4`.
[28] R. McKenzie and J. Snow, *Congruence modular varieties: commutator theory and its uses*, in Structural theory of automata, semigroups, and universal algebra, NATO Sci. Ser. II Math. Phys. Chem. **207**, 273–329, Springer, Dordrecht, 2005.
[29] G.P. Nagy and M. Valsecchi, *On nilpotent Moufang loops with central associators*, J. Algebra **307** (2007), no. **2**, 547–564.
[30] G.P. Nagy and P. Vojtěchovský, *Moufang loops with commuting inner mappings*, J. Pure Appl. Algebra **213** (2009), no. **11**, 2177–2186.
[31] G.P. Nagy and P. Vojtěchovský, `LOOPS`: Computing with quasigroups and loops in GAP, version 2.2.0, available at `www.math.du.edu/loops`.
[32] M. Niemenmaa, *Finite loops with nilpotent inner mapping groups are centrally nilpotent*, Bull. Aust. Math. Soc. **79** (2009), no. **1**, 109–114.
[33] M. Niemenmaa, M. Rytty, *Centrally nilpotent finite loops*, Quasigroups Related Systems **19** (2011), no. **1**, 123-132.
[34] H.O. Pflugfelder, *Quasigroups and loops: introduction*, Heldermann Verlag, Berlin, 1990.
[35] V.A. Shcherbakov, *Some properties of the full associated group of an IP-loop* (Russian), Izv. Akad. Nauk Moldav. SSR Ser. Fiz.-Tekhn. Mat. Nauk **79/2** (1984), 51-52.
[36] J.D.H. Smith, *Mal'cev varieties*, Lecture Notes in Mathematics **554**, Springer Verlag, Berlin, 1976.
[37] J.D.H. Smith, *On the nilpotence class of commutative Moufang loops*, Math. Proc. Cambridge Philos. Soc. **84** (1978), no. **3**, 387–404.
[38] A. Vesanen, *Solvable groups and loops*, J. Algebra **180/3** (1996), 862–876.
[39] C.R.B. Wright, *On the multiplication group of a loop*, Illinois J. Math. **13** (1969), 660-673.

(Stanovský, Vojtěchovský) Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, Colorado 80208, U.S.A.

(Stanovský) Department of Algebra, Faculty of Mathematics and Physics, Charles University, Praha 8, Sokolovská 83, 186 75, Czech Republic

E-mail address, Stanovský: stanovsk@karlin.mff.cuni.cz

E-mail address, Vojtěchovský: petr@math.du.edu