An algebraic motivation for loops

Paolo Aglianò
agliano@live.com

Novi Sad, June 15-18 2017

Dedicated to the memory of Bjarni Jónsson
(Feb 15, 1920 - Sep 30, 2016)

DISCLAIMER: There is no need of a further motivation to study loops.

The setting: Congruence Varieties

- for any variety of algebras $\mathcal{V}$, let $\mathrm{Con}(\mathcal{V})$ be the variety of lattices generated by the congruence lattices in $\mathcal{V}$;

The setting: Congruence Varieties

- for any variety of algebras $\mathcal{V}$, let $\mathrm{Con}(\mathcal{V})$ be the variety of lattices generated by the congruence lattices in $\mathcal{V}$;
- a variety $\mathcal{K}$ of lattices such that $\mathcal{K} = \mathrm{Con}(\mathcal{V})$ for some variety $\mathcal{V}$, is a **congruence variety**;

The setting: Congruence Varieties

- for any variety of algebras $\mathcal{V}$, let $\mathrm{Con}(\mathcal{V})$ be the variety of lattices generated by the congruence lattices in $\mathcal{V}$;
- a variety $\mathcal{K}$ of lattices such that $\mathcal{K} = \mathrm{Con}(\mathcal{V})$ for some variety $\mathcal{V}$, is a **congruence variety**;
- congruence varieties have been introduced by Bjarni Jónsson in the seventies and investigated extensively ever since.

Something we know

- The variety $\mathcal{L}$ of all lattices is a congruence variety; in fact if $\mathcal{S}$ is the variety of semilattices $\mathrm{Con}(\mathcal{S}) = \mathcal{L}$ [Freese-Nation 1973];

Something we know

- The variety $\mathcal{L}$ of all lattices is a congruence variety; in fact if $\mathcal{S}$ is the variety of semilattices $\mathrm{Con}(\mathcal{S}) = \mathcal{L}$ [Freese-Nation 1973];
- not every variety of lattices is a congruence variety [Nation 1974];

Something we know

- The variety $\mathcal{L}$ of all lattices is a congruence variety; in fact if $\mathcal{S}$ is the variety of semilattices $\mathrm{Con}(\mathcal{S}) = \mathcal{L}$ [Freese-Nation 1973];
- not every variety of lattices is a congruence variety [Nation 1974];
- there are proper congruence varieties that are not modular (i.e. are not contained in $\mathcal{M}$ the variety of all modular lattices) [Polin 1977, Day-Freese 1980];

Something we know

- The variety $\mathcal{L}$ of all lattices is a congruence variety; in fact if $\mathcal{S}$ is the variety of semilattices $\mathrm{Con}(\mathcal{S}) = \mathcal{L}$ [Freese-Nation 1973];
- not every variety of lattices is a congruence variety [Nation 1974];
- there are proper congruence varieties that are not modular (i.e. are not contained in $\mathcal{M}$ the variety of all modular lattices) [Polin 1977, Day-Freese 1980];
- there is no largest proper congruence variety [Kearnes-Kiss 2013];

Something we know

- The variety $\mathcal{L}$ of all lattices is a congruence variety; in fact if $\mathcal{S}$ is the variety of semilattices $\mathrm{Con}(\mathcal{S}) = \mathcal{L}$ [Freese-Nation 1973];
- not every variety of lattices is a congruence variety [Nation 1974];
- there are proper congruence varieties that are not modular (i.e. are not contained in $\mathcal{M}$ the variety of all modular lattices) [Polin 1977, Day-Freese 1980];
- there is no largest proper congruence variety [Kearnes-Kiss 2013];
- several other results of the same flavor in *The shape of congruence lattices* [Kearnes-Kiss 2013].

Modular Congruence Varieties

- since modularity is a lattice equation a congruence variety $\mathrm{Con}(\mathcal{V})$ is modular if and only if $\mathcal{V}$ is congruence modular;

Modular Congruence Varieties

- since modularity is a lattice equation a congruence variety $\mathrm{Con}(\mathcal{V})$ is modular if and only if $\mathcal{V}$ is congruence modular;
- by the same reason the variety $\mathcal{D}$ of distributive lattices is realized as $\mathrm{Con}(\mathcal{V})$ by any congruence distributive variety $\mathcal{V}$;

Modular Congruence Varieties

- since modularity is a lattice equation a congruence variety $\mathrm{Con}(\mathcal{V})$ is modular if and only if $\mathcal{V}$ is congruence modular;
- by the same reason the variety $\mathcal{D}$ of distributive lattices is realized as $\mathrm{Con}(\mathcal{V})$ by any congruence distributive variety $\mathcal{V}$;
- not every modular variety of lattices is a congruence variety [Nation 1974];

Modular Congruence Varieties

- since modularity is a lattice equation a congruence variety $\mathrm{Con}(\mathcal{V})$ is modular if and only if $\mathcal{V}$ is congruence modular;
- by the same reason the variety $\mathcal{D}$ of distributive lattices is realized as $\mathrm{Con}(\mathcal{V})$ by any congruence distributive variety $\mathcal{V}$;
- not every modular variety of lattices is a congruence variety [Nation 1974];
- the minimal non distributive modular congruence varieties are of the form $\mathrm{Con}(\mathcal{M}_{\mathbf{F}})$, where $\mathcal{M}_{\mathbf{F}}$ is the variety of modules over a field $\mathbf{F}$ of characteristic zero or prime [Czedli-Hutchinson 1978].

The problem

- we know that the variety of modular lattices is not a congruence variety;

The problem

- we know that the variety of modular lattices is not a congruence variety;
- in fact every congruence lattice in a congruence modular variety is *arguesian* [Freese-Jónnson 1976] and there are modular non arguesian lattices;

The problem

- we know that the variety of modular lattices is not a congruence variety;
- in fact every congruence lattice in a congruence modular variety is *arguesian* [Freese-Jónnson 1976] and there are modular non arguesian lattices;
- hence the problem: **is there a largest proper modular congruence variety?**

The problem

- we know that the variety of modular lattices is not a congruence variety;
- in fact every congruence lattice in a congruence modular variety is *arguesian* [Freese-Jónnson 1976] and there are modular non arguesian lattices;
- hence the problem: **is there a largest proper modular congruence variety?**
- the ideal candidate seems to be the congruence variety of groups.

The group case

- the operator Con cannot tell abelian from non abelian varieties of groups; in particular:

The group case

- the operator Con cannot tell abelian from non abelian varieties of groups; in particular:
- let $\mathcal{A}_n$ be the variety of abelian groups whose order divides n; if $\mathbf{G}$ is a finite group and all its Sylow p-subgroups are nilpotent of class $< p$, then $\mathrm{Con}(\boldsymbol{V}(\mathbf{G})) = \mathrm{Con}(\mathcal{A}_n)$ for some n [Burns-Oates Williams ca 1992];

The group case

- the operator Con cannot tell abelian from non abelian varieties of groups; in particular:
- let $\mathcal{A}_n$ be the variety of abelian groups whose order divides n; if $\mathbf{G}$ is a finite group and all its Sylow p-subgroups are nilpotent of class $< p$, then $\mathrm{Con}(\boldsymbol{V}(\mathbf{G})) = \mathrm{Con}(\mathcal{A}_n)$ for some n [Burns-Oates Williams ca 1992];
- however the congruence variety of groups is strictly larger than the congruence variety of abelian groups: there is a lattice equation holding in any subgroup lattice of an abelian group that does not hold in the lattice of normal subgroups of a certain non abelian group [Pálfy-Szabó 1995];

The group case

- the operator Con cannot tell abelian from non abelian varieties of groups; in particular:
- let $\mathcal{A}_n$ be the variety of abelian groups whose order divides n; if $\mathbf{G}$ is a finite group and all its Sylow p-subgroups are nilpotent of class $< p$, then $\mathrm{Con}(\boldsymbol{V}(\mathbf{G})) = \mathrm{Con}(\mathcal{A}_n)$ for some n [Burns-Oates Williams ca 1992];
- however the congruence variety of groups is strictly larger than the congruence variety of abelian groups: there is a lattice equation holding in any subgroup lattice of an abelian group that does not hold in the lattice of normal subgroups of a certain non abelian group [Pálfy-Szabó 1995];
- in fact the smallest example possible works; if $\mathbf{Q}_8$ is the quaternion group (a 2-group of class 2) then the lattice equation above does not hold in $\mathrm{Con}(\boldsymbol{V}(\mathbf{Q}_8))$.

Loops

- A **loop** $\langle A, \cdot, \backslash, /, 1\rangle$ is an algebra of type $\langle 2, 2, 2, 0\rangle$ such that for all $a, b \in A$

$$b = a(a\backslash b) = a\backslash(ab) = (b/a)a = b/(ab) \qquad a1 = 1a = a.$$

Loops

- A **loop** $\langle A, \cdot, \backslash, /, 1\rangle$ is an algebra of type $\langle 2, 2, 2, 0\rangle$ such that for all $a, b \in A$

$$b = a(a\backslash b) = a\backslash(ab) = (b/a)a = b/(ab) \qquad a1 = 1a = a.$$

- Every group is a loop, by defining $a\backslash b = a^{-1}b$ e $a/b = ab^{-1}$, but in general the binary multiplication is not associative.

Loops

- A **loop** $\langle A, \cdot, \backslash, /, 1\rangle$ is an algebra of type $\langle 2, 2, 2, 0\rangle$ such that for all $a, b \in A$

$$b = a(a\backslash b) = a\backslash(ab) = (b/a)a = b/(ab) \qquad a1 = 1a = a.$$

- Every group is a loop, by defining $a\backslash b = a^{-1}b$ e $a/b = ab^{-1}$, but in general the binary multiplication is not associative.
- The integers $\mathbb{Z}$ form a (commutative) loop $\langle \mathbb{Z}, -, /, 0\rangle$ (with binary subtraction)

Loops

- A **loop** $\langle A, \cdot, \backslash, /, 1\rangle$ is an algebra of type $\langle 2, 2, 2, 0\rangle$ such that for all $a, b \in A$

$$b = a(a\backslash b) = a\backslash(ab) = (b/a)a = b/(ab) \qquad a1 = 1a = a.$$

- Every group is a loop, by defining $a\backslash b = a^{-1}b$ e $a/b = ab^{-1}$, but in general the binary multiplication is not associative.
- The integers $\mathbb{Z}$ form a (commutative) loop $\langle \mathbb{Z}, -, /, 0\rangle$ (with binary subtraction)
- a binar wiht identity **A** is a loop iff for all $a, b \in A$ the equations $ax = b$, $ya = b$ have a unique solution.

Loops

- A **loop** $\langle A, \cdot, \backslash, /, 1\rangle$ is an algebra of type $\langle 2, 2, 2, 0\rangle$ such that for all $a, b \in A$

$$b = a(a\backslash b) = a\backslash(ab) = (b/a)a = b/(ab) \qquad a1 = 1a = a.$$

- Every group is a loop, by defining $a\backslash b = a^{-1}b$ e $a/b = ab^{-1}$, but in general the binary multiplication is not associative.
- The integers $\mathbb{Z}$ form a (commutative) loop $\langle \mathbb{Z}, -, /, 0\rangle$ (with binary subtraction)
- a binar wiht identity **A** is a loop iff for all $a, b \in A$ the equations $ax = b$, $ya = b$ have a unique solution.
- a finite binar with identity **A** is a loop iff its multiplication table is a latin square.

Why Loops?

- Loops are congruence permutable and congruence point regular at 1, so the have a *good theory of ideals* (in the sense of Agliano-Ursini).

Why Loops?

- Loops are congruence permutable and congruence point regular at 1, so the have a *good theory of ideals* (in the sense of Agliano-Ursini).
- Loops have a *decent* commutator theory.

Why Loops?

- Loops are congruence permutable and congruence point regular at 1, so the have a *good theory of ideals* (in the sense of Agliano-Ursini).
- Loops have a *decent* commutator theory.
- A loop is a group if and only if the multiplication is associative; hence the variety $\mathcal{G}$ of groups is properly contained in the variety $\mathcal{L}o$ of loops and $\mathrm{Con}(\mathcal{G}) \subseteq \mathrm{Con}(\mathcal{L}o)$.

Normal Subloops

- a subloop **N** of **A** is **normal** in **A** ($\mathbf{N} \lhd \mathbf{A}$) if for all $a, b \in A$

$$aN = Na \qquad a(bN) = (ab)N \qquad (Na)b = N(ab).$$

Normal Subloops

- a subloop **N** of **A** is **normal** in **A** ($\mathbf{N} \lhd \mathbf{A}$) if for all $a, b \in A$

$$aN = Na \qquad a(bN) = (ab)N \qquad (Na)b = N(ab).$$

- normal subloops form an algebraic lattice $\mathrm{N}(\mathbf{A})$ for the usual reasons;

Normal Subloops

- a subloop **N** of **A** is **normal** in **A** ($\mathbf{N} \lhd \mathbf{A}$) if for all $a, b \in A$

$$aN = Na \qquad a(bN) = (ab)N \qquad (Na)b = N(ab).$$

- normal subloops form an algebraic lattice $\mathrm{N}(\mathbf{A})$ for the usual reasons;
- moreover congruence permutability and regularity at 1 give the usual direct Galois Correspondence between $\mathrm{Con}(\mathbf{A})$ and $\mathrm{N}(\mathbf{A})$, that is in fact a lattice isomorphism:

$$\alpha \longmapsto 1/\alpha \qquad \mathbf{N} \longmapsto \theta_N = \{(a, b) : a\backslash b \in N\}$$

The Commutator

- Since loops are congruence permutable, they have the best possible commutator theory for congruences;

The Commutator

- Since loops are congruence permutable, they have the best possible commutator theory for congruences;
- And we can use the Galois Correspondence to define the commutator of normal subloops; if $\mathbf{N}, \mathbf{M} \lhd \mathbf{A}$

$$[\mathbf{N}, \mathbf{M}]_{\mathbf{A}} = 1/[\theta_N, \theta_M]$$

The Commutator

- Since loops are congruence permutable, they have the best possible commutator theory for congruences;
- And we can use the Galois Correspondence to define the commutator of normal subloops; if $\mathbf{N}, \mathbf{M} \lhd \mathbf{A}$

$$[\mathbf{N}, \mathbf{M}]_{\mathbf{A}} = 1/[\theta_N, \theta_M]$$

- alternatively we can use the general theory of ideal-determined varieties, define the commutator of subloops via terms and prove that it is exactly as above.

Bad news

- the fact that you can define formally the commutator as in groups, hides a significant difference;

Bad news

- the fact that you can define formally the commutator as in groups, hides a significant difference;
- in fact the commutator of two subgroups is an *absolute* concept in that it does not depend on the group of which they are subgroups;

Bad news

- the fact that you can define formally the commutator as in groups, hides a significant difference;
- in fact the commutator of two subgroups is an *absolute* concept in that it does not depend on the group of which they are subgroups;
- in loops this is not the case, so when we write $[\mathbf{N}, \mathbf{M}]_{\mathbf{A}}$, the decoration "$\mathbf{A}$" is necessary.

Bad news

- the fact that you can define formally the commutator as in groups, hides a significant difference;
- in fact the commutator of two subgroups is an *absolute* concept in that it does not depend on the group of which they are subgroups;
- in loops this is not the case, so when we write $[\mathbf{N}, \mathbf{M}]_{\mathbf{A}}$, the decoration "$\mathbf{A}$" is necessary.
- This has consequence if we want to define abelianity and solvability *as in groups*.

The center

- If we choose commutator theory for congruences as our framework then

The center

- If we choose commutator theory for congruences as our framework then
- the **center** of a loop $\mathbf{A}$ is the largest congruence $\zeta_{\mathbf{A}}$ such that $[\zeta_{\mathbf{A}}, 1_{\mathbf{A}}] = 0_{\mathbf{A}}$,

The center

- If we choose commutator theory for congruences as our framework then
- the **center** of a loop $\mathbf{A}$ is the largest congruence $\zeta_{\mathbf{A}}$ such that $[\zeta_{\mathbf{A}}, 1_{\mathbf{A}}] = 0_{\mathbf{A}}$,
- i.e. the largest congruence $\zeta_{\mathbf{A}}$ such that $\mathbf{A}/\zeta_{\mathbf{A}}$ is abelian (in the congruence sense).

The center

- If we choose commutator theory for congruences as our framework then
- the **center** of a loop $\mathbf{A}$ is the largest congruence $\zeta_{\mathbf{A}}$ such that $[\zeta_{\mathbf{A}}, 1_{\mathbf{A}}] = 0_{\mathbf{A}}$,
- i.e. the largest congruence $\zeta_{\mathbf{A}}$ such that $\mathbf{A}/\zeta_{\mathbf{A}}$ is abelian (in the congruence sense).
- if $\zeta(\mathbf{A})$ is the normal subloop corresponding to $\zeta_{\mathbf{A}}$, we call it the **center** as well and

$$\zeta(\mathbf{A}) = \{a : \text{per ogni } b, c \in A \; ab = ba, (ba)c = b(ac), \\ (ab)c = a(bc), (bc)a = b(ca)\}$$

The center

- If we choose commutator theory for congruences as our framework then
- the **center** of a loop $\mathbf{A}$ is the largest congruence $\zeta_{\mathbf{A}}$ such that $[\zeta_{\mathbf{A}}, 1_{\mathbf{A}}] = 0_{\mathbf{A}}$,
- i.e. the largest congruence $\zeta_{\mathbf{A}}$ such that $\mathbf{A}/\zeta_{\mathbf{A}}$ is abelian (in the congruence sense).
- if $\zeta(\mathbf{A})$ is the normal subloop corresponding to $\zeta_{\mathbf{A}}$, we call it the **center** as well and

$$\zeta(\mathbf{A}) = \{a : \text{per ogni } b, c \in A \; ab = ba, (ba)c = b(ac), \\ (ab)c = a(bc), (bc)a = b(ca)\}$$

- so an abelian loop is in fact an abelian group and everything works fine....

Two ways of being abelian

- however when we go to the commutator of subloops we start seeing the problem;

Two ways of being abelian

- however when we go to the commutator of subloops we start seeing the problem;
- in fact if $\mathbf{N} \lhd \mathbf{A}$, then $\mathbf{N}$ is abelian if $\zeta(\mathbf{N}) = \mathbf{N}$;

Two ways of being abelian

- however when we go to the commutator of subloops we start seeing the problem;
- in fact if $\mathbf{N} \lhd \mathbf{A}$, then $\mathbf{N}$ is abelian if $\zeta(\mathbf{N}) = \mathbf{N}$;
- however $[\mathbf{N}, \mathbf{N}]_{\mathbf{A}} = \{1\}$ if and only if $[\theta_N, \theta_N] = 0_{\mathbf{A}}$.

Two ways of being abelian

- however when we go to the commutator of subloops we start seeing the problem;
- in fact if $\mathbf{N} \lhd \mathbf{A}$, then $\mathbf{N}$ is abelian if $\zeta(\mathbf{N}) = \mathbf{N}$;
- however $[\mathbf{N}, \mathbf{N}]_{\mathbf{A}} = \{1\}$ if and only if $[\theta_N, \theta_N] = 0_{\mathbf{A}}$.
- this appears to be a different definition and it is easy to understand how it can create problems if we want to define abelianity and solvability in a "classical" way.

It really happens...

- in their monograph *Commutator Theory for Congruence Modular Varieties* R. Freese and R. McKenzie produced an example of a 16-element loop, having a normal abelian subloop $\mathbf{N}$ with $[\theta_N, \theta_N] \neq 0_{\mathbf{A}}$;

It really happens...

- in their monograph *Commutator Theory for Congruence Modular Varieties* R. Freese and R. McKenzie produced an example of a 16-element loop, having a normal abelian subloop $\mathbf{N}$ with $[\theta_N, \theta_N] \neq 0_{\mathbf{A}}$;
- recently D. Stanovskỳ and P. Vojtechowskỳ found a way to construct a class of examples satisfying Murphy's Law (anything that can go wrong, will go wrong...)

Good news: nilpotency works!

Lemma

For a loop $\mathbf{A}$ *the following are equivalent:*

1. $\mathbf{A}$ *is nilpotent (in the congruence sense);*
2. $\mathbf{A}$ *has a* central series, *i.e. there are subloops* $\mathbf{N}_0, \dots, \mathbf{N}_k$ *such that*

$$\{1\} = \mathbf{N}_0 \lhd \mathbf{N}_1 \lhd \dots \lhd \mathbf{N}_k = \mathbf{A}$$

   and $[\mathbf{A}, \mathbf{N}_{i+1}]_{\mathbf{A}} \leq \mathbf{N}_i$*;*
3. *there are* $\alpha_0, \dots, \alpha_k \in \mathrm{Con}(\mathbf{A})$ *with*

$$0_{\mathbf{A}} = \alpha_0 \leq \alpha_1 \leq \dots \leq \alpha_k = 1_{\mathbf{A}}$$

   such that $\alpha_{i+1}/\alpha_i \leq \zeta_{\mathbf{A}/\alpha_i}$.

Possible tools

Besides nilpotency the main tool used by R. Burns and S. Oates-Williams in their investigation is the following lemma, traditionally credited to P. Neumann

Lemma

For every finite group $\mathbf{G}$

1. *if* $\mathbf{G} \cong \mathbf{K} \times \mathbf{H}$ *and the orders of* $\mathbf{K}$ *and* $\mathbf{H}$ *are relatively prime, then*
$$\mathrm{N}(\mathbf{G}) \cong \mathrm{N}(\mathbf{K}) \times \mathrm{N}(\mathbf{H});$$
2. *if* $p_1, \ldots, p_n$ *are the distinct prime factors of the order of* $\mathbf{G}$ *and* $\mathbf{P}_1, \ldots, \mathbf{P}_n$ *are the associated Sylow p-subgroups, then the mapping*
$$N \longmapsto (N \cap P_1) \times \cdots \times (N \cap P_n)$$
is a monomorphism from $\mathrm{N}(\mathbf{G}) \longmapsto \mathrm{N}(\mathbf{P}_1) \times \cdots \times \mathrm{N}(\mathbf{P}_n)$.

Let's compare Neumann's Lemma with this result by D. Hobby and R. McKenzie

Theorem

Let $\mathbf{A}$ *be a finite algebra such that* $V(\mathbf{A})$ *is congruence modular. Then there are finite algebras* $\mathbf{B}, \mathbf{B}_1, \ldots, \mathbf{B}_n$ *such that*

- $\mathbf{B}, \mathbf{B}_1, \ldots, \mathbf{B}_n$ *are* loops with operators*;*
- $\mathbf{B}, \mathbf{B}_1, \ldots, \mathbf{B}_n$ *are nilpotent;*
- $\mathbf{B}, \mathbf{B}_1, \ldots, \mathbf{B}_n$ *are E-minimal;*
- $\mathrm{Con}(\mathbf{A}) \cong \mathrm{Con}(\mathbf{B}) \overset{sp}{\hookrightarrow} \prod_{i=1}^{n} \mathbf{B}_i$

A finite algebra $\mathbf{A}$ is *E*-**minimal** if the only unary non constant idempotent polynomial of $\mathbf{A}$ is the identity.

Final remarks

This is a (hard) exercise in Hobby-McKenzie's monograph

Lemma

Every finite p-group is E-minimal.

This in my opinion gives a very good reason to study E-minimal loops and p-loops in general. For instance there is an extensive theory on Moufang p-loops. Do they coincide with E-minimal Moufang loops? What can we say by applying Hobby-McKenzie's Lemma to this situation? Can we extract meaningful information about congruence varieties of loops? More to the point: is the congruence variety of loops equal to the congruence variety of groups?