Multiplicative lattices, groups, braces

Alberto Facchini
Università di Padova, Italy

Online Satellite Event to
Homological Methods in Representation Theory

A conference in honour of Lidia Angeleri Hügel

23 February 2022

From Lidia

From Lidia

Homological Methods $\mapsto$ a homological notion I have learnt from Lidia.

From Lidia

Homological Methods $\mapsto$ a homological notion I have learnt from Lidia.

[L. Angeleri Hügel and J. Sánchez, Tilting modules arising from ring epimorphisms, Algebr. Represent. Theory **14** (2011), 217–246]

From Lidia

Homological Methods $\mapsto$ a homological notion I have learnt from Lidia.

[L. Angeleri Hügel and J. Sánchez, Tilting modules arising from ring epimorphisms, Algebr. Represent. Theory **14** (2011), 217–246]

"We will mainly deal with injective ring epimorphisms which in addition satisfy the following homological property studied by Geigle and Lenzing in 1991:

Let R, S be two rings and $\lambda\colon R \to S$ a ring epimorphism. Then λ is a homological ring epimorphism if $\mathrm{Tor}_i^R(S, S) = 0$ for all $i > 0$.

We will see that in our context it is enough to require that $\mathrm{Tor}_1^R(S, S) = 0$."

From Lidia

On 14 July 2016 Fuchs gave a conference in Padova,
"When weak-injective modules admit canonical decompositions."

From Lidia

On 14 July 2016 Fuchs gave a conference in Padova,
"When weak-injective modules admit canonical decompositions."

[Fuchs and Salce, Almost perfect commutative rings, J. Pure Appl. Algebra **222**(12) (2018), 4223–4238].

From Lidia

On 14 July 2016 Fuchs gave a conference in Padova,
"When weak-injective modules admit canonical decompositions."

[Fuchs and Salce, Almost perfect commutative rings, J. Pure Appl. Algebra **222**(12) (2018), 4223–4238].

Equivalence of nine homological conditions.

From Lidia

Do it in for non-commutative rings! (July 2016)

From Lidia

Do it in for non-commutative rings! (July 2016)

At the beginning of Spring 2017 Zahra Nazemian and I began to work on it.

From Lidia

Do it in for non-commutative rings! (July 2016)

At the beginning of Spring 2017 Zahra Nazemian and I began to work on it.

In June 2017 we discovered that Lidia and Javier's injective ring epimorphisms $R \to S$ $+ \mathrm{Tor}_1^R(S, S) = 0$ was the right class of "ring extensions" to consider, they yield the correct setting to make a lot of things work. In Erice (July 2017), we adapted the paper to that setting. Under some further hypotheses, we also proved the existence a category equivalence similar to Matlis' one.

On 20 September 2017 we submitted our paper:

From Lidia

Do it in for non-commutative rings! (July 2016)

At the beginning of Spring 2017 Zahra Nazemian and I began to work on it.

In June 2017 we discovered that Lidia and Javier's injective ring epimorphisms $R \to S \ + \mathrm{Tor}_1^R(S,S) = 0$ was the right class of "ring extensions" to consider, they yield the correct setting to make a lot of things work. In Erice (July 2017), we adapted the paper to that setting. Under some further hypotheses, we also proved the existence a category equivalence similar to Matlis' one.

On 20 September 2017 we submitted our paper:
[Facchini and Nazemian, Equivalence of some homological conditions for ring epimorphism, J. Pure Appl. Algebra 223 (2019), no. 4, 1440–1455.]

From Lidia

That condition "injective ring epimorphisms $+\mathrm{Tor}_1^R(S,S)=0$" was later weakened by Leonid and Silvana to "ring epimorphisms $+\mathrm{Tor}_1^R(S,S)=0$" in their wonderful paper [Bazzoni and Positselski, Matlis category equivalences for a ring epimorphism, J. Pure Appl. Algebra 224 (2020), 106398], submitted in March 2020, using Lidia's idea, which we had developed.

From Lidia

That condition "injective ring epimorphisms $+\mathrm{Tor}_1^R(S,S) = 0$" was later weakened by Leonid and Silvana to "ring epimorphisms $+\mathrm{Tor}_1^R(S,S) = 0$" in their wonderful paper [Bazzoni and Positselski, Matlis category equivalences for a ring epimorphism, J. Pure Appl. Algebra 224 (2020), 106398], submitted in March 2020, using Lidia's idea, which we had developed.

This is a fruitful line of ideas originated in Lidia's work.

Now, for this talk, a different topic: multiplicative lattices

A *multiplicative lattice* is a complete lattice L equipped with a further binary operation $\cdot : L \times L \to L$ (multiplication) satisfying $x \cdot y \leq x \wedge y$ for all $x, y \in L$.

Now, for this talk, a different topic: multiplicative lattices

A *multiplicative lattice* is a complete lattice L equipped with a further binary operation $\cdot : L \times L \to L$ (multiplication) satisfying $x \cdot y \leq x \wedge y$ for all $x, y \in L$.

(No associativity, commutativity, identities, distributivity required.)

Two natural examples

Groups, rings $\mapsto$ the lattice of all normal subgroups, the lattice of all two-sided ideals.

Two natural examples

Groups, rings $\mapsto$ the lattice of all normal subgroups, the lattice of all two-sided ideals.

But these lattices are not sufficient to describe and explain several situations.

Two natural examples

Groups, rings $\mapsto$ the lattice of all normal subgroups, the lattice of all two-sided ideals.

But these lattices are not sufficient to describe and explain several situations. A product is necessary: the commutator $[N, M]$ of two normal subgroups, the product IJ of two ideals of a ring.

Two natural examples

Groups, rings $\mapsto$ the lattice of all normal subgroups, the lattice of all two-sided ideals.

But these lattices are not sufficient to describe and explain several situations. A product is necessary: the commutator $[N, M]$ of two normal subgroups, the product IJ of two ideals of a ring.

Hence we need a lattice $+$ a multiplication.

A non-associative multiplication!

Unlucky the multiplication is often not even associative (for normal subgroups $[M, [N, P]]$ can be different from $[[M, N], P]$.

A non-associative multiplication!

Unlucky the multiplication is often not even associative (for normal subgroups $[M, [N, P]]$ can be different from $[[M, N], P]$.

For instance, S_3 is solvable but not nilpotent.

A non-associative multiplication!

Unlucky the multiplication is often not even associative (for normal subgroups $[M, [N, P]]$ can be different from $[[M, N], P]$.

For instance, S_3 is solvable but not nilpotent. Calculations are easy, because S_3 has only three normal subgroups: S_3, A_3 and 1.

A non-associative multiplication!

Unlucky the multiplication is often not even associative (for normal subgroups $[M, [N, P]]$ can be different from $[[M, N], P]$.

For instance, S_3 is solvable but not nilpotent. Calculations are easy, because S_3 has only three normal subgroups: S_3, A_3 and 1. S_3 is solvable because $[S_3, S_3] = A_3 \cong \mathbb{Z}/3\mathbb{Z}$,

A non-associative multiplication!

Unlucky the multiplication is often not even associative (for normal subgroups $[M, [N, P]]$ can be different from $[[M, N], P]$.

For instance, S_3 is solvable but not nilpotent. Calculations are easy, because S_3 has only three normal subgroups: S_3, A_3 and 1. S_3 is solvable because $[S_3, S_3] = A_3 \cong \mathbb{Z}/3\mathbb{Z}$, but is not nilpotent because $[S_3, A_3] = A_3$. Hence

$$[A_3, [S_3, S_3]] = [A_3, A_3] = 1,$$

but

$$[[A_3, S_3], S_3] = A_3.$$

(1) Alberto Facchini, Carmelo Finocchiaro (Università di Catania, Italy) and George Janelidze (University of Cape Town, South Africa), “Abstractly constructed prime spectra”, Algebra Universalis 83(1) (February 2022)

(1) Alberto Facchini, Carmelo Finocchiaro (Università di Catania, Italy) and George Janelidze (University of Cape Town, South Africa), "Abstractly constructed prime spectra", Algebra Universalis 83(1) (February 2022)

(2) Alberto Facchini, Francesco de Giovanni and Marco Trombetti (Università di Napoli, Italy), "Spectra of groups", submitted for publication, 2021.

(1) Alberto Facchini, Carmelo Finocchiaro (Università di Catania, Italy) and George Janelidze (University of Cape Town, South Africa), “Abstractly constructed prime spectra”, Algebra Universalis 83(1) (February 2022)

(2) Alberto Facchini, Francesco de Giovanni and Marco Trombetti (Università di Napoli, Italy), “Spectra of groups”, submitted for publication, 2021.

(3) Alberto Facchini, “Algebraic structures from the point of view of complete multiplicative lattices”, submitted for publication, 2021, arXiv:2201.03295 .

(1) Alberto Facchini, Carmelo Finocchiaro (Università di Catania, Italy) and George Janelidze (University of Cape Town, South Africa), “Abstractly constructed prime spectra”, Algebra Universalis 83(1) (February 2022)

(2) Alberto Facchini, Francesco de Giovanni and Marco Trombetti (Università di Napoli, Italy), “Spectra of groups”, submitted for publication, 2021.

(3) Alberto Facchini, “Algebraic structures from the point of view of complete multiplicative lattices”, submitted for publication, 2021, arXiv:2201.03295 .

+ work in progress with Mara Pompili.

Multiplicative lattices

Multiplicative lattices are an algebraic structure to which little attention has been devoted, but which already appears in Krull (1924!), and has been studied by M. Ward (1937), Ward and R.P. Dilworth (1937), D.D. Anderson (1974), E.W. Johnson and J.A. Johnson (1970), Hofmann and Keimel (1978), quantales, frames, locales, . . .

Multiplicative lattices

Multiplicative lattices are an algebraic structure to which little attention has been devoted, but which already appears in Krull (1924!), and has been studied by M. Ward (1937), Ward and R.P. Dilworth (1937), D.D. Anderson (1974), E.W. Johnson and J.A. Johnson (1970), Hofmann and Keimel (1978), quantales, frames, locales, . . .

In all these papers, further axioms are required: associativity or commutativity of multiplication, distributivity with $\vee$, identity, compatibility of multiplication and partial order, the multiplication is the meet, . . .

Spectra of rings, of distributive lattices,...

R any commutative ring with identity $\quad \mapsto \quad \mathrm{Spec}(R)$.

Spectra of rings, of distributive lattices,...

R any commutative ring with identity $\quad \mapsto \quad \mathrm{Spec}(R)$.
This is a spectral topological space

Spectra of rings, of distributive lattices,. . .

R any commutative ring with identity $\quad \mapsto \quad \mathrm{Spec}(R)$.
This is a spectral topological space (= sober, compact, the intersection of two compact open sets is compact, and the compact opens form a basis for the topology).

Spectra of rings, of distributive lattices,...

R any commutative ring with identity $\quad\mapsto\quad \mathrm{Spec}(R)$.
This is a spectral topological space (= sober, compact, the intersection of two compact open sets is compact, and the compact opens form a basis for the topology).

Any bounded distributive lattice $L \quad\mapsto\quad \mathrm{Spec}(L)$. This is also a spectral topological space

Spectra of rings, of distributive lattices,...

R any commutative ring with identity $\quad \mapsto \quad \mathrm{Spec}(R)$.
This is a spectral topological space (= sober, compact, the intersection of two compact open sets is compact, and the compact opens form a basis for the topology).

Any bounded distributive lattice $L \quad \mapsto \quad \mathrm{Spec}(L)$. This is also a spectral topological space (Stone spectrum of the distributive lattice).

Spectra of rings, of distributive lattices,. . .

R any commutative ring with identity $\quad\mapsto\quad \mathrm{Spec}(R)$.
This is a spectral topological space (= sober, compact, the intersection of two compact open sets is compact, and the compact opens form a basis for the topology).

Any bounded distributive lattice $L \quad\mapsto\quad \mathrm{Spec}(L)$. This is also a spectral topological space (Stone spectrum of the distributive lattice).

Commutative semiring with identity $\quad\mapsto\quad$ spectral space.

Spectra of rings, of distributive lattices,...

R any commutative ring with identity $\quad\mapsto\quad \mathrm{Spec}(R)$.
This is a spectral topological space (= sober, compact, the intersection of two compact open sets is compact, and the compact opens form a basis for the topology).

Any bounded distributive lattice $L \quad\mapsto\quad \mathrm{Spec}(L)$. This is also a spectral topological space (Stone spectrum of the distributive lattice).

Commutative semiring with identity $\quad\mapsto\quad$ spectral space.

Commutative C^*-algebra $\quad\mapsto\quad$ spectral space

Spectra of rings, of distributive lattices,...

R any commutative ring with identity $\quad \mapsto \quad \mathrm{Spec}(R)$. This is a spectral topological space (= sober, compact, the intersection of two compact open sets is compact, and the compact opens form a basis for the topology).

Any bounded distributive lattice $L \quad \mapsto \quad \mathrm{Spec}(L)$. This is also a spectral topological space (Stone spectrum of the distributive lattice).

Commutative semiring with identity $\quad \mapsto \quad$ spectral space.

Commutative C^*-algebra $\quad \mapsto \quad$ spectral space (Gelfand spectrum).

Spectra of rings, of distributive lattices,...

R any commutative ring with identity $\quad \mapsto \quad \mathrm{Spec}(R)$.
This is a spectral topological space (= sober, compact, the intersection of two compact open sets is compact, and the compact opens form a basis for the topology).

Any bounded distributive lattice $L \quad \mapsto \quad \mathrm{Spec}(L)$. This is also a spectral topological space (Stone spectrum of the distributive lattice).

Commutative semiring with identity $\quad \mapsto \quad$ spectral space.

Commutative C^*-algebra $\quad \mapsto \quad$ spectral space (Gelfand spectrum).

Commutative monoids, abelian ℓ-groups, prime spectrum of an MV-algebra, Hofmann-Lawson spectrum of a continuous lattice, Zariski-Riemann spaces,...

On the ubiquity of spectral spaces

On the ubiquity of spectral spaces

Always these strange, particular spaces,...

On the ubiquity of spectral spaces

Always these strange, particular spaces,...

Sometimes a little less:

On the ubiquity of spectral spaces

Always these strange, particular spaces,...

Sometimes a little less:

Commutative rings without identity $\mapsto$ an open subset of a spectral space [Acosta-Rubio].

On the ubiquity of spectral spaces

Always these strange, particular spaces,...

Sometimes a little less:

Commutative rings without identity $\mapsto$ an open subset of a spectral space [Acosta-Rubio].

Noncommutative rings with identity $\mapsto$ "almost a spectral space" (it is compact and sober, but the intersection of two compact open sets is not necessarily compact, and the "open sets $U(f)$" are not always compact.)

On the ubiquity of spectral spaces

Always these strange, particular spaces,...

Sometimes a little less:

Commutative rings without identity $\mapsto$ an open subset of a spectral space [Acosta-Rubio].

Noncommutative rings with identity $\mapsto$ "almost a spectral space" (it is compact and sober, but the intersection of two compact open sets is not necessarily compact, and the "open sets $U(f)$" are not always compact.)

Why are spectra and spectral spaces so frequent in Algebra? Any deep reason? Motivation?

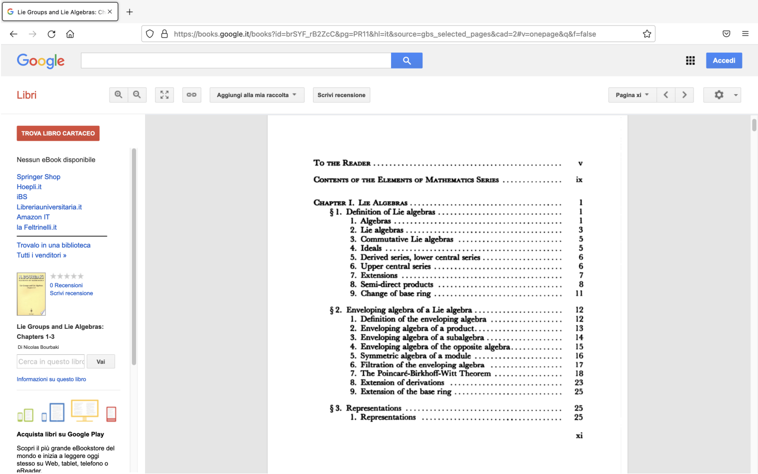
The answer is in multiplicative lattices.

In all the previous examples, there is a multiplicative lattice around:
For commutative rings: the lattice of its ideal with multiplication of ideals.
For noncommutative rings: the lattice of its two-sided ideal with multiplication of ideals, or $IJ + JI$ as a product, if you prefer.
For groups: the modular lattice of its normal subgroups with commutator of two normal subgroups.
For lattices: the lattice itself with multiplication $xy := x \wedge y$, or the lattice of its ideals.

A second motivation

If you take any standard text of Lie algebras, for instance the one by Bourbaki, you find these contents:

Lie Groups and Lie Algebras, Chapter 1, Bourbaki



xi

Why is the beginning of a course of Lie algebras so similar to the beginning of a course of groups?

Why is the beginning of a course of Lie algebras so similar to the beginning of a course of groups? The beginning of a course of elementary ring theory is completely different!

Why is the beginning of a course of Lie algebras so similar to the beginning of a course of groups? The beginning of a course of elementary ring theory is completely different! The motivation is that we study rings with identity.

Why is the beginning of a course of Lie algebras so similar to the beginning of a course of groups? The beginning of a course of elementary ring theory is completely different! The motivation is that we study rings with identity. Rngs (rings without identity) are much more similar to groups and Lie algebras.

Why is the beginning of a course of Lie algebras so similar to the beginning of a course of groups? The beginning of a course of elementary ring theory is completely different! The motivation is that we study rings with identity. Rngs (rings without identity) are much more similar to groups and Lie algebras. This is also explained well using multiplicative lattices.

A third motivation

The center of a group is a normal subgroup, and the center of a ring is a subring, not an ideal. This is very strange, in some sense it is not congruent.

A third motivation

The center of a group is a normal subgroup, and the center of a ring is a subring, not an ideal. This is very strange, in some sense it is not congruent. The answer again is in multiplicative lattices.

A third motivation

The center of a group is a normal subgroup, and the center of a ring is a subring, not an ideal. This is very strange, in some sense it is not congruent. The answer again is in multiplicative lattices. (They tell you simply that the names given are wrong. The (left) center of the ring R should have been defined as $\{ r \in R \mid rs = 0 \text{ for every } s \in R \}$, which is a two-sided ideal of R.)

A fourth motivation

The notions of solvable object (algebraic structure), nilpotent object, abelian object, idempotent objects, hyperabelian objects, find all their natural setting in multiplicative lattices.

A fourth motivation

The notions of solvable object (algebraic structure), nilpotent object, abelian object, idempotent objects, hyperabelian objects, find all their natural setting in multiplicative lattices. (And sometimes show that the names given are wrong.)

A multiplicative lattice L

For the rest of the talk, L will always be a complete multiplicative lattice, with 0 and 1.

A multiplicative lattice L

For the rest of the talk, L will always be a complete multiplicative lattice, with 0 and 1.

An element $p \neq 1$ is said to be *prime* if it satisfies the implication

$$xy \leq p \Rightarrow (x \leq p \text{ or } y \leq p).$$

Let $\mathrm{Spec}(L)$ be the set of all prime elements of L.

The mapping V

We have a mapping

$$\begin{aligned} V &: L \to \mathcal{P}(\mathrm{Spec}(L)) \\ V &: x \mapsto V(x) := \{\, p \in \mathrm{Spec}(L) \mid x \leq p \,\}. \end{aligned}$$

The mapping V

We have a mapping

$$V\colon L \to \mathcal{P}(\mathrm{Spec}(L))$$
$$V\colon x \mapsto V(x) := \{\, p \in \mathrm{Spec}(L) \mid x \leq p \,\}.$$

The mapping $V\colon L \to \mathcal{P}(\mathrm{Spec}(L))$ has the following properties:

The mapping V

(1) V transforms the multiplication in L into the union in $\mathcal{P}(\mathrm{Spec}(L))$, that is, V is a magma morphism of the magma $(L, \cdot)$ into the magma (the commutative monoid) $(\mathcal{P}(\mathrm{Spec}(L)), \cup)$:

$$V(xy) = V(x) \cup V(y) \qquad \text{for every } x, y \in L.$$

The mapping V

(1) V transforms the multiplication in L into the union in $\mathcal{P}(\mathrm{Spec}(L))$, that is, V is a magma morphism of the magma $(L, \cdot)$ into the magma (the commutative monoid) $(\mathcal{P}(\mathrm{Spec}(L)), \cup)$:

$$V(xy) = V(x) \cup V(y) \qquad \text{for every } x, y \in L.$$

(2) V transforms the $\vee$ in L into the intersection in $\mathcal{P}(\mathrm{Spec}(L))$ (more is true: it transforms an arbitrary $\bigvee$ in L into an arbitrary intersection in $\mathcal{P}(\mathrm{Spec}(L))$, even in the infinite case):

$$V(\bigvee_{i \in I} x_i) = \bigcap_{i \in I} V(x_i) \qquad \text{for every subset } \{\, x_i \mid i \in I \,\} \subseteq L.$$

The mapping V

(1) V transforms the multiplication in L into the union in $\mathcal{P}(\mathrm{Spec}(L))$, that is, V is a magma morphism of the magma $(L, \cdot)$ into the magma (the commutative monoid) $(\mathcal{P}(\mathrm{Spec}(L)), \cup)$:

$$V(xy) = V(x) \cup V(y) \qquad \text{for every } x, y \in L.$$

(2) V transforms the $\vee$ in L into the intersection in $\mathcal{P}(\mathrm{Spec}(L))$ (more is true: it transforms an arbitrary $\bigvee$ in L into an arbitrary intersection in $\mathcal{P}(\mathrm{Spec}(L))$, even in the infinite case):

$$V(\bigvee_{i \in I} x_i) = \bigcap_{i \in I} V(x_i) \qquad \text{for every subset } \{\, x_i \mid i \in I \,\} \subseteq L.$$

(3) The image $V(L)$ of the mapping V satisfies the axioms for the closed sets of a topology on $\mathrm{Spec}(L)$.

The mapping V

(1) V transforms the multiplication in L into the union in $\mathcal{P}(\mathrm{Spec}(L))$, that is, V is a magma morphism of the magma $(L, \cdot)$ into the magma (the commutative monoid) $(\mathcal{P}(\mathrm{Spec}(L)), \cup)$:

$$V(xy) = V(x) \cup V(y) \qquad \text{for every } x, y \in L.$$

(2) V transforms the $\vee$ in L into the intersection in $\mathcal{P}(\mathrm{Spec}(L))$ (more is true: it transforms an arbitrary $\bigvee$ in L into an arbitrary intersection in $\mathcal{P}(\mathrm{Spec}(L))$, even in the infinite case):

$$V(\bigvee_{i \in I} x_i) = \bigcap_{i \in I} V(x_i) \qquad \text{for every subset } \{\, x_i \mid i \in I \,\} \subseteq L.$$

(3) The image $V(L)$ of the mapping V satisfies the axioms for the closed sets of a topology on $\mathrm{Spec}(L)$.

$\mathrm{Spec}(L)$ with this topology is called the *Zariski spectrum* of L.

Always a sober space

Lemma

$\mathrm{Spec}(L)$ *is a sober space.*

The category MCL of multiplicative lattices

Objects: our multiplicative lattices. Morphisms?

The category MCL of multiplicative lattices

Objects: our multiplicative lattices. Morphisms?

Our multiplicative lattices are complete lattices, but it is better not to consider them complete lattices, but complete join-semilattices.

The category MCL of multiplicative lattices

Objects: our multiplicative lattices. Morphisms?

Our multiplicative lattices are complete lattices, but it is better not to consider them complete lattices, but complete join-semilattices. What is the difference between complete lattices and complete join-semilattices?

The category MCL of multiplicative lattices

Objects: our multiplicative lattices. Morphisms?

Our multiplicative lattices are complete lattices, but it is better not to consider them complete lattices, but complete join-semilattices. What is the difference between complete lattices and complete join-semilattices? None: a partially ordered set is a complete lattice if and only if it is a complete join-semilattice.

The category MCL of multiplicative lattices

Objects: our multiplicative lattices. Morphisms?

Our multiplicative lattices are complete lattices, but it is better not to consider them complete lattices, but complete join-semilattices. What is the difference between complete lattices and complete join-semilattices? None: a partially ordered set is a complete lattice if and only if it is a complete join-semilattice. They are exactly the same thing.

The category MCL of multiplicative lattices

Objects: our multiplicative lattices. Morphisms?

Our multiplicative lattices are complete lattices, but it is better not to consider them complete lattices, but complete join-semilattices. What is the difference between complete lattices and complete join-semilattices? None: a partially ordered set is a complete lattice if and only if it is a complete join-semilattice. They are exactly the same thing. But morphisms are different: if L and M are complete lattices, their morphisms as lattices are the mappings $f\colon L \to M$ such that $f(x \vee x') = f(x) \vee f(x')$ and $f(x \wedge x') = f(x) \wedge f(x')$ for every $x, x' \in L$,

The category MCL of multiplicative lattices

Objects: our multiplicative lattices. Morphisms?

Our multiplicative lattices are complete lattices, but it is better not to consider them complete lattices, but complete join-semilattices. What is the difference between complete lattices and complete join-semilattices? None: a partially ordered set is a complete lattice if and only if it is a complete join-semilattice. They are exactly the same thing. But morphisms are different: if L and M are complete lattices, their morphisms as lattices are the mappings $f\colon L \to M$ such that $f(x \vee x') = f(x) \vee f(x')$ and $f(x \wedge x') = f(x) \wedge f(x')$ for every $x, x' \in L$, and morphisms as complete join-semilattices are the mappings $f\colon L \to M$ such that $f(\bigvee X) = \bigvee f(X)$ for every subset $X \subseteq L$.

The category MCL of multiplicative lattices

Objects: our multiplicative lattices. Morphisms?

Our multiplicative lattices are complete lattices, but it is better not to consider them complete lattices, but complete join-semilattices. What is the difference between complete lattices and complete join-semilattices? None: a partially ordered set is a complete lattice if and only if it is a complete join-semilattice. They are exactly the same thing. But morphisms are different: if L and M are complete lattices, their morphisms as lattices are the mappings $f\colon L \to M$ such that $f(x \vee x') = f(x) \vee f(x')$ and $f(x \wedge x') = f(x) \wedge f(x')$ for every $x, x' \in L$, and morphisms as complete join-semilattices are the mappings $f\colon L \to M$ such that $f(\bigvee X) = \bigvee f(X)$ for every subset $X \subseteq L$.

In the category MCL of multiplicative lattices, whose objects are our complete multiplicative lattices $(L, \cdot)$, morphisms $L \to M$ are morphisms in the category of complete join-semilattices such that $f(x)f(x') \leq f(xx')$ for every $x, x' \in L$ and $f(1_L) = 1_M$.)

The category of multiplicative lattices

Proposition

There is a contravariant functor $\mathrm{Spec}\colon \mathsf{MCL} \to \mathsf{Top}$*.*

The category of multiplicative lattices

Proposition

There is a contravariant functor $\mathrm{Spec}\colon \mathsf{MCL} \to \mathsf{Top}$.

(For every morphism $(f, u)\colon L \to M$, one proves that $u(\mathrm{Spec}(M)) \subseteq \mathrm{Spec}(L)$, and the restriction of $u\colon M \to L$ to $\mathrm{Spec}(M) \to \mathrm{Spec}(L)$ is continuous.)

The category of multiplicative lattices

Proposition

There is a contravariant functor $\mathrm{Spec}\colon \mathsf{MCL} \to \mathsf{Top}$*.*

(For every morphism $(f, u)\colon L \to M$, one proves that $u(\mathrm{Spec}(M)) \subseteq \mathrm{Spec}(L)$, and the restriction of $u\colon M \to L$ to $\mathrm{Spec}(M) \to \mathrm{Spec}(L)$ is continuous.)

Proposition

There is a covariant functor $\mathsf{CommRings} \to \mathsf{MCL}$ *that associates to every commutative ring* R *with identity the multiplicative lattice* $\mathcal{L}(R)$ *of its ideals.*

The category of multiplicative lattices

Proposition

There is a contravariant functor $\mathrm{Spec}\colon \mathsf{MCL} \to \mathsf{Top}$.

(For every morphism $(f, u)\colon L \to M$, one proves that $u(\mathrm{Spec}(M)) \subseteq \mathrm{Spec}(L)$, and the restriction of $u\colon M \to L$ to $\mathrm{Spec}(M) \to \mathrm{Spec}(L)$ is continuous.)

Proposition

There is a covariant functor $\mathsf{CommRings} \to \mathsf{MCL}$ *that associates to every commutative ring* R *with identity the multiplicative lattice* $\mathcal{L}(R)$ *of its ideals.*

Clearly, the composite functor of the two functors

$$\mathsf{CommRings} \to \mathsf{MCL} \quad \text{and} \quad \mathrm{Spec}\colon \mathsf{MCL} \to \mathsf{Top}$$

is the usual contravariant functor Spec from the category of commutative rings with identity to the category Top of topological spaces.

Spec is a right adjoint

The functor $\mathrm{Spec}\colon \mathsf{MCL}^{\mathrm{op}} \to \{\,\text{sober spaces}\,\}$ is a right adjoint of the functor $\{\,\text{sober spaces}\,\} \to \mathsf{MCL}^{\mathrm{op}}$, that maps any sober space X to the complete lattice $\Omega(X)$ of its open subsets, with multiplication the intersection: $xy = x \wedge y$ for every $x, y \in \Omega(X)$.

An example: the case of groups

Let G be a group.

An example: the case of groups

Let G be a group. We can consider the multiplicative lattice $\mathcal{N}(G)$ of all normal subgroups of G.

An example: the case of groups

Let G be a group. We can consider the multiplicative lattice $\mathcal{N}(G)$ of all normal subgroups of G. The multiplication in this lattice is given by the *commutator operation*, i.e., the product of two normal subgroups A and B of G is the normal subgroup $[A, B]$.

An example: the case of groups

Let G be a group. We can consider the multiplicative lattice $\mathcal{N}(G)$ of all normal subgroups of G. The multiplication in this lattice is given by the *commutator operation*, i.e., the product of two normal subgroups A and B of G is the normal subgroup $[A, B]$.

The points of the *Zariski spectrum* $\mathrm{Spec}(G)$ of G are the *prime subgroups* of G, i.e. the prime elements of the multiplicative lattice $\mathcal{N}(G)$. Similarly, a normal subgroup of G is called *semiprime* if it is a semiprime element of $\mathcal{N}(G)$, that is, the meet (=the intersection) of a set of prime subgroups of G.

Prime subgroups, semiprime subgroups

Lemma

A subgroup N of G is a semiprime subgroup of G if and only if N is a normal subgroup of G and the factor group G/N has no abelian nontrivial normal subgroups.

Prime subgroups, semiprime subgroups

Lemma

A subgroup N of G is a semiprime subgroup of G if and only if N is a normal subgroup of G and the factor group G/N has no abelian nontrivial normal subgroups.

Lemma

Let N be a normal subgroup of a group G. Then N is prime in G if and only if N is semiprime in G and the factor group G/N is uniform (that is, the interval $[N, G]$ of the lattice $\mathcal{N}(G)$ is a uniform lattice).

Prime subgroups, semiprime subgroups

Lemma

A subgroup N of G is a semiprime subgroup of G if and only if N is a normal subgroup of G and the factor group G/N has no abelian nontrivial normal subgroups.

Lemma

Let N be a normal subgroup of a group G. Then N is prime in G if and only if N is semiprime in G and the factor group G/N is uniform (that is, the interval $[N, G]$ of the lattice $\mathcal{N}(G)$ is a uniform lattice).

The spectrum of a group G is endowed with the *Zariski topology*, in which the closed subsets are the sets $V(N) = \{P \in \mathrm{Spec}(G) \,:\, N \leq P\}$, $N \in \mathcal{N}(G)$. In such a way, $\mathrm{Spec}(G)$ becomes a sober topological space, which is not compact in general.

The first extreme case: "almost all" normal subgroups are prime.

Theorem

Let G be a group. Then all proper normal subgroups of G are prime if and only if the lattice $\mathcal{N}(G)$ is a chain and $H = H'$ for every normal subgroup H of G.

The first extreme case: "almost all" normal subgroups are prime.

Theorem

Let G be a group. Then all proper normal subgroups of G are prime if and only if the lattice $\mathcal{N}(G)$ is a chain and $H = H'$ for every normal subgroup H of G.
Moreover, in this case:

(a) *The topological space $\mathrm{Spec}(G)$ is sober, the intersection of two compact open sets is compact and the compact opens form a basis for the topology.*

The first extreme case: "almost all" normal subgroups are prime.

Theorem

Let G be a group. Then all proper normal subgroups of G are prime if and only if the lattice $\mathcal{N}(G)$ is a chain and $H = H'$ for every normal subgroup H of G.
Moreover, in this case:

(a) *The topological space $\mathrm{Spec}(G)$ is sober, the intersection of two compact open sets is compact and the compact opens form a basis for the topology.*

(b) *The topological space $\mathrm{Spec}(G)$ is spectral if and only if it is compact, if and only if G has a maximal normal subgroup.*

The other extreme case: no prime subgroups.

Recall that a *hyperabelian* group is a group which possesses an ascending (possibly transfinite) normal series where all the successive quotients are abelian.

The other extreme case: no prime subgroups.

Recall that a *hyperabelian* group is a group which possesses an ascending (possibly transfinite) normal series where all the successive quotients are abelian.

Theorem

A group G is hyperabelian if and only if $\mathrm{Spec}(G) = \emptyset$.

The other extreme case: no prime subgroups.

Recall that a *hyperabelian* group is a group which possesses an ascending (possibly transfinite) normal series where all the successive quotients are abelian.

Theorem

A group G is hyperabelian if and only if $\mathrm{Spec}(G) = \emptyset$.

The only ring with identity with empty spectrum is the zero ring. But for rings without identity there are several examples with empty spectrum, for instance all nil rings.

Direct product decomposition

For a commutative ring R there is a correspondence between ring direct product decompositions $R = R_1 \times R_2$, clopen subsets of $\mathrm{Spec}(R)$, and idempotents of the ring R. For instance, $\mathrm{Spec}(R_1 \times R_2)$ is homeomorphic to the disjoint union $\mathrm{Spec}(R_1) \dot{\cup} \mathrm{Spec}(R_2)$ of the two topological spaces $\mathrm{Spec}(R_1)$ and $\mathrm{Spec}(R_2)$.

Direct product decomposition

For a commutative ring R there is a correspondence between ring direct product decompositions $R = R_1 \times R_2$, clopen subsets of $\mathrm{Spec}(R)$, and idempotents of the ring R. For instance, $\mathrm{Spec}(R_1 \times R_2)$ is homeomorphic to the disjoint union $\mathrm{Spec}(R_1) \dot{\cup} \mathrm{Spec}(R_2)$ of the two topological spaces $\mathrm{Spec}(R_1)$ and $\mathrm{Spec}(R_2)$.The corresponding result for spectra of groups is:

Theorem

If G_1 and G_2 are groups, then the topological spaces $\mathrm{Spec}(G_1 \times G_2)$ and $\mathrm{Spec}(G_1) \dot{\cup} \mathrm{Spec}(G_2)$ are homeomorphic.

m-systems

There is a notion of m-systems for rings (book by Lam)

m-systems

There is a notion of m-systems for rings (book by Lam) $\Rightarrow$ there is a notion of m-systems for groups.

Some further terminology in multiplicative lattices

Keeping in mind the example of the multiplicative lattice $\mathcal{N}(G)$ of all normal subgroups of a group G, with the commutator of normal subgroups as multiplication, the following terminology turns out to be very natural.

Some further terminology in multiplicative lattices

Keeping in mind the example of the multiplicative lattice $\mathcal{N}(G)$ of all normal subgroups of a group G, with the commutator of normal subgroups as multiplication, the following terminology turns out to be very natural.

Let x be an element of a multiplicative lattice L. The element x is *abelian* if $x \cdot x = 0$, and is *idempotent* if $x \cdot x = x$.

Some further terminology in multiplicative lattices

The *lower left central series* (or *descending left central series*) of x is the descending series

$$x = x_1 \geq x_2 \geq x_3 \geq \dots,$$

where $x_{n+1} := x_n \cdot x$ for every $n \geq 1$. If $x_n = 0$ for some $n \geq 1$, then x is *left nilpotent*. The element x is *idempotent* if $x_2 = x$. Similarly, the element x is *right nilpotent* if ${}_n x = 0$ for some n, where now in the descending series the elements ${}_n x$ are defined recursively by ${}_{n+1} x := x \cdot {}_n x$. If the multiplication in the multiplicative lattice L is associative or commutative, then left nilpotency coincides with right nilpotency.

Some further terminology in multiplicative lattices

The *derived series* of x is the descending series

$$x := x^{(0)} \geq x^{(1)} \geq x^{(2)} \geq \dots,$$

where $x^{(n+1)} := x^{(n)} \cdot x^{(n)}$ for every $n \geq 0$.

Some further terminology in multiplicative lattices

The *derived series* of x is the descending series

$$x := x^{(0)} \geq x^{(1)} \geq x^{(2)} \geq \dots ,$$

where $x^{(n+1)} := x^{(n)} \cdot x^{(n)}$ for every $n \geq 0$. The term $x' := x_2 = x \cdot x = x^{(1)}$ is the *derived element* of x. The element x of L is *solvable* $x^{(n)} = 0$ for some integer $n \geq 0$.

Some further terminology in multiplicative lattices

The *derived series* of x is the descending series

$$x := x^{(0)} \geq x^{(1)} \geq x^{(2)} \geq \dots,$$

where $x^{(n+1)} := x^{(n)} \cdot x^{(n)}$ for every $n \geq 0$. The term $x' := x_2 = x \cdot x = x^{(1)}$ is the *derived element* of x. The element x of L is *solvable* $x^{(n)} = 0$ for some integer $n \geq 0$.

If the operation on the lattice is associative, then left nilpotent $\Leftrightarrow$ right nilpotenct $\Leftrightarrow$ solvable.

Some further terminology in multiplicative lattices

For the multiplicative lattice $\mathcal{N}(G)$ of a group G with operation the commutator of two normal subgroups (which is commutative, but not associative),

Some further terminology in multiplicative lattices

For the multiplicative lattice $\mathcal{N}(G)$ of a group G with operation the commutator of two normal subgroups (which is commutative, but not associative), the element $1 = G$ of $\mathcal{N}(G)$ is left (=right) nilpotent as an element of the multiplicative lattice in the sense just defined if and only if the group G is nilpotent,

Some further terminology in multiplicative lattices

For the multiplicative lattice $\mathcal{N}(G)$ of a group G with operation the commutator of two normal subgroups (which is commutative, but not associative), the element $1 = G$ of $\mathcal{N}(G)$ is left (=right) nilpotent as an element of the multiplicative lattice in the sense just defined if and only if the group G is nilpotent, is a solvable element if and only if G is a solvable group, and is an idempotent element if and only if the group G is perfect.

Some further terminology in multiplicative lattices

For the multiplicative lattice $\mathcal{N}(G)$ of a group G with operation the commutator of two normal subgroups (which is commutative, but not associative), the element $1 = G$ of $\mathcal{N}(G)$ is left (=right) nilpotent as an element of the multiplicative lattice in the sense just defined if and only if the group G is nilpotent, is a solvable element if and only if G is a solvable group, and is an idempotent element if and only if the group G is perfect.

For the multiplicative lattice $\mathcal{L}(R)$ of a ring R with operation the product of two ideals (which is associative, but not commutative in general), the element $1 = G$ of $\mathcal{N}(G)$ is left nilpotent (=right nilpotent=solvable) as an element of the multiplicative lattice if and only if the ring R is nilpotent.

From groups to multiplicative lattices

Theorem

Let L be a multiplicative lattice that satisfies the monotonicity condition $x \leq y$ and $x' \leq y'$ implies $xx \leq yy'$ for every $x, y, x', y' \in L$. Then all $\mathrm{Spec}(L) = L \setminus \{1\}$ if and only if L is linearly ordered and every element of L is idempotent.

Now suppose that $(L, \vee, \cdot)$ is a multiplicative lattice, which is algebraic (every element of L is the join of compact elements) and satisfies the monotonicity condition.

Now suppose that $(L, \vee, \cdot)$ is a multiplicative lattice, which is algebraic (every element of L is the join of compact elements) and satisfies the monotonicity condition. Let $C(L)$ denote the set of all compact elements of L.

Now suppose that $(L, \vee, \cdot)$ is a multiplicative lattice, which is algebraic (every element of L is the join of compact elements) and satisfies the monotonicity condition. Let $C(L)$ denote the set of all compact elements of L.

Lemma

An element $p \neq 1$ in L is prime if and only if

$$xy \leqslant p \Rightarrow (x \leqslant p \ \text{ or } \ y \leqslant p)$$

for every $x, y \in C(L)$.

Now suppose that $(L, \vee, \cdot)$ is a multiplicative lattice, which is algebraic (every element of L is the join of compact elements) and satisfies the monotonicity condition. Let $C(L)$ denote the set of all compact elements of L.

Lemma

An element $p \neq 1$ in L is prime if and only if

$$xy \leqslant p \Rightarrow (x \leqslant p \text{ or } y \leqslant p)$$

for every $x, y \in C(L)$.

An *m-system* in L is a nonempty subset S of $C(L)$ such that for every $x, y \in S$ there exists $z \in S$ such that $z \leq xy$.

Now suppose that $(L, \vee, \cdot)$ is a multiplicative lattice, which is algebraic (every element of L is the join of compact elements) and satisfies the monotonicity condition. Let $C(L)$ denote the set of all compact elements of L.

Lemma

An element $p \neq 1$ in L is prime if and only if

$$xy \leqslant p \Rightarrow (x \leqslant p \text{ or } y \leqslant p)$$

for every $x, y \in C(L)$.

An *m-system* in L is a nonempty subset S of $C(L)$ such that for every $x, y \in S$ there exists $z \in S$ such that $z \leq xy$.

Lemma

An element $p \in L$ is prime if and only if $S_p := \{ c \in C(L) \mid c \nleqslant p \}$ is an m-system in L.

Hyperabealian multiplicative lattices

Theorem

Let $(L, \vee, \cdot)$ be an algebraic multiplicative lattice in which m-distributivity holds. The following conditions are equivalent:
(a) 1 *is the unique semiprime element of* L.
(b) *For every* $x \in L$, $x \neq 1$, *there exists* $y \in L$ *such that* $y > x$ *and* $y^2 \leq x$.
(c) *There exists a strictly ascending chain*

$$0 := x_0 \leq x_1 \leq x_2 \leq \cdots \leq x_\omega \leq x_{\omega+1} \leq \cdots \leq x_\alpha := 1$$

in L *indexed in the ordinal numbers less or equal to* α *for some ordinal* α, *such that* $x_{\beta+1}^2 \leq x_\beta$ *for every ordinal* $\beta < \alpha$ *and* $x_\gamma = \bigvee_{\beta<\gamma} x_\beta$ *for every limit ordinal* $\gamma \leq \alpha$.
(d) *The lattice* L *has no prime elements, that is,* $\mathrm{Spec}(L) = \emptyset$.
(e) *The semiprime radical of* L *is* 1.
(f) *Every m-system of* L *contains* 0.

Another application: left skew braces

Following Drinfeld (1992), a *set-theoretic solution of the Yang-Baxter equation* is a pair (X, r), where X is a set and $r\colon X \times X \to X \times X$ is a bijection, such that

$$(r \times \mathrm{id})(\mathrm{id} \times r)(r \times \mathrm{id}) = (\mathrm{id} \times r)(r \times \mathrm{id})(\mathrm{id} \times r).$$

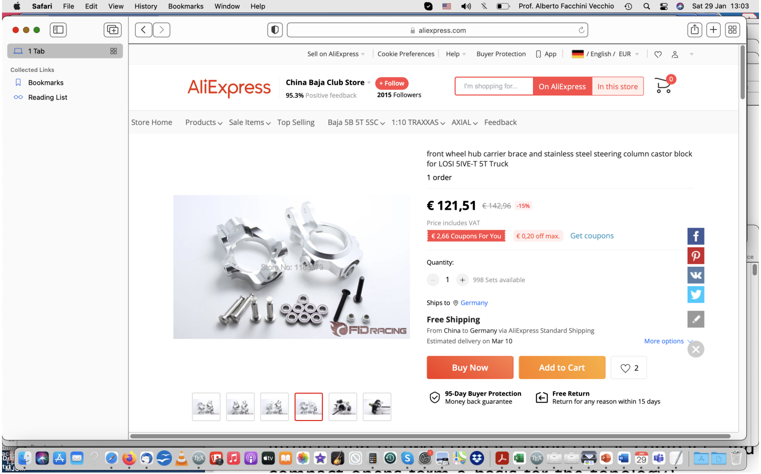
Another application: left skew braces

Following Drinfeld (1992), a *set-theoretic solution of the Yang-Baxter equation* is a pair (X, r), where X is a set and $r\colon X \times X \to X \times X$ is a bijection, such that

$$(r \times \mathrm{id})(\mathrm{id} \times r)(r \times \mathrm{id}) = (\mathrm{id} \times r)(r \times \mathrm{id})(\mathrm{id} \times r).$$

Braces were defined by Wolfgang Rump in 2007 (J. Algebra), and were generalized in 2017 to skew braces by L. Guarnieri and L. Vendramin.

What is a brace



What is a brace

“Braces” has a lot of meanings in English:

What is a brace

“Braces” has a lot of meanings in English:
tutori ortopedici, parentesi graffe, tiracche (bretelle), apparecchi per i denti, pilastri in edilizia, coppia di fagiani, trapano a mano, . . .

What is a brace

A *(left) skew brace* is a triple $(A, \circ, *)$, where $(A, \circ)$ and $(A, *)$ are groups (not necessarily abelian) such that

$$a \circ (b * c) = (a \circ b) * a^{-1} * (a \circ c) \qquad (1)$$

for every $a, b, c \in A$. Here a^{-1} denotes the inverse of a in the group $(A, *)$.

What is a brace

A *(left) skew brace* is a triple $(A, \circ, *)$, where $(A, \circ)$ and $(A, *)$ are groups (not necessarily abelian) such that

$$a \circ (b * c) = (a \circ b) * a^{-1} * (a \circ c) \tag{1}$$

for every $a, b, c \in A$. Here a^{-1} denotes the inverse of a in the group $(A, *)$. The inverse of a in the group $(A, \circ)$ will be denoted by a'.

What is a brace

A *(left) skew brace* is a triple $(A, \circ, *)$, where $(A, \circ)$ and $(A, *)$ are groups (not necessarily abelian) such that

$$a \circ (b * c) = (a \circ b) * a^{-1} * (a \circ c) \tag{1}$$

for every $a, b, c \in A$. Here a^{-1} denotes the inverse of a in the group $(A, *)$. The inverse of a in the group $(A, \circ)$ will be denoted by a'.

The simplest examples of left skew braces are:

What is a brace

A *(left) skew brace* is a triple $(A, \circ, *)$, where $(A, \circ)$ and $(A, *)$ are groups (not necessarily abelian) such that

$$a \circ (b * c) = (a \circ b) * a^{-1} * (a \circ c) \qquad (1)$$

for every $a, b, c \in A$. Here a^{-1} denotes the inverse of a in the group $(A, *)$. The inverse of a in the group $(A, \circ)$ will be denoted by a'.

The simplest examples of left skew braces are:

(1) For any associative ring $(R, +\cdot)$, the Jacobson radical $(J(R), \circ, +)$, where $\circ$ is the operation on $J(R)$ defined by $x \circ y = xy + x + y$ for every $x, y \in J(R)$.

What is a brace

A *(left) skew brace* is a triple $(A, \circ, *)$, where $(A, \circ)$ and $(A, *)$ are groups (not necessarily abelian) such that

$$a \circ (b * c) = (a \circ b) * a^{-1} * (a \circ c) \qquad (1)$$

for every $a, b, c \in A$. Here a^{-1} denotes the inverse of a in the group $(A, *)$. The inverse of a in the group $(A, \circ)$ will be denoted by a'.

The simplest examples of left skew braces are:

(1) For any associative ring $(R, +\cdot)$, the Jacobson radical $(J(R), \circ, +)$, where $\circ$ is the operation on $J(R)$ defined by $x \circ y = xy + x + y$ for every $x, y \in J(R)$.

(2) For any group $(G, *)$, the left skew brace $(G, *, *)$.

Left skew brace morphisms

Clearly, left skew braces also form an algebraic variety, whose morphisms $A \to A'$ are the mappings $f \colon A \to A'$ such that $f(a \circ b) = f(a) \circ f(b)$ and $f(a * b) = f(a) * f(b)$ for every $a, b \in A$.

Left skew brace morphisms

Clearly, left skew braces also form an algebraic variety, whose morphisms $A \to A'$ are the mappings $f\colon A \to A'$ such that $f(a \circ b) = f(a) \circ f(b)$ and $f(a * b) = f(a) * f(b)$ for every $a, b \in A$.

In particular, we have a category Bra of all left skew braces.

Left skew brace morphisms

Clearly, left skew braces also form an algebraic variety, whose morphisms $A \to A'$ are the mappings $f\colon A \to A'$ such that $f(a \circ b) = f(a) \circ f(b)$ and $f(a * b) = f(a) * f(b)$ for every $a, b \in A$.

In particular, we have a category Bra of all left skew braces.

For every skew brace $(A, \circ, *)$, the mapping

$$r\colon A \times A \to A \times A, \quad r(x, y) = (x^{-1} * (x \circ y), (x^{-1} * (x \circ y))' \circ x \circ y),$$

is a set-theoretic solution of the Yang-Baxter equation (Guarnieri-Vendramin, 2017).

Ideals in skew braces

The zero object of the category Bra is the left skew brace with one element.

Ideals in skew braces

The zero object of the category Bra is the left skew brace with one element. The product of two left skew braces is the cartesian product with the component-wise operations.

Ideals in skew braces

The zero object of the category Bra is the left skew brace with one element. The product of two left skew braces is the cartesian product with the component-wise operations. The category of braces is a semi-abelian category.

Ideals in skew braces

The zero object of the category Bra is the left skew brace with one element. The product of two left skew braces is the cartesian product with the component-wise operations. The category of braces is a semi-abelian category.

Lemma

[Bachiller, J. Pure Appl. Algebra, 2018] *Let A be a skew brace. Then $\lambda\colon (A, \circ) \to \mathrm{Aut}(A, *)$, given by $\lambda\colon a \mapsto \lambda_a$, where $\lambda_a(b) = a^{-1} * (a \circ b)$, is a well-defined group homomorphism.*

The action $\lambda\colon (A, \circ) \to \mathrm{Aut}(A, *)$ for a brace

In other words, for any skew brace $(A, \circ, *)$, we have that $(A, *)$ is an $(A, \circ)$-group with respect to the action $\lambda\colon (A, \circ) \to \mathrm{Aut}(A, *)$ described in the statement of the previous Lemma.

The action $\lambda\colon (A, \circ) \to \mathrm{Aut}(A, *)$ for a brace

In other words, for any skew brace $(A, \circ, *)$, we have that $(A, *)$ is an $(A, \circ)$-group with respect to the action $\lambda\colon (A, \circ) \to \mathrm{Aut}(A, *)$ described in the statement of the previous Lemma.

Conversely, suppose that a set A has two group structures $(A, \circ)$ and $(A, *)$ and that $(A, *)$ is an $(A, \circ)$-group with respect to the action $\lambda\colon (A, \circ) \to \mathrm{Aut}(A, *)$, defined by $\lambda\colon a \mapsto \lambda_a$, where $\lambda_a(b) = a^{-1} * (a \circ b)$. Then the fact that each λ_a is an automorphism yields that $\lambda_a(b * c) = \lambda_a(b) * \lambda_a(c)$, i.e., $a^{-1} * (a \circ (b * c)) = a^{-1} * (a \circ b) * a^{-1} * (a \circ c)$, from which $a \circ (b * c) = (a \circ b) * a^{-1} * (a \circ c)$.

The action $\lambda\colon (A, \circ) \to \mathrm{Aut}(A, *)$ for a brace

In other words, for any skew brace $(A, \circ, *)$, we have that $(A, *)$ is an $(A, \circ)$-group with respect to the action $\lambda\colon (A, \circ) \to \mathrm{Aut}(A, *)$ described in the statement of the previous Lemma.

Conversely, suppose that a set A has two group structures $(A, \circ)$ and $(A, *)$ and that $(A, *)$ is an $(A, \circ)$-group with respect to the action $\lambda\colon (A, \circ) \to \mathrm{Aut}(A, *)$, defined by $\lambda\colon a \mapsto \lambda_a$, where $\lambda_a(b) = a^{-1} * (a \circ b)$. Then the fact that each λ_a is an automorphism yields that $\lambda_a(b * c) = \lambda_a(b) * \lambda_a(c)$, i.e., $a^{-1} * (a \circ (b * c)) = a^{-1} * (a \circ b) * a^{-1} * (a \circ c)$, from which $a \circ (b * c) = (a \circ b) * a^{-1} * (a \circ c)$. Hence braces are exactly those particular G-groups (H, λ) for which $G = H$ as sets, and the action λ is defined by $\lambda_a(b) = a^{-1} * (a \circ b)$.

The group morphism $\lambda\colon (A,\circ) \to \mathrm{Aut}(A,*)$ for a brace

The semidirect product corresponding to such a group morphism $\lambda\colon (A,\circ) \to \mathrm{Aut}(A,*)$ is the group $P := (A,*) \ltimes (A,\circ)$, i.e., the cartesian product $P := A \times A$ with group operation defined by

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 * a_2^{-1} * (a_2 \circ b_1), a_2 \circ b_2). \tag{2}$$

The group morphism $\lambda\colon (A,\circ) \to \mathrm{Aut}(A,*)$ for a brace

The semidirect product corresponding to such a group morphism $\lambda\colon (A,\circ) \to \mathrm{Aut}(A,*)$ is the group $P := (A,*) \ltimes (A,\circ)$, i.e., the cartesian product $P := A \times A$ with group operation defined by

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 * a_2^{-1} * (a_2 \circ b_1), a_2 \circ b_2). \qquad (2)$$

Conversely, given two group structures $(A,\circ)$ and $(A,*)$ on the same set A such that $P := A \times A$ with the operation as in (2) is a group, then $(A,\circ,*)$ is a left skew brace.

The group morphism $\lambda\colon (A,\circ) \to \mathrm{Aut}(A,*)$ for a brace

The semidirect product corresponding to such a group morphism $\lambda\colon (A,\circ) \to \mathrm{Aut}(A,*)$ is the group $P := (A,*) \ltimes (A,\circ)$, i.e., the cartesian product $P := A \times A$ with group operation defined by

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 * a_2^{-1} * (a_2 \circ b_1), a_2 \circ b_2). \qquad (2)$$

Conversely, given two group structures $(A,\circ)$ and $(A,*)$ on the same set A such that $P := A \times A$ with the operation as in (2) is a group, then $(A,\circ,*)$ is a left skew brace.

This proves that left skew braces are particular groups, in the sense that there is a faithful functor $\mathrm{Bra} \to \mathrm{Group}$,
$A \mapsto P = (A,*) \ltimes (A,\circ)$, $f \mapsto f \times f$, because every brace morphism $f\colon A \to A'$ induces a corresponding group morphism $f \times f\colon P = A \ltimes A \to P' = A' \ltimes A'$, $(f \times f)(a,b) = (f(a), f(b))$.

The group morphism $\lambda\colon (A,\circ) \to \mathrm{Aut}(A,*)$ for a brace

The semidirect product corresponding to such a group morphism $\lambda\colon (A,\circ) \to \mathrm{Aut}(A,*)$ is the group $P := (A,*) \ltimes (A,\circ)$, i.e., the cartesian product $P := A \times A$ with group operation defined by

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 * a_2^{-1} * (a_2 \circ b_1), a_2 \circ b_2). \qquad (2)$$

Conversely, given two group structures $(A,\circ)$ and $(A,*)$ on the same set A such that $P := A \times A$ with the operation as in (2) is a group, then $(A,\circ,*)$ is a left skew brace.

This proves that left skew braces are particular groups, in the sense that there is a faithful functor $\mathrm{Bra} \to \mathrm{Group}$, $A \mapsto P = (A,*) \ltimes (A,\circ)$, $f \mapsto f \times f$, because every brace morphism $f\colon A \to A'$ induces a corresponding group morphism $f \times f\colon P = A \ltimes A \to P' = A' \ltimes A'$, $(f \times f)(a,b) = (f(a), f(b))$. This functor allows us to consider braces as "particular groups with less morphisms".

Kernel of a left skew brace morphism $f\colon A \to A'$

It is well known and very easy to prove that, in a left skew brace $(A, \circ, *)$, the two groups $(A, \circ)$ and $(A, *)$ have the same identity.

Kernel of a left skew brace morphism $f\colon A \to A'$

It is well known and very easy to prove that, in a left skew brace $(A, \circ, *)$, the two groups $(A, \circ)$ and $(A, *)$ have the same identity. From this, it follows in particular that the group morphisms $f\colon (A, \circ) \to (A, \circ)$ and $f\colon (A, *) \to (A, *)$ have the same kernel I, which is a normal subgroup both in $(A, \circ)$ and in $(A, *)$.

Kernel of a left skew brace morphism $f\colon A \to A'$

It is well known and very easy to prove that, in a left skew brace $(A, \circ, *)$, the two groups $(A, \circ)$ and $(A, *)$ have the same identity. From this, it follows in particular that the group morphisms $f\colon (A, \circ) \to (A, \circ)$ and $f\colon (A, *) \to (A, *)$ have the same kernel I, which is a normal subgroup both in $(A, \circ)$ and in $(A, *)$.

The kernel of $f \times f\colon P = A \ltimes A \to P' = A' \ltimes A'$ is $I \times I$.

Kernel of a left skew brace morphism $f\colon A \to A'$

The assignments $(A, \circ, *) \mapsto P := (A, *) \ltimes (A, \circ)$ and $f \mapsto f \times f$ define a faithful functor of the category of left skew braces into the category of groups.

Kernel of a left skew brace morphism $f\colon A \to A'$

The assignments $(A, \circ, *) \mapsto P := (A, *) \ltimes (A, \circ)$ and $f \mapsto f \times f$ define a faithful functor of the category of left skew braces into the category of groups.

This allows us to view left skew braces as groups and suggests us the definition of kernel of a left skew brace morphism $f\colon A \to A'$ and of factor skew brace, getting a left skew brace isomorphism $(A/I, *) \ltimes (A/I, \circ) \to (f \times f)(P)$, as follows.

Kernel of a left skew brace morphism $f\colon A \to A'$

The assignments $(A, \circ, *) \mapsto P := (A, *) \ltimes (A, \circ)$ and $f \mapsto f \times f$ define a faithful functor of the category of left skew braces into the category of groups.

This allows us to view left skew braces as groups and suggests us the definition of kernel of a left skew brace morphism $f\colon A \to A'$ and of factor skew brace, getting a left skew brace isomorphism $(A/I, *) \ltimes (A/I, \circ) \to (f \times f)(P)$, as follows. The *kernel* of a left skew brace morphism $f\colon A \to A'$ is the inverse image $f^{-1}(1_A)$ of the identity 1_A of $(A, \circ)$, (which coincides with the identity of $(A, *)$).

Ideals of a left skew brace

An *ideal* of a skew brace A is a normal subgroup I both of $(A, \circ)$ and $(A, *)$ such that $I \circ a = I * a$ for every $a \in I$.

Ideals of a left skew brace

An *ideal* of a skew brace A is a normal subgroup I both of $(A, \circ)$ and $(A, *)$ such that $I \circ a = I * a$ for every $a \in I$. Notice that this exactly means that the factor groups of $(A, \circ)$ and $(A, *)$ modulo I coincide as sets.

Ideals of a left skew brace

An *ideal* of a skew brace A is a normal subgroup I both of $(A, \circ)$ and $(A, *)$ such that $I \circ a = I * a$ for every $a \in I$. Notice that this exactly means that the factor groups of $(A, \circ)$ and $(A, *)$ modulo I coincide as sets.

Also notice that $I \circ a = I * a$ for every $a \in A$ if and only if, for every $a, b \in A$, one has $a * b^{-1} \in I \Leftrightarrow a \circ b' \in I$. Equivalently, if and only if $\lambda_a(I) \subseteq I$ for every $x \in I$ and every $a \in A$, that is, I is an $(A, \circ)$-subgroup of the left $(A, \circ)$-group $(A, *)$.

Ideals of a left skew brace

An *ideal* of a skew brace A is a normal subgroup I both of $(A, \circ)$ and $(A, *)$ such that $I \circ a = I * a$ for every $a \in I$. Notice that this exactly means that the factor groups of $(A, \circ)$ and $(A, *)$ modulo I coincide as sets.

Also notice that $I \circ a = I * a$ for every $a \in A$ if and only if, for every $a, b \in A$, one has $a * b^{-1} \in I \Leftrightarrow a \circ b' \in I$. Equivalently, if and only if $\lambda_a(I) \subseteq I$ for every $x \in I$ and every $a \in A$, that is, I is an $(A, \circ)$-subgroup of the left $(A, \circ)$-group $(A, *)$.

The semidirect product corresponding to the quotient left skew brace A/I is $(A/I, *) \ltimes (A/I, \circ)$.

Ideals of a left skew brace

Proposition

Let $(A, \circ, *)$ *be a left skew brace.*
(1) *If* $\sim$ *is an equivalence relation on the set* A *compatible with both the operations* $\circ$ *and* $*$ *of* A*, then the equivalence class* $[1_A]_\sim$ *of the identity of* A *is an ideal of the skew brace* A*.*

Ideals of a left skew brace

Proposition

Let $(A, \circ, *)$ *be a left skew brace.*
(1) *If* $\sim$ *is an equivalence relation on the set* A *compatible with both the operations* $\circ$ *and* $*$ *of* A*, then the equivalence class* $[1_A]_\sim$ *of the identity of* A *is an ideal of the skew brace* A*.*
(2) *Conversely, if* I *is an ideal of* A*, the relation* $\sim_I$ *on* A *defined, for every* $a, b \in A$*, by* $a \sim_I b$ *if* $a * b^{-1} \in I$*, is an equivalence relation on* A *compatible with both* $\circ$ *and* $*$*.*

Ideals of a left skew brace

Proposition

Let $(A, \circ, *)$ be a left skew brace.
(1) *If $\sim$ is an equivalence relation on the set A compatible with both the operations $\circ$ and $*$ of A, then the equivalence class $[1_A]_\sim$ of the identity of A is an ideal of the skew brace A.*
(2) *Conversely, if I is an ideal of A, the relation $\sim_I$ on A defined, for every $a, b \in A$, by $a \sim_I b$ if $a * b^{-1} \in I$, is an equivalence relation on A compatible with both $\circ$ and $*$.*
(3) *The two assignments in (1) and (2) determine a one-to-one correspondence between the set of all ideals of A and the set of all the equivalence relations on A compatible with both the operations $\circ$ and $*$.*

Ideal generated by a subset of a brace

Any intersection of ideals is an ideal, so that we get a complete lattice $\mathcal{I}(A)$ of ideals for any skew brace A. In particular, every subset X of A generates an ideal, the intersection of the ideals that contain X.

Ideal generated by a subset of a brace

Any intersection of ideals is an ideal, so that we get a complete lattice $\mathcal{I}(A)$ of ideals for any skew brace A. In particular, every subset X of A generates an ideal, the intersection of the ideals that contain X. It can be "constructively" described as follows. Given a subset X of a skew brace A, consider the increasing sequence X_n, $n \geq 0$, of subsets of A where $X_0 := X$, X_{n+1} is the normal closure of X_n in $(A, *)$ if $n \equiv 0 \pmod 3$, X_{n+1} is the normal closure of X_n in $(A, \circ)$ if $n \equiv 1$ (mod 3, $X_{n+1} := \bigcup_{a \in A} \lambda_a(X_n)$ if $n \equiv 2 \pmod 3$. The ideal of A generated by X is $\bigcup_{n \geq 0} X_n$.

The multiplicative lattice of ideals

If I and J are ideals of a skew brace A, then $I \cap J$ is an ideal of A. The sum $I + J$ of I and J is defined as the additive subgroup of A generated by all the elements of the form $u + v$, where $u \in I$ and $v \in J$. It is an ideal of A (A. Konovalov, A. Smoktunowicz and L. Vendramin, Exp. Math., 2021).

The multiplicative lattice of ideals

If I and J are ideals of a skew brace A, then $I \cap J$ is an ideal of A. The sum $I + J$ of I and J is defined as the additive subgroup of A generated by all the elements of the form $u + v$, where $u \in I$ and $v \in J$. It is an ideal of A (A. Konovalov, A. Smoktunowicz and L. Vendramin, Exp. Math., 2021).

More generally, any intersection of ideals is an ideal, so that we get a complete lattice $\mathcal{I}(A)$ of ideals for any skew brace A. In particular, every subset X of A generates an ideal, the intersection of the ideals that contain X.

The multiplicative lattice of ideals

If I and J are ideals of a skew brace A, then $I \cap J$ is an ideal of A. The sum $I + J$ of I and J is defined as the additive subgroup of A generated by all the elements of the form $u + v$, where $u \in I$ and $v \in J$. It is an ideal of A (A. Konovalov, A. Smoktunowicz and L. Vendramin, Exp. Math., 2021).

More generally, any intersection of ideals is an ideal, so that we get a complete lattice $\mathcal{I}(A)$ of ideals for any skew brace A. In particular, every subset X of A generates an ideal, the intersection of the ideals that contain X.

A ring is *abelian* if has zero multiplication. Abelian rings are radical rings. Adjoining them an identity (Dorroh), one gets a trivial extension $\mathbb{Z}\alpha A$, A an abelian group. Correspondingly, in abelian braces A we have that $(A, +)$ is an abelian group, the operations $+$ and $\circ$ coincide, and $\cdot$ is the zero multiplication.

Commutators

Huq commutator [Huq, 1968].

Commutators

Huq commutator [Huq, 1968].

The category of braces is semiabelian category with a zero object.

Commutators

Huq commutator [Huq, 1968].

The category of braces is semiabelian category with a zero object. If I, J are ideals of a left skew brace A, the Huq commutator $[I, J]_H$ is the smallest ideal X of A such that there is a left skew brace morphism $\varphi\colon I \times J \to A/X$ such that the diagram

$$\begin{array}{ccccc}
I & \xrightarrow{(1_I, 0_I)} & I \times J & \xleftarrow{(0_J, 1_J)} & J \\
\big\downarrow & & \big\downarrow{\scriptstyle \varphi} & & \big\downarrow \\
A & \twoheadrightarrow & A/X & \twoheadleftarrow & A
\end{array}$$

commute.

Maltsev

[Maltsev, 1954]. The following conditions are equivalent for any variety of algebras $\mathcal{V}$:
(a) $\mathcal{V}$ is congruence-permutable.
(b) There is a ternary term q such that

$$\mathcal{V} \models q(x, y, y) \approx x \approx q(y, y, x).$$

Maltsev

[Maltsev, 1954]. The following conditions are equivalent for any variety of algebras $\mathcal{V}$:
(a) $\mathcal{V}$ is congruence-permutable.
(b) There is a ternary term q such that

$$\mathcal{V} \models q(x, y, y) \approx x \approx q(y, y, x).$$

Such a term is called a *Maltsev term* and congruence-permutable varieties are called *Maltsev varieties*. Any variety that contains a group operation is congruence-permutable, and the Maltsev term is $xy^{-1}z$.

Smith commutator

For an algebra X in a Maltsev variety $\mathcal{V}$ with Maltsev term $q(x, y, z)$ and two congruences α and β on X, the Smith commutator $[\alpha, \beta]_S$ is the smallest congruence θ on X for which the mapping

$$p \colon \{ (x, y, z) \mid (x, y) \in \alpha \text{ and } (y, z) \in \beta \} \to X/\theta$$

that sends (x, y, z) to the θ-class of $p(x, y, z)$ is a morphism.

The notions of prime ideal, solvable, nilpotent, etc., skew braces are now natural, and depend on the commutator chosen. This must be compared with previous notions by Rump (J. Algebra 2007), Rowen (2017), Bachiller-Cedó-Jespers-Okniński (Commun. Contemp. Math. 2019), and Smoktunowicz (Appendix to the paper On skew braces and their ideals, available in arXiv.)