How do retracts depend on the endomorphism monoid?

Jens Hemelaer
jens.hemelaer@uantwerpen.be

Joint work with Morgan Rogers, see arXiv:2011.12129.

1. Universal Algebra

An algebra is a set S equipped with a collection of operations:

$$\mu : S^n \longrightarrow S$$

with n depending on μ, such that some equational laws between the operations are satisfied.

Here, μ is called an n-ary operation.

only involving the operations & free variables

A collection of algebras with given operations and satisfying certain equational laws is a variety.

EXAMPLES

- A semigroup is a set S together with a binary operation

  $$\mu : S \times S \longrightarrow S$$

  such that

  $$\mu(a, \mu(b,c)) = \mu(\mu(a,b), c).$$

- A monoid has in addition a 0-ary operation

  $$1 : \{*\} \longrightarrow S$$

such that

$$\mu(a,1) = a = \mu(1,a).$$

- for a monoid S, a right S-set is a set X equipped with a unary operation

$$\rho_a : X \longrightarrow X$$

for each $a \in S$, such that

$$\rho_b(\rho_a(x)) = \rho_{ab}(x)$$

for all $a, b \in S$, and

$$\rho_1(x) = x.$$

- the following structures can be interpreted as algebras:

structure	operations
group	$1 \quad \cdot \quad ()^{-1}$
ring	$0 \quad 1 \quad + \quad \cdot \quad -$
lattice	$\wedge \quad \vee$
bounded lattice	$0 \quad 1 \quad \wedge \quad \vee$

I forgot this one, thanks!

- the following structures can not be interpreted as algebras:

* fields — see "meadows"
* topological spaces
* small categories
* posets

However, compact totally disconnected Hausdorff spaces are dual to Boolean algebras

A function

$$f: R \longrightarrow S$$

between two algebras (with the same operations or "signature") is called a homomorphism if for each (n-ary) operation μ we have:

$$f(\mu(a_1, \ldots, a_n)) = \mu(f(a_1), \ldots, f(a_n))$$

For example, f is a group homomorphism if and only if

$$f(1) = 1$$
$$f(ab) = f(a)f(b)$$
$$f(a^{-1}) = f(a)^{-1}.$$

The notion of "homorphism" does not depend on the equational laws, only on the signature!

2. Retracts & Coretracts

Let A be an algebra.

A subalgebra $B \subseteq A$ is called a retract if there is a homomorphism

$$r : A \longrightarrow B \quad \text{(the "retraction")}$$

such that $r(b) = b$ for all

such that $r(b) = b$ for all $b \in B$.

Categorical reformulation:
a retract is a morphism
$$i : B \longrightarrow A$$
that has a left inverse.
$$(r \circ i = 1_B)$$

Examples:

① If V is a vector space, and $W \subseteq V$ is a subspace, then $W \subseteq V$ is always a retract.
(This depends on the axiom of choice!)

② Let G be a group with subgroup $H \leq G$.
If $H \leq G$ is a retract with retraction $r : G \longrightarrow H$,

then G is a semidirect product : $G = \ker(r) \rtimes H$.

The inclusion

$$\begin{aligned} \mathbb{Z}/2\mathbb{Z} &\hookrightarrow \mathbb{Z}/4\mathbb{Z} \\ 0 &\mapsto 0 \\ 1 &\mapsto 2 \end{aligned}$$

is <u>not</u> a retract.

<u>Question</u>: is the intersection of retracts again a retract?

<u>Question</u>: if $i : B \longrightarrow A$ is a retract, then is the retraction $r : A \longrightarrow B$ uniquely determined?

The questions depend both on the category of algebras and on the algebra A whose retracts we are studying.

<u>Example</u>: Let $V = \mathbb{R}^2$ in the category of $\mathbb{R}$-vector spaces. Then the inclusion of the x-axis

$\mathbb{R} \subseteq \mathbb{R}^2$

has multiple retractions:

$$\begin{aligned} \mathbb{R}^2 &\longrightarrow \mathbb{R} \\ (x,y) &\longmapsto (x,0) \\ (x,y) &\longmapsto (x+y,0) \\ (x,y) &\longmapsto (x+2y,0) \\ &\vdots \end{aligned}$$

Dually, a quotient

$$r : A \longrightarrow B$$

is called a coretract if there is a morphism

$$i : B \longrightarrow A$$

such that $r \circ i = 1_B$.

(In this case, i is called a section for r.)

The concept is the same, but r is the center of attention, rather than i.

Remark: if $r: A \longrightarrow B$ is any surjective homomorphism, then there is an equivalence relation ρ on A, that is compatible with the algebra operations

(i.e. for each operation μ: $\forall i \in \{1,\dots,n\}\ a_i \sim b_i \Rightarrow \mu(a_1,\dots,a_n) \sim \mu(b_1,\dots,b_n)$)

and such that

$$B \cong A/_\sim$$

with $r: A \longrightarrow B$ corresponding to the quotient map

$$\begin{aligned} A &\longrightarrow A/\rho . \\ a &\longmapsto [a] \end{aligned}$$

So it makes sense to call surjections "quotients".

An equivalence relation ρ that is compatible with the operations is called a congruence.

For two congruences ρ_1 and ρ_2 there is a smallest congruence

$$\rho_1 \vee \rho_2$$

that contains both.

<u>Question</u>: if A/ρ_1 and A/ρ_2 are coretracts, then is their "join" $A/\rho_1 \vee \rho_2$ again a coretract?

<u>Question</u>: if $r : A \longrightarrow B$ is a coretract, then does it have a unique section?

<u>Example</u>: the projection

$$\mathbb{R}^2 \longrightarrow \mathbb{R}$$
$$(x,y) \longmapsto x$$

has multiple sections, e.g.

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R}^2 \\ x & \longmapsto & (x,0) \\ x & \longmapsto & (x,x) \\ x & \longmapsto & (x,2x) \\ & \vdots & \end{array}$$

---

3. FitzGerald's question

Question (FitzGerald): (GAiA 2013 NCS 2018)

Let A be an algebra satisfying the following four properties:

(RI) The intersection of two retracts of A is again a retract.

(UR) Each retract has a unique left inverse/retraction.

(RI*) The join of two coretracts of A is again a coretract.

(UR*) Each coretract has a

unique section/right inverse.

Then does the monoid of endomorphisms of A have commuting idempotents?

Why would there be a relation with idempotents in the first place?

Suppose that $i : B \to A$ is a retract, with retraction $r : A \to B$, so $r \circ i = 1_B$.

Then
$$
\begin{aligned}
i \circ r \circ i \circ r &= i \circ 1_B \circ r \\
&= i \circ r
\end{aligned}
$$

so $i \circ r$ is an idempotent!

We write $e = i \circ r$.

Then $e(A) = i(B)$ and as a result $e(A) \subseteq A$ is a retract isomorphic to $i : B \to A$.

Conversely, for every idempotent $e : A \to A$, we have that $e(A) \subseteq A$ is a retract.

Suppose that $i \circ r = i \circ r'$. Then because i is injective, we also have $r = r'$.

So for $i : B \to A$ there is a bijective correspondence:

retractions of i

$$\updownarrow$$

idempotents $e : A \to A$ such that $e(A) = i(B)$

Dually, for a map

$$r: A \longrightarrow B$$

there is a bijective correspondence between sections $i: B \longrightarrow A$ and idempotents $e: A \longrightarrow A$ with $B \cong A/\rho_e$ and such that $r: A \to B$ corresponds to the quotient map $A \longrightarrow A/\rho_e$.

(Here ρ_e is the congruence generated by $e(a) \sim a$ for all $a \in A$.)

Now suppose that idempotents commute, so for $e, f \in \mathrm{End}(A)$ idempotent, we get that $ef = fe$.

Then $(ef)(A) \subseteq e(A) \cap f(A)$.

But also if $e(a) = a$ and $f(a) = a$

then $ef(a) = e(a) = a$, so

$$e(A) \cap f(A) = ef(A).$$

It follows that property (RI) holds! In fact, FitzGerald showed that:

End(A) has commuting idempotents
$\Rightarrow$ A satisfies properties (RI), (UR), (RI*), (UR*).

His question was then whether the converse implication holds.

4. Counterexample

Take the monoid

$$S = \left\langle e, f, g : \begin{array}{c} e^2 = e \\ f^2 = f \\ g^2 = g \end{array}, \begin{array}{c} fg = gf \\ = eg = ge \\ = g \end{array}, fef = g = efe \right\rangle.$$

Then $S = \{1, e, f, ef, fe, g\}$
has exactly six elements.

In particular, $ef \neq fe$.

To do:

1. Find an algebra A that has S as monoid of endomorphisms.
2. Show that A satisfies the four properties (RI), (UR), (RI*), (UR*).

Regarding step 1, there is a canonical such algebra!

Consider the set S itself, seen as a right S-set under multiplication. Call this A.

Each endomorphism $A \longrightarrow A$ is of the form

$$\begin{aligned} A &\xrightarrow{s\cdot} A \\ a &\longmapsto sa \end{aligned}$$

for some $s \in S$, so $\mathrm{End}(A) = S$.

What are the retracts of A?

The idempotents in S are

$$\{1, e, f, g\}$$

So the retracts are

$$1(A) = A$$
$$e(A) = \{e, ef, g\}$$
$$f(A) = \{f, fe, g\}$$
$$g(A) = \{g\}$$

To each retract corresponds a unique idempotent, so (UR) holds!

Further, $e(A) \cap f(A) = g(A)$.
So (RI) holds as well.

The coretracts are

$$A/\rho_1 = A$$
$$A/\rho_e = \{1 \sim e,\ f \sim ef,\ fe \sim g\}$$
$$A/\rho_f = \{1 \sim f,\ e \sim fe,\ ef \sim g\}$$
$$A/\rho_g = \{1 \sim e \sim f \sim ef \sim fe \sim g\}$$

To each coretract corresponds a unique idempotent, so (UR*) holds!

Further:

$$\begin{tikzcd}
g \arrow[r, dash, "\rho_f"'] & ef \arrow[d, dash, "\rho_e"] & & \\
& f \arrow[r, dash, "\rho_f"'] & 1 \arrow[d, dash, "\rho_e"] & \\
& & e \arrow[r, dash, "\rho_f"'] & fe
\end{tikzcd}$$

So $\rho_e \vee \rho_f = \rho_g$.

As a result, (RI*) holds!

5. Further remarks

The counterexample above is not difficult. The trick is to look at algebras with only unary operations, such as S-sets for a monoid S.

Most algebras arising naturally have binary operations

- monoids/groups
- rings
- lattices
- ...

Can we find a set A with a binary operation such that

$$\mathrm{End}(A) = S$$

with S the monoid from the counterexample ?

If $\#A = 6$, there are already

$$6^{36} \approx 10^{28}$$

possible binary operations

$$\mu : A \times A \longrightarrow A.$$

So this is not something you can check with a computer.

At the moment, we do not have a counterexample to FitzGerald's question for which the algebra A has at least one operation μ that is n-ary for $n \geq 2$ in a nontrivial way.

But we do know it exists!
For example, there exists a ring A such that (RI), (UR), (RI*), (UR*)

hold and such that $\mathrm{End}(A) = S$ with S the monoid from our counterexample.
We just don't know what it looks like!

Strategy behind the proof:

(1) Establish an equivalence of categories between retracts of A and retracts of S as a right S-set.
Here $e(A)$ corresponds to $e(S)$.
Keyword: Cauchy completion.

It then follows that both (UR) and (UR*) depend only on S and not on A.

(2) The equivalence above extends to a functor

$$X \longmapsto X \otimes_S A$$

for right S-sets X.
Use this functor to show that A satisfies (RI*) if and only if S as right S-set satisfies (RI*).

(3) We guess that the last property, (RI), also depends only on S and not on A.
But this is <u>false</u>!

Fortunately, it <u>is</u> true that A always satisfies (RI) as soon as for each two idempotents $e, f \in S$ there is an n such that

$$(ef)^n = (fe)^n.$$

This is the case for the monoid S from our original counterexample.

Conclusion: every algebra A with $\mathrm{End}(A) = S$, with S the 6-element monoid from the original counterexample, is a counterexample!

(4) Show that there is a ring A such that

$$\mathrm{End}(A) = S$$

for S as above. But this is already in the literature!

Keyword: (algebraically) universal

If a variety $\mathcal{C}$ is universal, then for each monoid M we can find an algebra A in $\mathcal{C}$ such that $\mathrm{End}(A) = M$.

Examples of universal varieties:

- rings
- semigroups