

# HOMOLOGICAL INVARIANTS FOR TERM REWRITING SYSTEMS

Philippe Malbos

**Samuel Mimram**



Journées Nationales Géocal – LAC 2016

Mardi 29 novembre 2016

# Algebraic theories

## An **algebraic theory**

$$\langle G \mid R \rangle$$

consists of

1.  $G$ : operations with given arities
2.  $R$ : equations between terms generated by operations

## Example

- ▶ the theory of groups is given by  $m : 2$ ,  $e : 0$ ,  $i : 1$  and

$$m(m(x_1, x_2), x_3) = m(x_1, m(x_2, x_3))$$

$$m(e, x_1) = x_1 \qquad m(x_1, e) = x_1$$

$$m(i(x_1), x_1) = e \qquad m(x_1, i(x_1)) = e$$

- ▶ rings, fields, etc.
- ▶ (semi)lattices, booleans algebras, etc.

# Algebraic theories

## An **algebraic theory**

$$\langle G \mid R \rangle$$

consists of

1.  $G$ : operations with given arities
2.  $R$ : equations between terms generated by operations

( $G =$  **generators**,  $R =$  **relations**)

### Example

- ▶ the theory of groups is given by  $m : 2$ ,  $e : 0$ ,  $i : 1$  and

$$m(m(x_1, x_2), x_3) = m(x_1, m(x_2, x_3))$$

$$m(e, x_1) = x_1 \qquad m(x_1, e) = x_1$$

$$m(i(x_1), x_1) = e \qquad m(x_1, i(x_1)) = e$$

- ▶ rings, fields, etc.
- ▶ (semi)lattices, booleans algebras, etc.

# Algebraic theories

## An **algebraic theory**

$$\langle G \mid R \rangle$$

consists of

1.  $G$ : operations with given arities
2.  $R$ : equations between terms generated by operations

( $G =$  **signature**,  $R =$  **rewriting system**)

### Example

- ▶ the theory of groups is given by  $m : 2$ ,  $e : 0$ ,  $i : 1$  and

$$m(m(x_1, x_2), x_3) = m(x_1, m(x_2, x_3))$$

$$m(e, x_1) = x_1 \qquad m(x_1, e) = x_1$$

$$m(i(x_1), x_1) = e \qquad m(x_1, i(x_1)) = e$$

- ▶ rings, fields, etc.
- ▶ (semi)lattices, booleans algebras, etc.

# Models

A **model** of an algebraic theory consists of

- ▶ a set  $X$ ,
- ▶ an interpretation  $\llbracket f \rrbracket : X^n \rightarrow X$   
for each operation  $f$  of arity  $n$ ,
- ▶ such that the axioms are satisfied.

## Example

Models of the theory of groups are groups.

## Equivalence between theories

Two theories are **equivalent** when they have the same models.

### Example

Consider the theory of groups, given by  $m : 2$ ,  $e : 0$ ,  $i : 1$  and

$$m(m(x_1, x_2), x_3) = m(x_1, m(x_2, x_3))$$

$$m(e, x_1) = x_1$$

$$m(i(x_1), x_1) = e$$

$$m(x_1, e) = x_1$$

$$m(x_1, i(x_1)) = e$$

The equations in red are derivable from the other.

## Equivalence between theories

Two theories are **equivalent** when they have the same models.

### Example

Consider the theory of groups, given by  $m : 2$ ,  $e : 0$ ,  $i : 1$  and

$$m(m(x_1, x_2), x_3) = m(x_1, m(x_2, x_3))$$

$$m(e, x_1) = x_1$$

$$m(x_1, e) = x_1$$

$$m(i(x_1), x_1) = e$$

$$m(x_1, i(x_1)) = e$$

The equations in red are derivable from the other.

$$\begin{aligned} xe &= (ex)e = ((x^{-1}x^{-1})x)e = (x^{-1}(x^{-1}x))e = (x^{-1}e)e \\ &= x^{-1}(ee) = x^{-1}e = x^{-1}(x^{-1}x) = (x^{-1}x^{-1})x = ex = x \end{aligned}$$

## Equivalence between theories

Two theories are **equivalent** when they have the same models.

### Example

Consider the theory of groups, given by  $m : 2$ ,  $e : 0$ ,  $i : 1$  and

$$m(m(x_1, x_2), x_3) = m(x_1, m(x_2, x_3))$$

$$m(e, x_1) = x_1$$

$$m(i(x_1), x_1) = e$$

The equations in red are derivable from the other.

$$\begin{aligned} xe &= (ex)e = ((x^{-}x^{-})x)e = (x^{-}(x^{-}x))e = (x^{-}e)e \\ &= x^{-}(ee) = x^{-}e = x^{-}(x^{-}x) = (x^{-}x^{-})x = ex = x \end{aligned}$$



## Equivalence between theories

Two theories are equivalent iff one can transform the first into the second using **Tietze transformations**:

## Equivalence between theories

Two theories are equivalent iff one can transform the first into the second using **Tietze transformations**:

1. add a definable generator

$$\langle G \mid R \rangle \rightsquigarrow \langle G, f : n \mid R, f(x_1, \dots, x_n) = t \rangle$$

### Example

The theory of groups can be axiomatized without or with unit:

$$\begin{array}{c} \langle m : 2, i : 1 \mid \dots \rangle \\ \Downarrow \\ \langle m : 2, i : 1, e : 0 \mid \dots, e = m(x, i(x)) \rangle \end{array}$$

## Equivalence between theories

Two theories are equivalent iff one can transform the first into the second using **Tietze transformations**:

1. add a definable generator

$$\langle G \mid R \rangle \rightsquigarrow \langle G, f : n \mid R, f(x_1, \dots, x_n) = t \rangle$$

2. remove a definable generator

### Example

The theory of groups can be axiomatized without or with unit:

$$\begin{array}{c} \langle m : 2, i : 1 \mid \dots \rangle \\ \updownarrow \\ \langle m : 2, i : 1, e : 0 \mid \dots, e = m(x, i(x)) \rangle \end{array}$$

## Equivalence between theories

Two theories are equivalent iff one can transform the first into the second using **Tietze transformations**:

1. add a definable generator

$$\langle G \mid R \rangle \rightsquigarrow \langle G, f : n \mid R, f(x_1, \dots, x_n) = t \rangle$$

2. remove a definable generator
3. add a derivable relation

$$\langle G \mid R \rangle \rightsquigarrow \langle G \mid R, t = t' \rangle$$

### Example

We can add derivable relations to the theory of groups:

$$\begin{aligned} &\langle m : 2, i : 1, e : 0 \mid \dots \rangle \\ &\quad \quad \quad \downarrow \\ &\langle m : 2, i : 1, e : 0 \mid \dots, m(e, e) = e \rangle \end{aligned}$$

## Equivalence between theories

Two theories are equivalent iff one can transform the first into the second using **Tietze transformations**:

1. add a definable generator

$$\langle G \mid R \rangle \rightsquigarrow \langle G, f : n \mid R, f(x_1, \dots, x_n) = t \rangle$$

2. remove a definable generator
3. add a derivable relation

$$\langle G \mid R \rangle \rightsquigarrow \langle G \mid R, t = t' \rangle$$

4. remove a definable relation

### Example

We can add derivable relations to the theory of groups:

$$\begin{array}{c} \langle m : 2, i : 1, e : 0 \mid \dots \rangle \\ \Downarrow \\ \langle m : 2, i : 1, e : 0 \mid \dots, m(e, e) = e \rangle \end{array}$$

# Finding small axiomatizations

Can we find minimal (or small) axiomatizations for theories?

## One relation for (abelian) groups



In 1938, Tarski observed that the theory of abelian groups can be axiomatized with two operations  $d : 2, a : 0$  and one relation

$$d(x_1, d(x_2, d(x_3, d(x_1, x_2)))) = x_3$$

where  $a$  ensure that the model is not empty.

A **one-based** theory is a theory which can be axiomatized with only one axiom.

# Remarks

Note that obtaining the axiom

$$d(x_1, d(x_2, d(x_3, d(x_1, x_2)))) = x_3$$

is not easy

- ▶ one has to think of using division instead of multiplication (there is no unique axiom with multiplication and unit)
- ▶ one has to show that this axiom is derivable and the other can be derived from it

254

A. Tarski:

Der Beweis ist entbehrlich: es handelt sich ja um Formeln, deren Gültigkeit innerhalb der Theorie der Abel'schen Gruppen offenkundig ist.

Satz 1 läßt sich folgendermaßen umkehren:

Satz 2. Es sei  $G$  eine beliebige Menge und  $a-b$  eine binäre Operation. Sind für beliebige Elemente  $a, b, e \in G$  die Formeln 1.1, 1.2 und 1.3 oder auch 1.1 und 1.4 erfüllt und bestimmt man die binäre Operation  $+$  durch die Formel 1.5, so wird  $G$  zu einer Abel'schen Gruppe mit der Grundoperation  $+$ ; dabei ist  $a-b$  (für beliebige  $a, b \in G$ ) mit dem einzigen Element  $x \in G$  identisch, für das  $a = b + x$  ist.

Beweis. Wir nehmen zunächst an, daß 1.1 und 1.4 erfüllt sind, und leiten daraus 1.2 und 1.3 ab:

- |      |  |                 |
|------|--|-----------------|
| (1)  | $a - \{b - [(e-b) - (a-b)]\} = e - b.$                           | [Nach 1.1, 1.4] |
| (2)  | $b - \{[(e-b) - (a-b)] - \{a - \{b - [(e-b) - (a-b)]\}\}\} = a.$ | [Nach 1.4]      |
| (3)  | $b - \{[(e-b) - (a-b)] - (e-b)\} = a.$                           | [Nach (2), (1)] |
| (4)  | $e - \{b - \{[(e-b) - (a-b)] - (e-b)\}\} = (e-b) - (a-b).$       | [Nach 1.4]      |
| (5)  | $e - a = (e-b) - (a-b).$   | [Nach (4), (3)] |
| (6)  | $a - [b - (e-a)] = e - b.$                                       | [Nach (1), (5)] |
| (7)  | $b - [e - (a-b)] = a - e.$                                       | [Nach (6)]      |
| (8)  | $a - (a - e) = e.$   | [Nach 1.4, (7)] |
| (9)  | $b - \{b - [e - (a-b)]\} = e - (a-b).$                           | [Nach (8)]      |
| (10) | $b - (a - e) = e - (a-b).$                                       | [Nach (9), (7)] |

Aus (8) und (10) ergeben sich sofort 1.2 und 1.3.  
 Wie man leicht aus 1.1, 1.2 und 1.3 die Multiplikation  $\cdot$  ableiten kann, ist ebenfalls leicht zu zeigen.

Beitrag zur Axiomatik der Abel'schen Gruppen 255

- |      |  |                         |
|------|--|-------------------------|
| (20) | $a + (b - e) = a - \{(a-a) - (b-e)\}.$                   | [Nach 1.5]              |
| (21) | $(a-a) - (b-e) = e - \{b - (a-a)\}.$                     | [Nach 1.3]              |
| (22) | $(a-a) - (b-e) = e - b.$                                 | [Nach (21), (13)]       |
| (23) | $a + (b-e) = a - (e-b).$                                 | [Nach (10), (22)]       |
| (24) | $a - (e-b) = b - (e-a).$                                 | [Nach 1.3]              |
| (25) | $b + (a-e) = b - (e-a).$                                 | [Nach (23)]             |
| (26) | $a + (b-e) = b + (a-e).$                                 | [Nach (23), (24), (25)] |
| (27) | $a + \{b - [(b-b) - e]\} = b + \{a - [(b-b) - e]\}.$     | [Nach (26)]             |
| (28) | $a + \{b - [(b-b) - e]\} = b + \{a - [(a-a) - e]\}.$     | [Nach (27), (15)]       |
| (29) | $b + e = b - [(b-b) - e]$ und $a + e = a - [(a-a) - e].$ | [Nach 1.5]              |
| (30) | $a + (b + e) = b + (a + e).$                             | [Nach (28), (29)]       |
| (31) | $a + e = e + a.$   | [Nach (19)]             |
| (32) | $a + (b + e) = b + (e + a).$                             | [Nach (30), (31)]       |
| (33) | $b + (e + a) = e + (b + a).$                             | [Nach (30)]             |
| (34) | $b + (e + a) = e + (a + b).$                             | [Nach (33), (19)]       |
| (35) | $e + (a + b) = (a + b) + e.$                             | [Nach (19), (11)]       |
| (36) | $a + (b + e) = (a + b) + e.$                             | [Nach (32), (34), (35)] |
| (37) | $b + (a - b) = b - (b - a).$                             | [Nach (23)]             |
| (38) | $b - (b - a) = a.$                                       | [Nach 1.2]              |
| (39) | $b + (a - b) = a.$                                       | [Nach (37), (38)]       |
| (40) | $b - \{b - [(b-b) - e]\} = (b-b) - e.$                   | [Nach 1.2]              |
| (41) | $b - (b + e) = (b-b) - e.$                               | [Nach (40), (29)]       |
| (42) | $(b-b) - \{(b-b) - e\} = e.$                             | [Nach 1.2]              |
| (43) | $(b-b) - (b - (b + e)) = e.$                             | [Nach (42), (41)]       |



## Remarks

In fact the story is not entirely exact:

- ▶ the models of

$$\langle m : 2, i : 1, e : 0 \mid \dots \rangle$$

and

$$\langle d : 2, a : 0 \mid \text{one relation} \rangle$$

are the “same”,

## Remarks

In fact the story is not entirely exact:

- ▶ the models of

$$\langle m : 2, i : 1, e : 0 \mid \dots \rangle$$

and

$$\langle d : 2, a : 0 \mid \text{one relation} \rangle$$

are the “same”,

- ▶ but morphisms are not (they have to preserve the arbitrary element  $a$  in the second case),

## Remarks

In fact the story is not entirely exact:

- ▶ the models of

$$\langle m : 2, i : 1, e : 0 \mid \dots \rangle$$

and

$$\langle d : 2, a : 0 \mid \text{one relation} \rangle$$

are the “same”,

- ▶ but morphisms are not (they have to preserve the arbitrary element  $a$  in the second case),
- ▶ so they are not equivalent in the earlier sense,

## Remarks

In fact the story is not entirely exact:

- ▶ the models of

$$\langle m : 2, i : 1, e : 0 \mid \dots \rangle$$

and

$$\langle d : 2, a : 0 \mid \text{one relation} \rangle$$

are the “same”,

- ▶ but morphisms are not (they have to preserve the arbitrary element  $a$  in the second case),
- ▶ so they are not equivalent in the earlier sense,

but you get the idea...

# The quest for one-based theories

There is an interesting line of efforts to find one-based theories:

- ▶ 1938: abelian groups is one-based
- ▶ 1952: groups is one-based
- ▶ 1965: semi-lattices is not one-based
- ▶ 1970: distributive lattices is not one-based  
lattices is one-based (300 000 sym. / 34 var.)
- ▶ 1973: boolean algebras is one-based ( $\geq 40\,000\,000$  symb.)
- ▶ 2002: boolean algebras is one-based (12 symb.)
- ▶ 2003: lattices is one-based (29 symb. / 8 var.)
- ▶ ...

## AXIOMS FOR SEMI-LATTICES

D. H. Potts

A semi-lattice (Birkhoff, Lattice Theory, p. 18, Ex. 1) is an algebra  $\langle A, . \rangle$  with a single binary operation satisfying: (1)  $x = xx$ , (2)  $xy = yx$ , and (3)  $(xy)z = x(yz)$ . In this note we show that the three identities may be reduced to two but cannot be reduced to one.

It is easy to see that (2), (3) imply (4)  $(uv)((wx)(yz)) = ((vu)(xw))(zy)$ . Setting  $w = y = u$  and  $x = z = v$  in (4) and using (1) we get  $uv = vu$ . Setting  $v = u$ ,  $x = w$ , and  $z = y$  in (4) and using (1) we get  $u(wy) = (uw)y$ . And so (1) and (4) imply (2) and (3).

If a single identity is sufficient to define the notion of semi-lattice it must be of form  $x = \dots$ . Any identity not of that form is satisfied by, e. g. the algebra  $\langle \{0, 1\}, . \rangle$  where  $00 = 01 = 10 = 11 = 0$ , which is not a semi-lattice.

Now suppose we have a semi-lattice with two distinct elements  $a, b$ . Let  $c = ab$ . Either  $c \neq a$  or  $c \neq b$ . We suppose the latter. Then  $bb = b$  and  $bc = cb = cc = c$ . Thus any identity holding in a semi-lattice with at least two elements must have the same variables occurring on each side of the equality sign. For suppose "x" occurs on the left but not on the right. Setting  $x = c$  and all other variables equal to  $b$  yields the contradiction  $c = b$ .

Thus a single sufficing identity would have to be of form  $x = f(x)$ . Clearly such an identity will not imply (2), for the algebra  $\langle \{0, 1\}, . \rangle$  where  $00 = 01 = 0$  and  $10 = 11 = 1$  satisfies  $x = f(x)$  for any  $f$  but is not commutative.

## Axioms for semi-lattices

A **semi-lattice** is a set equipped with a multiplication such that

$$(xy)z = x(yz)$$

$$xy = yx$$

$$xx = x$$

1. any axiom should be of the form  $x = t$  otherwise the non-semi-lattice

$\cdot$	$0$	$1$
$0$	$0$	$0$
$1$	$0$	$0$

would be a model

## Axioms for semi-lattices

A **semi-lattice** is a set equipped with a multiplication such that

$$(xy)z = x(yz)$$

$$xy = yx$$

$$xx = x$$

1. any axiom should be of the form  $x = t$
2. any axiom  $t = u$  should have  $FV(t) = FV(u)$  otherwise the semi-lattice

$\cdot$	$0$	$1$
$0$	$0$	$1$
$1$	$1$	$1$

would not be a model



## Axioms for semi-lattices

A **semi-lattice** is a set equipped with a multiplication such that

$$(xy)z = x(yz)$$

$$xy = yx$$

$$xx = x$$

1. any axiom should be of the form  $x = t$
2. any axiom  $t = u$  should have  $FV(t) = FV(u)$
3. the axiom cannot be of the form  $x = t(x)$  otherwise the non-semi-lattice

$\cdot$		0	1
0		0	0
1		1	1

would be a model

# Axioms for semi-lattices

A **semi-lattice** is a set equipped with a multiplication such that

$$(xy)z = x(yz)$$

$$xy = yx$$

$$xx = x$$

1. any axiom should be of the form  $x = t$
2. any axiom  $t = u$  should have  $FV(t) = FV(u)$
3. the axiom cannot be of the form  $x = t(x)$
4. we can also show that any other choice of generators suffers from the same problem!

# Not one-based theories

We are interested in showing that theories are *not* one-based:

- ▶ existing proofs are tricky and specific to particular theories
- ▶ they rely on finding counter-examples using some models

Here, instead

- ▶ we provide a method which is entirely automatic
- ▶ but it does not provide an answer in every case

# The general method

## Algorithm

1. start from a theory  $\mathcal{T}$ ,

# The general method

## Algorithm

1. start from a theory  $\mathcal{T}$ ,
2. orient it so that you get a terminating and confluent rewriting system,

# The general method

## Algorithm

1. start from a theory  $\mathcal{T}$ ,
2. orient it so that you get a terminating and confluent rewriting system,
3. feed it to the computer and compute

$$H_2(\mathcal{T}) \in \mathbb{N}$$

# The general method

## Algorithm

1. start from a theory  $\mathcal{T}$ ,
2. orient it so that you get a terminating and confluent rewriting system,
3. feed it to the computer and compute

$$H_2(\mathcal{T}) \in \mathbb{N}$$

4. we know that we need at least  $H_2(\mathcal{T})$  relations.

# The general method

## Algorithm

1. start from a theory  $\mathcal{T}$ ,
2. orient it so that you get a terminating and confluent rewriting system,
3. feed it to the computer and compute

$$H_2(\mathcal{T}) \in \mathbb{N}$$

4. we know that we need at least  $H_2(\mathcal{T})$  relations.

Note that:

- ▶ the theory might not be orientable as a convergent rs,
- ▶ we might compute  $H_2(\mathcal{T}) = 0$ ,
- ▶ we have examples where it works though :)

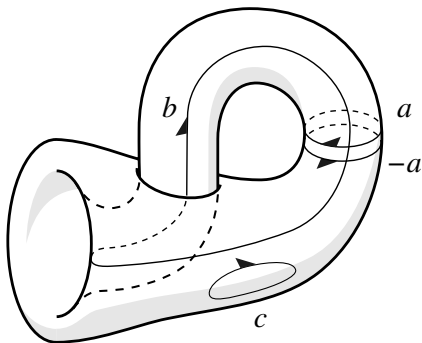


Good!

Let's switch to something else.

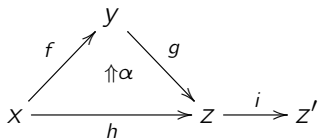
Suppose that you have a space (e.g. a simplicial complex) and you want to compute the number of “holes” in it. There is a very efficient way of doing this:

## homology



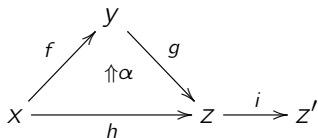
# Homology

Suppose that our space looks like this:



# Homology

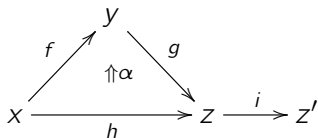
Suppose that our space looks like this:



- ▶ we allow taking linear combinations of “building blocks”

# Homology

Suppose that our space looks like this:



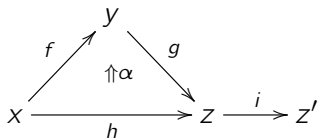
- ▶ we allow taking linear combinations of “building blocks”
- ▶ we define the boundary of a block as target - source:

$$\partial(f) = y - x$$

$$\partial(\alpha) = f + g - h$$

# Homology

Suppose that our space looks like this:



- ▶ we allow taking linear combinations of “building blocks”
- ▶ we define the boundary of a block as target - source:

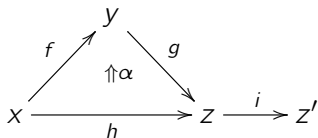
$$\partial(f) = y - x \qquad \partial(\alpha) = f + g - h$$

- ▶ “potential holes” can be detected as those with empty boundary:

$$\begin{aligned} \partial(f + g - h) &= \partial(f) + \partial(g) - \partial(h) \\ &= (y - x) + (z - y) - (z - x) = 0 \end{aligned}$$

# Homology

Suppose that our space looks like this:



- ▶ we allow taking linear combinations of “building blocks”
- ▶ we define the boundary of a block as target - source:

$$\partial(f) = y - x \qquad \partial(\alpha) = f + g - h$$

- ▶ “potential holes” can be detected as those with empty boundary:

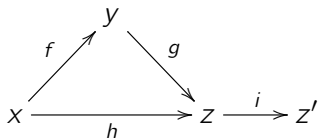
$$\begin{aligned} \partial(f + g - h) &= \partial(f) + \partial(g) - \partial(h) \\ &= (y - x) + (z - y) - (z - x) = 0 \end{aligned}$$

- ▶ we have to remove those that are boundaries

$$\partial(\alpha) = f + g - h$$

# Homology

Suppose that our space looks like this:



- ▶ we allow taking linear combinations of “building blocks”
- ▶ we define the boundary of a block as target - source:

$$\partial(f) = y - x \qquad \partial(\alpha) = f + g - h$$

- ▶ “potential holes” can be detected as those with empty boundary:

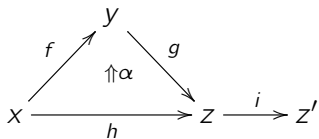
$$\begin{aligned} \partial(f + g - h) &= \partial(f) + \partial(g) - \partial(h) \\ &= (y - x) + (z - y) - (z - x) = 0 \end{aligned}$$

- ▶ we have to remove those that are boundaries



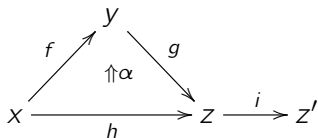
# Homology

Formally, given our space  $X$ :



# Homology

Formally, given our space  $X$ :



we consider the **chain complex**

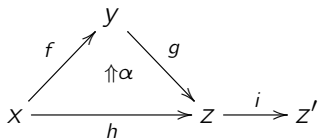
$$\begin{array}{ccccc} \dots & \xrightarrow{\partial_2} & \mathbb{k}\{\alpha\} & \xrightarrow{\partial_1} & \mathbb{k}\{f, g, h, i\} & \xrightarrow{\partial_0} & \mathbb{k}\{x, y, z, z'\} \\ & & \parallel & & \parallel & & \parallel \\ & & C_2 & & C_1 & & C_0 \end{array}$$

which means that

- ▶ the  $C_i$  are  $\mathbb{k}$ -vector spaces,
- ▶ the  $\partial_i : C_{i+1} \rightarrow C_i$  are linear maps,
- ▶ we have  $\partial_{i-1} \circ \partial_i = 0$  and thus  $\text{im } \partial_i \subseteq \ker \partial_{i-1}$ .

# Homology

Formally, given our space  $X$ :



we consider the **chain complex**

$$\begin{array}{ccccc} \dots & \xrightarrow{\partial_2} & \mathbb{k}\{\alpha\} & \xrightarrow{\partial_1} & \mathbb{k}\{f, g, h, i\} & \xrightarrow{\partial_0} & \mathbb{k}\{x, y, z, z'\} \\ & & \parallel & & \parallel & & \parallel \\ & & C_2 & & C_1 & & C_0 \end{array}$$

and we can compute  $i$ -th **homology groups**:

$$H_i(X) = \ker \partial_{i-1} / \operatorname{im} \partial_i$$

The intuition is that the rank of  $H_i(X)$  counts the number of holes in dimension  $i$ .

# Homology

The  $i$ -th homology group is defined by

$$H_i(X) = \ker \partial_{i-1} / \operatorname{im} \partial_i$$

with

$$\partial_i : C_{i+1} \rightarrow C_i$$

In particular, we have that

$$\dim(C_i) \geq \dim(H_i(X))$$

i.e.

$$C_i = \mathbb{k}\{x_1, \dots, x_n\}$$

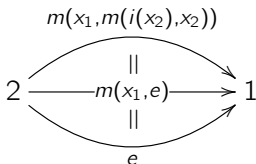
with

$$n \geq \dim(H_i(X))$$

## A theory as a space

Suppose that we can see a theory  $\mathcal{T}$  as a “space” with

- ▶ points:  $\mathbb{N}$
- ▶ edges: operations
- ▶ surfaces: relations
- ▶ volumes: relations between relations (e.g. critical pairs)



then

$$\dim(H_2(\mathcal{T}))$$

is a lower bound on the number of relations!

NB: in practice, we will consider a chain complex as a space...

## An example

Consider the term rewriting system with a generators

$$f : 2 \quad g : 2 \quad a : 0 \quad b : 0 \quad c : 0$$

together with rules

$$\begin{array}{ll} A & : \quad f(a, x_1) \Rightarrow g(a, x_1) \quad A' & : \quad f(x_1, a) \Rightarrow g(x_1, a) \\ B & : \quad f(b, b) \Rightarrow g(b, b) \quad C & : \quad f(c, c) \Rightarrow g(c, c) \end{array}$$

## An example

Consider the term rewriting system with a generators

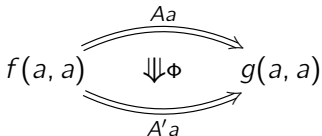
$$f : 2 \quad g : 2 \quad a : 0 \quad b : 0 \quad c : 0$$

together with rules

$$A : f(a, x_1) \Rightarrow g(a, x_1) \quad A' : f(x_1, a) \Rightarrow g(x_1, a)$$

$$B : f(b, b) \Rightarrow g(b, b) \quad C : f(c, c) \Rightarrow g(c, c)$$

It is terminating with one confluent critical pair



## An example

Note that all the rules

$$A : f(a, x_1) \Rightarrow g(a, x_1) \quad A' : f(x_1, a) \Rightarrow g(x_1, a)$$

$$B : f(b, b) \Rightarrow g(b, b) \quad C : f(c, c) \Rightarrow g(c, c)$$

have the same “balance”:

$$\partial_1(A) = g + a - f - a = g - f$$



## An example

Note that all the rules

$$A : f(a, x_1) \Rightarrow g(a, x_1) \quad A' : f(x_1, a) \Rightarrow g(x_1, a)$$

$$B : f(b, b) \Rightarrow g(b, b) \quad C : f(c, c) \Rightarrow g(c, c)$$

have the same “balance”:

$$\begin{aligned} \partial_1(A) &= g + a - f - a = g - f \\ &= \partial_1(A') = \partial_1(B) = \partial_1(C) \end{aligned}$$

## An example

Note that all the rules

$$\begin{array}{ll} A & : \quad f(a, x_1) \Rightarrow g(a, x_1) \\ B & : \quad f(b, b) \Rightarrow g(b, b) \end{array} \quad \begin{array}{ll} A' & : \quad f(x_1, a) \Rightarrow g(x_1, a) \\ C & : \quad f(c, c) \Rightarrow g(c, c) \end{array}$$

have the same “balance”:

$$\begin{aligned} \partial_1(A) &= g + a - f - a = g - f \\ &= \partial_1(A') = \partial_1(B) = \partial_1(C) \end{aligned}$$

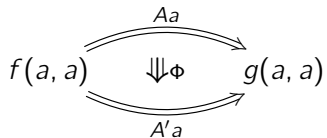
so that we have

$$\begin{aligned} \partial_1(A' - A) &= \partial_1(A') - \partial_1(A) = 0 \\ \partial_1(B - A) &= \partial_1(B) - \partial_1(A) = 0 \\ \partial_1(C - A) &= \partial_1(C) - \partial_1(A) = 0 \end{aligned}$$

i.e. there are 3 “potential holes”.

## An example

Similarly, the “balance” of the critical pair

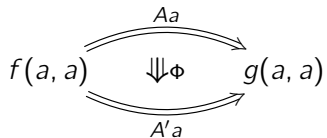


is

$$\partial_2(\Phi) = A' - A$$

## An example

Similarly, the “balance” of the critical pair



is

$$\partial_2(\Phi) = A' - A$$

Therefore, we have in fact two holes:

$$\cancel{A' - A}$$

$$B - A$$

$$C - A$$

## An example

Similarly, the “balance” of the critical pair

$$\begin{array}{ccc}
 & \xrightarrow{Aa} & \\
 f(a, a) & \Downarrow \Phi & g(a, a) \\
 & \xrightarrow{A'a} &
 \end{array}$$

is

$$\partial_2(\Phi) = A' - A$$

Therefore, we have in fact two holes:

$$\cancel{A' - A} \quad B - A \quad C - A$$

The vector space generated by these two holes is a subspace of the one generated by rules

$$H_2(\mathcal{T}) \subseteq C_2$$

and therefore we need at least two rules to present the theory.

## An example

For “technical” reasons, we will need to first recall the contexts when computing the balance. With

$$A \quad : \quad f(a, x_1) \Rightarrow g(a, x_1)$$

we first compute

$$\partial_1(A) \quad = \quad \underline{g}(a, x_1) + g(\underline{a}, x_1) - \underline{f}(a, x_1) - f(\underline{a}, x_1)$$

and then deduce

$$\partial_1(A) \quad = \quad g + a - f - a \quad = \quad g - f$$

# Invariance under axiomatization

Why do we need to use such tools?

- ▶ A fundamental property of homology is that  
homology is invariant under weak equivalences  
(= deformations of spaces)

# Invariance under axiomatization

Why do we need to use such tools?

- ▶ A fundamental property of homology is that

homology is invariant under weak equivalences

(= deformations of spaces)

- ▶ In the setting of theories, this will translate as

*homology is invariant under Tietze transformations*

i.e. we have bounds on *any* axiomatization of the theory



# Invariance under axiomatization

Why do we need to use such tools?

- ▶ A fundamental property of homology is that

homology is invariant under weak equivalences

(= deformations of spaces)

- ▶ In the setting of theories, this will translate as

*homology is invariant under Tietze transformations*

i.e. we have bounds on *any* axiomatization of the theory

- ▶ This is where we need the assumption that we have a convergent rewriting system!

## The balance of rules

Note that reductions can duplicate (or erase) other, e.g. with

$$F : f(x) \Rightarrow g(x, x) \qquad A : a \Rightarrow b$$

we have two equal paths

$$\begin{array}{ccc} f(a) & \xrightarrow{A} & f(b) \\ \Downarrow F & \cong & \Downarrow F \\ g(a, a) & \xrightarrow{A} g(b, a) \xrightarrow{A} & g(b, b) \end{array}$$

So, we cannot simply “count” the number of uses of each rule.

# HOMOLOGY OF LAWVERE THEORIES

## Lawvere theories

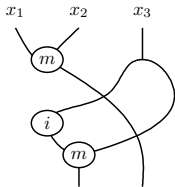
All the operations described by a Lawvere theory can be encoded into a category called a **Lawvere theory**:

- ▶ objects: natural numbers
- ▶ morphisms  $m \rightarrow n$ :  $n$ -uples of terms with variables in  $\{x_1, \dots, x_m\}$  up to the relations
- ▶ composition: substitution

### Example

In the theory of groups, we have the morphism

$$\langle m(i(x_3), x_3), m(x_1, x_2) \rangle : 3 \rightarrow 2$$



# Lawvere theories

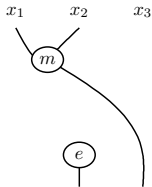
All the operations described by a Lawvere theory can be encoded into a category called a **Lawvere theory**:

- ▶ objects: natural numbers
- ▶ morphisms  $m \rightarrow n$ :  $n$ -uples of terms with variables in  $\{x_1, \dots, x_m\}$  up to the relations
- ▶ composition: substitution

## Example

In the theory of groups, we have the morphism

$$\langle \quad e \quad , \quad m(x_1, x_2) \quad \rangle : 3 \rightarrow 2$$



## Lawvere theories

All the operations described by a Lawvere theory can be encoded into a category called a **Lawvere theory**:

- ▶ objects: natural numbers
- ▶ morphisms  $m \rightarrow n$ :  $n$ -uples of terms with variables in  $\{x_1, \dots, x_m\}$  up to the relations
- ▶ composition: substitution

### Remark

The notion of equivalence can be changed from

- ▶ having the same models

to

- ▶ generating the same Lawvere theory

# Lawvere theories

## Definition

A **Lawvere theory** is a category

- ▶ whose objects are natural numbers
- ▶ cartesian with product given by addition

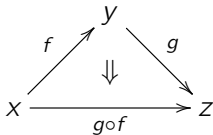
We write **Theories** for their category.

So, the question is, given  $\mathcal{T} \in \mathbf{Theories}$ , how do we define  $H_i(\mathcal{T})$ ?

# Homology of categories

To any category  $\mathcal{C}$  one can associate its **nerve**  $N\mathcal{C}$ :

- ▶ points: objects
- ▶ edges: morphisms
- ▶ triangles:



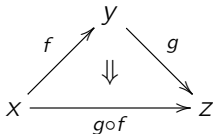
- ▶ etc.



# Homology of categories

To any category  $\mathcal{C}$  one can associate its **nerve**  $NC$ :

- ▶ points: objects
- ▶ edges: morphisms
- ▶ triangles:



- ▶ etc.

## Problem

*Since a Lawvere theory  $\mathcal{C}$  has a terminal object, we always have*

$$H_i(NC) = 0$$

*for  $i > 0$ .*

# Contexts

A **context**  $C$  is a term which contains exactly one instance of the “variable”  $\square$ .

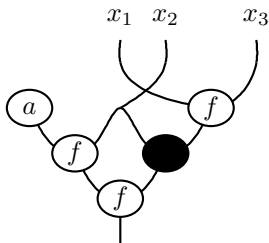
For instance,

$$f(g(x_1, x_2), \square)$$

## Contexts

A **bicontext** is a term with one “inside hole”.

For instance  $f(f(a, x_2), \bullet(x_2, f(x_1, x_3)))$



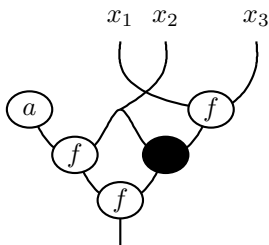
of type

$$2 \rightarrow 3$$

We write  $\mathcal{K}$  for the category of bicontexts.

# Contexts

A **bicontext**  $(C, u)$  consists of a context  $C$  and a morphism  $u$ :



is decomposed as

$$f(f(a, x_2), \square) \quad , \quad \langle x_2, f(x_1, x_3) \rangle$$

a context

a substitution

# The ringoid of bicontexts

A **ringoid**  $\mathcal{R}$  is a category enriched in **Ab**:

- ▶ each  $\mathcal{C}(A, B)$  has a structure of group
- ▶ the expected compatibility laws hold:

$$(g + g') \circ (f + f') = g \circ f + g \circ f' + g' \circ f + g' \circ f'$$

$$0 \circ f = 0$$

$$f \circ 0 = 0$$

# The ringoid of bicontexts

A **ringoid**  $\mathcal{R}$  is a category enriched in **Ab**:

- ▶ each  $\mathcal{C}(A, B)$  has a structure of group
- ▶ the expected compatibility laws hold:

$$(g + g') \circ (f + f') = g \circ f + g \circ f' + g' \circ f + g' \circ f'$$

$$0 \circ f = 0$$

$$f \circ 0 = 0$$

(a ringoid with one object is a ring)

# The ringoid of bicontexts

A **ringoid**  $\mathcal{R}$  is a category enriched in **Ab**:

- ▶ each  $\mathcal{C}(A, B)$  has a structure of group
- ▶ the expected compatibility laws hold:

$$(g + g') \circ (f + f') = g \circ f + g \circ f' + g' \circ f + g' \circ f'$$

$$0 \circ f = 0$$

$$f \circ 0 = 0$$

(a ringoid with one object is a ring)

We write  $\mathbb{Z}\mathcal{K}$ : the **free ringoid** over bicontexts, *modulo the rules*.

# The ringoid of bicontexts

A **ringoid**  $\mathcal{R}$  is a category enriched in **Ab**:

- ▶ each  $\mathcal{C}(A, B)$  has a structure of group
- ▶ the expected compatibility laws hold:

$$(g + g') \circ (f + f') = g \circ f + g \circ f' + g' \circ f + g' \circ f'$$

$$0 \circ f = 0$$

$$f \circ 0 = 0$$

(a ringoid with one object is a ring)

We write  $\mathbb{Z}\mathcal{K}$ : the **free ringoid** over bicontexts, *modulo the rules*.

(there is a subtlety here since rules are not necessarily linear)



## Contexts from terms

Given a term  $t$ , we write  $\kappa_i(t)$  for the formal sum of contexts obtained from  $t$  by replacing one instance of  $x_i$  with  $\square$ .

For instance,

$$\kappa_1(f(g(x_1, x_2), x_1)) = f(g(\square, x_2), x_1) + f(g(x_1, x_2), \square)$$

and

$$\kappa_3(f(g(x_1, x_2), x_1)) = 0$$

## Contexts from terms

Given a term  $t$ , we write  $\kappa_i(t)$  for the formal sum of contexts obtained from  $t$  by replacing one instance of  $x_i$  with  $\square$ .

For instance,

$$\kappa_1(f(g(x_1, x_2), x_1)) = f(g(\square, x_2), x_1) + f(g(x_1, x_2), \square)$$

and

$$\kappa_3(f(g(x_1, x_2), x_1)) = 0$$

Formally,

$$\kappa_i(x_i) = \square \quad \kappa_i(x_j) = 0 \quad \kappa_i(u \circ t) = \sum_{j \in \text{FV}(u)} (\kappa_j(u)t)[\kappa_i(t_j)]$$

where  $C[t]$  is  $C$  with  $\square$  replaced by  $t$ .

## The ringoid of bicontexts

In a bicontext  $(C, u)$ , we consider  $C$  modulo

$$\kappa_i(t) - \kappa_i(u)$$

and  $u$  modulo  $t - u$  for each rule  $R : t \Rightarrow u$ .

For instance, the relation  $f(x_1) \Rightarrow g(x_1, x_1)$  induces the relation

$$g(\square, x_1) + g(x_1, \square) - f(\square)$$

on contexts.

# The ringoid of bicontexts

## Lemma

$\mathbb{Z}\mathcal{K}$  only depends on the theory  $\mathcal{T}$  (not the presentation).

# Modules

A **module** over  $\mathbb{Z}\mathcal{K}$  is an **Ab**-enriched functor

$$\mathcal{M} : \mathbb{Z}\mathcal{K} \rightarrow \mathbf{Ab}$$

This means that we have things that

- ▶ we can add
- ▶ we can put into a bicontext

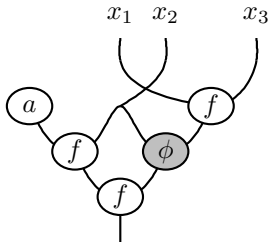
Given  $(C, u) : m \rightarrow n$  and  $t \in \mathcal{M}(m)$ , we write

$$C[t]u = (\mathcal{M}(C, u))(t)$$

# Free modules

Given a family  $(X_n)_{n \in \mathbb{N}}$  of sets, whose elements are “ $n$ -ary things”, we can form the **free  $\mathbb{Z}\mathcal{K}$ -module  $\mathbb{Z}\mathcal{K}\underline{X}_n$** .

For instance, we have



with  $\phi \in X_2$ .

## The trivial module

We also have a **trivial  $\mathbb{Z}\mathcal{K}$ -module**  $\mathcal{Z}$ .

This is the quotient of the free  $\mathbb{Z}\mathcal{K}$ -module generated by one operation  $\star_n$  in each arity  $n$  by

$$\sum_i \kappa_i(v) \star_1 u_i = \star_n$$

for each term  $v \circ u$  of arity  $n$ .

## The trivial module

We also have a **trivial  $\mathbb{Z}\mathcal{K}$ -module  $\mathcal{Z}$** .

This is the quotient of the free  $\mathbb{Z}\mathcal{K}$ -module generated by one operation  $\star_n$  in each arity  $n$  by

$$\sum_i \kappa_i(v) \star_1 u_i = \star_n$$

for each term  $v \circ u$  of arity  $n$ .

For instance, with  $f$  of arity 2,  $f \circ \text{id}_2 = \text{id}_1 \circ f$  implies

$$f(\square, x_2) \star_1 x_1 + f(x_1, \square) \star_1 x_2 = \star_2 = \square \star_1 f(x_1, x_2)$$



## The trivial module

We also have a **trivial  $\mathbb{Z}\mathcal{K}$ -module**  $\mathcal{Z}$ .

This is the quotient of the free  $\mathbb{Z}\mathcal{K}$ -module generated by one operation  $\star_n$  in each arity  $n$  by

$$\sum_i \kappa_i(v) \star_1 u_i = \star_n$$

for each term  $v \circ u$  of arity  $n$ .

Note that for every  $\mathbb{Z}\mathcal{K}$ -module  $\mathcal{M}$  we have

$$\partial_{-1}: \mathcal{M} \rightarrow \mathcal{Z}$$

defined by  $\varepsilon(t) = \star_n$  for  $t \in \mathcal{M}n$ .

# Resolutions

Suppose given a theory  $\mathcal{T}$  presented by a convergent algebraic theory (= term rewriting system) with

- ▶  $P_1$  as rules
- ▶  $P_2$  as relations
- ▶  $P_3$  as critical pairs

## Theorem

We have a partial free resolution, i.e. a complex

$$\mathbb{Z}\mathcal{K}\underline{P}_3 \xrightarrow{\partial_2} \mathbb{Z}\mathcal{K}\underline{P}_2 \xrightarrow{\partial_1} \mathbb{Z}\mathcal{K}\underline{P}_1 \xrightarrow{\partial_0} \mathbb{Z}\mathcal{K}\underline{1} \xrightarrow{\partial_{-1}} \mathcal{Z} \longrightarrow 0$$

of  $\mathcal{Z}$  by  $\mathbb{Z}\mathcal{K}$ -modules where

- ▶ the  $\partial_i$  are  $\mathbb{Z}\mathcal{K}$ -linear maps defined from source and target
- ▶  $\text{im } \partial_i = \ker \partial_{i-1}$

## Face maps

The face maps  $\partial_i : \mathbb{Z}\mathcal{K}P_{i+1} \rightarrow \mathbb{Z}\mathcal{K}P_i$  are defined by

“target”    –    “source”

e.g. for each rule  $R : t \Rightarrow u$  we have

$$\partial_1(\underline{R}) = \underline{u} - \underline{t}$$

# Homology

We define the **homology** (with trivial coefficients) of the theory  $\mathcal{T}$  as the homology of the deduced chain complex obtained by “erasing”  $\mathbb{Z}\mathcal{K}$ :

$$P_3 \xrightarrow{\partial'_2} P_2 \xrightarrow{\partial'_1} P_1 \xrightarrow{\partial'_0} 1$$

which means

$$H_i(\mathcal{T}) = \ker \partial_{i-1} / \operatorname{im} \partial_i$$

# Invariance

## Theorem

*The homology only depends on  $\mathcal{T}$ : if we started from another presentation we would have obtained the same homology.*

## Proof.

Between any two resolutions there is essentially one morphisms. Therefore any two deduced chain complexes (by “erasing”  $\mathbb{Z}\mathcal{K}$ ) are isomorphic and in particular the homologies are isomorphic.  $\square$

## Face maps (detailed)

The face maps  $\partial_i : \mathbb{Z}\mathcal{K}P_{i+1} \rightarrow \mathbb{Z}\mathcal{K}P_i$  are defined by

- ▶ for each  $t \in P_1$ , we have

$$\partial_0(\underline{t}) = \left( \sum_i \kappa_i(t) \underline{1} \langle x_i \rangle \right) - \underline{1}t$$

## Face maps (detailed)

The face maps  $\partial_i : \mathbb{Z}\mathcal{K}P_{i+1} \rightarrow \mathbb{Z}\mathcal{K}P_i$  are defined by

- ▶ for each  $t \in P_1$ , we have

$$\partial_0(\underline{t}) = \left( \sum_i \kappa_i(t) \underline{1} \langle x_i \rangle \right) - \underline{1}t$$

- ▶ for each rule  $R : t \Rightarrow u$  we have

$$\partial_1(\underline{R}) = \underline{u} - \underline{t}$$

with  $\underline{u \circ t} = \underline{u}t + \sum_{i=1}^n \kappa_i(u) t \underline{t}_i$

## Face maps (detailed)

The face maps  $\partial_i : \mathbb{Z}\mathcal{KP}_{i+1} \rightarrow \mathbb{Z}\mathcal{KP}_i$  are defined by

- ▶ for each  $t \in P_1$ , we have

$$\partial_0(\underline{t}) = \left( \sum_i \kappa_i(t) \underline{1} \langle x_i \rangle \right) - \underline{1}t$$

- ▶ for each rule  $R : t \Rightarrow u$  we have

$$\partial_1(\underline{R}) = \underline{u} - \underline{t}$$

with  $\underline{u \circ t} = \underline{ut} + \sum_{i=1}^n \kappa_i(u) t \underline{t}_i$

- ▶ for each critical pair

$$\partial_2 \left( \begin{array}{ccc} & t & \\ C_1[R_1]u_1 & \swarrow & \searrow C_2[R_2]u_2 \\ t_1 & & t_2 \\ S_1 & \swarrow & \searrow S_2 \\ & w & \end{array} \right) = C_2 \underline{R_2} u_2 + \underline{S_2} - C_1 \underline{R_1} u_1 - \underline{S_1}$$

with  $\underline{S \cdot R} = \underline{S} + \underline{R}$  and  $\underline{C[R]u} = C \underline{R} u$



## An example

- ▶ for  $f$  of arity 2, we have

$$\partial_0(\underline{f}) = f(\square, x_2)\underline{1} + f(x_1, \square)\underline{1} - \underline{1}f(x_1, x_2)$$

## An example

- ▶ for  $f$  of arity 2, we have

$$\partial_0(\underline{f}) = f(\square, x_2)\underline{1} + f(x_1, \square)\underline{1} - \underline{1}f(x_1, x_2)$$

- ▶ for a rule  $A : f(a, x_1) \Rightarrow g(a, x_1)$ , we have

$$\partial_1(\underline{A}) = \underline{g}\langle a, x_1 \rangle + g(\square, x_1)\underline{a} - \underline{f}\langle a, x_1 \rangle - f(\square, x_1)a$$

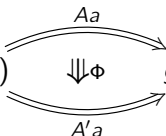
## An example

- ▶ for  $f$  of arity 2, we have

$$\partial_0(\underline{f}) = f(\square, x_2)\underline{1} + f(x_1, \square)\underline{1} - \underline{1}f(x_1, x_2)$$

- ▶ for a rule  $A : f(a, x_1) \Rightarrow g(a, x_1)$ , we have

$$\partial_1(\underline{A}) = \underline{g}\langle a, x_1 \rangle + g(\square, x_1)\underline{a} - \underline{f}\langle a, x_1 \rangle - f(\square, x_1)a$$

- ▶ for the critical pair  $f(a, a) \xrightarrow{Aa} g(a, a) \xleftarrow{A'a} f(a, a)$ , we have
- 

$$\partial_2(\underline{\Phi}) = \underline{A'}a - \underline{A}a$$

## About coefficients

How do we know that  $\mathbb{Z}\mathcal{K}$  is a “good” choice for coefficients?

- ▶ a theory  $\mathcal{T}$  is an object in the category **Theories** of Lawvere theories
- ▶ Beck discovered that coefficients should be taken in

**Ab(Theories/ $\mathcal{T}$ )**

- ▶ Jibladze–Pirashvily showed that this is equivalent to the category of *cartesian natural systems* in  $\mathcal{T}$
- ▶ the **category of factorizations** of  $\mathcal{T}$  is

$$\begin{array}{ccc} A & \xrightarrow{h_1} & B \\ f \downarrow & & \downarrow g \\ A' & \xrightarrow{h_2} & B' \end{array}$$

and **natural systems** are functors from it to **Ab**

- ▶ I presented a particular case of this

# CONCLUSION

# Conclusion

- ▶ we presented a generic method to compute lower bounds on generators / relations of a presentation of an algebraic theory
- ▶ it can serve to generate simple counter-examples
- ▶ it suggests considering higher-dimensional invariants
- ▶ most of the “usual” theories are out of reach for now ( $H_i(\mathcal{T}) = 0$ , commutativity, etc.)
- ▶ it suggests new research tracks in algebraic topology