Universal Algebra in HoTT

Andreas Lynge and Bas Spitters

Aarhus University

August 13, 2019

Introduction

- Universal algebra is a general study of algebraic structures. The results in universal algebra apply to all “algebras”, e.g. groups, rings, modules.
- We have formalized a part of universal algebra in the HoTT library for Coq, including the three isomorphism theorems.
- Based on the math-classes library.
- Type theoretic universal algebra often relies on setoids.
- We avoid setoids in the HoTT library, quotient sets are HITs.

Group

Example (Group)

A group is an h-set G : Set with

- unit $e : G$
- multiplication $\cdot : G \to G \to G$
- inversion $(-)^{-1} : G \to G$
- satisfying certain equations, e.g. $x \cdot x^{-1} = e$ for all $x : G$.

Group acting on a set

Example (Group)

A group is an h-set G : Set with

- unit $e : G$
- multiplication $\cdot : G \to G \to G$
- inversion $(-)^{-1} : G \to G$
- satisfying certain equations, e.g. $x \cdot x^{-1} = e$ for all $x : G$.

Example (Group acting on a set)

A group acting on a set is a group G and an h-set S with

- action $\alpha : G \to S \to S$
- $\alpha(x \cdot y) = \alpha(x) \circ \alpha(y)$
- $\alpha(e) = \mathrm{id}_S$

Signature

Definition (Signature)

A signature σ : Signature consists of

- $\mathsf{Sort}(\sigma) : \mathcal{U}$
- $\mathsf{Symbol}(\sigma) : \mathcal{U}$
- for each $u : \mathsf{Symbol}(\sigma)$, $\sigma_u : \mathsf{Sort}(\sigma) \times \mathsf{List}(\mathsf{Sort}(\sigma))$.

Algebra

Definition (Signature)

A signature σ : Signature consists of

- $\mathrm{Sort}(\sigma) : \mathcal{U}$
- $\mathrm{Symbol}(\sigma) : \mathcal{U}$
- for each $u : \mathrm{Symbol}(\sigma)$, $\sigma_u : \mathrm{Sort}(\sigma) \times \mathrm{List}(\mathrm{Sort}(\sigma))$.

Definition (Algebra)

An algebra $A : \mathrm{Algebra}(\sigma)$ for σ : Signature consists of

- for each $s : \mathrm{Sort}(\sigma)$, A_s : Set
- for each $u : \mathrm{Symbol}(\sigma)$, $u^A : A_{s_1} \to A_{s_2} \to \cdots \to A_{s_n}$, where $(s_1, [s_2, \ldots, s_n]) :\equiv \sigma_u$.

Example (Group acting on a set)

A group G acting on a set S,

- unit $e : G$
- multiplication $\cdot : G \to G \to G$
- inversion $(-)^{-1} : G \to G$
- action $\alpha : G \to S \to S$,

is an algebra A : Algebra(σ) for σ : Signature with

- Sort(σ) $\equiv \{g, s\}$
- Symbol(σ) $\equiv \{u, m, i, a\}$
- $\sigma_u \equiv (g, [])$, $\sigma_m \equiv (g, [g, g])$, $\sigma_i \equiv (g, [g])$, $\sigma_a \equiv (g, [s, s])$.

Carriers $A_g :\equiv G$ and $A_s :\equiv S$, and operations

- $u^A : A_g$ is unit
- $m^A : A_g \to A_g \to A_g$ is multiplication
- $i^A : A_g \to A_g$ is inversion
- $a^A : A_g \to A_s \to A_s$ is the action.

Let A, B, C : Algebra(σ).

Homomorphism

Let A, B, C : Algebra(σ).

Definition (Homomorphism)

A homomorphism $f : A \rightarrow B$ consists of

- $f_s : A_s \rightarrow B_s$ for all s : Sort(σ)
- $f_{s_t}(u^A(x_1, \ldots, x_n)) = u^B(f_{s_1}(x_1), \ldots, f_{s_n}(x_n))$,
  for all u : Symbol(σ).

Isomorphism

Let A, B, C : Algebra(σ).

Definition (Homomorphism)

A homomorphism $f : A \to B$ consists of

- $f_s : A_s \to B_s$ for all s : Sort(σ)
- $f_{s_t}(u^A(x_1, \ldots, x_n)) = u^B(f_{s_1}(x_1), \ldots, f_{s_n}(x_n))$, for all u : Symbol(σ).

Definition (Isomorphism)

An isomorphism is a homomorphism $f : A \to B$ where $f_s : A_s \to B_s$ is an equivalence for all s : Sort(σ).

Isomorphic

Let A, B, C : Algebra(σ).

Definition (Homomorphism)

A homomorphism $f : A \to B$ consists of

- $f_s : A_s \to B_s$ for all s : Sort(σ)
- $f_{s_t}(u^A(x_1, \ldots, x_n)) = u^B(f_{s_1}(x_1), \ldots, f_{s_n}(x_n))$,
  for all u : Symbol(σ).

Definition (Isomorphism)

An isomorphism is a homomorphism $f : A \to B$ where $f_s : A_s \to B_s$ is an equivalence for all s : Sort(σ).

Definition (Isomorphic)

Write $A \cong B$ for there is an isomorphism $A \to B$.

Isomorphic implies equal

Theorem (Isomrophic implies equal)

If $A \cong B$ *then* $A = B$.

- Coquand and Danielsson, Isomorphism is equality.

Lemma

Theorem (Isomrophic implies equal)

If $A \cong B$ *then* $A = B$*.*

- Coquand and Danielsson, Isomorphism is equality.

Lemma

Suppose

- $X, Y : \mathrm{Sort}(\sigma) \to \mathrm{Set}$
- $\alpha : X_{s_1} \to \cdots \to X_{s_n} \to X_t$ *and* $\beta : Y_{s_1} \to \cdots \to Y_{s_n} \to Y_t$
- $f : \prod_s X_s \simeq Y_s$
- $f_t(\alpha(x_1, \ldots, x_n)) = \beta(f_{s_1}(x_1), \ldots, f_{s_n}(x_n))$*.*

Then

$$\mathrm{transport}^{(\lambda Z.\ Z_{s_1} \to \cdots \to Z_{s_n} \to Z_t)} \underbrace{(\mathrm{funext}\ \overbrace{(\mathrm{ua} \circ f)}^{\prod_s X_s = Y_s})}_{X = Y}(\alpha) = \beta$$

Precategory of algebras

Lemma (Precategory of algebras)

There is a precategory σ-**Alg** *of* $\mathsf{Algebra}(\sigma)$ *and homomorphisms,*

- $(1_A)_s \equiv \lambda x.\ x, \qquad s : \mathsf{Sort}(\sigma)$
- $(gf)_s \equiv g_s \circ f_s, \qquad f : A \to B,\ g : B \to C$

Equal is equivalent to isomorphic

Lemma (Precategory of algebras)

There is a precategory σ-**Alg** *of* $\mathrm{Algebra}(\sigma)$ *and homomorphisms,*

- $(1_A)_s \equiv \lambda x.\ x, \qquad s : \mathrm{Sort}(\sigma)$
- $(gf)_s \equiv g_s \circ f_s, \qquad f : A \to B,\ g : B \to C$

Theorem (Equal is equivalent to isomorphic)

The function $(A = B) \to (A \cong B)$ *is an equivalence.*

Univalent category of algebras

Lemma (Precategory of algebras)

There is a precategory σ-**Alg** *of* $\mathsf{Algebra}(\sigma)$ *and homomorphisms,*

- $(1_A)_s \equiv \lambda x.\ x, \qquad s : \mathsf{Sort}(\sigma)$
- $(gf)_s \equiv g_s \circ f_s, \qquad f : A \to B,\ g : B \to C$

Theorem (Equal is equivalent to isomorphic)

The function $(A = B) \to (A \cong B)$ *is an equivalence.*

Theorem (Univalent category of algebras)

The precategory σ-**Alg** *is a univalent category.*

- HoTT book, `http://homotopytypetheory.org/book`.
- Arhens and Lumsdaine, Displayed Categories.

Congruence

Definition (Congruence)

A congruence on A is a family of mere equivalence relations $\Theta : \prod_s (A_s \to A_s \to \mathrm{Prop})$ where

$$\Theta_{s_1}(x_1, y_1) \times \cdots \times \Theta_{s_n}(x_n, y_n) \quad \text{implies}$$
$$\Theta_{s_t}\big(u^A(x_1, \ldots, x_n), u^A(y_1, \ldots, y_n)\big) \text{ for all } u : \mathrm{Symbol}(\sigma).$$

Quotient algebra

Definition (Congruence)

A congruence on A is a family of mere equivalence relations $\Theta : \prod_s (A_s \to A_s \to \mathrm{Prop})$ where

$$\Theta_{s_1}(x_1, y_1) \times \cdots \times \Theta_{s_n}(x_n, y_n) \quad \text{implies}$$
$$\Theta_{s_t}\big(u^A(x_1, \ldots, x_n), u^A(y_1, \ldots, y_n)\big) \text{ for all } u : \mathrm{Symbol}(\sigma).$$

Definition (Quotient algebra)

Let $\Theta : \prod_s (A_s \to A_s \to \mathrm{Prop})$ be a congruence. The quotient algebra A/Θ consists of

- $(A/\Theta)_s :\equiv A_s/\Theta_s$, the set-quotient
- operations $u^{A/\Theta}\big(q_1(x_1), \ldots, q_n(x_n)\big) = q_t\big(u^A(x_1, \ldots, x_n)\big)$, where $q_i : A_{s_i} \to A_{s_i}/\Theta_{s_i}$ are the set-quotient constructors.

Suppose $\Theta : \prod_s (A_s \to A_s \to \mathsf{Prop})$ is a congruence.

Quotient homomorphism

Suppose $\Theta : \prod_s (A_s \to A_s \to \mathrm{Prop})$ is a congruence.

Lemma (Quotient homomorphism)

There is a homomorphism $\rho : A \to A/\Theta$*, pointwise* $A_s \to A_s/\Theta_s$*.*

Quotient universal property

Suppose $\Theta : \prod_s (A_s \to A_s \to \mathrm{Prop})$ is a congruence.

Lemma (Quotient homomorphism)

There is a homomorphism $\rho : A \to A/\Theta$, pointwise $A_s \to A_s/\Theta_s$.

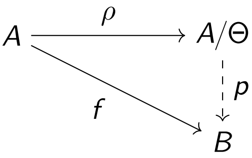
Lemma (Quotient universal property)

Precomposition with $\rho : A \to A/\Theta$ induces an equivalence

$$(A/\Theta \to B) \simeq \sum_{f:A\to B} \mathrm{resp}(f),$$

where $\mathrm{resp}(f) :\equiv \prod_{s:\mathrm{Sort}(\sigma)} \prod_{x,y:A_s} \left(\Theta_s(x,y) \to f_s(x) = f_s(y)\right)$.

Let $f : A \to B$ such that $\mathrm{resp}(f)$. Then there is a unique $p : A/\Theta \to B$ satisfying $f = pq$.



Coequalizers in σ-**Alg** are quotient algebras.

Product algebra

Product algebra

Let $F : I \to \text{Algebra}(\sigma)$. The product algebra $\bigtimes_i F(i)$ has carriers

$$(\bigtimes_i F(i))_s \equiv \prod_i (F(i))_s$$

There are projection homomorphisms $\pi_j : \bigtimes_i F(i) \to F(j)$.
Products in σ-**Alg** are product algebras.

Subalgebra

Product algebra

Let $F : I \to \text{Algebra}(\sigma)$. The product algebra $\bigtimes_i F(i)$ has carriers

$$(\bigtimes_i F(i))_s \equiv \prod_i (F(i))_s$$

There are projection homomorphisms $\pi_j : \bigtimes_i F(i) \to F(j)$.
Products in σ-**Alg** are product algebras.

Subalgebra

Let $P : \prod_s (A_s \to \text{Prop})$ such that, for any $u : \text{Symbol}(\sigma)$,

$$P_{s_1}(x_1) \times \cdots \times P_{s_n}(x_n) \qquad \text{implies} \qquad P_{n+1}(u^A(x_1, \ldots, x_n)),$$

where $(s_1, [s_2, \ldots, s_{n+1}]) \equiv \sigma_u$.
Then there is a subalgebra $A\&P$ with carriers

$$(A\&P)_s \equiv \sum_{x:A_s} P_s(x)$$

There exists an inclusion homomorphism $(A\&P) \to A$.
Equalizers in σ-**Alg** are subalgebras.

First isomorphism theorem

Theorem (First isomorphism/identification theorem)

Let $f : A \to B$ be a homomorphism.

- $\mathsf{ker}(f)(s,x,y) :\equiv \big(f_s(x) = f_s(y)\big)$ *is a congruence.*
- $\mathsf{inim}(f)(s,y) :\equiv \|\sum_x (f_s(x) = y)\|$ *is closed under operations, so it induces a subalgebra $B \& \mathsf{inim}(f)$ of B.*
- *There exists an isomorphism $A/\mathsf{ker}(f) \to B \& \mathsf{inim}(f)$.*

First identification theorem

Theorem (First isomorphism/identification theorem)

Let $f : A \to B$ be a homomorphism.

- $\mathrm{ker}(f)(s, x, y) :\equiv \big(f_s(x) = f_s(y)\big)$ *is a congruence.*
- $\mathrm{inim}(f)(s, y) :\equiv \|\sum_x (f_s(x) = y)\|$ *is closed under operations, so it induces a subalgebra $B\&\,\mathrm{inim}(f)$ of B.*
- *There exists an isomorphism $A/\,\mathrm{ker}(f) \to B\&\,\mathrm{inim}(f)$.*
- *Therefore $A/\,\mathrm{ker}(f) = B\&\,\mathrm{inim}(f)$.*

The category of algebras is regular

Theorem (First isomorphism/identification theorem)

Let $f : A \to B$ be a homomorphism.

- $\mathsf{ker}(f)(s, x, y) :\equiv \big(f_s(x) = f_s(y)\big)$ *is a congruence.*
- $\mathsf{inim}(f)(s, y) :\equiv \|\sum_x (f_s(x) = y)\|$ *is closed under operations, so it induces a subalgebra* $B\&\,\mathsf{inim}(f)$ *of* B*.*
- *There exists an isomorphism* $A/\,\mathsf{ker}(f) \to B\&\,\mathsf{inim}(f)$*.*
- *Therefore* $A/\,\mathsf{ker}(f) = B\&\,\mathsf{inim}(f)$*.*

Category σ-**Alg** is regular,

- $f : A \to B$ image factorizes $A \to B\&\,\mathsf{inim}(f) \hookrightarrow B$
- images are pullback stable.
- σ-**Alg** is complete

Conclusion and future work

- Type theoretic universal algebra without setoids.
- Port free algebras from math-classes.
- Define variety (equational theory), a subtype of Algebra(σ) satisfying equational laws involving operations.
- Birkhoff's HSP theorem.
- A verified computer algebra library.