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.
Example (Group)

A group is an h-set $G : \text{Set}$ 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 $G : \text{Set}$ 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 $\alpha : G \to S \to S$
- $\alpha(x \cdot y) = \alpha(x) \circ \alpha(y)$
- $\alpha(e) = \text{id}_S$
Signature

Definition (Signature)

A signature $\sigma : \text{Signature}$ consists of

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

**Definition (Signature)**

A signature $\sigma : \text{Signature}$ consists of

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

---

**Definition (Algebra)**

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

- for each $s : \text{Sort}(\sigma)$, $A_s : \text{Set}$
- for each $u : \text{Symbol}(\sigma)$, $u^A : A_{s_1} \rightarrow A_{s_2} \rightarrow \cdots \rightarrow A_{s_n}$, 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 $A : \text{Algebra}(\sigma)$ for $\sigma : \text{Signature}$ with

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

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 $A, B, C : \text{Algebra}(\sigma)$. 
Homomorphism

Let $A, B, C : \text{Algebra}(\sigma)$.

**Definition (Homomorphism)**

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

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

**Definition (Isomorphism)**

An isomorphism is a homomorphism $f : A \rightarrow B$ where $f_s : A_s \rightarrow B_s$ is an equivalence for all $s : \text{Sort}(\sigma)$.

**Definition (Isomorphic)**

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

Let $A, B, C : \text{Algebra}(\sigma)$.

**Definition (Homomorphism)**

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

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

**Definition (Isomorphism)**

An isomorphism is a homomorphism $f : A \rightarrow B$ where $f_s : A_s \rightarrow B_s$ is an equivalence for all $s : \text{Sort}(\sigma)$. 
Isomorphic

Let $A, B, C : \text{Algebra}(\sigma)$.

**Definition (Homomorphism)**

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

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

**Definition (Isomorphism)**

An isomorphism is a homomorphism $f : A \rightarrow B$ where $f_s : A_s \rightarrow B_s$ is an equivalence for all $s : \text{Sort}(\sigma)$.

**Definition (Isomorphic)**

Write $A \cong B$ for there is an isomorphism $A \rightarrow B$. 
Isomorphic implies equal

Theorem (Isomorphic implies equal)

If $A \simeq B$ then $A = B$.

- Coquand and Danielsson, Isomorphism is equality.
Lemma

Theorem (Isomorphic implies equal)

If $A \simeq B$ then $A = B$.

- Coquand and Danielsson, Isomorphism is equality.

Lemma

Suppose

- $X, Y : \text{Sort}(\sigma) \to \text{Set}$
- $\alpha : X_{s_1} \to \cdots \to X_{s_n} \to X_t$ 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

$$\text{transport}^((\lambda Z. Z_{s_1} \to \cdots \to Z_{s_n} \to Z_t) \left\{ \underbrace{\text{funext}(u \circ f)}_{X = Y} \right\})(\alpha) = \beta$$

$$\prod_s X_s = Y_s$$
**Lemma (Precategory of algebras)**

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

- $(1_A)_s \equiv \lambda x. x$, \hspace{1cm} $s : \text{Sort}(\sigma)$
- $((gf)_s \equiv g_s \circ f_s$, \hspace{1cm} $f : A \to B$, $g : B \to C$
### Lemma (Precategory of algebras)

There is a precategory $\sigma$-$\textbf{Alg}$ of $\text{Algebra}(\sigma)$ and homomorphisms,

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

### Theorem (Equal is equivalent to isomorphic)

The function $(A = B) \rightarrow (A \cong B)$ is an equivalence.
**Lemma (Precategory of algebras)**

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

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

**Theorem (Equal is equivalent to isomorphic)**

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

**Theorem (Univalent category of algebras)**

The precategory $\sigma$-**Alg** is a univalent category.

- Arhens and Lumsdaine, Displayed Categories.
A congruence on $A$ is a family of mere equivalence relations $\Theta : \prod_s (A_s \rightarrow A_s \rightarrow \text{Prop})$ where

$\Theta_s (x_1, y_1) \times \cdots \times \Theta_s (x_n, y_n)$ implies

$\Theta_{st} (u^A (x_1, \ldots, x_n), u^A (y_1, \ldots, y_n))$ for all $u : \text{Symbol}(\sigma)$.
Quotient algebra

Definition (Congruence)

A congruence on \( A \) is a family of mere equivalence relations \( \Theta : \prod_s(A_s \rightarrow A_s \rightarrow \text{Prop}) \) where
\[
\Theta_{s_1}(x_1, y_1) \times \cdots \times \Theta_{s_n}(x_n, y_n) \quad \text{implies}
\]
\[
\Theta_{s_t}(u^A(x_1, \ldots, x_n), u^A(y_1, \ldots, y_n)) \quad \text{for all } u : \text{Symbol}(\sigma).
\]

Definition (Quotient algebra)

Let \( \Theta : \prod_s(A_s \rightarrow A_s \rightarrow \text{Prop}) \) be a congruence. The quotient algebra \( A/\Theta \) consists of

- \((A/\Theta)_s \equiv A_s/\Theta_s\), the set-quotient
- operations \( u^{A/\Theta}(q_1(x_1), \ldots, q_n(x_n)) = q_t(u^A(x_1, \ldots, x_n)) \), where \( q_i : A_{s_i} \rightarrow A_{s_i}/\Theta_{s_i} \) are the set-quotient constructors.
Suppose $\Theta : \prod_s (A_s \to A_s \to \text{Prop})$ is a congruence.
Quotient homomorphism

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

Lemma (Quotient homomorphism)

There is a homomorphism $\rho : A \rightarrow A/\Theta$, pointwise $A_s \rightarrow A_s/\Theta_s$. 
Quotient universal property

Suppose $\Theta : \prod_s(A_s \to A_s \to \text{Prop})$ 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*

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

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

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

Coequalizers in $\sigma\text{-Alg}$ are quotient algebras.
### Product algebra

Let $F : I \to \text{Algebra}(\sigma)$. The product algebra $\prod_i F(i)$ has carriers
\[(\prod_i F(i))_s \equiv \prod_i (F(i))_s\]

There are projection homomorphisms $\pi_j : \prod_i F(i) \to F(j)$. Products in $\sigma$-$\text{Alg}$ are product algebras.
**Subalgebra**

**Product algebra**

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

$$\left(\times_i F(i)\right)_s \equiv \prod_i (F(i))_s$$

There are projection homomorphisms $\pi_j : \times_i F(i) \to F(j)$. Products in $\sigma\text{-Alg}$ are product algebras.

**Subalgebra**

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

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

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 $\sigma\text{-Alg}$ are subalgebras.
First isomorphism theorem

Theorem (First isomorphism/identification theorem)

Let \( f : A \rightarrow B \) be a homomorphism.

- \( \ker(f)(s, x, y) \equiv (f_s(x) = f_s(y)) \) is a congruence.
- \( \text{inim}(f)(s, y) \equiv \| \sum_x (f_s(x) = y) \| \) is closed under operations, so it induces a subalgebra \( B \& \text{inim}(f) \) of \( B \).
- There exists an isomorphism \( A/\ker(f) \rightarrow B \& \text{inim}(f) \).
First identification theorem

Theorem (First isomorphism/identification theorem)

Let \( f : A \to B \) be a homomorphism.

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

Theorem (First isomorphism/identification theorem)

Let \( f : A \to B \) be a homomorphism.

\begin{itemize}
  \item \( \ker(f)(s, x, y) \equiv (f_s(x) = f_s(y)) \) is a congruence.
  \item \( \text{inim}(f)(s, y) \equiv \| \sum_x (f_s(x) = y) \| \) is closed under operations, so it induces a subalgebra \( B \& \text{inim}(f) \) of \( B \).
  \item There exists an isomorphism \( A / \ker(f) \to B \& \text{inim}(f) \).
  \item Therefore \( A / \ker(f) = B \& \text{inim}(f) \).
\end{itemize}

Category \( \sigma\text{-Alg} \) is regular,

\begin{itemize}
  \item \( f : A \to B \) image factorizes \( A \to B \& \text{inim}(f) \leftarrow B \)
  \item images are pullback stable.
  \item \( \sigma\text{-Alg} \) 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 $\text{Algebra}(\sigma)$ satisfying equational laws involving operations.
- Birkhoff’s HSP theorem.
- A verified computer algebra library.