

The Agda Universal Algebra Library and Birkhoff's Theorem in Dependent Type Theory

William DeMeo   

Department of Algebra, Charles University in Prague

Abstract

The Agda Universal Algebra Library (UALib) is a library of types and programs (theorems and proofs) we developed to formalize the foundations of universal algebra in Martin-Löf-style dependent type theory using the Agda programming language and proof assistant. This paper describes the UALib and demonstrates that Agda is accessible to working mathematicians (such as ourselves) as a tool for formally verifying nontrivial results in general algebra and related fields. The library includes a substantial collection of definitions, theorems, and proofs from universal algebra and equational logic and as such provides many examples that exhibit the power of inductive and dependent types for representing and reasoning about general algebraic and relational structures.

The first major milestone of the UALib project is a complete proof of Birkhoff's HSP theorem. To the best of our knowledge, this is the first time Birkhoff's theorem has been formulated and proved in dependent type theory and verified with a proof assistant.

2012 ACM Subject Classification Theory of computation → Constructive mathematics; Theory of computation → Type theory; Theory of computation → Logic and verification; Computing methodologies → Representation of mathematical objects; Theory of computation → Type structures

Keywords and phrases Universal algebra, Equational logic, Martin-Löf Type Theory, Birkhoff's HSP Theorem, Formalization of mathematics, Agda, Proof assistant

Supplementary Material

Documentation: ualib.org

Software: <https://gitlab.com/ualib/ualib.gitlab.io.git>

Acknowledgements The author wishes to thank Hyeyoung Shin and Siva Somayajula for their contributions to this project and Martin Hötzel Escardo for creating the Type Topology library and teaching a course on Univalent Foundations of Mathematics with Agda at the 2019 Midlands Graduate School in Computing Science.

Contents

1	Prelude	7
1.1	Preliminaries	7
1.2	Equality	11
1.3	Inverses	12
1.4	Extensionality	16
2	Algebras	19
2.1	Operation and Signature Types	19
2.2	Algebra Types	20
2.3	Product Algebra Types	21
2.4	Product algebra type	21
2.5	The Universe Hierarchy and Lifts	22
3	Relations	25
3.1	Predicates	25
3.2	Binary Relation and Kernel Types	28

3.3	Equivalence Relation Types	30
3.4	Quotient Types	31
3.5	Congruence Relation Types	34
4	Homomorphisms	37
4.1	Basic Definitions	37
4.2	Kernels of Homomorphisms	38
4.3	Homomorphism Theorems	40
4.4	Products and Homomorphisms	44
4.5	Isomorphism Type	45
4.6	Homomorphic Image Type	51
5	Terms	55
5.1	Basic Definitions	55
5.2	The Term Algebra	55
5.3	Term Operations	57
5.4	Compatibility of Terms	59
6	Subalgebras	63
6.1	Types for Subuniverses	63
6.2	Subuniverse Generation	63
6.3	Subuniverse Lemmas	64
6.4	Homomorphisms and Subuniverses	66
6.5	Types for Subalgebra	67
6.6	WWMD	71
7	Equations and Varieties	75
7.1	Types for Theories and Models	75
7.2	Equational Logic Types	77
7.3	Inductive Types H, S, P, V	81
7.4	Equation Preservation Theorems	91
8	Birkhoff's HSP Theorem	99
8.1	The Free Algebra in Theory	99
8.2	The free algebra in Agda	99
8.3	HSP Lemmas	104
8.4	The HSP Theorem	109
9	Conclusion	110

Preface

To support formalization in type theory of research level mathematics in universal algebra and related fields, we present the Agda Universal Algebra Library (UALib), a software library containing formal statements and proofs of the core definitions and results of universal algebra. The UALib is written in Agda [8], a programming language and proof assistant based on Martin-Löf Type Theory that not only supports dependent and inductive types, but also provides powerful *proof tactics* for proving things about the objects that inhabit these types.

The seminal idea for the Agda UALib project was the observation that, on the one hand, a number of fundamental constructions in universal algebra can be defined recursively, and theorems about them proved by structural induction, while, on the other hand, inductive and dependent types make possible very precise formal representations of recursively defined objects, which often admit elegant constructive proofs of properties of such objects. An important feature of such proofs in type theory is that they are total functional programs and, as such, they are computable and composable.

Main Objectives

The first goal of the project is to express the foundations of universal algebra constructively, in type theory, and to formally verify the foundations using the Agda proof assistant. Thus we aim to codify the edifice upon which our mathematical research stands, and demonstrate that advancements in our field can be expressed in type theory and formally verified in a way that we, and other working mathematicians, can easily understand and check the results. We hope the library inspires and encourages others to formalize and verify their own mathematics research so that we may more easily understand and verify their results.

Our field is deep and broad, so codifying all of its foundations may seem like a daunting task and a risky investment of time and resources. However, we believe the subject is well served by a new, modern, *constructive* presentation of its foundations. Finally, the mere act of reinterpreting the foundations in an alternative system offers a fresh perspective, and this often leads to deeper insights and new discoveries.

Indeed, we wish to emphasize that our ultimate objective is not merely to translate existing results into a new more modern and formal language. Rather, an important goal of the UALib project is a system that is useful for conducting research in mathematics, and that is how we intend to use our library now that we have achieved our initial objective of implementing a substantial part of the foundations of universal algebra in Agda.

In our own mathematics research, experience has taught us that a proof assistant equipped with specialized libraries for universal algebra, as well as domain-specific tactics to automate proof idioms of our field, would be extremely valuable and powerful tool. Thus, we aim to build a library that serves as an indispensable part of our research tool kit. To this end, our intermediate-term objectives include

- developing domain specific “proof tactics” to express the idioms of universal algebra,
- implementing automated proof search for universal algebra,
- formalizing theorems from our own mathematics research,
- documenting the resulting software libraries so they are accessible to other mathematicians.

Prior art

There have been a number of efforts to formalize parts of universal algebra in type theory prior to ours, most notably

- Capretta [3] (1999) formalized the basics of universal algebra in the Calculus of Inductive Constructions using the Coq proof assistant;
- Spitters and van der Weegen [10] (2011) formalized the basics of universal algebra and some classical algebraic structures, also in the Calculus of Inductive Constructions using the Coq proof assistant, promoting the use of type classes as a preferable alternative to setoids;
- Gunther, et al [6] (2018) developed what seems to be (prior to the UALib) the most extensive library of formal universal algebra to date; in particular, this work includes a formalization of some basic equational logic; the project (like the UALib) uses Martin-Löf Type Theory and the Agda proof assistant.

Some other projects aimed at formalizing mathematics generally, and algebra in particular, have developed into very extensive libraries that include definitions, theorems, and proofs about algebraic structures, such as groups, rings, modules, etc. However, the goals of these efforts seem to be the formalization of special classical algebraic structures, as opposed to the general theory of (universal) algebras. Moreover, the part of universal algebra and equational logic formalized in the UALib extends beyond the scope of prior efforts, including those listed above. In particular, the UALib now includes a proof of Birkhoff’s variety theorem. Most other proofs of this theorem that we know of are informal and nonconstructive.¹

Contributions

Apart from the library itself, we describe the formal implementation and proof of a deep result, Garrett Birkhoff’s celebrated HSP theorem [2], which was among the first major results of universal algebra. The theorem states that a **variety** (a class of algebras closed under quotients, subalgebras, and products) is an equational class (defined by the set of identities satisfied by all its members). The fact that we now have a formal proof of this is noteworthy, not only because this is the first time the theorem has been proved in dependent type theory and verified with a proof assistant, but also because the proof is constructive. As the paper [4] of Carlström makes clear, it is a highly nontrivial exercise to take a well-known informal proof of a theorem like Birkhoff’s and show that it can be formalized using only constructive logic and natural deduction, without appealing to, say, the Law of the Excluded Middle or the Axiom of Choice.

Logical foundations

The Agda UALib is based on a minimal version of Martin-Löf dependent type theory (MLTT) that is the same or very close to the type theory on which Martín Escardó’s Type Topology Agda library is based. This is also the type theory that Escardó taught us in the short course Introduction to Univalent Foundations of Mathematics with Agda at the Midlands Graduate School in the Foundations of Computing Science at University of Birmingham in 2019.

We won’t go into great detail here because there are already other very nice resources available, such as the section A spartan Martin-Löf type theory of the lecture notes by Escardó just mentioned, as well as the ncatlab entry on Martin-Löf dependent type theory.

We will have much more to say about types and type theory as we progress. For now, suffice it to recall the handfull of objects that are assumed at the jumping-off point for MLTT: “primitive” **types** (0 , 1 , and \mathbb{N} , denoting the empty type, one-element type, and natural numbers),

¹ After the completion of this work, the author learned about a constructive version of Birkhoff’s theorem that was proved by Carlström in [4]. The latter is presented in the standard, informal style of mathematical writing in the current literature, and as far as we know it was never implemented formally and type-checked with a proof assistant. Nonetheless, a comparison of the version of the theorem presented in [4] to the Agda proof we give here would be interesting.

type formers ($+$, Π , Σ , Id , denoting binary sum, product, sum, and the identity type), and an infinite collection of **universes** (types of types) and universe variables to denote them (for which we will use upper-case caligraphic letters like \mathcal{U} , \mathcal{V} , \mathcal{W} , etc., typically from the latter half of the English alphabet).

Intended audience

This document describes Agda UALib in enough detail so that working mathematicians (and possibly some normal people, too) might be able to learn enough about Agda and its libraries to put them to use when creating, formalizing, and verifying new theorems in universal algebra and model theory.

While there are no strict prerequisites, we expect anyone with an interest in this work will have been motivated by prior exposure to universal algebra, as presented in, say, [1], or [7], or category theory, as presented in, say, [9] or <https://categorytheory.gitlab.io>.

Some prior exposure to type theory and Agda would be helpful, but even without this background one might still be able to get something useful out of this by referring to one or more of the resources mentioned in the references section below to fill in gaps as needed.

It is assumed that readers of this documentation are actively experimenting with Agda using Emacs with the `agda2-mode` extension installed. If you don't have Agda and `agda2-mode`, follow the directions on the main Agda website: <https://wiki.portal.chalmers.se/agda/pmwiki.php> or consult Martín Escardó's installation instructions or our modified version of Martin's instructions.

The main repository for the Agda UALib is gitlab.com/ualib/ualib.gitlab.io. There are more installation instructions in the `README.md` file of the UALib repository, but a summary of what's required is

- GNU Emacs (www.gnu.org/software/emacs/)
- Agda (version 2.6.1) (wiki.portal.chalmers.se/agda/pmwiki.php)
- `agda2-mode` for Emacs (agda.readthedocs.io/en/v2.6.0.1/tools/emacs-mode.html)
- A copy (or "clone") of the gitlab.com/ualib/ualib.gitlab.io repository.

Instructions for installing each of these are available in the `README.md` file of the UALib repository.

Attributions and citations

Most of the mathematical results that formalized in the UALib are well known. Regarding the Agda source code in the Agda UALib, this is mainly due to William DeMeo with one major caveat: we benefited greatly from, and the library depends upon, the lecture notes on Introduction to Univalent Foundations of Mathematics with Agda and the Type Topology Agda Library by Escardó [5]. The author is indebted to Martin for making his library and notes available and for teaching a course on type theory in Agda at the Midlands Graduate School in the Foundations of Computing Science in Birmingham in 2019.

The following Agda documentation and tutorials helped inform and improve the UALib, especially the first one in the list.

- Escardó, Introduction to Univalent Foundations of Mathematics with Agda
- Wadler, Programming Languages Foundations in Agda
- Altenkirk, Computer Aided Formal Reasoning
- Bove and Dybjer, Dependent Types at Work
- Gunther, Gadea, Pagano, Formalization of Universal Algebra in Agda
- Norell and Chapman, Dependently Typed Programming in Agda

References and resources

The official sources of information about Agda are

- Agda Wiki
- Agda Tutorial
- Agda User's Manual
- Agda Language Reference
- Agda Standard Library
- Agda Tools

The official sources of information about the Agda UALib are

- ualib.org (the web site) includes every line of code in the library, rendered as html and accompanied by documentation, and
- gitlab.com/ualib/ualib.gitlab.io (the source code) freely available and licensed under the Creative Commons Attribution-ShareAlike 4.0 International License.

License and citation information

This document and the Agda Universal Algebra Library by William DeMeo are licensed under a Creative Commons Attribution-ShareAlike BY-SA 4.0 International License and is based on work at <https://gitlab.com/ualib/ualib.gitlab.io>.

If you use the Agda UALib and/or you wish to refer to it or its documentation (e.g., in a publication), then please use the following BibTeX data (or refer to the dblp entry):

```
@article{DeMeo:2021,
  author      = {William DeMeo},
  title       = {The {A}gda {U}niversal {A}lgebra {L}ibrary and
                {B}irkhoff's {T}heorem in {D}ependent {T}ype {T}heory},
  journal     = {CoRR},
  volume      = {abs/2101.10166},
  year        = {2021},
  eprint      = {2101.10166},
  archivePrefix = {arXiv},
  primaryClass = {cs.LO},
  url         = {https://arxiv.org/abs/2101.10166},
  note        = {source code: \url{https://gitlab.com/ualib/ualib.gitlab.io}}
```

Acknowledgments

The author wishes to thank Siva Somayyajula for the valuable contributions he made during the projects crucial early stages. Thanks also to Andrej Bauer, Clifford Bergman, Venanzio Capretta, Martin Escardo, Ralph Freese, Bill Lampe, Miklós Maróti, Peter Mayr, JB Nation, and Hyeyoung Shin for helpful discussions, instruction, advice, inspiration and encouragement.

Contributions welcomed!

Readers and users are encouraged to suggest improvements to the Agda UALib and/or its documentation by submitting a new issue or merge request to the main repository at gitlab.com/ualib/ualib.gitlab.io/.

1 Prelude

This section presents the `UALib.Prelude` submodule of the Agda UALib.

1.1 Preliminaries

This subsection presents the `UALib.Prelude.Preliminaries` submodule of the Agda UALib.

Notation. Here are some acronyms that we use frequently.

- MHE = Martín Hötzel Escardó
- MLTT = Martin-Löf Type Theory

1.1.1 Options and imports

Agda programs typically begin by setting some options and by importing from existing libraries. Options are specified with the `OPTIONS pragma` and control the way Agda behaves by, for example, specifying which logical foundations should be assumed when the program is type-checked to verify its correctness. All Agda programs in the UALib begin with the pragma

```
{-# OPTIONS -without-K -exact-split -safe #-}
```

 (1)

This has the following effects:

1. `without-K` disables Streicher’s K axiom; see [11];
2. `exact-split` makes Agda accept only definitions that are *judgmental* or *definitional* equalities. As Escardó explains, this “makes sure that pattern matching corresponds to Martin-Löf eliminators;” for more details see [13];
3. `safe` ensures that nothing is postulated outright—every non-MLTT axiom has to be an explicit assumption (e.g., an argument to a function or module); see [12] and [13].

Throughout the UALib documentation assumptions 1–3 are taken for granted without mentioning them explicitly.

1.1.2 Modules

The `OPTIONS` pragma is followed by some imports or the start of a module. Sometimes we want to pass in parameters that will be assumed throughout the module. For instance, when working with algebras we often assume they come from a particular fixed signature S , which we could fix as a parameter at the start of a module. We’ll see many examples later, but here’s an example: `module _ {S : Signature 0 V} where.`

1.1.3 Imports from Type Topology

Throughout we use many of the nice tools that Escardó has developed and made available in the Type Topology repository of Agda code for the “Univalent Foundations” of mathematics. (See [5] for more details.) We import these as follows.

```
open import universes public
open import Identity-Type renaming (_≡_ to infix 0 _≡_ ; refl to refl) public
pattern refl x = refl {x = x}
open import Sigma-Type renaming (_,_ to infixr 50 _,_ ) public
open import MGS-MLTT using (_o_ ; domain ; codomain ; transport ; _≡⟨_⟩_ ; _■_ ;
  pr1 ; pr2 ; -Σ ; J ; II ; ¬ ; _×_ ; id ; _~_ ; _+_ ; 0 ; 1 ; 2 ; _⇔_ ;
  lr-implication ; rl-implication ; id ; _-1 ; ap) public
```

Standard Agda	Type Topology/UALib
<code>Level</code>	<code>Universe</code>
<code>$\mathcal{U} : \text{Level}$</code>	<code>$\mathcal{U} : \text{Universe}$</code>
<code><code>Set</code> \mathcal{U}</code>	<code>$\mathcal{U} \cdot$</code>
<code><code>Isuc</code> \mathcal{U}</code>	<code>\mathcal{U}^+</code>
<code><code>Set</code> (<code>Isuc</code> \mathcal{U})</code>	<code>\mathcal{U}^{++}</code>
<code><code>lzero</code></code>	<code>\mathcal{U}_0</code>
<code><code>Setω</code></code>	<code>\mathcal{U}_ω</code>

■ **Table 1** Special notation for universe levels

```

open import MGS-Equivalences using (is-equiv; inverse; invertible) public
open import MGS-Subsingleton-Theorems using (funext; global-hfunext; dfunext;
  is-singleton; is-subsingleton; is-prop; Univalence; global-dfunext;
  univalence-gives-global-dfunext;  $\cdot$ ;  $\simeq$ ; II-is-subsingleton;  $\Sigma$ -is-subsingleton;
  logically-equivalent-subsingletons-are-equivalent) public
open import MGS-Powerset
  renaming (_ $\in$ _ to _ $\in_0$ _; _ $\subseteq$ _ to _ $\subseteq_0$ _;  $\in$ -is-subsingleton to  $\in_0$ -is-subsingleton)
  using ( $\mathcal{P}$ ; equiv-to-subsingleton; powersets-are-sets'; subset-extensionality'; propext; _holds;  $\Omega$ ) public
open import MGS-Embeddings
  using (Nat; NatII; NatII-is-embedding; is-embedding; pr1-embedding;  $\circ$ -embedding; is-set;
  _ $\hookrightarrow$ _; embedding-gives-ap-is-equiv; embeddings-are-ic;  $\times$ -is-subsingleton; id-is-embedding) public
open import MGS-Solved-Exercises using (to-subtype $\equiv$ ) public
open import MGS-Unique-Existence using ( $\exists!$ ;  $\neg\exists!$ ) public
open import MGS-Subsingleton-Truncation using (_ $\cdot$ _; to- $\Sigma$ - $\equiv$ ; equivs-are-embeddings;
  invertibles-are-equivs; fiber;  $\subseteq$ -refl-consequence; hfunext) public

```

Notice that we carefully specify which definitions and theorems we want to import from each module. This is not absolutely necessary, but it helps us avoid name clashes and, more importantly, makes explicit on which components of the type theory our development depends.

1.1.4 Special notation for Agda universes

The first import in the list of `open import` directives above imports the universes module from Martin Escardo's Type Topology library. This provides, among other things, an elegant notation for type universes that we have fully adopted and we use it throughout the Agda UALib.²

The Agda UALib adopts the notation of the Type Topology library. In particular, universes are denoted by capitalized script letters from the second half of the alphabet, e.g., \mathcal{U} , \mathcal{V} , \mathcal{W} , etc. Also defined in Type Topology are the operators \cdot and $^+$. These map a universe \mathcal{U} to $\mathcal{U} \cdot := \text{Set } \mathcal{U}$ and $\mathcal{U}^+ := \text{Isuc } \mathcal{U}$, respectively. Thus, $\mathcal{U} \cdot$ is simply an alias for `Set \mathcal{U}` , and we have $\mathcal{U} \cdot : (\mathcal{U}^+) \cdot$. Table 1 translates between standard Agda syntax and Type Topology/UALib notation.

To justify the introduction of this somewhat nonstandard notation for universe levels, MHE

² We won't discuss every line of the universes module of the Type Topology library. Instead we merely touch upon the few lines of code that define the notational devices we adopt throughout the UALib. For those who wish for more details, MHE has made available an excellent set of notes from his course, MGS 2019. We highly recommend Martin's notes to anyone who wants more information than we provide here about Martin-Löf Type Theory and the Univalent Foundations/HoTT extensions thereof.

points out that the Agda library uses `Level` for universes (so what we write as $\mathcal{U} \cdot$ is written `Set \mathcal{U}` in standard Agda), but in univalent mathematics the types in $\mathcal{U} \cdot$ need not be sets, so the standard Agda notation can be misleading.

There will be many occasions calling for a type living in the universe that is the least upper bound of two universes, say, $\mathcal{U} \cdot$ and $\mathcal{V} \cdot$. The universe $(\mathcal{U} \sqcup \mathcal{V}) \cdot$ denotes this least upper bound.³ Here $\mathcal{U} \sqcup \mathcal{V}$ is used to denote the universe level corresponding to the least upper bound of the levels \mathcal{U} and \mathcal{V} , where the `_⊔_` is an Agda primitive designed for precisely this purpose.

1.1.5 Dependent pair type

Dependent pair types (or *Sigma types*) are defined in the Type Topology library as a record, as follows:

```
record  $\Sigma$  { $\mathcal{U} \mathcal{V}$ } { $X : \mathcal{U} \cdot$ } ( $Y : X \rightarrow \mathcal{V} \cdot$ ) :  $\mathcal{U} \sqcup \mathcal{V} \cdot$  where
  constructor _,_
  field
    pr1 : X
    pr2 : Y pr1
  infixr 50 _,_
```

We prefer the notation $\Sigma x : X, y$, which is closer to the standard syntax appearing in the literature than Agda's default syntax $(\Sigma \lambda(x : X) \rightarrow y)$. MHE makes the preferred notation available by making the index type explicit, as follows.

```
- $\Sigma$  : { $\mathcal{U} \mathcal{V} : \text{Universe}$ } ( $X : \mathcal{U} \cdot$ ) ( $Y : X \rightarrow \mathcal{V} \cdot$ )  $\rightarrow \mathcal{U} \sqcup \mathcal{V} \cdot$ 
- $\Sigma$  X Y =  $\Sigma$  Y
syntax - $\Sigma$  X ( $\lambda x \rightarrow y$ ) =  $\Sigma$  x : X, y
infixr -1 - $\Sigma$ 
```

N.B. The symbol `:` used here is not the same as the ordinary colon symbol `(:)`, despite how similar they may appear. The symbol in the expression $\Sigma x : X, y$ above is obtained by typing `\:4` in `agda2-mode`.

Our preferred notations for the first and second projections of a product are `|_` and `||_||`, respectively; however, we sometimes use more standard alternatives, such as `pr1` and `pr2`, or `fst` and `snd`, or some combination of these, to improve readability, or to avoid notation clashes with other modules.

```
module _ { $\mathcal{U} : \text{Universe}$ } where
  |_ $\_$  fst : { $X : \mathcal{U} \cdot$ } { $Y : X \rightarrow \mathcal{V} \cdot$ }  $\rightarrow \Sigma$  Y  $\rightarrow X$ 
  |  $x, y$  | = x
  fst (x, y) = x
  ||_ $\_$ || snd : { $X : \mathcal{U} \cdot$ } { $Y : X \rightarrow \mathcal{V} \cdot$ }  $\rightarrow (z : \Sigma$  Y)  $\rightarrow Y$  (pr1 z)
  ||  $x, y$  || = y
  snd (x, y) = y
```

³ Actually, because `_⊔_` has higher precedence than `_·`, we could omit parentheses here and simply write $\mathcal{U} \sqcup \mathcal{V} \cdot$.

1.1.6 Dependent function type

The so-called **dependent function type** (or “Pi type”) is defined in the Type Topology library as follows.

```

Π : {X :  $\mathcal{U}$  · } (A : X →  $\mathcal{V}$  · ) →  $\mathcal{U}$   $\sqcup$   $\mathcal{V}$  ·
Π { $\mathcal{U}$ } { $\mathcal{V}$ } {X} A = (x : X) → A x

```

To make the syntax for Π conform to the standard notation for Pi types, MHE uses the same trick as the one used above for Sigma types.

```

-Π : { $\mathcal{U}$   $\mathcal{V}$  : Universe} (X :  $\mathcal{U}$  · ) (Y : X →  $\mathcal{V}$  · ) →  $\mathcal{U}$   $\sqcup$   $\mathcal{V}$  ·
-Π X Y = Π Y
syntax -Π A (λ x → b) = Π x : A , b
infixr -1 -Π

```

1.1.7 Truncation and sets

In general, we may have many inhabitants of a given type and, via the Curry-Howard correspondence, many proofs of a given proposition. For instance, suppose we have a type X and an identity relation \equiv_x on X . Then, given two inhabitants a and b of type X , we may ask whether $a \equiv_x b$.

Suppose p and q inhabit the identity type $a \equiv_x b$; that is, p and q are proofs of $a \equiv_x b$, in which case we write $p \ q : a \equiv_x b$. Then we might wonder whether and in what sense are the two proofs p and q the “same.” We are asking about an identity type on the identity type \equiv_x , and whether there is some inhabitant r of this type; i.e., whether there is a proof $r : p \equiv_{x1} q$ that the proof of $a \equiv_x b$ is unique. (This property is sometimes called *uniqueness of identity proofs*.)

Perhaps we have two proofs, say, $r \ s : p \equiv_{x1} q$. Then of course our next question will be whether $r \equiv_{x2} s$ has a proof! But at some level we may decide that the potential to distinguish two proofs of an identity in a meaningful way (so-called *proof relevance*) is not useful or desirable. At that point, say, at level k , we might assume that there is at most one proof of any identity of the form $p \equiv_{xk} q$. This is called truncation.

We will see some examples of truncation later when we require it to complete some of the UALib modules leading up to the proof of Birkhoff’s HSP Theorem. Readers who want more details should refer to Section 34 and 35 of MHE’s notes, or Guillaume Brunerie, Truncations and truncated higher inductive types, or Section 7.1 of the HoTT book.

We take this opportunity to say what it means in type theory to say that a type is a *set*. A type $X : \mathcal{U} \cdot$ with an identity relation \equiv_x is called a **set** (or **0-groupoid**) if for every pair $a \ b : X$ of elements of type X there is at most one proof of $a \equiv_x b$. This is formalized in the Type Topology library as follows:⁴

```

is-set :  $\mathcal{U}$  · →  $\mathcal{U}$  ·
is-set X = (x y : X) → is-subsingleton (x ≡ y)

```

⁴ As MHE explains, “at this point, with the definition of these notions, we are entering the realm of univalent mathematics, but not yet needing the univalence axiom.”

1.2 Equality

This subsection presents the `UALib.Relations.Equality` submodule of the Agda UALib.

1.2.1 refl

Perhaps the most important types in type theory are the equality types. The *definitional equality* we use is a standard one and is often referred to as “reflexivity” or “refl”. In our case, it is defined in the Identity-Type module of the Type Topology library, but apart from syntax it is equivalent to the identity type used in most other Agda libraries. Here is the definition.

```
data ==_ { $\mathcal{U}$ } { $X : \mathcal{U} \cdot$ } :  $X \rightarrow X \rightarrow \mathcal{U} \cdot$  where
  refl : { $x : X$ }  $\rightarrow x \equiv x$ 
```

We begin the `UALib.Relations.Equality` module by formalizing the proof that `\equiv` is an equivalence relation.

```
module UALib.Prelude.Equality where
```

```
open import UALib.Prelude.Preliminaries using ( $\mathbb{0}$ ;  $\mathcal{V}$ ; Universe;  $_*$ ;  $_{\perp}$ ;  $_{\perp}^+$ ;  $_{\equiv}$ ; refl;  $\Sigma$ ;  $-\Sigma$ ;  $_{\times}$ ;  $_{\rightarrow}$ ;
  is-subsingleton; is-prop;  $|\_$ ;  $\|\_$ ;  $\mathbb{1}$ ;  $pr_1$ ;  $pr_2$ ; ap) public
```

```
module  $_$  { $\mathcal{U} : Universe$ } { $X : \mathcal{U} \cdot$ } where
```

```
 $\equiv$ -rfl : ( $x : X$ )  $\rightarrow x \equiv x$ 
 $\equiv$ -rfl  $x =$  refl  $_$ 
 $\equiv$ -sym : ( $x y : X$ )  $\rightarrow x \equiv y \rightarrow y \equiv x$ 
 $\equiv$ -sym  $x y$  (refl  $_$ ) = refl  $_$ 
 $\equiv$ -trans : ( $x y z : X$ )  $\rightarrow x \equiv y \rightarrow y \equiv z \rightarrow x \equiv z$ 
 $\equiv$ -trans  $x y z$  (refl  $_$ ) (refl  $_$ ) = refl  $_$ 
 $\equiv$ -Trans : ( $x : X$ ) { $y : X$ } { $z : X$ }  $\rightarrow x \equiv y \rightarrow y \equiv z \rightarrow x \equiv z$ 
 $\equiv$ -Trans  $x$  { $y$ }  $z$  (refl  $_$ ) (refl  $_$ ) = refl  $_$ 
```

The only difference between `\equiv -trans` and `\equiv -Trans` is that the second argument to `\equiv -Trans` is implicit so we can omit it when applying `\equiv -Trans`. This is sometimes convenient; after all, `\equiv -Trans` is used to prove that the first and last arguments are the same, and often we don’t care about the middle argument.

1.2.2 Functions preserve refl

A function is well defined only if it maps equivalent elements to a single element and we often use this nature of functions in Agda proofs. If we have a function $f : X \rightarrow Y$, two elements $x x' : X$ of the domain, and an identity proof $p : x \equiv x'$, then we obtain a proof of $f x \equiv f x'$ by simply applying the `ap` function like so, `ap f p : f x \equiv f x'`.

MHE defines `ap` in the Type Topology library so we needn’t redefine it here. Instead, we define two variations of `ap` that are sometimes useful.

```
ap-cong : { $\mathcal{U} \mathcal{W} : Universe$ } { $A : \mathcal{U} \cdot$ } { $B : \mathcal{W} \cdot$ }
  { $f g : A \rightarrow B$ } { $a b : A$ }
 $\rightarrow$     $f \equiv g \rightarrow a \equiv b$ 
  -----
 $\rightarrow$     $f a \equiv g b$ 
```

`ap-cong (refl _) (refl _) = refl _`

We sometimes need a version of `ap-cong` that works for dependent types, such as the following (which we borrow from the `Relation/Binary/Core.agda` module of the Agda Standard Library, transcribed into MHE/UALib notation of course).

$$\begin{array}{l} \text{cong-app} : \{ \mathcal{U} \mathcal{W} : \text{Universe} \} \{ A : \mathcal{U} \cdot \} \{ B : A \rightarrow \mathcal{W} \cdot \} \\ \quad \{ f g : (a : A) \rightarrow B a \} \\ \rightarrow \quad f \equiv g \rightarrow (a : A) \\ \quad \text{-----} \\ \rightarrow \quad f a \equiv g a \\ \text{cong-app (refl _) } a = \text{refl } _ \end{array}$$

1.2.3 \equiv -intro and \equiv -elim for pairs

We conclude the Equality module with some occasionally useful introduction and elimination rules for the equality relation on (nondependent) pair types.

$$\begin{array}{l} \equiv\text{-elim-left} : \{ \mathcal{U} \mathcal{W} : \text{Universe} \} \{ A_1 A_2 : \mathcal{U} \cdot \} \{ B_1 B_2 : \mathcal{W} \cdot \} \\ \rightarrow \quad (A_1 , B_1) \equiv (A_2 , B_2) \\ \quad \text{-----} \\ \rightarrow \quad A_1 \equiv A_2 \\ \equiv\text{-elim-left } e = \text{ap pr}_1 e \end{array}$$

$$\begin{array}{l} \equiv\text{-elim-right} : \{ \mathcal{U} \mathcal{W} : \text{Universe} \} \{ A_1 A_2 : \mathcal{U} \cdot \} \{ B_1 B_2 : \mathcal{W} \cdot \} \\ \rightarrow \quad (A_1 , B_1) \equiv (A_2 , B_2) \\ \quad \text{-----} \\ \rightarrow \quad B_1 \equiv B_2 \\ \equiv\text{-elim-right } e = \text{ap pr}_2 e \end{array}$$

$$\begin{array}{l} \equiv\text{-}\times\text{-intro} : \{ \mathcal{U} \mathcal{W} : \text{Universe} \} \{ A_1 A_2 : \mathcal{U} \cdot \} \{ B_1 B_2 : \mathcal{W} \cdot \} \\ \rightarrow \quad A_1 \equiv A_2 \rightarrow B_1 \equiv B_2 \\ \quad \text{-----} \\ \rightarrow \quad (A_1 , B_1) \equiv (A_2 , B_2) \\ \equiv\text{-}\times\text{-intro (refl _) (refl _) = (refl _) \end{array}$$

$$\begin{array}{l} \equiv\text{-}\times\text{-int} : \{ \mathcal{U} \mathcal{W} : \text{Universe} \} \{ A : \mathcal{U} \cdot \} \{ B : \mathcal{W} \cdot \} \\ \quad (a a' : A)(b b' : B) \\ \rightarrow \quad a \equiv a' \rightarrow b \equiv b' \\ \quad \text{-----} \\ \rightarrow \quad (a , b) \equiv (a' , b') \\ \equiv\text{-}\times\text{-int } a a' b b' \text{ (refl _) (refl _) = (refl _) \end{array}$$

1.3 Inverses

This subsection presents the `UALib.Prelude.Inverses` submodule of the Agda UALib. Here we define (the syntax of) a type for the (semantic concept of) **inverse image** of a function.

`gpgpmodule UALib.Prelude.Inverses where`

```
open import UALib.Prelude.Equality public
open import UALib.Prelude.Preliminaries using (⊔-1; funext; ⊔o; ⊔·; id; fst; snd; is-set; is-embedding;
transport; to-Σ≡; invertible; eqvs-are-embeddings; invertibles-are-equivs; fiber; refl) public
```

```
gpmodule _ { $\mathcal{U}$   $\mathcal{W}$  : Universe} where
```

```
data Image ⊔· {A :  $\mathcal{U}$  · } {B :  $\mathcal{W}$  · } (f : A → B) : B →  $\mathcal{U}$  ⊔ $\mathcal{W}$  ·
```

```
where
```

```
im : (x : A) → Image f ⊔· f x
```

```
eq : (b : B) → (a : A) → b ≡ f a → Image f ⊔· b
```

```
ImageIsImage : {A :  $\mathcal{U}$  · } {B :  $\mathcal{W}$  · }
                (f : A → B) (b : B) (a : A)
→
                b ≡ f a
```

```
→
                Image f ⊔· b
```

```
ImageIsImage {A} {B} f b a b≡fa = eq b a b≡fa
```

Note that an inhabitant of `Image f ⊔· b` is a dependent pair (a, p) , where $a : A$ and $p : b ≡ f a$ is a proof that f maps a to b . Thus, a proof that b belongs to the image of f (i.e., an inhabitant of `Image f ⊔· b`), always has a witness $a : A$, and a proof that $b ≡ f a$, so a (pseudo)inverse can actually be *computed*.

For convenience, we define a pseudo-inverse function, which we call `Inv`, that takes $b : B$ and $(a, p) : \text{Image } f \sqcup b$ and returns a .

```
Inv : {A :  $\mathcal{U}$  · } {B :  $\mathcal{W}$  · } (f : A → B) (b : B) → Image f ⊔· b → A
```

```
Inv f.(f a) (im a) = a
```

```
Inv f b (eq b a b≡fa) = a
```

Of course, we can prove that `Inv f` is really the (right-)inverse of f .

```
InvIsInv : {A :  $\mathcal{U}$  · } {B :  $\mathcal{W}$  · } (f : A → B)
           (b : B) (b∈Imgf : Image f ⊔· b)
```

```
→
           f (Inv f b b∈Imgf) ≡ b
```

```
InvIsInv f.(f a) (im a) = refl _
```

```
InvIsInv f b (eq b a b≡fa) = b≡fa-1
```

1.3.1 Surjective functions

An epic (or surjective) function from type $A : \mathcal{U} \cdot$ to type $B : \mathcal{W} \cdot$ is as an inhabitant of the `Epic` type, which we define as follows.

```
Epic : {A :  $\mathcal{U}$  · } {B :  $\mathcal{W}$  · } (g : A → B) →  $\mathcal{U}$  ⊔ $\mathcal{W}$  ·
```

```
Epic g =  $\forall$  y → Image g ⊔· y
```

We obtain the right-inverse (or pseudoinverse) of an epic function f by applying the function `EpicInv` (which we now define) to the function f along with a proof, $fE : \text{Epic } f$, that f is surjective.

```
EpicInv : {A :  $\mathcal{U}$  · } {B :  $\mathcal{W}$  · }
           (f : A → B) → Epic f
```

$$\begin{aligned} &\rightarrow B \rightarrow A \\ \text{EpicInv } f \text{ fE } b &= \text{Inv } f b (\text{fE } b) \end{aligned}$$

The function defined by `EpicInv f fE` is indeed the right-inverse of f .

$$\begin{aligned} \text{EpicInvsRightInv} &: \text{funext } \mathcal{W} \mathcal{W} \rightarrow \{A : \mathcal{U} \cdot\} \{B : \mathcal{W} \cdot\} \\ &\quad (f : A \rightarrow B) (fE : \text{Epic } f) \\ &\quad \text{-----} \\ &\rightarrow f \circ (\text{EpicInv } f \text{ fE}) \equiv \text{id } B \\ \text{EpicInvsRightInv } f \text{ fE } &= f e (\lambda x \rightarrow \text{InvsInv } f x (\text{fE } x)) \end{aligned}$$

1.3.2 Injective functions

We say that a function $g : A \rightarrow B$ is monic (or injective) if we have a proof of `Monic g`, where

$$\begin{aligned} \text{Monic} &: \{A : \mathcal{U} \cdot\} \{B : \mathcal{W} \cdot\} (g : A \rightarrow B) \rightarrow \mathcal{U} \sqcup \mathcal{W} \cdot \\ \text{Monic } g &= \forall a_1 a_2 \rightarrow g a_1 \equiv g a_2 \rightarrow a_1 \equiv a_2 \end{aligned}$$

Again, we obtain a pseudoinverse. Here it is obtained by applying the function `MonicInv` to g and a proof that g is monic.

$$\begin{aligned} &\text{--The (pseudo-)inverse of a monic function} \\ \text{MonicInv} &: \{A : \mathcal{U} \cdot\} \{B : \mathcal{W} \cdot\} \\ &\quad (f : A \rightarrow B) \rightarrow \text{Monic } f \\ &\quad \text{-----} \\ &\rightarrow (b : B) \rightarrow \text{Image } f \ni b \rightarrow A \end{aligned}$$

$$\text{MonicInv } f _ = \lambda b \text{ Imf} \ni b \rightarrow \text{Inv } f b \text{ Imf} \ni b$$

The function defined by `MonicInv f fM` is the left-inverse of f .

$$\begin{aligned} &\text{--The (psudo-)inverse of a monic is the left inverse.} \\ \text{MonicInvsLeftInv} &: \{A : \mathcal{U} \cdot\} \{B : \mathcal{W} \cdot\} \\ &\quad (f : A \rightarrow B) (fmonic : \text{Monic } f) (x : A) \\ &\quad \text{-----} \\ &\rightarrow (\text{MonicInv } f \text{ fmonic}) (f x) (\text{im } x) \equiv x \\ \text{MonicInvsLeftInv } f \text{ fmonic } x &= \text{refl } _ \end{aligned}$$

1.3.3 Bijective functions

Finally, bijective functions are defined.

$$\begin{aligned} \text{Bijective} &: \{A : \mathcal{U} \cdot\} \{B : \mathcal{W} \cdot\} (f : A \rightarrow B) \rightarrow \mathcal{U} \sqcup \mathcal{W} \cdot \\ \text{Bijective } f &= \text{Epic } f \times \text{Monic } f \\ \text{Inverse} &: \{A : \mathcal{U} \cdot\} \{B : \mathcal{W} \cdot\} (f : A \rightarrow B) \rightarrow \text{Bijective } f \rightarrow B \rightarrow A \\ \text{Inverse } f \text{ fbi } b &= \text{Inv } f b (\text{fst } (fbi) b) \end{aligned}$$

1.3.4 Injective functions are set embeddings

This is the first point at which truncation comes into play. An embedding is defined in the Type Topology library as follows:

```
is-embedding : {X :  $\mathcal{U}$  · } {Y :  $\mathcal{V}$  · } → (X → Y) →  $\mathcal{U} \sqcup \mathcal{V}$  ·
is-embedding f = (y : codomain f) → is-subsingleton (fiber f y)
```

where

```
is-subsingleton :  $\mathcal{U}$  · →  $\mathcal{U}$  ·
is-subsingleton X = (x y : X) → x ≡ y
```

and

```
fiber : {X :  $\mathcal{U}$  · } {Y :  $\mathcal{V}$  · } (f : X → Y) → Y →  $\mathcal{U} \sqcup \mathcal{V}$  ·
fiber f y =  $\Sigma$  x : domain f , f x ≡ y
```

This is a natural way to represent what we usually mean in mathematics by embedding. It does not correspond simply to an injective map. However, if we assume that the codomain type, B , is a *set* (i.e., has *unique identity proofs*), then we can prove that a injective (i.e., *monic*) function into B is an embedding as follows:

```
module _ { $\mathcal{U} \mathcal{W}$  : Universe} where

monic-into-set-is-embedding : {A : {A :  $\mathcal{U}$  · } {B :  $\mathcal{W}$  · } } → is-set B
→ (f : A → B) → Monic f
-----
→ is-embedding f

monic-into-set-is-embedding {A} Bset f fmon b (a , fa≡b) (a' , fa'≡b) =  $\gamma$ 
where
  faa' : f a ≡ f a'
  faa' = ≡-Trans (f a) (f a') fa≡b (fa'≡b  $^{-1}$ )

  aa' : a ≡ a'
  aa' = fmon a a' faa'

   $\mathcal{A}$  : A →  $\mathcal{W}$  ·
   $\mathcal{A}$  a = f a ≡ b

  arg1 :  $\Sigma$  p : (a ≡ a') , (transport  $\mathcal{A}$  p fa≡b) ≡ fa'≡b
  arg1 = aa' , Bset (f a') b (transport  $\mathcal{A}$  aa' fa≡b) fa'≡b

   $\gamma$  : a , fa≡b ≡ a' , fa'≡b
   $\gamma$  = to- $\Sigma$ -≡ arg1
```

Of course, invertible maps are embeddings.

```
invertibles-are-embeddings : {X :  $\mathcal{U}$  · } {Y :  $\mathcal{W}$  · } (f : X → Y)
→ invertible f → is-embedding f
invertibles-are-embeddings f fi = equivs-are-embeddings f (invertibles-are-equivs f fi)
```

Finally, if we have a proof p : `is-embedding f` that the map f is an embedding, here's a tool that makes it easier to apply p .

```
- Embedding elimination (makes it easier to apply is-embedding)
embedding-elim : {X :  $\mathcal{U}$  · } {Y :  $\mathcal{W}$  · } {f : X → Y}
→ is-embedding → (x x' : X)
```

```

→      -----
      f x ≡ f x' → x ≡ x'
embedding-elim {f = f} femb x x' fxfx' = γ
where
  fibx : fiber f (f x)
  fibx = x , refl
  fibx' : fiber f (f x)
  fibx' = x' , ((fxfx')-1)
  iss-fibffx : is-subsingleton (fiber f (f x))
  iss-fibffx = femb (f x)
  fibxfibx' : fibx ≡ fibx'
  fibxfibx' = iss-fibffx fibx fibx'
  γ : x ≡ x'
  γ = ap pr1 fibxfibx'

```

1.4 Extensionality

This subsection presents the `UALib.Prelude.Extensionality` submodule of the Agda `UALib`.

```

module UALib.Prelude.Extensionality where

open import UALib.Prelude.Inverses public
open import UALib.Prelude.Preliminaries
using ( _~_ ;  $\mathcal{U}\omega$ ;  $\Pi$ ;  $\Omega$ ;  $\mathcal{P}$ ;  $\subseteq$ -refl-consequence;  $\_ \in \_$ ;  $\_ \subseteq \_$ ;  $\_$ holds) public

```

1.4.1 Function extensionality

Extensional equality of functions, or function extensionality, means that any two point-wise equal functions are equal. As MHE points out, this is known to be not provable or disprovable in Martin-Löf type theory. It is an independent statement, which MHE abbreviates as `funext`. Here is how this notion is given a type in the Type Topology library

```

funext :  $\forall \mathcal{U} \mathcal{V} \rightarrow (\mathcal{U} \sqcup \mathcal{V})^+ \cdot$ 
funext  $\mathcal{U} \mathcal{V} = \{X : \mathcal{U} \cdot\} \{Y : \mathcal{V} \cdot\} \{f g : X \rightarrow Y\} \rightarrow f \sim g \rightarrow f \equiv g$ 

```

For readability we occasionally use the following alias for the `funext` type.

```

extensionality :  $\forall \mathcal{U} \mathcal{W} \rightarrow \mathcal{U}^+ \sqcup \mathcal{W}^+ \cdot$ 
extensionality  $\mathcal{U} \mathcal{W} = \{A : \mathcal{U} \cdot\} \{B : \mathcal{W} \cdot\} \{f g : A \rightarrow B\} \rightarrow f \sim g \rightarrow f \equiv g$ 

```

Pointwise equality of functions is typically what one means in informal settings when one says that two functions are equal. Here is how MHE defines pointwise equality of (dependent) function in Type Topology.

```

_~_ :  $\{X : \mathcal{U} \cdot\} \{A : X \rightarrow \mathcal{V} \cdot\} \rightarrow \Pi A \rightarrow \Pi A \rightarrow \mathcal{U} \sqcup \mathcal{V} \cdot$ 
f ~ g =  $\forall x \rightarrow f x \equiv g x$ 

```

In fact, if one assumes the univalence axiom, then the `_~_` relation is equivalent to equality of functions. See Function extensionality from univalence.

1.4.2 Dependent function extensionality

Extensionality for dependent function types is defined as follows.

```
dep-extensionality : ∀  $\mathcal{U} \mathcal{W} \rightarrow \mathcal{U}^+ \sqcup \mathcal{W}^+ \cdot$ 
dep-extensionality  $\mathcal{U} \mathcal{W} = \{A : \mathcal{U} \cdot\} \{B : A \rightarrow \mathcal{W} \cdot\}$ 
  {f g : ∀(x : A) → B x} → f ~ g → f ≡ g
```

Sometimes we need extensionality principles that work at all universe levels, and Agda is capable of expressing such principles, which belong to the special $\mathcal{U}\omega$ type, as follows:

```
∀-extensionality :  $\mathcal{U}\omega$ 
∀-extensionality = ∀ { $\mathcal{U} \mathcal{V}$ } → extensionality  $\mathcal{U} \mathcal{V}$ 
```

```
∀-dep-extensionality :  $\mathcal{U}\omega$ 
∀-dep-extensionality = ∀ { $\mathcal{U} \mathcal{V}$ } → dep-extensionality  $\mathcal{U} \mathcal{V}$ 
```

More details about the $\mathcal{U}\omega$ type are available at agda.readthedocs.io.

```
extensionality-lemma : ∀ { $\mathcal{F} \mathcal{U} \mathcal{V} \mathcal{T}$ } →
  {I :  $\mathcal{F} \cdot\}$  {X :  $\mathcal{U} \cdot\}$  {A : I →  $\mathcal{V} \cdot\}$ 
  {p q : (i : I) → (X → A i) →  $\mathcal{T} \cdot\}$ 
  {args : X → (Π A)}
  →
  p ≡ q
  -----
  →
  (λ i → (p i)(λ x → args x i)) ≡ (λ i → (q i)(λ x → args x i))

extensionality-lemma p q args p≡q =
  ap (λ - → λ i → (- i) (λ x → args x i)) p≡q
```

1.4.3 Function intensionality

This is the opposite of function extensionality and is defined as follows.

```
intensionality : { $\mathcal{U} \mathcal{W} : \text{Universe}$ } {A :  $\mathcal{U} \cdot\}$  {B :  $\mathcal{W} \cdot\}$  {f g : A → B}
  →
  f ≡ g → (x : A)
  -----
  →
  f x ≡ g x

intensionality (refl _) _ = refl _
```

Of course, the intensionality principle has an analogue for dependent function types.

```
dep-intensionality – alias (we sometimes give multiple names to a function, like this)
dintensionality : { $\mathcal{U} \mathcal{W} : \text{Universe}$ } {A :  $\mathcal{U} \cdot\}$  {B : A →  $\mathcal{W} \cdot\}$  {f g : (x : A) → B x}
  →
  f ≡ g → (x : A)
  -----
  →
  f x ≡ g x

dintensionality (refl _) _ = refl _
dep-intensionality = dintensionality
```

(This page is almost entirely blank on purpose.)

2 Algebras

This section presents the `UALib.Algebras` module of the Agda `UALib`.

2.1 Operation and Signature Types

This subsection presents the `UALib.Algebras.Signatures` submodule of the Agda `UALib`.

```
open import universes using (ℳ₀)

module UALib.Algebras.Signatures where

open import UALib.Prelude.Extensionality public
open import UALib.Prelude.Preliminaries using (0; 2) public
```

2.1.1 Operation type

We define the type of **operations** and, as an example, the type of **projections**.

```
module _ {ℳ ℳ' : Universe} where

  -The type of operations
  Op : ℳ' → ℳ → ℳ ⊔ ℳ'
  Op I A = (I → A) → A

  -Example. the projections
  π : {I : ℳ' } {A : ℳ' } → I → Op I A
  π i x = x i
```

The type `Op` encodes the arity of an operation as an arbitrary type $I : \mathcal{V}'$, which gives us a very general way to represent an operation as a function type with domain $I \rightarrow A$ (the type of “tuples”) and codomain A . The last two lines of the code block above codify the i -th I -ary projection operation on A .

2.1.2 Signature type

We define the signature of an algebraic structure in Agda like this.

```
Signature : (ℳ ℳ' : Universe) → (ℳ ⊔ ℳ')+
Signature ℳ ℳ' = Σ F : ℳ' , (F → ℳ')
```

Here \mathcal{O} is the universe level of operation symbol types, while \mathcal{V} is the universe level of arity types.

In the `UALib.Prelude` module we define special syntax for the first and second projections—namely, `|_|` and `||_||`, resp (see Subsection 1.1.5). Consequently, if $\{S : \text{Signature } \mathcal{O} \mathcal{V}\}$ is a signature, then $|S|$ denotes the type of **operation symbols**, and $||S||$ denotes the **arity** function. If $f : |S|$ is an operation symbol in the signature S , then $||S|| f$ is the arity of f .

2.1.3 Example

Here is how we might define the signature for *monoids* as a member of the type `Signature ℳ ℳ'`.

```
module _ {ℳ : Universe} where
```

```

data monoid-op :  $\mathbb{0}$  * where
  e : monoid-op
  · : monoid-op

monoid-sig : Signature  $\mathbb{0}$   $\mathcal{U}_0$ 
monoid-sig = monoid-op ,  $\lambda$  { e  $\rightarrow$   $\mathbb{0}$ ; ·  $\rightarrow$   $\mathbb{2}$  }

```

As expected, the signature for a *monoid* consists of two operation symbols, `e` and `·`, and a function λ { `e` \rightarrow $\mathbb{0}$; `·` \rightarrow $\mathbb{2}$ } which maps `e` to the empty type $\mathbb{0}$ (since `e` is the nullary identity) and maps `·` to the two element type $\mathbb{2}$ (since `·` is binary).

2.2 Algebra Types

This subsection presents the `UALib.Algebras.Algebras` submodule of the Agda `UALib`.

```

module UALib.Algebras.Algebras where
open import UALib.Algebras.Signatures public
open import UALib.Prelude.Preliminaries using ( $\mathcal{U}_0$ ;  $\mathbb{0}$ ;  $\mathbb{2}$ ) public

```

2.2.1 The Sigma type of Algebras

For a fixed signature S : `Signature $\mathbb{0}$ \mathcal{V}` and universe \mathcal{U} , we define the type of **algebras in the signature S** (or *S*-algebras) and with **domain** (or **carrier**) A : \mathcal{U} * as follows

```

Algebra : ( $\mathcal{U}$  : Universe)( $S$  : Signature  $\mathbb{0}$   $\mathcal{V}$ )  $\rightarrow$   $\mathbb{0}$   $\sqcup$   $\mathcal{V}$   $\sqcup$   $\mathcal{U}$  + *
Algebra  $\mathcal{U}$   $S$  =  $\Sigma$   $A$  :  $\mathcal{U}$  * , (( $f$  : |  $S$  |)  $\rightarrow$  Op ( $\|$   $S$   $\|$   $f$ )  $A$ )

```

We may refer to an inhabitant of `Algebra S \mathcal{U}` as an “ ∞ -algebra” because its domain can be an arbitrary type, say, A : \mathcal{U} * and need not be truncated at some level; in particular, A need to be a *set*. (See the discussion in Section 1.1.7.)

We take this opportunity to define the type of “0-algebras” which are algebras whose domains are *sets* (as defined in Section 1.1.7). This type is probably closer to what most of us think of when doing informal universal algebra. However, in the `UALib` will have so far only needed to know that a domain of an algebra is a set in a handful of specific instances, so it seems preferable to work with general (∞ -)algebras throughout the library and then assume *uniqueness of identity proofs* explicitly wherever a proof relies on this assumption.

The type `Algebra \mathcal{U} S` itself has a type; it is $\mathbb{0} \sqcup \mathcal{V} \sqcup \mathcal{U} + *$. This type appears so often in the `UALib` that we will define the following shorthand for its universe level: `OV \mathcal{U} = $\mathbb{0} \sqcup \mathcal{V} \sqcup \mathcal{U} + *$` .

2.2.2 The record type of algebras

Sometimes records are more convenient than sigma types. For such cases, we might prefer the following representation of the type of algebras.

```

module _ { $\mathbb{0}$   $\mathcal{V}$  : Universe} where
record algebra ( $\mathcal{U}$  : Universe) ( $S$  : Signature  $\mathbb{0}$   $\mathcal{V}$ ) : ( $\mathbb{0} \sqcup \mathcal{V} \sqcup \mathcal{U}$ ) + * where
  constructor mkalg
  field
    univ :  $\mathcal{U}$  *
    op : ( $f$  : |  $S$  |)  $\rightarrow$  (( $\|$   $S$   $\|$   $f$ )  $\rightarrow$  univ)  $\rightarrow$  univ

```

Of course, we can go back and forth between the two representations of algebras, like so.

```

module _ { $\mathcal{U} \ \mathcal{V} : \text{Universe}$ } { $S : \text{Signature } \mathcal{U} \ \mathcal{V}$ } where

  open algebra

  algebra $\rightarrow$ Algebra : algebra  $\mathcal{U} \ S \rightarrow$  Algebra  $\mathcal{U} \ S$ 
  algebra $\rightarrow$ Algebra  $\mathbf{A} = (\text{univ } \mathbf{A} , \text{op } \mathbf{A})$ 

  Algebra $\rightarrow$ algebra : Algebra  $\mathcal{U} \ S \rightarrow$  algebra  $\mathcal{U} \ S$ 
  Algebra $\rightarrow$ algebra  $\mathbf{A} = \text{mkalg } | \mathbf{A} | | \mathbf{A} ||$ 

```

2.2.3 Operation interpretation syntax

We conclude this module by defining a convenient shorthand for the interpretation of an operation symbol that we will use often.

```

 $\hat{\_} \_ : (f : | S |)(\mathbf{A} : \text{Algebra } \mathcal{U} \ S) \rightarrow (| S || f \rightarrow | \mathbf{A} |) \rightarrow | \mathbf{A} |$ 

 $f \hat{\_} \mathbf{A} = \lambda x \rightarrow (| \mathbf{A} || f) x$ 

```

This is similar to the standard notation that one finds in the literature and seems much more natural to us than the double bar notation that we started with.

2.2.4 Arbitrarily many variable symbols

Finally, we will want to assume that we always have at our disposal an arbitrary collection X of variable symbols such that, for every algebra \mathbf{A} , no matter the type of its domain, we have a surjective map $h_0 : X \rightarrow | \mathbf{A} |$ from variables onto the domain of \mathbf{A} .

```

 $\_ \rightarrow \_ : \{\mathcal{X} \ \mathcal{Y} : \text{Universe}\} \rightarrow \mathcal{X} \cdot \rightarrow \text{Algebra } \mathcal{U} \ S \rightarrow \mathcal{X} \sqcup \mathcal{Y} \cdot$ 
 $X \rightarrow \mathbf{A} = \Sigma h : (X \rightarrow | \mathbf{A} |) , \text{Epic } h$ 

```

2.3 Product Algebra Types

This subsection presents the `UALib.Algebras.Products` submodule of the Agda `UALib`.

2.4 Product algebra type

Suppose we are given a type $I : \mathcal{F}$ (of “indices”) and an indexed family $\mathcal{A} : I \rightarrow \text{Algebra } \mathcal{U} \ S$ of S -algebras. Then we define the *product algebra* $\prod \mathcal{A}$ in the following natural way.⁵

```

 $\prod : \{\mathcal{F} : \text{Universe}\}\{I : \mathcal{F} \cdot\}(\mathcal{A} : I \rightarrow \text{Algebra } \mathcal{U} \ S) \rightarrow \text{Algebra } (\mathcal{F} \sqcup \mathcal{U}) \ S$ 
 $\prod \{\mathcal{F}\}\{I\} \mathcal{A} =$ 
 $((i : I) \rightarrow | \mathcal{A} \ i |) , \lambda(f : | S |)(\mathbf{a} : || S || f \rightarrow (j : I) \rightarrow | \mathcal{A} \ j |)(i : I) \rightarrow (f \hat{\_} \mathcal{A} \ i) \lambda\{x \rightarrow \mathbf{a} \ x \ i\}$ 

```

Here, the domain is the dependent function type $\prod | \mathcal{A} | := (i : I) \rightarrow | \mathcal{A} \ i |$ of “tuples”, the i -th components of which live in $| \mathcal{A} \ i |$, and the operations are simply the operations of the $\mathcal{A} \ i$, interpreted component-wise.

⁵ To distinguish the product algebra from the standard product type available in the Agda Standard Library, instead of \prod (`\prod`) or Π (`\Pi`), we use the symbol \prod , which is typed in agda2-mode as `\G1b`.

The Birkhoff theorem involves products of entire arbitrary (nonindexed) classes of algebras, and it is not obvious how to handle this constructively, or whether it is even possible to do so without making extra assumptions about the class. (See [4] for a discussion of this issue.) We describe our solution to this problem in §7.3.8.

2.5 The Universe Hierarchy and Lifts

This subsection presents the `UALib.Algebras.Lifts` submodule of the Agda `UALib`. This section presents the `UALib.Algebras.Lifts` module of the Agda `UALib`.

```
module UALib.Algebras.Lifts where
open import UALib.Algebras.Products public
```

2.5.1 The noncumulative hierarchy

The hierarchy of universe levels in Agda is structured as $\mathcal{U}_0 : \mathcal{U}_1$, $\mathcal{U}_1 : \mathcal{U}_2$, $\mathcal{U}_2 : \mathcal{U}_3$, This means that \mathcal{U}_0 has type $\mathcal{U}_1 \cdot$ and \mathcal{U}_n has type $\mathcal{U}_{n+1} \cdot$ for each n .

It is important to note, however, this does *not* imply that $\mathcal{U}_0 : \mathcal{U}_2$ and $\mathcal{U}_0 : \mathcal{U}_3$, and so on. In other words, Agda’s universe hierarchy is *noncumulative*. This makes it possible to treat universe levels more generally and precisely, which is nice. On the other hand, it is this author’s experience that a noncumulative hierarchy can sometimes make for a nonfun proof assistant.

Luckily, there are ways to subvert noncumulativity which, when used with care, do not introduce logical inconsistencies into the type theory. We describe some techniques we developed for this purpose that are specifically tailored for our domain of applications.

2.5.2 Lifting and lowering

Let us be more concrete about what is at issue here by giving an example. Unless we are pedantic enough to worry about which universe level each of our types inhabits, then eventually we will encounter an error like the following:

```
Birkhoff.lagda:498,20-23
( $\mathcal{U}^+$ ) := ( $\mathcal{O}^+$ )  $\sqcup$  ( $\mathcal{V}^+$ )  $\sqcup$  (( $\mathcal{U}^+$ )+)
when checking that the expression SP $\mathcal{K}$  has type
Pred ( $\Sigma$  ( $\lambda A \rightarrow (f_1 : | S |) \rightarrow \text{Op} (|| S || f_1) A$ )) _W_ _2346
```

Just to confirm we all know the meaning of such errors, let’s translate the one above. This error means that Agda encountered a type at universe level \mathcal{U}^+ , on line 498 (in columns 20–23) of the file `Birkhoff.lagda`, but was expecting a type at level $\mathcal{O}^+ \sqcup \mathcal{V}^+ \sqcup \mathcal{U}^{++}$ instead.

To make these situations easier to deal with, the `UALib` offers some domain specific tools for the *lifting* and *lowering* of universe levels of the main types in the library. In particular, we have functions that will lift or lower the universes of algebra types, homomorphisms, subalgebras, and products.

Of course, messing with the universe level of a type must be done carefully to avoid making the type theory inconsistent. In particular, a necessary condition is that a type of a given universe level may not be converted to a type of lower universe level *unless the given type was obtained from lifting another type to a higher-than-necessary universe level*. If this is not clear, don’t worry; just press on and soon enough there will be examples that make it clear.

A general `Lift` record type, similar to the one found in the Agda Standard Library (in the `Level` module), is defined as follows.

```
record Lift {U W : Universe} (X : U ·) : U ⊔ W · where
  constructor lift
  field lower : X
open Lift
```

Next, we give various ways to lift function types.

```
lift-dom : {X Y W : Universe}{X : X ·}{Y : Y ·} → (X → Y) → (Lift{X}{W} X → Y)
lift-dom f = λ x → (f (lower x))
```

```
lift-cod : {X Y W : Universe}{X : X ·}{Y : Y ·} → (X → Y) → (X → Lift{Y}{W} Y)
lift-cod f = λ x → lift (f x)
```

```
lift-fun : {X Y W X : Universe}{X : X ·}{Y : Y ·} → (X → Y) → (Lift{X}{W} X → Lift{Y}{X} Y)
lift-fun f = λ x → lift (f (lower x))
```

We will also need to know that lift and lower compose to the identity.

```
lower~lift : {X W : Universe}{X : X ·} → lower{X}{W} ∘ lift ≡ id X
lower~lift = refl _
```

```
lift~lower : {X W : Universe}{X : X ·} → lift ∘ lower ≡ id (Lift{X}{W} X)
lift~lower = refl _
```

Now, to be more domain-specific, we show how to lift algebraic operation types and then, finally, how to lift algebra types.

```
module _ {S : Σ F : O ·, ( F → V ·)} where
```

```
lift-op : {U : Universe}{I : V ·}{A : U ·}
  → ((I → A) → A) → (W : Universe)
  → ((I → Lift{U}{W} A) → Lift{U}{W} A)
lift-op f W = λ x → lift (f (λ i → lower (x i)))
```

```
open algebra
```

```
lift-alg-record-type : {U : Universe} → algebra U S → (W : Universe) → algebra (U ⊔ W) S
lift-alg-record-type A W = mkalg (Lift (univ A)) (λ (f : | S |) → lift-op ((op A) f) W)
```

```
lift-∞-algebra lift-alg : {U : Universe} → Algebra U S → (W : Universe) → Algebra (U ⊔ W) S
```

```
lift-∞-algebra A W = Lift | A |, (λ (f : | S |) → lift-op (|| A || f) W)
```

```
lift-alg = lift-∞-algebra
```

(This page is almost entirely blank on purpose.)

3 Relations

This section presents the `UALib.Relations` module of the Agda `UALib`.

3.1 Predicates

This subsection presents the `UALib.Relations.Unary` submodule of the Agda `UALib`. We need a mechanism for implementing the notion of subsets in Agda. A typical one is called `Pred` (for predicate). More generally, `Pred A \mathcal{U}` can be viewed as the type of a property that elements of type A might satisfy. We write $P : \text{Pred } A \mathcal{U}$ to represent the semantic concept of a collection of elements of type A that satisfy the property P .

```
module UALib.Relations.Unary where
open import UALib.Algebras.Lifts public
open import UALib.Prelude.Preliminaries using (¬; propext; global-dfunext ) public
```

Here is the definition, which is similar to the one found in the `Relation/Unary.agda` file of the Agda Standard Library.

```
module _ { $\mathcal{U}$  : Universe} where
  Pred :  $\mathcal{U} \rightarrow (\mathcal{V} : Universe) \rightarrow \mathcal{U} \sqcup \mathcal{V}^+ \cdot$ 
  Pred A  $\mathcal{V} = A \rightarrow \mathcal{V} \cdot$ 
```

3.1.1 Unary relation truncation

Section 1.1.7 describes the concepts of *truncation* and *set* for “proof-relevant” mathematics. Sometimes we will want to assume “proof-irrelevance” and assume that certain types are sets. Recall, this mean there is at most one proof that two elements are the same. For predicates, analogously, we may wish to assume that there is at most one proof that a given element satisfies the predicate.

```
Pred0 :  $\mathcal{U} \rightarrow (\mathcal{V} : Universe) \rightarrow \mathcal{U} \sqcup \mathcal{V}^+ \cdot$ 
Pred0 A  $\mathcal{V} = \Sigma P : (A \rightarrow \mathcal{V} \cdot) , \forall x \rightarrow \text{is-subsingleton } (P x)$ 
```

Below we will often consider predicates over the class of all algebras of a particular type. We will define the type of algebras `Algebra $\mathcal{U} S$` (for some universe level \mathcal{U}). Like all types, `Algebra $\mathcal{U} S$` itself has a type which happens to be $\mathcal{O} \sqcup \mathcal{V} \sqcup \mathcal{U}^+ \cdot$ (see Section 2.2). Therefore, the type of `Pred (Algebra $\mathcal{U} S$) \mathcal{U}` is $\mathcal{O} \sqcup \mathcal{V} \sqcup \mathcal{U}^+ \cdot$ as well.

The inhabitants of the type `Pred (Algebra $\mathcal{U} S$) \mathcal{U}` are maps of the form $\mathbf{A} \rightarrow \mathcal{U} \cdot$; given an algebra $\mathbf{A} : \text{Algebra } \mathcal{U} S$, we have `Pred $\mathbf{A} \mathcal{U} = \mathbf{A} \rightarrow \mathcal{U} \cdot$` .

3.1.2 The membership relation

We introduce notation for denoting that x “belongs to” or “inhabits” type P , or that x “has property” P , by writing either $x \in P$ or $P x$ (cf. `Relation/Unary.agda` in the Agda Standard Library).

```
module _ { $\mathcal{U} \mathcal{W} : Universe$ } where
  _ $\in$ _ : {A :  $\mathcal{U} \cdot$ }  $\rightarrow A \rightarrow \text{Pred } A \mathcal{W} \rightarrow \mathcal{W} \cdot$ 
   $x \in P = P x$ 
```

$$\begin{aligned} _ \notin _ &: \{A : \mathcal{U} \cdot\} \rightarrow A \rightarrow \text{Pred } A \mathcal{W} \rightarrow \mathcal{W} \cdot \\ x \notin P &= \neg (x \in P) \end{aligned}$$

$$\text{infix 4 } _ \in _ \notin _$$

The “subset” relation is denoted, as usual, with the \subseteq symbol (cf. `Relation/Unary.agda` in the Agda Standard Library).

$$\begin{aligned} _ \subseteq _ &: \{\mathcal{U} \mathcal{W} \mathcal{T} : \text{Universe}\} \{A : \mathcal{U} \cdot\} \rightarrow \text{Pred } A \mathcal{W} \rightarrow \text{Pred } A \mathcal{T} \rightarrow \mathcal{U} \sqcup \mathcal{W} \sqcup \mathcal{T} \cdot \\ P \subseteq Q &= \forall \{x\} \rightarrow x \in P \rightarrow x \in Q \end{aligned}$$

$$\begin{aligned} _ \supseteq _ &: \{\mathcal{U} \mathcal{W} \mathcal{T} : \text{Universe}\} \{A : \mathcal{U} \cdot\} \rightarrow \text{Pred } A \mathcal{W} \rightarrow \text{Pred } A \mathcal{T} \rightarrow \mathcal{U} \sqcup \mathcal{W} \sqcup \mathcal{T} \cdot \\ P \supseteq Q &= Q \subseteq P \end{aligned}$$

$$\text{infix 4 } _ \subseteq _ \supseteq _$$

In type theory everything is a type. As we have just seen, this includes subsets. Since the notion of equality for types is usually a nontrivial matter, it may be nontrivial to represent equality of subsets. Fortunately, it is straightforward to write down a type that represents what it means for two subsets to be the in informal (pencil-paper) mathematics. In the Agda UALib this *subset equality* is denoted by $=\cdot$ and define as follows.

$$\begin{aligned} _ =\cdot _ &: \{\mathcal{U} \mathcal{W} \mathcal{T} : \text{Universe}\} \{A : \mathcal{U} \cdot\} \rightarrow \text{Pred } A \mathcal{W} \rightarrow \text{Pred } A \mathcal{T} \rightarrow \mathcal{U} \sqcup \mathcal{W} \sqcup \mathcal{T} \cdot \\ P =\cdot Q &= (P \subseteq Q) \times (Q \subseteq P) \end{aligned}$$

3.1.3 Predicates toolbox

Here is a small collection of tools that will come in handy later. Hopefully the meaning of each is self-explanatory.

$$\begin{aligned} _ \in _ &: \{\mathcal{U} \mathcal{W} \mathcal{T} : \text{Universe}\} \{A : \mathcal{U} \cdot\} \{B : \mathcal{W} \cdot\} \rightarrow (A \rightarrow B) \rightarrow \text{Pred } B \mathcal{T} \rightarrow \mathcal{U} \sqcup \mathcal{T} \cdot \\ _ \in _ f S &= (x : _) \rightarrow f x \in S \end{aligned}$$

$$\text{Pred-refl} : \{\mathcal{U} \mathcal{W} : \text{Universe}\} \{A : \mathcal{U} \cdot\} \{P Q : \text{Pred } A \mathcal{W}\}$$

$$\rightarrow P \equiv Q \rightarrow (a : A)$$

$$\rightarrow a \in P \rightarrow a \in Q$$

$$\text{Pred-refl (refl } _) = \lambda z \rightarrow z$$

$$\text{Pred-}\equiv : \{\mathcal{U} \mathcal{W} : \text{Universe}\} \{A : \mathcal{U} \cdot\} \{P Q : \text{Pred } A \mathcal{W}\} \rightarrow P \equiv Q \rightarrow P =\cdot Q$$

$$\text{Pred-}\equiv (\text{refl } _) = (\lambda z \rightarrow z), \lambda z \rightarrow z$$

$$\text{Pred-}\equiv \rightarrow \subseteq : \{\mathcal{U} \mathcal{W} : \text{Universe}\} \{A : \mathcal{U} \cdot\} \{P Q : \text{Pred } A \mathcal{W}\} \rightarrow P \equiv Q \rightarrow (P \subseteq Q)$$

$$\text{Pred-}\equiv \rightarrow \subseteq (\text{refl } _) = (\lambda z \rightarrow z)$$

$$\text{Pred-}\equiv \rightarrow \supseteq : \{\mathcal{U} \mathcal{W} : \text{Universe}\} \{A : \mathcal{U} \cdot\} \{P Q : \text{Pred } A \mathcal{W}\} \rightarrow P \equiv Q \rightarrow (P \supseteq Q)$$

$$\text{Pred-}\equiv \rightarrow \supseteq (\text{refl } _) = (\lambda z \rightarrow z)$$

$$\text{Pred-}=\cdot \equiv : \{\mathcal{U} \mathcal{W} : \text{Universe}\} \rightarrow \text{propext } \mathcal{W} \rightarrow \text{global-dfunext}$$

$$\rightarrow \{A : \mathcal{U} \cdot\} \{P Q : \text{Pred } A \mathcal{W}\}$$

$$\rightarrow ((x : A) \rightarrow \text{is-subsingleton } (P x))$$

$$\rightarrow ((x : A) \rightarrow \text{is-subsingleton } (Q x))$$

$$\rightarrow P =\cdot Q \rightarrow P \equiv Q$$

```

Pred ::= pe gfe {A}{P}{Q} ssP ssQ (pq , qp) = gfe γ
  where
    γ : (x : A) → P x ≡ Q x
    γ x = pe (ssP x) (ssQ x) pq qp

- Disjoint Union.
data _∪_ {U W : Universe} (A : U ·) (B : W ·) : U ∪ W · where
  inj₁ : (x : A) → A ∪ B
  inj₂ : (y : B) → A ∪ B
infixr 1 _∪_

- Union.
_∪_ : {U W T : Universe} {A : U ·} → Pred A W → Pred A T → Pred A _
P ∪ Q = λ x → x ∈ P ∪ x ∈ Q
infixr 1 _∪_

- The empty set.
∅ : {U : Universe} {A : U ·} → Pred A U₀
∅ = λ _ → 0

- Singletons.
{ _ } : {U : Universe} {A : U ·} → A → Pred A _
{ x } = x ≡ _

Im _⊆_ : {U W T : Universe} {A : U ·} {B : W ·} → (A → B) → Pred B T → U ∪ T ·
Im _⊆_ {A = A} f S = (x : A) → f x ∈ S

img : {U : Universe} {X : U ·} {Y : U ·}
      (f : X → Y) (P : Pred Y U)
      → Im f ⊆ P → X → Σ P
img {Y = Y} f P Imf ⊆ P = λ x₁ → f x₁ , Imf ⊆ P x₁

```

3.1.4 Predicate product and transport

The product $\prod P$ of a predicate $P : \text{Pred } X \mathcal{U}$ is inhabited iff P holds for all $x : X$.

```

IIP-meaning : {X U : Universe} {X : X ·} {P : Pred X U} → ∏ P → (x : X) → P x
IIP-meaning f x = f x

```

The following is a pair of useful “transport” lemmas for predicates.

```

module _ {U W : Universe} where

  cong-app-pred : {A : U ·} {B₁ B₂ : Pred A W}
                 (x : A) → x ∈ B₁ → B₁ ≡ B₂
                 -----
                 → x ∈ B₂
  cong-app-pred x x ∈ B₁ (refl _) = x ∈ B₁

  cong-pred : {A : U ·} {B : Pred A W}
              (x y : A) → x ∈ B → x ≡ y
              -----
              → y ∈ B
  cong-pred x .x x ∈ B (refl _) = x ∈ B

```

3.2 Binary Relation and Kernel Types

This subsection presents the `UALib.Relations.Binary` submodule of the Agda `UALib`. In set theory, a binary relation on a set A is simply a subset of the product $A \times A$. As such, we could model these as predicates over the type $A \times A$, or as relations of type $A \rightarrow A \rightarrow \mathfrak{R}$ (for some universe \mathfrak{R}). We define these below.

A generalization of the notion of binary relation is a *relation from A to B* , which we define first and treat binary relations on a single A as a special case.

```

module UALib.Relations.Binary where

open import UALib.Relations.Unary public

module _ { $\mathcal{U}$  : Universe} where

  REL : { $\mathfrak{R}$  : Universe}  $\rightarrow$   $\mathcal{U}$   $\cdot$   $\rightarrow$   $\mathfrak{R}$   $\cdot$   $\rightarrow$  ( $\mathcal{N}$  : Universe)  $\rightarrow$  ( $\mathcal{U} \sqcup \mathfrak{R} \sqcup \mathcal{N}^+$ )  $\cdot$ 
  REL A B  $\mathcal{N}$  = A  $\rightarrow$  B  $\rightarrow$   $\mathcal{N}$   $\cdot$ 

```

3.2.1 Kernels

The kernel of a function can be defined in many ways. For example,

```

KER : { $\mathfrak{R}$  : Universe} {A :  $\mathcal{U}$   $\cdot$ } {B :  $\mathfrak{R}$   $\cdot$ }  $\rightarrow$  (A  $\rightarrow$  B)  $\rightarrow$   $\mathcal{U} \sqcup \mathfrak{R}$   $\cdot$ 
KER { $\mathfrak{R}$ } {A} g =  $\Sigma$  x : A ,  $\Sigma$  y : A , g x  $\equiv$  g y

```

or as a unary relation (predicate) over the Cartesian product,

```

KER-pred : { $\mathfrak{R}$  : Universe} {A :  $\mathcal{U}$   $\cdot$ } {B :  $\mathfrak{R}$   $\cdot$ }  $\rightarrow$  (A  $\rightarrow$  B)  $\rightarrow$  Pred (A  $\times$  A)  $\mathfrak{R}$ 
KER-pred g (x , y) = g x  $\equiv$  g y

```

or as a relation from A to B ,

```

Rel :  $\mathcal{U}$   $\cdot$   $\rightarrow$  ( $\mathcal{N}$  : Universe)  $\rightarrow$   $\mathcal{U} \sqcup \mathcal{N}^+$   $\cdot$ 
Rel A  $\mathcal{N}$  = REL A A  $\mathcal{N}$ 

KER-rel : { $\mathfrak{R}$  : Universe} {A :  $\mathcal{U}$   $\cdot$ } {B :  $\mathfrak{R}$   $\cdot$ }  $\rightarrow$  (A  $\rightarrow$  B)  $\rightarrow$  Rel A  $\mathfrak{R}$ 
KER-rel g x y = g x  $\equiv$  g y

```

3.2.2 Examples

```

ker : {A B :  $\mathcal{U}$   $\cdot$ }  $\rightarrow$  (A  $\rightarrow$  B)  $\rightarrow$   $\mathcal{U}$   $\cdot$ 
ker = KER{ $\mathcal{U}$ }

ker-rel : {A B :  $\mathcal{U}$   $\cdot$ }  $\rightarrow$  (A  $\rightarrow$  B)  $\rightarrow$  Rel A  $\mathcal{U}$ 
ker-rel = KER-rel { $\mathcal{U}$ }

ker-pred : {A B :  $\mathcal{U}$   $\cdot$ }  $\rightarrow$  (A  $\rightarrow$  B)  $\rightarrow$  Pred (A  $\times$  A)  $\mathcal{U}$ 
ker-pred = KER-pred { $\mathcal{U}$ }

--The identity relation.
0 : {A :  $\mathcal{U}$   $\cdot$ }  $\rightarrow$   $\mathcal{U}$   $\cdot$ 
0 {A} =  $\Sigma$  a : A ,  $\Sigma$  b : A , a  $\equiv$  b

--...as a binary relation...
0-rel : {A :  $\mathcal{U}$   $\cdot$ }  $\rightarrow$  Rel A  $\mathcal{U}$ 

```

0-rel $a b = a \equiv b$

—...as a binary predicate...

0-pred : $\{A : \mathcal{U} \cdot\} \rightarrow \text{Pred } (A \times A) \mathcal{U}$

0-pred $(a, a') = a \equiv a'$

0-pred' : $\{A : \mathcal{U} \cdot\} \rightarrow \mathcal{U} \cdot$

0-pred' $\{A\} = \Sigma p : (A \times A), | p | \equiv || p ||$

—...on the domain of an algebra...

0-alg-rel : $\{S : \text{Signature } \mathcal{O} \mathcal{V}\} \{A : \text{Algebra } \mathcal{U} S\} \rightarrow \mathcal{U} \cdot$

0-alg-rel $\{A = \mathbf{A}\} = \Sigma a : | \mathbf{A} |, \Sigma b : | \mathbf{A} |, a \equiv b$

— The total relation $A \times A$

1 : $\{A : \mathcal{U} \cdot\} \rightarrow \text{Rel } A \mathcal{U}_0$

1 $a b = \mathbb{1}$

3.2.3 Properties of binary relations

reflexive : $\{\mathcal{R} : \text{Universe}\} \{X : \mathcal{U} \cdot\} \rightarrow \text{Rel } X \mathcal{R} \rightarrow \mathcal{U} \sqcup \mathcal{R} \cdot$

reflexive $_ \approx _ = \forall x \rightarrow x \approx x$

symmetric : $\{\mathcal{R} : \text{Universe}\} \{X : \mathcal{U} \cdot\} \rightarrow \text{Rel } X \mathcal{R} \rightarrow \mathcal{U} \sqcup \mathcal{R} \cdot$

symmetric $_ \approx _ = \forall x y \rightarrow x \approx y \rightarrow y \approx x$

transitive : $\{\mathcal{R} : \text{Universe}\} \{X : \mathcal{U} \cdot\} \rightarrow \text{Rel } X \mathcal{R} \rightarrow \mathcal{U} \sqcup \mathcal{R} \cdot$

transitive $_ \approx _ = \forall x y z \rightarrow x \approx y \rightarrow y \approx z \rightarrow x \approx z$

is-singleton-valued : $\{\mathcal{R} : \text{Universe}\} \{A : \mathcal{U} \cdot\} \rightarrow \text{Rel } A \mathcal{R} \rightarrow \mathcal{U} \sqcup \mathcal{R} \cdot$

is-singleton-valued $_ \approx _ = \forall x y \rightarrow \text{is-prop } (x \approx y)$

3.2.4 Binary relation truncation

Recall, in Section 1.1.7 we described the concept of truncation as it relates to “proof-relevant” mathematics. Given a binary relation P , it may be necessary or desirable to assume that there is at most one way to prove that a given pair of elements is P -related⁶ We use Escardo’s **is-singleton** type to express this strong (truncation at level 1) assumption in the following definition: We say that (x, y) belongs to P , or that x and y are P -related if and only if both $P x y$ and **is-singleton** $(P x y)$ holds.

Rel₀ : $\mathcal{U} \cdot \rightarrow (\mathcal{N} : \text{Universe}) \rightarrow \mathcal{U} \sqcup \mathcal{N}^+ \cdot$

Rel₀ $A \mathcal{N} = \Sigma P : (A \rightarrow A \rightarrow \mathcal{N} \cdot), \forall x y \rightarrow \text{is-singleton } (P x y)$

As above we define a **set** to be a type X with the following property: for all $x y : X$ there is at most one proof that $x \equiv y$. In other words, X is a set if and only if it satisfies the following:

$\forall x y : X \rightarrow \text{is-singleton } (x \equiv y)$

⁶ This is another example of “proof-irrelevance”; indeed, proofs of $P x y$ are indistinguishable, or rather any distinctions are irrelevant in the context of interest.

3.2.5 Implication

We denote and define implication as follows.

```

- (syntactic sugar)

$$\_on\_ : \{ \mathcal{U} \mathcal{V} \mathcal{W} : \text{Universe} \} \{ A : \mathcal{U} \cdot \} \{ B : \mathcal{V} \cdot \} \{ C : \mathcal{W} \cdot \} \\ \rightarrow (B \rightarrow B \rightarrow C) \rightarrow (A \rightarrow B) \rightarrow (A \rightarrow A \rightarrow C)$$


```

```


$$\_*_\_ \text{ on } g = \lambda x y \rightarrow g x *_ g y$$


```

```


$$\_ \Rightarrow \_ : \{ \mathcal{U} \mathcal{V} \mathcal{W} \mathcal{X} : \text{Universe} \} \{ A : \mathcal{U} \cdot \} \{ B : \mathcal{V} \cdot \} \\ \rightarrow \text{REL } A B \mathcal{W} \rightarrow \text{REL } A B \mathcal{X} \rightarrow \mathcal{U} \sqcup \mathcal{V} \sqcup \mathcal{W} \sqcup \mathcal{X} \cdot$$


```

```


$$P \Rightarrow Q = \forall \{ i j \} \rightarrow P i j \rightarrow Q i j$$


```

```

infixr 4 
$$\_ \Rightarrow \_$$


```

Here is a more general version that we borrow from the standard library and translate into MHE/UALib notation.

```


$$\_=[\_]\Rightarrow\_ : \{ \mathcal{U} \mathcal{V} \mathcal{R} \mathcal{S} : \text{Universe} \} \{ A : \mathcal{U} \cdot \} \{ B : \mathcal{V} \cdot \} \\ \rightarrow \text{Rel } A \mathcal{R} \rightarrow (A \rightarrow B) \rightarrow \text{Rel } B \mathcal{S} \rightarrow \mathcal{U} \sqcup \mathcal{R} \sqcup \mathcal{S} \cdot$$


```

```


$$P = [ g ] \Rightarrow Q = P \Rightarrow (Q \text{ on } g)$$


```

```

infixr 4 
$$\_=[\_]\Rightarrow\_$$


```

3.3 Equivalence Relation Types

This subsection presents the `UALib.Relations.Equivalences` submodule of the Agda UALib. This is all standard stuff. The notions of reflexivity, symmetry, and transitivity are defined as one would hope and expect, so we present them here without further explanation.

```

module UALib.Relations.Equivalences where

```

```

open import UALib.Relations.Binary public

```

```

module 
$$\_ \{ \mathcal{U} \mathcal{R} : \text{Universe} \} \text{ where}$$


```

```

record IsEquivalence { A : 
$$\mathcal{U} \cdot \} ( \_ \approx \_ : \text{Rel } A \mathcal{R} ) : \mathcal{U} \sqcup \mathcal{R} \cdot \text{ where}$$


```

```

  field

```

```

    rfl  : reflexive 
$$\_ \approx \_$$


```

```

    sym  : symmetric 
$$\_ \approx \_$$


```

```

    trans : transitive 
$$\_ \approx \_$$


```

```

is-equivalence-relation : { X : 
$$\mathcal{U} \cdot \} \rightarrow \text{Rel } X \mathcal{R} \rightarrow \mathcal{U} \sqcup \mathcal{R} \cdot$$


```

```

is-equivalence-relation 
$$\_ \approx \_ = \text{is-singleton-valued } \_ \approx \_$$


```

```

    × reflexive 
$$\_ \approx \_$$
 × symmetric 
$$\_ \approx \_$$
 × transitive 
$$\_ \approx \_$$


```

3.3.1 Examples

The zero relation `0-rel` is equivalent to the identity relation `≡` and, of course, these are both equivalence relations. Indeed, we saw in Subsection 1.2.1 that `≡` is reflexive, symmetric, and transitive, so we simply apply the corresponding proofs where appropriate.

```
module _ { $\mathcal{U}$  : Universe} where

  0-IsEquivalence : {A :  $\mathcal{U}$  ·} → IsEquivalence{ $\mathcal{U}$ }{A = A} 0-rel
  0-IsEquivalence = record { rfl = ≡-rfl; sym = ≡-sym; trans = ≡-trans }

  ≡-IsEquivalence : {A :  $\mathcal{U}$  ·} → IsEquivalence{ $\mathcal{U}$ }{A = A} ≡≡_
  ≡-IsEquivalence = record { rfl = ≡-rfl ; sym = ≡-sym ; trans = ≡-trans }
```

Finally, it's useful to have on hand a proof of the fact that the kernel of a function is an equivalence relation.

```
map-kernel-IsEquivalence : { $\mathcal{W}$  : Universe}{A :  $\mathcal{U}$  ·}{B :  $\mathcal{W}$  ·}
  (f : A → B) → IsEquivalence (KER-rel f)

map-kernel-IsEquivalence { $\mathcal{W}$ } f =
  record { rfl = λ x → refl
        ; sym = λ x y x1 → ≡-sym{ $\mathcal{W}$ } (f x) (f y) x1
        ; trans = λ x y z x1 x2 → ≡-trans (f x) (f y) (f z) x1 x2 }
```

3.4 Quotient Types

This subsection presents the `UALib.Relations.Quotients` submodule of the Agda `UALib`.

```
module UALib.Relations.Quotients where

  open import UALib.Relations.Equivalences public
  open import UALib.Prelude.Preliminaries using (≡⇔≡; id) public

  module _ { $\mathcal{U}$   $\mathcal{R}$  : Universe} where
```

For a binary relation R on A , we denote a single R -class as $[a] R$ (the class containing a). This notation is defined in `UALib` as follows.

```
– relation class
  [ ] : {A :  $\mathcal{U}$  ·} → A → Rel A  $\mathcal{R}$  → Pred A  $\mathcal{R}$ 
  [ a ] R = λ x → R a x
```

So, $x \in [a] R$ iff $R a x$, and the following elimination rule is a tautology.

```
[ ]-elim : {A :  $\mathcal{U}$  ·}{a x : A}{R : Rel A  $\mathcal{R}$ } → R a x ⇔ (x ∈ [ a ] R)
[ ]-elim = id , id
```

We define type of all classes of a relation R as follows.

```
 $\mathcal{C}$  : {A :  $\mathcal{U}$  ·}{R : Rel A  $\mathcal{R}$ } → Pred A  $\mathcal{R}$  → ( $\mathcal{U} \sqcup \mathcal{R}^+$ ) ·
 $\mathcal{C}$  {A}{R} = λ (C : Pred A  $\mathcal{R}$ ) →  $\Sigma$  a : A , C ≡ ([ a ] R)
```

There are a few ways we could define the quotient with respect to a relation. We have found the following to be the most convenient.

$$\begin{aligned}
 & \text{-- relation quotient (predicate version)} \\
 \underline{_} / \underline{_} & : (A : \mathbf{U} \cdot) \rightarrow \mathbf{Rel} A \mathfrak{R} \rightarrow \mathbf{U} \sqcup (\mathfrak{R}^+) \cdot \\
 A / R & = \Sigma C : \mathbf{Pred} A \mathfrak{R} , \mathcal{C}\{A\}\{R\} C \\
 & \text{-- old version: } A / R = \Sigma C : \mathbf{Pred} A \mathfrak{R} , \Sigma a : A , C \equiv ([a] R)
 \end{aligned}$$

We then define the following introduction rule for a relation class with designated representative.

$$\begin{aligned}
 \llbracket _ \rrbracket & : \{A : \mathbf{U} \cdot\} \rightarrow A \rightarrow \{R : \mathbf{Rel} A \mathfrak{R}\} \rightarrow A / R \\
 \llbracket a \rrbracket \{R\} & = ([a] R) , a , \mathit{refl}
 \end{aligned}$$

--So, $x \in [a]_p R$ iff $R a x$, and the following elimination rule is a tautology.

$$\begin{aligned}
 \llbracket _ \rrbracket \text{-elim} & : \{A : \mathbf{U} \cdot\} \{a x : A\} \{R : \mathbf{Rel} A \mathfrak{R}\} \rightarrow R a x \Leftrightarrow (x \in [a] R) \\
 \llbracket _ \rrbracket \text{-elim} & = \mathit{id} , \mathit{id}
 \end{aligned}$$

If the relation is reflexive, then we have the following elimination rules.

$$\begin{aligned}
 \text{/refl} & : \{A : \mathbf{U} \cdot\} \{a a' : A\} \{R : \mathbf{Rel} A \mathfrak{R}\} \rightarrow \mathit{reflexive} R \rightarrow [a] R \equiv [a'] R \rightarrow R a a' \\
 \text{/refl} \{A = A\} \{a\} \{a'\} \{R\} & \mathit{rfl} x = \gamma \\
 \text{where} & \\
 \mathbf{a}'\mathit{in} & : a' \in [a'] R \\
 \mathbf{a}'\mathit{in} & = \mathit{rfl} a' \\
 \gamma & : a' \in [a] R \\
 \gamma & = \mathit{cong-app-pred} a' \mathbf{a}'\mathit{in} (x^{-1})
 \end{aligned}$$

$$\begin{aligned}
 \text{/refl}' & : \{A : \mathbf{U} \cdot\} \{a a' : A\} \{R : \mathbf{Rel} A \mathfrak{R}\} \rightarrow \mathit{transitive} R \rightarrow R a' a \rightarrow ([a] R) \subseteq ([a'] R) \\
 \text{/refl}' \{A = A\} \{a\} \{a'\} \{R\} & \mathit{trn} Ra'a \{x\} aRx = \mathit{trn} a' a x Ra'a aRx
 \end{aligned}$$

$$\begin{aligned}
 \ulcorner _ \urcorner & : \{A : \mathbf{U} \cdot\} \{R : \mathbf{Rel} A \mathfrak{R}\} \rightarrow A / R \rightarrow A \\
 \ulcorner a \urcorner & = \llbracket a \rrbracket \mid \text{-- type } \ulcorner \text{ and } \urcorner \text{ as 'cul' and 'cur'}
 \end{aligned}$$

and an elimination rule for relation class representative, defined as follows.

$$\begin{aligned}
 \text{/Refl} & : \{A : \mathbf{U} \cdot\} \{a a' : A\} \{R : \mathbf{Rel} A \mathfrak{R}\} \rightarrow \mathit{reflexive} R \rightarrow \llbracket a \rrbracket \{R\} \equiv \llbracket a' \rrbracket \rightarrow R a a' \\
 \text{/Refl} \mathit{rfl} (\mathit{refl} _) & = \mathit{rfl} _
 \end{aligned}$$

Later we will need the following additional quotient tools.

$$\mathit{open} \mathit{IsEquivalence} \{ \mathbf{U} \} \{ \mathfrak{R} \}$$

$$\begin{aligned}
 \text{/subset} & : \{A : \mathbf{U} \cdot\} \{a a' : A\} \{R : \mathbf{Rel} A \mathfrak{R}\} \\
 & \rightarrow \mathit{IsEquivalence} R \rightarrow R a a' \rightarrow ([a] R) \subseteq ([a'] R) \\
 \text{/subset} \{A = A\} \{a\} \{a'\} \{R\} & \mathit{Req} Raa' \{x\} Rax = (\mathit{trans} \mathit{Req}) a' a x (\mathit{sym} \mathit{Req} a a' Raa') Rax
 \end{aligned}$$

$$\begin{aligned}
 \text{/supset} & : \{A : \mathbf{U} \cdot\} \{a a' : A\} \{R : \mathbf{Rel} A \mathfrak{R}\} \\
 & \rightarrow \mathit{IsEquivalence} R \rightarrow R a a' \rightarrow ([a] R) \supseteq ([a'] R) \\
 \text{/supset} \{A = A\} \{a\} \{a'\} \{R\} & \mathit{Req} Raa' \{x\} Ra'x = (\mathit{trans} \mathit{Req}) a a' x Raa' Ra'x
 \end{aligned}$$

$$\begin{aligned}
 \text{/=} & : \{A : \mathbf{U} \cdot\} \{a a' : A\} \{R : \mathbf{Rel} A \mathfrak{R}\} \\
 & \rightarrow \mathit{IsEquivalence} R \rightarrow R a a' \rightarrow ([a] R) = ([a'] R) \\
 \text{/=} \{A = A\} \{a\} \{a'\} \{R\} & \mathit{Req} Raa' = \text{/subset} \mathit{Req} Raa' , \text{/supset} \mathit{Req} Raa'
 \end{aligned}$$

3.4.1 Quotient extensionality

We need a (subsingleton) identity type for congruence classes over sets so that we can equate two classes even when they are presented using different representatives. For this we assume that our relations are on sets, rather than arbitrary types. As mentioned earlier, this is equivalent to assuming that there is at most one proof that two elements of a set are the same.

(Recall, a type is called a **set** if it has *unique identity proofs*; as a general principle, this is sometimes referred to as “proof irrelevance” or “uniqueness of identity proofs”—two proofs of a single identity are the same.)

```

class-extensionality : propext  $\mathfrak{R}$  → global-dfunext
  → {A :  $\mathcal{U}$  ·}{a a' : A}{R : Rel A  $\mathfrak{R}$ }
  → (∀ a x → is-subsingleton (R a x))
  → IsEquivalence R
  -----
  → R a a' → ([ a ] R) ≡ ([ a' ] R)

class-extensionality pe gfe {A = A}{a}{a'}{R} ssR Req Raa' =
  Pred-≡-≡ pe gfe {A}{[ a ] R}{[ a' ] R} (ssR a) (ssR a') (/≡- Req Raa')

to-subtype-[] : {A :  $\mathcal{U}$  ·}{R : Rel A  $\mathfrak{R}$ }{C D : Pred A  $\mathfrak{R}$ }
  {c :  $\mathcal{C}$  C}{d :  $\mathcal{C}$  D}
  → (∀ C → is-subsingleton ( $\mathcal{C}$  {A}{R} C))
  → C ≡ D → (C , c) ≡ (D , d)

to-subtype-[] {D = D}{c}{d} ssA CD = to- $\Sigma$ -≡ (CD , ssA D (transport  $\mathcal{C}$  CD c) d)

class-extensionality' : propext  $\mathfrak{R}$  → global-dfunext
  → {A :  $\mathcal{U}$  ·}{a a' : A}{R : Rel A  $\mathfrak{R}$ }
  → (∀ a x → is-subsingleton (R a x))
  → (∀ C → is-subsingleton ( $\mathcal{C}$  C))
  → IsEquivalence R
  -----
  → R a a' → ([ a ] {R}) ≡ ([ a' ] {R})

class-extensionality' pe gfe {A = A}{a}{a'}{R} ssR ssA Req Raa' =  $\gamma$ 
  where
    CD : ([ a ] R) ≡ ([ a' ] R)
    CD = class-extensionality pe gfe {A}{a}{a'}{R} ssR Req Raa'

     $\gamma$  : ([ a ] {R}) ≡ ([ a' ] {R})
     $\gamma$  = to-subtype-[] ssA CD
  
```

3.4.2 Compatibility

The following definitions and lemmas are useful for asserting and proving facts about **compatibility** of relations and functions.

```

module _ { $\mathcal{U}$   $\mathcal{V}$   $\mathcal{W}$  : Universe} { $\gamma$  :  $\mathcal{V}$  ·} {Z :  $\mathcal{U}$  ·} where

  lift-rel : Rel Z  $\mathcal{W}$  → ( $\gamma$  → Z) → ( $\gamma$  → Z) →  $\mathcal{V}$   $\sqcup$   $\mathcal{W}$  ·
  lift-rel R f g = ∀ x → R (f x) (g x)
  
```

```
compatible-fun : (f : (γ → Z) → Z)(R : Rel Z ℳ) → ℳ ⊔ ℳ ⊔ ℳ ·
compatible-fun f R = (lift-rel R) =[ f ]⇒ R
```

– relation compatible with an operation

```
module _ {ℳ ℳ : Universe} {S : Signature ℔ ℳ} where
  compatible-op : {A : Algebra ℳ S} → | S | → Rel | A | ℳ → ℳ ⊔ ℳ ⊔ ℳ ·
  compatible-op {A} f R = ∀{a}{b} → (lift-rel R) a b → R ((f ^ A) a) ((f ^ A) b)
  – alternative notation: (lift-rel R) =[ f ^ A ]⇒ R
```

–The given relation is compatible with all ops of an algebra.

```
compatible : (A : Algebra ℳ S) → Rel | A | ℳ → ℔ ⊔ ℳ ⊔ ℳ ⊔ ℳ ·
compatible A R = ∀ f → compatible-op{A} f R
```

cpad We'll see this definition of compatibility at work very soon when we define congruence relations in the next section.

3.5 Congruence Relation Types

This subsection presents the `UALib.Relations.Congruences` submodule of the Agda `UALib`. Notice that module begins by assuming a signature $S : \text{Signature } \mathbb{O} \mathcal{V}$ which is then present and available throughout the module.

```
open import UALib.Algebras.Signatures using (Signature; ℔; ℳ)
module UALib.Relations.Congruences {S : Signature ℔ ℳ} where
open import UALib.Relations.Quotients hiding (Signature; ℔; ℳ) public
Con : {ℳ : Universe}(A : Algebra ℳ S) → ℔ ⊔ ℳ ⊔ ℳ ⊔ ℳ + ·
Con {ℳ} A = Σ θ : ( Rel | A | ℳ ) , IsEquivalence θ × compatible A θ

con : {ℳ : Universe}(A : Algebra ℳ S) → Pred (Rel | A | ℳ) (℔ ⊔ ℳ ⊔ ℳ)
con A = λ θ → IsEquivalence θ × compatible A θ

record Congruence {ℳ ℳ : Universe} (A : Algebra ℳ S) : ℔ ⊔ ℳ ⊔ ℳ ⊔ ℳ + · where
  constructor mkcon
  field
    ⟨_⟩ : Rel | A | ℳ
    Compatible : compatible A ⟨_⟩
    IsEquiv : IsEquivalence ⟨_⟩

open Congruence

compatible-equivalence : {ℳ ℳ : Universe}{A : Algebra ℳ S} → Rel | A | ℳ → ℔ ⊔ ℳ ⊔ ℳ ⊔ ℳ ⊔ ℳ ·
compatible-equivalence {ℳ}{ℳ} {A} R = compatible A R × IsEquivalence R
```

3.5.1 Example

We defined the *trivial* (or “diagonal” or “identity” or “zero”) relation `0-rel` in Subsection 3.2.2, and we observed in Subsection 3.3.1 that `0-rel` is equivalent to the identity relation `≡` and that these are both equivalence relations. Therefore, in order to build a congruence of some algebra A out of the trivial relation, it remains to show that `0-rel` is compatible with all operations of A . We do this now and immediately after we construct the corresponding congruence.

```
module _ {ℳ : Universe} {S : Signature ℔ ℳ} where
```

```

0-compatible-op : funext  $\mathcal{V} \mathcal{U} \rightarrow \{A : \text{Algebra } \mathcal{U} S\} (f : | S |)
  \rightarrow \text{compatible-op } \{\mathcal{U} = \mathcal{U}\} \{A = A\} f \mathbf{0}\text{-rel}
0-compatible-op fe  $\{A\}$  f ptws0 = ap (f  $\hat{\ } A$ ) (fe ( $\lambda x \rightarrow ptws0 x$ ))

0-compatible : funext  $\mathcal{V} \mathcal{U} \rightarrow \{A : \text{Algebra } \mathcal{U} S\} \rightarrow \text{compatible } A \mathbf{0}\text{-rel}
0-compatible fe  $\{A\} = \lambda f \text{ args} \rightarrow \mathbf{0}\text{-compatible-op } fe \{A\} f \text{ args}$$$ 
```

Now that we have the ingredients required to construct a congruence, we carry out the construction as follows.

```

 $\Delta$  :  $\{\mathcal{U} : \text{Universe}\} \rightarrow \text{funext } \mathcal{V} \mathcal{U} \rightarrow (A : \text{Algebra } \mathcal{U} S) \rightarrow \text{Congruence } A
\Delta fe A = \text{mkcon } \mathbf{0}\text{-rel } (\mathbf{0}\text{-compatible } fe) (\mathbf{0}\text{-IsEquivalence})$ 
```

3.5.2 Quotient algebras

An important construction in universal algebra is the quotient of an algebra A with respect to a congruence relation θ of A . This quotient is typically denote by A / θ and Agda allows us to define and express quotients using the standard notation.

```

 $\_/\_$  :  $\{\mathcal{U} \mathcal{R} : \text{Universe}\} (A : \text{Algebra } \mathcal{U} S)
  \rightarrow \text{Congruence } \{\mathcal{U}\} \{\mathcal{R}\} A
  \text{-----}
  \rightarrow \text{Algebra } (\mathcal{U} \sqcup \mathcal{R}^+) S$ 
```

```

 $A / \theta = (( | A | / \langle \theta \rangle ) , - \text{carrier (i.e. domain or universe)})
  (\lambda f \text{ args} - \text{operations}
    \rightarrow ([ (f \hat{\ } A) (\lambda i_1 \rightarrow | \| \text{args } i_1 \| |) ] \langle \theta \rangle ) ,
    ((f \hat{\ } A) (\lambda i_1 \rightarrow | \| \text{args } i_1 \| |) , \text{refl } \_))
  )$ 
```

3.5.3 Examples

The zero element of a quotient can be expressed as follows.

```

Zero $\_/\_$  :  $\{\mathcal{U} \mathcal{R} : \text{Universe}\} \{A : \text{Algebra } \mathcal{U} S\}
  (\theta : \text{Congruence } \{\mathcal{U}\} \{\mathcal{R}\} A)
  \rightarrow \text{Rel } (| A | / \langle \theta \rangle) (\mathcal{U} \sqcup \mathcal{R}^+)

Zero $\_/\_ \theta = \lambda x x_1 \rightarrow x \equiv x_1$$ 
```

Finally, the following elimination rule is sometimes useful.

```

 $\_/\text{-refl}$  :  $\{\mathcal{U} \mathcal{R} : \text{Universe}\} (A : \text{Algebra } \mathcal{U} S)
  \{\theta : \text{Congruence } \{\mathcal{U}\} \{\mathcal{R}\} A\} \{a a' : | A |\}
  \rightarrow [ a ] \langle \theta \rangle \equiv [ a' ] \rightarrow \langle \theta \rangle a a'

 $\_/\text{-refl } A \{\theta\} (\text{refl } \_) = \text{IsEquivalence.rfl } (\text{IsEquiv } \theta) \_$$ 
```

(This page is almost entirely blank on purpose.)

4 Homomorphisms

This section presents the `UALib.Homomorphisms` module of the Agda UALib.

4.1 Basic Definitions

This subsection describes the `UALib.Homomorphisms.Basic` submodule of the Agda UALib. The definition of homomorphism in the Agda UALib is an *extensional* one; that is, the homomorphism condition holds pointwise. This will become clearer once we have the formal definitions in hand. Generally speaking, though, we say that two functions $f g : X \rightarrow Y$ are extensionally equal iff they are pointwise equal, that is, for all $x : X$ we have $f x \equiv g x$.

Now let's quickly dispense with the usual preliminaries so we can get down to the business of defining homomorphisms.

```
open import UALib.Algebras.Signatures using (Signature;  $\mathbb{O}$ ;  $\mathcal{V}$ )
module UALib.Homomorphisms.Basic {S : Signature  $\mathbb{O}$   $\mathcal{V}$ } where
open import UALib.Relations.Congruences{S = S} public
open import UALib.Prelude.Preliminaries using ( $\_ \equiv \_$ ;  $\_ \blacksquare$ ) public
```

To define *homomorphism*, we first say what it means for an operation f , interpreted in the algebras \mathbf{A} and \mathbf{B} , to commute with a function $g : A \rightarrow B$.

```
compatible-op-map : { $\mathbb{Q}$   $\mathcal{U}$  : Universe}(A : Algebra  $\mathbb{Q}$  S)(B : Algebra  $\mathcal{U}$  S)
  (f : | S |)(g : | A |  $\rightarrow$  | B |)  $\rightarrow$   $\mathcal{V} \sqcup \mathcal{U} \sqcup \mathbb{Q}$  .
```

```
compatible-op-map A B f g =  $\forall$  a  $\rightarrow$  g ((f  $\hat{\ } \mathbf{A}$ ) a)  $\equiv$  (f  $\hat{\ } \mathbf{B}$ ) (g  $\circ$  a)
```

Note the appearance of the shorthand $\forall \mathbf{a}$ in the definition of `compatible-op-map`. We can get away with this in place of the fully type-annotated equivalent, $(\mathbf{a} : \llbracket S \rrbracket f \rightarrow \mathbf{A})$ since Agda is able to infer that the \mathbf{a} here must be a tuple on \mathbf{A} of “length” $\llbracket S \rrbracket f$ (the arity of f).

```
op_interpreted-in_and_commutates-with : { $\mathbb{Q}$   $\mathcal{U}$  : Universe}
  (f : | S |)(A : Algebra  $\mathbb{Q}$  S)(B : Algebra  $\mathcal{U}$  S)
  (g : | A |  $\rightarrow$  | B |)  $\rightarrow$   $\mathcal{V} \sqcup \mathbb{Q} \sqcup \mathcal{U}$  .
```

```
op f interpreted-in A and B commutes-with g = compatible-op-map A B f g
```

We now define the type `hom A B` of **homomorphisms** from \mathbf{A} to \mathbf{B} by first defining the property `is-homomorphism`, as follows.

```
is-homomorphism : { $\mathbb{Q}$   $\mathcal{U}$  : Universe}(A : Algebra  $\mathbb{Q}$  S)(B : Algebra  $\mathcal{U}$  S)
   $\rightarrow$  (| A |  $\rightarrow$  | B |)  $\rightarrow$   $\mathbb{O} \sqcup \mathcal{V} \sqcup \mathbb{Q} \sqcup \mathcal{U}$  .
is-homomorphism A B g =  $\forall$  (f : | S |)  $\rightarrow$  compatible-op-map A B f g

hom : { $\mathbb{Q}$   $\mathcal{U}$  : Universe}  $\rightarrow$  Algebra  $\mathbb{Q}$  S  $\rightarrow$  Algebra  $\mathcal{U}$  S  $\rightarrow$   $\mathbb{O} \sqcup \mathcal{V} \sqcup \mathbb{Q} \sqcup \mathcal{U}$  .
hom A B =  $\Sigma$  g : (| A |  $\rightarrow$  | B |) , is-homomorphism A B g
```

4.1.1 Examples

A simple example is the identity map, which is proved to be a homomorphism as follows.

```
id : { $\mathcal{U}$  : Universe} (A : Algebra  $\mathcal{U}$  S)  $\rightarrow$  hom A A
id _ = ( $\lambda$  x  $\rightarrow$  x) ,  $\lambda$  _  $\rightarrow$  refl
```

```
id-is-hom : { $\mathcal{U}$  : Universe}{ $\mathbf{A}$  : Algebra  $\mathcal{U}$   $S$ } → is-homomorphism  $\mathbf{A}$   $\mathbf{A}$  (id |  $\mathbf{A}$  |)
id-is-hom = λ _ _ → refl _
```

4.1.2 Equalizers in Agda

Recall, the equalizer of two functions (resp., homomorphisms) $g h : A \rightarrow B$ is the subset of A on which the values of the functions g and h agree. We define the **equalizer** of functions and homomorphisms in Agda as follows.

–Equalizers of functions

```
 $\mathbf{E}$  : { $\mathcal{U}$   $\mathcal{W}$  : Universe}{ $A$  :  $\mathcal{U}$  ·}{ $B$  :  $\mathcal{W}$  ·}( $g h$  :  $A \rightarrow B$ ) → Pred  $A$   $\mathcal{W}$ 
 $\mathbf{E}$   $g h x = g x \equiv h x$ 
```

–Equalizers of homomorphisms

```
 $\mathbf{EH}$  : { $\mathcal{U}$   $\mathcal{W}$  : Universe}{ $\mathbf{A}$  : Algebra  $\mathcal{U}$   $S$ }{ $\mathbf{B}$  : Algebra  $\mathcal{W}$   $S$ }( $g h$  : hom  $\mathbf{A}$   $\mathbf{B}$ ) → Pred |  $\mathbf{A}$  |  $\mathcal{W}$ 
 $\mathbf{EH}$   $g h x = | g | x \equiv | h | x$ 
```

We will define subuniverses in the `UALib.Subalgebras.Subuniverses` module, but we note here that the equalizer of homomorphisms from \mathbf{A} to \mathbf{B} will turn out to be subuniverse of \mathbf{A} . Indeed, this easily follow from,

```
 $\mathbf{EH}$ -is-closed : { $\mathcal{U}$   $\mathcal{W}$  : Universe} → funext  $\mathcal{V}$   $\mathcal{W}$ 
→ { $\mathbf{A}$  : Algebra  $\mathcal{U}$   $S$ }{ $\mathbf{B}$  : Algebra  $\mathcal{W}$   $S$ }
  ( $g h$  : hom  $\mathbf{A}$   $\mathbf{B}$ ) { $f$  : |  $S$  | } ( $a$  : (||  $S$  ||  $f$ ) → |  $\mathbf{A}$  |)
→ ( ( $x$  : ||  $S$  ||  $f$ ) → ( $a x$ ) ∈ ( $\mathbf{EH}$  { $\mathbf{A} = \mathbf{A}$ }{ $\mathbf{B} = \mathbf{B}$ }  $g h$ ) )
-----
→ |  $g$  | (( $f$  ^  $\mathbf{A}$ )  $a$ ) ≡ |  $h$  | (( $f$  ^  $\mathbf{A}$ )  $a$ )

 $\mathbf{EH}$ -is-closed  $fe$  { $\mathbf{A}$ }{ $\mathbf{B}$ }  $g h$  { $f$ }  $a p =$ 
  |  $g$  | (( $f$  ^  $\mathbf{A}$ )  $a$ ) ≡ < ||  $g$  ||  $f a$  >
  ( $f$  ^  $\mathbf{B}$ )(|  $g$  | ◦  $a$ ) ≡ < ap ( _ ^  $\mathbf{B}$  )(  $fe p$  ) >
  ( $f$  ^  $\mathbf{B}$ )(|  $h$  | ◦  $a$ ) ≡ < (||  $h$  ||  $f a$ )1 >
  |  $h$  | (( $f$  ^  $\mathbf{A}$ )  $a$ ) ■
```

4.2 Kernels of Homomorphisms

This subsection describes the `UALib.Homomorphisms.Kernels` submodule of the Agda `UALib`. The kernel of a homomorphism is a congruence and conversely for every congruence θ , there exists a homomorphism with kernel θ .

```
open import UALib.Algebras.Signatures using (Signature;  $\mathfrak{G}$ ;  $\mathcal{V}$ )
open import UALib.Prelude.Preliminaries using (global-dfunext)

module UALib.Homomorphisms.Kernels { $S$  : Signature  $\mathfrak{G}$   $\mathcal{V}$ } { $gfe$  : global-dfunext} where

open import UALib.Homomorphisms.Basic{ $S = S$ } public

module _ { $\mathcal{U}$   $\mathcal{W}$  : Universe} where

  open Congruence
```

```
hom-kernel-is-compatible : (A : Algebra  $\mathcal{U}$  S){B : Algebra  $\mathcal{W}$  S}(h : hom A B)
  → compatible A (KER-rel | h |)
```

```
hom-kernel-is-compatible A {B} h f {a}{a'} Kerhab =  $\gamma$ 
```

where

```
 $\gamma$  : | h | ((f ^ A) a)   ≡ | h | ((f ^ A) a')
 $\gamma$  = | h | ((f ^ A) a) ≡ ⟨ || h || f a ⟩
      (f ^ B) (| h | ∘ a) ≡ ⟨ ap (λ - → (f ^ B) -) (gfe λ x → Kerhab x) ⟩
      (f ^ B) (| h | ∘ a') ≡ ⟨ (|| h || f a')-1 ⟩
      | h | ((f ^ A) a') ■
```

```
hom-kernel-is-equivalence : (A : Algebra  $\mathcal{U}$  S){B : Algebra  $\mathcal{W}$  S}(h : hom A B)
  → IsEquivalence (KER-rel | h |)
```

```
hom-kernel-is-equivalence A h = map-kernel-IsEquivalence | h |
```

It is convenient to define a function that takes a homomorphism and constructs a congruence from its kernel. We call this function `hom-kernel-congruence`, but since we will use it often we also give it a short alias—`kercon`.

`kercon` – (*alias*)

```
hom-kernel-congruence : (A : Algebra  $\mathcal{U}$  S){B : Algebra  $\mathcal{W}$  S}
  (h : hom A B) → Congruence A
```

```
hom-kernel-congruence A {B} h = mkcon (KER-rel | h |)
  (hom-kernel-is-compatible A {B} h)
  (hom-kernel-is-equivalence A {B} h)
```

`kercon` = `hom-kernel-congruence` – (*alias*)

```
quotient-by-hom-kernel : (A : Algebra  $\mathcal{U}$  S){B : Algebra  $\mathcal{W}$  S}
  (h : hom A B) → Algebra ( $\mathcal{U} \sqcup \mathcal{W}^+$ ) S
```

```
quotient-by-hom-kernel A {B} h = A / (hom-kernel-congruence A {B} h)
```

– NOTATION.

```
_[_]/ker_ : (A : Algebra  $\mathcal{U}$  S){B : Algebra  $\mathcal{W}$  S}(h : hom A B) → Algebra ( $\mathcal{U} \sqcup \mathcal{W}^+$ ) S
A [ B ]/ker h = quotient-by-hom-kernel A {B} h
```

```
epi : { $\mathcal{U} \mathcal{W}$  : Universe} → Algebra  $\mathcal{U}$  S → Algebra  $\mathcal{W}$  S →  $\mathcal{O} \sqcup \mathcal{V} \sqcup \mathcal{U} \sqcup \mathcal{W}^+$ 
```

```
epi A B =  $\Sigma$  g : (| A | → | B |) , is-homomorphism A B g × Epic g
```

```
epi-to-hom : { $\mathcal{U} \mathcal{W}$  : Universe}{A : Algebra  $\mathcal{U}$  S}{B : Algebra  $\mathcal{W}$  S}
```

```
  → epi A B → hom A B
```

```
epi-to-hom A  $\phi$  = |  $\phi$  | , fst ||  $\phi$  ||
```

`module` _ { $\mathcal{U} \mathcal{W}$: Universe} where

open Congruence

```
canonical-projection : (A : Algebra  $\mathcal{U}$  S) ( $\theta$  : Congruence{ $\mathcal{U}$ }{ $\mathcal{W}$ } A)
```

```
  → epi A (A /  $\theta$ )
```

canonical-projection $\mathbf{A} \theta = \mathbf{c}\pi$, $\mathbf{c}\pi$ -is-hom , $\mathbf{c}\pi$ -is-epic

where

$\mathbf{c}\pi : | \mathbf{A} | \rightarrow | \mathbf{A} / \theta |$
 $\mathbf{c}\pi a = \llbracket a \rrbracket - ([a] (KER-rel | h |)) , ?$

$\mathbf{c}\pi$ -is-hom : is-homomorphism $\mathbf{A} (\mathbf{A} / \theta) \mathbf{c}\pi$

$\mathbf{c}\pi$ -is-hom $f \mathbf{a} = \gamma$

where

$\gamma : \mathbf{c}\pi ((f \hat{\ } \mathbf{A}) \mathbf{a}) \equiv (f \hat{\ } (\mathbf{A} / \theta)) (\lambda x \rightarrow \mathbf{c}\pi (\mathbf{a} x))$
 $\gamma = \mathbf{c}\pi ((f \hat{\ } \mathbf{A}) \mathbf{a}) \equiv \langle refl \rangle$
 $\llbracket (f \hat{\ } \mathbf{A}) \mathbf{a} \rrbracket \equiv \langle refl \rangle$
 $(f \hat{\ } (\mathbf{A} / \theta)) (\lambda x \rightarrow \llbracket \mathbf{a} x \rrbracket) \equiv \langle refl \rangle$
 $(f \hat{\ } (\mathbf{A} / \theta)) (\lambda x \rightarrow \mathbf{c}\pi (\mathbf{a} x)) \blacksquare$

$\mathbf{c}\pi$ -is-epic : Epic $\mathbf{c}\pi$

$\mathbf{c}\pi$ -is-epic $(\langle \theta \rangle a) , a , refl _ = Image_ \exists _ .im a$

π^k - alias

kernel-quotient-projection : $\{\mathcal{U} \mathcal{W} : Universe\} - (pe : propext \mathcal{W})$
 $(\mathbf{A} : Algebra \mathcal{U} S)\{\mathbf{B} : Algebra \mathcal{W} S\}$
 $(h : hom \mathbf{A} \mathbf{B})$

\rightarrow $epi \mathbf{A} (\mathbf{A} [\mathbf{B}] / ker h)$

kernel-quotient-projection $\mathbf{A} \{\mathbf{B}\} h = \text{canonical-projection } \mathbf{A} (kercon \mathbf{A} \{\mathbf{B}\} h)$

$\pi^k = \text{kernel-quotient-projection}$

4.3 Homomorphism Theorems

This subsection describes the `UALib.Homomorphisms.Noether` submodule of the Agda `UALib`.

`open import UALib.Algebras.Signatures using (Signature; \mathcal{O} ; \mathcal{V})`
`open import UALib.Prelude.Preliminaries using (global-dfunext)`

`module UALib.Homomorphisms.Noether $\{S : Signature \mathcal{O} \mathcal{V}\} \{gfe : global-dfunext\}$ where`

`open import UALib.Homomorphisms.Kernels $\{S = S\} \{gfe\}$ hiding (global-dfunext) public`

4.3.1 The First Homomorphism Theorem

Here is a version of the so-called *First Homomorphism Theorem* (aka, the *First Isomorphism Theorem*).

`open Congruence`

`FirstIsomorphismTheorem : $\{\mathcal{U} \mathcal{W} : Universe\}$`
 `$(\mathbf{A} : Algebra \mathcal{U} S)(\mathbf{B} : Algebra \mathcal{W} S)$`
 `$(\phi : hom \mathbf{A} \mathbf{B}) (\phi E : Epic | \phi |)$`
`- extensionality assumptions:`
 `$\{pe : propext \mathcal{W}\}$`
 `$(Bset : is-set | \mathbf{B} |)$`

→ (∀ a x → is-subsingleton (⟨ kercon A{B} φ ⟩ a x))
 → (∀ C → is-subsingleton (℄{A = | A |}{⟨ kercon A{B} φ ⟩} C))

→ Σ f : (epi (A [B]/ker φ) B) , (| φ | ≡ | f | ∘ | π^k A {B} φ |) × is-embedding | f |

FirstIsomorphismTheorem {ℳ}{ℳ'} A B φ φE {pe} Bset ssR ssA =
 (fmap , fhom , fepic) , commuting , femb

where

θ : Congruence A

θ = kercon A{B} φ

A/θ : Algebra (ℳ ⊔ ℳ' +) S

A/θ = A [B]/ker φ

fmap : | A/θ | → | B |

fmap a = | φ | ⌈ a ⌋

fhom : is-homomorphism A/θ B fmap

fhom f a = | φ | (fst || (f ^ A/θ) a ||) ≡⟨ refl ⟩

| φ | ((f ^ A) (λ x → ⌈ (a x) ⌋)) ≡⟨ || φ || f (λ x → ⌈ (a x) ⌋) ⟩

(f ^ B) (| φ | ∘ (λ x → ⌈ (a x) ⌋)) ≡⟨ ap (λ - → (f ^ B) -) (gfe λ x → refl) ⟩

(f ^ B) (λ x → fmap (a x)) ■

fepic : Epic fmap

fepic b = γ

where

a : | A |

a = EpicInv | φ | φE b

a/θ : | A/θ |

a/θ = [a]

bfa : b ≡ fmap a/θ

bfa = (cong-app (EpicInvsRightInv gfe | φ | φE) b)⁻¹

γ : Image fmap ∋ b

γ = Image_∋_.eq b a/θ bfa

commuting : | φ | ≡ fmap ∘ | π^k A {B} φ |

commuting = refl

fmon : Monic fmap

fmon (.(⟨ θ ⟩ a) , a , refl _) (.(⟨ θ ⟩ a') , a' , refl _) faa' = γ

where

aθa' : ⟨ θ ⟩ a a'

aθa' = faa'

γ : (⟨ θ ⟩ a , a , refl) ≡ (⟨ θ ⟩ a' , a' , refl)

γ = class-extensionality' pe gfe ssR ssA (IsEquiv θ) aθa'

femb : is-embedding fmap

femb = monic-into-set-is-embedding Bset fmap fmon

4.3.2 Homomorphism composition

The composition of homomorphisms is again a homomorphism. For convenience, we give a few versions of this theorem which differ only with respect to which of their arguments are implicit.

`module` $_$ $\{ \mathcal{Q} \ \mathcal{U} \ \mathcal{W} : \text{Universe} \}$ `where`

– composition of homomorphisms 1

`HCompClosed` : $(\mathbf{A} : \text{Algebra } \mathcal{Q} \ S)(\mathbf{B} : \text{Algebra } \mathcal{U} \ S)(\mathbf{C} : \text{Algebra } \mathcal{W} \ S)$
 \rightarrow $\text{hom } \mathbf{A} \ \mathbf{B} \rightarrow \text{hom } \mathbf{B} \ \mathbf{C}$
 \rightarrow $\text{hom } \mathbf{A} \ \mathbf{C}$

`HCompClosed` $(A, FA) (B, FB) (C, FC) (g, ghom) (h, hhom) = h \circ g, \gamma$

`where`

$\gamma : (f : | S |)(a : \| S \| f \rightarrow A) \rightarrow (h \circ g)(FA \ f \ a) \equiv FC \ f \ (h \circ g \circ a)$

$\gamma \ f \ a = (h \circ g) \ (FA \ f \ a) \equiv \langle \text{ap } h \ (ghom \ f \ a) \rangle$
 $h \ (FB \ f \ (g \circ a)) \equiv \langle hhom \ f \ (g \circ a) \rangle$
 $FC \ f \ (h \circ g \circ a) \blacksquare$

– composition of homomorphisms 2

`HomComp` : $(\mathbf{A} : \text{Algebra } \mathcal{Q} \ S)\{\mathbf{B} : \text{Algebra } \mathcal{U} \ S\}(\mathbf{C} : \text{Algebra } \mathcal{W} \ S)$
 \rightarrow $\text{hom } \mathbf{A} \ \mathbf{B} \rightarrow \text{hom } \mathbf{B} \ \mathbf{C}$
 \rightarrow $\text{hom } \mathbf{A} \ \mathbf{C}$

`HomComp` $\mathbf{A} \ \{\mathbf{B}\} \ \mathbf{C} \ f \ g = \text{HCompClosed } \mathbf{A} \ \mathbf{B} \ \mathbf{C} \ f \ g$

– composition of homomorphisms 3

`o-hom` : $\{\mathcal{X} \ \mathcal{Y} \ \mathcal{Z} : \text{Universe}\}$
 $(\mathbf{A} : \text{Algebra } \mathcal{X} \ S)(\mathbf{B} : \text{Algebra } \mathcal{Y} \ S)(\mathbf{C} : \text{Algebra } \mathcal{Z} \ S)$
 $\{f : | \mathbf{A} | \rightarrow | \mathbf{B} |\} \{g : | \mathbf{B} | \rightarrow | \mathbf{C} |\}$
 \rightarrow $\text{is-homomorphism } \{\mathcal{X}\}\{\mathcal{Y}\} \ \mathbf{A} \ \mathbf{B} \ f \rightarrow \text{is-homomorphism } \{\mathcal{Y}\}\{\mathcal{Z}\} \ \mathbf{B} \ \mathbf{C} \ g$
 \rightarrow $\text{is-homomorphism } \{\mathcal{X}\}\{\mathcal{Z}\} \ \mathbf{A} \ \mathbf{C} \ (g \circ f)$

`o-hom` $\mathbf{A} \ \mathbf{B} \ \mathbf{C} \ \{f\} \ \{g\} \ fhom \ ghom = \| \text{HCompClosed } \mathbf{A} \ \mathbf{B} \ \mathbf{C} \ (f, fhom) \ (g, ghom) \|$

– composition of homomorphisms 4

`o-Hom` : $\{\mathcal{X} \ \mathcal{Y} \ \mathcal{Z} : \text{Universe}\}$
 $(\mathbf{A} : \text{Algebra } \mathcal{X} \ S)\{\mathbf{B} : \text{Algebra } \mathcal{Y} \ S\}(\mathbf{C} : \text{Algebra } \mathcal{Z} \ S)$
 $\{f : | \mathbf{A} | \rightarrow | \mathbf{B} |\} \{g : | \mathbf{B} | \rightarrow | \mathbf{C} |\}$
 \rightarrow $\text{is-homomorphism } \{\mathcal{X}\}\{\mathcal{Y}\} \ \mathbf{A} \ \mathbf{B} \ f \rightarrow \text{is-homomorphism } \{\mathcal{Y}\}\{\mathcal{Z}\} \ \mathbf{B} \ \mathbf{C} \ g$
 \rightarrow $\text{is-homomorphism } \{\mathcal{X}\}\{\mathcal{Z}\} \ \mathbf{A} \ \mathbf{C} \ (g \circ f)$

`o-Hom` $\mathbf{A} \ \{\mathbf{B}\} \ \mathbf{C} \ \{f\} \ \{g\} = \text{o-hom } \mathbf{A} \ \mathbf{B} \ \mathbf{C} \ \{f\} \ \{g\}$

`trans-hom` : $\{\mathcal{X} \ \mathcal{Y} \ \mathcal{Z} : \text{Universe}\}$

$(\mathbf{A} : \text{Algebra } \mathcal{X} \ S)(\mathbf{B} : \text{Algebra } \mathcal{Y} \ S)(\mathbf{C} : \text{Algebra } \mathcal{Z} \ S)$
 $(f : | \mathbf{A} | \rightarrow | \mathbf{B} |)(g : | \mathbf{B} | \rightarrow | \mathbf{C} |)$

$$\begin{aligned} &\rightarrow \text{is-homomorphism}\{\mathfrak{X}\}\{\mathfrak{Y}\} \mathbf{A} \mathbf{B} f \rightarrow \text{is-homomorphism}\{\mathfrak{Y}\}\{\mathfrak{Z}\} \mathbf{B} \mathbf{C} g \\ &\quad \text{-----} \\ &\rightarrow \text{is-homomorphism}\{\mathfrak{X}\}\{\mathfrak{Z}\} \mathbf{A} \mathbf{C} (g \circ f) \\ \text{trans-hom } \{\mathfrak{X}\}\{\mathfrak{Y}\}\{\mathfrak{Z}\} \mathbf{A} \mathbf{B} \mathbf{C} f g = \text{o-hom } \{\mathfrak{X}\}\{\mathfrak{Y}\}\{\mathfrak{Z}\} \mathbf{A} \mathbf{B} \mathbf{C} \{f\}\{g\} \end{aligned}$$

4.3.3 Homomorphism decomposition

If $g : \text{hom } \mathbf{A} \mathbf{B}$, $h : \text{hom } \mathbf{A} \mathbf{C}$, h is surjective, and $\ker h \subseteq \ker g$, then there exists $\phi : \text{hom } \mathbf{C} \mathbf{B}$ such that $g = \phi \circ h$, that is, such that the following diagram commutes.

$$\begin{array}{ccc} \mathbf{A} & \xrightarrow{h} & \mathbf{C} \\ & \searrow g & \downarrow \exists \phi \\ & & \mathbf{B} \end{array}$$

This, or some variation of it, is sometimes referred to as the *Second Isomorphism Theorem*. We formalize its statement and proof as follows. (Notice that the proof is constructive.)

$$\begin{aligned} \text{homFactor} &: \{\mathfrak{U} : \text{Universe}\} \rightarrow \text{funext } \mathfrak{U} \mathfrak{U} \rightarrow \{\mathbf{A} \mathbf{B} \mathbf{C} : \text{Algebra } \mathfrak{U} S\} \\ &\quad (g : \text{hom } \mathbf{A} \mathbf{B}) (h : \text{hom } \mathbf{A} \mathbf{C}) \\ &\rightarrow \text{ker-pred } | h | \subseteq \text{ker-pred } | g | \rightarrow \text{Epic } | h | \\ &\quad \text{-----} \\ &\rightarrow \Sigma \phi : (\text{hom } \mathbf{C} \mathbf{B}), | g | \equiv | \phi \circ | h | \end{aligned}$$

$$\begin{aligned} \text{homFactor } fe \{ \mathbf{A} = A, FA \} \{ \mathbf{B} = B, FB \} \{ \mathbf{C} = C, FC \} \\ (g, ghom) (h, hhom) Kh \subseteq Kg hEpi = (\phi, \phi \text{IsHomCB}), g \equiv \phi \circ h \end{aligned}$$

where

$$\begin{aligned} \text{hInv} &: C \rightarrow A \\ \text{hInv} &= \lambda c \rightarrow (\text{EpicInv } h hEpi) c \end{aligned}$$

$$\begin{aligned} \phi &: C \rightarrow B \\ \phi &= \lambda c \rightarrow g (\text{hInv } c) \end{aligned}$$

$$\begin{aligned} \xi &: (x : A) \rightarrow \text{ker-pred } h (x, \text{hInv } (h x)) \\ \xi x &= (\text{cong-app } (\text{EpicInvsRightInv } fe h hEpi) (h x))^{-1} \end{aligned}$$

$$\begin{aligned} g \equiv \phi \circ h &: g \equiv \phi \circ h \\ g \equiv \phi \circ h &= fe \lambda x \rightarrow Kh \subseteq Kg (\xi x) \end{aligned}$$

$$\begin{aligned} \zeta &: (f : | S |)(c : || S || f \rightarrow C)(x : || S || f) \\ &\rightarrow c x \equiv (h \circ \text{hInv})(c x) \end{aligned}$$

$$\zeta f c x = (\text{cong-app } (\text{EpicInvsRightInv } fe h hEpi) (c x))^{-1}$$

$$\begin{aligned} \iota &: (f : | S |)(c : || S || f \rightarrow C) \\ &\rightarrow (\lambda x \rightarrow c x) \equiv (\lambda x \rightarrow h (\text{hInv } (c x))) \end{aligned}$$

$$\iota f c = \text{ap } (\lambda - \rightarrow - \circ c) (\text{EpicInvsRightInv } fe h hEpi)^{-1}$$

```

useker : (f : | S |) (c : || S || f → C)
  → g (hInV (h (FA f (hInV o c)))) ≡ g(FA f (hInV o c))

```

```

useker = λ f c
  → Kh⊆Kg (cong-app
    (EpicInVlsRightInv fe h hEpi)
    (h(FA f(hInV o c)))
  )

```

```

phiHomCB : (f : | S |)(a : || S || f → C)
  → φ (FC f a) ≡ FB f (φ o a)

```

```

phiHomCB f c =
  g (hInV (FC f c))           ≡⟨ i ⟩
  g (hInV (FC f (h o (hInV o c)))) ≡⟨ ii ⟩
  g (hInV (h (FA f (hInV o c)))) ≡⟨ iii ⟩
  g (FA f (hInV o c))         ≡⟨ iv ⟩
  FB f (λ x → g (hInV (c x))) ■

```

where

```

i = ap (g o hInV) (ap (FC f) (ι f c))
ii = ap (λ - → g (hInV -)) (ghom f (hInV o c))1
iii = useker f c
iv = ghom f (hInV o c)

```

4.4 Products and Homomorphisms

This subsection describes the `UALib.Homomorphisms.Products` submodule of the Agda `UALib`.

```

open import UALib.Algebras.Signatures using (Signature; ⓪; ℱ)
open import UALib.Prelude.Preliminaries using (global-dfunext)

module UALib.Homomorphisms.Products {S : Signature ⓪ ℱ}{gfe : global-dfunext} where

open import UALib.Homomorphisms.Noether{S = S}{gfe} public

⊓-hom : global-dfunext → {⓪ ℱ : Universe}
  {I : ℱ ·}{ℳ : I → Algebra ⓪ S}{ℬ : I → Algebra ℱ S}
  → ((i : I) → hom (ℳ i)(ℬ i))
  →
  -----
  → hom (⊓ ℳ) (⊓ ℬ)

⊓-hom gfe {⓪}{ℱ}{I}{ℳ}{ℬ} homs = φ , φhom
where
  φ : | ⊓ ℳ | → | ⊓ ℬ |
  φ = λ x i → | homs i | (x i)

φhom : is-homomorphism (⊓ ℳ) (⊓ ℬ) φ
φhom f a = gfe (λ i → || homs i || f (λ x → a x i))

```

4.4.1 Projection homomorphisms

Later we will need a proof of the fact that projecting out of a product algebra onto one of its factors is a homomorphism.

$$\begin{array}{c} \prod\text{-projection-hom} : \{ \mathcal{U} \mathcal{F} : \text{Universe} \} \\ \{ I : \mathcal{F} \cdot \} \{ \mathcal{A} : I \rightarrow \text{Algebra } \mathcal{U} S \} \\ \hline \rightarrow (i : I) \rightarrow \text{hom} (\prod \mathcal{A}) (\mathcal{A} i) \end{array}$$

$$\prod\text{-projection-hom} \{ \mathcal{U} \} \{ \mathcal{F} \} \{ I \} \{ \mathcal{A} \} i = \phi i, \phi \text{ihom}$$

where

$$\begin{array}{l} \phi i : | \prod \mathcal{A} | \rightarrow | \mathcal{A} i | \\ \phi i = \lambda x \rightarrow x i \end{array}$$

$$\begin{array}{l} \phi \text{ihom} : \text{is-homomorphism} (\prod \mathcal{A}) (\mathcal{A} i) \phi i \\ \phi \text{ihom} f \mathbf{a} = \phi i ((f \hat{\ } \prod \mathcal{A}) \mathbf{a}) \equiv \langle \text{refl} \rangle \\ ((f \hat{\ } \prod \mathcal{A}) \mathbf{a}) i \equiv \langle \text{refl} \rangle \\ (f \hat{\ } \mathcal{A} i) (\lambda x \rightarrow \mathbf{a} x i) \equiv \langle \text{refl} \rangle \\ (f \hat{\ } \mathcal{A} i) (\lambda x \rightarrow \phi i (\mathbf{a} x)) \blacksquare \end{array}$$

(Of course, we could prove a more general result involving projections onto multiple factors, but so far the single-factor result has sufficed.)

4.5 Isomorphism Type

This subsection describes the `UALib.Homomorphisms.Isomorphisms` submodule of the Agda UALib. We implement (the extensional version of) the notion of isomorphism between algebraic structures.

```
open import UALib.Algebras.Signatures using (Signature;  $\mathfrak{O}$ ;  $\mathcal{V}$ )
open import UALib.Prelude.Preliminaries using (global-dfunext)
```

```
module UALib.Homomorphisms.Isomorphisms {S : Signature  $\mathfrak{O}$   $\mathcal{V}$ } {gfe : global-dfunext} where
```

```
open import UALib.Homomorphisms.Products {S = S} {gfe} public
open import UALib.Prelude.Preliminaries using (is-equiv; hfnext; Nat; NatII; NatII-is-embedding) public
```

$$\begin{array}{l} \cong : \{ \mathcal{U} \mathcal{W} : \text{Universe} \} (A : \text{Algebra } \mathcal{U} S) (B : \text{Algebra } \mathcal{W} S) \rightarrow \mathfrak{O} \sqcup \mathcal{V} \sqcup \mathcal{U} \sqcup \mathcal{W} \cdot \\ A \cong B = \Sigma f : (\text{hom } A B), \Sigma g : (\text{hom } B A), ((| f | \circ | g |) \sim | id B |) \times ((| g | \circ | f |) \sim | id A |) \end{array}$$

Recall, $f \sim g$ means f and g are extensionally equal; i.e., $\forall x, f x \equiv g x$.

4.5.1 Isomorphism toolbox

Here are some useful definitions and theorems for working with isomorphisms of algebraic structures.

```
module  $\_$  {  $\mathcal{U} \mathcal{W} : \text{Universe} \} \{ A : \text{Algebra } \mathcal{U} S \} \{ B : \text{Algebra } \mathcal{W} S \} where

   $\cong$ -hom : ( $\phi : A \cong B$ )  $\rightarrow$  hom A B
   $\cong$ -hom  $\phi = | \phi |$ 

   $\cong$ -inv-hom : ( $\phi : A \cong B$ )  $\rightarrow$  hom B A$ 
```

$\cong\text{-inv-hom } \phi = \text{fst } \parallel \phi \parallel$

$\cong\text{-map} : (\phi : \mathbf{A} \cong \mathbf{B}) \rightarrow | \mathbf{A} | \rightarrow | \mathbf{B} |$

$\cong\text{-map } \phi = | \cong\text{-hom } \phi |$

$\cong\text{-map-is-homomorphism} : (\phi : \mathbf{A} \cong \mathbf{B}) \rightarrow \text{is-homomorphism } \mathbf{A} \mathbf{B} (\cong\text{-map } \phi)$

$\cong\text{-map-is-homomorphism } \phi = \parallel \cong\text{-hom } \phi \parallel$

$\cong\text{-inv-map} : (\phi : \mathbf{A} \cong \mathbf{B}) \rightarrow | \mathbf{B} | \rightarrow | \mathbf{A} |$

$\cong\text{-inv-map } \phi = | \cong\text{-inv-hom } \phi |$

$\cong\text{-inv-map-is-homomorphism} : (\phi : \mathbf{A} \cong \mathbf{B}) \rightarrow \text{is-homomorphism } \mathbf{B} \mathbf{A} (\cong\text{-inv-map } \phi)$

$\cong\text{-inv-map-is-homomorphism } \phi = \parallel \cong\text{-inv-hom } \phi \parallel$

$\cong\text{-map-invertible} : (\phi : \mathbf{A} \cong \mathbf{B}) \rightarrow \text{invertible } (\cong\text{-map } \phi)$

$\cong\text{-map-invertible } \phi = (\cong\text{-inv-map } \phi), (\parallel \text{snd } \parallel \phi \parallel \parallel, | \text{snd } \parallel \phi \parallel |)$

$\cong\text{-map-is-equiv} : (\phi : \mathbf{A} \cong \mathbf{B}) \rightarrow \text{is-equiv } (\cong\text{-map } \phi)$

$\cong\text{-map-is-equiv } \phi = \text{invertibles-are-equivs } (\cong\text{-map } \phi) (\cong\text{-map-invertible } \phi)$

$\cong\text{-map-is-embedding} : (\phi : \mathbf{A} \cong \mathbf{B}) \rightarrow \text{is-embedding } (\cong\text{-map } \phi)$

$\cong\text{-map-is-embedding } \phi = \text{equivs-are-embeddings } (\cong\text{-map } \phi) (\cong\text{-map-is-equiv } \phi)$

4.5.2 Isomorphism is an equivalence relation

$\text{REFL-}\cong \text{ID}\cong : \{\mathcal{U} : \text{Universe}\} (\mathbf{A} : \text{Algebra } \mathcal{U} S) \rightarrow \mathbf{A} \cong \mathbf{A}$

$\text{ID}\cong \mathbf{A} = \text{id } \mathbf{A}, \text{id } \mathbf{A}, (\lambda a \rightarrow \text{refl}), (\lambda a \rightarrow \text{refl})$

$\text{REFL-}\cong = \text{ID}\cong$

$\text{refl-}\cong \text{id}\cong : \{\mathcal{U} : \text{Universe}\} \{\mathbf{A} : \text{Algebra } \mathcal{U} S\} \rightarrow \mathbf{A} \cong \mathbf{A}$

$\text{id}\cong \{\mathcal{U}\}\{\mathbf{A}\} = \text{ID}\cong \{\mathcal{U}\} \mathbf{A}$

$\text{refl-}\cong = \text{id}\cong$

$\text{sym-}\cong : \{\mathcal{Q} \mathcal{U} : \text{Universe}\} \{\mathbf{A} : \text{Algebra } \mathcal{Q} S\} \{\mathbf{B} : \text{Algebra } \mathcal{U} S\}$

$\rightarrow \mathbf{A} \cong \mathbf{B} \rightarrow \mathbf{B} \cong \mathbf{A}$

$\text{sym-}\cong h = \text{fst } \parallel h \parallel, \text{fst } h, \parallel \text{snd } \parallel h \parallel \parallel, | \text{snd } \parallel h \parallel |$

$\text{trans-}\cong : \{\mathcal{Q} \mathcal{U} \mathcal{W} : \text{Universe}\}$

$(\mathbf{A} : \text{Algebra } \mathcal{Q} S)(\mathbf{B} : \text{Algebra } \mathcal{U} S)(\mathbf{C} : \text{Algebra } \mathcal{W} S)$

$\rightarrow \mathbf{A} \cong \mathbf{B} \rightarrow \mathbf{B} \cong \mathbf{C}$

$\rightarrow \mathbf{A} \cong \mathbf{C}$

$\text{trans-}\cong \mathbf{A} \mathbf{B} \mathbf{C} \text{ } ab \text{ } bc = f, g, \alpha, \beta$

where

$f1 : \text{hom } \mathbf{A} \mathbf{B}$

$f1 = | ab |$

$f2 : \text{hom } \mathbf{B} \mathbf{C}$

$f2 = | bc |$

$f : \text{hom } \mathbf{A} \mathbf{C}$

$f = \text{HCompClosed } \mathbf{A} \mathbf{B} \mathbf{C} f1 f2$

```

g1 : hom C B
g1 = fst || bc ||
g2 : hom B A
g2 = fst || ab ||
g : hom C A
g = HCompClosed C B A g1 g2

f1~g2 : | f1 | o | g2 | ~ | id B |
f1~g2 = | snd || ab || |

g2~f1 : | g2 | o | f1 | ~ | id A |
g2~f1 = || snd || ab ||

f2~g1 : | f2 | o | g1 | ~ | id C |
f2~g1 = | snd || bc || |

g1~f2 : | g1 | o | f2 | ~ | id B |
g1~f2 = || snd || bc ||

α : | f | o | g | ~ | id C |
α x = ( | f | o | g | ) x ≡⟨ refl ⟩
      | f2 | ( ( | f1 | o | g2 | ) ( | g1 | x ) ) ≡⟨ ap | f2 | ( f1~g2 ( | g1 | x ) ) ⟩
      | f2 | ( | id B | ( | g1 | x ) ) ≡⟨ refl ⟩
      ( | f2 | o | g1 | ) x ≡⟨ f2~g1 x ⟩
      | id C | x ■

β : | g | o | f | ~ | id A |
β x = ( ap | g2 | ( g1~f2 ( | f1 | x ) ) ) · g2~f1 x

TRANS-≅ : {Q U W : Universe}
          {A : Algebra Q S}{B : Algebra U S}{C : Algebra W S}
→ A ≅ B → B ≅ C
-----
→ A ≅ C
TRANS-≅ {A = A}{B = B}{C = C} = trans-≅ A B C

Trans-≅ : {Q U W : Universe}
          (A : Algebra Q S){B : Algebra U S}(C : Algebra W S)
→ A ≅ B → B ≅ C
-----
→ A ≅ C
Trans-≅ A {B} C = trans-≅ A B C

```

4.5.3 Lift is an algebraic invariant

Fortunately, the lift operation preserves isomorphism (i.e., it's an “algebraic invariant”), which is why it's a workable solution to the “level hell” problem we mentioned earlier.

open Lift

–An algebra is isomorphic to its lift to a higher universe level

```
lift-alg-≅ : {U W : Universe}{A : Algebra U S} → A ≅ (lift-alg A W)
```

```
lift-alg-≅ = (lift , λ _ _ → refl) ,
```

$$\begin{aligned}
& (\text{lower}, \lambda _ _ \rightarrow \text{refl}), \\
& (\lambda _ \rightarrow \text{refl}), (\lambda _ \rightarrow \text{refl})
\end{aligned}$$

lift-*alg-hom* : (\mathfrak{X} : Universe){ \mathfrak{Y} : Universe}
(\mathfrak{X} : Universe){ \mathfrak{W} : Universe}
(A : Algebra \mathfrak{X} S) (B : Algebra \mathfrak{Y} S)
→ hom A B

→ hom (lift-*alg* A \mathfrak{X}) (lift-*alg* B \mathfrak{W})
lift-*alg-hom* \mathfrak{X} \mathfrak{X} { \mathfrak{W} } A B (f , $f\text{hom}$) = lift \circ f \circ lower , γ
where
lh : is-homomorphism (lift-*alg* A \mathfrak{X}) A lower
lh = $\lambda _ _ \rightarrow \text{refl}$
IABh : is-homomorphism (lift-*alg* A \mathfrak{X}) B (f \circ lower)
IABh = \circ -hom (lift-*alg* A \mathfrak{X}) A B {lower}{ f } lh $f\text{hom}$
Lh : is-homomorphism B (lift-*alg* B \mathfrak{W}) lift
Lh = $\lambda _ _ \rightarrow \text{refl}$
 γ : is-homomorphism (lift-*alg* A \mathfrak{X}) (lift-*alg* B \mathfrak{W}) (lift \circ (f \circ lower))
 γ = \circ -hom (lift-*alg* A \mathfrak{X}) B (lift-*alg* B \mathfrak{W}) { f \circ lower}{lift} IABh Lh

lift-*alg-iso* : (\mathfrak{X} : Universe){ \mathfrak{Y} : Universe}
(\mathfrak{X} : Universe){ \mathfrak{W} : Universe}
(A : Algebra \mathfrak{X} S) (B : Algebra \mathfrak{Y} S)
→ $A \cong B$

→ (lift-*alg* A \mathfrak{X}) \cong (lift-*alg* B \mathfrak{W})

lift-*alg-iso* \mathfrak{X} { \mathfrak{Y} } \mathfrak{X} { \mathfrak{W} } A B $A \cong B$ = TRANS- \cong (TRANS- \cong IA \cong A $A \cong B$) lift-*alg- \cong*
where
IA \cong A : (lift-*alg* A \mathfrak{X}) \cong A
IA \cong A = sym- \cong lift-*alg- \cong*

4.5.4 Lift associativity

The lift is also associative, up to isomorphism at least.

$$\begin{aligned}
\text{lift-*alg- assoc*$$
 : { \mathfrak{U} \mathfrak{W} \mathfrak{F} : Universe}{ A : Algebra \mathfrak{U} S }
→ lift-*alg* A ($\mathfrak{W} \sqcup \mathfrak{F}$) \cong (lift-*alg* (lift-*alg* A \mathfrak{W}) \mathfrak{F})
lift-*alg- assoc* { \mathfrak{U} } { \mathfrak{W} } { \mathfrak{F} } { A } = TRANS- \cong (TRANS- \cong ζ lift-*alg- \cong*) lift-*alg- \cong*
where
 ζ : lift-*alg* A ($\mathfrak{W} \sqcup \mathfrak{F}$) \cong A
 ζ = sym- \cong lift-*alg- \cong*

$$\begin{aligned}
\text{lift-*alg- associative*$$
 : { \mathfrak{U} \mathfrak{W} \mathfrak{F} : Universe}{ A : Algebra \mathfrak{U} S)
→ lift-*alg* A ($\mathfrak{W} \sqcup \mathfrak{F}$) \cong (lift-*alg* (lift-*alg* A \mathfrak{W}) \mathfrak{F})
lift-*alg- associative* { \mathfrak{U} }{ \mathfrak{W} }{ \mathfrak{F} } A = lift-*alg- assoc* { \mathfrak{U} }{ \mathfrak{W} }{ \mathfrak{F} }{ A }

4.5.5 Products preserve isomorphisms

$$\begin{aligned}
\sqcup \cong : \text{global-dfunext} \rightarrow \{\mathfrak{Q} \mathfrak{U} \mathfrak{F} : \text{Universe}\} \\
\{I : \mathfrak{F} \cdot\} \{sI : I \rightarrow \text{Algebra } \mathfrak{Q} \mathfrak{S}\} \{\mathfrak{B} : I \rightarrow \text{Algebra } \mathfrak{U} \mathfrak{S}\}
\end{aligned}$$

$$\begin{aligned} &\rightarrow ((i : I) \rightarrow (\mathcal{A} i) \cong (\mathcal{B} i)) \\ &\quad \text{-----} \\ &\rightarrow \prod \mathcal{A} \cong \prod \mathcal{B} \\ \prod \cong & \text{ gfe } \{\mathcal{Q}\}\{\mathcal{U}\}\{\mathcal{J}\}\{I\}\{\mathcal{A}\}\{\mathcal{B}\} \text{ AB} = \gamma \\ \text{where} & \\ \text{F} & : \forall i \rightarrow | \mathcal{A} i | \rightarrow | \mathcal{B} i | \\ \text{F } i & = | \text{fst } (\text{AB } i) | \\ \text{Fhom} & : \forall i \rightarrow \text{is-homomorphism } (\mathcal{A} i) (\mathcal{B} i) (\text{F } i) \\ \text{Fhom } i & = || \text{fst } (\text{AB } i) || \\ \\ \text{G} & : \forall i \rightarrow | \mathcal{B} i | \rightarrow | \mathcal{A} i | \\ \text{G } i & = \text{fst } | \text{snd } (\text{AB } i) | \\ \text{Ghom} & : \forall i \rightarrow \text{is-homomorphism } (\mathcal{B} i) (\mathcal{A} i) (\text{G } i) \\ \text{Ghom } i & = \text{snd } | \text{snd } (\text{AB } i) | \\ \\ \text{F}\sim\text{G} & : \forall i \rightarrow (\text{F } i) \circ (\text{G } i) \sim (| \text{id } (\mathcal{B} i) |) \\ \text{F}\sim\text{G } i & = \text{fst } || \text{snd } (\text{AB } i) || \\ \\ \text{G}\sim\text{F} & : \forall i \rightarrow (\text{G } i) \circ (\text{F } i) \sim (| \text{id } (\mathcal{A} i) |) \\ \text{G}\sim\text{F } i & = \text{snd } || \text{snd } (\text{AB } i) || \\ \\ \phi & : | \prod \mathcal{A} | \rightarrow | \prod \mathcal{B} | \\ \phi \text{ a } i & = \text{F } i (\text{a } i) \\ \\ \phi\text{hom} & : \text{is-homomorphism } (\prod \mathcal{A}) (\prod \mathcal{B}) \phi \\ \phi\text{hom } f \text{ a} & = \text{gfe } (\lambda i \rightarrow (\text{Fhom } i) f (\lambda x \rightarrow \text{a } x i)) \\ \\ \psi & : | \prod \mathcal{B} | \rightarrow | \prod \mathcal{A} | \\ \psi \text{ b } i & = | \text{fst } || \text{AB } i || | (\text{b } i) \\ \\ \psi\text{hom} & : \text{is-homomorphism } (\prod \mathcal{B}) (\prod \mathcal{A}) \psi \\ \psi\text{hom } f \text{ b} & = \text{gfe } (\lambda i \rightarrow (\text{Ghom } i) f (\lambda x \rightarrow \text{b } x i)) \\ \\ \phi\sim\psi & : \phi \circ \psi \sim | \text{id } (\prod \mathcal{B}) | \\ \phi\sim\psi \text{ b} & = \text{gfe } \lambda i \rightarrow \text{F}\sim\text{G } i (\text{b } i) \\ \\ \psi\sim\phi & : \psi \circ \phi \sim | \text{id } (\prod \mathcal{A}) | \\ \psi\sim\phi \text{ a} & = \text{gfe } \lambda i \rightarrow \text{G}\sim\text{F } i (\text{a } i) \\ \\ \gamma & : \prod \mathcal{A} \cong \prod \mathcal{B} \\ \gamma & = (\phi, \phi\text{hom}), ((\psi, \psi\text{hom}), \phi\sim\psi, \psi\sim\phi) \end{aligned}$$

A nearly identical proof goes through for isomorphisms of lifted products.

$$\begin{aligned} \text{lift-alg-}\prod \cong & : \text{global-dfunext} \rightarrow \{\mathcal{Q} \mathcal{U} \mathcal{J} \mathcal{X} : \text{Universe}\} \\ & \{I : \mathcal{J} \cdot\} \{\mathcal{A} : I \rightarrow \text{Algebra } \mathcal{Q} S\} \{\mathcal{B} : (\text{Lift } \{\mathcal{J}\}\{\mathcal{X}\} I) \rightarrow \text{Algebra } \mathcal{U} S\} \\ & \rightarrow ((i : I) \rightarrow (\mathcal{A} i) \cong (\mathcal{B} (\text{lift } i))) \\ & \quad \text{-----} \\ & \rightarrow \text{lift-alg } (\prod \mathcal{A}) \mathcal{X} \cong \prod \mathcal{B} \\ \text{lift-alg-}\prod \cong & \text{ gfe } \{\mathcal{Q}\}\{\mathcal{U}\}\{\mathcal{J}\}\{\mathcal{X}\}\{I\}\{\mathcal{A}\}\{\mathcal{B}\} \text{ AB} = \gamma \\ \text{where} & \end{aligned}$$

$$\begin{aligned}
& \mathbf{F} : \forall i \rightarrow | \mathcal{A} \ i | \rightarrow | \mathcal{B} \ (\text{lift } i) | \\
& \mathbf{F} \ i = | \text{fst } (AB \ i) | \\
& \mathbf{Fhom} : \forall i \rightarrow \text{is-homomorphism } (\mathcal{A} \ i) (\mathcal{B} \ (\text{lift } i)) (\mathbf{F} \ i) \\
& \mathbf{Fhom} \ i = || \text{fst } (AB \ i) || \\
\\
& \mathbf{G} : \forall i \rightarrow | \mathcal{B} \ (\text{lift } i) | \rightarrow | \mathcal{A} \ i | \\
& \mathbf{G} \ i = \text{fst } | \text{snd } (AB \ i) | \\
& \mathbf{Ghom} : \forall i \rightarrow \text{is-homomorphism } (\mathcal{B} \ (\text{lift } i)) (\mathcal{A} \ i) (\mathbf{G} \ i) \\
& \mathbf{Ghom} \ i = \text{snd } | \text{snd } (AB \ i) | \\
\\
& \mathbf{F} \sim \mathbf{G} : \forall i \rightarrow (\mathbf{F} \ i) \circ (\mathbf{G} \ i) \sim (| \text{id } (\mathcal{B} \ (\text{lift } i)) |) \\
& \mathbf{F} \sim \mathbf{G} \ i = \text{fst } || \text{snd } (AB \ i) || \\
\\
& \mathbf{G} \sim \mathbf{F} : \forall i \rightarrow (\mathbf{G} \ i) \circ (\mathbf{F} \ i) \sim (| \text{id } (\mathcal{A} \ i) |) \\
& \mathbf{G} \sim \mathbf{F} \ i = \text{snd } || \text{snd } (AB \ i) || \\
\\
& \phi : | \prod \mathcal{A} | \rightarrow | \prod \mathcal{B} | \\
& \phi \ a \ i = \mathbf{F} \ (\text{lower } i) \ (a \ (\text{lower } i)) \\
\\
& \phi\text{hom} : \text{is-homomorphism } (\prod \mathcal{A}) (\prod \mathcal{B}) \ \phi \\
& \phi\text{hom} \ f \ \mathbf{a} = \text{gfe } (\lambda i \rightarrow (\mathbf{Fhom} \ (\text{lower } i)) \ f \ (\lambda x \rightarrow \mathbf{a} \ x \ (\text{lower } i))) \\
\\
& \psi : | \prod \mathcal{B} | \rightarrow | \prod \mathcal{A} | \\
& \psi \ b \ i = | \text{fst } || AB \ i || | \ (b \ (\text{lift } i)) \\
\\
& \psi\text{hom} : \text{is-homomorphism } (\prod \mathcal{B}) (\prod \mathcal{A}) \ \psi \\
& \psi\text{hom} \ f \ \mathbf{b} = \text{gfe } (\lambda i \rightarrow (\mathbf{Ghom} \ i) \ f \ (\lambda x \rightarrow \mathbf{b} \ x \ (\text{lift } i))) \\
\\
& \phi \sim \psi : \phi \circ \psi \sim | \text{id } (\prod \mathcal{B}) | \\
& \phi \sim \psi \ \mathbf{b} = \text{gfe } \lambda i \rightarrow \mathbf{F} \sim \mathbf{G} \ (\text{lower } i) \ (\mathbf{b} \ i) \\
\\
& \psi \sim \phi : \psi \circ \phi \sim | \text{id } (\prod \mathcal{A}) | \\
& \psi \sim \phi \ \mathbf{a} = \text{gfe } \lambda i \rightarrow \mathbf{G} \sim \mathbf{F} \ i \ (\mathbf{a} \ i) \\
\\
& \mathbf{A} \cong \mathbf{B} : \prod \mathcal{A} \cong \prod \mathcal{B} \\
& \mathbf{A} \cong \mathbf{B} = (\phi, \phi\text{hom}), ((\psi, \psi\text{hom}), \phi \sim \psi, \psi \sim \phi) \\
\\
& \gamma : \text{lift-alg } (\prod \mathcal{A}) \ \mathfrak{X} \cong \prod \mathcal{B} \\
& \gamma = \text{Trans-}\cong (\text{lift-alg } (\prod \mathcal{A}) \ \mathfrak{X}) (\prod \mathcal{B}) \ (\text{sym-}\cong \text{ lift-alg-}\cong) \ \mathbf{A} \cong \mathbf{B}
\end{aligned}$$

4.5.6 Embedding tools

Here are some useful tools for working with embeddings.

$$\begin{aligned}
& \text{embedding-lift-nat} : \{\mathcal{Q} \ \mathcal{U} \ \mathcal{F} : \text{Universe}\} \rightarrow \text{hfunext } \mathcal{F} \ \mathcal{Q} \rightarrow \text{hfunext } \mathcal{F} \ \mathcal{U} \\
& \rightarrow \{I : \mathcal{F} \ \cdot\} \{A : I \rightarrow \mathcal{Q} \ \cdot\} \{B : I \rightarrow \mathcal{U} \ \cdot\} \\
& \quad (h : \text{Nat } A \ B) \\
& \rightarrow ((i : I) \rightarrow \text{is-embedding } (h \ i)) \\
& \quad \text{-----} \\
& \rightarrow \text{is-embedding}(\text{NatII } h)
\end{aligned}$$

$$\text{embedding-lift-nat} \ \text{hfiq} \ \text{hfiu} \ h \ \text{hem} = \text{NatII-is-embedding} \ \text{hfiq} \ \text{hfiu} \ h \ \text{hem}$$

```

embedding-lift-nat' : {Q U F : Universe} → hfunext F Q → hfunext F U
→ {I : F *} {A : I → Algebra Q S} {B : I → Algebra U S}
(h : Nat (fst ∘ A) (fst ∘ B))
→ ((i : I) → is-embedding (h i))
→ is-embedding(NatII h)

embedding-lift-nat' hfiq hfiu h hem = NatII-is-embedding hfiq hfiu h hem

embedding-lift : {Q U F : Universe} → hfunext F Q → hfunext F U
→ {I : F *} - global-dfunext → {Q U F : Universe} {I : F *}
{A : I → Algebra Q S} {B : I → Algebra U S}
(h : ∀ i → | A i | → | B i |)
→ ((i : I) → is-embedding (h i))
→ is-embedding(λ (x : | ∏ A |) (i : I) → (h i) (x i))
embedding-lift {Q} {U} {F} hfiq hfiu {I} {A} {B} h hem =
embedding-lift-nat' {Q} {U} {F} hfiq hfiu {I} {A} {B} h hem

iso→embedding : {U W : Universe} {A : Algebra U S} {B : Algebra W S}
→ (φ : A ≅ B) → is-embedding (fst | φ |)
iso→embedding {U} {W} {A} {B} φ = γ
where
  f : hom A B
  f = | φ |
  g : hom B A
  g = | snd φ |

  finv : invertible | f |
  finv = | g | , (snd || snd φ || , fst || snd φ ||)

  γ : is-embedding | f |
  γ = equivs-are-embeddings | f | (invertibles-are-equivs | f | finv)

```

4.6 Homomorphic Image Type

This subsection describes the `UALib.Homomorphisms.HomomorphicImages` submodule of the Agda UALib.

```

open import UALib.Algebras.Signatures using (Signature; 0; V)
open import UALib.Prelude.Preliminaries using (global-dfunext)

module UALib.Homomorphisms.HomomorphicImages {S : Signature 0 V} {gfe : global-dfunext} where

open import UALib.Homomorphisms.Isomorphisms {S = S} {gfe} public

```

4.6.1 Images of a single algebra

We begin with what seems to be (for our purposes at least) the most useful way to represent, in Martin-Löf type theory, the class of **homomomorphic images** of an algebra.

$\text{HomImage} : \{\mathcal{U} \mathcal{W} : \text{Universe}\} \{A : \text{Algebra } \mathcal{U} S\} (B : \text{Algebra } \mathcal{W} S) (\phi : \text{hom } A B) \rightarrow |B| \rightarrow \mathcal{U} \sqcup \mathcal{W} \cdot$
 $\text{HomImage } B \phi = \lambda b \rightarrow \text{Image } | \phi | \ni b$

$\text{HomImagesOf} : \{\mathcal{U} \mathcal{W} : \text{Universe}\} \rightarrow \text{Algebra } \mathcal{U} S \rightarrow \mathcal{O} \sqcup \mathcal{V} \sqcup \mathcal{U} \sqcup \mathcal{W}^+ \cdot$

$\text{HomImagesOf } \{\mathcal{U}\}\{\mathcal{W}\} A = \Sigma B : (\text{Algebra } \mathcal{W} S), \Sigma \phi : (|A| \rightarrow |B|), \text{is-homomorphism } A B \phi \times \text{Epic } \phi$

4.6.2 Images of a class of algebras

Here are a few more definitions, derived from the one above, that will come in handy.

$_ \text{is-hom-image-of} _ : \{\mathcal{U} \mathcal{W} : \text{Universe}\} (B : \text{Algebra } \mathcal{W} S)$
 $\rightarrow (A : \text{Algebra } \mathcal{U} S) \rightarrow \mathcal{O} \sqcup \mathcal{V} \sqcup \mathcal{U} \sqcup \mathcal{W}^+ \cdot$

$_ \text{is-hom-image-of} _ \{\mathcal{U}\}\{\mathcal{W}\} B A = \Sigma C \phi : (\text{HomImagesOf } \{\mathcal{U}\}\{\mathcal{W}\} A), |C \phi| \cong B$

$_ \text{is-hom-image-of-class} _ : \{\mathcal{U} : \text{Universe}\} \rightarrow \text{Algebra } \mathcal{U} S \rightarrow \text{Pred } (\text{Algebra } \mathcal{U} S) (\mathcal{U}^+) \rightarrow \mathcal{O} \sqcup \mathcal{V} \sqcup \mathcal{U}^+ \cdot$

$_ \text{is-hom-image-of-class} _ \{\mathcal{U}\} B \mathcal{K} = \Sigma A : (\text{Algebra } \mathcal{U} S), (A \in \mathcal{K}) \times (B \text{ is-hom-image-of } A)$

$\text{HomImagesOfClass} : \{\mathcal{U} : \text{Universe}\} \rightarrow \text{Pred } (\text{Algebra } \mathcal{U} S) (\mathcal{U}^+) \rightarrow \mathcal{O} \sqcup \mathcal{V} \sqcup \mathcal{U}^+ \cdot$

$\text{HomImagesOfClass } \mathcal{K} = \Sigma B : (\text{Algebra } _ S), (B \text{ is-hom-image-of-class } \mathcal{K})$

$\text{all-ops-in_and_commute-with} : \{\mathcal{U} \mathcal{W} : \text{Universe}\}$
 $(A : \text{Algebra } \mathcal{U} S) (B : \text{Algebra } \mathcal{W} S)$
 $\rightarrow (|A| \rightarrow |B|) \rightarrow \mathcal{O} \sqcup \mathcal{V} \sqcup \mathcal{U} \sqcup \mathcal{W} \cdot$

$\text{all-ops-in } A \text{ and } B \text{ commute-with } g = \text{is-homomorphism } A B g$

4.6.3 Lifting tools

open Lift

$\text{lift-function} : (\mathcal{X} : \text{Universe}) \{ \mathcal{Y} : \text{Universe} \}$
 $(\mathcal{Z} : \text{Universe}) \{ \mathcal{W} : \text{Universe} \}$
 $(A : \mathcal{X}^+) (B : \mathcal{Y}^+) \rightarrow (f : A \rightarrow B)$
 $\rightarrow \text{Lift } \{ \mathcal{X} \} \{ \mathcal{Z} \} A \rightarrow \text{Lift } \{ \mathcal{Y} \} \{ \mathcal{W} \} B$

$\text{lift-function } \mathcal{X} \{ \mathcal{Y} \} \mathcal{Z} \{ \mathcal{W} \} A B f = \lambda la \rightarrow \text{lift } (f (\text{lower } la))$

$\text{lift-of-alg-epic-is-epic} : (\mathcal{X} : \text{Universe}) \{ \mathcal{Y} : \text{Universe} \}$
 $(\mathcal{Z} : \text{Universe}) \{ \mathcal{W} : \text{Universe} \}$
 $(A : \text{Algebra } \mathcal{X} S) (B : \text{Algebra } \mathcal{Y} S)$
 $(f : \text{hom } A B) \rightarrow \text{Epic } |f|$
 $\rightarrow \text{Epic } | \text{lift-alg-hom } \mathcal{X} \mathcal{Z} \{ \mathcal{W} \} A B f |$

$\text{lift-of-alg-epic-is-epic } \mathcal{X} \{ \mathcal{Y} \} \mathcal{Z} \{ \mathcal{W} \} A B f \text{epi} = \text{IE}$

where

$\text{IA} : \text{Algebra } (\mathcal{X} \sqcup \mathcal{Z}) S$

$\text{IA} = \text{lift-alg } A \mathcal{Z}$

$\text{IB} : \text{Algebra } (\mathcal{Y} \sqcup \mathcal{W}) S$

$\text{IB} = \text{lift-alg } B \mathcal{W}$

```

If : hom (lift-alg A  $\mathfrak{X}$ ) (lift-alg B  $\mathfrak{W}$ )
If = lift-alg-hom  $\mathfrak{X}$   $\mathfrak{X}$  A B f

IE : (y : | B |) → Image | f |  $\ni$  y
IE y =  $\xi$ 
  where
    b : | B |
    b = lower y

     $\zeta$  : Image | f |  $\ni$  b
     $\zeta$  = fepi b

    a : | A |
    a = Inv | f | b  $\zeta$ 

     $\eta$  : y  $\equiv$  | f | (lift a)
     $\eta$  = y  $\equiv$  (intensionality lift~lower) y
      lift b  $\equiv$  (ap lift (InvlInv | f | (lower y)  $\zeta$ )-1)
      lift (| f | a)  $\equiv$  (ap ( $\lambda$  -  $\rightarrow$  lift (| f | (- a)))) (lower~lift{ $\mathfrak{W}$  =  $\mathfrak{W}$ })
      lift (| f | ((lower{ $\mathfrak{W}$  =  $\mathfrak{W}$ }  $\circ$  lift) a))  $\equiv$  (refl)
      (lift  $\circ$  | f |  $\circ$  lower{ $\mathfrak{W}$  =  $\mathfrak{W}$ }) (lift a)  $\equiv$  (refl)
      | f | (lift a) ■

     $\xi$  : Image | f |  $\ni$  y
     $\xi$  = eq y (lift a)  $\eta$ 

lift-alg-hom-image : { $\mathfrak{X}$   $\mathfrak{Y}$   $\mathfrak{X}$   $\mathfrak{W}$  : Universe}
                    {A : Algebra  $\mathfrak{X}$  S}{B : Algebra  $\mathfrak{Y}$  S}
  → B is-hom-image-of A
  → (lift-alg B  $\mathfrak{W}$ ) is-hom-image-of (lift-alg A  $\mathfrak{X}$ )

lift-alg-hom-image { $\mathfrak{X}$ }{ $\mathfrak{Y}$ }{ $\mathfrak{X}$ }{ $\mathfrak{W}$ }{A}{B} ((C ,  $\phi$  ,  $\phi$ hom ,  $\phi$ epic) , C $\cong$ B) =  $\gamma$ 
  where
    IA : Algebra ( $\mathfrak{X}$   $\sqcup$   $\mathfrak{X}$ ) S
    IA = lift-alg A  $\mathfrak{X}$ 
    IB IC : Algebra ( $\mathfrak{Y}$   $\sqcup$   $\mathfrak{W}$ ) S
    IB = lift-alg B  $\mathfrak{W}$ 
    IC = lift-alg C  $\mathfrak{W}$ 

    I $\phi$  : hom IA IC
    I $\phi$  = (lift-alg-hom  $\mathfrak{X}$   $\mathfrak{X}$  A C) ( $\phi$  ,  $\phi$ hom)

    I $\phi$ epic : Epic | I $\phi$  |
    I $\phi$ epic = lift-of-alg-epic-is-epic  $\mathfrak{X}$   $\mathfrak{X}$  A C ( $\phi$  ,  $\phi$ hom)  $\phi$ epic

    IC $\phi$  : HomImagesOf { $\mathfrak{X}$   $\sqcup$   $\mathfrak{X}$ }{ $\mathfrak{Y}$   $\sqcup$   $\mathfrak{W}$ } IA
    IC $\phi$  = IC , | I $\phi$  | , || I $\phi$  || , I $\phi$ epic

    IC $\cong$ IB : IC  $\cong$  IB
    IC $\cong$ IB = lift-alg-iso  $\mathfrak{Y}$   $\mathfrak{W}$  C B C $\cong$ B

     $\gamma$  : IB is-hom-image-of IA
     $\gamma$  = IC $\phi$  , IC $\cong$ IB

```

(This page is almost entirely blank on purpose.)

5 Terms

This section presents the `UALib.Terms` module of the Agda `UALib`.

5.1 Basic Definitions

This subsection describes the `UALib.Terms.Basic` submodule of the Agda `UALib`.

```
open import UALib.Algebras using (Signature;  $\mathbb{O}$ ;  $\mathcal{V}$ ; Algebra;  $\_ \rightarrow \_$ )
open import UALib.Prelude.Preliminaries using (global-dfunext; Universe;  $\_ \cdot$ )

module UALib.Terms.Basic
  {S : Signature  $\mathbb{O}$   $\mathcal{V}$ } {gfe : global-dfunext}
  { $\mathcal{X}$  : { $\mathcal{U}$   $\mathfrak{X}$  : Universe} {X :  $\mathfrak{X}$   $\cdot$ } } {A : Algebra  $\mathcal{U}$  S}  $\rightarrow$  X  $\rightarrow$  A}
  where

  open import UALib.Homomorphisms.HomomorphicImages {S = S} {gfe} hiding (Universe;  $\_ \cdot$ ) public
```

5.1.1 The inductive type of terms

We define a type called `Term` which represents the type of terms of a given signature. As usual, the type $X : \mathcal{U}$ represents an arbitrary collection of variable symbols.

```
data Term { $\mathfrak{X}$  : Universe} {X :  $\mathfrak{X}$   $\cdot$ } :  $\mathbb{O} \sqcup \mathcal{V} \sqcup \mathfrak{X}^+ \cdot$  where
  generator : X  $\rightarrow$  Term { $\mathfrak{X}$ } {X}
  node : (f : | S |) (args : || S || f  $\rightarrow$  Term { $\mathfrak{X}$ } {X})  $\rightarrow$  Term

open Term
```

5.2 The Term Algebra

This subsection describes the `UALib.Terms.Free` submodule of the Agda `UALib`.

```
open import UALib.Algebras using (Signature;  $\mathbb{O}$ ;  $\mathcal{V}$ ; Algebra;  $\_ \rightarrow \_$ )
open import UALib.Prelude.Preliminaries using (global-dfunext; Universe;  $\_ \cdot$ )

module UALib.Terms.Free
  {S : Signature  $\mathbb{O}$   $\mathcal{V}$ } {gfe : global-dfunext}
  { $\mathcal{X}$  : { $\mathcal{U}$   $\mathfrak{X}$  : Universe} {X :  $\mathfrak{X}$   $\cdot$ } } {A : Algebra  $\mathcal{U}$  S}  $\rightarrow$  X  $\rightarrow$  A}
  where

  open import UALib.Terms.Basic {S = S} {gfe} { $\mathcal{X}$ } hiding (Algebra) public
```

Terms can be viewed as acting on other terms and we can form an algebraic structure whose domain and basic operations are both the collection of term operations. We call this the **term algebra** and denote it by $\mathbf{T} X$. In the Agda this algebra can be defined quite simply, as one would hope and expect.

```
-The term algebra  $\mathbf{T} X$ .
 $\mathbf{T}$  : { $\mathfrak{X}$  : Universe} {X :  $\mathfrak{X}$   $\cdot$ }  $\rightarrow$  Algebra ( $\mathbb{O} \sqcup \mathcal{V} \sqcup \mathfrak{X}^+$ ) S
 $\mathbf{T}$  { $\mathfrak{X}$ } X = Term { $\mathfrak{X}$ } {X} , node
```

5.2.1 The universal property

The Term algebra is **absolutely free** (or “universal”) for algebras in the signature S . That is, for every S -algebra \mathbf{A} ,

1. every map $h : X \rightarrow |\mathbf{A}|$ lifts to a homomorphism from $\mathbf{T} X$ to \mathbf{A} , and
2. the induced homomorphism is unique.

-1.a. Every map $(X \rightarrow \mathbf{A})$ lifts.

free-lift : $\{\mathfrak{X} \mathfrak{U} : \text{Universe}\}\{X : \mathfrak{X} \cdot\}(\mathbf{A} : \text{Algebra } \mathfrak{U} S)(h : X \rightarrow |\mathbf{A}|) \rightarrow |\mathbf{T} X| \rightarrow |\mathbf{A}|$

free-lift $_ h$ (**generator** x) = $h x$

free-lift $\mathbf{A} h$ (**node** f $args$) = $(f \hat{\ } \mathbf{A}) \lambda i \rightarrow \text{free-lift } \mathbf{A} h (args i)$

-1.b. The lift is (extensionally) a hom

lift-hom : $\{\mathfrak{X} \mathfrak{U} : \text{Universe}\}\{X : \mathfrak{X} \cdot\}(\mathbf{A} : \text{Algebra } \mathfrak{U} S)(h : X \rightarrow |\mathbf{A}|) \rightarrow \text{hom } (\mathbf{T} X) \mathbf{A}$

lift-hom $\mathbf{A} h$ = **free-lift** $\mathbf{A} h$, $\lambda f a \rightarrow \text{ap } (_ \hat{\ } \mathbf{A}) \text{ refl}$

-2. The lift to $(\text{free} \rightarrow \mathbf{A})$ is (extensionally) unique.

free-unique : $\{\mathfrak{X} \mathfrak{U} : \text{Universe}\}\{X : \mathfrak{X} \cdot\} \rightarrow \text{funext } \mathfrak{V} \mathfrak{U}$

$\rightarrow (\mathbf{A} : \text{Algebra } \mathfrak{U} S)(g h : \text{hom } (\mathbf{T} X) \mathbf{A})$

$\rightarrow (\forall x \rightarrow |g| (\text{generator } x) \equiv |h| (\text{generator } x))$

$\rightarrow (t : \text{Term } \{\mathfrak{X}\}\{X\})$

$\rightarrow |g| t \equiv |h| t$

free-unique $_ _ _ p$ (**generator** x) = $p x$

free-unique $fe \mathbf{A} g h p$ (**node** f $args$) =

$|g| (\text{node } f args) \equiv \langle |g| f args \rangle$

$(f \hat{\ } \mathbf{A})(\lambda i \rightarrow |g| (args i)) \equiv \langle \text{ap } (_ \hat{\ } \mathbf{A}) \gamma \rangle$

$(f \hat{\ } \mathbf{A})(\lambda i \rightarrow |h| (args i)) \equiv \langle (|h| f args)^{\perp} \rangle$

$|h| (\text{node } f args) \blacksquare$

where $\gamma = fe \lambda i \rightarrow \text{free-unique } fe \mathbf{A} g h p (args i)$

5.2.2 Lifting and imaging tools

Next we note the easy fact that the lift induced by h_0 agrees with h_0 on X and that the lift is surjective if h_0 is.

lift-agrees-on-X : $\{\mathfrak{X} \mathfrak{U} : \text{Universe}\}\{X : \mathfrak{X} \cdot\}$
 $(\mathbf{A} : \text{Algebra } \mathfrak{U} S)(h_0 : X \rightarrow |\mathbf{A}|)(x : X)$

$\rightarrow h_0 x \equiv | \text{lift-hom } \mathbf{A} h_0 | (\text{generator } x)$

lift-agrees-on-X $_ h_0 x = \text{refl}$

lift-of-epi-is-epi : $\{\mathfrak{X} \mathfrak{U} : \text{Universe}\}\{X : \mathfrak{X} \cdot\}$
 $(\mathbf{A} : \text{Algebra } \mathfrak{U} S)(h_0 : X \rightarrow |\mathbf{A}|)$

$\rightarrow \text{Epic } h_0 \rightarrow \text{Epic } | \text{lift-hom } \mathbf{A} h_0 |$

lift-of-epi-is-epi $\{\mathfrak{X}\}\{\mathfrak{U}\}\{X\} \mathbf{A} h_0 hE y = \gamma$


```

where
  h0pre : Image h0 ∋ y
  h0pre = hE y

  h0-1y : X
  h0-1y = Inv h0 y (hE y)

  η : y ≡ | lift-hom A h0 | (generator h0-1y)
  η =
    y      ≡⟨ (InvInv h0 y h0pre)-1 ⟩
    h0 h0-1y ≡⟨ lift-agrees-on-X A h0 h0-1y ⟩
    | lift-hom A h0 | (generator h0-1y) ■

  γ : Image | lift-hom A h0 | ∋ y
  γ = eq y (generator h0-1y) η

```

Since it's absolutely free, $\mathbf{T} X$ is the domain of a homomorphism to any algebra we like. The following function makes it easy to lay our hands on such homomorphisms.

```

Thom-gen : {X U : Universe}{X : X ·} (C : Algebra U S)
  → Σ h : (hom (T X) C), Epic | h |
Thom-gen {X}{U}{X} C = h , lift-of-epi-is-epi C h0 hE
where
  h0 : X → | C |
  h0 = fst (X C)

  hE : Epic h0
  hE = snd (X C)

  h : hom (T X) C
  h = lift-hom C h0

```

5.3 Term Operations

This subsection describes the `UALib.Terms.Operations` submodule of the Agda `UALib`.

```

open import UALib.Algebras using (Signature; 0; V; Algebra; _→_)
open import UALib.Prelude.Preliminaries using (global-dfunext; Universe; ·)

module UALib.Terms.Operations
  {S : Signature 0 V}{gfe : global-dfunext}
  {X : {U X : Universe}{X : X ·}(A : Algebra U S) → X → A}
  where

  open import UALib.Terms.Free{S = S}{gfe}{X} public

```

When we interpret a term in an algebra we call the result a **term operation**. Given a term p : `Term` and an algebra \mathbf{A} , we denote by $p \cdot \mathbf{A}$ the **interpretation** of p in \mathbf{A} . This is defined inductively as follows:

1. if p is $x : X$ (a variable) and if $\mathbf{a} : X \rightarrow |\mathbf{A}|$ is a tuple of elements of $|\mathbf{A}|$, then define $(p \cdot \mathbf{A}) \mathbf{a} = \mathbf{a} x$;

2. if $p = f \mathbf{s}$, where $f : |S|$ is an operation symbol and $\mathbf{s} : \|S\| f \rightarrow \mathbf{T} X$ is an $(\|S\| f)$ -tuple of terms and $\mathbf{a} : X \rightarrow |\mathbf{A}|$ is a tuple from \mathbf{A} , then define $(p \cdot \mathbf{A}) \mathbf{a} = ((f \mathbf{s}) \cdot \mathbf{A}) \mathbf{a} = (f \hat{\ } \mathbf{A}) \lambda i \rightarrow ((\mathbf{s} i) \cdot \mathbf{A}) \mathbf{a}$

In the Agda UALib term interpretation is defined as follows.

```

_·_ : { $\mathfrak{X} \mathfrak{U} : \mathbf{Universe}$ }{ $X : \mathfrak{X} \cdot$ }  $\rightarrow$   $\mathbf{Term}\{\mathfrak{X}\}\{X\} \rightarrow (\mathbf{A} : \mathbf{Algebra} \mathfrak{U} S) \rightarrow (X \rightarrow |\mathbf{A}|) \rightarrow |\mathbf{A}|$ 
((generator  $x$ )  $\cdot$   $\mathbf{A}$ )  $\mathbf{a} = \mathbf{a} x$ 
((node  $f$   $args$ )  $\cdot$   $\mathbf{A}$ )  $\mathbf{a} = (f \hat{\ } \mathbf{A}) \lambda i \rightarrow (args i \cdot \mathbf{A}) \mathbf{a}$ 

```

Observe that interpretation of a term is the same as **free-lift** (modulo argument order).

```

free-lift-interpretation : { $\mathfrak{X} \mathfrak{U} : \mathbf{Universe}$ }{ $X : \mathfrak{X} \cdot$ }
 $\rightarrow$   $(\mathbf{A} : \mathbf{Algebra} \mathfrak{U} S)(h : X \rightarrow |\mathbf{A}|)(p : \mathbf{Term})$ 
 $(p \cdot \mathbf{A}) h \equiv \mathbf{free-lift} \mathbf{A} h p$ 

```

```

free-lift-interpretation  $\mathbf{A} h$  (generator  $x$ ) = refl
free-lift-interpretation  $\mathbf{A} h$  (node  $f$   $args$ ) =  $\mathbf{ap} (f \hat{\ } \mathbf{A}) (gfe \lambda i \rightarrow \mathbf{free-lift-interpretation} \mathbf{A} h (args i))$ 

```

```

lift-hom-interpretation : { $\mathfrak{X} \mathfrak{U} : \mathbf{Universe}$ }{ $X : \mathfrak{X} \cdot$ }
 $\rightarrow$   $(\mathbf{A} : \mathbf{Algebra} \mathfrak{U} S)(h : X \rightarrow |\mathbf{A}|)(p : \mathbf{Term})$ 
 $(p \cdot \mathbf{A}) h \equiv \mathbf{lift-hom} \mathbf{A} h | p$ 

```

lift-hom-interpretation = free-lift-interpretation

Here we want $(\mathbf{t} : X \rightarrow |\mathbf{T}(X)|) \rightarrow ((p \cdot \mathbf{T}(X)) \mathbf{t}) \equiv p \mathbf{t} \dots$, but what is $(p \cdot \mathbf{T}(X)) \mathbf{t}$? By definition, it depends on the form of p as follows:

- if $p \equiv (\mathbf{generator} x)$, then $(p \cdot \mathbf{T}(X)) \mathbf{t} \equiv ((\mathbf{generator} x) \cdot \mathbf{T}(X)) \mathbf{t} \equiv \mathbf{t} x$
- if $p \equiv (\mathbf{node} f \mathbf{args})$, then $(p \cdot \mathbf{T}(X)) \mathbf{t} \equiv ((\mathbf{node} f \mathbf{args}) \cdot \mathbf{T}(X)) \mathbf{t} \equiv (f \hat{\ } \mathbf{T}(X)) \lambda i \rightarrow (args i \cdot \mathbf{T}(X)) \mathbf{t}$.

We claim that if $p : | \mathbf{T}(X) |$ then there exists $\mathbf{p} : | \mathbf{T}(X) |$ and $\mathbf{t} : X \rightarrow | \mathbf{T}(X) |$ such that $p \equiv (\mathbf{p} \cdot \mathbf{T}(X)) \mathbf{t}$. We prove this fact as follows.

```

term-op-interp1 : { $\mathfrak{X} : \mathbf{Universe}$ }{ $X : \mathfrak{X} \cdot$ }( $f : |S|$ )( $args : \|S\| f \rightarrow \mathbf{Term}$ )
 $\rightarrow$   $\mathbf{node} f \mathbf{args} \equiv (f \hat{\ } \mathbf{T} X) \mathbf{args}$ 
term-op-interp1 =  $\lambda f \mathbf{args} \rightarrow \mathbf{refl}$ 

```

```

term-op-interp2 : { $\mathfrak{X} : \mathbf{Universe}$ }{ $X : \mathfrak{X} \cdot$ }( $f : |S|$ ){ $a1 a2 : \|S\| f \rightarrow \mathbf{Term}\{\mathfrak{X}\}\{X\}$ }
 $\rightarrow$   $a1 \equiv a2 \rightarrow \mathbf{node} f a1 \equiv \mathbf{node} f a2$ 
term-op-interp2  $f a1 \equiv a2 = \mathbf{ap} (\mathbf{node} f) a1 \equiv a2$ 

```

```

term-op-interp3 : { $\mathfrak{X} : \mathbf{Universe}$ }{ $X : \mathfrak{X} \cdot$ }( $f : |S|$ ){ $a1 a2 : \|S\| f \rightarrow \mathbf{Term}$ }
 $\rightarrow$   $a1 \equiv a2 \rightarrow \mathbf{node} f a1 \equiv (f \hat{\ } \mathbf{T} X) a2$ 
term-op-interp3  $f \{a1\}\{a2\} a1 a2 = (\mathbf{term-op-interp2} f a1 a2) \cdot (\mathbf{term-op-interp1} f a2)$ 

```

```

term-gen : { $\mathfrak{X} : \mathbf{Universe}$ }{ $X : \mathfrak{X} \cdot$ }( $p : | \mathbf{T} X |$ )  $\rightarrow$   $\Sigma \mathbf{p} : | \mathbf{T} X |, p \equiv (\mathbf{p} \cdot \mathbf{T} X) \mathbf{generator}$ 
term-gen (generator  $x$ ) = (generator  $x$ ) , refl
term-gen (node  $f$   $args$ ) =  $\mathbf{node} f (\lambda i \rightarrow | \mathbf{term-gen} (args i) |)$  ,
 $\mathbf{term-op-interp3} f (gfe \lambda i \rightarrow \| \mathbf{term-gen} (args i) \|)$ 

```

```

tg : { $\mathfrak{X} : \mathbf{Universe}$ }{ $X : \mathfrak{X} \cdot$ }( $p : | \mathbf{T} X |$ )  $\rightarrow$   $\Sigma \mathbf{p} : | \mathbf{T} X |, p \equiv (\mathbf{p} \cdot \mathbf{T} X) \mathbf{generator}$ 
tg  $p = \mathbf{term-gen} p$ 

```

```

term-equality : { $\mathfrak{X}$  : Universe}{ $X$  :  $\mathfrak{X}$  ·}( $p$   $q$  : |  $\mathbf{T}$   $X$  |)
  →  $p \equiv q \rightarrow (\forall t \rightarrow (p \cdot \mathbf{T} X) t \equiv (q \cdot \mathbf{T} X) t)$ 
term-equality  $p$   $q$  (refl _) _ = refl _

term-equality' : { $\mathfrak{U}$   $\mathfrak{X}$  : Universe}{ $X$  :  $\mathfrak{X}$  ·}{ $\mathbf{A}$  : Algebra  $\mathfrak{U}$   $S$ }( $p$   $q$  : |  $\mathbf{T}$   $X$  |)
  →  $p \equiv q \rightarrow (\forall \mathbf{a} \rightarrow (p \cdot \mathbf{A}) \mathbf{a} \equiv (q \cdot \mathbf{A}) \mathbf{a})$ 
term-equality'  $p$   $q$  (refl _) _ = refl _

term-gen-agreement : { $\mathfrak{X}$  : Universe}{ $X$  :  $\mathfrak{X}$  ·}( $p$  : |  $\mathbf{T}$   $X$  |)
  →  $(p \cdot \mathbf{T} X)$  generator  $\equiv$  (| term-gen  $p$  | ·  $\mathbf{T} X$ ) generator
term-gen-agreement (generator  $x$ ) = refl
term-gen-agreement { $\mathfrak{X}$ }{ $X$ }(node  $f$   $args$ ) = ap ( $f \hat{\ } \mathbf{T} X$ ) ( $gfe \lambda x \rightarrow$  term-gen-agreement ( $args$   $x$ ))

term-agreement : { $\mathfrak{X}$  : Universe}{ $X$  :  $\mathfrak{X}$  ·}( $p$  : |  $\mathbf{T}$   $X$  |)
  →  $p \equiv (p \cdot \mathbf{T} X)$  generator
term-agreement  $p$  = snd (term-gen  $p$ ) · (term-gen-agreement  $p$ )⊥

```

5.3.1 Interpretation of terms in product algebras

```

interp-prod : { $\mathfrak{X}$   $\mathfrak{U}$  : Universe} → funext  $\mathcal{V}$   $\mathfrak{U}$ 
  → { $X$  :  $\mathfrak{X}$  ·}( $p$  : Term){ $I$  :  $\mathfrak{U}$  ·}
  (  $\mathcal{A}$  :  $I \rightarrow$  Algebra  $\mathfrak{U}$   $S$ )( $x$  :  $X \rightarrow \forall i \rightarrow | \mathcal{A} i |$ )
  -----
  →  $(p \cdot (\prod \mathcal{A})) x \equiv (\lambda i \rightarrow (p \cdot \mathcal{A} i) (\lambda j \rightarrow x j i))$ 

interp-prod _ (generator  $x_1$ )  $\mathcal{A} x$  = refl

interp-prod  $fe$  (node  $f$   $t$ )  $\mathcal{A} x$  =
  let  $IH = \lambda x_1 \rightarrow$  interp-prod  $fe$  ( $t x_1$ )  $\mathcal{A} x$  in
  ( $f \hat{\ } \prod \mathcal{A})(\lambda x_1 \rightarrow (t x_1 \cdot \prod \mathcal{A}) x) \equiv \langle$  ap ( $f \hat{\ } \prod \mathcal{A})(fe IH)$   $\rangle$ 
  ( $f \hat{\ } \prod \mathcal{A})(\lambda x_1 \rightarrow (\lambda i_1 \rightarrow (t x_1 \cdot \mathcal{A} i_1)(\lambda j_1 \rightarrow x j_1 i_1))) \equiv \langle$  refl  $\rangle$ 
  ( $\lambda i_1 \rightarrow (f \hat{\ } \mathcal{A} i_1) (\lambda x_1 \rightarrow (t x_1 \cdot \mathcal{A} i_1) (\lambda j_1 \rightarrow x j_1 i_1)))$  ■

interp-prod2 : { $\mathfrak{U}$   $\mathfrak{X}$  : Universe} → global-dfunext
  → { $X$  :  $\mathfrak{X}$  ·}( $p$  : Term){ $I$  :  $\mathfrak{U}$  ·}( $\mathcal{A}$  :  $I \rightarrow$  Algebra  $\mathfrak{U}$   $S$ )
  -----
  →  $(p \cdot \prod \mathcal{A}) \equiv \lambda(args : X \rightarrow | \prod \mathcal{A} |) \rightarrow (\lambda i \rightarrow (p \cdot \mathcal{A} i)(\lambda x \rightarrow args x i))$ 

interp-prod2 _ (generator  $x_1$ )  $\mathcal{A}$  = refl

interp-prod2  $gfe$  { $X$ } (node  $f$   $t$ )  $\mathcal{A} = gfe \lambda (tup : X \rightarrow | \prod \mathcal{A} |) \rightarrow$ 
  let  $IH = \lambda x \rightarrow$  interp-prod  $gfe$  ( $t x$ )  $\mathcal{A}$  in
  let  $tA = \lambda z \rightarrow t z \cdot \prod \mathcal{A}$  in
  ( $f \hat{\ } \prod \mathcal{A})(\lambda s \rightarrow tA s tup) \equiv \langle$  ap ( $f \hat{\ } \prod \mathcal{A})(gfe \lambda x \rightarrow IH x tup)$   $\rangle$ 
  ( $f \hat{\ } \prod \mathcal{A})(\lambda s \rightarrow \lambda j \rightarrow (t s \cdot \mathcal{A} j)(\lambda \ell \rightarrow tup \ell j)) \equiv \langle$  refl  $\rangle$ 
  ( $\lambda i \rightarrow (f \hat{\ } \mathcal{A} i)(\lambda s \rightarrow (t s \cdot \mathcal{A} i)(\lambda \ell \rightarrow tup \ell i)))$  ■

```

5.4 Compatibility of Terms

This subsection describes the `UALib.Terms.Compatibility` submodule of the Agda UALib. Here we prove that every term commutes with every homomorphism and is compatible with every

congruence.

```

open import UALib.Algebras using (Signature; 0; V; Algebra; _→_)
open import UALib.Prelude.Preliminaries using (global-dfunext; Universe; _)

module UALib.Terms.Compatibility
  {S : Signature 0 V}{gfe : global-dfunext}
  {X : {U X : Universe}{X : X ·}(A : Algebra U S) → X → A}
  where

  open import UALib.Terms.Operations{S = S}{gfe}{X} public

```

5.4.1 Homomorphism compatibility

We first prove an extensional version of this fact.

```

comm-hom-term : {U W X : Universe} → funext V W
→ {X : X ·}(A : Algebra U S) (B : Algebra W S)
  (h : hom A B) (t : Term) (a : X → | A |)
→ | h | ((t · A) a) ≡ (t · B) (| h | ∘ a)

```

`comm-hom-term _ A B h (generator x) a = refl`

```

comm-hom-term fe A B h (node f args) a =
  | h | ((f ^ A) λ i₁ → (args i₁ · A) a) ≡ (| h | f (λ r → (args r · A) a))
  (f ^ B)(λ i₁ → | h | ((args i₁ · A) a)) ≡ (ap (λ r → (f ^ B)(λ i₁ → comm-hom-term fe A B h (args i₁) a)))
  (f ^ B)(λ r → (args r · B)(| h | ∘ a)) ■

```

Here is an intensional version.

```

comm-hom-term-intensional : global-dfunext → {U W X : Universe}{X : X ·}
→ (A : Algebra U S) (B : Algebra W S)(h : hom A B) (t : Term)
→ | h | ∘ (t · A) ≡ (t · B) ∘ (λ a → | h | ∘ a)

```

`comm-hom-term-intensional gfe A B h (generator x) = refl`

`comm-hom-term-intensional gfe {X = X} A B h (node f args) = γ`

where

```

γ : | h | ∘ (λ a → (f ^ A) (λ i → (args i · A) a))
  ≡ (λ a → (f ^ B)(λ i → (args i · B) a)) ∘ _o_ | h |
γ = (λ a → | h | ((f ^ A)(λ i → (args i · A) a))) ≡ (gfe (λ a → | h | f (λ r → (args r · A) a)))
  (λ a → (f ^ B)(λ i → | h | ((args i · A) a))) ≡ (ap (λ - → (λ a → (f ^ B)(- a))) ih)
  (λ a → (f ^ B)(λ i → (args i · B) a)) ∘ _o_ | h | ■

```

where

`IH : (a : X → | A |)(i : || S || f) → (| h | ∘ (args i · A)) a ≡ ((args i · B) ∘ _o_ | h |) a`

`IH a i = intensionality (comm-hom-term-intensional gfe A B h (args i)) a`

`ih : (λ a → (λ i → | h | ((args i · A) a))) ≡ (λ a → (λ i → ((args i · B) ∘ _o_ | h |) a))`

`ih = gfe λ a → gfe λ i → IH a i`

5.4.2 Congruence compatibility

If $t : \text{Term}$, $\theta : \text{Con } \mathbf{A}$, then $a \theta b \rightarrow t(a) \theta t(b)$. The statement and proof of this obvious but important fact may be formalized in Agda as follows.

```
compatible-term : { $\mathcal{U} : \text{Universe}$ } { $X : \mathcal{U} \cdot$ }
  ( $\mathbf{A} : \text{Algebra } \mathcal{U} S$ ) ( $t : \text{Term} \{ \mathcal{U} \} \{ X \}$ ) ( $\theta : \text{Con } \mathbf{A}$ )
  -----
  → compatible-fun (t ·  $\mathbf{A}$ ) |  $\theta$  |
```

```
compatible-term  $\mathbf{A}$  (generator x)  $\theta$  p = p x
```

```
compatible-term  $\mathbf{A}$  (node f args)  $\theta$  p = snd ||  $\theta$  || f  $\lambda$  x → (compatible-term  $\mathbf{A}$  (args x)  $\theta$ ) p
```

```
compatible-term' : { $\mathcal{U} : \text{Universe}$ } { $X : \mathcal{U} \cdot$ }
  ( $\mathbf{A} : \text{Algebra } \mathcal{U} S$ ) ( $t : \text{Term} \{ \mathcal{U} \} \{ X \}$ ) ( $\theta : \text{Con } \mathbf{A}$ )
  -----
  → compatible-fun (t ·  $\mathbf{A}$ ) |  $\theta$  |
```

```
compatible-term'  $\mathbf{A}$  (generator x)  $\theta$  p = p x
```

```
compatible-term'  $\mathbf{A}$  (node f args)  $\theta$  p = snd ||  $\theta$  || f  $\lambda$  x → (compatible-term'  $\mathbf{A}$  (args x)  $\theta$ ) p
```

(This page is almost entirely blank on purpose.)

6 Subalgebras

This section presents the `UALib.Subalgebras` module of the Agda `UALib`.

6.1 Types for Subuniverses

This subsection describes the `UALib.Subalgebras.Subuniverses` submodule of the Agda `UALib`. We show how to represent in Agda *subuniverses* of a given algebra or collection of algebras. As usual, we start with the required imports.

```
open import UALib.Algebras using (Signature;  $\mathfrak{G}$ ;  $\mathcal{V}$ ; Algebra;  $\_ \rightarrow \_$ )
open import UALib.Prelude.Preliminaries using (global-dfunext; Universe;  $\_ \cdot$ )

module UALib.Subalgebras.Subuniverses
  {S : Signature  $\mathfrak{G}$   $\mathcal{V}$ } {gfe : global-dfunext}
  { $\mathcal{X}$  : { $\mathcal{U}$   $\mathfrak{X}$  : Universe} {X :  $\mathfrak{X}$   $\cdot$ } (A : Algebra  $\mathcal{U}$  S)  $\rightarrow$  X  $\rightarrow$  A}
  where

  open import UALib.Terms.Compatibility {S = S} {gfe} { $\mathcal{X}$ } public

  Subuniverses : { $\mathfrak{Q}$   $\mathcal{U}$  : Universe} (A : Algebra  $\mathfrak{Q}$  S)  $\rightarrow$  Pred (Pred | A |  $\mathcal{U}$ ) ( $\mathfrak{G} \sqcup \mathcal{V} \sqcup \mathfrak{Q} \sqcup \mathcal{U}$ )
  Subuniverses A B = (f : | S |) (a : || S || f  $\rightarrow$  | A |)  $\rightarrow$  Im a  $\subseteq$  B  $\rightarrow$  (f  $\hat{}$  A) a  $\in$  B

  SubunivAlg : { $\mathfrak{Q}$   $\mathcal{U}$  : Universe} (A : Algebra  $\mathfrak{Q}$  S) (B : Pred | A |  $\mathcal{U}$ )
     $\rightarrow$  B  $\in$  Subuniverses A
     $\rightarrow$  Algebra ( $\mathfrak{Q} \sqcup \mathcal{U}$ ) S
  SubunivAlg A B B  $\in$  SubA =  $\Sigma$  B ,  $\lambda$  f x  $\rightarrow$  (f  $\hat{}$  A) (|_|  $\circ$  x) ,
    B  $\in$  SubA f (|_|  $\circ$  x) (||_|  $\circ$  x)

  record Subuniverse { $\mathfrak{Q}$   $\mathcal{U}$  : Universe} {A : Algebra  $\mathfrak{Q}$  S} :  $\mathfrak{G} \sqcup \mathcal{V} \sqcup (\mathfrak{Q} \sqcup \mathcal{U})$   $^+ \cdot$  where
    constructor mksub
    field
      sset : Pred | A |  $\mathcal{U}$ 
      isSub : sset  $\in$  Subuniverses A
```

6.2 Subuniverse Generation

This subsection describes the `UALib.Subalgebras.Generation` submodule of the Agda `UALib`. Here we define the inductive type of the subuniverse generated by a given collection of elements from the domain of an algebra, and prove that what we have defined is indeed the smallest subuniverse containing the given elements.

```
open import UALib.Algebras using (Signature;  $\mathfrak{G}$ ;  $\mathcal{V}$ ; Algebra;  $\_ \rightarrow \_$ )
open import UALib.Prelude.Preliminaries using (global-dfunext; Universe;  $\_ \cdot$ )

module UALib.Subalgebras.Generation
  {S : Signature  $\mathfrak{G}$   $\mathcal{V}$ } {gfe : global-dfunext}
  { $\mathcal{X}$  : { $\mathcal{U}$   $\mathfrak{X}$  : Universe} {X :  $\mathfrak{X}$   $\cdot$ } (A : Algebra  $\mathcal{U}$  S)  $\rightarrow$  X  $\rightarrow$  A}
  where
```

```
open import UALib.Subalgebras.Subuniverses{S = S}{gfe}{X} public
```

We define an inductive type representing the subuniverse generated by a set in the obvious way.

```
data Sg {U W : Universe}(A : Algebra U S)(X : Pred | A | W) :
  Pred | A | (O U V U W U U) where
  var : ∀ {v} → v ∈ X → v ∈ Sg A X
  app : (f : | S |)(a : || S || f → | A |) → Im a ⊆ Sg A X → (f ^ A) a ∈ Sg A X
```

For any subset X of the domain $| \mathbf{A} |$ of an algebra \mathbf{A} , $\text{Sg } X$ is a subuniverse.

```
sgIsSub : {U W : Universe}{A : Algebra U S}{X : Pred | A | W} → Sg A X ∈ Subuniverses A
sgIsSub = app
```

By induction on the shape of elements of $\text{Sg } X$, we prove that $\text{Sg } X$ is the smallest subuniverse of \mathbf{A} containing X .

```
sgIsSmallest : {U W R : Universe}(A : Algebra U S)(X : Pred | A | W)(Y : Pred | A | R)
  → Y ∈ Subuniverses A → X ⊆ Y → Sg A X ⊆ Y
```

```
sgIsSmallest _ _ _ XinY (var Xv) = XinY Xv
sgIsSmallest A Y YsubA XinY (app f a SgXa) = fa ∈ Y
```

where

```
IH : Im a ⊆ Y
IH i = sgIsSmallest A Y YsubA XinY (SgXa i)
```

```
fa ∈ Y : (f ^ A) a ∈ Y
fa ∈ Y = YsubA f a IH
```

When the element of $\text{Sg } X$ is constructed as $\text{app } f \mathbf{a} \text{ Sg } X \mathbf{a}$, we may assume (the induction hypothesis) that the arguments \mathbf{a} belong to Y . Then the result of applying f to \mathbf{a} must also belong to Y , since Y is a subuniverse.

6.3 Subuniverse Lemmas

This subsection describes the `UALib.Subalgebras.Properties` submodule of the Agda `UALib`. Here we formalize and prove a few basic properties of subuniverses.

```
open import UALib.Algebras using (Signature; O; V; Algebra; _→_)
open import UALib.Prelude.Preliminaries using (global-dfunext; Universe; _)

module UALib.Subalgebras.Properties
  {S : Signature O V}{gfe : global-dfunext}
  {X : {U X : Universe}{X : X ·}(A : Algebra U S) → X → A}
  where
    open import UALib.Subalgebras.Generation{S = S}{gfe}{X} renaming (generator to g) public
    open import Relation.Unary using (∩) public

  sub-inter-is-sub : {Q U : Universe}(A : Algebra Q S)
    (I : U ·)(A : I → Pred | A | U)
    → ((i : I) → A i ∈ Subuniverses A)
```


$\rightarrow \bigcap I \mathcal{A} \in \text{Subuniverses } \mathbf{A}$

`sub-inter-is-sub` $\mathbf{A} I \mathcal{A} \text{ Ai-is-Sub } f a \text{ ima} \subseteq \bigcap A = \alpha$

where

$\alpha : (f \hat{=} \mathbf{A}) a \in \bigcap I \mathcal{A}$

$\alpha \ i = \text{Ai-is-Sub } i f a \ \lambda j \rightarrow \text{ima} \subseteq \bigcap A \ j \ i$

6.3.1 Conservativity of term operations

`sub-term-closed` $\{ \mathcal{X} \ \mathcal{Q} \ \mathcal{U} : \text{Universe} \} \{ X : \mathcal{X} \cdot \} (\mathbf{A} : \text{Algebra } \mathcal{Q} \ S) (B : \text{Pred } | \mathbf{A} | \mathcal{U}) :$

$\rightarrow B \in \text{Subuniverses } \mathbf{A}$

$\rightarrow (t : \text{Term}) (b : X \rightarrow | \mathbf{A} |)$

$\rightarrow (\forall x \rightarrow b \ x \in B)$

$\rightarrow ((t \cdot \mathbf{A}) \ b) \in B$

`sub-term-closed` $_ _ B \leq A \ (g \ x) \ b \ b \in B = b \in B \ x$

`sub-term-closed` $\mathbf{A} \ B \ B \leq A \ (\text{node } f \ t) \ b \ b \in B =$

$B \leq A \ f \ (\lambda z \rightarrow (t \ z \cdot \mathbf{A}) \ b)$

$(\lambda x \rightarrow \text{sub-term-closed } \mathbf{A} \ B \ B \leq A \ (t \ x) \ b \ b \in B)$

6.3.2 Term images

`data TermImage` $\{ \mathcal{Q} \ \mathcal{U} : \text{Universe} \} (\mathbf{A} : \text{Algebra } \mathcal{Q} \ S) (Y : \text{Pred } | \mathbf{A} | \mathcal{U}) :$

$\text{Pred } | \mathbf{A} | \ (\mathcal{Q} \sqcup \mathcal{V} \sqcup \mathcal{Q} \sqcup \mathcal{U})$ where

`var` $: \forall \{ y : | \mathbf{A} | \} \rightarrow y \in Y \rightarrow y \in \text{TermImage } \mathbf{A} \ Y$

`app` $: (f : | S |) (t : \| S \| f \rightarrow | \mathbf{A} |)$

$\rightarrow (\forall i \rightarrow t \ i \in \text{TermImage } \mathbf{A} \ Y)$

$\rightarrow (f \hat{=} \mathbf{A}) \ t \in \text{TermImage } \mathbf{A} \ Y$

-1. *TermImage* is a subuniverse

`TermImagesSub` $: \{ \mathcal{Q} \ \mathcal{U} : \text{Universe} \}$

$\{ \mathbf{A} : \text{Algebra } \mathcal{Q} \ S \} \{ Y : \text{Pred } | \mathbf{A} | \mathcal{U} \}$

$\rightarrow \text{TermImage } \mathbf{A} \ Y \in \text{Subuniverses } \mathbf{A}$

`TermImagesSub` $= \text{app} - \lambda f \ a \ x \rightarrow \text{app } f \ a \ x$

-2. $Y \subseteq \text{TermImage } Y$

`Y ⊆ TermImage Y` $: \{ \mathcal{Q} \ \mathcal{U} : \text{Universe} \}$

$\{ \mathbf{A} : \text{Algebra } \mathcal{Q} \ S \} \{ Y : \text{Pred } | \mathbf{A} | \mathcal{U} \}$

$\rightarrow Y \subseteq \text{TermImage } \mathbf{A} \ Y$

`Y ⊆ TermImage Y` $\{ a \} \ a \in Y = \text{var } a \in Y$

- 3. $\text{Sg} \hat{=} A(Y)$ is the smallest subuniverse containing Y

- Proof: see ‘*sgIsSmallest*’

`Sg Y ⊆ TermImage Y` $: \{ \mathcal{Q} \ \mathcal{U} : \text{Universe} \}$

$$\frac{(\mathbf{A} : \text{Algebra } \mathcal{Q} \ S) (Y : \text{Pred} \mid \mathbf{A} \mid \mathcal{U})}{\text{Sg } \mathbf{A} \ Y \subseteq \text{TermlImage } \mathbf{A} \ Y}$$

$$\text{Sg } Y \subseteq \text{TermlImage } Y \ \mathbf{A} \ Y = \text{sglsSmallest } \mathbf{A} \ (\text{TermlImage } \mathbf{A} \ Y) \ \text{TermlImageSub } Y \subseteq \text{TermlImage } Y$$

6.4 Homomorphisms and Subuniverses

This subsection describes the `UALib.Subalgebras.Homomorphisms` submodule of the Agda `UALib`. Here we mechanize the interaction between homomorphisms and subuniverses—two central cogs of the universal algebra machine.

```
open import UALib.Algebras using (Signature;  $\mathcal{Q}$ ;  $\mathcal{V}$ ; Algebra;  $\_ \rightarrow \_$ )
open import UALib.Prelude.Preliminaries using (global-dfunext; Universe;  $\_ \cdot$ )

module UALib.Subalgebras.Homomorphisms
  {S : Signature  $\mathcal{Q}$   $\mathcal{V}$ } {gfe : global-dfunext}
  { $\mathcal{X}$  : { $\mathcal{U}$   $\mathcal{X}$  : Universe} {X :  $\mathcal{X}$   $\cdot$ } (A : Algebra  $\mathcal{U}$  S)  $\rightarrow$  X  $\rightarrow$  A}
  where

  open import UALib.Subalgebras.Properties {S = S} {gfe} { $\mathcal{X}$ } public
```

6.4.1 Homomorphic images are subuniverses

The image of a homomorphism is a subuniverse of its codomain.

```
hom-image-is-sub : { $\mathcal{U}$   $\mathcal{W}$  : Universe}  $\rightarrow$  global-dfunext
 $\rightarrow$  {A : Algebra  $\mathcal{U}$  S} {B : Algebra  $\mathcal{W}$  S} ( $\phi$  : hom A B)
  -----
 $\rightarrow$  (HomImage B  $\phi$ )  $\in$  Subuniverses B

hom-image-is-sub gfe {A} {B}  $\phi$  f b b $\in$ Imf = eq ((f  $\hat{\ } B$ ) b) ((f  $\hat{\ } A$ ) ar)  $\gamma$ 
where
  ar : || S || f  $\rightarrow$  | A |
  ar =  $\lambda$  x  $\rightarrow$  Inv |  $\phi$  |(b x)(b $\in$ Imf x)

   $\zeta$  : |  $\phi$  |  $\circ$  ar  $\equiv$  b
   $\zeta$  = gfe ( $\lambda$  x  $\rightarrow$  InvlInvl |  $\phi$  |(b x)(b $\in$ Imf x))

   $\gamma$  : (f  $\hat{\ } B$ ) b  $\equiv$  |  $\phi$  | ((f  $\hat{\ } A$ ) ( $\lambda$  x  $\rightarrow$  Inv |  $\phi$  |(b x)(b $\in$ Imf x)))

   $\gamma$  = (f  $\hat{\ } B$ ) b  $\equiv$  ( ap (f  $\hat{\ } B$ ) ( $\zeta$   $^{-1}$ ) )
      (f  $\hat{\ } B$ ) (|  $\phi$  |  $\circ$  ar)  $\equiv$  ( (||  $\phi$  || f ar)  $^{-1}$  )
      |  $\phi$  | ((f  $\hat{\ } A$ ) ar) ■
```

6.4.2 Uniqueness property for homomorphisms

Here we formalize the proof that homomorphisms are uniquely determined by their values on a generating set.

```
HomUnique : { $\mathcal{U}$   $\mathcal{W}$  : Universe}  $\rightarrow$  funext  $\mathcal{V}$   $\mathcal{U}$   $\rightarrow$  {A B : Algebra  $\mathcal{U}$  S}
  (X : Pred | A |  $\mathcal{U}$ ) (g h : hom A B)
```


6.5.3 Subalgebras of a class

$_IsSubalgebraOfClass_ : \{\mathcal{U} \ \mathcal{Q} \ \mathcal{W} : \text{Universe}\}(\mathbf{B} : \text{Algebra } \mathcal{U} \ S) \rightarrow \text{Pred } (\text{Algebra } \mathcal{Q} \ S) \ \mathcal{W} \rightarrow _ \cdot$
 $_IsSubalgebraOfClass_ \{\mathcal{U}\} \ \mathbf{B} \ \mathcal{K} = \Sigma \ \mathbf{A} : (\text{Algebra } _ \ S) , \Sigma \ SA : (\text{Subalgebra}\{\mathcal{U}\} \ \mathbf{A}) ,$
 $(\mathbf{A} \in \mathcal{K}) \times (\mathbf{B} \cong | SA |)$

$\text{SUBALGEBRAOFCCLASS} : \{\mathcal{U} \ \mathcal{Q} \ \mathcal{W} : \text{Universe}\} \rightarrow \text{Pred } (\text{Algebra } \mathcal{Q} \ S) \ \mathcal{W} \rightarrow _ \cdot$
 $\text{SUBALGEBRAOFCCLASS} \{\mathcal{U}\} \ \mathcal{K} = \Sigma \ \mathbf{B} : (\text{Algebra } \mathcal{U} \ S) , \mathbf{B} \ \text{IsSubalgebraOfClass} \ \mathcal{K}$

$\text{SubalgebraOfClass} : \{\mathcal{U} \ \mathcal{Q} : \text{Universe}\} \rightarrow \text{Pred } (\text{Algebra } \mathcal{Q} \ S)(\mathcal{O} \sqcup \mathcal{V} \sqcup \mathcal{Q}^+) \rightarrow \mathcal{O} \sqcup \mathcal{V} \sqcup (\mathcal{Q} \sqcup \mathcal{U})^+ \cdot$
 $\text{SubalgebraOfClass} \{\mathcal{U}\}\{\mathcal{Q}\} = \text{SUBALGEBRAOFCCLASS} \{\mathcal{U}\}\{\mathcal{Q}\}\{\mathcal{O} \sqcup \mathcal{V} \sqcup \mathcal{Q}^+\}$

6.5.4 Subalgebra lemmas

Here are a number of useful facts about subalgebras. Many of them seem redundant, and they are to some extent. However, each one differs slightly from the next, if only with respect to the explicitness or implicitness of their arguments. The aim is to make it as convenient as possible to apply the lemmas in different situations. (We're in the UALib utility closet now, and elegance is not the priority.)

-Transitivity of IsSubalgebra (explicit args)

$\text{TRANS-}\leq : \{\mathcal{X} \ \mathcal{Y} \ \mathcal{Z} : \text{Universe}\}(\mathbf{A} : \text{Algebra } \mathcal{X} \ S)(\mathbf{B} : \text{Algebra } \mathcal{Y} \ S)(\mathbf{C} : \text{Algebra } \mathcal{Z} \ S)$
 $\rightarrow \mathbf{B} \leq \mathbf{A} \rightarrow \mathbf{C} \leq \mathbf{B}$

 $\rightarrow \mathbf{C} \leq \mathbf{A}$

$\text{TRANS-}\leq \ \mathbf{A} \ \mathbf{B} \ \mathbf{C} \ \mathbf{BA} \ \mathbf{CB} = | \ \mathbf{BA} \ | \circ \ | \ \mathbf{CB} \ | , \ \alpha , \ \beta$

where

$\alpha : \text{is-embedding } (| \ \mathbf{BA} \ | \circ \ | \ \mathbf{CB} \ |)$
 $\alpha = \text{o-embedding } (\text{fst } \| \ \mathbf{BA} \ \|) (\text{fst } \| \ \mathbf{CB} \ \|)$
 $\beta : \text{is-homomorphism } \ \mathbf{C} \ \mathbf{A} \ (| \ \mathbf{BA} \ | \circ \ | \ \mathbf{CB} \ |)$
 $\beta = \text{o-hom } \ \mathbf{C} \ \mathbf{B} \ \mathbf{A} \ \{| \ \mathbf{CB} \ |\}\{| \ \mathbf{BA} \ |\}(\text{snd } \| \ \mathbf{CB} \ \|) (\text{snd } \| \ \mathbf{BA} \ \|)$

-Transitivity of IsSubalgebra (implicit args)

$\text{Trans-}\leq : \{\mathcal{X} \ \mathcal{Y} \ \mathcal{Z} : \text{Universe}\}(\mathbf{A} : \text{Algebra } \mathcal{X} \ S)(\mathbf{B} : \text{Algebra } \mathcal{Y} \ S)(\mathbf{C} : \text{Algebra } \mathcal{Z} \ S)$
 $\rightarrow \mathbf{B} \leq \mathbf{A} \rightarrow \mathbf{C} \leq \mathbf{B} \rightarrow \mathbf{C} \leq \mathbf{A}$

$\text{Trans-}\leq \ \mathbf{A} \ \{\mathbf{B}\} \ \mathbf{C} = \text{TRANS-}\leq \ \mathbf{A} \ \mathbf{B} \ \mathbf{C}$

-Transitivity of IsSubalgebra (implicit args)

$\text{trans-}\leq : \{\mathcal{X} \ \mathcal{Y} \ \mathcal{Z} : \text{Universe}\}(\mathbf{A} : \text{Algebra } \mathcal{X} \ S)(\mathbf{B} : \text{Algebra } \mathcal{Y} \ S)(\mathbf{C} : \text{Algebra } \mathcal{Z} \ S)$
 $\rightarrow \mathbf{B} \leq \mathbf{A} \rightarrow \mathbf{C} \leq \mathbf{B} \rightarrow \mathbf{C} \leq \mathbf{A}$

$\text{trans-}\leq \ \{\mathbf{A} = \mathbf{A}\}\{\mathbf{B} = \mathbf{B}\}\{\mathbf{C} = \mathbf{C}\} = \text{TRANS-}\leq \ \mathbf{A} \ \mathbf{B} \ \mathbf{C}$

$\text{transitivity-}\leq : \{\mathcal{X} \ \mathcal{Y} \ \mathcal{Z} : \text{Universe}\}(\mathbf{A} : \text{Algebra } \mathcal{X} \ S)(\mathbf{B} : \text{Algebra } \mathcal{Y} \ S)(\mathbf{C} : \text{Algebra } \mathcal{Z} \ S)$
 $\rightarrow \mathbf{A} \leq \mathbf{B} \rightarrow \mathbf{B} \leq \mathbf{C} \rightarrow \mathbf{A} \leq \mathbf{C}$

$\text{transitivity-}\leq \ \mathbf{A} \ \{\mathbf{B}\}\{\mathbf{C}\} \ \mathbf{A} \leq \mathbf{B} \ \mathbf{B} \leq \mathbf{C} = | \ \mathbf{B} \leq \mathbf{C} \ | \circ \ | \ \mathbf{A} \leq \mathbf{B} \ | ,$

$\text{o-embedding } (\text{fst } \| \ \mathbf{B} \leq \mathbf{C} \ \|)(\text{fst } \| \ \mathbf{A} \leq \mathbf{B} \ \|) , \text{o-hom } \ \mathbf{A} \ \mathbf{B} \ \mathbf{C} \ \{| \ \mathbf{A} \leq \mathbf{B} \ |\}\{| \ \mathbf{B} \leq \mathbf{C} \ |\}(\text{snd } \| \ \mathbf{A} \leq \mathbf{B} \ \|)(\text{snd } \| \ \mathbf{B} \leq \mathbf{C} \ \|)$

–Reflexivity of IsSubalgebra (explicit arg)

REFL-≤ : { \mathcal{U} : Universe}(A : Algebra \mathcal{U} S) → A ≤ A
 REFL-≤ A = id | A | , id-is-embedding , id-is-hom

–Reflexivity of IsSubalgebra (implicit arg)

refl-≤ : { \mathcal{U} : Universe}{A : Algebra \mathcal{U} S} → A ≤ A
 refl-≤ {A = A} = REFL-≤ A

–Reflexivity of IsSubalgebra (explicit arg)

ISO-≤ : { \mathcal{X} \mathcal{Y} \mathcal{Z} : Universe}(A : Algebra \mathcal{X} S)(B : Algebra \mathcal{Y} S)(C : Algebra \mathcal{Z} S)
 → B ≤ A → C ≅ B

 → C ≤ A

ISO-≤ A B C B≤A C≅B = h , hemb , hhom

where

f : | C | → | B |
 f = fst | C≅B |
 g : | B | → | A |
 g = | B≤A |
 h : | C | → | A |
 h = g ∘ f

hemb : is-embedding h

hemb = o-embedding (fst || B≤A ||) (iso→embedding C≅B)

hhom : is-homomorphism C A h

hhom = o-hom C B A {f}{g} (snd | C≅B |) (snd || B≤A ||)

Iso-≤ : { \mathcal{X} \mathcal{Y} \mathcal{Z} : Universe}(A : Algebra \mathcal{X} S)(B : Algebra \mathcal{Y} S)(C : Algebra \mathcal{Z} S)
 → B ≤ A → C ≅ B → C ≤ A

Iso-≤ A {B} C = ISO-≤ A B C

iso-≤ : { \mathcal{X} \mathcal{Y} \mathcal{Z} : Universe}{A : Algebra \mathcal{X} S}{B : Algebra \mathcal{Y} S}{C : Algebra \mathcal{Z} S}
 → B ≤ A → C ≅ B → C ≤ A

iso-≤ {A = A} {B = B} C = ISO-≤ A B C

trans-≤≅ : { \mathcal{X} \mathcal{Y} \mathcal{Z} : Universe}(A : Algebra \mathcal{X} S)(B : Algebra \mathcal{Y} S)(C : Algebra \mathcal{Z} S)
 → A ≤ B → A ≅ C → C ≤ B

trans-≤≅ { \mathcal{X} }{ \mathcal{Y} }{ \mathcal{Z} } A {B} C A≤B B≅C = ISO-≤ B A C A≤B (sym-≅ B≅C)

TRANS-≤≅ : { \mathcal{X} \mathcal{Y} \mathcal{Z} : Universe}(A : Algebra \mathcal{X} S)(B : Algebra \mathcal{Y} S)(C : Algebra \mathcal{Z} S)
 → A ≤ B → B ≅ C → A ≤ C

TRANS- \leq - \cong $\{\mathcal{X}\}\{\mathcal{Y}\}\{\mathcal{Z}\} \mathbf{A} \{\mathbf{B}\} \mathbf{C} \ A \leq B \ B \cong C = \mathbf{h}$, **hemb** , **hhom**

where

$\mathbf{f} : | \mathbf{A} | \rightarrow | \mathbf{B} |$
 $\mathbf{f} = | A \leq B |$
 $\mathbf{g} : | \mathbf{B} | \rightarrow | \mathbf{C} |$
 $\mathbf{g} = \mathbf{fst} \ | B \cong C |$
 $\mathbf{h} : | \mathbf{A} | \rightarrow | \mathbf{C} |$
 $\mathbf{h} = \mathbf{g} \circ \mathbf{f}$

hemb : is-embedding \mathbf{h}
hemb = \circ -embedding (iso \rightarrow embedding $B \cong C$)($\mathbf{fst} \ || A \leq B \ ||$)

hhom : is-homomorphism $\mathbf{A} \ \mathbf{C} \ \mathbf{h}$
hhom = \circ -hom $\mathbf{A} \ \mathbf{B} \ \mathbf{C} \ \{\mathbf{f}\}\{\mathbf{g}\} \ (\mathbf{snd} \ || A \leq B \ ||) \ (\mathbf{snd} \ | B \cong C \ |)$

mono- \leq : $\{\mathcal{U} \ \mathcal{Q} \ \mathcal{W} : \text{Universe}\}\{\mathbf{B} : \text{Algebra } \mathcal{U} \ S\}\{\mathcal{K} \ \mathcal{K}' : \text{Pred} (\text{Algebra } \mathcal{Q} \ S) \ \mathcal{W}\}$
 $\rightarrow \mathcal{K} \subseteq \mathcal{K}' \rightarrow \mathbf{B} \ \text{IsSubalgebraOfClass } \mathcal{K} \rightarrow \mathbf{B} \ \text{IsSubalgebraOfClass } \mathcal{K}'$

mono- \leq $\mathbf{B} \ \mathbf{K} \ \mathbf{K}' \ \mathbf{K} \ \mathbf{B} = | \mathbf{K} \ \mathbf{B} |$, $\mathbf{fst} \ || \mathbf{K} \ \mathbf{B} \ ||$, $\mathbf{K} \ \mathbf{K}' \ (| \mathbf{snd} \ || \mathbf{K} \ \mathbf{B} \ ||)$, $|| \ (\mathbf{snd} \ || \mathbf{K} \ \mathbf{B} \ ||) \ ||$

lift-alg-is-sub : $\{\mathcal{U} : \text{Universe}\}\{\mathcal{K} : \text{Pred} (\text{Algebra } \mathcal{U} \ S)(\mathbf{0} \sqcup \mathcal{V} \sqcup \mathcal{U}^+)\}\{\mathbf{B} : \text{Algebra } \mathcal{U} \ S\}$
 $\rightarrow \mathbf{B} \ \text{IsSubalgebraOfClass } \mathcal{K} \rightarrow (\text{lift-alg } \mathbf{B} \ \mathcal{U}) \ \text{IsSubalgebraOfClass } \mathcal{K}$

lift-alg-is-sub $\{\mathcal{U}\}\{\mathcal{K}\}\{\mathbf{B}\}(\mathbf{A} , (sa , (KA , B \cong sa))) =$
 $\mathbf{A} , sa , KA , \text{trans-}\cong _ _ _ (\text{sym-}\cong \ \text{lift-alg-}\cong) \ B \cong sa$

lift-alg-lift- \leq -lower : $\{\mathcal{X} \ \mathcal{Y} \ \mathcal{Z} : \text{Universe}\}(\mathbf{A} : \text{Algebra } \mathcal{X} \ S)\{\mathbf{B} : \text{Algebra } \mathcal{Y} \ S\}$
 $\rightarrow \mathbf{B} \leq \mathbf{A} \rightarrow (\text{lift-alg } \mathbf{B} \ \mathcal{Z}) \leq \mathbf{A}$

lift-alg-lift- \leq -lower $\{\mathcal{X}\}\{\mathcal{Y}\}\{\mathcal{Z}\} \mathbf{A} \{\mathbf{B}\} \ B \leq A =$
 $\text{iso-}\leq \{\mathcal{X}\}\{\mathcal{Y}\}\{\mathcal{Z}\} = (\mathcal{Y} \sqcup \mathcal{Z})\{\mathbf{A}\}\{\mathbf{B}\} \ (\text{lift-alg } \mathbf{B} \ \mathcal{Z}) \ B \leq A \ (\text{sym-}\cong \ \text{lift-alg-}\cong)$

lift-alg-lower- \leq -lift : $\{\mathcal{X} \ \mathcal{Y} \ \mathcal{Z} : \text{Universe}\}(\mathbf{A} : \text{Algebra } \mathcal{X} \ S)\{\mathbf{B} : \text{Algebra } \mathcal{Y} \ S\}$
 $\rightarrow \mathbf{B} \leq \mathbf{A} \rightarrow \mathbf{B} \leq (\text{lift-alg } \mathbf{A} \ \mathcal{Z})$

lift-alg-lower- \leq -lift $\{\mathcal{X}\}\{\mathcal{Y}\}\{\mathcal{Z}\} \mathbf{A} \{\mathbf{B}\} \ B \leq A = \mathbf{g} \circ \mathbf{f} , \alpha , \beta$

where

$\mathbf{IA} : \text{Algebra } (\mathcal{X} \sqcup \mathcal{Z}) \ S$
 $\mathbf{IA} = \text{lift-alg } \mathbf{A} \ \mathcal{Z}$
 $\mathbf{A} \cong \mathbf{IA} : \mathbf{A} \cong \mathbf{IA}$
 $\mathbf{A} \cong \mathbf{IA} = \text{lift-alg-}\cong$

$\mathbf{f} : | \mathbf{B} | \rightarrow | \mathbf{A} |$
 $\mathbf{f} = | B \leq A |$
 $\mathbf{g} : | \mathbf{A} | \rightarrow | \mathbf{IA} |$
 $\mathbf{g} = \cong\text{-map } \mathbf{A} \cong \mathbf{IA}$

$\alpha : \text{is-embedding } (\mathbf{g} \circ \mathbf{f})$

$\alpha = \text{o-embedding } (\cong\text{-map-is-embedding } A \cong IA) (\text{fst } \parallel B \leq A \parallel)$

$\beta : \text{is-homomorphism } B \text{ IA } (g \circ f)$

$\beta = \text{o-hom } B \text{ A IA } \{f\}\{g\} (\text{snd } \parallel B \leq A \parallel) (\text{snd } \mid A \cong IA \mid)$

$\text{lift-alg-sub-lift} : \{\mathcal{U} \ \mathcal{W} : \text{Universe}\}(\mathbf{A} : \text{Algebra } \mathcal{U} \ S)\{\mathbf{C} : \text{Algebra } (\mathcal{U} \sqcup \ \mathcal{W}) \ S\}$
 $\rightarrow \mathbf{C} \leq \mathbf{A} \rightarrow \mathbf{C} \leq (\text{lift-alg } \mathbf{A} \ \mathcal{W})$

$\text{lift-alg-sub-lift } \{\mathcal{U}\}\{\mathcal{W}\} \ \mathbf{A} \ \{\mathbf{C}\} \ C \leq A = g \circ f, \ \alpha, \ \beta$

where

$\text{IA} : \text{Algebra } (\mathcal{U} \sqcup \ \mathcal{W}) \ S$

$\text{IA} = \text{lift-alg } \mathbf{A} \ \mathcal{W}$

$A \cong IA : \mathbf{A} \cong \text{IA}$

$A \cong IA = \text{lift-alg-}\cong$

$f : \mid \mathbf{C} \mid \rightarrow \mid \mathbf{A} \mid$

$f = \mid C \leq A \mid$

$g : \mid \mathbf{A} \mid \rightarrow \mid \text{IA} \mid$

$g = \cong\text{-map } A \cong IA$

$\alpha : \text{is-embedding } (g \circ f)$

$\alpha = \text{o-embedding } (\cong\text{-map-is-embedding } A \cong IA) (\text{fst } \parallel C \leq A \parallel)$

$\beta : \text{is-homomorphism } \mathbf{C} \ \text{IA} \ (g \circ f)$

$\beta = \text{o-hom } \mathbf{C} \ \mathbf{A} \ \text{IA} \ \{f\}\{g\} (\text{snd } \parallel C \leq A \parallel) (\text{snd } \mid A \cong IA \mid)$

$\text{lift-alg-}\leq : \{\mathcal{X} \ \mathcal{Y} \ \mathcal{Z} \ \mathcal{W} : \text{Universe}\}(\mathbf{A} : \text{Algebra } \mathcal{X} \ S)\{\mathbf{B} : \text{Algebra } \mathcal{Y} \ S\}$
 $\rightarrow \mathbf{A} \leq \mathbf{B} \rightarrow (\text{lift-alg } \mathbf{A} \ \mathcal{Z}) \leq (\text{lift-alg } \mathbf{B} \ \mathcal{W})$

$\text{lift-alg-}\leq \ \{\mathcal{X}\}\{\mathcal{Y}\}\{\mathcal{Z}\}\{\mathcal{W}\} \ \mathbf{A} \ \{\mathbf{B}\} \ A \leq B =$

$\text{transitivity-}\leq \ \text{IA} \ \{\mathbf{B}\}\{\text{lift-alg } \mathbf{B} \ \mathcal{W}\} \ (\text{transitivity-}\leq \ \text{IA} \ \{\mathbf{A}\}\{\mathbf{B}\} \ \text{IAA } A \leq B) \ \mathbf{B} \leq \text{IB}$

where

$\text{IA} : \text{Algebra } (\mathcal{X} \sqcup \ \mathcal{Z}) \ S$

$\text{IA} = \text{lift-alg } \mathbf{A} \ \mathcal{Z}$

$\text{IAA} : \text{IA} \leq \mathbf{A}$

$\text{IAA} = \text{lift-alg-lift-}\leq\text{-lower } \mathbf{A} \ \{\mathbf{A}\} \ \text{refl-}\leq$

$\mathbf{B} \leq \text{IB} : \mathbf{B} \leq \text{lift-alg } \mathbf{B} \ \mathcal{W}$

$\mathbf{B} \leq \text{IB} = \text{lift-alg-lower-}\leq\text{-lift } \mathbf{B} \ \{\mathbf{B}\} \ \text{refl-}\leq$

6.6 WWMD

This subsection describes the [UALib.Subalgebras.WWMD](#) submodule of the Agda UALib. In his Type Topology library, Martin Escardo gives a nice formalization of the notion of subgroup and its properties. In this module we merely do for general algebras what Martin does for groups.

This is our first foray into univalent foundations, and our first chance to put Voevodsky's univalence axiom to work.

The present module is called `WWMD`.⁷ Evidently, as one sees from the lengthy import statement that starts with `open import Prelude.Preliminaries`, we import many definitions and theorems from the Type Topology library here. Most of these will not be discussed. (See www.cs.bham.ac.uk/~mhe/HoTT-UF-in-Agda-Lecture-Notes to learn about the imported modules.)

The `WWMD` module can be safely skipped. As of 22 Jan 2021, it plays no role in any of the other modules of the Agda UALib.

```

open import UALib.Algebras using (Signature;  $\mathfrak{O}$ ;  $\mathfrak{V}$ ; Algebra;  $\_ \rightarrow \_$ )
open import UALib.Prelude.Preliminaries using (global-dfunext; Universe;  $\_ \cdot$ )

module UALib.Subalgebras.WWMD
  {S : Signature  $\mathfrak{O}$   $\mathfrak{V}$ } {gfe : global-dfunext}
  { $\mathfrak{X}$  : { $\mathfrak{U}$   $\mathfrak{X}$  : Universe} {X :  $\mathfrak{X}$   $\cdot$ } (A : Algebra  $\mathfrak{U}$  S)  $\rightarrow$  X  $\rightarrow$  A}
  where

open import UALib.Subalgebras.Homomorphisms {S = S} {gfe} { $\mathfrak{X}$ } public
open import UALib.Prelude.Preliminaries using (o-embedding; id-is-embedding; Univalence; II-is-subsingleton;
   $\epsilon_0$ -is-subsingleton; pr1-embedding; embedding-gives-ap-is-equiv; equiv-to-subsingleton; powersets-are-sets';
  Ir-implication; rl-implication; subset-extensionality'; inverse;  $\times$ -is-subsingleton;  $\_ \simeq \_$ ;
  logically-equivalent-subsingletons-are-equivalent;  $\_ \cdot \_$ )

module mhe_subgroup_generalization { $\mathfrak{W}$  : Universe} {A : Algebra  $\mathfrak{W}$  S} (ua : Univalence) where

op-closed : (| A |  $\rightarrow$   $\mathfrak{W}$   $\cdot$ )  $\rightarrow$   $\mathfrak{O} \sqcup \mathfrak{V} \sqcup \mathfrak{W}$   $\cdot$ 
op-closed B = (f : | S |)(a : || S || f  $\rightarrow$  | A |)
   $\rightarrow$  ((i : || S || f)  $\rightarrow$  B (a i))  $\rightarrow$  B ((f  $\hat{\ } A$ ) a)

subuniverse :  $\mathfrak{O} \sqcup \mathfrak{V} \sqcup \mathfrak{W}$   $\cdot$ 
subuniverse =  $\Sigma$  B : ( $\mathcal{P}$  | A |) , op-closed (  $\_ \in_0$  B)

being-op-closed-is-subsingleton : (B :  $\mathcal{P}$  | A |)
   $\rightarrow$  is-subsingleton (op-closed (  $\_ \in_0$  B ))
being-op-closed-is-subsingleton B = II-is-subsingleton gfe
  ( $\lambda$  f  $\rightarrow$  II-is-subsingleton gfe
    ( $\lambda$  a  $\rightarrow$  II-is-subsingleton gfe
      ( $\lambda$   $\_ \rightarrow$   $\epsilon_0$ -is-subsingleton B ((f  $\hat{\ } A$ ) a))))

pr1-is-embedding : is-embedding | $\_$ |
pr1-is-embedding = pr1-embedding being-op-closed-is-subsingleton

--so equality of subalgebras is equality of their underlying
--subsets in the powerset:
ap-pr1 : (B C : subuniverse)  $\rightarrow$  B  $\equiv$  C  $\rightarrow$  | B |  $\equiv$  | C |
ap-pr1 B C = ap | $\_$ |

ap-pr1-is-equiv : (B C : subuniverse)  $\rightarrow$  is-equiv (ap-pr1 B C)
ap-pr1-is-equiv =
  embedding-gives-ap-is-equiv | $\_$ | pr1-is-embedding

```

⁷ For lack of a better alternative, we named this module with the acronym for “What would Martin do?”


```

subuniverse-is-a-set : is-set subuniverse
subuniverse-is-a-set B C = equiv-to-subsingleton
    (ap-pr1 B C , ap-pr1-is-equiv B C)
    (powersets-are-sets' ua | B | | C |)

subuniverse-equality-gives-membership-equiv : (B C : subuniverse)
→ B ≡ C
-----
→ ( x : | A | ) → ( x ∈0 | B | ) ⇔ ( x ∈0 | C | )
subuniverse-equality-gives-membership-equiv B C B≡C x =
  transport (λ - → x ∈0 | - | ) B≡C ,
  transport (λ - → x ∈0 | - | ) ( B≡C-1 )

membership-equiv-gives-carrier-equality : (B C : subuniverse)
→ (( x : | A | ) → x ∈0 | B | ⇔ x ∈0 | C | )
-----
→ | B | ≡ | C |
membership-equiv-gives-carrier-equality B C φ =
  subset-extensionality' ua α β
  where
    α : | B | ⊆0 | C |
    α x = lr-implication (φ x)

    β : | C | ⊆0 | B |
    β x = rl-implication (φ x)

membership-equiv-gives-subuniverse-equality : (B C : subuniverse)
→ (( x : | A | ) → x ∈0 | B | ⇔ x ∈0 | C | )
-----
→ B ≡ C
membership-equiv-gives-subuniverse-equality B C =
  inverse (ap-pr1 B C)
  (ap-pr1-is-equiv B C)
  o (membership-equiv-gives-carrier-equality B C)

membership-equiv-is-subsingleton : (B C : subuniverse)
→ is-subsingleton (( x : | A | ) → x ∈0 | B | ⇔ x ∈0 | C | )
membership-equiv-is-subsingleton B C =
  Π-is-subsingleton gfe
  (λ x → ×-is-subsingleton
    (Π-is-subsingleton gfe (λ _ → ∈0-is-subsingleton | C | x ))
    (Π-is-subsingleton gfe (λ _ → ∈0-is-subsingleton | B | x )))

subuniverse-equality : (B C : subuniverse)
→ (B ≡ C) ≃ (( x : | A | ) → ( x ∈0 | B | ) ⇔ ( x ∈0 | C | ))

subuniverse-equality B C =
  logically-equivalent-subsingletons-are-equivalent _ _
  (subuniverse-is-a-set B C)
  (membership-equiv-is-subsingleton B C)

```

(subuniverse-equality-gives-membership-equiv $B C$,
 membership-equiv-gives-subuniverse-equality $B C$)

carrier-equality-gives-membership-equiv : ($B C$: subuniverse)
 $\rightarrow | B | \equiv | C |$

$\rightarrow ((x : | \mathbf{A} |) \rightarrow x \in_0 | B | \Leftrightarrow x \in_0 | C |)$

carrier-equality-gives-membership-equiv $B C$ (refl _) $x = \text{id}$, id

–so we have...

carrier-equiv : ($B C$: subuniverse)

$\rightarrow ((x : | \mathbf{A} |) \rightarrow x \in_0 | B | \Leftrightarrow x \in_0 | C |) \simeq (| B | \equiv | C |)$

carrier-equiv $B C =$

logically-equivalent-subsingletons-are-equivalent _ _

(membership-equiv-is-subsingleton $B C$)

(powersets-are-sets' ua | B | | C |)

(membership-equiv-gives-carrier-equality $B C$,

carrier-equality-gives-membership-equiv $B C$)

– ...which yields an alternative subuniverse equality lemma.

subuniverse-equality' : ($B C$: subuniverse)

$\rightarrow (B \equiv C) \simeq (| B | \equiv | C |)$

subuniverse-equality' $B C =$

(subuniverse-equality $B C$) • (carrier-equiv $B C$)

7 Equations and Varieties

This section presents the `UALib.Varieties` module of the Agda `UALib`.

7.1 Types for Theories and Models

This subsection presents the `UALib.Varieties.ModelTheory` submodule of the Agda `UALib`.

Let S be a signature. By an **identity** or **equation** in S we mean an ordered pair of terms, written $p \approx q$, from the term algebra $\mathbf{T} X$. If \mathbf{A} is an S -algebra we say that \mathbf{A} **satisfies** $p \approx q$ provided $p \cdot \mathbf{A} \equiv q \cdot \mathbf{A}$ holds. In this situation, we write $\mathbf{A} \models p \approx q$ and say that \mathbf{A} **models** the identity $p \approx q$. If \mathcal{K} is a class of algebras of the same signature, we write $\mathcal{K} \models p \approx q$ if $\mathbf{A} \models p \approx q$ for all $\mathbf{A} \in \mathcal{K}$.⁸

Unicode Hints. To produce the symbols \approx and \models in Emacs `agda2`-mode, type `\~~` and `\models` (resp.). The symbol \approx is produced in Emacs `agda2`-mode with `\~~~`.

```
open import UALib.Algebras using (Signature; 0; V; Algebra; _→_)
open import UALib.Prelude.Preliminaries using (global-dfunext; Universe; _·)

module UALib.Varieties.ModelTheory
  {S : Signature 0 V}{gfe : global-dfunext}
  {X : {U X : Universe}{X : X ·}(A : Algebra U S) → X → A}
  where

  open import UALib.Subalgebras.Subalgebras{S = S}{gfe}{X} public
```

7.1.1 The models relation

We define the binary “models” relation \models relating algebras (or classes of algebras) to the identities that they satisfy. Agda supports the definition of infix operations and relations, and we use this to define \models so that we may write, e.g., $\mathbf{A} \models p \approx q$ or $\mathcal{K} \models p \approx q$.

After \models is defined, we prove just a couple of useful facts about \models . However, more is proved about the models relation in the next section (Section 7.2).

```
_|=≈_| : {U X : Universe}{X : X ·} → Algebra U S → Term {X}{X} → Term → U ⊔ X ·
A |= p ≈ q = (p · A) ≡ (q · A)

_|=≈_| : {U X : Universe}{X : X ·} → Pred (Algebra U S) (OV U)
→ Term {X}{X} → Term → 0 ⊔ V ⊔ X ⊔ U + ·

_|=≈_| K p q = {A : Algebra _ S} → K A → A |= p ≈ q
```

7.1.2 Equational theories and models

The set of identities that hold for all algebras in a class \mathcal{K} is denoted by $\mathbf{Th} \mathcal{K}$, which we define as follows.

⁸ Because a class of structures has a different type than a single structure, we must use a slightly different syntax to avoid overloading the relations \models and \approx . As a reasonable alternative to what we would normally express informally as $\mathcal{K} \models p \approx q$, we have settled on $\mathcal{K} \models p \approx q$ to denote this relation.

$$\begin{aligned} \text{Th} : \{ \mathcal{U} \mathcal{X} : \text{Universe} \} \{ X : \mathcal{X} \cdot \} &\rightarrow \text{Pred} (\text{Algebra } \mathcal{U} S) (\text{OV } \mathcal{U}) \\ &\rightarrow \text{Pred} (\text{Term} \{ \mathcal{X} \} \{ X \} \times \text{Term}) (\mathbb{O} \sqcup \mathcal{V} \sqcup \mathcal{X} \sqcup \mathcal{U}^+) \end{aligned}$$

$$\text{Th } \mathcal{K} = \lambda (p, q) \rightarrow \mathcal{K} \models p \approx q$$

The class of algebras that satisfy all identities in a given set \mathcal{E} is denoted by $\text{Mod } \mathcal{E}$. We give three nearly equivalent definitions for this below. The only distinction between these is whether the arguments are explicit (so must appear in the argument list) or implicit (so we may let Agda do its best to guess the argument).

$$\begin{aligned} \text{MOD} : (\mathcal{U} \mathcal{X} : \text{Universe}) (X : \mathcal{X} \cdot) &\rightarrow \text{Pred} (\text{Term} \{ \mathcal{X} \} \{ X \} \times \text{Term} \{ \mathcal{X} \} \{ X \}) (\mathbb{O} \sqcup \mathcal{V} \sqcup \mathcal{X} \sqcup \mathcal{U}^+) \\ &\rightarrow \text{Pred} (\text{Algebra } \mathcal{U} S) (\mathbb{O} \sqcup \mathcal{V} \sqcup \mathcal{X}^+ \sqcup \mathcal{U}^+) \end{aligned}$$

$$\text{MOD } \mathcal{U} \mathcal{X} X \mathcal{E} = \lambda A \rightarrow \forall p q \rightarrow (p, q) \in \mathcal{E} \rightarrow A \models p \approx q$$

$$\begin{aligned} \text{Mod} : \{ \mathcal{U} \mathcal{X} : \text{Universe} \} (X : \mathcal{X} \cdot) &\rightarrow \text{Pred} (\text{Term} \{ \mathcal{X} \} \{ X \} \times \text{Term} \{ \mathcal{X} \} \{ X \}) (\mathbb{O} \sqcup \mathcal{V} \sqcup \mathcal{X} \sqcup \mathcal{U}^+) \\ &\rightarrow \text{Pred} (\text{Algebra } \mathcal{U} S) (\mathbb{O} \sqcup \mathcal{V} \sqcup \mathcal{X}^+ \sqcup \mathcal{U}^+) \end{aligned}$$

$$\text{Mod } X \mathcal{E} = \lambda A \rightarrow \forall p q \rightarrow (p, q) \in \mathcal{E} \rightarrow A \models p \approx q$$

$$\begin{aligned} \text{mod} : \{ \mathcal{U} \mathcal{X} : \text{Universe} \} \{ X : \mathcal{X} \cdot \} &\rightarrow \text{Pred} (\text{Term} \{ \mathcal{X} \} \{ X \} \times \text{Term} \{ \mathcal{X} \} \{ X \}) (\mathbb{O} \sqcup \mathcal{V} \sqcup \mathcal{X} \sqcup \mathcal{U}^+) \\ &\rightarrow \text{Pred} (\text{Algebra } \mathcal{U} S) (\mathbb{O} \sqcup \mathcal{V} \sqcup \mathcal{X}^+ \sqcup \mathcal{U}^+) \end{aligned}$$

$$\text{mod } \mathcal{E} = \lambda A \rightarrow \forall p q \rightarrow (p, q) \in \mathcal{E} \rightarrow A \models p \approx q$$

7.1.3 Computing with \models

We have formally defined $\mathbf{A} \models p \approx q$, which represents the assertion that $p \approx q$ holds when this identity is interpreted in the algebra \mathbf{A} ; syntactically, $p \cdot \mathbf{A} \equiv q \cdot \mathbf{A}$. Hopefully we already grasp the semantic meaning of these strings of symbols, but our understanding is at best tenuous unless we have a handle on their computational meaning, since this tells us how we can *use* the definitions. So we pause to emphasize that we interpret the expression $p \cdot \mathbf{A} \equiv q \cdot \mathbf{A}$ as an *extensional equality*, by which we mean that for each *assignment function* $\mathbf{a} : X \rightarrow |\mathbf{A}|$ —assigning values in the domain of \mathbf{A} to the variable symbols in X —we have $(p \cdot \mathbf{A}) \mathbf{a} \equiv (q \cdot \mathbf{A}) \mathbf{a}$.

The binary relation \models would be practically useless if it were not an *algebraic invariant* (i.e., invariant under isomorphism), and this fact is proved by showing that a certain term operation identity—namely, $(p \cdot \mathbf{B}) \equiv (q \cdot \mathbf{B})$ —holds *extensionally*, in the sense of the previous paragraph.

$\models \cong$

$$\begin{aligned} \models\text{-transport} : \{ \mathbb{Q} \mathcal{U} \mathcal{X} : \text{Universe} \} \{ X : \mathcal{X} \cdot \} \{ \mathbf{A} : \text{Algebra } \mathbb{Q} S \} \{ \mathbf{B} : \text{Algebra } \mathcal{U} S \} \\ (p q : \text{Term} \{ \mathcal{X} \} \{ X \}) &\rightarrow (\mathbf{A} \models p \approx q) \rightarrow (\mathbf{A} \cong \mathbf{B}) \rightarrow \mathbf{B} \models p \approx q \\ \models\text{-transport } \{ \mathbb{Q} \} \{ \mathcal{U} \} \{ \mathcal{X} \} \{ X \} \{ \mathbf{A} \} \{ \mathbf{B} \} p q & \text{Apq } (f, g, f \sim g, g \sim f) = \gamma \end{aligned}$$

where

$$\begin{aligned} \gamma : (p \cdot \mathbf{B}) &\equiv (q \cdot \mathbf{B}) \\ \gamma &= gfe \lambda x \rightarrow \\ & (p \cdot \mathbf{B}) x \equiv \langle \text{refl} \rangle \\ & (p \cdot \mathbf{B}) (| \text{id } \mathbf{B} | \circ x) \equiv \langle \text{ap } (\lambda - \rightarrow (p \cdot \mathbf{B}) -) (gfe \lambda i \rightarrow ((f \sim g)(x i))^{-1}) \rangle \\ & (p \cdot \mathbf{B}) ((| f | \circ | g |) \circ x) \equiv \langle \text{comm-hom-term } gfe \mathbf{A} \mathbf{B} f p (| g | \circ x) \rangle^{-1} \\ & | f | ((p \cdot \mathbf{A}) (| g | \circ x)) \equiv \langle \text{ap } (\lambda - \rightarrow | f | (- (| g | \circ x))) \text{Apq} \rangle \end{aligned}$$

$$\begin{aligned} & | f | ((q \cdot \mathbf{A}) (| g | \circ x)) \equiv \langle \text{comm-hom-term } gfe \mathbf{A} \mathbf{B} f q (| g | \circ x) \rangle \\ & (q \cdot \mathbf{B}) (| f | \circ | g | \circ x) \equiv \langle \text{ap } (\lambda - \rightarrow (q \cdot \mathbf{B}) -) (gfe \lambda i \rightarrow (f \sim g) (x i)) \rangle \\ & (q \cdot \mathbf{B}) x \blacksquare \end{aligned}$$

$\models \cong = \models\text{-transport} -$ (*alias*)

The \models relation is also compatible with the lift operation.

```
lift-alg- $\models$  : { $\mathcal{U} \mathcal{W} \mathcal{X}$  : Universe}{ $X$  :  $\mathcal{X}$  *}
  ( $\mathbf{A}$  : Algebra  $\mathcal{U} S$ )( $p q$  : Term{ $\mathcal{X}$ }{ $X$ })
   $\rightarrow \mathbf{A} \models p \approx q \rightarrow (\text{lift-alg } \mathbf{A} \mathcal{W}) \models p \approx q$ 
lift-alg- $\models$   $\mathbf{A} p q \text{Apq} = \models \cong p q \text{Apq lift-alg-}\cong$ 

lower-alg- $\models$  : { $\mathcal{U} \mathcal{W} \mathcal{X}$  : Universe}{ $X$  :  $\mathcal{X}$  *}( $\mathbf{A}$  : Algebra  $\mathcal{U} S$ )
  ( $p q$  : Term{ $\mathcal{X}$ }{ $X$ })
   $\rightarrow$ 
  lift-alg  $\mathbf{A} \mathcal{W} \models p \approx q \rightarrow \mathbf{A} \models p \approx q$ 
lower-alg- $\models$  { $\mathcal{U}$ }{ $\mathcal{W}$ }{ $\mathcal{X}$ }{ $X$ }  $\mathbf{A} p q \text{lApq} = \models \cong p q \text{lApq (sym-}\cong \text{lift-alg-}\cong)$ 
```

7.2 Equational Logic Types

This subsection presents the `UAlib.Varieties.EquationalLogic` submodule of the Agda `UAlib`. We establish some important features of the “models” relation, which demonstrate the nice relationships \models has with the other protagonists of our story, `H`, `S`, and `P`. We prove the following closure properties, or “invariance,” of the models relation. (These are needed, for example, in the proof the Birkhoff HSP Theorem.)

- Algebraic invariance. The \models relation is an *algebraic invariant* (stable under isomorphism).
- Product invariance. Identities modeled by a class of algebras are also modeled by all products of algebras in the class.
- Subalgebra invariance. Identities modeled by a class of algebras are also modeled by all subalgebras of algebras in the class;
- Homomorphism invariance. Identities modeled by a class of algebras are also modeled by all homomorphic images (equivalently, all quotients) of algebras in the class;

```
open import UAlib.Algebras using (Signature;  $\mathcal{G}$ ;  $\mathcal{V}$ ; Algebra;  $\_ \rightarrow \_$ )
open import UAlib.Prelude.Preliminaries using (global-dfunext; Universe;  $\_*$ )
```

```
module UAlib.Varieties.EquationalLogic
  { $S$  : Signature  $\mathcal{G} \mathcal{V}$ }{ $gfe$  : global-dfunext}
  { $\mathcal{X}$  : { $\mathcal{U} \mathcal{X}$  : Universe}{ $X$  :  $\mathcal{X}$  *}}( $\mathbf{A}$  : Algebra  $\mathcal{U} S$ )  $\rightarrow X \rightarrow \mathbf{A}$ 
  where
```

```
open import UAlib.Varieties.ModelTheory { $S = S$ }{ $gfe$ }{ $\mathcal{X}$ } public
open import UAlib.Prelude.Preliminaries using ( $\circ$ -embedding; domain; embeddings-are-1c) public
```

```
ov : Universe  $\rightarrow$  Universe
ov  $\mathcal{U} = \mathcal{G} \sqcup \mathcal{V} \sqcup \mathcal{U}^+$ 
```

7.2.1 Computing with \models

We have formally defined $\mathbf{A} \models p \approx q$, which represents the assertion that $p \approx q$ holds when this identity is interpreted in the algebra \mathbf{A} ; syntactically, $p \cdot \mathbf{A} \equiv q \cdot \mathbf{A}$. It should be emphasized

that the expression $p \cdot \mathbf{A} \equiv q \cdot \mathbf{A}$ is interpreted computationally as an *extensional equality*, by which we mean that for each *assignment function* $\mathbf{a} : X \rightarrow |\mathbf{A}|$, assigning values in the domain of \mathbf{A} to the variable symbols in X , we have $(p \cdot \mathbf{A}) \mathbf{a} \equiv (q \cdot \mathbf{A}) \mathbf{a}$.

7.2.2 Algebraic invariance

The binary relation \models would be practically useless if it were not an *algebraic invariant* (i.e., invariant under isomorphism).

$$\begin{aligned} \models\text{-I-invariance} : \{ \mathcal{U} \mathcal{X} : \text{Universe} \} \{ X : \mathcal{X} \cdot \} \{ \mathbf{A} : \text{Algebra } \mathcal{U} S \} \{ \mathbf{B} : \text{Algebra } \mathcal{U} S \} \\ (p q : \text{Term} \{ \mathcal{X} \} \{ X \}) \rightarrow \mathbf{A} \models p \approx q \rightarrow \mathbf{A} \cong \mathbf{B} \rightarrow \mathbf{B} \models p \approx q \end{aligned}$$

$$\models\text{-I-invariance } \{ \mathbf{A} = \mathbf{A} \} \{ \mathbf{B} = \mathbf{B} \} p q \text{ Apq } (f, g, f \sim g, g \sim f) = \gamma$$

where

$$\begin{aligned} \gamma : p \cdot \mathbf{B} &\equiv q \cdot \mathbf{B} \\ \gamma = gfe \lambda x \rightarrow & \\ (p \cdot \mathbf{B}) x &\equiv \langle \text{refl} \rangle \\ (p \cdot \mathbf{B}) (| \text{id } \mathbf{B} | \circ x) &\equiv \langle \text{ap } (\lambda - \rightarrow (p \cdot \mathbf{B}) -) (gfe \lambda i \rightarrow ((f \sim g)(x i))^{-1}) \rangle \\ (p \cdot \mathbf{B}) ((| f | \circ | g |) \circ x) &\equiv \langle \text{comm-hom-term } gfe \mathbf{A} \mathbf{B} f p (| g | \circ x) \rangle^{-1} \rangle \\ | f | ((p \cdot \mathbf{A}) (| g | \circ x)) &\equiv \langle \text{ap } (\lambda - \rightarrow | f | (- (| g | \circ x))) \text{ Apq} \rangle \\ | f | ((q \cdot \mathbf{A}) (| g | \circ x)) &\equiv \langle \text{comm-hom-term } gfe \mathbf{A} \mathbf{B} f q (| g | \circ x) \rangle \\ (q \cdot \mathbf{B}) ((| f | \circ | g |) \circ x) &\equiv \langle \text{ap } (\lambda - \rightarrow (q \cdot \mathbf{B}) -) (gfe \lambda i \rightarrow (f \sim g)(x i)) \rangle \\ (q \cdot \mathbf{B}) x &\blacksquare \end{aligned}$$

As the proof makes clear, we show $\mathbf{B} \models p \approx q$ by showing that $p \cdot \mathbf{B} \equiv q \cdot \mathbf{B}$ holds *extensionally*, that is, $\forall x, (p \cdot \mathbf{B}) x \equiv (q \cdot \mathbf{B}) x$.

7.2.3 Lift-invariance

The \models relation is also invariant under the algebraic lift and lower operations.

$$\begin{aligned} \models\text{-lift-alg-invariance} : \{ \mathcal{U} \mathcal{W} \mathcal{X} : \text{Universe} \} \{ X : \mathcal{X} \cdot \} \\ (\mathbf{A} : \text{Algebra } \mathcal{U} S) (p q : \text{Term} \{ \mathcal{X} \} \{ X \}) \end{aligned}$$

$$\rightarrow \mathbf{A} \models p \approx q \rightarrow \text{lift-alg } \mathbf{A} \mathcal{W} \models p \approx q$$

$$\models\text{-lift-alg-invariance } \mathbf{A} p q \text{ Apq} = \models\text{-I-invariance } p q \text{ Apq } \text{lift-alg-}\cong$$

$$\begin{aligned} \models\text{-lower-alg-invariance} : \{ \mathcal{U} \mathcal{W} \mathcal{X} : \text{Universe} \} \{ X : \mathcal{X} \cdot \} (\mathbf{A} : \text{Algebra } \mathcal{U} S) \\ (p q : \text{Term} \{ \mathcal{X} \} \{ X \}) \end{aligned}$$

$$\rightarrow \text{lift-alg } \mathbf{A} \mathcal{W} \models p \approx q \rightarrow \mathbf{A} \models p \approx q$$

$$\models\text{-lower-alg-invariance } \mathbf{A} p q \text{ lApq} = \models\text{-I-invariance } p q \text{ lApq } (\text{sym-}\cong \text{lift-alg-}\cong)$$

7.2.4 Subalgebraic invariance

We show that identities modeled by a class of algebras is also modeled by all subalgebras of the class. In other terms, every term equation $p \approx q$ that is satisfied by all $\mathbf{A} \in \mathcal{K}$ is also satisfied by every subalgebra of a member of \mathcal{K} .

$$\begin{array}{c} \models\text{-S-invariance} : \{ \mathcal{U} \ \mathcal{Q} \ \mathfrak{X} : \text{Universe} \} \{ X : \mathfrak{X} \cdot \} \{ \mathcal{K} : \text{Pred} (\text{Algebra } \mathcal{Q} \ S) (\text{ov } \mathcal{Q}) \} \{ p \ q : \text{Term} \\ \quad (\mathbf{B} : \text{SubalgebraOfClass} \{ \mathcal{U} \} \{ \mathcal{Q} \} \ \mathcal{K}) \} \\ \hline \rightarrow \quad \mathcal{K} \models p \approx q \rightarrow | \mathbf{B} | \models p \approx q \\ \\ \models\text{-S-invariance } \{ X = X \} \ p \ q \ (\mathbf{B} , \mathbf{A} , SA , (ka , \text{BisSA})) \ Kpq = gfe \ \lambda \ b \rightarrow \\ \quad (\text{embeddings-are-lc} \ | \ h \ | \ \text{hem}) (\xi \ b) \\ \\ \text{where} \\ \quad h' : \text{hom} \ | \ SA \ | \ \mathbf{A} \\ \quad h' = (| \ \text{snd} \ SA \ | , \ \text{snd} \ \| \ \text{snd} \ SA \ \|) \\ \\ \quad h : \text{hom} \ \mathbf{B} \ \mathbf{A} \\ \quad h = \text{HCompClosed} \ \mathbf{B} \ (| \ SA \ |) \ \mathbf{A} \ (| \ \text{BisSA} \ |) \ h' \\ \\ \quad \text{hem} : \text{is-embedding} \ | \ h \ | \\ \quad \text{hem} = \text{o-embedding} \ (\text{fst} \ \| \ \text{snd} \ SA \ \|) \ (\text{iso} \rightarrow \text{embedding} \ \text{BisSA}) \\ \\ \quad \xi : (b : X \rightarrow | \mathbf{B} |) \rightarrow | h | ((p \cdot \mathbf{B}) \ b) \equiv | h | ((q \cdot \mathbf{B}) \ b) \\ \quad \xi \ b = | h | ((p \cdot \mathbf{B}) \ b) \equiv \langle \text{comm-hom-term} \ gfe \ \mathbf{B} \ \mathbf{A} \ h \ p \ b \rangle \\ \quad \quad (p \cdot \mathbf{A}) (| h | \circ b) \equiv \langle \text{intensionality} \ (Kpq \ ka) \ (| h | \circ b) \rangle \\ \quad \quad (q \cdot \mathbf{A}) (| h | \circ b) \equiv \langle \text{comm-hom-term} \ gfe \ \mathbf{B} \ \mathbf{A} \ h \ q \ b \rangle^{-1} \rangle \\ \quad \quad | h | ((q \cdot \mathbf{B}) \ b) \blacksquare \end{array}$$

7.2.5 Product invariance

An identities satisfied by all algebras in a class are also satisfied by the product of algebras in that class.

$$\begin{array}{c} \models\text{-P-invariance} : \{ \mathcal{U} \ \mathfrak{X} : \text{Universe} \} \{ X : \mathfrak{X} \cdot \} \{ p \ q : \text{Term} \{ \mathfrak{X} \} \{ X \} \} \\ \quad (I : \mathcal{U} \cdot) (\mathcal{A} : I \rightarrow \text{Algebra } \mathcal{U} \ S) \\ \hline \rightarrow \quad (\forall i \rightarrow (\mathcal{A} \ i) \models p \approx q) \rightarrow \prod \mathcal{A} \models p \approx q \\ \\ \models\text{-P-invariance} \ p \ q \ I \ \mathcal{A} \ \mathcal{A}pq = \gamma \\ \\ \text{where} \\ \quad \gamma : p \cdot \prod \mathcal{A} \equiv q \cdot \prod \mathcal{A} \\ \quad \gamma = gfe \ \lambda \ a \rightarrow \\ \quad \quad (p \cdot \prod \mathcal{A}) \ a \equiv \langle \text{interp-prod} \ gfe \ p \ \mathcal{A} \ a \rangle \\ \quad \quad (\lambda i \rightarrow ((p \cdot (\mathcal{A} \ i)) (\lambda x \rightarrow (a \ x) \ i))) \equiv \langle gfe \ (\lambda i \rightarrow \text{cong-app} \ (\mathcal{A}pq \ i) \ (\lambda x \rightarrow (a \ x) \ i)) \rangle \\ \quad \quad (\lambda i \rightarrow ((q \cdot (\mathcal{A} \ i)) (\lambda x \rightarrow (a \ x) \ i))) \equiv \langle (\text{interp-prod} \ gfe \ q \ \mathcal{A} \ a)^{-1} \rangle \\ \quad \quad (q \cdot \prod \mathcal{A}) \ a \blacksquare \\ \\ \models\text{-P-class-invariance} : \{ \mathcal{U} \ \mathfrak{X} : \text{Universe} \} \{ X : \mathfrak{X} \cdot \} \{ \mathcal{K} : \text{Pred} (\text{Algebra } \mathcal{U} \ S) (\text{ov } \mathcal{U}) \} \\ \quad (p \ q : \text{Term} \{ \mathfrak{X} \} \{ X \}) (I : \mathcal{U} \cdot) (\mathcal{A} : I \rightarrow \text{Algebra } \mathcal{U} \ S) \\ \rightarrow \quad (\forall i \rightarrow \mathcal{A} \ i \in \mathcal{K}) \\ \hline \rightarrow \quad \mathcal{K} \models p \approx q \rightarrow \prod \mathcal{A} \models p \approx q \\ \\ \models\text{-P-class-invariance} \ p \ q \ I \ \mathcal{A} \ K\mathcal{A} \ \alpha = \gamma \\ \\ \text{where} \\ \quad \beta : \forall i \rightarrow (\mathcal{A} \ i) \models p \approx q \end{array}$$

$$\begin{aligned} \beta \ i &= \alpha \ (K \mathcal{A} \ i) \\ \gamma &: p \cdot \prod \mathcal{A} \equiv q \cdot \prod \mathcal{A} \\ \gamma &= \models\text{-P-invariance } p \ q \ I \mathcal{A} \ \beta \end{aligned}$$

Another fact that will turn out to be useful is that a product of a collection of algebras models $p \approx q$ if the lift of each algebra in the collection models $p \approx q$.

$$\begin{aligned} \models\text{-P-lift-invariance} &: \{ \mathcal{U} \ \mathcal{W} \ \mathcal{X} : \text{Universe} \} \{ X : \mathcal{X} \cdot \} (p \ q : \text{Term} \{ \mathcal{X} \} \{ X \}) \\ & \quad (I : \mathcal{U} \cdot) (\mathcal{A} : I \rightarrow \text{Algebra } \mathcal{U} \ S) \\ \rightarrow & \quad \frac{}{(\forall i \rightarrow (\text{lift-alg } (\mathcal{A} \ i) \ \mathcal{W}) \models p \approx q) \rightarrow \prod \mathcal{A} \models p \approx q} \\ \models\text{-P-lift-invariance } \{ \mathcal{U} \} \{ \mathcal{W} \} \ p \ q \ I \mathcal{A} \ lApq &= \models\text{-P-invariance } p \ q \ I \mathcal{A} \ \text{Aipq} \\ \text{where} & \\ \text{Aipq} &: (i : I) \rightarrow (\mathcal{A} \ i) \models p \approx q \\ \text{Aipq } i &= \models\text{-I-invariance } p \ q \ (lApq \ i) \ (\text{sym-}\cong \ \text{lift-alg-}\cong) \end{aligned}$$

7.2.6 Homomorphic invariance⁹

If an algebra \mathbf{A} models an identity $p \approx q$, then the pair (p, q) belongs to the kernel of every homomorphism $\varphi : \text{hom}(\mathbf{T} \ X) \ \mathbf{A}$ from the term algebra to \mathbf{A} ; that is, every homomorphism from $\mathbf{T} \ X$ to \mathbf{A} maps p and q to the same element of \mathbf{A} .

$$\begin{aligned} \models\text{-H-invariance} &: \{ \mathcal{U} \ \mathcal{X} : \text{Universe} \} (X : \mathcal{X} \cdot) (p \ q : \text{Term} \{ \mathcal{X} \} \{ X \}) \\ & \quad (\mathbf{A} : \text{Algebra } \mathcal{U} \ S) (\varphi : \text{hom} (\mathbf{T} \ X) \ \mathbf{A}) \\ \rightarrow & \quad \frac{}{\mathbf{A} \models p \approx q \rightarrow |\varphi| \ p \equiv |\varphi| \ q} \\ \models\text{-H-invariance } X \ p \ q \ \mathbf{A} \ \varphi \ \beta &= \\ |\varphi| \ p & \equiv \langle \text{ap } |\varphi| \ (\text{term-agreement } p) \rangle \\ |\varphi| \ ((p \cdot \mathbf{T} \ X) \ \mathcal{g}) & \equiv \langle \text{comm-hom-term } gfe \ (\mathbf{T} \ X) \ \mathbf{A} \ \varphi \ p \ \mathcal{g} \rangle \\ (p \cdot \mathbf{A}) \ (|\varphi| \circ \mathcal{g}) & \equiv \langle \text{intensionality } \beta \ (|\varphi| \circ \mathcal{g}) \rangle \\ (q \cdot \mathbf{A}) \ (|\varphi| \circ \mathcal{g}) & \equiv \langle \text{comm-hom-term } gfe \ (\mathbf{T} \ X) \ \mathbf{A} \ \varphi \ q \ \mathcal{g} \rangle^{-1} \\ |\varphi| \ ((q \cdot \mathbf{T} \ X) \ \mathcal{g}) & \equiv \langle \text{ap } |\varphi| \ (\text{term-agreement } q) \rangle^{-1} \\ |\varphi| \ q & \quad \blacksquare \end{aligned}$$

More generally, an identity is satisfied by all algebras in a class if and only if that identity is invariant under all homomorphisms from the term algebra $\mathbf{T} \ X$ into algebras of the class. More precisely, if \mathcal{K} is a class of S -algebras and p, q terms in the language of S , then,

$$\begin{aligned} \mathcal{K} \models p \approx q &\Leftrightarrow \forall \mathbf{A} \in \mathcal{K}, \forall \varphi : \text{hom} (\mathbf{T} \ X) \ \mathbf{A}, \varphi \circ (p \cdot (\mathbf{T} \ X)) = \varphi \circ (q \cdot (\mathbf{T} \ X)). \\ & \quad \text{--} \Rightarrow \text{(the "only if" direction)} \\ \models\text{-H-class-invariance} &: \{ \mathcal{U} \ \mathcal{X} : \text{Universe} \} \{ X : \mathcal{X} \cdot \} \{ \mathcal{K} : \text{Pred} (\text{Algebra } \mathcal{U} \ S) (\text{ov } \mathcal{U}) \} (p \ q : \text{Term}) \\ \rightarrow & \quad \mathcal{K} \models p \approx q \\ \rightarrow & \quad (\mathbf{A} : \text{Algebra } \mathcal{U} \ S) (\varphi : \text{hom} (\mathbf{T} \ X) \ \mathbf{A}) \\ \rightarrow & \quad \frac{}{\mathbf{A} \in \mathcal{K} \rightarrow |\varphi| \circ (p \cdot \mathbf{T} \ X) \equiv |\varphi| \circ (q \cdot \mathbf{T} \ X)} \end{aligned}$$

⁹ Those mainly interested in the formal proof of Birkhoff's HSP theorem can safely skip this section; it is not needed elsewhere in the UALib

\models -H-class-invariance $X p q \alpha \mathbf{A} \varphi ka = gfe \xi$

where

$\xi : \forall (\mathbf{a} : X \rightarrow | \mathbf{T} X |) \rightarrow | \varphi | ((p \cdot \mathbf{T} X) \mathbf{a}) \equiv | \varphi | ((q \cdot \mathbf{T} X) \mathbf{a})$

$\xi \mathbf{a} = | \varphi | ((p \cdot \mathbf{T} X) \mathbf{a}) \equiv \langle \text{comm-hom-term } gfe (\mathbf{T} X) \mathbf{A} \varphi p \mathbf{a} \rangle$
 $(p \cdot \mathbf{A})(| \varphi | \circ \mathbf{a}) \equiv \langle \text{intensionality } (\alpha ka) (| \varphi | \circ \mathbf{a}) \rangle$
 $(q \cdot \mathbf{A})(| \varphi | \circ \mathbf{a}) \equiv \langle \text{comm-hom-term } gfe (\mathbf{T} X) \mathbf{A} \varphi q \mathbf{a} \rangle^{-1}$
 $| \varphi | ((q \cdot \mathbf{T} X) \mathbf{a}) \blacksquare$

$- \Leftarrow$ (the "if" direction)

\models -H-class-coinvariance : $\{\mathcal{U} \mathcal{X} : \text{Universe}\}(X : \mathcal{X} \cdot)\{\mathcal{K} : \text{Pred } (\text{Algebra } \mathcal{U} S)(\text{ov } \mathcal{U})\}(p q : \text{Term})$
 $\rightarrow ((\mathbf{A} : \text{Algebra } \mathcal{U} S)(\varphi : \text{hom } (\mathbf{T} X) \mathbf{A})$
 $\rightarrow \mathbf{A} \in \mathcal{K} \rightarrow | \varphi | \circ (p \cdot \mathbf{T} X) \equiv | \varphi | \circ (q \cdot \mathbf{T} X))$

$\rightarrow \mathcal{K} \models p \approx q$

\models -H-class-coinvariance $X p q \beta \{\mathbf{A}\} ka = \gamma$

where

$\varphi : (\mathbf{a} : X \rightarrow | \mathbf{A} |) \rightarrow \text{hom } (\mathbf{T} X) \mathbf{A}$

$\varphi \mathbf{a} = \text{lift-hom } \mathbf{A} \mathbf{a}$

$\gamma : \mathbf{A} \models p \approx q$

$\gamma = gfe \lambda \mathbf{a} \rightarrow$

$(p \cdot \mathbf{A})(| \varphi \mathbf{a} | \circ \mathbf{q}) \equiv \langle \text{comm-hom-term } gfe (\mathbf{T} X) \mathbf{A} (\varphi \mathbf{a}) p \mathbf{q} \rangle^{-1}$
 $(| \varphi \mathbf{a} | \circ (p \cdot \mathbf{T} X)) \mathbf{q} \equiv \langle \text{ap } (\lambda - \rightarrow - \mathbf{q}) (\beta \mathbf{A} (\varphi \mathbf{a}) ka) \rangle$
 $(| \varphi \mathbf{a} | \circ (q \cdot \mathbf{T} X)) \mathbf{q} \equiv \langle \text{comm-hom-term } gfe (\mathbf{T} X) \mathbf{A} (\varphi \mathbf{a}) q \mathbf{q} \rangle$
 $(q \cdot \mathbf{A})(| \varphi \mathbf{a} | \circ \mathbf{q}) \blacksquare$

\models -H-compatibility : $\{\mathcal{U} \mathcal{X} : \text{Universe}\}(X : \mathcal{X} \cdot)\{\mathcal{K} : \text{Pred } (\text{Algebra } \mathcal{U} S)(\text{ov } \mathcal{U})\}(p q : \text{Term})$

$\rightarrow \mathcal{K} \models p \approx q \Leftrightarrow ((\mathbf{A} : \text{Algebra } \mathcal{U} S)(\varphi : \text{hom } (\mathbf{T} X) \mathbf{A})$
 $\rightarrow \mathbf{A} \in \mathcal{K} \rightarrow | \varphi | \circ (p \cdot \mathbf{T} X) \equiv | \varphi | \circ (q \cdot \mathbf{T} X))$

\models -H-compatibility $X p q = \models$ -H-class-invariance $X p q, \models$ -H-class-coinvariance $X p q$

7.3 Inductive Types H, S, P, V

This subsection presents the `UALib.Varieties.Varieties` submodule of the Agda UALib. Fix a signature S , let \mathcal{K} be a class of S -algebras, and define

- $\mathbf{H} \mathcal{K}$ = algebras isomorphic to a homomorphic image of a members of \mathcal{K} ;
- $\mathbf{S} \mathcal{K}$ = algebras isomorphic to a subalgebra of a member of \mathcal{K} ;
- $\mathbf{P} \mathcal{K}$ = algebras isomorphic to a product of members of \mathcal{K} .

A straight-forward verification confirms that \mathbf{H} , \mathbf{S} , and \mathbf{P} are **closure operators** (expansive, monotone, and idempotent). A class \mathcal{K} of S -algebras is said to be *closed under the taking of homomorphic images* provided $\mathbf{H} \mathcal{K} \subseteq \mathcal{K}$. Similarly, \mathcal{K} is *closed under the taking of subalgebras* (resp., *arbitrary products*) provided $\mathbf{S} \mathcal{K} \subseteq \mathcal{K}$ (resp., $\mathbf{P} \mathcal{K} \subseteq \mathcal{K}$).

An algebra is a homomorphic image (resp., subalgebra; resp., product) of every algebra to which it is isomorphic. Thus, the class $\mathbf{H} \mathcal{K}$ (resp., $\mathbf{S} \mathcal{K}$; resp., $\mathbf{P} \mathcal{K}$) is closed under isomorphism.

The operators **H**, **S**, and **P** can be composed with one another repeatedly, forming yet more closure operators.

A **variety** is a class \mathcal{K} of algebras in a fixed signature that is closed under the taking of homomorphic images (**H**), subalgebras (**S**), and arbitrary products (**P**). That is, \mathcal{K} is a variety if and only if $\mathbf{H S P} \mathcal{K} \subseteq \mathcal{K}$.

This module defines what we have found to be the most useful inductive types representing the closure operators **H**, **S**, and **P**. Separately, we define the inductive type V for simultaneously representing closure under **H**, **S**, and **P**.

```
open import UALib.Algebras using (Signature;  $\mathfrak{G}$ ;  $\mathcal{V}$ ; Algebra;  $\_ \rightarrow \_$ )
open import UALib.Prelude.Preliminaries using (global-dfunext; Universe;  $\_ \cdot$ )

module UALib.Varieties.Varieties
  {S : Signature  $\mathfrak{G}$   $\mathcal{V}$ } {gfe : global-dfunext}
  { $\mathcal{X}$  : { $\mathcal{U}$   $\mathcal{X}$  : Universe} {X :  $\mathcal{X}$   $\cdot$ } } (A : Algebra  $\mathcal{U}$  S)  $\rightarrow$  X  $\rightarrow$  A}
  where

  open import UALib.Varieties.EquationalLogic {S = S} {gfe} { $\mathcal{X}$ } public
```

7.3.1 Homomorphism closure

We define the inductive type **H** to represent classes of algebras that include all homomorphic images of algebras in the class; i.e., classes that are closed under the taking of homomorphic images.

```
data H { $\mathcal{U}$   $\mathcal{W}$  : Universe} ( $\mathcal{K}$  : Pred (Algebra  $\mathcal{U}$  S) (ov  $\mathcal{U}$ )) :
  Pred (Algebra ( $\mathcal{U}$   $\sqcup$   $\mathcal{W}$ ) S) (ov ( $\mathcal{U}$   $\sqcup$   $\mathcal{W}$ )) where
  hbase : {A : Algebra  $\mathcal{U}$  S}  $\rightarrow$  A  $\in$   $\mathcal{K}$   $\rightarrow$  lift-alg A  $\mathcal{W}$   $\in$  H  $\mathcal{K}$ 
  hlift : {A : Algebra  $\mathcal{U}$  S}  $\rightarrow$  A  $\in$  H { $\mathcal{U}$ } { $\mathcal{U}$ }  $\mathcal{K}$   $\rightarrow$  lift-alg A  $\mathcal{W}$   $\in$  H  $\mathcal{K}$ 
  hhimg : {A B : Algebra  $\_$  S}  $\rightarrow$  A  $\in$  H { $\mathcal{U}$ } { $\mathcal{W}$ }  $\mathcal{K}$   $\rightarrow$  B is-hom-image-of A  $\rightarrow$  B  $\in$  H  $\mathcal{K}$ 
  hiso : {A : Algebra  $\_$  S} {B : Algebra  $\_$  S}  $\rightarrow$  A  $\in$  H { $\mathcal{U}$ } { $\mathcal{U}$ }  $\mathcal{K}$   $\rightarrow$  A  $\cong$  B  $\rightarrow$  B  $\in$  H  $\mathcal{K}$ 
```

7.3.2 Subalgebra closure

The most useful inductive type that we have found for representing classes of algebras that are closed under the taking of subalgebras as an inductive type.

```
data S { $\mathcal{U}$   $\mathcal{W}$  : Universe} ( $\mathcal{K}$  : Pred (Algebra  $\mathcal{U}$  S) (ov  $\mathcal{U}$ )) :
  Pred (Algebra ( $\mathcal{U}$   $\sqcup$   $\mathcal{W}$ ) S) (ov ( $\mathcal{U}$   $\sqcup$   $\mathcal{W}$ )) where
  sbase : {A : Algebra  $\mathcal{U}$  S}  $\rightarrow$  A  $\in$   $\mathcal{K}$   $\rightarrow$  lift-alg A  $\mathcal{W}$   $\in$  S  $\mathcal{K}$ 
  slift : {A : Algebra  $\mathcal{U}$  S}  $\rightarrow$  A  $\in$  S { $\mathcal{U}$ } { $\mathcal{U}$ }  $\mathcal{K}$   $\rightarrow$  lift-alg A  $\mathcal{W}$   $\in$  S  $\mathcal{K}$ 
  ssub : {A : Algebra  $\mathcal{U}$  S} {B : Algebra  $\_$  S}  $\rightarrow$  A  $\in$  S { $\mathcal{U}$ } { $\mathcal{U}$ }  $\mathcal{K}$   $\rightarrow$  B  $\leq$  A  $\rightarrow$  B  $\in$  S  $\mathcal{K}$ 
  ssubw : {A B : Algebra  $\_$  S}  $\rightarrow$  A  $\in$  S { $\mathcal{U}$ } { $\mathcal{W}$ }  $\mathcal{K}$   $\rightarrow$  B  $\leq$  A  $\rightarrow$  B  $\in$  S  $\mathcal{K}$ 
  siso : {A : Algebra  $\mathcal{U}$  S} {B : Algebra  $\_$  S}  $\rightarrow$  A  $\in$  S { $\mathcal{U}$ } { $\mathcal{U}$ }  $\mathcal{K}$   $\rightarrow$  A  $\cong$  B  $\rightarrow$  B  $\in$  S  $\mathcal{K}$ 
```

7.3.3 Product closure

The most useful inductive type that we have found for representing classes of algebras closed under arbitrary products is the following.

```
data P { $\mathcal{U}$   $\mathcal{W}$  : Universe} ( $\mathcal{K}$  : Pred (Algebra  $\mathcal{U}$  S) (ov  $\mathcal{U}$ )) : Pred (Algebra ( $\mathcal{U}$   $\sqcup$   $\mathcal{W}$ ) S) (ov ( $\mathcal{U}$   $\sqcup$   $\mathcal{W}$ )) where
  pbase : {A : Algebra  $\mathcal{U}$  S}  $\rightarrow$  A  $\in$   $\mathcal{K}$   $\rightarrow$  lift-alg A  $\mathcal{W}$   $\in$  P  $\mathcal{K}$ 
```

```

pliftu : {A : Algebra U S} → A ∈ P{U}{U} K → lift-alg A W ∈ P K
pliftw : {A : Algebra (U ⊔ W) S} → A ∈ P{U}{W} K → lift-alg A (U ⊔ W) ∈ P K
produ : {I : W · } {A : I → Algebra U S} → (∀ i → (A i) ∈ P{U}{U} K) → ∏ A ∈ P K
prodw : {I : W · } {A : I → Algebra _ S} → (∀ i → (A i) ∈ P{U}{W} K) → ∏ A ∈ P K
pisou : {A : Algebra U S} {B : Algebra _ S} → A ∈ P{U}{U} K → A ≅ B → B ∈ P K
pisow : {A B : Algebra _ S} → A ∈ P{U}{W} K → A ≅ B → B ∈ P K

```

7.3.4 Varietal closure

A class \mathcal{K} of S -algebras is called a **variety** if it is closed under each of the closure operators **H**, **S**, and **P** introduced above; the corresponding closure operator is often denoted \mathbb{V} , but we will typically denote it by \mathbb{V} .

Thus, if \mathcal{K} is a class of S -algebras, then the **variety generated by** \mathcal{K} is denoted by $\mathbb{V} \mathcal{K}$ and defined to be the smallest class that contains \mathcal{K} and is closed under **H**, **S**, and **P**.

We now define \mathbb{V} as an inductive type.

```

data V {U W : Universe} (K : Pred (Algebra U S) (ov U)) :
  Pred (Algebra (U ⊔ W) S) (ov (U ⊔ W)) where
  vbase : {A : Algebra U S} → A ∈ K → lift-alg A W ∈ V K
  vlift  : {A : Algebra U S} → A ∈ V{U}{U} K → lift-alg A W ∈ V K
  vliftw : {A : Algebra _ S} → A ∈ V{U}{W} K → lift-alg A (U ⊔ W) ∈ V K
  vhmig : {A B : Algebra _ S} → A ∈ V{U}{W} K → B is-hom-image-of A → B ∈ V K
  vssub  : {A : Algebra U S} {B : Algebra _ S} → A ∈ V{U}{U} K → B ≤ A → B ∈ V K
  vssubw : {A B : Algebra _ S} → A ∈ V{U}{W} K → B ≤ A → B ∈ V K
  vprodu : {I : W · } {A : I → Algebra U S} → (∀ i → (A i) ∈ V{U}{U} K) → ∏ A ∈ V K
  vprodw : {I : W · } {A : I → Algebra _ S} → (∀ i → (A i) ∈ V{U}{W} K) → ∏ A ∈ V K
  visou  : {A : Algebra U S} {B : Algebra _ S} → A ∈ V{U}{U} K → A ≅ B → B ∈ V K
  visow  : {A B : Algebra _ S} → A ∈ V{U}{W} K → A ≅ B → B ∈ V K

```

7.3.5 Closure properties

The types defined above represent operators with useful closure properties. We now prove a handful of such properties since we will need them later.

– P is a closure operator; in particular, it's expansive.

```

P-expa : {U : Universe} {K : Pred (Algebra U S) (ov U)} → K ⊆ P{U}{U} K
P-expa {U}{K} {A} KA = pisou {A = (lift-alg A U)} {B = A} (pbase KA) (sym-≅ lift-alg-≅)

```

– P is a closure operator; in particular, it's idempotent.

```

P-idemp : {U : Universe} {W : Universe} {K : Pred (Algebra U S) (ov U)}
  → P{U ⊔ W}{U ⊔ W} (P{U}{U ⊔ W} K) ⊆ P{U}{U ⊔ W} K

```

```

P-idemp (pbase x) = pliftw x
P-idemp {U}{W} (pliftu x) = pliftw (P-idemp{U}{W} x)
P-idemp {U}{W} (pliftw x) = pliftw (P-idemp{U}{W} x)
P-idemp {U}{W} (produ x) = prodw (λ i → P-idemp{U}{W} (x i))
P-idemp {U}{W} (prodw x) = prodw (λ i → P-idemp{U}{W} (x i))
P-idemp {U}{W} (pisou x x1) = pisow (P-idemp{U}{W} x) x1
P-idemp {U}{W} (pisow x x1) = pisow (P-idemp{U}{W} x) x1

```

– S is a closure operator; in particular, it's monotone.

$S\text{-mono} : \{\mathcal{U} \mathcal{W} : \text{Universe}\} \{\mathcal{K} \mathcal{K}' : \text{Pred} (\text{Algebra } \mathcal{U} S)(\text{ov } \mathcal{U})\}$
 $\rightarrow \mathcal{K} \subseteq \mathcal{K}' \rightarrow S\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K} \subseteq S\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K}'$
 $S\text{-mono } \text{ante} (\text{sbase } x) = \text{sbase } (\text{ante } x)$
 $S\text{-mono } \{\mathcal{U}\}\{\mathcal{W}\}\{\mathcal{K}\}\{\mathcal{K}'\} \text{ante} (\text{slift}\{\mathbf{A}\} x) = \text{slift}\{\mathcal{U}\}\{\mathcal{W}\}\{\mathcal{K}'\} (S\text{-mono}\{\mathcal{U}\}\{\mathcal{U}\} \text{ante } x)$
 $S\text{-mono } \text{ante} (\text{ssub}\{\mathbf{A}\}\{\mathbf{B}\} sA B \leq A) = \text{ssub} (S\text{-mono } \text{ante } sA) B \leq A$
 $S\text{-mono } \text{ante} (\text{ssubw}\{\mathbf{A}\}\{\mathbf{B}\} sA B \leq A) = \text{ssubw} (S\text{-mono } \text{ante } sA) B \leq A$
 $S\text{-mono } \text{ante} (\text{siso } x x_1) = \text{siso} (S\text{-mono } \text{ante } x) x_1$

We sometimes want to go back and forth between our two representations of subalgebras of algebras in a class. The tools `subalgebra→S` and `S→subalgebra` were designed with that purpose in mind.

$\text{subalgebra} \rightarrow S : \{\mathcal{U} \mathcal{W} : \text{Universe}\} \{\mathcal{K} : \text{Pred} (\text{Algebra } \mathcal{U} S)(\text{OV } \mathcal{U})\}$
 $\{\mathbf{C} : \text{Algebra } (\mathcal{U} \sqcup \mathcal{W}) S\} \rightarrow \mathbf{C} \text{ IsSubalgebraOfClass } \mathcal{K}$

 $\rightarrow \mathbf{C} \in S\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K}$

$\text{subalgebra} \rightarrow S \{\mathcal{U}\}\{\mathcal{W}\}\{\mathcal{K}\}\{\mathbf{C}\} (\mathbf{A}, ((\mathbf{B}, B \leq A), KA, C \cong B)) = \text{ssub } sA \mathbf{C} \leq A$

where

$\mathbf{C} \leq A : \mathbf{C} \leq \mathbf{A}$
 $\mathbf{C} \leq A = \text{Iso-} \leq \mathbf{A} \mathbf{C} B \leq A C \cong B$

$s\mathbf{A}u : \text{lift-alg } \mathbf{A} \mathcal{U} \in S\{\mathcal{U}\}\{\mathcal{U}\} \mathcal{K}$
 $s\mathbf{A}u = \text{sbase } KA$

$sA : \mathbf{A} \in S\{\mathcal{U}\}\{\mathcal{U}\} \mathcal{K}$
 $sA = \text{siso } s\mathbf{A}u (\text{sym-} \cong \text{lift-alg-} \cong)$

`module` $_ \{\mathcal{U} : \text{Universe}\} \{\mathcal{K} : \text{Pred} (\text{Algebra } \mathcal{U} S)(\text{OV } \mathcal{U})\}$ where

$S \rightarrow \text{subalgebra} : \{\mathbf{B} : \text{Algebra } \mathcal{U} S\} \rightarrow \mathbf{B} \in S\{\mathcal{U}\}\{\mathcal{U}\} \mathcal{K} \rightarrow \mathbf{B} \text{ IsSubalgebraOfClass } \mathcal{K}$

$S \rightarrow \text{subalgebra} (\text{sbase}\{\mathbf{B}\} x) = \mathbf{B}, (\mathbf{B}, \text{refl-} \leq), x, (\text{sym-} \cong \text{lift-alg-} \cong)$

$S \rightarrow \text{subalgebra} (\text{slift}\{\mathbf{B}\} x) = | \text{BS} |, \text{SA}, \text{KA}, \text{TRANS-} \cong (\text{sym-} \cong \text{lift-alg-} \cong) \text{B} \cong \text{SA}$

where

$\text{BS} : \mathbf{B} \text{ IsSubalgebraOfClass } \mathcal{K}$
 $\text{BS} = S \rightarrow \text{subalgebra } x$

$\text{SA} : \text{SUBALGEBRA } | \text{BS} |$
 $\text{SA} = \text{fst } || \text{BS} ||$

$\text{KA} : | \text{BS} | \in \mathcal{K}$
 $\text{KA} = | \text{snd } || \text{BS} || |$

$\text{B} \cong \text{SA} : \mathbf{B} \cong | \text{SA} |$
 $\text{B} \cong \text{SA} = || \text{snd } || \text{BS} || ||$

$S \rightarrow \text{subalgebra } \{\mathbf{B}\} (\text{ssub}\{\mathbf{A}\} sA B \leq A) = \gamma$

where

$\text{AS} : \mathbf{A} \text{ IsSubalgebraOfClass } \mathcal{K}$
 $\text{AS} = S \rightarrow \text{subalgebra } sA$
 $\text{SA} : \text{SUBALGEBRA } | \text{AS} |$

```

SA = fst || AS ||
B≤SA : B ≤ | SA |
B≤SA = TRANS-≤-≅ B | SA | B≤A (|| snd || AS ||)
B≤AS : B ≤ | AS |
B≤AS = transitivity-≤ B{| SA |}{| AS |} B≤SA || SA ||
γ : B IsSubalgebraOfClass K
γ = | AS | , (B , B≤AS) , | snd || AS || | , refl-≅

```

$S \rightarrow \text{subalgebra } \{\mathbf{B}\} (\text{ssubw}\{\mathbf{A}\} \text{ } sA \text{ } B \leq A) = \gamma$

where

```

AS : A IsSubalgebraOfClass K
AS = S→subalgebra sA
SA : SUBALGEBRA | AS |
SA = fst || AS ||
B≤SA : B ≤ | SA |
B≤SA = TRANS-≤-≅ B | SA | B≤A (|| snd || AS ||)
B≤AS : B ≤ | AS |
B≤AS = transitivity-≤ B{| SA |}{| AS |} B≤SA || SA ||
γ : B IsSubalgebraOfClass K
γ = | AS | , (B , B≤AS) , | snd || AS || | , refl-≅

```

$S \rightarrow \text{subalgebra } \{\mathbf{B}\} (\text{siso}\{\mathbf{A}\} \text{ } sA \text{ } A \cong B) = \gamma$

where

```

AS : A IsSubalgebraOfClass K
AS = S→subalgebra sA
SA : SUBALGEBRA | AS |
SA = fst || AS ||
A≅SA : A ≅ | SA |
A≅SA = snd || snd AS ||
γ : B IsSubalgebraOfClass K
γ = | AS | , SA , | snd || AS || | , (TRANS-≅ (sym-≅ A ≅ B) A ≅ SA)

```

Next we observe that lifting to a higher universe does not break the property of being a subalgebra of an algebra of a class. In other words, if we lift a subalgebra of an algebra in a class, the result is still a subalgebra of an algebra in the class.

$\text{lift-alg-subP} : \{\mathcal{U} \mathcal{W} : \text{Universe}\} \{\mathcal{K} : \text{Pred } (\text{Algebra } \mathcal{U} \text{ } S)(\text{ov } \mathcal{U})\} \{\mathbf{B} : \text{Algebra } \mathcal{U} \text{ } S\}$

$\rightarrow \mathbf{B} \text{ IsSubalgebraOfClass } (\text{P}\{\mathcal{U}\}\{\mathcal{U}\} \mathcal{K})$

$\rightarrow (\text{lift-alg } \mathbf{B} \mathcal{W}) \text{ IsSubalgebraOfClass } (\text{P}\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K})$

$\text{lift-alg-subP } \{\mathcal{U}\} \{\mathcal{W}\} \{\mathcal{K}\} \{\mathbf{B}\} (\mathbf{A} , (\mathbf{C} , C \leq A) , pA , B \cong C) = \gamma$

where

```

IA IB IC : Algebra (U ⊔ W) S
IA = lift-alg A W
IB = lift-alg B W
IC = lift-alg C W

IC≤IA : IC ≤ IA
IC≤IA = lift-alg-≤ C {A} C≤A

```

$$\begin{aligned} \text{plA} &: \text{IA} \in \text{P}\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K} \\ \text{plA} &= \text{pliftu } pA \end{aligned}$$

$$\begin{aligned} \gamma &: \text{IB IsSubalgebraOfClass} (\text{P}\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K}) \\ \gamma &= \text{IA} , (\text{IC} , \text{IC} \leq \text{IA}) , \text{plA} , (\text{lift-alg-iso } \mathcal{U} \mathcal{W} \text{ B C } B \cong C) \end{aligned}$$

The next lemma would be too obvious to care about were it not for the fact that we'll need it later, so it too must be formalized.

$$\begin{aligned} \text{S} \subseteq \text{SP} &: \{\mathcal{U} \mathcal{W} : \text{Universe}\} \{\mathcal{K} : \text{Pred} (\text{Algebra } \mathcal{U} S) (\text{ov } \mathcal{U})\} \\ &\rightarrow \text{S}\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K} \subseteq \text{S}\{\mathcal{U} \sqcup \mathcal{W}\}\{\mathcal{U} \sqcup \mathcal{W}\} (\text{P}\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K}) \end{aligned}$$

$$\begin{aligned} \text{S} \subseteq \text{SP} \{\mathcal{U}\} \{\mathcal{W}\} \{\mathcal{K}\} \{(\text{lift-alg } \mathbf{A} \mathcal{W})\} (\text{sbase}\{\mathbf{A}\} x) &= \\ \text{siso splIA} (\text{sym-}\cong \text{ lift-alg-}\cong) & \end{aligned}$$

where

$$\begin{aligned} \text{IIA} &: \text{Algebra} (\mathcal{U} \sqcup \mathcal{W}) S \\ \text{IIA} &= \text{lift-alg} (\text{lift-alg } \mathbf{A} \mathcal{W}) (\mathcal{U} \sqcup \mathcal{W}) \end{aligned}$$

$$\begin{aligned} \text{splIA} &: \text{IIA} \in \text{S}\{\mathcal{U} \sqcup \mathcal{W}\}\{\mathcal{U} \sqcup \mathcal{W}\} (\text{P}\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K}) \\ \text{splIA} &= \text{sbase}\{\mathcal{U} = (\mathcal{U} \sqcup \mathcal{W})\}\{\mathcal{W} = (\mathcal{U} \sqcup \mathcal{W})\} (\text{pbase } x) \end{aligned}$$

$$\begin{aligned} \text{S} \subseteq \text{SP} \{\mathcal{U}\} \{\mathcal{W}\} \{\mathcal{K}\} \{(\text{lift-alg } \mathbf{A} \mathcal{W})\} (\text{slift}\{\mathbf{A}\} x) &= \\ \text{subalgebra} \rightarrow \text{S}\{\mathcal{U} \sqcup \mathcal{W}\}\{\mathcal{U} \sqcup \mathcal{W}\} \{\text{P}\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K}\} \{\text{lift-alg } \mathbf{A} \mathcal{W}\} \text{IAsc} & \end{aligned}$$

where

$$\begin{aligned} \text{splAu} &: \mathbf{A} \in \text{S}\{\mathcal{U}\}\{\mathcal{U}\} (\text{P}\{\mathcal{U}\}\{\mathcal{U}\} \mathcal{K}) \\ \text{splAu} &= \text{S} \subseteq \text{SP}\{\mathcal{U}\}\{\mathcal{U}\} x \end{aligned}$$

$$\begin{aligned} \text{Asc} &: \mathbf{A} \text{ IsSubalgebraOfClass} (\text{P}\{\mathcal{U}\}\{\mathcal{U}\} \mathcal{K}) \\ \text{Asc} &= \text{S} \rightarrow \text{subalgebra}\{\mathcal{U}\}\{\text{P}\{\mathcal{U}\}\{\mathcal{U}\} \mathcal{K}\}\{\mathbf{A}\} \text{splAu} \end{aligned}$$

$$\begin{aligned} \text{IAsc} &: (\text{lift-alg } \mathbf{A} \mathcal{W}) \text{ IsSubalgebraOfClass} (\text{P}\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K}) \\ \text{IAsc} &= \text{lift-alg-subP Asc} \end{aligned}$$

$$\begin{aligned} \text{S} \subseteq \text{SP} \{\mathcal{U}\} \{\mathcal{W}\} \{\mathcal{K}\} \{\mathbf{B}\} (\text{ssub}\{\mathbf{A}\} sA B \leq A) &= \\ \text{ssub}\{\mathcal{U} \sqcup \mathcal{W}\}\{\mathcal{U} \sqcup \mathcal{W}\} \text{IAsp} (\text{lift-alg-sub-lift } \mathbf{A} B \leq A) & \end{aligned}$$

where

$$\begin{aligned} \text{IA} &: \text{Algebra} (\mathcal{U} \sqcup \mathcal{W}) S \\ \text{IA} &= \text{lift-alg } \mathbf{A} \mathcal{W} \end{aligned}$$

$$\begin{aligned} \text{splAu} &: \mathbf{A} \in \text{S}\{\mathcal{U}\}\{\mathcal{U}\} (\text{P}\{\mathcal{U}\}\{\mathcal{U}\} \mathcal{K}) \\ \text{splAu} &= \text{S} \subseteq \text{SP}\{\mathcal{U}\}\{\mathcal{U}\} sA \end{aligned}$$

$$\begin{aligned} \text{Asc} &: \mathbf{A} \text{ IsSubalgebraOfClass} (\text{P}\{\mathcal{U}\}\{\mathcal{U}\} \mathcal{K}) \\ \text{Asc} &= \text{S} \rightarrow \text{subalgebra}\{\mathcal{U}\}\{\text{P}\{\mathcal{U}\}\{\mathcal{U}\} \mathcal{K}\}\{\mathbf{A}\} \text{splAu} \end{aligned}$$

$$\begin{aligned} \text{IAsc} &: \text{IA} \text{ IsSubalgebraOfClass} (\text{P}\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K}) \\ \text{IAsc} &= \text{lift-alg-subP Asc} \end{aligned}$$

$$\begin{aligned} \text{IAsp} &: \text{IA} \in \text{S}\{\mathcal{U} \sqcup \mathcal{W}\}\{\mathcal{U} \sqcup \mathcal{W}\} (\text{P}\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K}) \\ \text{IAsp} &= \text{subalgebra} \rightarrow \text{S}\{\mathcal{U} \sqcup \mathcal{W}\}\{\mathcal{U} \sqcup \mathcal{W}\} \{\text{P}\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K}\} \{\text{IA}\} \text{IAsc} \end{aligned}$$

$$\text{S} \subseteq \text{SP} \{\mathcal{U}\} \{\mathcal{W}\} \{\mathcal{K}\} \{\mathbf{B}\} (\text{ssubw}\{\mathbf{A}\} sA B \leq A) = \gamma$$

where

```

spA : A ∈ S{U ⊔ W}{U ⊔ W} (P{U}{W} K)
spA = S⊆SP sA
γ : B ∈ S{U ⊔ W}{U ⊔ W} (P{U}{W} K)
γ = ssubw{U ⊔ W}{U ⊔ W} spA B≤A

S⊆SP {U} {W} {K} {B} (siso{A} sA A≅B) = siso{U ⊔ W}{U ⊔ W} IAsp IA≅B
where
IA : Algebra (U ⊔ W) S
IA = lift-alg A W

splAu : A ∈ S{U}{U} (P{U}{U} K)
splAu = S⊆SP{U}{U} sA

IAsc : IA IsSubalgebraOfClass (P{U}{W} K)
IAsc = lift-alg-subP (S→subalgebra{U}{P{U}{U} K}{A} splAu)

IAsp : IA ∈ S{U ⊔ W}{U ⊔ W} (P{U}{W} K)
IAsp = subalgebra→S{U ⊔ W}{U ⊔ W}{P{U}{W} K}{IA} IAsc

IA≅B : IA ≅ B
IA≅B = Trans≅ IA B (sym≅ lift-alg≅) A≅B

```

We need to formalize one more lemma before arriving the short term objective of this section, which is the proof of the inclusion $PS \subseteq SP$.

```

lemPS⊆SP : {U W : Universe}{K : Pred (Algebra U S)}(ov U){hfe : hfunext W U}
→ {I : W → Algebra U S}
→ (∀ i → (B i) IsSubalgebraOfClass K)
→ ∏ B IsSubalgebraOfClass (P{U}{W} K)

```

```

lemPS⊆SP {U}{W}{K}{hfe}{I}{B} B≤K = ∏ A , (∏ SA , ∏ SA≤A ) , ξ , γ

```

where

```

A : I → Algebra U S
A = λ i → | B≤K i |

SA : I → Algebra U S
SA = λ i → | fst || B≤K i || |

KA : ∀ i → A i ∈ K
KA = λ i → | snd || B≤K i || |

B≅SA : ∀ i → B i ≅ SA i
B≅SA = λ i → || snd || B≤K i || |

pA : ∀ i → lift-alg (A i) W ∈ P{U}{W} K
pA = λ i → pbase (KA i)

SA≤A : ∀ i → (SA i) IsSubalgebraOfClass (A i)
SA≤A = λ i → snd | || B≤K i || |

h : ∀ i → | SA i | → | A i |
h = λ i → | SA≤A i |

```

$$\prod SA \leq \prod \mathcal{A} : \prod SA \leq \prod \mathcal{A}$$

$$\prod SA \leq \prod \mathcal{A} = i, ii, iii$$

where

$$i : |\prod SA| \rightarrow |\prod \mathcal{A}|$$

$$i = \lambda x i \rightarrow (h i) (x i)$$

ii : is-embedding i

$$ii = \text{embedding-lift} \{ \mathcal{Q} = \mathcal{U} \} \{ \mathcal{U} = \mathcal{U} \} \{ \mathcal{F} = \mathcal{W} \} hfe hfe \{ I \} \{ SA \} \{ \mathcal{A} \} h (\lambda i \rightarrow \text{fst} \parallel SA \leq \mathcal{A} i \parallel)$$

iii : is-homomorphism $(\prod SA) (\prod \mathcal{A}) i$

$$iii = \lambda f a \rightarrow gfe \lambda i \rightarrow (\text{snd} \parallel SA \leq \mathcal{A} i \parallel) f (\lambda x \rightarrow a x i)$$

$$\xi : \prod \mathcal{A} \in P \mathcal{K}$$

$$\xi = \text{produ} \{ \mathcal{U} \} \{ \mathcal{W} \} \{ I = I \} \{ \mathcal{A} = \mathcal{A} \} (\lambda i \rightarrow P\text{-expa} (KA i))$$

$$\gamma : \prod \mathcal{B} \cong \prod SA$$

$$\gamma = \prod \cong gfe B \cong SA$$

7.3.6 $PS(\mathcal{K}) \subseteq SP(\mathcal{K})$

Finally, we are in a position to prove that a product of subalgebras of algebras in a class \mathcal{K} is a subalgebra of a product of algebras in \mathcal{K} .

module $_ \{ \mathcal{U} : \text{Universe} \} \{ \mathcal{K} : \text{Pred} (\text{Algebra } \mathcal{U} S) (\text{ov } \mathcal{U}) \} \{ hfe : \text{hfunext} (\text{ov } \mathcal{U}) (\text{ov } \mathcal{U}) \}$ where

ov \mathcal{U} : Universe

ov \mathcal{U} = ov \mathcal{U}

$$PS \subseteq SP : (P \{ \text{ov}\mathcal{U} \} \{ \text{ov}\mathcal{U} \} (S \{ \mathcal{U} \} \{ \text{ov}\mathcal{U} \} \mathcal{K})) \subseteq (S \{ \text{ov}\mathcal{U} \} \{ \text{ov}\mathcal{U} \} (P \{ \mathcal{U} \} \{ \text{ov}\mathcal{U} \} \mathcal{K}))$$

$$PS \subseteq SP (\text{pbase} (\text{sbase } x)) = \text{sbase} (\text{pbase } x)$$

$$PS \subseteq SP (\text{pbase} (\text{slift} \{ \mathbf{A} \} x)) = \text{slift} (S \subseteq SP \{ \mathcal{U} \} \{ \text{ov}\mathcal{U} \} \{ \mathcal{K} \} (\text{slift } x))$$

$$PS \subseteq SP (\text{pbase} \{ \mathbf{B} \} (\text{ssub} \{ \mathbf{A} \} sA B \leq A)) =$$

$$\text{siso} (\text{ssub} \{ \mathcal{U} = \text{ov}\mathcal{U} \} (S \subseteq SP \{ \mathcal{U} \} \{ \text{ov}\mathcal{U} \} \{ \mathcal{K} \} (\text{slift } sA)) (\text{lift-alg-}\leq \mathbf{B} \{ \mathbf{A} \} B \leq A)) \text{ refl-}\cong$$

$$PS \subseteq SP (\text{pbase} \{ \mathbf{B} \} (\text{ssubw} \{ \mathbf{A} \} sA B \leq A)) =$$

$$\text{ssub} \{ \mathcal{U} = \text{ov}\mathcal{U} \} (\text{slift} \{ \text{ov}\mathcal{U} \} \{ \text{ov}\mathcal{U} \} (S \subseteq SP sA)) (\text{lift-alg-}\leq \mathbf{B} \{ \mathbf{A} \} B \leq A)$$

$$PS \subseteq SP (\text{pbase} (\text{siso} \{ \mathbf{A} \} \{ \mathbf{B} \} x A \cong B)) = \text{siso} (S \subseteq SP (\text{slift } x)) (\text{lift-alg-iso } \mathcal{U} \text{ ov}\mathcal{U} \mathbf{A} \mathbf{B} A \cong B)$$

$$PS \subseteq SP (\text{pliftu } x) = \text{slift} (PS \subseteq SP x)$$

$$PS \subseteq SP (\text{pliftw } x) = \text{slift} (PS \subseteq SP x)$$

$$PS \subseteq SP (\text{produ} \{ I \} \{ \mathcal{A} \} x) = \gamma$$

where

$$\xi : (i : I) \rightarrow (\mathcal{A} i) \text{ IsSubalgebraOfClass } (P \{ \mathcal{U} \} \{ \text{ov}\mathcal{U} \} \mathcal{K})$$

$$\xi i = S \rightarrow \text{subalgebra} \{ \mathcal{K} = (P \mathcal{K}) \} (PS \subseteq SP (x i))$$

$$\eta' : \prod \mathcal{A} \text{ IsSubalgebraOfClass } (P \{ \text{ov}\mathcal{U} \} \{ \text{ov}\mathcal{U} \} (P \{ \mathcal{U} \} \{ \text{ov}\mathcal{U} \} \mathcal{K}))$$

$$\eta' = \text{lemPS} \subseteq SP \{ \mathcal{U} = \text{ov}\mathcal{U} \} \{ \text{ov}\mathcal{U} \} \{ \mathcal{K} = (P \mathcal{K}) \} \{ hfe \} \{ I = I \} \{ \mathcal{B} = \mathcal{A} \} \xi$$

$$\eta : \prod \mathcal{A} \in S \{ \text{ov}\mathcal{U} \} \{ \text{ov}\mathcal{U} \} (P \{ \text{ov}\mathcal{U} \} \{ \text{ov}\mathcal{U} \} (P \{ \mathcal{U} \} \{ \text{ov}\mathcal{U} \} \mathcal{K}))$$

$$\eta = \text{subalgebra} \rightarrow S \{ \mathcal{U} = (\text{ov}\mathcal{U}) \} \{ \mathcal{W} = \text{ov}\mathcal{U} \} \{ \mathcal{K} = (P (P \mathcal{K})) \} \{ C = \prod \mathcal{A} \} \eta'$$

$$\gamma : \prod \mathcal{A} \in S \{ \text{ov}\mathcal{U} \} \{ \text{ov}\mathcal{U} \} (P \{ \mathcal{U} \} \{ \text{ov}\mathcal{U} \} \mathcal{K})$$

$$\gamma = (S\text{-mono} \{ \mathcal{U} = \text{ov}\mathcal{U} \} \{ \mathcal{K} = (P (P \mathcal{K})) \} \{ \mathcal{K}' = (P \mathcal{K}) \} (P\text{-idemp})) \eta$$


```

PSCSP (prodw{I}{A} x) = γ
where
  ξ : (i : I) → (A i) IsSubalgebraOfClass (P{U}{OvU} K)
  ξ i = S→subalgebra{K = (P K)} (PSCSP (x i))

  η' : ∏ A IsSubalgebraOfClass (P{OvU}{OvU} (P{U}{OvU} K))
  η' = lemPSCSP{U = OvU}{OvU}{K = (P K)}{hfe}{I = I}{B = A} ξ

  η : ∏ A ∈ S{OvU}{OvU} (P{OvU}{OvU} (P{U}{OvU} K))
  η = subalgebra→S{U = (OvU)}{W = OvU}{K = (P (P K))}{C = ∏ A} η'

  γ : ∏ A ∈ S{OvU}{OvU} (P{U}{OvU} K)
  γ = (S-mono{U = OvU}{K = (P (P K))}{K' = (P K)} (P-idemp)) η

PSCSP (pisou{A}{B} pA A≅B) = siso{OvU}{OvU}{P{U}{OvU} K}{A}{B} (PSCSP pA) A≅B
PSCSP (pisow{A}{B} pA A≅B) = siso{OvU}{OvU}{P{U}{OvU} K}{A}{B} (PSCSP pA) A≅B

```

7.3.7 More class inclusions

Here we prove three more inclusion relations (which will have bit parts to play in the formal proof of Birkhoff's Theorem).

```

PCV : {U W : Universe}{K : Pred (Algebra U S)(ov U)} → P{U}{W} K ⊆ V{U}{W} K
PCV (pbase x) = vbase x
PCV{U} (pliftu x) = vlift (PCV{U}{U} x)
PCV{U}{W} (pliftw x) = vliftw (PCV{U}{W} x)
PCV (produ x) = vprodu (λ i → PCV (x i))
PCV (prodw x) = vprodw (λ i → PCV (x i))
PCV (pisou x x1) = visou (PCV x) x1
PCV (pisow x x1) = visow (PCV x) x1

SPCV : {U W : Universe}{K : Pred (Algebra U S)(ov U)}
  → S{U □ W}{U □ W} (P{U}{W} K) ⊆ V{U}{W} K
SPCV (sbase{A} PCloA) = PCV (pisow PCloA lift-alg-≅)
SPCV (slift{A} x) = vliftw (SPCV x)
SPCV{U}{W}{K} (ssub{A}{B} spA B≤A) = vssubw (SPCV spA) B≤A
SPCV{U}{W}{K} (ssubw{A}{B} spA B≤A) = vssubw (SPCV spA) B≤A
SPCV (siso x x1) = visow (SPCV x) x1

```

7.3.8 Products of classes

Next we formally state and prove that, given an arbitrary class \mathcal{K} of algebras, the product of all algebras in the class $S(\mathcal{K})$ belongs to $SP(\mathcal{K})$. That is, $\prod S(\mathcal{K}) \in SP(\mathcal{K})$. This turns out to be a nontrivial exercise. In fact, it is not even immediately obvious (at least not to this author) how one expresses the product of an entire class of algebras as a dependent type. Nonetheless, after a number of failed attempts, the right type revealed itself. (Not surprisingly, now that we have it, it seems almost obvious.)

```

module class-product {U : Universe}{K : Pred (Algebra U S)(ov U)} where

```

First, we define the type that will serve to index the class (as well as the product of its members), as follows.

$$\begin{aligned} \mathcal{J} &: \{\mathcal{U} : \text{Universe}\} \rightarrow \text{Pred} (\text{Algebra } \mathcal{U} \ S)(\text{ov } \mathcal{U}) \rightarrow (\text{ov } \mathcal{U}) \cdot \\ \mathcal{J} \{\mathcal{U}\} \mathcal{K} &= \Sigma \mathbf{A} : (\text{Algebra } \mathcal{U} \ S), \mathbf{A} \in \mathcal{K} \end{aligned}$$

Taking the product over this index type \mathcal{J} requires a function like the following, which takes an index ($i : \mathcal{J}$) and returns the corresponding algebra.

$$\begin{aligned} \mathfrak{A} &: \{\mathcal{U} : \text{Universe}\} \{\mathcal{K} : \text{Pred} (\text{Algebra } \mathcal{U} \ S)(\text{ov } \mathcal{U})\} \rightarrow \mathcal{J} \mathcal{K} \rightarrow \text{Algebra } \mathcal{U} \ S \\ \mathfrak{A} \{\mathcal{U}\} \{\mathcal{K}\} &= \lambda (i : (\mathcal{J} \mathcal{K})) \rightarrow | i | \end{aligned}$$

Finally, the product of all members of \mathcal{K} is represented by the following type.

$$\begin{aligned} \text{class-product} &: \{\mathcal{U} : \text{Universe}\} \rightarrow \text{Pred} (\text{Algebra } \mathcal{U} \ S)(\text{ov } \mathcal{U}) \rightarrow \text{Algebra } (\text{ov } \mathcal{U}) \ S \\ \text{class-product } \{\mathcal{U}\} \mathcal{K} &= \prod (\mathfrak{A} \{\mathcal{U}\} \{\mathcal{K}\}) \end{aligned}$$

Alternatively, we could have defined the class product in a way that explicitly displays the index, like so.

$$\begin{aligned} \text{class-product}' &: \{\mathcal{U} : \text{Universe}\} \rightarrow \text{Pred} (\text{Algebra } \mathcal{U} \ S)(\text{ov } \mathcal{U}) \rightarrow \text{Algebra } (\text{ov } \mathcal{U}) \ S \\ \text{class-product}' \{\mathcal{U}\} \mathcal{K} &= \prod \lambda (i : (\Sigma \mathbf{A} : (\text{Algebra } \mathcal{U} \ S), \mathbf{A} \in \mathcal{K})) \rightarrow | i | \end{aligned}$$

If $p : \mathbf{A} \in \mathcal{K}$ is a proof that \mathbf{A} belongs to \mathcal{K} , then we can view the pair $(\mathbf{A}, p) \in \mathcal{J} \mathcal{K}$ as an index over the class, and $\mathfrak{A}(\mathbf{A}, p)$ as the result of projecting the product onto the (\mathbf{A}, p) -th component.

7.3.9 $\prod \mathbf{S}(\mathcal{K}) \in \mathbf{SP}(\mathcal{K})$

Thus, the (informal) product $\prod \mathbf{S}(\mathcal{K})$ of all subalgebras of algebras in \mathcal{K} is implemented (formally) in the UALib as $\prod (\mathfrak{A} \{\mathcal{U}\} \{\mathbf{S}(\mathcal{K})\})$, and our goal is to prove that this product belongs to $\mathbf{SP}(\mathcal{K})$. This is done in the UALib by first proving that the product belongs to $\mathbf{PS}(\mathcal{K})$ (see the proof of `class-prod-s- \in -ps` in `UALib.Varieties`) and then applying the `PS \subseteq SP` lemma described above.

– *The product of all subalgebras of a class \mathcal{K} belongs to $\mathbf{SP}(\mathcal{K})$.*

```

module class-product-inclusions { $\mathcal{U} : \text{Universe}$ } { $\mathcal{K} : \text{Pred} (\text{Algebra } \mathcal{U} \ S)(\text{OV } \mathcal{U})$ } where

  open class-product { $\mathcal{U} = \mathcal{U}$ } { $\mathcal{K} = \mathcal{K}$ }

  class-prod-s- $\in$ -ps : class-product (S{ $\mathcal{U}$ } { $\mathcal{U}$ }  $\mathcal{K}$ )  $\in$  (P{OV  $\mathcal{U}$ } {OV  $\mathcal{U}$ } (S{ $\mathcal{U}$ } {OV  $\mathcal{U}$ }  $\mathcal{K}$ ))

  class-prod-s- $\in$ -ps = pisou{ $\mathcal{U} = (\text{OV } \mathcal{U})$ } { $\mathcal{W} = (\text{OV } \mathcal{U})$ } ps $\prod$ IIA  $\prod$ IIA $\cong$ cpK
  where
    I : (OV  $\mathcal{U}$ )  $\cdot$ 
    I =  $\mathcal{J}$  (S{ $\mathcal{U}$ } { $\mathcal{U}$ }  $\mathcal{K}$ )

    sA : (i : I)  $\rightarrow$  ( $\mathfrak{A}$  i)  $\in$  (S{ $\mathcal{U}$ } { $\mathcal{U}$ }  $\mathcal{K}$ )
    sA i = || i ||

    IA IIA : I  $\rightarrow$  Algebra (OV  $\mathcal{U}$ ) S
    IA i = lift-alg ( $\mathfrak{A}$  i) (OV  $\mathcal{U}$ )
    IIA i = lift-alg (IA i) (OV  $\mathcal{U}$ )

    sIA : (i : I)  $\rightarrow$  (IA i)  $\in$  (S{ $\mathcal{U}$ } {(OV  $\mathcal{U}$ )}  $\mathcal{K}$ )
    sIA i = siso (sA i) lift-alg- $\cong$ 

```

```
psIIA : (i : I) → (IIA i) ∈ (P{OV  $\mathcal{U}$ }{OV  $\mathcal{U}$ } (S{ $\mathcal{U}$ }{(OV  $\mathcal{U}$ )}  $\mathcal{K}$ ))
psIIA i = pbase{ $\mathcal{U}$  = (OV  $\mathcal{U}$ )}{ $\mathcal{W}$  = (OV  $\mathcal{U}$ )} (sIA i)
```

```
ps $\prod$ IIA :  $\prod$  IIA ∈ P{OV  $\mathcal{U}$ }{OV  $\mathcal{U}$ } (S{ $\mathcal{U}$ }{(OV  $\mathcal{U}$ )}  $\mathcal{K}$ )
ps $\prod$ IIA = produ{ $\mathcal{U}$  = (OV  $\mathcal{U}$ )}{ $\mathcal{W}$  = (OV  $\mathcal{U}$ )} psIIA
```

```
IIA $\cong$ A : (i : I) → (IIA i)  $\cong$  ( $\mathfrak{A}$  i)
IIA $\cong$ A i = Trans- $\cong$  (IIA i) ( $\mathfrak{A}$  i) (sym- $\cong$  lift- $\text{alg-}\cong$ ) (sym- $\cong$  lift- $\text{alg-}\cong$ )
```

```
 $\prod$ IIA $\cong$ cpK :  $\prod$  IIA  $\cong$  class-product (S{ $\mathcal{U}$ }{ $\mathcal{U}$ }  $\mathcal{K}$ )
 $\prod$ IIA $\cong$ cpK =  $\prod$  $\cong$  gfe IIA $\cong$ A
```

– $PS \subseteq SP$, so the product of all subalgebras of algebras in \mathcal{K} belongs to $SP(\mathcal{K})$.

```
class-prod-s- $\in$ -sp : hfunext (OV  $\mathcal{U}$ ) (OV  $\mathcal{U}$ )
→ class-product (S{ $\mathcal{U}$ }{ $\mathcal{U}$ }  $\mathcal{K}$ ) ∈ (S{OV  $\mathcal{U}$ }{OV  $\mathcal{U}$ } (P{ $\mathcal{U}$ }{OV  $\mathcal{U}$ }  $\mathcal{K}$ ))
```

```
class-prod-s- $\in$ -sp hfe = PS $\subseteq$ SP{hfe = hfe} (class-prod-s- $\in$ -ps)
```

7.4 Equation Preservation Theorems

This subsection presents the `UALib.Varieties.Preservation` submodule of the Agda `UALib`. In this module we show that identities are preserved by closure operators `H`, `S`, and `P`. This will establish the easy direction of Birkhoff's HSP Theorem.

```
open import UALib.Algebras using (Signature;  $\mathfrak{G}$ ;  $\mathcal{V}$ ; Algebra;  $\_ \rightarrow \_$ )
open import UALib.Prelude.Preliminaries using (global-dfunext; Universe;  $\_ \cdot$ )

module UALib.Varieties.Preservation
  {S : Signature  $\mathfrak{G}$   $\mathcal{V}$ }{gfe : global-dfunext}
  { $\mathcal{X}$  : { $\mathcal{U}$   $\mathfrak{X}$  : Universe}{X :  $\mathfrak{X}$   $\cdot$ }(A : Algebra  $\mathcal{U}$  S) → X → A}
  where
    open import UALib.Varieties.Varieties {S = S}{gfe}{ $\mathcal{X}$ } public
```

7.4.1 H preserves identities

– H preserves identities

```
H-id1 : { $\mathcal{U}$   $\mathfrak{X}$  : Universe}{X :  $\mathfrak{X}$   $\cdot$ }
  { $\mathcal{K}$  : Pred (Algebra  $\mathcal{U}$  S)(OV  $\mathcal{U}$ )}
  (p q : Term{ $\mathfrak{X}$ }{X})
  -----
  → ( $\mathcal{K} \models p \approx q$ ) → (H{ $\mathcal{U}$ }{ $\mathcal{U}$ }  $\mathcal{K} \models p \approx q$ )
```

```
H-id1 p q  $\alpha$  (hbase x) = lift- $\text{alg-}\models \_ p q (\alpha x)$ 
```

```
H-id1 { $\mathcal{U}$ } p q  $\alpha$  (hlift{A} x) =  $\gamma$ 
```

where

```
 $\beta$  : A  $\models p \approx q$ 
 $\beta$  = H-id1 p q  $\alpha$  x
 $\gamma$  : lift- $\text{alg}$  A  $\mathcal{U} \models p \approx q$ 
```

$$\gamma = \text{lift-alg-}\models _ p q \beta$$

$$\text{H-id1 } p q \alpha (\text{hhimg}\{\mathbf{A}\}\{\mathbf{C}\} \text{ HA } ((\mathbf{B}, \phi, (\phi\text{hom}, \phi\text{sur})), B \cong C)) = \models \cong p q \gamma B \cong C$$

where

$$\beta : \mathbf{A} \models p \approx q$$

$$\beta = (\text{H-id1 } p q \alpha) \text{ HA}$$

$$\text{preim} : \forall \mathbf{b} x \rightarrow | \mathbf{A} |$$

$$\text{preim } \mathbf{b} x = (\text{Inv } \phi (\mathbf{b} x) (\phi\text{sur } (\mathbf{b} x)))$$

$$\zeta : \forall \mathbf{b} \rightarrow \phi \circ (\text{preim } \mathbf{b}) \equiv \mathbf{b}$$

$$\zeta \mathbf{b} = \text{gfe } \lambda x \rightarrow \text{InvlInv } \phi (\mathbf{b} x) (\phi\text{sur } (\mathbf{b} x))$$

$$\gamma : (p \cdot \mathbf{B}) \equiv (q \cdot \mathbf{B})$$

$$\gamma = \text{gfe } \lambda \mathbf{b} \rightarrow$$

$$(p \cdot \mathbf{B}) \mathbf{b} \equiv \langle (\text{ap } (p \cdot \mathbf{B}) (\zeta \mathbf{b}))^{-1} \rangle$$

$$(p \cdot \mathbf{B}) (\phi \circ (\text{preim } \mathbf{b})) \equiv \langle (\text{comm-hom-term } \text{gfe } \mathbf{A} \mathbf{B} (\phi, \phi\text{hom}) p (\text{preim } \mathbf{b}))^{-1} \rangle$$

$$\phi((p \cdot \mathbf{A})(\text{preim } \mathbf{b})) \equiv \langle \text{ap } \phi (\text{intensionality } \beta (\text{preim } \mathbf{b})) \rangle$$

$$\phi((q \cdot \mathbf{A})(\text{preim } \mathbf{b})) \equiv \langle \text{comm-hom-term } \text{gfe } \mathbf{A} \mathbf{B} (\phi, \phi\text{hom}) q (\text{preim } \mathbf{b}) \rangle$$

$$(q \cdot \mathbf{B})(\phi \circ (\text{preim } \mathbf{b})) \equiv \langle \text{ap } (q \cdot \mathbf{B}) (\zeta \mathbf{b}) \rangle$$

$$(q \cdot \mathbf{B}) \mathbf{b} \quad \blacksquare$$

$$\text{H-id1 } p q \alpha (\text{hiso}\{\mathbf{A}\}\{\mathbf{B}\} x x_1) = \models \text{-transport } p q (\text{H-id1 } p q \alpha x) x_1$$

The converse is almost too obvious to bother with. Nonetheless, we formalize it for completeness.

$$\text{H-id2} : \{\mathcal{U} \mathcal{W} \mathcal{X} : \text{Universe}\}\{X : \mathcal{X} \cdot\}\{\mathcal{K} : \text{Pred } (\text{Algebra } \mathcal{U} S)(\text{OV } \mathcal{U})\}$$

$$\{p q : \text{Term}\{\mathcal{X}\}\{X\}\} \rightarrow (\text{H}\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K} \models p \approx q) \rightarrow (\mathcal{K} \models p \approx q)$$

$$\text{H-id2 } \{\mathcal{U}\}\{\mathcal{W}\}\{\mathcal{X}\}\{X\} \{\mathcal{K}\} \{p\}\{q\} \text{Hpq } \{\mathbf{A}\} \text{KA} = \gamma$$

where

$$\text{IA} : \text{Algebra } (\mathcal{U} \sqcup \mathcal{W}) S$$

$$\text{IA} = \text{lift-alg } \mathbf{A} \mathcal{W}$$

$$\text{pIA} : \text{IA} \in \text{H}\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K}$$

$$\text{pIA} = \text{hbase } \text{KA}$$

$$\xi : \text{IA} \models p \approx q$$

$$\xi = \text{Hpq } \text{pIA}$$

$$\gamma : \mathbf{A} \models p \approx q$$

$$\gamma = \text{lower-alg-}\models \mathbf{A} p q \xi$$

7.4.2 S preserves identities

$$\text{S-id1} : \{\mathcal{U} \mathcal{X} : \text{Universe}\}\{X : \mathcal{X} \cdot\}$$

$$(\mathcal{K} : \text{Pred } (\text{Algebra } \mathcal{U} S)(\text{OV } \mathcal{U}))$$

$$(p q : \text{Term}\{\mathcal{X}\}\{X\})$$

$$\rightarrow (\mathcal{K} \models p \approx q) \rightarrow (\text{S}\{\mathcal{U}\}\{\mathcal{U}\} \mathcal{K} \models p \approx q)$$

$$\text{S-id1 } _ p q \alpha (\text{sbase } x) = \text{lift-alg-}\models _ p q (\alpha x)$$

S-id1 $\mathcal{K} p q \alpha$ (**slift** x) = **lift-alg- \models** $_ p q$ ((**S-id1** $\mathcal{K} p q \alpha$) x)

S-id1 $\mathcal{K} p q \alpha$ (**ssub**{**A**}{**B**} $sA B \leq A$) =
S- \models $p q$ ((**B** , **A** , (**B** , $B \leq A$) , **inj₂** **refl** , **id \cong**)) γ
where -Apply **S- \models** to the class $\mathcal{K} \cup \{ \mathbf{A} \}$
 $\beta : \mathbf{A} \models p \approx q$
 $\beta = \mathbf{S-id1} \mathcal{K} p q \alpha sA$

Apq : { **A** } $\models p \approx q$
Apq (**refl** $_$) = β

 $\gamma : (\mathcal{K} \cup \{ \mathbf{A} \}) \models p \approx q$
 $\gamma \{ \mathbf{B} \} (\mathbf{inj}_1 x) = \alpha x$
 $\gamma \{ \mathbf{B} \} (\mathbf{inj}_2 y) = \mathbf{Apq} y$

S-id1 $\mathcal{K} p q \alpha$ (**ssubw**{**A**}{**B**} $sA B \leq A$) =
S- \models $p q$ ((**B** , **A** , (**B** , $B \leq A$) , **inj₂** **refl** , **id \cong**)) γ
where -Apply **S- \models** to the class $\mathcal{K} \cup \{ \mathbf{A} \}$
 $\beta : \mathbf{A} \models p \approx q$
 $\beta = \mathbf{S-id1} \mathcal{K} p q \alpha sA$

Apq : { **A** } $\models p \approx q$
Apq (**refl** $_$) = β

 $\gamma : (\mathcal{K} \cup \{ \mathbf{A} \}) \models p \approx q$
 $\gamma \{ \mathbf{B} \} (\mathbf{inj}_1 x) = \alpha x$
 $\gamma \{ \mathbf{B} \} (\mathbf{inj}_2 y) = \mathbf{Apq} y$

S-id1 $\mathcal{K} p q \alpha$ (**siso**{**A**}{**B**} $x x_1$) = γ
where
 $\zeta : \mathbf{A} \models p \approx q$
 $\zeta = \mathbf{S-id1} \mathcal{K} p q \alpha x$
 $\gamma : \mathbf{B} \models p \approx q$
 $\gamma = \models\text{-transport } p q \zeta x_1$

Again, the obvious converse is barely worth the bits needed to formalize it.

S-id2 : {**U** **W** **X** : **Universe**} { $X : \mathbf{X} \cdot$ } { $\mathcal{K} : \mathbf{Pred} (\mathbf{Algebra} \mathbf{U} S)(\mathbf{OV} \mathbf{U})$ }
 $\{ p q : \mathbf{Term} \{ \mathbf{X} \} \{ X \} \} \rightarrow (\mathbf{S} \{ \mathbf{U} \} \{ \mathbf{W} \} \mathcal{K} \models p \approx q) \rightarrow (\mathcal{K} \models p \approx q)$
S-id2 {**U**}{**W**}{**X**}{ X } { \mathcal{K} } { p }{ q } **Spg** {**A**} $KA = \gamma$
where
IA : **Algebra** (**U** \sqcup **W**) S
IA = **lift-alg** **A** **W**

plA : **IA** $\in \mathbf{S} \{ \mathbf{U} \} \{ \mathbf{W} \} \mathcal{K}$
plA = **sbase** KA

 $\xi : \mathbf{IA} \models p \approx q$
 $\xi = \mathbf{Spg} \mathbf{plA}$
 $\gamma : \mathbf{A} \models p \approx q$
 $\gamma = \mathbf{lower-alg-}\models \mathbf{A} p q \xi$

7.4.3 P preserves identities

P-id1 : $\{\mathcal{U} \mathfrak{X} : \text{Universe}\}\{X : \mathfrak{X} \cdot\}$
 $\{\mathcal{K} : \text{Pred}(\text{Algebra } \mathcal{U} S)(\text{OV } \mathcal{U})\}$
 $(p \ q : \text{Term}\{\mathfrak{X}\}\{X\})$

→ $(\mathcal{K} \models p \approx q) \rightarrow (\text{P}\{\mathcal{U}\}\{\mathcal{U}\} \mathcal{K} \models p \approx q)$

P-id1 $p \ q \ \alpha \ (\text{pbase } x) = \text{lift-alg} \models _ \ p \ q \ (\alpha \ x)$

P-id1 $p \ q \ \alpha \ (\text{pliftu } x) = \text{lift-alg} \models _ \ p \ q \ ((\text{P-id1 } p \ q \ \alpha) \ x)$

P-id1 $p \ q \ \alpha \ (\text{pliftw } x) = \text{lift-alg} \models _ \ p \ q \ ((\text{P-id1 } p \ q \ \alpha) \ x)$

P-id1 $\{\mathcal{U}\} \{\mathfrak{X}\} \ p \ q \ \alpha \ (\text{produ}\{I\}\{\mathcal{A}\} \ x) = \gamma$

where

IA : $I \rightarrow \text{Algebra } \mathcal{U} S$

IA $i = (\text{lift-alg} \ (\mathcal{A} \ i) \ \mathcal{U})$

IH : $(i : I) \rightarrow (p \cdot (\text{IA } i)) \equiv (q \cdot (\text{IA } i))$

IH $i = \text{lift-alg} \models (\mathcal{A} \ i) \ p \ q \ ((\text{P-id1 } p \ q \ \alpha) \ (x \ i))$

$\gamma : p \cdot (\prod \mathcal{A}) \equiv q \cdot (\prod \mathcal{A})$

$\gamma = \text{lift-products-preserve-ids } p \ q \ I \ \mathcal{A} \ \text{IH}$

P-id1 $\{\mathcal{U}\} \ p \ q \ \alpha \ (\text{prodw}\{I\}\{\mathcal{A}\} \ x) = \gamma$

where

IA : $I \rightarrow \text{Algebra } \mathcal{U} S$

IA $i = (\text{lift-alg} \ (\mathcal{A} \ i) \ \mathcal{U})$

IH : $(i : I) \rightarrow (p \cdot (\text{IA } i)) \equiv (q \cdot (\text{IA } i))$

IH $i = \text{lift-alg} \models (\mathcal{A} \ i) \ p \ q \ ((\text{P-id1 } p \ q \ \alpha) \ (x \ i))$

$\gamma : p \cdot (\prod \mathcal{A}) \equiv q \cdot (\prod \mathcal{A})$

$\gamma = \text{lift-products-preserve-ids } p \ q \ I \ \mathcal{A} \ \text{IH}$

P-id1 $p \ q \ \alpha \ (\text{pisou}\{\mathbf{A}\}\{\mathbf{B}\} \ x \ x_1) = \gamma$

where

$\gamma : \mathbf{B} \models p \approx q$

$\gamma = \models\text{-transport } p \ q \ (\text{P-id1 } p \ q \ \alpha \ x) \ x_1$

P-id1 $p \ q \ \alpha \ (\text{pisow}\{\mathbf{A}\}\{\mathbf{B}\} \ x \ x_1) = \models\text{-transport } p \ q \ \zeta \ x_1$

where

$\zeta : \mathbf{A} \models p \approx q$

$\zeta = \text{P-id1 } p \ q \ \alpha \ x$

...and conversely...

P-id2 : $\{\mathcal{U} \mathcal{W} \mathfrak{X} : \text{Universe}\}\{X : \mathfrak{X} \cdot\}$
 $(\mathcal{K} : \text{Pred}(\text{Algebra } \mathcal{U} S)(\text{OV } \mathcal{U}))$
 $\{p \ q : \text{Term}\{\mathfrak{X}\}\{X\}\}$

→ $((\text{P}\{\mathcal{U}\}\{\mathcal{W}\} \mathcal{K} \models p \approx q) \rightarrow (\mathcal{K} \models p \approx q))$

P-id2 $\{\mathcal{U}\}\{\mathcal{W}\} \ \mathcal{K} \ \{p\}\{q\} \ PKpq \ \{\mathbf{A}\} \ KA = \gamma$

where

```

IA : Algebra (U ⊔ W) S
IA = lift-alg A W

pIA : IA ∈ P{U}{W} K
pIA = pbase KA

ξ : IA ⊨ p ≈ q
ξ = PKpq pIA
γ : A ⊨ p ≈ q
γ = lower-alg-⊨ A p q ξ

```

7.4.4 V preserves identities

– *V preserves identities*

```

V-id1 : {U X : Universe}{X : X}{K : Pred (Algebra U S)(OV U)}
        (p q : Term{X}{X}) → (K ⊨ p ≈ q) → (V{U}{U} K ⊨ p ≈ q)
V-id1 p q α (vbase x) = lift-alg-⊨ _ p q (α x)
V-id1 {U}{X}{X}{K} p q α (vlift{A} x) = γ
  where
    β : A ⊨ p ≈ q
    β = (V-id1 p q α) x
    γ : lift-alg A U ⊨ p ≈ q
    γ = lift-alg-⊨ A p q β
V-id1 {U}{X}{X}{K} p q α (vliftw{A} x) = γ
  where
    β : A ⊨ p ≈ q
    β = (V-id1 p q α) x
    γ : lift-alg A U ⊨ p ≈ q
    γ = lift-alg-⊨ A p q β
V-id1 p q α (vhimg{A}{C} VA ((B , φ , (φh , φE)) , B≅C)) = ⊨≅ p q γ B≅C
  where
    IH : A ⊨ p ≈ q
    IH = V-id1 p q α VA

preim : ∀ b x → | A |
preim b x = (Inv φ (b x) (φE (b x)))

ζ : ∀ b → φ ∘ (preim b) ≡ b - (b : → | B |)(x : X)
ζ b = gfe λ x → InvlInv φ (b x) (φE (b x))

γ : (p · B) ≡ (q · B)
γ = gfe λ b →
  (p · B) b ≡ ⟨ ap (p · B) (ζ b) -1 ⟩
  (p · B) (φ ∘ (preim b)) ≡ ⟨ comm-hom-term gfe A B (φ , φh) p (preim b) -1 ⟩
  φ((p · A)(preim b)) ≡ ⟨ ap φ (intensionality IH (preim b)) ⟩
  φ((q · A)(preim b)) ≡ ⟨ comm-hom-term gfe A B (φ , φh) q (preim b) ⟩
  (q · B)(φ ∘ (preim b)) ≡ ⟨ ap (q · B) (ζ b) ⟩
  (q · B) b ■

```

V-id1{U}{X}{X}{K} p q α (vssub {A}{B} VA B≤A) =

$$S \models p q ((\mathbf{B}, \mathbf{A}, (\mathbf{B}, B \leq A), \text{inj}_2 \text{ refl}, \text{id} \cong)) \gamma$$

where

$$\begin{aligned} \text{IH} &: \mathbf{A} \models p \approx q \\ \text{IH} &= \text{V-id1 } \{\mathbf{u}\}\{\mathfrak{X}\}\{X\} p q \alpha \text{ VA} \end{aligned}$$

$$\begin{aligned} \text{Asinglepq} &: \{ \mathbf{A} \} \models p \approx q \\ \text{Asinglepq} (\text{refl } _) &= \text{IH} \end{aligned}$$

$$\begin{aligned} \gamma &: (\mathcal{K} \cup \{ \mathbf{A} \}) \models p \approx q \\ \gamma \{ \mathbf{B} \} (\text{inj}_1 x) &= \alpha x \\ \gamma \{ \mathbf{B} \} (\text{inj}_2 y) &= \text{Asinglepq } y \end{aligned}$$

$$\text{V-id1 } \{\mathbf{u}\}\{\mathfrak{X}\}\{X\}\{\mathcal{K}\} p q \alpha (\text{vssubw } \{ \mathbf{A} \} \{ \mathbf{B} \} \text{ VA } B \leq A) =$$

$$S \models p q ((\mathbf{B}, \mathbf{A}, (\mathbf{B}, B \leq A), \text{inj}_2 \text{ refl}, \text{id} \cong)) \gamma$$

where

$$\begin{aligned} \text{IH} &: \mathbf{A} \models p \approx q \\ \text{IH} &= \text{V-id1 } \{\mathbf{u}\}\{\mathfrak{X}\}\{X\} p q \alpha \text{ VA} \end{aligned}$$

$$\begin{aligned} \text{Asinglepq} &: \{ \mathbf{A} \} \models p \approx q \\ \text{Asinglepq} (\text{refl } _) &= \text{IH} \end{aligned}$$

$$\begin{aligned} \gamma &: (\mathcal{K} \cup \{ \mathbf{A} \}) \models p \approx q \\ \gamma \{ \mathbf{B} \} (\text{inj}_1 x) &= \alpha x \\ \gamma \{ \mathbf{B} \} (\text{inj}_2 y) &= \text{Asinglepq } y \end{aligned}$$

$$\text{V-id1 } \{\mathbf{u}\}\{\mathfrak{X}\}\{X\} p q \alpha (\text{vprodu } \{ I \} \{ \mathcal{A} \} \text{ V}\mathcal{A}) = \gamma$$

where

$$\begin{aligned} \text{IH} &: (i : I) \rightarrow \mathcal{A} i \models p \approx q \\ \text{IH } i &= \text{V-id1 } \{\mathbf{u}\}\{\mathfrak{X}\}\{X\} p q \alpha (\text{V}\mathcal{A} i) \end{aligned}$$

$$\begin{aligned} \gamma &: p \cdot (\prod \mathcal{A}) \equiv q \cdot (\prod \mathcal{A}) \\ \gamma &= \text{product-id-compatibility } p q I \mathcal{A} \text{ IH} \end{aligned}$$

$$\text{V-id1 } \{\mathbf{u}\}\{\mathfrak{X}\}\{X\} p q \alpha (\text{vprodw } \{ I \} \{ \mathcal{A} \} \text{ V}\mathcal{A}) = \gamma$$

where

$$\begin{aligned} \text{IH} &: (i : I) \rightarrow \mathcal{A} i \models p \approx q \\ \text{IH } i &= \text{V-id1 } \{\mathbf{u}\}\{\mathfrak{X}\}\{X\} p q \alpha (\text{V}\mathcal{A} i) \end{aligned}$$

$$\begin{aligned} \gamma &: p \cdot (\prod \mathcal{A}) \equiv q \cdot (\prod \mathcal{A}) \\ \gamma &= \text{product-id-compatibility } p q I \mathcal{A} \text{ IH} \end{aligned}$$

$$\text{V-id1 } p q \alpha (\text{visou } \{ \mathbf{A} \} \{ \mathbf{B} \} \text{ VA } A \cong B) = \models \cong p q (\text{V-id1 } p q \alpha \text{ VA}) A \cong B$$

$$\text{V-id1 } p q \alpha (\text{visow } \{ \mathbf{A} \} \{ \mathbf{B} \} \text{ VA } A \cong B) = \models \cong p q (\text{V-id1 } p q \alpha \text{ VA}) A \cong B$$

Once again, and for the last time, completeness dictates that we formalize the converse, however obvious it may be.

$$\begin{aligned} \text{V-id2} &: \{ \mathbf{u} \ \mathcal{W} \ \mathfrak{X} : \text{Universe} \} \{ X : \mathfrak{X} \} \{ \mathcal{K} : \text{Pred } (\text{Algebra } \mathbf{u} \ S) (\text{OV } \mathbf{u}) \} \\ &\quad \{ p q : \text{Term } \{ \mathfrak{X} \} \{ X \} \} \rightarrow (\text{V } \{ \mathbf{u} \} \{ \mathcal{W} \} \ \mathcal{K} \models p \approx q) \rightarrow (\mathcal{K} \models p \approx q) \end{aligned}$$

$$\text{V-id2 } \{ \mathbf{u} \} \{ \mathcal{W} \} \{ \mathfrak{X} \} \{ X \} \{ \mathcal{K} \} \{ p \} \{ q \} \text{ Vpq } \{ \mathbf{A} \} \text{ KA} = \gamma$$

where

$$\begin{aligned} \text{IA} &: \text{Algebra } (\mathbf{u} \sqcup \mathcal{W}) \ S \\ \text{IA} &= \text{lift-alg } \mathbf{A} \ \mathcal{W} \end{aligned}$$


```

vIA : IA ∈ V{U}{W}  $\mathcal{K}$ 
vIA = vbase KA

ξ : IA ⊨ p ≈ q
ξ = Vpq vIA

γ : A ⊨ p ≈ q
γ = lower-alg-⊨ A p q ξ

```

7.4.5 Class identities

It follows from **V-id1** that, if \mathcal{K} is a class of structures, the set of identities modeled by all structures in \mathcal{K} is the same as the set of identities modeled by all structures in $\mathbf{V} \mathcal{K}$.

– *Th (V \mathcal{K}) is precisely the set of identities modeled by \mathcal{K}*

```

class-identities : {U X : Universe}{X : X ·}{ $\mathcal{K}$  : Pred (Algebra U S) (OV U)}
                (p q : | T X |)

```

→ $\mathcal{K} \models p \approx q \Leftrightarrow ((p, q) \in \text{Th} (\mathbf{V} \mathcal{K}))$

```

class-identities{U}{X}{X}{ $\mathcal{K}$ } p q = ⇒ , ⇐

```

where

⇒ : $\mathcal{K} \models p \approx q \rightarrow p, q \in \text{Th} (\mathbf{V} \mathcal{K})$

⇒ = $\lambda \alpha \text{ VCloA} \rightarrow \mathbf{V-id1} \ p \ q \ \alpha \ \text{VCloA}$

⇐ : $p, q \in \text{Th} (\mathbf{V} \mathcal{K}) \rightarrow \mathcal{K} \models p \approx q$

⇐ = $\lambda \text{Thpq} \{**A**\} \ KA \rightarrow \text{lower-alg-⊨} \ **A** \ p \ q \ (\text{Thpq} \ (\text{vbase} \ KA))$

(This page is almost entirely blank on purpose.)

8 Birkhoff's HSP Theorem

This section presents the `UALib.Birkhoff` module of the Agda `UALib`.

8.1 The Free Algebra in Theory

Recall, we proved in Section 5.2 that the term algebra $\mathbf{T} X$ is the absolutely free algebra in the class of all S -structures. In this section, we formalize, for a given class \mathcal{K} of S -algebras, the (relatively) free algebra in $\mathbf{SP}(\mathcal{K})$ over X . Indeed, a free algebra *for* a class \mathcal{K} induces the free algebra *in* the variety generated by \mathcal{K} , via the following definitions:¹⁰

$$\Theta(\mathcal{K}, \mathbf{A}) := \{\theta \in \mathbf{Con} \mathbf{A} : \mathbf{A} / \theta \in \mathcal{K}\} \quad \text{and} \quad \psi(\mathcal{K}, \mathbf{A}) := \bigcap \Theta(\mathcal{K}, \mathbf{A}).$$

The free algebra *in* the variety generated by \mathcal{K} is constructed by applying these definitions to the special case in which \mathbf{A} is the term algebra $\mathbf{T} X$ of S -terms over X .

Since $\mathbf{T} X$ is free for (and in) the class $\mathcal{A}lq(S)$ of all S -algebras, it is free for every subclass \mathcal{K} of S -algebras. Although $\mathbf{T} X$ is not necessarily a member of \mathcal{K} , if we form the quotient $\mathfrak{F} := (\mathbf{T} X) / \psi(\mathcal{K}, \mathbf{T} X)$, then it is not hard to see that \mathfrak{F} is a subdirect product of the algebras in $\{(\mathbf{T} X) / \theta\}$, where θ ranges over $\Theta(\mathcal{K}, \mathbf{T} X)$, so \mathfrak{F} belongs to $\mathbf{SP}(\mathcal{K})$, and it follows that \mathfrak{F} satisfies all the identities modeled by \mathcal{K} . Indeed, for each pair $p q : \mathbf{T} X$, if $\mathcal{K} \models p \approx q$, then p and q must belong to the same $\psi(\mathcal{K}, \mathbf{T} X)$ -class, so p and q are identified in the quotient \mathfrak{F} .

The \mathfrak{F} so defined is called the **free algebra over \mathcal{K} generated by X** and, because of what we just observed, we say that \mathfrak{F} is free *in* $\mathbf{SP}(\mathcal{K})$.¹¹

8.2 The free algebra in Agda

This section presents the `[UALib.Birkhoff.FreeAlgebra]` module of the `[Agda Universal Algebra Library]`. Here we represent \mathfrak{F} as a type in Agda by first constructing the congruence $\psi(\mathcal{K}, \mathbf{T} X)$ described above.

```
open import UALib.Algebras using (Signature;  $\mathfrak{O}$ ;  $\mathcal{V}$ ; Algebra;  $\_ \rightarrow \_$ )
open import UALib.Prelude.Preliminaries using (global-dfunext; Universe;  $\_ \cdot$ )

module UALib.Birkhoff.FreeAlgebra
  {S : Signature  $\mathfrak{O}$   $\mathcal{V}$ } {gfe : global-dfunext}
  { $\mathcal{U}$  : { $\mathcal{U}$   $\mathcal{X}$  : Universe} {X :  $\mathcal{X}$   $\cdot$ } (A : Algebra  $\mathcal{U}$  S)  $\rightarrow$  X  $\rightarrow$  A}
  where

  open import UALib.Varieties.Preservation {S = S} {gfe} { $\mathcal{X}$ } public
```

We assume two ambient universes \mathcal{U} and \mathcal{X} , as well as a type $X : \mathcal{X} \cdot$. As usual, this is accomplished with the `module` directive.

```
module the-free-algebra { $\mathcal{U}$   $\mathcal{X}$  : Universe} {X :  $\mathcal{X}$   $\cdot$ } where
```

We begin by defining the collection `Timg` of homomorphic images of the term algebra that belong to a given class \mathcal{K} .

¹⁰If $\Theta(\mathcal{K}, \mathbf{A})$ is empty, then $\psi(\mathcal{K}, \mathbf{A}) = 1$ and $\mathbf{A} / \psi(\mathcal{K}, \mathbf{A})$ is trivial.

¹¹Since X is not a subset of \mathfrak{F} , technically it doesn't make sense to say “ X generates \mathfrak{F} .” But as long as \mathcal{K} contains a nontrivial algebra, $\psi(\mathcal{K}, \mathbf{T} X) \cap X^2$ will be nonempty, and we can identify X with $X / \psi(\mathcal{K}, \mathbf{T} X)$ which does belong to \mathfrak{F} .

– $H(\mathbf{T} X)$ (hom images of $\mathbf{T} X$)

$\mathbf{Timg} : \text{Pred}(\text{Algebra } \mathcal{U} S) (\text{OV } \mathcal{U}) \rightarrow \mathfrak{O} \sqcup \mathcal{V} \sqcup (\mathcal{U} \sqcup \mathcal{X})^+ \cdot$

$\mathbf{Timg} \mathcal{K} = \Sigma \mathbf{A} : (\text{Algebra } \mathcal{U} S), \Sigma \phi : \text{hom}(\mathbf{T} X) \mathbf{A}, (\mathbf{A} \in \mathcal{K}) \times \text{Epic} \mid \phi \mid$

The inhabitants of this Sigma type represent algebras $\mathbf{A} \in \mathcal{K}$ such that there exists a surjective homomorphism $\phi : \text{hom}(\mathbf{T} X) \mathbf{A}$. Thus, \mathbf{Timg} represents the collection of all homomorphic images of $\mathbf{T} X$ that belong to \mathcal{K} . Of course, this is the entire class \mathcal{K} , since the term algebra is absolutely free. Nonetheless, this representation of \mathcal{K} is useful since it endows each element with extra information. Indeed, each inhabitant of $\mathbf{Timg} \mathcal{K}$ is a quadruple, $(\mathbf{A}, \phi, ka, p)$, where \mathbf{A} is an S -algebra, ϕ is a homomorphism from $\mathbf{T} X$ to \mathbf{A} , ka is a proof that \mathbf{A} belongs to \mathcal{K} , and p is a proof that the underlying map $\mid \phi \mid$ is epic.

Next we define a function \mathbf{mkti} that takes an arbitrary algebra \mathbf{A} in \mathcal{K} and returns the corresponding quadruple in $\mathbf{Timg} \mathcal{K}$.

$\mathbf{mkti} : \{\mathcal{K} : \text{Pred}(\text{Algebra } \mathcal{U} S) \text{ o v u}\} (\mathbf{A} : \text{Algebra } \mathcal{U} S) \rightarrow \mathbf{A} \in \mathcal{K} \rightarrow \mathbf{Timg} \mathcal{K}$
 $\mathbf{mkti} \mathbf{A} ka = (\mathbf{A}, \mid \text{Thom-gen } \mathbf{A} \mid, ka, \parallel \text{Thom-gen } \mathbf{A} \parallel)$

Occasionally we want to extract the homomorphism ϕ from an inhabitant of \mathbf{Timg} , so we define.

– *The hom part of a hom image of $\mathbf{T} X$.*

$\mathbf{T}\phi : (\mathcal{K} : \text{Pred}(\text{Algebra } \mathcal{U} S) (\text{OV } \mathcal{U})) (ti : \mathbf{Timg} \mathcal{K})$

$\rightarrow \text{hom}(\mathbf{T} X) \mid ti \mid$

$\mathbf{T}\phi _ ti = \text{fst} \parallel ti \parallel$

Finally, it is time to define the congruence relation modulo which $\mathbf{T} X$ will yield the relatively free algebra, $\mathfrak{F} \mathcal{K} X$.

We start by letting ψ be the collection of all identities (p, q) satisfied by all subalgebras of algebras in \mathcal{K} .

$\psi : (\mathcal{K} : \text{Pred}(\text{Algebra } \mathcal{U} S) (\text{OV } \mathcal{U})) \rightarrow \text{Pred}(\mid \mathbf{T} X \mid \times \mid \mathbf{T} X \mid) (\text{OV } \mathcal{U})$

$\psi \mathcal{K} (p, q) = \forall (\mathbf{A} : \text{Algebra } \mathcal{U} S) \rightarrow (sA : \mathbf{A} \in \mathcal{S}\{\mathcal{U}\}\{\mathcal{U}\} \mathcal{K})$

$\rightarrow \mid \text{lift-hom } \mathbf{A} (\text{fst}(\mathcal{X} \mathbf{A})) \mid p \equiv \mid \text{lift-hom } \mathbf{A} (\text{fst}(\mathcal{X} \mathbf{A})) \mid q$

We convert the predicate ψ into a relation by Currying.

$\psi\text{Rel} : (\mathcal{K} : \text{Pred}(\text{Algebra } \mathcal{U} S) (\text{OV } \mathcal{U})) \rightarrow \text{Rel} \mid (\mathbf{T} X) \mid (\text{OV } \mathcal{U})$

$\psi\text{Rel} \mathcal{K} p q = \psi \mathcal{K} (p, q)$

We will want to express ψRel as a congruence of the term algebra $\mathbf{T} X$, so we must prove that ψRel is compatible with the operations of $\mathbf{T} X$ (which are just the terms themselves) and that ψRel an equivalence relation.

$\psi\text{compatible} : (\mathcal{K} : \text{Pred}(\text{Algebra } \mathcal{U} S) (\text{OV } \mathcal{U}))$

$\rightarrow \text{compatible}(\mathbf{T} X) (\psi\text{Rel} \mathcal{K})$

$\psi\text{compatible} \mathcal{K} f \{i\} \{j\} \text{ i } \psi j \mathbf{A} sA = \gamma$

where

$ti : \mathbf{Timg}(\mathcal{S}\{\mathcal{U}\}\{\mathcal{U}\} \mathcal{K})$

$ti = \mathbf{mkti} \mathbf{A} sA$

$\phi : \text{hom}(\mathbf{T} X) \mathbf{A}$

$\phi = \text{fst} \parallel ti \parallel$

$\gamma : \mid \phi \mid ((f \hat{\ } \mathbf{T} X) i) \equiv \mid \phi \mid ((f \hat{\ } \mathbf{T} X) j)$

$\gamma = \mid \phi \mid ((f \hat{\ } \mathbf{T} X) i) \equiv \langle \parallel \phi \parallel f i \rangle$

$$\begin{aligned}
& (f \hat{\ } \mathbf{A}) (| \phi | \circ i) \equiv \langle \text{ap } (f \hat{\ } \mathbf{A}) (gfe \ \lambda \ x \rightarrow ((i\psi j \ x) \ \mathbf{A} \ sA)) \rangle \\
& (f \hat{\ } \mathbf{A}) (| \phi | \circ j) \equiv \langle (| \phi | \parallel f j)^{\perp} \rangle \\
& | \phi | ((f \hat{\ } \mathbf{T} \ X) j) \blacksquare
\end{aligned}$$

$\psi\text{Refl} : \{\mathcal{K} : \text{Pred } (\text{Algebra } \mathcal{U} \ S) (\text{OV } \mathcal{U})\} \rightarrow \text{reflexive } (\psi\text{Rel } \mathcal{K})$

$\psi\text{Refl} = \lambda \ x \ \mathbf{C} \ \phi \rightarrow \text{refl}$

$\psi\text{Symm} : \{\mathcal{K} : \text{Pred } (\text{Algebra } \mathcal{U} \ S) (\text{OV } \mathcal{U})\} \rightarrow \text{symmetric } (\psi\text{Rel } \mathcal{K})$

$\psi\text{Symm} \ p \ q \ p\psi\text{Rel}q \ \mathbf{C} \ \phi = (p\psi\text{Rel}q \ \mathbf{C} \ \phi)^{\perp}$

$\psi\text{Trans} : \{\mathcal{K} : \text{Pred } (\text{Algebra } \mathcal{U} \ S) (\text{OV } \mathcal{U})\} \rightarrow \text{transitive } (\psi\text{Rel } \mathcal{K})$

$\psi\text{Trans} \ p \ q \ r \ p\psi q \ q\psi r \ \mathbf{C} \ \phi = (p\psi q \ \mathbf{C} \ \phi) \cdot (q\psi r \ \mathbf{C} \ \phi)$

$\psi\text{IsEquivalence} : \{\mathcal{K} : \text{Pred } (\text{Algebra } \mathcal{U} \ S) (\text{OV } \mathcal{U})\} \rightarrow \text{IsEquivalence } (\psi\text{Rel } \mathcal{K})$

$\psi\text{IsEquivalence} = \text{record } \{ \text{rfl} = \psi\text{Refl} ; \text{sym} = \psi\text{Symm} ; \text{trans} = \psi\text{Trans} \}$

We have collected all the pieces necessary to express the collection of identities satisfied by all algebras in the class as a congruence relation of the term algebra. We call this congruence ψCon and define it using the Congruence constructor `mkcon`.

$\psi\text{Con} : (\mathcal{K} : \text{Pred } (\text{Algebra } \mathcal{U} \ S) (\text{OV } \mathcal{U})) \rightarrow \text{Congruence } (\mathbf{T} \ X)$

$\psi\text{Con } \mathcal{K} = \text{mkcon } (\psi\text{Rel } \mathcal{K}) (\psi\text{compatible } \mathcal{K}) \ \psi\text{IsEquivalence}$

We denote the free algebra by \mathfrak{F} and construct it as the quotient $\mathbf{T} \ X / (\psi\text{Con } \mathcal{K})$.

`open the-free-algebra`

`module the-relatively-free-algebra`

$\{\mathcal{U} \ \mathfrak{X} : \text{Universe}\} \{X : \mathfrak{X} \ \cdot\}$

$\{\mathcal{K} : \text{Pred } (\text{Algebra } \mathcal{U} \ S) (\text{OV } \mathcal{U})\}$ `where`

$\mathfrak{F} : \text{Universe}$ – *(universe level of the relatively free algebra)*

$\mathfrak{F} = (\mathfrak{X} \sqcup (\text{OV } \mathcal{U}))^+$

$\mathfrak{F} : \text{Algebra } \mathfrak{F} \ S$

$\mathfrak{F} = \mathbf{T} \ X / (\psi\text{Con } \mathcal{K})$

Here $\mathfrak{F} = (\mathfrak{X} \sqcup \text{ov}\mathcal{U})^+$ happens to be the universe level of \mathfrak{F} . The domain of the free algebra is $|\mathbf{T} \ X| / \langle \psi\text{Con } \mathcal{K} \rangle$, which is $\Sigma \ \mathbf{C} : _ , \Sigma \ p : |\mathbf{T} \ X| , \ \mathbf{C} \equiv ([p] \langle \psi\text{Con } \mathcal{K} \rangle)$, by definition; i.e., the collection $\{\mathbf{C} : \exists p \in |\mathbf{T} \ X| , \ \mathbf{C} \equiv [p] \langle \psi\text{Con } \mathcal{K} \rangle\}$ of $\langle \psi\text{Con } \mathcal{K} \rangle$ -classes of $\mathbf{T} \ X$.

$\mathfrak{F}\text{-free-lift} : \{\mathcal{W} : \text{Universe}\} (\mathbf{A} : \text{Algebra } \mathcal{W} \ S)$

$(h_0 : X \rightarrow |\mathbf{A}|) \rightarrow |\mathfrak{F}| \rightarrow |\mathbf{A}|$

$\mathfrak{F}\text{-free-lift } \{\mathcal{W}\} \ \mathbf{A} \ h_0 \ (_ , x , _) = (\text{free-lift } \{\mathfrak{X}\} \{\mathcal{W}\} \ \mathbf{A} \ h_0) \ x$

$\mathfrak{F}\text{-lift-hom} : \{\mathcal{W} : \text{Universe}\} (\mathbf{A} : \text{Algebra } \mathcal{W} \ S)$

$(h_0 : X \rightarrow |\mathbf{A}|) \rightarrow \text{hom } \mathfrak{F} \ \mathbf{A}$

$\mathfrak{F}\text{-lift-hom } \ \mathbf{A} \ h_0 = \mathbf{f} , \ \text{fhom}$

`where`

$\mathbf{f} : |\mathfrak{F}| \rightarrow |\mathbf{A}|$

$\mathbf{f} = \mathfrak{F}\text{-free-lift } \ \mathbf{A} \ h_0$

$$\phi : \text{hom } (\mathbf{T} X) \mathbf{A}$$

$$\phi = \text{lift-hom } \mathbf{A} h_0$$

$$\text{fhom} : \text{is-homomorphism } \mathfrak{F} \mathbf{A} f$$

$$\text{fhom } f \mathbf{a} = \llbracket \phi \rrbracket f (\lambda i \rightarrow \ulcorner \mathbf{a} i \urcorner)$$

$$\mathfrak{F}\text{-lift-agrees-on-X} : \{\mathfrak{W} : \text{Universe}\}(\mathbf{A} : \text{Algebra } \mathfrak{W} S)$$

$$(h_0 : X \rightarrow | \mathbf{A} |)(x : X)$$

$$\rightarrow h_0 x \equiv (| \mathfrak{F}\text{-lift-hom } \mathbf{A} h_0 | \llbracket \mathfrak{g} x \rrbracket)$$

$$\mathfrak{F}\text{-lift-agrees-on-X } _ h_0 x = \text{refl}$$

$$\mathfrak{F}\text{-lift-of-epic-is-epic} : \{\mathfrak{W} : \text{Universe}\}(\mathbf{A} : \text{Algebra } \mathfrak{W} S)$$

$$(h_0 : X \rightarrow | \mathbf{A} |) \rightarrow \text{Epic } h_0$$

$$\rightarrow \text{Epic } | \mathfrak{F}\text{-lift-hom } \mathbf{A} h_0 |$$

$$\mathfrak{F}\text{-lift-of-epic-is-epic } \mathbf{A} h_0 hE y = \gamma$$

where

$$h_0\text{pre} : \text{Image } h_0 \ni y$$

$$h_0\text{pre} = hE y$$

$$h_0^{-1}y : X$$

$$h_0^{-1}y = \text{Inv } h_0 y (hE y)$$

$$\eta : y \equiv (| \mathfrak{F}\text{-lift-hom } \mathbf{A} h_0 | \llbracket \mathfrak{g} (h_0^{-1}y) \rrbracket)$$

$$\eta = y \equiv \langle (\text{InvlInv } h_0 y h_0\text{pre})^{-1} \rangle$$

$$h_0 h_0^{-1}y \equiv \langle \mathfrak{F}\text{-lift-agrees-on-X } \mathbf{A} h_0 h_0^{-1}y \rangle$$

$$| \mathfrak{F}\text{-lift-hom } \mathbf{A} h_0 | \llbracket \mathfrak{g} h_0^{-1}y \rrbracket \blacksquare$$

$$\gamma : \text{Image } | \mathfrak{F}\text{-lift-hom } \mathbf{A} h_0 | \ni y$$

$$\gamma = \text{eq } y (\llbracket \mathfrak{g} h_0^{-1}y \rrbracket) \eta$$

$$\mathfrak{F}\text{-canonical-projection} : \text{epi } (\mathbf{T} X) \mathfrak{F}$$

$$\mathfrak{F}\text{-canonical-projection} = \text{canonical-projection } (\mathbf{T} X) (\psi\text{Con } \mathcal{K})$$

$$\pi\mathfrak{F} : \text{hom } (\mathbf{T} X) \mathfrak{F}$$

$$\pi\mathfrak{F} = \text{epi-to-hom } (\mathbf{T} X) \{\mathfrak{F}\} \mathfrak{F}\text{-canonical-projection}$$

$$\pi\mathfrak{F}\text{-X-defined} : (g : \text{hom } (\mathbf{T} X) \mathfrak{F})$$

$$\rightarrow ((x : X) \rightarrow | g | (\mathfrak{g} x) \equiv \llbracket \mathfrak{g} x \rrbracket)$$

$$\rightarrow (t : | \mathbf{T} X |)$$

$$\rightarrow | g | t \equiv \llbracket t \rrbracket$$

$$\pi\mathfrak{F}\text{-X-defined } g \text{ g}x t = \text{free-unique } gfe \mathfrak{F} g \pi\mathfrak{F} g\pi\mathfrak{F}\text{-agree-on-X } t$$

where

$$g\pi\mathfrak{F}\text{-agree-on-X} : ((x : X) \rightarrow | g | (\mathfrak{g} x) \equiv | \pi\mathfrak{F} | (\mathfrak{g} x))$$

$$g\pi\mathfrak{F}\text{-agree-on-X } x = gx x$$

$$\begin{aligned} X \hookrightarrow \mathfrak{F} &: X \rightarrow |\mathfrak{F}| \\ X \hookrightarrow \mathfrak{F} \ x &= \llbracket \mathfrak{g} \ x \rrbracket \end{aligned}$$

The remainder of §8.2 is not needed for the proof of Birkhoff's theorem.

$$\begin{aligned} \mathfrak{F}\text{-free-lift-interpretation} &: (\mathbf{A} : \text{Algebra } \mathfrak{U} \ S) \\ & \quad (h_0 : X \rightarrow |\mathbf{A}|)(x : |\mathfrak{F}|) \end{aligned}$$

$$\rightarrow \frac{}{(\ulcorner \mathbf{x} \urcorner \cdot \mathbf{A}) \ h_0 \equiv \mathfrak{F}\text{-free-lift } \mathbf{A} \ h_0 \ \mathbf{x}}$$

$$\mathfrak{F}\text{-free-lift-interpretation } \mathbf{A} \ f \ \mathbf{x} = \text{free-lift-interpretation } \mathbf{A} \ f \ \ulcorner \mathbf{x} \urcorner$$

$$\mathbf{T}\text{-canonical-projection} : (\theta : \text{Congruence}\{\text{ov } \mathfrak{X}\}\{\mathfrak{U}\} (\mathbf{T} \ X)) \rightarrow \text{epi } (\mathbf{T} \ X) ((\mathbf{T} \ X) / \theta)$$

$$\mathbf{T}\text{-canonical-projection } \theta = \text{canonical-projection } (\mathbf{T} \ X) \ \theta$$

8.2.1 Properties of ψ

$$\begin{aligned} \psi\text{lem} &: (p \ q : |\mathbf{T} \ X|) \\ & \rightarrow \frac{|\text{lift-hom } \mathfrak{F} \ X \hookrightarrow \mathfrak{F}| \ p \equiv |\text{lift-hom } \mathfrak{F} \ X \hookrightarrow \mathfrak{F}| \ q}{(p, q) \in \psi \ \mathcal{K}} \end{aligned}$$

$$\psi\text{lem } p \ q \ gpgq \ \mathbf{A} \ sA = \gamma$$

where

$$\begin{aligned} g &: \text{hom } (\mathbf{T} \ X) \ \mathfrak{F} \\ g &= \text{lift-hom } \mathfrak{F} \ (X \hookrightarrow \mathfrak{F}) \end{aligned}$$

$$\begin{aligned} h_0 &: X \rightarrow |\mathbf{A}| \\ h_0 &= \text{fst } (\mathbb{X} \ \mathbf{A}) \end{aligned}$$

$$\begin{aligned} f &: \text{hom } \mathfrak{F} \ \mathbf{A} \\ f &= \mathfrak{F}\text{-lift-hom } \mathbf{A} \ h_0 \end{aligned}$$

$$\begin{aligned} h \ \phi &: \text{hom } (\mathbf{T} \ X) \ \mathbf{A} \\ h &= \text{HomComp } (\mathbf{T} \ X) \ \mathbf{A} \ g \ f \\ \phi &= \mathbf{T}\phi \ (S \ \mathcal{K}) \ (\text{mkti } \mathbf{A} \ sA) \end{aligned}$$

–(homs from $\mathbf{T} \ X$ to \mathbf{A} that agree on X are equal)

$$\text{lift-agreement} : (x : X) \rightarrow h_0 \ x \equiv |f| \llbracket \mathfrak{g} \ x \rrbracket$$

$$\text{lift-agreement } x = \mathfrak{F}\text{-lift-agrees-on-}X \ \mathbf{A} \ h_0 \ x$$

$$\text{fgx} \equiv \phi : (x : X) \rightarrow (|f| \circ |g|) (\mathfrak{g} \ x) \equiv |f| (\mathfrak{g} \ x)$$

$$\text{fgx} \equiv \phi \ x = (\text{lift-agreement } x)^{\perp}$$

$$h \equiv \phi : \forall t \rightarrow (|f| \circ |g|) \ t \equiv |f| \ t$$

$$h \equiv \phi \ t = \text{free-unique } gfe \ \mathbf{A} \ h \ \phi \ \text{fgx} \equiv \phi \ t$$

$$\gamma : |f| \ p \equiv |f| \ q$$

$$\gamma = |f| \ p \equiv \langle (h \equiv \phi \ p)^{\perp} \rangle (|f| \circ |g|) \ p$$

$$\equiv \langle \text{refl} \rangle |f| (|g| \ p)$$

$$\equiv \langle \text{ap } |f| \ gpgq \rangle |f| (|g| \ q)$$

$$\equiv \langle h \equiv \phi \ q \rangle |f| \ q \blacksquare$$

$$\begin{aligned} \mathbf{Ti} \models \psi & : (\mathcal{K} : \text{Pred (Algebra } \mathcal{U} S) \text{ } \mathbf{ov} \mathcal{U}) \\ & (\mathbf{C} : \text{Algebra } \mathcal{U} S) (sC : \mathbf{C} \in \mathbf{S}\{\mathcal{U}\}\{\mathcal{U}\} \mathcal{K}) \\ & (p \ q : | (\mathbf{T} X) |) \rightarrow (p \ , \ q) \in \psi \ \mathcal{K} \\ \hline & \rightarrow \quad | \mathbf{T}\phi (\mathbf{S} \mathcal{K})(\text{mkti } \mathbf{C} \ sC) | \ p \equiv | \mathbf{T}\phi (\mathbf{S} \mathcal{K})(\text{mkti } \mathbf{C} \ sC) | \ q \\ \mathbf{Ti} \models \psi \ \mathcal{K} \ \mathbf{C} \ sC \ p \ q \ p\psi q & = p\psi q \ \mathbf{C} \ sC \end{aligned}$$

8.3 HSP Lemmas

This subsection presents the `UALib.Birkhoff.HSPLemmas` submodule of the Agda `UALib`. This subsection gives formal statements of four lemmas that we will string together in §8.4 to complete the proof of Birkhoff's theorem. **Warning:** not all of these are very interesting!

```
open import UALib.Algebras using (Signature;  $\mathbf{O}$ ;  $\mathcal{V}$ ; Algebra;  $\_ \rightarrow \_$ )
open import UALib.Prelude.Preliminaries using (global-dfunext; Universe;  $\_ \cdot$ )

module UALib.Birkhoff.HSPLemmas
  {S : Signature  $\mathbf{O}$   $\mathcal{V}$ }{gfe : global-dfunext}
  { $\mathcal{X}$  : { $\mathcal{U}$   $\mathcal{X}$  : Universe}{X :  $\mathcal{X}$  · } (A : Algebra  $\mathcal{U}$  S)  $\rightarrow$  X  $\rightarrow$  A}
  { $\mathcal{U}$  : Universe} {X :  $\mathcal{U}$  ·}
  where

  open import UALib.Birkhoff.FreeAlgebra {S = S}{gfe}{ $\mathcal{X}$ } public

  open the-free-algebra { $\mathcal{U}$ }{ $\mathcal{U}$ }{X}

  module class-inclusions
    { $\mathcal{K}$  : Pred (Algebra  $\mathcal{U}$  S) (ov  $\mathcal{U}$ )}
    - extensionality assumptions:
    {hfe : hfunext (ov  $\mathcal{U}$ )(ov  $\mathcal{U}$ )}
    {pe : propext (ov  $\mathcal{U}$ )}
    - truncation assumptions:
    {ssR :  $\forall$  p q  $\rightarrow$  is-subsingleton (( $\psi$ Rel  $\mathcal{K}$ ) p q)}
    {ssA :  $\forall$  C  $\rightarrow$  is-subsingleton ( $\mathcal{C}\{\text{ov } \mathcal{U}\}\{\text{ov } \mathcal{U}\}\{| \mathbf{T} X | \}\{\psi \text{Rel } \mathcal{K}\} C$ )}
    where

    - NOTATION.
    ovu+ : Universe
    ovu =  $\mathbf{O} \sqcup \mathcal{V} \sqcup \mathcal{U}^+$ 
    ovu+ = ovu+
```

8.3.1 \mathbf{V} is closed under lift

The first hurdle is the `lift- alg-V -closure` lemma, which says that if an algebra \mathbf{A} belongs to the variety \mathbf{V} , then so does its lift. This dispenses with annoying universe level problems that arise later—a minor technical issue, but the proof is long and tedious, not to mention uninteresting.

```
open Lift
lift- $\text{alg-V}$ -closure - (alias)
```



```

VIA : {A : Algebra ovu S}
  → A ∈ V{U}{ovu} K

-----

→ lift-alg A ovu+ ∈ V{U}{ovu+} K

VIA (vbase{A} x) = visow (vbase{U}{W = ovu+} x) (lift-alg-associative A)
VIA (vlift{A} x) = visow (vlift{U}{W = ovu+} x) (lift-alg-associative A)
VIA (vliftw{A} x) = visow (VIA x) (lift-alg-associative A)
VIA (vhimg{A}{B} x hB) = vhimg (VIA x) (lift-alg-hom-image hB)
VIA (vssub{A}{B} x B≤A) = vssubw (vlift{U}{W = ovu+} x) (lift-alg-≤ B{A} B≤A)
VIA (vssubw{A}{B} x B≤A) = vssubw (VIA x) (lift-alg-≤ B{A} B≤A)
VIA (vprodu{I}{A} x) = visow (vprodw vA) (sym-≅ B≅A)

where
  I : ovu+ ·
  I = Lift{ovu}{ovu+} I

  IA+ : Algebra ovu+ S
  IA+ = lift-alg (∏ A) ovu+

  IA : I → Algebra ovu+ S
  IA i = lift-alg (A (lower i)) ovu+

  vA : (i : I) → (IA i) ∈ V{U}{ovu+} K
  vA i = vlift (x (lower i))

  iso-components : (i : I) → A i ≅ IA (lift i)
  iso-components i = lift-alg-≅

  B≅A : IA+ ≅ ∏ IA
  B≅A = lift-alg-∏≅ gfe iso-components

VIA (vprodw{I}{A} x) = visow (vprodw vA) (sym-≅ B≅A)

where
  I : ovu+ ·
  I = Lift{ovu}{ovu+} I

  IA+ : Algebra ovu+ S
  IA+ = lift-alg (∏ A) ovu+

  IA : I → Algebra ovu+ S
  IA i = lift-alg (A (lower i)) ovu+

  vA : (i : I) → (IA i) ∈ V{U}{ovu+} K
  vA i = VIA (x (lower i))

  iso-components : (i : I) → A i ≅ IA (lift i)
  iso-components i = lift-alg-≅

  B≅A : IA+ ≅ ∏ IA
  B≅A = lift-alg-∏≅ gfe iso-components

VIA (visou{A}{B} x A≅B) = visow (vlift x) (lift-alg-iso U ovu+ A B A≅B)
VIA (visow{A}{B} x A≅B) = visow (VIA x) (lift-alg-iso ovu ovu+ A B A≅B)

lift-alg-V-closure = VIA - (alias)

```

8.3.2 $\text{SP}(\mathcal{K}) \subseteq \mathbf{V}(\mathcal{K})$

In the `UALib.Varieties` module, we proved that $\text{SP}(\mathcal{K}) \subseteq \mathbf{V}(\mathcal{K})$ holds with fairly general universe level parameters. Unfortunately, this was not general enough for our purposes, so we prove the inclusion again for the specific universe parameters that align with subsequent applications of this result. This proof also suffers from the unfortunate defect of being boring.

$$\text{SP}_{\subseteq \mathbf{V}}' : S\{\text{ovu}\}\{\text{ovu}+\} (P\{\mathcal{U}\}\{\text{ovu}\} \mathcal{K}) \subseteq V\{\mathcal{U}\}\{\text{ovu}+\} \mathcal{K}$$

$$\text{SP}_{\subseteq \mathbf{V}}' (\text{sbase}\{\mathbf{A}\} x) = \gamma$$

where

$$\text{IIA} \text{ IA}+ : \text{Algebra ovu}+ S$$

$$\text{IA}+ = \text{lift-alg } \mathbf{A} \text{ ovu}+$$

$$\text{IIA} = \text{lift-alg (lift-alg } \mathbf{A} \text{ ovu) ovu}+$$

$$\text{vIIA} : \text{IIA} \in V\{\mathcal{U}\}\{\text{ovu}+\} \mathcal{K}$$

$$\text{vIIA} = \text{lift-alg-V-closure (SP}_{\subseteq \mathbf{V}}' (\text{sbase } x))$$

$$\text{IIA} \cong \text{IA}+ : \text{IIA} \cong \text{IA}+$$

$$\text{IIA} \cong \text{IA}+ = \text{sym-}\cong (\text{lift-alg-associative } \mathbf{A})$$

$$\gamma : \text{IA}+ \in (V\{\mathcal{U}\}\{\text{ovu}+\} \mathcal{K})$$

$$\gamma = \text{visow vIIA II} \cong \text{IA}+$$

$$\text{SP}_{\subseteq \mathbf{V}}' (\text{slift}\{\mathbf{A}\} x) = \text{lift-alg-V-closure (SP}_{\subseteq \mathbf{V}}' x)$$

$$\text{SP}_{\subseteq \mathbf{V}}' (\text{ssub}\{\mathbf{A}\}\{\mathbf{B}\} \text{ spA } B \leq A) = \text{vssubw vIA } B \leq \text{IA}$$

where

$$\text{IA} : \text{Algebra ovu}+ S$$

$$\text{IA} = \text{lift-alg } \mathbf{A} \text{ ovu}+$$

$$\text{vIA} : \text{IA} \in V\{\mathcal{U}\}\{\text{ovu}+\} \mathcal{K}$$

$$\text{vIA} = \text{lift-alg-V-closure (SP}_{\subseteq \mathbf{V}}' \text{ spA)}$$

$$B \leq \text{IA} : \mathbf{B} \leq \text{IA}$$

$$B \leq \text{IA} = (\text{lift-alg-lower-}\leq\text{-lift } \{\text{ovu}\}\{\text{ovu}+\}\{\text{ovu}+\} \mathbf{A} \{\mathbf{B}\}) B \leq A$$

$$\text{SP}_{\subseteq \mathbf{V}}' (\text{ssubw}\{\mathbf{A}\}\{\mathbf{B}\} \text{ spA } B \leq A) = \text{vssubw (SP}_{\subseteq \mathbf{V}}' \text{ spA) } B \leq A$$

$$\text{SP}_{\subseteq \mathbf{V}}' (\text{siso}\{\mathbf{A}\}\{\mathbf{B}\} x A \cong B) = \text{visow (lift-alg-V-closure vA) IA} \cong \mathbf{B}$$

where

$$\text{IA} : \text{Algebra ovu}+ S$$

$$\text{IA} = \text{lift-alg } \mathbf{A} \text{ ovu}+$$

$$\text{pIA} : \mathbf{A} \in S\{\text{ovu}\}\{\text{ovu}\} (P\{\mathcal{U}\}\{\text{ovu}\} \mathcal{K})$$

$$\text{pIA} = x$$

$$\text{vA} : \mathbf{A} \in V\{\mathcal{U}\}\{\text{ovu}\} \mathcal{K}$$

$$\text{vA} = \text{SP}_{\subseteq \mathbf{V}}' x$$

$$\text{IA} \cong \mathbf{B} : \text{IA} \cong \mathbf{B}$$

$$\text{IA} \cong \mathbf{B} = \text{Trans-}\cong \text{IA } \mathbf{B} (\text{sym-}\cong \text{ lift-alg-}\cong) A \cong B$$

8.3.3 $\mathfrak{F} \leq \prod \mathbf{S}(\mathcal{K})$

Now we come to a step in the Agda formalization of Birkhoff's theorem that turns out to be surprisingly nontrivial. We must show that the relatively free algebra \mathfrak{F} embeds in the product \mathfrak{C} of all subalgebras of algebras in the given class \mathcal{K} . Incidentally, this seems to be the only stage in the proof of Birkhoff's theorem that requires the truncation assumption that \mathfrak{C} be a set.

We begin by constructing \mathfrak{C} , using the class-product types described in §7.3.8.

```
open the-relatively-free-algebra { $\mathfrak{U} = \mathfrak{U}$ } { $\mathfrak{X} = \mathfrak{U}$ } { $X = X$ } { $\mathcal{K} = \mathcal{K}$ }
open class-product { $\mathfrak{U} = \mathfrak{U}$ } { $\mathcal{K} = \mathcal{K}$ }
```

– NOTATION.

– \forall is $HSP(\mathcal{K})$

\forall : Pred (Algebra ovu+ S) (ovu+ +)

$\forall = \mathbf{V}\{\mathfrak{U}\}\{\text{ovu+}\} \mathcal{K}$

$\mathfrak{I}s$: ovu *

$\mathfrak{I}s = \mathfrak{I}(\mathbf{S}\{\mathfrak{U}\}\{\mathfrak{U}\} \mathcal{K})$

$\mathfrak{A}s$: $\mathfrak{I}s \rightarrow$ Algebra \mathfrak{U} S

$\mathfrak{A}s = \lambda (i : \mathfrak{I}s) \rightarrow | i |$

$SK\mathfrak{A}$: $(i : \mathfrak{I}s) \rightarrow (\mathfrak{A}s i) \in \mathbf{S}\{\mathfrak{U}\}\{\mathfrak{U}\} \mathcal{K}$

$SK\mathfrak{A} = \lambda (i : \mathfrak{I}s) \rightarrow || i ||$

– \mathfrak{C} is the product of all subalgebras of algebras in \mathcal{K} .

\mathfrak{C} : Algebra ovu S

$\mathfrak{C} = \prod \mathfrak{A}s$

Observe that the elements of \mathfrak{C} are maps from $\mathfrak{I}s$ to $\{\mathfrak{A}s i : i \in \mathfrak{I}s\}$.

Next, we construct an embedding \mathfrak{f} from \mathfrak{F} into \mathfrak{C} using a UALib tool called \mathfrak{F} -free-lift.

\mathfrak{h}_0 : $X \rightarrow | \mathfrak{C} |$

$\mathfrak{h}_0 x = \lambda i \rightarrow (\text{fst } (\mathfrak{X} (\mathfrak{A}s i))) x$

$\phi_{\mathfrak{C}}$: hom (T X) \mathfrak{C}

$\phi_{\mathfrak{C}} = \text{lift-hom } \mathfrak{C} \mathfrak{h}_0$

\mathfrak{g} : hom (T X) \mathfrak{F}

$\mathfrak{g} = \text{lift-hom } \mathfrak{F} (X \hookrightarrow \mathfrak{F})$

\mathfrak{f} : hom \mathfrak{F} \mathfrak{C}

$\mathfrak{f} = \mathfrak{F}\text{-free-lift } \mathfrak{C} \mathfrak{h}_0 , \lambda f \mathfrak{a} \rightarrow || \phi_{\mathfrak{C}} || f (\lambda i \rightarrow \ulcorner \mathfrak{a} i \urcorner)$

$\mathfrak{g}\text{-}\llbracket \rrbracket$: $\forall p \rightarrow | \mathfrak{g} | p \equiv \llbracket p \rrbracket$

$\mathfrak{g}\text{-}\llbracket \rrbracket p = \pi_{\mathfrak{F}\text{-}X\text{-defined } \mathfrak{g}} (\mathfrak{F}\text{-lift-agrees-on-}X \mathfrak{F} X \hookrightarrow \mathfrak{F}) p$

– $\mathfrak{p} i$ is the projection out of the product \mathfrak{C} onto the i -th factor.

\mathfrak{p} : $(i : \mathfrak{I}s) \rightarrow | \mathfrak{C} | \rightarrow | \mathfrak{A}s i |$

$\mathfrak{p} i \mathfrak{a} = \mathfrak{a} i$

phom : $(i : \mathfrak{I}s) \rightarrow \text{hom } \mathfrak{C} (\mathfrak{A}s i)$

$\text{p}f\text{hom} = \prod\text{-projection-hom } \{I = \mathcal{I}s\}\{sA = \mathcal{A}s\}$

- $\text{p}f$ is the composition: $\mathcal{F} - f \rightarrow \mathcal{C} - \text{p } i \rightarrow \mathcal{A}s \ i$

$\text{p}f : \forall i \rightarrow | \mathcal{F} | \rightarrow | \mathcal{A}s \ i |$

$\text{p}f \ i = (\text{p } i) \circ | f |$

$\text{p}f\text{hom} : (i : \mathcal{I}s) \rightarrow \text{hom } \mathcal{F} \ (\mathcal{A}s \ i)$

$\text{p}f\text{hom } i = \text{HomComp } \mathcal{F} \ (\mathcal{A}s \ i) \ f \ (\text{p}f\text{hom } i)$

We now proceed to the proof that the free algebra \mathcal{F} is a subalgebra of the product \mathcal{C} of all subalgebras of algebras in \mathcal{K} . The hard part of the proof is showing that $f : \text{hom } \mathcal{F} \ \mathcal{C}$ is a monomorphism. Let's dispense with that first.

$\Psi : \text{Rel } | \mathbf{T} \ X | \ (\text{ov } \mathcal{U})$

$\Psi = \psi\text{Rel } \mathcal{K}$

$\text{mon}f : \text{Monic } | f |$

$\text{mon}f \ (\cdot (\Psi \ p) , p , \text{refl } _) \ (\cdot (\Psi \ q) , q , \text{refl } _) \ f p q = \gamma$

where

$\text{p}\Psi q : \Psi \ p \ q$

$\text{p}\Psi q \ \mathbf{A} \ sA = \gamma'$

where

$\text{p}A : \text{hom } \mathcal{F} \ \mathbf{A}$

$\text{p}A = \text{p}f\text{hom} \ (\mathbf{A} , sA)$

$f p q : | \text{p}A | \llbracket p \rrbracket \equiv | \text{p}A | \llbracket q \rrbracket$

$f p q = | \text{p}A | \llbracket p \rrbracket \equiv \langle \text{refl} \rangle$

$| \text{p}f\text{hom} \ (\mathbf{A} , sA) | \ (| f | \llbracket p \rrbracket) \equiv \langle \text{ap } (\lambda \ - \rightarrow (| \text{p}f\text{hom} \ (\mathbf{A} , sA) | \ -)) \ f p q \rangle$

$| \text{p}f\text{hom} \ (\mathbf{A} , sA) | \ (| f | \llbracket q \rrbracket) \equiv \langle \text{refl} \rangle$

$| \text{p}A | \llbracket q \rrbracket \blacksquare$

$h \phi : \text{hom} \ (\mathbf{T} \ X) \ \mathbf{A}$

$h = \text{HomComp} \ (\mathbf{T} \ X) \ \mathbf{A} \ g \ \text{p}A$

$\phi = \text{lift-hom } \mathbf{A} \ ((\text{p} \ (\mathbf{A} , sA)) \circ h_0)$

$f g x \equiv \phi : (x : X) \rightarrow (| \text{p}A | \circ | g |) \ (g \ x) \equiv | \phi | \ (g \ x)$

$f g x \equiv \phi \ x = | \text{p}A | \ (| g | \ (g \ x)) \equiv \langle \text{ap } | \text{p}A | \ (g \llbracket g \ x \rrbracket) \rangle$

$| \text{p}A | \ (\llbracket g \ x \rrbracket) \equiv \langle (\mathcal{F}\text{-lift-agrees-on-}X \ \mathbf{A} \ ((\text{p} \ (\mathbf{A} , sA)) \circ h_0) \ x)^{-1} \rangle$

$| \phi | \ (g \ x) \blacksquare$

$h \equiv \phi' : \forall t \rightarrow (| \text{p}A | \circ | g |) \ t \equiv | \phi | \ t$

$h \equiv \phi' \ t = \text{free-unique } g f e \ \mathbf{A} \ h \ \phi \ f g x \equiv \phi \ t$

$\gamma' : | \phi | \ p \equiv | \phi | \ q$

$\gamma' = | \phi | \ p \equiv \langle (h \equiv \phi')^{-1} \rangle$

$| \text{p}A | \ (| g | \ p) \equiv \langle \text{ap } | \text{p}A | \ (g \llbracket p \rrbracket) \rangle$

$| \text{p}A | \llbracket p \rrbracket \equiv \langle f p q \rangle$

$| \text{p}A | \llbracket q \rrbracket \equiv \langle (\text{ap } | \text{p}A | \ (g \llbracket q \rrbracket))^{-1} \rangle$

$| \text{p}A | \ (| g | \ q) \equiv \langle h \equiv \phi' \ q \rangle$

$| \phi | \ q \blacksquare$

```

γ : ( Ψ p , p , refl ) ≡ ( Ψ q , q , refl )
γ = class-extensionality' pe gfe ssR ssA ψIsEquivalence pΨq

```

With that out of the way, the proof that \mathbb{F} is (isomorphic to) a subalgebra of \mathcal{C} is all but complete.

```

f̄ ≤ C : is-set | C | → f̄ ≤ C
f̄ ≤ C Cset = | f | , ( embf , || f || )
where
  embf : is-embedding | f |
  embf = monic-into-set-is-embedding Cset | f | monf

```

8.3.4 $\mathfrak{F} \in \mathbf{V}(\mathcal{K})$

With the foregoing results in hand, along with what we proved earlier—namely, that $\mathbf{PS}(\mathcal{K}) \subseteq \mathbf{SP}(\mathcal{K}) \subseteq \mathbf{V}(\mathcal{K})$ —it is not hard to show that \mathfrak{F} belongs to $\mathbf{SP}(\mathcal{K})$, and hence to $\mathbf{V}(\mathcal{K})$.

```

open class-product-inclusions {U = U}{K = K}

f̄ ∈ SP : is-set | C | → f̄ ∈ ( S{ovu}{ovu+} ( P{U}{ovu} K ) )
f̄ ∈ SP Cset = ssub spC ( f̄ ≤ C Cset )
where
  spC : C ∈ ( S{ovu}{ovu} ( P{U}{ovu} K ) )
  spC = ( class-prod-s-∈-sp hfe )

f̄ ∈ V : is-set | C | → f̄ ∈ V
f̄ ∈ V Cset = SP ⊆ V' ( f̄ ∈ SP Cset )

```

8.4 The HSP Theorem

This subsection presents the `UALib.Birkhoff.HSPTheorem` submodule of the Agda `UALib`. It is now all but trivial to use what we have already proved and piece together a complete proof of Birkhoff’s celebrated HSP theorem asserting that every variety is defined by a set of identities (is an “equational class”).

```

open import UALib.Algebras using ( Signature ; 0 ; V ; Algebra ; _→_ )
open import UALib.Prelude.Preliminaries using ( global-dfunext ; Universe ; _' )

module UALib.Birkhoff.HSPTheorem
  { S : Signature 0 V } { gfe : global-dfunext }
  { X : { U X : Universe } { X : X · } { A : Algebra U S } → X → A }
  { U : Universe } { X : U · }
  where
    open import UALib.Birkhoff.HSPLemmas { S = S } { gfe } { X } { U } { X } public
    open the-free-algebra { U } { U } { X }

  module Birkhoffs-Theorem
    { K : Pred ( Algebra U S ) ovu }
    – extensionality assumptions
    { hfe : hfnext ovu ovu }
    { pe : propext ovu }

```

– *truncation assumptions:*

$\{ssR : \forall p q \rightarrow \text{is-subsingleton } ((\psi\text{Rel } \mathcal{K}) p q)\}$

$\{ssA : \forall C \rightarrow \text{is-subsingleton } (\mathcal{C}\{\mathbf{ouu}\}\{\mathbf{ouu}\}\{\mathbf{T } X \mid\}\{\psi\text{Rel } \mathcal{K}\} C)\}$

where

open the-relatively-free-algebra $\{\mathcal{U}\}\{\mathcal{U}\}\{X\}\{\mathcal{K}\}$

open class-inclusions $\{\mathcal{K} = \mathcal{K}\}\{hfe\}\{pe\}\{ssR\}\{ssA\}$

– *Birkhoff’s theorem: every variety is an equational class.*

$\text{birkhoff} : \text{is-set } \mid \mathcal{C} \mid \rightarrow \text{Mod } X (\text{Th } \mathbb{V}) \subseteq \mathbb{V}$

$\text{birkhoff } Cset \{\mathbf{A}\} \alpha = \gamma$

where

$\phi : \Sigma h : (\text{hom } \mathfrak{F} \mathbf{A}) , \text{Epic } \mid h \mid$

$\phi = (\mathfrak{F}\text{-lift-hom } \mathbf{A} \mid \times \mathbf{A} \mid) , \mathfrak{F}\text{-lift-of-epic-is-epic } \mathbf{A} \mid \times \mathbf{A} \mid \parallel \times \mathbf{A} \parallel$

$\text{AiF} : \mathbf{A} \text{ is-hom-image-of } \mathfrak{F}$

$\text{AiF} = (\mathbf{A} , \mid \text{fst } \phi \mid , (\parallel \text{fst } \phi \parallel , \text{snd } \phi)) , \text{refl-}\cong$

$\gamma : \mathbf{A} \in \mathbb{V}$

$\gamma = \text{vhimg } (\mathfrak{F} \in \mathbb{V} Cset) \text{ AiF}$

Some readers might worry that we haven’t quite achieved our goal because what we just proved (`birkhoff`) is not an “if and only if” assertion. Those fears are quickly put to rest by noting that the converse—that every equational class is closed under HSP—was already established in the `UALib.Varieties.Preservation` module. Indeed, there we proved the following identity preservation lemmas:

- (H-id1) $\mathcal{K} \models p \approx q \rightarrow \text{H } \mathcal{K} \models p \approx q$
- (S-id1) $\mathcal{K} \models p \approx q \rightarrow \text{S } \mathcal{K} \models p \approx q$
- (P-id1) $\mathcal{K} \models p \approx q \rightarrow \text{P } \mathcal{K} \models p \approx q$

From these it follows that every equational class is a variety.

9 Conclusion

Now that we have accomplished our initial goal of formalizing Birkhoff’s HSP theorem in Agda, our next goal is to support current mathematical research by formalizing some recently proved theorems. For example, we intend to formalize theorems about the computational complexity of decidable properties of algebraic structures. Part of this effort will naturally involve further work on the library itself, and may lead to new observations about dependent type theory.

One natural question is whether there are any objects of our research that cannot be represented constructively in type theory. As mentioned in the preface, a constructive version of Birkhoff’s theorem was presented by Carlström in [4]. We should determine how the two new hypotheses required by Carlström compare with the assumptions we make in our Agda proof.

Finally, as one of the goals of the Agda UALib project is to make computer formalization of mathematics more accessible to mathematicians working in universal algebra and model theory, we welcome feedback from the community and are happy to field questions about the UALib, how it is installed, and how it can be used to prove theorems that are not yet part of the library.

References

- 1 Clifford Bergman. *Universal Algebra: fundamentals and selected topics*, volume 301 of *Pure and Applied Mathematics (Boca Raton)*. CRC Press, Boca Raton, FL, 2012.
- 2 G Birkhoff. On the structure of abstract algebras. *Proceedings of the Cambridge Philosophical Society*, 31(4):433–454, Oct 1935.
- 3 Venanzio Capretta. Universal algebra in type theory. In *Theorem proving in higher order logics (Nice, 1999)*, volume 1690 of *Lecture Notes in Comput. Sci.*, pages 131–148. Springer, Berlin, 1999. URL: http://dx.doi.org/10.1007/3-540-48256-3_10, doi:10.1007/3-540-48256-3_10.
- 4 Jesper Carlström. A constructive version of birkhoff’s theorem. *Mathematical Logic Quarterly*, 54(1):27–34, 2008. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1002/malq.200710023>, arXiv:<https://onlinelibrary.wiley.com/doi/pdf/10.1002/malq.200710023>, doi:<https://doi.org/10.1002/malq.200710023>.
- 5 Martín Hötzel Escardó. Introduction to univalent foundations of mathematics with Agda. *CoRR*, abs/1911.00580, 2019. URL: <http://arxiv.org/abs/1911.00580>, arXiv:1911.00580.
- 6 Emmanuel Gunther, Alejandro Gadea, and Miguel Pagano. Formalization of universal algebra in Agda. *Electronic Notes in Theoretical Computer Science*, 338:147 – 166, 2018. The 12th Workshop on Logical and Semantic Frameworks, with Applications (LSFA 2017). URL: <http://www.sciencedirect.com/science/article/pii/S1571066118300768>, doi:<https://doi.org/10.1016/j.entcs.2018.10.010>.
- 7 Ralph N. McKenzie, George F. McNulty, and Walter F. Taylor. *Algebras, lattices, varieties. Vol. I*. The Wadsworth & Brooks/Cole Mathematics Series. Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, CA, 1987.
- 8 Ulf Norell. Dependently typed programming in Agda. In *Proceedings of the 6th International Conference on Advanced Functional Programming*, AFP’08, pages 230–266, Berlin, Heidelberg, 2009. Springer-Verlag. URL: <http://dl.acm.org/citation.cfm?id=1813347.1813352>.
- 9 E. Riehl. *Category Theory in Context*. Aurora: Dover Modern Math Originals. Dover Publications, 2017. URL: <http://www.math.jhu.edu/~eriehl/context/>.
- 10 Bas Spitters and Eelis van der Weegen. Type classes for mathematics in type theory. *CoRR*, abs/1102.1323, 2011. URL: <http://arxiv.org/abs/1102.1323>, arXiv:1102.1323.
- 11 The Agda Team. Agda Language Reference section on Axiom K, 2021. URL: <https://agda.readthedocs.io/en/v2.6.1/language/without-k.html>.
- 12 The Agda Team. Agda Language Reference section on Safe Agda, 2021. URL: <https://agda.readthedocs.io/en/v2.6.1/language/safe-agda.html#safe-agda>.
- 13 The Agda Team. Agda Tools Documentation section on Pattern matching and equality, 2021. URL: <https://agda.readthedocs.io/en/v2.6.1/tools/command-line-options.html#pattern-matching-and-equality>.