ALGEBRAIC STRUCTURES IN PROOF ASSISTANT

SYSTEMS

ALGEBRAIC STRUCTURES IN PROOF ASSISTANT SYSTEMS

BY

AKSHOBHYA KATTE MADHUSUDANA, B.Eng.

A REPORT

SUBMITTED TO THE DEPARTMENT OF COMPUTING AND SOFTWARE

AND THE SCHOOL OF GRADUATE STUDIES

OF MCMASTER UNIVERSITY

IN PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTERS OF SCIENCE

Masters of Science (2023)   McMaster University

(Department of Computing and Software)   Hamilton, Ontario, Canada

TITLE: Algebraic Structures in Proof Assistant Systems

AUTHOR: Akshobhya Katte Madhusudana

                    B.Eng. (Computer Science and Engineering),

                    Bangalore University, Bangalore, India

SUPERVISOR: Dr. Jacques Carette

NUMBER OF PAGES: xiii, 88

Lay Abstract

A lay abstract of not more 150 words must be included explaining the key goals and contributions of the thesis in lay terms that is accessible to the general public.

Abstract

Abstract here (no more than 300 words)

Your Dedication

Optional second line

Acknowledgements

Acknowledgements go here.

Contents

List of Figures

List of Tables

Notation, Definitions, and Abbreviations

Notation

$A \leq B$ A is less than or equal to B

Definitions

Challenge   With respect to video games, a challenge is a set of goals presented to the player that they are tasks with completing; challenges can test a variety of player skills, including accuracy, logical reasoning, and creative problem solving

Abbreviations

AI   Artificial intelligence

Declaration of Academic Achievement

The student will declare his/her research contribution and, as appropriate, those of colleagues or other contributors to the contents of the thesis.

Chapter 1

Background Universal Algebra

set relation -> reflexive, symmetric, transitive, equivalence function -> injective , surjective, bijective Product Morphism -> homomorphism, monomorphism, isomorphism

Chapter 2

Background Agda

Agda is a functional programming language developed by Ulf Norell. Agda is used as a proof assistant system that supports higher order logic with dependently typed pattern matching that is used to prove theorems about inductive types.

2.1   Agda Notation

In this section we discuss the programming notations in Agda that will be used in the later chapters of the thesis. A → B denotes a function from set A to set B

a : A denotes a is an element in A

f : A → B denotes that f is a some map from set A to set B

Op1 denotes the unary operation on the set. {a : A} denotes the implicit argument a in A.

```
Op1 : ∀ {ℓ} → Set ℓ → Set ℓ
Op1 A = A → A
```

_· denotes unary operation · and underscore denotes the placement of the argument.

Op2 denotes binary operation on the set

```
Op2 : ∀ {ℓ} → Set ℓ → Set ℓ
Op2 A = A → A → A
```

level (or universe) is a primitive type in Agda.

a ⊔ ℓ denotes the least upper bound of the levels a and ℓ. _·_denotes binary operation ·
. Underscore denotes the placement of the arguments.

2.2   Structure definition

Algebraic structures are defined as record types in Agda. Record types are defined using
the keyword record. Records types are used to group values together and they provide
named fields to generalise dependent product types. The structures are obtained by
wrapping the predicates that are expressed as "is-a" relation. (Hu and Carette, 2021)

```
record IsMagma (· : Op2 A) : Set (a ⊔ ℓ) where
  field
    isEquivalence : IsEquivalence _≈_
    ·-cong        : Congruent2 ·

  open IsEquivalence isEquivalence public
```

In the above example structure IsMagma is defined as a record type with fields isEquiv-
alence and ·-cong. · is a binary operation on set A. a ⊔ ℓ is the least upper bound for the

set. _≈ _is the binary operation argument for IsEquivalence. If a relation P on set A is equivalent to relation Q on set B, then we say f preserves p for some map f from set A to B. Congruent2 · represents that the binary operation · preserves equivalence relation. IsEquivalence and Congruent2 are predicates defined in standard library.

We open the module isEquivalence to be able to use it in defining other structures in the algebra hierarchy. The open statement is made public using the keyword public to be able to re-export the names from another module.

Morphisms of the structure are defined as record type in Agda standard library.

Agda standart library defines the bundled version of the structures that contains the operations of the structures, sets and axioms.

```
record Magma c ℓ : Set (suc (c ⊔ ℓ)) where
  infixl 7 _·_
  infix  4 _≈_
  field
    Carrier : Set c
    _≈_     : Rel Carrier ℓ
    _·_     : Op2 Carrier
    isMagma : IsMagma _≈_ _·_


  open IsMagma isMagma public


  rawMagma : RawMagma _ _
  rawMagma = record { _≈_ = _≈_; _·_ = _·_ }
```

```
open RawMagma rawMagma public

  using (_≉_)
```

Above is the bundled version of IsMagma structure. RawMagma is the raw version of the magma with only the operators and set. infix<l,r> denotes the fixity and precedence of the operator. using keyword is used to export only the fields that are mentioned in its arguments.

When exporting the modules we may need to rename the fields to avoid having duplicate names.

```
open IsMagma *-isMagma public

  using ()

  renaming

  ( ·-cong𝑙   to *-cong𝑙

  ; ·-cong𝑟   to *-cong𝑟

  )
```

Keyword renaming is used to rename the fields. In the above sample code, we rename ·-cong𝑙 to *-cong𝑙 and ·-cong𝑟 to *-cong𝑟.

2.2.1 Proofs in Agda

A setoid is a set with equivalence relation. In Agda beginning of the proof is given using "begin". IsRelatedTo is a type defined to infer arguments even if the underlying equality evaluates.

```
begin_ : ∀ {x y} → x IsRelatedTo y → x ~ y

begin relTo x~y = x~y
```

standard step to relation is defined as step-~

```
step-~ : ∀ x {y z} → y IsRelatedTo z → x ~ y → x IsRelatedTo z
step-~ _ (relTo y~z) x~y = relTo (trans x~y y~z)
```

step using equality is given as

```
step-≈ = Base.step-~
syntax step-≈ x y≈z x≈y = x ≈⟨ x≈y ⟩ y≈z
```

The termination of the proof is given using _■

```
_■ : ∀ x → x IsRelatedTo x
x ■ = relTo refl
```

Agda supports quantifiers. Universal quantifier is denoted as ∀ and existential quantifier is denoted as ∃

Below is the example to the proposition x · (y · z) = (x · y) · z for a semigroup i.e., a Magma with associative property (x · (y · z) = (x · y) · z)

```
x·yz≈xy·z : ∀ x y z → x · (y · z) ≈ (x · y) · z
x·yz≈xy·z x y z = begin
  x · (y · z) ≈⟨ sym (assoc x y z) ⟩
  (x · y) · z ■
```

In the proposition x y z are in set S that is a semigroup. "sym (assoc x y z)" is the reasoning for the proof.

Chapter 3

Introduction

Every thesis needs an introductory chapter

While you're here, you need to go into `definitions.tex` to set all the information needed for the front matter (e.g. title, author) and page header/footer.

You will also find the School of Graduate Studies' preparation guide (August 2021) for theses and reports. I would give it a quick read so you know what's expected.

Chapter 4

Algebraic Structures in Proof Assistant Systems - Survey

The proof assistant systems are computer software that helps to derive formal proofs with a joint effort of computers and humans. Computer proof assistants are used to formalize theories, and extend them by logical reasoning and defining properties. Saqib Nawaz et al. (2019) These systems are used to perform mathematics on computers. The proof assistant systems are widely used in defining and proving rather than doing numerical computations. The automated theorem proving is different from proof assistants in that they have less expressivity and make it almost impossible to define a generic mathematical theory. In Michael and Florian (2021). the author discusses several concerns on considering the proofs that are exclusively verified using a computer to be considered as a valid mathematical proof. However, the proofs written using the proof assistant systems are widely accepted among mathematicians and computer scientists.

The strength of any system is directly dependent on the availability of standard libraries

for those systems. The standard libraries are expected to provide resources to ease the use of such systems. In Jacques Carette and Sharoda (2019), the author discusses the difficulties in building such large libraries. One such problem is to structurally derive algebraic structures from one another in the hierarchy without explicitly defining axioms that become redundant. The author also proposes a solution to make use of the interrelationship in mathematics and thus reduce the efforts in building the library.

We consider the four more commonly used proof assistant systems that are all dependently typed, higher order programming languages that supports (atleast partially) proof by reflection. Proof by reflection is a technique where the system allows to derive proofs by systematic reasoning methods.

Agda 2 is a proof assistant system where proofs are expressed in a functional programming style. The Agda standard library aims to provide tools to ease the effort of writing proofs and also programs. The current version of the Agda standard library (1.7) is fully supported for the changes and developments in Agda. It provides clear documentation for installation, contribution, and style guide for the standard library.

Idris is developed as a functional programming language but is also used as a proof assistant system. The proofs are alike with coq and the type systems in Idris is uniform with agda. Idris 2 is a self-hosted programming language that combines linear-type-system. In this article, Idris 2 and Idris in used interchangeably and refer to Idris 2. Currently, there are no official package managers for Idris 2. However, several versions are under development.

Coq Paulin-Mohring (2012) is a theorem proving system that is written in the Ocaml programming language. It was first released in 1989 and is one of the most widely used proof assistant systems to define mathematical definitions, theory and to write proofs. The mathematical components library (1.12.0) includes various topics from data structures to algebra. In this article, we consider the mathematical component repository (mathcomp) that contains formalized mathematical theories. Mahboubi and Tassi (2021) The latest available release of mathcomp library is 1.12.0. The mathcomp library was started with the Four Colour Theorem to support formal proof of the odd order theorem.

Lean mathlib Community (2020) is an open-source project by Microsoft Research. Lean is a proof assistant system written in C++. The last official version of Lean was 3.4.2 and is now supported by the lean community. Lean 4 is the latest version of Lean and is a complete rewrite of previous versions of Lean. The mathlib mathlib Community (2020) library for lean 3 has the most coverage of algebra compared to the other 3 proof assistant systems discussed in the paper. The mathlib library of Lean is also maintained by the lean community for community versions of lean. It was developed on a small library that was in lean. It contained definitions of natural numbers, integers, and lists and had some coverage over algebra hierarchy. The latest version of mathlib has over 2794 definitions of algebra [3].

The main aim of this paper is to provide documentation for the algebraic coverage in various proof assistant systems. The most commonly used proof assistant systems are Agda, Idris2, Coq, and Lean. In this article, the latest available versions are considered i.e., Agda standard library 1.7, Idris 2.0,The Mathematical Components Library 1.13.0,

and The Lean mathematical library.

4.1 Experimental setup

It is not time efficient to manually look for the definitions in a large library. The source code of the standard libraries of Agda, Idris, Coq and lean are publicly available. We created a web crawler that extracts the code from the source code webpage and built a regular expression that is unique to each system to extract definitions. Thus a part of the process of building the table 1. was automated. Since the standard libraries are open source projects, it is difficult to maintain uniformity in the code. For example the definition might start with comment in the same line or structure parameters might be written in a new line. All this makes it difficult to correctly build the regular expression and will necessitate the task of verifying the results manually to some extent.

The rest of the article is structured as follows. Section 2 discuss about the algebraic structure definitions and its coverage in the proof assistant systems, while the section 3 covers the morphism definitions in those systems. The properties and solvers coverage in presented in section 4. The last section of the paper is the conclusion and discussion.

4.2 Algebraci Structures

The Agda standard library provides definitions with bundled versions of several algebraic structures. Algebra hierarchy is followed in defining structures Michael and Florian (2021). As an example, a semigroup is derived from magma and a monoid from semigroup.

```
record IsMagma (· : Op₂ A) : Set (a ⊔ ℓ) where

  field
    isEquivalence : IsEquivalence _≈_
    ·-cong        : Congruent₂ ·


  open IsEquivalence isEquivalence public

record IsSemigroup (· : Op₂ A) : Set (a ⊔ ℓ) where

  field
    isMagma : IsMagma ·
    assoc   : Associative ·


  open IsMagma isMagma public
```

The same follows for the bundle definitions of respective structures. Since the current version of the library has a limited number of structures, there might arise a problem of extending the hierarchy as described in [2]. One exemption for this hierarchical definition is the definition of a lattice. A lattice is defined independently in the standard library to overcome the redundant idempotent fields. A lattice structure that is defined in terms of join and meet semilattice is being added as a biased structure. The 1.7 version of the agda standard library has the definitions of structures with the respective bundle versions of Magma, Commutative Magma, to Ring, CommutativeRing, and Boolean Algebra. Another definition of most of the above algebraic structures is provided as a direct product of two other instances of algebraic structures. However, from semigroups, the structures are defined in terms of relevant categories. The structures also include

respective bundle definitions. A module is an abelian group with the ring of scalars. The ring of scalars has an identity element. The agda standard library defines left, right, and bi semimodules and modules. A similar hierarchical approach as other algebraic structures is followed in defining modules. As an example, a module is defined using bimodules and bimodules using bi-semimodules. An alternative definition of modules is given in "Algebra.Module.Structure.Biased". The structures have respective bundled versions.

In Idris 2, there is a considerable overlap of abstract algebra and category theory. The library defines various algebraic structures that include semigroup, monoid, group, abelian-group, semiring, and ring. It follows a hierarchical approach in defining structures similar to that in agda. For example, a semigroup is defined as a set with a binary operation that is associative and a monoid is defined in terms of semigroup with an identity element. Idris addresses identity as a neutral element.

```
interface Semigroup t where
  (<+>) : t -> t -> t
  semigroupOpIsAssociative : (l, c, r : t) -> l <+> (c <+> r) = (l <+> c) <+> r


interface Semigroup t => Monoid t where
  neutral : t
  monoidNeutralIsNeutralL : (l : t) -> l <+> neutral = l
  monoidNeutralIsNeutralR : (r : t) -> neutral <+> r = r
```

The algebra structures design hierarchy of the mathcomp library is inspired by the Packing mathematical structures. The ssralg file defines most of the basic algebraic

structures with their type, packers, and canonical properties. The hierarchy extends from Zmodule, rings to ring morphisms. The countalg file extends ssralg file to define countable types.

The mathlib extends the algebra hierarchy from semigroup to ordered fields. The library defines instances of free magma, free semigroup, free Abelian group, etc. An example of semigroup structure definition in the library is given below:

```
structure semigroup (G : Type u) :
  Type u
  mul : G → G → G
  mul_assoc : forall (a b c : G), (a * b) * c = a * b * c
```

Other instances of semigroups are derived from the definition of semigroup structure such as commutative semigroup, left and right cancellative semgroup. Similar definitions are extended from monoid and other structures.

Table 4.1: Algebraic structures in proof assistant systems

Algebraic Structure	Agda	Coq	Idris	Lean
Magma	✓	-	-	-
Commutative Magma	✓	-	-	-
Selective Magma	✓	-	-	-
Continued on next page				

Table 4.1 – continued from previous page

Algebraic Structure	Agda	Coq	Idris	Lean
IdempotentMagma	✓	-	-	-
AlternativeMagma	✓	-	-	-
FlexibleMagma	✓	-	-	-
MedialMagma	✓	-	-	-
SemiMedialMagma	✓	-	-	-
Semigroup	✓	✓	✓	✓
Band	✓	-	-	-
Commutative Semigroup	✓	-	-	✓
Semilattice	✓	-	-	✓
Unital magma	✓	-	-	-
Monoid	✓	✓	✓	✓
Commutative monoid	✓	✓	-	✓
Idempotent commutative monoid	✓	-	-	-
Bounded Semilattice	✓	-	-	-
Bounded Meetsemilattice	✓	-	-	-
Bounded Joinsemilattice	✓	-	-	-
Invertible Magma	✓	-	-	-
IsInvertible UnitalMagma	✓	-	-	-
Quasigroup	✓	-	-	-
Loop	✓	-	-	-
Continued on next page				

Table 4.1 – continued from previous page

Algebraic Structure	Agda	Coq	Idris	Lean
Moufang Loop	✓	-	-	-
Left Bol Loop	✓	-	-	-
Middle Bol Loop	✓	-	-	-
Right Bol Loop	✓	-	-	-
NilpotentGroup	-	-	-	✓
CyclicGroup	-	-	-	✓
SubGroup	-	-	-	✓
Group	✓	✓	✓	✓
Abelian group	✓	-	✓	✓
Lattice	✓	-	-	✓
Distributive lattice	✓	-	-	-
Near semiring	✓	-	-	-
Semiringwithout one	✓	-	-	-
Idempotent Semiring	✓	-	-	-
Commutative semiring without one	✓	-	-	-
Semiring without annihilating zero	✓	-	-	-
Semiring	✓	✓	-	✓
Commutative semiring	✓	-	-	✓
Non associative ring	✓	-	-	-
Nearring	✓	-	-	-
<td colspan="5" align="right">Continued on next page</td>

Table 4.1 – continued from previous page

Algebraic Structure	Agda	Coq	Idris	Lean
Quasiring	✓	-	-	-
Local ring	-	-	-	✓
Noetherian ring	-	-	-	✓
Ordered ring	-	-	-	✓
Cancellative commutative semiring	✓	-	-	-
Sub ring	-	-	-	✓
Ring	✓	✓	✓	✓
Unit Ring	✓	✓	✓	-
Commutative Unit ring	-	✓	-	-
Commutative ring	✓	✓	-	✓
Integral Domain	-	✓	-	-
LieAlgebra	-	-	-	✓
LieRing module	-	-	-	✓
Lie module	-	-	-	✓
Boolean algebra	✓	-	-	-
Preleft semimodule	✓	-	-	-
Left semimodule	✓	-	-	-
Preright semimodule	✓	-	-	-
right semimodule	✓	-	-	-
Bi semimodule	✓	-	-	-
			Continued on next page	

17

Table 4.1 – continued from previous page

Algebraic Structure	Agda	Coq	Idris	Lean
Semimodule	✓	-	-	-
Left module	✓	✓	-	-
Right module	✓	-	-	-
Bi module	✓	-	-	-
Module	✓	✓	-	✓
Field	-	✓	✓	✓
Decidable Field	-	✓	-	-
Closed field	-	✓	-	-
Algebra	-	✓	-	-
Unit algebra	-	✓	-	✓
Lalgebra	-	✓	-	-
Commutative unit algebra	-	✓	-	-
Commutative algebra	-	✓	-	-
NumDomain	-	✓	-	-
Normed Zmodule	-	✓	-	-
Num field	-	✓	-	-
Real domain	-	✓	-	-
Real field	-	✓	-	-
Real closed field	-	✓	-	-
Vector space	-	✓	-	-
Continued on next page				

Table 4.1 – continued from previous page

Algebraic Structure	Agda	Coq	Idris	Lean
Zmodule Quotients type	-	✓	-	-
Ring Quotient type	-	✓	-	-
Unit rint quotient type	-	✓	-	-
Additive group	-	✓	-	-
characteristic zero	-	-	-	✓
Domain	-	-	-	✓
Chain Complex	-	-	-	✓
Kleene Algebra	✓	-	-	-
IsHeytingCommutativeRing	✓	-	-	-
IsHeytingField	✓	-	-	-

4.3 Morphism

One of the benefits of the Agda standard library is that it provides morphisms for the structures defined in the library. A raw bundle instance is defined in Algebra. Bundles and the morphisms for those raw structures are provided. For example, raw magma is used in magma morphisms. The library defines homomorphism, monomorphism, and isomorphism for those structures. The library also provides the composition of morphisms between algebraic structures. The morphism definitions for Magma, Monoid, Group, NearSemiring, Semiring, Ring, Lattice are available in the standard library. An example of magma morphisms as defined in the standard library is as follows.

```
record IsMagmaHomomorphism (⟦_⟧ : A → B) : Set (a ⊔ ℓ₁ ⊔ ℓ₂) where

  field

    isRelHomomorphism : IsRelHomomorphism _≈₁_ _≈₂_ ⟦_⟧

    homo              : Homomorphic₂ ⟦_⟧  _·_ _∘_


  open IsRelHomomorphism isRelHomomorphism public

    renaming (cong to ⟦⟧ -cong)
```

Similar definitions for monomorphism and isomorphism are included in agda standard library.

The morphism definitions in the Idris library define morphisms in category theory. A group homomorphism is a structure-preserving function between two groups and is defined as follows :

```
interface (Group a, Group b) => GroupHomomorphism a b where

  to : a -> b


  toGroup : (x, y : a) ->  to (x <+> y) = (to x) <+> (to y)
```

The group theory directory defines groups, group morphisms, subgroups, cyclic, nilpotent groups, and isomorphism theorems. There is no group homomorphism instead, it is defined with proofs for map-one and map-mul for monoid homomorphism. The definition of monoid homomorphism is give below:

```
structure monoid_hom (M : Type*) (N : Type*) [mul_one_class M] [mul_one_class N]

  extends one_hom M N, mul_hom M N
```

The mathlib library extends monoid and groups to define rings and ring morphisms. Bundled structure is used to define ring morphisms.

4.4   Properties

The Agda standard library provides constructs of modules such as a bi-product construct and tensor unit using two R-modules. The library also includes the relation between function properties with basal setoid and sets for propositional equalities. The library includes ring, monoid solvers for equations of the same. However, these solvers are under construction and not optimized for performance.

The coq library has rings and field tactics to achieve algebraic manipulations in some of the algebraic structures. The library also includes specialized tactics such as interval and gappa to work with real numbers and floating point nubmers. Paulin-Mohring (2012)

The Idris library defines properties or laws of algebraic structures. The unique-Inverse defines that the inverses of monoids are unique. Other laws on groups include self-squaring i.e., identity element of a group is self-squaring, inverse elements of a group satisfy the commutative property, laws of double negation. It also defines squareId-Commutative i.e., a group is abelian if every square in a group is neutral, inverseNeutralIsNeutral, and other properties of an algebraic group. The Latin-square-property is defined as for any two elements a and b, ax =b and ya = b exists. Other algebraic properties for groups are y = z if x + y = x + z, y = z if y + x = z + x, ab = 0 -> a = b-1, and ab = 0 -> a-1 = b. An example of a definition is shown below.

```
public export

neutralProductInverseL : Group ty => (a, b : ty) ->

  a <+> b = neutral {ty} -> inverse a = b

neutralProductInverseL a b prf =

  cancelLeft a (inverse a) b $

    trans (groupInverseIsInverseL a) $ sym prf
```

The library also includes laws on homomorphism that homomorphism over group preserves identity and inverses. Some laws on ring structures are also included in the library such as x0 = 0, (-x)y = -(xy), x(-y) = -(xy), (-x)(-y) = xy, (-1)x = -x, and x(-1) = -x. The algebraic coverage of Idris 2 is limited and is under development. There are no official definitions for solvers or higher structures such as modules, fields, or vector space. The Idris 2 is comparatively new and is under continuous development to strengthen the language and also as a mechanical reasoning system.

The mathlib library of Lean 3 includes algebra over rings such as associative algebra over a commutative ring, Lie algebra, Clifford algebra, etc. Lie algebra is defined as a module satisfying Jacobi identity. Without scalar multiplication, a lie algebra is a lie ring. The library extends rings to define fields and division ring covering many aspects of fields such as the existence of closure for a field, Galois correspondence, rupture field, and others.

Chapter 5

Theory Of Quasigroup and Loop in Agda

Applications of non associative algebras are explored in various fields of study. For example, Einstein's formula of addition of velocities gives a loop structure, Quasigroups of various orders are used in field of cryptography, Lie algebra is used in differential geometry. Proof assistant systems such as Agda are helpful in verifying some of the properties of these structures. They are interactive software that help to derive complex mathematical proofs. In this chapter we formalize two important non associative algebras - quasigroup, loop structure. A Quasigroup (Q, ·, /, \) is a type (2,2,2) algebra for which the binary operations \and / are defined such that division is always possible. A loop is a quasigroup with identity. We explore morphisms and direct product for these structures and derive proofs for some of the properties of these structures.

5.1   Definition

A set that has a binary operation is called Magma. In this case a Magma is total and should not be confused with groupoid that need not be total. Let Q be a non empty set. Left and division is defined with identities.

$$y = x \cdot (x \backslash y) \tag{5.1.1}$$

$$y = x \backslash (x \cdot y) \tag{5.1.2}$$

$$y = (y/x) \cdot x \tag{5.1.3}$$

$$y = (y \cdot x)/x \tag{5.1.4}$$

The Agda definition is given below

```
LeftDivides^l  : Op₂ A → Op₂ A → Set _
LeftDivides^l  _·_  _\\_ = ∀ x y → (x · (x \\ y)) ≈ y


LeftDivides^r : Op₂ A → Op₂ A → Set _
LeftDivides^r _·_ _\\_ = ∀ x y → (x \\ (x · y)) ≈ y


RightDivides^l  : Op₂ A → Op₂ A → Set _
RightDivides^l  _·_ _//_ = ∀ x y → ((y // x) · x) ≈ y


RightDivides^r : Op₂ A → Op₂ A → Set _
RightDivides^r _·_ _//_ = ∀ x y → ((y · x) // x) ≈ y
```

We can combine the left and right division as follows

```
LeftDivides : Op₂ A → Op₂ A → Set _
LeftDivides · \\ = (LeftDivides¹ · \\) × (LeftDividesʳ · \\)


RightDivides : Op₂ A → Op₂ A → Set _
RightDivides · // = (RightDivides¹ · //) × (RightDividesʳ · //)
```

Note that we use // and \\instead of / and \respectively to overcome the conflict with overloaded or escape characters.

The Quasigroup structure can be structurally derived from Magma in Agda as

```
record IsQuasigroup (· \\ // : Op₂ A) : Set (a ⊔ ℓ) where
  field
    isMagma        : IsMagma ·
    \\-cong        : Congruent₂ \\
    //-cong        : Congruent₂ //
    leftDivides    : LeftDivides · \\
    rightDivides   : RightDivides · //


  open IsMagma isMagma public
```

A loop is a quasigroup that has identity element.

$$x \cdot e = e \cdot x = x \tag{5.1.5}$$

```
LeftIdentity : A → Op₂ A → Set _
LeftIdentity e _·_ = ∀ x → (e · x) ≈ x


RightIdentity : A → Op₂ A → Set _
RightIdentity e _·_ = ∀ x → (x · e) ≈ x


Identity : A → Op₂ A → Set _
Identity e · = (LeftIdentity e ·) × (RightIdentity e ·)
```

Loop structure can be structurally derived from quasigroup.

```
record IsLoop (· \\ // : Op₂ A) (ε : A) : Set (a ⊔ ℓ) where
  field
    isQuasigroup : IsQuasigroup · \\ //
    identity          : Identity ε ·


  open IsQuasigroup isQuasigroup public
```

A loop is called a right bol loop if it satisfies the identity (Equation 5.1.6)

$$((z{\cdot}x){\cdot}y){\cdot}x = z{\cdot}((x{\cdot}y){\cdot}x) \tag{5.1.6}$$

A loop is called a left bol loop if it satisfies the identity (Equation 5.1.7)

$$x{\cdot}(y{\cdot}(x{\cdot}z)) = (x{\cdot}(y{\cdot}x)){\cdot}z \tag{5.1.7}$$

A loop is called middle bol loop if it satisfies the identity (Equation 5.1.8)

$$(z{\cdot}x){\cdot}(y{\cdot}z) = z{\cdot}((x{\cdot}y){\cdot}z) \qquad\qquad (5.1.8)$$

A left-right bol loop is called a moufang loop if it satisfies identity (Equation 5.1.9)

$$(z{\cdot}x){\cdot}(y{\cdot}z) = z{\cdot}((x{\cdot}y){\cdot}z) \qquad\qquad (5.1.9)$$

```
LeftBol : Op₂ A → Set _
LeftBol _·_ = ∀ x y z → (x · (y · (x · z))) ≈ ((x · (y · x)) · z )


RightBol : Op₂ A → Set _
RightBol _·_ = ∀ x y z → (((z · x) · y) · x) ≈ (z · ((x · y) · x))


MiddleBol : Op₂ A → Op₂ A  → Op₂ A  → Set _
MiddleBol _·_ _\\_ _//_ = ∀ x y z → (x · ((y · z) \\ x)) ≈ ((x // z) · (y \\ x))

Identical : Op₂  A → Set _
Identical _·_ = ∀ x y z → ((z · x) · (y · z)) ≈ (z · ((x · y) · z))
```

5.2 Morphism

A structure preserving map f between two structures of same type is called morphism or homomorphism. That is f : A → B and · is an operation on the structure then homomorphism is defined as f(x · y) = f(x) · f(y). A homomorphism that is injective is called monomorphism. If the structures are identical that is they are more than just similar

in structure then we can compare the structures with isomorphism. A homomorphism that is bijective is called isomorphism. The quasigroup homomorphism preserves both left and right division operations.

```
record IsQuasigroupHomomorphism (⟦_⟧ : A → B) : Set (a ⊔ ℓ₁ ⊔ ℓ₂) where
    field
      isRelHomomorphism :  IsRelHomomorphism _≈₁_ _≈₂_ ⟦_⟧
      ·-homo              : Homomorphic₂ ⟦_⟧ _·₁_ _·₂_
      \\-homo             : Homomorphic₂ ⟦_⟧ _\\₁_ _\\₂_
      //-homo             : Homomorphic₂ ⟦_⟧ _//₁_ _//₂_


    open IsRelHomomorphism isRelHomomorphism public
      renaming (cong to ⟦⟧-cong)

 record IsQuasigroupMonomorphism (⟦_⟧ : A → B) : Set (a ⊔ ℓ₁ ⊔ ℓ₂) where
    field
      isQuasigroupHomomorphism : IsQuasigroupHomomorphism ⟦_⟧
      injective                : Injective ⟦_⟧


    open IsQuasigroupHomomorphism isQuasigroupHomomorphism public

 record IsQuasigroupIsomorphism (⟦_⟧ : A → B) : Set (a ⊔ b ⊔ ℓ₁ ⊔ ℓ₂) where
     field
       isQuasigroupMonomorphism : IsQuasigroupMonomorphism ⟦_⟧
       surjective               : Surjective ⟦_⟧


     open IsQuasigroupMonomorphism isQuasigroupMonomorphism public
```

28

The loop morphism preserves left and right divisions along with the identity element

```
record IsLoopHomomorphism (⟦_⟧ : A → B) : Set (a ⊔ ℓ₁ ⊔ ℓ₂) where
   field
      isQuasigroupHomomorphism : IsQuasigroupHomomorphism ⟦_⟧
      ε-homo                   : Homomorphic₀ ⟦_⟧ ε₁ ε₂


   open IsQuasigroupHomomorphism isQuasigroupHomomorphism public


 record IsLoopMonomorphism (⟦_⟧ : A → B) : Set (a ⊔ ℓ₁ ⊔ ℓ₂) where
   field
      isLoopHomomorphism  : IsLoopHomomorphism ⟦_⟧
      injective           : Injective ⟦_⟧


   open IsLoopHomomorphism isLoopHomomorphism public


 record IsLoopIsomorphism (⟦_⟧ : A → B) : Set (a ⊔ b ⊔ ℓ₁ ⊔ ℓ₂) where
   field
      isLoopMonomorphism  : IsLoopMonomorphism ⟦_⟧
      surjective          : Surjective ⟦_⟧


     open IsLoopMonomorphism isLoopMonomorphism public
```

5.3   Morphism composition

If f is a morphism such that f : a → b and g is a morphism on same structure such that g : b → c then composition of morphism can be defined as g ∘ f : a → c.

```
isQuasigroupHomomorphism : IsQuasigroupHomomorphism Q₁ Q₂ f
  → IsQuasigroupHomomorphism Q₂ Q₃ g
  → IsQuasigroupHomomorphism Q₁ Q₃ (g ∘ f)
isQuasigroupHomomorphism f-homo g-homo = record
  { isRelHomomorphism = isRelHomomorphism
              F.isRelHomomorphism
              G.isRelHomomorphism
  ; ∙-homo    = λ x y → ≈₃-trans
              (G.⟦⟧-cong ( F.∙-homo x y ))
              ( G.∙-homo (f x) (f y) )
  ; \\-homo    = λ x y → ≈₃-trans
              (G.⟦⟧-cong ( F.\\-homo x y ))
              ( G.\\-homo (f x) (f y) )
  ; //-homo    = λ x y → ≈₃-trans
              (G.⟦⟧-cong ( F.//-homo x y ))
              ( G.//-homo (f x) (f y) )
  } where module F = IsQuasigroupHomomorphism f-homo;
          module G = IsQuasigroupHomomorphism g-homo
```

```
isLoopHomomorphism : IsLoopHomomorphism L₁ L₂ f
  → IsLoopHomomorphism L₂ L₃ g → IsLoopHomomorphism L₁ L₃ (g ∘ f)
isLoopHomomorphism f-homo g-homo = record
  { isQuasigroupHomomorphism = isQuasigroupHomomorphism ≈₃-trans
                    F.isQuasigroupHomomorphism G.isQuasigroupHomomorphism
  ; ε-homo                = ≈₃-trans (G.⟦⟧-cong F.ε-homo) G.ε-homo
  } where module F = IsLoopHomomorphism f-homo;
          module G = IsLoopHomomorphism g-homo
```

Monomorphism and isomorphism compositions constructs for quasigroup and loop are defined similar to homomorphism and can be found in agda standard library.

5.4   DirectProduct

The direct product M × N of two quasigroups M and N is defined as a pair (m,n) where m ∈ M and n ∈ N. The direct product construct of left (right/middle) bol loop and moufang loop can be found in agda standard library and can be derived from loop structure.

```
quasigroup : Quasigroup a ℓ₁ → Quasigroup b ℓ₂
                 → Quasigroup (a ⊔ b) (ℓ₁ ⊔ ℓ₂)
quasigroup M N = record
  { _\\_  = zip M._\\_ N._\\_
  ; _//_   = zip M._//_ N._//_
  ; isQuasigroup = record
    { isMagma = Magma.isMagma (magma M.magma N.magma)
    ; \\-cong = zip M.\\-cong N.\\-cong
    ; //-cong = zip M.//-cong N.//-cong
    ; leftDivides = (λ x y → M.leftDividesˡ ,
               N.leftDividesˡ <*> x <*> y),
               (λ x y → M.leftDividesʳ ,
               N.leftDividesʳ <*> x <*> y)
    ; rightDivides = (λ x y → M.rightDividesˡ ,
               N.rightDividesˡ <*> x <*> y),
               (λ x y → M.rightDividesʳ ,
               N.rightDividesʳ <*> x <*> y)
    }
  } where module M = Quasigroup M; module N = Quasigroup N
```

```
loop : Loop a ℓ₁ → Loop b ℓ₂ → Loop (a ⊔ b) (ℓ₁ ⊔ ℓ₂)

loop M N = record

  { ε = M.ε , N.ε

  ; isLoop = record

    { isQuasigroup = Quasigroup.isQuasigroup

                  (quasigroup M.quasigroup N.quasigroup)

    ; identity = (M.identityˡ , N.identityˡ <*>_),

                    (M.identityʳ , N.identityʳ <*>_)

    }

  } where module M = Loop M; module N = Loop N
```

5.5 Properties

In this section we prove some of the properties of quasigroups and loops in Agda.

5.5.1 Properties of Quasigroup

Let $(Q, \cdot, /, \backslash)$ be a quasigroup then

a) Q is cancellative A quasigroup is left cancellative if $x \cdot y = x \cdot z$ then $y = z$ and a quasigroup is right cancellative if $y \cdot x = z \cdot x$ then $y = z$. A quasigroup is cancellative if it is both left and right cancellative.

b) $\forall x, y, z \in Q$: $x \cdot y = z$ then $y = x \backslash z$

c) $\forall x, y, z \in Q$: $x \cdot y = z$ then $x = z / y$

Proof:

a)

```
cancelˡ : LeftCancellative _·_
cancelˡ x {y} {z} eq = begin
  y                ≈⟨ sym( leftDividesʳ  x y) ⟩
  x \\ (x · y)  ≈⟨ \\-congˡ eq ⟩
  x \\ (x · z)  ≈⟨ leftDividesʳ  x z ⟩
  z                ∎
```


```
cancelʳ : RightCancellative _·_
cancelʳ {x} y z eq = begin
  y                ≈⟨ sym( rightDividesʳ  x y) ⟩
  (y · x) // x  ≈⟨ //-congʳ  eq ⟩
  (z · x) // x  ≈⟨ rightDividesʳ  x z ⟩
  z                ∎
```


```
cancel : Cancellative _·_
cancel = cancelˡ , cancelʳ
```

b)

```
y≈x\z : ∀ x y z → x · y ≈ z → y ≈ x \\  z
y≈x\z x y z eq = begin
  y                ≈⟨ sym (leftDividesʳ x y) ⟩
  x \\  (x · y) ≈⟨ \\ -congˡ eq ⟩
  x \\  z        ∎
```

c)

```
x≈z/y : ∀ x y z → x · y ≈ z → x ≈ z // y

x≈z/y x y z eq = begin

  x                 ≈⟨ sym (rightDividesʳ y x) ⟩

  (x · y) // y ≈⟨ //-congʳ eq ⟩

  z // y        ∎
```

5.5.2 Properties of Loop

Properties of division operation holds for a loop.

Let (L, ·, /, \) be a Loop with identity x · e = x then the following properties holds

a)$\forall x \in L$: x / x = e

b)$\forall x \in L$: x \x = e

c)$\forall x \in L$: e \x = x

d)$\forall x \in L$: x / e = x

Proof:

a)

```
x//x≈ϵ : ∀ x → x // x ≈ ϵ

x//x≈ϵ x = begin

  x // x       ≈⟨ //-congʳ (sym (identityˡ x)) ⟩

  (ϵ · x) // x  ≈⟨ rightDividesʳ x ϵ ⟩

  ϵ              ∎
```

b)

```
x\\x≈ϵ : ∀ x → x \\ x ≈ ϵ

x\\x≈ϵ x = begin

  x \\ x       ≈⟨ \\-cong¹ (sym (identity^r x )) ⟩

  x \\ (x · ϵ) ≈⟨ leftDivides^r x ϵ ⟩

  ϵ                  ∎
```

c)

```
ϵ\\x≈x : ∀ x → ϵ \\ x ≈ x

ϵ\\x≈x x = begin

  ϵ \\ x        ≈⟨ sym (identity^l (ϵ \\ x)) ⟩

  ϵ · (ϵ \\ x) ≈⟨ leftDivides^l ϵ x ⟩

  x                  ∎
```

d)

```
x//ϵ≈x : ∀ x → x // ϵ ≈ x

x//ϵ≈x x = begin

 x // ϵ        ≈⟨ sym (identity^r (x // ϵ)) ⟩

 (x // ϵ) · ϵ  ≈⟨ rightDivides^l ϵ x ⟩

 x                  ∎
```

5.5.3   Properties of Middle bol loop

Let (M, ·, /, \) be a middle bol loop then the following identities holds.

a)$\forall xyz \in M$: x · ((y · x) \x) = y \x

b)$\forall\,xyz \in M$: x · ((x · z) \x) = x // z

c)$\forall\,xyz \in M$: x · (z \x) ≈ (x / z) · x

d)$\forall\,xyz \in M$: (x / (y · z)) · x ≈ (x / z) · (y \x)

e)$\forall\,xyz \in M$: (x / (y · x)) · x ≈ y \x

f)$\forall\,xyz \in M$: (x / (x · z)) · x ≈ x / z

   Proof:

a)

```
xyx\x≈y\\x : ∀ x y → x · ((y · x) \\ x) ≈ y \\ x

xyx\x≈y\\x x y = begin

  x · ((y · x) \\ x)   ≈⟨ middleBol x y x ⟩

  (x // x) · (y \\ x) ≈⟨ ·-congʳ (x//x≈ϵ x) ⟩

  ϵ · (y \\ x)         ≈⟨ identityˡ ((y \\ x)) ⟩

  y \\ x              ■
```

b)

```
xxz\\x≈x//z : ∀ x z → x · ((x · z) \\ x) ≈ x // z

xxz\\x≈x//z x z = begin

  x · ((x · z) \\ x)  ≈⟨ middleBol x x z ⟩

  (x // z) · (x \\ x) ≈⟨ ·-congˡ (x\\x≈ϵ x) ⟩

  (x // z) · ϵ        ≈⟨ identityʳ ((x // z)) ⟩

  x // z              ■
```

c)

```
xz\\x≈x//zx : ∀ x z → x · (z \\ x) ≈ (x // z) · x

xz\\x≈x//zx x z = begin

  x · (z \\ x)        ≈⟨ ·-cong¹ (\\-congʳ( sym (identity¹ z))) ⟩

  x · ((ϵ · z) \\ x) ≈⟨ middleBol x ϵ z ⟩

  x // z · (ϵ \\ x) ≈⟨ ·-cong¹ (ϵ\\x≈x x) ⟩

  x // z · x          ∎
```

d)

```
x//yzx≈x//zy\\x : ∀ x y z → (x // (y · z)) · x ≈ (x // z) · (y \\ x)

x//yzx≈x//zy\\x x y z = begin

 (x // (y · z)) · x  ≈⟨ sym (xz\\x≈x//zx x ((y · z))) ⟩

 x · ((y · z) \\ x)  ≈⟨ middleBol x y z ⟩

 (x // z) · (y \\ x) ∎
```

e)

```
x//yxx≈y\\x : ∀ x y → (x // (y · x)) · x ≈ y \\ x

x//yxx≈y\\x x y = begin

  (x // (y · x)) · x  ≈⟨ x//yzx≈x//zy\\x  x y x ⟩

  (x // x) · (y \\ x) ≈⟨ ·-congʳ(x//x≈ϵ x) ⟩

  ϵ · (y \\ x)         ≈⟨ identity¹ ((y \\ x)) ⟩

  y \\ x               ∎
```

```
f)

x//xzx≈x//z : ∀ x z → (x // (x · z)) · x ≈ x // z

x//xzx≈x//z x z = begin

  (x // (x · z)) · x  ≈⟨ x//yzx≈x//zy\\x x x z ⟩

  (x // z) · (x \\ x) ≈⟨ ·-cong¹ (x\\x≈ϵ x) ⟩

  (x // z) · ϵ         ≈⟨ identityʳ (x // z) ⟩

  x // z                ∎
```

5.5.4   Properties of Moufang Loop

Let $(M, \cdot, /, \backslash)$ be a moufang loop then the following identities holds.

a) Moufang loop is alternative.

A moufang loop is left alternative if it satisfies $(x \cdot x) \cdot y = x \cdot (x \cdot y)$, a moufang loop is right alternative if it satisfies $x \cdot (y \cdot y) = (x \cdot y) \cdot y$ and if a moufang loop alternative if it is both left and right alternative.

b) Moufang loop is flexible

A Moufant loop is flexible if it satisfies flexible identity $(x \cdot y) \cdot x = x \cdot (y \cdot x)$

c)$\forall xyz \in M$: $z \cdot (x \cdot (z \cdot y)) = ((z \cdot x) \cdot z) \cdot y$

d)$\forall xyz \in M$: $x \cdot (z \cdot (y \cdot z)) = ((x \cdot z) \cdot y) \cdot z$

e)$\forall xyz \in M$: $z \cdot ((x \cdot y) \cdot z) = (z \cdot (x \cdot y)) \cdot z$

Proof:

a)

```
alternativeˡ : LeftAlternative _·_

alternativeˡ x y = begin

  (x · x) · y        ≈⟨ ·-congʳ (·-congˡ (sym (identityˡ x))) ⟩

  (x · (ε · x)) · y ≈⟨ sym (leftBol x ε y) ⟩

  x · (ε · (x · y)) ≈⟨ ·-congˡ (identityˡ ((x · y))) ⟩

  x · (x · y)        ∎


alternativeʳ : RightAlternative _·_

alternativeʳ x y = begin

  x · (y · y)        ≈⟨ ·-congˡ (·-congʳ(sym (identityʳ y))) ⟩

  x · ((y · ε) · y)  ≈⟨ sym (rightBol y ε x) ⟩

  ((x · y) · ε ) · y ≈⟨ ·-congʳ (identityʳ ((x · y))) ⟩

  (x · y) · y        ∎


alternative : Alternative _·_

alternative = alternativeˡ , alternativeʳ
```

b)

```
flex : Flexible _·_

flex x y = begin

  (x · y) · x        ≈⟨ ·-congˡ (sym (identityˡ x)) ⟩

  (x · y) · (ε · x) ≈⟨ identical y ε x ⟩

  x · ((y · ε) · x) ≈⟨ ·-congˡ (·-congʳ (identityʳ y)) ⟩

  x · (y · x)        ∎
```

c)

```
z·xzy≈zxz·y : ∀ x y z → (z · (x · (z · y))) ≈ (((z · x) · z) · y)

z·xzy≈zxz·y x y z = sym (begin

  ((z · x) · z) · y ≈⟨ (·-congʳ  (flex z x )) ⟩

  (z · (x · z)) · y ≈⟨ sym (leftBol z x y) ⟩

  z · (x · (z · y)) ■)
```

d)

```
x·zyz≈xzy·z : ∀ x y z → (x · (z · (y · z))) ≈ (((x · z) · y) · z)

x·zyz≈xzy·z x y z = begin

  x · (z · (y · z))  ≈⟨ (·-congˡ  (sym (flex z y ))) ⟩

  x · ((z · y) ·  z) ≈⟨ sym (rightBol z y x) ⟩

  ((x · z) · y) · z  ■
```

e)

```
z·xyz≈zxy·z : ∀ x y z → (z · ((x · y) · z)) ≈ ((z · (x · y)) · z)

z·xyz≈zxy·z x y z = sym (flex z (x · y))
```

Chapter 6

Theory of Semigroup and Ring in Agda

6.1 Definition

A set that has a binary operation is called Magma. Magma with associative property is called a semigroup. For binary operation $\cdot$ on a set S, the associative property is defined as

$$\forall\, xyz \in S : x{\cdot}(y{\cdot}z) = (x{\cdot}y){\cdot}z. \tag{6.1.1}$$

A semigroup that satisfies commutative property is called commutative semigroup. For binary operation $\cdot$ on a set S, commutative property is defined as

$$\forall\, xy \in S : x{\cdot}y = y{\cdot}x \tag{6.1.2}$$

The definition of associative and commutative property in Agda.

```
Associative : Op₂ A → Set _

Associative _·_ = ∀ x y z → ((x · y) · z) ≈ (x · (y · z))


Commutative : Op₂ A → Set _

Commutative _·_ = ∀ x y → (x · y) ≈ (y · x)
```

The Semigroup structure can be structurally derived from Magma in Agda as

```
record IsSemigroup (· : Op₂ A) : Set (a ⊔ ℓ) where

  field

    isMagma : IsMagma ·

    assoc   : Associative ·


  open IsMagma isMagma public
```

Similarly commutative semigroup can be derived from semigroup as

```
record IsCommutativeSemigroup (· : Op₂ A) : Set (a ⊔ ℓ) where

  field

    isSemigroup : IsSemigroup ·

    comm        : Commutative ·


  open IsSemigroup isSemigroup public
```

Semigroup and commutative semigroup structure definitions with direct product and morphism constructs were previously defined in agda standard library and hence will not be discussed in details in this chapter.

Non associative ring is an algebraic structure with two binary operations addition and

multiplication. Addition is an abelian group and multiplication is unital magma and multiplication distributes over addition. A unital magma is a magma with identity element.

```
record IsNonAssociativeRing (+ * : Op2 A) (-_ : Op1 A) (0# 1# : A) : Set (a ⊔ ℓ) w
  field
    +-isAbelianGroup  :  IsAbelianGroup + 0# -_
    *-cong            :  Congruent2 *
    identity          :  Identity 1# *
    distrib           :  * DistributesOver +
    zero              :  Zero 0# *


  open IsAbelianGroup +-isAbelianGroup public
```

A quasiring is a type (2,2) algebraic structure for which both addition and multiplication is a monoid and multiplication distributes over addition.

```
record IsQuasiring (+ * : Op2 A) (0# 1# : A) : Set (a ⊔ ℓ) where
  field
    +-isMonoid    :  IsMonoid + 0#
    *-cong        :  Congruent2 *
    *-assoc       :  Associative *
    *-identity    :  Identity 1# *
    distrib       :  * DistributesOver +
    zero          :  Zero 0# *


  open IsMonoid +-isMonoid public
```

44

A quasiring with additive inverse is called a nearring. This implies that for nearring addition is a group and multiplication is a monoid and multiplication distributes over addition.

```
record IsNearring (+ * : Op2 A) (0# 1# : A) (_⁻¹ : Op1 A) : Set (a ⊔ ℓ) where
  field
    isQuasiring : IsQuasiring + * 0# 1#
    +-inverse   : Inverse 0# _⁻¹ +
    ⁻¹-cong     : Congruent1 _⁻¹


  open IsQuasiring isQuasiring public
```

Ring without one or rig or ring without unit is an algebraic structure with two binary operations such that addition is an abelian group and multiplication is a semigroup and multiplication distributes over addition Ring is rig with identity.

```
record IsRingWithoutOne (+ * : Op2 A) (-_ : Op1 A) (0# : A) : Set (a ⊔ ℓ) where
  field
    +-isAbelianGroup : IsAbelianGroup + 0# -_
    *-cong           : Congruent2 *
    *-assoc          : Associative *
    distrib          : * DistributesOver +
    zero             : Zero 0# *


  open IsAbelianGroup +-isAbelianGroup public
```

45

6.2 Morphism

A structure preserving map between two structures is called morphism. In this section morphism of ring without one is given. Morphisms of other structures that are structurally different from ring without one discussed in this section can be found in agda standard library

```
record IsRingWithoutOneHomomorphism (⟦_⟧ : A → B) : Set (a ⊔ ℓ1 ⊔ ℓ2) where
  field
    +-isGroupHomomorphism : +.IsGroupHomomorphism ⟦_⟧
    *-homo : Homomorphic2 ⟦_⟧ _*1_ _*2_


  open +.IsGroupHomomorphism +-isGroupHomomorphism public
    renaming (homo to +-homo; ε-homo to 0#-homo;
              isMagmaHomomorphism to +-isMagmaHomomorphism)
```

A Homomorphism that is injective is called monomorphism

```
record IsRingWithoutOneMonomorphism (⟦_⟧ : A → B) : Set (a ⊔ ℓ1 ⊔ ℓ2) where
  field
    isRingWithoutOneHomomorphism : IsRingWithoutOneHomomorphism ⟦_⟧
    injective                    : Injective ⟦_⟧


  open IsRingWithoutOneHomomorphism isRingWithoutOneHomomorphism public
```

A monomorphism that is bijective is called an isomorphism

```
record IsRingWithoutOneMonomorphism (⟦_⟧ : A → B) : Set (a ⊔ ℓ1 ⊔ ℓ2) where
  field
```

```
    isRingWithoutOneHomomorphism : IsRingWithoutOneHomomorphism ⟦_⟧

    injective                    : Injective ⟦_⟧
```

```
  open IsRingWithoutOneHomomorphism isRingWithoutOneHomomorphism public
```

6.3 Morphism composition

If f is a morphism such that f : a → b and g is a morphism on same structure such that g
: b → c then composition of morphism can be defined as g ∘ f : a → c.

```
  isRingWithoutOneHomomorphism

    : IsRingWithoutOneHomomorphism R1 R2 f

    → IsRingWithoutOneHomomorphism R2 R3 g

    → IsRingWithoutOneHomomorphism R1 R3 (g ∘ f)
  isRingWithoutOneHomomorphism f-homo g-homo = record
    { +-isGroupHomomorphism = isGroupHomomorphism ≈3-trans
                F.+-isGroupHomomorphism G.+-isGroupHomomorphism
    ; *-homo                 = λ x y → ≈3-trans
                (G.⟦⟧-cong (F.*-homo x y)) (G.*-homo (f x) (f y))
    } where module F = IsRingWithoutOneHomomorphism f-homo;
                module G = IsRingWithoutOneHomomorphism g-homo
```

6.4 Direct Product

The direct product M × N of two ring without one structures M and N is defined as a pair
(m,n) where m ∈ M and n ∈ N.

```
ringWithoutOne : RingWithoutOne a ℓ1 →

                 RingWithoutOne b ℓ2 → RingWithoutOne (a ⊔ b) (ℓ1 ⊔ ℓ2)
ringWithoutOne R S = record
  { isRingWithoutOne = record
      { +-isAbelianGroup = AbelianGroup.isAbelianGroup
                 ((abelianGroup R.+-abelianGroup S.+-abelianGroup))
      ; *-cong          = Semigroup.∙-cong
                 (semigroup R.*-semigroup S.*-semigroup)
      ; *-assoc   = Semigroup.assoc (semigroup R.*-semigroup S.*-semigroup)
      ; distrib      = (λ x y z →
                 (R.distribl , S.distribl) <*> x <*> y <*> z)
                          , (λ x y z →
                 (R.distribr , S.distribr) <*> x <*> y <*> z)
      ; zero      = uncurry (λ x y → R.zerol x , S.zerol y)
                          , uncurry (λ x y → R.zeror x , S.zeror y)
      }


  } where module R = RingWithoutOne R; module S = RingWithoutOne S
```

The direct product M × N of two non associative ring a structures M and N is defined as a pair (m,n) where m ∈ M and n ∈ N.

```
nonAssociativeRing : NonAssociativeRing a ℓ1 →

                 NonAssociativeRing b ℓ2 → NonAssociativeRing (a ⊔ b) (ℓ1 ⊔ ℓ2)
nonAssociativeRing R S = record
  { isNonAssociativeRing = record
```

```
{ +-isAbelianGroup = AbelianGroup.isAbelianGroup

        ((abelianGroup R.+-abelianGroup S.+-abelianGroup))

; *-cong           = UnitalMagma.·-cong

        (unitalMagma R.*-unitalMagma S.*-unitalMagma)

; *-identity       = UnitalMagma.identity

        (unitalMagma R.*-unitalMagma S.*-unitalMagma)

; distrib          = (λ x y z →

        (R.distribl , S.distribl) <*> x <*> y <*> z)

                    , (λ x y z →

        (R.distribr , S.distribr) <*> x <*> y <*> z)

; zero             = uncurry (λ x y → R.zerol x , S.zerol y)

                    , uncurry (λ x y → R.zeror x , S.zeror y)

}


} where module R = NonAssociativeRing R; module S = NonAssociativeRing S
```

The direct product M × N of two quasiring a structures M and N is defined as a pair (m,n) where m ∈ M and n ∈ N.

```
quasiring : Quasiring a ℓ1 →

              Quasiring b ℓ2 → Quasiring (a ⊔ b) (ℓ1 ⊔ ℓ2)
quasiring R S = record
  { isQuasiring = record
    { +-isMonoid = Monoid.isMonoid

            ((monoid R.+-monoid S.+-monoid))

    ; *-cong            = Monoid.·-cong
```

```
                    (monoid R.*-monoid S.*-monoid)

    ; *-assoc           = Monoid.assoc

                    (monoid R.*-monoid S.*-monoid)

    ; *-identity        = Monoid.identity

                    ((monoid R.*-monoid S.*-monoid))

    ; distrib           = (λ x y z →

                    (R.distribl , S.distribl) <*> x <*> y <*> z)

                          , (λ x y z →

                    (R.distribr , S.distribr) <*> x <*> y <*> z)

    ; zero              = uncurry (λ x y → R.zerol x , S.zerol y)

                          , uncurry (λ x y → R.zeror x , S.zeror y)

    }


  } where module R = Quasiring R; module S = Quasiring S
```

The direct product M × N of two nearring a structures M and N is defined as a pair (m,n) where m ∈ M and n ∈ N.

```
nearring : Nearring a ℓ1 →

              Nearring b ℓ2 → Nearring (a ⊔ b) (ℓ1 ⊔ ℓ2)

nearring R S =  record

  { isNearring = record

      { isQuasiring = Quasiring.isQuasiring

                (quasiring R.quasiring S.quasiring)

      ; +-inverse   = (λ x → (R.+-inversel , S.+-inversel) <*> x)

                    , (λ x → (R.+-inverser , S.+-inverser) <*> x)
```

```
    ;  −¹-cong     = map R.−¹-cong S.−¹-cong

    }

} where module R = Nearring R; module S = Nearring S
```

6.5 Properties

This provide proof that was contributed by the author and other proofs can be found in agda standard library.

6.5.1 Properties of Semigroup

Let $(S, \cdot)$ be a semigroup then

a) S is alternative. The Semigroup S left alternative if $\forall x, y \in S : (x\cdot x)\cdot y = x\cdot(x\cdot y)$ and right alternative is $\forall x, y \in S : x\cdot(y\cdot y) = (x\cdot y)\cdot y$. Semigroup is said to be alternative if it is both left and right alternative.

b) S is flexible. The Semigroup S is flexible if $\forall x y \in S : x\cdot(y\cdot x) = (x\cdot y)\cdot x$

c) S has Jordan identity. Jordan identity for binary operation $\cdot$ can be defined on set S as $\forall x y z \in S : (x\cdot y)\cdot(x\cdot x) = x\cdot(y\cdot(x\cdot x))$

Proof:

a)

```
alternativeˡ : LeftAlternative _·_

alternativeˡ x y = assoc x x y
```

```
alternativeʳ : RightAlternative _·_

alternativeʳ x y = sym (assoc x y y)
```

```
alternative : Alternative _·_

alternative = alternativeˡ , alternativeʳ
```

b)

```
flexible : Flexible _·_

flexible x y = assoc x y x
```

c)

```
xy·xx≈x·yxx : ∀ x y → (x · y) · (x · x) ≈ x · (y · (x · x))

xy·xx≈x·yxx x y = assoc x y ((x · x))
```

6.5.2   Properties of Commutative Semigroup

Let (S, ·) be a commutative semigroup then

a) S is semimedial. The commutative semigroup S is left semimedial if $\forall\, x\,y\,z \in S : (x{\cdot}x){\cdot}(y{\cdot}z) = (x{\cdot}y){\cdot}(x{\cdot}z)$ and right semimedial if $\forall\, x\,y\,z \in S : (y{\cdot}z){\cdot}(x{\cdot}x) = (y{\cdot}x){\cdot}(z{\cdot}x)$. A structure is semimedial if it is both left and right semimedial.

b) S is middle semimedia. The commutative semigroup S is middle semimedial if $\forall\, x\,y\,z \in S : (x{\cdot}y){\cdot}(z{\cdot}x) = (x{\cdot}z){\cdot}(y{\cdot}x)$

a)

semimedial^l : LeftSemimedial _·_

semimedial^l x y z = begin

  (x · x) · (y · z) ≈⟨ assoc x x (y · z) ⟩

  x · (x · (y · z)) ≈⟨ ·-cong^l (sym (assoc x y z)) ⟩

  x · ((x · y) · z) ≈⟨ ·-cong^l (·-cong^r (comm x y)) ⟩

  x · ((y · x) · z) ≈⟨ ·-cong^l (assoc y x z) ⟩

  x · (y · (x · z)) ≈⟨ sym (assoc x y ((x · z))) ⟩

  (x · y) · (x · z) ∎

semimedial^r : RightSemimedial _·_

semimedial^r x y z = begin

  (y · z) · (x · x) ≈⟨ assoc y z (x · x) ⟩

  y · (z · (x · x)) ≈⟨ ·-cong^l (sym (assoc z x x)) ⟩

  y · ((z · x) · x) ≈⟨ ·-cong^l (·-cong^r (comm z x)) ⟩

  y · ((x · z) · x) ≈⟨ ·-cong^l (assoc x z x) ⟩

  y · (x · (z · x)) ≈⟨ sym (assoc y x ((z · x))) ⟩

  (y · x) · (z · x) ∎

semimedial : Semimedial _·_

semimedial = semimedial^l , semimedial^r

b)

```
middleSemimedial : ∀ x y z → (x · y) · (z · x) ≈ (x · z) · (y · x)

middleSemimedial x y z = begin

  (x · y) · (z · x) ≈⟨ assoc x y ((z · x)) ⟩

  x · (y · (z · x)) ≈⟨ ·-cong¹ (sym (assoc y z x)) ⟩

  x · ((y · z) · x) ≈⟨ ·-cong¹ (·-congʳ (comm y z)) ⟩

  x · ((z · y) · x) ≈⟨ ·-cong¹ ( assoc z y x) ⟩

  x · (z · (y · x)) ≈⟨ sym (assoc x z ((y · x))) ⟩

  (x · z) · (y · x) ∎
```

6.5.3 Properties of Ring without one

Let (R, +, *, -, 0) be ring without one structure then a) $\forall x, y \in R$: - (x * y) = - x * y

b) $\forall x, y \in R$: - (x * y) = x * - y

proof:

a)

```
-⌣distribl-* : ∀ x y → - (x * y) ≈ - x * y

-⌣distribl-* x y = sym $ begin

  - x * y                       ≈⟨ sym $ +-identityr (- x * y) ⟩

  - x * y + 0#                  ≈⟨ +-congl $ sym ( -⌣inverser (x * y) ) ⟩

  - x * y + (x * y + - (x * y)) ≈⟨ sym $ +-assoc (- x * y) (x * y) (- (x * y)) ⟩

  - x * y + x * y + - (x * y)   ≈⟨ +-congr $ sym ( distribr y (- x) x ) ⟩

  (- x + x) * y + - (x * y)     ≈⟨ +-congr $ *-congr $ -⌣inversel x ⟩

  0# * y + - (x * y)            ≈⟨ +-congr $ zerol y ⟩

  0# + - (x * y)                ≈⟨ +-identityl (- (x * y)) ⟩
```

```
  - (x * y)                              ■
```

b)

```
-‿distribr-* : ∀ x y → - (x * y) ≈ x * - y

-‿distribr-* x y = sym $ begin

  x * - y                           ≈⟨ sym $ +-identityl (x * (- y)) ⟩

   0# + x * - y                     ≈⟨ +-congr $ sym ( -‿inversel (x * y) ) ⟩

    - (x * y) + x * y + x * - y     ≈⟨ +-assoc (- (x * y)) (x * y) (x * (- y)) ⟩

    - (x * y) + (x * y + x * - y)   ≈⟨ +-congl $ sym ( distribl x y ( - y) )  ⟩

    - (x * y) + x * (y + - y)       ≈⟨ +-congl $ *-congl $ -‿inverser y ⟩

    - (x * y) + x * 0#              ≈⟨ +-congl $ zeror x ⟩

    - (x * y) + 0#                  ≈⟨ +-identityr (- (x * y)) ⟩

    - (x * y)                       ■
```

6.5.4　Properties of Ring

Let (R, +, *, -, 0, 1) be a ring structure then a) $\forall x \in R$: - 1 * x = -x

b) $\forall x \in R$: if x + x = 0 then x = 0

c) $\forall x, y, z \in R$: x * (y - z) = x * y - x * z

d) $\forall x, y, z \in R$: (y - z) * x = (y * x) - (z * x)

Proof

a)

```
-1*x≈-x : ∀ x → - 1# * x ≈ - x

-1*x≈-x x = begin

  - 1# * x    ≈⟨ sym (-‿distribl-* 1# x ) ⟩
```

```
  - (1# * x)  ≈⟨ -⌣cong ( *-identityl x ) ⟩

  - x           ■
```

b)

```
x+x≈x⇒x≈0 : ∀ x → x + x ≈ x → x ≈ 0#

x+x≈x⇒x≈0 x eq = begin

  x ≈⟨ sym(+-identityr x) ⟩

  x + 0# ≈⟨ +-congl (sym (-⌣inverser x)) ⟩

  x + (x - x) ≈⟨ sym (+-assoc x x (- x)) ⟩

  x + x - x ≈⟨ +-congr(eq) ⟩

  x - x ≈⟨ -⌣inverser x ⟩

  0# ■
```

c)

```
x[y-z]≈xy-xz : ∀ x y z → x * (y - z) ≈ x * y - x * z

x[y-z]≈xy-xz x y z = begin

  x * (y - z)      ≈⟨ distribl x y (- z) ⟩

  x * y + x * - z  ≈⟨ +-congl (sym (-⌣distribr-* x z)) ⟩

  x * y - x * z    ■
```

d)

```
[y-z]x≈yx-zx : ∀ x y z → (y - z) * x ≈ (y * x) - (z * x)

[y-z]x≈yx-zx x y z = begin

  (y - z) * x      ≈⟨ distribr x y (- z) ⟩

  y * x + - z * x  ≈⟨ +-congl (sym (-⌣distribl-* z x)) ⟩

  y * x - z * x    ■
```

Chapter 7

Theory of Kleene Algebra in Agda

7.1 Definition

A set S with two binary operations + and * generally called addition and multiplica-
tion such that (S,+) is a commutative monoid, (S,*) is a monoid and + distributes over *
with annhiliating zero is called a semiring. A semiring satisfying idempotent property is
called idempotent semiring. A Kleene Algebra over set S is idempotent semiring with $\star$
operator that satisfies the following axioms.

$$1 + (x \cdot (x*)) \leq x* \tag{7.1.1}$$

$$1 + (x*) \cdot x \leq x* \tag{7.1.2}$$

$$\forall a, b, x \in S : If\ b + a \cdot x \leq x\ then, (a*) \cdot b \leq x \tag{7.1.3}$$

$$\forall a, b, x \in S : If\ b + x \cdot a \leq x\ then, b \cdot (a*) \leq x \tag{7.1.4}$$

In Agda, strong axioms of $\star$ are given. That is equivalance is directly given and kleene algebra with partial and pre order structures are defined in Algebra.Ordered hierarchy.

```
StarRightExpansive : A → Op\textsubscript{2} A → Op\textsubscript{2} A
        → Op\textsubscript{1} A → Set _
StarRightExpansive e _+_ _·_ _* = ∀ x → (e + (x · (x *))) ≈ (x *)


StarLeftExpansive : A → Op\textsubscript{2} A → Op\textsubscript{2} A
        → Op\textsubscript{1} A → Set _
StarLeftExpansive e _+_ _·_ _* = ∀ x →  (e + ((x *) · x)) ≈ (x *)


StarLeftDestructive : Op\textsubscript{2} A → Op\textsubscript{2} A
        → Op\textsubscript{1} A → Set _
StarLeftDestructive _+_ _·_ _* = ∀ a b x → (b + (a · x)) ≈ x
        → ((a *) · b) ≈ x


StarRightDestructive : Op\textsubscript{2} A → Op\textsubscript{2} A
        → Op\textsubscript{1} A → Set _
StarRightDestructive _+_ _·_ _* = ∀ a b x → (b + (x · a)) ≈ x
        → (b · (a *)) ≈ x
```

The Kleene algebra can be structurally derived from idempotent semiring.

```
record IsKleeneAlgebra (+ * : Op\textsubscript{2} A) (⋆ : Op\textsubscript{1} A)
                (0# 1# : A) : Set (a ⊔ ℓ) where
  field
    isIdempotentSemiring  : IsIdempotentSemiring + * 0# 1#
```

```
      starExpansive           : StarExpansive 1# + * ⋆

      starDestructive         : StarDestructive + * ⋆


  open IsIdempotentSemiring isIdempotentSemiring public
```

The bundle version of kleene algebra is defined as:

```
record KleeneAlgebra c ℓ : Set (suc (c ⊔ ℓ)) where
  infix  8 _⋆
  infixl 7 _*_
  infixl 6 _+_
  infix  4 _≈_
  field
    Carrier               : Set c
    _≈_                   : Rel Carrier ℓ
    _+_                   : Op2 Carrier
    _*_                   : Op2 Carrier
    _⋆                    : Op1 Carrier
    0#                    : Carrier
    1#                    : Carrier
    isKleeneAlgebra       : IsKleeneAlgebra _≈_ _+_ _*_ _⋆ 0# 1#


  open IsKleeneAlgebra isKleeneAlgebra public


  idempotentSemiring : IdempotentSemiring _ _
  idempotentSemiring = record \{ isIdempotentSemiring = isIdempotentSemiring \}
```

```
open IdempotentSemiring idempotentSemiring public

  using

  ( _≉_; +-rawMagma; +-magma; +-unitalMagma; +-commutativeMagma

  ; +-semigroup; +-commutativeSemigroup

  ; *-rawMagma; *-magma; *-semigroup

  ; +-rawMonoid; +-monoid; +-commutativeMonoid

  ; *-rawMonoid; *-monoid

  ; nearSemiring; semiringWithoutOne

  ; semiringWithoutAnnihilatingZero

  ; rawSemiring; semiring

  )
```

7.2 Direct Product

The direct product K × L of two kleene algebra structures K and NL is defined as a pair

(k,l) where k∈ K and l ∈ L.

```
kleeneAlgebra : KleeneAlgebra a ℓ\textsubscript{1}

        → KleeneAlgebra b ℓ\textsubscript{2} →

        KleeneAlgebra (a ⊔ b) (ℓ\textsubscript{1} ⊔ ℓ\textsubscript{2})
kleeneAlgebra K L = record

  { isKleeneAlgebra = record

     { isIdempotentSemiring = IdempotentSemiring.isIdempotentSemiring

                (idempotentSemiring K.idempotentSemiring L.idempotentSemiring)
```

```
    ; starExpansive = (λ x → (K.starExpansivel   , L.starExpansivel) <*> x)

                     , (λ x → (K.starExpansiver   , L.starExpansiver) <*> x)

    ; starDestructive = (λ a b x x1 →

              (K.starDestructivel   , L.starDestructivel)

              <*> a <*> b <*> x <*> x1)

                       , (λ a b x x1 →

              (K.starDestructiver   , L.starDestructiver)

              <*> a <*> b <*> x <*> x1)

    }

  } where module K = KleeneAlgebra K;  module L = KleeneAlgebra L
```

7.3 Properties

In this section we prove some of the properties of Kleene algebra

Let (K, +, *, ⋆, 0, 1) be a Kleene algebra then, a) $0\star = 1$

b) $1\star = 1$

c) $\forall x \in K$: $1 + x\star = x\star$

d) $\forall x \in K$: $x + x * x\star = x\star$

e) $\forall x \in K$: $x + x\star * x = x\star$

f) $\forall x \in K$: $x + x\star = x\star$

g) $\forall x \in K$: $1 + x + x\star = x\star$

h) $\forall x \in K$: $0 + x + x\star = x\star$

i) $\forall x \in K$: $x\star * x\star = x\star$

j) $\forall x \in K$: $x\star\star = x\star$

k) $\forall x, y \in K$: If $x = y$ then, $x\star = y\star$

l) $\forall a, b, x \in K$: If a * x = x * b then, a$\star$ * x = x * b$\star$

m) $\forall x, y \in K$: (x * y) $\star$ * x $\approx$ x * (y * x) $\star$

Proof:

a)

```
0★≈1 : 0# ★ ≈ 1#

0★≈1 = begin

  0# ★              ≈⟨ sym (starExpansivel 0#) ⟩

  1# + 0# ★ * 0# ≈⟨ +-congl ( zeror (0# ★)) ⟩

  1# + 0#          ≈⟨ +-identityr 1# ⟩

  1#                ■
```

b)

```
1+11≈1 : 1# + 1# * 1# ≈ 1#

1+11≈1 = begin

  1# + 1# * 1#  ≈⟨ +-congl ( *-identityr 1#) ⟩

  1# + 1#        ≈⟨ +-idem 1# ⟩

  1#                ■
```


```
1★≈1 : 1# ★ ≈ 1#

1★≈1 = begin

  1# ★          ≈⟨ sym (*-identityr (1# ★)) ⟩

  1# ★ * 1#  ≈⟨ starDestructivel 1# 1# 1# 1+11≈1 ⟩

  1#                ■
```

c)

```
1+x★≈x★ : ∀ x → 1# + x ★ ≈ x ★
```

```
1+x⋆≈x⋆ x = sym (begin

  x ⋆                       ≈⟨ sym (starExpansiver x) ⟩

  1# + x * x ⋆              ≈⟨ +-congr (sym (+-idem 1#)) ⟩

  1# + 1# + x * x ⋆         ≈⟨ +-assoc 1# 1# ((x * x ⋆ )) ⟩

  1# + (1# + x * x ⋆)       ≈⟨ +-congl (starExpansiver x) ⟩

  1# + x ⋆                  ∎)
```

d)

```
x⋆+xx⋆≈x⋆ : ∀ x → x ⋆ + x * x ⋆ ≈ x ⋆

x⋆+xx⋆≈x⋆ x = begin

  x ⋆ + x * x ⋆             ≈⟨ +-congr (sym (1+x⋆≈x⋆ x)) ⟩

  1# + x ⋆ + x * x ⋆        ≈⟨ +-congr (+-comm 1# ((x ⋆))) ⟩

  x ⋆ + 1# + x * x ⋆        ≈⟨ +-assoc ((x ⋆)) 1# ((x * x ⋆ )) ⟩

  x ⋆ + (1# + x * x ⋆)      ≈⟨ +-congl (starExpansiver x) ⟩

  x ⋆ + x ⋆                 ≈⟨ +-idem (x ⋆) ⟩

  x ⋆                       ∎
```

e)

```
x⋆+x⋆x≈x⋆ : ∀ x → x ⋆ + x ⋆ * x ≈ x ⋆

x⋆+x⋆x≈x⋆ x = begin

  x ⋆ + x ⋆ * x             ≈⟨ +-congr (sym (1+x⋆≈x⋆ x)) ⟩

  1# + x ⋆ + x ⋆ * x        ≈⟨ +-congr (+-comm 1# (x ⋆)) ⟩

  x ⋆ + 1# + x ⋆ * x        ≈⟨ +-assoc (x ⋆) 1# (x ⋆ * x) ⟩

  x ⋆ + (1# + x ⋆ * x)      ≈⟨ +-congl (starExpansivel x) ⟩

  x ⋆ + x ⋆                 ≈⟨ +-idem (x ⋆) ⟩

  x ⋆                       ∎
```

f)

x+x⋆≈x⋆ : ∀ x → x + x ⋆ ≈ x ⋆

x+x⋆≈x⋆ x = begin

  x + x ⋆   ≈⟨ +-cong*l* (sym (starExpansive*r* x)) ⟩

  x + (1# + x * x ⋆)   ≈⟨ +-cong*r* (sym (*-identity*r* x)) ⟩

  x * 1# + (1# + x * x ⋆) ≈⟨ sym (+-assoc (x * 1#) 1# (x * x ⋆)) ⟩

  x * 1# + 1# + x * x ⋆   ≈⟨ +-cong*r* (+-comm (x * 1#) 1#) ⟩

  1# + x * 1# + x * x ⋆   ≈⟨ +-assoc 1# (x * 1#) (x * x ⋆) ⟩

  1# + (x * 1# + x * x ⋆) ≈⟨ +-cong*l* (sym (distrib*l* x 1# ((x ⋆)))) ⟩

  1# + x * (1# + x ⋆)   ≈⟨ +-cong*l* (*-cong*l* (1+x≈x⋆ x)) ⟩

  1# + x * x ⋆   ≈⟨ (starExpansive*r* x) ⟩

  x ⋆   ∎

g)

1+x+x⋆≈x⋆ : ∀ x → 1# + x + x ⋆ ≈ x ⋆

1+x+x⋆≈x⋆ x = begin

  1# + x + x ⋆   ≈⟨ +-assoc 1# x (x ⋆) ⟩

  1# + (x + x ⋆)   ≈⟨ +-cong*l* (x+x⋆≈x⋆ x) ⟩

  1# + x ⋆   ≈⟨ 1+x⋆≈x⋆ x ⟩

  x ⋆   ∎

h)

0+x+x⋆≈x⋆ : ∀ x → 0# + x + x ⋆ ≈ x ⋆

0+x+x⋆≈x⋆ x = begin

  0# + x + x ⋆   ≈⟨ +-assoc 0# x (x ⋆) ⟩

  0# + (x + x ⋆)   ≈⟨ +-identity*l* ((x + x ⋆)) ⟩

```
  (x + x ⋆)          ≈⟨ x+x⋆≈x⋆ x ⟩

  x ⋆                ∎
```

i)
```
x⋆x⋆≈x⋆ : ∀ x → x ⋆ * x ⋆ ≈ x ⋆

x⋆x⋆≈x⋆ x = starDestructivel x (x ⋆) (x ⋆) (x⋆+xx⋆≈x⋆ x)
```

j)
```
1+x⋆x⋆≈x⋆ : ∀ x → 1# + x ⋆ * x ⋆ ≈ x ⋆

1+x⋆x⋆≈x⋆ x = begin

  1# + x ⋆ * x ⋆  ≈⟨ +-congl (x⋆x⋆≈x⋆ x) ⟩

  1# + x ⋆         ≈⟨ 1+x⋆≈x⋆ x ⟩

  x ⋆              ∎
```

```
x⋆⋆≈x⋆ : ∀ x → (x ⋆) ⋆ ≈ x ⋆

x⋆⋆≈x⋆ x = begin

  (x ⋆) ⋆          ≈⟨ sym (*-identityr ((x ⋆) ⋆)) ⟩

  (x ⋆) ⋆ * 1#    ≈⟨ starDestructivel (x ⋆) 1# (x ⋆) (1+x⋆x⋆≈x⋆ x) ⟩

  x ⋆              ∎
```

k)
```
x≈y⇒1+xy⋆≈y⋆ : ∀ x y → x ≈ y → 1# + x * y ⋆ ≈ y ⋆

x≈y⇒1+xy⋆≈y⋆ x y eq = begin

  1# + x * y ⋆  ≈⟨ +-congl (*-congr (eq)) ⟩

  1# + y * y ⋆  ≈⟨ starExpansiver y ⟩

  y ⋆              ∎
```

```
x≈y⇒x★≈y★ : ∀ x y → x ≈ y → x ★ ≈ y ★

x≈y⇒x★≈y★ x y eq = begin

  x ★          ≈⟨ sym (*-identityr (x ★)) ⟩

  x ★ * 1#  ≈⟨ (starDestructivel x 1# (y ★) (x≈y⇒1+xy★≈y★ x y eq)) ⟩

  y ★          ∎
```

l)

```
ax≈xb⇒x+axb★≈xb★ : ∀ x a b → a * x ≈ x * b → x + a * (x * b ★) ≈ x * b ★

ax≈xb⇒x+axb★≈xb★ x a b eq = begin

  x + a * (x * b ★)        ≈⟨ +-congl (sym(*-assoc a x (b ★))) ⟩

  x + a * x * b ★          ≈⟨ +-congr (sym (*-identityr x)) ⟩

  x * 1# + a * x * b ★    ≈⟨ +-congl (*-congr (eq)) ⟩

  x * 1# + x * b * b ★    ≈⟨ +-congl (*-assoc x b (b ★) ) ⟩

  x * 1# + x * (b * b ★)  ≈⟨ sym (distribl x 1# (b * b ★)) ⟩

  x * (1# + b * b ★)      ≈⟨ *-congl (starExpansiver b) ⟩

  x * b ★                        ∎
```

```
ax≈xb⇒a★x≈xb★ : ∀ x a b → a * x ≈ x * b → a ★ * x ≈ x * b ★

ax≈xb⇒a★x≈xb★ x a b eq = starDestructivel a x ((x * b ★)) (ax≈xb⇒x+axb★≈xb★ x
```

m)

```
[xy]★x≈x[yx]★ : ∀ x y → (x * y) ★ * x ≈ x * (y * x) ★

[xy]★x≈x[yx]★ x y = ax≈xb⇒a★x≈xb★ x (x * y) (y * x) (*-assoc x y x)
```

Chapter 8

Problem in Programming Algebra

Algebraic structures show variations in syntax and semantics depending on the system or language in which they are defined. Each systems discussed in chapter 1 have their own style of defining structures in the standard libraries. For example, in Coq Ring is defined without multiplicative identity. However, in Agda, Ring has multiplicative identity and Rng is defined as RingWithoutOne that has no multiplicative identity. This ambiguity in naming is also seen in literature. Another example is same structure having multiple definitions like Quasigroups. Quasigroups can be defined as type(2) algebra with latin square property or as type(2,2,2) with left and right division operators. Both the definitions are equivalent but they are structurally different. This chapter identifies and classifies five important problems that arises when defining algebraic structures in proof assistant systems.

8.1   Ambiguity in naming

Ambiguity arises when something can be interpreted in more than one way. The example of quasigroup having more than one definition can give rise to a scenario of making an incorrect interpretation of the algebraic structure when it is not clearly stated. In abstract algebra and algebraic structure these scenarios can be more common. This can be attributed to lack of naming convention that is followed in naming algebraic structures and it's properties. For example Ring and Rng. Some mathematicians define Ring as an algebraic structure that is an abelian group under addition and a monoid under multiplication. This definition is also be named explicitly as ring with unit or ring with identity. Rng is defined as an algebraic structure that is an abelian group under addition and a semigroup under multiplication. The same structure is also defined as ring without identity. However, this definitions are often interchanged i.e., some mathematicians define ring as ring without identity that is multiplication has no identity or is a semigroup. This ambiguity is some time attributed to the language of origin of the algebraic structures. In this case rng is used in French where as ring in english. These confusions can be seen in literature and in online blogs where it is difficult to imply the definition of intent when they are not explicitly defined.

In Agda, ring is defined as an algebraic structure with two binary operations + and * where + is an abelian group and * is a monoid. The binary operation * distributes over + that is multiplication distributes over addition and it has a zero.

```
record IsRing (+ * : Op₂ A) (-_ : Op₁ A) (0# 1# : A) : Set (a ⊔ ℓ) where
  field
    +-isAbelianGroup : IsAbelianGroup + 0# -_
    *-cong           : Congruent₂ *
    *-assoc          : Associative *
    *-identity       : Identity 1# *
    distrib          : * DistributesOver +
    zero             : Zero 0# *


  open IsAbelianGroup +-isAbelianGroup public
```

Rng is defined as ring wihthout one where one is assumend to be multiplication identity.

```
record IsRingWithoutOne (+ * : Op₂ A) (-_ : Op₁ A) (0# : A) : Set (a ⊔ ℓ) where
  field
    +-isAbelianGroup : IsAbelianGroup + 0# -_
    *-cong           : Congruent₂ *
    *-assoc          : Associative *
    distrib          : * DistributesOver +
    zero             : Zero 0# *
```

Another example of ambiguity is Nearring. In some papers, Nearring is defined as a structure where addition is a group and multiplication is a monoid. But some mathematicians use the definition where multiplication is a semigroup. The same confusion also arises in defining semiring and rig structures. Wikipedia states that the term rig originated as a joke that it is similar to rng that is missing alphabet n and i to represent

69

the identity does not exist for these structures. In Agda rig is defined as semiring without one where one is represents the multiplicative identity.

For axioms of structures, the names are usually invented when defining the structure. As an example when defining Kleene Algebra in Agda, starExpansive and starDestructive names were invented (inspired from what is used in literature). Due to lack of common practice many names can be coined for the same axiom.

```
record IsKleeneAlgebra (+ * : Op₂ A) ( ⁻* : Op₁ A)
                                      (0# 1# : A) : Set (a ⊔ ℓ) where
  field
    isIdempotentSemiring    : IsIdempotentSemiring + * 0# 1#
    starExpansion             : StarLeftExpansion 1# + * ⁻*
    starDestructive           : StarRightExpansion+ * ⁻*
  open IsIdempotentSemiring isIdempotentSemiring public
```

8.2   Equivalent but structurally different

Quasigroup structure is an example that can be defined in two ways. A type (2) Quasigroup can be defined as a set Q and binary operation · can be defined as that is a magma and satisfies latin square property. Quasigroup of type (2,2,2) is a structure with three binary operations, a magma for which division is always possible. Latin square property states that for each a , b in set Q there exists unique elements x , y in Q such that the following property is satisfied (Wikipedia contributors, 2022c)

$$a \cdot x = b$$

$$y \cdot a = b$$

Another definition of quasigroup is given as type (2,2,2) algebra in which for a set Q and binary operations $\cdot$, \ , / quasigroup should satisfy the below identities that implies left division and right division.

$$y = x \cdot (x \setminus y)$$

$$y = x \setminus (x \cdot y)$$

$$y = (y \, / \, x) \cdot x$$

$$y = (y \cdot x) \, / \, x$$

In Agda standard library the quasigroup is defined as type (2,2,2) algebra given below.

```
record IsQuasigroup (· \ \ // : Op₂ A) : Set (a ⊔ ℓ) where
  field
    isMagma       : IsMagma ·
    \ \-cong       : Congruent₂ \ \
    //-cong       : Congruent₂ //
    leftDivides   : LeftDivides · \\
    rightDivides  : RightDivides · //


  open IsMagma isMagma public
```

A quasigroup with signature (2) and a quasigroup with signature (2,2,2) are equivalent but are structurally different. In the algebra hierarchy, a Loop is an algebraic structure that is a quasigroup with identity. It can be observed the same problem persists through the hierarchy. If a loop is defined with a quasigroup that is type (2,2,2) algebra

then it a loop structure of type (2) will be forced to be defined with sub-optimal name. One plausible solution to this problem is to define the structures in different modules and import restrict them when using. This problem of not being able to overload names for structures also affects when defining types of quasigroup or loops such as bol loop and moufang loop.

Since quasigroup is defined in terms of division operation, loop is also defined as a type (2,2,2) algebra in Agda. The definition of loop structure in Agda is given below.

```
record IsLoop (· \ \ // : Op₂ A) (ε : A) : Set (a ⊔ ℓ) where
  field
    isQuasigroup : IsQuasigroup · \ \ //
    identity     : Identity ε ·

  open IsQuasigroup isQuasigroup public
```

8.3   Redundant field in structural inheritance

Redundancy arises when there is duplication of the same field. In programming redundant of code is considered a bad practice and is usually avoided by modularising and creating functions that perform similar tasks. In algebraic structures, redundant fields can be introduced in structures that are defined in terms of two or more structures. For example semiring can be as commutative monoid under addition and a monoid under multiplication and multiplication distributes over addition. In Agda, both monoid and commutative monoid have an instance of equivalence relation. If semiring is defined in

terms of commutative monoid and monoid then this definition of the semiring will have a redundant equivalence field. This redundancy can also be seen in other structures like ring, lattice, module, etc., To remove this redundant field in Agda the structure except the first is opened and expressed in terms of independent axioms that they satisfy. For example, semiring without identity or rig structure in Agda is defined as

```
record IsSemiringWithoutOne (+ * : Op₂ A) (0# : A) : Set (a ⊔ ℓ) where
  field
    +-isCommutativeMonoid : IsCommutativeMonoid + 0#
    *-cong                      : Congruent₂ *
    *-assoc                     : Associative *
    distrib                      : * DistributesOver +
    zero                         : Zero 0# *


  open IsCommutativeMonoid +-isCommutativeMonoid public
```

From the above definition it is evident that an instance of semigroup should be constructed and is not directly available when using semiring without one structure. To overcome this problem an instance is created in the definition as follows along with near semiring structure.

```
  *-isMagma : IsMagma *
  *-isMagma = record
    { isEquivalence = isEquivalence
    ; ·-cong        = *-cong
```

```
  }


*-isSemigroup : IsSemigroup *
*-isSemigroup = record
  { isMagma = *-isMagma
  ; assoc   = *-assoc
  }


isNearSemiring : IsNearSemiring + * 0#
isNearSemiring = record
  { +-isMonoid     = +-isMonoid
  ; *-cong         = *-cong
  ; *-assoc        = *-assoc
  ; distribʳ       = proj₂ distrib
  ; zeroˡ          = zeroˡ
  }
```

The above technique will effectively remove the redundant equivalence relation but it also fails to express the structure in terms of two or more structures that is commonly used in literature and in other systems. Agda 2.0 removed redundancy by unfolding the structure. This solution should make sure that the structure clearly exports the unfolded structure whose properties can be imported when required.

8.4   Identical structures

In abstract algebra when formalising algebraic structures from the hierarchy, same alge-
braic structure can be derived from two or more structures. One such example is Near-
ring. Nearring is an algebraic structure with two binary operations addition and multi-
plication. Near ring is a group under addition and is a monoid under multiplication and
multiplication right distributes over addition. In this case near-ring is defined using two
algebraic structures group and monoid. Other definition of near-ring can be derived
using the structure quasiring. Quasiring is an algebraic structure in which addition is a
monoid, multiplication is a monoid and multiplication distributes over addition. Using
this definition of quasiring, near-ring can be defined as a quasiring which has additive
inverse.

In Agda nearring is defined in terms of quasiring with additive inverse

```
record IsNearring (+ * : Op₂ A) (0# 1# : A) (_⁻¹ : Op₁ A) : Set (a ⊔ ℓ) where
  field
    isQuasiring : IsQuasiring + * 0# 1#
    +-inverse   : Inverse 0# _⁻¹ +
    ⁻¹-cong     : Congruent₁ _⁻¹


  open IsQuasiring isQuasiring public
```

Note that in some literature, near-ring is defined in which multiplication is a semigroup
that is without identity. This can be attributed to the problem with ambiguity. It can be
analysed that having two different definitions for same structure is not a good practice. If
near-ring is defined using quasiring then it should also give an instance of additive group
without having it to construct it when using the above formalisation. This solution might

solve the problem at first but in practice this becomes tedious and can go to a point at which this can be impractical especially when formalising structures at higher level in the algebra hierarchy.

8.5   Equivalent structures

Consider the example of idempotent-commutative-monoid and bounded semilattice. It can be observed that both are essentially same structure. In this case it could be redundant to define two different structures from different hierarchy. Instead in Agda, aliasing is used. Idempotent-commutative-monoid is defined and an aliasing for bounded semilattice is given.

```
record IsIdempotentCommutativeMonoid (· : Op₂ A) (ϵ : A) : Set (a ⊔ ℓ) where
  field
    isCommutativeMonoid : IsCommutativeMonoid · ϵ
    idem                : Idempotent ·


  open IsCommutativeMonoid isCommutativeMonoid public


IsBoundedSemilattice = IsIdempotentCommutativeMonoid
module IsBoundedSemilattice · ϵ (L : IsBoundedSemilattice · ϵ) where


  open IsIdempotentCommutativeMonoid L public
```

Note that some mathematicians argue that bounded semilattice and idempotent commutative monoid are not structurally the same structures but are isomorphic to

each other. We do not consider this argument in the scope of this thesis.

8.6   Mitigation using product family algebra

A product family algebra is an idempotent commutative semiring (S, +, ·, 0, 1) where S is the set of product families.

∀ a, b ∈ S: a + b represents the choice between a and b.

∀ a, b ∈ S: a · b represents combinations between a and b.

0 is the additive identity that is the empty product family

1 is the multiplicative identity that is the product family containing empty product with no features.

This section provides a brief insight over feature modelling and product family algebra but developing the model that satisfies the idea is out of scope of this thesis.

The feature model is an and/or diagram as in Feature Oriented Domain Analysis (FODA) Kang et al. (1990). Single arc between two arrows represent and decomposition and double arcs between two arrows represent or decomposition of features. The root node is the algebraic structure and the leaf nodes represent the axioms or the identities that the algebraic structure satisfy. The nodes that are not leaf or root nodes represent an algebraic structure that is below the hierarchy of the root node.

The semigroup structure can be represented using algebraic structure magma with associative property. In the figure 8.1 the arrow has single arc between them. That means all the properties are essential in defining a semigroup.

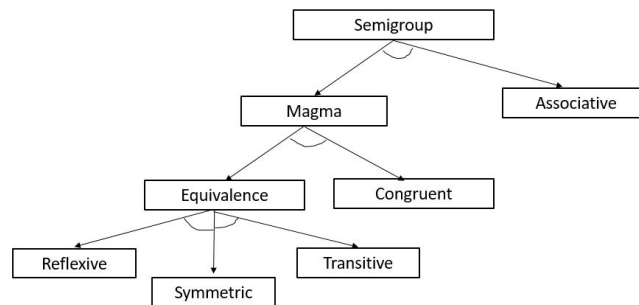Using product family algebra, a semigroup is represented as

Figure 8.1: Feature diagram of semigroup

Equivalence = Reflexive · Symmetric · Transitive

Magma = Equivalence · Congruent

Semigroup = Magma · Associativity

A nearring has the problem of identical structure definition that can be defined using quasiring or group and semigroup. This figure 8.2 shows the feature diagram of nearring.
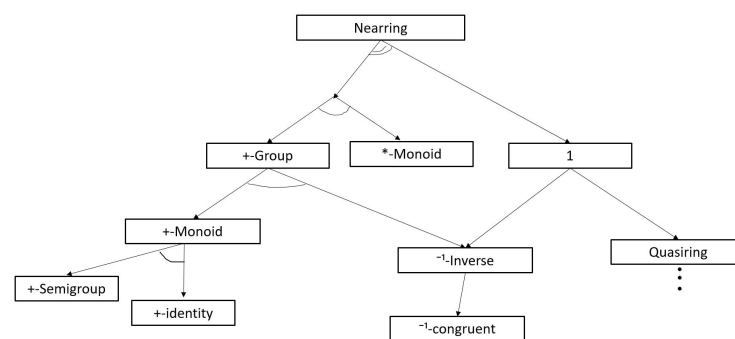

Figure 8.2: Feature diagram of nearring

Using product family algebra, nearring can be represented using above semigroup

definition as

+-Monoid = +-Semigroup · +-identity

+-Group = +-Monoid · $-^1$-Inverse

Nearring = (+-Group · *-Monoid) + (Quasiring · $-^1$-Inverse)

In the above representation of the issue with identical structures, operation + represents a union. That means Nearring can have both (+-Group · *-Monoid) and (Quasiring · $-^1$-Inverse) but it will have many redundant fields. To over come this problem it is best to use XOR decomposition (filled diamond) that prevents having two full definition of the same structure. Figure 8.3 shows an example of xor decomposition when defining quasigroup The product family algebra of quasigroup can be defined as
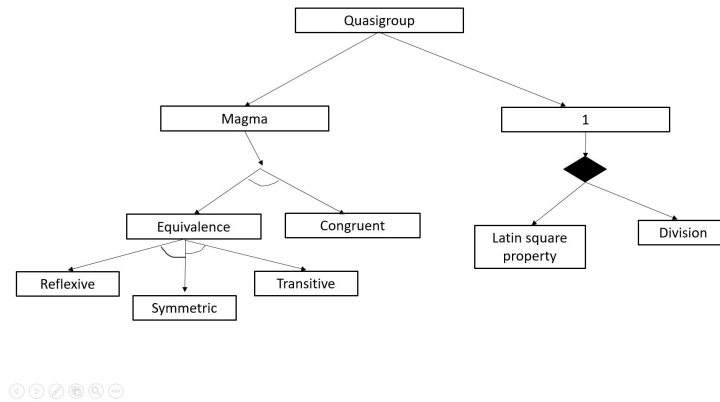

Figure 8.3: Feature diagram of quasigroup

Equivalence = Reflexive · Symmetric · Transitive

Magma = Equivalence · Congruent

Quasigroup = Magma · (Latin Square Property ⊕ Division)

In figure 8.2 there are multiple definition of same structures for different operations. In the feature diagram this can be eliminated by mentioning the operation as weight to the arrow. Figure 8.4 shows the feature diagram where the binary operation is represented at the highest possible arrow. The product family algebra of does not change as
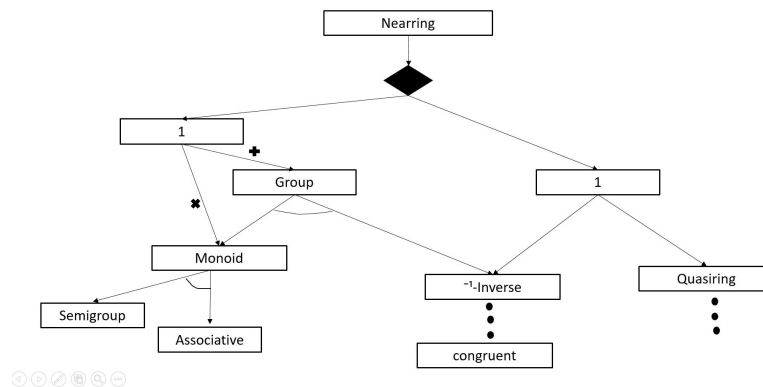

Figure 8.4: Feature diagram of Nearring

it should explicitly mention the operations of the structures.

Chapter 9

Conclusion

Every thesis also needs a concluding chapter

Appendix A

Your Appendix

Your appendix goes here.

Appendix B

Long Tables

This appendix demonstrates the use of a long table that spans multiple pages.

Col A	Col B	Col C	Col D
A	B	C	D
A	B	C	D
A	B	C	D
A	B	C	D
A	B	C	D
A	B	C	D
A	B	C	D
A	B	C	D

Continued from previous page

Col A	Col B	Col C	Col D
A	B	C	D
A	B	C	D
A	B	C	D
A	B	C	D
A	B	C	D
A	B	C	D
A	B	C	D
A	B	C	D
A	B	C	D
A	B	C	D
A	B	C	D
A	B	C	D

Bibliography

Sabine Broda, Sílvia Cavadas, and Nelma Moreira. 2014. *Kleene algebra completeness.* Technical Report. Technical report, Universidade de Porto.

Richard H Bruck. 1944. Some results in the theory of quasigroups. *Trans. Amer. Math. Soc.* 55 (1944), 19–52.

Fang-an Deng, Lu Chen, ShouHeng Tuo, and ShengZhang Ren. 2016. Characterizations of Algebras. *Algebra* 2016 (2016).

Natalia N Didurik and Victor A Shcherbacov. 2018. Some properties of Neumann quasi-groups. *arXiv preprint arXiv:1809.07095* (2018).

Zoltán Ésik and Laszlo Bernátsky. 1995. Equational properties of Kleene algebras of relations with conversion. *Theoretical Computer Science* 137, 2 (1995), 237–251.

Trevor Evans. 1974. Identities and relations in commutative Moufang loops. *Journal of Algebra* 31, 3 (1974), 508–513.

Jean-Gabriel Ganascia. 1993. Algebraic structure of some learning systems. In *International Workshop on Algorithmic Learning Theory*. Springer, 398–409.

J.H. Geuvers. 2009. Proof assistants : history, ideas and future. *Sadhana : Academy Proceedings in Engineering Sciences (Indian Academy of Sciences)* 34, 1 (2009), 3–25. `https://doi.org/10.1007/s12046-009-0001-5`

Jason ZS Hu and Jacques Carette. 2021. Formalizing category theory in agda. In *Proceedings of the 10th ACM SIGPLAN International Conference on Certified Programs and Proofs.* 327–342.

Russell O'Connor Jacques Carette and Yasmine Sharoda. 2019. Building on the Diamonds between Theories: Theory Presentation Combinators. *arXiv preprint arXiv:1812.08079* (2019).

Temitope Gbolahan Jaiyeola, Sunday Peter David, and Oyeyemi O Oyebola. 2021. New algebraic properties of middle Bol loops II. *Proyecciones (Antofagasta)* 40, 1 (2021), 85–106.

Kyo C Kang, Sholom G Cohen, James A Hess, William E Novak, and A Spencer Peterson. 1990. *Feature-oriented domain analysis (FODA) feasibility study.* Technical Report. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

Dexter Kozen. 1994. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and computation* 110, 2 (1994), 366–390.

Kenneth Kunen. 1996. Moufang quasigroups. *Journal of Algebra* 183, 1 (1996), 231–234.

Iqra Liaqat and Wajeeha Younas. 2021. Some important applications of semigroups. *Journal of Mathematical Sciences & Computational Mathematics* 2, 2 (2021), 317–321.

Assia Mahboubi and Enrico Tassi. 2021. *Mathematical Components.* Zenodo. `https://doi.org/10.5281/zenodo.4457887`

The mathlib Community. 2020. The Lean Mathematical Library. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs* (New Orleans, LA, USA) *(CPP 2020)*. Association for Computing Machinery, New York, NY, USA, 367–381. `https://doi.org/10.1145/3372885.3373824`

Carette Jacques Farmer William M. Kohlhase Michael and Rabe Florian. 2021. Big Math and the One-Brain Barrier: The Tetrapod Model of Mathematical Knowledge. *Math Intelligencer* 43 (2021), 78–87. `https://doi.org/doi.org/10.1007/s00283-020-10006-0`

Christine Paulin-Mohring. 2012. *Introduction to the Coq Proof-Assistant for Practical Software Verification.* Springer Berlin Heidelberg, Berlin, Heidelberg, 45–95. `https://doi.org/10.1007/978-3-642-35746-6_3`

JD Phillips and David Stanovskỳ. 2010. Automated theorem proving in quasigroup and loop theory. *Ai Communications* 23, 2-3 (2010), 267–283.

M. Saqib Nawaz, Moin Malik, Yi Li, Meng Sun, and M. Ikram Ullah Lali. 2019. A Survey on Theorem Provers in Formal Methods. *arXiv e-prints*, Article arXiv:1912.03028 (Dec. 2019), arXiv:1912.03028 pages. arXiv:1912.03028 [cs.SE]

Mikael Stener. 2016. Moufang Loops: General theory and visualization of non-associative Moufang loops of order 16.

Wikipedia contributors. 2022a. Magma (algebra) — Wikipedia, The Free Encyclopedia. `https://en.wikipedia.org/w/index.php?title=Magma_(algebra)&oldid=1125597787` [Online; accessed 16-January-2023].

Wikipedia contributors. 2022b. Outline of algebraic structures — Wikipedia, The Free
Encyclopedia. `https://en.wikipedia.org/w/index.php?title=Outline_of_`
`algebraic_structures&oldid=1107380309` [Online; accessed 16-January-2023].

Wikipedia contributors. 2022c. Quasigroup — Wikipedia, The Free Encyclope-
dia. `https://en.wikipedia.org/w/index.php?title=Quasigroup&oldid=`
`1123964335` [Online; accessed 7-January-2023].

Wikipedia contributors. 2023a. Group (mathematics) — Wikipedia, The Free Encyclo-
pedia. `https://en.wikipedia.org/w/index.php?title=Group_(mathematics)`
`&oldid=1133598242` [Online; accessed 16-January-2023].

Wikipedia contributors. 2023b. Ring (mathematics) — Wikipedia, The Free Encyclo-
pedia. `https://en.wikipedia.org/w/index.php?title=Ring_(mathematics)`
`&oldid=1133737666` [Online; accessed 16-January-2023].