GROUPS

ARTHUR RYMAN

Abstract. This article formalizes group-like algebraic structures, namely magmas, semigroups, monoids, groups, and abelian groups, using Z Notation. It has been type checked by fUZZ.

Contents

Date: April 11, 2025.

1. Introduction

Groups are ubiquitous in mathematics and physics. This article formalizes groups and related group-like algebraic structures using Z Notation[1]. It has been type checked by *f*uzz[2].

2. Group-like Algebraic Structures

In general, an *algebraic structure* consists of one or mores sets of elements equipped with one or more objects, such as operations, defined on them. A group is an algebraic structure equipped with one binary operation, typically referred to as its *product* or *group law*.

Magmas, semigroups, monoids, and abelian groups are algebraic structures that are like groups but differ from them in terms of the properties imposed on their product operation.

2.1. **Genericity.** In general, the definition of a structure does not depend on the concrete types of its underlying sets of elements. Instead, the definition of a structure is usually given in terms of one or more *generic parameters* that represent arbitrary given sets. We use symbols like t, u, and v as generic parameters in definitions. We use symbols like T, U, and V as arbitrary sets in propositions.

2.2. **Partial Binary Operations.** A *partial binary operation* on a set of elements t is a partial function from pairs of elements to elements.

Define $PBINOP[\mathsf{t}]$ to be the set of all partial binary operations on t.

$$PBINOP[\mathsf{t}] == \mathsf{t} \times \mathsf{t} \pfun \mathsf{t}$$

Here we are using the convention that uppercase names denote *type abbreviations* declared for use by the *f*UZZ type checker.

Example (Integer Division and Modulus)**.** *Integer division and modulus are partial binary operations on* $\mathbb{Z}$*.*

$$(\_ \mathsf{div} \_) \in PBINOP[\mathbb{Z}]$$

$$(\_ \mathsf{mod} \_) \in PBINOP[\mathbb{Z}]$$

2.3. **Total Binary Operations.** A *total binary operation*, or simply a *binary operation*, is a partial binary operation that is defined for every pair of elements.

Define $binop[\mathsf{t}]$ to be the set of all binary operations on t.

$$binop[\mathsf{t}] == \mathsf{t} \times \mathsf{t} \fun \mathsf{t}$$

Remark. *Every binary operation is a partial binary operation.*

$$binop[\mathsf{T}] \subseteq PBINOP[\mathsf{T}]$$

Example (Integer Addition, Subtraction, and Multiplication)**.** *Integer addition, subtraction, and multiplication are binary operations on* $\mathbb{Z}$*.*

$$(\_ + \_) \in binop[\mathbb{Z}]$$

$$(\_ - \_) \in binop[\mathbb{Z}]$$

$$(\_ * \_) \in binop[\mathbb{Z}]$$

Counterexample (Integer Division and Modulus)**.** *Integer division and modulus by* 0 *is undefined.*

$$\forall\, n : \mathbb{Z} \bullet (n, 0) \notin \mathrm{dom}(\_ \mathsf{div} \_)$$

$$\forall\, n : \mathbb{Z} \bullet (n, 0) \notin \mathrm{dom}(\_ \mathsf{mod} \_)$$

Therefore, integer division and modulus are not total binary operations on $\mathbb{Z}$*.*

$$(\_ \mathsf{div} \_) \notin binop[\mathbb{Z}]$$

$$(\_ \mathsf{mod} \_) \notin binop[\mathbb{Z}]$$

2.4. **Carriers.** The main underlying set of elements in an algebraic structure is sometimes referred to as its *carrier*. When writing informal mathematics, it is normally unnecessary to distinguish between a structure and its carrier since the intended meaning is usually clear from context. For example, consider the following statement:

> Let G be a group and let g be an element of G.

Here the first instance of G stands for the group structure while the second stands for its carrier.

However, a given set of elements may participate in more than one structure in some contexts. For example, the set of integers has both additive and multiplicative structures. In such cases it may be ambiguous if only the carrier is specified. Furthermore, if the mathematics is expressed using a formal language such as Z Notation, distinct mathematical objects must be referred to using distinct names or expressions.

In order to differentiate between structures and their carriers, this article adopts the common mathematical practice of defining structures as *tuples* consisting of a carrier together with one or more additional objects such as operations or distinguished elements.

When introducing variables to refer to structures and their carriers, we'll use some typographical convention such as bold font to relate the two. For example, we'll use $\mathbf{A}$ to refer to the structure that has carrier A.

Let A be a subset of t. We say that a structure $\mathbf{A}$ with carrier A is a *structure in* t. If A coincides with t we say that $\mathbf{A}$ is a *structure on* t. Note that a structure on t is also a structure in t.

3. Magmas

3.1. **Magmas.** A *magma* is a set A equipped with a total binary operation, generically referred to as a *product*. Let $x \cdot y$ denote the product of x and y. Regarded as a structure $\mathbf{A}$, a magma is a pair $(A, (\_ \cdot \_))$.

Example (Integer Arithmetic)**.** *Define int_add, int_sub, and int_mul to be the integers equipped with addition, subtraction, and multiplication. These are magmas on the set of integers because the operations are total binary operations on the set of integers.*

$int\_add == (\mathbb{Z}, (\_ + \_))$

$int\_sub == (\mathbb{Z}, (\_ - \_))$

$int\_mul == (\mathbb{Z}, (\_ * \_))$

Define $MAGMA[\mathsf{t}]$ to be the type abbreviation for a magma structure.

$MAGMA[\mathsf{t}] == \mathbb{P}\,\mathsf{t} \times PBINOP[\mathsf{t}]$

Example (Integer Arithmetic)**.** *Integer addition, subtraction, and multiplication belong to the type of integer magma structures.*

$int\_add \in MAGMA[\mathbb{Z}]$

$int\_sub \in MAGMA[\mathbb{Z}]$

$int\_mul \in MAGMA[\mathbb{Z}]$

Magma[t]

$A : \mathbb{P}\, \mathsf{t}$
$\_ \cdot \_ : PBINOP[\mathsf{t}]$
$\mathbf{A} : MAGMA[\mathsf{t}]$

$(\_ \cdot \_) \in binop[A]$

$\mathbf{A} = (A, (\_ \cdot \_))$

- The product is a total binary operation on A.
- The structure is the pair consisting of the carrier and the binary operation.

Example (Integer Arithmetic)**.** *Integer addition, subtraction, and multiplication are integer magmas.*

(**let** $A == \mathbb{Z}$; $(\_ \cdot \_) == (\_ + \_)$; $\mathbf{A} == int\_add \bullet Magma[\mathbb{Z}]$)

(**let** $A == \mathbb{Z}$; $(\_ \cdot \_) == (\_ - \_)$; $\mathbf{A} == int\_sub \bullet Magma[\mathbb{Z}]$)

(**let** $A == \mathbb{Z}$; $(\_ \cdot \_) == (\_ * \_)$; $\mathbf{A} == int\_mul \bullet Magma[\mathbb{Z}]$)

Observe that giving examples in terms of schema components can become somewhat verbose. We'll therefore define simpler, related sets in terms of previously defined schemas.

Define $magma[\mathsf{t}]$ to be the set of all magmas in t.

$magma[\mathsf{t}] == \{\, Magma[\mathsf{t}] \bullet \mathbf{A} \,\}$

Remark. *Every magma in* t *has type* $MAGMA[\mathsf{t}]$.

$magma[\mathsf{T}] \subseteq MAGMA[\mathsf{T}]$

Example (Integer Arthmetic)**.** *Integer addition, subtraction, and multiplication are magmas in the set of integers.*

$int\_add \in magma[\mathbb{Z}]$

$int\_sub \in magma[\mathbb{Z}]$

$int\_mul \in magma[\mathbb{Z}]$

Define $magma\_on(A)$ to be the set of all magmas on A.

$magma\_on[\mathsf{t}] == (\lambda\, A : \mathbb{P}\, \mathsf{t} \bullet \{\, A \,\} \lhd magma[\mathsf{t}])$

Remark. $magma\_on(A)$ *is a subset of* $magma[\mathsf{t}]$.

$\forall\, A : \mathbb{P}\, \mathsf{T} \bullet magma\_on(A) \subseteq magma[\mathsf{T}]$

Remark. *Every magma is a magma on its carrier.*

$\forall\, Magma[\mathsf{T}] \bullet \mathbf{A} \in magma\_on(A)$

Example (Integer Arithmetic)**.** *Integer addition, subtraction, and multiplication are magmas on* $\mathbb{Z}$*.*

$int\_add \in magma\_on(\mathbb{Z})$

$int\_sub \in magma\_on(\mathbb{Z})$

$int\_mul \in magma\_on(\mathbb{Z})$

3.2. **Maps and Homomorphisms.**

3.2.1. *Maps.* A *magma map* from $\mathbf{A}$ to $\mathbf{A}'$ is a map of their carriers. We refer to A as the *domain* of the map and A' as its *codomain*. Alternatively, we refer to A as the *source* of the map and A' its *target*.

Just as magmas are structures, so also are magma maps. Recall that we may informally use the same name, say A, to refer to both a magma and its carrier. Similarly, we may informally use the same name, say f, to refer to both a magma map structure and its underlying map of the carriers. When we need to distinguish between the structure and its underlying map, we'll use some typographic convention to relate the two. For example, we may use F for the structure and f for its underlying map. That being said, the formal text will always use distinct names in any given context.

Define $MAGMA\_MAP[\mathsf{t}, \mathsf{u}]$ to be the type abbreviation for the set of all maps from magmas in t to magmas in u.

$MAGMA\_MAP[\mathsf{t}, \mathsf{u}] == (MAGMA[\mathsf{t}] \times MAGMA[\mathsf{u}]) \times (\mathsf{t} \pfun \mathsf{u})$

Example. *Define nat_id to be the identity map on the set of natural numbers.*

$nat\_id == \mathrm{id}\, \mathbb{N}$

Define int_add_nat_id to be the following (not very useful) candidate magma map structure.

$int\_add\_nat\_id == (int\_add, int\_add) \mapsto nat\_id$

This structure has the required type.

$int\_add\_nat\_id \in MAGMA\_MAP[\mathbb{Z}, \mathbb{Z}]$

In order for a candidate magma map structure F from $\mathbf{A}$ to $\mathbf{A}'$ to be useful, we further require the underlying map f to be a function from A to A'.

Magma_Map$[\mathsf{t}, \mathsf{u}]$

$Magma[\mathsf{t}]$
$Magma'[\mathsf{u}]$
$f : \mathsf{t} \pfun \mathsf{u}$
$F : MAGMA\_MAP[\mathsf{t}, \mathsf{u}]$

$f \in A \longrightarrow A'$

$F = (\mathbf{A}, \mathbf{A}') \mapsto f$

- f maps A to A'
- A magma map structure F consists of a pair of magmas and a map f between their carriers.

Define $magma\_Map[\mathsf{t}, \mathsf{u}]$ to be the set of all magma maps from magmas in t to magmas in u.

$$magma\_Map[\mathsf{t}, \mathsf{u}] == \{ Magma\_Map[\mathsf{t}, \mathsf{u}] \bullet F \}$$

Counterexample. *The structure int_add_nat_id is not a magma map because the domain of its underlying function* $\mathrm{id}\,\mathbb{N}$ *is* $\mathbb{N}$ *which is a proper subset of* $\mathbb{Z}$ *which is the carrier of int_add.*

$$int\_add\_nat\_id \notin magma\_Map[\mathbb{Z}, \mathbb{Z}]$$

Example. *Define int_square to be the function that maps an integer to its square.*

$$int\_square == (\lambda\, x : \mathbb{Z} \bullet x * x)$$

Define int_squares to be the set of all integers that are squares.

$$int\_squares == \mathrm{ran}\, int\_square$$

Define the following candidate magma map structures.

$$int\_add\_square == (int\_add, int\_add) \mapsto int\_square$$

$$int\_mul\_square == (int\_mul, int\_mul) \mapsto int\_square$$

These structures are in fact magma maps because the domain of underlying map int_square is equal to the source carrier $\mathbb{Z}$*.*

$$int\_add\_square \in magma\_Map[\mathbb{Z}, \mathbb{Z}]$$

$$int\_mul\_square \in magma\_Map[\mathbb{Z}, \mathbb{Z}]$$

Define $magma\_map(\mathbf{A}, \mathbf{A}')$ to be the subset of magma maps from $\mathbf{A}$ to $\mathbf{A}'$.

$$\begin{array}{l} magma\_map[\mathsf{t}, \mathsf{u}] == \\ \quad (\lambda\, \mathbf{A} : magma[\mathsf{t}];\ \mathbf{A}' : magma[\mathsf{u}] \bullet \\ \qquad \{(\mathbf{A}, \mathbf{A}')\} \lhd magma\_Map[\mathsf{t}, \mathsf{u}]) \end{array}$$

Remark. $magma\_map(\mathbf{A}, \mathbf{A}')$ *is a subset of* $magma\_Map[\mathsf{t}, \mathsf{u}]$.

$$\begin{array}{l} \forall\, \mathbf{A} : magma[\mathsf{T}];\ \mathbf{A}' : magma[\mathsf{U}] \bullet \\ \quad magma\_map(\mathbf{A}, \mathbf{A}') \subseteq magma\_Map[\mathsf{T}, \mathsf{U}] \end{array}$$

Example.

$$int\_add\_square \in magma\_map(int\_add, int\_add)$$

$$int\_mul\_square \in magma\_map(int\_mul, int\_mul)$$

3.2.2. *Homomorphisms.* A *magma homomorphism* is magma map that preserves products.

Magma_Hom[t, u]

Magma_Map[t, u]

$\forall x, y : A \bullet f(x \cdot y) = f(x) \cdot' f(y)$

- f preserves the product operation

Define *magma_Hom*[t, u] to be the set of all magma homomorphisms from magmas in t to magmas in u.

$$magma\_Hom[\mathsf{t}, \mathsf{u}] == \{ Magma\_Hom[\mathsf{t}, \mathsf{u}] \bullet F \}$$

Define $magma\_hom(\mathbf{A}, \mathbf{A}')$ to be the subset of magma homomorphisms from $\mathbf{A}$ to $\mathbf{A}'$.

$$magma\_hom[\mathsf{t}, \mathsf{u}] == (\lambda\, \mathbf{A} : magma[\mathsf{t}]; \mathbf{A}' : magma[\mathsf{u}] \bullet \{(\mathbf{A}, \mathbf{A}')\} \lhd magma\_Hom[\mathsf{t}, \mathsf{u}])$$

Remark. *$magma\_hom(\mathbf{A}, \mathbf{A}')$ is a subset of $magma\_Hom[\mathsf{t}, \mathsf{u}]$.*

$$\forall\, \mathbf{A} : magma[\mathsf{T}]; \mathbf{A}' : magma[\mathsf{U}] \bullet magma\_hom(\mathbf{A}, \mathbf{A}') \subseteq magma\_Hom[\mathsf{T}, \mathsf{U}]$$

Counterexample. *The magma map int_add_square is not a magma homomorphism because, in general, the sum of squares is not the square of the sum.*

$$int\_add\_square \notin magma\_hom(int\_add, int\_add)$$

It suffices to show that

$$int\_square(1 + 1) \neq int\_square(1) + int\_square(1)$$

Proof.

$$\begin{aligned} &int\_square(1 + 1) \\ &\quad = int\_square(2) \\ &\quad = 4 \\ &\quad \neq 2 \\ &\quad = 1 + 1 \\ &\quad = int\_square(1) + int\_square(1) \end{aligned}$$

□

Example. *The magma map int_mul_square is a magma homomorphism because, in general, the product of squares is the square of the product.*

$$int\_mul\_square \in magma\_hom(int\_mul, int\_mul)$$

It suffices to show that

$$\forall\, x, y : \mathbb{Z} \bullet int\_square(x * y) = int\_square(x) * int\_square(y)$$

Proof.

$$\forall x, y : \mathbb{Z} \bullet$$
$$int\_square(x * y)$$
$$= (x * y) * (x * y)$$
$$= x * x * y * y$$
$$= (x * x) * (y * y)$$
$$= int\_square(x) * int\_square(y)$$

□

Example (Multiplication by a Constant)**.** *Define* $mul\_const(c)$ *to be the function that multiplies integers by a given integer* c*.*

$$mul\_const ==$$
$$(\lambda\, c : \mathbb{Z} \bullet$$
$$(\lambda\, x : \mathbb{Z} \bullet c * x))$$

Consider this function acting on the integers under addition.

MulConst

$$Magma\_Map[\mathbb{Z}, \mathbb{Z}]$$
$$c : \mathbb{Z}$$

$$\mathbf{A} = \mathbf{A}' = int\_add$$
$$f = mul\_const(c)$$

Define $int\_add\_mul\_const(c)$ *to be the corresponding magma map.*

$$int\_add\_mul\_const == \{\, MulConst \bullet c \mapsto F \,\}$$

The magma map $int\_add\_mul\_const(c)$ *sends* $\mathbb{Z}$ *to* $\mathbb{Z}$ *and preserves addition. Therefore this map is a magma homomorphism from* int_add *to itself.*

$$\forall\, c : \mathbb{Z} \bullet$$
$$int\_add\_mul\_const(c) \in magma\_hom(int\_add, int\_add)$$

Proof.

$$\forall\, c, x, y : \mathbb{Z} \bullet$$
$$c * (x + y) = c * x + c * y$$

□

Example (Exponentiation by a Constant)**.** *Define* $exp\_const(n)$ *to be the function that exponentiates integers to a given natural number* n*.*

$$exp\_const ==$$
$$(\lambda\, n : \mathbb{N} \bullet$$
$$(\lambda\, x : \mathbb{Z} \bullet x ** n))$$

Consider this function acting on the integers under multiplication.

ExpConst

$$Magma\_Map[\mathbb{Z}, \mathbb{Z}]$$
$$n : \mathbb{N}$$

$$\mathbf{A} = \mathbf{A}' = int\_mul$$
$$f = exp\_const(n)$$

Define $int\_mul\_exp\_const(n)$ *to be the corresponding magma map.*

$$int\_mul\_exp\_const == \{ ExpConst \bullet n \mapsto F \}$$

The magma map $int\_mul\_exp\_const(n)$ *sends* $\mathbb{Z}$ *to* $\mathbb{Z}$ *and preserves multiplication. Therefore this map is a magma homomorphism.*

$$\forall n : \mathbb{N} \bullet int\_mul\_exp\_const(n) \in magma\_hom(int\_mul, int\_mul)$$

Proof.

$$\forall n : \mathbb{N}; x, y : \mathbb{Z} \bullet (x * y) ** n = x ** n * y ** n$$

□

3.3. **Identity Maps.**

Remark. *The identity map on the carrier* A *of a magma* $\mathbf{A}$ *is a function from the carrier to itself.*

$$\forall Magma[\mathsf{T}] \bullet \mathrm{id}\, A \in A \longrightarrow A$$

The identity map therefore defines a magma map from any magma to itself.

Magma_Id[t]

$$Magma\_Map[\mathsf{t}, \mathsf{t}]$$

$$\mathbf{A} = \mathbf{A}'$$
$$f = \mathrm{id}\, A$$

- the identity magma map sends a magma to itself
- the underlying map of carriers is the identity map

Define $magma\_id(\mathbf{A})$ to be the magma identity map of $\mathbf{A}$.

$$magma\_id[\mathsf{t}] == \{ Magma\_Id[\mathsf{t}] \bullet \mathbf{A} \mapsto F \}$$

Remark. *magma_id maps magmas to magma maps.*

$$magma\_id[\mathsf{T}] \in MAGMA[\mathsf{T}] \nrightarrow MAGMA\_MAP[\mathsf{T}, \mathsf{T}]$$

Remark. *The identity map preserves products.*

$$\forall Magma[\mathsf{T}] \bullet \forall x, y : A \bullet (\mathrm{id}\, A)(x \cdot y) = x \cdot y = ((\mathrm{id}\, A)x) \cdot ((\mathrm{id}\, A)y)$$

Remark. *The identity map is therefore a magma homomorphism.*

$$\forall\, \mathbf{A} : magma[\mathsf{T}] \bullet \\ magma\_id(\mathbf{A}) \in magma\_hom(\mathbf{A}, \mathbf{A})$$

Example (Identity Maps)**.** *Define the identity magma homomorphisms for integer addition, subtraction, and multiplication.*

$$int\_add\_id == magma\_id(int\_add)$$

$$int\_sub\_id == magma\_id(int\_sub)$$

$$int\_mul\_id == magma\_id(int\_mul)$$

3.4. **Composition.** Let f be a magma map from A to A' and let f' be a magma map from A' to A''. The function composition $g = f' \circ f$ is a magma map from A to A''. The composition is read as "f' after f". Composition of the underlying maps is illustrated in Figure 1.

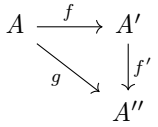

FIGURE 1. Commutative diagram for the composition g of f' after f.

Magma_Composition[t, u, v]

$$Magma\_Map[\mathsf{t}, \mathsf{u}]$$
$$Magma\_Map'[\mathsf{u}, \mathsf{v}]$$
$$g : \mathsf{t} \pfun \mathsf{v}$$
$$G : magma\_Map[\mathsf{t}, \mathsf{v}]$$

$$g = f' \circ f$$
$$G = (\mathbf{A}, \mathbf{A}'') \mapsto g$$

Remark. *The composition of two magma maps is a magma map.*

$$\forall\, Magma\_Composition[\mathsf{T}, \mathsf{U}, \mathsf{V}] \bullet \\ G \in magma\_map(\mathbf{A}, \mathbf{A}'')$$

Let $G = F' \circ F$ denote the composition of magma maps.

$$(\_ \circ \_)[\mathsf{t}, \mathsf{u}, \mathsf{v}] == \{\, Magma\_Composition[\mathsf{t}, \mathsf{u}, \mathsf{v}] \bullet (F', F) \mapsto G \,\}$$

Composition of magma map structures is illustrated in Figure 2.

Remark. *The identity map is a left and right identity element with respect to composition.*

$$\forall\, Magma\_Map[\mathsf{T}, \mathsf{U}] \bullet \\ magma\_id(\mathbf{A}') \circ F = F = F \circ magma\_id(\mathbf{A})$$

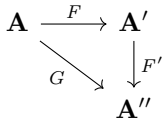

FIGURE 2. Commutative diagram for the composition G of F' after F.

Although we have defined the composition of magma maps we are, of course, more interested the composition of magma homomorphisms.

Remark. *The composition of magma homomorphisms is a magma homomorphism.*

$$\forall\, Magma\_Composition[\mathsf{T}, \mathsf{U}, \mathsf{V}] \mid \\ F \in magma\_hom(\mathbf{A}, \mathbf{A}') \land F' \in magma\_hom(\mathbf{A}', \mathbf{A}'') \bullet \\ G \in magma\_hom(\mathbf{A}, \mathbf{A}'')$$

Example (Multiplication by a Constant)**.** *The composition of multiplication by constants is multiplication by the product of the constants.*

$$\forall\, a, b : \mathbb{Z} \bullet \\ int\_add\_mul\_const(a) \circ int\_add\_mul\_const(b) = int\_add\_mul\_const(a * b)$$

Example (Exponentiation by a Constant)**.** *The composition of exponentiation by constants is exponentiation by the product of the constants.*

$$\forall\, m, n : \mathbb{N} \bullet \\ int\_mul\_exp\_const(m) \circ int\_mul\_exp\_const(n) = int\_mul\_exp\_const(m * n)$$

3.5. **Subsets and Submagmas.**

3.5.1. *Subsets.* Consider a subset S of the elements A of magma $\mathbf{A}$. Let $\mathbf{S}$ be the structure that consists of the pair $(\mathbf{A}, S)$.

Define $MAGMA\_SUBSET[\mathsf{t}]$ to be the type abbreviation for magma subset structures in t.

$$MAGMA\_SUBSET[\mathsf{t}] == MAGMA[\mathsf{t}] \times \mathbb{P}\, \mathsf{t}$$

Magma_Subset[t]

$S : \mathbb{P}\, \mathsf{t}$
$Magma[\mathsf{t}]$
$\mathbf{S} : MAGMA\_SUBSET[\mathsf{t}]$

$S \subseteq A$

$\mathbf{S} = (\mathbf{A}, S)$

Define $magma\_Subset[\mathsf{t}]$ to be the set of all magma subset structures in t.

$$magma\_Subset[\mathsf{t}] == \{\, Magma\_Subset[\mathsf{t}] \bullet \mathbf{S} \,\}$$

Define $magma\_subset(\mathbf{A})$ to be the set of all magma subset structures of $\mathbf{A}$.

$$magma\_subset[\mathsf{t}] == (\lambda\, \mathbf{A} : magma[\mathsf{t}] \bullet \{\, \mathbf{A} \,\} \lhd magma\_Subset[\mathsf{t}])$$

Example. *The natural numbers are a subset of the integers.*

$\mathbb{N} \subset \mathbb{Z}$

Define the corresponding subset structures for the integers under addition, subtraction, and multiplication.

$int\_add\_nat == (int\_add, \mathbb{N})$

$int\_sub\_nat == (int\_sub, \mathbb{N})$

$int\_mul\_nat == (int\_mul, \mathbb{N})$

They are therefore magma subsets of the corresponding magmas.

$int\_add\_nat \in magma\_subset(int\_add)$

$int\_sub\_nat \in magma\_subset(int\_sub)$

$int\_mul\_nat \in magma\_subset(int\_mul)$

3.5.2. *Submagmas.* A *submagma* is a magma subset that is closed under products.

Magma_Submagma[t]

$Magma\_Subset[\mathsf{t}]$

$\forall x, y : S \bullet x \cdot y \in S$

Define $magma\_Submagma[\mathsf{t}]$ to be the set of all submagma structures in t.

$magma\_Submagma[\mathsf{t}] == \{ Magma\_Submagma[\mathsf{t}] \bullet \mathbf{S} \}$

Remark. *Every submagma structure is a subset structure.*

$magma\_Submagma[\mathsf{T}] \subseteq magma\_Subset[\mathsf{T}]$

Define $magma\_submagma(\mathbf{A})$ to be the set of all submagmas of $\mathbf{A}$.

$magma\_submagma[\mathsf{t}] == (\lambda \mathbf{A} : magma[\mathsf{t}] \bullet \{ \mathbf{A} \} \lhd magma\_Submagma[\mathsf{t}])$

Example. *Natural numbers are closed under the operations of addition and multiplication. Therefore, they are submagmas of the integers under addition and multiplication.*

$int\_add\_nat \in magma\_submagma(int\_add)$

$int\_mul\_nat \in magma\_submagma(int\_mul)$

Counterexample. *The natural numbers are not closed under subtraction and so are not a submagma of the integers under subtraction.*

$int\_sub\_nat \notin magma\_submagma(int\_sub)$

3.6. **Restriction.** The *restriction* of a submagma S' of $\mathbf{A}'$ is the magma $\mathbf{A}$ whose elements are S' and whose product is the restriction of the product of $\mathbf{A}'$ to S'.

Magma_Restriction[t]
$Magma[\mathsf{t}]$
$Magma\_Submagma'[\mathsf{t}]$

$A = S'$

$\forall\, x, y : A \bullet x \cdot y = x \cdot' y$

Define *magma_Restriction*[t] to be the set of all restrictions of submagmas in t.

$magma\_Restriction[\mathsf{t}] == \{\, Magma\_Restriction[\mathsf{t}] \bullet \mathbf{S}' \mapsto \mathbf{A} \,\}$

Remark. *Magma restriction maps submagmas to magmas.*

$magma\_Restriction[\mathsf{T}] \in magma\_Submagma[\mathsf{T}] \longrightarrow magma[\mathsf{T}]$

Example (Natural Number Arithmetic)**.** *Define the restrictions of integer addition and multiplication to the natural numbers.*

$nat\_add == magma\_Restriction(int\_add\_nat)$

$nat\_mul == magma\_Restriction(int\_mul\_nat)$

Define *magma_restriction*($\mathbf{A}$) to be the set of all restrictions of submagmas of $\mathbf{A}$.

$magma\_restriction[\mathsf{t}] == (\lambda\, \mathbf{A} : magma[\mathsf{t}] \bullet$
$\quad magma\_submagma(\mathbf{A}) \lhd magma\_Restriction[\mathsf{t}])$

Remark. *Restriction is a function from submagmas of* $\mathbf{A}$ *to magmas.*

$\forall\, \mathbf{A} : magma[\mathsf{T}] \bullet$
$\quad magma\_restriction(\mathbf{A}) \in magma\_submagma(\mathbf{A}) \longrightarrow magma[\mathsf{T}]$

Example (Natural Number Arithmetic)**.**

$nat\_add = magma\_restriction(int\_add) int\_add\_nat$

$nat\_mul = magma\_restriction(int\_mul) int\_mul\_nat$

3.7. **Inclusion.** The identity map is a magma map from the restriction of a submagma to its enclosing magma.

Magma_Inclusion[t]
$Magma\_Restriction[\mathsf{t}]$
$Magma\_Map[\mathsf{t}, \mathsf{t}]$

$f = \mathrm{id}\, A$

Define *magma_Inclusion* to be the set of all magma inclusions.

$magma\_Inclusion[\mathsf{t}] == \{\, Magma\_Inclusion[\mathsf{t}] \bullet F \,\}$

Example (Natural Number Arithmetic)**.** *Define magma maps from natural number arithmetic to integer arithmetic.*

$nat\_int\_add == (nat\_add, int\_add) \mapsto \mathrm{id}\,\mathbb{N}$

$nat\_int\_mul == (nat\_mul, int\_mul) \mapsto \mathrm{id}\,\mathbb{N}$

These maps are inclusions.

$nat\_int\_add \in magma\_Inclusion[\mathbb{Z}]$

$nat\_int\_mul \in magma\_Inclusion[\mathbb{Z}]$

Define $magma\_inclusion(\mathbf{A}, \mathbf{A}')$ to be the set of all magma inclusions of $\mathbf{A}$ as a submagma of $\mathbf{A}'$.

$$
\begin{array}{l}
magma\_inclusion[\mathsf{t}] == \\
\quad (\lambda\, \mathbf{A}, \mathbf{A}' : magma[\mathsf{t}] \bullet \\
\qquad \{\, (\mathbf{A}, \mathbf{A}')\, \} \lhd magma\_Inclusion[\mathsf{t}])
\end{array}
$$

Example (Natural Number Arithmetic)**.** *The previously defined inclusions are inclusions from nat_add to int_add and from nat_mul to int_mul.*

$nat\_int\_add \in magma\_inclusion(nat\_add, int\_add)$

$nat\_int\_mul \in magma\_inclusion(nat\_mul, int\_mul)$

Remark. *Inclusion maps are magma homomorphisms.*

$$
\begin{array}{l}
\forall\, \mathbf{A}, \mathbf{A}' : magma[\mathsf{T}] \bullet \\
\quad magma\_inclusion(\mathbf{A}, \mathbf{A}') \subseteq magma\_hom(\mathbf{A}, \mathbf{A}')
\end{array}
$$

3.8. **Images.** The *subimage* of a magma map f from A to A' is the magma subset $\mathbf{S}'$ of $\mathbf{A}'$ that consists of the images of the elements of A under f.

Magma_Subimage[t, u]

$Magma\_Map[\mathsf{t}, \mathsf{u}]$
$Magma\_Subset'[\mathsf{u}]$

$S' = \mathrm{ran}\, f$

Define *magma_Subimage* to be the function that associates any magma map F with its subimage $\mathbf{S}'$.

$magma\_Subimage[\mathsf{t}, \mathsf{u}] == \{\, Magma\_Subimage[\mathsf{t}, \mathsf{u}] \bullet F \mapsto \mathbf{S}' \,\}$

Example (Subimage of *int_add_square*)**.**

$magma\_Subimage(int\_add\_square) = (int\_add, int\_squares)$

Define $magma\_subimage(\mathbf{A}, \mathbf{A}')$ to be the function that associates any magma map F from $\mathbf{A}$ to $\mathbf{A}'$ with its subimage $\mathbf{S}'$ in $\mathbf{A}'$.

$$
\begin{array}{l}
magma\_subimage[\mathsf{t}, \mathsf{u}] == \\
\quad (\lambda\, \mathbf{A} : magma[\mathsf{t}]; \mathbf{A}' : magma[\mathsf{u}] \bullet \\
\qquad magma\_map(\mathbf{A}, \mathbf{A}') \lhd magma\_Subimage[\mathsf{t}, \mathsf{u}])
\end{array}
$$

Remark. *The subimage of a magma homomorphism is a submagma of its target.*

$$\begin{array}{l}\forall\, \mathbf{A} : \mathit{magma}[\mathsf{T}];\ \mathbf{A}' : \mathit{magma}[\mathsf{U}] \bullet \\ \quad \forall\, F : \mathit{magma\_hom}(\mathbf{A}, \mathbf{A}') \bullet \\ \qquad \mathit{magma\_subimage}(\mathbf{A}, \mathbf{A}')\, F \in \mathit{magma\_submagma}(\mathbf{A}')\end{array}$$

Proof. It suffices to show that the product of any two elements x', y' in the subimage S' is also in S'. By definition of the image, there exists elements x and y in A such that $x' = f(x)$ and $y' = f(y)$. Therefore $x' \mathbin{.'} y' = f(x) \mathbin{.'} f(y) = f(x \cdot y)$ which is clearly in the image of f. □

Here is a second, more formal, proof of the remark. It is set out in a way that lends itself to translation into a formal proof language such as Lean 4.

Proof.

$$\begin{array}{ll}
\mathbf{A} : \mathit{magma}[\mathsf{T}] & [\text{hypothesis}] \\
\mathbf{A}' : \mathit{magma}[\mathsf{U}] & [\text{hypothesis}] \\
F : \mathit{magma_hom}(\mathbf{A}, \mathbf{A}') & [\text{hypothesis}] \\
(A, (_ \cdot _)) == \mathbf{A} & [\text{definition of } \mathit{magma}] \\
(A', (_ \cdot' _)) == \mathbf{A}' & [\text{definition of } \mathit{magma}] \\
(\mathbf{A}, \mathbf{A}') \mapsto f == F & [\text{definition of } \mathit{magma_hom}] \\
\mathbf{S}' == \mathit{magma_subimage}(\mathbf{A}, \mathbf{A}')F & \\
(\mathbf{A}', S') == \mathbf{S}' & [\text{definition of } \mathit{magma_subimage}] \\
S' = \operatorname{ran} f & [\text{definition of } \mathit{magma_subimage}] \\
\quad x', y' : S' & [\text{introduce assumption } [h]] \\
\quad f\ x == x' & [x' \in \operatorname{ran} f] \\
\quad f\ y == y' & [y' \in \operatorname{ran} f] \\
\quad x' \cdot' y' = (f\ x) \cdot' (f\ y) & \\
\qquad = f(x \cdot y) & [f \text{ is a homomorphism}] \\
\qquad \in \operatorname{ran} f & \\
\qquad = S' & \\
\forall\, x', y' : S' \bullet x' \cdot' y' \in S' & [\text{eliminate assumption } [h]] \\
\mathbf{S}' \in \mathit{magma_submagma}(\mathbf{A}') & [\text{definition of } \mathit{magma_submagma}]
\end{array}$$

□

Given a magma homomorphism $F = (\mathbf{A}, \mathbf{A}) \mapsto f$, its subimage $(\mathbf{A}', \operatorname{ran} f)$ is a submagma of $\mathbf{A}'$. The restriction of this submagma is therefore a magma on $\operatorname{ran} f$. We refer to this magma as the *image* of F.

Magma_Image[t, u]
Magma_Hom[t, u]
Magma_Subimage[t, u]
Magma_Restriction′[u]

Define *magma_image* to be the function that sends a magma homomorphism to the restriction of its subimage.

$$magma\_image[\mathsf{t}, \mathsf{u}] == \{\, Magma\_Image[\mathsf{t}, \mathsf{u}] \bullet F \mapsto \mathbf{A}'' \,\}$$

Example. *The image of int_mul_square.*

Define int_squares_mul to be the magma on int_squares under multiplication.

$$int\_squares\_mul == magma\_image(int\_mul\_square)$$

3.9. **Containment.** Let $\mathbf{S}_1 = (\mathbf{A}, S_1)$ and $\mathbf{S}_2 = (\mathbf{A}, S_2)$ be magma subsets of $\mathbf{A}$. Define *containment* of $\mathbf{S}_1$ in $\mathbf{S}_2$ to mean that S_1 is contained is S_2.

Magma_Containment[t]

$Magma\_Subset_1[\mathsf{t}]$
$Magma\_Subset_2[\mathsf{t}]$
$Magma[\mathsf{t}]$

$\mathbf{A}_1 = \mathbf{A}_2 = \mathbf{A}$

$S_1 \subseteq S_2$

Define *magma_Containment* to be the set of all pairs of magma subsets that are related by containment.

$$magma\_Containment[\mathsf{t}] == \{\, Magma\_Containment[\mathsf{t}] \bullet \mathbf{S}_1 \mapsto \mathbf{S}_2 \,\}$$

Remark. *Containment is a binary relation on the set of all magma subsets.*

$$magma\_Containment[\mathsf{T}] \in magma\_Subset[\mathsf{T}] \leftrightarrow magma\_Subset[\mathsf{T}]$$

Let $\mathbf{S}_1 \subseteq \mathbf{S}_2$ denote containment of magma subsets.

$$(\_ \subseteq \_)[\mathsf{t}] == magma\_Containment[\mathsf{t}]$$

Example. *The empty and full subsets.*

$$\forall\, Magma[\mathsf{T}] \bullet (\mathbf{A}, \varnothing) \subseteq (\mathbf{A}, \varnothing)$$

$$\forall\, Magma[\mathsf{T}] \bullet (\mathbf{A}, \varnothing) \subseteq (\mathbf{A}, A)$$

$$\forall\, Magma[\mathsf{T}] \bullet (\mathbf{A}, A) \subseteq (\mathbf{A}, A)$$

Define *magma_containment*($\mathbf{A}$) to be the set of all pairs of magma subsets of $\mathbf{A}$ that are related by containment.

$$\begin{aligned} &magma\_containment[\mathsf{t}] == \\ &\quad (\lambda\, \mathbf{A} : magma[\mathsf{t}] \bullet \\ &\qquad magma\_subset(\mathbf{A}) \lhd magma\_Containment[\mathsf{t}]) \end{aligned}$$

3.10. **Intersection.** Given two subsets S_1, S_2 of magma $\mathbf{A}$, their intersection S is a subset of A. The intersection of two subset structures is therefore another subset structure.

Magma_Intersection[t]

$Magma\_Subset_1[\mathsf{t}]$
$Magma\_Subset_2[\mathsf{t}]$
$Magma\_Subset[\mathsf{t}]$

$\mathbf{A}_1 = \mathbf{A}_2 = \mathbf{A}$

$S = S_1 \cap S_2$

Define *magma_Intersection* to be the relation between compatible pairs of magma subsets and their intersection.

$magma\_Intersection[\mathsf{t}] == \{\, Magma\_Intersection[\mathsf{t}] \bullet (\mathbf{S}_1, \mathbf{S}_2) \mapsto \mathbf{S} \,\}$

Remark. *Intersection is a partial binary operation on the set of subsets of magmas.*

$magma\_Intersection[\mathsf{T}] \in PBINOP[magma\_Subset[\mathsf{T}]]$

Let $\mathbf{S} = \mathbf{S}_1 \cap \mathbf{S}_2$ denote the intersection of magma subsets.

$(\_ \cap \_)[\mathsf{t}] == magma\_Intersection[\mathsf{t}]$

Remark. *The intersection of subsets of* $\mathbf{A}$ *is a subset of* $\mathbf{A}$.

$$\forall\, \mathbf{A} : magma[\mathsf{T}] \bullet \\ \quad \forall\, \mathbf{S}_1, \mathbf{S}_2 : magma\_subset(\mathbf{A}) \bullet \\ \quad\quad \mathbf{S}_1 \cap \mathbf{S}_2 \in magma\_subset(\mathbf{A})$$

Remark. *The intersection of submagmas of* $\mathbf{A}$ *is a submagma of* $\mathbf{A}$.

$$\forall\, \mathbf{A} : magma[\mathsf{T}] \bullet \\ \quad \forall\, \mathbf{S}_1, \mathbf{S}_2 : magma\_submagma(\mathbf{A}) \bullet \\ \quad\quad \mathbf{S}_1 \cap \mathbf{S}_2 \in magma\_submagma(\mathbf{A})$$

TODO: prove the above and then generalize it to the intersection of an arbitrary nonempty family of submagmas.

3.11. **Generation.** Let $\mathbf{A}$ be a magma, and let $(\mathbf{A}, S)$ be a magma subset. Define the submagma *generated* by S to be the smallest submagma $(\mathbf{A}, S')$ that contains S.

Magma_Generation[t]

$Magma\_Subset[\mathsf{t}]$
$Magma\_Submagma'[\mathsf{t}]$

$\mathbf{A}' = \mathbf{A}$

$S \subseteq S'$

$$\forall\, Magma\_Submagma''[\mathsf{t}] \mid \\ \quad \mathbf{A}'' = \mathbf{A} \bullet \\ \quad\quad S \subseteq S'' \Rightarrow S' \subseteq S''$$

Submagma generation defines a relation between magma subsets and submagmas. Define *magma_Generation* to be this relation.

$$magma\_Generation[\mathsf{t}] == \{ Magma\_Generation[\mathsf{t}] \bullet (\mathbf{A}, S) \mapsto (\mathbf{A}, S') \}$$

Define $magma\_generation(\mathbf{A})$ to be this relation restricted to $\mathbf{A}$.

$$magma\_generation[\mathsf{t}] == (\lambda\, \mathbf{A} : magma[\mathsf{t}] \bullet magma\_subset(\mathbf{A}) \lhd magma\_Generation[\mathsf{t}])$$

Remark. *Recall that the intersection of submagmas is a submagma. The submagma generated by a magma subset is therefore the intersection of all submagmas that contain the subset.*

true

TODO: define the submagma generated by a subset to be the smallest submagma that contains the subset. The submagmas are ordered by containment. The smallest submagma is the intersection of the family of all submagmas that contain the subset.

4. Semigroups

4.1. **Semigroups.** A magma is said to be *associative* if the result of applying its operation to any three elements is independent of the order in which it is applied pairwise. An associative magma is called a *semigroup*.

Semigroup[t]

$Magma[\mathsf{t}]$

$$\forall\, x, y, z : A \bullet x \cdot y \cdot z = x \cdot (y \cdot z)$$

Let $semigroup[\mathsf{t}]$ denote the set of all semigroups in t.

$$semigroup[\mathsf{t}] == \{ Semigroup[\mathsf{t}] \bullet \mathbf{A} \}$$

Remark. *Every semigroup is a magma.*

$$semigroup[\mathsf{T}] \subseteq magma[\mathsf{T}]$$

Example (Sequence Concatenation)**.** *Let X be a subset of* t*. Finite sequences in X with the operation of concatenation form a semigroup since concatenation is associative.*

SequenceConcat[t]

$Magma[\operatorname{seq} \mathsf{t}]$

$X : \mathbb{P}\, \mathsf{t}$

$$A = \operatorname{seq} X$$

$$\forall\, x, y : A \bullet x \cdot y = x \frown y$$

Define seq_concat(X) to be the set of all magmas that consists of finite sequences in some subset X of t *under concatenation.*

$$seq\_concat[\mathsf{t}] == \{\, SequenceConcat[\mathsf{t}] \bullet X \mapsto \mathbf{A} \,\}$$

$$\forall\, X : \mathbb{P}\, \mathsf{T} \bullet seq\_concat(X) \in semigroup[\mathrm{seq}\, X]$$

4.2. **Homomorphisms.** A *semigroup homomorphism* is a homomorphism of the underlying magmas.

Semigroup_Hom[t, u]

$Magma\_Hom[\mathsf{t}, \mathsf{u}]$

$\mathbf{A} \in semigroup[\mathsf{t}]$

$\mathbf{A}' \in semigroup[\mathsf{u}]$

- $\mathbf{A}$ is a semigroup in t
- $\mathbf{A}'$ is a semigroup in u

Let $semigroup\_Hom[\mathsf{t}, \mathsf{u}]$ be the set of all homomorphisms from semigroups in t to semigroups in u.

$$semigroup\_Hom[\mathsf{t}, \mathsf{u}] == \{\, Semigroup\_Hom[\mathsf{t}, \mathsf{u}] \bullet F \,\}$$

Let $semigroup\_hom(\mathbf{A}, \mathbf{A}')$ be the subset of semigroup homomorphisms from $\mathbf{A}$ to $\mathbf{A}'$.

$$\begin{array}{l} semigroup\_hom[\mathsf{t}, \mathsf{u}] == \\ \quad (\lambda\, \mathbf{A} : semigroup[\mathsf{t}];\ \mathbf{A}' : semigroup[\mathsf{u}] \bullet \\ \quad\quad \{\, (\mathbf{A}, \mathbf{A}') \,\} \lhd semigroup\_Hom[\mathsf{t}, \mathsf{u}]) \end{array}$$

Remark. *The identity mapping of a semigroup to itself is a semigroup homomorphism.*

$$\begin{array}{l} \forall\, Magma\_Id[\mathsf{T}] \bullet \\ \quad \mathbf{A} \in semigroup[\mathsf{T}] \Rightarrow \\ \quad\quad Semigroup\_Hom[\mathsf{T}, \mathsf{T}] \end{array}$$

Remark. *Every magma homomorphism of semigroups is a semigroup homomorphism.*

$$\begin{array}{l} \forall\, Magma\_Hom[\mathsf{T}, \mathsf{U}] \bullet \\ \quad \mathbf{A} \in semigroup[\mathsf{T}] \land \mathbf{A}' \in semigroup[\mathsf{U}] \Rightarrow \\ \quad\quad F \in semigroup\_hom(\mathbf{A}, \mathbf{A}') \end{array}$$

Remark. *If F is magma homomorphism from* $\mathbf{A}$ *to* $\mathbf{A}'$ *and* $\mathbf{A}$ *is a semigroup then the image of F is a semigroup.*

$$\begin{array}{l} \forall\, Magma\_Hom[\mathsf{T}, \mathsf{U}] \bullet \\ \quad \mathbf{A} \in semigroup[\mathsf{T}] \Rightarrow magma\_image(F) \in semigroup[\mathsf{U}] \end{array}$$

4.3. **Composition.** Consider the composition of semigroup homomorphisms.

Semigroup_Composition[t, u, v]
Magma_Composition[t, u, v]
Semigroup[t]
Semigroup′[u]

Remark. *The composition of semigroup homomorphisms is a semigroup homomorphism.*

$\forall$ *Semigroup_Composition*[T, U, V] •
$G \in semigroup\_hom(\mathbf{A}, \mathbf{A}'')$

5. Monoids

5.1. **Identity Elements.** Let **A** be a magma and let e be an element of A. The element e is said to be an *identity element* of **A** if left and right products with it leave all elements unchanged.

IdentityElement[t]
Magma[t]
e : t

$e \in A$
$\forall x : A \bullet e \cdot x = x = x \cdot e$

Clearly, not all magmas have identity elements. For example, consider the set of even integers under multiplication. However, if a magma has an identity element, then it is unique. This will be proved next.

Let *identity_element* denote the relation between magmas and their identity elements.

identity_element[t] ==
{ *IdentityElement*[t] • **A** $\mapsto$ e }

Remark.

identity_element[T] $\in$ *magma*[T] $\leftrightarrow$ T

Consider the case of a magma **A** that has, possibly distinct, identity elements e, e'.

IdentityElements[t]
Magma[t]
e, e' : t

A $\mapsto$ $e \in$ *identity_element*[t]
A $\mapsto$ $e' \in$ *identity_element*[t]

Remark. *If a magma has an identity element then it is unique.*

$\forall$ *IdentityElements*[T] •
$e = e'$

Proof.

$$
\begin{aligned}
& e \\
&= e \cdot e' && [e' \text{ is an identity element}] \\
&= e' && [e \text{ is an identity element}]
\end{aligned}
$$

□

Remark. *The preceding remark shows that if an identity element exists then it is unique. This means that the relation from magmas to identity elements is a partial function.*

$identity\_element[\mathsf{T}] \in magma[\mathsf{T}] \pfun \mathsf{T}$

Identity elements are typically denoted by the symbol 0 when the operation is thought of as an addition or the symbol 1 when the operation is thought of as a multiplication.

5.2. **Monoids.** A *monoid* in t is a semigroup in t that has an identity element.

Monoid[t]
- *Semigroup*[t]
- *IdentityElement*[t]

Let $monoid[\mathsf{t}]$ be the set of all monoids in t.

$monoid[\mathsf{t}] == \{\, Monoid[\mathsf{t}] \bullet \mathbf{A} \,\}$

Remark. *Given a monoid we can recover its identity element by applying the identity_element function to it.*

$identity\_element[\mathsf{T}] \in monoid[\mathsf{T}] \fun \mathsf{T}$

5.3. **Homomorphisms.** Let $\mathbf{A}$ and $\mathbf{A}'$ be monoids and let f map the elements of A to the elements of A'. The map f is said to *preserve identity elements* if it maps the identity element of $\mathbf{A}$ to the identity element of $\mathbf{A}'$.

MapPreservesIdentity[t, u]
- *Magma_Map*[t, u]
- *Monoid*[t]
- *Monoid′*[u]

- $f(e) = e'$

A *monoid homomorphism* is a homomorphism of the underlying semigroups that preserves identity.

Monoid_Hom[t, u]
- *Semigroup_Hom*[t, u]
- *MapPreservesIdentity*[t, u]

Let $monoid\_Hom[\mathsf{t}, \mathsf{u}]$ be the set of all homomorphisms from monoids in t to monoids in u.

$monoid\_Hom[\mathsf{t}, \mathsf{u}] == \{\, Monoid\_Hom[\mathsf{t}, \mathsf{u}] \bullet F \,\}$

Let $monoid\_hom(\mathbf{A}, \mathbf{A}')$ denote the set of all monoid homomorphisms from $\mathbf{A}$ to $\mathbf{A}'$.

$$monoid\_hom[\mathsf{t}, \mathsf{u}] == (\lambda\, \mathbf{A} : monoid[\mathsf{t}]; \mathbf{A}' : monoid[\mathsf{u}] \bullet \{\, (\mathbf{A}, \mathbf{A}') \,\} \lhd monoid\_Hom[\mathsf{t}, \mathsf{u}])$$

Remark. *The identity mapping is a monoid homomorphism.*

Remark. *The composition of two monoid homomorphisms is another monoid homomorphism.*

6. Groups

6.1. **Inverse Operations.** Let $\mathbf{A}$ be a magma that has an identity element. A unary operation *inv* on A is said to be an *inverse operation* if it maps each element to an element whose product with it is the identity element.

InverseOperation[t]

$IdentityElement[\mathsf{t}]$

$inv : \mathsf{t} \pfun \mathsf{t}$

$inv \in A \longrightarrow A$

$\forall\, x : A \bullet x \cdot (inv\, x) = e = (inv\, x) \cdot x$

Let *inverse_operation* denote the relation between magmas and their inverse operations.

$$inverse\_operation[\mathsf{t}] == \{\, InverseOperation[\mathsf{t}] \bullet \mathbf{A} \mapsto inv \,\}$$

Remark. *If a monoid has an inverse operation then it is unique.*

InverseOperations[t]

$Monoid[\mathsf{t}]$

$inv, inv' : \mathsf{t} \pfun \mathsf{t}$

$(\mathbf{A}, inv) \in inverse\_operation[\mathsf{t}]$

$(\mathbf{A}, inv') \in inverse\_operation[\mathsf{t}]$

$\forall\, InverseOperations[\mathsf{T}] \bullet inv = inv'$

Proof. Suppose *inv* and inv' are inverse operations. Let x be any element.

$$\begin{aligned} & inv'\, x \\ &= (inv'\, x) \cdot e && [e \text{ is an identity element}] \\ &= (inv'\, x) \cdot (x \cdot (inv\, x)) && [inv\, x \text{ is an inverse of } x] \\ &= ((inv'\, x) \cdot x) \cdot (inv\, x) && [\text{associativity}] \end{aligned}$$

$= e \cdot (inv\ x)$ [$inv'\ x$ is an inverse of x]

$= inv\ x$ [e is an identity element]

□

Remark. *Since inverse operations are unique if exist they, the relation between monoids and inverse operations is a partial function.*

$inverse\_operation[\mathsf{T}] \in monoid[\mathsf{T}] \pfun \mathsf{T} \pfun \mathsf{T}$

6.2. **Groups.** A *group* is a monoid that has an inverse operation.

Group[t]
$Monoid[\mathsf{t}]$
$InverseOperation[\mathsf{t}]$

Let $group[\mathsf{t}]$ be the set of all groups in t.

$group[\mathsf{t}] == \{\ Group[\mathsf{t}] \bullet \mathbf{A}\ \}$

6.3. **Homomorphisms.** Let $\mathbf{A}$ and $\mathbf{A}'$ be groups and let F be a monoid homomorphism. The map f is said to *preserve inverses* if it maps the inverses to the inverses. A *group homomorphism* is a monoid homomorphism that preserves inverses.

Group_Hom[t, u]
$Monoid\_Hom[\mathsf{t}, \mathsf{u}]$
$Group[\mathsf{t}]$
$Group'[\mathsf{u}]$

$\forall x : A \bullet f(inv\ x) = inv'(f\ x)$

Let $group\_Hom[\mathsf{t}, \mathsf{u}]$ be the set of all group homomorphisms.

$group\_Hom[\mathsf{t}, \mathsf{u}] == \{\ Group\_Hom[\mathsf{t}, \mathsf{u}] \bullet F\ \}$

Let $group\_hom(\mathbf{A}, \mathbf{A}')$ denote the set of all group homomorphisms from $\mathbf{A}$ to $\mathbf{A}'$.

$group\_hom[\mathsf{t}, \mathsf{u}] ==$
$\quad (\lambda\, \mathbf{A} : group[\mathsf{t}];\ \mathbf{A}' : group[\mathsf{u}] \bullet$
$\quad\quad \{\ (\mathbf{A}, \mathbf{A}')\ \} \lhd group\_Hom[\mathsf{t}, \mathsf{u}])$

Example (Identity)**.** *The identity mapping is a group homomorphism.*

$\forall\, Magma\_Id[\mathsf{T}] \bullet F \in group\_hom(\mathbf{A}, \mathbf{A})$

6.4. **Composition.** Consider the composition of two group homomorphisms.

Group_Composition[t, u, v]
$Magma\_Composition[\mathsf{t}, \mathsf{u}, \mathsf{v}]$
$Group\_Hom[\mathsf{t}, \mathsf{u}]$
$Group\_Hom'[\mathsf{u}, \mathsf{v}]$

Remark. *The composition of two group homomorphisms is another group homomorphism.*

$\forall\, Group\_Composition[\mathsf{T}, \mathsf{U}, \mathsf{V}] \bullet G \in group\_Hom[\mathsf{T}, \mathsf{V}]$

6.5. **Bijections.** Let $bij[\mathsf{t}]$ denote the set of all bijections from t to itself.

$bij[\mathsf{t}] == \mathsf{t} \rightarrowtail\!\!\!\!\!\twoheadrightarrow \mathsf{t}$

Let $Bij[\mathsf{t}]$ be the structure whose carrier is $bij[\mathsf{t}]$ and whose product is composition.

$Bij[\mathsf{t}] == (bij[\mathsf{t}], (\lambda f, g : bij[\mathsf{t}] \bullet g \circ f))$

Remark. *The composition of bijections is a bijection.*

$\forall f, g : bij[\mathsf{T}] \bullet$
$\quad f \circ g \in bij[\mathsf{T}]$

Since bijections are closed under composition, $Bij[\mathsf{t}]$ *is a magma.*

$Bij[\mathsf{T}] \in magma[bij[\mathsf{T}]]$

Remark. *Composition is associative.*

$\forall f, g, h : bij[\mathsf{T}] \bullet$
$\quad f \circ (g \circ h) = (f \circ g) \circ h$

Since composition is associative, $Bij[\mathsf{t}]$ *is a semigroup.*

$Bij[\mathsf{T}] \in semigroup[bij[\mathsf{T}]]$

Remark. *The identity function* $\mathrm{id}\,\mathsf{t}$ *is an identity element for* $Bij[\mathsf{t}]$.

$\forall f : bij[\mathsf{T}] \bullet$
$\quad \mathrm{id}\,\mathsf{T} \circ f = f = f \circ \mathrm{id}\,\mathsf{T}$

Since $Bij[\mathsf{t}]$ *has an identity element, it is a monoid.*

$Bij[\mathsf{T}] \in monoid[bij[\mathsf{T}]]$

Remark. *The relational inverse* $f^\sim$ *of a bijection* f *is its inverse under composition.*

$\forall f : bij[\mathsf{T}] \bullet$
$\quad f \circ f^\sim = \mathrm{id}\,\mathsf{T} = f^\sim \circ f$

Since $Bij[\mathsf{t}]$ *has an inverse operation, it is a group.*

$Bij[\mathsf{T}] \in group[bij[\mathsf{T}]]$

6.6. **Subgroups.** A *subgroup* A of a group A' is a nonempty subset that is closed under the group product and inverse operation.

Subgroup[t]

$A : \mathbb{P}_1\, \mathsf{t}$

Group′[t]

$A \subseteq A'$

$\forall\, x, y : A \bullet x \cdot' y \in A$

$\forall\, x : A \bullet inv'(x) \in A$

- the subgroup is a subset of the group
- the subgroup is closed under products
- the subgroup is closed under inverses

Remark. *A subgroup contains the group identity element.*

$\forall\, Subgroup[\mathsf{T}] \bullet identity\_element(\mathbf{A}') \in A$

Proof. By definition, the subgroup A is nonempty. Let $x \in A$. Therefore $inv'(x) \in A$ since the subgroup is closed under inverses. Therefore $x \cdot' inv'(x) \in A$ since the subgroup is closed under product. But $x \cdot' inv'(x) = e$ the identity element of A'. Therefore $e \in A$. □

A subgroup inherits a group structure from its enclosing group.

Subgroup_Group[t]

Subgroup[t]

Magma[t]

$e : \mathsf{t}$

$inv : \mathsf{t} \pfun \mathsf{t}$

$(\_ \cdot \_) = (\lambda\, x, y : A \bullet x \cdot' y)$

$e = e'$

$inv = (\lambda\, x : A \bullet inv'(x))$

- the subgroup product is the restriction of the group product
- the subgroup identity element is the group identity element
- the subgroup inverse operation is the restriction of the group inverse operation

Remark. *A subgroup is a group.*

$\forall\, Subgroup\_Group[\mathsf{T}] \bullet Group[\mathsf{T}]$

There is a natural inclusion map from the subgroup to the group.

Subgroup_Inclusion[t]

Subgroup_Group[t]
Magma_Map[t, t]

$f = \mathrm{id}\ A$

- the map is the inclusion of the subgroup into the group

Remark. *The subgroup inclusion map is a group homomorphism.*

$\forall$ *Subgroup_Inclusion*[T] • *Group_Hom*[T, T]

7. Abelian Groups

7.1. **Commutativity.** A magma **A** in t is said to be *commutative* when the product of two elements doesn't depend on their order.

Commutative[t]

Magma[t]

$\forall x, y : A \bullet x \cdot y = y \cdot x$

7.2. **Abelian Groups.** An *abelian group* is a group in which the product is commutative.

AbelianGroup[t]

Group[t]
Commutative[t]

Let *abgroup*[t] denote the set of all abelian groups in t.

abgroup[t] == { *AbelianGroup*[t] • **A** }

Often in an abelian group the binary operation is denoted as addition $x + y$, the identity element as a zero 0, and the inverse operation as negation - x.

Example (Integer Addition)**.** *Addition over the integers is an abelian group.*

$(\mathbb{Z}, (\_ + \_)) \in$ *abgroup*[$\mathbb{Z}$]

7.3. **Homomorphisms.** A homomorphism of abelian groups is a homomorphism of the underlying groups.

AbelianGroup_Hom[t, u]

Group_Hom[t, u]
Group[t]
Group′[u]

Let *abgroup_Hom*[t, u] be the set of all abelian group homomorphisms from abelian groups in t to abelian groups in u.

abgroup_Hom[t, u] == { *AbelianGroup_Hom*[t, u] • F }

Let $abgroup\_hom(\mathbf{A}, \mathbf{A}')$ be the subset of abelian group homomorphisms from $\mathbf{A}$ to $\mathbf{A}'$.

$$abgroup\_hom[\mathsf{t}, \mathsf{u}] == \\ (\lambda\, \mathbf{A} : abgroup[\mathsf{t}]; \mathbf{A}' : abgroup[\mathsf{u}] \bullet \\ \{\, (\mathbf{A}, \mathbf{A}') \,\} \lhd abgroup\_Hom[\mathsf{t}, \mathsf{u}])$$

STOPPED HERE

References

[1] J. M. Spivey. *The Z Notation*. Second Edition. Prentice Hall International, 1992. URL: https://spivey.oriel.ox.ac.uk/wiki/files/zrm/zrm.pdf.

[2] Mike Spivey. *The fuzz Manual*. Second Edition. The Spivey Partnership, 2000. URL: https://github.com/Spivoxity/fuzz/blob/59313f201af2d536f5381e65741ee6d98db54a70/doc/fuzzman-pub.pdf.

Email address, Arthur Ryman: arthur.ryman@gmail.com