

# GROUPS

ARTHUR RYMAN

ABSTRACT. This article formalizes groups and related group-like algebraic structures using Z Notation and has been type checked by *f*UZZ.

## CONTENTS

1. Introduction	2
2. Group-like Algebraic Structures	2
2.1. Genericity	3
2.2. Partial Binary Operations	3
2.3. Total Binary Operations	3
2.4. Carriers	4
3. Magmas	4
3.1. Magmas	4
3.2. Maps and Homomorphisms	6
3.2.1. Maps	6
3.2.2. Homomorphisms	8
3.3. Identity Maps	10
3.4. Composition	10
3.5. Subsets and Submagmas	11
3.5.1. Subsets	11
3.5.2. Submagmas	12
3.6. Restriction	12
3.7. Inclusion	13
3.8. Images	13
3.9. Containment	14
3.10. Intersection	14
3.11. Generation	15

---

*Date:* March 6, 2025.

4. Semigroups	15
4.1. Semigroups	15
4.2. Homomorphisms	16
4.3. Composition	16
5. Monoids	17
5.1. Identity Elements	17
5.2. Monoids	18
5.3. Homomorphisms	18
6. Groups	19
6.1. Inverse Operations	19
6.2. Groups	20
6.3. Homomorphisms	20
6.4. Composition	20
6.5. Bijections	21
6.6. Subgroups	21
7. Abelian Groups	23
7.1. Commutativity	23
7.2. Abelian Groups	23
7.3. Homomorphisms	23
References	24

## 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 *fuzz*[2].

## 2. GROUP-LIKE ALGEBRAIC STRUCTURES

In general, an *algebraic structure* consists of one or more 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  $\mathbf{t}$ ,  $\mathbf{u}$ , and  $\mathbf{v}$  as generic parameters in definitions. We use symbols like  $\mathbf{T}$ ,  $\mathbf{U}$ , and  $\mathbf{V}$  as arbitrary sets in propositions.

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

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

$$PBINOP[\mathbf{t}] == \mathbf{t} \times \mathbf{t} \rightharpoonup \mathbf{t}$$

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

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

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

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

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

$$binop[\mathbf{t}] == \mathbf{t} \times \mathbf{t} \longrightarrow \mathbf{t}$$

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

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

**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.*

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

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

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

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

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

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

### 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  $\text{MAGMA}[\mathbf{t}]$  to be the type abbreviation for a magma structure.

$\text{MAGMA}[\mathbf{t}] == \mathbf{P} \mathbf{t} \times \text{PBINOP}[\mathbf{t}]$

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

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

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

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

$\begin{array}{l} \text{Magma}[\mathbf{t}] \text{ —————} \\ A : \mathbb{P} \mathbf{t} \\ \_ \cdot \_ : \text{PBINOP}[\mathbf{t}] \\ \mathbf{A} : \text{MAGMA}[\mathbf{t}] \\ \hline (\_ \cdot \_) \in \text{binop}[A] \\ \mathbf{A} = (A, (\_ \cdot \_)) \end{array}$
---

- 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.*

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

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

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

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

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

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

$$\text{magma}[\mathbf{T}] \subseteq \text{MAGMA}[\mathbf{T}]$$

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

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

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

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

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

$$\text{magma\_on}[\mathbf{t}] == (\lambda A : \mathbb{P} \mathbf{t} \bullet \{ A \} \triangleleft \text{magma}[\mathbf{t}])$$

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

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

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

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

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

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

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

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

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

$$\text{MAGMA\_MAP}[\mathbf{t}, \mathbf{u}] == (\text{MAGMA}[\mathbf{t}] \times \text{MAGMA}[\mathbf{u}]) \times (\mathbf{t} \rightarrow \mathbf{u})$$

**Example** (Identity Maps). *The identity map on the set of integers extends to a magma map structure from any magma on the integers to itself. Define these structures for integer addition, subtraction, and multiplication.*

$$\text{int\_add\_id} == (\text{int\_add}, \text{int\_add}) \mapsto \text{id } \mathbb{Z}$$

$$\text{int\_sub\_id} == (\text{int\_sub}, \text{int\_sub}) \mapsto \text{id } \mathbb{Z}$$

$$\text{int\_mul\_id} == (\text{int\_mul}, \text{int\_mul}) \mapsto \text{id } \mathbb{Z}$$

*These structures all have type  $\text{MAGMA\_MAP}[\mathbb{Z}, \mathbb{Z}]$ .*

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

$$\text{int\_sub\_id} \in \text{MAGMA\_MAP}[\mathbb{Z}, \mathbb{Z}]$$

$$\text{int\_mul\_id} \in \text{MAGMA\_MAP}[\mathbb{Z}, \mathbb{Z}]$$

TODO: This is too repetitive. It would be better to move the section on identity maps here and use it to construct identity map structures. Then prove that they are magma maps and homomorphisms. Alternatively, move the *MulConst* and *ExpConst* examples here and defer the discussion of identity maps. For example, define standalone integer partial and total functions, then use them to construct  $\text{MAGMA\_MAP}$  objects. One should fail to be a total function, hence not a map.

One should be a map but fail to be a homomorphism. One should be a homomorphism.

We further require the underlying map  $f$  of a magma map structure  $F$  from  $\mathbf{A}$  to  $\mathbf{A}'$  to be a function from  $A$  to  $A'$ .

$Magma\_Map[t, u]$	_____
$Magma[t]$ $Magma'[u]$ $f : t \rightarrow u$ $F : MAGMA\_MAP[t, u]$	
$f \in A \rightarrow A'$ $F = (\mathbf{A}, \mathbf{A}') \mapsto f$	

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

**Remark.** *The identity map on the carrier of a magma is a function from the carrier to itself.*

$$\forall Magma[T] \bullet \text{id } A \in A \rightarrow A$$

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

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

**Example.** *The previously defined identity map structures are magma maps.*

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

$$\text{int\_sub\_id} \in magma\_Map[\mathbb{Z}, \mathbb{Z}]$$

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

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

$$magma\_map[t, u] ==$$

$$(\lambda \mathbf{A} : magma[t]; \mathbf{A}' : magma[u] \bullet$$

$$\{(\mathbf{A}, \mathbf{A}')\} \triangleleft magma\_Map[t, u])$$

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

$$\forall \mathbf{A} : magma[T]; \mathbf{A}' : magma[U] \bullet$$

$$magma\_map(\mathbf{A}, \mathbf{A}') \subseteq magma\_Map[T, U]$$

**Example.** *The previously defined identity map structures are magma maps from each magma to itself.*

$$\text{int\_add\_id} \in magma\_map(\text{int\_add}, \text{int\_add})$$

$$\text{int\_sub\_id} \in magma\_map(\text{int\_sub}, \text{int\_sub})$$

$$\text{int\_mul\_id} \in magma\_map(\text{int\_mul}, \text{int\_mul})$$

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

**Remark.** *The identity map preserves products.*

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

Define  $magma\_Hom[t, u]$  to be the set of all magma homomorphisms from magmas in  $t$  to magmas in  $u$ .

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

**Example.** *The previously defined identity map structures are magma homomorphisms.*

$$int\_add\_id \in magma\_Hom[Z, Z]$$

$$int\_sub\_id \in magma\_Hom[Z, Z]$$

$$int\_mul\_id \in magma\_Hom[Z, Z]$$

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

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

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

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

**Example.** *The previously defined identity map structures are magma homomorphisms from each magma to itself.*

$$int\_add\_id \in magma\_hom(int\_add, int\_add)$$

$$int\_sub\_id \in magma\_hom(int\_sub, int\_sub)$$

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

**Example** (Multiplication by a Constant). *Consider multiplication by a given integer  $c$ .*



<i>MulConst</i>
<i>Magma_Map</i> [ $\mathbb{Z}, \mathbb{Z}$ ]
$c : \mathbb{Z}$
$\mathbf{A} = \mathbf{A}' = \text{int\_add}$
$f = (\lambda x : \mathbb{Z} \bullet c * x)$

Define  $\text{mul\_const}(c)$  to be the corresponding magma map.

$$\text{mul\_const} == \{ \text{MulConst} \bullet c \mapsto F \}$$

The magma map  $\text{mul\_const}(c)$  sends  $\mathbb{Z}$  to  $\mathbb{Z}$  and preserves addition. Therefore this map is a magma homomorphism.

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

*Proof.*

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

□

**Example** (Exponentiation by a Constant). Consider exponentiation by a given natural number  $n$ .

<i>ExpConst</i>
<i>Magma_Map</i> [ $\mathbb{Z}, \mathbb{Z}$ ]
$n : \mathbb{N}$
$\mathbf{A} = \mathbf{A}' = \text{int\_mul}$
$f = (\lambda x : \mathbb{Z} \bullet x ** n)$

Define  $\text{exp\_const}(n)$  to be the corresponding magma map.

$$\text{exp\_const} == \{ \text{ExpConst} \bullet n \mapsto F \}$$

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

$$\forall \text{ExpConst} \bullet \\ \text{exp\_const}(n) \in \text{magma\_hom}(\text{int\_mul}, \text{int\_mul})$$

*Proof.*

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

□

**3.3. Identity Maps.** Consider the identity map from the carrier of a magma to itself.

$\frac{\text{Magma\_Id}[t]}{\text{Magma\_Map}[t, t]}$	
$\mathbf{A} = \mathbf{A}'$	
$f = \text{id } A$	

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

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

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

**Remark.**

$$\text{magma\_id}[T] \in \text{MAGMA}[T] \rightarrow \text{MAGMA\_MAP}[T, T]$$

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

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

**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  $A''$ .

$\frac{\text{Magma\_Composition}[t, u, v]}{\text{Magma\_Map}[t, u]}$	
$\text{Magma\_Map}'[u, v]$	
$g : t \rightarrow v$	
$G : \text{magma\_Map}[t, v]$	
$g = f' \circ f$	
$G = (\mathbf{A}, \mathbf{A}'') \mapsto g$	

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

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

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

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

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

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

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

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

$$\begin{aligned} \forall \text{ Magma\_Composition}[\mathbf{T}, \mathbf{U}, \mathbf{V}] \mid \\ F \in \text{magma\_hom}(\mathbf{A}, \mathbf{A}') \wedge F' \in \text{magma\_hom}(\mathbf{A}', \mathbf{A}'') \bullet \\ G \in \text{magma\_hom}(\mathbf{A}, \mathbf{A}'') \end{aligned}$$

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

$$\text{MAGMA\_SUBSET}[\mathbf{t}] == \text{MAGMA}[\mathbf{t}] \times \mathbb{P} \mathbf{t}$$

$\text{Magma\_Subset}[\mathbf{t}]$	_____
$S : \mathbb{P} \mathbf{t}$	
$\text{Magma}[\mathbf{t}]$	
$\mathbf{S} : \text{MAGMA\_SUBSET}[\mathbf{t}]$	
$S \subseteq A$	
$\mathbf{S} = (\mathbf{A}, S)$	

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

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

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

$$\text{magma\_subset}[\mathbf{t}] == (\lambda \mathbf{A} : \text{magma}[\mathbf{t}] \bullet \{ \mathbf{A} \} \triangleleft \text{magma\_Subset}[\mathbf{t}])$$

**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.*

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

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

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

*They are therefore magma subsets of the corresponding magmas.*

$$\text{nat\_add} \in \text{magma\_subset}(\text{int\_add})$$

$$\text{nat\_sub} \in \text{magma\_subset}(\text{int\_sub})$$

$$\text{nat\_mul} \in \text{magma\_subset}(\text{int\_mul})$$

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

$\frac{\text{Magma\_Submagma}[\mathbf{t}] \quad \text{Magma\_Subset}[\mathbf{t}]}{\forall x, y : S \bullet x \cdot y \in S}$
--

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

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

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

$$\text{magma\_Submagma}[\mathbf{T}] \subseteq \text{magma\_Subset}[\mathbf{T}]$$

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

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

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

$$\text{nat\_add} \in \text{magma\_submagma}(\text{int\_add})$$

$$\text{nat\_mul} \in \text{magma\_submagma}(\text{int\_mul})$$

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

$$\text{nat\_sub} \notin \text{magma\_submagma}(\text{int\_sub})$$

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  $S'$ .

$\frac{\text{Magma\_Restriction}[\mathbf{t}] \quad \text{Magma}[\mathbf{t}] \quad \text{Magma\_Submagma}'[\mathbf{t}]}{A = S'}$
$\forall x, y : A \bullet x \cdot y = x \cdot' y$

Define  $\text{magma\_Restriction}[\mathbf{t}]$  to be the set of all restrictions of submagmas in  $\mathbf{t}$ .

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

**Remark.** Magma restriction maps submagmas to magmas.

$$\text{magma\_Restriction}[\mathbf{T}] \in \text{magma\_Submagma}[\mathbf{T}] \rightarrow \text{magma}[\mathbf{T}]$$

Define  $\text{magma\_restriction}(\mathbf{A})$  to be the set of all restrictions of submagmas of  $\mathbf{A}$

$$\text{magma\_restriction}[\mathbf{t}] == (\lambda \mathbf{A} : \text{magma}[\mathbf{t}] \bullet \text{magma\_submagma}(\mathbf{A}) \triangleleft \text{magma\_Restriction}[\mathbf{t}])$$

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

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

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

$\frac{\text{Magma\_Inclusion}[\mathbf{t}] \quad \text{Magma\_Restriction}[\mathbf{t}] \quad \text{Magma\_Map}[\mathbf{t}, \mathbf{t}]}{f = \text{id } A}$
--

Define *magma\_Inclusion* to be the set of all magma inclusions.

$$\text{magma\_Inclusion}[\mathbf{t}] == \{ \text{Magma\_Inclusion}[\mathbf{t}] \bullet F \}$$

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

$$\text{magma\_inclusion}[\mathbf{t}] == \\ (\lambda \mathbf{A}, \mathbf{A}' : \text{magma}[\mathbf{t}] \bullet \\ \{ (\mathbf{A}, \mathbf{A}') \} \triangleleft \text{magma\_Inclusion}[\mathbf{t}])$$

**Remark.** *Inclusion maps are magma homomorphisms.*

$$\forall \mathbf{A}, \mathbf{A}' : \text{magma}[\mathbf{T}] \bullet \\ \text{magma\_inclusion}(\mathbf{A}, \mathbf{A}') \subseteq \text{magma\_hom}(\mathbf{A}, \mathbf{A}')$$

**3.8. Images.** The *image* of a magma map  $f$  from  $A$  to  $A'$  is the subset  $S'$  of  $A'$  that consists of the image under the map of the elements in  $A$ .

$\frac{\text{Magma\_Image}[\mathbf{t}, \mathbf{u}] \quad \text{Magma\_Map}[\mathbf{t}, \mathbf{u}] \quad \text{Magma\_Subset}'[\mathbf{u}]}{S' = f(A)}$
---

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

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

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

$$\text{magma\_image}[\mathbf{t}, \mathbf{u}] == \\ (\lambda \mathbf{A} : \text{magma}[\mathbf{t}]; \mathbf{A}' : \text{magma}[\mathbf{u}] \bullet \\ \text{magma\_map}(\mathbf{A}, \mathbf{A}') \triangleleft \text{magma\_Image}[\mathbf{t}, \mathbf{u}])$$

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

$$\begin{aligned} \forall \mathbf{A} : \text{magma}[\mathbf{T}]; \mathbf{A}' : \text{magma}[\mathbf{U}] \bullet \\ \forall F : \text{magma\_hom}(\mathbf{A}, \mathbf{A}') \bullet \\ \text{magma\_image}(\mathbf{A}, \mathbf{A}') F \in \text{magma\_submagma}(\mathbf{A}') \end{aligned}$$

*Proof.* It suffices to show that the product of any two elements  $x', y'$  in the image  $S'$  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  $x' \cdot y' = f(x) \cdot f(y) = f(x \cdot y)$  which is clearly in the image of  $f$ .  $\square$

STOPPED HERE

Consider the restriction of the image of a magma homomorphism.

$$\begin{array}{l} \text{Magma\_Im}[\mathbf{t}, \mathbf{u}] \text{ -----} \\ \text{Magma\_Image}[\mathbf{t}, \mathbf{u}] \\ \text{Magma\_Hom}[\mathbf{t}, \mathbf{u}] \\ \text{Magma\_Restriction}'[\mathbf{u}] \end{array}$$

Define  $\text{magma\_im}$  to be the function that sends a magma homomorphism to the restriction of its image.

$$\text{magma\_im}[\mathbf{t}, \mathbf{u}] == \{ \text{Magma\_Im}[\mathbf{t}, \mathbf{u}] \bullet F \mapsto \mathbf{A}'' \}$$

### 3.9. Containment.

**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.

$$\begin{array}{l} \text{Magma\_Intersection}[\mathbf{t}] \text{ -----} \\ \text{Magma\_Subset}_1[\mathbf{t}] \\ \text{Magma\_Subset}_2[\mathbf{t}] \\ \text{Magma\_Subset}[\mathbf{t}] \\ \hline \mathbf{A}_1 = \mathbf{A}_2 = \mathbf{A} \\ S = S_1 \cap S_2 \end{array}$$

Intersection is therefore a partial binary operation on the set of subsets of magmas. Let  $\mathbf{S} = \mathbf{S}_1 \cap \mathbf{S}_2$  denote the intersection of magma subsets.

$$(\_ \cap \_)[\mathbf{t}] == \{ \text{Magma\_Intersection}[\mathbf{t}] \bullet (\mathbf{S}_1, \mathbf{S}_2) \mapsto \mathbf{S} \}$$

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

$$\begin{aligned} \forall \mathbf{A} : \text{magma}[\mathbf{T}] \bullet \\ \forall \mathbf{S}_1, \mathbf{S}_2 : \text{magma\_subset}(\mathbf{A}) \bullet \\ \mathbf{S}_1 \cap \mathbf{S}_2 \in \text{magma\_subset}(\mathbf{A}) \end{aligned}$$

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

$$\begin{aligned} \forall \mathbf{A} : \text{magma}[\mathbf{T}] \bullet \\ \forall \mathbf{S}_1, \mathbf{S}_2 : \text{magma\_submagma}(\mathbf{A}) \bullet \\ \mathbf{S}_1 \cap \mathbf{S}_2 \in \text{magma\_submagma}(\mathbf{A}) \end{aligned}$$

### 3.11. Generation.

## 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*.

$\text{Semigroup}[\mathbf{t}]$	_____
$\text{Magma}[\mathbf{t}]$	
$\forall x, y, z : A \bullet$	
$x \cdot y \cdot z = x \cdot (y \cdot z)$	

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

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

**Remark.** *Every semigroup is a magma.*

$$\text{semigroup}[\mathbf{T}] \subseteq \text{magma}[\mathbf{T}]$$

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

$\text{SequenceConcat}[\mathbf{t}]$	_____
$\text{Magma}[\text{seq } \mathbf{t}]$	
$X : \mathbb{P} \mathbf{t}$	
$A = \text{seq } X$	
$\forall x, y : A \bullet x \cdot y = x \frown y$	

Define  $\text{seq\_concat}(X)$  to be the set of all magmas that consists of finite sequences in some subset  $X$  of  $\mathbf{t}$  under concatenation.

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

$$\forall X : \mathbb{P} \mathbf{T} \bullet \text{seq\_concat}(X) \in \text{semigroup}[\text{seq } X]$$

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

$\frac{\text{Semigroup\_Hom}[\mathbf{t}, \mathbf{u}]}{\text{Magma\_Hom}[\mathbf{t}, \mathbf{u}]}$
$\mathbf{A} \in \text{semigroup}[\mathbf{t}]$
$\mathbf{A}' \in \text{semigroup}[\mathbf{u}]$

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

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

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

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

$$\begin{aligned} \text{semigroup\_hom}[\mathbf{t}, \mathbf{u}] == \\ (\lambda \mathbf{A} : \text{semigroup}[\mathbf{t}]; \mathbf{A}' : \text{semigroup}[\mathbf{u}] \bullet \\ \{ (\mathbf{A}, \mathbf{A}') \} \triangleleft \text{semigroup\_Hom}[\mathbf{t}, \mathbf{u}]) \end{aligned}$$

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

$$\begin{aligned} \forall \text{Magma\_Id}[\mathbf{T}] \bullet \\ \mathbf{A} \in \text{semigroup}[\mathbf{T}] \Rightarrow \\ \text{Semigroup\_Hom}[\mathbf{T}, \mathbf{T}] \end{aligned}$$

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

$$\begin{aligned} \forall \text{Magma\_Hom}[\mathbf{T}, \mathbf{U}] \bullet \\ \mathbf{A} \in \text{semigroup}[\mathbf{T}] \wedge \mathbf{A}' \in \text{semigroup}[\mathbf{U}] \Rightarrow \\ F \in \text{semigroup\_hom}(\mathbf{A}, \mathbf{A}') \end{aligned}$$

**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.

$$\begin{aligned} \forall \text{Magma\_Hom}[\mathbf{T}, \mathbf{U}] \bullet \\ \mathbf{A} \in \text{semigroup}[\mathbf{T}] \Rightarrow \text{magma\_im}(F) \in \text{semigroup}[\mathbf{U}] \end{aligned}$$

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

$\frac{\text{Semigroup\_Composition}[\mathbf{t}, \mathbf{u}, \mathbf{v}]}{\text{Magma\_Composition}[\mathbf{t}, \mathbf{u}, \mathbf{v}]}$
$\text{Semigroup}[\mathbf{t}]$
$\text{Semigroup}'[\mathbf{u}]$



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

$$\forall \text{Semigroup\_Composition}[\mathbf{T}, \mathbf{U}, \mathbf{V}] \bullet \\ G \in \text{semigroup\_hom}(\mathbf{A}, \mathbf{A}'')$$

## 5. MONOIDS

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

$\text{IdentityElement}[\mathbf{t}]$	_____
$\text{Magma}[\mathbf{t}]$	
$e : \mathbf{t}$	
$e \in A$	
$\forall x : A \bullet e \cdot x = x = x \cdot e$	

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.

$$\text{identity\_element}[\mathbf{t}] == \\ \{ \text{IdentityElement}[\mathbf{t}] \bullet \mathbf{A} \mapsto e \}$$

**Remark.**

$$\text{identity\_element}[\mathbf{T}] \in \text{magma}[\mathbf{T}] \leftrightarrow \mathbf{T}$$

Consider the case of a magma  $\mathbf{A}$  that has, possibly distinct, identity elements  $e, e'$ .

$\text{IdentityElements}[\mathbf{t}]$	_____
$\text{Magma}[\mathbf{t}]$	
$e, e' : \mathbf{t}$	
$\mathbf{A} \mapsto e \in \text{identity\_element}[\mathbf{t}]$	
$\mathbf{A} \mapsto e' \in \text{identity\_element}[\mathbf{t}]$	

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

$$\forall \text{IdentityElements}[\mathbf{T}] \bullet \\ e = e'$$

*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.*

$$\text{identity\_element}[\mathbf{T}] \in \text{magma}[\mathbf{T}] \leftrightarrow \mathbf{T}$$

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  $\mathbf{t}$  is a semigroup in  $\mathbf{t}$  that has an identity element.

$\begin{array}{l} \text{Monoid}[\mathbf{t}] \\ \text{Semigroup}[\mathbf{t}] \\ \text{IdentityElement}[\mathbf{t}] \end{array}$
--

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

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

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

$$\text{identity\_element}[\mathbf{T}] \in \text{monoid}[\mathbf{T}] \rightarrow \mathbf{T}$$

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

$\begin{array}{l} \text{MapPreservesIdentity}[\mathbf{t}, \mathbf{u}] \\ \text{Magma\_Map}[\mathbf{t}, \mathbf{u}] \\ \text{Monoid}[\mathbf{t}] \\ \text{Monoid}'[\mathbf{u}] \end{array}$
$f(e) = e'$

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

$\begin{array}{l} \text{Monoid\_Hom}[\mathbf{t}, \mathbf{u}] \\ \text{Semigroup\_Hom}[\mathbf{t}, \mathbf{u}] \\ \text{MapPreservesIdentity}[\mathbf{t}, \mathbf{u}] \end{array}$
---

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

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

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

$$\begin{aligned} \text{monoid\_hom}[\mathbf{t}, \mathbf{u}] = & \\ & (\lambda \mathbf{A} : \text{monoid}[\mathbf{t}]; \mathbf{A}' : \text{monoid}[\mathbf{u}] \bullet \\ & \{ (\mathbf{A}, \mathbf{A}') \} \triangleleft \text{monoid\_Hom}[\mathbf{t}, \mathbf{u}]) \end{aligned}$$

**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  $\text{inv}$  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.

$\frac{\text{InverseOperation}[\mathbf{t}] \quad \text{IdentityElement}[\mathbf{t}]}{\text{inv} : \mathbf{t} \rightarrow \mathbf{t}}$
$\text{inv} \in A \rightarrow A$
$\forall x : A \bullet x \cdot (\text{inv } x) = e = (\text{inv } x) \cdot x$

Let  $\text{inverse\_operation}$  denote the relation between magmas and their inverse operations.

$$\begin{aligned} \text{inverse\_operation}[\mathbf{t}] = & \\ & \{ \text{InverseOperation}[\mathbf{t}] \bullet \mathbf{A} \mapsto \text{inv} \} \end{aligned}$$

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

$\frac{\text{InverseOperations}[\mathbf{t}] \quad \text{Monoid}[\mathbf{t}]}{\text{inv}, \text{inv}' : \mathbf{t} \rightarrow \mathbf{t}}$
$(\mathbf{A}, \text{inv}) \in \text{inverse\_operation}[\mathbf{t}]$
$(\mathbf{A}, \text{inv}') \in \text{inverse\_operation}[\mathbf{t}]$

$$\forall \text{InverseOperations}[\mathbf{T}] \bullet \text{inv} = \text{inv}'$$

*Proof.* Suppose  $\text{inv}$  and  $\text{inv}'$  are inverse operations. Let  $x$  be any element.

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

□

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

$$\text{inverse\_operation}[\mathbf{T}] \in \text{monoid}[\mathbf{T}] \rightarrow \mathbf{T} \rightarrow \mathbf{T}$$

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

$\frac{\text{Group}[\mathbf{t}]}{\text{Monoid}[\mathbf{t}] \quad \text{InverseOperation}[\mathbf{t}]}$
--

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

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

**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.

$\frac{\text{Group\_Hom}[\mathbf{t}, \mathbf{u}]}{\text{Monoid\_Hom}[\mathbf{t}, \mathbf{u}] \quad \text{Group}[\mathbf{t}] \quad \text{Group}'[\mathbf{u}]}$
$\forall x : \mathbf{A} \bullet f(\text{inv } x) = \text{inv}'(f x)$

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

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

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

$$\begin{aligned} \text{group\_hom}[\mathbf{t}, \mathbf{u}] == \\ (\lambda \mathbf{A} : \text{group}[\mathbf{t}]; \mathbf{A}' : \text{group}[\mathbf{u}] \bullet \\ \{ (\mathbf{A}, \mathbf{A}') \} \triangleleft \text{group\_Hom}[\mathbf{t}, \mathbf{u}]) \end{aligned}$$

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

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

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

$\frac{\text{Group\_Composition}[\mathbf{t}, \mathbf{u}, \mathbf{v}]}{\text{Magma\_Composition}[\mathbf{t}, \mathbf{u}, \mathbf{v}] \quad \text{Group\_Hom}[\mathbf{t}, \mathbf{u}] \quad \text{Group\_Hom}'[\mathbf{u}, \mathbf{v}]}$
--

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

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

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

$$\text{bij}[\mathbf{t}] == \mathbf{t} \succ \gg \mathbf{t}$$

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

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

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

$$\begin{aligned} \forall f, g : \text{bij}[\mathbf{T}] \bullet \\ f \circ g \in \text{bij}[\mathbf{T}] \end{aligned}$$

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

$$\text{Bij}[\mathbf{T}] \in \text{magma}[\text{bij}[\mathbf{T}]]$$

**Remark.** *Composition is associative.*

$$\begin{aligned} \forall f, g, h : \text{bij}[\mathbf{T}] \bullet \\ f \circ (g \circ h) = (f \circ g) \circ h \end{aligned}$$

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

$$\text{Bij}[\mathbf{T}] \in \text{semigroup}[\text{bij}[\mathbf{T}]]$$

**Remark.** *The identity function  $\text{id } \mathbf{t}$  is an identity element for  $\text{Bij}[\mathbf{t}]$ .*

$$\begin{aligned} \forall f : \text{bij}[\mathbf{T}] \bullet \\ \text{id } \mathbf{T} \circ f = f = f \circ \text{id } \mathbf{T} \end{aligned}$$

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

$$\text{Bij}[\mathbf{T}] \in \text{monoid}[\text{bij}[\mathbf{T}]]$$

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

$$\begin{aligned} \forall f : \text{bij}[\mathbf{T}] \bullet \\ f \circ f^\sim = \text{id } \mathbf{T} = f^\sim \circ f \end{aligned}$$

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

$$\text{Bij}[\mathbf{T}] \in \text{group}[\text{bij}[\mathbf{T}]]$$

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

$\text{Subgroup}[\mathbf{t}]$
$A : \mathbb{P}_1 \mathbf{t}$ $\text{Group}'[\mathbf{t}]$
$A \subseteq A'$
$\forall x, y : A \bullet x \cdot' y \in A$
$\forall x : A \bullet \text{inv}'(x) \in A$

- 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.*

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

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

A subgroup inherits a group structure from its enclosing group.

$\frac{\text{Subgroup\_Group}[\mathbf{t}] \quad \text{Subgroup}[\mathbf{t}] \quad \text{Magma}[\mathbf{t}] \quad e : \mathbf{t} \quad \text{inv} : \mathbf{t} \leftrightarrow \mathbf{t}}{(\_ \cdot \_) = (\lambda x, y : A \bullet x \cdot' y) \quad e = e' \quad \text{inv} = (\lambda x : A \bullet \text{inv}'(x))}$
--

- 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.*

$$\forall \text{Subgroup\_Group}[\mathbf{T}] \bullet \text{Group}[\mathbf{T}]$$

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

$\frac{\text{Subgroup\_Inclusion}[\mathbf{t}] \quad \text{Subgroup\_Group}[\mathbf{t}] \quad \text{Magma\_Map}[\mathbf{t}, \mathbf{t}]}{f = \text{id } A}$
--

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

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

$$\forall \text{Subgroup\_Inclusion}[\mathbf{T}] \bullet \text{Group\_Hom}[\mathbf{T}, \mathbf{T}]$$

## 7. ABELIAN GROUPS

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

$Commutative[\mathbf{t}]$	_____
$Magma[\mathbf{t}]$	
$\forall x, y : A \bullet x \cdot y = y \cdot x$	

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

$AbelianGroup[\mathbf{t}]$	_____
$Group[\mathbf{t}]$	
$Commutative[\mathbf{t}]$	

Let  $abgroup[\mathbf{t}]$  denote the set of all abelian groups in  $\mathbf{t}$ .

$$abgroup[\mathbf{t}] == \{ AbelianGroup[\mathbf{t}] \bullet \mathbf{A} \}$$

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.

$AbelianGroup\_Hom[\mathbf{t}, \mathbf{u}]$	_____
$Group\_Hom[\mathbf{t}, \mathbf{u}]$	
$Group[\mathbf{t}]$	
$Group'[\mathbf{u}]$	

Let  $abgroup\_Hom[\mathbf{t}, \mathbf{u}]$  be the set of all abelian group homomorphisms from abelian groups in  $\mathbf{t}$  to abelian groups in  $\mathbf{u}$ .

$$abgroup\_Hom[\mathbf{t}, \mathbf{u}] == \{ AbelianGroup\_Hom[\mathbf{t}, \mathbf{u}] \bullet F \}$$

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

$$abgroup\_hom[\mathbf{t}, \mathbf{u}] ==$$

$$(\lambda \mathbf{A} : abgroup[\mathbf{t}]; \mathbf{A}' : abgroup[\mathbf{u}] \bullet$$

$$\{ (\mathbf{A}, \mathbf{A}') \} \triangleleft abgroup\_Hom[\mathbf{t}, \mathbf{u}])$$

## 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](mailto:arthur.ryman@gmail.com)