GROUPS

ARTHUR RYMAN

Abstract. This article formalizes groups and related group-like algebraic structures using Z Notation and has been type checked by fUZZ.

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 5
3.2.1. Maps 5
3.2.2. Homomorphisms 6
3.3. Identity Maps 8
3.4. Composition 8
3.5. Subsets and Submagmas 9
3.5.1. Subsets 9
3.5.2. Submagmas 10
3.6. Restriction 10
3.7. Inclusion 11
3.8. Images 11
3.9. Containment 11
3.10. Intersection 12
3.11. Generation 12

Date: February 28, 2025.

4. Semigroups 12
4.1. Semigroups 12
4.2. Homomorphisms 13
4.3. Composition 14
5. Monoids 14
5.1. Identity Elements 14
5.2. Monoids 15
5.3. Homomorphisms 16
6. Groups 16
6.1. Inverse Operations 16
6.2. Groups 17
6.3. Homomorphisms 17
6.4. Composition 18
6.5. Bijections 18
6.6. Subgroups 19
7. Abelian Groups 20
7.1. Commutativity 20
7.2. Abelian Groups 20
7.3. Homomorphisms 21
References 21

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.

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

Here I am using the convention of defining names consisting of all uppercase letters for sets that are declared as *type abbreviations* to the fUZZ 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 defined on every pair of elements.

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

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

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* $\mathbb{Z}$.

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

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

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

Example (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 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 structure while the second stands for its carrier.

However, a set of elements may have more than one structure in a given context. 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 distinguish 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, the structure $\mathbf{A}$ 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 $(A, (\_ \cdot \_))$.

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

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

$Magma[\mathsf{t}]$

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

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

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

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

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* $MAGMA[\mathsf{t}]$.

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

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 Addition)**.** *Define* int_add *to be the set of integers equipped with addition.*

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

Integer addition is a magma on $\mathbb{Z}$.

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

Example (Integer Subtraction)**.** *Define* int_sub *to be the set of integers equipped with subtraction.*

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

Integer subtraction is a magma on $\mathbb{Z}$.

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

Example (Integer Multiplication)**.** *Define* int_mul *to be the set of integers equipped with multiplication.*

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

Integer multiplication is a 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.

$$MAGMA\_MAP[\mathsf{t}, \mathsf{u}] == (MAGMA[\mathsf{t}] \times MAGMA[\mathsf{u}]) \times (\mathsf{t} \mathrel{+\!\!\!\rightarrow} \mathsf{u})$$

$$\begin{array}{|l}
\hline
\textit{Magma_Map}[\mathsf{t}, \mathsf{u}] \\
\textit{Magma}[\mathsf{t}] \\
\textit{Magma}'[\mathsf{u}] \\
f : \mathsf{t} \mathrel{+\!\!\!\rightarrow} \mathsf{u} \\
F : MAGMA_MAP[\mathsf{t}, \mathsf{u}] \\
\hline
f \in A \longrightarrow A' \\
F = (\mathbf{A}, \mathbf{A}') \mapsto f \\
\hline
\end{array}$$

- 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.

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

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 $magma\_Map[\mathsf{t}, \mathsf{u}]$.*

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

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

$$\begin{array}{|l}
\hline
\textit{Magma_Hom}[\mathsf{t}, \mathsf{u}] \\
\textit{Magma_Map}[\mathsf{t}, \mathsf{u}] \\
\hline
\forall\, x, y : A \bullet f(x \cdot y) = f(x) \cdot' f(y) \\
\hline
\end{array}$$

- f preserves the product operation

Define $magma\_Hom[\mathsf{t}, \mathsf{u}]$ 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 $\mathbf{A}'$.

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

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

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

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

$$
\begin{array}{|l}
\multicolumn{1}{l}{\textit{MulConst}} \\
\hline
Magma\_Map[\mathbb{Z}, \mathbb{Z}] \\
c : \mathbb{Z} \\
\hline
\mathbf{A} = \mathbf{A}' = int\_add \\
f = (\lambda x : \mathbb{Z} \bullet c * x) \\
\hline
\end{array}
$$

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

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

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

$$
\begin{array}{l}
\forall c : \mathbb{Z} \bullet \\
\quad mul\_const(c) \in magma\_hom(int\_add, int\_add)
\end{array}
$$

Proof.

$$
\begin{array}{l}
\forall c, x, y : \mathbb{Z} \bullet \\
\quad c * (x + y) = c * x + c * y
\end{array}
$$

$\square$

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

$$
\begin{array}{|l}
\multicolumn{1}{l}{\textit{ExpConst}} \\
\hline
Magma\_Map[\mathbb{Z}, \mathbb{Z}] \\
n : \mathbb{N} \\
\hline
\mathbf{A} = \mathbf{A}' = int\_mul \\
f = (\lambda x : \mathbb{Z} \bullet x ** n) \\
\hline
\end{array}
$$

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

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

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

$$
\begin{array}{l}
\forall ExpConst \bullet \\
\quad exp\_const(n) \in magma\_hom(int\_mul, int\_mul)
\end{array}
$$

Proof.

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

□

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

$$\begin{array}{|l} \hline \textit{Magma\_Id}[\mathsf{t}] \\ \textit{Magma\_Map}[\mathsf{t}, \mathsf{t}] \\ \hline \mathbf{A} = \mathbf{A}' \\ f = \mathrm{id}\, A \\ \hline \end{array}$$

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

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

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

Remark.

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

Remark. *The identity map is a homomorphism.*

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

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''.

$$\begin{array}{|l} \hline \textit{Magma\_Composition}[\mathsf{t}, \mathsf{u}, \mathsf{v}] \\ \textit{Magma\_Map}[\mathsf{t}, \mathsf{u}] \\ \textit{Magma\_Map}'[\mathsf{u}, \mathsf{v}] \\ g : \mathsf{t} \nrightarrow \mathsf{v} \\ G : \textit{magma\_Map}[\mathsf{t}, \mathsf{v}] \\ \hline g = f' \circ f \\ G = (\mathbf{A}, \mathbf{A}'') \mapsto g \\ \hline \end{array}$$

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

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

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

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

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

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

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.*

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

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

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

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

$S \subseteq A$

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

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

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

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

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

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.

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

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

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

They are therefore magma subsets of the corresponding magmas.

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

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

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

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

$$\begin{array}{|l}
\textit{Magma_Submagma}[\mathsf{t}] \\
\hline
\textit{Magma_Subset}[\mathsf{t}] \\
\hline
\forall x, y : S \bullet x \cdot y \in S \\
\hline
\end{array}$$

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.*

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

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

However, natural numbers are not closed under subtraction and so are not a submagma in this case.

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

3.6. **Restriction.** A submagma S of $\mathbf{A}$ defines a magma $\mathbf{A}'$ by restricting the product to S.

$$\begin{array}{|l}
\textit{Magma_Restriction}[\mathsf{t}] \\
\hline
\textit{Magma_Submagma}[\mathsf{t}] \\
\textit{Magma}'[\mathsf{t}] \\
\hline
A' = S \\
\forall x, y : A' \bullet x \cdot' y = x \cdot y \\
\hline
\end{array}$$

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

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

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.*

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

3.7. **Inclusion.** There is a natural magma homomorphism from the restriction of a submagma to its enclosing magma.

$\mathit{Magma\_Inclusion}[\mathsf{t}]$

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

3.8. **Images.** The *image* of a magma map is the subset of the target magma that consists of the image under the map of the elements in the source magma.

$\mathit{Magma\_Image}[\mathsf{t}, \mathsf{u}]$

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

$S' = f(\!| A |\!)$

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

$$\forall\, \mathit{Magma\_Image}[\mathsf{T}, \mathsf{U}] \mid$$
$$\quad \mathit{Magma\_Hom}[\mathsf{T}, \mathsf{U}] \bullet$$
$$\qquad \mathit{Magma\_Submagma}'[\mathsf{U}]$$

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. $\square$

Define *magma_image* to be the function that sends a magma map to its image.

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

Consider the restriction of the image of a magma homomorphism.

$\mathit{Magma\_Im}[\mathsf{t}, \mathsf{u}]$

$\mathit{Magma\_Image}[\mathsf{t}, \mathsf{u}]$
$\mathit{Magma\_Hom}[\mathsf{t}, \mathsf{u}]$
$\mathit{Magma\_Restriction}'[\mathsf{u}]$

Define *magma_im* to be the function that sends a magma homomorphism to the restriction of its image.

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

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.

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

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.

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

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

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

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

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

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*.

$$
\begin{array}{|l}
\hline
\textit{Semigroup}[\mathsf{t}] \\
\textit{Magma}[\mathsf{t}] \\
\hline
\forall x, y, z : A \bullet \\
\quad x \cdot y \cdot z = x \cdot (y \cdot z) \\
\hline
\end{array}
$$

Let *semigroup*[t] denote the set of all semigroups in t.

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

Remark. *Every semigroup is a magma.*

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

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.*

$$
\begin{array}{|l}
\multicolumn{1}{l}{\mathit{SequenceConcat}[\mathsf{t}]} \\
\mathit{Magma}[\operatorname{seq} \mathsf{t}] \\
X : \mathbb{P}\, \mathsf{t} \\
\hline
A = \operatorname{seq} X \\
\forall x, y : A \bullet x \cdot y = x \frown y \\
\hline
\end{array}
$$

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

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

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

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

$$
\begin{array}{|l}
\multicolumn{1}{l}{\mathit{Semigroup\_Hom}[\mathsf{t}, \mathsf{u}]} \\
\mathit{Magma\_Hom}[\mathsf{t}, \mathsf{u}] \\
\hline
\mathbf{A} \in \mathit{semigroup}[\mathsf{t}] \\
\mathbf{A}' \in \mathit{semigroup}[\mathsf{u}] \\
\hline
\end{array}
$$

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

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

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

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

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

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

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

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

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

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.*

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

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

$$\begin{array}{|l}
\hline
\textit{Semigroup_Composition}[\mathsf{t},\mathsf{u},\mathsf{v}] \\
\textit{Magma_Composition}[\mathsf{t},\mathsf{u},\mathsf{v}] \\
\textit{Semigroup}[\mathsf{t}] \\
\textit{Semigroup}'[\mathsf{u}] \\
\hline
\end{array}$$

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

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

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.

$$\begin{array}{|l}
\hline
\textit{IdentityElement}[\mathsf{t}] \\
\textit{Magma}[\mathsf{t}] \\
e : \mathsf{t} \\
\hline
e \in A \\
\forall\, x : A \bullet e \cdot x = x = x \cdot e \\
\hline
\end{array}$$

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.

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

Remark.

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

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

$$
\begin{array}{|l}
\textit{IdentityElements}[\mathsf{t}] \\
\hline
\textit{Magma}[\mathsf{t}] \\
e, e' : \mathsf{t} \\
\hline
\mathbf{A} \mapsto e \in \textit{identity\_element}[\mathsf{t}] \\
\mathbf{A} \mapsto e' \in \textit{identity\_element}[\mathsf{t}] \\
\hline
\end{array}
$$

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

$$
\begin{array}{l}
\forall\ \textit{IdentityElements}[\mathsf{T}] \bullet \\
\quad e = e'
\end{array}
$$

Proof.

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

$\square$

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.*

$$\textit{identity\_element}[\mathsf{T}] \in \textit{magma}[\mathsf{T}] \rightarrow\!\!\!\!\!\!+ \ \mathsf{T}$$

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.

$$
\begin{array}{|l}
\textit{Monoid}[\mathsf{t}] \\
\hline
\textit{Semigroup}[\mathsf{t}] \\
\textit{IdentityElement}[\mathsf{t}] \\
\hline
\end{array}
$$

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

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

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

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

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 $\mathbf{A}'$.

$$
\begin{array}{|l}
\hline
\textit{MapPreservesIdentity}[\mathsf{t}, \mathsf{u}] \\
\hline
\textit{Magma\_Map}[\mathsf{t}, \mathsf{u}] \\
\textit{Monoid}[\mathsf{t}] \\
\textit{Monoid}'[\mathsf{u}] \\
\hline
f(e) = e' \\
\hline
\end{array}
$$

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

$$
\begin{array}{|l}
\hline
\textit{Monoid\_Hom}[\mathsf{t}, \mathsf{u}] \\
\hline
\textit{Semigroup\_Hom}[\mathsf{t}, \mathsf{u}] \\
\textit{MapPreservesIdentity}[\mathsf{t}, \mathsf{u}] \\
\hline
\end{array}
$$

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

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

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

$$
\begin{aligned}
&\textit{monoid\_hom}[\mathsf{t}, \mathsf{u}] == \\
&\quad (\lambda\, \mathbf{A} : \textit{monoid}[\mathsf{t}];\ \mathbf{A}' : \textit{monoid}[\mathsf{u}] \bullet \\
&\qquad \{ (\mathbf{A}, \mathbf{A}') \} \lhd \textit{monoid\_Hom}[\mathsf{t}, \mathsf{u}])
\end{aligned}
$$

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 *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.

$$
\begin{array}{|l}
\hline
\textit{InverseOperation}[\mathsf{t}] \\
\hline
\textit{IdentityElement}[\mathsf{t}] \\
\textit{inv} : \mathsf{t} \mathrel{+\!\!\!\!\rightarrow} \mathsf{t} \\
\hline
\textit{inv} \in A \longrightarrow A \\
\forall\, x : A \bullet x \cdot (\textit{inv}\ x) = e = (\textit{inv}\ x) \cdot x \\
\hline
\end{array}
$$

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

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

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

$$\begin{array}{|l}
\hline
\textit{InverseOperations}[\mathsf{t}] \\
\textit{Monoid}[\mathsf{t}] \\
\textit{inv}, \textit{inv}' : \mathsf{t} \rightarrow\!\!\!\!\!+ \mathsf{t} \\
\hline
(\mathbf{A}, \textit{inv}) \in \textit{inverse_operation}[\mathsf{t}] \\
(\mathbf{A}, \textit{inv}') \in \textit{inverse_operation}[\mathsf{t}] \\
\hline
\end{array}$$

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

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

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

□

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

$\textit{inverse\_operation}[\mathsf{T}] \in \textit{monoid}[\mathsf{T}] \rightarrow\!\!\!\!\!+ \mathsf{T} \rightarrow\!\!\!\!\!+ \mathsf{T}$

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

$$\begin{array}{|l}
\hline
\textit{Group}[\mathsf{t}] \\
\textit{Monoid}[\mathsf{t}] \\
\textit{InverseOperation}[\mathsf{t}] \\
\hline
\end{array}$$

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

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

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.

$$\begin{array}{|l}
\hline
\textit{Group_Hom}[\mathsf{t}, \mathsf{u}] \\
\textit{Monoid_Hom}[\mathsf{t}, \mathsf{u}] \\
\textit{Group}[\mathsf{t}] \\
\textit{Group}'[\mathsf{u}] \\
\hline
\forall\, x : A \bullet f(\textit{inv}\, x) = \textit{inv}'(f\, x) \\
\hline
\end{array}$$

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

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

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

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

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.

$$
\begin{array}{|l}
\hline
Group\_Composition[\mathsf{t}, \mathsf{u}, \mathsf{v}] \\
Magma\_Composition[\mathsf{t}, \mathsf{u}, \mathsf{v}] \\
Group\_Hom[\mathsf{t}, \mathsf{u}] \\
Group\_Hom'[\mathsf{u}, \mathsf{v}] \\
\hline
\end{array}
$$

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.*

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

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

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

Remark. *Composition is associative.*

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

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 $Bij[\mathsf{t}]$.*

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

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.

$$
\begin{array}{|l}
\hline
\textit{Subgroup}[\mathsf{t}] \\
A : \mathbb{P}_1\,\mathsf{t} \\
\textit{Group}'[\mathsf{t}] \\
\hline
A \subseteq A' \\
\forall x, y : A \bullet x \cdot' y \in A \\
\forall x : A \bullet inv'(x) \in A \\
\hline
\end{array}
$$

- 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.

$$
\begin{array}{|l}
\hline
\textit{Subgroup\_Group}[\mathsf{t}] \\
\textit{Subgroup}[\mathsf{t}] \\
\textit{Magma}[\mathsf{t}] \\
e : \mathsf{t} \\
inv : \mathsf{t} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathsf{t} \\
\hline
(\_ \cdot \_) = (\lambda\, x, y : A \bullet x \cdot' y) \\
e = e' \\
inv = (\lambda\, x : A \bullet inv'(x)) \\
\hline
\end{array}
$$

- 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.*

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

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

$$
\begin{array}{|l}
\hline
\mathit{Subgroup\_Inclusion}[\mathsf{t}] \\
\mathit{Subgroup\_Group}[\mathsf{t}] \\
\mathit{Magma\_Map}[\mathsf{t}, \mathsf{t}] \\
\hline
f = \mathrm{id}\, A \\
\hline
\end{array}
$$

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

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

$\forall\, \mathit{Subgroup\_Inclusion}[\mathsf{T}] \bullet \mathit{Group\_Hom}[\mathsf{T}, \mathsf{T}]$

7. Abelian Groups

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

$$
\begin{array}{|l}
\hline
\mathit{Commutative}[\mathsf{t}] \\
\mathit{Magma}[\mathsf{t}] \\
\hline
\forall\, x, y : A \bullet x \cdot y = y \cdot x \\
\hline
\end{array}
$$

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

$$
\begin{array}{|l}
\hline
\mathit{AbelianGroup}[\mathsf{t}] \\
\mathit{Group}[\mathsf{t}] \\
\mathit{Commutative}[\mathsf{t}] \\
\hline
\end{array}
$$

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

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

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 $\text{-}\, x$.

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

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

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

$$\begin{array}{|l}
\hline
\textit{AbelianGroup_Hom}[\mathsf{t}, \mathsf{u}] \\
\textit{Group_Hom}[\mathsf{t}, \mathsf{u}] \\
\textit{Group}[\mathsf{t}] \\
\textit{Group}'[\mathsf{u}] \\
\hline
\end{array}$$

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

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

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

$$\begin{aligned}
&abgroup_hom[\mathsf{t}, \mathsf{u}] == \\
&\quad (\lambda \, \mathbf{A} : abgroup[\mathsf{t}]; \mathbf{A}' : abgroup[\mathsf{u}] \bullet \\
&\qquad \{ \, (\mathbf{A}, \mathbf{A}') \, \} \lhd abgroup_Hom[\mathsf{t}, \mathsf{u}])
\end{aligned}$$

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`