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

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

A general *algebraic structure* consists of a set equipped with one or more operations. 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 the properties imposed on their product operations.

The underlying set of an algebraic structure is sometimes referred to as its *carrier*. It is unnecessary to distinguish between a structure and its carrier when the intended meaning is clear from context. For example, in the statement: "Let G be a group

Date: January 26, 2025.

and let g be an element of G." 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 addition and multiplication. 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 practice of defining structures as *tuples* consisting of a carrier together with one or more additional features.

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 t be a set and let A be a subset of it. We say that a structure with carrier A is a *structure in* t. If $A = \mathsf{t}$ we say that the structure is a *structure on* t or a *structure over* t. Note that a structure on or over t is also a structure in t.

3. Binary Operations

A *partial binary operation* on a set t maps some subset of pairs of elements to other elements.

$$PBinOp[\mathsf{t}] == \mathsf{t} \times \mathsf{t} \mathrel{+\!\!\!\rightarrow} \mathsf{t}$$

Example. *Integer division and modulus are partial binary operations on $\mathbb{Z}$ since division by 0 is undefined.*

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

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

A *total binary operation*, or simply a *binary operation*, is a partial binary operation defined on every pair of elements.

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

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

$$BinOp[\mathsf{T}] \subseteq PBinOp[\mathsf{T}]$$

Example. *Integer addition, subtraction, and multiplication are binary operations on $\mathbb{Z}$.*

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

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

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

4. 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 $(A, (\_ \cdot \_))$.

$$
\begin{array}{|l}
\hline
\textit{Magma}[\mathsf{t}] \\
A : \mathbb{P}\,\mathsf{t} \\
\_ \cdot \_ : \textit{PBinOp}[\mathsf{t}] \\
\mathbf{A} : \mathbb{P}\,\mathsf{t} \times \textit{PBinOp}[\mathsf{t}] \\
\hline
(\_ \cdot \_) \in \textit{BinOp}[A] \\
\mathbf{A} = (A, (\_ \cdot \_)) \\
\hline
\end{array}
$$

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

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

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

4.1. **Integer Addition.** Let *int_add* be the set of integers equipped with addition.

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

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

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

4.2. **Integer Subtraction.** Let *int_sub* be the set of integers equipped with subtraction.

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

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

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

4.3. **Integer Multiplication.** Let *int_mul* be the set of integers equipped with multiplication.

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

Example. *Integer multiplication is a magma on* $\mathbb{Z}$.

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

4.4. **Magma Homomorphisms.** Let A and A' be a magmas and let f be a map from A to A'. We refer to A as the *domain* and A' as the *codomain* of the map. Alternatively, we refer to A as the *source* and A' as the *target* of the map.

Just as magmas are structures, so also are magma maps. A *magma map* is a pair of magmas $(\mathbf{A}, \mathbf{A}')$ and a map f between their carriers.

Recall that we may informally use the same name, say A, to refer to both a magma and its carrier. Similarly, we may 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 map 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. In any case, the formal text must always use distinct names in any given context.

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

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

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

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

A magma map f is a *magma homomorphism* if it 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

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

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

Let $\textit{magma\_hom}(\mathbf{A}, \mathbf{A}')$ be the subset of $\textit{magma\_Hom}[\mathsf{t},\mathsf{u}]$ that consists of all homomorphisms from $\mathbf{A}$ to $\mathbf{A}'$.

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

Remark. *$\textit{magma\_hom}(\mathbf{A}, \mathbf{A}')$ is a subset of $\textit{magma\_Hom}$.*

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

4.4.1. *The Identity Map.*

Example. *The identity map is a homomorphism.*

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

$$\forall\, \textit{Magma\_Id}[\mathsf{T}] \bullet \\ \quad \textit{Magma\_Hom}[\mathsf{T},\mathsf{T}]$$

4.4.2. *Multiplication by a Fixed Integer.*

Example. *Multiplication by a fixed integer c maps $\mathbb{Z}$ to $\mathbb{Z}$ and preserves addition.*

$$\begin{array}{|l}
\hline \textit{MulConst} \\
\textit{Magma_Map}[\mathbb{Z},\mathbb{Z}] \\
c : \mathbb{Z} \\
\hline
\mathbf{A} = \mathbf{A}' = \textit{int_add} \\
f = (\lambda\, x : \mathbb{Z} \bullet c * x) \\
\hline
\end{array}$$

Therefore

$$\forall\, \textit{MulConst} \bullet \\ \quad \textit{Magma\_Hom}[\mathbb{Z},\mathbb{Z}]$$

Proof.

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

□

4.4.3. *Exponentiation by a Fixed Natural Number.*

Example. *Exponentiation by a fixed natural number n maps $\mathbb{Z}$ to $\mathbb{Z}$ and preserves multiplication.*

$$\begin{array}{|l}
\hline \textit{ExpConst} \\
\textit{Magma_Map}[\mathbb{Z},\mathbb{Z}] \\
n : \mathbb{N} \\
\hline
\mathbf{A} = \mathbf{A}' = \textit{int_mul} \\
f = (\lambda\, x : \mathbb{Z} \bullet x ** n) \\
\hline
\end{array}$$

Therefore

$$\forall\, \textit{ExpConst} \bullet \\ \quad \textit{Magma\_Hom}[\mathbb{Z},\mathbb{Z}]$$

Proof.

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

□

4.5. **Subset.** Given a subset S of the elements of a magma A we can restrict the product $x \cdot y$ to pairs in S. Let $x \centerdot y$ denote the restriction of the product to S. We get a new structure $\mathbf{S} = (S, (\_ \centerdot \_))$ which may or may not itself be a magma.

$$\begin{array}{|l}
\hline \textit{Magma_Subset}[\mathsf{t}] \\
\textit{Magma}[\mathsf{t}] \\
S : \mathbb{P}\,\mathsf{t} \\
_ \centerdot _ : \textit{PBinOp}[\mathsf{t}] \\
\mathbf{S} : \mathbb{P}\,\mathsf{t} \times \textit{PBinOp}[\mathsf{t}] \\
\hline
S \subseteq A \\
(_ \centerdot _) = (S \times S) \lhd (_ \cdot _) \\
\mathbf{S} = (S, (_ \centerdot _)) \\
\hline
\end{array}$$

4.6. **Submagma.** A subset S of a magma is a *submagma* if the product of any pair of elements of S is an element of S.

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

4.7. **Image.** The *image* of a magma homomorphism consists of the image of the map and the product restricted to those elements.

$$\begin{array}{|l}
\hline \textit{Magma_Image}[\mathsf{t}, \mathsf{u}] \\
\textit{Magma_Hom}[\mathsf{t}, \mathsf{u}] \\
\textit{Magma_Subset}'[\mathsf{u}] \\
\hline
S' = f\,(\!| A |\!) \\
\hline
\end{array}$$

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

$$\forall\, \textit{Magma\_Image}[\mathsf{T}, \mathsf{U}] \bullet \textit{Submagma}'[\mathsf{U}]$$

4.8. **Composition.** Let f be a homomorphism from A to A' and let f' be a homomorphism from A' to A''. The function composition $g = f' \circ f$ is a map from A to A''.

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

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

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

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

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

5. 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*.

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

Let $\textit{semigroup}[\mathsf{t}]$ 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.*

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

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

$$\begin{array}{|l}
\hline
\textit{Semigroup_Hom}[\mathsf{t},\mathsf{u}] \\
\textit{Magma_Hom}[\mathsf{t},\mathsf{u}] \\
\hline
\mathbf{A} \in \textit{semigroup}[\mathsf{t}] \\
\mathbf{A}' \in \textit{semigroup}[\mathsf{u}] \\
\hline
\end{array}$$

- $\mathbf{A}$ 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. *Every magma homomorphism of semigroups is a semigroup homomorphism.*

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

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

TODO: Define the image of a magma homomorphism.

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

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

Consider the composition of semigroup homomorphisms.

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

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

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

6. Monoids

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.

$$
\begin{array}{|l}
\hline
\multicolumn{1}{l}{\mathit{IdentityElement}[\mathsf{t}]} \\
\mathit{Magma}[\mathsf{t}] \\
e : \mathsf{t} \\
\hline
e \in A \\
\forall\, x : A \bullet e \cdot x = x = x \cdot e \\
\hline
\end{array}
$$

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 identity elements.

$$
\begin{aligned}
&\mathit{identity\_element}[\mathsf{t}] == \\
&\quad \{\, \mathit{IdentityElement}[\mathsf{t}] \bullet \mathbf{A} \mapsto e \,\}
\end{aligned}
$$

Remark.

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

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

$$
\begin{array}{|l}
\hline
\multicolumn{1}{l}{\mathit{IdentityElements}[\mathsf{t}]} \\
\mathit{Magma}[\mathsf{t}] \\
e, e' : \mathsf{t} \\
\hline
\mathbf{A} \mapsto e \in \mathit{identity\_element}[\mathsf{t}] \\
\mathbf{A} \mapsto e' \in \mathit{identity\_element}[\mathsf{t}] \\
\hline
\end{array}
$$

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

$$
\begin{aligned}
&\forall\, \mathit{IdentityElements}[\mathsf{T}] \bullet \\
&\quad e = e'
\end{aligned}
$$

Proof.

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

□

Remark. *If an identity element exists then it is unique. Therefore the relation from magmas to identity elements is a partial function.*

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

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

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

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

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

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

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

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

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 the identity element* if it maps the identity element of A to the identity element of B.

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

A *monoid homomorphism* from $\mathbf{A}$ to $\mathbf{A}'$ is a homomorphism f of the underlying semigroups that preserves identity.

$$\begin{array}{|l}
\hline
\textit{Monoid_Hom}[\mathsf{t}, \mathsf{u}] \\
\textit{Semigroup_Hom}[\mathsf{t}, \mathsf{u}] \\
\textit{MapPreservesIdentity}[\mathsf{t}, \mathsf{u}] \\
\hline
\end{array}$$

Let *monoid_Hom*[t, u] be the set of all homomorphisms from monoids in $\mathtt{t}$ to monoids in $\mathtt{u}$.

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

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

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

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

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

7. Groups

Let $\mathbf{A}$ be a magma in t 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.

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

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

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

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

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.*

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

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 t be a set of elements. Let *group*[t] be the set of all groups in t.

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

Let t and u be sets of elements, let $\mathbf{A}$ and $\mathbf{A}'$ be groups in t and u, and let f map t to u. The map f is said to *preserve the inverses* if it maps the inverses of elements of A to the inverses of the corresponding elements of A'.

$$\begin{array}{|l}
\hline
\multicolumn{1}{l}{\mathit{MapPreservesInverse}[\mathsf{t}, \mathsf{u}]} \\
\mathit{Group}[\mathsf{t}] \\
\mathit{Group}'[\mathsf{u}] \\
\mathit{Magma_Map}[\mathsf{t}, \mathsf{u}] \\
\hline
\forall x : A \bullet f(\mathit{inv}\ x) = \mathit{inv}'(f\ x) \\
\hline
\end{array}$$

Let $\mathbf{A}$ and $\mathbf{A}'$ be groups. A *group homomorphism* from $\mathbf{A}$ to $\mathbf{A}'$ is a monoid homomorphism from $\mathbf{A}$ to $\mathbf{A}'$ that preserves inverses.

$$\begin{array}{|l}
\hline
\multicolumn{1}{l}{\mathit{Group_Hom}[\mathsf{t}, \mathsf{u}]} \\
\mathit{Monoid_Hom}[\mathsf{t}, \mathsf{u}] \\
\mathit{MapPreservesInverse}[\mathsf{t}, \mathsf{u}] \\
\hline
\end{array}$$

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

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

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

$$\begin{array}{l}
\mathit{group_hom}[\mathsf{t}, \mathsf{u}] == \\
\quad (\lambda\, \mathbf{A} : \mathit{group}[\mathsf{t}]; \mathbf{A}' : \mathit{group}[\mathsf{u}] \bullet \\
\quad\quad \{\ (\mathbf{A}, \mathbf{A}')\ \} \lhd \mathit{group_Hom}[\mathsf{t}, \mathsf{u}])
\end{array}$$

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

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

7.1. **Bijections.** Let t be a set and let $\mathit{bij}[\mathsf{t}]$ denote the set of all bijections $\mathsf{t} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathsf{t}$ from t to itself.

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

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

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

Remark. *Composition is associative.*

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

Remark. *The identity function* $\mathrm{id}\,\mathsf{T}$ *acts as a left and right identity element under composition.*

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

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

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

The preceding remarks show that set $bij[\mathsf{t}]$ under the operation of composition has the structure of a group. Let $Bij[\mathsf{t}]$ denote the composition of bijections.

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

Example. *Let T be any set. The composition of bijections of T is a group.*

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

8. Abelian Groups

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

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

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

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

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

$$abelian\_group[\mathsf{t}] == \{ AbelianGroup[\mathsf{t}] \bullet \mathbf{A} \}$$

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 $-x$.

Example. *Addition over the integers is an abelian group.*

$$(\mathbb{Z}, (\_ + \_)) \in abelian\_group[\mathbb{Z}]$$

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`