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

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.

Date: February 12, 2025.

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

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

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

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

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

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

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

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.

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

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

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

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

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

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

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

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

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

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

Integer division and modulus are not total binary operations on $\mathbb{Z}$ *because division or modulus by* 0 *is undefined.*

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.

3. Magmas

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.

3.1. **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 $(A, (\_ \cdot \_))$.

Magma[t]

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

$\_ \cdot \_ : pbinop[\mathsf{t}]$

$\mathbf{A} : \mathbb{P}\,\mathsf{t} \times pbinop[\mathsf{t}]$

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

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

- 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.

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

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*$[\mathsf{t}]$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.2. **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* 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. 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 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 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. That being said, the formal text will always use distinct names in any given context.

Magma_Map[t, u]

$Magma[\mathsf{t}]$
$Magma'[\mathsf{u}]$
$f : \mathsf{t} \pfun \mathsf{u}$
$F : (magma[\mathsf{t}] \times magma[\mathsf{u}]) \times (\mathsf{t} \pfun \mathsf{u})$

$f \in A \longrightarrow A'$

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

- f maps A to A'
- A magma map structure consists of a pair of magmas and a map 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 all magma maps from $\mathbf{A}$ to $\mathbf{A}'$.

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

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

$$\forall\, Magma[\mathsf{T}]; Magma'[\mathsf{U}] \bullet magma\_map(\mathbf{A}, \mathbf{A}') \subseteq magma\_Map[\mathsf{T}, \mathsf{U}]$$

A magma map f is a *magma homomorphism* if it preserves products.

Magma_Hom[t, u]

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

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

- 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 $\mathbf{A}'$.

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

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

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

Consider the identity map from the carrier of a magma to itself.

Magma_Id[t]

Magma_Map[t, t]

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

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

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

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

Remark. *The identity map is a homomorphism.*

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

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

MulConst

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

$c : \mathbb{Z}$

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

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

Therefore this map is a homomorphism.

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

Proof.

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

□

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

ExpConst

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

$n : \mathbb{N}$

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

$f = (\lambda\, x : \mathbb{Z} \bullet x \mathbin{**} n)$

Therefore this map is a homomorphism.

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

Proof.

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

□

3.3. **Subsets.** 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 depending on whether or not S is closed under the product.

Magma_Subset[t]

$Magma$[t]
$S : \mathbb{P}\, \mathsf{t}$
$\_ \centerdot \_ : pbinop$[t]
$\mathbf{S} : \mathbb{P}\, \mathsf{t} \times pbinop$[t]

$S \subseteq A$

$(\_ \centerdot \_) = (S \times S) \lhd (\_ \cdot \_)$

$\mathbf{S} = (S, (\_ \centerdot \_))$

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

Submagma[t]

$Magma\_Subset$[t]

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

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

Magma_Image[t, u]

$Magma\_Hom$[t, u]
$Magma\_Subset'$[u]

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

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

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

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 $x' \centerdot' y' = f(x) \centerdot' f(y) = f(x \cdot y)$ which is clearly in the image of f. □

Let *magma_im* be the function that maps a magma homomorphism to its image.

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

3.6. **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''.

Magma_Composition[t, u, v]

Magma_Hom[t, u]
Magma_Hom′[u, v]
$g : \mathsf{t} \pfun \mathsf{v}$
G : *magma_Map*[t, v]

$g = f' \circ f$

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

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

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

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

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

4. Semigroups

4.1. **Associativity.** 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.

Associative[t]

Magma[t]

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

4.2. **Semigroups.** An associative magma is called a *semigroup*.

Semigroup[t]

Associative[t]

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

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

Remark. *Every semigroup is a magma.*

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

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

SequenceConcat[t]

Magma[seq t]

$A = \operatorname{seq} \mathsf{t}$

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

$\forall\, \mathit{SequenceConcat}[\mathsf{T}] \bullet \mathbf{A} \in \mathit{semigroup}[\operatorname{seq} \mathsf{T}]$

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

Semigroup_Hom[t, u]

Magma_Hom[t, u]

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

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

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

Let *semigroup_Hom*[t, 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 *semigroup_hom*$(\mathbf{A}, \mathbf{A}')$ be the subset of semigroup homomorphisms from $\mathbf{A}$ to $\mathbf{A}'$.

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

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

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

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

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

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.*

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

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

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

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

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

5. Monoids

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

IdentityElement[t]
Magma[t]
e : t

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

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

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

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

Remark.

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

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

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

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

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

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

Proof.

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

□

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

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

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

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

Monoid[t]

$Semigroup[\mathsf{t}]$
$IdentityElement[\mathsf{t}]$

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

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

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

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

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

MapPreservesIdentity[t, u]

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

$f(e) = e'$

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

Monoid_Hom[t, u]

$Semigroup\_Hom[\mathsf{t}, \mathsf{u}]$
$MapPreservesIdentity[\mathsf{t}, \mathsf{u}]$

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

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

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

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

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

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

6. Groups

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

InverseOperation[t]

$IdentityElement[\mathsf{t}]$

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

$inv \in A \longrightarrow A$

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

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

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

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

InverseOperations[t]

$Monoid[\mathsf{t}]$

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

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

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

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

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

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

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

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

□

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Remark. *Composition is associative.*

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

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

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

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

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

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

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

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

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

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

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

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

Subgroup[t]

$A : \mathbb{P}_1\, \mathsf{t}$
Group′[t]

$A \subseteq A'$

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

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

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

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

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

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

A subgroup inherits a group structure from its enclosing group.

Subgroup_Group[t]

Subgroup[t]
Magma[t]
$e : \mathsf{t}$
$inv : \mathsf{t} \pfun \mathsf{t}$

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

$e = e'$

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

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

Remark. *A subgroup is a group.*

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

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

Subgroup_Inclusion[t]

Subgroup_Group[t]
Magma_Map[t, t]

$f = \mathrm{id}\ A$

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

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

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

7. Abelian Groups

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

Commutative[t]

Magma[t]

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

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

AbelianGroup[t]

Group[t]
Commutative[t]

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

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

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

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

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

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

AbelianGroup_Hom[t, u]

Group_Hom[t, u]
Group[t]
Group′[u]

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

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

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

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

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`