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 21, 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.

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

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

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

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

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

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

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

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

Example. *Integer addition, subtraction, and multiplication 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.

Magma[t]

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

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

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

- The product is a binary operation on A.

Regarded as a structure $\mathbf{A}$, a magma is a pair $(A, (\_ \cdot \_))$.

Magma_Struc[t]

Magma[t]

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

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

- the structure $\mathbf{A}$ is the pair consisting of the carrier A and the product $(\_ \cdot \_)$

Let *magma*[t] denote the set of all magma structures in t.

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

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

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

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

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

4.2. **Integer Multiplication.** Let *int_mul* denote the set of integers equipped with multiplication.

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

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

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

4.3. **Magma Homomorphisms.** Let A and A' be a magmas and let f be a map from A to A'.

Magma_Map[t, u]

Magma_Struc[t]

Magma_Struc′[u]

$f : \mathsf{t} \pfun \mathsf{u}$

$f \in A \longrightarrow A'$

- f maps A to A'

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

Magma_Hom[t, u]

Magma_Map[t, u]

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

- f preserves the product operation

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

$$magma\_Hom[\mathsf{t}, \mathsf{u}] == \{\ Magma\_Hom[\mathsf{t}, \mathsf{u}] \bullet (\mathbf{A}, \mathbf{A}') \mapsto f\ \}$$

Let *magma_hom*($\mathbf{A}, \mathbf{A}'$) be the subset of all 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.*

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

4.3.1. *The Identity Map.*

Example. *The identity map is a homomorphism.*

Magma_Id[t]

Magma_Map[t, t]

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

$f = \mathrm{id}\ A$

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

4.3.2. *Multiplication by a Fixed Integer.*

Example. *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

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

Proof.

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

□

4.3.3. *Exponentiation by a Fixed Natural Number.*

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

ExpConst

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

$$\mathbf{A} = \mathbf{A}' = int\_mul$$
$$f = (\lambda\, x : \mathbb{Z} \bullet x ** n)$$

Therefore

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

Proof.

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

□

4.4. **Composition.** TODO: Define 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]

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

$$g = f' \circ f$$

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

$$\forall\, \mathbf{A} : \mathrm{magma}\, \mathsf{X};\ \mathbf{B} : \mathrm{magma}\, \mathsf{Y};\ \mathbf{C} : \mathrm{magma}\, \mathsf{Z} \bullet \\ \quad \forall\, f : \hom_{\mathrm{mgm}}(\mathbf{A}, \mathbf{B});\ g : \hom_{\mathrm{mgm}}(\mathbf{B}, \mathbf{C}) \bullet \\ \quad\quad g \circ f \in \hom_{\mathrm{mgm}}(\mathbf{A}, \mathbf{C})$$

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.

Magma_IsAssociative_A[t]

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

An associative magma is called a *semigroup*.

$\textit{Semigroup\_A}[\mathsf{t}] \mathrel{\widehat=} \textit{Magma\_IsAssociative\_A}[\mathsf{t}]$

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

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

Let the notation semigroup t, typeset using the prefix generic command `\semigroup`, denote the set of all semigroups in t.

$\text{semigroup}\, \mathsf{t} == \textit{semigroup}[\mathsf{t}]$

Remark.

$\text{semigroup}\, \mathsf{T} \subseteq \text{magma}\, \mathsf{T}$

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

Let $\mathbf{A}, \mathbf{B}$ be semigroups in t, u. Let *hom_semigroup*$(\mathbf{A}, \mathbf{B})$ denote the set of semigroup homomorphisms from $\mathbf{A}$ to $\mathbf{B}$.

$$\textit{hom\_semigroup}[\mathsf{t}, \mathsf{u}] == \\ \quad (\lambda\, \mathbf{A} : \text{semigroup}\, \mathsf{t}; \mathbf{B} : \text{semigroup}\, \mathsf{u} \bullet \hom_{\text{mgm}}(\mathbf{A}, \mathbf{B}))$$

Note that as structures, semigroups are a subset of magmas. Every magma homomorphism of a semigroup is a semigroup homomorphism.

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

Let $\hom_{\text{sg}}(\mathbf{A}, \mathbf{B})$ denote the set of all semigroup homomorphisms from $\mathbf{A}$ to $\mathbf{B}$.

[t, u]

$$\begin{array}{l} \hom_{\text{sg}} : \text{semigroup}\, \mathsf{t} \times \text{semigroup}\, \mathsf{u} \longrightarrow \mathbb{P}(\mathsf{t} \nrightarrow \mathsf{u}) \\ \hline \hom_{\text{sg}} = \\ \quad (\lambda\, \mathbf{A} : \text{semigroup}\, \mathsf{t}; \mathbf{B} : \text{semigroup}\, \mathsf{u} \bullet \hom_{\text{mgm}}(\mathbf{A}, \mathbf{B})) \end{array}$$

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

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

6. Monoids

Let t be a set, let $\mathbf{A} = (A, (\_ * \_))$ be a magma in t, 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.

IdentityElement_A[t]

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

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.

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

Remark.

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

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

IdentityElements_A[t]

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

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

$$\forall\, \textit{IdentityElements\_A}[\mathsf{T}] \bullet e = e'$$

Proof.

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

□

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

$$\textit{identity\_element}[\mathsf{T}] \in \mathrm{magma}\, \mathsf{T} \nrightarrow \mathsf{T}$$

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.

Monoid_A[t]

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

Let monoid t denote the set of all monoids in t.

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

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

MapPreservesIdentity[t, u]

$$f : \mathsf{t} \pfun \mathsf{u}$$
$$\mathbf{A} : \text{monoid}\,\mathsf{t}$$
$$\mathbf{B} : \text{monoid}\,\mathsf{u}$$

$$\textbf{let}\ e == \textit{identity\_element}\,\mathbf{A};$$
$$e' == \textit{identity\_element}\,\mathbf{B} \bullet$$
$$f\ e = e'$$

A *monoid homomorphism* from $\mathbf{A}$ to $\mathbf{B}$ is a homomorphism f of the underlying semigroups that preserves identity. Let $\hom_{\text{mnd}}(\mathbf{A}, \mathbf{B})$ denote the set of all monoid homomorphisms from $\mathbf{A}$ to $\mathbf{B}$.

[t, u]

$$\hom_{\text{mnd}} : \text{monoid}\,\mathsf{t} \times \text{monoid}\,\mathsf{u} \longrightarrow \mathbb{P}(\mathsf{t} \longrightarrow \mathsf{u})$$

$$\hom_{\text{mnd}} =$$
$$(\lambda\, \mathbf{A} : \text{monoid}\,\mathsf{t}; \mathbf{B} : \text{monoid}\,\mathsf{u} \bullet$$
$$\{ f : \hom_{\text{sg}}(\mathbf{A}, \mathbf{B}) \mid$$
$$\textit{MapPreservesIdentity}[\mathsf{t}, \mathsf{u}] \,\})$$

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 monoid in t. A function $inv \in A \longrightarrow A$ is said to be an *inverse operation* if it maps each element to an element whose product with it is the identity element. Typically, the postfix expression x^{-1} is used to denote the inverse of x.

InverseOperation_A[t]

$$
\begin{array}{l}
\mathit{Monoid\_A}[\mathsf{t}] \\
\mathit{inv} : \mathsf{t} \pfun \mathsf{t} \\
\hline
\mathit{inv} \in A \fun A \\
\textbf{let } (\_^{-1}) == \mathit{inv} \bullet \\
\quad \forall\, x : A \bullet \\
\qquad x * x^{-1} = e = x^{-1} * x
\end{array}
$$

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

$$
\begin{array}{l}
\mathit{inverse\_operation}[\mathsf{t}] == \\
\quad \{\, \mathit{InverseOperation\_A}[\mathsf{t}] \bullet \mathbf{A} \mapsto \mathit{inv} \,\}
\end{array}
$$

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

Proof. Let x be any element. Suppose x^{-1} and $x^\dagger$ are inverses of x.

$$
\begin{array}{lr}
x^\dagger & \\
\quad = x^\dagger * 1 & [1 \text{ is an identity element}] \\
\quad = x^\dagger * (x * x^{-1}) & [x^{-1} \text{ is an inverse}] \\
\quad = (x^\dagger * x) * x^{-1} & [\text{associativity}] \\
\quad = 1 * x^{-1} & [x^\dagger \text{ is an inverse}] \\
\quad = x^{-1} & [1 \text{ is an identity element}]
\end{array}
$$

□

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

$$\mathit{inverse\_operation} \in \mathrm{monoid}\, \mathsf{T} \pfun \mathsf{T} \pfun \mathsf{T}$$

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

Group_A[t]

$$
\begin{array}{l}
\mathit{InverseOperation\_A}[\mathsf{t}]
\end{array}
$$

Let t be a set of elements. Let group t denote the set of all groups over t.

$$\mathrm{group}\, \mathsf{t} == \{\, \mathit{Group\_A}[\mathsf{t}] \bullet \mathbf{A} \,\}$$

Let t and u be sets of elements, let **A** and **B** be groups over 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 B.

MapPreservesInverse[t, u]

$f : \mathsf{t} \pfun \mathsf{u}$
$\mathbf{A} : \mathrm{group}\, \mathsf{t}$
$\mathbf{B} : \mathrm{group}\, \mathsf{u}$

---

let $(\_^{-1}) == \mathit{inverse\_operation}\, \mathbf{A}$;
$(\_^{\dagger}) == \mathit{inverse\_operation}\, \mathbf{B} \bullet$
$\forall x : \mathsf{t} \bullet$
$f(x^{-1}) = (f\ x)^{\dagger}$

Let $\mathbf{A}$ and $\mathbf{B}$ be groups. A *group homomorphism* from $\mathbf{A}$ to $\mathbf{B}$ is a monoid homomorphism from $\mathbf{A}$ to $\mathbf{B}$ that preserves inverses. Let $\hom_{\mathrm{grp}}(\mathbf{A}, \mathbf{B})$ denote the set of all group homomorphisms from $\mathbf{A}$ to $\mathbf{B}$.

[t, u]

$\hom_{\mathrm{grp}} : \mathrm{group}\, \mathsf{t} \times \mathrm{group}\, \mathsf{u} \longrightarrow \mathbb{P}(\mathsf{t} \longrightarrow \mathsf{u})$

$\hom_{\mathrm{grp}} =$
$(\lambda\, \mathbf{A} : \mathrm{group}\, \mathsf{t}; \mathbf{B} : \mathrm{group}\, \mathsf{u} \bullet$
$\{ f : \hom_{\mathrm{mnd}}(\mathbf{A}, \mathbf{B}) \mid$
MapPreservesInverse[t, u] $\})$

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 *bij*[t] denote the set of a 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.*

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

Remark. *Composition is associative.*

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

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

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

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

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

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.*

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

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.

OperationIsCommutative_A[t]

Magma_A[t]

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

An *abelian group* is a group in which the binary operation is commutative.

AbelianGroup_A[t]

Group_A[t]
OperationIsCommutative_A[t]

Let $\mathrm{abgroup}\,\mathsf{t}$ denote the set of all abelian groups in t.

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

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.*

$(\mathbb{Z}, (\_ + \_)) \in \mathrm{abgroup}\,\mathbb{Z}$

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`