GROUPS

ARTHUR RYMAN

ABSTRACT. This article contains Z Notation definitions for groups and some related objects, namely magmas, semigroups, and monoids. It has been type checked with fUZZ.

CONTENTS

1. INTRODUCTION

Groups are ubiquitous throughout mathematics and physics. This article defines groups, and their homomorphisms, gradually building up the definitions in terms of some simpler, related mathematical objects, namely magmas, semigroups, and monoids.

These objects are *mathematical structures*, namely sets of elements equipped with additional features. The set of elements of a structure is often referred to as its *carrier*. In particular, magmas, semigroups, monoids, and groups are *algebraic structures*.

2. STRUCTURES

In normal mathematical writing, authors do not need to distinguish between a structure and it carrier because the structure is usually clear from context. For example, one typically see statements such as: "Let G be a group and let g be an element of G." Here the first instance of the variable G stands for the structure while the second stands for its carrier.

Date: January 18, 2025.

However, a set of elements may have more than one structure in a given context. For example, the set of integers has the distinct binary operations of 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, 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. This article also adopts the notational convention of using bold font variables, e.g. $\mathbf{A}, \mathbf{B}, \mathbf{C}$, to denote structures, and the corresponding Roman font variables, e.g. A, B, C, to denote their carriers.

TO DO: update the article to define structures as tuples of a carrier and a binary operation. Also better integrate the informal text notation with the formal text by using the variable names in the schema.

3. Carriers

Let t be a set and let *elements* be a nonempty subset of t. The set t can be thought of as the *universe of discourse* from which the elements are drawn. The set *elements* in the context of some mathematical structure is said to be the *carrier* of that structure. Such a structure is said to be *on* or *over* its set of elements and *in* the universe from which its elements are drawn.

$$\begin{array}{|l}
\hline
\textit{Carrier}[\mathsf{t}] \\
\textit{elements} : \mathbb{P}_1\, \mathsf{t} \\
\hline
\end{array}$$

Let $\mathbf{A}$ and $\mathbf{B}$ be structures with carriers A and B. A *carrier map* from $\mathbf{A}$ to $\mathbf{B}$ is a triple (f, A, B) where f is a function from A to B. In this situation, the carrier A of the source structure $\mathbf{A}$ is called the *domain* of the map and the carrier B of the target structure $\mathbf{B}$ is called its *codomain*.

TO DO: The following schemas do not mention the variables introduced above. Fix this by introducing schemas that incorporate the variables. Also note that the text mentions structures but does not formally define them. Perhaps eliminate the Carrier schema and start with the Magma schema.

$\textit{Carrier\_Domain}[\mathsf{t}] \mathrel{\widehat=} \textit{Carrier}[\mathsf{t}][\textit{domain}/\textit{elements}]$

$\textit{Carrier\_Codomain}[\mathsf{t}] \mathrel{\widehat=} \textit{Carrier}[\mathsf{t}][\textit{codomain}/\textit{elements}]$

$$\begin{array}{|l}
\hline
\textit{Carrier\_Map}[\mathsf{t}, \mathsf{u}] \\
\textit{Carrier\_Domain}[\mathsf{t}] \\
\textit{Carrier\_Codomain}[\mathsf{u}] \\
\textit{function} : \mathsf{t} \mathrel{⇸} \mathsf{u} \\
\hline
\textit{function} \in \textit{domain} \longrightarrow \textit{codomain} \\
\hline
\end{array}$$

Remark. *The domain of a carrier map is uniquely determined by its function.*

$\forall\, \textit{Carrier\_Map}[\mathsf{T}, \mathsf{U}] \bullet \operatorname{dom} \textit{function} = \textit{domain}$

Remark. *The codomain of a carrier map is a superset of the range of its function. This means that carrier maps that have the same function but distinct codomains are distinct carrier maps.*

$\forall\, \mathit{Carrier\_Map}[\mathsf{T}, \mathsf{U}] \bullet \operatorname{ran} \mathit{function} \subseteq \mathit{codomain}$

Let $\mathit{carrier\_maps}[\mathsf{t}]$ denote the set of all carrier maps of structures in t.

$\mathit{carrier\_maps}[\mathsf{t}] == \{\, \mathit{Carrier\_Map}[\mathsf{t}, \mathsf{t}] \bullet (\mathit{function}, \mathit{domain}, \mathit{codomain}) \,\}$

Let A, B, C be carriers of some structures. Consider functions $f : A \longrightarrow B$, $g : B \longrightarrow C$, and $h : A \longrightarrow C$.

$\mathit{Carrier\_Map\_fAB}[\mathsf{t}, \mathsf{u}] \mathrel{\widehat=} \mathit{Carrier\_Map}[\mathsf{t}, \mathsf{u}][f/\mathit{function}, A/\mathit{domain}, B/\mathit{codomain}]$

$\mathit{Carrier\_Map\_gBC}[\mathsf{t}, \mathsf{u}] \mathrel{\widehat=} \mathit{Carrier\_Map}[\mathsf{t}, \mathsf{u}][g/\mathit{function}, B/\mathit{domain}, C/\mathit{codomain}]$

$\mathit{Carrier\_Map\_hAC}[\mathsf{t}, \mathsf{u}] \mathrel{\widehat=} \mathit{Carrier\_Map}[\mathsf{t}, \mathsf{u}][h/\mathit{function}, A/\mathit{domain}, C/\mathit{codomain}]$

The carrier map (g, B, C) is said to be *composable* with the carrier map (f, A, B).

$$
\begin{array}{|l}
\hline
\mathit{Carrier\_Composable\_gf}[\mathsf{t}, \mathsf{u}, \mathsf{v}] \\
\hline
\mathit{Carrier\_Map\_fAB}[\mathsf{t}, \mathsf{u}] \\
\mathit{Carrier\_Map\_gBC}[\mathsf{u}, \mathsf{v}] \\
\hline
\end{array}
$$

Let $\mathit{carrier\_composable}[\mathsf{t}]$ denote the set of composable pairs of carrier maps in t.

$\mathit{carrier\_composable}[\mathsf{t}] ==$
$\quad \{\, \mathit{Carrier\_Composable\_gf}[\mathsf{t}, \mathsf{t}, \mathsf{t}] \bullet (g, B, C) \mapsto (f, A, B) \,\}$

The carrier map (h, A, C) is said to be the *composition* of (g, B, C) with (f, A, B) when h is the function composition $g \circ f$.

$$
\begin{array}{|l}
\hline
\mathit{Carrier\_Composition\_hgf}[\mathsf{t}, \mathsf{u}, \mathsf{v}] \\
\hline
\mathit{Carrier\_Map\_fAB}[\mathsf{t}, \mathsf{u}] \\
\mathit{Carrier\_Map\_gBC}[\mathsf{u}, \mathsf{v}] \\
\mathit{Carrier\_Map\_hAC}[\mathsf{t}, \mathsf{v}] \\
\hline
h = g \circ f \\
\hline
\end{array}
$$

Let $\mathit{carrier\_composition}[\mathsf{t}]$ denote the composition operation on composable carrier maps for structures in t.

$\mathit{carrier\_composition}[\mathsf{t}] ==$
$\quad \{\, \mathit{Carrier\_Composition\_hgf}[\mathsf{t}, \mathsf{t}, \mathsf{t}] \bullet ((g, B, C), (f, A, B)) \mapsto (h, A, C) \,\}$

4. Magmas

Let t be a set. A *binary operator* in t is a partial function from pairs of elements of t to elements of t.

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

Let *elements* be a subset of t and let *op* be binary operator defined on all pairs of elements. We call the structure $(\mathit{elements}, \mathit{op})$ a *magma on the set elements*. Furthermore, we say that it is a *magma in* t.

$$
\begin{array}{|l}
\hline
\textit{Magma}[\mathsf{t}] \\
\textit{Carrier}[\mathsf{t}] \\
\textit{op} : \textit{BINOP}[\mathsf{t}] \\
\textit{structure} : \mathbb{P}\,\mathsf{t} \times \textit{BINOP}[\mathsf{t}] \\
\hline
\textit{op} \in \textit{elements} \times \textit{elements} \longrightarrow \textit{elements} \\
\textit{structure} = (\textit{elements}, \textit{op}) \\
\hline
\end{array}
$$

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

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

Let the notation $\mathrm{magma}\,\mathsf{t}$ denote the set of all magmas in t.

$\mathrm{magma}\,\mathsf{t} == \textit{magma}[\mathsf{t}]$

Let *integer_addition* denote the binary operation of integer addition.

$\textit{integer\_addition} == (\mathbb{Z}, (\_ + \_))$

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

$\textit{integer\_addition} \in \mathrm{magma}\,\mathbb{Z}$

Let *integer_multiplication* denote the magma of integer multiplication.

$\textit{integer\_multiplication} == (\mathbb{Z}, (\_ * \_))$

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

$\textit{integer\_multiplication} \in \mathrm{magma}\,\mathbb{Z}$

The result of applying a binary operator to a pair of elements (x, y) is normally denoted by an expression formed using an infix operator such as $x + y$ or $x * y$.

Let t and u be sets, let $A \subseteq \mathsf{t}$ and $B \subseteq \mathsf{u}$ be subsets of elements, and let the infix expression $x * y$ denote binary operators on both A and B. Here we follow the standard practice of using visually indistinguishable symbols to denote distinct mathematical objects when no confusion can occur. Although the symbols look the same, they are encoded distinctly at the source level, in this case using the operator names `\mulA` and `\mulB`. This practice makes the typeset expressions look as close as possible to informal mathematical notation while at the same time satisfying the strict requirements of the type checker.

Let *Magma_A* denote the magma $\mathbf{A}$ where A is the set of elements and $\_ * \_$ is the infix operator named `\mulA`.

$$
\begin{array}{l}
\textit{Magma\_A}[\mathsf{t}] \mathrel{\widehat=} \\
\quad \textit{Magma}[\mathsf{t}][A/\textit{elements}, \_ * \_/\textit{op}, \mathbf{A}/\textit{structure}]
\end{array}
$$

Similarly, let *Magma_B* denote the magma $\mathbf{B}$ where B is the set of elements and $\_ * \_$ is the infix operator named `\mulB`.

$$
\begin{array}{l}
\textit{Magma\_B}[\mathsf{t}] \mathrel{\widehat=} \\
\quad \textit{Magma}[\mathsf{t}][B/\textit{elements}, \_ * \_/\textit{op}, \mathbf{B}/\textit{structure}]
\end{array}
$$

Let $\mathbf{A}$ and $\mathbf{B}$ be magmas and let f map A to B.

$$\begin{array}{|l}
\multicolumn{1}{l}{\mathit{Magma\_Map\_AB}[\mathsf{t},\mathsf{u}]} \\
\mathit{Magma\_A}[\mathsf{t}] \\
\mathit{Magma\_B}[\mathsf{u}] \\
f : \mathsf{t} \pfun \mathsf{u} \\
\hline
f \in A \longrightarrow B \\
\hline
\end{array}$$

The map f is said to *preserve the operations* if it maps the product of elements of A to the product of the mapped elements of B.

$$\begin{array}{|l}
\multicolumn{1}{l}{\mathit{Magma\_MapPreservesOperations\_AB}[\mathsf{t},\mathsf{u}]} \\
\mathit{Magma\_Map\_AB}[\mathsf{t},\mathsf{u}] \\
\hline
\forall x, y : A \bullet \\
\qquad f(x * y) = (f\ x) * (f\ y) \\
\hline
\end{array}$$

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

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

Therefore

$$\begin{array}{l}
\forall \mathit{Magma\_Map\_AB}[\mathbb{Z},\mathbb{Z}];\ c : \mathbb{Z} \mid \\
\qquad \mathbf{A} = \mathbf{B} = (\mathbb{Z}, (\_ + \_)) \land \\
\qquad f = (\lambda x : \mathbb{Z} \bullet c * x) \bullet \\
\qquad\qquad \mathit{Magma\_MapPreservesOperations\_AB}[\mathbb{Z},\mathbb{Z}]
\end{array}$$

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

$$\begin{array}{l}
\forall n : \mathbb{N};\ x, y : \mathbb{Z} \bullet \\
\qquad (x * y) ** n = x ** n * y ** n
\end{array}$$

A map that preserves operations is said to be a *magma homomorphism.*

Let $\mathbf{A}, \mathbf{B}$ be magmas in t and u. Let $\mathit{hom\_magma}[\mathsf{t},\mathsf{u}](\mathbf{A},\mathbf{B})$ denote the set of all magma homomorphisms from $\mathbf{A}$ to $\mathbf{B}$.

$$\begin{array}{l}
\mathit{hom\_magma}[\mathsf{t},\mathsf{u}] == \\
\qquad (\lambda \alpha : \mathrm{magma}\,\mathsf{t};\ \beta : \mathrm{magma}\,\mathsf{u} \bullet \\
\qquad\qquad \{\ \mathit{Magma\_MapPreservesOperations\_AB}[\mathsf{t},\mathsf{u}] \mid \\
\qquad\qquad\qquad \alpha = \mathbf{A} \land \beta = \mathbf{B} \bullet f\ \})
\end{array}$$

Remark.

$$\mathit{hom\_magma}[\mathsf{T},\mathsf{U}] \in \mathrm{magma}\,\mathsf{T} \times \mathrm{magma}\,\mathsf{U} \longrightarrow \mathbb{P}(\mathsf{T} \pfun \mathsf{U})$$

Let the notation $\hom_{\mathrm{mgm}}(\alpha, \beta)$, typeset using the command `\homBinOp`, denote the set of magma homomorphisms from α to β.

$$\hom_{\mathrm{mgm}}[\mathsf{t},\mathsf{u}] == \mathit{hom\_magma}[\mathsf{t},\mathsf{u}]$$

Remark. *The identity map preserves all operations.*

$$\begin{array}{l} \forall\, \mathbf{A} : \operatorname{magma} \mathsf{X} \bullet \\ \qquad \operatorname{id} \mathsf{X} \in \hom_{\mathrm{mgm}}(\mathbf{A}, \mathbf{A}) \end{array}$$

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

$$\begin{array}{l} \forall\, \mathbf{A} : \operatorname{magma} \mathsf{X};\ \mathbf{B} : \operatorname{magma} \mathsf{Y};\ \mathbf{C} : \operatorname{magma} \mathsf{Z} \bullet \\ \qquad \forall\, f : \hom_{\mathrm{mgm}}(\mathbf{A}, \mathbf{B});\ g : \hom_{\mathrm{mgm}}(\mathbf{B}, \mathbf{C}) \bullet \\ \qquad\qquad g \circ f \in \hom_{\mathrm{mgm}}(\mathbf{A}, \mathbf{C}) \end{array}$$

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.

$$\begin{array}{|l} \multicolumn{1}{l}{\mathit{Magma\_IsAssociative\_A}[\mathsf{t}]} \\ \mathit{Magma\_A}[\mathsf{t}] \\ \hline \forall\, x, y, z : A \bullet \\ \qquad x * y * z = x * (y * z) \\ \hline \end{array}$$

An associative magma is called a *semigroup.*

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

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

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

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

$\operatorname{semigroup} \mathsf{t} == \mathit{semigroup}[\mathsf{t}]$

Remark.

$\operatorname{semigroup} \mathsf{T} \subseteq \operatorname{magma} \mathsf{T}$

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

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

$$\begin{array}{l} \mathit{hom\_semigroup}[\mathsf{t}, \mathsf{u}] == \\ \qquad (\lambda\, \mathbf{A} : \operatorname{semigroup} \mathsf{t};\ \mathbf{B} : \operatorname{semigroup} \mathsf{u} \bullet \hom_{\mathrm{mgm}}(\mathbf{A}, \mathbf{B})) \end{array}$$

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

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

$$\mathrm{hom}_{\mathrm{sg}} : \mathrm{semigroup}\,\mathsf{t} \times \mathrm{semigroup}\,\mathsf{u} \longrightarrow \mathbb{P}(\mathsf{t} \mathrel{+\!\!\!\to\!\!\!\!\to} \mathsf{u})$$

$$\begin{array}{l} \mathrm{hom}_{\mathrm{sg}} = \\ \qquad (\lambda\, \mathbf{A} : \mathrm{semigroup}\,\mathsf{t};\ \mathbf{B} : \mathrm{semigroup}\,\mathsf{u} \bullet \mathrm{hom}_{\mathrm{mgm}}(\mathbf{A}, \mathbf{B})) \end{array}$$

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.

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

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.

$$\begin{array}{l} \mathit{identity\_element}[\mathsf{t}] == \\ \qquad \{\, \mathit{IdentityElement\_A}[\mathsf{t}] \bullet \mathbf{A} \mapsto e \,\} \end{array}$$

Remark.

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

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

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

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

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

Proof.

e

$= e * e'$ [e' is an identity element]

$= e'$ [e is an identity element]

□

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

$\mathit{identity\_element}[\mathsf{T}] \in \mathrm{magma}\,\mathsf{T} \rightarrowtail\!\!\!\!\!\!+\;\, \mathsf{T}$

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.

$\mathit{Monoid\_A}[\mathsf{t}]$

$\mathit{Semigroup\_A}[\mathsf{t}]$

$\mathit{IdentityElement\_A}[\mathsf{t}]$

Let $\mathrm{monoid}\,\mathsf{t}$ denote the set of all monoids in t.

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

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.

$\mathit{MapPreservesIdentity}[\mathsf{t}, \mathsf{u}]$

$f : \mathsf{t} \rightarrowtail\!\!\!\!\!\!+\;\, \mathsf{u}$

$\mathbf{A} : \mathrm{monoid}\,\mathsf{t}$

$\mathbf{B} : \mathrm{monoid}\,\mathsf{u}$

$\mathbf{let}\ e == \mathit{identity\_element}\,\mathbf{A};$

$\quad e' == \mathit{identity\_element}\,\mathbf{B} \bullet$

$\qquad f\,e = e'$

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

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

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

$\hom_{\mathrm{mnd}} =$

$\quad (\lambda\, \mathbf{A} : \mathrm{monoid}\,\mathsf{t};\ \mathbf{B} : \mathrm{monoid}\,\mathsf{u} \bullet$

$\qquad \{\, f : \hom_{\mathrm{sg}}(\mathbf{A}, \mathbf{B}) \mid$

$\qquad\quad \mathit{MapPreservesIdentity}[\mathsf{t}, \mathsf{u}] \,\})$

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.

$$\begin{array}{|l}
\multicolumn{1}{l}{InverseOperation\_A[\mathsf{t}]} \\
\hline
Monoid\_A[\mathsf{t}] \\
inv : \mathsf{t} \nrightarrow \mathsf{t} \\
\hline
inv \in A \longrightarrow A \\
\\
\textbf{let } (\_^{-1}) == inv \bullet \\
\quad \forall x : A \bullet \\
\qquad x * x^{-1} = e = x^{-1} * x \\
\hline
\end{array}$$

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

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

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.

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

□

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

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

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

$$\begin{array}{|l}
\multicolumn{1}{l}{Group\_A[\mathsf{t}]} \\
\hline
InverseOperation\_A[\mathsf{t}] \\
\hline
\end{array}$$

Let t be a set of elements. Let $\mathrm{group}\,\mathsf{t}$ denote the set of all groups over t.

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

Let t and u be sets of elements, let $\mathbf{A}$ and $\mathbf{B}$ 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]

$f : \mathsf{t} ⇸ \mathsf{u}$
$\mathbf{A} : \text{group}\,\mathsf{t}$
$\mathbf{B} : \text{group}\,\mathsf{u}$

$$
\begin{aligned}
&\textbf{let } (\_^{-1}) == \textit{inverse\_operation}\,\mathbf{A};\\
&\qquad (\_^{\dagger}) == \textit{inverse\_operation}\,\mathbf{B} \bullet\\
&\qquad\quad \forall\, x : \mathsf{t} \bullet\\
&\qquad\qquad f(x^{-1}) = (f\ x)^{\dagger}
\end{aligned}
$$

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

[t, u]

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

$$
\begin{aligned}
&\hom_{\text{grp}} =\\
&\qquad (\lambda\, \mathbf{A} : \text{group}\,\mathsf{t};\ \mathbf{B} : \text{group}\,\mathsf{u} \bullet\\
&\qquad\quad \{\, f : \hom_{\text{mnd}}(\mathbf{A}, \mathbf{B}) \mid\\
&\qquad\qquad \textit{MapPreservesInverse}[\mathsf{t}, \mathsf{u}]\,\})
\end{aligned}
$$

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 $\mathsf{t} ⤖ \mathsf{t}$ from t to itself.

$\textit{bij}[\mathsf{t}] == \mathsf{t} ⤖ \mathsf{t}$

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

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

Remark. *Composition is associative.*

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

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

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

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

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

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

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

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

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

8. Abelian Groups

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

$\mathit{OperationIsCommutative\_A}[\mathsf{t}]$
$\mathit{Magma\_A}[\mathsf{t}]$

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

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

$\mathit{AbelianGroup\_A}[\mathsf{t}]$
$\mathit{Group\_A}[\mathsf{t}]$
$\mathit{OperationIsCommutative\_A}[\mathsf{t}]$

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

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

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 $\text{-}\, x$.

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

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

Email address, Arthur Ryman: `arthur.ryman@gmail.com`