GROUPS

ARTHUR RYMAN

ABSTRACT. This article contains Z Notation definitions for groups and some related objects. It has been type checked with *f*UZZ.

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 related, simpler algebraic objects, namely binary operations, semigroups, and monoids. These objects are *mathematical structures*, namely sets of elements equipped with additional features. In particular, binary operations, semigroups, monoids, and groups are *algebraic structures*.

2. CARRIERS

Let `t` be a set and let *elements* be a 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.

Date: October 20, 2022.

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

Let $\mathbf{A}, \mathbf{B}$ be structures with carriers A, 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*.

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

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

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

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

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

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).

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

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 $g \circ f$.

$$
\begin{array}{|l}
\multicolumn{1}{l}{\textit{Carrier\_Composition\_hgf}[\mathsf{t},\mathsf{u},\mathsf{v}]} \\
\textit{Carrier\_Map\_fAB}[\mathsf{t},\mathsf{u}] \\
\textit{Carrier\_Map\_gBC}[\mathsf{u},\mathsf{v}] \\
\textit{Carrier\_Map\_hAC}[\mathsf{t},\mathsf{v}] \\
\hline
h = g \circ f \\
\hline
\end{array}
$$

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

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

3. Structures

In normal mathematical writing, authors do not need to distinguish between a carrier and its structure 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.

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 carriers and structures on them, this article adopts the common practice of defining structures as being *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.

4. Binary Operations

STOPPED HERE

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

$$\textit{BINOP}[\mathsf{t}] == \mathsf{t} \times \mathsf{t} \pfun \mathsf{t}$$

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

$$
\begin{array}{|l}
\multicolumn{1}{l}{\textit{BinaryOperation}[\mathsf{t}]} \\
\textit{Carrier}[\mathsf{t}] \\
\textit{op} : \textit{BINOP}[\mathsf{t}] \\
\textit{structure} : \mathbb{P}\,\mathsf{t} \times \textit{BINOP}[\mathsf{t}] \\
\hline
\textit{op} \in \textit{elements} \times \textit{elements} \longrightarrow \textit{elements} \\
\textit{structure} = (\textit{elements}, \textit{op}) \\
\hline
\end{array}
$$

Let $\mathit{binary\_operation}[\mathsf{t}]$ denote the set of all binary operations in t.

$\mathit{binary\_operation}[\mathsf{t}] == \{ \mathit{BinaryOperation}[\mathsf{t}] \bullet \mathit{structure} \}$

Let the notation $\mathrm{binop}\,\mathsf{t}$ denote the set of all binary operations in t.

$\mathrm{binop}\,\mathsf{t} == \mathit{binary\_operation}[\mathsf{t}]$

Let $\mathit{integer\_addition}$ denote the binary operation of integer addition.

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

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

$\mathit{integer\_addition} \in \mathrm{binop}\,\mathbb{Z}$

Let $\mathit{integer\_multiplication}$ denote the binary operation of integer multiplication.

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

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

$\mathit{integer\_multiplication} \in \mathrm{binop}\,\mathbb{Z}$

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 $\mathit{BinaryOperation\_A}$ denote the binary operation $\mathbf{A}$ where A is the set of elements and $\_ * \_$ is the infix operator named `\mulA`.

$\mathit{BinaryOperation\_A}[\mathsf{t}] \mathrel{\widehat{=}}$
$\quad \mathit{BinaryOperation}[\mathsf{t}][A/\mathit{elements}, \_ * \_/\mathit{op}, \mathbf{A}/\mathit{structure}]$

Similarly, let $\mathit{BinaryOperation\_B}$ denote the binary operation $\mathbf{B}$ where B is the set of elements and $\_ * \_$ is the infix operator named `\mulB`.

$\mathit{BinaryOperation\_B}[\mathsf{t}] \mathrel{\widehat{=}}$
$\quad \mathit{BinaryOperation}[\mathsf{t}][B/\mathit{elements}, \_ * \_/\mathit{op}, \mathbf{B}/\mathit{structure}]$

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

$\mathit{BinaryOperation\_Map\_AB}[\mathsf{t}, \mathsf{u}]$
$\mathit{BinaryOperation\_A}[\mathsf{t}]$
$\mathit{BinaryOperation\_B}[\mathsf{u}]$
$f : \mathsf{t} \pfun \mathsf{u}$
$f \in A \longrightarrow B$

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.

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

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

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

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 an *operation homomorphism*.

Let $\mathbf{A}, \mathbf{B}$ be binary operations in t and u. Let $\textit{hom\_op}[\mathsf{t},\mathsf{u}](\mathbf{A},\mathbf{B})$ denote the set of all operation homomorphisms from $\mathbf{A}$ to $\mathbf{B}$.

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

Remark.

$$\textit{hom\_op}[\mathsf{T},\mathsf{U}] \in \mathrm{binop}\,\mathsf{T} \times \mathrm{binop}\,\mathsf{U} \longrightarrow \mathbb{P}(\mathsf{T} \mathrel{+\!\!\!\!\rightarrow} \mathsf{U})$$

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

$$\mathrm{hom}[\mathsf{t},\mathsf{u}] == \textit{hom\_op}[\mathsf{t},\mathsf{u}]$$

Remark. *The identity map preserves all operations.*

$$
\begin{array}{l}
\forall \mathbf{A} : \mathrm{binop}\,\mathsf{X} \bullet \\
\qquad \mathrm{id}\,\mathsf{X} \in \mathrm{hom}(\mathbf{A},\mathbf{A})
\end{array}
$$

Remark. *The composition of two operation homomorphisms is an operation homomorphism.*

$$\forall \mathbf{A} : \operatorname{binop} \mathsf{X}; \mathbf{B} : \operatorname{binop} \mathsf{Y}; \mathbf{C} : \operatorname{binop} \mathsf{Z} \bullet$$
$$\quad \forall f : \hom(\mathbf{A}, \mathbf{B}); g : \hom(\mathbf{B}, \mathbf{C}) \bullet$$
$$\quad\quad g \circ f \in \hom(\mathbf{A}, \mathbf{C})$$

5. Semigroups

A binary operation is said to be *associative* if the result of applying it to any three elements is independent of the order in which it is applied pairwise.

$$\mathit{BinaryOperation\_IsAssociative\_A}[\mathsf{t}]$$
$$\mathit{BinaryOperation\_A}[\mathsf{t}]$$
$$\forall x, y, z : A \bullet$$
$$\quad x * y * z = x * (y * z)$$

An associative binary operation is called a *semigroup*.

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

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.

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

A *semigroup homomorphism* is a homomorphism of the underlying binary operation.

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 $\mathbf{B}$.

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

Note that as a type, semigroups are a subset of binary operations. The operation homomorphisms of a semigroup are the same as the semigroup homomorphisms.

If A is a semigroup and B is a binary operation and f is an operation homomorphism then the image of f is a semigroup.

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

$$
\begin{array}{|l}
\hline
[\mathsf{t}, \mathsf{u}] \\
\mathrm{hom}_{\mathrm{sg}} : \mathrm{semigroup}\,\mathsf{t} \times \mathrm{semigroup}\,\mathsf{u} \longrightarrow \mathbb{P}(\mathsf{t} \rightarrow\!\!\!\!\!\rightarrow \mathsf{u}) \\
\hline
\mathrm{hom}_{\mathrm{sg}} = \\
\qquad (\lambda\, A : \mathrm{semigroup}\,\mathsf{t};\ B : \mathrm{semigroup}\,\mathsf{u} \bullet \mathrm{hom}(A, B)) \\
\hline
\end{array}
$$

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 binary operation in t, 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.

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

Let *identity_element* denote the relation between binary operations 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.

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

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

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

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

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

Proof.

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

□

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

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

Identity elements are typically denoted by the symbols 0 or 1.

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

$$\begin{array}{|l}
\hline
\textit{Monoid_A}[\mathsf{t}] \\
\textit{Semigroup_A}[\mathsf{t}] \\
\textit{IdentityElement_A}[\mathsf{t}] \\
\hline
\end{array}$$

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

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

Let A and 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.

$$\begin{array}{|l}
\hline
\textit{MapPreservesIdentity}[\mathsf{t}, \mathsf{u}] \\
f : \mathsf{t} \nrightarrow \mathsf{u} \\
A : \mathrm{monoid}\,\mathsf{t} \\
B : \mathrm{monoid}\,\mathsf{u} \\
\hline
\mathbf{let}\ e == identity_element\ A; \\
\qquad e' == identity_element\ B \bullet \\
\qquad\qquad f\ e = e' \\
\hline
\end{array}$$

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

$$\begin{array}{|l}
\hline\hline
[\mathsf{t}, \mathsf{u}] \\
\hom_{\mathrm{mon}} : \mathrm{monoid}\,\mathsf{t} \times \mathrm{monoid}\,\mathsf{u} \longrightarrow \mathbb{P}(\mathsf{t} \longrightarrow \mathsf{u}) \\
\hline
\hom_{\mathrm{mon}} = \\
\qquad (\lambda\, A : \mathrm{monoid}\,\mathsf{t};\ B : \mathrm{monoid}\,\mathsf{u} \bullet \\
\qquad\qquad \{\, f : \hom_{\mathrm{sg}}(A, B) \mid \\
\qquad\qquad\qquad \textit{MapPreservesIdentity}[\mathsf{t}, \mathsf{u}] \,\}) \\
\hline
\end{array}$$

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

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

7. Groups

Let **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.

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

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

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

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.*

$$\textit{inverse\_operation} \in \text{monoid}\,\mathsf{T} \rightarrow\!\!\!\!\!\!+ \ \mathsf{T} \rightarrow\!\!\!\!\!\!+ \ \mathsf{T}$$

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

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

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

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

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.

$$
\begin{array}{|l}
\multicolumn{1}{l}{\textit{MapPreservesInverse}[\mathsf{t}, \mathsf{u}]} \\
f : \mathsf{t} \leftrightarrow \mathsf{u} \\
A : \mathrm{group}\, \mathsf{t} \\
B : \mathrm{group}\, \mathsf{u} \\
\hline
\textbf{let } (\_^{-1}) == \textit{inverse\_operation}\ A; \\
\quad (\_^{\dagger}) == \textit{inverse\_operation}\ B \bullet \\
\qquad \forall x : \mathsf{t} \bullet \\
\qquad\quad f(x^{-1}) = (f\ x)^{\dagger}
\end{array}
$$

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

$$
\begin{array}{|l}
\multicolumn{1}{l}{[\mathsf{t}, \mathsf{u}]} \\
\hom_{\mathrm{grp}} : \mathrm{group}\, \mathsf{t} \times \mathrm{group}\, \mathsf{u} \longrightarrow \mathbb{P}(\mathsf{t} \longrightarrow \mathsf{u}) \\
\hline
\hom_{\mathrm{grp}} = \\
\quad (\lambda\, A : \mathrm{group}\, \mathsf{t};\ B : \mathrm{group}\, \mathsf{u} \bullet \\
\qquad \{\, f : \hom_{\mathrm{mon}}(A, B) \mid \\
\qquad\quad \textit{MapPreservesInverse}[\mathsf{t}, \mathsf{u}] \,\})
\end{array}
$$

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 $\textit{bij}[\mathrm{t}]$ denote the set of a bijections $\mathsf{t} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathsf{t}$ from t to itself.

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

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

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

Remark. *Composition is associative.*

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

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

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

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

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

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.*

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

8. Abelian Groups

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

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

$BinaryOperation\_A[\mathsf{t}]$

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

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

$AbelianGroup\_A[\mathsf{t}]$

$Group\_A[\mathsf{t}]$

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

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

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

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 $\text{-}\,x$.

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

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

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