Groups

Arthur Ryman, `arthur.ryman@gmail.com`

June 25, 2022

Abstract

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

Contents

1 Introduction

Groups are ubiquitous throughout mathematics and physics. This article defines the basic algebraic objects related to groups and their homomorphisms.

2 Binary Operations

Let `t` be a set. We refer to the members of `t` as its *elements*. A *binary operation* on `t` is a function that maps pairs of elements to elements.

2.1 binop `\binop`

Let binop `t` denote the set of all binary operations on `t`.

$$\mathrm{binop}\,\mathtt{t} == \mathtt{t} \times \mathtt{t} \longrightarrow \mathtt{t}$$

2.2 Infix Operator Symbols $\times$ `\timesG`, $*$ `\mulG`, and $+$ `\addG`

The result of applying a binary operation to the pair of elements (x, y) is often denoted by an expression formed using an infix operator symbol, e.g. $x \times y$, $x * y$ or $x + y$.

2.3 *MapPerservesOperation*

Let `t` and `u` be sets and let A and B be binary operations on them. Let f be a function that maps `t` to `u`. The function f is said to *preserve the operations* if it maps the product of elements to the product of the mapped elements.

Let *MapPreservesOperation* denote this situation.

$$
\begin{array}{|l}
\hline
\textit{MapPreservesOperation}[\mathsf{t}, \mathsf{u}] \\
f : \mathsf{t} \longrightarrow \mathsf{u} \\
A : \mathrm{binop}\,\mathsf{t} \\
B : \mathrm{binop}\,\mathsf{u} \\
\hline
\mathbf{let}\ (\_ * \_) == A; (\_ \times \_) == B \bullet \\
\quad \forall x, y : \mathsf{t} \bullet \\
\quad\quad f(x * y) = (f\ x) \times (f\ y) \\
\hline
\end{array}
$$

2.4 $\hom_{\mathrm{op}}$ `\homBinOp`

A map that preserves operations is said to be an *operation homomorphism.*

Let A and B be binary operations. Let $\hom_{\mathrm{op}}(A, B)$ denote the set of operation homomorphisms from A to B.

$$
\begin{array}{|l}
\hline
[\mathsf{t}, \mathsf{u}] \\
\hom_{\mathrm{op}} : \mathrm{binop}\,\mathsf{t} \times \mathrm{binop}\,\mathsf{u} \longrightarrow \mathbb{P}(\mathsf{t} \longrightarrow \mathsf{u}) \\
\hline
\hom_{\mathrm{op}} = (\lambda A : \mathrm{binop}\,\mathsf{t}; B : \mathrm{binop}\,\mathsf{u} \bullet \\
\quad \{ f : \mathsf{t} \longrightarrow \mathsf{u} \mid \textit{MapPreservesOperation}[\mathsf{t}, \mathsf{u}] \}) \\
\hline
\end{array}
$$

Remark. *The identity map is an operation homomorphism.*

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

3 Semigroups

3.1 *OperationIsAssociative*

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

Let *OperationIsAssociative* denote this situation.

$$
\begin{array}{|l}
\hline
\textit{OperationIsAssociative}[\mathsf{t}] \\
A : \mathrm{binop}\,\mathsf{t} \\
\hline
\mathbf{let}\ (\_ * \_) == A \bullet \\
\quad \forall x, y, z : \mathsf{t} \bullet \\
\quad\quad (x * y) * z = x * (y * z) \\
\hline
\end{array}
$$

3.2 semigroup \semigroup

Let semigroup t denote the set of all semigroups on the set of elements t.

$$\text{semigroup}\,\mathsf{t} == \{\, A : \text{binop}\,\mathsf{t} \mid \mathit{OperationIsAssociative}[\mathsf{t}] \,\}$$

3.3 hom_{sg} \homSemigroup

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

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

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

$$\text{hom}_{\text{sg}} : \text{semigroup}\,\mathsf{t} \times \text{semigroup}\,\mathsf{u} \longrightarrow \mathbb{P}(\mathsf{t} \nrightarrow \mathsf{u})$$

$$\text{hom}_{\text{sg}} = (\lambda\, A : \text{semigroup}\,\mathsf{t};\ B : \text{semigroup}\,\mathsf{u} \bullet \text{hom}_{\text{op}}(A, B))$$

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

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

4 Monoids

4.1 *IdentityElement*

Let t be a set, let A be a binary operation over t, and let e be an element of t. The element e is said to be an *identity element* of A if left and right products with it leave all elements unchanged.

Let *IdentityElement* denote this situation.

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

$A : \text{binop}\,\mathsf{t}$

$e : \mathsf{t}$

$$\textbf{let } (\_ * \_) == A \bullet \forall\, x : \mathsf{t} \bullet e * x = x = x * e$$

4.2 *identity_element*

Let *identity_element* denote the relation that associates a binary operation one of its identity elements.

$$
\begin{array}{|l}
\hline
[\mathsf{t}] \\
\mathit{identity\_element} : \mathrm{binop}\,\mathsf{t} \leftrightarrow \mathsf{t} \\
\hline
\mathit{identity\_element} = \\
\quad \{\, \mathit{IdentityElement}[\mathsf{t}] \bullet A \mapsto e \,\} \\
\hline
\end{array}
$$

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

Proof. Let $*$ be a binary operation. Suppose e and e' are identity elements.

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

□

Remark. *Since identity elements are unique if they exist, the relation from binary operations to identity elements is a partial function.*

$$\mathit{identity\_element} \in \mathrm{binop}\,\mathsf{T} \rightarrowtail\!\!\!\!\!\!+\, \mathsf{T}$$

4.3 Identity Element Symbols 0 `\zeroG`, and 1 `\oneG`

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

4.4 monoid `\monoid`

Let `t` be a set of elements. A *monoid* over `t` is a semigroup over `t` that has an identity element.

Let monoid `t` denote the set of all monoids over `t`.

$$\mathrm{monoid}\,\mathsf{t} == \{\, A : \mathrm{semigroup}\,\mathsf{t} \mid \exists\, e : \mathsf{t} \bullet \mathit{IdentityElement}[\mathsf{t}] \,\}$$

4.5 *MapPreservesIdentity*

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.

Let *MapPreservesIdentity* denote this situation.

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

4.6 $\hom_{\mathrm{mon}}$ `\homMonoid`

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.*

5 Groups

5.1 *InverseOperation* and Postfix Operator symbol $^{-1}$ `\invG`

Let t be a set of elements and let A be a monoid on t. A function $inv \in \mathsf{t} \longrightarrow \mathsf{t}$ 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 expression x^{-1} is used to denote the inverse of x.

Let *InverseOperation* denote this situation.

$$
\begin{array}{|l}
\multicolumn{1}{l}{\underline{\quad \textit{InverseOperation}[\mathsf{t}] \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}} \\
A : \text{monoid}\,\mathsf{t} \\
\mathit{inv} : \mathsf{t} \longrightarrow \mathsf{t} \\
\hline
\textbf{let } (\_ * \_) == A; \\
\quad 1 == \mathit{identity\_element}\ A; \\
\quad (\_^{-1}) == \mathit{inv} \bullet \\
\qquad \forall\, x : \mathsf{t} \bullet \\
\qquad\quad x * x^{-1} = 1 = x^{-1} * x \\
\hline
\end{array}
$$

5.2 *inverse_operation*

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

$$
\begin{array}{|l}
\multicolumn{1}{l}{[\mathsf{t}]} \\
\mathit{inverse\_operation} : \text{monoid}\,\mathsf{t} \leftrightarrow \mathsf{t} \longrightarrow \mathsf{t} \\
\hline
\mathit{inverse\_operation} = \\
\quad \{\, \mathit{InverseOperation}[\mathsf{t}] \bullet A \mapsto \mathit{inv} \,\} \\
\hline
\end{array}
$$

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.

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

□

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

$$\mathit{inverse\_operation} \in \text{monoid}\,\mathsf{T} \rightarrowtail\!\!\!\!\!+\ \mathsf{T} \longrightarrow \mathsf{T}$$

5.3 group

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

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

$$\text{group}\,\mathsf{t} == \{\, A : \text{monoid}\,\mathsf{t} \mid \exists\, \mathit{inv} : \mathsf{t} \longrightarrow \mathsf{t} \bullet \mathit{InverseOperation}[\mathsf{t}] \,\}$$

5.4 *MapPreservesInverse*

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.

Let *MapPreservesInverse* denote this situation.

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

5.5 $\mathrm{hom}_{\mathrm{grp}}$ `\homGroup`

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 $\mathrm{hom}_{\mathrm{grp}}(A, B)$ denote the set of all group homomorphisms from A to B.

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

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

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

5.6 *bij*

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

$$
\begin{array}{|l}
\hline
[\mathsf{t}] \\
\textit{bij} : \mathbb{P}(\mathsf{t} \longrightarrow \mathsf{t}) \\
\hline
\textit{bij} = \mathsf{t} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathsf{t} \\
\hline
\end{array}
$$

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

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

Remark. *Composition is associative.*

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

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

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

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

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

5.7 *Bij*

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 this group.

$$[\mathsf{t}]$$

$$\mathit{Bij} : \mathit{bij}[\mathsf{t}] \times \mathit{bij}[\mathsf{t}] \longrightarrow \mathit{bij}[\mathsf{t}]$$

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

Example. *Let* T *be any non-empty set. The composition operation* $\mathit{Bij}[\mathsf{T}]$ *is a group over the set of bijections* $\mathit{bij}[\mathsf{T}]$ *from* T *to* T*.*

$$\mathsf{T} \neq \varnothing \Rightarrow \\ \quad \mathit{Bij}[\mathsf{T}] \in \mathrm{group}\, \mathit{bij}[\mathsf{T}]$$

6 Abelian Groups

6.1 OperationIsCommutative

Let $\mathtt{t}$ be a set of elements. A binary operation A over $\mathtt{t}$ is said to be *commutative* when the product of two elements doesn't depend on their order.

Let *OperationIsCommutative* denote this situation.

$$
\begin{array}{|l}
\multicolumn{1}{l}{\textit{OperationIsCommutative}[\mathtt{t}]} \\
A : \mathrm{binop}\,\mathtt{t} \\
\hline
\textbf{let}\ (\_ * \_) == A \bullet \\
\quad \forall\, x, y : \mathtt{t} \bullet \\
\qquad x * y = y * x \\
\hline
\end{array}
$$

6.2 abgroup `\abgroup`

An *Abelian group* is a group in which the binary operation is commutative. Let `t` be a set of elements.

Let abgroup `t` denote the set of all Abelian groups over `t`.

$$\mathrm{abgroup}\,\mathtt{t} == \{\, A : \mathrm{group}\,\mathtt{t} \mid \textit{OperationIsCommutative}[\mathtt{t}] \,\}$$

6.3 + `\addG`, 0 `\zeroG`, and - `\negG`

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.*

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