# Strictly Associative Group Theory using Univalence

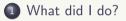
Alex Rice<sup>1</sup>

University of Cambridge

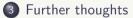
HoTT/UF 2023







### 2 How did I do it?



# Motivation

$$\begin{array}{l} \mathsf{InvUniqueLeft} : \forall \{\ell\} \ (\mathcal{G} : \mathsf{Group} \ \ell) \to \mathsf{Type} \ \ell \\ \mathsf{InvUniqueLeft} \ \mathcal{G} = \forall \ g \ h \to h \cdot g \equiv \mathsf{1g} \to h \equiv \mathsf{inv} \ g \\ & \mathsf{where} \\ & \mathsf{open} \ \mathsf{GroupStr} \ (\mathcal{G} \ \mathsf{.snd}) \end{array}$$

# Motivation

```
InvUniqueLeft : \forall \{\ell\} (\mathcal{G} : \text{Group } \ell) \rightarrow \text{Type } \ell
InvUniqueLeft \mathcal{G} = \forall g \ h \rightarrow h \cdot g \equiv 1 g \rightarrow h \equiv inv g
   where
   open GroupStr (\mathcal{G} .snd)
inv-unique-left : \forall \{\ell\} (\mathcal{G} : \text{Group } \ell) \rightarrow \text{InvUniqueLeft } \mathcal{G}
inv-unique-left \mathcal{G} g h p =
   h \equiv \langle \text{sym}(\cdot \text{IdR } h) \rangle
    h \cdot 1g \equiv ( \operatorname{cong} (h \cdot ) (\operatorname{sym} (\cdot \operatorname{InvR} g)) )
    h \cdot (g \cdot inv g) \equiv \langle Assoc h g (inv g) \rangle
    (h \cdot g) \cdot \text{inv } g \equiv \langle \text{ cong } (\_\cdot \text{ inv } g) p \rangle
    \lg \cdot \operatorname{inv} g \equiv \langle \operatorname{-IdL} (\operatorname{inv} g) \rangle
    inv g
               where
       open GroupStr (\mathcal{G} .snd)
```

What did I do? How did I do it? Further thoughts

# Motivation

```
InvUniqueLeft : \forall \{\ell\} (\mathcal{G} : \text{Group } \ell) \rightarrow \text{Type } \ell
InvUniqueLeft \mathcal{G} = \forall g \ h \rightarrow h \cdot g \equiv 1 g \rightarrow h \equiv inv g
   where
   open GroupStr (\mathcal{G} .snd)
inv-unique-left-strict : \forall \{\ell\} (\mathcal{G} : \text{Group } \ell) \rightarrow \text{InvUniqueLeft } \mathcal{G}
inv-unique-left-strict \mathcal{G} = strictify InvUniqueLeft
   \lambda \not e h \not p \rightarrow
       h \cdot 1g \equiv ( \operatorname{cong} (h \cdot ) (\operatorname{sym} (\cdot \operatorname{InvR} g)) )
       h \cdot g \cdot inv g \equiv (cong (-inv g)) p
       1g \cdot inv g \square
       where
          open GroupStr (RSymGroup \mathcal{G} .snd)
          open import Groups. Reasoning \mathcal{G} using (strictify)
```

# Strictify

 $\bullet$  Given a group  $\mathcal G,$  we create a new group RSymGroup  $\mathcal G.$ 

#### Theorem (Cayley's Theorem)

Every group is isomorphic to a subgroup of a symmetric group.

- In RSymGroup  $\mathcal{G}$ , various rules hold by reflexivity.
- We show that RSymGroup  $\mathcal{G}$  is isomorphic to  $\mathcal{G}$ .
- $\bullet$  By univalence and the structure identity principle, RSymGroup  ${\cal G}$  is equal to  ${\cal G}.$
- $\bullet$  The strictify function transports a proof from RSymGroup  ${\cal G}$  back to  ${\cal G}.$

In the strictified group the following equations hold definitionally:

- a(bc) = (ab)c,
- a1 = a = 1a,
- $a^{-1-1} = a$ ,
- and  $(fg)^{-1} = g^{-1} \cdot f^{-1}$ .

## Functions compose strictly

### Theorem (Cayley's Theorem)

Every group is isomorphic to a subgroup of a symmetric group.

## Functions compose strictly

### Theorem (Cayley's Theorem)

Every group is isomorphic to a subgroup of a symmetric group.

$$\_\circ\_: (f : B \to C) \to (g : A \to B) \to (A \to C)$$
  
 $(f \circ g) x = f (g x)$ 

$$\begin{array}{rl} \mathsf{comp-assoc} : & (f: \ C \to D) \\ & \to (g: \ B \to C) \\ & \to (h: \ A \to B) \\ & \to f \circ (g \circ h) \equiv (f \circ g) \circ h \end{array}$$
$$\begin{array}{r} \mathsf{comp-assoc} \ f \ g \ h = \mathsf{refl} \end{array}$$

# Do invertible functions compose strictly?

```
record Inverse (A : Type) (B : Type) : Type where
field

\uparrow : A \rightarrow B

\downarrow : B \rightarrow A

\varepsilon : \forall x \rightarrow \downarrow (\uparrow x) \equiv x

\eta : \forall y \rightarrow \uparrow (\downarrow y) \equiv y
```

# Strict invertible functions

record Inverse (A : Type) (B : Type) : Type where
constructor [_,_,_]
field
$\uparrow: A  ightarrow B$
$\downarrow:B\to A$
$arepsilon: orall \ b \ \{x\}  ightarrow x \equiv \downarrow \ b  ightarrow \uparrow x \equiv b$
$\eta: orall a \left\{y ight\}  ightarrow y \equiv \uparrow a  ightarrow \downarrow y \equiv a$
_o_ : Inverse $B \ C  ightarrow$ Inverse $A \ B  ightarrow$ Inverse $A \ C$
_o_ $\lfloor$ $f$ , $g$ , $p$ , $q$ $\rfloor$ $\lfloor$ $f'$ , $g'$ , $p'$ , $q'$ $\rfloor$ $=$
$ig \ (\lambda \; x  o f \; (f' \; x))$ ,
$(\lambda  {m y}  ightarrow {m g}^{\prime}  ({m g}  {m y}))$ ,
$(\lambda  b  r  ightarrow p  b  (p'  (g  b)  r))$ ,
$(\lambda \; a \; r  o q' \; a \; (q \; (f' \; a) \; r)) \; ig ]$

## Strict invertible functions

```
assoc : (f : Inverse \ C \ D)
        \rightarrow (g : Inverse B C)
        \rightarrow (h : Inverse A B)
        \rightarrow f \circ (g \circ h) \equiv (f \circ g) \circ h
assoc f g h = refl
id-inv: Inverse A A
id-inv = |(\lambda x \rightarrow x), (\lambda x \rightarrow x)|
               (\lambda \ b \ r \rightarrow r), (\lambda \ a \ r \rightarrow r)
id-unit-left : (f : Inverse A B)
                \rightarrow id-inv \circ f = f
id-unit-left f = refl
id-unit-right : (f : Inverse \ A \ B)
                  \rightarrow f \circ id - inv = f
id-unit-right f = refl
```

## Strict invertible functions

```
inv-inv \cdot Inverse A B \rightarrow Inverse B A
inv-inv |f, g, \varepsilon, \eta| = |g, f, \eta, \varepsilon|
inv-involution : (f : Inverse A B)
                 \rightarrow inv-inv (inv-inv f) \equiv f
inv-involution f = refl
inv-comp : (f : Inverse B C)
            \rightarrow (g : Inverse A B)
            \rightarrow inv-inv (f \circ g) \equiv inv-inv g \circ inv-inv f
inv-comp f g = refl
```

### Representable functions

The map  $\iota : g \mapsto g \cdot _{-}$  includes the group  $\mathcal{G}$  in the symmetric group. We now want to restrict the symmetric group to those functions that are in the image of  $\iota$ .

#### Proposition

A function  $f : \mathcal{G} \to \mathcal{G}$  is in the image of  $\iota$  if and only if for all  $g, h \in \mathcal{G}$ ,  $f(g \cdot h) = f(g) \cdot h$ .

### Representable functions

The map  $\iota : g \mapsto g \cdot _{-}$  includes the group  $\mathcal{G}$  in the symmetric group. We now want to restrict the symmetric group to those functions that are in the image of  $\iota$ .

#### Proposition

A function  $f : \mathcal{G} \to \mathcal{G}$  is in the image of  $\iota$  if and only if for all  $g, h \in \mathcal{G}$ ,  $f(g \cdot h) = f(g) \cdot h$ .

Representable : Inverse  $\langle \mathcal{G} \rangle \langle \mathcal{G} \rangle \rightarrow \text{Type}$ Representable  $f = \forall x \ g \ h \rightarrow x \equiv g \cdot h \rightarrow \uparrow f \ x \equiv \uparrow f \ g \cdot h$ 

 $\begin{array}{l} \mathsf{Repr} : \mathsf{Type} \\ \mathsf{Repr} = \Sigma[ \ f \in \mathsf{Inverse} \ \langle \ \mathcal{G} \ \rangle \ \langle \ \mathcal{G} \ \rangle \ ] \ \mathsf{Representable} \ f \end{array}$ 

## Representable symmetric group

• Let RSymGroup  $\mathcal{G}$  be the subgroup of the symmetric group on  $\mathcal{G}$  consisting of those functions that are representable.

- Let RSymGroup  $\mathcal{G}$  be the subgroup of the symmetric group on  $\mathcal{G}$  consisting of those functions that are representable.
- This subgroup still has strict composition.

- Let RSymGroup G be the subgroup of the symmetric group on G consisting of those functions that are representable.
- This subgroup still has strict composition.
- The inclusion  $\iota$  is an isomorphism from  $\mathcal{G}$  to the representable symmetric group.

- Let RSymGroup  $\mathcal{G}$  be the subgroup of the symmetric group on  $\mathcal{G}$  consisting of those functions that are representable.
- This subgroup still has strict composition.
- The inclusion  $\iota$  is an isomorphism from  $\mathcal G$  to the representable symmetric group.
- By univalence we get an equality:

 $\iota \equiv \mathcal{G} : \mathcal{G} \equiv \mathsf{RSymGroup} \ \mathcal{G}$ 

- Let RSymGroup  $\mathcal{G}$  be the subgroup of the symmetric group on  $\mathcal{G}$  consisting of those functions that are representable.
- This subgroup still has strict composition.
- $\bullet$  The inclusion  $\iota$  is an isomorphism from  ${\cal G}$  to the representable symmetric group.
- By univalence we get an equality:

 $\iota \equiv \mathcal{G}: \mathcal{G} \equiv \mathsf{RSymGroup}\ \mathcal{G}$ 

• This lets us define:

# Further thoughts

# Further thoughts

#### Does this all work with categories instead of groups?

# Conclusion

- For each group  $\mathcal{G}$  we can generate an isomorphic group RSymGroup  $\mathcal{G}$ .
- This group has nice definitional properties
- Univalence allows us to generate an equality between the two groups.
- This allows us to prove theorems about an arbitrary group by instead proving them on the strictified group.
- https://alexarice.github.io/posts/sgtuf/Strict-Group-Theory-UF.html