Permutations of 4 objects

A permutation of the 4 objects is an "action"

α_1 : $A \to B$, $B \to A$, $C \to D$, $D \to C$

α_2 : $A \to B$, $B \to C$, $C \to A$, $D \to D$

Combining permutations

$\alpha_2 \circ \alpha_1$: $A \to C$, $B \to B$, $C \to D$, $D \to A$

Properties

- "Closure" any combination of doing two "actions" give an "action"
- Combining actions is not ambiguous (ie $(a \circ b) \circ c = a \circ (b \circ c)$)
- "Identity action" is an action that doesn't do anything
- Every action has an "inverse" action

Rubik cube

An action is any number of rotations counterclockwise in one or several of 6 directions.

Integers

The set of which can be combined by adding them.

Actions → integers   Composition → adding

Groups

Let G be a set and $*$ a function that combines an ordered pair of elements of G, $a * b$. We say that $(G, *)$ is a group if the 4 properties hold.

- Closure: $\forall a, b \in G, \quad a * b \in G$
- Associativity: $\forall a, b, c \in G, \quad (a * b) * c = a * (b * c)$
- Identity: $\exists e \in G$ s.t. $\forall a \in G \quad a * e = e * a = a$
- Inverse: $\forall a \in G \quad \exists a' \in G$ s.t. $a * a' = a' * a = e$

Identifying Groups

- $(\mathbb{Z}, +)$ Group
- $(\mathbb{Z}, \times)$ Not a group, fails at "inverse"
- (all integers except 0, $\times$) Not a group, fails at "inverse"
- $(\mathbb{Q}, \times)$ Not a group, fails at "inverse"
- (all rational except 0, $\times$) Group
- $(\mathbb{Z}^+, -)$ Not a group, fails at "closure"
- $(\mathbb{R}^+, +)$ Not a group, fails at "identity"
- $(\mathbb{R}, *)$ Not a group, fails at "associativity"

  $x * y = xy + 1$

General Linear Group - $GL(n, \mathbb{R})$

- Let G be the set of $n \times n$ matrices with real entries and with with non-zero determinand. Operation is matrix multiplication.

Closure : $\underset{n\times n}{A} \cdot \underset{n\times n}{B} = \underset{n\times n}{AB}$ $\qquad \underset{\neq 0}{\det(AB)} = \underset{\neq 0}{\det(A)} \cdot \underset{\neq 0}{\det(B)}$ ✓

Associativity : $(AB)C = A(BC)$ ✓

Identity : Identity matrix $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$ $I \cdot A = A$, $A \cdot I = A$ ✓

$\det(I) = 1$, $\therefore I \in G$

Inverse : let $A \in G$, s.t. $\det(A) \neq 0$ so A' exists

A' is $n \times n$, real entries and $\det(A') = \frac{1}{\det(A)} \neq 0$

So $A' \in G$

$A \cdot A' = A' \cdot A = I$

Symbol example

Let $G = \{ ☾ , \square \}$ and $\ast$ is given by

$\ast$	☾	$\square$
☾	☾	$\square$
$\square$	$\square$	☾

- Closure ✓
- Associativity ✓
- Identity : ☾ is identity ✓
- Inverse : ☾$'$ = ☾

  $\square' = \square$ ✓

$\square \ast \underset{\square'}{\square} = ☾$

$\underset{\square'}{\square} \ast \square = ☾$

- See page 44-49 for more examples
- If $\ast$ is understood or not important we often write ab instead of $a \ast b$

Abelian

A group G such that $ab = ba$ for all $a, b \in G$ is called Abelian

All others are called non-Abelian

- $(\mathbb{Q}^*, \times)$ is abelian
- $GL(n, \mathbb{R})$ is non-Abelian

Theorem 1

In any group G there is only one identity element (ie it is unique)

Proof by contradiction

Suppose that there are two identities, e_1 and e_2

Then $e_1 * a = a * e_1 = a \quad \forall a \in G$

$e_2 * a = a * e_2 = a \quad \forall a \in G$