Group Theory

Peter Rowlett

Sheffield Hallam University

p.rowlett@shu.ac.uk

Starter: The Number Fancy Dress Party

All the natural numbers have come to a party in fancy dress costume. They all know themselves which costume everyone is wearing, but you don't know.

If you pick any two of them and ask them to combine with $+$, $-$, $\times$ or $\div$, they will point out which costume is the correct answer, and they'll happily do it as often as you want. For example, you might ask for hamburger $+$ bear and they will point to unicorn. (If the answer isn't at the party, they'll tell you that too.)

How can you correctly identify the numbers 0, 1, 2 and 3? How do you do it in as few steps as possible?

Binary operation

Recall that we defined $(G, \circ)$ as a set G and a binary operation on that set, $\circ$.

Remember that the definition of a binary operation tells us that $(G, \circ)$ has **closure**.

- **Closure**: $\forall a, b \in G \ (a \circ b \in G)$.

Group

If $(G, \circ)$ satisfies the following, then it is called a *group*.

- **Associativity**: $\forall a, b, c \in G \ (a \circ (b \circ c) = (a \circ b) \circ c)$.
- **Identity**: $\exists e \in G \ \forall a \in G \ (e \circ a = a \circ e = a)$.
- **Inverse**: $\forall a \in G \ \exists b \in G \ (a \circ b = b \circ a = e)$

Abelian group

If $(G, \circ)$ is a group that also satisfies commutativity, it is called an *Abelian group*.

- **Commutativity**: $\forall a, b \in G \ (a \circ b = b \circ a)$.

Algebraic structures that are not groups

- If $(G, \circ)$ satisfies closure but none of the other properties, it is called a *magma*, or sometimes a *groupoid*.
- If $(G, \circ)$ satisfies closure and associativity only, it is a *semi-group*.
- If $(G, \circ)$ satisfies closure, associativity, and has an identity, it is a *monoid*.

Coins game

- Position two coins in a row, one on the left and one on the right. The following operations may be performed on them:

l: flip over the left-hand coin;

r: flip over the right-hand coin;

b: flip over both coins.

- Let $a \circ b$ denote doing operation a then operation b.
- Do $a \circ b$ and $b \circ a$ give the same result for all operations here?
- How can we get from HH to TT? Is there more than one way?
- Are there changes that are impossible?
- Is it always possible to undo a change?

Coins game

- For a set of operations $C = \{e, l, r, b\}$ and an operation $\circ$, we can form a table of outcomes:

	e	l	r	b
e	e	l	r	b
l	l	e	b	r
r	r	b	e	l
b	b	r	l	e

- Does $(C, \circ)$ form a group?

Coins game

- For a set of operations $C = \{e, l, r, b\}$ and an operation $\circ$, we can form a table of outcomes:

$\circ$	e	l	r	b
e	e	l	r	b
l	l	e	b	r
r	r	b	e	l
b	b	r	l	e

- We have closure – every combination forms an element in the group.

Coins game

- For a set of operations $C = \{e, l, r, b\}$ and an operation $\circ$, we can form a table of outcomes:

	e	l	r	b
e	e	l	r	b
l	l	e	b	r
r	r	b	e	l
b	b	r	l	e

- Identity, e.

Coins game

- For a set of operations $C = \{e, l, r, b\}$ and an operation $\circ$, we can form a table of outcomes:

	e	l	r	b
e	e	l	r	b
l	l	e	b	r
r	r	b	e	l
b	b	r	l	e

- Inverse: each element is its own inverse, e.g. $l \circ l = e$.

Coins game

- For a set of operations $C = \{e, l, r, b\}$ and an operation $\circ$, we can form a table of outcomes:

	e	l	r	b
e	e	l	r	b
l	l	e	b	r
r	r	b	e	l
b	b	r	l	e

- Associativity is a bit of a nuisance to demonstrate.

Associativity

- Any $(a \circ b) \circ c$ or $a \circ (b \circ c)$ that involves the identity is associative.

$$(e \circ a) \circ b = a \circ b = e \circ (a \circ b);$$
$$(a \circ e) \circ b = a \circ b = a \circ (e \circ b);$$
$$(a \circ b) \circ e = a \circ b = a \circ (b \circ e).$$

Associativity

$(a \circ b) \circ c$:

	l	r	b
$l \circ l = e$	l	r	b
$l \circ r = b$	r	l	e
$l \circ b = r$	b	e	l
$r \circ l = b$	r	l	e
$r \circ r = e$	l	r	b
$r \circ b = l$	e	b	r
$b \circ l = r$	b	e	l
$b \circ r = l$	e	b	r
$b \circ b = e$	l	r	b

$a \circ (b \circ c)$:

	$l \circ l = e$	$l \circ r = b$	$l \circ b = r$	$r \circ l = b$	$r \circ r = e$	$r \circ b = l$	$b \circ l = r$	$b \circ r = l$	$b \circ b = e$
l	l	r	b	r	l	e	b	e	l
r	r	l	e	l	r	b	e	b	r
b	b	e	l	e	b	r	l	r	b

- Since one table is the transpose of the other, we see that we have associativity.

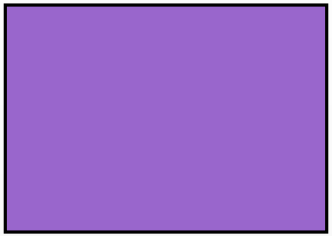
Coins game group

- $(C, \circ)$:

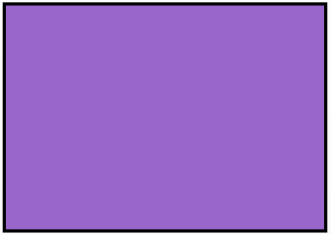
	e	l	r	b
e	e	l	r	b
l	l	e	b	r
r	r	b	e	l
b	b	r	l	e

- Since we have confirmed closure and established that we have an associative operation with identity and inverses, $(C, \circ)$ is a group.
- Actually, since we have commutativity, it is an Abelian group.

- What symmetry operations can I perform on a rectangle like this?
- These are things I can do that leave it within the same outline.

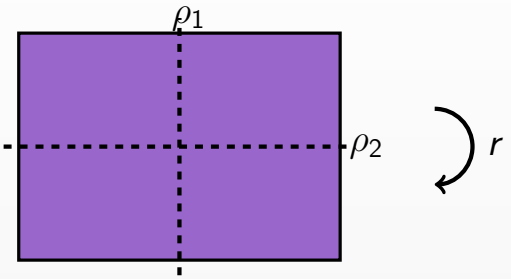


- What symmetry operations can I perform on a rectangle like this?
- These are things I can do that leave it within the same outline.



- Do nothing;
- Rotate by 180°;
- reflect in the vertical mirror line;
- reflect in the horizontal mirror line.

- What symmetry operations can I perform on a rectangle like this?
- These are things I can do that leave it within the same outline.



- Do nothing (e);
- Rotate by 180° (r);
- reflect in the vertical mirror line (ρ_1);
- reflect in the horizontal mirror line (ρ_2).

- Addition modulo 4 on $\{0, 1, 2, 3\}$.
- Symmetries of the rectangle e, r, ρ_1, ρ_2 with the operation $a \circ b$ meaning perform a and then perform b on the result.

- Addition modulo 4 on $\{0, 1, 2, 3\}$.

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- Symmetries of the rectangle e, r, ρ_1, ρ_2 with the operation $a \circ b$ meaning perform a and then perform b on the result.

- Addition modulo 4 on $\{0, 1, 2, 3\}$.

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- Symmetries of the rectangle e, r, ρ_1, ρ_2 with the operation $a \circ b$ meaning perform a and then perform b on the result.

	e	r	ρ_1	ρ_2
e	e	r	ρ_1	ρ_2
r	r	e	ρ_2	ρ_1
ρ_1	ρ_1	ρ_2	e	r
ρ_2	ρ_2	ρ_1	r	e

Order of an element

- For a group with identity e, the *order* of an element a is the smallest positive integer power of a such that $a^n = e$.

- For example, consider the table for multiplication modulo 5 on $\{1, 2, 3, 4\}$.

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

- Order of 2:
  - $2^1 = 2$;
  - $2^2 = 4$;
  - $2^3 = 3$;
  - $2^4 = 1$.

  So the order of 2 is 4.
- Order of 4:
  - $4^1 = 1$.

  So the order of 4 is 1.

Generators

- In the previous example, we could express every element as a power of 2 and so 2 is called a *generator* for this group.
- A group with a generator is called a *cyclic group*.

Generators

- If g is a generator for a group and $g^n = e$, then we can draw a general group table.

	e	g	g^2	g^3	$\dots$	g^{n-2}	g^{n-1}
e	e	g	g^2	g^3	$\dots$	g^{n-2}	g^{n-1}
g	g	g^2	g^3	g^4	$\dots$	g^{n-1}	e
g^2	g^2	g^3	g^4	g^5	$\dots$	e	g
g^3	g^3	g^4	g^5	g^6	$\dots$	g	g^2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
g^{n-2}	g^{n-2}	g^{n-1}	e	g	$\dots$	g^{n-4}	g^{n-3}
g^{n-1}	g^{n-1}	e	g	g^2	$\dots$	g^{n-3}	g^{n-2}

Subgroups

- A *subgroup* of a group $(G, \circ)$ is some $H \subseteq G$ such that $(H, \circ)$ forms a group in its own right.
- You need to check for closure, an identity and whether each element has an inverse.
- You do not need to check for associativity.