Group Theory (uh oh)

Symmetries: A symmetry of an object is a transformation which leaves the object unchanged

e.g. the graph of cosx

Is symmetric under reflection $x \to -x$

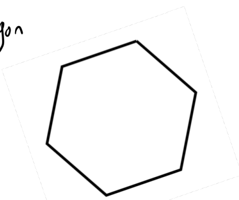
and translation $x \to x + 2\pi$

A circle is symmetric under an arbitrary rotation about its centre

= continuous symmetry

Rotation by any angle is a symmetry of the circle.

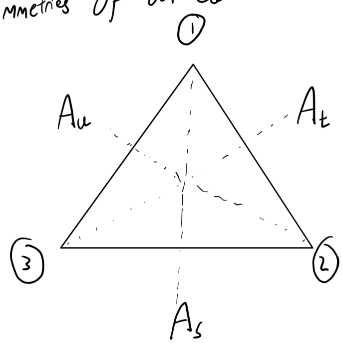
A hexagon



Rotation by angle $\frac{\pi}{3}, \frac{2\pi}{3}, \ldots$ is a symmetry

Reflection in different axes is also a symmetry

- Symmetries of an equilateral triangle



Symmetries?

- r = rotate by $\frac{2\pi}{3}$ clockwise

$r({}^{1}_{3}\triangle_{2}) = {}^{3}_{2}\triangle_{1}$

- r^2 = rotate by $\frac{4\pi}{3}$ clockwise = r twice

$r(r({}^{1}_{3}\triangle_{2})) = r^2({}^{1}_{3}\triangle_{2}) = {}^{2}_{1}\triangle_{3}$

- r^3 = rotate by 2π = do nothing

We call this the identity transformation, id

$$r^3 = id$$

- s = reflection in A_s

$$s\left({}_{3}\overset{1}{\triangle}_{2}\right) = {}_{2}\overset{1}{\triangle}_{3}$$

- t = reflection in A_t

$$t\left({}_{3}\overset{1}{\triangle}_{2}\right) = {}_{3}\overset{2}{\triangle}_{1}$$

- u = reflection in A_u

$$u\left({}_{3}\overset{1}{\triangle}_{2}\right) = {}_{1}\overset{3}{\triangle}_{2}$$

We have found 6 symmetries of the triangle.

Relations between symmetries

e.g. do r then do s

$$sr\left({}_{3}\overset{1}{\triangle}_{2}\right) = s\left({}_{2}\overset{3}{\triangle}_{1}\right) = \left({}_{1}\overset{3}{\triangle}_{2}\right) = u\left({}_{3}\overset{1}{\triangle}_{2}\right)$$

So we can write this as $sr = u$.

In fact all 6 transformations can be generated from just s and r

e.g. $rs\left({}_{3}\overset{1}{\triangle}_{2}\right) = r\left({}_{2}\overset{1}{\triangle}_{3}\right) = {}_{3}\overset{2}{\triangle}_{1} = t\left({}_{3}\overset{1}{\triangle}_{2}\right)$

The group of symmetries of the equilateral triangle is:

$$(id, r, s, r^2, rs, sr) \qquad (s^2 = id = r^3)$$

What if I do rs followed by sr?

$$rssr = rs^2r = r\,id\,r = r^2$$

The six symmetries of the triangle form a group, called the Dihedral Group D_3

It satisfies the following properties:

- If I do one transformation then another, I get a third transformation (within this group)
- There is an identity transformation - "do nothing" = id
  satisfies $r\,id = r = id\,r$
- every element of D_3 has an inverse - something we compose with it to get the identity
  e.g. inverse of r is r^2

$r^2(r) = r^3 = id$

Group Definition

Roughly: a group is a collection of 'things', e.g. symmetry transformations, numbers, functions, matrices etc, where we can combine two of them to get a third. There is always an 'identity thing' and each thing has an 'inverse thing'.

Definition: A group G consists of a set of elements $\{x, y, \dots\}$ and a binary operation $*$ $x * y$ satisfying axioms of group theory:

1. Closure - for any two elements x, y in the group $x * y$ is also in the group.
2. Associativity - for any three elements $x, y, z \in G$ we have $x*(y*z) = (x*y)*z$
3. Identity - There exists an identity element $e \in G$ such that $e * x = x * e = x$ for any $x \in G$
4. Inverse - For every $x \in G$ there exists an inverse $y \in G$ such that $y * x = x * y = e$

Sometimes call the inverse of x x^{-1} but this can cause confusion.

$*$ = binary operation $\Rightarrow$ a way of combining two elements, producing a third

$x * y$ need not equal $y * x$

Examples

- The set of integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ is a group if we make the binary operation, $*$ = ordinary addition, $+$

  Proof: need to check the 4 conditions

  1. Closure - for any $a, b \in \mathbb{Z}$, $a+b \in \mathbb{Z}$ (e.g. $3+(-7) = -4 \in \mathbb{Z}$)
  2. Associativity - for any $a, b, c \in \mathbb{Z}$, $a+(b+c) = (a+b)+c$
  3. Identity - There's an identity element, $e = 0 \Rightarrow a + 0 = 0 + a = a$ for any $a \in \mathbb{Z}$
  4. Inverses - for every $a \in \mathbb{Z}$ there is an inverse in $\mathbb{Z}$, namely $-a$, since $a + (-a) = 0 = e$

- What about $\mathbb{Z}$ with $*$ = ordinary multiplication, $\times$?

  1. Closure - for any $a, b \in \mathbb{Z}$ $a \times b \in \mathbb{Z}$
  2. Associativity - for any $a, b, c \in \mathbb{Z}$ $a \times (b \times c) = (a \times b) \times c$
  3. Identity - $e = 1$ satisfies $a \times 1 = 1 \times a = a$ for all $a \in \mathbb{Z}$
  4. Inverses - For any a $\exists b$ s.t. $ab = 1$ $\Rightarrow$ not true
     e.g. if $a = 2$ then there is no $b \in \mathbb{Z}$ s.t. $a \times b = b \times a = 1$

$\therefore$ not a group

- Consider the set of rational numbers $\mathbb{Q} = \{ \frac{a}{b}, a,b \in \mathbb{Z}, b \neq 0 \}$?

This forms a group under addition

What about multiplication?

Axioms 1-3 hold as with $\mathbb{Z}$.

4. Inverses : for any a, $\exists\, b$ s.t. $ab = 1$ $\rightarrow$ not true for $a = 0$

no b exists s.t. $0 \times b = 1$

But $\mathbb{Q}^{\times} = \mathbb{Q} \setminus \{0\}$ IS a group under multiplication ☺

- Inverse of $\frac{a}{b} = \frac{b}{a} \in \mathbb{Q}^{\times}$

$\mathbb{Q}$ with 0 removed

<u>Note</u>

$\mathbb{R}$ and $\mathbb{C}$ are groups under addition

$\mathbb{R}^{\times}$ and $\mathbb{C}^{\times}$ are both groups under multiplication

Proofs same as with $\mathbb{Z}$ and $\mathbb{Q}^{\times}$

<u>Example</u> The set of complex numbers $z \in \mathbb{C}$ with $|z| = 1$ is a group under multiplication

<u>Proof</u>: 1. Closure - If $|z| = 1$, $|w| = 1$ for any $z, w \in \mathbb{Z}$ then $|zw| = 1$ Since $|zw| = |z||w| = 1 \times 1 = 1$

2. Associativity - True for all $\mathbb{C}$

3. Identity - is $1 \rightarrow 1$ is in the group Since $|1| = 1$

and $z \times 1 = 1 \times z = z$ for all z

4. Inverse - for any z with $|z| = 1$, $\frac{1}{z} \times z = z \times \frac{1}{z} = 1 = e$

and $\left|\frac{1}{z}\right| = \frac{1}{|z|} = \frac{1}{1} = 1 \rightarrow$ is in the group

$\therefore z^{-1} = \frac{1}{z}$

This is sometimes called the <u>circle group</u>

$$S^1 = \{ z \in \mathbb{C} : |z| = 1 \} = \{ e^{i\theta} : 0 \leq \theta < 2\pi \}$$

Looks like addition of angles, since $e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1 + \theta_2)}$

This group is also known as $U(1)$

Note - we do not require $x \circ y = y \circ x$ (Commutativity) for all $x, y \in G$. This is true for most examples above though. $\rightarrow$ was not the case for D_3 (triangles).

<u>Definition</u> - two elements x, y in a group are said to commute if $x \circ y = y \circ x$. If all pairs of elements commute, the group is called an abelian group.

<u>Abelian groups</u>

so:

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with $\circ = +$
- $\mathbb{Q}^{\times}, \mathbb{R}^{\times}, \mathbb{C}^{\times}$ with $\circ = \times$
- $U(1)$ (circle group) $e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1 + \theta_2)} = e^{i\theta_2} e^{i\theta_1}$

are all abelian groups.

But D_3 is not an abelian group.

Non-examples of groups

1. $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ with $\bullet = +$ is not a group
   - It is closed $\to$ If $a, b \in \mathbb{N}$, $a+b \in \mathbb{N}$
   - It is associative $a+(b+c) = (a+b)+c$
   - It has an identity, $e = 0$ $\to$ $a+0 = 0+a = a$ for all $a \in \mathbb{N}$
   - But we do not have inverse, eg inverse of 1?

     $a+1 = 1+a = 0$

     no a exists in $\mathbb{N}$

     $\therefore$ not a group.

2. $\mathbb{Z}$ with Subtraction $\to$ $\bullet = -$
   - It is closed $\to$ If $a, b \in \mathbb{Z}$, $a-b \in \mathbb{Z}$
   - Associativity $a-(b-c)$ $(a-b)-c$

     $= a-b+c \neq a-b-c$
   - No identity - need $a-e = e-a = a$ for all $a \in \mathbb{Z}$

     $e=0$ does not satisfy this one

3. $\mathbb{Z}$ with $a \bullet b = \frac{a}{b}$ Satisfies None of the axioms

More examples of groups

Finite Cyclic groups

Modulo arithmetic: Given $n \in \mathbb{N}, n \geq 1$ and $a \in \mathbb{Z}$, there is a remainder r between 0 and $n-1$ if we divide a by n. We write $a \pmod{n}$ for this remainder.

$17 \pmod 3 = 2$ (Since $17 = 3 \times 5 + \underset{\text{omg remainder}}{2}$)

$27 \pmod 5 = 2$

$57 \pmod 7 = 1$

We call this group $\mathbb{Z}/n = \{0, 1, 2, \dots, n-1\}$, with $\bullet =$ addition modulo n

i.e. $a \bullet b = (a+b) \bmod n$

This is called the cyclic group of order n

Definition - a finite group with n elements is said to have order n

Check if a group
- Closed - $a \bullet b = (a+b) \bmod n$ is in $\mathbb{Z}/n$
- Associativity - $a \bullet b \bullet c = (a+(b+c)) \bmod n = ((a+b)+c) \bmod n$
- Identity - $a \bullet 0 = 0 \bullet a = (a+0) \bmod n = a$
- Inverse - need b s.t. $a+b = 0 \bmod n$ $\to$ b is the inverse here

  $b = n-a$ Since $a+(n-a) = n$, $n \bmod n = 0$

Called a Cyclic group Since you cycle around e.g $\mathbb{Z}/4 \; + \; 0,\; 0+1=1,\; 1+1=2,\; 2+1=3,\; 3+1=0$

Group table

For small finite groups it is useful to lay all the info via a group table. Just list all elements, a, of the group on the LHS and all elements, b, of the group along the top. Write $a \bullet b$ in the relevant space of the table

e.g. for $\mathbb{Z}/4$

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

abelian groups symmetrical across this axis

Consider group table for $D_3 = \{id, r, r^2, s, t, u\}$

$\bullet$	id	r	r^2	s	t	u
id	id	r	r^2	s	t	u
r	r	r^2	id	u	s	t
r^2	r^2	id	r	t	u	s
s	s	t	u	id	r	r^2
t	t	u	s	r	id	r
u	u	s	t	r	r^2	id

etc.

Not symmetric
$\therefore$ non-abelian

- much simpler way to convey all info about this group:
  (recall we can generate all elements using just r and s)
  $D_3 = \{r, s \mid r^3 = id,\; s^2 = id,\; srs = r^{-1}\}$
- Can generalise to D_n: (D = Dihedral group)
  $D_n = \{r, s \mid r^n = id,\; s^2 = id,\; srs = r^{-1}\}$

Symmetries of a regular n-gon.

r is a $\frac{2\pi}{n}$ clockwise rotation through the centre
s is a reflection

Subgroups

If there is a group sitting inside another group, it is called a subgroup.

Definition

Let G be a group with binary operation $\bullet$. Then H is called a subgroup of G if H is a subset of G and H is also a group with $\bullet$.

To check H is a subgroup:

- Associativity is auto $\to$ If $a\bullet(b\bullet c) = (a\bullet b)\bullet c$ for all $a,b,c \in G$ then $a\bullet(b\bullet c) = (a\bullet b)\bullet c$ for all $a,b,c \in H$

  i.e. do not need to check this.

- Do need to check the other 3 axioms for H.
  - Closure - need $x \bullet y \in H$ for all $x,y \in H$.
  - Identity - need $e \in H$
  - Inverses - If $x \in H$, need $x^{-1} \in H$.

Examples

1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

   Subsets (not subgroups as no operation)

   $\to$ all are groups under $\bullet = +$

   $\therefore$ are all subgroups

2. $\underbrace{\mathbb{Q}^\times \subset \mathbb{R}^\times \subset \mathbb{C}^\times}_{\text{Removed } 0}$ all are groups under $\bullet = \times$

   So $\mathbb{Q}^\times$ is a subgroup of $\mathbb{R}^\times$ and $\mathbb{C}^\times$

   $\mathbb{R}^\times$ is a subgroup of $\mathbb{C}^\times$

   already proved this is a group in previous lecture.

3. The circle group $\{z \in \mathbb{C} : |z| = 1\}$ with $\bullet = \times$

   is a subgroup of $\mathbb{C}^\times$ with $\bullet = \times$

4. D_3 (= Symmetries of equilateral Triangle) is a subgroup of D_6 (= Symmetries of a regular hexagon)

5. The subset $\{id, r, r^2, \dots, r^{n-1}\} \subset D_n = \{id, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$

   and is also a group $\to$ this is the group of rotational symmetries of an n-gon.

   Check: Closure $\to$ $r^k r^l = r^{k+l} \in$ Subset

   Identity: $id \in$ Subset

   Inverse: If $r^k \in$ Subset, $r^{n-k} \in$ Subset and $r^k r^{n-k} = r^n = id$

6. Even integers $\{0, \pm 2, \pm 4, \dots\}$ are a subgroup of $\mathbb{Z}$ under $+$.

Closed ✓ even + even = even
Identity ✓ 0
Inverse ✓ negatives

(all integers divisible by $n \in \mathbb{Z}$ are also subgroups under +)

7. Arbitrary rotations in 3D form a group
Rotations around the z axis form a subgroup. This can be done using matrices.
also any other axis.

Maps between groups

Definition Let G be a group with operation $\bullet_G$ and H another group with operation $\bullet_H$
Then a function $\varphi : G \to H$ is called a homomorphism if

$$\varphi(x \bullet_G y) = \varphi(x) \bullet_H \varphi(y)$$

If G, H have the same order and there is a unique map for each element (bijection) then it is called an isomorphism.
num of elements
i.e. they are the same group.

2 groups that have an isomorphism are called isomorphic.

Example - rotations of an n-gon are isomorphic to cyclic group $\mathbb{Z}/_n$ of order n
after doing n rotations it resets - similar to → modulo stuff → resets after adding n

The map from $G = \{id, r, r^2, \ldots, r^{n-1}\}$ to $H = \{0, 1, 2, \ldots, n-1 \text{ mod } n\}$
is simply $\varphi(r^k) = k$
Then: $\varphi(r^k r^{k'}) = \varphi(r^{k+k'}) = k+k' = \varphi(r^k) + \varphi(r^{k'})$
So $\varphi(a \bullet_G b) = \varphi(a) \bullet_H \varphi(b)$