Def. A concrete group on a set X is a set G of bijections $X \to X$ such that

(i) $id_X \in G$

(ii) if $f \in G$, then $f^{-1} \in G$

(iii) if $f, g \in G$, then $f \circ g \in G$ (binary operation)

Examples.

(1) the set $\{f \in X^X : f \text{ is a bijection}\}$ is a concrete group on X, called the symmetric group on X, denoted $Sym(X)$. The elements of $Sym(X)$ are called permutations of X.

Note: every concrete group is a subgroup of the symmetric group (with ALL bijections) But they're not the same!

(2) $\{id_X\}$ is a concrete group.

(3) $I := \{f \in Sym(\mathbb{R}) : \forall x, y \in \mathbb{R},\ x < y \Rightarrow f(x) < f(y)\}$

↑ set of increasing bijection

is a concrete group on $\mathbb{R}$

(i) $id_{\mathbb{R}} \in I$

(ii) $f \in I \overset{?}{\Rightarrow} f^{-1} \in I$

Take $x, y \in \mathbb{R}$, $x < y$. NTS $f^{-1}(x) < f^{-1}(y)$

AFSOC, suppose $f^{-1}(x) \geq f^{-1}(y) \Rightarrow f^{-1}(y) \leq f^{-1}(x)$

f increasing, so $f(f^{-1}(y)) \leq f(f^{-1}(x))$

$\Rightarrow y \leq x$, contradiction

(iii) $f, g \in I$, $f \circ g \in I$.

(4) Let $X \subseteq \mathbb{R}^n$

A bijection $f: X \to X$ is an isometry if

$\forall x, y \in X$, $\text{dist}(x,y) = \text{dist}(f(x), f(y))$

$\text{Iso}(X) = \{ f \in \text{sym}(X) : f \text{ is an isometry} \}$

$\text{Iso}(X)$ is a group on X.

Proof: i) $id_X \in \text{Iso}(X)$?

$id_X \in \text{sym}(X)$

$\text{dist}(x,y) = \text{dist}(id_X(x), id_X(y))$ ✓

ii) $f \in \text{Iso}(X) \Rightarrow f^{-1} \in \text{Iso}(X)$?

$f^{-1} \in \text{sym}(X)$.

$\forall x, y \in X$, $\text{dist}(x,y) = \text{dist}(f(x), f(y))$

$\text{dist}(f(f^{-1}(x)), f(f^{-1}(y)) = \text{dist}(f(x), f(y))$

Since $f^{-1}(x), f^{-1}(y) \in X$, f is isometry:

$\text{dist}(f^{-1}(x), f^{-1}(y)) = \text{dist}(x,y)$ ✓

(iii) $f, g \in \text{Iso}(X) \Rightarrow f \circ g \in \text{Iso}(X)$?

$f \circ g \in \text{sym}(X)$

$\forall x, y \in X$: $\text{dist}(f(x), f(y)) = \text{dist}(x,y)$

$\text{dist}(g(x), g(y)) = \text{dist}(x,y)$ ✓

Then $\text{dist}(f(g(x)), f(g(y)) = \text{dist}(g(x), g(y)) = \text{dist}(x,y)$ □

(5) $X \subseteq \mathbb{R}^n$. A bijection $f: X \to X$ is a homeomorphism if f and f^{-1} are continuous.

i) Every isometry is a homeomorphism

Proof: Let f be an isometry. Then

$f \in Sym(X)$ and $\forall x, y \in X$:

$dist(f(x), f(y)) = dist(x, y)$

NTS: $\forall \varepsilon > 0$, $dist(x,y) < \varepsilon \Rightarrow dist(f(x), f(y)) < \delta$

By isometry, $dist(f(x), f(y)) = dist(x,y) < \varepsilon$

So f is uniformly continuous.

By isometry, f^{-1} is also uniformly continuous □

ii) $Homeo(X) := \{ f \in Sym(X), f \text{ is homeo} \}$ is a group on X

$id_X \in Homeo(X)$

f^{-1} and $(f^{-1})^{-1}$ continuous $\Rightarrow f^{-1} \in Homeo(X)$

Composition of continuous functions is continuous.

iii) $\{ f \in Sym(X) : f \text{ is continuous} \}$ may not be a group

inverse of continuous functions may not be continuous. e.g. $f: [0, 2\pi) \to \mathbb{R}^2 : \theta \mapsto (\cos\theta, \sin\theta)$

f is bijective, but f^{-1} is discontinuous □

(6) Graphs Γ

vertex set: $V(\Gamma)$

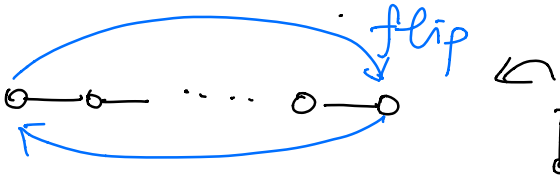
edge set: $E(\Gamma)$

Each edge is a 2-element subset of $V(\Gamma)$

An automorphism of Γ is a bijection $f: V(\Gamma) \to V(\Gamma)$ such that $\forall x, y \in V(\Gamma)$:

$$\{x, y\} \in E(\Gamma) \Leftrightarrow \{f(x), f(y)\} \in E(\Gamma)$$

denote the set as $Aut(\Gamma)$, which is a concrete group on $V(\Gamma)$

(6.1) $\Gamma =$ 

path of finite len

$|Aut(\Gamma)| = 2$

$Aut(\Gamma) = \{id, flip\}$

Composition table

$x \circ y$	id	flip
id	id	flip
flip	flip	id

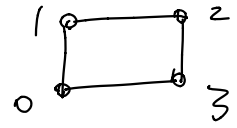
Notice the comp table doesn't depend on len of path

(6.ii) $T =$ 

rotate & Reflect

$Aut(T) = Sym(\{0, 1, 2\})$

$|Aut(T)| = 6$

$T =$ 

$4 \times 2 = 8 = |Aut(T)|$

- choose where the 0 goes (4)
- decide where to send 1 (2)

C_n : cycle of length n

$Aut(C_n) =: D_{2n}$ ← the dihedral group

$|D_{2n}| = 2n$

逆方向 逆预选

(7) Let G be a concrete group on X.

A function $f \in Sym(G)$ is an automorphism of G if $\forall g, h \in G$:

$$f(g \circ h) = f(g) \circ f(h)$$

Denote $Aut(G)$

Ex. If f is an automorphism of G, then $f(id_X) = id_X$

proof. Let $g \in G$, then

$$f(g) = f(g \circ id_X) = f(g) \circ f(id_X)$$

$$f(id_X) = id_X \quad \square$$

Let X be a set, let $f \in Sym(X)$. For $n \in \mathbb{N}$, we write $f^n := \underbrace{f \circ f \circ \dots \circ f}_{n \text{ times}}$

$f^0 := id_X$, $f^{n+1} := f \circ f^n$

Also, let $f^{-n} := (f^{-1})^n$ (inverse)

Ex. $\forall n, m \in \mathbb{Z}$: (a) $f^{-n} = (f^n)^{-1}$

(b) $(f^n)^m = f^{nm}$

(c) $f^n \circ f^m = f^{n+m}$

From this it follows that

$\langle f \rangle := \{f^n : n \in \mathbb{Z}\}$ is a group on X.

This group is called the cyclic group generated by f.

Why cyclic? Consider composition table

$\circ$	$\cdots$	f^{-2}	f^{-1}	f^0	f^1	f^2	$\cdots$
$\vdots$							
f^{-1}	$\cdots$	-3	(-2) $\overset{\text{mod}_k}{}$	-1	(0) $\overset{\text{mod}_k}{}$	(1)	$\cdots$
f^0	$\cdots$	-2	-1	0	(1)	(2)	$\cdots$
f^1	$\cdots$	-1	0	1	(2)	(3)	$\cdots$
$\vdots$							

Note: powers of f are not necessarily different. e.g. $f := id$.

It could happen that $f^n = f^m$ for some m, n: $m > n$

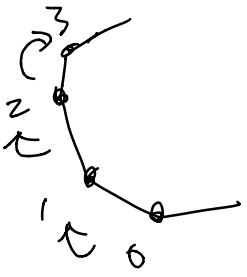
$\hookrightarrow$ $f^{-n} \circ f^n = id = f^{m-n}$

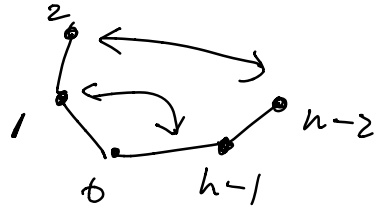
$\Rightarrow$ Let $k := m-n$, $f^k = id$

Fix the smallest such k

(cycles back after k)

example. dihedral group

$g :=$ 

$h :=$ 

fix zero, switch others

claim: the elements of D_{2n} are

$$id = g^0,\ g = g^1,\ g^2, g^3, \dots, g^{n-1}$$
$$h = g^k \circ h$$

$$\langle g \rangle = \{id, g, g^2, \dots, g^{n-1}\}$$
$$\langle h \rangle = \{id, h\}$$

proof. Take any $f \in D_{2n}$

Let $k := f(0)$ ← 顶点

wish to express f as either g^k or $g^k \circ h$

Let $f' := g^{-k} \circ f$ ← 转回顶点0

(Note: $f'(0) = (g^{-k} \circ f)(0) = g^{-k}(k) = 0$)

So $f' \in \{id, h\}$, as desired.

Ex. For each $k, \ell \in \mathbb{Z}$
compute $(g^k \circ h^\ell)(0)$ and $(g^k \circ h^\ell)(1)$
and conclude that $2n$ functions
listed in the claim are distinct,
thus getting a second proof of claim.

why? we showed there are $2n$ automorphisms.
If the $2n$ functions generated by f, g are all
distinct and automorphisms, then they must
include all elements of P_{2n}. $\langle g, h \rangle = D_{2n}$ because
every $a \in D_{2n}$ is composed with f, g.
if ℓ even, $g^k(0) = k$, $g^k(1) = (1+k) \bmod N$
if ℓ odd, $(g^k \circ h^\ell)(0) = N-k$, $(g^k \circ h^\ell)(1) = (N-1+k) \bmod N$

Observe. D_{2n} is the smallest group
containing g and h.

Indeed, if G is a group containing g, h
then $\forall k, \ell$, $g^k \circ h^\ell \in G$ so $D_{2n} \subseteq G$
P_{2n} is generated by g and h.

Lemma. Let X be a set and let $\mathcal{G}$ be a set
of concrete groups on X. ↑ may be infinite
Then $\bigcap \mathcal{G} = \{ f \in \mathrm{Sym}(X) : f \in G \text{ for all } G \in \mathcal{G} \}$
is also a group

(Unlike real number line
intersection of infinite open interval
is a closed interval)

Pf. $id_X \in \bigcap \mathcal{G}_T$, since every group contains id_X

If $f \in \bigcap \mathcal{G}_T$, then $f^{-1} \in \bigcap \mathcal{G}_T$ (consider $G_T \in \mathcal{G}_T$)

If $f, g \in \bigcap \mathcal{G}_T$, then $f \circ g \in \bigcap \mathcal{G}_T$

Note: $\bigcup \mathcal{G}_T$ is not necessarily a group, because composition will fail for $f \in G_1$, $g \in G_2$, $G_1 \neq G_2$

Group Generated by Sets

If $S \subseteq Sym(X)$ ← bijective functions

Then $\langle S \rangle := \bigcap \{G_T : G_T \text{ is a concrete group on } X \text{ s.t. } S \subseteq G\}$

is a group and $S \subseteq \langle S \rangle$

So $\langle S \rangle$ is the smallest group containing S (as subset). It's called the group generated by S.

e.g. If $f \in Sym(X)$, $\langle f \rangle = \langle \{f\} \rangle$

More generally, we write

$\langle \{f_1, \dots, f_k\} \rangle =: \langle f_1, \dots, f_k \rangle$

e.g. with $g, h \in D_{2n}$ as before

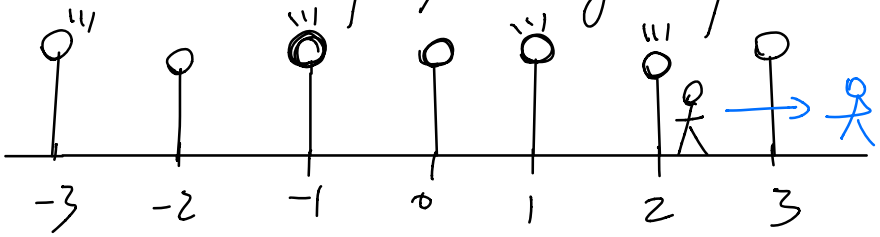
$D_{2n} = \langle g, h \rangle$ ← generated by g, h

Examples: (1) Rubik's Cube group $\langle X \rangle$

X = set of size $(8 \times 6 = 48)$

S = the set of 6 individual rotations, represented as rotations on X.

(2) the lamplighter group



g: move to next light

h: switch the current light

$X = \{0,1\}^{\mathbb{Z}} \times \mathbb{Z}$ ← position of lamplighter

$g_k(x,n) := (x, n+k)$, $k \in \mathbb{Z}$

$h(x,n) := (x', n)$ where

$$x'(i) = \begin{cases} x(i) & \text{if } i \neq 0 \\ 1 - x(i), & \text{if } i = 0 \end{cases}$$

The group generated by these two operations is called the lamplighter group.