Lecture 0

(0.0) **Definition of a group.** A group G is a set and

- a function $G \times G \to G$ called { group operation or multiplication
  $(a, b) \mapsto a * b$
  ↑ just a notation.

- an element $e \in G$ called (the) unit element { or identity or neutral

such that the following properties hold:

(1) Associativity of the group operation:

$$(a * b) * c = a * (b * c) \quad \underbrace{\text{for every}}_{\text{symbol } \forall} \; a, b, c \in G$$

(2) e is neutral:

$$e * a = a * e = a \quad \forall a \in G.$$

(3) Existence of inverses:

for every $a \in G$, there exists $b \in G$ such that

$$a * b = e = b * a$$

[In symbols: $\forall a \in G, \ \exists b \in G : a * b = e = b * a$]

(0.1) Some examples.

"Group" is given to us as a set and a binary operation

2 inputs a, b ; 1 output $a * b$

(i) $G = \mathbb{Z}$ = set of all integers

$= \{ \ldots, -1, 0, 1, 2, \ldots \}$.

$a * b = a + b$ $\qquad e = 0$

Inverse of $a = -a$.

(ii) $G = \mathbb{R}_{>0}$ = set of positive real numbers

$a * b = a \cdot b$ (multiplication)

$e = 1$

Inverse of $a = \frac{1}{a}$

iii) <u>Not a group</u> : $G = \mathbb{R}_{>0}$ = set of positive real numbers.

$a * b = a^b$ (binary operation)

$(= e^{b \ln(a)})$

Euler's constant, not group unit

Ex. $a * b = a^b$ is not an associative operation.

(0.2) **Definition.** We say that a group G is <u>abelian</u> (or <u>commutative</u>) if $a * b = b * a \quad \forall\, a, b \in G$.

(Examples (i) and (ii) of (0.1) are abelian.)

Example. (of a non-abelian group)

$G = GL_2(\mathbb{R})$ = set of 2×2 matrices with real entries and non-zero determinant.

group operation = matrix multiplication.

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{(identity matrix)}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Check : $A \cdot B \neq B \cdot A$ for <u>any</u> two $A, B \in GL_2(\mathbb{R})$

e.g. $A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

$AB = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ but $BA = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$.

(0.3) Lemma. Let G be a group and $x \in G$. If y and y' are two inverses of x, then $y = y'$.
[uniqueness of inverse - henceforth <u>the</u> inverse of x, denoted by x^{-1}.]

Proof

$$y \overset{①}{=} y * e \overset{②}{=} y * (x * y')$$

$$\underset{③}{=} (y * x) * y' \underset{④}{=} e * y' \underset{⑤}{=} y'$$

①, ⑤ : because e is a unit.

②, ④ : because y and y' are inverses of x

③ : associativity.

$\square$ (end of proof)

(0.4) Examples of groups continued.

"Group" is given to us as "symmetries of a structure".

Note: in such a description of a group, associativity is automatic!

(i) "Structure" = finite set

$$X = \{1, 2, \dots, n\}$$

↑ some positive integer.

"symmetries" = bijections

$$\sigma : X \longrightarrow X$$

Notation S_n (<u>symmetric group</u> on n elements)

S_n = set of all bijections $X \xrightarrow{\sigma} X$

group operation = compose two maps

$$\begin{tikzcd} X \arrow[r, "\sigma"] \arrow[rr, bend right, "\tau * \sigma := \tau\sigma"'] & X \arrow[r, "\tau"] & X \end{tikzcd}$$

$\leftarrow$ (I will omit $*$ symbol here)

Hence S_n = permutations of n symbols

Ex: $|S_n|$ = number of elements of S_n

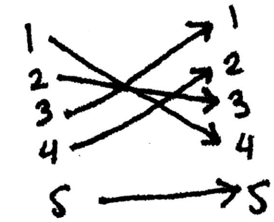
$= n! \quad (= 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n)$

e.g. S_3 has 6 elements. For instance,

$$\sigma(1) = 2 \qquad\qquad \tau(1) = 3$$
$$\sigma(2) = 1 \qquad \text{or} \qquad \tau(2) = 1$$
$$\sigma(3) = 3 \qquad\qquad \tau(3) = 2$$

Various ways of writing a permutation.

- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix} \in S_5$ or



- cyclic notation : $\sigma = (1\,4\,2\,3) \in S_4$ means

$$1 \mapsto 4 \mapsto 2 \mapsto 3 \mapsto 1$$

$\Big($ i.e. $\sigma(1) = 4$, $\sigma(2) = 3$, $\sigma(3) = 1$, $\sigma(4) = 2$ $\Big)$.

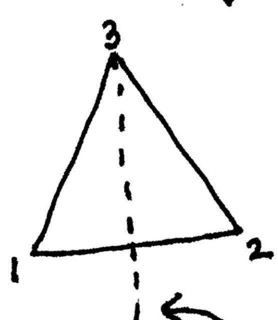
(ii) Dihedral group D_{2n} $\quad$ ($n \in \mathbb{Z}_{>0}$ non-neg. int.)

Assume $n \geq 3$.

"structure" = regular n-gon

"symmetries" = permuting the vertices so that the shape does not change (i.e. edges of the n-gon are preserved.)

e.g. $n = 3$

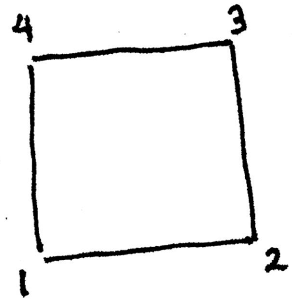


$$\delta : \begin{array}{l} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{array} \in D_6$$

$\parallel$

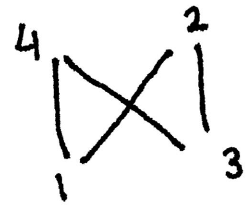
reflection about the dotted line

e.g. $n = 4$



$$\sigma : \begin{array}{ccc} 1 & \longrightarrow & 1 \\ 2 & \searrow & 2 \\ & \times & \\ 3 & \nearrow & 3 \\ 4 & \longrightarrow & 4 \end{array}$$

is <u>not</u> in D_8, because σ



changes the shape.

[In other words, 3 & 4 are connected before σ but $\sigma(3) = 2$ & $\sigma(4) = 4$ are <u>not</u> - so σ does not respect the edges.]

Ex. $|D_{2n}| = 2n$ (there are exactly $2n$ symmetries of the regular n-gon)

[Hint: if $\sigma \in D_{2n}$, $\sigma(1) \in \{1, \dots, n\}$ has <u>n options</u>. Say, $\sigma(1) = k$

$\sigma(2)$ has <u>two options</u> $k-1$ or $k+1$.

The rest is determined by the fact that the edges need to be preserved.]

(0.5) A group can be described by "generators and relations".

e.g. ~~#~~ G = free group on 2 letters. ← generators

As a set G consists of "words" in the "alphabet" $\{a, b\}$ (2 symbols). Including ϕ = "empty word"

e.g. $a^{5} b^{-2} a b^{6} a^{-1} \in G$

In general, $w \in G$ has the form:

$$w = a^{m_1} b^{n_1} a^{m_2} b^{n_2} \cdots a^{m_\ell} b^{n_\ell}$$

[exponents $m_1, \ldots, m_\ell$, $n_1, \ldots, n_\ell$ are integers]

Group operation - concatenation.

[only one rule: $x^k x^\ell = x^{k+\ell}$; $x = a$ or b]
$(x^0 = \phi)$

"relations"

e.g. $w_1 = a b a b^{-1}$ $\Rightarrow$ $w_1 w_2 = a b a b^{-1} b^{4} a^{-3}$
$w_2 = b^{4} a^{-3}$ $\qquad = a b a b^{3} a^{-3}$

$w_2 w_1 = b^{4} a^{-2} b a b^{-1}.$