Groups

- It's like fields, but with only one operation!
- It helps in studying symmetries of an object.

eg. $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \text{---}$

id = $\quad (2\ 3)$ " $\quad (1\ 3\ 2)$ " is the cycle-notation for permutation.

$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\ 3)(2\ 4)$

- Set of permutations on $[n]$ is S_n.

– Defn: Group G is a set with operator $*$, s.t.
- Closure: $\forall a, b \in G$, $a * b \in G$.
- Associativity: $a*(b*c) = (a*b)*c =: a*b*c$.
- Identity: $\exists e \in G$, $\forall a \in G$, $a*e = e*a = a$.
- Inverse: $\forall a \in G$, $\exists a^{-1} \in G$, $a * a^{-1} = a^{-1} * a = e$.

– Eg. $(S_n, *)$ is a group of size $n!$.
$a * b \neq b * a$.

– Eg. $(\mathbb{Z}, +)$ is an infinite group. $(a+b = b+a)$

Defn: G is <u>abelian</u> (or <u>commutative</u>) if $(G,*)$ is group & $\forall a,b \in G$, $a*b = b*a$.

- Eg. $(\mathbb{F}^{m\times n}, +)$ is an abelian group.
- Eg. $(\mathbb{F}^{n\times n}, *)$ is <u>not</u> group.
- Eg. $(\underbrace{GL_n(\mathbb{F})}_{\text{set of invertible matrices}}, *)$ is the <u>general-linear group</u>. <u>not</u> abelian for $n>1$.

▷ e in G is unique.

Pf: · e_1, e_2 are identities in $(G,*)$.

· $e_2 = e_1 * e_2 = e_1$. $\square$

▷ Inverse is unique in G.

Pf: Suppose $a * a_1 = a_1 * a = e$

$= a * a_2 = a_2 * a$.

$\Rightarrow a_2(a a_1) = a_2 * e = a_2$

$= (a_2 a) a_1 = e * a_1 = a_1 \quad \Rightarrow a_1 = a_2 =: a^{-1}$. $\square$

- Eg. $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ $\to$ abelian. $e=0$.

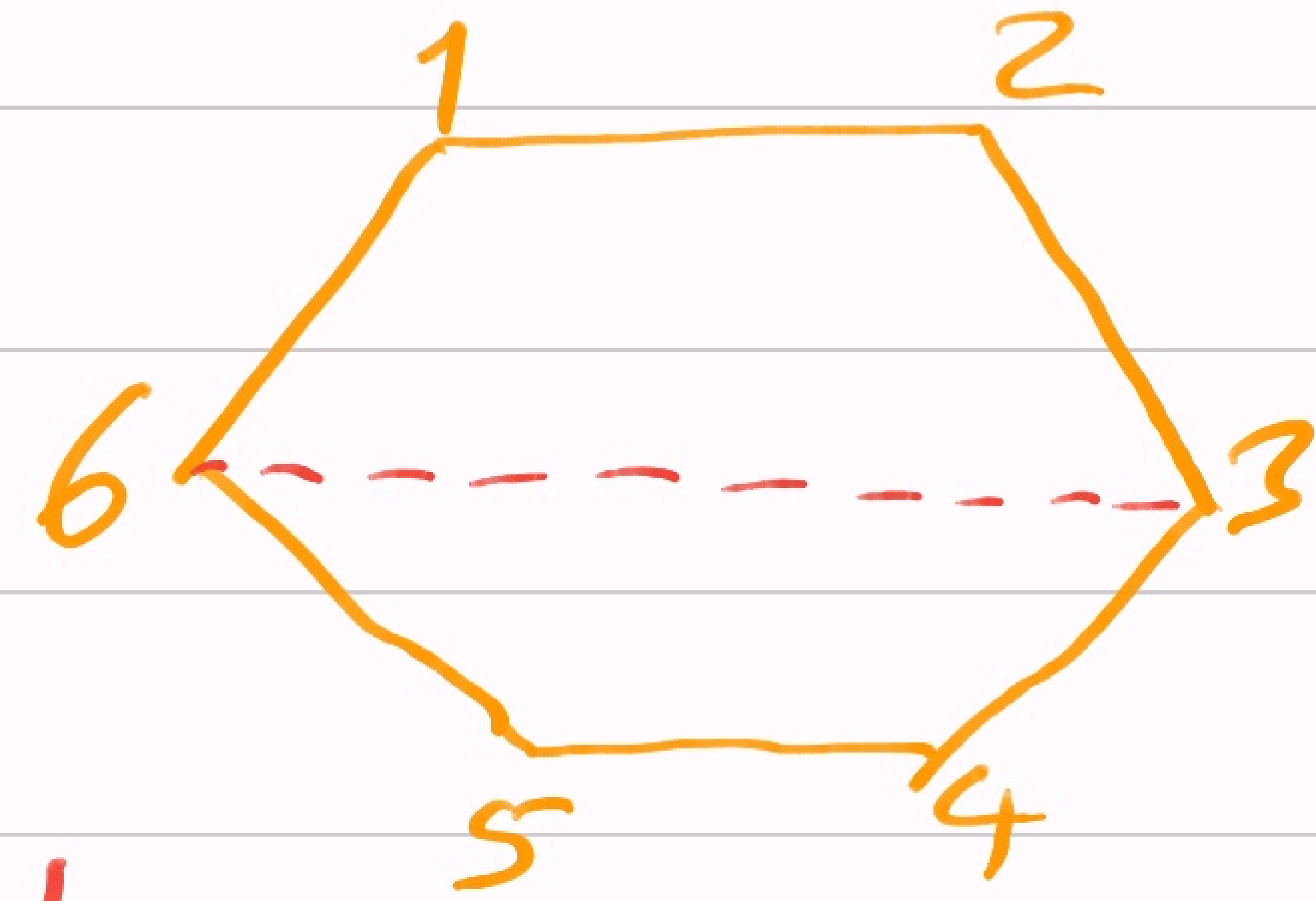
$\cancel{(\mathbb{Z}^*,*)}$, $(\mathbb{Q}^*,*)$, $(\mathbb{R}^*,*)$, $(\mathbb{C}^*,*)$ $\to$ abelian; $e=1$.

$(\mathbb{Q}_{>0},*)$, $(\mathbb{R}_{>0},*)$ $\to$ " "

$(\mathbb{Z}/n,+)$ $\to$ abelian ; $e=0$

$\cancel{(\mathbb{Z}/p,*)}$, $((\mathbb{Z}/p)^*,*)$ " ; $e=1$. $\underbrace{((\mathbb{Z}/n)^*,*)}_{}$ = of size $\varphi(n)$

- Symmetries of a regular n-gon under composition (eg. rotations/reflections/~) → is called Dihedral group $D_n \subset S_n$.



- Exercise: $|D_6| = 6 \times 2$.

▷ $(\mathbb{F}, +, *)$ is a field $\Rightarrow$ $(\mathbb{F}, +)$ is abelian gp.
& $(\mathbb{F}^*, *)$ " " " .

- A group gets completely specified by its multiplication table.

G:
$$\begin{array}{c|ccccc} & a_1 & a_2 & \cdots & a_i & \cdots \\ \hline a_1 & & & & & \\ \vdots & & & & & \\ a_j & \cdots & & & (a_j * a_i) & \\ \vdots & & & & & \end{array}$$

▷ Every row (resp. column) has all the elements of G.

Pf: • j-th-row : $a_j * \{a_1, a_2, \dots, a_i, \dots\}$

• So, $a_j a_i = a_j a_{i'} \Rightarrow a_i = a_{i'}$. □

- Eg. $G = ((\mathbb{Z}/5)^*, *) = (\mathbb{F}_5^*, *)$

$*$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

- Defn: For $x \in G$, ord(x) is the least $j \in \mathbb{N}_{>0}$ s.t. $x^j = e$.

▷ ord$(x) = 1$ iff $x = e$.

▷ ord(x^{-1}) = ord(x).

- $x^{-j} := (x^{-1})^j$; $\forall j \in \mathbb{Z}$, $x \in G$.

D $(x^j)^{-1} = x^{-j}$.

- Claim: $|G| < \infty \Rightarrow \forall x \in G$, $1 \leq \text{ord}(x) \leq |G|$.

Pf: Cyclic group generated by x is $\langle x \rangle := \{x^j \mid j \in \mathbb{Z}\}$.
$\leq G$.

- $\langle x \rangle$ has two elements equal

$\Rightarrow x^j = x^{j'}$ for $j \neq j'$.

$\Rightarrow x^{j-j'} = 1$

$\Rightarrow \text{ord}(x) < \infty$. $\square$

$G = \{g_1, g_2, \ldots, g_n\}$

$\{xg_1, xg_2, \ldots, xg_n\}$

$\prod_{g \in G} g = \prod_{g \in G} (xg) = x^n \cdot \prod_{g \in G} g$

(for abelian G)

$\Rightarrow x^{|G|} = e$.

<u>Theorem</u>: $\forall x \in G$, $\operatorname{ord}(x)^{=:d} \mid |G|^{=:n}$.

<u>Pf</u>: · <u>Qn</u>: How to show $x^n = e$?

· If $x^n = e$ & $x^d = e$ $\Rightarrow$ $n =: kd + r$ $(0 \leq r < d)$

$\Rightarrow$ $x^{kd} \cdot x^r = e$

$$= (x^d)^k \cdot x^r = x^r \Rightarrow r = 0.$$

$\square$

▷ Recall the proofs of FLT & Euler's thm, in this new light; for $G := ((\mathbb{Z}/n)^*, *)$.

- <u>Defn</u>: · G is <u>cyclic</u> group if $\exists x \in G$, $\langle x \rangle = G$.
  · x is called a <u>generator of G</u>.

• Consider $S \subseteq G$, then S generates the group $\langle S \rangle := \{ \prod_{t \in T} t \mid T$ is an ordered subset of S, with repetition $\}$.

Subgroups

- Defn: Subset H of a group $(G, *)$ is called subgroup of G ($H \leq G$) if $H \neq \phi$, closed under $*$ and has inverses (& $e \in H$).
- Eg. $(\mathbb{Z}, +) =: G$: $\{0\} \leq G$, $G \leq G$, $(2\mathbb{Z}, +) \leq G$, $(n\mathbb{Z}, +) \leq G$. ▷ $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq (\mathbb{C}, +)$.

- $(\mathbb{Z}[\sqrt{2}], +) \leq (\mathbb{R}, +)$

$:= \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$

▷ Abelian $G \Longrightarrow$ abelian $H \leq G$.

▷ $C(G) := \{ h \in G \mid hg = gh, \ \forall g \in G \}$

center of G is abelian subgroup.

▷ G is abelian $\Longleftrightarrow C(G) = G$.

Exercise: What are the subgroups of cyclic G?

– Idea: $H \leq G$, consider $g \in G$ & $gH := \{gh \mid h \in H\}$

▷ $g \in H \Rightarrow gh \in H$. If, $g \notin H$, then $gh \notin H$.

- Let $g_1, g_2 \in G$. What about g_1H & g_2H?
- Is gH a subgroup?

▷ $|g_1H| = |g_2H|$, for (finite) group $G \geq H$; $g_1, g_2 \in G$.

Pf: • $\varphi : g_1H \longrightarrow g_2H$

$$a \longmapsto g_2g_1^{-1}a$$

[• a is of the form g_1h. So, $g_2g_1^{-1}a = g_2h$.]

• $\varphi(g_1h) = \varphi(g_1h') \Rightarrow g_2h = g_2h' \Rightarrow h = h'$.

$\Rightarrow \varphi$ is injective & surjective $\Rightarrow \varphi$ is bijection.

$$\Rightarrow |g_1H| = |g_2H|.$$

$\square$

▷ $eH = H$. For $g_1 \in H$, $g_1H = H$.

▷ $\forall g \in G$, $|gH| = |H|$.

- **Defn:** $G/H := \{gH \mid g \in G\}$.

▷ $\bigcup_{g\in G} gH = G$.

Pf: $\forall g \in G$, $g \cdot e = g$ & $e \in H$. □

▷ $g_1 H \cap g_2 H \ni a \Rightarrow g_1^{-1}a, g_2^{-1}a \in H$.

$\Leftrightarrow a =: g_1 h_1 = g_2 h_2 \Rightarrow g_1^{-1} g_2 = h_1 h_2^{-1} \in H$.

$\Rightarrow (g_1^{-1} g_2) H = H$

$\Rightarrow g_2 H = g_1 H$.

- Eg. $H = (2\mathbb{Z}, +) \leq G := (\mathbb{Z}, +)$; $g_1 := 1, g_2 := 2, g_3 := 3$

$g_1 H = 1 + 2\mathbb{Z}$ & $g_2 H = 2 + 2\mathbb{Z}$ & $g_3 H = 3 + 2\mathbb{Z}$

▷ $g_1 H \cap g_2 H \neq \phi$ iff $g_1 H = g_2 H$.

(Lagrange's) Theorem: Group $G \geq H \Rightarrow$
G/H is a partition of G into equal parts. [$\Rightarrow |H| \mid |G|$.]

Corollary 1: $|G/H| = |G|/|H|$.

Corollary 2: $\forall g \in G$, $\operatorname{ord}(g) \mid |G|$ & $g^{|G|} = e$.

Pf: Take $H := (g) \leq G$.
(Lagrange's thm) $\Rightarrow |G/H| = |G|/|(g)|$
$= |G|/\operatorname{ord}(g)$. □

- Given $H \leq G$, we can define the relation:

$$g_1 \sim_H g_2 \quad \text{if} \quad g_1 \in g_2 H$$

▷ $\sim_H$ is an equivalence relation.

▷ It partitions G into cosets in G/H.

- Defn: gH is called coset of $G \geq H$.

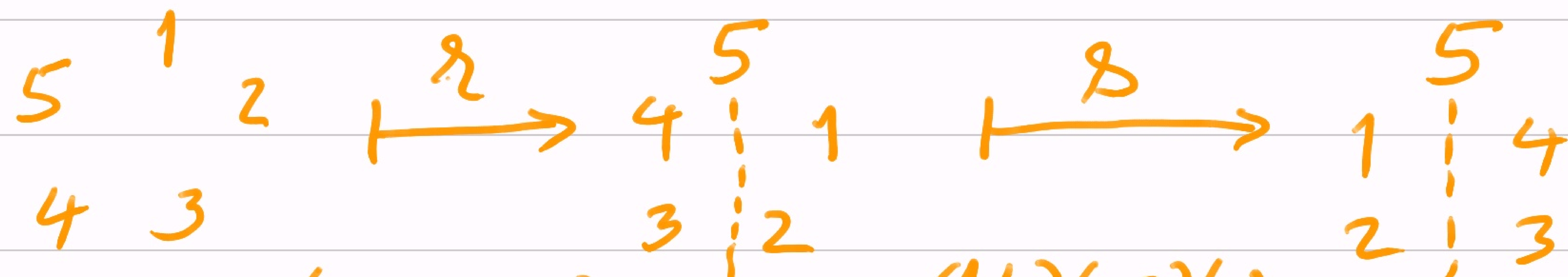
▷ Coset gH gives an equivalence class, where g is one of the representatives. (other reps. are $g \cdot h$, $h \in H$).

▷ $g \cdot H = (gh) \cdot H$.

Dihedral group (revisited)

- **Defn:** $D_n := (r, s)$, where r rotates the vertices of a regular n-gon & s reflects the vertices along the median axis.
  - Dihedral group D_n has elements:
    $\{r, r^2, \ldots, r^n, rs, r^2 s, \ldots, r^n s\}$

- Eg.



$(1\,2\,3\,4\,5)$ $\quad$ $(1\,4)(2\,3)(5)$

- Eg. $|D_n/(r)| = 2$; $|D_n/(s)| = n$

$\quad = \{D_n, sD_n\}$ $\qquad\qquad$ $= \{r^i \cdot D_n \mid i \geq 0\}$

▷ $rs = sr^{-1}$. [$\Leftrightarrow rsr = s \Leftrightarrow s^{-1}rs = r^{-1}$]

Count colored necklaces

- Qn: # distinct necklaces of 4 beads with 2 colors?

$$\begin{matrix} B & - & W \\ | & & | \\ W & - & B \end{matrix} \quad \text{or} \quad \begin{matrix} W & - & B \\ | & & | \\ B & - & W \end{matrix} \quad \text{or} \quad \begin{matrix} B & - & W \\ | & & | \\ B & - & W \end{matrix}$$

▷ I, II same under D_4. III is different.

$$\begin{array}{ccc} B & \vdots & W \\ | & \vdots & | \\ W & \vdots & W \end{array} \quad \text{or} \quad \begin{array}{ccc} W & - & B \\ | & & | \\ W & - & W \end{array} \quad \text{or} \quad \cdots$$

▷ #(0 black beads) = 1

#(1 " ") = 1

#(3 " ") = 1

#(4 " ") = 1

$\Longrightarrow$ ▷ #(necklaces$/D_4$) = 6.

▷ Without symmetry, its $= 2^4 = 16$.

— As #beads & #colors increases this count is a complicated process.

- This is done by:

<u>Burnside's Lemma</u> or <u>Orbit-counting</u>.

- <u>Reading exercise</u>: (1) Burnside Lemma.
  (2) Normal subgroups.