• Ye

Lecture II: More examples, Subgroups

Recall: A group is a triple $(G, *, e)$ where G is a set, $*: G\times G \to G$, $e \in G$ satisfying

(1) Associativity $(a*b)*c = a*(b*c)$ $\forall a,b,c \in G$

(2) $a*e = e*a = a$ $\forall a \in G$

(3) Inverse of elements $\forall a \in G$ $\exists \underset{a^{-1}}{\underset{\shortparallel}{b}} \in G$ with $a*b = b*a = e$

Properties:
- $(a*b)^{-1} = b^{-1} * a^{-1}$ & $(a^{-1})^{-1} = a$ $\forall a,b \in G$
- Cancellation Laws: $a*b = c*b \Rightarrow a=c$
  $b*a = b*c \Rightarrow a=c$

Definition: The order or size of a group G is its cardinality. Write $|G|$

Example: $|S_n| = n!$; $|\mathbb{Z}| = \infty$

§2.1 More examples:

- One source: symmetries of a structure.

EXAMPLE 1: S_n = permutation (or symmetric) group on n letters.

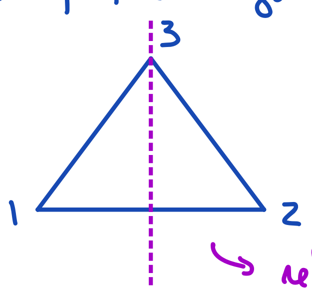
EXAMPLE 2: Dihedral group D_{2n} ($n \in \mathbb{Z}_{>0}$ non-negative integer, $n \geq 3$)

⚠ Some books use the notation D_n for this!

"Structure" = a regular n-gon

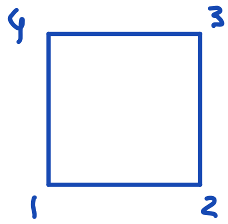
"symmetries" = permutation of vertices so that the shape does not change, ie edges of the n-gon are preserved.

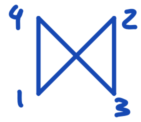
Ex $n=3$



$s:$ $\begin{array}{l} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{array}$ $\in D_6$

↳ reflection about dotted line

$n=4$ 

σ : $1 \to 1$, $2 \to 3$, $3 \to 2$, $4 \to 4$ is <u>not</u> in D_8 because  $= \sigma(\square)$

Proposition: $|D_{2n}| = 2n$ (exactly $2n$ symmetries on an n-gon)

Proof: Label the vertices of the n-gon counter-clockwise, as above.

If $\sigma \in D_{2n}$, $\sigma(1) \in \{1, \ldots, n\}$ has n-options. Say $\sigma(1) = k$.

Now $\sigma(2)$ has only 2 options: $k-1$ or $k+1$ (vertices connected to the vertex labeled k). Once this value is fixed, the rest is determined

Ex If $\sigma(2) = k+1$, then $\sigma(3) = k+2 \pmod{n}$, etc...

If $\sigma(2) = k-1$ — $\sigma(3) = k-2 \pmod{n}$, ... $\square$

- A group can also be described by "generators & relations".

EXAMPLE: 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"

  Ex: $a^5 b^{-2} a\, b^6 a^{-1} \in G$ $\quad (b^{-2} = b^{-1} b^{-1})$

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

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

exponents $m_1, m_2, \ldots, m_\ell$ & $n_1, n_2, \ldots, n_\ell$ are integers

Convention: a^0, b^0 are omitted. (empty word)

- Group operation : concatenation , subject to only one rule "relations"

$$x^k x^l = x^{k+l} \quad \& \quad x^0 = \emptyset \quad \text{for } x = a \text{ or } b$$

Ex: $w_1 = abab^{-1}$ $\Rightarrow$ $w_1 w_2 = abab^{-1}b^4a^{-3} = abab^3a^{-3}$

$w_2 = b^4a^{-3}$ $\quad w_2 w_1 = b^4 a^{-3} abab^{-1} = b^4a^{-2}bab^{-1}$ $\square$

§2.2 Subgroups:

Definition: Let G be a group and H a subset of G. We say H is a subgroup of G (denoted by $H \leq G$) if
(1) $e \in H$
(2) $a, b \in H \Rightarrow a * b \in H$ (H is closed under $*$)
(3) $a \in H \Rightarrow a^{-1} \in H$ (H is closed under inverses)

In other words: H inherits a group structure from G.

Lemma: $H \subseteq G$ is a subgroup if, and only if:
(i) $H \neq \emptyset$
(ii) $a, b \in H \Rightarrow ab^{-1} \in H$

Proof: ($\Rightarrow$) If $H \leq G$ then $e \in H$, so $H \neq \emptyset$. Thus, (i) holds. Next, we check (ii). Pick $a, b \in H$. Since $b \in H$, then $b^{-1} \in H$ (by (3)). Using (2) for a, b^{-1} we conclude $a * b^{-1} \in H$.

($\Leftarrow$) We check the 3 properties:

(1) Pick $a \in H$ (we can by (i)). Then, $a * a^{-1} \in H$ by (ii). So $e \in H$.

(3) By (1) & (ii), we have $e, a \in H \Rightarrow e * a^{-1} = a^{-1} \in H$.

(2) Assume $a, b \in H$. Then, by (3) $b^{-1} \in H$. Now, by (ii), $a, b^{-1} \in H$ yields $a * (b^{-1})^{-1} = a * b \in H$.

Q: How can we build subgroups?

A: Subgroups generated by a subset.

Definition: Let G be a group & $A \subseteq G$ a subset. The subgroup of G generated by A is defined as the smallest subgroup of G containing A. We write it as $\langle A \rangle$

Lemma: $\langle A \rangle = \bigcap_{\substack{H \leq G \\ A \subseteq H}} H$ (Convention, if $A = \emptyset$, $\langle A \rangle = \{e\}$ trivial subgroup)

Proof: It's enough to show that intersection of subgroups is a subgroup. □

Definition: • We say A generates G (A is a set of generators of G) if $\langle A \rangle = G$ non-uniqueness!

• We say G is finitely generated if $\exists$ finite set $A \subseteq G$ which generates G.

Examples ① Any finite group (ie $|G| < \infty$) is finitely generated.

② S_n is finitely generated.

Cyclic notation shows every permutation is a product of disjoint cycles, so $S_n = \langle (i_1 i_2 \cdots i_k) \;\; \substack{k \geq 1 \\ \{i_1, \cdots i_k\} \subseteq \{1, \cdots n\} \\ \text{has size } k} \rangle$

§ 2.3 Cyclic groups:

Definition: A group G is cyclic if it admits one generator, ie $G = \langle \{a\} \rangle$ for some $a \in G$. Write $G = \langle a \rangle$

So, $G = \left\{ e, \begin{matrix} a, & a^2, & \cdots \\ a^{-1}, & a^{-2}, & \cdots \end{matrix} \right\}$

There are two options: $\{e, a, a^2, \ldots\}$ is infinite Ⓐ

$\underline{\hspace{8em}}$ is finite Ⓑ

• Option Ⓐ G is the same as $\mathbb{Z}$ (To be made precise later, when we discuss group homomorphisms)

$$\begin{matrix} G & & \mathbb{Z} \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ a^n & \longleftrightarrow & n \end{matrix}$$

• Option Ⓑ Let k be the smallest positive integer such that $a^k \in \{e, a, a^2, \ldots, a^{k-1}\}$

Then, $a^k = e$. Otherwise, $a^k = a^\ell$ $(0 < \ell < k)$ $\Rightarrow a^{k-\ell} \cancel{a^\ell} = e \cancel{a^\ell}$

(Cancellation Laws)

so $a^{k-l} \in \{e, a, \dots, a^{k-l-1}\}$ & $0 < k-l < k$

This contradicts the minimality of k.

Conclusion: $G = \{e, a, a^2, \dots, a^{k-1}\} \longleftrightarrow \mathbb{Z}/k\mathbb{Z}$

Here, $\mathbb{Z}/k\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{k-1}\}$ with group operation: $\bar{a} + \bar{b} = \overline{a+b}$

(remainder modulo k)

Our calculation give a full classification of all cyclic groups:

$\mathbb{Z}$ or $\mathbb{Z}/k\mathbb{Z}$ for $k = 1, 2, 3, 4, \dots$

only infinite cyclic group

finite cyclic group