Lecture 1

(1.0) Recall: • a group consists of a set G together with a binary operation $G \times G \to G$, $(a,b) \mapsto a*b$ and a distinguished element $e \in G$ such that (i) $(a*b)*c = a*(b*c)$ $\forall\, a,b,c \in G$

(ii) $a*e = e*a = a$ $\forall\, a \in G$

(iii) $\forall\, a \in G$, $\exists\, b \in G$ such that $a*b = e = b*e$

• Inverse of an element is unique. So is identity element (or unit).

And $(a*b)^{-1} = b^{-1} * a^{-1}$; $(a^{-1})^{-1} = a$.

[Cancellation: $a*b = c*b \Rightarrow a = c$
$a*b = a*c \Rightarrow b = c$.]

• Order (or size) of a group G = $|G|$ = cardinality (i.e., number of elements of) G.

e.g. $|S_n| = n!$ $\qquad$ $|D_{2n}| = 2n$

S_n: symmetric gp. on n letters (all permutations of $\{1, \dots, n\}$)

D_{2n}: dihedral gp. (symmetries of regular n-gon)

(1.1) <u>Subgroups.</u> Let G be a group and H a subset of G. Then H is <u>a subgroup of G</u>, denoted by $H \leq G$, if

(i) $e \in H$

(ii) $a, b \in H \Rightarrow a * b \in H$.

(iii) $a \in H \Rightarrow a^{-1} \in H$

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

Lemma.— $H \subset G$ $(H \neq \phi)$ is a subgroup if, and only if

$$a, b \in H \Rightarrow a * b^{-1} \in H. \quad - (*)$$

Proof.— $(\Rightarrow)$ If $H \leq G$ and $a, b \in H$, then $b^{-1} \in H$ and $a * b^{-1} \in H$.

$(\Leftarrow)$ (i) Pick $a \in H$ (as $H \neq \phi$). Then $e = a * a^{-1} \in H$ (take $a = b$ in the given condition $(*)$)

(iii) Take $a = e$ to get: $b \in H \Rightarrow b^{-1} \in H$

(ii) $a, b \in H \Rightarrow a, b^{-1} \in H$ (just proved)

$$\Rightarrow \underbrace{a * (b^{-1})^{-1}}_{a * b} \in H \qquad \square$$

(1.2) Subgroups generated by a set of elements.

Let G be a group and $A \subset G$ a subset.

$\langle A \rangle$ = subgroup of G generated by A, is defined as the smallest subgroup of G which contains A.

$$= \bigcap_{\substack{H \leq G \\ A \subset H}} H$$

[Ex. intersection of subgps. is a subgroup.]

Convention: if $A = \phi$, $\langle A \rangle = \{e\}$ "trivial subgroup"

(remember: empty set can not be a group!)

We say A generates G if $\langle A \rangle = G$.
(or is a set of generators of G)

We say G is finitely generated if $\exists$ finite $A \subset G$ which generates G.

(1.3) Cyclic groups : group G that admits one generator

i.e., $G = \langle \{a\} \rangle$ for some $a \in G$.

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

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

" is finite - B

Option A. G is same as $\mathbb{Z}$ (please stay tuned for defn. of group homomorphisms isomorphisms)

$$\begin{matrix} G & & \mathbb{Z} \\ \Psi & & \Psi \\ a^n & \longleftrightarrow & n \end{matrix}$$

Option B. Let k be smallest positive integer such that $a^k \in \{e, a, a^2, \dots, a^{k-1}\}$. Then $a^k = e$. Because, otherwise, $a^k = a^l$ $(0 < l < k)$

$$\Rightarrow a^{k-l} = e \in \{e, a, \dots, a^{k-l-1}\}$$

contradicting minimality of k.

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

$$\mathbb{Z}/_{k\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{k-1}\}$$

group operation: $\bar{a} + \bar{b} = \overline{a+b}$ ← remainder modulo k.

Examples of group presentation:

$$\mathbb{Z} \cong \langle a \rangle \cong \langle a \mid \text{only obvious rules } (a^0 = e,\ a^k \cdot a^l = a^{k+l}) \rangle$$

a: 1 of $\mathbb{Z}$

just switch b/w additive and multiplicative notation

will be omitted in the future

$$\mathbb{Z}/_{k\mathbb{Z}} \cong \langle a \mid a^k (= e) \rangle$$

a: one generator

a^k: one relation (see ↑)

List of all cyclic groups: $\mathbb{Z}$; $\underbrace{\mathbb{Z}/_{k\mathbb{Z}} \quad (k = 1, 2, 3, \ldots)}_{\text{finite cyclic}}$

$k=1$: "trivial group"

$\mathbb{Z}$: only infinite cyclic

(1.4) Example of S_n. (~~Let us take $n=5$ for definiteness~~) We know we can write permutations as product (in any order) of disjoint cycles.

e.g $(1\,2\,3)(4\,5) = (4\,5)(1\,2\,3)$ represent the permutation

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 & 5 & 4 \end{array}$$

Now, for instance, $(1\,2\,3) = (1\,2)(2\,3)$
$(\neq (2\,3)(1\,2))$

$$\left[\text{In } S_n: \quad (i_1, i_2, \ldots, i_k) = (i_1\, i_2)(i_2\, i_3)\cdots(i_{k-1}\, i_k)\right]$$

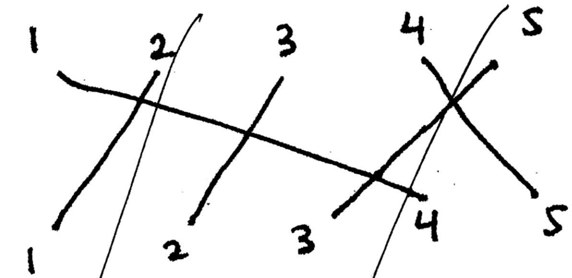
(a typical k-cycle).

Let $\sigma_{ij} := (i\, j)$ (called a transposition)
$(1 \le i < j \le n)$

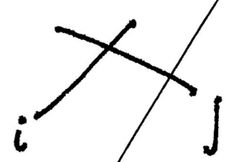
We just proved S_n ~~$= \langle \{\sigma_{ij} : 1 \le i < j \le n\} \rangle$~~ is generated by $\{\sigma_{ij} : 1 \le i < j \le n\}$ (we don't know the relations yet.)

(total $\binom{n}{2}$ of them)

Pictorial proofs:



assign (ij) to each cross



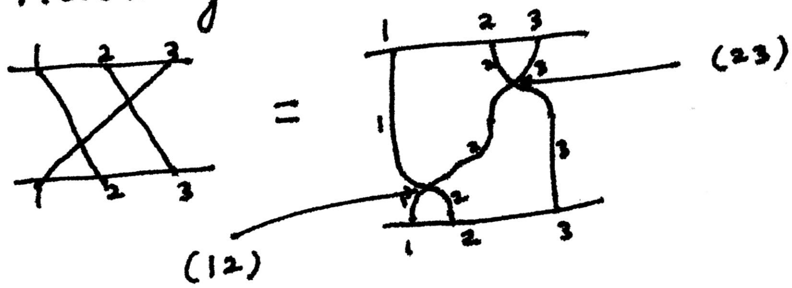
(picture of (1 4 5 3 2))

read top to bottom

correct but immaterial! (14) (24) (35) (34) [not disjoint - order matters]

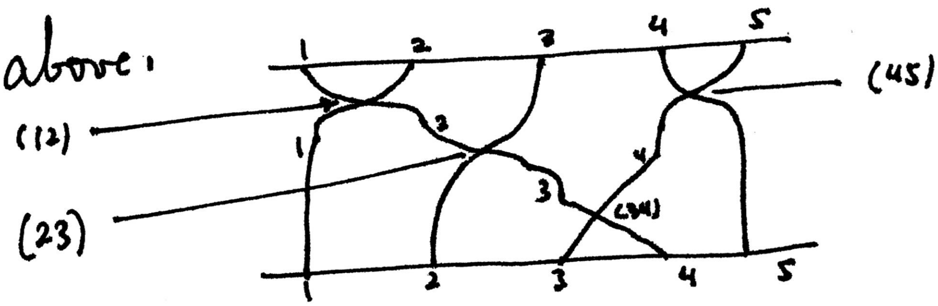
$(1\,2\,3) = (1\,2)(2\,3)$.

Pictorially



. Apply to the permutation

above:



gives

$(1\,4\,5\,3\,2) = (34)(45)(23)(12)$

Ex. Turn this into a proof that $\{\sigma_{i,i+1} : 1 \le i \le n-1\}$ generates S_n.