Notes from chapter 6 | week 4)

Consider S_3. Its Cayley table might be

	σ_1	σ_2	σ_3
σ_1	σ_1	σ_2	σ_3
σ_2	σ_2	σ_3	σ_1
σ_3	σ_3	σ_1	σ_2

then $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

but this is only a subgroup. The full group includes

$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ etc.

Let G be a group, H be a subgroup

$S \subset H : (x \in G \Rightarrow x \in H)$ iff.
(it can be written as a product where the factors are in S or or inverses of elements in S)

6.1 let $H \leq G$ (subgroup)

Then H is generated by $S \subseteq G$
(S is a generating set of H)

iff.

$H = \{a_1, a_2, a_3, \dots, a_n \mid 1 \leq i \leq n, n \in \mathbb{N}, a_i \in S \text{ or } a_i \in S^{-1}\}$

- G is cyclic iff. it is generated by a singleton.

I think that S_3 is not this, since one of σ, τ needed to generate S_3

But $H < S_3$ is a subgroup defined by the Cayley table and it is cyclic

- G is finitely generated iff. S is finite

Q: is $\{\sigma_1, \tau_1\}$ a finitely generating set of S_3

Let $S \subseteq G$. Consider $\{H_\alpha\}_{\alpha \in \Lambda}$, where each $H_\alpha \leq G$
$S \subset H_\alpha$

Since $S \subset G$
Then by (5.7),

$$H_S := \bigcap_{\alpha \in A} H_\alpha \text{ is a subgroup}$$

This is the smallest subgroup of G that contains S

Every subgroup that contains S must contain:

$$\langle S \rangle := \{a_1, a_2, a_3, \dots, a_n \mid 1 \leq i \leq n, n \in \mathbb{N}, a_i \in S \text{ or } a_i \in S^{-1}\}$$

does this mean that it must contain the generating set?

$\therefore \langle S \rangle \leq H_S$

$S \subset \langle S \rangle$ my understanding stops, but

$\langle S \rangle = H_S$: this means that H_S is the smallest subgroup that contains S

Also S is the generating set

(6.2) let G be a group,

S is a finite subset
$S = \{s_1, s_2, s_3, \dots, s_n\}$
or $\langle S \rangle = \langle s_1, s_2, s_3, \dots, s_n \rangle$

for $a \in G$
$\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ is cyclic

(6.3) The order of an element $a \in G$ is the order of of subgroup $\langle a \rangle$ of G

eg.
$S_3 = \langle \sigma_1, \tau_1 \rangle$ this implies that $\langle \sigma_1, \tau_1 \rangle$ generates the group S_3

subgroups $\begin{cases} \langle \sigma_1 \rangle = \langle e_{S_3}, \sigma_1, \sigma_2 \rangle & \text{order } 3 \\ \langle \tau_1 \rangle = \langle e_{S_3}, \tau_1 \rangle & \text{order } 2 \end{cases}$

(6.5) let G be a group

The powers a^k, $(k \in \mathbb{N})$ of $a \in G$ are either distinct <u>or</u>
there is a positive integer n s.t.
$a^m = 1 (= e_G)$ iff. $n \mid m$

Proof is incomprehensible :(

6.6 Given $\varphi: G \to H$ (homomorphism)

$$\varphi(\langle a_1, a_2, a_3, a_4, \dots a_n \rangle) = \langle \varphi(a_1), \varphi(a_2), \varphi(a_3), \dots, \varphi(a_n) \rangle$$

So, a generating set in G must also be a generating set in H (to prove)

since φ is a homomorphism:

$$\varphi(ab) = \varphi(a)\varphi(b)$$

6.7 If H is a non-trivial subgroup of $\mathbb{Z}$ then $H = \langle m \rangle$ for some $m \in \mathbb{Z}$

~

Sets of generators

Consider the $S_n := \{\text{permutations of } n\}$

or bijections

$(S_n, \circ)$

$|S_n| = n!$

6.8

- A cycle is a permutation $\sigma \in S_n$ of length r or r-cycle iff. there is a subset

$$\{i_1, i_2, i_3, \dots, i_r\} \subseteq \{1, 2, 3, \dots, n\}$$

of order r s.t.

i) $\sigma(i_j) = i_{j+1}$ for $1 \leq j < r$

ii) $\sigma(i_r) = i_1$

iii) $\sigma(m) = m$ where $m \notin \{i_1, i_2, i_3, \dots, i_r\}$

iii) implies that if m isn't in the list of indices, then the mth element stays where it is

ii) implies that the last element moves to the first place

i) implies that every other element in the cycle shifts along 1

eg $(2,3,7) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 2 & 4 & 5 & 6 & 3 \end{pmatrix}$

$2 \to 3$,

$3 \to 7$

$7 \to 2$

- Than this is a formalism for the cycle rotation on page 25

(6.9) r-cycles on S_n satisfy

a) $(i_1\, i_2\, i_3 \dots, i_r) = (i_2\, i_3 \dots i_r\, i_1)$

This means that $(2,3,7) = (3,7,2)$ (eg.)

b) $(i_1\, i_2 \dots i_r) = (i_1 \dots i_j)(i_j \dots i_r)$ (composition)

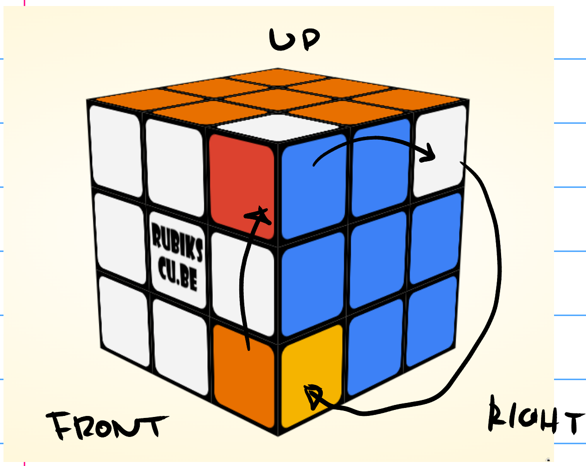
eg. $(2\ 3\ 7) = (2\ 3)(3\ 7) = (2\ 3) \circ (3\ 7)$

c) the order of $(i_1 \dots i_r)$ is r

d) Given $\tau \in S_n$, $\tau(i_1 \dots i_r)\tau^{-1} = (\tau(i_1) \dots \tau(i_r))$

Example of conjugate cycles

moves are U = Up clockwise
R = right clockwise
D = Down clockwise



r = right square
d = down square
f = front square
u = upper square
b = back square

this cycle is: ((rdf), (ruf), (rub))
and is equivalent to some combination of face turns A

By Corollary 6.10, any two cycles are conjugate

let σ be UP clockwise
((ruf), (luf), (lub), (rub)) is a cycle of corners
((uf), (ul), (ub), (ur)) is a cycle of edges

Then σ <=> UP clockwise is a disjoint cycle.

$\sigma \cdot A \cdot \sigma^{-1}$