Group Theory
7th Class

I More about cyclic groups

Recall G is a <u>cyclic group</u> if $G = \langle a \rangle$, for some $a \in G$
$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

<u>Prop</u> Every subgroup of a cyclic group is itself a cyclic group.

<u>Ex</u>
- $G = \mathbb{Z}$ subgroups are $\{0\} = \langle 0 \rangle$ and $n\mathbb{Z} = \langle n \rangle$ ← all cyclic subgroups
- $G = \mathbb{Z}_4$ subgroups are
  $\{[0]\} = \langle 0 \rangle$
  $\{[0], [2]\} = \langle 2 \rangle$
  $\{[0], [1], [2], [3]\} = \langle 1 \rangle$ ✓

<u>Proof</u> Let $G = \langle a \rangle$ be a cyclic group
Let $H \leq G$ be a subgroup

If H is the trivial subgroup, then $H = \{e\} = \langle e \rangle$ — done

Otherwise, $\exists\, a^k \in H$ with $a^k \neq e$.
note: $a^{-k} = (a^k)^{-1}$ is also in H, so we may assume $k > 0$

<u>Claim</u> $\boxed{H = \langle a^m \rangle}$, where $m = \min\{k : a^k \in H,\ a^k \neq e,\ k \in \mathbb{Z}_{>0}\}$

(Such an m exists by the well-ordering principle & above note)

<u>Proof of claim</u>

($\supseteq$) Since $a^m \in H$, we also have $\langle a^m \rangle \subseteq H$ (by a Prop proved last time)

($\subseteq$) Let $h \in H$. Then $h \in G = \langle a \rangle$, so $h = a^n$, for some $n \in \mathbb{Z}$

Write $n = mq + r$, for $q, r \in \mathbb{Z}$, $0 \leq r < m$

Then $a^{-mq} = (a^m)^{-q} \in \langle a^m \rangle \subseteq H$

$$\therefore\ H \ni \underset{\underset{H}{\Uparrow}}{a^n} \cdot \underset{\underset{H}{\Uparrow}}{a^{-mq}} = a^{n-mq} = a^r$$

$\therefore\ r = 0$ (since m is smallest $k>0$ s.t. $a^k \in H$

$\therefore\ n = mq$

$\therefore\ h = a^n = (a^m)^q \in \langle a^m \rangle$

This proves the claim, and hence the Prop. $\square$

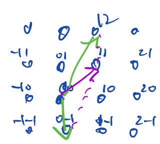
II A bit more on direct products of groups

$$G_1 \times G_2 = \{ (a_1, a_2) \mid a_1 \in G_1,\ a_2 \in G_2 \}$$

with $(a_1, a_2) \underset{\substack{\uparrow \\ \text{gp. op on } G}}{*} (b_1, b_2) := (a_1 \underset{\substack{\uparrow \\ \text{gp. op. on } G_1}}{*_1} b_1,\ a_2 \underset{\substack{\nwarrow \\ \text{gp. op. on } G_2}}{*_2} b_2)$

eg: (1) $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z} \subset \mathbb{R} \times \mathbb{R}$

$(0,-1) + (1,2) = (1,1)$



(2) $\underset{\substack{\{[0]_4,[1]_4,[2]_4,[3]_4\} \\ \uparrow \\ *_1 = + \\ e_1 = 0}}{\mathbb{Z}_4} \times \underset{\substack{\{[1]_3,[2]_3\} \\ \uparrow \\ *_2 = \cdot \\ e_2 = [1]}}{\mathbb{Z}_3^\times} = \{ ([0]_4, [1]_3), \ldots, ([3]_4, [2]_3) \}$

8 elements in all

Note: If $|G_1| = n_1$ & $|G_2| = n_2$, then $|G_1 \times G_2| = n_1 n_2$

or, $|G_1 \times G_2| = |G_1| \cdot |G_2|$

Question: If we know the orders of all elements in a pair of finite groups, G_1 and G_2, how can we find the orders of all elements in $G_1 \times G_2$?

Proof If $o(a_1) = n_1$ and $o(a_2) = n_2$, then

$$o(a_1, a_2) = \operatorname{lcm}(n_1, n_2)$$

that is: $\boxed{o(a_1, a_2) = \operatorname{lcm}(o(a_1), o(a_2))}$

Proof Suppose $(a_1,a_2)^k = e = (e_1,e_2)$. Then
$$\boxed{a_1^k = e_1 \ \& \ a_2^k = e_2.} \quad (*)$$

Recall:
$$\boxed{o(a_1,a_2) = \min\{\ell \in \mathbb{Z}_{>0} : (a_1,a_2)^\ell = e\}} \quad (**)$$

also
$$\boxed{\begin{array}{l} o(a_1) = n_1 = \min\{k_1 \mid a_1^{k_1} = e_1\} \\ o(a_2) = n_2 = \min\{k_2 \mid a_2^{k_2} = e_2\} \end{array}} \quad (***)$$

Hence:
$$\boxed{\underset{o(a_1)}{n_1} \mid \underset{a_1^k = e_1}{k} \quad \text{and} \quad n_2 \mid k} \quad (!) \quad (\text{by } (*) \text{ and Prop last time})$$

[recall: in general, if $b^m = e$ and $o(b) = n$, then $n \mid m$]

$\therefore \quad \operatorname{lcm}(n_1, n_2) \mid k \qquad$ (by def of lcm and (!))

$\therefore \quad o(a_1,a_2) = \operatorname{lcm}(n_1,n_2) \qquad$ (by $(**)$) $\qquad \boxtimes$

Ex (1) $G = \mathbb{Z}_4 \times \mathbb{Z}_6 \qquad$ What is $o([2]_4,[2]_6) = \operatorname{lcm}(2,3) = 6$

$o([2]_4) = 2 \qquad o([2]_6) = 3 \qquad o([3]_6) = 2$

How about $o([2]_4, [3]_6) = \operatorname{lcm}(2,2) = 2$

(2) $G = \mathbb{Z}_2 \times \mathbb{Z}_4$

$\mathbb{Z}_2$

a	$[0]_2$	$[1]_2$
$o(a)$	1	2

$\mathbb{Z}_4$

a	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$o(a)$	1	4	2	4

$\mathbb{Z}_2 \times \mathbb{Z}_4$

a	(0,0)	(0,1)	(0,2)	(0,3)	(1,0)	(1,1)	(1,2)	(1,3)
$o(a)$	1	4	2	4	2	4	2	4

Remark The lcm and gcd of two integers are related by the formula
$$\boxed{\gcd(a,b) \cdot \operatorname{lcm}(a,b) = a \cdot b}$$

$\alpha_i + \beta_i = \min(\alpha_i,\beta_i) + \max(\alpha_i,\beta_i)$

This can be shown, for instance, once we know the prime factorizations of a and b:

$$\begin{array}{l} a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \\ b = p_1^{\beta_1} \cdots p_k^{\beta_k} \end{array} \longrightarrow \begin{array}{l} \gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_k^{\min(\alpha_k,\beta_k)} \\ \operatorname{lcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \cdots p_k^{\max(\alpha_k,\beta_k)} \end{array}$$

III Revisit equivalence relations

Let S be a set w/ equiv relation $\sim$ on it. Recall $\sim$ satisfies 3 properties:

(1) reflexivity $a \sim a$

(2) symmetry $a \sim b \Rightarrow b \sim a$ $\quad \forall a,b,c \in S$

(3) transitivity $a \sim b,\ b \sim c \Rightarrow a \sim c$

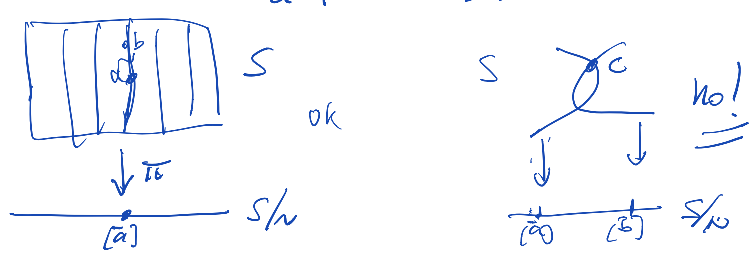
Let $[a] = \{ b \in S : b \sim a \}$ be the equivalence class of a.

and $S/\sim \; := \{$ equivalence classes of elements in $S\}$

We then have a function: $S \xrightarrow{\pi} S/\sim$

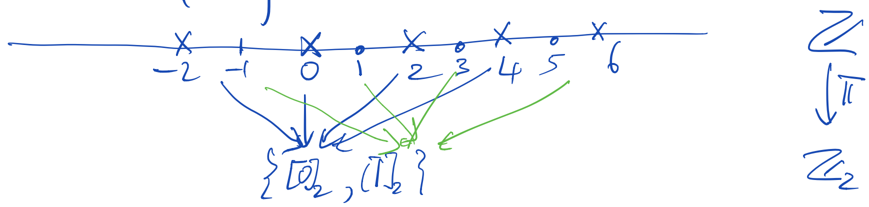
$a \longmapsto [a]$

Visually



Example On $\mathbb{Z}$, define for every n the equiv. relation $a \equiv b$ if $n \mid a-b$. Then $\mathbb{Z}_n$ is the set of equiv. classes.

eg:



Prop (1) $a \in [a]$

(2) $a \sim b \iff [a] = [b]$

(3) $[a] \cap [b] \neq \emptyset \iff [a] = [b]$

Proof (1) $a \sim a \overset{\text{(reflexivity)}}{\Longrightarrow} a \in [a]$

(2) ($\Rightarrow$) Suppose $a \sim b$. Then

$x \in [a] \Rightarrow x \sim a \underset{\text{since } a \sim b \text{ and transitivity}}{\Longrightarrow} x \sim b \Rightarrow x \in [b]$

similarly, $x \in [b] \Rightarrow x \in [a]$ (by symmetry) This shows $[a]=[b]$

$(\Leftarrow)$ Suppose $[a]=[b]$. Then $\underset{\text{by (1)}}{a \in [a]} = [b] \overset{\text{def}}{\Longleftrightarrow} a \sim b$

(3) Suppose $[a] \cap [b] \neq \emptyset$. Then $\exists x \in [a] \cap [b]$, i.e., $x \in [a]$ and $x \in [b]$, i.e., $x \sim a$ and $x \sim b$

$\underset{\text{by symmetry}}{\Longrightarrow} a \sim x$ and $x \sim b \underset{\text{by transitivity}}{\Longrightarrow} a \sim b \underset{\text{by (2)}}{\Longrightarrow} [a]=[b]$ ∎

Consequently, $\sim$ defines a partition of S into disjoint, non-empty subsets of S, whose union is all of S:

$$S = \coprod_{[x] \in S/\sim} \pi^{-1}([x])$$

where, for a function $f: S \to T$, and a subset $A \subset T$, $f^{-1}(A) = \{s \in S : f(s) \in A\}$

IV Cosets of a subgroup

Def/Prop Let $H \leq G$ be a subgroup of G. Define an equiv. relation on G by setting, for $a, b \in G$:

$$a \sim b \Longleftrightarrow ab^{-1} \in H$$

Verify that $\sim$ is, indeed, an equiv. rel:

(1) $a \sim a$: $aa^{-1} \in H$, since $aa^{-1} = e \in H$

(2) $a \sim b \Rightarrow b \sim a$: $a \sim b \Rightarrow ab^{-1} \in H \Rightarrow (\underset{ba^{-1}}{\underset{\shortparallel}{ab^{-1}}})^{-1} \in H \Rightarrow b \sim a$

(3) $a \sim b \;\&\; b \sim c \Rightarrow a \sim c$ $\quad ab^{-1} \in H \;\&\; bc^{-1} \in H$

$$\Rightarrow \underbrace{(ab^{-1}) \cdot (bc^{-1})}_{\parallel} \in H \qquad \Rightarrow a \sim c$$

$$a(b^{-1}b)c^{-1} = a \cdot e \cdot c^{-1} = ac^{-1}$$

$\boxed{}$

To be continued.