Group Theory
6^{th} class

I Subgroups

Let G be a group (written multiplicatively: $*=\cdot$)

$\emptyset \neq H \subseteq G$ is a subgroup if $(H,\cdot)$ is a group.

Notation: $H \leq G$ (or, $H < G$)

Criteria: H is a subgroup $\iff \begin{cases} ab \in H & \forall a,b \in H \\ a^{-1} \in H & \forall a \in H \end{cases}$

$\iff ab^{-1} \in H, \ \forall a,b \in H$

II Cyclic groups

For $a \in G$, write:

$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ – the subgroup generated by a

$= \{\ldots, a^{-2}, a^{-1}, \underset{e}{a^0}, a, a^2, a^3, \ldots\}$

G is cyclic if: $G = \langle a \rangle$, for some $a \in G$

Eg: (1) $G = (\mathbb{Z}, +, 0)$ $\quad \mathbb{Z} = \langle 1 \rangle$ (and also $\mathbb{Z} = \langle -1 \rangle$)

the infinite cyclic group

(2) $G = (\mathbb{Z}_n, +, [0])$ $\quad \mathbb{Z}_n = \langle [1] \rangle = \{[0], [1], [2], \ldots, [n-1]\}$

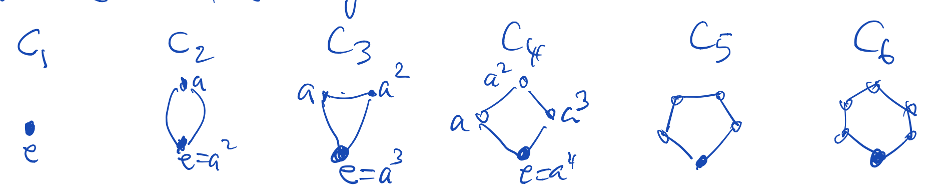
the cyclic group of order n

Rem This group also can be written multiplicatively:

$C_n = \langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ $\quad (a^n = e)$

$C_n \longleftrightarrow \mathbb{Z}_n \qquad a^k \longleftrightarrow [k]_n$

Visualize these cycles:



Another criterion for deciding when a subset $\emptyset \neq H \subseteq G$ is a subgroup, but only valid for finite (sub)groups.

Prop A finite, non-empty subset H of a group G is a subgroup $\iff$ ($ab \in H$, for all $a, b \in H$)

Proof ($\Longrightarrow$) clear

($\Longleftarrow$) Let $b \in H$. We claim: $b^{-1} \in H$

- if $b = e$, then $b^{-1} = e \in H$. So we may assume $b \neq e$
- Clearly, $\{b, b^2, \dots\} \subseteq H$ (since H is closed under multiplication)

hence this set is also finite; finite set (by assumption)

$\therefore$ there must be at least one repetition (i.e., not all powers of b are distinct). That is:

$\exists\, n > m$ st $b^n = b^m$

$\therefore \quad b^{n-m} = e$

$\left(\underset{\text{since } b \neq e}{\Longrightarrow} \quad n - m > 1 \right)$

$\therefore \quad b \cdot b^{n-m-1} = e$

$\therefore \quad b^{-1} = b^{n-m-1}$

This proves the claim. Thus $ab^{-1} \in H$, $\forall a, b \in H$

$\therefore$ H is a subgroup by previous criterion $\blacksquare$

Lemma Let $H \leq G$ be a subgroup, and $a \in H$.

Then $\langle a \rangle \leq H$

the subgroup of G generated by $a \in H \leq G$

Proof $a \in H \Rightarrow \begin{cases} a^n \in H & , \forall n \geq 1 \\ a^0 = e \in H & , n = 0 \\ a^n = (a^{-n})^{-1} \in H & , \forall n < 0 \end{cases}$

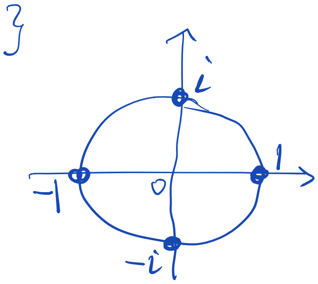
$\therefore a^n \in H, \ \forall n \in \mathbb{Z}$, i.e., $\langle a \rangle \subseteq H$ ∎

Examples

(1) $G = \mathbb{Z}_6 = \{0,1,2,3,4,5\}$ $\quad H = \langle 2 \rangle = \{0, 2, 4\}$

$K = \langle 3 \rangle = \{0, 3\}$

(2) $G = \{1, i, -1, -i\} \subseteq \mathbb{C}^{\times}$



1	i	-1	$-i$
i	-1	$-i$	1
-1	$-i$	1	i
$-i$	1	i	-1

$\langle 1 \rangle = \{1\}$

$\langle i \rangle = \{1, i, -1, -i\} = G$

$\langle -1 \rangle = \{1, -1\}$

$\langle -i \rangle = \{1, -i, -1, i\} = G$

III Orders of elements in a group

Want to define a function $\quad G \xrightarrow{o} \mathbb{Z}_{>0} \cup \{\infty\}$

$a \longmapsto o(a)$

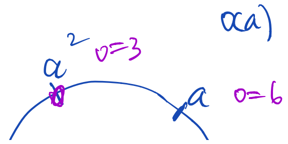
Def The __order__ of an element $a \in G$, written $o(a)$, is the smallest positive integer m such that $a^m = e$ (if such exists), or ∞ (otherwise).

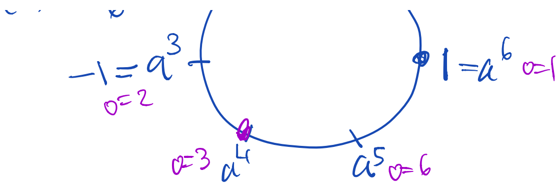
Ex (1) $G = \mathbb{Z}_6 = \{0, \dots, 5\}$

a	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$o(a)$	1	6	3	2	3	6

$(\underset{\#}{4} \quad 4+4=8=\underset{\#}{2} \quad 4+4+4=12=0)$

(2) G





$\therefore\ o([4]_6) = 3$

$\mathbb{Z}_8^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

(3) $G = \mathbb{Z}_8^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\}$
$= (\mathbb{Z}_8^\times, \cdot, [1])$

(note: in $(\mathbb{Z}_8, +, 0)$: $o([1]) = 8$)

a	$[1]$	$[3]$	$[5]$	$[7]$
$o(a)$	1	2	2	2

$3^2 = 9 \equiv 1 \pmod 8$
$5^2 = 25 \equiv 1 \pmod 8$
$7^2 = 49 \equiv 1 \pmod 8$

(4) $G = \{1, i, -1, -i\} = \langle i \rangle \subset \mathbb{C}^\times$

Orders: 1 4 2 4

We shall see: $\{\pm 1, \pm i\} \cong C_4 \cong \mathbb{Z}_4$

Prop Let $a \in G$. Then

(a) If $o(a) = \infty$, then $a^m \neq a^n$, $\forall m \neq n$.

(b) Suppose $o(a) = n$ and $k \in \mathbb{Z}$. Then
$$\boxed{a^k = e \iff n \mid k}$$

(c) Suppose $o(a) = n$ and $k, m \in \mathbb{Z}$. Then
$$a^k = a^m \iff k \equiv m \pmod n,$$
and so $\langle a \rangle = \{\underset{\substack{\shortparallel \\ e}}{a^0}, a^1, \dots, a^{n-1}\}$ and $|\langle a \rangle| = n$.
(that is $|\langle a \rangle| = o(a)$)

Proof (sketch) (a) Suppose $a^m = a^n$ for some $m, n \in \mathbb{Z}$ (say $m \geq n$)
Then $a^{m-n} = e$ $\underset{\text{since } o(a)=\infty}{\Longrightarrow}$ $m - n = 0 \Rightarrow m = n$.

(b) ($\Rightarrow$) Suppose $o(a) = n$. Write $k = nq + r$ w/ $0 \leq r < n$

$a^k = e \Rightarrow e = a^k = a^{nq+r} = a^{nq} \cdot a^r = (a^n)^q \cdot a^r$
$\underset{\text{since } o(a)=n}{=} e^q \cdot a^r$
$= e \cdot a^r = a^r$

$\therefore\ a^r = e$

$\therefore\ r = 0$ (since $o(a) = n$ & $r < n$)

$\therefore\ k = nq$, i.e. $n \mid k$

($\Leftarrow$) if $n|k$, then $k=nq \Rightarrow a^k=(a^n)^q=e^q=e$

(c) Exercise. $\boxed{\not{k}}$

(IV) Direct Products of Groups

Let G_1 & G_2 be two groups. Then their direct product,

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

is a group with:

* $(a_1,a_2)\cdot(b_1,b_2) = (a_1b_1,\ a_2b_2)$
* $e = (e_1,e_2)$
* $(a_1,a_2)^{-1} = (a_1^{-1}, a_2^{-1})$

Ex (1) $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R}$

* $(x_1,y_1)+(x_2,y_2)=(x_1+x_2, y_1+y_2)$
* $e=(0,0)$
* $-(x,y) = (-x,-y)$

similarly for $\mathbb{R}^n$ — underlying group structure on the vector space $\mathbb{R}^n$
$+$ = vector addition

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

multiplication table:

(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,0)	(0,1)	(0,0)

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

multiplication table courtesy of Group Explorer v.3.0 $\downarrow$

Multiplication Table for $\mathbb{Z}_2 \times \mathbb{Z}_4$

$\langle e,e\rangle$	$\langle a,e\rangle$	$\langle e,b\rangle$	$\langle a,b\rangle$	$\langle e,b^2\rangle$	$\langle a,b^2\rangle$	$\langle e,b^3\rangle$	$\langle a,b^3\rangle$
$\langle a,e\rangle$	$\langle e,e\rangle$	$\langle a,b\rangle$	$\langle e,b\rangle$	$\langle a,b^2\rangle$	$\langle e,b^2\rangle$	$\langle a,b^3\rangle$	$\langle e,b^3\rangle$
$\langle e,b\rangle$	$\langle a,b\rangle$	$\langle e,b^2\rangle$	$\langle a,b^2\rangle$	$\langle e,b^3\rangle$	$\langle a,b^3\rangle$	$\langle e,e\rangle$	$\langle a,e\rangle$
$\langle a,b\rangle$	$\langle e,b\rangle$	$\langle a,b^2\rangle$	$\langle e,b^2\rangle$	$\langle a,b^3\rangle$	$\langle e,b^3\rangle$	$\langle a,e\rangle$	$\langle e,e\rangle$
$\langle e,b^2\rangle$	$\langle a,b^2\rangle$	$\langle e,b^3\rangle$	$\langle a,b^3\rangle$	$\langle e,e\rangle$	$\langle a,e\rangle$	$\langle e,b\rangle$	$\langle a,b\rangle$
$\langle a,b^2\rangle$	$\langle e,b^2\rangle$	$\langle a,b^3\rangle$	$\langle e,b^3\rangle$	$\langle a,e\rangle$	$\langle e,e\rangle$	$\langle a,b\rangle$	$\langle e,b\rangle$
$\langle e,b^3\rangle$	$\langle a,b^3\rangle$	$\langle e,e\rangle$	$\langle a,e\rangle$	$\langle e,b\rangle$	$\langle a,b\rangle$	$\langle e,b^2\rangle$	$\langle a,b^2\rangle$
$\langle a,b^3\rangle$	$\langle e,b^3\rangle$	$\langle a,e\rangle$	$\langle e,e\rangle$	$\langle a,b\rangle$	$\langle e,b\rangle$	$\langle a,b^2\rangle$	$\langle e,b^2\rangle$

Subgroups

$H_0 = \langle\ \langle e,e\rangle\ \rangle$ is the trivial subgroup $\{\ \langle e,e\rangle\ \}$.
$H_1 = \langle\ \langle a,e\rangle\ \rangle$ is a subgroup of order 2.
$H_2 = \langle\ \langle e,b^2\rangle\ \rangle$ is a subgroup of order 2.
$H_3 = \langle\ \langle a,b^2\rangle\ \rangle$ is a subgroup of order 2.
$H_4 = \langle\ \langle a,e\rangle, \langle e,b^2\rangle\ \rangle$ is a subgroup of order 4.
$H_5 = \langle\ \langle e,b\rangle\ \rangle$ is a subgroup of order 4.
$H_6 = \langle\ \langle a,b\rangle\ \rangle$ is a subgroup of order 4.
$H_7 = \langle\ \langle a,e\rangle, \langle e,b\rangle\ \rangle$ is the group itself.

User-defined subsets

(None)

Partitions

(None)