Ch3: Finite Groups ; subgroups.

Def: The order of a group G in the number of element in G, the order of G is denoted by $|G|$.

exp: $|\mathbb{Z}_7^*, \otimes_7| = 6$

$|\mathbb{Z}_4, \oplus_4| = 4$

$|\mathbb{Z}, +| = \infty$

exp: $(U(10), \otimes_{10})$

$U(10) = \{1, 3, 7, 9\}$

$U(12) = \{m \in \{1, 2, \dots 12\}, g.c.d(m, 12) = 1, \otimes_{12}\}$

$|U(12), \otimes_{12}| = 4$

$U(12) = \{1, 5, 7, 11\}$

is a group.

Def: Let G be a group, let $g \in G$ then the order of g written $|g|$ is the smallest positive integer n such that $g^n = e$.

If No such integer exists then $|g| = \infty$ (Def of order of an element).

Def: if $(G, *)$ is a group, let $g \in G$ then $g^0 = e$.

exps:

① $G = (\mathbb{Z}, +)$, Find the order of 2, 1.

order of 2		order of 1	order of 0 :
	$2^1 = 2$	$1^1 = 1$	$0^1 = 0$
2+2	$2^2 = 4$	$1^2 = 2$	
2+2+2	$2^3 = 6$	$1^3 = 3$	$\|0\| = 1$
2+2+2+2	$2^4 = 8$	$1^4 = 4$	
	⋮	⋮	
	$2^{\boxed{x}} = \textcircled{0}$ → identity	$\|1\| = \infty$	

$|2| = \infty$ ∴ ما في x يعطيني 0

② $G = (\mathbb{Z}_{12}, \oplus_{12})$ Find order of 2, ⑤, ④, ⑪ → 12 (classes).

(5 → 12, 4 → 3)

$\mathbb{Z}_{12} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

2	5	4	11
$2^1 = 2$	$5^1 = 5$	$4^1 = 4$	$11^1 = 11$
$2^2 = 4$	$5^2 = 10$	$4^2 = 8$	⋮
$2^3 = 6$	$5^3 = 3$	$4^3 = 12 = 0$	
$2^4 = 8$	$5^4 = 8$	so $\|4\| = 3$	⋮
$2^5 = 10$	$5^5 = 1$		
$2^6 = 0$	$5^6 = 6$		$11^{12} = 0$
	$5^7 = 11$		so $\|11\| = 12$
$\|2\| = 6$	$5^8 = 4$		
	$5^9 = 9$		
	$5^{10} = 2$		
	$5^{11} = 7$		
	$5^{12} = \textcircled{12} = 0$		
	$5^{12} = 0$		
	so $\|5\| = 12$		

15 عدد صحيح موجب أولي مع 1

الأعداد من 1 ← 14 حيث أن العدد الصحيح المشترك بينهم واحد

Exp 1: $(U(15), \otimes_{15})$, $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$

Book

$|2| \Rightarrow 2^1 = 2$

$2^2 = 4$

$2^3 = 8$

$16 = 2^4 = 1$

mod 15 = 1

So $|2| = 4$

$|11| \rightarrow 11^1 = 11$

$11^2 = 1$

So $|11| = 2$

$|7| \Rightarrow 7^1 = 7$

$7^2 = 4$

$7^3 = 13$

$7^4 = 1$

So $|7| = 4$

---

exp 2: $(Z_6, \oplus_6)$:

Note, $|e| = 1$ دائماً

Book

$|2| \rightarrow 2^1 = 2$

$2^2 = 4$

$2^3 = 6$

$2^4 = 8$

$2^5 = 0 = e$

So $|2| = 5$

$|7| \rightarrow 7^1 = 7$

$7^2 = 4$

$7^3 = 1$

$7^4 = 8$

$7^5 = 5$

$7^6 = 2$

$7^7 = 9$

$7^8 = 6$

$7^9 = 3$

$7^{10} = 0$

$|7| = 10$

$|5| \rightarrow 5^1 = 5$

$5^2 = 0$

$|5| = 2$

$|6| \rightarrow 6^1 = 6$

$6^2 = 2$

$6^3 = 8$

$6^4 = 4$

$6^5 = 0$

$|6| = 5$

exp 3 : $(\mathbb{Z}, \oplus)$ $|2| = \infty$

Back

$|3| = \infty$

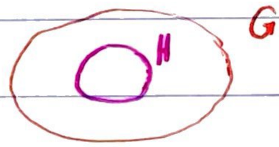
$|5| = \infty$

$|0| = 1$ because its e.

Def (subgroup): If a subset H of a group G is itself a group under the operation of G, we say that H is a subgroup of G.

صياغة ثانية

let G be a group, let H a nonempty subset of G, then H is a subgroup of G iff $(H, *)$ is a group. where $*$ is the same operation on G and we write $H \leq G$.



exp: - $H = (2\mathbb{Z}, \oplus)$ is a subgroup of $G = (\mathbb{Z}, \oplus)$.

الأعداد الزوجية الصحيحة

H its a group and G its a group

$\rightarrow$ H subgroup of G.

subgroup لـ

- $(5\mathbb{Z}, \oplus) \leq (\mathbb{Z}, \oplus)$
- $(7\mathbb{Z}, \oplus) \leq (\mathbb{Z}, \oplus)$
- $\{0\} \leq (\mathbb{Z}, \oplus)$.

$\leftarrow$ الأعداد الفردية مش ما بتشكل subgroups لأنه

لما أجمعهم ما بعطوني أعداد فردية ∴ ما بنفع لـ H فالجمع

$H = (1, 3, 5)^{\times}$

Note: subgroup

$H \neq \emptyset$, $H \subseteq G$. then $(H, *)$ is a subgroup of G.

Written $H \leq G$ iff $(H, *)$ is a group.

i.e. iff
1. closure $a * b \in H$ $\forall a, b \in H$.
2. $e \in H$.
3. $a * (b * c) = (a * b) * c$, $\forall a, b, c \in H$
4. $\forall a \in H$, $\exists a^{-1} \in H$.

exp: $(\mathbb{R}, +)$ is a group, $H = (\mathbb{Z}, +)$ is a group

So $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$

exp. $G(\mathbb{Z}, \oplus_4)$

① $(H = \{0, 2\}, \oplus_4)$

$\oplus_4$	0	2
0	0	2
2	2	0

Associative ✓

$e = 0$ ✓

$0^{-1} = 0$, $2^{-1} = 2$ } inverses ✓

$H \leq G$; H is a subgroup of G. So H its a group

② $G(\mathbb{Z}, \oplus_4)$

$(K = \{0, 1\}, \oplus_4)$

$\oplus$	0	1
0	0	1
1	1	2

$e = 0$

$0^{-1} = 0$

$1^{-1} = \emptyset$ inverse(s) is to

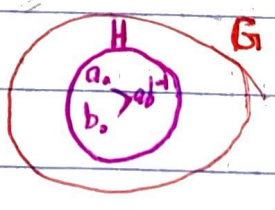
So K not a group

So $K \not\leq G$; K not a subgroup of G

Theorem (one step subgroup Test):

Let G be a group and H a nonempty subset of G. If ab^{-1} is in H whenever a and b are in H, then H is a subgroup of G.

(In additive notation if $a-b$ is in H whenever a and b are in H, then H is a subgroup of G)



exp: let $G(\mathbb{Z}, +)$ → $e = 0$.

$H = (2\mathbb{Z}, +)$.

$H \neq \emptyset$ (nonempty) since $0 \in H$, let $a, b \in H$

$a = 2K$, $b = 2L$ $\Rightarrow a - b = 2K - 2L = 2(K-L) \in 2\mathbb{Z}$

So $(2\mathbb{Z}, +) \leq (\mathbb{Z}, +)$

proof of Theorem :

يعني اوصل $ab^{-1} \in H$

$\Rightarrow$ Given $H \neq \phi$, $H \subseteq G$ and H is a subgroup of G

So let $a, b \in H$

$\rightarrow a, b^{-1} \in H$

$\Rightarrow ab^{-1} \in H$ ✓

$\Leftarrow$ conversly, suppose $H \neq \phi$ and whenever $a, b \in H$ then $ab^{-1} \in H$.

need to show H is subgroup of G : 1, 2, 3.

1. Associative : $\forall a, b, c \in H \Rightarrow a, b, c \in G$.

So since G is a group $a(bc) = (ab)c$.

حطيت بدل b

2. Identity. $H \neq \phi \Rightarrow \exists a \in H \Rightarrow a, a \in H \Rightarrow aa^{-1} = e \in H$.

3. let $a \in H \Rightarrow e, a \in H \Rightarrow ea^{-1} = a^{-1} \in H$.

#

exp 5 : let G be abelian group under multiplication with identity e, then $H = \{x^2 : x \in G\}$ is a subgroup.

proof : By one step test

$H \neq \phi$ since $e = e^2 \in H$

Next, suppose $a, b \in H$

$\rightarrow a = x^2$, $b = y^2$

$ab^{-1} = x^2 (y^2)^{-1}$

$= x x y^{-1} y^{-1}$

التبديل لأنه Abelian

$= x y^{-1} x y^{-1}$

$= (xy^{-1})^2$, $xy^{-1} \in H$

$\Rightarrow (xy^{-1})^2 \in H$ #.

Theorem 3.2 (Two step subgroup Test)

Let G be a group and let H be a nonempty subset of G. If ab is in H whenever a and b are in H (H is closed under the operation), and a^{-1} is in H whenever a is in H (H is closed under taking inverse), then H is a subgroup of G.

↳ $H \neq \phi$, $H \subset G$ is a subgroup $\Leftrightarrow$ 1. closure $\forall a,b \in H$, $ab \in H$.

2. $\forall a \in H \Rightarrow a^{-1} \in H$.

$\Rightarrow$ Trivial

$\Leftarrow$ so condition 1, 3 on left side are satisfied.

left 2, 4 above.

② let $a,b,c \in H$ is $(ab)c = a(bc)$ since G is a group.

③ let $a \in H \Rightarrow a^{-1} \in H \Rightarrow a.a^{-1} = e \in H$. #

---

exp 6 : $G = (\mathbb{R}^*, .)$

$H = Q^c \cup \{1\}$.

$K = \{x \geq 1\}$.

} subgroup or not.

H not subgroup of G : $\sqrt{2} \in H$ but $\sqrt{2}.\sqrt{2} = 2 \notin H$.

K not subgroup of G : $2 \in K$ but $2^{-1} \notin K$.

exp 8 : In $\mathbb{Z}_{10}$, $\langle 2 \rangle$ its mean : $\{ 2^n, n \in \mathbb{Z} \} = \{ 0, 2, 4, 6, 8 \}$ (finite)

$\{0, 2, 4, 6, 8\} \leq \mathbb{Z}_{10}$.

exp 9 : In $\mathbb{Z}$, $\langle -1 \rangle = \mathbb{Z}$, addition.

$(-1)^2 = -1 + -1 = -2$

$\rightsquigarrow \{ \ldots, 3, 2, 1, 0, -1, -2, -3, -4, \ldots \}$

$\Rightarrow \langle -1 \rangle = \mathbb{Z}$.

Theorem : Finite subgroup test

Let G be a group, let H be a nonempty subset of G, then $H \leq G$ iff $ab \in H \quad \forall a, b \in H$.

pf:

$\Rightarrow$ suppose $H \leq G \Rightarrow a, b \in H$ then $ab \in H$

$\Leftarrow$ if $a, b \in H \quad \forall a, b \in H$ then $H \leq G$. ✓

proof: ① closure : given

② Inverse ; let $x \in H \rightarrow (H \neq \emptyset)$

then if $x = e$ then we are done.

if $x \neq e$ then $x^{-1} \in H$ (why?) $\rightarrow x, x^2, x^3, \ldots x^n \in H$

But H is finite so

$\exists K, L ; x^K = x^L , K > L$

$\Rightarrow x^{K-L} = e , K-L > 1$

$\Rightarrow x^{K-L} = x^1 . x^{K-L-x} = e$

$x^{-1} \in H$

③ Identity : $e = x . x^{-1} \in H$.

④ Associative : ✓

Def (Center of group)

The center, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G. In symbols,

$$Z(G) = \{ a \in G \ / \ ax = xa \text{ for all } x \text{ in } G \}.$$

[The notation $Z(G)$ comes from the fact that the German word for center in Zentrum. The term was coined by j.A. de squier in 1904]

← يعني لو أجيب أي رقمين داخل G وأجمعهم من اليمين او اليسار بيطلع متساوي .

exp: $(Z_6, \oplus_6) = G$, What is the center of G?

if G is abelian then $\underset{\text{center}}{Z(G)} = G$ — كل عناصر G اللي تتبدل مع كل العناصر .

$$Z(G) = \{0, 1, 2, 3, 4, 5, 6\}.$$

exp: $G = GL(2, \mathbb{R})$ matrises

$$Z(G) = \{ A \ / \ A \cdot B = B \cdot A \quad \forall \ B \in G \}$$ — ما بقدر أحدد بالزبط

$$= \{ I_2, \begin{bmatrix} \circ & \circ \\ \circ & \circ \end{bmatrix}, \ldots \}$$

بس مطلوب تحفظوها

$$\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} \notin Z(G)$$

عشان أثبت بجيب مصفوفة بضربها من اليمين ومن اليسار ولازم الجواب يطلع مش متساوي .

Thm 3.5 : Center is a subgroup.

The center of a group G is a subgroup of G.

proof: By two step test:

$Z(G) \neq \emptyset$ since $e \in Z(G)$.

① let $a, b \in Z(G) \Rightarrow (ab)g \overset{\text{Ass.}}{=} a(bg) \overset{b \in Z}{=} a(gb) = (ag)b \overset{a \in Z}{=} (ga)b = g(ab)$

So $ab \in Z(G)$ — لأنه ab تبدلت مع كلشي

H 3 - X

proof: ② let $a \in Z(G), g \in G$ to prove $a^{-1}g = g a^{-1}$, $g \in G$.

$\Rightarrow ag = ga$ (multiply a^{-1} from right)

$a^{-1}ag = a^{-1}ga$

$g = a^{-1}ga$ (multiply a^{-1} from left)

$ga^{-1} = a^{-1}gaa^{-1}$

$\boxed{ga^{-1} = a^{-1}g}$

So $a^{-1} \in Z(G)$ #

So center of group G is a subgroup of G.

Def ; Centralizer of a in G

let a be a fixed element of a group G. The centralizer of a in G, C(a) is the set of all elements in G that commute with a, In symbols

$C(a) = \{ g \in G \mid ga = ag \}$.

Note: $Z(G) = \cap C(g)$, $g \in G$.

Thm 3.6: C(a) is a subgroup

For each a in group G, the centralizer of a is a subgroup of G.

Examples to center of groups:

① $(\mathbb{Z}_4, \oplus_4)$

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Identity = 0

Identity always on the center

$1+2=3$, $2+1=3$ ✓ } So $1 \in Z(G)$.

$3+1=0$, $3+1=0$ }

$2+1=3$, $1+2=3$ ✓ } So $2 \in Z(G)$

$2+3=1$ $3+2=1$ }

$\rightarrow Z(G) = \{0, 1, 2, 3\} = \mathbb{Z}_4$ 3 same ↑ so $3 \in Z(G)$.

Note: If G is Abelian Then $Z(G) = G$.

② S_3 not Abelian

	P_0	P_1	P_2	μ_1	μ_2	μ_3
P_0	P_0	P_1	P_2	μ_1	μ_2	μ_3
P_1	P_1	P_2	P_0	μ_3	μ_1	μ_2
P_2	P_2	P_0	P_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	P_0	P_1	P_2
μ_2	μ_2	μ_3	μ_1	P_2	P_0	P_1
μ_3	μ_3	μ_1	μ_2	P_1	P_2	P_0

$\rightarrow P_1 \mu_1 = \mu_3$ $\mu_1 P_1 = \mu_2$ $\times P_1$

$P_2 \mu_1 = \mu_2$ $\mu_1 P_2 = \mu_3$ $\times P_2$

μ_1, μ_2, μ_3 ✗

$Z(G) = \{P_0\}$ P_0 only the center.

e