① MATH 407

3/30/18

⊛ Cyclic Groups $\langle a \rangle = G$, some a:

<u>Infinite:</u> $k \Rightarrow a^k$ bijection

<u>Finite:</u> $\langle a \rangle = \{a^0, a^1, \dots, a^{k-1}\}$

<u>Thm:</u> All subgroups of cyclic group are cyclic.

$H = \langle a^k \rangle$

$o(a^k) = l = |H|$

$n \mid kl$ since $(a^k)^l = e$

Let $\gcd(n,k) = d$

$n' = \frac{n}{d}$, $k' = \frac{k}{d}$

$n' \mid k'l$ so $n' \mid l$

$a^{kn'} = a^{k'(dn')} = a^{k'n} = a^{nk'} = e$

* If $\langle a^k \rangle = G$

$o(a^k) = n$

$d = 1$

$\gcd(k,n) = 1 \in \{1, \dots, k-1\}$

$|\text{generators of } G| = \varphi(n)$

* Groups order $1, 2, 3, 5, 7, \dots, p$ (prime) $\Rightarrow$ all cyclic

* Order 4: a) Cyclic group

b) klein 4-group

$(\longrightarrow)$

×	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

∵ $a \cdot b \neq e$ or $a \cdot b \neq b$,
$a \cdot b = c$
∴ Abelian, reflection over main diagonal

* Order 6 : a) Cyclic group
b) Non-cyclic group
i) All elements $\neq e$, $o(g) = 2$

×	e	a	b
e	e	a	b
a	a	e	
b	b		e

∵ $a \cdot b \neq e$,
$a \cdot b \neq a$,
$a \cdot b \neq b$
then, $a \cdot b = c$

extend to order-4 klein-group

	×	e	a	b	c	d	f
	e	e	a	b	c	d	f
	a	a	e	c	b	f	d
	b	b	c	e	a	$\boxed{f}$	$\boxed{d}$
	c	c	b	a	e		
add for order-6	d	d					
	f	f					

contradiction

ii) There is element a of order 3
$(\longrightarrow)$

③

×	e	a	a^2
e	e	a	a^2
a	a	a^2	e
a^2	a^2	e	a

$\therefore \langle a \rangle = \{e, a, a^2\}$

$\langle a \rangle b = \{eb, ab, a^2b\}$
$= [b]$

↓

extend to

↓

×	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	ab ①	a^2b ②	$b^2=e$ ③	$ab^2=a$	$a^2b^2=a^2$
ab	ab	a^2b	b	a	a^2	e
a^2b	a^2b	a	ab	a^2	e	a

$☆_1$: $ba = ab$ or a^2b

$☆_2$: $ba^2 = aba = a^2b$

$☆_3$: $(ab)(ab) = a^2b^2 = a^2$

$(a^2b)(a^2b) = a$

$\therefore b^2 = e$

or $(ab)^2 = e$

or $(a^2b) = e$

$o(a)=3$, $o(b)=2$
$o(ab)=6$

$e, (ab)^1 = ab, (ab)^2 = a^2, (ab)^3 = b, (ab)^4 = a, (ab)^5 = a^2 b$

$\therefore$ If Abelian, then cyclic
Must have $ba = a^2 b$

$$\begin{aligned} ba &= a^2 b \\ ba^2 &= (ba)a \\ &= (a^2 b)a \\ &= a^2(a^2 b) \\ &= ab, \quad \because o(a)=3,\ a^2 \cdot a^2 = a^4 = a^1 \end{aligned}$$

* Note: Look up Table 3.3.3 in book for example of non-Abelian S_3

* $G = H \cdot K = \{hk : h \in H, k \in K\}$
  $H = \langle a \rangle$ $K = \langle b \rangle$

In general, $H \cdot K \subseteq G$ (instead of $H \cdot K = G$)

Thm. Suppose $\star$ for any h, k in $H \times K$, $\exists k' \in K$ s.t. $hkh^{-1} = k'$.

$\star$ $hKh^{-1} \subseteq K = \{hkh^{-1} : k \in K\}$

⑤

$hK \subseteq Kh \ , \ \forall h \in H$

$h^{-1}K \subseteq Kh^{-1}$

$h(h^{-1}K)h \subseteq h(Kh^{-1})h$

$h^{-1}K = \{h^{-1}k : k \in K\}$

$h(h^{-1}K) = \{h(h^{-1}k) : k \in K\}$

$h(h^{-1}K)h = \{\cancel{h}(\cancel{h}^{-1}k)h : k \in K\}$

$= \{kh : k \in K\}$

$Kh \subseteq hK$