(1) MATH 407
3/28/18
$\underline{G}$ group, $\underline{H}$ subgroup

$a \sim_H b$ iff $ab^{-1} \in H$
iff $a \in Hb = \{hb : h \in H\}$
right coset of H containing B

$[b]_H = [b]_{\sim H} = Hb$

$\{[b]_H : b \in G\}$ partition H
$\{Hb : b \in G\} = \{Hb_1, \ldots, Hb_k\}$
$|Hb| = |H|$
$|G| = k|H|$
$\frac{|G|}{|H|} = k = ind_G(H)$

* Lagrange Thm. If G is a finite group, H subgroup, then $|H|$ divides $|G|$

x $G = \mathbb{Z}$
Subgroup $H = n\mathbb{Z}$, $n \in \mathbb{N}$, $n > 1$
$= \langle n \rangle$
$a \sim_H b$ iff $a - b \in H$
$a - b \in n\mathbb{Z}$
$n \mid (a-b)$
$a \equiv b \pmod{n}$

$\{k + n\mathbb{Z} : k = 0, 1, \cdots, n-1\}$
Partition of $\mathbb{Z}$

* Cyclic group: $G = \langle a \rangle$ some $a \in G$
$= \{a^k : k \in \mathbb{Z}\}$

* Thm. If H is a subgroup of cyclic group G, then H is cyclic

Pf. Let $I \subseteq \mathbb{Z}$ consist of k s.t. $a^k \in H$
If $k, l \in I$,

$$a^{k-l} = a^k a^{-l} = a^k (a^l)^{-1}$$

$\because a^k \in H$, $a^l \in H$, then $a^k (a^l)^{-1} \in H$
$k - l \in I$

I is closed under subtraction. There is $d \in \mathbb{Z}^+$ s.t. $I = d\mathbb{Z} = \{dn : n \in \mathbb{Z}\}$

$$H = \{(a^d)^n : n \in \mathbb{Z}\} = \langle a^d \rangle$$

Note if $a \in G$, $|G| = n < \infty$ then $o(a) = |\langle a \rangle|$ is a divisor of $|G|$

* Let $G = \langle a \rangle$, $o(a) = |G| = n$
Let $H = \langle a^d \rangle$, then $|H| \mid |G|$

($\longrightarrow$)

(3)

$o(a^d) \mid n$

$(a^d)^k = a^0 = e$, if $k = o(a^d)$

dk is a multiple of n.

* Let $(d, n) = \Delta$

$d = d'\Delta$

$n = n'\Delta$

$(a^d)^{n'} = a^{d'(\Delta n')} = (a^{\Delta n'})^{d'}$

$= (a^n)^{d'}$

$= e^{d'} = e$

* $o(a^d) \cdot n'$ is a period of a

$n \mid o(a^d)\, n'$

$n'\Delta \mid o(a^d)\, n'$

$\Delta \mid o(a^d)$

$\therefore\ n' = o(a^d)$

If $a^{dk} = e$, $k < n'$, then $n \mid dk$

$n'\Delta \mid \Delta d'k'$

$n' \mid d'k$

$n' \mid k$

$$o(a^d) = \frac{n}{\gcd(n,d)} = n'$$

* If $H = G$

$|H| = |G|$

$o(a^d) = n$, so $\gcd(n,d) = 1$

$\langle a^d \rangle = G$ iff $(n,d) = 1$

The number of a^d w/ $\langle a^d \rangle = G$ is $\varphi(n)$

Thm. $|G|$ prime $\Rightarrow$ G is cyclic

Pf. If $|G| = 1$, $G = \{e\}$

$|G| = 2$, $G = \{e, a\}$

$|G| = 3$, G is cyclic $\langle a \rangle$, $o\langle a \rangle = 3$

$|G| = p$, (p prime) G is cyclic

$|G| = 4$,

Case 1: $a \in G$

$o(a) = 4$

G is cyclic

Case 2: $a \neq e$ has $o(a) = 2$

$(\longrightarrow)$

(5)

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