MATH 407

4/11/18

* Lemma: G group, a,b commute
If $\gcd(o(a), o(b)) = 1$,
then $o(ab) = o(a)\,o(b)$

Pf. $o(a) = n$, $o(b) = m$
$(ab)^{mn} = (a^n)^m (b^m)^n = e$
so $o(ab) \mid mn$

Let $k = o(ab)$
then, $e = a^k b^k$
thus, $b^{-k} = a^k$
$a^{km} = (a^k)^m = (b^{-k})^m = (b^m)^{-k} = e^k = e$
$o(a) = n \Rightarrow n \mid km \Rightarrow n \mid k$
$o(b) = m \Rightarrow m \mid kn \Rightarrow m \mid k$
$\Rightarrow mn \mid k$

* Prop 3.5.9: G is a finite abelian group
a) $\exp(G) = \max\{o(g) : g \in G\}$
b) G is cyclic iff $\exp(G) = |G|$

Pf. Let $o(a) = \max\{o(g) : g \in G\}$ and assume $b \in G$ has $o(b) \nmid o(a)$

There is a prime p s.t. $o(b) = p^{\beta} m$, $\gcd(m, p) = 1$
$o(a) = p^{\alpha} n$, $\gcd(n, p) = 1$
$\beta > \alpha$

②

$o(a^{p^\alpha}) = n$, $o(a^n) = p^\alpha$
$o(b^{p^\beta}) = m$, $o(b^m) = p^\beta$

$a^{np^\alpha} = e = (a^{p^\alpha})^n$

$o(a^{p^\alpha} b^m) = np^\beta > np^\alpha = o(a)$, but $\beta > \alpha$ (contradiction)

$\therefore$ a, b commute w/in an abelian group

⊛ Section 3.6

* Let S be a set, H be a subgroup of $Sym(S)$. We call H a permutation group

* Thm. All groups are isomorphic to a permutation group. Specifically, $G \cong H$ subgroup of $Sym(G)$

* Pf. Look at $H = \{ m_a^l : a \in G \}$
$\Rightarrow m_a^l(g) = ag \ \forall g$

Let $m^l : a \to m_a^l$
$m_b^l \circ m_a^l(g) = m_b^l(ag) = (ba)g$
$= m_{ba}^l$

$\therefore m^l$ is homomorphic

To show one-to-one,

$$m_a^l \stackrel{?}{=} m_e^l = 1_G$$

$$\Rightarrow ag \stackrel{?}{=} eg, \ \forall g$$

$$\Rightarrow a = e$$

$$m^l : G \to H = \{ m_a^l : a \in G \}$$

⊛ Symmetry Groups of geometric objects:
Rigid Motion in $\mathbb{R}^2$ (or $\mathbb{R}^n$)

$T : \mathbb{R}^2 \to \mathbb{R}^2$ is rigid motion iff $\| \bar{X} - \bar{Y} \| = \| T(\bar{X}) - T(\bar{Y}) \|$
(isometry)

* Inverse $T^{-1} = S$ of rigid motion

$$U = T(\bar{X}), \quad \bar{X} = S(U)$$

$$V = T(\bar{Y}), \quad \bar{Y} = S(V)$$

$$\| S(U) - S(V) \| = \| U - V \|$$