MATH 407 ①

4/9/18

* Lemma: If G_1, G_2, G_3 are groups then

$$(G_1 \oplus G_2) \oplus G_3 \cong G_1 \oplus (G_1 \oplus G_3)$$

($\oplus$ is direct-sum)

Pf. $\phi((g_1, g_2), g_3) = (g_1, (g_2, g_3))$

$$\phi(((a_1, a_2), a_3) \cdot ((b_1, b_2), b_3))$$
$$= \phi((a_1b_1, a_2b_2), a_3b_3) = (a_1b_1, (a_2b_2, a_3b_3))$$
$$= (a_1 b_1) \cdot (a_2b_2, a_3b_3)$$
$$= (a_1 b_1)[(a_2, b_2) \cdot (a_3, b_3)]$$

Cor. All $G_1 \oplus \dots \oplus G_k$ are isomorphic independent of order of direct products

ex. $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ of order 8 $\mathbb{Z}_8$

$\Rightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_4 \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2$

* $G_1 \oplus G_2 \cong G_2 \oplus G_1$

In fact, if $H_1 = G_1 \oplus \{e_2\}$

$H_2 = \{e_1\} \oplus G_2$

then $H_1 H_2 = H_2 H_1$

$$(h_1, e_2)(e_1, h_2) = (h_1, h_2) = (e_1, h_2)(h_1, e_2)$$

* Thm 3.5.5 Let $G = \langle a \rangle$, $o(a) = n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$

$$G \cong \mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1}} \oplus \dots \oplus \mathbb{Z}_{p_k^{r_k}}$$

②

* **Prop 3.4.5** If $\langle n, m\rangle = 1$ then $\mathbb{Z}_{n,m} \cong \mathbb{Z}_n \oplus \mathbb{Z}_m$

* $\mathbb{Z}_n = \mathbb{Z}_{(p_1^{r_1} \cdots p_k^{r_k}) p_{k+1}^{r_{k+1}}}$

$\Rightarrow \mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1} \cdots p_k^{r_k}} \oplus \mathbb{Z}_{p_{k+1}^{r_{k+1}}}$

$\cong \left(\mathbb{Z}_{p_1^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{r_k}}\right) \oplus \mathbb{Z}_{p_{k+1}^{r_{k+1}}}$

* **Euler's phi (totient) function : $\varphi(n)$**

* **Cor. 3.5.6:** $n = p_1^{r_1} \cdots p_k^{r_k}$ then $\varphi(n)$ is $(p_1^{r_1} - p_1^{r_1 - 1}) \cdots (p_k^{r_k} - p_k^{r_k - 1})$

Pf $\varphi(n)$ is $|\mathbb{Z}_n^{\times}| = |\{k : \langle k, n\rangle = 1, 0 < k < n\}|$
$= |\{a : o(a) = n, a \in \mathbb{Z}_n\}|$

* $(a_1, \ldots, a_k) \in \mathbb{Z}_{p_1^{r_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{r_k}}$

$o(a_1, \ldots, a_k) = \mathrm{lcm}(o(a_1), \ldots, o(a_k))$
$= o(a_1) \cdot o(a_2) \cdots o(a_k)$
$\leq p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} = n$

If $o(a_i) = p_i^{r_i}$, then $\mathbb{Z}_{p_i^{r_i}} = \langle a_i \rangle$

$(\longrightarrow)$

* $\langle a_i \rangle = \mathbb{Z}_{p_i^{r_i}}$ iff $(a_i, p_i^{r_i}) = 1$

$$\# = \varphi(p_i^{r_i}) = p_i^{r_i} - p_i^{r_i - 1}$$

$$\varphi(n) = \# \{(a_1, \dots a_p)\}$$

$$= \prod_{i=1}^{k} (p_i^{r_i} - p_i^{r_i - 1})$$

* Def. Let G be a group. N is the exponent of the group iff $a \in G$ implies $o(a) | N$ and N is smallest.

* If $|G| < \infty$ then $o(a) \,|\, |G| \; \forall a$ so $N \,|\, |G|$

* Thm. If G is finite, a) then $\exp(G) = \max(o(a)), a \in G$
  b) G is cyclic iff there is $a \in G$, $o(a) = \exp(G)$

* Lemma. Let a, b be commuting elements of finite order in a group G.
  Then, if $\langle o(a), o(b) \rangle = 1$
  $$o(ab) = o(a) \cdot o(b)$$