Sylow Theorems

由有限個元素所生成出來的交換群 (Finitely Generated Abelian Group) 可以由以 F 的定理加以刻劃.

Theorem Let G be a finitely generated abelian group. Then G is isomorphic to $\mathbb{Z}_{p_1}^{r_1} \times \mathbb{Z}_{p_2}^{r_2} \times \cdots \mathbb{Z}_{p_n}^{r_n} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \mathbb{Z}$ where p_i are primes and r_i are positive integers.

From this theorem, we can prove that if G is a finite abelian group of order n and $m \mid n$, then G has a subgroup of order m. But, if G is not an abelian group, then the above conclusion may not be true.

Example The group of even permutations on $\{1, 2, 3, 4\}$ contains 12 elements and it is known as A_4. But, A_4 does not have a subgroup of order 6.

換言之, Lagrange 定理的逆敍述不一定會成立. 所以, 對於不可交換群的結構要更仔細研究才會有所了解.

Defn. (G-set)

Let G be a group and X be a set. An action of G on X is a map $* : G \times X \to X$ such that

1. $ex = x \ \ \forall \ \ x \in X$.
2. $(g_1 g_2)x = g_1(g_2 x) \ \ \forall \ \ x \in X$ and $g_1, g_2 \in G$.

Under this definition, X is a G-set (or X is a set with an action of G on X).

Defn. Let $x \in X$ (G-set). The orbit of x in X under G is

$Gx = \{gx \mid g \in G\}$.

$(*)$ $Gx_1 \cap Gx_2 \neq \phi$ *Rightarrow* $Gx_1 = Gx_2$.

Proof. $\forall$ $y \in Gx_1$, $y = gx_1$ for aome $g \in G$. By assumption, let $g_1x_1 = g_2x_2$. Therefore $y = gx_1 = gg_1^{-1}(g_2x_2) = g'x_2$ for some $g' \in G$. This implies that $Gx_1 \subseteq Gx_2$. Similarly, $Gx_2 \subseteq Gx_1$. Now, let X be a G-set. Then $\{Gx\}_{x \in X}$ forms a partition of X.

Let $\{x_1, x_2, \cdots, x_n\}$ contain exactly one element from each orbit in X. Then, we have $|X| = \sum_{i=1}^{r} |Gx_i|$. (1)

Let $X_G = \{x \mid gx = x \ \forall \ g \in G\}$. Assume that $|X_G| = s$.

Then $|X| = |X_G| + \sum_{i=s+1}^{r} |Gx_i|$. (2)

(註) $X_G = \{x_1, x_2, \cdots, x_s\}$.

Theorem Let G be a group of order p^n and let X be a G-set. Then $|X| \equiv |X_G| \pmod{p}$.

Proof. Let $G_x = \{g \in G \mid gx = x\}$. Then $G_x \leq G$. Let $(G : G_x)$ denoted the number of left cosets of G_x in G.

Claim : $|Gx| = (G : G_x)$.

Let $x_1 \in Gx$. Then, $\exists$ $g_1 \in G$s.t. $x_1 = g_1x$. Define $\psi : Gx \to \{$ left cosets of G_x in $G\}$ by letting $\psi(x_1) = g_1G_x$. ψ is $1-1$. Since $g_1G_x = g_2G_x \Rightarrow g_2^{-1}g_1 \in G_x$, i.e., $g_2^{-1}g_1x = x$ $g_1x = g_2x$ *rightarrow* $x_1 = x_2$. Onto can be checked easily. (?)

By (2) $|X| = |X_G| + \sum_{i=s+i}^{r} |Gx_i|$. Since $|Gx_i| \Big| |G|$, $|X| = |X_G| \pmod{p}$. (因爲 $|G| = p^n$, 它的因數也是 p 的次方.) ■

Defn. Let p be a prime. A group G is a p-group if element in G has order a power of the prime p. A subgroup of a group is a p-subgroup if the p-subgroup is itself a p-group.

Theorem (Cauchy's Theorem)

Let p be a prime. Let G be a finite group and $p \Big| |G|$. Then G has an element if order p and, thus, a subgroup of order p.
(注意：這裡是有 p 個元素的子群, 其中 p 爲質數.)

Proof. (這是一個非常有技巧的證明)

令 $X = \{(g_1, g_2, \cdots, g_p \mid \prod_{i=1}^{p} g_i = e,\ g_i \in G\}$, 於是 $|X| = |G|^{p-1}$. 所以 $p \Big| |X|$. $|X|$ 可以看成是一個 S_p-set 其中 S_p 爲所有 $\{1, 2, \cdots, p\}$ 的排列所成的集合, 作用的方式如 F: 令 $\sigma \in S_p$, 則

$$\sigma(g_1, g_2, \cdots, g_p) = (g_{\sigma(1)}, g_{\sigma(2)}, \cdots, g_{\sigma(p)}).$$ 例如

$\sigma = (123 \cdots p)$, 則 $\sigma(g_1, g_2, \cdots, g_p) = (g_2, g_3, \cdots, g_p, g_1) \in X$. (?)

現在, 再把 X 看成是 $\langle\sigma\rangle$-set, 其中 $|\langle\sigma\rangle| = p$.

由上述定理 $|X| \equiv |X_{\langle\sigma\rangle}| \pmod{p}$. 因爲 $p \Big| |X|$, 所以 $p \Big| |X_{\langle\sigma\rangle}|$. 然而 $X_{\langle\sigma\rangle}$ 中的元素必爲 $(g_1, g_2, \cdots, g_p)$, 其中 $g_1 = g_2 = g_3 = \cdots = g_p$, 所以必定存在一個 $a \in G$, s.t., $(a, a, \cdots, a) \in X_{\langle\sigma\rangle}$ 於 $a^p = e$, $|\langle a\rangle| = p$. $\langle a\rangle$ 即爲具有 p 個元素的子群. ■

(∗∗) 接下來的目標是證明當 $p^i \mid |G|$.時, G 中會有一個子群它具有 p^i 個元素.

Let G be a group, and let $\mathcal{G}$ be the collection of all subgroups of G. We can consider $\mathcal{G}$ as a G-set by using the action $* : G \times \mathcal{G} \to \mathcal{G}$ defined by $g * H = gHg^{-1}$ where $g \in G$ and $H \in \mathcal{G}$.

(∗) $G_H = \{g \in G | gHg^{-1} = H\} \leq G$.

Defn. G_H is called the normalizer of H in G, also denoted by $N[H]$.

Lemma Let H be a p-subgroup of a finite group G. Then
$(N[H] : H) \equiv (G : H) \pmod{p}$.