大學基礎代數

李華介

國立台灣師範大學數學系

Chapter 4

進階 Group 的性質

在這一章中我們將介紹另一種方法來處理更深一點的 group 理論. 這個方法稱之為 group action. 其實 group action 的理論基礎並不難, 困難的是當你碰到問題時要用哪種 group action 來解決問題. 不過這一點是經驗上的問題, 大家不必太在意. 所以當我們在介紹某種 group action 來處理問題時, 希望大家不要太害怕不知為何會想到用這種 action, 而將注意力集中在如何用這種 group action 產生的結果結合我們之前學的理論來得到更深的理論.

4.1. Group Action

給定一集合 S 和一個 group G, 如果對於任意 $a \in G$, $s \in S$, a 可作用在 s 上, 其作用的結果我們定成 $a * s$. 注意: 這裡我們稱為'作用'不稱為'運算', 主要原因是在我們想區分清楚在介紹 group 時我們稱的運算是指 group 同一個集合自己元素間的運算, 而這裡我們是可以有兩個不同的集合 G 和 S. 當然了照定義當 $S = G$ 時, G 當然還是可以作用在 G 上, 所以這裡還是要區分清楚作用和運算的不同.

Definition 4.1.1. 當 G 對 S 的作用 $*$ 符合以下三點我們就稱 $(G, S, *)$ 為一個 group action.

(Act1): $\forall\, a \in G$, $s \in S$, 皆有 $a * s \in S$.

(Act2): $\forall\, s \in S$, 皆有 $e * s = s$, 其中 e 是 G 的 identity.

(Act3): $\forall\, a, b \in G$, $s \in S$, 皆有 $(a \cdot b) * s = a * (b * c)$.

條件 (Act1) 是說 action 必須是封閉的, 也就是說 G 中的元素對 S 中的元素作用後還是要在 S 中. 這樣 G 中的元素就可以一直作用下去. 也就是說若 $b \in G$, $s \in S$, 則 $b * s$ 會在 S 中所以 G 中的元素 a 才可以再對 $b * s$ 作用得 $a * (b * s)$. 就因如此 (Act3) 中 $a * (b * s)$ 才有意義. (Act3) 告訴我們: b 對 s 作用後 a 再作用上去和 $a \cdot b$ 直接作用在 s 上是一樣的. 這有點像結合率對吧! 事實上若考慮 $S = G$, 而 G 對 G 的作用是 G 上的乘法, 則沒錯 G 上的乘法事實上就是一個 group action.

其實在證明 Theorem 3.4.15 時我們就引進了 S_n 對 $n \times n$ 矩陣的 group action. 我們不在這裡介紹其他的 group action 的例子, 我們留待要用到時再個別介紹.

談 group action 最主要的原因就是想用 G 的 action 將 S 中的元素分類. 若 $(G, S, *)$ 是一個 group action. 我們說 $x, y \in S$ 是同類的 (記作 $x \sim y$) 若且為若存在 $a \in G$ 使得 $a * x = y$. 我們曾說過一個好的分類必須是一個 equivalence relation. 下一個 Lemma 告訴我們當 $(G, S, *)$ 是一個 group action 時, 這樣的分類是一個好的分類.

Lemma 4.1.2. 若 $(G, S, *)$ 是一個 *group action,* 對於 $x, y \in S$ 我們定

$$x \sim y \Leftrightarrow \text{存在 } a \in G \text{ 使得 } a * x = y,$$

則 $\sim$ 是 S 中的一個 *equivalence relation.*

Proof. 我們證明 $\sim$ 符合 Definition 2.1.1 中的三個性質.

(equiv1) 任取 $x \in S$, 由 (Act2) 知 $e * x = x$ 故 $x \sim x$.

(equiv2) 若 $x \sim y$, 則由定義知: 存在 $a \in G$ 使得 $a * x = y$. 等式兩邊用 a^{-1} 作用, 由 (Act2) 和 (Act3) 得

$$a^{-1} * y = a^{-1} * (a * x) = (a^{-1} \cdot a) * x = e * x = x.$$

因為 $a^{-1} \in G$, 故知 $y \sim x$.

(equiv3) 若 $x \sim y$ 且 $y \sim z$, 知存在 $a, b \in G$ 使得 $a * x = y$ 且 $b * y = z$. 故由 (Act3) 知 $(b \cdot a) * x = b * (a * x) = b * y = z$. 因為 $b \cdot a \in G$, 故知 $x \sim z$. □

在第二章我們提過用 equivalence relation 分類的好處是 S 內的每一個元素都會被分到某一類, 且不同類的集合不會有交集. 現在若 S 是一個有限集合, 且 S 可分成 $[x_1], \ldots, [x_r]$ 這 r 個同類集, 其中 $[x_i]$ 表示 S 中與 x_i 同類的元素所成的集合. 則由 Lemma 2.1.2 知

$$|S| = \sum_{i=1}^{r} |[x_i]|. \tag{4.1}$$

所以現在重要的工作就是計算每個 $[x_i]$ 的個數.

Lemma 4.1.3. 若 $(G, S, *)$ 是一個 *group action,* $x \in S$.

(1) 若令 $G_x = \{g \in G \mid g * x = x\}$, 則 G_x 是 G 的一個 *subgroup.*

(2) 令 $[x]$ 表示 S 中所有和 x 同類的元素所成的集合. 若 G 和 S 都是 *finite,* 則

$$|[x]| = \frac{|G|}{|G_x|}.$$

Proof. (1) 若 $a, b \in G_x$, 即 $a * x = x$ 且 $b * x = x$, 故利用 (Act3) 知

$$(a \cdot b) * x = a * (b * x) = a * x = x,$$

也就是說 $a \cdot b \in G_x$. 再來因

$$x = e * x = a^{-1} * (a * x) = a^{-1} * x,$$

故得 $a^{-1} \in G_x$. 由此知 G_x 是 G 的 subgroup.

(2) 首先我們觀察若 $y \in [x]$, 表示存在 $a \in G$ 使得 $y = a * x$. 反之, 若給定 $a \in G$, 令 $y = a * x$, 則 y 和 x 是同類. 所以我們知 $[x] = \{g * x \,|\, g \in G\}$, 也就是每個 $[x]$ 中的元素都是 $g * x$ 這種形式. 不過要注意有可能存在 $a, b \in G$ 且 $a \neq b$ 但 $a * x = b * x$. 所以要真正算出 $[x]$ 有多少元素, 等於要算出到底有多少 G 中的元素會讓 $g * x$ 相異. 然而若 $a, b \in G$ 且 $a * x = b * x$, 則在等式兩邊用 a^{-1} 作用, 得

$$x = a^{-1} * (a * x) = a^{-1} * (b * x) = (a^{-1} \cdot b) * x.$$

也就是說 $a^{-1} \cdot b \in G_x$. 反之, 若 $a^{-1} \cdot b \in G_x$ 可得 $a * x = b * x$. 大家該記得 $a^{-1} \cdot b \in G_x$ 表示什麼吧! 這表示若用 G_x 這個 subgroup 對 G 中的元素分類, 和 a 同類的元素對 x 作用都會等於 $a * x$. 反之若 $a, b \in G$ 在用 G_x 這個 subgroup 分類之下是不同類的, 則 $a * x \neq b * x$. 所以 $[x]$ 內的元素個數是和 G 中用 G_x 分類之下可分成多少類是一樣的. 在證明 Lagrange 定理 (Theorem 2.2.2) 時我們曾證明若用 G_x 將 G 分類, 則 G 可分成 $|G|/|G_x|$ 類, 故得證本定理. □

Lemma 4.1.3 告訴我們, 給定 $x \in S$, 可由 G_x 得到 $[x]$ 的訊息. 例如若 $G_x = G$ (即所有 G 中的元素對 x 作用仍是 x), 則知 $|[x]| = 1$. 也就是說在 S 中和 x 同類的只有 x 本身, 其他的元素都和 x 不同類. 這樣的 x 對我們很有用, 我們將這種特別的 x 所成的集合記為 S_0.

Proposition 4.1.4. 令 p 是一個質數. 若 G 是一個 *p-group,* 且 $(G, S, *)$ 是一個 *group action,* 其中 S 是一個有限集合. 令

$$S_0 = \{s \in S \,|\, g * s = s, \forall\, g \in G\},$$

則

$$|S| \equiv |S_0| \pmod{p}.$$

Proof. 假設 S 可分成 $[x_1], \ldots, [x_r]$ 這 r 個同類集, 其中 $x_1, \ldots, x_t$ 在 S_0, 而 $x_{t+1}, \ldots, x_r$ 皆不屬於 S_0. 由此假設我們可知 $S_0 = \{x_1, \ldots, x_t\}$. 這是因為由假設已知 $\{x_1, \ldots, x_t\} \subseteq S_0$, 然而若 $x \in S_0$, 由於 x 只和自己同類, 它必是某個 x_i 但由 $x_{t+1}, \ldots, x_r$ 皆不屬於 S_0 的假設知 $x \in \{x_1, \ldots, x_t\}$.

回顧一下 G 是一個 p-group, 表示 $|G| = p^n$ 這種形式. 由 Lagrange 定理 (Theorem 2.2.2) 知 G 的所有的 subgroup 也是 p-group. 現若 $x \notin S_0$, 由定義知 $G_x \neq G$, 因此 $|G_x| = p^m$ 其中 $0 \leq m < n$. 也就是說 p 整除 $|G|/|G_x|$. 因此當 $i \in \{t+1, \ldots, r\}$ 時, 由於 $x_i \notin S_0$, 故由 Lemma 4.1.3 知 p 整除 $|[x_i]| = |G|/|G_{x_i}|$.

由於

$$|S| = \sum_{i=1}^{r} |[x_i]| = |S_0| + \sum_{i=t+1}^{r} |[x_i]|,$$

且由前面的討論知 p 整除 $\sum_{i=t+1}^{r} |[x_i]|$, 因此 p 整除 $|S| - |S_0|$, 也就是說 $|S| \equiv |S_0| \pmod{p}$. □

最後我們要強調, 之後我們就是要利用 Proposition 4.1.4 來證明幾個重要的定理, 因此給了一個 group action, 要知道 S_0 是哪些元素就顯得特別重要.

4.2. Cauchy's Theorem

我們曾在 Theorem 3.3.2 證明 Cauchy's Theorem, 不過當時的証明仰賴著 abelian group 的假設. 在這一節中我們將利用 group action 的方法證明 Cauchy's Theorem 事實在一般的 finite group 都是對的.

4.2.1. 證明 Cauchy's Theorem 所用的 group action. Cauchy's Theorem 有許多種的證明, 大部分都是用 group action 來處理. 而我們這裡要介紹的證明最簡明, 唯一的缺憾是所用的 group action 很特別. 不過我們曾提過, 我們不要把重點放在如何想到用這種 group action, 而是把重點放在如何利用這種 group action 所得的結果.

設 $m \in \mathbb{N}$ 是一個正整數, 令 H 是 S_m 中由 $(1\ 2 \cdots m)$ 這一個 m-cycle 所產生的 cyclic subgroup. 給定一個 group G, 我們考慮以下的一個集合 S:

$$S = \{(a_1, a_2, \ldots, a_m) \in G^m \mid a_1 \cdot a_2 \cdots a_m = e\}.$$

也就是說每一個 S 中的元素是由 m 個 G 中的元素所形成, 不過這 m 個元素是有次序性的, 而且按照這次序相乘的乘積是 identity.

現在我們要定義一個 H 對 S 的 group action. 任取 $\rho \in H, x \in S$. 我們定義 $\rho * x$ 是將原來 x 的第 i 個位置的元素放在第 $\rho(i)$ 個位置, 也就是將第 1 個位置的放在第 $\rho(1)$ 個位置, ... 依此類推. 例如若 $\sigma = (1\ 2 \cdots m)$, 任取 $x = (a_1, a_2, \ldots, a_m) \in S$. 我們有

$$\sigma * x = (a_m, a_1, a_2, \ldots, a_{m-1}).$$

也就是 $\sigma * x$ 是將原來 x 的第一個位置的元素放在第二個位置, 第二個位置的放在第三個, 依此類推, 最後因為 σ 是將 $m \mapsto 1$, 故 $\sigma * x$ 是將原來 x 第 m 個位置的元素放到第一個位置.

要證明 $(H, S, *)$ 是一個 group action, 我們首先證明 (Act3). 若 $\rho, \tau \in H$, 對任意的 $x \in S$, $\rho * x$ 是將原來 x 的第 i 個位置的元素放在第 $\rho(i)$ 個位置; 而 $\tau * x$ 是將原來 x 的第 i 個位置的元素放在第 $\tau(i)$ 個位置. 因此 $\tau * (\rho * x)$ 是將原來 $\rho * x$ 的第 $\rho(i)$ 個位置的元素放在第 $\tau(\rho(i))$ 個位置. 但 $\rho * x$ 的第 $\rho(i)$ 個位置的元素是原來 x 的第 i 個位置的元素, 因此知 $\tau * (\rho * x)$ 是將原來 x 的第 i 個位置的元素放在第 $\tau(\rho(i))$ 個位置. 而按照定義 $(\tau \cdot \rho) * x$ 是將原來 x 的第 i 個位置的元素放在第 $(\tau \cdot \rho)(i) = \tau(\rho(i))$ 個位置. 因為這是對所有的 $i \in \{1, \ldots, m\}$ 都對故得 $\tau * (\rho * x) = (\tau \cdot \rho) * x$.

接下來證明 (Act1). 因為 H 是由 $\sigma = (1\ 2\ \cdots\ m)$ 產成的 cyclic group, 故任意的 $\rho \in H$ 都是 σ^j 這種形式, 其中 $j \in \mathbb{N}$. 因此若我們證得對任意的 $x \in S$ 皆有 $\sigma * x \in S$, 則由於 (Act3) 知 $\sigma^2 * x = \sigma * (\sigma * x)$ (別忘了我們已證明了 (Act3)), 故可得 $\sigma^2 * x \in S$. 依此用數學歸納法就可得對任意的 $j \in \mathbb{N}$ 皆有 $\sigma^j * x \in S$. 所以現在我們只要證明若 $x = (a_1, a_2, \ldots, a_{m-1}, a_m) \in S$ 則 $\sigma * x \in S$. 前面我們已知 $\sigma * x = (a_m, a_1, a_2, \ldots, a_{m-1})$, 由於這些 a_i 皆在 G 中, 要證明 $\sigma * x \in S$, 我們只要證明 $a_m \cdot a_1 \cdot a_2 \cdots a_{m-1} = e$ 就可. 已知 $x = (a_1, a_2, \ldots, a_{m-1}, a_m) \in S$, 因此 $(a_1 \cdot a_2 \cdots a_{m-1}) \cdot a_m = e$. 換句話說 $a_1 \cdot a_2 \cdots a_{m-1} = a_m^{-1}$. 由於 G 是一個 group, $a_m \cdot a_m^{-1} = a_m^{-1} \cdot a_m = e$, 所以我們有 $a_m \cdot a_m^{-1} = a_m \cdot (a_1 \cdot a_2 \cdots a_{m-1}) = e$. 故知 $\sigma * x \in S$.

最後我們證 (Act2). 若 $I \in H$ 是 H 的 identity, 則由定義知 $I(i) = i$, $\forall i \in \{1, \ldots, m\}$. 所以由我們定的作用知 $I * x$ 是將 x 的第 i 個位置的元素放在第 i 個位置. 換句話說對所有的 $x \in S$, $I * x = x$.

好了, 我們已知 $(H, S, *)$ 是一個 group action. 現在來看看 S 有多少個元素. 若 $|G| = n$, 如果 S 的元素只是要求是 $(a_1, \ldots, a_m)$ 這種形式, 由於每一個座標可以任填 G 中的元素, 所以 S 共有 n^m 個元素. 不過我們的 S 還有另一個條件就是 $a_1 \cdot a_2 \cdots a_{m-1} \cdot a_m = e$. 所以前面 $m-1$ 個座標我們可以任填 G 中的元素 $a_1, \ldots, a_{m-1}$ 只要在第 m 個位置填上 $(a_1 \cdots a_{m-1})^{-1}$ 就可. 因為每一個 S 的元素都可以用這種方法得到, 所以知

$$|S| = n^{m-1}. \tag{4.2}$$

最後我們來討論 S_0 是由哪些元素組成. 若 $x = (a_1, a_2, \ldots, a_{m-1}, a_m) \in S_0$, 表示 $\sigma * x = x$. 不過已知 $\sigma * x = (a_m, a_1, \ldots, a_{m-1})$, 故得

$$a_m = a_1,\ a_1 = a_2, \ldots,\ a_{m-1} = a_m.$$

換句話說

$$a_1 = a_2 = \cdots = a_{m-1} = a_m.$$

也就是說 S_0 的元素必須是 $(a, a, \ldots, a)$ 這種形式, 但並不是任意的 $a \in G$ 都可以; 別忘了 $S_0 \subseteq S$, 故 $(a, a, \ldots, a) \in S$ 的條件告訴我們 $a^m = e$. 反之我們很容易檢驗若 $x = (a, a, \ldots, a)$, 其中 $a^m = e$, 則 $x \in S_0$. 所以我們得

$$S_0 = \{(a, a, \ldots, a) \in G^m \,|\, a \in G,\ a^m = e\}. \tag{4.3}$$

最後我們強調因 $e^m = e$, 故 $(e, e, \ldots, e) \in S_0$. 也就是說 S_0 是非空的, 即

$$|S_0| \geq 1. \tag{4.4}$$

4.2.2. Cauchy 定理. 我們現在用前面介紹的 group action 證明 Cauchy's Theorem. 再次強調前面的 G 並沒有要求 abelian, 所以我們的証明適用於一般的 group.

Theorem 4.2.1 (Cauchy's Theorem)**.** 若 G 是一個 *group* 且 p 整除 G 的個數, 其中 p 是一個質數, 則存在 $a \in G$ 滿足 $\mathrm{ord}(a) = p$.

Proof. 我們利用前面介紹的 group action, 這裡我們令 $m = p$, H 是 S_p 中由 $(1\ 2\ \cdots\ p)$ 這一個 p-cycle 所產生的 cyclic subgroup. 而

$$S = \{(a_1, \ldots, a_p) \in G^p \mid a_1 \cdot a_2 \cdots a_p = e\}.$$

若 $|G| = n$ 利用前面式子 (4.2) 知 $|S| = n^{p-1}$, 故由假設 $p \mid n$ 得 p 整除 $|S|$. 也就是說

$$|S| \equiv 0 \pmod{p} \tag{4.5}$$

由 lemma 3.4.7 知 $(1\ 2 \cdots p)$ 這一個 p-cycle 的 order 為 p, 故知 $|H| = p$. 也就是說 H 是一個 p-group. 因此利用 Proposition 4.1.4 和式子 (4.5) 知

$$|S_0| \equiv |S| \equiv 0 \pmod{p}.$$

也就是說 p 整除 $|S_0|$. 不過由式子 (4.4) 知 $|S_0| \geq 1$, 再加上 p 整除 $|S_0|$, 也就是 $|S_0|$ 是 p 的倍數且不是 0. 因此我們知

$$|S| > 1.$$

換句話說 S_0 中除了已知的 $(e, e, \ldots, e)$ 這個元素外還有其他的元素. 由式子 (4.3), 我們知道在這些元素都是 $(a, a, \ldots, a)$ 這種形式, 且 $a^p = e$. 因此得 $a \neq e$ 且 $a^p = e$, 也就是說 $\mathrm{ord}(a) = p$. □

回顧一下從前我們先證明了在 abelian group 情形下的 Cauchy 定理, 再利用它證得 abelian group 的 Sylow 定理. 將來我們也會用這一般 group 的 Cauchy 定理證明一般 group 的 Sylow 定理.

4.3. p-Group

我們曾探討過 abelian p-group. 在這一節我們特別來談一般的 p-group.

4.3.1. Conjugation as a group action. 回顧一下我們曾提過若固定 $x \in G$, 對任意的 $g \in G$, $g \cdot x \cdot g^{-1}$ 稱為 x 的一個 conjugation. 事實上這是 G 對 $S = G$ 的一個 group action.

若 G 是一個 group. 令 $S = G$, 而僅把 S 看成是一個集合. 考慮 G 對 S 的作用如下: 對任意的 $a \in G$, $x \in S$, 我們定義 $a * x = a \cdot x \cdot a^{-1}$.

我們要證明這種 $(G, S, *)$ 是一個 group action. 首先檢查 (Act1). 若 $a \in G$, $x \in S$, 則 $a * x = a \cdot x \cdot a^{-1}$. 因 a, x, a^{-1} 皆在 G 中而 G 是一個 group, 故 $a \cdot x \cdot a^{-1} \in G = S$. 得知 $a * x \in S$. 再來因 $e * x = e \cdot x \cdot e^{-1} = x$, 故知 (Act2) 也符合. 最後若 $a, b \in G$, $x \in S$, 則

$$a * (b * x) = a * (b \cdot x \cdot b^{-1}) = a \cdot (b \cdot x \cdot b^{-1}) \cdot a^{-1},$$

然而

$$(a \cdot b) * x = (a \cdot b) \cdot x \cdot (a \cdot b)^{-1} = (a \cdot b) \cdot x \cdot (b^{-1} \cdot a^{-1}).$$

故由結合率知 $a * (b * x) = (a \cdot b) * x$, 得證 (Act3).

在這個 action 中因 $S = G$, 故自然知 $|S| = |G|$. 現在來看 S_0 是什麼? 照定義若 $x \in S_0$ 表示對所有的 $g \in G$ 皆有 $g * x = x$. 也就是對於此 x, 對任意的 $g \in G$, 皆須符合 $g \cdot x \cdot g^{-1} = x$. 由此推得 $g \cdot x = x \cdot g, \forall\, g \in G$. 換句話說 S_0 的元素皆需和所有 G 中的元素可交換. 反之若 $x \in S$ 可以和 G 中所有元素交換的話, 則

$$g * x = g \cdot x \cdot g^{-1} = x \cdot g \cdot g^{-1} = x,$$

也就是說 $x \in S_0$.

如果大家不健忘的話, 我們曾在 1.4 節中介紹這樣的元素所成的集合 $Z(G)$ 稱為 G 的 center, 且利用 Lemma 1.5.1 說明過 $Z(G)$ 是一個 G 的 subgroup. 總知, 我們證得了

$$S_0 = Z(G) = \{x \in G \,|\, g \cdot x = x \cdot g, \forall\, g \in G\}. \tag{4.6}$$

最後我們還是要強調因已知 $e \in Z(G)$, 故知

$$|S_0| \geq 1. \tag{4.7}$$

4.3.2. *p*-group 的性質. 在 abelian group 最好用的性質就是其每個 subgroup 都是 normal subgroup, 所以每次碰到有關 abelian group 的性質時, 我們都可先找一個 nontrivial subgroup 再利用其為 normal 得到一個 order 比較小的 quotient group, 然後就可以用 induction. 在一般的 group 這方法就不再適用了, 因為可能並不存在 nontrivial normal subgroup 讓你做 quotient group. 接下來我們將證明 p-group 就有類似的好處, 除了個數是 p 的情況外 (這是 cyclic group 所以也不會造成麻煩), 其他的 p-group 都可找到一個 nontrivial normal subgroup. 所以一些 p-group 的性質就可以用 induction 得到.

Theorem 4.3.1. *若 G 是一個 p-group, 則*

$$Z(G) \neq \{e\}.$$

也就是說在 G 中存在一個元素 $a \neq e$ 且 $a \cdot g = g \cdot a, \forall\, g \in G$.

Proof. 我們利用前面介紹的 conjugation 所造的 group action $(G, S, *)$. 由於 $|G| = |S|$, 且因 G 是一個 p-group, 故得

$$|S| \equiv 0 \pmod{p}. \tag{4.8}$$

再因 G 是 p-group, 我們可以利用 Lemma 4.1.4 和式子 (4.8) 得

$$|S_0| \equiv |S| \equiv 0 \pmod{p}.$$

再加上式子 (4.7) 我們知 $|S_0|$ 是一個正整數且是 p 的倍數. 故由式子 (4.6) 知 $|Z(G)| = |S_0| > 1$. 也因此得 $Z(G)$ 中存在著 identity 以外的元素, 故得證本定理. □

Theorem 4.3.1 和前面談的 normal subgroup 有什麼關係呢? 其實 $Z(G)$ 不只是 G 的 subgroup, 它是 G 的 normal subgroup. 因為若 $a \in Z(G)$, 則對任意的 $g \in G$, 我們皆有 $g \cdot a \cdot g^{-1} = a \in Z(G)$. 所以 $Z(G)$ 是 G 的 normal subgroup.

Corollary 4.3.2. *若 G 是一個 p-group 且 $|G| \neq p$, 則 G 不是一個 simple group.*

Proof. 若 G 是 abelian, 從前已提過這時只有當 $|G| = p$ 時才會是 simple group. 所以由假設 $|G| \neq p$ 知 G 不會是 simple group.

若 G 不是 abelian, 則 $Z(G) \subsetneq G$ 且由 Theorem 4.3.1 知 $Z(G) \neq \{e\}$, 故知 $Z(G)$ 是 G 的一個 nontrivial proper normal subgroup. 所以 G 不是一個 simple group. □

我們已知最簡單的 p-group, 即 order 為 p 的 group 是 cyclic. 我們現在來探討 order 為 p^2 的 group.

Proposition 4.3.3. *若 G 是一個 group 且 $|G| = p^2$, 則 G 是一個 abelian group.* 也就是說我們有

$$G \simeq \mathbb{Z}/p^2\mathbb{Z} \quad \text{or} \quad G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Proof. 如果 G 不是 abelian group 即表示 $Z(G) \neq G$, 再由 Theorem 4.3.1 知 $Z(G) \neq \{e\}$, 故由 Lagrange 定理 (Theorem 2.2.2) 知 $|Z(G)| = p$. 現任取 $a \in G$ 但 $a \notin Z(G)$. 考慮 a 的 centralizer

$$C(a) = \{g \in G \,|\, g \cdot a = a \cdot g\}.$$

由 Proposition 1.4.2 我們知 $C(a)$ 是 G 的一個 subgroup. 不過若 $x \in Z(G)$, 則 $x \cdot a = a \cdot x$, 故知 $x \in C(a)$. 也就是說 $Z(G) \subseteq C(a)$. 不過由假設 $a \notin Z(G)$, 但 a 本身在 $C(a)$ 中 (因 $a \cdot a = a \cdot a$), 故知 $Z(G) \subsetneq C(a)$. 這告訴我們 $|C(a)| > |Z(G)| = p$. 然而 Lagrange 定理告訴我們 $|C(a)|$ 必須整除 p^2, 因此得 $|C(a)| = p^2$. 由此推得 $C(a) = G$, 也就是所有 G 中的元素都在 $C(a)$. 換句話說所有 G 的元素都可和 a 交換. 這和我們當初假設 $a \notin Z(G)$ 相矛盾. 所以知 G 一定是 abelian group. □

Proposition 4.3.3 並不能推廣到 $|G| = p^n$, 其中 $n \geq 3$ 的狀況. 比方說將來我們將會看到存在 order 為 $8 = 2^3$ 的 nonabelian group. 不過我們倒可以用前面所提的歸納法得到以下的結果:

Proposition 4.3.4. *若 G 是一個 group, 且 $|G| = p^n$, 則 G 中存在一個 normal subgroup N 其 order 為 p^{n-1}.*

Proof. 我們用數學歸納法證明此定理. 當 $n = 1$ 時 $|G| = p$, 而 $\{e\}$ 是 G 的 normal subgroup 且 $|\{e\}| = p^{1-1} = 1$. 故在此情形是成立的.

假設對於 $|G| = p^r$, 且 $1 \leq r \leq n-1$ 時, 本定理也成立. 當 $|G| = p^n$ 時, 由 Theorem 4.3.1 知 $Z(G) \neq \{e\}$, 故由 Lagrange 定理知 $Z(G)$ 也是一個 p-group. 因 p

整除 $|Z(G)|$, 故由 Cauchy 定理 (Theorem 4.2.1) 知存在一個 $Z(G)$ 的 subgroup H 其 order 為 p. 因 $H \subseteq Z(G)$, 故若 $a \in H$, 對於所有的 $g \in G$ 皆有 $a \cdot g = g \cdot a$. 因此 $g \cdot a \cdot g^{-1} = a \cdot g \cdot g^{-1} = a \in H$, 故知 H 是 G 的一個 normal subgroup. 因 H 在 G 中 normal, 我們可考慮 $G' = G/H$ 這個 quotient group. 因 $|G'| = |G|/|H| = p^{n-1}$ 我們可以用 induction 的假設知 G' 中存在一個 normal subgroup N' 其 order 為 p^{n-2}. 然而 Correspondence 定理 (Theorem 2.7.3) 告訴我們 G 中存在一個 normal subgroup N, 符合 $H \subseteq N$ 且 $N/H = N'$. 也就是說

$$|N| = |H| \cdot |N'| = p \cdot p^{n-2} = p^{n-1}.$$

故完成本定理的証明. □

Proposition 4.3.4 的結果當然比 Corollary 4.3.2 強, 它告訴我們當 $|G| = p^n$ 時我們可找到一個 G 的 normal subgroup G_{n-1} 其 order 為 p^{n-1}. 再對 G_{n-1} 使用 Proposition 4.3.4 可得一個 G_{n-1} 的 normal subgroup G_{n-2} 其 order 為 p^{n-2}. 如此一直下去我們可得一串 G 的 subgroup:

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{n-1} \subseteq G_n = G,$$

其中 $|G_i| = p^i$, 且是 G_{i+1} 的 normal subgroup. 由於 G_{i+1}/G_i 是一個 order 為 p 的 group, 所以這一個 quotient group 是一個 cyclic group. 一般來說一個 group G 中若可以找到一串 subgroups: $\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{n-1} \subseteq G_n = G$, 其中 G_i 是 G_{i+1} 的 normal subgroup, 且 G_{i+1}/G_i 是一個 cyclic group, 則我們就說這個 group G 是一個 *solvable group*. Proposition 4.3.4 告訴我們一個 p-group 一定是一個 solvable group.

4.4. First Sylow's Theorem

接下來我們將介紹 Sylow 定理. Sylow 定理也有三個, 不過不像 Isomorphism 定理其他兩個可以用第一個輕鬆得到. 我們將用不同的 group action 來處理這三個定理, 為了避免造成混搖我們分成三節來個別討論它們. 在這一節我們介紹第一個 Sylow 定理.

4.4.1. Group action on left coset. 若 H 是 G 的一個 subgroup, 用 $a^{-1} \cdot b \in H$ 表示 a, b 同類的分類方法, 我們在 Lemma 2.2.1 中知道和 a 同類的元素所成的集合可用

$$a \cdot H = \{a \cdot h \,|\, h \in H\}$$

來表示. 因此我們將用 $a \cdot H$ 來表示和 a 同類的元素所成的集合, 一般來說稱 $a \cdot H$ 這樣的集合為 H 在 G 中 的一個 *left coset*. 我們再次強調一次若 $a \cdot H = b \cdot H$ 表示 $a^{-1} \cdot b \in H$. 反之, 若 $a \cdot H \neq b \cdot H$, 則 $a^{-1} \cdot b \notin H$.

若 G 是一個 finite group, 且 H 是 G 的一個 subgroup. 令 S 為所有 H 在 G 中的 left coset 所成的集合. 換言之,

$$S = \{a \cdot H \,|\, a \in G\}.$$

也就是說我們將 $a \cdot H$ 看成是一個元素. 現在我們要定一個 H 對 S 的作用: 對任意的 $h \in H$, $a \cdot H \in S$, 我們定義

$$h * (a \cdot H) = (h \cdot a) \cdot H.$$

我們要證明這樣定的 $(H, S, *)$ 是一個 group action. 首先證明 (Act1). 對任意的 $h \in H$, $a \cdot H \in S$, 由於 $h * (a \cdot H) = (h \cdot a) \cdot H$, 而 $h \cdot a$ 是 G 的一個元素, 由定義知它當然是 H 在 G 中的一個 left coset. 再來因

$$e * (a \cdot H) = (e \cdot a) \cdot H = a \cdot H,$$

故知 (Act2) 也成立. 最後若 $h, h' \in H$, 則對於任意的 $a \cdot H \in S$, 我們皆有

$$h * (h' * (a \cdot H)) = h * ((h' \cdot a) \cdot H) = (h \cdot (h' \cdot a)) \cdot H,$$

和

$$(h \cdot h') * (a \cdot H) = ((h \cdot h') \cdot a) \cdot H.$$

所以利用結合率知 (Act3) 也成立.

S 是所有 H 在 G 中的 left coset 所成的集合, 也就是說 S 的個數就是 H 在 G 中分類後可分的類別個數. 我們在證明 Lagrange 定理 (Theorem 2.2.2) 時已算出此數為 $|G|/|H|$, 故得

$$|S| = \frac{|G|}{|H|}. \tag{4.9}$$

什麼會是 S_0 呢? 若 $a \cdot H \in S_0$, 則對於所有 $h \in H$ 皆有 $h * (a \cdot H) = a \cdot H$. 然而 $h * (a \cdot H) = (h \cdot a) \cdot H$, 這告訴我們

$$a \cdot H = (h \cdot a) \cdot H.$$

也就是 $a^{-1} \cdot h \cdot a \in H$. 所以若 $a \cdot H \in S_0$ 則對於所有的 $h \in H$, 皆有 $a^{-1} \cdot h \cdot a \in H$. 反之, 若 a 符合對於所有的 $h \in H$, 皆有 $a^{-1} \cdot h \cdot a \in H$, 則 $a \cdot H \in S_0$. 所以我們得到

$$S_0 = \{a \cdot H \,|\, a^{-1} \cdot h \cdot a \in H,\ \forall\, h \in H\}. \tag{4.10}$$

由於我們想了解 S_0, 我們必須更深入的討論像 a 這種對於所有的 $h \in H$, 皆有 $a^{-1} \cdot h \cdot a \in H$ 這樣性質的元素. 若 a 有這種性質, 由定義知 $a^{-1} \cdot H \cdot a \subseteq H$. 由於 G 是一個 finite group, 由 Lemma 1.5.2 我們知 $|a^{-1} \cdot H \cdot a| = |H|$, 因此得 $a^{-1} \cdot H \cdot a = H$. 所以我們可以將式子 (4.10) 改寫成

$$S_0 = \{a \cdot H \,|\, a^{-1} \cdot H \cdot a = H\}. \tag{4.11}$$

其實我們常把符合 $a^{-1} \cdot H \cdot a = H$ 的 a 所成的集合寫成 $N(H)$, 也就是

$$N(H) = \{a \in G \,|\, a^{-1} \cdot H \cdot a = H\}.$$

其實 $N(H)$ 是 G 的一個 subgroup. 這是因為若 $a, b \in N(H)$, 則 $a^{-1} \cdot H \cdot a = H$ 且 $b^{-1} \cdot H \cdot b = H$, 所以

$$(b \cdot a)^{-1} \cdot H \cdot (b \cdot a) = a^{-1} \cdot (b^{-1} \cdot H \cdot b) \cdot a = a^{-1} \cdot H \cdot a = H.$$

也就是 $b \cdot a \in N(H)$, 這證得了封閉性. 至於 inverse, 由於 $a^{-1} \cdot H \cdot a = H$, 所以

$$a \cdot (a^{-1} \cdot H \cdot a) \cdot a^{-1} = a \cdot H \cdot a^{-1}.$$

不過以上等式左邊等於 H, 而右邊可寫成 $(a^{-1})^{-1} \cdot H \cdot a^{-1}$, 故知 $a^{-1} \in N(H)$.

若 $h \in H$, 因 H 是一個 group, 我們知 $h^{-1} \in H$, 所以對於所有的 $h' \in H$ 皆有 $h^{-1} \cdot h' \cdot h \in H$. 由此知 $h^{-1} \cdot H \cdot h = H$, 也就是 $h \in N(H)$. 所以 $H \subseteq N(H)$, 換句話說 H 是 $N(H)$ 的一個 subgroup. 既然 H 是 $N(H)$ 的一個 subgroup, 由 Lagrange 定理知 $|H|$ 整除 $|N(H)|$. 別忘了由式子 (4.11) 我們有 $S_0 = \{a \cdot H \,|\, a \in N(H)\}$, 也就是說 S_0 的個數應該是 $N(H)$ 裡的元素用 H 分類後所得的類別個數, 因此我們有

$$|S_0| = \frac{|N(H)|}{|H|}. \tag{4.12}$$

我們要強調因 H 是 $N(H)$ 的 subgroup, 所以在分類時至少有 $e \cdot H = H$ 這一類. 所以知

$$|S_0| \geq 1. \tag{4.13}$$

通常我們稱 $N(H)$ 是 H 的 *normalizer*, 這是因為 H 不只是 $N(H)$ 的 subgroup, 其實是 $N(H)$ 的 normal subgroup. 要證 normal, 我們需要證: 給定 $h \in H$, 對任意的 $a \in N(H)$ 皆有 $a^{-1} \cdot h \cdot a \in H$. 然而 $a^{-1} \cdot H \cdot a = H$, 當然得 $a^{-1} \cdot h \cdot a \in H$. 我們將此寫成以下的 Lemma.

Lemma 4.4.1. *若 H 是 G 的 subgroup. 令 $N(H) = \{a \in G \,|\, a^{-1} \cdot H \cdot a = H\}$, 則 H 是 $N(H)$ 的一個 normal subgroup.*

4.4.2. Sylow p-subgroup 的存在性. 回顧一下: 若 $|G| = p^n m$, 其中 p 是一個質數且 $p \nmid m$. 如果 H 是 G 的一個 p-subgroup 且其 order 為 p^n, 則我們稱 H 是 G 的一個 Sylow p-subgroup. 第一個 Sylow 定理是說 G 中一定存在一個 Sylow p-subgroup. 事實上我們將證明比這更強一點的定理.

Theorem 4.4.2 (First Sylow's Theorem)**.** *若 G 是一個 group 且 $|G| = p^n m$, 其中 $n \geq 1$, p 是一個質數且 $p \nmid m$.*

(1) *若在 G 中存在一個 subgroup H 其 order 為 p^r 其中 $1 \leq r \leq n-1$, 則在 G 中可找到一個 subgroup K 其 order 為 p^{r+1} 且 H 是 K 的 normal subgroup.*

(2) *G 中存在一個 subgroup P 其 order 為 p^n, 也就是說 G 中存在 Sylow p-subgroup.*

Proof. (1) 我們考慮如前面提的 action 將 H 作用在 $S = \{a \cdot H \,|\, a \in G\}$. 式子 (4.10) 告訴我們

$$|S| = |G|/|H| = p^n m/p^r = p^{n-r}m.$$

故由 $r < n$ 知

$$|S| \equiv 0 \pmod{p}. \tag{4.14}$$

由於 H 是 p-group, 利用 Proposition 4.1.4 和式子 (4.14) 知

$$|S_0| \equiv |S| \equiv 0 \pmod{p}. \tag{4.15}$$

不過由 Lemma 4.4.1 知 H 是 $N(H)$ 的 normal subgroup, 所以我們可以考慮 $G' = N(H)/H$ 這一個 quotient group. 因為 $|G'| = |N(H)|/|H|$, 故式子 (4.12) 告訴我們 $|G'| = |S_0|$. 所以利用式子 (4.15) 知 p 整除 $|G'|$. 對 G' 使用 Cauchy 定理知在 G' 中存在一個 subgroup K' 其 order 為 p. 然而 $G' = N(H)/H$ 利用 Correspondence 定理 (Corollary 2.7.3) 知 $N(H)$ 中存在一個 subgroup K 符合 $H \subseteq K$ 且 $K' = K/H$. 故

$$|K| = |K'| \cdot |H| = p \cdot p^r = p^{r+1}.$$

又因為 $H \subseteq K \subseteq N(H)$, 且 H 在 $N(H)$ 中 normal, 所以當然 H 在 K 中 normal (見 Remark 2.4.2 (1)).

(2) 我們要利用 (1) 來證明 Sylow p-subgroup 是存在的. 首先因 p 整除 $|G|$ 故由 Cauchy 定理知 G 中存在一個 subgroup H_1 其 order 為 p. 如果 $n = 1$, 則證明完成. 否則因 $1 \leq n-1$ 利用 (1) 得到 G 的 subgroup H_2 其 order 為 p^2. 如此一直下去直到我們得到一個 G 的 subgroup 其 order 為 p^n. □

Theorem 4.4.2 告訴我們可以由一個小一點的 p-subgroup H 往上找到大一點的 p-subgroup K 且 H 是 K 的 normal subgroup. 而 Proposition 4.3.4 是說我們可以由一個大一點的 p-subgroup k 往下找到小一點的 p-subgroup h 且 H 是 K 的 normal subgroup. 希望大家能分辨其不同.

4.5. Second Sylow's Theorem

第一個 Sylow 定理告訴我們若 p 整除 $|G|$ 則 G 中存在 Sylow p-subgroup. 既然存在我們自然會想知道會唯一嗎? 第二個 Sylow 定理就是回答此問題.

4.5.1. Another group action on left coset. 前一節證明 First Sylow's Theorem 我們是用 H 對 G 中 H 的 left coset 作用. 這裡我們考慮 H 對 G 中令一個 subgroup P 的 left coset 作用.

若 G 是一個 finite group, H 和 P 是 G 的 subgroups. 令 $S = \{a \cdot P \,|\, a \in G\}$ 是 G 中 P 的 left coset 所成的集合. 我們定義 H 對 S 的作用如下: 對任意的 $h \in H$, $a \cdot P \in S$, 我們定義

$$h * (a \cdot P) = (h \cdot a) \cdot P.$$

利用和前一節相同的證明可知 $(H, S, *)$ 是一個 group action. 同樣的我們也知

$$|S| = \frac{|G|}{|P|}. \tag{4.16}$$

而什麼會是 S_0 呢? 若 $a \cdot P \in S_0$, 則對於所有 $h \in H$ 皆有

$$(h \cdot a) \cdot P = h * (a \cdot P) = a \cdot P.$$

這告訴我們 a 和 $h \cdot a$ 在 P 的分類之下是同類的, 也就是 $a^{-1} \cdot h \cdot a \in P$. 因為這是對所有的 $h \in H$ 都是對的, 我們可以寫成 $a^{-1} \cdot H \cdot a \subseteq P$. 因此若 $a \cdot P \in S_0$ 則我們有 $a^{-1} \cdot H \cdot a \subseteq P$. 反之, 若 a 符合 $a^{-1} \cdot H \cdot a \subseteq P$, 則 $a \cdot P \in S_0$. 所以我們得到

$$S_0 = \{a \cdot P \,|\, a^{-1} \cdot H \cdot a \subseteq P\}. \tag{4.17}$$

這裡我們要說明一件事 (和 Sylow 定理無關只是要釐清觀念). 若我們如前一節收集 G 中的元素 a 符合 $a^{-1} \cdot H \cdot a \subseteq P$ 成為一個集合 $\{a \in G \,|\, a^{-1} \cdot H \cdot a \subseteq P\}$. 這一個集合並不一定會是 G 的 subgroup (缺封閉性), 而且 P 也不會包含於它 (除非 $H \subseteq P$). 所以我們沒有如前面幾種 group action 去算 $|S_0|$ 的式子. 不過沒有關係, 在證 Second Sylow's Theorem 時我們不需要直接算 $|S_0|$.

4.5.2. Sylow p-subgroups 之間的關係. 由第一 Sylow 定理我們可找到一個 G 的 Sylow p-subgroup. 第二 Sylow 定理告訴我們如何由這一個 Sylow p-subgroup, 得到所有 G 的 Sylow p-subgroup.

Theorem 4.5.1 (Second Sylow's Theorem)**.** *令 p 是一質數. 若 G 是一個 finite group, 而 P 是 G 的一個 Sylow p-subgroup.*

(1) *若 H 是 G 的一個 p-subgroup, 則存在 $a \in G$ 使得*

$$H \subseteq a \cdot P \cdot a^{-1}.$$

(2) *若 P' 是 G 的另一個 Sylow p-subgroup, 則存在 $a \in G$ 使得*

$$P' = a \cdot P \cdot a^{-1}.$$

Proof. (1) 我們考慮前面所述 H 對 $S = \{a \cdot P \,|\, a \in G\}$ 的 group action. 假設 $|G| = p^n m$, 其中 $p \nmid m$. 因 P 是 G 的 Sylow p-subgroup, 由定義知 $|P| = p^n$. 故由式子 (4.16) 知 $|S| = |G|/|P| = m$. 然而 $p \nmid m$, 故知 p 不能整除 $|S|$, 也就是說

$$|S| \not\equiv 0 \pmod{p}. \tag{4.18}$$

由假設 H 是一個 p-group, 故由 Proposition 4.1.4 和前一式子 (4.18) 知

$$|S_0| \equiv |S| \not\equiv 0 \pmod{p}.$$

也就是說 p 不能整除 $|S_0|$. 這告訴我們 S_0 是非空的集合; 否則 $|S_0| = 0$, 這和 p 不能整除 $|S_0|$ 矛盾. 既然 S_0 是非空的, 所以存在 $a \in G$ 使得 $a \cdot P \in S_0$. 故由式子 (4.17) 知 $a^{-1} \cdot H \cdot a \subseteq P$. 這告訴我們 $H \subseteq a \cdot P \cdot a^{-1}$.

(2) 當 P' 是 G 中另一個 Sylow p-subgroup, 我們直接套用 (1) 的結果知存在 $a \in G$ 使得 $P' \subseteq a \cdot P \cdot a^{-1}$. 然而 Lemma 1.5.2 告訴我們 $|P| = |a \cdot P \cdot a^{-1}|$, 且又由定義 $|P'| = |P|$, 故得 $|P'| = |a \cdot P \cdot a^{-1}|$. 所以得證 $P' = a \cdot P \cdot a^{-1}$. □

Theorem 4.5.1 告訴我們若在 G 找到一個 Sylow p-subgroup P, 則所有的 Sylow p-subgroup 都是 $a \cdot P \cdot a^{-1}$, 這種形式. 如果 P 剛好是 G 的一個 normal subgroup, 則知任意的 $a \in G$ 都符合 $a \cdot P \cdot a^{-1} = P$, 換句話說 G 只有一個 Sylow p-subgroup. 反之, 若 P 不是 G 的 normal subgroup, 則存在一個 $a \in G$ 使得 $a \cdot P \cdot a^{-1} \neq P$. 然而 Lemma 1.5.2 告訴我們 $a \cdot P \cdot a^{-1}$ 是 G 的一個 subgroup, 且 $|a \cdot P \cdot a^{-1}| = |P|$, 換句話說 $a \cdot P \cdot a^{-1}$ 是 G 中另一個不等於 P 的 Sylow p-subgroup. 故此時 Sylow p-subgroup 並不唯一. 我們證得:

Corollary 4.5.2. *若 P 是 G 的一個 Sylow p-subgroup, 則 G 僅有一個 Sylow p-subgroup 若且為若 P 是 G 的 normal subgroup.*

Example 4.5.3. 我們知 $|A_4| = 4!/2 = 2^2 \cdot 3$. 我們考慮 A_4 的 Sylow 2-subgroup 和 Sylow 3-subgroup. 已知 A_4 中有一個 order 4 的 normal subgroup

$$N = \{I, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

因為 N 是 A_4 的 Sylow 2-subgroup, 故知 A_4 中不會有其他 order 為 4 的 subgroup. 而 $(1\ 2\ 3)$ 在 A_4 中產生的 cyclic subgroup 是 order 3, 故 $\langle(1\ 2\ 3)\rangle$ 是 A_4 的一個 Sylow 3-subgroup. 同理 $\langle(1\ 2\ 4)\rangle$ 是另一個 Sylow 3-subgroup. 所以知 $\langle(1\ 2\ 3)\rangle$ 不可能是 A_4 的 normal subgroup.

4.6. Third Sylow's Theorem

第二個 Sylow 定理很清楚的告訴我們什麼時候 Sylow p-subgroup 是唯一的. 而萬一不唯一它也告訴我們此時其他的 Sylow p-subgroup 長什麼樣子. 不過並沒有告訴我們若不唯一那麼應該有多少個. 第三 Sylow Theorem 給了我們一個還算不錯的答案.

4.6.1. Group action on the set of Sylow p-subgroups. 若 G 是一個 finite group, p 是一個整除 $|G|$ 的質數. 令 S 為 G 中所有的 Sylow p-subgroup 所成的集合 (也就是每個 Sylow p-subgroup 都看成是 S 的一個元素). 我們要介紹兩種 group action, 一個是將 G 作用在 S 上. 另一個是選定 G 中任一個 Sylow p-subgroup P 而考慮 P 對 S 的作用.

我們定義 G 對 S 的作用如下: 對任意 $a \in G$, $P' \in S$, 我們定義

$$a * P' = a \cdot P' \cdot a^{-1}.$$

我們證明 $(G, S, *)$ 是一個 group action. 首先證明 (Act1). 因 P' 是 G 的 Sylow p-subgroup, 前面已提過 Lemma 1.5.2 告訴我們 $a \cdot P' \cdot a^{-1}$ 也是 G 的 Sylow

p-subgroup. 故得 $a * P' \in S$. 而 $e * P' = e \cdot P' \cdot e^{-1} = P'$ 故 (Act2) 也成立. 最後若 $a, b \in G$, 因為

$$(a \cdot b) * P' = (a \cdot b) \cdot P' \cdot (a \cdot b)^{-1} = (a \cdot b) \cdot P' \cdot (b^{-1} \cdot a^{-1}),$$

且

$$a * (b * P') = a \cdot (b * P') \cdot a^{-1} = a \cdot (b \cdot P' \cdot b^{-1}) \cdot a^{-1},$$

故由結合率知 $(a \cdot b) * P' = a * (b * P')$. 這證明了 (Act3).

$|S|$ 是什麼呢? 無庸置疑的就是 G 中所有 Sylow p-subgroup 的個數. 這裡我們並不關心 S_0 是什麼, 主要原因在這個 group action 之下只分成一類, 所以我們可以直接計算 $|S|$. 為什麼只分成一類呢? 任選 $P_1, P_2 \in S$ 由第二 Sylow 定理 (Theorem 4.5.1) 我們知存在 $a \in G$ 使得

$$P_2 = a \cdot P_1 \cdot a^{-1} = a * P_1.$$

換句話說任選 S 中的兩元素都是同類的, 所以在此分類之下當然只有一類了. 現在我們任取一 $P' \in S$, 由式子 (4.1) 知 $|S| = |[P']|$. 所以我們只要算 $[P']$ 有多少就可以了. Lemma 4.1.3 告訴我們 $|[P']| = |G|/|G_{P'}|$, 其中 $G_{P'} = \{a \in G \,|\, a * P' = P'\}$. $G_{P'}$ 到底是什麼呢? 由定義知任何 $G_{P'}$ 中的元素 a 皆須滿足

$$P' = a * P' = a \cdot P' \cdot a^{-1}.$$

如果大家還不健忘的話該記得我們曾在 4.4 節中介紹過這樣的元素所成的集合就是 P' 的 normalizer $N(P')$. 所以我們知 $G_{P'} = N(P')$. 因此我們可得

$$|S| = |[P']| = \frac{|G|}{|N(P')|} \tag{4.19}$$

現在我們介紹另一個類似的 group action. 選定 G 中任一個 Sylow p-subgroup P, 我們定義 P 對 S (和前面同樣的 S) 的作用如下: 對任意 $x \in P$, $P' \in S$, 我們定義

$$x * P' = x \cdot P' \cdot x^{-1}.$$

這個作用和前一個幾乎相同, 只是我們拿比較小的 group 去作用. 不難看出 $(P, S, *)$ 也是一個 group action.

同樣的 S 的個數仍是所有 G 的 Sylow p-subgroup 的個數. 要注意的是這次我們作用的 group 比較小, 所以同類的元素會比較少, 因此前一次所得只分成一類的結果這兒並不一定對. 這一次我們需要算 $|S_0|$.

S_0 是什麼呢? 由定義若 $P' \in S_0$, 表示對所有 $x \in P$,

$$x \cdot P' \cdot x^{-1} = x * P' = P',$$

由 normalizer 的定義知這表示 $x \in N(P')$. 換句話說若 $P' \in S_0$ 則 P' 必須具有對所有 $x \in P$ 皆可得 $x \in N(P')$ 的性質. 也就是說: 若 $P' \in S_0$, 則 $P \subseteq N(P')$. 反

之, 若 P' 是 G 的一個 Sylow p-subgroup 且符合 $P \subseteq N(P')$, 則對任意的 $x \in P$, 皆有 $x * P' = P'$. 所以我們證得

$$S_0 = \{P' \in S \mid P \subseteq N(P')\}. \tag{4.20}$$

最後我們強調因 $P \in S$ 且 Lemma 4.4.1 告訴我們 $P \subseteq N(P)$, 故知

$$P \in S_0. \tag{4.21}$$

4.6.2. Sylow p-subgroups 的個數. 第三 Sylow 定理可以幫我們由 G 的 order 來判斷 G 的 Sylow p-subgroups 大致有多少個.

Theorem 4.6.1 (Third Sylow's Theorem)**.** 若 G 是一個 *group* 且 $|G| = p^n m$, 其中 $n \geq 1$, p 是一個質數且 $p \nmid m$. 令 r 表示 G 中所有 *Sylow p-subgroup* 的個數, 則

$$(1) \quad r \mid m; \qquad (2) \quad r \equiv 1 \pmod{p}.$$

Proof. (1) 我們利用第一個 group action $(G, S, *)$ 來證明 $r \mid m$. 由式子 (4.19) 知: 任選 $P' \in S$, 我們有 $r = |G|/|N(P')|$. 不過 Lemma 4.4.1 告訴我們 P' 是 $N(P')$ 的 subgroup. 由於 $|P'| = p^n$, Lagrange 定理告訴我們 $|N(P')|$ 是 p^n 的倍數, 又由於 $N(P')$ 是 G 的 subgroup, 再用一次 Lagrange 定理得 $|N(P')| = p^n d$ 其中 $d \mid m$. 故知

$$r = \frac{|G|}{|N(P')|} = \frac{p^n m}{p^n d} = \frac{m}{d}.$$

因此 $r \mid m$.

(2) 我們利用第二個 group action $(P, S, *)$ 來證明 $r \equiv 1 \pmod{p}$. 因 P 是一個 p-group, 由 Proposition 4.1.4 知

$$r = |S| \equiv |S_0| \pmod{p}. \tag{4.22}$$

我們現在來計算 $|S_0|$. 由式子 (4.20) 知若 $P' \in S_0$ 則 $P \subseteq N(P')$. 不過前面已知 $|N(P')| = p^n d$, 其中 $d \mid m$. 然而由 $p \nmid m$ 知 $p \nmid d$, 因此由 $|P| = p^n$ 知 P 是 $N(P')$ 的一個 Sylow p-subgroup. 另一方面, 由 Lemma 4.4.1 知, P' 是 $N(P')$ 的 normal subgroup. 但 P' 也是 $N(P')$ 的 Sylow p-subgroup. Corollary 4.5.2 告訴我們 P' 是 $N(P')$ 唯一的 Sylow p-subgroup. 故得 $P = P'$. 換句話說 S_0 中只可能有 P 這個元素. 因此由式子 (4.21) 知 $S_0 = \{P\}$, 也就是說 S_0 只有一個元素. 故由式子 (4.22) 得 $r \equiv 1 \pmod{p}$. □

Example 4.6.2. (1) 我們知道在 A_4 中 Sylow 3-subgroup 並不唯一 (Example 4.5.3), 那麼 A_4 到底有多少個 Sylow 3-subgroup 呢? 假設有 r 個, 由於 $|A_4| = 4 \cdot 3$, 由第三 Sylow 定理 (Theorem 4.6.1) 知 $r \mid 4$ 且 $r = 3k + 1$. 也就是 $r = 1$ 或 $r = 4$. 由於已知 $r \neq 1$, 故得 $r = 4$. 事實上在 A_4 中由

$$(1\ 2\ 3), \quad (1\ 2\ 4), \quad (1\ 3\ 4), \quad (2\ 3\ 4)$$

這四個 3-cycles 個別產生的 cyclic group 皆相異, 故知這些就是所有 A_4 的 Sylow 3-subgroup.

(2) 在 A_5 中有多少 Sylow 5-subgroups 呢? 假設有 r 個, 由於 $|A_5| = 5!/2 = 5\cdot 12$, 由第三 Sylow 定理 (Theorem 4.6.1) 知 $r \mid 12$ 且 $r = 5k+1$. 也就是 $r = 1$ 或 $r = 6$. 由於已知 A_5 是 simple (Theorem 3.4.26) 所以 A_5 的 Sylow 5-subgroup 不可能是 A_5 的 normal subgroup. 因此由第二 Sylow 定理 (Corollary 4.5.2) 知 $r \neq 1$. 故得 $r = 6$. 事實上在 A_5 中所有的 5-cycle 共有 $4! = 24$ 個 (為甚麼呢? 這是高中的排列組合中五個人坐圓桌的問題吧!). 不過任一個 5-cycle 所產生的 cyclic group 中有 4 個 5-cycle 出現. 例如:

$$\langle (1\ 2\ 3\ 4\ 5)\rangle = \{(1\ 2\ 3\ 4\ 5), (1\ 3\ 5\ 2\ 4), (1\ 4\ 2\ 5\ 3), (1\ 5\ 4\ 3\ 2), I\}$$

因此這 24 個 5 cycle 只產生 $24/4 = 6$ 個相異的 order 5 的 subgroup. 這就是所有 A_5 的 Sylow 5-subgroup.

大家不要被 Example 4.6.2 誤導. 第三 Sylow 定理並不是萬靈丹, 一般來說並不能單單由一個 group 的 order 再利用第三 Sylow 定理就能算出有多少個 Sylow p-subgroup. 有時要加入所考慮的 group 的性質, 例如在 A_5 中 Sylow 2-subgroup 只用 Third Sylow's Theorem 來算就有可能有 3, 5 或 15 個. 所以要進一層的考量才可算出真正有幾個.

4.7. Sylow 定理的應用

我們已大致介紹完了 group 的一些基本性質. 在這有關 group 的最後一節中我們介紹一些可以利用 Sylow 定理得到的性質. 其實這些性質不只要用到 Sylow 定理, 還需要一些前面學過的定理輔助, 所以把它放在 group 的最後一節讓大家複習一下前面所學的, 也算給 group 一個完美的結局.

我們曾碰過有些特殊 order 的 group, 我們可以僅由其 order 就能判斷出這個 group 長甚麼樣子 (例如 order p 的 group 是 cyclic, order p^2 的 group 是 abelian). 現在我們要談更多類似的結果.

Proposition 4.7.1. *若 G 是一個 group 且 $|G| = p^n q$, 其中 $n \geq 1$, p 和 q 是相異質數且 $p > q$. 則 G 的 Sylow p-group 是 G 的 normal subgroup.*

Proof. 我們只知道 group 的 order, 沒有其他的訊息, 所以知道不可能用 normal 的定義來直接證得本定理. 相信大家會想到 Second Sylow's Theorem 吧. 如果我們能證得 G 中的 Sylow p-subgroup 只有一個, 那麼利用第二 Sylow 定理 (Corollary 4.5.2) 就可知它是 G 的 normal subgroup 了.

假設 G 有 r 個 Sylow p-subgroup. 由第三 Sylow 定理 (Theorem 4.6.1) 知 $r \mid q$ 且 $r = pk+1$. 不過若 $r \neq 1$, 表示 $r \geq p+1 > q$, 這和 $r \mid q$ 相矛盾. 因此得 $r = 1$, 故知 G 的 Sylow p-group 是 G 的 normal subgroup. □

我們接下來看 $n = 1$ 的情況.

Proposition 4.7.2. 若 G 是一個 *group* 且 $|G| = pq$, 其中 p 和 q 是相異質數且 $p > q$. 若又知 $q \nmid p-1$, 則 G 是一個 *cyclic group.*

Proof. 這就更難直接證明了. 首先由於 p, q 皆是質數, Cauchy 定理 (Theorem 4.2.1) 告訴我們 G 中有兩個 subgroups P 和 Q 其 order 分別為 p 和 q. 其實 P 是 G 的 Sylow p-subgroup, Q 是 Sylow q-subgroup. 由 Proposition 4.7.1 知 P 是 G 的 normal subgroup, 而 Q 呢? 假設 G 中有 r 個 Sylow q-subgroup. 由第三 Sylow 定理 (Theorem 4.6.1) 知 $r \mid p$ 且 $r = qk+1$. 如果 $r \neq 1$, 由 $r \mid p$ 知 $r = p$, 因此得 $p = qk+1$. 也就是 $qk = p-1$. 此和 $q \nmid p-1$ 相矛盾. 故知 $r = 1$, 也因此由第二 Sylow 定理 (Corollary 4.5.2) 知 Q 也是 G 的 normal subgroup.

P 和 Q 既然都是 normal subgroup, 如果能證明 $P \cap Q = \{e\}$ 的話由 Theorem 3.2.4 可得 $G \simeq P \times Q$. 然而 $P \cap Q$ 同時是 P 和 Q 的 subgroup (Lemma 1.5.1), 故由 Lagrange 定理 (Theorem 2.2.2) 知 $|P \cap Q|$ 同時整除 $|P| = p$ 和 $|Q| = q$. 因此得 $|P \cap Q| = 1$, 也就是說 $P \cap Q = \{e\}$.

好了我們知 $G \simeq P \times Q$, 然而 $|P| = p$, $|Q| = q$ 都是質數, 故由 Corollary 2.2.3 和 Theorem 3.1.1 知 $P \simeq \mathbb{Z}/p\mathbb{Z}$ 且 $Q \simeq \mathbb{Z}/q\mathbb{Z}$. 因此利用 Lemma 3.2.5 和 Corollary 3.2.3 得

$$G \simeq P \times Q \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}.$$

故得 G 是一個 cyclic group. □

如果 $q \mid p-1$ 怎麼辦? 我們來看最簡單的 $q = 2$ 的情況. 也就是說 $|G| = 2p$, 其中 p 是一個奇質數. 此時由 Proposition 4.7.1 知, G 中唯一的 Sylow p-subgroup P 是 G 的 normal subgroup. 又由於 $|P| = p$, 故由 Corollary 2.2.3 知存在 $a \in G$ 且 $\mathrm{ord}(a) = p$ 使得 $P = \langle a \rangle$. 因 2 整除 $|G|$, 利用 Cauchy 定理 (Theorem 4.2.1) 知存在 $b \in G$ 且 $\mathrm{ord}(b) = 2$. (注意: 此時因 Lagrange's Theorem 知 $b \notin P$ 且 $P \cap \langle b \rangle = \{e\}$.) 由 P 是 G 的 normal subgroup 知存在 $i \in \mathbb{N}$, 使得 $b \cdot a \cdot b^{-1} = a^i$. 我們要知道 i 是多少. 由於

$$b \cdot (b \cdot a \cdot b^{-1}) \cdot b^{-1} = b \cdot a^i \cdot b^{-1} = (b \cdot a \cdot b^{-1})^i = a^{i^2}.$$

而 $b^2 = (b^{-1})^2 = e$, 故 $a = a^{i^2}$. 也就是說 $a^{i^2-1} = e$. 利用 Lemma 2.3.2 得 $\mathrm{ord}(a) = p \mid i^2 - 1$. 由於 p 是質數, 我們得 $p \mid i-1$ 或 $p \mid i+1$. 也就是說 $i = pk+1$ 或 $i = pk-1$.

若 $i = pk+1$, 表示 $b \cdot a = a \cdot b$. 然而 $\langle a \rangle \cap \langle b \rangle = \{e\}$. 由 Lemma 3.4.8 知 $\mathrm{ord}(a \cdot b) = 2p = |G|$. 換句話說 G 是一個 cyclic group.

若 $i = pk-1$, 表示 $b \cdot a = a^{-1} \cdot b$, 而 $a^{-1} \neq a$ (因 $\mathrm{ord}(a) = p \neq 2$), 故知 G 不是 abelian. 若令 $B = \langle b \rangle$, 因 P 是 G 的 normal subgroup, 由第二 Isomorphism 定理 (Theorem 2.6.4) 知 $P \cdot B$ 是 G 的一個 subgroup, 且

$$P \cdot B/P \simeq B/P \cap B.$$

由於 $P \cap B = \{e\}$, 知 $|P \cdot B| = |P| \cdot |B| = 2p$. 也就是說 $P \cdot B = G$. 換句話說

$$G = \{a^i \cdot b^j \,|\, 0 \le i \le p-1,\, 0 \le j \le 1\}.$$

事實上我們可證明存在這樣的一個 group. 我們稱之為 *dihedral group of degree p*, 記作 D_p. 綜合以上我們證得了以下的結果.

Proposition 4.7.3. *若 G 是一個 group 且 $|G| = 2p$, 其中 p 是一個奇質數, 則*

$$G \simeq \mathbb{Z}/2p\mathbb{Z} \quad \text{or} \quad G \simeq D_p.$$

Proposition 4.7.3 告訴我們 D_p 是唯一的 order 為 $2p$ 的 nonabelian group. 事實上對所有的 $n \ge 3$, 都存在一個 nonabelian group

$$D_n = \{a^i \cdot b^j \,|\, 0 \le i \le n-1,\, 0 \le j \le 1\},$$

是由兩個元素 a, b 所產生, 其中 $\mathrm{ord}(a) = n$, $\mathrm{ord}(b) = 2$ 且 $b \cdot a = a^{-1} \cdot b$. 這樣的 nonabelian group, 我們稱之為 *dihedral group of degree n*. 它的 order 為 $2n$. 不過當 n 不是質數時, D_n 就不一定是唯一的 order 為 $2n$ 的 nonabelian group 了.

最後我們想以探討所有 order 小於 10 的 group 有哪些作為 group 這個部份的結束.

當然 order 為 1 的就只有 identity. order 為 2, 3, 5, 7 的 group 都是 cyclic 分別 isomorphic to, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$.

order 為 4 的 group 由 Proposition 4.3.3 知有兩種, 分別 isomorphic to $\mathbb{Z}/4\mathbb{Z}$ 和 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. 同理 order 為 9 的也只有兩種, 分別 isomorphic to $\mathbb{Z}/9\mathbb{Z}$ 和 $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

order 為 6 的 group 由 Proposition 4.7.3 知也有兩種, 一個是 abelian 另一個是 nonabelian, 它們分別 isomorphic to $\mathbb{Z}/6\mathbb{Z}$ 和 D_3. 有的同學或許會疑問: 我們學過 S_3 它也有 $3! = 6$ 個元素, 為何沒有列出呢? 別緊張! 事實上 S_3 是 nonabelian, 我們可以證得 $S_3 \simeq D_3$. 其中 S_3 的 (1 2 3) 就對應到 D_3 中的 order 為 3 的元素 a, 而 (1 2) 就對應到 D_3 中的 order 為 2 的元素 b, 且

$$(1\ 2)(1\ 2\ 3) = (2\ 3) = (3\ 2\ 1)(1\ 2).$$

同理 order 為 10 的 group 也有兩種, 它們分別 isomorphic to $\mathbb{Z}/10\mathbb{Z}$ 和 D_5.

最後有點棘手的是 order 為 8 的 group. Abelian 的部分還好處理, 我們知道有 $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 和 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. 至於 nonabelian 部分我們已知有個

$$D_4 = \{a^i \cdot b^j \,|\, 0 \le i \le 3,\, 0 \le j \le 1\},$$

其中 $\mathrm{ord}(a) = 4$, $\mathrm{ord}(b) = 2$ 且 $b \cdot a = a^{-1} \cdot b$. 事實上還有另一個很常見的 order 為 8 的 nonabelian group Q_8, 稱之為 *quaternion group*. 最常見的 Q_8 表示法如下:

$$Q_8 = \{\pm 1, \pm i, \pm j \pm k\},$$

其中 $i^2 = j^2 = k^2 = -1$ 且 $i \cdot j = -j \cdot i = k$. 因為 Q_8 中 order 為 4 的元素有 6 個 (即 $\pm i, \pm j$ 和 $\pm k$), 而 D_4 中只有兩個 (即 a 和 a^3) 故知 Q_8 和 D_4 並不 isomorphic. 我們要證明 order 8 的 nonabelian group 只有這兩種.

Proposition 4.7.4. *若 G 是一個 order 為 8 的 nonabelian group, 則*

$$G \simeq D_4 \quad \text{or} \quad G \simeq Q_8.$$

Proof. 因 $|G| = 8$, 由 Lagrange 定理 (Corollary 2.3.4) 知 G 中元素的 order 只能是 1, 2, 4 或 8. 我們要證明 G 中必有一元素其 order 為 4. 若 G 中有元素之 order 為 8, 知 G 為 cyclic 和 G 是 nonabelian 相矛盾. 因此若沒有元素 order 為 4 表示任意 G 中非 identity 的元素的 order 皆為 2, 也就是說所有的 $g \in G$ 都滿足 $g^2 = e$. 若真如此, 任取 $a, b \in G$, 我們知

$$e = (a \cdot b)^2 = (a \cdot b) \cdot (a \cdot b),$$

故得

$$a \cdot b = a \cdot (a \cdot b) \cdot (a \cdot b) \cdot b = b \cdot a$$

這又和 G 是 nonabelian 相矛盾. 故知 G 中必存在 order 為 4 的元素.

現取 $a \in G$ 其中 $\text{ord}(a) = 4$. 因 $\langle a \rangle$ 是一個 order 為 $4 = 2^2$ 的 subgroup 而 $|G| = 8 = 2^3$, 故由第一 Sylow 定理 (Theorem 4.4.2) 知, G 存在一個 subgroup K 其中 $|K| = 2^{2+1}$ 且 $\langle a \rangle$ 是 K 的 normal subgroup. 但由於 $|K| = |G|$, 故知 $K = G$. 因此 $\langle a \rangle$ 是 K 的 normal subgroup.

既然 $\langle a \rangle$ 是 K 的 normal subgroup, 任取 $b \in G$ 但 $b \notin \langle a \rangle$, 皆存在 $i \in \mathbb{N}$ 使得 $b \cdot a \cdot b^{-1} = a^i$. 我們想要知道 i 為多少. 首先觀察若 $\text{ord}(b \cdot a \cdot b^{-1}) = r$, 即

$$(b \cdot a \cdot b^{-1})^r = b \cdot a^r \cdot b^{-1} = e,$$

則得 $a^r = e$. 故由 Lemma 2.3.2 知 $4 \,|\, r$. 然而 $(b \cdot a \cdot b^{-1})^4 = b \cdot a^4 \cdot b^{-1} = e$ 故知 $r \,|\, 4$. 也就是說 $\text{ord}(b \cdot a \cdot b^{-1}) = 4$. 由 Lemma 2.3.3 之只有當 $i = 1, 3$ 時 $\text{ord}(a^i) = 4$, 故知若 $b \cdot a \cdot b^{-1} = a^i$, 則 $i = 1$ 或 $i = 3$. 不過如果 $i = 1$ 表示 $b \cdot a = a \cdot b$ 故知 G 是 abelian, 此又和 G 是 nonabelian 的假設相矛盾. 因此知

$$b \cdot a = a^3 \cdot b = a^{-1} \cdot b.$$

最後由於 $b \notin \langle a \rangle$, 只有可能 $\text{ord}(b) = 2$ 或 $\text{ord}(b) = 4$. 若 $\text{ord}(b) = 2$ 則知 $G \simeq D_4$; 若 $\text{ord}(b) = 4$, 則知 $G \simeq Q_8$. 故得證 order 8 的 nonabelian group 只有兩種. □

如果同學有興趣當然可以一直找下去: order 11 的 group 有多少 (這個簡單)? order 12 的有多少? 這樣一直下去問題越來越困難. 大家應不難了解問題的困難度和 order 大小無關, 而是和其質因數的分解有關. 大家應能體會次方越大就越複雜, 例如 order 16 的 group 就有 14 個, 而 order 32 的 group 就有高達 51 個之多.