大學基礎代數

李華介

國立台灣師範大學數學系

Chapter 3

一些常見的 Groups

這一章中我們介紹一些常見的 groups: cyclic groups, abelian groups 和 symmetric groups.

3.1. Cyclic Groups

回顧一下, 一個 group G 是所謂的 cyclic group 就是在 G 中可以找到一個元素 $a \in G$ 使得 a 產生的 cyclic group $\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$ 就是 G. 換句話說 G 中的元素都是 a^i 這種形式. Cyclic group 可以說是 group 中最簡單的一種. 其實我們可以知道所有的 cyclic groups 有哪些.

Theorem 3.1.1. *若 G 是一個 cyclic group. 則:*

(1) *若 G 的個數有無窮多 (infinite group), 則 $G \simeq \mathbb{Z}$.*

(2) *若 G 的個數有 n 個 (order 為 n), 則 $G \simeq \mathbb{Z}/n\mathbb{Z}$.*

Proof. 若 G 是 cyclic, 假設 G 可由 a 生成. 考慮 $\phi : \mathbb{Z} \to G$ 定義成 $\phi(i) = a^i$. 很容易看出

$$\phi(i+j) = a^{i+j} = a^i \cdot a^j = \phi(i) \cdot \phi(j).$$

所以 ϕ 是由 $\mathbb{Z}$ 這個加法 group 到 G 的 group homomorphism. 再加上 G 中的元素都是 a^i 這種形式所以可知 ϕ 是 onto 的. 既然 ϕ 是 epimorphism 我們就可以利用 First Isomorphism 定理 (Corollary 2.6.2).

(1) 若 G 是 infinite group. 我們欲證 ϕ 是一對一的. 由於 0 是 $\mathbb{Z}$ 的 identity, Lemma 2.5.6 告訴我們這等同於要證明 $\ker(\phi) = \{0\}$. 若 $m \in \ker(\phi)$, 則 $\phi(m) = a^m = e$. 若 $m \neq 0$, 則利用任何整數 i 都可寫成 $i = mh + r$ 的形式, 其中 $h \in \mathbb{Z}$, $0 \leq r < |m|$. 可得任何 G 中的元素 a^i 都可寫成

$$a^i = (a^m)^h \cdot a^r = e^h \cdot a^r = a^r.$$

換句話說 G 的元數都可寫成 a^r, 其中 $0 \le r < |m|$; 也就是說 G 最多只有 $|m|$ 個元素. 這和 G 有無窮多個元素相違背. 所以我們的假設 $m \neq 0$ 是不可能發生的. 不過 $\phi(0) = a^0 = e$, 故 $0 \in \ker(\phi)$. 因此得 $\ker(\phi) = \{0\}$.

(2) 若 G 是一個 cyclic group of order n, 由於 $G = \langle a \rangle$ 故 $\mathrm{ord}(a) = n$. 而 Lemma 2.3.2 告訴我們若 $a^m = e$ 則 $n \,|\, m$. 今若 $m \in \ker(\phi)$, 及 $\phi(m) = a^m = e$. 故由前述結果知 $n \,|\, m$: 也就是說 m 是 n 的倍數. 另一方面若 $m = nh$ 是 n 的倍數, 則 $\phi(m) = a^m = (a^n)^h = e$: 也就是說 $m \in \ker(\phi)$. 我們得到 $\ker(\phi)$ 是由 n 的倍數所成的集合. 因此 $\ker(\phi) = n\mathbb{Z}$. 故由 Corollary 2.6.2 知 $G \simeq \mathbb{Z}/n\mathbb{Z}$. □

Theorem 3.1.1 告訴我們說 cyclic groups 是可以用其個數來分類的. 也就是說給定一正整數 n 用 isomorphism 的觀點來看就只有一種 cyclic group 其 order 為 n, 但是要注意這並不表示沒有其他的 group 其 order 是 n. 然而若是給定的是一個質數 p, 那麼 Corollary 2.2.3 告訴我們的確只有一種 group 其 order 為 p, 就是 cyclic group $\mathbb{Z}/p\mathbb{Z}$. 事實上在證明 Corollary 2.2.3 時我們是利用 Lagrange's Theorem 知道當 $|G| = p$ 時除了 identity 及 G 本身外 G 不會有其他的 nontrivial proper subgroup. 反之下一個 Lemma 告訴我們如果 G 沒有 nontrivial proper subgroup, 則 G 一定是 cyclic group.

Lemma 3.1.2. 如果 G 是一個 *group* 且沒有 *nontrivial* 的 *nontrivial proper subgroup,* 則 G 一定是一個 *cyclic group* 且 $|G| = p$, 其中 p 為一個質數.

Proof. 任選 $a \in G$ 且 $a \neq e$, 則由 a 產生的 cyclic group $\langle a \rangle$ 是 G 的一個 subgroup. 不過由於 $\langle a \rangle \neq \{e\}$, 故由假設 G 沒有 nontrivial proper subgroup 知, $\langle a \rangle = G$. 另外若 $|G| = \mathrm{ord}(a)$ 不是質數, 即 $\mathrm{ord}(a) = mn$ 其中 $m > 1$ 且 $n > 1$, 則由 Proposition 2.3.3 知

$$\mathrm{ord}(a^m) = \frac{mn}{\gcd(mn, m)} = n,$$

也就是說 a^m 產生的 cyclic subgroup of G 其個數是 n. 故 $\langle a^m \rangle \neq \{e\}$ 且 $\langle a^m \rangle \neq G$. 換句話說 $\langle a^m \rangle$ 是 G 的 nontrivial proper subgroup. 這與假設不符, 故 G 的 order 是一個質數. □

若 G 是一個 cyclic group, 大家或許會猜它的 subgroup 應該也都是 cyclic group. 沒錯, 可是數學不能用猜的, 我們還是得給個證明.

Proposition 3.1.3. 若 G 是一個 *cyclic group,* 則 G 中任意的 *subgroup* 也是一個 *cyclic group.*

Proof. 假設 $G = \langle a \rangle$ 是一個 cyclic group, 且 H 是 G 中任意的一個 subgroup. 別忘了要證明 H 也是一個 cyclic group 就必須找一個元素可以產生 H. 要找甚麼元素呢? 當然要靠 a 來幫忙了.

如果 H 中的元素只有 identity e, 那當然 $H = \langle e \rangle$ 是一個 cyclic group. 如果 H 不是 $\langle e \rangle$, 由於 $H \subseteq G$, H 中的元素都是 a^i, $i \in \mathbb{Z}$ 這種形式, 我們一定可以找到

一個最小的正整數 n 滿足 $a^n \in H$. 我們要證明 $H = \langle a^n \rangle$. 由於 $a^n \in H$ 所以自然知 $\langle a^n \rangle \subseteq H$. 我們只剩下要說明 $H \subseteq \langle a^n \rangle$, 也就是說 H 中的元素都是 $(a^n)^h$, $h \in \mathbb{Z}$ 這種形式. 假設 $a^m \in H$, 我們利用整數的餘數定理, 知存在整數 h 及 r, 其中 $0 \leq r < n$ 使得 $m = n \cdot h + r$. 因此得

$$a^r = a^m \cdot (a^{nh})^{-1}.$$

不過由假設 $a^m \in H$ 且 $(a^{nh})^{-1} \in H$, 故知 $a^r \in H$. 但是我們已選 n 是最小的正整數滿足 $a^n \in H$, 而又 $0 \leq r < n$, 所以 $a^r \in H$ 表示 $r = 0$. 因此我們得證 H 中的元素都是 $(a^n)^h$ 這種形式. □

3.2. Direct Product

若給定兩個(或更多) groups, 在這節中我們將介紹一種方法可以利用這些 groups 創造出新的 group. 這個方法稱之為 direct product.

Definition 3.2.1. 給定兩 groups, G_1 和 G_2, 則定義

$$G_1 \times G_2 = \{(a_1, a_2) \,|\, a_1 \in G_1,\, a_2 \in G_2\}.$$

若 $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$, 則定義其乘法為

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot b_1, a_2 \cdot b_2).$$

我們稱 $G_1 \times G_2$ 為 G_1 和 G_2 的 *direct product*.

事實上利用上述的乘法 $G_1 \times G_2$ 是一個 group. 其中封閉性和結合率可以用原來 G_1 和 G_2 的封閉性與結合濾輕鬆得證. 什麼會是 $G_1 \times G_2$ 的 identity 呢? 若 e_1 和 e_2 分別是 G_1 和 G_2 的 identity, 應該很容易看出 (e_1, e_2) 就是 $G_1 \times G_2$ 的 identity 吧! 至於 (a_1, a_2) 的 inverse 是 (a_1^{-1}, a_2^{-1}) 直接相乘就可得知.

Proposition 3.2.2. 若 G_1 和 G_2 都是 *cyclic groups,* 且其 *order* 分別為 n 和 m.

(1) 若 n 和 m 互質, 則 $G_1 \times G_2$ 仍是一個 *cyclic group.*

(2) 若 n 和 m 不互質, 則 $G_1 \times G_2$ 不是 *cyclic group.*

Proof. 因 G_1 和 G_2 是 cyclic, 假設 G_1 和 G_2 分別是由 a 和 b 生成. 注意: 從定義知 $G_1 \times G_2$ 的 order 為 nm.

(1) 假設 n 和 m 互質, 要證明 $G_1 \times G_2$ 是 cyclic 我們只要證明 $G_1 \times G_2$ 中存在一元素其 order 為 nm. 因為如此一來, 這個元素生成的 group 和 $G_1 \times G_2$ 個數一樣多, 所以 $G_1 \times G_2$ 就可由其生成. 該找什麼元素呢? 讓我們試試 (a, b) 吧. 由 Lemma 2.3.1 要說 (a, b) 的 order 為 nm, 等同於說 nm 是最小的正整數使得

$$(a, b)^{nm} = (e_1, e_2).$$

首先觀察

$$(a, b)^{nm} = ((a^n)^m, (b^m)^n) = (e_1^m, e_2^n) = (e_1, e_2).$$

接著要說明 nm 是符合上式的最小的正整數. 假設 $(a,b)^r=(e_1,e_2)$, 則因 $(a,b)^r=(a^r,b^r)$, 故得 $a^r=e_1$ 且 $b^r=e_2$. 因 $\mathrm{ord}(a)=n$ 且 $\mathrm{ord}(b)=m$, 由 Lemma 2.3.2 知 $n\,|\,r$ 且 $m\,|\,r$. 然而由假設 n 和 m 互質可得 $nm\,|\,r$, 故若 r 是一個正整數使得 $(a,b)^r=(e_1,e_2)$ 則 $r\geq nm$. 由此證得 (a,b) 的 order 為 nm, 換句話說 $G_1\times G_2$ 是一個由 (a,b) 生成的 cyclic group.

(2) 假設 n 和 m 不互質, 令 l 為 n 和 m 的最小公倍數. 注意因 n 和 m 不互質, 此時 $l<nm$. 因 a 生成 G_1, 故 G_1 的元素都可寫成 a^i 這種形式. 同理 G_2 的元素都可寫成 b^j 這種形式. 因此 $G_1\times G_2$ 的元素都可寫成 (a^i,b^j) 這種形式. 考慮

$$(a^i,b^j)^l=(a^{il},b^{jl}).$$

因 l 是 n 的倍數, 故 $a^{il}=e_1$. 同理 $b^{jl}=e_2$. 也就是說 $(a^i,b^j)^l=(e_1,e_2)$. 由 Lemma 2.3.1 知 $G_1\times G_2$ 中的任一元素 (a^i,b^j) 其 order 小於或等於 l. 所以在 $G_1\times G_2$ 中找不到一個元素其 order 為 nm. 故 $G_1\times G_2$ 不可能是 cyclic. □

Corollary 3.2.3. *若 m, n 互質, 則*

$$\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}\simeq\mathbb{Z}/(nm)\mathbb{Z}.$$

Proof. 由 Proposition 3.2.2 知 $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ 是一個 cyclic group. 然而 $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$ 的 order 為 nm, 故由 Theorem 3.1.1 知其和 $\mathbb{Z}/(nm)\mathbb{Z}$ isomorphic. □

由 Proposition 3.2.2 知道兩個 cyclic groups 的 direct product 並不一定會依然是 cyclic, 所以 direct product 確實能幫我們產生新的 group. 以後我們可以看到所有的 finite abelian group 都可以用 cyclic groups 作 direct product 得到.

接下來我們來看看一個 group 若是由其他的 groups 用 direct product 得到, 那麼這一個 group 會有甚麼特性? 若 G_1 和 G_2 是兩個 groups, 且 e_1 和 e_2 分別為其 identity. 若 $G'=G_1\times G_2$, 我們觀察 G' 中兩個很特別的集合:

$$N'=\{(a,e_2)\,|\,a\in G_1\}\quad\text{and}\quad M'=\{(e_1,b)\,|\,b\in G_2\}.$$

很容易就可檢查出 N' 和 M' 都是 G' 的 subgroups. 事實上它們都是 G' 的 normal subgroups. 這是因為對於 G' 中的任一元素 (g_1,g_2), 由於 $g_1\in G_1$ 所以 若 $a\in G_1$ 則 $g_1\cdot a\cdot g_1^{-1}\in G_1$, 因此

$$(g_1,g_2)\cdot(a,e_2)\cdot(g_1,g_2)^{-1}=(g_1\cdot a\cdot g_1^{-1},g_2\cdot e_2\cdot g_2^{-1})=(g_1\cdot a\cdot g_1^{-1},e_2)\in N'.$$

同理

$$(g_1,g_2)\cdot(e_1,b)\cdot(g_1,g_2)^{-1}\in M'.$$

我們也很容易看出 $N'\simeq G_1$: 這是因為考慮函數 $\pi_1:N\to G_1$ 定為 $\pi_1((a,e_2))=a$, 則不難看出 π_1 是一個 group isomorphism. 同理可得 $M'\simeq G_2$. 另外 N' 和 M' 的特點是

$$G=N'\cdot M'\quad\text{and}\quad N'\cap M'=\{(e_1,e_2)\}.$$

因為 G' 中的元素都是 (g_1, g_2) 這種形式, 其中 $g_1 \in G_1$, $g_2 \in G_2$. 然而 $(g_1, e_2) \in N'$ 且 $(e_1, g_2) \in M'$, 故

$$(g_1, g_2) = (g_1, e_2) \cdot (e_1, g_2) \in N' \cdot M'.$$

另一方面若 $(g_1, g_2) \in N' \cap M'$, 則由 $(g_1, g_2) \in N'$ 得 $g_2 = e_2$, 再由 $(g_1, g_2) \in M'$ 得 $g_1 = e_1$. 故知 $\{(e_1, e_2)\} = N' \cap M'$.

Theorem 3.2.4. $G \simeq G_1 \times G_2$ 若且為若 G 中存在兩個 *normal subgroups* N 和 M 符合以下條件

(1) $N \simeq G_1$ 且 $M \simeq G_2$.

(2) $G = N \cdot M$

(3) $N \cap M = \{e\}$, 其中 e 是 G 的 *identity.*

Proof. 利用前面所定的 N' 及 M', 我們知 N' 和 M' 是 $G_1 \times G_2$ 的 normal subgroups, 且 $N' \simeq G_1$ 及 $M' \simeq G_2$. 我們也知 $G_1 \times G_2 = N' \cdot M'$ 及 $N' \cap M' = \{(e_1, e_2)\}$.

假設 $\phi : G \to G_1 \times G_2$ 是一個 isomorphism. 則令

$$N = \{a \in G \,|\, \phi(a) \in N'\} \quad \text{and} \quad M = \{b \in G \,|\, \phi(b) \in M'\}.$$

由 Correspondence 定理 (Theorem 2.7.1), 知 N 和 M 都是 G 的 normal subgroups, 又 $N/\ker(\phi) \simeq N'$ 且 $M/\ker(\phi) \simeq M'$. 但因 ϕ 是一對一, 故由 Lemma 2.5.6 得 $\ker(\phi) = \{e\}$. 因此

$$N \simeq N' \simeq G_1 \quad \text{and} \quad M \simeq M' \simeq G_2.$$

再來對於所有 $x \in G$, 我們得 $\phi(x) \in G_1 \times G_2$, 但因 $G_1 \times G_2 = N' \cdot M'$, 故知 $\phi(x) = N' \cdot M'$. 也就是說存在 $n' \in N'$ 和 $m' \in M'$ 使得 $\phi(x) = n' \cdot m'$. 但因 ϕ 是 onto 的故存在 $n \in N$ 和 $m \in M$ 使得 $\phi(n) = n'$ 且 $\phi(m) = m'$. 換句話說:

$$\phi(x) = \phi(n) \cdot \phi(m) = \phi(n \cdot m).$$

然而 ϕ 是一對一的故上式得 $x = n \cdot m$. 我們得 G 中的任一元素都可寫成 $n \cdot m$ 這種形式, 其中 $n \in N$, $m \in M$. 換句話說

$$G = N \cdot M.$$

最後, 若 $x \in N \cap M$, 則由 $x \in N$ 得 $\phi(x) \in N'$, 再由 $x \in M$ 得 $\phi(x) \in M'$. 也就是 $\phi(x) \in N' \cap M'$. 然而已知 $N' \cap M'$ 是 $G_1 \times G_2$ 的 identity, 故知 $x \in \ker(\phi)$. 再由 $\ker(\phi) = \{e\}$ 知 $x = e$. 故得證

$$N \cap M = \{e\}.$$

反知若 G 中存在兩個 normal subgroup N 和 M 滿足 (1), (2), (3). 考慮函數 $\psi : G \to N \times M$ 定義成: 若 $x = n \cdot m \in G$, 其中 $n \in N$ 和 $m \in M$, 則 $\psi(x) = (n, m)$. 這裡要注意 ψ 是否為 well-defined function? G 中的任一元素由於 $G = N \cdot M$, 確實可以寫成 $n \cdot m$ 這種形式, 不過寫法唯一嗎? 萬一不唯一, 即 $x = n \cdot m = n' \cdot m'$,

其中 $n \neq n'$ 或 $m \neq m'$, 則 $\psi(x) = (n, m)$ 又等於 (n', m') 表示 ψ 是一對多, 那就不是好函數了. 事實上這種寫法是唯一的: 這是因為若 $n \cdot m = n' \cdot m'$ 其中 $n, n' \in N$, $m, m' \in M$. 則

$$n'^{-1} \cdot n = m' \cdot m^{-1}.$$

然而 $n'^{-1} \cdot n \in N$ 且 $m' \cdot m^{-1} \in M$, 故知

$$n'^{-1} \cdot n \in N \cap M.$$

再利用假設 $N \cap M = \{e\}$ 知 $n'^{-1} \cdot n = e$, 也就是說 $n = n'$. 同理可得 $m = m'$. 所以寫法唯一. 好了! 既然 ψ 是一個好函數, 我們接下來證 ψ 是一個 group homomorphism. 也就是若 $x = n \cdot m$, $x' = n' \cdot m'$ 其中 $n, n' \in N$ 且 $m, m' \in M$, 則要證明 $\psi(x \cdot x') = \psi(x) \cdot \psi(x')$. 不過

$$\psi(x) \cdot \psi(x') = (n, m) \cdot (n', m') = (n \cdot n', m \cdot m'),$$

如果我們能證明 $x \cdot x' = (n \cdot n') \cdot (m \cdot m')$, 則由於 $n \cdot n' \in N$ 且 $m \cdot m' \in M$, 故利用 ψ 的定義我們有

$$\psi(x \cdot x') = (n \cdot n', m \cdot m').$$

因此得 $\psi(x \cdot x') = \psi(x) \cdot \psi(x')$. 換句話說要證明 ψ 是一個 group homomorphism 等於要證

$$(n \cdot m) \cdot (n' \cdot m') = (n \cdot n') \cdot (m \cdot m').$$

利用結合率

$$(n \cdot m) \cdot (n' \cdot m') = n \cdot (m \cdot n') \cdot m'$$

且

$$(n \cdot n') \cdot (m \cdot m') = n \cdot (n' \cdot m) \cdot m',$$

也就是說我們只要證明 $m \cdot n' = n' \cdot m$ 就可. 要怎麼證 $m \cdot n' = n' \cdot m$ 呢? 我們知 $a = b$ 若且為若 $a \cdot b^{-1} = e$. 所以我們考慮

$$(m \cdot n') \cdot (n' \cdot m)^{-1} = m \cdot n' \cdot m^{-1} \cdot n'^{-1}.$$

然而 $m \cdot n' \cdot m^{-1} \in N$ (這是因為 $n' \in N$ 且 N 是 G 的 normal subgroup), 我們有

$$m \cdot n' \cdot m^{-1} \cdot n'^{-1} = (m \cdot n' \cdot m^{-1}) \cdot n'^{-1} \in N.$$

同理利用 M 是 G 的 normal subgroup, 我們有

$$m \cdot n' \cdot m^{-1} \cdot n'^{-1} = m \cdot (n' \cdot m^{-1} \cdot n'^{-1}) \in M.$$

因此知

$$(m \cdot n') \cdot (n' \cdot m)^{-1} \in N \cap M.$$

再利用 $N \cap M = \{e\}$ 得 $(m \cdot n') \cdot (n' \cdot m)^{-1} = e$, 也就是說 $m \cdot n' = n' \cdot m$. 最後我們證 ψ 是 1-1 and onto. 若 $x \in \ker(\psi)$, 也就是說 $\psi(x)$ 是 $N \times M$ 中的 identity (e, e) (別忘了 e 是 G 的 identity 所以當然是 N 和 M 的 identity). 因 $x \in G$ 故存在 $n \in N$, $m \in M$ 使得 $x = n \cdot m$. 由此得 $\psi(x) = (n, m) = (e, e)$. 也就是說 $n = e$ 且 $m = e$, 故 $x = e \cdot e = e$. 得證 $\ker(\psi) = \{e\}$ 故 ψ 是一對一. 要證明 ψ 是

onto, 我們必須任取 $N \times M$ 中的任一元素 (n, m), 然後說 G 中存在一元素 x 使得 $\psi(x) = (n, m)$. 我們只要令 $x = n \cdot m$ 即可, 因為由定義此時 $\psi(x) = (n, m)$. 好了我們證得 ψ 是一個 isomorphism 故

$$G \simeq N \times M.$$

不過我們不是該證 $G \simeq G_1 \times G_2$ 嗎? 沒關係, 因為由假設 $N \simeq G_1$ 且 $M \simeq G_2$, 利用下一個 Lemma, 我們就可知

$$G \simeq N \times M \simeq G_1 \times G_2.$$

□

Lemma 3.2.5. 若 $G_1 \simeq G_1'$ 且 $G_2 \simeq G_2'$ 則

$$G_1 \times G_2 \simeq G_1' \times G_2'.$$

Proof. 由假設我們之存在 isomorphisms: $\phi_1 : G_1 \to G_1'$, 且 $\phi_2 : G_2 \to G_2'$. 定義新的函數 $\phi : G_1 \times G_2 \to G_1' \times G_2'$, 使得對所有的 $(g_1, g_2) \in G_1 \times G_2$,

$$\phi((g_1, g_2)) = (\phi_1(g_1), \phi_2(g_2)).$$

因為 $\phi_1(g_1) \in G_1'$, $\phi_2(g_2) \in G_2'$, ϕ 真的把 $G_1 \times G_2$ 的元素送到 $G_1' \times G_2'$. 利用 ϕ_1 和 ϕ_2 是 group homomorphism, 我們很容易驗證 ϕ 也是一個 group homomorphism.

ϕ 是 onto 的嗎? 若 $(y_1, y_2) \in G_1' \times G_2'$, 即 $y_1 \in G_1'$ 且 $y_2 \in G_2'$, 則因 ϕ_1 和 ϕ_2 是 onto, 故存在 $x_1 \in G_1$ 且 $x_2 \in G_2$ 使得 $\phi_1(x_1) = y_1$ 且 $\phi_2(x_2) = y_2$. 故選 $(x_1, x_2) \in G_1 \times G_2$, 則

$$\phi((x_1, x_2)) = (\phi_1(x_1), \phi_2(x_2)) = (y_1, y_2).$$

所以 ϕ 是 onto.

什麼是 $\ker(\phi)$ 呢? 若 $(a, b) \in \ker(\phi)$, 因 $G_1' \times G_2'$ 的 identity 是 (e_1', e_2'), 其中 e_1' 和 e_2' 分別是 G_1' 和 G_2' 的 identity, 故得

$$\phi((a, b)) = (\phi_1(a), \phi_2(b)) = (e_1', e_2').$$

由此知 $\phi_1(a) = e_1'$ 且 $\phi_2(b) = e_2'$. 換句話說 $a \in \ker(\phi_1)$ 且 $b \in \ker(\phi_2)$. 然而 ϕ_1 和 ϕ_2 由假設都是一對一的, 故 $\ker(\phi_1) = \{e_1\}$ 且 $\ker(\phi_2) = \{e_2\}$, 其中 e_1 和 e_2 分別是 G_1 和 G_2 的 identity. 故得 $a = e_1$, $b = e_2$, 換句話說 $\ker(\phi)$ 是 $G_1 \times G_2$ 的 identity, 故由 Lemma 2.5.6 知 ϕ 是一對一的. 因而得證 ϕ 是一個 isomorphism, 即

$$G_1 \times G_2 \simeq G_1' \times G_2'.$$

□

我們已了解兩個 group 的 direct product 相關的性質, 其實兩個 groups G_1 和 G_2 的 direct product $G_1 \times G_2$ 仍是一個 group 所以還可以和第三個 group G_3 作 direct product 得 $(G_1 \times G_2) \times G_3$. 這樣一直推演下去, 可以得到任意 n 個 groups 的 direct product.

3.3. Finite Abelian Groups

這一節我們討論另一種簡單的 groups, abelian groups. 回憶一下所謂 G 是一個 abelian group 表示 G 中的任意兩元素 a 和 b 都滿足 $a \cdot b = b \cdot a$.

3.3.1. Cauchy and Sylow's Theorems for finite abelian groups. G 是abelain 最好的地方是 G 的任意的 subgroup 都是 normal. 所以很多有關 abelian groups 的性質我們都可以在 G 中找到一個 subgroup 然後再做 quotient group 這樣新的 group 的 order 變小了, 我們就可以用數學歸納法.

要用這種取 quotient group 的數學歸納法一般來說會牽扯上 Correspondence 定理 (忘記這是什麼的同學趕快退回去看一下 Corollary 2.7.3), 另外就是考慮 $\mathrm{ord}(a)$ 和 $\mathrm{ord}(\overline{a})$ 的關係了. 下一個 Lemma 就是告訴我們這個關係, 要注意的是這個 Lemma 並不需要 abelian 的假設:

Lemma 3.3.1. *若 N 是 group G 的一個 normal subgroup, $a \in G$. 考慮 $\overline{a} \in G/N$,* 則

$$\mathrm{ord}(\overline{a}) \,|\, \mathrm{ord}(a).$$

而且 $\mathrm{ord}(\overline{a}) = \mathrm{ord}(a)$ 若且為若

$$N \cap \langle a \rangle = \{e\}.$$

Proof. 假設 $\mathrm{ord}(a) = n$. 則因 $a^n = e$ 得 $\overline{a}^n = \overline{a^n} = \overline{e}$, 故由 Lemma 2.3.2 知 $ord(\overline{a}) \,|\, n$.

假設 $\mathrm{ord}(\overline{a}) = m$. 今若 $N \cap \langle a \rangle = \{e\}$, 則因 $\overline{a}^m = \overline{e}$ 表示 $a^m \in N$, 所以得 $a^m \in N \cap \langle a \rangle = \{e\}$. 換句話說 $a^m = e$, 再由 Lemma 2.3.2 得 $\mathrm{ord}(a) = n \,|\, m$. 然而前已知 $m \,|\, n$, 所以 $n = m$: 也就是說如果 $N \cap \langle a \rangle = \{e\}$, 則 $\mathrm{ord}(\overline{a}) = \mathrm{ord}(a)$.

反之, 假設 $\mathrm{ord}(\overline{a}) = \mathrm{ord}(a)$. 若 $x \in N \cap \langle a \rangle$, 由 $x \in \langle a \rangle$ 知: 存在一整數 i 使得 $x = a^i$. 不過又由 $x \in N$, 知 $\overline{a}^i = \overline{x} = \overline{e}$. 由此知 $\mathrm{ord}(\overline{a}) \,|\, i$. 然而由假設 $\mathrm{ord}(\overline{a}) = \mathrm{ord}(a)$ 得 $\mathrm{ord}(a) \,|\, i$, 因此得證 $x = a^i = e$. 也就是說若 $\mathrm{ord}(\overline{a}) = \mathrm{ord}(a)$ 則 $N \cap \langle a \rangle = \{e\}$. □

以下就是利用數學歸納法來證明一些 abelian groups 的性質的例子:

Theorem 3.3.2 (Cauchy's Theorem for Abelian Groups)**.** *若 G 是一個 finite abelian group, p 是一個質數, 且 p 整除 G 的 order,* 則 *G 中存在一個元素其 order 為 p.*

Proof. 前面提過我們要用 induction 來證明此定理. 如何用 induction 呢? 我們將對所有的 finite abelian group 的 order 作 induction. 也就是我們將證明這個定理對 order 為 p 的 abelian group 是對的. 然後利用歸納法假設對 order 小於 pk 的 abelian group 也對, 來證出對於 order 為 pk 的 abelian group 也對.

假設 G 的 order 為 p, 由 Corollary 2.2.3 知 G 是一個 cyclic group, 所以若 $a \in G$ 使得 $G = \langle a \rangle$, 則 $\mathrm{ord}(a) = p$.

現在假設對於所有的 abelian group G' 如果 $|G'| = pr$ 且 $r < k$, 則存在 $a \in G'$ 使得 $\text{ord}(a) = p$. 若 $|G| = pk$, 則有以下三種狀況:

(1) G 中無 nontrivial proper subgroup.

(2) G 中有一 nontrivial proper subgroup H 且 p 整除 $|H|$.

(3) G 中所有的 nontrivial proper subgroup 其 order 都不能被 p 整除.

如果是狀況 1. 則由 Lemma 3.1.2 知 $|G| = p$, 這情形已證過. 如果是狀況 2. 則因 H 是 nontrivial proper subgroup 故 $|H| < |G|$, 而 p 整除 $|H|$ 故 $|H| = pr$, 其中 $r < k$. 故由 induction 的假設之存在 $a \in H \subset G$ 且 $\text{ord}(a) = p$. 所以在這情況也得證. 我們真正得處理的就是狀況 3. 在這情況之下我們任取一個 G 的 nontrivial proper subgroup H, 然後考慮 G/H 這個 quotient group (別忘了在此我們用到 G 是 abelian 故 H 是 normal). 由於 $p \nmid |H|$, 所以 p 整除 $|G/H| = |G|/|H|$. 再加上 G/H 仍是 abelian group 且 $|G/H| < |G|$ 所以我們可以套用 induction 的假設在 G/H 上, 也就是存在 $\overline{a} \in G/H$ 且 $\text{ord}(\overline{a}) = p$. 現在我們利用前面的 Lemma 3.3.1 知 $p \,|\, \text{ord}(a)$; 也就是存在正整數 t 使得 $\text{ord}(a) = pt$. 利用 Proposition 2.3.3 得

$$\text{ord}(a^t) = \frac{pt}{\gcd(pt, t)} = p.$$

得證在 G 中存在一元素 a^t 其 order 為 p. □

這裡要強調這裡我們證的 Cauchy's Theorem 是利用 G 是 abelian 的假設下證明, 雖然這一個證明對 G 不是 abelian 時並不適用, 不過將來我們會用另外的方法證明一般的 Cauchy's Theorem. 也就是說這個定理在 G 不是 abelian 時仍是對的.

我們可以用類似的方法證以下的定理:

Theorem 3.3.3 (Sylow's Theorem for Abelian Groups)**.** *若 G 是一個 finite abelian group, 且 $|G| = p^n m$, 其中 p 是質數且 $p \nmid m$, 則在 G 中存在一個 subgroup P 其 order 為 p^n.*

Proof. 我們用類似前面 Theorem 3.3.2 的 induction. 當 $|G| = pm$ 時, Theorem 3.3.2 告訴我們存在 $a \in G$ 其 order 為 p, 故此時取 $P = \langle a \rangle$ 即可.

現在假設當 $|G'| = p^r m$, $r < n$ 時, 在 G' 中可找到 subgroup P' 其 order 為 p^r. 當 $|G| = p^n m$ 時, 由 Theorem 3.3.2 知存在 G 的 subgroup N 其 order 為 p. 因 G 是 abelian 故 N 是 G 的 normal subgroup, 故考慮 G/N 這一個 quotient group. G/N 的 order 是 $|G|/|N| = p^{n-1}m$. 故由 induction 的假設知在 G/N 中存在一個 subgroup P' 其 order 為 p^{n-1}. 再利用 Correspondence 定理 (Corollary 2.7.3) 知 G 中存在一 subgroup P 使得 $P' = P/N$. 然而 $|P| = |P'| \cdot |N| = p^{n-1} \cdot p = p^n$, 故得證. □

若 p 是一個質數, 而一個 group 的個數是 p^n 這種形式時, 我們稱這種 group 為一個 *p-group*. 當 G 的個數是 $p^n m$, 其中 p 和 m 互質時, 若 G 中的 subgroup H

其 order 又剛好是 p^n, 則稱 H 是 G 的一個 *Sylow p-subgroup*. Theorem 3.3.3 告訴我們當 G 是一個 abelian group 時, 其 Sylow p-subgroup 一定存在. 以後我們也會學到在一般的 group 中 Sylow p-subgroup 也一定存在, 這就是所謂的 Sylow 定理.

3.3.2. 一些 abelian groups 特有的性質. 現在我們來探討一些在一般 groups 不一定對但在 abelian groups 會對的一些性質.

當 G 是 abelian 時, 任取 $a, b \in G$, 因 $a \cdot b = b \cdot a$ 我們可以得

$$(a \cdot b)^2 = (a \cdot b) \cdot (a \cdot b) = a \cdot (b \cdot a) \cdot b = a \cdot (a \cdot b) \cdot b = a^2 \cdot b^2.$$

利用數學歸納法我們很容易知對所有的 $n \in \mathbb{N}$,

$$(a \cdot b)^n = a^n \cdot b^n.$$

以下的 Lemma 告訴我們 G 是 abelian 的另一個好處:

Lemma 3.3.4. *若 G 是一個 finite abelian group, m 是一個大於 1 的整數且 m 整除 G 的 order. 考慮集合 $M = \{g \in G \,|\, g^m = e\}$. 則 M 是 G 的一個 subgroup 且 $M \neq \{e\}$.*

Proof. 因 $m > 1$ 故必存在一質數 p 使得 $p \,|\, m$. 由 Theorem 3.3.2 知存在一元素 $a \in G$ 其 order 為 p. 故知 $a \neq e$ 且 $a^p = e$, 但 $p \,|\, m$ 故 $a^m = e$. 也就是 $a \in M$ 故 $M \neq \{e\}$.

現在證 M 是 G 的 subgroup. 首先證封閉性: 若 $a, b \in M$, 即 $a^m = e$, $b^m = e$. 故 $(a \cdot b)^m = a^m \cdot b^m = e$, 也就是說 $a \cdot b \in M$. 接下來證反元素存在: 若 $a \in M$, 因 $a^m = e$ 故 $(a^m)^{-1} \cdot a^m = (a^m)^{-1} = (a^{-1})^m$. 然而又 $(a^m)^{-1} \cdot a^m = e$, 故 $(a^{-1})^m = e$. 也就是說 $a^{-1} \in M$. □

別忘了因 G 是 abelian 所以 M 會是 G 的一個 normal subgroup, 利用這一點我們可以得到以下有關 finite abelian group 非常重要的性質.

Lemma 3.3.5. *設 G 是一個 finite abelian group, 且 $|G| = p^n m$, 其中 $p \nmid m$. 令*

$$P = \{g \in G \,|\, g^{p^n} = e\} \quad \text{and} \quad M = \{g \in G \,|\, g^m = e\},$$

則

$$G \simeq P \times M.$$

Proof. 由 Lemma 3.3.4 知 P 和 M 都是 G 的 normal subgroups. 要證明 $G \simeq P \times M$, 我們得利用 Theorem 3.2.4 證明 $G = P \cdot M$ 及 $P \cap M = \{e\}$ 就好. 這兩個性質都要用到 p^n 和 m 互質來得到.

因為 p^n 和 m 互質, 故存在整數 r 和 s 使得 $rp^n + sm = 1$. 因此對任意的 $a \in G$, 我們都可寫成

$$a = a^{rp^n + sm} = a^{sm} \cdot a^{rp^n}.$$

因為

$$((a^{sm})^{p^n} = (a^{p^n m})^s,$$

而 $|G| = p^n m$, 由 Corollary 2.3.4 知

$$(a^{sm})^{p^n} = e;$$

也就是說 $a^{sm} \in P$. 同理知 $a^{rp^n} \in M$. 由此知任意的 G 中元素都可寫成一個 P 中的元素乘以 M 中的元素, 所以 $G = P \cdot M$.

另一方面, 若 $g \in P \cap M$, 因 $g \in M$, 故 $g^m = e$. 則由 Lemma 2.3.2 知 $\mathrm{ord}(g) \,|\, m$. 同理得 $\mathrm{ord}(g) \,|\, p^n$. 也就是說 $\mathrm{ord}(g)$ 整除 g^n 和 m 的最大公因數. 但 g^n 和 m 互質, 故得 $\mathrm{ord}(g) = 1$; 也就是說 $g = e$. 因此得證 $P \cap M = \{e\}$. □

Lemma 3.3.5 中 P 元素的個數是多少呢? 雖然是收集所有 G 中元素 g 符合 $g^{p^n} = e$ 的元素但不表示其 order 就是 p^n. 不過很巧妙的利用 Cauchy 的定理我們確實可以得到 $|P| = p^n$.

Lemma 3.3.6. 設 G 是一個 *finite abelian group,* 且 $|G| = p^n m$, 其中 $p \nmid m$. 令

$$P = \{g \in G \,|\, g^{p^n} = e\},$$

則 P 是 G 的一個 *Sylow p-subgroup,* 而且 P 是 G 中唯一的 *Sylow p-subgroup.*

Proof. 首先我們說明若令 $M = \{g \in G \,|\, g^m = e\}$, 則 p 不能整除 M 的 order. 這是因為若 p 整除 M 的 order, 則由 Cauchy's Theorem 知 M 中存在一元素 a 其 order 為 p, 但 $a^m = e$, 由 Lemma 2.3.2 知 $p \,|\, m$. 這和假設 $p \nmid m$ 矛盾. 故 p 不能整除 $|M|$.

接下來我們證 P 是一個 p-group. 假設除了 p 以外存在另一質數 q 整除 $|P|$, 則用和前面相同的方法可得 $q \,|\, p^n$, 這又和 p, q 是相異質數矛盾. 換句話說 $|P|$ 除了 p 以外不會有其他的質因數, 所以知存在 $r \in \mathbb{N}$ 使得 $|P| = p^r$.

由 Lemma 3.3.5 知 $G \simeq P \times M$, 故 $|G| = |P| \cdot |M|$. 因此得

$$|M| = |G|/|P| = p^{n-r} m.$$

但 p 不整除 M, 故得 $n = r$. 也就是說 P 是 G 的一個 Sylow p-subgroup.

最後假設 P' 是 G 中任意的一個 Sylow p-subgroup. 因 $|P'| = p^n$, 由 Lagrange 定理(Corollary 2.3.4) 知對於所有 $a \in P'$, $a^{p^n} = e$. 也就是說 $a \in P$. 得證 $P' \subseteq P$. 然而 $|P'| = |P| = p^n$, 故 $P' = P$. 這證明了唯一性. □

這一次我們要強調 Lemma 3.3.6 是 abelian groups 特有的性質. 它告訴我們此時 Sylow p-subgroup 是長什麼樣子的, 而且是唯一的. 在一般的 group 這不一定是對的.

綜合以上幾個 Lemmas, 我們有以下的結論:

Proposition 3.3.7. 設 G 是一個 *finite abelian group,* 其 *order* 為

$$|G| = p_1^{n_1} \cdots p_r^{n_r},$$

其中 $p_1, \ldots, p_r$ 是相異的質數. 令 P_i 是 G 中對每一個 p_i 所對應的 *Sylow* p_i*-subgroup,* $i \in \{1, \ldots, r\}$. 則

$$G \simeq P_1 \times \cdots \times P_r.$$

Proof. 若令 $m = p_2^{n_2} \cdots p_r^{n_r}$, 且令 $M = \{g \in G \mid g^m = e\}$, 則由 Lemmas 3.3.5, 3.3.6 知 $G \simeq P_1 \times M$. 然而因 $|M| = p_2^{n_2} \cdots p_r^{n_r}$ 故由數學歸納法可知 $M \simeq P_2 \times \cdots \times P_n$. 因此由 Lemma 3.2.5 得

$$G \simeq P_1 \times M \simeq P_1 \times P_2 \times \cdots \times P_r.$$

□

3.3.3. Abelian p-groups. Proposition 3.3.7 告訴我們一個 finite abelian group 可以寫成一些 p-subgroups 的 direct product, 這些 p-subgroup 當然都還是 abelian. 因此若我們能了解 abelian p-groups, 則對於一般的 finite abelian groups 就完全清楚了.

大家都知道 cyclic group 一定是 abelian. 不過若只知一個 group 是 abelian 它並不一定會是 cyclic. 下一個 Lemma 告訴我們一個判斷 abelian group 是否為 cyclic 的方法.

Lemma 3.3.8. 若 G 是一個 *abelian p-group,* 且 $a \in G$ 是 G 中任一個 *order* 最大的元素. 則*:*

(1) 若 G 是 *cyclic* 則 $G = \langle a \rangle$.

(2) 若 G 不是 *cyclic* 則在 G 中存在 $b \notin \langle a \rangle$, 使得 $\mathrm{ord}(b) = p$.

Proof. 若 $|G| = p^n$, 由 Lagrange 定理 (Corollary 2.3.4) 知 $\mathrm{ord}(a) = p^r$, 其中 r 是一個正整數且 $r \leq n$.

(1) 若 G 是 cyclic, 即 G 中存在一元素 x 使得 $G = \langle x \rangle$. 也就是說 $\mathrm{ord}(x) = p^n$. 然而已知 a 是 G 中元素 order 最大的之一. 所以知 $\mathrm{ord}(a) = p^n$ (注意這個元素並不唯一, 所以我們並不可得 $x = a$). 換句話說 G 和 $\langle a \rangle$ 的元素個數一樣多, 即 $G = \langle a \rangle$.

(2) 若 G 不是 cyclic, 則當然 $\langle a \rangle \subsetneq G$. 記 $A = \langle a \rangle$. 可知 quotient group G/A 仍是一個 abelian p-group, 即 $|G/A| = p^{n-r}$. 利用 Cauchy 定理 (Theorem 3.3.2) 知存在 $\overline{x} \in G/A$ 使得 $\mathrm{ord}(\overline{x}) = p$. 也就是說 $\overline{x} \neq \overline{e}$ 不過 $\overline{x}^p = \overline{e}$, 因此 $x \notin A$ 但 $x^p \in A$. 因為 $A = \langle a \rangle$, $x^p \in A$ 表示存在一整數 i 使得 $x^p = a^i$. 我們用反證法證明 $p \mid i$.

如果 $p \nmid i$, 則由 Proposition 2.3.3 知

$$\mathrm{ord}(a^i) = \frac{p^r}{\gcd(p^r, i)} = p^r.$$

也就是說 $\mathrm{ord}(x^p) = \mathrm{ord}(a) = p^r$. 別忘了 $x \in G$, 而 G 是 p-group, 因此如前知 $\mathrm{ord}(x) = p^s$, 其中 s 是一正整數. 再用一次 Proposition 2.3.3 知

$$\mathrm{ord}(x^p) = \frac{p^s}{\gcd(p^s, p)} = p^{s-1}.$$

利用前面所求之 $\mathrm{ord}(x^p) = p^r$ 得 $s = r + 1$. 也就是說 $\mathrm{ord}(x) = p^s = p^{r+1}$. 別忘了當初我們假設 $\mathrm{ord}(a) = p^r$. $\mathrm{ord}(x) > \mathrm{ord}(a)$ 這和 a 的 order 是最大的相矛盾. 所以得證 $p \mid i$.

假設 $i = pt$, 令 $b = a^{-t} \cdot x$. 注意若 $b \in A$, 則因 $x = a^t \cdot b$, 會導致 $x \in A$, 這和 $x \notin A$ 相矛盾, 故知 $b \notin A$, 且當然 $b \neq e$ (因 $e \in A$). 然而因 G 是 abelian, $b^p = a^{-pt} \cdot x^p$. 利用 $pt = i$ 及 $a^i = x^p$, 我們推得 $b^p = e$. 由此可得 $\mathrm{ord}(b) = p$. 這是因為由 Lemma 2.3.2 知 $\mathrm{ord}(b) \mid p$. 但 p 是質數, 所以得 $\mathrm{ord}(b) = 1$ or $\mathrm{ord}(b) = p$. 然而已知 $b \neq e$ 即 $\mathrm{ord}(b) \neq 1$, 故可得 $\mathrm{ord}(b) = p$. □

下一個 Lemma 告訴我們如果一個 abelian p-group 不是 cyclic 那麼它在某種程度上和 cyclic group 還是相差不遠.

Lemma 3.3.9. *若 G 是一個 abelian p-group, 且 $a \in G$ 是 G 中任一個 order 最大的元素. 則要不然 G 是一個 cyclic group; 要不然就是在 G 中存在一個 subgroup Q 使得*

$$G \simeq \langle a \rangle \times Q.$$

Proof. 令 $A = \langle a \rangle$. 若 G 不是 cyclic 則由 Lemma 3.3.8 知存在 $b \in G$ 但 $b \notin A$ 使得 $\mathrm{ord}(b) = p$. 令 $B = \langle b \rangle$. 首先證明 $A \cap B = \{e\}$. 這是因為 $A \cap B$ 會是 B 的一個 subgroup. 利用 Lagrange 定理 (Theorem 2.2.2) 知 $A \cap B$ 的 order 需整除 B 的 order. 但 B 的 order 為質數 p, 故知 $|A \cap B| = 1$ 或 $|A \cap B| = p$. 若 $|A \cap B| = p$, 表示 $A \cap B = B$, 即 $B \subseteq A$. 這和 $b \notin A$ 不合. 因此 $A \cap B$ 的 order 不是 p. 故得 $|A \cap B| = 1$, 即 $A \cap B = \{e\}$.

接下來我們想用 B 來幫我們以數學歸納法證明這個 Lemma. 若 G 的 order 為 p, 由 Corollary 2.2.3 知 G 是一個 cyclic group. 若 $|G| = p^n$. 假設此 Lemma 在所有 order 小於 p^n 的 abelian p-groups 都對.

當然若 G 是 cyclic 則證明完成, 但 G 是有可能不是 cyclic 的. 若 G 不是 cyclic, 考慮 G/B 這一個 abelian group. 因 $|G/B| = p^{n-1}$, 故 G/B 是一個 order 小於 p^n 的 abelian p-group. 此時我們就可以用 induction 的假設, 不過要用這個假設我們得先在 G/B 中找到一個 order 最大的元素. 事實上 $\overline{a}$ 會是 G/B 中 order 最大的元素. 主要原因是由 Lemma 3.3.1 知對所有的 $\overline{x} \in G/B$, 都有 $\mathrm{ord}(\overline{x}) \leq \mathrm{ord}(x)$. 又因 $B \cap \langle a \rangle = \{e\}$ 故再由 Lemma 3.3.1 得 $\mathrm{ord}(\overline{a}) = \mathrm{ord}(a)$. 因為 a 是 G 中 order 最大的元素, 故得在 G/B 中對任意的 $\overline{x} \in G/B$ 皆有

$$\mathrm{ord}(\overline{a}) = \mathrm{ord}(a) \geq \mathrm{ord}(x) \geq \mathrm{ord}(\overline{x}).$$

現在我們可以套用歸納的假設了. 由假設知有可能 G/B 是 cyclic, 要不然在 G/B 中存在一個 subgroup Q' 使得 $G/B \simeq \langle \overline{a} \rangle \times Q'$.

若 G/B 是 cyclic, 由 Lemma 3.3.8 知 $G/B = \langle \overline{a} \rangle$. 此時我們要證明 $G \simeq \langle a \rangle \times B$. 由 Theorem 3.2.4 知這相當於要證明 $G = A \cdot B$ 且 $A \cap B = \{e\}$ (別忘了 A, B 都是 normal). 不過由於我們已證得 $A \cap B = \{e\}$, 所以只要證 $G = A \cdot B$. 對任意的 $x \in G$, 考慮 $\overline{x} \in G/B$. 則由於 $G/B = \langle \overline{a} \rangle$, 故存在一整數 i 使得 $\overline{x} = \overline{a}^i$. 這表示 x 和 a^i 在 B 的分類下是同類的. 也就是 $(a^i)^{-1} \cdot x \in B$. 換句話說存在一整數 j 使得 $x = a^i \cdot b^j$. 得證 G 中的元素都可寫成一個 A 中元素乘上一個 B 中元素的形式, 即 $G = A \cdot B$. 故加上 $A \cap B = \{e\}$ 得 $G \simeq A \times B$.

若 G/B 不是 cyclic 則由 induction 的假設知在 G/B 中存在一個 subgroup Q' 使得 $G/B \simeq \langle \overline{a} \rangle \times Q'$. 利用 Theorem 3.2.4 知此時 $G/B = \langle \overline{a} \rangle \cdot Q'$ 且 $\langle \overline{a} \rangle \cap Q' = \{\overline{e}\}$. 因為我們要把問題拉回到 G 來看, 利用 Correspondence 定理 (Corollary 2.7.3) 知在 G 中存在一個 subgroup Q 符合 $B \subseteq Q$ 且 $Q/B = Q'$. 我們要證明 $G \simeq \langle a \rangle \times Q$.

首先證 $G = A \cdot Q$. 任取 $x \in G$, 由於 $\overline{x} \in G/B$, 且 $G/B = \langle \overline{a} \rangle \cdot Q/B$, 故存在一整數 i 和 $q \in Q$ 使得

$$\overline{x} = \overline{a}^i \cdot \overline{q} = \overline{a^i \cdot q}.$$

也就是說 $(a^i \cdot q)^{-1} \cdot x \in B$. 因 $B = \langle b \rangle$, 由此知存在一整數 j 使得 $(a^i \cdot q)^{-1} \cdot x = b^j$. 換句話說 $x = a^i \cdot (q \cdot b^j)$. 然而 $a^i \in A$, 且 $q \cdot b^j \in Q$ (別忘了 $B \subseteq Q$). 故知 $G = A \cdot Q$.

最後要證 $A \cap Q = \{e\}$. 若 $x \in A \cap Q$, 由 $x \in A = \langle a \rangle$ 知 存在一整數 i 使得 $x = a^i$. 故在 G/B 中 $\overline{x} = \overline{a^i} = \overline{a}^i$. 另一方面 $a \in Q$ 故在 G/B 中 $\overline{x} \in Q/B = Q'$. 也就是說

$$\overline{x} \in \langle \overline{a} \rangle \cap Q' = \{\overline{e}\}.$$

由此知在 G/B 中 $\overline{x} = \overline{e}$, 也就是說 $x \in B$. 但一開始已假設 $x \in A \cap Q$, 當然有 $x \in A$. 所以得 $x \in A \cap B$. 別忘了我們已知 $A \cap B = \{e\}$, 故得 $x = e$. 也就是說 $A \cap Q = \{e\}$. □

Lemma 3.3.9 告訴我們什麼呢? 如果 G 是 abelian p-group, 且 $|G| = p^n$. 則有可能 G 是 cyclic group: 若是如此則由 Theorem 3.1.1 知 $G \simeq \mathbb{Z}/p^n\mathbb{Z}$. G 也有可能不是 cyclic, 那麼 Lemma 3.3.9 就告訴我們若 G 中 order 最大的元素其 order 是 p^{n_1}, 則存在一個 subgroup Q 使得 $G \simeq (\mathbb{Z}/p^{n_1}\mathbb{Z}) \times Q$. 這裡因 G 是 abelian p-group, 其 subgroup Q 當然也是 abelian p-group. 如果 Q 是 cyclic, 那麼我們就可得 $G \simeq (\mathbb{Z}/p^{n_1}\mathbb{Z}) \times Q \simeq (\mathbb{Z}/p^{n_1}\mathbb{Z}) \times (\mathbb{Z}/p^{n_2}\mathbb{Z})$; 如果 Q 不是 cyclic 則再用一次 Lemma 3.3.9 知 Q 會 isomorphic to 一個 cyclic group 和 Q 的 subgroup 的 direct product. 這樣一直下去, 由於 G 的 order 是有限的經過有限次後一定會停. 我們可以有以下的結果:

Proposition 3.3.10. 如果 G 是一個 *abelian p-group,* 且 $|G| = p^n$. 則存在 $n_1, \ldots, n_r \in \mathbb{N}$ 符合 $n_1 + \cdots + n_r = n$ 使得

$$G \simeq (\mathbb{Z}/p^{n_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{n_r}\mathbb{Z}).$$

Proof. 由前面的討論之 G 可以寫成一些 cyclic groups 的 direct product. 這些 cyclic groups 由於都是 G 的 subgroups, 所以也都是 p-group. 因此它們都會是 isomorphic to $\mathbb{Z}/p^{n_i}\mathbb{Z}$ 這種形式, 最後由於

$$p^n = |G| = |\mathbb{Z}/p^{n_1}\mathbb{Z}| \cdots |\mathbb{Z}/p^{n_r}\mathbb{Z}| = p^{n_1} \cdots p^{n_r},$$

我們知 $n = n_1 + \cdots + n_r$. □

3.3.4. Finite abelian groups 的基本定理. 既然每一個 finite abelian group 都可寫成一些 abelian p-groups 的 direct product, 而每一個 abelian p-group 也都可寫成一些 cyclic groups 的 direct product, 因此由這兩個結果我們可以說完整的掌握了 finite abelian groups.

Theorem 3.3.11 (Fundamental Theorem on Finite Abelian Groups)**.** 若 G 是一個 *finite abelian group,* 則 G 可以寫成一些 *cyclic groups* 的 *direct product.*

Proof. 由 Proposition 3.3.7 知 $G \simeq P_1 \times \cdots \times P_r$, 其中 P_i 都是某個質數 p_i 的 abelian p_i-group. 再由 3.3.10 知對所有的 P_i, 都可找到 cyclic groups $C_{i1}, \ldots C_{in_i}$ 使得 $P_i \simeq C_{i1} \times \cdots \times C_{in_i}$. 因此得證本定理. □

這裡很有趣的是我們都知道所有的 cyclic groups 長什麼樣子, 既然 finite abelian groups 都是 cyclic groups 的 direct product, 我們當然就知道所有的 finite abelian groups 長什麼樣子了. 比方說若 G 是一個 abelian group 且 $|G| = 6$, 那麼 G 有可能長什麼樣子呢? 由 Proposition 3.3.7 知 $G \simeq P_1 \times P_2$ 其中 P_1 的 order 是 2, P_2 的 order 是 3. 而 order 是 2 的 group 一定是 cyclic (Corollary 2.2.3) 故 $P_1 \simeq \mathbb{Z}/2\mathbb{Z}$. 同理 $P_2 \simeq \mathbb{Z}/3\mathbb{Z}$. 故 $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. 不過由 3.2.2 知 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$, 所以 $G \simeq \mathbb{Z}/6\mathbb{Z}$. 也就是所有的元素個數為 6 的 abelian group 都是 cyclic group. 相信大家不難利用這個例子推廣到以下的 Corollary:

Corollary 3.3.12. 若 G 是一個 *abelian group* 且 $|G| = p_1 \cdots p_r$ 其中 $p_1, \ldots p_r$ 是相異的質數, 則 G 是一個 *cyclic group.*

至於若 G 的 order 的質因數分解中存在高次方的話, 那麼問題就複雜一點了. 例如考慮 order 為 144 的 abelian group G. 因 $144 = 2^4 \cdot 3^2$, 由 Proposition 3.3.7 知 $G \simeq P_1 \times P_2$ 其中 P_1 的 order 是 2^4, P_2 的 order 是 3^2. 再由 Proposition 3.3.10 計算

$$4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$$

知 P_1 有可能是 isomorphic to

$$(1)\ \mathbb{Z}/16\mathbb{Z} \quad \text{or} \quad (2)\ \mathbb{Z}/8\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \quad \text{or} \quad (3)\ \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z},$$

$$(4)\ \mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \quad \text{or} \quad (5)\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},$$

這五種情況. 同理 P_3 可能 isomorphic to

$$(1)\ \mathbb{Z}/9\mathbb{Z} \quad \text{or} \quad (2)\ \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$$

這兩種情況. 因此元素個數為 144 的 abelian groups 共有十種可能.

3.4. The Symmetric Group

這一節我們將討論一個複雜但重要的 group 稱之為 symmetric group.

3.4.1. The group $A(S)$ and Cayley's Theorem. 給定一集合 S 我們定義 $A(S)$ 是所有從 S 到 S 的 1-1 且 onto 的函數所成的集合. 若 $f, g \in A(S)$ 那麼它們的合成函數 $f\circ g$ 依然是 1-1 且 onto, 所以知 $f\circ g \in A(S)$. 因此我們就考慮合成 $\circ$ 為 $A(S)$ 中的運算. 前面已知這個運算有封閉性, 相信大家也知合成運算有結合率. 至於在這個運算之下 $A(S)$ 的 identity 是什麼呢? 當然就是所謂的 identity function I_S 了: I_S 是一個從 S 到 S 的函數它符合 $I_S(x) = x, \forall\, x \in S$. 而對任意的 $f \in A(S)$ 由 1-1 和 onto 的性質知存在 $g \in A(S)$ 使得 $f\circ g = g\circ f = I_S$ (即 g 是 f 的反函數), 所以知任何 $A(S)$ 的元素其 inverse 存在. 我們說明了 $A(S)$ 是一個 group. 下一個定理告訴我們為何 $A(S)$ 這一個 group 這麼重要.

Theorem 3.4.1 (Cayley's Theorem)**.** 給定任一個 *group* G, 則 G 會 *isomorphic to* $A(G)$ 的一個 *subgroup.*

Proof. 這裡我們先強調在 $A(G)$ 中我們僅將 G 視為一個集合, 所以 $A(G)$ 是從 G 到 G 的 1-1 和 onto 的函數所成的集合而不是 group homomorphism 所成的集合.

我們現在想定一個從 G 這一個 group 到 $A(G)$ 這一個 group 的 group homomorphism $\phi : G \to A(G)$. 對任意的 $a \in G$, 我們定義 $\phi(a) \in A(S)$ 這一個函數為 $T_a : G \to G$, 其中對於任意的 $x \in G$, $T_a(x) = a\cdot x$.

我們當然要檢查 ϕ 是不是一個 well-defined function. 這裡唯一要檢查的就是: 是否 $\phi(a) = T_a \in A(S)$? 由定義當然知道 T_a 是一個從 G 送到 G 的函數. 所以我們只要檢查是否 T_a 是一個 1-1 且 onto 的函數. 這裡千萬不要搞錯了, T_a 只是一個函數所以要證它是一對一的不能看 kernel (事實上 $\ker(T_a)$ 是無定義的). 給定任意的 $b \in G$, 要證明 T_a 是 1-1 且 onto 就是要證明 G 中存在唯一的元素 c 使得 $T_a(c) = b$. 然而 $T_a(x) = a\cdot x$, 故由 Theorem 1.2.3 知 T_a 是 1-1 且 onto.

接下來我們證明 $\phi : a \mapsto T_a$ 是一個從 G 到 $A(G)$ 的 group homomorphism. 也就是證對所有的 $a, b \in G$, $\phi(a\cdot b) = \phi(a)\circ\phi(b)$ (別忘了 $\phi(a)$ 和 $\phi(b)$ 是在 $A(G)$ 中所以它們間的乘法是 $\phi(a)\circ\phi(b)$). 要檢查 $\phi(a\cdot b)$ 和 $\phi(a)\circ\phi(b)$ 這兩個函數是否相

同, 就是要檢驗這兩個函數對定義域裡的每個元素取值是否相同. 因 $\phi(a\cdot b)=T_{a\cdot b}$ 故對所有的 $x\in G$, 皆有

$$T_{a\cdot b}(x)=(a\cdot b)\cdot x.$$

而 $\phi(a)\circ\phi(b)=T_a\circ T_b$, 故對所有的 $x\in G$, 皆有

$$T_a\circ T_b(x)=T_a(T_b(x))=T_a(b\cdot x)=a\cdot(b\cdot x).$$

因此由 G 的結合率知對所有的 $x\in G$, $T_{a\cdot b}(x)=T_a\circ T_b(x)$. 也就是說 $\phi(a\cdot b)=\phi(a)\circ\phi(b)$.

最後證 ϕ 是一對一的. 已證 ϕ 是 group homomorphism, 所以只要證 $\ker(\phi)=\{e\}$. 若 $a\in\ker(\phi)$, 即 $\phi(a)$ 為 $A(G)$ 的 identity I_G. 換句話說, 對所有的 $x\in G$ 皆有 $T_a(x)=x$. 但 $T_a(x)=a\cdot x$, 故得 $a=e$. 因此我們證得了 $G\simeq\mathrm{im}(\phi)$. 利用 Lemma 2.5.4 知 $\mathrm{im}(\phi)$ 是 $A(G)$ 的一個 subgroup, 故得證此定理. □

Cayley's Theorem 是想將抽象的 group 用具體的方法表示出來. 或許大家會疑惑: 原本 G 都不知是什麼樣子了, 用 $A(G)$ 來表示能告訴我們什麼訊息呢? 仔細想想 $A(G)$ 的結構, 它和 G 的 group 性質無關, 事實上只和 G 的個數有關. 換句話說當我們要了解有多少 order 為 n 的 group 時, 只要任選一個元素個數為 n 的集合 S, 再討論 $A(S)$ 中有多少個 order 為 n 的 subgroup 就好了 (因為 Cayley's Theorem 告訴我們所有的 order 為 n 的 group 必在其中). 可惜 $A(S)$ 這一個 group 經常是太大了. 有時是可以考慮小一點的集合 S', 不過這裡我們就不多做討論.

3.4.2. The symmetric group of degree n. 前面提過 $A(S)$ 這一個 group 只和 S 的元素個數有關. 今若 S 有 n 個元素, 那麼我們不妨考慮 $S=\{1,2,\ldots,n\}$ 這一個集合. 此時我們將 $A(S)$ 也就是從 $\{1,2,\ldots,n\}$ 到 $\{1,2,\ldots,n\}$ 所有 1-1 且 onto 的函數所成的集合特別記做 S_n, 稱之為 the *symmetric group of degree* n. Cayley's Theorem 告訴我們所有 order 為 n 的 group 都會 isomorphic 到 S_n 的某一個 subgroup, 所以研究 S_n 顯得特別重要.

從 $\{1,2,\ldots,n\}$ 到 $\{1,2,\ldots,n\}$ 所有 1-1 且 onto 的函數到底有多少個呢? 相信大家在高中都已學過了. 先考慮 1 可以送到什麼? 結果有 n 種選擇, 不過因 1 已選擇去哪個數了, 因要求一對一, 2 只剩下 $n-1$ 個選擇. 由此繼續下去我們得知 S_n 的 order.

Lemma 3.4.2.

$$|S_n|=n\cdot(n-1)\cdots2\cdot1=n!.$$

一般談 S_n 我們是不談 $n=1$ 和 $n=2$ 的狀況: 因 S_1 只有一個元素, 所以只有 identity. 而 S_2 只有 2 個元素, 一定是 cyclic. 所以我們以後只談 $n\geq3$ 的狀況.

要討論 S_n 我們當然要想個法子將其元素表示出來. 例如在 S_5 中若 σ 是將 $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$, $4 \mapsto 5$ 及 $5 \mapsto 4$, 則我們可以用

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \tag{3.1}$$

來表示. 而

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} \tag{3.2}$$

表示 τ 將 $1 \mapsto 3$, $2 \mapsto 4$, $3 \mapsto 5$, $4 \mapsto 1$ 且 $5 \mapsto 2$. 那麼 $\sigma \circ \tau$ 是甚麼呢? 因為 τ 將 $1 \mapsto 3$, 而 σ 將 $3 \mapsto 1$ 所以合成起來得 $\sigma \circ \tau$ 將 $1 \mapsto 1$. 而 τ 將 $2 \mapsto 4$, σ 將 $4 \mapsto 5$ 故 $\sigma \circ \tau$ 將 $2 \mapsto 5$. 同理一個一個計算下去我們可得

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 2 & 3 \end{pmatrix} \tag{3.3}$$

同理考慮 $\tau \circ \sigma$ 可得

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 & 1 \end{pmatrix} \tag{3.4}$$

由式子 (3.3) 和 (3.4) 知 $\sigma \circ \tau \neq \tau \circ \sigma$ 所以 S_5 不是 abelian. 事實上對於所有的 $n \geq 3$, S_n 都不是 abelian.

當 $\sigma, \tau \in S_n$, 由於 σ, τ 都是函數, 其乘法就是函數的合成. 為了方便起見以後我們不再用 $\sigma \circ \tau$ 表示其合成而用 $\sigma \cdot \tau$ 取代.

3.4.3. Disjoint cycle decomposition. 用如式子 (3.1) 的方法表示 S_n 的元素有時稍嫌麻煩. 我們介紹一個簡便的表示法. 這個方法稱為 cycle 表示法. 它不只使用簡便, 而且許多 S_n 的性質都可利用這方法簡單求得. 可以說是相當的重要.

Definition 3.4.3. 令 $i_1, i_2 \ldots, i_k$ 是在 $\{1, 2, \ldots, n\}$ 中 k 個相異整數. 我們用

$$(i_1\ i_2\ \cdots\ i_k)$$

表示 S_n 中的一個元素 σ 將 $s \in \{1, 2, \ldots, n\}$ 送到

$$\sigma(s) = \begin{cases} i_{j+1}, & \text{若 } s = i_j \text{ 且 } 1 \leq j \leq k-1; \\ i_1, & \text{若 } s = i_k; \\ s, & \text{若 } s \notin \{i_1, \ldots, i_k\}. \end{cases}$$

換句話說 σ 將 $i_1 \mapsto i_2$, $i_2 \mapsto i_3$, $\ldots$, $i_{k-1} \mapsto i_k$, 而將 i_k 送回 i_1, 而將 $i_1, \ldots, i_k$ 以外的元素原封不動.

我們稱 $(i_1\ i_2\ \cdots\ i_k)$ 是一個 k-cycle.

例如在 S_5 中我們有以下的等式:

$$(1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$

一個 cycle 是 S_n 中的元素, 反之任一 S_n 中的元素未必是一個 cycle. 不過它們都可寫成一些 cycle 的乘積 (別忘了這裡指的是合成). 我們就用式子 (3.1) 當例子

來將 σ 用 cycle 表示出來. 因 σ 將 $1 \mapsto 2$ 所以我們先寫下

$$(1\ 2$$

接著 σ 將 $2 \mapsto 3$ 所以繼續寫下

$$(1\ 2\ 3$$

然後 σ 將 $3 \mapsto 1$ 所以我們寫下

$$(1\ 2\ 3)$$

用 ")" 將 3 框住表示 σ 將 3 送回 1. 這樣我們寫下了一個 3-cycle. 不過這 (1 2 3) 並不是 σ, 別忘了 σ 還將 $4 \mapsto 5$ 及 $5 \mapsto 4$. 所以需補上 (4 5) 這一個 cycle. 因此我們將式子 (3.1) 表成

$$\sigma = (4\ 5)(1\ 2\ 3).$$

這裡其實我們是將 (1 2 3) 看成是 S_5 中的

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$

這一個元素, 而

$$(4\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$

所以將之相乘得 σ. 同法式子 (3.2) 中的 τ 將 $1 \mapsto 3$, 故先寫下

$$(1\ 3$$

接著 τ 將 $3 \mapsto 5$ 所以繼續寫下

$$(1\ 3\ 5$$

而後 τ 將 $5 \mapsto 2$, 故寫

$$(1\ 3\ 5\ 2$$

接著 τ 將 $2 \mapsto 4$, 所以寫下

$$(1\ 3\ 5\ 2\ 4$$

最後 τ 將 4 送回 1 故補上 ")" 得

$$\tau = (1\ 3\ 5\ 2\ 4).$$

注意此時每一個元素的動作都用這一個 cycle 表示出來了, 所以 τ 是一個 5-cycle.

接下來我們看

$$\sigma \cdot \tau = (4\ 5)(1\ 2\ 3)(1\ 3\ 5\ 2\ 4)$$

會是甚麼? 當然了你可以將這些 cycles 還原成原來複雜的形式再計算, 不過這裡我們想直接用 cycle 的看法來處理. 首先觀察 (1 3 5 2 4) 將 $1 \mapsto 3$, 不過後面的 (1 2 3) 將 $3 \mapsto 1$, 最後 (4 5) 固定 1 所以知 $\sigma \cdot \tau$ 將 $1 \mapsto 1$. 也就是說在 $\sigma \cdot \tau$ 的 cycle 寫法中 1 不會出現. 現在看 2: (1 3 5 2 4) 將 $2 \mapsto 4$, 而後面的 (1 2 3) 將 4 固定住, 最後 (4 5) 將 $4 \mapsto 5$ 故知 $\sigma \cdot \tau$ 將 $2 \mapsto 5$, 所以我們寫下

$$(2\ 5$$

然而 (1 3 5 2 4) 將 $5 \mapsto 2$, 而後面的 (1 2 3) 將 $2 \mapsto 3$, 最後 (4 5) 固定 3, 所以得 $\sigma \cdot \tau$ 將 $5 \mapsto 3$, 我們記下

$$(2\ 5\ 3$$

然而 (1 3 5 2 4) 將 $3 \mapsto 5$, 且 (1 2 3) 將 5 固定住, 最後 (4 5) 將 $5 \mapsto 4$ 故知 $\sigma \cdot \tau$ 將 $3 \mapsto 4$, 所以繼續寫下

$$(2\ 5\ 3\ 4$$

最後 (1 3 5 2 4) 將 $4 \mapsto 1$, 而後面的 (1 2 3) 將 $1 \mapsto 2$, 然後 (4 5) 固定 2, 所以得 $\sigma \cdot \tau$ 將 4 送回了 2, 我們得知

$$\sigma \cdot \tau = (2\ 5\ 3\ 4).$$

兩個 cycles $(i_1\ \cdots\ i_k)$ 和 $(j_1\ \cdots\ j_l)$ 如果其中 $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \emptyset$ 則稱此兩 cycle 為 *disjoint cycles.* 如果將 S_n 中的元素寫成一些兩兩 disjoint 的 cycles 的乘積 (當然包括只有一個 cycle 的情況), 我們就稱之為 disjoint cycle decomposition. 如前面 (4 5)(1 2 3) 和 (1 3 5 2 4) 就分別是 σ 和 τ 的 disjoint cycle decomposition.

我們簡單的說明一下對任意的 $\sigma \in S_n$, 其 disjoint cycle decomposition 是存在的. 作法就如同前面的例子, 任取一數 $a_1 \in \{1, \ldots, n\}$ 我們先考慮 σ 將 a_1 送到何處? 若 $\sigma(a_1) = a_1$, 則知 a_1 不會出現在 cycle decomposition 之中, 所以我們繼續考慮其他的數. 如果 $\sigma(a_1) = a_2 \neq a_1$ 則寫下

$$(a_1\ a_2$$

接下來看 $\sigma(a_2)$ 為何? ...如此繼續下去直到第一個 a_k 使得 $\sigma(a_k)$ 會和前面的某數相同. 也就是說 $a_1, \ldots, a_k$ 都相異但 $\sigma(a_k) \in \{a_1, \ldots, a_{k-1}\}$. 不過此時 $\sigma(a_k)$ 非得等於 a_1 不可, 因為若 $\sigma(a_k) = a_i$, 其中 $i > 1$, 則已知 $\sigma(a_{i-1}) = a_i$, 由 σ 是 1-1 知 $a_k = a_{i-1}$ 這和 $a_1, \ldots, a_k$ 兩兩相異矛盾, 所以得 $\sigma(a_k) = a_1$. 也就是說我們得到一個 cycle:

$$(a_1\ \cdots\ a_k).$$

接下來我們考慮 $\{a_1, \ldots, a_k\}$ 以外的數 b_1, 再利用同樣的方式得到一個 cycle. 如此繼續下去直到將所有 $\{1, \ldots, n\}$ 考慮完畢, 然後得 σ 就是這些 cycles 的乘積. 當然了利用 σ 是 1-1 我們很容易看出這樣做出的 cycles 都是 disjoint.

接下來我們要說 disjoint cycle decomposition 是唯一的. 不過這裡的唯一性要說明一下. 首先觀察 (1 2 3) 這一個 cycle 其實它和 (2 3 1) 及 (3 1 2) 都表示同一個函數: 即 $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$. 因此我們將之視為同一 cycle (不過要注意 (1 3 2) 是不同的 cycle). 另外 (1 2 3)(4 5) 和 (4 5)(1 2 3) 也是同一個函數所以我們也將之視為同樣的 decomposition.

Lemma 3.4.4. 令 $\sigma = (a_1\ a_2 \cdots a_k)$ 和 $\tau = (b_1\ b_2 \cdots b_l)$ 是 S_n 的兩個 *cycles.*

(1) 如果 $k = l$ 且 $a_1 = b_2$, $a_2 = b_3$, ..., $a_{k-1} = b_k$, $a_k = b_1$, 則 $\sigma = \tau$.

(2) 如果 σ 和 τ 是 *disjoint,* 即 $\{a_1, \ldots, a_k\} \cap \{b_1, \ldots, b_l\} = \emptyset$, 則 $\sigma \cdot \tau = \tau \cdot \sigma$.

Proof. 我們曾經強調過, 要說明兩個 S_n 中的元素是相同的只要將之視為函數, 將 $\{1,\ldots,n\}$ 中任意數代入都相等就可.

(1) 若 $x \in \{1,\ldots,n\}$ 但 $x \notin \{a_1,\ldots,a_k\}$, 則知 $\sigma(x) = x$, 但由假設知

$$\{a_1,\ldots,a_k\} = \{b_1,\ldots,b_l\},$$

所以 $x \notin \{b_1,\ldots,b_l\}$, 也就是說 $\tau(x) = x$.

若 $x \in \{a_1,\ldots,a_k\}$, 假設 $x = a_i$, $1 \le i \le k-2$, 則

$$\sigma(x) = \sigma(a_i) = a_{i+1} = b_{i+2}.$$

此時因 $a_i = b_{i+1}$, 所以

$$\tau(x) = \tau(b_{i+1}) = b_{i+2}.$$

而當 $x = a_{k-1}$ 時,

$$\sigma(x) = \sigma(a_{k-1}) = a_k = b_1.$$

此時因 $a_{k-1} = b_k$, 故

$$\tau(x) = \tau(b_k) = b_1.$$

最後當 $x = a_k$ 時,

$$\sigma(x) = \sigma(a_k) = a_1 = b_2.$$

此時因 $a_k = b_1$ 所以

$$\tau(x) = \tau(b_1) = b_2.$$

得證對所有的 $x \in \{1,\ldots,n\}$ 皆有 $\sigma(x) = \tau(x)$, 因此知 $\sigma = \tau$.

(2) 此時由假設 σ 和 τ 是 disjoint, 所以 $x \in \{1,\ldots,n\}$ 可分成三種情況: (a) $x \notin \{a_1,\ldots,a_k\} \cup \{b_1,\ldots,b_l\}$; (b) $x \in \{a_1,\ldots,a_k\}$; (c) $x \in \{b_1,\ldots,b_l\}$.

當 x 是屬狀況 (a) 時, 得 $\sigma(x) = \tau(x) = x$ 故

$$(\sigma\cdot\tau)(x) = \sigma(\tau(x)) = \sigma(x) = x,$$

同理知 $(\tau\cdot\sigma)(x) = x$.

當 x 是屬狀況 (b) 時, 得 $\sigma(x) \in \{a_1,\ldots,a_k\}$ 但由 disjoint 知 x 和 $\sigma(x)$ 皆不屬於 $\{b_1,\ldots,b_l\}$ 故 $\tau(x) = x$ 且 $\tau(\sigma(x)) = \sigma(x)$. 所以知

$$(\sigma\cdot\tau)(x) = \sigma(\tau(x)) = \sigma(x)$$

且

$$(\tau\cdot\sigma)(x) = \tau(\sigma(x)) = \sigma(x).$$

最後若 x 是屬狀況 (c) 時, 同狀況 (b) 可知

$$(\sigma\cdot\tau)(x) = \tau(x) = (\tau\cdot\sigma)(x).$$

故得 $\sigma\cdot\tau = \tau\cdot\sigma$. □

Remark 3.4.5. 在 Lemma 3.4.4 中我們證得

$$(a_1\ a_2\ \cdots\ a_{k-1}\ a_k)$$

和

$$(a_k\ a_1\ \cdots\ a_{k-2}\ a_{k-1})$$

為同一 cycle. 對 $(a_k\ a_1\ \cdots\ a_{k-2}\ a_{k-1})$ 再套用一次 Lemma 3.4.4 可得

$$(a_{k-1}\ a_k\ \cdots\ a_{k-3}\ a_{k-2})$$

也是同一 cycle. 如此一直循環下去我們可得到同一個 k-cycle 有 k 種寫法.

另外我們要強調的是若 σ 和 τ 不是 disjoint 時, 則 $\sigma\cdot\tau$ 並不一定等於 $\tau\cdot\sigma$ (前面已給過例子了).

現在我們可以說如果將 Lemma 3.4.4 的這兩種狀況忽略 (即不管一個 cycle 的循環或兩個 disjoint cycle 的順序), 那麼任一個 S_n 的元素寫成 disjoint cycle decomposition 的寫法唯一. 假設 $\sigma \in S_n$ 有兩種 disjoint cycle decompositions: $\sigma = \sigma_1\cdots\sigma_r$ 和 $\sigma = \tau_1\cdots\tau_s$, 其中 $\sigma_1,\ldots,\sigma_r$ 和 $\tau_1,\ldots,\tau_s$ 分別是兩組 disjoint cycles. 假設 $a_1 \in \{1,\ldots,n\}$ 在 σ_1 這個 cycle 出現, 而 $\sigma_1(a_1) = a_2$, 則我們有

$$\sigma_1 = (a_1\ a_2\ \cdots$$

然而 $\sigma_1,\ldots,\sigma_r$ 是 disjoint 所以 a_1, a_2 不會在 $\sigma_2,\ldots,\sigma_r$ 中出現; 也就是說當 i 符合 $2 \le i \le r$ 時 $\sigma_i(a_1) = a_1$ 因此由 $\sigma = \sigma_1\cdots\sigma_r$ 知

$$\sigma(a_1) = (\sigma_1\cdots\sigma_r)(a_1) = \sigma_1(a_1) = a_2. \tag{3.5}$$

不過由於 $\sigma = \tau_1\cdots\tau_s$, a_1 一定會在某一個 τ_i 中出現, 否則如果 a_1 在所有的 τ_i 都沒出現則知 $\tau_i(a_1) = a_1$, 然而若真如此, 則得

$$\sigma(a_1) = \tau_1\cdots\tau_s(a_1) = a_1.$$

此和上式 (3.5) 相矛盾. 其實由於 $\tau_1,\ldots,\tau_s$ 是 disjoint, a_1 只會出現在唯一的 τ_i 中. 我們不妨假設 a_1 出現在 τ_1 中 (別忘了 $\tau_1,\ldots,\tau_s$ 是 disjoint 所以它們可以兩兩交換). 因為 a_1 不會在其他的 τ_i 出現, 當 i 符合 $2 \le i \le s$ 時, 我們有 $\tau_i(a_1) = a_1$. 因此知

$$\sigma(a_1) = (\tau_1\cdots\tau_s)(a_1) = \tau_1(a_1). \tag{3.6}$$

結合 (3.5) 和 (3.6) 兩式, 我們得 $\tau_1(a_1) = a_2$. 也就是說

$$\tau_1 = (a_1\ a_2\ \cdots$$

對 a_2 用同樣的論述可得 $\sigma_1(a_2) = \tau_1(a_2)$, 如此一直下去我們可得 $\sigma_1 = \tau_1$. 因此用歸納法可知 $r = s$ 且 對所有的 i 皆有 $\sigma_i = \tau_i$. 我們證得了 S_n 中所有的元素皆存在唯一的 disjoint cycle decomposition.

3.4.4. Disjoint cycle 的性質. 我們現在來看看寫成 disjoint cycle 到底有哪些好處.

其中一個好處就是很容易求出 inverse. 首先來看單一一個 cycle 的情況.

Lemma 3.4.6. *若*

$$\sigma = (a_1\ a_2\ \cdots\ a_{k-1}\ a_k)$$

是 S_n 中的一個 k-cycle. 則 σ^{-1} 也是一個 k-cycle 且

$$\sigma^{-1} = (a_k\ a_{k-1}\ \cdots\ a_2\ a_1).$$

Proof. 令 $\tau = (a_k\ a_{k-1}\ \cdots\ a_2\ a_1)$ 我們直接證明 $\tau\cdot\sigma$ 是 identity. 也就是要證對所有 $x \in \{1,\ldots,n\}$, $(\tau\cdot\sigma)(x) = x$.

如果 $x \notin \{a_1,\ldots,a_k\}$ 則自然 $\sigma(x) = \tau(x) = x$, 所以此時

$$(\tau\cdot\sigma)(x) = \tau(\sigma(x)) = \tau(x) = x.$$

反之, 如果 $x \in \{a_1,\ldots,a_k\}$, 則當 $x = a_i$, 其中 $1 \le i \le k-1$ 時, 因 $\sigma(x) = \sigma(a_i) = a_{i+1}$ 且 $2 \le i+1 \le k$, 故

$$(\tau\cdot\sigma)(x) = \tau(\sigma(a_i)) = \tau(a_{i+1}) = a_i = x.$$

而當 $x = a_k$ 時

$$(\tau\cdot\sigma)(x) = \tau(\sigma(a_k)) = \tau(a_1) = a_k = x.$$

故得 $\tau\cdot\sigma$ 是 S_n 的 identity, 也就是說 $\tau = \sigma^{-1}$. □

若 $\sigma = \sigma_1\cdots\sigma_r$ 是 σ 的 disjoint cycle decomposition. 則我們可以利用 Lemma 3.4.6 將每一個 σ_i 的 inverse 求出. Lemma 3.4.6 也告訴我們這些 $\sigma_1^{-1},\ldots,\sigma_r^{-1}$ 是 disjoint cycles. 所以可以很容易的就將 σ^{-1} 的 disjoint cycle decomposition 寫出. 例如若 $\sigma = (1\ 2\ 3)(4\ 5)$, 我們馬上得 $\sigma^{-1} = (3\ 2\ 1)(5\ 4)$.

寫成 disjoint cycle 的另一個好處是能夠很快的求出 S_n 中元素的 order. 我們還是先來看單一一個 cycle 的情況.

Lemma 3.4.7. *若 σ 是 S_n 中的一個 k-cycle. 則 $\mathrm{ord}(\sigma) = k$.*

Proof. 若 $\sigma = (a_1\ a_2\ \cdots\ a_{k-1}\ a_k)$, 我們要證當 $1 \le i \le k-1$ 時, σ^i 不是 S_n 中的 identity, 而 σ^k 是 S_n 的 identity.

當 $1 \le i \le k-1$ 時, $\sigma^i(a_1) = a_{i+1}$. 由於 $2 \le i+1 \le k$, 我們知 $a_{i+1} \ne a_1$, 也就是說 $\sigma^i(a_1) \ne a_1$. 所以 σ^i 不可能是 identity.

另外,若 $x \notin \{a_1,\ldots,a_k\}$ 時, 當然有 $\sigma^k(x) = x$. 而由定義知對所有的 $x \in \{a_1,\ldots a_k\}$ 皆有 $\sigma^k(x) = x$. 所以得 σ^k 是 identity. □

我們已知一個 cycle 的 order 為何, 但要求一些 disjoint cycles 的乘積的 order 我們需要以下這個一般 group 的性質:

Lemma 3.4.8. 令 $a, b \in G$ 且 $a \cdot b = b \cdot a$. 若 $\langle a \rangle \cap \langle b \rangle = \{e\}$, 則

$$\mathrm{ord}(a \cdot b) = \mathrm{lcm}[\mathrm{ord}(a), \mathrm{ord}(b)],$$

其中 lcm 表最小公倍數.

Proof. 回顧一下, $\mathrm{ord}(a) = n$ 等價於下面兩條件: (1) $a^n = e$; (2) 如果 $a^r = e$ 則 $n \mid r$.

若令 $\mathrm{ord}(a) = n$ 且 $\mathrm{ord}(b) = m$, 而 $l = \mathrm{lcm}[n, m]$, 則由 $a \cdot b = b \cdot a$ 知 $(a \cdot b)^l = a^l \cdot b^l = e$. 此證明了 l 符合 $\mathrm{ord}(a \cdot b)$ 的條件 (1).

現若 $(a \cdot b)^r = e$, 知 $a^r \cdot b^r = e$, 也就是 $a^r = b^{-r}$. 然而 $a^r \in \langle a \rangle$ 且 $b^{-r} \in \langle b \rangle$, 故知 $a^r \in \langle a \rangle \cap \langle b \rangle$. 利用假設 $\langle a \rangle \cap \langle b \rangle = \{e\}$, 得 $a^r = e$ 且 $b^{-r} = (b^r)^{-1} = e$ (也就是 $b^r = e$). 因 $\mathrm{ord}(a) = n$, $\mathrm{ord}(b) = m$, 利用條件 (2) 知 $n \mid r$ 且 $m \mid r$. 也就是 r 是 n, m 的公倍數. 再利用最小公倍數的性質知 $l = \mathrm{lcm}[n, m] \mid r$. 此證明了 l 符合 $\mathrm{ord}(a \cdot b)$ 的條件 (2). 所以 $\mathrm{ord}(a \cdot b) = l = \mathrm{lcm}[\mathrm{ord}(a), \mathrm{ord}(b)]$. □

Proposition 3.4.9. 令 $\sigma \in S_n$, 若 $\sigma = \sigma_1 \cdot \sigma_2 \cdots \sigma_r$ 是 σ 的 *disjoint cycle decomposition,* 其中 σ_i 是一個 n_i-*cycle.* 則

$$\mathrm{ord}(\sigma) = \mathrm{lcm}[n_1, n_2, \ldots, n_r].$$

Proof. 我們首先證 $\mathrm{ord}(\sigma_1 \cdot \sigma_2) = \mathrm{lcm}[n_1, n_2]$. 因 σ_1 和 σ_2 是 disjoint, 所以 $\sigma_1 \cdot \sigma_2 = \sigma_2 \cdot \sigma_1$. 因此只要我們證得 $\langle \sigma_1 \rangle \cap \langle \sigma_2 \rangle = \{e\}$, 則由 Lemma 3.4.7 和 Lemma 3.4.8 知 $\mathrm{ord}(\sigma_1 \cdot \sigma_2) = \mathrm{lcm}[n_1, n_2]$. 現若 $\tau \in \langle \sigma_1 \rangle \cap \langle \sigma_2 \rangle$, 則存在 i 和 j 使得 $\tau = \sigma_1^i = \sigma_2^j$. 若 τ 不是 S_n 的 identity, 即存在 $a \in \{1, \ldots, n\}$ 使得 $\tau(a) \neq a$. 也就是說 $\sigma_1^i(a) \neq a$. 這當然就保證 a 必須出現在 σ_1 的 cycle 中 (否則 $\sigma_1(a) = a$ 會得到 $\sigma_1^i(a) = a$). 然而 σ_2 和 σ_1 是 disjoint, 故 a 必不會出現在 σ_2 的 cycle 中. 也就是說 $\sigma_2(a) = a$. 這會造成 $\sigma_2^j(a) = a$, 與當初假設 $\sigma_2^j(a) = \tau(a) \neq a$ 相矛盾. 因此 τ 非得是 S_n 的 identity 不可. 因此得證 $\langle \sigma_1 \rangle \cap \langle \sigma_2 \rangle = \{e\}$, 同時得 $\mathrm{ord}(\sigma_1 \cdot \sigma_2) = \mathrm{lcm}[n_1, n_2]$.

接下來我們可以用數學歸納法. 因 $\sigma_1, \ldots \sigma_{r-1}, \sigma_r$ 是 disjoint, 故有

$$(\sigma_1 \cdots \sigma_{r-1}) \cdot \sigma_r = \sigma_r \cdot (\sigma_1 \cdots \sigma_{r-1}).$$

再套用前面的論述, 我們有

$$\langle \sigma_1 \cdots \sigma_{r-1} \rangle \cap \langle \sigma_r \rangle = \{e\}.$$

因此由歸納假設 $\mathrm{ord}(\sigma_1 \cdots \sigma_{r-1}) = \mathrm{lcm}[n_1, \ldots, n_{r-1}]$ 及 Lemma 3.4.8 得

$$\begin{aligned} \mathrm{ord}(\sigma) &= \mathrm{ord}((\sigma_1 \cdots \sigma_{r-1}) \cdot \sigma_r) \\ &= \mathrm{lcm}[\mathrm{lcm}[n_1, \ldots, n_{r-1}], n_r] \\ &= \mathrm{lcm}[n_1, \ldots, n_{r-1}, n_r]. \end{aligned}$$

□

Proposition 3.4.9 告訴我們一個很快的方法計算 S_n 的元素的 order. 例如若 $\sigma = (1\ 2\ 3)(4\ 5)$ 則 $\mathrm{ord}(\sigma) = \mathrm{lcm}[2,3] = 6$. 這比你一個一個去乘快多了. 不過要記住 Proposition 3.4.9 只能當 disjoint cycle 乘在一起才適用. 例如 $(1\ 2\ 3)(3\ 2\ 1)$ 是 identity. 其 order 為 1 不是 $\mathrm{lcm}[3,3] = 3$.

3.4.5. 一些 cycles 的運算. 我們曾經提過 cycles 如何相乘, 由於有一些型態的 cycles 的運算以後經常會出現, 在這裡我們將其整理出來以方便以後使用.

Conjugation 是一種運算, 若 $a \in G$, 則對任意的 $x \in G$, $x \cdot a \cdot x^{-1}$ 就稱為 a 的一個 conjugate. 在 S_n 中, 若 $\sigma = \sigma_1 \cdots \sigma_r$ 是 σ 的一個 disjoint cycle decomposition, 則對任意的 $\tau \in S_n$ 我們有

$$\tau \cdot \sigma \cdot \tau^{-1} = \tau \cdot (\sigma_1 \cdots \sigma_r) \cdot \tau^{-1} = (\tau \cdot \sigma_1 \cdot \tau^{-1}) \cdots (\tau \cdot \sigma_r \cdot \tau^{-1}).$$

因此要算出這一個 conjugate 我們只要算出每一個 cycle 的 conjugate 為何即可.

Lemma 3.4.10. 若

$$\sigma = (a_1\ a_2 \cdots a_{k-1}\ a_k)$$

是 S_n 中的一個 *k-cycle*. 則對任意的 $\tau \in S_n$, $\tau \cdot \sigma \cdot \tau^{-1}$ 是一個 *k-cycle* 且

$$\tau \cdot \sigma \cdot \tau^{-1} = \big(\tau(a_1)\ \tau(a_2) \cdots \tau(a_{k-1})\ \tau(a_k)\big).$$

Proof. 首先注意因 $(a_1 \cdots a_k)$ 是一個 k-cycle, 這些 a_i 都相異, 再利用 $\tau \in S_n$ 是 1-1 所以 $\tau(a_i)$ 也都相異. 因此 $(\tau(a_1) \cdots \tau(a_k))$ 確實是一個 k-cycle.

令 $\delta = \big(\tau(a_1) \cdots \tau(a_k)\big)$, 要證明 $\tau\cdot\sigma\cdot\tau^{-1} = \delta$, 我們只要證明對所有 $x \in \{1, \ldots, n\}$, $\tau(\sigma(\tau^{-1}(x)))$ 和 $\delta(x)$ 相同就好.

若 $x \notin \{\tau(a_1), \ldots, \tau(a_k)\}$ 則 $\tau^{-1}(x) \notin \{a_1, \ldots, a_k\}$, 故得 $\sigma(\tau^{-1}(x)) = \tau^{-1}(x)$. 因此

$$\tau(\sigma(\tau^{-1}(x))) = \tau(\tau^{-1}(x)) = x,$$

然而 $x \notin \{\tau(a_1), \ldots, \tau(a_k)\}$, 故 $\delta(x) = x$. 所以在這情況下它們的作用相同.

若 $x = \tau(a_1)$ 則

$$\tau(\sigma(\tau^{-1}(x))) = \tau(\sigma(a_1)) = \tau(a_2)$$

且 $\delta(x) = \delta(\tau(a_1)) = \tau(a_2)$. 同理得對所有的 $x \in \{\tau(a_1), \ldots, \tau(a_k)\}$, $\tau \cdot \sigma \cdot \tau^{-1}$ 和 δ 對 x 的作用都相同. 因此知在 S_n 中它們是相同的元素. □

Example 3.4.11. 若 $\sigma = (1\ 2\ 3)(4\ 5)$, 而 $\tau = (3\ 4)$ 則

$$\begin{aligned} \tau \cdot \sigma \cdot \tau^{-1} &= (\tau \cdot (1\ 2\ 3) \cdot \tau^{-1}) \cdot (\tau \cdot (4\ 5) \cdot \tau^{-1}) \\ &= \big(\tau(1)\ \tau(2)\ \tau(3)\big)\big(\tau(4)\ \tau(5)\big) \\ &= (1\ 2\ 4)(3\ 5) \end{aligned}$$

另一種常見的運算是 S_n 中的一個 2-cycle 和另一元素的乘法. 我們看兩種基本的形式.

Lemma 3.4.12. 令 $\tau = (a\ b)$ 是 S_n 中的一個 2-*cycle*.

(1) 若 $\sigma = (a\ a_2 \cdots a_k)$ 是一個 S_n 中的 k-*cycle*, 其中 $a_2, \ldots, a_k \neq b$, 則

$$\tau \cdot \sigma = (a\ a_2 \cdots a_k\ b)$$

(2) 若 $\sigma = (a\ a_2 \cdots a_k\ b\ b_2 \cdots b_l)$ 是一個 S_n 中的 $k+l$-*cycle*, 則

$$\tau \cdot \sigma = (a\ a_2 \cdots a_k)(b\ b_2 \cdots b_l)$$

Proof. (1) 當 $\sigma = (a\ a_2 \cdots a_k)$ 時, 若 $x \in \{1, \ldots, n\}$ 但 $x \notin \{a, a_2, \ldots, a_k, b\}$, 則 $(\tau \cdot \sigma)(x) = \tau(x) = x$, 故 x 不回出現在 $\tau \cdot \sigma$ 的 disjoint cycle decomposition 中. 若 $x \in \{a, a_2, \ldots, a_{k-1}\}$, 則 $\sigma(x) \notin \{a, b\}$, 故 $(\tau \cdot \sigma)(x) = \sigma(x)$. 故可寫下

$$(a\ a_2 \cdots a_k$$

而當 $x = a_k$ 時 $(\tau \cdot \sigma)(a_k) = \tau(\sigma(a_k)) = \tau(a) = b$, 故可繼續寫下

$$(a\ a_2 \cdots a_k\ b$$

最後因 $(\tau \cdot \sigma)(b) = \tau(\sigma(b)) = \tau(b) = a$, 故可得一個 cycle

$$(a\ a_2 \cdots a_k\ b)$$

由於我們已考慮 $\tau \cdot \sigma$ 對所有 $x \in \{1, \ldots, n\}$ 的作用故可得

$$(a\ b)(a\ a_2 \cdots a_k) = (a\ a_2 \cdots a_k\ b) \tag{3.7}$$

(2) 同前面, 當 $x \notin \{a, a_2, \ldots, a_k, b, b_2, \ldots, b_l\}$ 時, $(\tau \cdot \sigma)(x) = \tau(x) = x$, 故 x 不回出現在 $\tau \cdot \sigma$ 的 disjoint cycle decomposition 中. 若 $x \in \{a, a_2, \ldots, a_{k-1}\}$, 則 $\sigma(x) \notin \{a, b\}$, 故 $(\tau \cdot \sigma)(x) = \sigma(x)$. 故可寫下

$$(a\ a_2 \cdots a_k$$

而當 $x = a_k$ 時 $(\tau \cdot \sigma)(a_k) = \tau(\sigma(a_k)) = \tau(b) = a$, 故可得一個 cycle

$$(a\ a_2 \cdots a_k)$$

然而這還並不一定是 $\tau \cdot \sigma$ 因為還有 $x \in \{b, b_2, \ldots, b_l\}$ 的情況未討論. 事實上同前一情況此時我們可得另一 cycle

$$(b\ b_2 \cdots b_l)$$

因我們已考慮完所有的 $x \in \{1, \ldots, n\}$ 故得

$$(a\ b)(a\ a_2 \cdots a_k\ b\ b_2 \cdots b_l) = (a\ a_2 \cdots a_k)(b\ b_2 \cdots b_l) \tag{3.8}$$

□

Remark 3.4.13. 在式子 (3.8) 中若在等式兩邊乘上 τ, 則因 τ^2 是 identity, 我們有

$$\sigma = \tau \cdot (\tau \cdot \sigma) = \tau \cdot (a\ a_2 \cdots a_k)(b\ b_2 \cdots b_l)$$

換句話說得到另一個有用的式子

$$(a\ b)(a\ a_2 \cdots a_k)(b\ b_2 \cdots b_l) = (a\ a_2 \cdots a_k\ b\ b_2 \cdots b_l) \tag{3.9}$$

3.4.6. Even and odd permutations. 因為 S_n 中的元素可以看成將 $\{1,\dots,n\}$ 的元素做排列組合, S_n 中的元素稱之為一個 *permutation.* 一個 permutation 應該是可以用每次只將 $\{1,\dots,n\}$ 中某兩個元素互換的方式組合得到. 將 $\{1\dots,n\}$ 中的某兩個元素互換的這個動作我們稱之為 *transposition.* 其實它只是 S_n 中的一個 2-cycle 罷了. 為了方便起見, 在這兒我們還是用 2-cycle 這個稱呼.

前面提到每個 permutation 可以用一些 transposition 組合而成, 這用數學的方法表達就是如下:

Lemma 3.4.14. *若 $\sigma \in S_n$, 則存在 S_n 的 2-cycles, $\tau_1,\dots,\tau_s$ 使得*

$$\sigma = \tau_1 \cdots \tau_s.$$

Proof. 因為 σ 可以寫成一些 cycles 的乘積, 要證明 σ 可以寫成 2-cycles 的乘積, 我們只要證明每一個 cycle 都可寫成 2-cycles 的乘積即可. 事實上由式子 (3.7) 知 $(a_1\ a_3)(a_1\ a_2) = (a_1\ a_2\ a_3)$, 如此一直下去可之任意的 k-cycle $(a_1\ a_2\ \cdots\ a_{k-1}\ a_k)$ 可寫成

$$(a_1\ a_2\ \cdots\ a_{k-1}\ a_k) = (a_1\ a_k)(a_1\ a_{k-1})\cdots(a_1\ a_2).$$

□

這裡要注意: Lemma 3.4.14 並沒有說每一個 S_n 的元素都可以寫成 'disjoint' 2-cycle 的乘積. 事實上這是不對的, 如 (1 2 3) 就沒法子寫成 disjoint 2-cycle 的乘積. 你知道為什麼嗎? 其實很簡單: 因為若 (1 2 3) 是一些 disjoint 2-cycle 的乘積, 則利用 Proposition 3.4.9 知其 order 應該為 2, 不過 (1 2 3) 的 order 是 3 故一定不可能寫成 disjoint 2-cycle 的乘積. 另外 Lemma 3.4.14 也沒有提及寫成 2-cycle 的乘積寫法會唯一, 因為這也是錯的. 例如

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

其實連可寫成多少個 2-cycle 的乘積都不一定. 例如 (1 2) 這一個 2-cycle 就可以寫成 (1 3)(2 3)(1 3) 這三個 2-cycle 的乘積.

從上面這個觀點來看, 將一個 S_n 的元素寫成 2-cycle 的乘積好像沒什麼好處. 事實上在大學的代數中我們學 2-cycle decomposition 只是為了方便去定義什麼是 even permutation 和 odd permutation 罷了. 我們稱 S_n 中的元素是 even 如果它可以寫成偶數個 2-cycle 的乘積, 反之則稱為 odd. 你應該會覺得這個定義有點奇怪吧! 前面提過一個 S_n 的元素可以寫成多少個 2-cycle 的乘積是不一定的. 有沒有可能它一下可寫成偶數個乘積, 而又可以寫成奇數個呢? 下一個定理告訴我們這是不可能的.

Theorem 3.4.15. *若 $\sigma \in S_n$ 且 $\sigma = \tau_1\cdot\tau_2\cdots\tau_r = \tau_1'\cdot\tau_2'\cdots\tau_s'$, 其中 $\tau_1,\dots,\tau_r$ 和 $\tau_1',\dots,\tau_s'$ 都是 2-cycles.* 則

$$r \equiv s \pmod 2 \quad (\text{即 } r \text{ 和 } s \text{ 同奇同偶：}\ \ 2 \mid r-s).$$

Proof. 我們利用大家都學過的線性代數裡有關行列式的性質來證明此定理. 回顧一下: 給定一 $n \times n$ 的矩陣 A, 如果將 A 中的某兩列互換所得的矩陣 A', 其行列式 $\det(A')$ 會等於 $-\det(A)$.

現在任取 $\sigma \in S_n$ 我們定義 $\sigma * A$ 這個矩陣是將 A 的第 i 列換到第 $\sigma(i)$ 列. 例如若 $\sigma = (i\ j)$ 則 $\sigma * A$ 就是將 A 的第 i 列換到第 j 列, 且將第 j 列換到第 i 列, 換句話說若 σ 是一個 2 cycle 則 $\sigma * A$ 就是如上述將 A 的某兩列互換. 若 $\sigma, \tau \in S_n$, 則 $(\sigma \cdot \tau) * A$ 是將 A 的第 i 列換到第 $(\sigma \cdot \tau)(i) = \sigma(\tau(i))$ 列. 而 $\tau * A$ 的第 $\tau(i)$ 列是 A 的第 i 列 且 $\sigma * (\tau * A)$ 是將 $\tau * A$ 的第 $\tau(i)$ 列換到第 $\sigma(\tau(i))$ 列. 換句話說 $\sigma * (\tau * A)$ 是將 A 的第 i 列換到第 $\sigma(\tau(i))$ 列. 這和 $(\sigma \cdot \tau) * A$ 是一樣的, 所以我們有

$$(\sigma \cdot \tau) * A = \sigma * (\tau * A) \quad \forall \sigma, \tau \in S_n. \tag{3.10}$$

現在若 $\sigma = \tau_1 \cdot \tau_2 \cdots \tau_r = \tau'_1 \cdot \tau'_2 \cdots \tau'_s$, 考慮 $\sigma * I_n$, 其中 I_n 是 $n \times n$ 的單位矩陣. 則由式子 (3.10) 知

$$\sigma * I_n = \tau_1 * (\cdots * (\tau_r * I_n)) = \tau'_1 * (\cdots * (\tau'_s * I_n)).$$

然而 τ_i, τ'_j 是 2-cycles, 它們每作用一次行列式值會變號, 所以得

$$\det(\sigma * I_n) = (-1)^r = (-1)^s.$$

也就是說 $r - s$ 是一個偶數. □

Theorem 3.4.15 告訴我們如果你找到偶數個 2-cycles 將 σ 寫成這些 2-cycle 的乘積, 則 σ 就不可能寫成奇數個 2-cycle 的乘積. 反之亦然. 因此我們有下面這個正式的定義:

Definition 3.4.16. 若 $\sigma \in S_n$ 可寫成偶數個 2-cycles 的乘積, 則稱 σ 為一個 *even permutation.* 反之, 若 σ 可寫成奇數個 2-cycles 的乘積, 則稱 σ 為一個 *odd permutation*

在 Lemma 3.4.14 的證明中我們曾證得一個 k-cycle 可以寫成 $k-1$ 個 2-cycle 的乘積, 因此一個 k-cycle 是 even 若 k 是奇數. 反之, 若 k 是偶數則此 k-cycle 就是 odd 了. 另外若 σ 可寫成 r 個 2-cycles 的乘積, 而 τ 可寫成 s 個 2-cycles 的乘積, 則 $\sigma \cdot \tau$ 可寫成 $r + s$ 個 2-cycles 的乘積. 因此我們有下一個結果:

Lemma 3.4.17. 令 $\sigma, \tau \in S_n$.

(1) 若 σ, τ 同為 *even permutations,* 或同為 *odd permutations,* 則 $\sigma \cdot \tau$ 為 *even permutation.*

(2) 若 σ 和 τ 其中一個是 *even permutation* 另一個是 *odd permutation,* 則 $\sigma \cdot \tau$ 為 *odd permutation.*

利用 Lemma 3.4.17 若將一個 S_n 的元素寫成 disjoint cycle decomposition, 就可以很快的判斷其為 even 或 odd. 這也是寫成 disjoint cycle decomposition 的另一個好處.

3.4.7. The alternating group. 在 S_n 中的 even permutations 所成的集合形成一個 group 稱之為 alternating group.

Theorem 3.4.18. 令 A_n 是 S_n 中所有的 *even permutation* 所成的集合.

(1) A_n 是 S_n 的一個 *normal subgroup.*

(2)
$$|A_n| = \frac{1}{2}n \cdot (n-1) \cdots 2 \cdot 1 = \frac{n!}{2}.$$

Proof. 考慮 $\text{sgn} : S_n \to \{1, -1\}$ 這個函數其中
$$\text{sgn}(\sigma) = \begin{cases} 1, & \text{若 } \sigma \text{ 是 even;} \\ -1, & \text{若 } \sigma \text{ 是 odd.} \end{cases}$$
若將 $\{1, -1\}$ 看成是一個乘法群, 則 1 是其 identity, 且 Lemma 3.4.17 告訴我們 sgn 是一個 group homomorphism. 由定義知 $\ker(\text{sgn}) = A_n$, 故由 Lemma 2.5.4 知 A_n 是 S_n 的一個 normal subgroup. 又任意的 2-cycle 是 odd, 故知 sgn 是 onto, 所以由 First Isomorphism 定理 (Corollary 2.6.2) 知 $S_n/A_n \simeq \{1, -1\}$. 也就是說 $|A_n| = |S_n|/2$. □

Definition 3.4.19. 我們將 S_n 中所有的 even permutation 所成的集合定為 A_n 稱之為 the *alternating group* of degree n.

Remark 3.4.20. 由於 A_n 的個數是 S_n 的一半, 那麼令一半當然是 S_n 中的 odd permutations 了, 所以在 S_n 中 odd permutation 和 even permutation 的個數一樣多.

每一個 S_n 的元素可以寫成一些 2-cycle 的乘積 (Lemma 3.4.14). 那麼 A_n 的元素都可以有甚麼特殊的表示法嗎?

Lemma 3.4.21. 若 $\sigma \in A_n$, 則存在 S_n 的 3-*cycles,* $\gamma_1, \ldots, \gamma_s$ 使得
$$\sigma = \gamma_1 \cdots \gamma_s.$$

Proof. 因 $\sigma \in A_n$ 故存在 $2r$ 個 2-cycles $\tau_1, \ldots, \tau_{2r}$ 使得 $\sigma = \tau_1 \cdot \tau_2 \cdots \tau_{2r-1} \cdot \tau_{2r}$. 我們將這些 τ_i 兩個兩個先擺一起, 也就是考慮 $\sigma = (\tau_1 \cdot \tau_2) \cdots (\tau_{2r-1} \cdot \tau_{2r})$. 若能證明任兩個 2-cycle 相乘都能寫成一些 3-cycles 的乘積, 那麼證明就完成了.

考慮 $\tau = (a\ b)$, $\tau' = (c\ d)$ 是 S_n 中兩個 2-cycle. 有三種可能情況:

(1) $\{a, b\} = \{c, d\}$, 此時 $\tau \cdot \tau'$ 是 identity, 所以我們可以將 $\tau \cdot \tau'$ 寫成
$$(1\ 2\ 3)(3\ 2\ 1)$$

(2) $\{a,b\}$ 和 $\{c,d\}$ 中恰有一數相同, 不失一般性我們假設 $a=c$ 但 $b\neq d$. 此時由式子 (3.7) 知

$$\tau\cdot\tau' = (a\ b)(a\ d) = (a\ d\ b)$$

(3) $\{a,b\}$ 和 $\{c,d\}$ 皆相異, 此時我們有

$$\tau\cdot\tau' = (a\ b)(c\ d) = (a\ d\ b)(a\ d\ c)$$

□

因為 3-cycle 是 even permutation, 所以所有的 3-cycles 都在 A_n 中. 下一個定理告訴我們反過來也是對的.

Proposition 3.4.22. *若 H 是 S_n 的一個 nontrivial proper subgroup, 假如 H 中含有所有的 3-cycles, 則 $H=A_n$.*

Proof. 若 $\sigma\in A_n$, 則由 Lemma 3.4.21 知存在 3-cycles, $\gamma_1,\ldots,\gamma_s$ 使得 $\sigma=\gamma_1\cdots\gamma_s$. 由假設, 這些 γ_i 都在 H 中. 又因 H 是 group, 由封閉性知 $\gamma_1\cdots\gamma_s\in H$. 也就是說 $\sigma\in H$. 故得 $A_n\subseteq H$. 然而 $H\neq S_n$ 故 $|H|<n!=2|A_n|$ 再由 Lagrange 定理 (Theorem 2.2.2) 知 $|H|$ 是 $|A_n|$ 的倍數. 唯一的可能就是 $|H|=|A_n|$. 故得 $H=A_n$ □

3.4.8. S_n 的 normal subgroup. 我們將介紹當 $n\geq 5$ 時 A_n 是 S_n 中唯一的 nontrivial normal subgroup.

因 S_3 只有 6 個元素, 我們將它們一一列出, 記有: (1 2), (1 3), (2 3), (1 2 3), (1 3 2) 和 identity. 其中 A_3 就是由 (1 2 3) 所產生的 cyclic group. 其他的 2-cycle 都只生成 order 2 的 subgroup. 考慮 (1 2) 所生成的 cyclic group $\langle(1\ 2)\rangle$, 由於

$$(1\ 3)(1\ 2)(1\ 3) = (3\ 2)\notin\langle(1\ 2)\rangle$$

可知 $\langle(1\ 2)\rangle$ 不是 S_3 的 normal subgroup. 同理知其他 order 為 2 的 subgroup 皆不是 normal. 因此在 S_3 中只有一個 nontrivial normal subgroup, 就是 A_3.

在 S_4 中情況就不一樣了. 除了 A_4 外 還有一個 normal subgroup

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

很容易看出 N 中除了 identity 以外, 每個元素都是 order 2, 也就是自己是自己的 inverse. 我們來檢查 N 是乘法封閉的. 由

$$(1\ 2)(3\ 4)\cdot(1\ 3)(2\ 4) = (1\ 4)(2\ 3)$$

就可以知 N 是乘法封閉的, 由此知 N 是 S_4 的 subgroup. (由於 N 中的元素都是 even permutation 可知 N 也是 A_4 的 subgroup.) 仔細觀察 N 中除了 identity 外其他的元素都是兩個 disjoint 2-cycle 相乘. 而且在 S_4 中所有可能的兩個 disjoint

2-cycle 相乘的 permutation 都在 N 中. 若 $\sigma = (a\ b)(c\ d)$ 是兩個 disjoint 2-cycle 相乘, 則由 Lemma 3.4.10 知對任意的 $\tau \in S_4$,

$$\tau \cdot \sigma \cdot \tau^{-1} = (\tau(a)\ \tau(b))(\tau(c)\ \tau(d))$$

也是由兩個 disjoint 2-cycle 相乘的 permutation. 換言知, 若 $\sigma \in N$, 則對任意的 $\tau \in S_4$ 皆得 $\tau \cdot \sigma \cdot \tau^{-1} \in N$, 故 N 是 S_4 的 normal subgroup.

當 $n \geq 5$ 時, 由於 S_n 的 order 已很大, 我們不可能如前面的方式討論下去. 我們有一個很重要的 Lemma 可以幫我們處理一般的狀況.

Lemma 3.4.23. 若 N 是 S_n 的一個 *nontrivial proper normal subgroup,* 且 N 中存在一個 3-*cycle,* 則 $N = A_n$.

Proof. Proposition 3.4.22, 告訴我們要證明 $N = A_n$, 只要證明所有的 3-cycle 皆在 N 中就可. 因此若 $(a\ b\ c)$ 是 N 中的一個 3-cycle, 我們想利用 N 是 normal 的性質證明任意的 3-cycle $(a'\ b'\ c')$ 也在 N 中.

由於 N 在 S_n 中 normal, 對任意的 $\tau \in S_n$, 因為 $(a\ b\ c) \in N$, 故有 $\tau \cdot (a\ b\ c) \cdot \tau^{-1} \in N$. 然而由 Lemma 3.4.10 知

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

因此對任意的 3-cycle $(a'\ b'\ c')$, 我們只要在 S_n 找到一個 τ 滿足 $\tau(a) = a'$, $\tau(b) = b'$ 和 $\tau(c) = c'$ 即可. 這當然做得到, 因為 a, b, c 皆相異, 而 a', b', c' 也都相異, 我們當然可找到一個 1-1 的函數將 $a \mapsto a'$, $b \mapsto b'$, $c \mapsto c'$. 也就是說對任意的 3-cycle $(a'\ b'\ c')$, 我們都可以在 S_n 找到一個 τ 滿足 $\tau \cdot (a\ b\ c) \cdot \tau^{-1} = (a'\ b'\ c')$. 所以由 $\tau \cdot (a\ b\ c) \cdot \tau^{-1} \in N$ 得 $(a'\ b'\ c') \in N$. □

綜合一下我們所知的結果: Lemma 3.4.22 告訴我們若已知 H 是 S_n 的一個 nontrivial proper subgroup, 則要證明 $H = A_n$ 須證明所有 S_n 的 3-cycle 都在 H 中才行; 然而若已知 H 是 normal 那麼 Lemma 3.4.23 告訴我們只要在 H 中找到一個 3-cycle 就可得 $H = A_n$.

現在我們可以證明當 $n \geq 5$ 時 A_n 是 S_n 唯一的 nontrivial normal subgroup.

Theorem 3.4.24. 當 $n \geq 5$ 時, 若 N 是 S_n 的 *nontrivial proper normal subgroup,* 則 $N = A_n$.

Proof. 由 Lemma 3.4.23 知我們只要想辦法在 N 中找到一個 3-cycle, 就可得 $N = A_n$.

現因 N 是 nontrivial, 所以 N 不是 identity. 換句話說在 N 中存在一個 σ 不是 identity. 既然 σ 不是 identity, 那麼 σ 必將 $\{1 \ldots, n\}$ 中某一整數 a 送到另一數 b, 即 $\sigma(a) = b \neq a$. σ 是我們在 N 中隨便挑的非 identity 的元素, 它長怎樣我們一點都不清楚. 它有可能將 b 送回到 a 也有可能送到另一個數 a', 所以我們可分成以下兩個 cases:

(1) $\sigma(a) = b$, 且 $\sigma(b) = a$;

(2) $\sigma(a) = b$ 但 $\sigma(b) = a' \neq a$.

我們接下來想利用 N normal 和利用 σ 這個微弱的訊息來幫我們在 N 中找到更具體一點的元素. 我們的方法是這樣的: 試著在 S_n 中找到一個 2-cycle τ, 使得 $\sigma \cdot \tau \cdot \sigma^{-1} \neq \tau$. 如此一來 $(\sigma \cdot \tau \cdot \sigma^{-1}) \cdot \tau^{-1}$ 就不會是 identity. 然而

$$(\sigma \cdot \tau \cdot \sigma^{-1}) \cdot \tau^{-1} = \sigma \cdot (\tau \cdot \sigma^{-1} \cdot \tau^{-1})$$

由 $\sigma \in N$, 得 $\sigma^{-1} \in N$ 再利用 N 是 normal 知 $\tau \cdot \sigma^{-1} \cdot \tau^{-1} \in N$. 因此 $\sigma \cdot (\tau \cdot \sigma^{-1} \cdot \tau^{-1}) \in N$. 也就是我們又在 N 中找到一個新的不是 identity 的元素.

當 σ 是 case 1 時, 我們在 $\{1, \ldots, n\}$ 中找另一個數 c, 使得 $c \neq a$ 且 $c \neq b$. 令 $\tau = (a\ c)$. 則由 Lemma 3.4.10 知

$$\sigma \cdot \tau \cdot \sigma^{-1} = (\sigma(a)\ \sigma(c)) = (b\ \sigma(c)).$$

注意此時因 $\sigma(b) = a$ 但 $c \neq b$ 故知 $\sigma(c) \neq a$. 也就是說

$$\sigma \cdot \tau \cdot \sigma^{-1} = (b\ \sigma(c)) \neq (b\ a) = \tau.$$

當 σ 是 case 2 時, 我們只要考慮 $\tau = (a\ b)$ 就可. 因為此時 $\sigma(b) = a' \neq a$, 故

$$\sigma \cdot \tau \cdot \sigma^{-1} = (\sigma(a)\ \sigma(b)) = (b\ a') \neq (a\ b) = \tau.$$

綜合以上 cases 1 和 2, 我們知: 不管 σ 為何我們都可以在 S_n 中找到一個 2-cycle τ 使得

$$(\sigma \cdot \tau \cdot \sigma^{-1}) \cdot \tau^{-1} \in N$$

且不是 identity. 更重要的是 $\tau = \tau^{-1}$ 和 $\sigma \cdot \tau \cdot \sigma^{-1}$ 都是 2-cycles. 也就是在 N 中存在一個元素 δ 是兩個 2-cycle 相乘且不是 identity.

這個 N 中的元素 δ 有可能是以下兩種情況:

甲: $\delta = (i\ j)(j\ k)$, 其中 i, j, k 皆相異.

乙: $\delta = (i\ j)(k\ l)$, 其中 i, j, k, l 皆相異.

若是 case 甲, 則

$$\delta = (i\ j)(j\ k) = (i\ j\ k) \in N,$$

故知 N 中有一個 3-cycle.

若是 case 乙, 我們選一個在 $\{1, \ldots, n\}$ 中但在 $\{i, j, k, l\}$ 以外的元素 m (這就是為何此定理需假設 $n \geq 5$ 的原因). 令 $\gamma = (i\ m)$, 則因 $\delta \in N$ 且 N 是 normal, 知 $\gamma \cdot \delta \cdot \gamma^{-1} = (m\ j)(k\ l) \in N$. 再由 $\delta \in N$ 知 $\delta \cdot (\gamma \cdot \delta \cdot \gamma^{-1}) \in N$. 然而

$$\begin{aligned} \delta \cdot (\gamma \cdot \delta \cdot \gamma^{-1}) &= (i\ j)(k\ l)(m\ j)(k\ l) \\ &= (i\ j)(m\ j) \\ &= (i\ j\ m) \end{aligned}$$

故知 N 中有一個 3-cycle.

我們證明了在任何狀況下 N 中皆有一個 3-cycle, 故得 $N = A_n$. □

記得我們在 S_4 中找到一個不是 A_4 的 normal subgroup, 它是由一些兩個 disjoint 2-cycle 相乘的 permutation 所形成. 當初我們證這些元素相乘有封閉性, 不過在 Theorem 3.4.24 的證明 (case 乙) 我們證得在 $n \geq 5$ 時這類元素相乘不再封閉.

3.4.9. A_n 的 **normal subgroup.** 若 B 是 A 的 subgroup, C 是 B 的 subgroup, 且知 C 是 A 的 normal subgroup, 則當然 C 也會是 B 的 normal subgroup. 然而若僅知 C 是 B 的 subgroup, 並不表示 C 會是 A 的 normal subgroup (參見 Remark 2.4.2). 所以雖然我們知在 $n \geq 5$ 時除了 A_n 外, S_n 沒有其他的 nontrivial proper normal subgroup, 但這並不表示 A_n 本身不會有 nontrivial normal subgroup.

我們將證事實上當 $n \geq 5$ 時 A_n 確實沒有 nontrivial normal subgroup. 我們將利用類似在 S_n 的方法處理, 唯一要克服的是我們只能考慮 A_n 裡的元素.

Lemma 3.4.25. 當 $n \geq 5$, 若 N 是 A_n 的一個 *normal subgroup,* 且 N 中存在一個 3-*cycle,* 則 $N = A_n$.

Proof. 首先再次強調在 Lemma 3.4.23 中的假設是 N 是 S_n 的 normal subgroup, 而這裡我們僅假設 N 是 A_n 的 normal subgroup, 由於此時 N 未必會是 S_n 的 normal subgroup 所以無法用 Lemma 3.4.23 來直接證明本 Lemma. 不過我們還是用類似的想法, 利用存在一個 3-cycle 和 N 在 A_n 中 normal 的假設得到所有的 3-cycle 都會在 N 中. 再利用 Proposition 3.4.22 得到 $N = A_n$.

假設 $(a\ b\ c) \in N$, 在 Lemma 3.4.23 的証明中我們是證明: 對任意的 3-cycle, $(a'\ b'\ c')$ 皆可找到 $\tau \in S_n$ 使得

$$\tau \cdot (a\ b\ c) \cdot \tau^{-1} = (a'\ b'\ c').$$

如今這件事還是對的. 唯一不同的是當初 N 是在 S_n 中 normal, 所以因 $(a\ b\ c) \in N$ 可得 $\tau \cdot (a\ b\ c) \cdot \tau^{-1} \in N$, 如今 N 只在 A_n 中 normal, 如果當初選的 τ 不屬於 A_n 則無法保證 $\tau \cdot (a\ b\ c) \cdot \tau^{-1}$ 會在 N 中 (回顧一下: N 在 A_n 中 normal 只告訴我們若 $\sigma \in N$, 且 $\tau \in A_n$ 才可保證 $\tau \cdot \sigma \cdot \tau^{-1} \in N$). 所以我們現在的策略是利用這個 τ 找到另一個 γ 在 A_n 使得 $\gamma \cdot (a\ b\ c) \cdot \gamma^{-1} = (a'\ b'\ c')$.

當然了, 如果當初找的 τ 已在 A_n 中那麼令 $\gamma = \tau$ 即可. 如果 τ 不在 A_n 呢? 這表示 τ 是 odd permutation, 所以只要找到一個 2-cycle 乘上 τ 就會成為 even permutation, 也就落入 A_n 了. 別忘了和 Lemma 3.4.23 不同, 這裡我們還多假設了 $n \geq 5$. 所以我們可選 $i, j \in \{1, \ldots, n\}$ 但 i 和 j 都不屬於 $\{a, b, c\}$, 而令 $\gamma = \tau \cdot (i\ j)$. 如此一來不但 $\gamma \in A_n$ 且

$$\begin{aligned}
\gamma \cdot (a\ b\ c) \cdot \gamma^{-1} &= (\tau \cdot (i\ j)) \cdot (a\ b\ c) \cdot (\tau \cdot (i\ j))^{-1} \\
&= \tau \cdot (i\ j)(a\ b\ c)(i\ j) \cdot \tau^{-1} \\
&= \tau \cdot (a\ b\ c) \cdot \tau^{-1} \quad (\text{因 } (a\ b\ c) \text{ 和 } (i\ j) \text{ disjoint}) \\
&= (a'\ b'\ c').
\end{aligned}$$

故由 $(a\ b\ c) \in N$ 且 N 在 A_n 中 normal, 得 $(a'\ b'\ c') \in N$. □

這裡要說明一下: 雖然 Lemma 3.4.25 我們用到了 $n \geq 5$ 這個假設, 不過當 $n = 3, 4$ 時, 我們可以直接證明 Lemma 3.4.25 也是對的.

最後我們依然要用類似證明 Theorem 3.4.24 的方法來證明以下的 Theorem.

Theorem 3.4.26. 當 $n \geq 5$ 時 A_n 沒有 *nontrivial proper normal subgroup.*

Proof. 我們要證明, 若 N 不是 identity 且是 A_n 的 normal subgroup, 則存在一個 3-cycle 在 N 中. 如此一來, 由 Lemma 3.4.25 知 $N = A_n$, 因而得證本定理.

回顧一下在 Theorem 3.4.24 的証明中, 我們是利用 N 中一個非 identity 的元素 σ, 找到一個 2-cycle τ 使得 $\sigma \cdot \tau \cdot \sigma^{-1} \neq \tau$. 如此就可以得到另一個在 N 中但不等於 identity 的元素, $\sigma \cdot (\tau \cdot \sigma^{-1} \cdot \tau^{-1})$. 這個元素當初會在 N 中完全是由於當時 N 假設是 S_n 的 normal subgroup, 所以利用 σ^{-1} 也在 N 中可得 $\tau \cdot \sigma^{-1} \cdot \tau^{-1} \in N$. 如今 N 是在 A_n normal, 而 τ 是 2-cycle 並不在 A_n 中, 我們不再有 $\tau \cdot \sigma^{-1} \cdot \tau^{-1} \in N$. 因此我們不能再用原來的 τ, 而是要找一個 A_n 中的元素. 事實上我們要找的是一個 3-cycle 就可. 也就是說我們希望找到一個 3-cycle ρ 使得 $\sigma \cdot \rho \cdot \sigma^{-1} \neq \rho$.

由於假設 $\sigma \in N$ 且不是 identity, 故存在 $a \in \{1, \ldots, n\}$ 使得 $\sigma(a) = b \neq a$. 由於我們要找的是 3-cycle, 我們要把 σ 細分成以下三種狀況:

(1) $\sigma(a) = b$, 且 $\sigma(b) = a$;

(2) $\sigma(a) = b$, $\sigma(b) = c$ 且 $\sigma(c) = a$;

(3) $\sigma(a) = b$, $\sigma(b) = c$ 且 $\sigma(c) = d \neq a$.

當σ 是 case 1 時, 我們可找 $\rho = (a\ b\ i)$, 其中 $i \in \{1 \ldots, n\}$ 但 $i \notin \{a, b\}$. 此時由 Lemma 3.4.10 得

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

注意 $\sigma(a) = b$, 而 $i \neq a$ 故 $\sigma(i) \neq b$. 由於 ρ 是將 $a \mapsto b$, 而 $\sigma \cdot \rho \cdot \sigma^{-1}$ 是將 $a \mapsto \sigma(i)$ 故知 $\sigma \cdot \rho \cdot \sigma^{-1} \neq \rho$.

當σ 是 case 2 時, 我們可找 $\rho = (a\ b\ i)$, 其中 $i \in \{1 \ldots, n\}$ 但 $i \notin \{a, b, c\}$ (別忘了 $n \geq 5$ 所以一定可以找到這樣的 i). 此時由 Lemma 3.4.10 得

$$\sigma \cdot \rho \cdot \sigma^{-1} = (b\ \ c\ \ \sigma(i)).$$

由於 ρ 是將 $b \mapsto i$, 而 $\sigma \cdot \rho \cdot \sigma^{-1}$ 是將 $b \mapsto c$, 故由 $i \neq c$ 知 $\sigma \cdot \rho \cdot \sigma^{-1} \neq \rho$.

當σ 是 case 3 時, 我們令 $\rho = (a\ b\ c)$ 就可. 因為此時

$$\sigma \cdot \rho \cdot \sigma^{-1} = (b\ \ c\ \ d),$$

由 $a \neq d$ 的假設知 $\sigma \cdot \rho \cdot \sigma^{-1} \neq \rho$.

綜合以上的結果我們知: 在 N 中任取一個不是 identity 的元素 σ, 存在一個 3-cycle ρ 符合 $\sigma \cdot \rho \cdot \sigma^{-1} \neq \rho$. 由於 $\rho \in A_n$, 而 N 在 A_n 中 normal, 故由 $\sigma^{-1} \in N$

得 $\rho \cdot \sigma^{-1} \cdot \rho^{-1} \in N$. 因此若令 $\gamma = (\sigma \cdot \rho \cdot \sigma^{-1}) \cdot \rho^{-1}$ 則 γ 不是 identity, 且 $\gamma = \sigma \cdot (\rho \cdot \sigma^{-1} \cdot \rho^{-1}) \in N$. 更重要的是由於 ρ 是一個 3-cycle, Lemma 3.4.10 告訴我們 $\sigma \cdot \rho \cdot \sigma^{-1}$ 也是一個 3-cycle. 所以 $\gamma = (\sigma \cdot \rho \cdot \sigma^{-1}) \cdot \rho^{-1}$ 是由兩個 3-cycle 相乘所得的 permutation. 簡言之: 我們在 N 中找到一個非 identity 的元素 γ, 而且 γ 是由兩個 3-cycle 相乘而得.

現在我們將 γ 的這兩個 3-cycles 可能的形式列出:

甲: 此二 3-cycles 中的元素都相同;

乙: 此二 3-cycles 中, 有兩個元素相同;

丙: 此二 3-cycles 中, 僅有一個元素相同;

丁: 此二 3-cycles 中的元素皆相異.

若是 case 甲, γ 可寫成 $(i\ j\ k)(i\ j\ k)$ (不可能是 $(i\ j\ k)(i\ k\ j)$ 因若如此則為 identity). 在此情形我們得

$$\gamma = (i\ \ j\ \ k)(i\ \ j\ \ k) = (i\ \ k\ \ j) \in N.$$

故知 N 中有一個 3-cycle.

若是 case 乙, γ 可寫成 $(i\ j\ k)(j\ i\ r)$ 或 $(i\ j\ k)(i\ j\ r)$. 在第一種情形,

$$\gamma = (i\ \ j\ \ k)(j\ \ i\ \ r) = (i\ \ r\ \ k) \in N;$$

在第二種情形,

$$\gamma = (i\ \ j\ \ k)(i\ \ j\ \ r) = (i\ \ k)(j\ \ r).$$

此時由於 $n \geq 5$, 在 $\{1, \ldots, n\}$ 中我們選擇 $s \notin \{i, j, k, r\}$, 而令 $\delta = (i\ k\ s) \in N$. 則由於 $\gamma \in N$ 且 N 在 A_n 中 normal, 故 $\delta \cdot \gamma \cdot \delta^{-1} \in N$. 然而 $\delta \cdot \gamma \cdot \delta^{-1} = (k\ s)(j\ r)$ 故得

$$\gamma \cdot (\delta \cdot \gamma \cdot \delta^{-1}) = (i\ \ k)(j\ \ r)(k\ \ s)(j\ \ r) = (i\ \ k\ \ s) \in N.$$

所以在此情形, N 中有一個 3-cycle.

若是 case 丙, γ 可寫成 $(i\ j\ k)(i\ s\ t)$. 在此情形我們得

$$\gamma = (i\ \ j\ \ k)(i\ \ s\ \ t) = (i\ \ s\ \ t\ \ j\ \ k).$$

故知 N 中有一個 5-cycle. 此時令 $\delta = (i\ s\ t) \in A_n$, 則 $\delta \cdot \gamma \cdot \delta^{-1} = (s\ t\ i\ j\ k) \in N$. 故得

$$\gamma^{-1} \cdot (\delta \cdot \gamma \cdot \delta^{-1}) = (k\ \ j\ \ t\ \ s\ \ i)(s\ \ t\ \ i\ \ j\ \ k) = (i\ \ t\ \ k) \in N.$$

所以在此情形, N 中有一個 3-cycle.

最後若是 case 丁, γ 可寫成 $(i\ j\ k)(r\ s\ t)$. 此時令 $\delta = (i\ j\ r) \in A_n$, 則 $\delta \cdot \gamma \cdot \delta^{-1} = (j\ r\ k)(i\ s\ t) \in N$. 故得

$$\gamma^{-1} \cdot (\delta \cdot \gamma \cdot \delta^{-1}) = (k\ \ j\ \ i)(t\ \ s\ \ r)(j\ \ r\ \ k)(i\ \ s\ \ t) = (i\ \ r\ \ j\ \ t\ \ k) \in N.$$

也就是說 N 中有一個 5-cycle. 此時用和上一個 (case 丙) 處理 5-cycle 相同的方法, 可得 N 中有一個 3-cycle.

由以上之結果知, 在任何情況下 N 中都有一個 3-cycle. 所以由 Lemma 3.4.25 知 $N = A_n$. □

當一個 group 它沒有 nontrivial proper normal subgroup 時, 我們稱這種 group 是 *simple group*. 若 G 是 abelian, 它所有的 subgroup 都是 normal subgroup, 所以此時若 G 又是 simple, 表示 G 沒有 nontrivial proper subgroup. 之前已知在這種情形 G 一定是 cyclic 且其個數一定是一質數. 不過在一般情況下, simple group 並不如其名那麼 "simple". Theorem 3.4.26 告訴我們當 $n \geq 5$ 時 A_n 是 simple group, 不過事實上 A_n 是蠻複雜的.