大學基礎代數

李華介

國立台灣師範大學數學系

Chapter 2

中級 Group 的性質

這一章中我們將介紹一些更進一步的 group 的理論, 包括 Lagrange's Theorem, Cauchy's Theorem for abelian groups 以及三個 isomorphism theorems.

2.1. 分類

一般來說要將一個集合分類必須符合以下三個要素. 第一個就是, 自己和自己是同類的; 另一要素是若甲和乙是同類的則乙也必須和甲是同類的; 最後一個要素是如果甲和乙同類且乙和丙同類, 則甲必須和丙同類. 很多同學應該知道這樣的分類同類間的關係稱之為 *equivalence relation*. 我們還是用數學的方法給 equivalence relation 正式的定義.

Definition 2.1.1. 若一集合 S 中我們用 $a \sim b$ 表示 a 和 b 是同類的, 則這樣的分類若符合以下性質我們稱之為 equivalence relation:

(equiv1): 對所有 $a \in S$, 我們都有 $a \sim a$ (reflexivity).

(equiv2): 若 $a \sim b$, 則 $b \sim a$ (symmetry).

(equiv3): 若 $a \sim b$ 且 $b \sim c$, 則 $a \sim c$ (transitivity).

有些同學可能會覺得奇怪既然 (equiv2) 說: 若 $a \sim b$ 則 $b \sim a$. 那麼再利用 (equiv3) 我們可得 $a \sim a$. 為什麼還要強調 (equiv1) 呢? 主要原因是 (equiv1) 強調是 S 中的任一元素 a 都須符合 $a \sim a$. 如果我們只要求 (equiv2) 和 (equiv3), 那麼如果 S 中有一元素 a 在 S 中找不到任何的元素 b 使得 $a \sim b$, 那麼 a 就不一定滿足 $a \sim a$ 了. 因此會造成有的元素有可能沒有被分類到. 而符合 equivalence relation 的分類就確保每一個元素都會被分到某一類 (不過有可能某一類中只有一個元素).

到底用 equivalence relation 分類有什麼好處呢? 首先當然是如前所說由 (equiv1) 可得每一個元素都會被分到某一類. 另外由 (equiv2) 和 (equiv3) 知兩個不同類的集合不會有交集; 這是因為如果 b 在 A 類且在 B 類中, 則在 A 類中的任一元素 a 因和 b 是同類的故 $a \sim b$ 而 B 類中的任一元素 c 因也和 b 同類故 $b \sim c$. 故由

(equiv2) 和 (equiv3) 知 $a \sim c$. 也就是說 A 中的所有元素和 B 中的所有元素都同類. 這和 A 與 B 是不同類的假設相矛盾。

這樣的分類到底有什麼好處呢? 它可以幫我們計算一個有限集合的個數. 事實上我們有以下的 Lemma.

Lemma 2.1.2. 假設 S 是一個有限集合, 且用一個 *equivalence relation* 將其分成 $C_1, \ldots, C_n$ 等不同的類別. 若 $|S|$ 及 $|C_i|$ 表示這些集合的元素的個數, 則

$$|S| = \sum_{i=1}^{n} |C_i|.$$

Proof. 由前面說明已知利用 (equiv2) 和 (equiv3) 可得: 當 $i \neq j$ 時, $C_i \cap C_j = \emptyset$. 也就是說這些 C_i 是兩兩不相交的. 再加上由 (equiv1) 知每個 S 中的元素都會落在某個 C_i 中, 所以 S 的元素的個數剛好是這些 $C_1, \ldots, C_n$ 的元素個數之和. □

這個 Lemma 2.1.2 和 group 會有什麼關係呢? 若 H 是 group G 的一個 subgroup, 我們可以利用 H 對 G 中的元素定義一種分類的方法. 當然我們希望這種分類法是一個 equivalence relation, 因此可以用 Lemma 2.1.2 來算出 G 的個數.

怎樣利用 H 來定一個 equivalence relation 呢? 我們定 $a \sim b$ 如果 $a^{-1} \cdot b \in H$. 也就是說如果 $a^{-1} \cdot b \in H$, 則我們就說 a 和 b 是同類的. 這樣的分類會符合 equivalence relation 的三要素嗎? 我們一個一個來檢查:

首先, 給訂任一 G 中的元素 a, 由於 $a^{-1} \cdot a = e$, 且 H 是 subgroup 所以 $e \in H$. 因此 $a^{-1} \cdot a \in H$. 也就是說 $a \sim a$. 這證明了 (equiv1).

再來, 如果 $a \sim b$, 也就是說 $a^{-1} \cdot b \in H$. 則因 H 是 subgroup, 由 $a^{-1} \cdot b \in H$ 可得

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

也就是說 $b \sim a$. 這證明了 (equiv2).

最後, 若 $a \sim b$ 且 $b \sim c$, 則 $a^{-1} \cdot b \in H$ 且 $b^{-1} \cdot c \in H$. 再由 subgroup 的封閉性 (SGP1), 我們可得

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

換句話說 $a \sim c$, 所以我們證了 (equiv3).

既然這個分類法是一個 equivalence relation. 由 Lemma 2.1.2, 如果 G 是一個 finite group, 我們只要想辦法算出這種分類法之下每一類的個數, 就可以算出 G 的個數.

2.2. Lagrange's Theorem

Lagrange 的定理告訴我們一個 finite group 和它的 subgroup 之間各數的關係. 我們想利用上一節的結果來計算, 所以必須要知道若用上節提到的分類法, 那麼每一類的元素個數有多少.

Lemma 2.2.1. 如果 G 是一個 *group,* H 是其 *subgroup.* 若利用 $a^{-1}\cdot b\in H$ 則 a 和 b 同類 $(a\sim b)$ 的方法來將 G 分類, 則和 a 同類的元素所成的集合為

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

倘若 H 是一個 *finite subgroup,* 則和 a 同類的元素的個數和 H 的元素個數一樣多.

Proof. 若 a 和 b 同類, 則表示 $a\sim b$. 故 $a^{-1}\cdot b=h$ 且 $h\in H$. 所以 $b=a\cdot h\in a\cdot H$. 反之, 若 $b\in a\cdot H$, 則表示在 H 中可找到一元素 h 使得 $b=a\cdot h$. 故 $a^{-1}\cdot b=h\in H$. 也就是說 a 和 b 同類.

前面提過要證明兩個集合有相同的元素個數最好的方法就是在兩集合中找到 1-1 且 onto 的函數. 因為和 a 同類的元素所成的集合是 $a\cdot H$, 所以我們只要找到一個函數從 H 送到 $a\cdot H$ 且證明這個函數是 1-1 且 onto 就可. 給定任一 $h\in H$, 我們可以定義 $f(h)=a\cdot h$. 這樣一來 $f:H\to a\cdot H$ 就是一個從 H 到 $a\cdot H$ 的函數. 給定任一 $y\in a\cdot H$, 由定義知必可找到一 $h\in H$ 使得 $y=a\cdot h$. 因此我們得 $f(h)=y$, 也就是說 f 是 onto. 假設 $h\neq h'$ 是 H 中任兩個相異元素, 則 $f(h)=a\cdot h$ 和 $f(h')=a\cdot h'$ 是 $a\cdot H$ 中兩相異元素. 這是因為如果 $a\cdot h=a\cdot h'$, 則兩邊同乘 a^{-1}, 可得 $h=h'$ 而與當初假設 $h\neq h'$ 矛盾. 這證明了 f 是一對一的, 也因此證得了 H 和 $a\cdot H$ 有相同的元素個數. □

現在如果 G 是一個 finite group 且 H 是其 subgroup, 其中 G 的 order 為 n, H 的 order 為 m. 如果用我們一直討論的分類方法利用 H 可將 G 分成 k 類, 由 Lemma 2.2.1 知每一類共有 m 個元素, 再由 Lemma 2.1.2 知 G 的個數 $n=m\cdot k$. 所以我們證得了以下 Lagrange's Theorem.

Theorem 2.2.2 (Lagrange)**.** 若 G 是一個 *finite group* 且 H 是其 *subgroup,* 其中 G 的 *order* 為 n, H 的 *order* 為 m, 則 $m\,|\,n$.

這裡要注意的是: 一般同學們最常犯的錯是以為 Lagrange's Theorem 的逆命題是對的. 其實不然! 也就是說若 G 的 order 為 n, 且 $m\,|\,n$, 並不表示一定存在一個 G 的 subgroup H 使得 H 的 order 為 m. 另外要注意的是: Lagrange's Theorem 只適用於 G 是一個 finite group. 若 G 的個數是無窮大時, 我們無從得知 H 個數的訊息. 此時 H 的 order 有可能為 ∞, 或是任何的正整數.

Lagrange's Theorem 有許多的應用我們先介紹一個特殊的狀況的應用, 更一般的狀況我們留到下一節討論.

Corollary 2.2.3. 若 G 是一個 *finite group* 且其 *order* 為 p, 其中 p 為一個質數. 則 G 為一個 *cyclic group,* 而且 G 中的任一元素除了 *identity* 以外皆可 *generates* G.

Proof. 我們複習一下: G 是一個 cyclic group 且 a generates G 表示 a 產生的 cyclic group $\langle a\rangle$ 就是 G. 今若 a 不是 identity, 則 $\langle a\rangle$ 的 order 必不等於 1, 因為已知 $\langle a\rangle$ 中必有 e 和 a 這兩個元素. 但由 Lagrange's Theorem (2.2.2) 知 $|\langle a\rangle|$ 一定是 $|G|=p$ 的一個因數. 但是 p 是個質數, 其因數只有 1 及 p. 故可得 $|\langle a\rangle|=p$. 既然 $\langle a\rangle$ 是 G 的 subgroup 且它們的個數又相等, 故得 $\langle a\rangle = G$. □

2.3. 元素的 order

前面定義過一個 group 的 order 為其元素的個數. 而一個 group 中的元素 a, 其產生的 cyclic group $\langle a\rangle$ 的 order 就稱為此元素 a 的 order. 我們記為 $\mathrm{ord}(a)$. 若 G 為一個 group 且 $a\in G$, 由 Lagrange's Theorem 知 $\mathrm{ord}(a)\,|\,|G|$. 因此若我們知 G 中元素的 order 或多或少就可知道 G 的 order 的一些訊息, 反之亦然.

以下的 Lemma 給我們一個明確的方法來計算一個元素的 order.

Lemma 2.3.1. 令 a 為一個 *group* G 中的元素, e 為 G 的 *identity.* 假設 $n\in\mathbb{N}$ 是最小的正整數使得 $a^n=e$, 則 $\mathrm{ord}(a)=n$.

Proof. 我們要證明當 n 是最小的正整數使得 $a^n=e$ 則 $\langle a\rangle$ 有 n 個元素. 事實上我們要證明 $\langle a\rangle=\{e,a,a^2,\ldots,a^{n-1}\}$. 首先回顧 $\langle a\rangle$ 中的元素都是 a^k, $k\in\mathbb{Z}$ 這種形式. 利用整數的餘數定理: 當 $n>1$ 時, 可以找到整數 h 和 r 使得 $k=h\cdot n+r$, 其中 $0\le r<n$. 因此

$$a^k=a^{h\cdot n+r}=(a^n)^h\cdot a^r=e\cdot a^r=a^r.$$

換句話說我們利用 $a^n=e$ 得到 $\langle a\rangle$ 中的元素可表為 a^r, $0\le r<n$ 這種形式, 也就是說 $\langle a\rangle=\{e,a,a^2,\ldots,a^{n-1}\}$. 但這並不表示 $\langle a\rangle$ 有 n 個元素, 除非我們知道它們都相異. 因此我們還得證明當 $0\le i<j<n$ 時, $a^i\neq a^j$. 別忘了我們尚未用到 n 是最小的這個性質. 如果 $0\le i<j<n$ 且 $a^i=a^j$, 則 $a^{j-i}=a^j\cdot a^{-i}=e$. 但 $j-i\in\mathbb{N}$ 且 $n>j-i$. 這和 n 是最小的正整數使得 $a^n=e$ 矛盾. 故 $a^j\neq a^i$. 也就是說 $\langle a\rangle$ 的 order 為 n. □

假設 a 的 order 為 n. 由 n 是最小的正整數使得 $a^n=e$ 這個性質知如果 $m\in\mathbb{N}$ 且 $a^m=e$, 則 $m\ge n$. 事實上我們可得到 m 與 n 更好的關係式.

Lemma 2.3.2. 令 a 為 *group* G 中的一元素. 若 $a^m=e$, 則 $\mathrm{ord}(a)\,|\,m$.

Proof. 假設 $\mathrm{ord}(a)=n$. 利用整數的餘數定理, 存在整數 h 及 r, 其中 $0\le r<n$ 使得 $m=n\cdot h+r$. 故得

$$a^m=a^{n\cdot h}\cdot a^r=e\cdot a^r=a^r.$$

也就是說 $a^r=e$. 如果 $r\neq 0$, 則 r 是一個比 n 還小的正整數使得 $a^r=e$. 此和 Lemma 2.3.1 相違背. 故知 $r=0$; 換句話說 n 可整除 m. □

當然了, 從若 $a^m = e$ 則 $n \mid m$ 這個性質我們可推得 n 是最小的正整數滿足 $a^n = e$. 所以整合 Lemma 2.3.1 及 Lemma 2.3.2, 當我們要說 $\mathrm{ord}(a) = n$ 時, 我們只要驗證:

(1) $a^n = e$.

(2) 若 $a^m = e$ 則 $n \mid m$.

下一個 Proposition 不但是一個很有用的定理, 而且其證明可以幫助我們了解前面提到如何驗證一個元素的 order 的方法.

Proposition 2.3.3. 令 a 為 *group* G 中的一元素. 若 $\mathrm{ord}(a) = n$, 則對於任意的整數 i,

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

Proof. 為了方便, 我們令 $d = \gcd(i, n)$. 欲證明 $\mathrm{ord}(a^i) = n/d$, 首先得證明 $(a^i)^{n/d} = e$. 事實上因為 d 是 i 的因數, i/d 是個整數. 再加上由假設 n 為 a 的 order, 故 $a^n = e$. 所以可得 $(a^i)^{n/d} = (a^n)^{i/d} = e$.

接下來我們須證明, 若 $(a^i)^m = e$ 則 $(n/d) \mid m$. 若 $(a^i)^m = e$, 即 $a^{mi} = e$. 故由 Lemma 2.3.2, 我們可得 $n \mid mi$. 但因 d 是 n 和 i 的最大公因數. 我們有 n/d 和 i/d 皆為整數且互質. 故由 $n \mid mi$ 可得 $(n/d) \mid m(i/d)$. 再由 n/d 和 i/d 互質, 得 $(n/d) \mid m$.

□

讓我們回到 Lagrange's Theorem 的應用. 若 G 是一個 finite group, 而 $a \in G$, 則 Lagrange's Theorem (2.2.2) 告訴我們說: $\langle a \rangle$ 的 order 整除 G 的 order. 也就是說若 a 的 order 為 m, G 的 order 為 n, 則存在 $r \in \mathbb{N}$ 使得 $n = m \cdot r$. 又因 a 的 order 為 m, 由 Lemma 2.3.1 知 $a^m = e$. 故 $a^n = a^{mr} = (a^m)^r = e$. 因此我們有以下重要的結果.

Corollary 2.3.4. 若 G 是一個 *finite group,* 且其 *order* 為 n. 令 $a \in G$ 是 G 中一元素. 則 $a^n = e$.

2.4. Normal Subgroups 和 Quotient Groups

當 H 是 G 的 subgroup 時, 前面介紹過我們可以用 $a^{-1} \cdot b \in H$ 的方法將 G 分類. 如果我們將同類的元素收集起來看成一個元素, 那麼這個新的集合的元素就明顯比 G 少多了. 如果能在這個新集合上定義一個運算和原來 G 的運算有關, 那麼這個小一點的集合或多或少能幫助我們了解一些有關 G 的性質. 怎樣來定這個運算呢? 給定 $a \in G$, 若 $\overline{a}$ 表示所有和 a 同類的元素所成的集合. 那麼要如何定 $\overline{a} \cdot \overline{b}$ 呢? 很自然的我們會希望定成 $\overline{a \cdot b}$. 也就是說我們希望和 a 同類的元素乘以和 b 同類的元素會和 $a \cdot b$ 同類. 一般來講這是不一定對的, 除非 H 有一些特性. 現在就讓我們談談 H 要有怎樣的特性才能達到我們的希望.

首先若 a 和 a' 同類, b 和 b' 同類; 也就是說 $a^{-1}\cdot a' = h_1 \in H$ 且 $b^{-1}\cdot b' = h_2 \in H$. 則 $a'\cdot b' = (a\cdot h_1)\cdot(b\cdot h_2)$. 要怎樣才能保證 $a\cdot b$ 和 $a'\cdot b'$ 同類呢? 也就是說

$$(a\cdot b)^{-1}\cdot(a'\cdot b') \in H?$$

事實上

$$(a\cdot b)^{-1}\cdot(a'\cdot b') = (b^{-1}\cdot a^{-1})\cdot(a\cdot h_1)\cdot(b\cdot h_2) = (b^{-1}\cdot h_1\cdot b)\cdot h_2.$$

所以要求 $a\cdot b$ 和 $a'\cdot b'$ 同類, 也就是要求 $(b^{-1}\cdot h_1\cdot b)\cdot h_2 \in H$. 又因 $h_2 \in H$, 這等同於要求 $b^{-1}\cdot h_1\cdot b \in H$. 但是別忘了, 我們希望這是對於任意的 $a \sim a'$ 和 $b \sim b'$ 都對, 所以這裡 b 可以是 G 中任意的元素, 同樣的 h_1 可以是 H 中的任意元素. 因此我們很自然的有下列的定義:

Definition 2.4.1. 若 H 是 G 的一個 subgroup 且 H 滿足對所有的 $a \in G$ 及 $h \in H$ 都有 $a^{-1}\cdot h\cdot a \in H$. 則稱 H 為 G 的一個 *normal subgroup*.

千萬要記得這裡我們要求對 G 中的所有元素都要符合這個性質. 如果將上面定義的 a 用 a^{-1} 替代, 則 normal 的條件會變成 $(a^{-1})^{-1}\cdot h\cdot a^{-1} = a\cdot h\cdot a^{-1} \in H$. 有的書用 $a\cdot h\cdot a^{-1} \in H$ 這個定義, 其實都是一樣的. 我們以後會因問題的方便性兩種替換選擇使用.

Remark 2.4.2. 對一個 group 我們若要提到其 normal 的性質, 則一定要確切的提到是在哪一個 group 之下是 normal 的. 同學經常會把以下的幾種情況搞混, 我們特別把它們列出來: 假設有三個 groups, N, H, G, 且 $N \subseteq H \subseteq G$.

(1) 如果已知 N 是 G 的 normal subgroup, 那麼 N 也會是 H 的 normal subgroup. 這是因為若 $n \in N, h \in H$, 則由於 h 也在 G 中, 所以由 N 在 G 中 normal 知 $h^{-1}\cdot n\cdot h \in N$.

(2) 如果已知 N 在 H 中 normal, 那麼 N 不一定在 G 中 normal. 這是因為 G 中可能有元素不在 H 中. 所以我們不能擔保所有 $g \in G$ 都會符合 $g^{-1}\cdot n\cdot g \in N$.

(3) 如果已知 H 在 G 中 normal, 那麼 N 不一定在 G 或 H 中 normal. 這是因為雖然可由 $n \in N$ 得到 $n \in H$. 不管如何, 利用 H 在 G 中 normal, 我們僅能得到 $g^{-1}\cdot n\cdot g \in H$, 而不是在 N.

(4) 如果已知 N 在 H 中 normal 且 H 在 G 中normal, 那麼 N 還是不一定能在 G 中 normal. 這利用和 (2), (3) 相同的解釋就可知.

有的書習慣用集合的方式來表示 normal. 也就是說 N 在 G normal 表示 $\forall a \in G$, $a^{-1}\cdot N\cdot a \subseteq N$. 這和我們前面用元素來定義是一樣的. 還有的書定義 normal subgroup 是要求: $\forall a \in G$, $a^{-1}\cdot N\cdot a = N$. 這樣的定義看似條件比較強不過其實是一樣的. 主要的原因是既然對於所有的 $a \in G$, $a^{-1}\cdot N\cdot a \subseteq N$. 所以在兩邊分別乘上 a 和 a^{-1} 得

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

也就是說 $N = a \cdot N \cdot a^{-1}$, 同理得 $a^{-1} \cdot N \cdot a = N$.

所以當你要證明一個 group N 是 G 的 normal subgroup 時, 你只要證明 $a \cdot N \cdot a^{-1} \subseteq N$ 就好, 然而若你已知 N 在 G 中 normal 時, 那你當然可以用 $a \cdot N \cdot a^{-1} = N$ 這個等式了. 畢竟條件越強越好用啊!

若 N 是 G 的 normal subgroup, 則用元素的寫法我們可以寫成: 對於所有 $g \in G$, $n \in N$ 都可找到 $n' \in N$ 使得 $g \cdot n = n' \cdot g$ (或是找到 $n'' \in N$ 使得 $n \cdot g = g \cdot n''$). 當然了若 G 是 abelian, 則當 $n' = n$ (或 $n'' = n$) 時, 上面的等式都對. 也就是說:

Lemma 2.4.3. 當 G 是一個 *abelian group* 時, 所有的 *subgroup* 都是 *normal subgroup*.

現在回到我們考慮 normal subgroup 的真正目的. 我們想利用 G 來創造另一個小一點的 group 來幫助我們了解 G. 給定一個 subgroup N 若我們考慮用前面的分類方法用 N 將 G 分類然後將同類的元素所成的集合看成一個新的元素, 那麼從集合的觀點來看這些新的元素所成的集合自然比原來 G 小. 例如前面在證明 Lagrange 定理時, 我們知道若 G 是 finite group 則可用 N 將 G 分成 $|G|/|N|$ 類. 所以在這情況下新的集合就只有 $|G|/|N|$ 個元素了. 然而若 N 是 G 的 normal subgroup 時, 前面提到我們就可以給這一個新的集合一個運算. 也就是說若 $\overline{a}$ 是與 a 同類的元素所成的集合, $\overline{b}$ 是與 b 同類的元素所成的集合, 則我們定 $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. (再次強調一定要是 normal subgroup 定出的運算才是 well defined. 否則和 a 同類的元素乘以和 b 同類的元素不一定和 $a \cdot b$ 同類.) 我們將說明這一個運算給了這個新的集合一個 group 的結構. 這個新的 group 我們稱之為 the *quotient group of* G *by* N (有的書稱作 *factor group*), 記作: G/N.

(GP1): 若 $\overline{a}, \overline{b} \in G/N$, 則由於 $a \cdot b \in G$ 故 $\overline{a \cdot b} \in G/N$. 也就是說 $\overline{a} \cdot \overline{b} \in G/N$.

(GP2): 我們要證明 $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$. 然而

$$(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a \cdot b} \cdot \overline{c} = \overline{(a \cdot b) \cdot c},$$

且

$$\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{b \cdot c} = \overline{a \cdot (b \cdot c)}$$

再加上 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ 所以等式成立.

(GP3): 甚麼會是 G/N 的 identity 呢? 若 e 是 G 的 identity, 則對所有的 $\overline{a} \in G/N$. 我們自然有 $\overline{a} \cdot \overline{e} = \overline{a \cdot e} = \overline{a}$. 同理 $\overline{e} \cdot \overline{a} = \overline{e \cdot a} = \overline{a}$. 所以 $\overline{e}$ 是 G/N 的 identity.

(GP4): 若 $\overline{a} \in G/N$ 甚麼會是 $\overline{a}$ 的 inverse 呢? 相信大家都可以猜到就是 $\overline{a^{-1}}$ 了. 我們驗證 $\overline{a} \cdot \overline{a^{-1}} = \overline{a \cdot a^{-1}} = \overline{e}$. 同理 $\overline{a^{-1}} \cdot \overline{a} = \overline{e}$. 所以 $\overline{a^{-1}}$ 就是 $\overline{a}$ 的 inverse. 我們可以記作 $(\overline{a})^{-1} = \overline{a^{-1}}$.

Example 2.4.4. Quotient group 的例子很多. 大家最常見的例子就是在整數用加法所成的 group 中的 quotient group. 例如 $5\mathbb{Z}$ 就是 $\mathbb{Z}$ 的一個 normal subgroup (別忘了 $\mathbb{Z}$ 是 abelian). 而 $\mathbb{Z}/5\mathbb{Z}$ 就是 the quotient group of $\mathbb{Z}$ by $5\mathbb{Z}$. 到底 $\mathbb{Z}/5\mathbb{Z}$ 是甚

麼呢? 比方說利用 $5\mathbb{Z}$ 來分類哪些整數和 1 同類呢? 照定義來看就是那些 $n \in \mathbb{Z}$ 使得 $1 \cdot (n)^{-1} \in 5\mathbb{Z}$. 錯! 別忘了我們是看加法群你必須把上式的 $\cdot$ 改成 $+$, 而 n^{-1} 改成 $-n$. 所以和 1 同類的就是那些整數符合 $1 - n \in 5\mathbb{N}$. 也就是除以 5 餘 1 的整數. 由此知 $\mathbb{Z}/5\mathbb{Z}$ 可以用 $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ 來表示. 其中 $\overline{0}$, 也就是所有 5 的倍數所成的集合, 是其 identity. 這就是大家在基礎數論學的 congruence.

2.5. Group Homomorphisms

在數學中要描繪兩種東西間的關係最好的方法就是利用函數 function. 當然並不是所有這兩東西間的函數都很重要. 例如我們只關心兩個 groups 間的 group 架構, 因此我們只對某種特殊的函數有興趣. 這種函數我們稱之為 *group homomorphism.*

Definition 2.5.1. 當 G, G' 是 groups 而 $\phi : G \to G'$ 是從 G 映射到 G' 的函數. 如果 ϕ 滿足對於所有 $a, b \in G$ 皆有 $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$, 則稱此函數 ϕ 是一個 group homomorphism.

要注意的是: 因為 $a, b \in G$, 所以這裡 $a \cdot b$ 是在 G 中的乘法; 而 $\phi(a), \phi(b) \in G'$, 所以 $\phi(a) \cdot \phi(b)$ 是在 G' 中的乘法. 簡單地說: 一個從 G 到 G' 的 group homomorphism 就是一個函數它能保持 G 和 G' 元素間的運算. 以下的 Lemma 就是說明這個觀點的一個很好的例子. 它告訴我們 group homomorphism 會把 identity 送到 identity, 把 inverse 送到 inverse.

Lemma 2.5.2. 設 G 和 G' 是 *groups* 且 e 和 e' 分別為其 *identity.* 若 ϕ 是一個從 G 映到 G' 的 *group homomorphism,* 則*:*

(1) $\phi(e) = e'$.

(2) 給定任意的 $a \in G$, $\phi(a^{-1}) = \phi(a)^{-1}$.

Proof. 由 Theorem 1.2.3 知: 要證明 $\phi(e)$ 是 G' 的 identity, 我們只要在 G' 中找到一元素 b 使得 $b \cdot \phi(e) = b$ 就可以 (再次強調我們不需證所有的 $g \in G'$ 都會使得 $g \cdot \phi(e) = g$). 其實我們只要找 $b = \phi(e) \in G'$ 就好了. 這樣一來,

$$b \cdot \phi(e) = \phi(e) \cdot \phi(e) = \phi(e \cdot e) = \phi(e) = b.$$

所以得證 $\phi(e)$ 是 G' 的 identity.

同樣的要證明 $\phi(a^{-1})$ 是 $\phi(a)$ 的 inverse, 我們只要證 $\phi(a^{-1}) \cdot \phi(a) = e'$ 就可. 然而

$$\phi(a^{-1}) \cdot \phi(a) = \phi(a^{-1} \cdot a) = \phi(e) = e'.$$

所以 $\phi(a^{-1}) = \phi(a)^{-1}$. □

一般的函數有兩個集合是很重要的: 一個是在對應域裡的值域(像); 另一個就是定義域裡的解集合(送到 0 的元素所成的集合). 同樣的在 group homomorphism 中這兩個集合也很重要. 一個稱為 *image*; 另一個稱為 *kernel*.

Definition 2.5.3. 若 $\phi : G \to G'$ 是一個 group homomorphism, 則

$$\mathrm{im}(\phi) = \{\phi(a) \in G' \,|\, a \in G\}$$

稱為 ϕ 的 *image.*

$$\ker(\phi) = \{a \in G \,|\, \phi(a) = e'\},$$

稱為 ϕ 的 *kernel.*

從定義可知 $\mathrm{im}(\phi)$ 是 G' 的一個子集合, 而 $\ker(\phi)$ 是 G 的子集合. 事實上它們有很好的性質.

Lemma 2.5.4. 若 $\phi : G \to G'$ 是一個 *group homomorphism,* 則 $\mathrm{im}(\phi)$ 是 G' 的 *subgroup,* 而 $\ker(\phi)$ 是 G 的 *normal subgroup.*

Proof. 我們可以利用定義直接證 $\mathrm{im}(\phi)$ 和 $\ker(\phi)$ 分別是 G' 和 G 的 subgroup. 我們這裡想直接利用 Lemma 1.3.4 來證.

若 $\phi(a), \phi(b) \in \mathrm{im}(\phi)$, 其中 $a, b \in G$, 則利用 Lemma 2.5.2 我們知 $\phi(b)^{-1} = \phi(b^{-1})$. 故

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

又因 $a \cdot b^{-1} \in G$, 故 $\phi(a) \cdot \phi(b)^{-1} \in \mathrm{im}(\phi)$. 另外若 $a, b \in \ker(\phi)$, 即 $\phi(a) = \phi(b) = e'$, 則

$$\phi(a \cdot b^{-1}) = \phi(a) \cdot \phi(b)^{-1} = e' \cdot e' = e'.$$

也就是說 $a \cdot b^{-1} \in \ker(\phi)$. 由以上二式知 $\mathrm{im}(\phi)$ 和 $\ker(\phi)$ 分別是 G' 和 G 的 subgroup.

最後我們證 $\ker(\phi)$ 事實上是 G 的 normal subgroup. 也就是要證明: 對於所有的 $g \in G$, 我們都有 $g \cdot \ker(\phi) \cdot g^{-1} \subseteq \ker(\phi)$. 換句話說: 若 $a \in \ker(\phi)$, 則我們要證 $g \cdot a \cdot g^{-1} \in \ker(\phi)$. 然而

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

再利用 $\phi(a) = e'$ 及 $\phi(g^{-1}) = \phi(g)^{-1}$, 我們可得

$$\phi(g \cdot a \cdot g^{-1}) = \phi(g) \cdot e' \cdot \phi(g)^{-1} = e'.$$

故 $g \cdot a \cdot g^{-1} \in \ker(\phi)$. □

Definition 2.5.5. 令 $\phi : G \to G'$ 是一個 group homomorphism:

(1) 若 ϕ 是 onto, 則稱之為 *epimorphism.*

(2) 若 ϕ 1-1, 則稱之為 *monomorphism.*

(3) 若 ϕ 是 1-1 且 onto, 則稱之為 *isomorphism.*

當然了我們可以用 $\mathrm{im}(\phi)$ 來判定 ϕ 是否為 epimorphism. 事實上若 $\mathrm{im}(\phi) = G'$, 則 ϕ 為 onto, 故為 epimorphism. 我們也可以用 $\ker(\phi)$ 來判定 ϕ 是否為 monomorphism.

Lemma 2.5.6. 已知 $\phi : G \to G'$ 是一個 *group homomorphism,* 則 ϕ 是一個 *monomorphism* 若且為若 $\ker(\phi) = \{e\}$.

Proof. 假設 ϕ 是 monomorphism (即 1-1). 若 $g \in \ker(\phi)$, 則由 Lemma 2.5.2 知 $\phi(g) = \phi(e) = e'$. 但若 $g \neq e$, 則由 ϕ 是 1-1 知 $\phi(g) \neq \phi(e)$. 故得 $g = e$, 也就是說 $\ker(\phi) = \{e\}$.

反之, 假設 $\ker(\phi) = \{e\}$. 若存在 $g_1 \neq g_2$ 使得 $\phi(g_1) = \phi(g_2)$, 則

$$\phi(g_1 \cdot g_2^{-1}) = \phi(g_1) \cdot \phi(g_2)^{-1} = e'.$$

也就是說 $g_1 \cdot g_2^{-1} \in \ker(\phi)$. 但這代表 $g_1 \cdot g_2^{-1} = e$, 即 $g_1 = g_2$, 和當初假設 $g_1 \neq g_2$ 矛盾. 換句話說若 $g_1 \neq g_2$ 則 $\phi(g_1) \neq \phi(g_2)$. 這告訴我們 ϕ 是 1-1 的. □

這個定理告訴我們: 要檢查一個 group homomorphism 是否為 1-1, 只要檢查其 kernel 是否為 identity 即可. 不過千萬要切記, 我們是在假設 ϕ 是一個 group homomorphism 的前題之下才有這個結果. 你不可以拿到一個函數馬上就檢查其 kernel 為 identity 然後就下斷語說它是 1-1. 除非你已先知其為一個 group homomorphism. 最簡單的反例就是若 $f : \mathbb{R} \to \mathbb{R}$ 是一個實數到實數的函數, 你不能因為 $x = 0$ 是 $f(x) = 0$ 的唯一解就說 $f(x)$ 是 1-1.

有時候兩個 groups 的元素看起來是不一樣的不過它們在結構上是相同的. 在代數的眼光中不應該把它們看成是不同的 groups. 不過怎樣來判定兩個 groups 結構相同呢? 如果兩個 groups G 和 G' 間你可以找到一個 group homomorphism 是 isomorphism (即 1-1 且 onto), 則我們稱 G 和 G' 這兩個 group 是 *isomorphic*, 記為: $G \simeq G'$. 意思是我們把它們看作是同樣的 group. 這樣的看法是合理的: 因為 1-1 和 onto 表示 G 和 G' 看成集合是一樣的, 在加上 group homomorphism 保持它們 group 的結構, 所以我們把它們看作是一樣的 group.

這樣的看法在 finite group 之下大致上同學們就知道兩個 groups 若是 isomorphic 則它們的 order (元素個數) 要一樣. 不過要注意的是若兩個 groups 其 order 相同不見得它們就 isomorphic. 不管如何若兩個 groups 其 order 不同則它們一定不 isomorphic.

當考慮 infinite group 情況複雜多了; 主要是此時我們無法算個數. 這時有很多特殊現象發生, 例如一個 group 的 subgroup 可以和它 isomorphic. 我們有以下的簡單例子:

Example 2.5.7. 考慮 $\mathbb{Z}$ 是一個加法之下的 group, 則所有偶數所成的集合 $2\mathbb{Z}$ 是其 subgroup. 考慮 $\phi : \mathbb{Z} \to 2\mathbb{Z}$ 是一個 group homomorphism 定義成: $\phi(n) = 2n$. 很容易看出來 ϕ 是一個 isomorphism. 所以 $\mathbb{Z}$ 和 $2\mathbb{Z}$ 是 isomorphic.

其實我們可以證得 $\mathbb{Z}$ 中所有的 nontrivial subgroup 都和 $\mathbb{Z}$ isomorphic. 不過我們別擔心太多 infinite group 因為前面已提過了, 在大學代數課中我們只要關心 finite group 就好了.

最後要強調的是: G 和 G' 是 isomorphic 表示在 G 和 G' 之間可以找到一個 isomorphism. 這並不表示 G 和 G' 間所有的 homomorphism 都是 isomorphism. 同學們常常誤解這一點以致於當碰到要你證明 G 和 G' 不是 isomorphic 時, 有的同學會在 G 和 G' 中找到一個 homomorphism 不是 1-1 及 onto 就斷言 G 和 G' 不是 isomorphism. 這是大錯特錯的!

2.6. 三個 Isomorphism 定理

給定 G 和 G' 要說明它們是 isomorphic 時, 若想真正找到它們之間一個具體的 isomorphism 一般來說並不容易. 在這一節中我們將介紹三個定理來幫助我們確認 $G \simeq G'$ 而不必真正找到一個 isomorphism. 別害怕! 雖然是三個定理, 不過後兩個定理可以利用第一個定理輕鬆推得. 所以大家務必要學好第一個 isomorphism 定理.

Theorem 2.6.1 (First Isomorphism Theorem)**.** *若 $\phi : G \to G'$ 是一個 group homomorphism,* 則

$$G/\ker(\phi) \simeq \mathrm{im}(\phi).$$

Proof. 首先我們回顧一下: 因 $\phi : G \to G'$ 是一個 group homomorphism, 由 Lemma 2.5.4 知 $\mathrm{im}(\phi)$ 是 G' 的 subgroup, 而 $\ker(\phi)$ 是 G 的 normal subgroup. 所以要證得這一個定理, 我們必須先在 $G/\ker(\phi)$ 這一個 quotient group 和 $\mathrm{im}(\phi)$ 這個 group 之間找到一個函數. 再說明這個函數是 group homomorphism, 最後再驗證它是 1-1 且 onto.

$G/\ker(\phi)$ 和 $\mathrm{im}(\phi)$ 長甚麼樣子我們都不知道, 如何能無中生有創造出一個函數呢? 當然不可能無中生有! 我們可以用已經有的函數來創造它. 別忘了在假設中有一個 ϕ, 我們可以利用 ϕ 製造以下的函數:

$$\psi : G/\ker(\phi) \to \mathrm{im}(\phi); \quad \overline{a} \mapsto \phi(a), \ \forall \overline{a} \in G/\ker(\phi).$$

具體來說 ψ 是把和 a 同類的元素送到 $\phi(a)$ 這個值. 先別急著驗證 ψ 是一個 group homomorphism. 你確定 ψ 是一個'好函數' (well defined function) 嗎? 別忘了要成為一個好函數必須有以下兩個要素:(1) 每一個定義域裡的元素都必須送到對應域裡; (2) 不可以"一對多": 也就是同一個元素不可以有兩種送法. 關於 (1) 我們的函數 ψ 是 O.K. 的. 因為每個定義域 (即 $G/\ker(\phi)$) 裡的元素都是長 $\overline{a}$ 這個樣子, 其中 $a \in G$. 所以 ψ 把 $\overline{a}$ 送到 $\phi(a)$. 依定義 $\phi(a)$ 當然在對應域 $\mathrm{im}(\phi)$ 內. 至於 (2) 就需要驗證了. 這是因為 $G/\ker(\phi)$ 內的元素並沒有唯一的方法用 G 中的元素表示出來. 也就是說在 G 中可以找到兩個不同的元素 a, b 使得 $\overline{a}$ 和 $\overline{b}$ 在 $G/\ker(\phi)$ 中是相同的. 所以要說明 ψ 不是一對多, 我們必須說明 $\phi(a) = \phi(b)$. 雖然 $a \neq b$, 不過由 $\overline{a} = \overline{b}$ 知 a 和 b 在以 $\ker(\phi)$ 這個 subgroup 的分類下是同類的. 別忘了 a 和 b 同類表示 $a^{-1} \cdot b \in \ker(\phi)$. 也就是說 $\phi(a^{-1} \cdot b) = e'$. 再利用 ϕ 是 group homomorphism 的假設, 我們得

$$\phi(a)^{-1} \cdot \phi(b) = \phi(a^{-1} \cdot b) = e'.$$

等式兩邊乘上 $\phi(a)$, 可得 $\phi(a) = \phi(b)$. 所以我們製造的 ψ 是一個 well defined function.

接下來證 ψ 是一個 group homomorphism: 這不難, 只要記住 $G/\ker(\phi)$ 中的乘法是定義成: $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. 因此對任意的 $\overline{a}, \overline{b} \in G/\ker(\phi)$, 我們有

$$\psi(\overline{a} \cdot \overline{b}) = \psi(\overline{a \cdot b}) = \phi(a \cdot b).$$

另一方面因為 ϕ 是 group homomorphism, 所以

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b) = \psi(\overline{a}) \cdot \psi(\overline{b}).$$

結合以上二式, 我們可得 $\psi(\overline{a} \cdot \overline{b}) = \psi(\overline{a}) \cdot \psi(\overline{b})$.

證明 ψ 是 onto 純粹是定義: 給定任意元素 $y \in \mathrm{im}(\phi)$, 依定義知存在 $x \in G$ 使得 $y = \phi(x)$. 因此我們可找 $\overline{x} \in G/\ker(\phi)$ 代入 ψ 得 $\psi(\overline{x}) = \phi(x) = y$. 因此 ψ 是 onto.

既然 ψ 是 group homomorphism, 我們可以利用 Lemma 2.5.6: 也就是證明 $\ker(\psi)$ 是 $G/\ker(\phi)$ 的 identity. 別忘了 $G/\ker(\phi)$ 的 identity 是 $\overline{e}$. 假設 $\overline{x} \in \ker(\psi)$, 即 $\psi(\overline{x}) = e'$, 其中 e' 是 G' 的 identity. 但是由 ψ 的定義: $\psi(\overline{x}) = \phi(x)$, 故知 $x \in \ker(\phi)$. 然而 G 中元素用 $\ker(\phi)$ 來分類的話 x 和 e 是同類的 (因 $e^{-1} \cdot x = x \in \ker(\phi)$). 故在 $G/\ker(\phi)$ 中 $\overline{x} = \overline{e}$.

總結: 我們證得了 ψ 是一個從 $G/\ker(\phi)$ 到 $\mathrm{im}(\phi)$ 的 isomorphism. 所以 $G/\ker(\phi) \simeq \mathrm{im}(\phi)$. □

當然了如果定理中的 ϕ 是 onto. 那麼我們知 $\mathrm{im}(\phi) = G'$. 因此我們有以下的引理:

Corollary 2.6.2. *若 $\phi : G \to G'$ 是一個 group epimorphism,* 則

$$G/\ker(\phi) \simeq G'.$$

First Isomorphism Theorem 告訴我們甚麼呢? 如果有一個 group G, 而 N 是其 normal subgroup. 則當我們要證明另一個 group G' 和 G/N 是 isomorphic 時. 我們不必辛苦的去找 G/N 和 G' 間的 isomorphism. 我們只要去找到一個 G 到 G' 的 epimorphism, ϕ, 如果又剛好 $\ker(\phi) = N$. 那麼由 First Isomorphism Theorem 我們就可知 $G/N \simeq G'$ 了.

讓我們就利用證明第二個 isomorphism 定理來說明 First Isomorphism Theorem 的妙用吧! 給定一 group G, 若 H, N 是 G 的 subgroups, 考慮以下之集合:

$$H \cdot N = \{h \cdot n \,|\, h \in H, n \in N\}.$$

因為 H 和 N 都在 G 中所以 $H \cdot N$ 當然是 G 的一個子集合. 不過它不一定是 G 的 subgroup 喔! 主要的問題出在封閉性. 在 $H \cdot N$ 中任取兩元素, $h \cdot n$ 和 $h' \cdot n'$, 其中 $h, h' \in H$, $n, n' \in N$. 則 $(h \cdot n) \cdot (h' \cdot n')$ 不一定可以寫成一個 H 中的元素乘上一個

N 中的元素這樣的形式. 不過若 H 和 N 其中一個是 G 的 normal subgroup, 那麼 $H \cdot N$ 就是 G 的 subgroup 了. 我們就把這個事實寫成 Lemma 吧!

Lemma 2.6.3. *若 H 是 G 的 subgroup 且 N 是 G 的 normal subgroup. 則 $H \cdot N = N \cdot H$ 且是 G 的 subgroup.*

Proof. 因為 N 是 G 的 normal subgroup, 故因 $H \subseteq G$, 對於所有 $h \in H$ 及 $n \in N$, $h \cdot n \cdot h^{-1} \in N$. 換句話說存在 $n' \in N$ 使得 $h \cdot n \cdot h^{-1} = n'$. 因此 $h \cdot n = n' \cdot h$. 由此可得 $H \cdot N \subseteq N \cdot H$. 同理可得 $N \cdot H \subseteq H \cdot N$.

利用以上的結果, 前面所提的封閉性就可以解決了. 因為存在 $n'' \in N$ 使得 $h' \cdot n' = n'' \cdot h'$ 故

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

又因 $n \cdot n'' \in N$, 故存在 $\hat{n} \in N$ 使得 $(n \cdot n'') \cdot h' = h' \cdot \hat{n}$. 故

$$(h \cdot n) \cdot (h' \cdot n') = (h \cdot h') \cdot \hat{n} \in H \cdot N.$$

反元素的存在也可用相同的看法: 若 $h \cdot n \in H \cdot N$, 則

$$(h \cdot n)^{-1} = n^{-1} \cdot h^{-1} \in N \cdot H.$$

又 $N \cdot H = H \cdot N$, 故 $(h \cdot n)^{-1} \in H \cdot N$. □

現在讓我們看看第二個 isomorphism 定理在談甚麼?

Theorem 2.6.4 (Second Isomorphism Theorem)**.** *若 H 是 G 的 subgroup 且 N 是 G 的 normal subgroup. 則 $H \cap N$ 是 H 的 normal subgroup, 且*

$$H/(H \cap N) \simeq (H \cdot N)/N.$$

Proof. 雖然定理提到 $H \cap N$ 是 H 的 normal subgroup, 不過我們先不證它, 而直接用 first isomorphism 定理, normal subgroup 的部分會自然成立. 另外要注意的是定理中有另一個 quotient group $(H \cdot N)/N$. 前面提到這是一個 group 非得要 N 在 $H \cdot N$ 中 normal, 為甚麼定理不談 N 在 $H \cdot N$ 中 normal 呢? 學代數到現在你應該了解這是很 trivial 的事實了. 因為 H 中有 identity 故對任意的 $n \in N$ 皆可寫成 $n = e \cdot n \in H \cdot N$. 因此得 $N \subseteq H \cdot N$. 換句話說 H 是 $H \cdot N$ 的 subgroup. 那為甚麼 normal? 既然 N 在 G 中 normal, 當然對任意的元素 $g \in H \cdot N \subseteq G$ 都有 $g \cdot N \cdot g^{-1} = N$ 了.

怎麼用 first isomorphism 定理呢? 前面提到你要證明一個 quotient group 和另一個 group 是 isomorphism 時, 可以先不管 quotient group 中那個在底下的 normal subgroup. 在目前的情況我們有兩種選擇: (1) 從 H 到 $(H \cdot N)/N$ 的 homomorphism; (2) 從 $H \cdot N$ 到 $H/(H \cap N)$ 的 homomorphism. 你會選哪一個呢? 當然是 (1) 了! 主要原因不只是 (2) 中的 $H \cap N$ 在 H 中 normal 還沒證. 更重要的是從 H 到

$(H\cdot N)/N$ 的 homomorphism 比從 $H\cdot N$ 到 $H/(H\cap N)$ 的 homomorphism 更自然更好找. (為甚麼呢? 只能說是憑感覺吧!)

讓我們先找一個從 H 到 $(H\cdot N)/N$ 的函數吧! 因為 H 是 $H\cdot N$ 的 subgroup, 我們有一個很自然的映射把 H 的元素送到 $H\cdot N$: 也就是把 H 中的元素乖乖的原封不動的放到 $H\cdot N$ 中. 即 $\iota : H \to H\cdot N$ 其中 $\iota(h) = h$. 又 N 在 $H\cdot N$ 中 normal, 我們又有一個很自然的可將 $H\cdot N$ 的元素用 N 分類的函數. 即 $\pi : H\cdot N \to (H\cdot N)/N$ 其中對所有的 $g \in H\cdot N$ 我們有 $\pi(g) = \overline{g}$. 將 π 和 ι 合成, 我們自然有一個函數

$$\phi = \pi\circ\iota : H \to (H\cdot N)/N,$$

其中對所有的 $h \in H$ 我們有

$$\phi(h) = \pi(\iota(h)) = \overline{h}.$$

現在要證 ϕ 是一個 group homomorphism. (我們不必證 ϕ 是 well defined, 這是因為 ϕ 這個函數'明明白白'的把 h 送到 $\overline{h}$ 這一個元素. 沒有前面那種一對多的可能.) 事實上對任意的 $h, h' \in H$, 我們有

$$\phi(h\cdot h') = \overline{h\cdot h'} = \overline{h}\cdot\overline{h'} = \phi(h)\cdot\phi(h').$$

接下來證 ϕ 是 onto. 任意的 $H\cdot N$ 中的元素可寫成 $h\cdot n$, 其中 $h \in H$, $n \in N$. 所以任意的 $(H\cdot N)/N$ 中的元素都可寫成 $\overline{h\cdot n}$. 但是 $\overline{h\cdot n} = \overline{h}\cdot\overline{n}$. 別忘了我們是用 N 來分類所以 N 中的元素都和 identity 同類. 也就是說 $\overline{n} = \overline{e}$. 因此 $\overline{h\cdot n} = \overline{h}$. 由此知任意 $(H\cdot N)/N$ 中的元素 $\overline{h\cdot n}$ 我們都可找 $h \in H$ 使得 $\phi(h) = \overline{h} = \overline{h\cdot n}$. 因此 ϕ 是 onto.

既然 ϕ 是一個從 H 到 $(H\cdot N)/N$ 的 epimorphism, 我們可以用 First Isomorphism Theorem (Corollary 2.6.2) 得到

$$H/\ker(\phi) \simeq (H\cdot N)/N.$$

甚麼是 $\ker(\phi)$ 呢? 依定義 $\ker(\phi)$ 是 H 中的元素 h 使得 $\phi(h)$ 是 $(H\cdot N)/N$ 的 identity, $\overline{e}$. 也就是說 $\phi(h) = \overline{h} = \overline{e}$. 別忘了 $(H\cdot N)/N$ 中的元素是對 N 分類, 故 $\overline{h} = \overline{e}$ 表示 h 和 e 同類, 也就是說 $e^{-1}\cdot h = h \in N$. 由此知 $\ker(\phi)$ 的元素既要在 H 中也要在 N 中; 換句話說 $\ker(\phi) \subseteq H\cap N$. 反之若 $a \in H\cap N$, 則因 $a \in N$ 得 $\phi(a) = \overline{a} = \overline{e}$. 故 $H\cap N \subseteq \ker(\phi)$. 由此知 $\ker(\phi) = H\cap N$. 因此我們由 Lemma 2.5.4 知 $H\cap N$ 是 H 的 normal subgroup 也由 First Isomorphism Theorem 知

$$H/(H\cap N) \simeq (H\cdot N)/N.$$

□

相信大家已經看出 First Isomorphism Theorem 的妙用了. 讓我們再用它來證第三個 isomorphism 定理吧!

Theorem 2.6.5 (Third Isomorphism Theorem)**.** 若 $\phi : G \to G'$ 是一個 *group epimorphism.* 假設 N' 是 G' 的一個 *normal subgroup.* 令

$$N = \{a \in G \,|\, \phi(a) \in N'\}.$$

則 N 是 G 的 *normal subgroup* 且

$$G/N \simeq G'/N'.$$

Proof. 令 $\pi : G' \to G'/N'$ 是 G' 對 N' 來分類的函數. 如前一定理的證明我們可定 $\psi = \pi \circ \phi : G \to G'/N'$. 也就是說 $\psi(a) = \overline{\phi(a)}, \forall\, a \in G$.

由 ϕ 是 group homomorphism 知

$$\psi(a \cdot b) = \overline{\phi(a \cdot b)} = \overline{\phi(a) \cdot \phi(b)} = \overline{\phi(a)} \cdot \overline{\phi(b)} = \psi(a) \cdot \psi(b).$$

故 ψ 是一個從 G 到 G'/N' 的 group homomorphism.

任意 G'/N' 的元素都可寫成 $\overline{g}$ 其中 $g \in G'$ 這種形式. 但因 ϕ 是 onto, 故存在 $a \in G$ 使得 $\phi(a) = g$. 所以

$$\psi(a) = \overline{\phi(a)} = \overline{g}.$$

因此 ψ 也是 onto. (其實若同學了解一些合成函數的性質, 馬上可以利用兩個 onto 的函數其合成函數也是 onto 知 ψ 是 onto.)

既然知 $\psi : G \to G'/N'$ 是一個 epimorphism, 我們再次用 First Isomorphism Theorem 知

$$G/\ker(\psi) \simeq G'/N'.$$

甚麼是 $ker(\psi)$ 呢? 若 $a \in \ker(\psi)$ 即 $\psi(a) = \overline{\phi(a)} = \overline{e'}$, 其中 e' 是 G' 的 identity. 也就是說 $\phi(a)$ 和 e' 在用 N' 的分類下是同類的. 所以 $\phi(a) \in N'$. 由 N 的定義知, 這表示 $a \in N$. 故 $\ker(\psi) \subseteq N$. 另外若 $a \in N$, 則 $\phi(a) \in N'$ 故在 G'/N 中 $\psi(a) = \overline{\phi(a)} = \overline{e'}$, 因此 $a \in \ker(\psi)$. 得 $N \subseteq \ker(\psi)$. 也就是說 $\ker(\psi) = N$ 且 N 是 G 的 normal subgroup.

□

2.7. Correspondence Theorem

既然 group homomorphism 保持了兩 group 間乘法的運算結構. 那麼這兩個 group 在某種程度來說應該有些關係. Correspondence Theorem 就是描繪這種關係.

Theorem 2.7.1 (Correspondence Theorem)**.** 若 $\phi : G \to G'$ 是一個 *group epimorphism.* 若 H' 是 G' 的 *subgroup* 且令

$$H = \{a \in G \,|\, \phi(a) \in H'\},$$

則 H 是 G 的一個 *subgroup* 且 $H \supseteq \ker(\phi)$. 另外若令

$$\phi(H) = \{\phi(a) \,|\, a \in H\},$$

則 $\phi(H) = H'$ 且

$$H/\ker(\phi) \simeq H'.$$

如果又假設 H' 是 G' 的 *normal subgroup.* 則前面所定的 H 也會是 G 的 *normal subgroup.*

Proof. 首先先證 H 是一個 subgroup of G. 若 $a, b \in H$, 我們要證明 $a \cdot b \in H$ 且 $a^{-1} \in H$. 由定義知 $a, b \in H$ 表示 $\phi(a) \in H'$ 且 $\phi(b) \in H'$, 故 $\phi(a) \cdot \phi(b) \in H'$. 又因 ϕ 是 group homomorphism, 故 $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$. 因此 $\phi(a \cdot b) \in H'$, 也就是說 $a \cdot b \in H$. 另外又因 $\phi(a) \in H'$ 故 $\phi(a)^{-1} \in H'$, 再加上 $\phi(a^{-1}) = \phi(a)^{-1}$, 可知 $\phi(a^{-1}) \in H'$. 故 a^{-1} 也在 H 中. (注意這個部分的證明只用到 ϕ 是 group homomorphism, 並不需要 onto.)

若 $a \in \ker(\phi)$, 則 $\phi(a) = e'$. 因 e' 是 G' 的 identity 且 H' 是 G' 的 subgroup, 當然 $e' \in H'$. 也就是說 $\phi(a) \in H'$, 故 $a \in H$. 所以 $\ker(\phi) \subseteq H$. (這部分的證明也不需 epimorphism.)

現在證 $\phi(H) = H'$. $\phi(H) \subseteq H'$ 是容易的. 主要是因 $\phi(H)$ 的元素都是 $\phi(a)$ 這種形式, 其中 $a \in H$. 由定義 $a \in H$, 表示 $\phi(a) \in H'$. 故 $\phi(H)$ 的元素都落在 H' 中. 很多同學都會認為 H' 的元素也會在 $\phi(H)$ 中; 一般這是不一定對的. 因為在一般的情況 $b \in H'$ 不代表有元素 $a \in G$ 使得 $\phi(a) = b$. 這裡我們就要用到 onto 的性質了. 因為 ϕ 是 onto 故對任意 $b \in G'$, 當然可以找到 $a \in G$ 使得 $\phi(a) = b$. 現在若 $b \in H'$ 那當然 $b \in G'$ 故可找到 $a \in G$ 使得 $\phi(a) = b$. 既然 $\phi(a) = b \in H'$, 這一個 a 也就在 H 中了. 所以 $b = \phi(a) \in \phi(H)$, 也就是說 $H' \subseteq \phi(H)$. 由此得證 $H' = \phi(H)$.

$\phi(H) = H'$ 告訴我們 ϕ 這個函數若限制在 H 中來看是把 H onto 送到 H'. ϕ 對 G 中所有的元素來看是 group homomorphism, 那限制在 H 中當然是 group homomorphism. 而 ϕ 限制在 H 中來看它的 kernel 會是甚麼呢? 當然是在原本的 $\ker(\phi)$ 中也在 H 中的元素. 也就是 $\ker(\phi) \cap H$. 但已知 $\ker(\phi) \subseteq H$ 故 $\ker(\phi) \cap H = \ker(\phi)$. 故由 First Isomorphism Theorem 知

$$H/\ker(\phi) \simeq H'.$$

別忘了在 Theorem 2.6.5 已證過: 若 H' 在 G' 中 normal 則 H 在 G 中 normal. 我們這裡再給一個一般的證明(因為這不需用到 ϕ 是 onto.) 我們要證明若 $a \in H$ 對任意的 $g \in G$ 皆有 $g \cdot a \cdot g^{-1} \in H$. 要驗證 $g \cdot a \cdot g^{-1}$ 有沒有在 H 當然就是帶入 ϕ 看看是否送到 H'. 然而

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

再因 $\phi(g) \in G'$, $\phi(a) \in H'$ 及 H' 是 G' 的 normal subgroup, 我們有

$$\phi(g) \cdot \phi(a) \cdot \phi(g)^{-1} \in H'.$$

故 $\phi(g \cdot a \cdot g^{-1}) \in H'$, 也就是說 $g \cdot a \cdot g^{-1} \in H$. 所以 H 是 G 的 normal subgroup. □

再次強調這個定理中除了 $\phi(H) = H'$ 及 $H/\ker(\phi) \simeq H'$ 需用到 ϕ 是 onto 外, 其他性質並不需 onto 的假設.

Remark 2.7.2. Correspondence Theorem 告訴我們說若 $\phi : G \to G'$ 是一個 epimorphism, 則在 G' 中任選一個 subgroup H' 都可在 G 中找到一個 subgroup H 使得 $\phi(H) = H'$, 而且 $\ker(\phi) \subseteq H$. 其實在 G 中符合 $\phi(H) = H'$ 及 $\ker(\phi) \subseteq H$ 的 subgroup 是唯一的. 假設 G 中有另一個 subgroup N 符合 $\phi(N) = H'$ 及 $\ker(\phi) \subseteq N$. 則對於所有 $a \in N$, 因 $\phi(a) \in \phi(N) = H'$, 故由假設 $\phi(H) = H'$ 知在 H 中必存在一元素 b 使得 $\phi(b) = \phi(a)$. 換句話說 $\phi(a) \cdot \phi(b)^{-1} = e'$. 由此得 $\phi(a \cdot b^{-1}) = e'$. 也就是說 $a \cdot b^{-1} \in \ker(\phi)$. 由此知 $a \in \ker(\phi) \cdot b$. 別忘了 $\ker(\phi) \subseteq H$ 且 $b \in H$ 故 $\ker(\phi) \cdot b \subseteq H$. 所以 $a \in H$, 也就是說 $N \subseteq H$. 用同樣的方法 (將 H 和 N 角色互換) 可得 $H \subseteq N$. 所以 $H = N$. 由上知真正的 Correspondence Theorem 是說:

若 $\phi : G \to G'$ 是一個 epimorphism, 則對於 G' 中任一 subgroup H', 在 G 中皆 '存在' "唯一" 的 subgroup H 使得 $\phi(H) = H'$ 且符合 $\ker(\phi) \subseteq H$.

不過在大學的代數中我們只要用到存在性而已, 所以我們不去強調唯一性.

Correspondence Theorem 最常用的情況是當 N 是 G 的一個 normal subgroup, 而 ϕ 是 G 到 G/N 的 group homomorphism 其中對任意的 $a \in G$, 定義 $\phi(a) = \overline{a}$.

Corollary 2.7.3. 假設 G 是一個 *group* 且 N 是 G 的一個 *normal subgroup.* 則對任意 G/N 中的 *subgroup* H' 都可在 G 中找到 *subgroup* H 符合 $N \subseteq H$ 且 $H/N = H'$.

當 H' 是 G/N 的 *normal subgroup* 時, 則 H 也會是 G 的 *normal subgroup.*

Proof. ϕ 是 group homomorphism 是因為

$$\phi(a \cdot b) = \overline{a \cdot b},$$

且

$$\overline{a \cdot b} = \overline{a} \cdot \overline{b} = \phi(a) \cdot \phi(b).$$

再證明 ϕ 是 onto 的, 事實上對所有 $y \in G/N$ 都是 $y = \overline{a}$, 其中 $a \in G$ 這種形式. 故選 $a \in G$ 帶入 ϕ 得 $\phi(a) = \overline{a} = y$. 得證 ϕ 是 epimorphism.

$\ker(\phi)$ 是甚麼呢? 若 $a \in \ker(\phi)$ 則 $\phi(a) = \overline{e}$, 但由 ϕ 的定義 $\phi(a) = \overline{a}$. 故由 $\overline{a} = \overline{e}$, 得 $a \in N$. 反之若 $a \in N$, 則 $\phi(a) = \overline{a} = \overline{e}$, 故 $a \in \ker(\phi)$. 由此得 $\ker(\phi) = N$.

現在 Correspondence Theorem 中的條件都找到了, 所以利用 Theorem 2.7.1 知任取 G/N 中的一個 subgroup H', 在 G 中都可以找到一個 subgroup H 符合 $N = \ker(\phi) \subseteq H$ 且 $\phi(H) = H/N = H'$. □

有許多書也稱 Corollary 2.7.3 為 Correspondence Theorem. 它告訴我們 G/N 中的 subgroup 都是長 H/N 這種形式, 其中 H 是 G 的 subgroup 且 $N \subseteq H$. G/N 中的 normal subgroup 也是有 H/N 這種形式不過其中 H 是 G 的 normal subgroup.

最後我們想利用 Correspondence Theorem 來談談 Third Isomorphism Theorem 的一個特殊狀況. 令 K 是 G 的 normal subgroup, $\phi : G \to G/K$ 是定義成 $\phi(a) = \overline{a}$ 的 epimorphism. 任意 G/K 中的 normal subgroup N' 由前 Corollary 2.7.3 知是由 G 中的某一 normal subgroup N 利用 ϕ 得到: 也就是說 $N' = \phi(N) = N/K$. 故由 Theorem 2.6.5 我們有以下的定理通常也稱之為 Third Isomorphism Theorem.

Theorem 2.7.4 (Third Isomorphism Theorem)**.** *若 G 是一個 group, K 是 G 的一個 normal subgroup. 則 G/K 中的任一 normal subgroup 都是 N/K 這種形式, 其中 $K \subseteq N$ 且 N 是 G 的 normal subgroup. 而且我們有*

$$(G/K)/(N/K) \simeq G/N.$$

Proof. 任一 G/K 的 normal subgroup 都是 N/K 這種形式已在 Corollary 2.7.3 證得. 而

$$(G/K)/(N/K) \simeq G/N$$

可由 Theorem 2.6.5 直接得到. 也就是代: $G' = G/K$, $N' = N/K$. 此時可得 $N = \{a \in G \,|\, \phi(a) \in N'\}$. 故由 $G/N \simeq G'/N'$ 得證. □