大學基礎代數

李華介

國立台灣師範大學數學系

Chapter 1

初級 Group 的性質

在本章中我們將介紹 group 的定義及其基本性質, 我們也會介紹一些重要常見的 group 的例子.

1.1. Group 的基本定義

任意給一集合 S 若要在這集合內的元素之間給一個運算「$*$」怎樣的運算才算是好的運算呢？首先我們很自然的會希望集合中任兩元素運算後仍然在原集合內：也就是說若 $a, b \in S$ 則 $a * b \in S$. 這個性質就是所謂的封閉性 *closed*. 比方說在負整數中的乘法運算就不是 closed, 而在正整數中的乘法運算就是 closed.

好了！既然我們要求運算有封閉性, a 和 b 運算後仍然在 S 我們自然可以再和 S 中的元素再運算. 一般來說我們定義元素間的運算是兩個、兩個來定義的. 如何讓三個元素或更多的元素運算在一起呢？ 換句話說：該如何定 $a*b*c$ 呢？我們可以先讓 a 和 b 運算然後再和 c 運算；即$(a*b)*c$；或是先運算 b 和 c 再和 a 運算：即 $a*(b*c)$. 若這兩種運算的結果得到不同的結果那你將遭遇到天大的麻煩. 因為當你要更多元素運算在一起時你得小心翼翼的注意哪些元素要先運算. 甚至當你要算 $a*a*a$ 時到底要算 $a*(a*a)$ 或 $(a*a)*a$ 都會讓你搞昏頭. 為了省卻這些複雜性我們可以進一步要求：$a*(b*c) = (a*b)*c$. 這樣一來當你要運算 $a*b*c*d$ 時你可以算 $a*(b*(c*d))$, $(a*b)*(c*d)$ 或 $((a*b)*c)*d$ 都沒關係, 你都會得到同樣的結果. $a*(b*c) = (a*b)*c$ 這個性質我們稱之為結合率 *associative law*.

一般來說給定一集合要定義一個符合上面兩個性質的運算 (尤其是結合率) 並不是容易的事. (當然除了一些很簡單的運算, 比方說：定義每個元素運算後都取相同值.) 符合這兩個性質的集合與其運算我們稱之為 *semigroup*. 在本課程中我們將不會討論 semigroup. 畢竟它的條件太少, 很難依此得到有趣的性質. 在一般我們有興趣的代數體系中通常都有一個很特別的元素稱為 *identity*. 這個元素我們通常會用 e 來表示, 它擁有的特殊性質是對集合中任意的元素 a, $a*e$ 和 $e*a$ 的值都還是 a.

有了 e 這一個重要的元素外, 我們進而要求在集合中任意給定一個元素 a, 我們都能在集合中找到一個元素 b 使得 $a*b=b*a=e$. 這個元素我們稱之為 a 的 *inverse*. 要注意的是 e 是一個固定的元素它和任意的元素 a 運算後還是 a, 而這裡的 b 是隨 a 而變的, 不同的 a 會有不同的 b 為其 inverse. 為了強調這一點我們通常用 a^{-1} 來表示 a 的 inverse.

一個集合若有一個運算擁有前面所提的這四個性質我們稱這個集合及其運算為一個 *group*. 我們正式將這個定義寫下：

Definition 1.1.1. 一個集合 G 若元素間有一個運算 $*$ 且符合下列性質則稱為一個 *group*.

(GP1): 若 $a,b\in G$ 則 $a*b\in G$.

(GP2): 若 $a,b,c\in G$ 則 $(a*b)*c=a*(b*c)$.

(GP3): 在 G 中存在一個元素 e 使得 G 中所有元素 g 都有 $g*e=e*g=g$.

(GP4): 對 G 任一元素 g 都可在 G 中找到某一元素 g' 使得 $g*g'=g'*g=e$.

Remark 1.1.2. 要注意我們不能說一個集合是一個 group, 嚴格來說還必須指出在哪種運算下才是 group. 所以我們不能說整數 $\mathbb{Z}$ 是一個 group, 而必須說整數在加法的運算下是個 group. 不過在以後我們談到 group 時因為已經假設有運算在其中所以我們往往會省略地說 G 是一個 group. 而且除非在具體的例子中我們將統一用 「$\cdot$」 來表示運算.

我們簡單的看看哪些熟悉的東西是 group. 前面提到 $\mathbb{Z}$ 在加法的運算下是 group, 其中 0 是其 identity, 而任意的整數 n, $-n$ 是其 inverse. 不過若考慮 $\mathbb{Z}$ 在乘法的運算下它就不再是一個 group. 雖然 1 是乘法的 identity 不過並不是所有的整數都有乘法的 inverse, 例如 2 就沒法在 $\mathbb{Z}$ 中找到一個數使得 2 乘以它以後會是 1. 當然了你很快的會反應說：有理數 $\mathbb{Q}$ 在乘法下是一個 group. 可惜不是, 因為 $0\in\mathbb{Q}$ 不過 0 沒有乘法 inverse. 但如果我們考慮非 0 的有理數所成的集合, 則在乘法的運算下它就是一個 group. 要說明這件事很簡單但別忘了我們不只要說明所有非 0 的有理數有乘法反元素, 我們還要注意其他的性質. 在這裡 (GP1) 中 closed 的性質還是被保持著, 因為兩個非 0 的有理數相乘還是一個不等於 0 的有理數.

要特別注意的是, 一些我們熟悉的例子往往都有 $a\cdot b=b\cdot a$ 的性質, 不過在 group 的定義中並沒有這項要求. 以後我們將會看到很多不符合這性質的 group. 不過若一個 group 有上述這個性質我們就多給它一個名字稱之為 *abelian group*；而不符合這性質的 group 就稱為 *nonabelian group*.

Definition 1.1.3. 若 G 是一個 group 且對任意的 $a,b\in G$ 我們都有 $a\cdot b=b\cdot a$, 則稱 G 為一個 *abelian group*.

Group 的定義也沒有對元素的個數有所要求. 事實上有很多重要的 group 它只有有限多個元素. 我們也對這類的 group 給特殊的名字.

Definition 1.1.4. 若 G 是一個 group 且只有有限多個元素, 則我們稱 G 為一個 *finite group*；若 G 中元素的個數為 n, 則我們稱 G 是一個 *order* n 的 group. 通常用 $|G| = n$ 來表示.

事實上在大學的基礎代數中我們只討論 finite group.

1.2. 由 Group 的定義所得的性質

在 Group 的定義中既然我們對其有些特殊的要求, 當然很自然的想看看能否因為這些要求推得一些性質. 簡單的來說我們檢驗一個集合是否為一個 group 只需檢查其是否符合 (GP1) 到 (GP4) 這四項要求, 然而會不會因為符合了這四項要求而讓 group 有其他更多更有用的共通性質呢？答案是有的. 事實上這四項要求就讓 group 有很豐富的結構性質. 將來我們會更進一步的討論這些衍生出來的重要性質. 在這一節我們只討論幾項直接用定義得到的基本性質.

首先我們注意到在 group 的定義中 (GP3) 的性質提到存在一個 identity, 而我們也提到用 e 來表示它. 有警覺性的同學馬上會注意到 something is wrong. 甚麼問題呢？我們並不知道 identity 是否唯一怎們可以這麼快就給它一個代號. 還好, 雖然在 (GP3) 並沒有提及唯一性, 不過以下我們可以發現它的唯一性會自動成立.

在數學中證明一個東西的存在性及唯一性是非常重要的課題, 將來大家會不時的碰到這一類的問題. 一般的同學在碰到存在唯一的證明時往往分不清楚哪個是證明存在哪個是證明唯一, 所以我們將很小心的談論這類的問題.

(GP3)的性質很明顯的就是所謂的存在性. 怎樣用它來得到唯一性呢？一般的直覺證明唯一就是說找不到另外一個元素符合這個性質, 但這是很難直接證明的. 所以幾乎在證明唯一性時我們都用反證法, 也就是說假設找到兩個相異的東西有這個性質我們要證明這是矛盾的. 矛盾這個辭的由來相信大家都知道：有個人在賣矛和盾. 他一下子說他的矛無堅不催可以刺穿所有的盾牌；一下子又說他的盾堅固無比沒有矛可以刺穿它. 所以有人就問說那你的矛刺你的盾後會怎樣呢？我們就用這以子之矛攻子之盾的方法來證明矛盾. 也就是如果 e 和 e' 是 G 中兩個相異的元素且都符合 identity 的性質, 那麼 $e \cdot e'$ 會是什麼呢？

Proposition 1.2.1. 若 G 是一個 *group,* 則 G 中只有唯一的元素會符合 *identity* 的性質.

Proof. 假設 e 和 e' 是 G 中兩個相異的元素且都符合 identity 的性質, 則考慮 $e \cdot e'$. 因為 e 是 identity 所以 $e \cdot e' = e'$. 另一方面由於 e' 也是 identity 所以 $e \cdot e' = e$. 因此我們得 $e = e'$, 此和原假設 $e \neq e'$ 矛盾, 故 G 中僅有一個元素會是 identity. □

注意在以上的証明中 e 是乘在左邊而 e' 是在右邊, 也就是說在 (GP3) 中 identity 的性質若只要求對所有的 $a \in G$ 要符合 $e \cdot a = a$ (或只要求 $a \cdot e = a$) 則 identity 的唯一性並不一定會對. 所以要謹記 identity 必須要符合 $e \cdot a = a$ 且 $a \cdot e = a$.

我們很自然會問：那給定 G 中的任一元素 a, 其 inverse 是否也唯一呢？用類似的方法, 我們有以下之結果：

Proposition 1.2.2. *若 G 是一個 group, 則給定 G 中任一元素 a, 在 G 中只有唯一的元素 b 會符合 $a \cdot b = b \cdot a = e$.*

Proof. 假設 G 中有兩相異元素 b 和 b' 符合 a 的 inverse 之條件. 也就是 $a \cdot b = b \cdot a = e$ 且 $a \cdot b' = b' \cdot a = e$. 則

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

此與 $b \neq b'$ 矛盾, 故得証. □

注意以上之證明我們用到 (GP2) 及 (GP3), 另外 inverse 必須是乘在兩邊都會成 identity. 如果我們對 inverse 的條件只要求 $a \cdot b = e$ (或只要求 $b \cdot a = e$) 那麼 inverse 的唯一性定不一定會成立. 所以要謹記若 b 為 a 之 inverse, 則必須符合 $a \cdot b = e$ 且 $b \cdot a = e$.

在此再次強調由於 Proposition 1.2.2, 給定一元素 a 我們將記 a^{-1} 為其 inverse.

事實上 group 有比以上兩個 Propositions 更強的性質：

Theorem 1.2.3. *若 G 是一個 group, 給定 G 中任意元素 a 和 b, 則方程式 $a \cdot x = b$ 在 G 中有解且其解唯一. 同理, 方程式 $y \cdot a = b$ 在 G 中也有唯一解.*

Proof. 這就是一個證明存在及唯一的典型例子.

要證明存在性, 我們只要在 G 中真的找到一個元素 c 使得 $a \cdot c = b$. 很容易就知道若令 $c = a^{-1} \cdot b$, 則由於 $a^{-1} \in G$ 且 $b \in G$, 由 (GP1) 我們知 $c \in G$. 然而,

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

故知 c 是 $a \cdot x = b$ 在 G 中的一個解.

好了, 我們找到一個解了如何證明唯一呢？一個同學經常犯的錯誤是說：因為 a^{-1} 是唯一的所以解 $a^{-1} \cdot b$ 是唯一的. 這裡出錯的原因是：要證明唯一性就是要你說明為何此解一定是 $a^{-1} \cdot b$. 上述的證法並沒有真正回答這個問題. 前面提過要直接證明唯一性是頗困難的, 我們還是用反證法比較好.

假設 c 和 c' 是 G 中方程式 $a \cdot x = b$ 的兩個相異的解, 則由 $a \cdot c = a \cdot c'$ 我們可得 $a^{-1} \cdot (a \cdot c) = a^{-1} \cdot (a \cdot c')$. 由於 $a^{-1} \cdot (a \cdot c) = (a^{-1} \cdot a) \cdot c = c$ 及 $a^{-1} \cdot (a \cdot c') = (a^{-1} \cdot a) \cdot c' = c'$ 我們得 $c = c'$. 此與 $c \neq c'$ 矛盾, 故得証. □

Remark 1.2.4. 前面提過, 若我們不知道 G 是否是一個 group 時若要說 G 中的某一元素 a 是 G 的 identity, 我們必需驗證對所有的 $g \in G$ 皆有 $g \cdot a = a \cdot g = g$. 不過若已知 G 是一個 group, 那麼 Theorem 1.2.3 告訴我們說: 如果要說明 a 是 G 的 identity, 我們只要在 G 中找到一個元素 b 使得 $a \cdot b = b$ (或 $b \cdot a = b$) 就好. 不必驗證 G 中所有的元素 g 都要滿足 $g \cdot a = a \cdot g = g$.

利用 Theorem 1.2.3 我們很快的有以下的很基本但也很重要的等式：

Corollary 1.2.5. 若 G 是一個 *group*, 給定 G 中任意元素 a 和 b, 則

$$(a^{-1})^{-1} = a \quad \text{and} \quad (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}.$$

Proof. 由於 $(a^{-1})^{-1}$ 須符合 $a^{-1} \cdot x = e$, 然而已知 $x = a$ 符合此方程式, 故由 Theorem 1.2.3 的唯一性知 $(a^{-1})^{-1} = a$.

同理 $(a \cdot b)^{-1}$ 須符合 $(a \cdot b) \cdot x = e$, 然而已知 $x = b^{-1} \cdot a^{-1}$ 符合此方程式, 故由 Theorem 1.2.3 的唯一性知 $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. □

1.3. Subgroup

上一節提到 group 的基本性質幾乎是由定義直接推得, 我們若想得到更豐富的性質, 則不得不引進特殊的技巧來處理. 當然一開始最直接的想法就是如果一個 group 不是很容易被掌握, 我們是不是可以考慮其內部的子集合來幫助我們了解它. 當然了我們知道一般的子集合幫不了我們什麼忙, 因為 group 本身的運算才是我們關注的重點. 所以我們有興趣的是那些在原本 group 的運算下也是 group 的子集合. 這樣的子集合我們稱之為 *subgroup*. 以後我們將會學到如何利用 subgroup 來進一步了解原先的 group. 在本節中我們先了解一些 subgroup 的特性.

首先我們還是給 subgroup 一個正式的定義.

Definition 1.3.1. 給定一個 group G, 如果 G 中的一個非空的子集 H 在 G 的運算之下也是一個 group, 則稱 H 為 G 的一個 *subgroup*.

要注意的是, 我們強調要在 G 原本的運算下才可以. 例如在整數的加法運算下所有的偶數所成的子集合就是其 subgroup；然而集合 $\{1, -1\}$ 雖然是整數的一個子集合而且在乘法的運算下是一個 group, 不過它卻不是整數這個 group 的一個 subgroup.

給定一個 group G, 我們很容易找到兩個 subgroup: 一個就是 G 本身, 另一個就是僅由 identity 一個元素所成的子集合. 這兩個 subgroup 對我們來說沒有什麼用處, 所以稱之為 *trivial subgroups*, 其他的 subgroup 則稱之為 *nontrivial proper subgroups*. 要注意的是將來我們會看到有些 group 並沒有 nontrivial proper subgroups.

介紹完基本定義, 我們自然想知道如何判定一個 group 之子集合 H 是否為 G 的 subgroup？ 當然就是前面 group 的定義 (GP1) 到 (GP4) 都要符合. 首先注意在 subgroup 的定義中並沒有要求 H 的 identity 就是 G 的 identity. 不過若給定 H 中一元素 a, H 的 identity 必須符合 $a \cdot x = x \cdot a = a$. 由 Theorem 1.2.3, 知道在 G 中只有唯一的元素符合 $a \cdot x = a$ (或 $x \cdot a = a$), 而 G 中的 identity 又符合這等式, 所以 H 的 identity 非得是 G 中的 identity. 同理在 (GP4) 中要求對任意 H 中之元素 a 都可以在 H 中找到 a 的 inverse. 再由 Theorem 1.2.3 我們可得 a 在 H

中的 inverse 恰就是 a 在 G 中的 inverse. 由這些觀察我們用比較數學的方法再重寫 subgroup 的定義.

Definition 1.3.2. 給定一個 group G, 如果 G 中的一個非空的子集 H 在 G 的運算之下符合：

(SGP1): 若 $a, b \in H$ 則 $a \cdot b \in H$.

(SGP2): 若 $a, b, c \in H$ 則 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(SGP3): G 的 identity e 必須屬於 H.

(SGP4): 對 H 中任一元素 h 其在 G 中的 inverse h^{-1} 必須也屬於 H.

則稱 H 為 G 的一個 subgroup.

其實要檢查 H 是否為 G 之 subgroup 我們不必全部檢查 (SGP1) 到 (SGP4) 這四項. 事實上 G 中的元素都符合 (GP2), 而 H 中的元素必定在 G, 所以 H 中的元素自然符合 (SGP2). 另外 (SGP3) 也是可以省略的. 這是因為既然 H 是非空的, 我們可以在 H 中任找一元素 a. 而 (SGP4) 告訴我們若 $a \in H$ 則 $a^{-1} \in H$ 又 (SGP1) 告訴我們若 $a \in H$ 且 $a^{-1} \in H$ 則 $e = a \cdot a^{-1} \in H$, 故 (SGP3) 可由 (SGP1) 及 (SGP4) 推得. 總結以上討論, 我們有：

Lemma 1.3.3. 給定一個 *group* G, H 為 G 中的一個非空的子集. 則 H 是 G 的 *subgroup* 若且為若 H 在 G 的運算之下符合以下兩點：

(1) 若 $a, b \in H$ 則 $a \cdot b \in H$.

(2) 若 $a \in H$ 則 $a^{-1} \in H$.

有許多書將以上驗證 subgroup 的方法用更簡明的方式表示. 在實際狀況下它並沒有比較好用; 只是大部分的同學都覺得它比較好記憶所以我們還是介紹一下吧!

Lemma 1.3.4. 給定一個 *group* G, 且 H 為 G 中的一個非空的子集. 則 H 是 G 的 *subgroup* 若且為若在 G 的運算之下給定任意的 $a, b \in H$, 皆有 $a \cdot b^{-1} \in H$.

Proof. (先證明 trivial 的一邊) $\Rightarrow$: 若 H 是 G 的 subgroup, 則給定任意的 $a, b \in H$, 因 $b \in H$, 由 (SGP4) 我們可得 $b^{-1} \in H$. 又因 $a \in H$ 及 $b^{-1} \in H$, 再由 (SGP1) 我們可得 $a \cdot b^{-1} \in H$. 故得證.

(再證明較難的一邊) $\Leftarrow$: 我們主要的策略是找到 H 中特殊的 a 和 b 來證明 H 符合 (SGP1) 到 (SGP4) 這四個性質. 雖然 Lemma 1.3.3 告訴我們只要驗證 (SGP1) 及 (SGP4) 就可, 不過由於技術性上的困難我們得先證明 (SGP3) 再利用它來證明 (SGP4) 及 (SGP1). 也就是說我們先證明 $e \in H$: 這其實不難, 因為已知 H 是非空的故任取 $a \in H$, 知因 $a \in H$ 故當 $b = a$ 時, $b \in H$. 故由假設知

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

現在既然知道 $e \in H$, 則對任意的 $b \in H$ 我們可令 $a = e \in H$, 再由假設的條件 $a \cdot b^{-1} \in H$ 可得

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

這證明了 (GP4). 接下來給定任意的 $c, d \in H$, 由前已知 $d^{-1} \in H$. 故可令 $a = c$ 和 $b = d^{-1}$, 我們有 $a, b \in H$. 所以由假設知 $a \cdot b^{-1} \in H$. 也就是說 $a \cdot b^{-1} = c \cdot (d^{-1})^{-1} = c \cdot d \in H$. 這證明了 (SGP1), 故知 H 是 G 的一個 subgroup. □

注意: 如果 H 中的元素符合若 $a, b \in H$ 則 $a^{-1} \cdot b \in H$, 那麼我們也可用同樣的方法證明 H 是 G 的一個 subgroup.

前面提過以後我們將會專注於 finite group 的 case. 當我們碰到 finite group 時要檢查其中的子集合是否為 subgroup 時所要檢查的項目就更少了. 事實上我們有以下的定理:

Proposition 1.3.5. 給定一個 *"finite" group* G, 且 H 為 G 中的一個非空的子集. 則 H 是 G 的 *subgroup* 若且為若在 G 的運算之下 H 是 *closed.*

Proof. 我們僅要證明當 H 在 G 的運算下是 closed 則 H 是 G 的 subgroup. 然而利用 Lemma 1.3.3, 因為已知 H 在 G 的運算下是 closed, 所以要證明H 是 G 的 subgroup 我們只要證明給定任何的 $a \in H$ 皆有 $a^{-1} \in H$ 就可. 若 $a \in H$, 因 H 在 G 的運算下是 closed, 故 $a^2 = a \cdot a \in H$, $a^3 = a \cdot a^2 \in H$, ... 這樣一直下去我們可得對任一的 $n \in \mathbb{N}$, 皆有 $a^n \in H$. 然而 G 只有有限多個元素, 而 H 是 G 的一個子集合, 所以 H 必只有有限多個元素. 換句話說 $\{a, a^2, a^3, \dots a^n, \dots\}$ 這些 H 的元素一定不可能兩兩相異. 所以可以找到兩個相異的整數 m 和 n 使得 $a^n = a^m$. 不失一般性, 我們假設 $m > n$. 等式兩邊同乘 $(a^n)^{-1}$, 我們得 $a^{m-n} = e$. 如果 $m - n = 1$, 這表示 $a = e$, 所以 $a^{-1} = e = a \in H$. 如果 $m - n > 1$, 則 $m - n - 1 \in \mathbb{N}$. 故知 $a^{m-n-1} \in H$. 再由 $a^{m-n} = e$ 知 $a^{m-n-1} \cdot a = a \cdot a^{m-n-1} = e$. 故得 $a^{-1} = a^{m-n-1} \in H$. □

1.4. 一些特殊的 subgroup

前面提及我們希望利用一個 group 的 subgroup 來幫我們了解這一個 group. 給定一個 group 除了 trivial subgroup 外到底要怎樣找到其他的 subgroup 呢?當然了有些 group 是沒有 nontrivial proper subgroup 的(以後我們會介紹), 在這一節我們希望介紹一些可能找到 nontrivial proper subgroup 的方法.

當 G 是一個 group 給定 $a \in G$, 我們希望用 a 來產生一個 subgroup. 很自然的我們知道 $a^2, a^3, \dots, a^n, \dots$ 都要在這個 subgroup 中, 還有 $a^{-1}, (a^2)^{-1}, \dots, (a^n)^{-1}, \dots$ 也要在其中, 最後別忘了 e 也要在裡面. 由 Corollary 1.2.5, 我們知 $(a^n)^{-1} = (a^{-1})^n$, 所以我們很自然的會定義以下的集合:

$$\langle a \rangle := \{a^n \mid n \in \mathbb{N}\} \cup \{(a^{-1})^m \mid m \in \mathbb{N}\} \cup \{e\}.$$

很容易由 Lemma 1.3.3 (或 Lemma 1.3.4) 知道 $\langle a\rangle$ 會是 G 的一個 subgroup. 我們稱 $\langle a\rangle$ 為 the *cyclic subgroup* of G generated by a. 當然了, 如果我們選到 $a = e$ 則 $\langle a\rangle = \{e\}$ 這一個 trivial subgroup. 另一方面如果我們可以找到一個 a 使得 $\langle a\rangle = G$, 那麼我們就稱 G 為一個 *cyclic group*. 要注意的是並不是所有的 group G 都可以找到 $a \in G$ 使得 $\langle a\rangle = G$.

Example 1.4.1. 我們給一個有些同學會搞混的例子. 會搞混的原因是前面提過, 為了簡便的因素我們都用 「$\cdot$」 來表示 group 的運算, 所以 $a^2 = a\cdot a$ 表示 a 和 a 運算兩次, a^3 表示運算三次... 依此類推. 現在我們考慮 $\mathbb{Z}$ 以加法形成的 group. 那麼 $\langle 2\rangle$ 應該是怎樣的 subgroup 呢? 它應該是由 $2, 4 = 2+2, 6 = 2+2+2$, ...(千萬別搞錯, 不是由 $2, 4 = 2^2, 8 = 2^3$,...) 以及 $-2, -4, -6$, ... 等所組成. 換句話說在此 group 中以 2 所形成的 cyclic subgroup 即是由所有偶數所組成的. 另外大家很容易看出來 -2 也可產生同樣的 subgroup. 大家也可很容易看出 1 所產生的 cyclic subgroup 就是 $\mathbb{Z}$ 本身所以我們知道 $\mathbb{Z}$ 所形成的加法群是一個 cyclic group.

大家應該都還記得, 在一般的 group 中, $a\cdot b$ 不見得等於 $b\cdot a$. 不過因 $a\cdot e = e\cdot a = a$ 所以 identity 總是和所有元素可交換的. 至於給定一元素, 有哪些元素可以和它交換是一個很有趣的話題. 給定 $a \in G$, 我們可以考慮

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

這個集合就是搜集 G 中可以和 a 交換的元素. 我們稱之為 the *centralizer* of a. 給定任意的 $a \in G$, 事實上 $C(a)$ 會是 G 的一個 subgroup. 例如 the centralizer of identity $C(e)$ 就是 G 本身.

Proposition 1.4.2. *若 G 是一個 group 且 $a \in G$, 則 $C(a)$ 是 G 的一個 subgroup.*

Proof. 由 Lemma 1.3.3, 我們要證明: 若 $g_1, g_2 \in C(a)$ 則 $g_1\cdot g_2 \in C(a)$ 還有 $g_1^{-1} \in C(a)$. 事實上 $g_1, g_2 \in C(a)$ 告訴我們 $g_1\cdot a = a\cdot g_1$ 及 $g_2\cdot a = a\cdot g_2$. 因此

$$(g_1\cdot g_2)\cdot a = g_1\cdot(g_2\cdot a) = g_1\cdot(a\cdot g_2) = (g_1\cdot a)\cdot g_2 = (a\cdot g_1)\cdot g_2 = a\cdot(g_1\cdot g_2).$$

也就是說 $g_1\cdot g_2 \in C(a)$. 另一方面, 由於 $g_1\cdot a = a\cdot g_1$, 各乘上 g_1^{-1} 在兩邊等式的右邊. 我們得到 $(g_1\cdot a)\cdot g_1^{-1} = a$. 再乘以 g_1^{-1} 於兩邊等式之左邊. 我們得 $a\cdot g_1^{-1} = g_1^{-1}\cdot a$. 也就是說 $g_1^{-1} \in C(a)$. □

另外一種常見的 subgroup 是考慮

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

我們一般稱 $Z(G)$ 為 G 的 *center*. 注意 $C(a)$ 是和 G 中的特定元素 a 可交換的元素所成的集合, 而 $Z(G)$ 是和 G 中所有的元素可交換的元素所成的集合. 所以我們很容易可證得

$$Z(G) = \bigcap_{a\in G} C(a).$$

類似於證明 $C(a)$ 是 G 的 subgroup 的方法我們也可以證明 $Z(G)$ 也是 G 的 subgroup. 在這裡我們不再給證明不過等一下我們將會用另一種看法來說明 $Z(G)$ 是 G 的 subgroup.

1.5. 製造更多的 subgroups

前一節中我們介紹了幾種 subgroup. 如果你已有了一些 subgroups 這一節中我們將介紹一些簡單的利用這些 subgroups 製造出新的 subgroup 的方法.

Lemma 1.5.1. *若 H_1, H_2 是 G 的 subgroups, 則 $H_1 \cap H_2$ 也是 G 的 subgroup.*

Proof. 我們先證明封閉性. 若 $x, y \in H_1 \cap H_2$, 則利用 $x, y \in H_1$ 及 H_1 是一個 subgroup, 我們有 $x \cdot y \in H_1$. 同理可得 $x \cdot y \in H_2$. 故 $x \cdot y \in H_1 \cap H_2$.

另外證明 inverse 存在. 若 $x \in H_1 \cap H_2$, 則利用 $x \in H_1$ 及 H_1 是一個 subgroup, 我們有 $x^{-1} \in H_1$. 同理可得 $x^{-1} \in H_2$. 故 $x^{-1} \in H_1 \cap H_2$. □

注意從證明中不難發現若將此 Lemma 1.5.1 中的交集改成聯集則結果不一定成立. 即 $H_1 \cup H_2$ 不一定會是 subgroup. 例如在整數 $\mathbb{Z}$ 所成的加法群中, $2\mathbb{Z}$ 和 $3\mathbb{Z}$ 這兩個 subgroups 的聯集不是 subgroup. 很容易就知 $2 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ 且 $3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ 但是 $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

從 Lemma 1.5.1 的證明也不難看出不只兩個 subgroups 的交集是 subgroup, 其實任意有限多個 subgroups 的交集也是 subgroup. 甚至無窮多個 subgroups 的交集也是 subgroup. 所以我們可利用 $C(a)$ 是 subgroup 得到 $Z(G) = \cap_{a \in G} C(a)$ 也是一個 subgroup.

給定 G 中的任一元素 a 及一個 subgroup H, 我們可以考慮

$$a^{-1} \cdot H \cdot a = \{a^{-1} \cdot h \cdot a \,|\, h \in H\}$$

這個集合 (當然了若 G 是 abelian 則 $H = a^{-1} \cdot H \cdot a$).

Lemma 1.5.2. *若 $a \in G$ 且 H 是 G 的一個 subgroup, 則 $a^{-1} \cdot H \cdot a$ 也是 G 的 subgroup. 若又知 H 是 finite group, 則 $|H| = |a^{-1} \cdot H \cdot a|$.*

Proof. 若 $x_1, x_2 \in a^{-1} \cdot H \cdot a$, 表示存在 $h_1, h_2 \in H$ 使得 $x_1 = a^{-1} \cdot h_1 \cdot a$ 且 $x_2 = a^{-1} \cdot h_2 \cdot a$. 故由結合率知

$$x_1 \cdot x_2 = (a^{-1} \cdot h_1 \cdot a) \cdot (a^{-1} \cdot h_2 \cdot a) = a^{-1} \cdot (h_1 \cdot h_2) \cdot a.$$

又 $h_1 \cdot h_2 \in H$, 故 $x_1 \cdot x_2 \in a^{-1}Ha$. 這證明了封閉性.

又若 $x \in a^{-1} \cdot H \cdot a$, 則存在 $h \in H$ 使得 $x = a^{-1} \cdot h \cdot a$. 故

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

再由 $h^{-1} \in H$ 故得 $x^{-1} \in a^{-1} \cdot H \cdot a$.

最後若 H 是 G 的一個 finite subgroup, 我們要證明 $|H| = |a^{-1} \cdot H \cdot a|$. 一般來說要證明兩個集合的元素個數是相同的, 我們只要在這兩個集合間找到一個 1-1 且 onto 的函數就可. 固定 $a \in G$, 我們考慮 f 是從 H 到 $a^{-1} \cdot H \cdot a$ 的函數, 定義為: 對於所有 $h \in H$, $f(h) = a^{-1} \cdot h \cdot a$. 由定義知 $f(h) \in a^{-1} \cdot H \cdot a$. 我們現在檢查 f 是 1-1, 也就是若 $h \neq h'$ 則要證明 $f(h) \neq f(h')$. (一般來說我們不容易直接證明不等, 所以都會用反證法.) 如果 $f(h) = f(h')$, 即 $a^{-1} \cdot h \cdot a = a^{-1} \cdot h' \cdot a$, 馬上知 $h = h'$. 這和 $h \neq h'$ 的假設矛盾, 故知 $f(h) \neq f(h')$. 最後證明 f 是 onto, 也就是任取 $a^{-1} \cdot H \cdot a$ 中的元素 y, 我們要在 H 中找到一個 x 使得 $f(x) = y$. 不過由定義, $y \in a^{-1} \cdot H \cdot a$ 表示存在 $h \in H$ 使得 $y = a^{-1} \cdot h \cdot a$, 故取 $x = h$, 則得 $f(x) = y$. 我們證得了 $|H| = |a^{-1} \cdot H \cdot a|$. □