感受伽羅瓦：子群與商群

本章將延續上一章的主題，介紹與群有關的重要概念，包括「子群」、「陪集」、「正規子群」等，讀者會發現這些概念與前面介紹與環相關的概念存在對應關係，以至同名。在抽象代數學上，群一般記作有序對 $(G,\circ)$，但如果這個群上的運算 $\circ$ 根據上下文確定無疑，常常也可僅記作 G，以下我們將視乎情況採取這種簡記法。首先介紹子群(subgroup) 的概念，給定一個群 $(G,\circ)$，其子群就是代數結構 $(H,\circ)$，其中 $H\subseteq G$，$\circ$ 則是繼承自 $(G,\circ)$ 中的同類運算，而 $(H,\circ)$ 本身必須滿足群的定義。

為證明 $(H,\circ)$ 是 $(G,\circ)$ 的子群，必須證明：(i)$\circ$ 運算在 H 上封閉和 (ii)H 包含 G 中的單位元，並且 H 中每個元素的加法逆元都在 H 中。請注意由於 $(H,\circ)$ 中的 $\circ$ 是繼承自 $(G,\circ)$ 中的同類運算，必然繼承了該運算的結合性，因此在證明 $(H,\circ)$ 是 $(G,\circ)$ 的子群時無須證明這一點。

容易看到，給定群 G，G 本身和 $\{e\}$(其中 e 代表 G 中的單位元) 都是 G 的子群。除了這些「平凡」(trivial) 子群的例子外，也不難找出非平凡子群的例子，例如由於 $\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}\subset\mathbb{C}$，而這些數系加上 $+$ 運算都構成群，由此便有 $(\mathbb{Z},+)$ 是 $(\mathbb{Q},+)$ 的子群，$(\mathbb{Q},+)$ 是 $(\mathbb{R},+)$ 的子群，等等。

我們在上一章介紹了循環群的概念，並指出循環群可寫成 $\langle a\rangle$ 的形式，當 $\langle a\rangle=G$(其中 $a\in G$) 時，G 便是循環群。但其實即使 $\langle a\rangle\neq G$，$\langle a\rangle$ 本身也構成一個群，因而是 G 的子群，這樣的子群稱為循環子群(cyclic subgroup)。因此從 G 中任選一個元素 a，都能生成 G 的循環子群 $\langle a\rangle$。舉例說，容易看到 $\langle e\rangle=\{e\}$，而 $\{e\}$ 正是 G 的一個 (平凡) 循環子群。

以下讓我們看一些非平凡循環子群的例子。首先考慮 $(\mathbb{Z},+)$，在 $\mathbb{Z}$ 中，2 可生成所有偶數，即 $\langle 2\rangle=2\mathbb{Z}$，因此 $(2\mathbb{Z},+)$ 是 $(\mathbb{Z},+)$ 的循環子群。其次考慮 S_3，即由三個元素 (如 A、B 和 C) 的各種可能排列組成的對稱群，在 S_3 中，由於 $(ABC)^2=(ACB)$ 而 $(ABC)^3=(A)$，由此有 $\langle(ABC)\rangle=\{(A),(ABC),(ACB)\}$，因此 $\langle(ABC)\rangle$ 是 S_3 的循環子群。再其次考慮 D_4，即由正方形的對稱變換組成的群。為方便以下討論，現先把 D_4 中元素的各種運算結果總結成下表 (在抽象代數學上，以下這種表又稱為凱萊表(Cayley table))：

$\circ$	I	R_{90}	R_{180}	R_{270}	R_v	R_h	R_{d_1}	R_{d_2}
I	I	R_{90}	R_{180}	R_{270}	R_v	R_h	R_{d_1}	R_{d_2}
R_{90}	R_{90}	R_{180}	R_{270}	I	R_{d_1}	R_{d_2}	R_h	R_v
R_{180}	R_{180}	R_{270}	I	R_{90}	R_h	R_v	R_{d_2}	R_{d_1}
R_{270}	R_{270}	I	R_{90}	R_{180}	R_{d_2}	R_{d_1}	R_v	R_h
R_v	R_v	R_{d_2}	R_h	R_{d_1}	I	R_{180}	R_{270}	R_{90}
R_h	R_h	R_{d_1}	R_v	R_{d_2}	R_{180}	I	R_{90}	R_{270}
R_{d_1}	R_{d_1}	R_v	R_{d_2}	R_h	R_{90}	R_{270}	I	R_{180}
R_{d_2}	R_{d_2}	R_h	R_{d_1}	R_v	R_{270}	R_{90}	R_{180}	I

請注意上表最左一欄代表參與二元運算的第一個元素，最上一行則代表參與二元運算的第二個元素，例如 $R_v \circ R_{270} = R_{d_1}$，而 $R_{270} \circ R_v = R_{d_2}$。根據上表，${R_v}^2 = I$，由此有 $\langle R_v \rangle = \{I, R_v\}$，因此 $\langle R_v \rangle$ 是 D_4 的循環子群。

我們在《感受伽羅瓦：子環與商環》中介紹了「陪集」的概念，此一概念也適用於群，但要作出一些調整。設 $(G, \circ)$ 為群，$(H, \circ)$ 為其子群，$a, b \in G$，現定義以下關係：

$$a \sim_L b \text{ iff } a^{-1} \circ b \in H \qquad (1)$$

$$a \sim_R b \text{ iff } b \circ a^{-1} \in H \qquad (2)$$

請注意由於 G 不一定是交換群，上面要定義兩種關係，其中的下標 L 和 R 是「左」(left) 和「右」(right) 的縮寫，分別代表 a^{-1} 是在 b 的左方和右方與 b 進行運算。以前述的 D_4 及其子群 $\{I, R_v\}$ 為例，由於 ${R_{90}}^{-1} \circ R_{d_1} = R_v$，根據 (1)，有 $R_{90} \sim_L R_{d_1}$。另一方面，由於 $R_{d_2} \circ {R_{90}}^{-1} = R_v$，根據 (2)，有 $R_{90} \sim_R R_{d_2}$。

容易證明上述 (1) 和 (2) 定義的關係都是等價關係，根據我們在《感受伽羅瓦：等價關係與分數域》中的討論，可以為這兩個等價關係確定等價類，以下僅討論 $\sim_L$ 的情況。設 $(G, \circ)$ 為群，$(H, \circ)$ 為其子群，$a \in G$，則以 a 作為代表的等價類的定義如下：

$$\begin{aligned}
[a] &= \{b \in G : a \sim_L b\} \\
&= \{b \in G : a^{-1} \circ b \in H\} \\
&= \{b \in G : \text{存在 } h \in H \text{ 使得} a^{-1} \circ b = h\} \\
&= \{b \in G : \text{存在 } h \in H \text{ 使得} b = a \circ h\} \\
&= \{a \circ h : h \in H\}
\end{aligned}$$

仿照《感受伽羅瓦：子環與商環》的做法，我們為上列最後一行所定義的集合起一個特殊名稱－左陪集(left coset)，並記作 $a \circ H$，即

$$a \circ H = \{a \circ h : h \in H\} \qquad (3)$$

類似地，從 $\sim_R$ 也可以推導出右陪集(right coset)[1]，並記作 $H \circ a$，即

$$H \circ a = \{h \circ a : h \in H\} \qquad (4)$$

以前述的 D_4 及其子群 $\{I, R_v\}$ 為例，根據 (1) 和 (2)，可以定義以下等價關係 (在下式中，$a, b \in D_4$)：

$$a \sim_{L_1} b \text{ iff } a^{-1} \circ b \in \{I, R_v\}$$

$$a \sim_{R_1} b \text{ iff } b \circ a^{-1} \in \{I, R_v\}$$

上述兩個等價關係可以分別衍生出 $\{I, R_v\}$ 的左陪集和右陪集，現根據 (3) 和 (4) 計算左陪集 $R_{90} \circ \{I, R_v\}$ 和右陪集 $\{I, R_v\} \circ R_{90}$ 如下：

$$\begin{aligned} R_{90} \circ \{I, R_v\} &= \{R_{90} \circ I, R_{90} \circ R_v\} \\ &= \{R_{90}, R_{d_1}\} \\ \{I, R_v\} \circ R_{90} &= \{I \circ R_{90}, R_v \circ R_{90}\} \\ &= \{R_{90}, R_{d_2}\} \end{aligned}$$

請注意上面的計算結果顯示，$R_{90} \circ \{I, R_v\} \neq \{I, R_v\} \circ R_{90}$。

如前所述，左陪集 (或右陪集) 實質上是 (1)(或 (2)) 所定義的等價關係的等價類，根據《感受伽羅瓦：等價關係與分數域》中的「定理 1」，這些等價類構成 G 的一個劃分。仍以前述的 D_4 及其子群 $\{I, R_v\}$ 為例，只需簡單計算，便可找出 $\{I, R_v\}$ 的所有相異左陪集如下：

$$\begin{aligned} I \circ \{I, R_v\} &= \{I, R_v\} \\ R_{90} \circ \{I, R_v\} &= \{R_{90}, R_{d_1}\} \\ R_{180} \circ \{I, R_v\} &= \{R_{180}, R_h\} \\ R_{270} \circ \{I, R_v\} &= \{R_{270}, R_{d_2}\} \end{aligned}$$

由此可見，$\{I, R_v\}(= I \circ \{I, R_v\})$、$R_{90} \circ \{I, R_v\}$、$R_{180} \circ \{I, R_v\}$ 和 $R_{270} \circ \{I, R_v\}$ 窮盡了 $\{I, R_v\}$ 的所有左陪集，而且這四個左陪集構成 D_4 的一個劃分。我們可以把這四個左陪集組成一個商集 (請參閱《感受伽羅瓦：等價關係與分數域》對商集的討論)，記作 $D_4/\sim_{L_1}$，即

$$D_4/\sim_{L_1} = \{\{I, R_v\}, R_{90} \circ \{I, R_v\}, R_{180} \circ \{I, R_v\}, R_{270} \circ \{I, R_v\}\} \qquad (5)$$

[1]我們在《感受伽羅瓦：子環與商環》中曾介紹環的陪集的概念，根據環的定義，環的加法運算必須滿足交換性，因此對於環的任何子集和元素而言，其左陪集與右陪集必然相等，因此無須就環區分「左陪集」與「右陪集」。可是，群的運算卻不必滿足交換性，因此有必要就群區分「左陪集」與「右陪集」。

讀者可自行驗證，$\{I, R_v\}$ 也有四個相異右陪集，這些右陪集構成 D_4 的另一個劃分，並且組成另一個商集 $D_4/\sim_{R_1}$。

在上面的例子中，$\{I, R_v\}$ 的左陪集與右陪集雖然各不相等，但相異左陪集和相異右陪集的數目卻是相等的 (即都等於 4)，每個左陪集或右陪集的元素個數都是相等的 (即都等於 2)，而且以上兩個數字的乘積 (即 4×2) 剛好等於 D_4 的元素個數 (即 8)。上述結果不是偶然的，而是所有有限群的共通結果，現總結成以下定理。

定理 1：設 $(G, \circ)$ 為有限群，$(H, \circ)$ 為其子群，則 H 有相同數目的相異左陪集和相異右陪集，這個數目稱為 $(H, \circ)$ 關於 $(G, \circ)$ 的指數(index)。如用 $|G|$ 和 $|H|$ 分別代表 G 和 H 的階 (即所含元素的個數)，並用 $|G : H|$ 代表 $(H, \circ)$ 關於 $(G, \circ)$ 的指數，則 H 的所有左陪集和右陪集的元素個數都等於 $|H|$，並且

$$|G| = |H| \times |G : H| \qquad (6)$$

上述等式在抽象代數學上又稱拉格朗日定理(Lagrange's Theorem)，它的一個重要推論是如果 $(H, \circ)$ 是有限群 $(G, \circ)$ 的子群，則 $|H|$ 必然是 $|G|$ 的因數。根據此一推論，由於 $|D_4| = 8$，D_4 只可能有包含 1 個、2 個、4 個或 8 個元素的子群。

前面的例子顯示，在一般情況下，$a \circ H \neq H \circ a$。但這並不排除存在 G 的某個子群 N 使得對於任何 $a \in G$，都有 $a \circ N = N \circ a$，我們把具有這種特性的子群稱為正規子群(normal subgroup)。接下來讓我們看正規子群的例子。首先，如果 G 是交換群，那麼 G 的任何子群都是正規子群，這是因為對任何 $a, b \in G$，均有 $a \circ b = b \circ a$。由此可知，$(2\mathbb{Z}, +)$ 是 $(\mathbb{Z}, +)$ 的正規子群。其次，容易看到平凡子群 $\{e\}$ 和 G 本身都是 G 的正規子群，這是因為對任何 $a \in G$, 都有 $a \circ \{e\} = \{e\} \circ a = \{a\}$ 以及 $a \circ G = G \circ a = G$。

如要找出非交換群的非平凡正規子群，可以應用以下定理。

定理 2：設 $(G, \circ)$ 為群，$(N, \circ)$ 為其子群，則 $(N, \circ)$ 是 $(G, \circ)$ 的正規子群當且僅當對任何 $n \in N$ 和 $g \in G$，均有 $g \circ n \circ g^{-1} \in N$。

在抽象代數學上，$g \circ n \circ g^{-1}$ 稱為 g 對 n 的共軛運算(conjugation)[2]，上述定理是說，N 是 G 的正規子群當且僅當 N 像一個「共軛運算黑洞」，即 G 的任何元素一旦對 N 的元素進行共軛運算，所得結果都被「吸進」N 中。我們在《感受伽羅瓦：子環與商環》中曾指出，某個環的理想就像一個「乘法黑洞」，現在我們看到某個群的正規子群就像一個「共軛運算黑洞」，由此可見，理想與正規子群存在某種對應關係，讀者將在下文更清楚地看到

[2]請注意這個「共軛運算」跟「共軛複數」無關。

這種對應關係。

根據前面的討論，我們知道 $\{I, R_v\}$ 不是 D_4 的正規子群，但這並不排除 D_4 的其他子群是正規子群。事實上，$\{I, R_{180}\}$ 是正規子群。為用上述定理證明這一點，我們可以用 D_4 中的每個元素對 $\{I, R_{180}\}$ 中的每個元素進行共軛運算，看看其結果是否都屬於對 $\{I, R_{180}\}$；不過由於對任何元素 $g \in D_4$，都必然有 $g \circ I \circ g^{-1} = g \circ\ g^{-1} = I \in \{I, R_{180}\}$，我們實際只需對 R_{180} 進行共軛運算，其結果如下：

$$\begin{aligned}
I \circ R_{180} \circ I^{-1} &= R_{180} \in \{I, R_{180}\} \\
R_{90} \circ R_{180} \circ {R_{90}}^{-1} &= R_{180} \in \{I, R_{180}\} \\
R_{180} \circ R_{180} \circ {R_{180}}^{-1} &= R_{180} \in \{I, R_{180}\} \\
R_{270} \circ R_{180} \circ {R_{270}}^{-1} &= R_{180} \in \{I, R_{180}\} \\
R_v \circ R_{180} \circ {R_v}^{-1} &= R_{180} \in \{I, R_{180}\} \\
R_h \circ R_{180} \circ {R_h}^{-1} &= R_{180} \in \{I, R_{180}\} \\
R_{d_1} \circ R_{180} \circ {R_{d_1}}^{-1} &= R_{180} \in \{I, R_{180}\} \\
R_{d_2} \circ R_{180} \circ {R_{d_2}}^{-1} &= R_{180} \in \{I, R_{180}\}
\end{aligned}$$

上述結果顯示，$\{I, R_{180}\}$ 確是 D_4 的正規子群。據此，我們知道 $\{I, R_{180}\}$ 的每個左陪集都等於相對應的右陪集，例如

$$\begin{aligned}
R_{90} \circ \{I, R_{180}\} &= \{R_{90}, R_{270}\} \\
\{I, R_{180}\} \circ R_{90} &= \{R_{90}, R_{270}\}
\end{aligned}$$

讀者可自行驗證，$\{I, R_{180}\}$ 的其他左陪集都等於相對應的右陪集。

給定一個群 G 及其正規子群 N，由於 N 是 G 的子群，我們也可應用前述的方法定義 N 的陪集 (由於正規子群的每個左陪集都等於相對應的右陪集，所以無需區分左／右陪集)，從而得到一個商集。有趣的是，這個商集不僅是一個集合，而且是一個代數結構。事實上，我們有以下定理。

定理 3：設 $(G, \circ)$ 為群，$(N, \circ)$ 為其子群，則 N 的陪集構成一個群，當且僅當 $(N, \circ)$ 是 $(G, \circ)$ 的正規子群。上述由陪集組成的群的運算定義如下。設 $a \circ N$ 和 $b \circ N$ 為 N 的兩個陪集，則

$$(a \circ N) \circ (b \circ N) = (a \circ b) \circ N \qquad (7)$$

這個群的單位元是 $N\,(= e \circ N)$，$a \circ N$ 的逆元是 $a^{-1} \circ N$。

以下把上述定理中由陪集組成的群記作 $(G/N, \circ)$，這個群稱為 G 關於 N 的商群(quotient group)。請注意上述定理跟《感受伽羅瓦：子環與商環》

中的「定理 1」存在對應關係，其中「群」對應著「環」、「商群」對應著「商環」、「正規子群」對應著「理想」(這兩者各自在群和環中扮演著相同的角色)，至此我們再次看到正規子群與理想的對應關係。

接下來讓我們看商群的具體例子。前面曾指出 $\{I, R_{180}\}$ 是 D_4 的正規子群，根據 (6)，$|D_4 : \{I, R_{180}\}| = |D_4| \div |\{I, R_{180}\}| = 8 \div 2 = 4$，即這個正規子群共有四個陪集。只需簡單計算，便可確定這四個陪集如下：$\{I, R_{180}\}$、$R_{90} \circ \{I, R_{180}\}\,(= \{R_{90}, R_{270}\})$、$R_v \circ \{I, R_{180}\}\,(= \{R_v, R_h\})$ 和 $R_{d_1} \circ \{I, R_{180}\}\,(= \{R_{d_1}, R_{d_2}\})$。由此根據「定理 3」，可知

$$D_4/\{I, R_{180}\} = \{\{I, R_{180}\}, R_{90} \circ \{I, R_{180}\}, R_v \circ \{I, R_{180}\}, R_{d_1} \circ \{I, R_{180}\}\}$$

構成一個商群。這個商群的單位元是 $\{I, R_{180}\}$，它的每個元素都是自身的逆元。

此外，根據 (7)，還可以計算上述商群中元素之間的乘積，例如 (請注意 $R_h \circ \{I, R_{180}\} = R_v \circ \{I, R_{180}\}$)：

$$\begin{aligned}(R_{90} \circ \{I, R_{180}\}) \circ (R_{d_1} \circ \{I, R_{180}\}) &= (R_{90} \circ R_{d_1}) \circ \{I, R_{180}\} \\ &= R_h \circ \{I, R_{180}\} \\ &= R_v \circ \{I, R_{180}\} \qquad (8)\end{aligned}$$

請注意 (7) 是良定義的，這即是說在對兩個陪集進行運算時，不論採用陪集中的哪個元素作為代表，都會得到相同的結果。舉例說，$R_{90} \circ \{I, R_{180}\}$ 和 $R_{d_1} \circ \{I, R_{180}\}$ 可分別改寫成 $R_{270} \circ \{I, R_{180}\}$ 和 $R_{d_2} \circ \{I, R_{180}\}$，而根據 (7)，

$$(R_{270} \circ \{I, R_{180}\}) \circ (R_{d_2} \circ \{I, R_{180}\}) = R_h \circ \{I, R_{180}\}$$

但 $R_h \circ \{I, R_{180}\}$ 等於 $R_v \circ \{I, R_{180}\}$，所以上述計算實質上等同於 (8)。

根據「定理 3」，只有當 N 是 G 的正規子群 (而非僅普通子群) 時，N 的陪集才構成商群。前面曾指出 $\{I, R_v\}$ 不是 D_4 的正規子群，現在讓我們來看 $\{I, R_v\}$ 的左陪集 (這些左陪集列於 (5)) 並不構成商群，為證明這一點，只須證明 (7) 所定義的運算對於這些左陪集來說不是良定義的。為此，首先根據 (7) 計算：

$$(R_{90} \circ \{I, R_v\}) \circ (R_{90} \circ \{I, R_v\}) = R_{180} \circ \{I, R_v\}$$

其次，把 $R_{90} \circ \{I, R_v\}$ 改寫成 $R_{d_1} \circ \{I, R_v\}$，並再次根據 (7) 計算 (請注意 $\{I, R_v\} = I \circ \{I, R_v\}$)：

$$(R_{d_1} \circ \{I, R_v\}) \circ (R_{d_1} \circ \{I, R_v\}) = \{I, R_v\}$$

可是，$R_{180} \circ \{I, R_v\} \neq \{I, R_v\}$，因此上述兩個運算結果不相等，由此可見 (7) 所定義的運算對於 (5) 中的左陪集來說不是良定義的，即 (5) 中的左陪集並不構成商群。

為加深讀者對商群的認識，讓我們再看另一個例子，考慮群 $(\mathbb{R}-\{0\}, \times)$ 及其子群 $(\{1,-1\}, \times)$。由於 $(\mathbb{R}-\{0\}, \times)$ 是交換群，它的任何子群都是正規子群，所以 $\{1,-1\}$ 是 $\mathbb{R}-\{0\}$ 的正規子群。現在考慮 $(\mathbb{R}-\{0\})/\{1,-1\}$，這是一個由 $\{1,-1\}$ 的陪集組成的集合，其中每個陪集都是把某個非零實數逐一乘以 1 和 -1 後所得乘積組成的集合，即以下 (無限) 集合：

$$\begin{aligned} & (\mathbb{R}-\{0\})/\{1,-1\} \\ = \ & \{\{1,-1\}, 2\times\{1,-1\}, \frac{1}{2}\times\{1,-1\}, \sqrt{2}\times\{1,-1\}, \pi\times\{1,-1\}, \cdots\} \\ = \ & \{\{1,-1\}, \{2,-2\}, \{\frac{1}{2},-\frac{1}{2}\}, \{\sqrt{2},-\sqrt{2}\}, \{\pi,-\pi\}, \cdots\} \end{aligned}$$

根據「定理 3」，$((\mathbb{R}-\{0\})/\{1,-1\}, \times)$ 是一個商群，這個商群的單位元是 $\{1,-1\}$,它的每個元素都有逆元,例如 $\pi\times\{1,-1\}$ 的逆元就是 $\frac{1}{\pi}\times\{1,-1\}$。

此外，還可以根據 (7) 計算上述商群中元素之間的乘積，例如

$$\begin{aligned} (2\times\{1,-1\})\times(\sqrt{2}\times\{1,-1\}) &= (2\times\sqrt{2})\times\{1,-1\} \\ &= 2\sqrt{2}\times\{1,-1\} \end{aligned}$$

不難看到 (7) 所定義的運算對於上述商群中的元素來說是良定義的。

連結至數學專題
連結至周家發網頁