感受伽羅瓦：群的同態與同構

在讀完上兩章後，讀者應已能看到群在很多方面都跟環存在對應關係，例如「子群」對應著「子環」，「正規子群」對應著「理想」，「商群」對應著「商環」等。在《感受伽羅瓦：環的同態與同構》中，我們曾介紹環的「同態」與「同構」, 這兩個概念在群中也有對應概念, 這是本章要介紹的內容。

以下首先定義群的「同態」的概念，由於群只有一種運算，其同態概念較環的同態概念簡單。設有兩個群 $(G, \circ)$ 和 $(H, \circ')$, 一個從 $(G, \circ)$ 到 $(H, \circ')$ 的同態就是一個從 G 到 H 的函數 $\phi : G \to H$，使得對任何 $a, b \in G$，均有

$$\phi(a \circ b) = \phi(a) \circ' \phi(b) \qquad (1)$$

舉例說，如用 $\mathbb{R}^+$ 代表正實數組成的集合，並定義以下函數 $\phi_1 : \mathbb{R} - \{0\} \to \mathbb{R}^+$：

$$\phi_1(a) = |a| \qquad (2)$$

其中 $|a|$ 代表 a 的絕對值，那麼 ϕ_1 是從 $(\mathbb{R} - \{0\}, \times)$ 到 $(\mathbb{R}^+, \times)$ 的同態, 我們可以作以下計算驗證上述同態關係：一方面，我們有 $\phi_1(2 \times (-3)) = \phi_1(-6) = 6$；另一方面，我們有 $\phi_1(2) \times \phi_1(-3) = 2 \times 3 = 6$，由此驗證了 $\phi_1(2 \times (-3)) = \phi_1(2) \times \phi_1(-3)$。

上面定義的 ϕ_1 是用來作為兩個乘法群之間的同態函數，如把這兩個群中的運算改為加法，同態關係便不再成立，例如一方面，我們有 $\phi_1(2 + (-3)) = \phi_1(-1) = 1$；另一方面，我們有 $\phi_1(2) + \phi_1(-3) = 2 + 3 = 5$，由此可見 $\phi_1(2 + (-3)) \neq \phi_1(2) + \phi_1(-3)$。

跟環的情況相似，我們也可以就同態定義兩個重要集合－核和像。設 $\phi : G \to H$ 為從群 G 到群 H 的同態 (也就是兩個群之間的對應關係)，並且 e' 是 H 中的單位元，那麼 ϕ 的核，記作 $\mathrm{Ker}(\phi)$，包含 G 中所有與 e' 對應的元素，即

$$\mathrm{Ker}(\phi) = \{g \in G : \phi(g) = e'\}$$

ϕ 的像，記作 $\mathrm{Im}(\phi)$，則包含 H 中與 G 中至少一個元素對應的元素，即

$$\mathrm{Im}(\phi) = \{h \in H : \text{存在 } g \in G \text{ 使得} \phi(g) = h\}$$

以前述的 ϕ_1 為例，由於 $\mathbb{R}^+$ 中的單位元是 1 (請注意這是一個乘法群)，而在 $\mathbb{R}-\{0\}$ 中，只有 1 和 -1 的絕對值等於 1，故有 $\mathrm{Ker}(\phi_1)=\{1,-1\}$。另外，由於每個正實數 a 都可作為恰好兩個非零實數 (即 a 和 $-a$) 的絕對值，故有 $\mathrm{Im}(\phi_1)=\mathbb{R}^+$。

群同態跟環同態的相似之處還在於，兩者的核和像具有相似的性質，請把以下定理跟《感受伽羅瓦：環的同態與同構》中的「定理 1」作比較。

定理 1：設 $\phi: G\to H$ 為從群 G 到群 H 的同態，e 和 e' 分別為 G 和 H 中的單位元，g 為 G 中的元素，n 為正整數，則

(i) $\phi(e)=e'$

(ii) $\phi(g^{-1})=(\phi(g))^{-1}$

(iii) $\phi(g^n)=(\phi(g))^n$

(iv) $\mathrm{Ker}(\phi)$ 是 G 的正規子群

(v) $\mathrm{Im}(\phi)$ 是 H 的子群

以前述的 ϕ_1 為例，由於 1 是 $\mathbb{R}-\{0\}$ 和 $\mathbb{R}^+$ 這兩個乘法群中的單位元，而我們有 $\phi_1(1)=1$，由此驗證了上述定理中的 (i)。為驗證 (ii) 和 (iii)，設 $g=-2$ 和 $n=3$。首先，有 $\phi_1((-2)^{-1})=\phi_1(-\frac{1}{2})=\frac{1}{2}=2^{-1}=(\phi_1(-2))^{-1}$。其次，有 $\phi_1((-2)^3)=\phi_1(-8)=8=2^3=(\phi_1(-2))^3$。另外，根據前面的討論，我們知道 $\mathrm{Ker}(\phi_1)=\{1,-1\}$ 和 $\mathrm{Im}(\phi_1)=\mathbb{Z}^+$。由於 $\mathbb{R}-\{0\}$ 是交換群，它的任何子群都是正規子群，而由於 $\{1,-1\}$ 確是 $\mathbb{R}-\{0\}$ 的子群，故必然也是其正規子群，由此驗證了 (iv)。最後，$\mathbb{Z}^+$ 當然是 $\mathbb{Z}^+$ 的子群，由此驗證了 (v)。

如同環的情況，如在上述定義中，規定 ϕ 是一一到上函數，所得關係便稱為「同構」，是同態的一個子類，我們用 $(G,\circ)\cong(H,\circ')$ (或者 $G\cong H$，如果兩個群的運算確定無疑) 表示群 G 與群 H 同構。舉例說，如果定義以下函數 $\phi_2:\mathbb{R}^+\to\mathbb{R}$：

$$\phi_2(a)=\log_{10}(a)$$

那麼 $(\mathbb{R}^+,\times)\cong(\mathbb{R},+)$，請注意 ϕ_2 是兩個具有不同運算的群之間的同構函數，其中 $(\mathbb{R}^+,\times)$ 是乘法群，$(\mathbb{R},+)$ 則是加法群。不難證明 ϕ_2 是一一到上函數，而且 ϕ_2 滿足 (1) 所示的條件：

$$\phi_2(a\times b)=\log_{10}(a\times b)=\log_{10}(a)+\log_{10}(b)=\phi_2(a)+\phi_2(b)$$

因此 ϕ 確是一個同構。

上述例子顯示某個特定乘法群與另一個加法群的同構關係，此一關係就

是人們利用「對數」(logarithm) 函數化乘除為加減的理論基礎。此外，上述例子也顯示環同態／同構與群同態／同構的一個重要差異。由於環包含兩個運算，尋找環的同態／同構關係比尋找群的同態／同構關係一般較難，而且兩個環之間如果有同態／同構關係，它們的兩種運算都各自對應，即加法對應加法，乘法對應乘法，不能出現交叉對應的情況。但由於群只有一個運算，自由度增大了許多，因此有可能出現兩個具有不同運算的群互相對應的情況，上例就是乘法群對應加法群的情況。

不僅如此，任何循環群 (不論其運算是甚麼) 都與加法群 $(\mathbb{Z}, +)$ 或 $(\mathbb{Z}_n, +)$ 存在同構關係，即循環群的運算 (不管是何種運算) 與整數或 $\mathbb{Z}_n$ 下的加法存在對應關係，這是以下定理的內容。

定理 2：

(i) 設 $(G, \circ)$ 為由 a 生成的無限循環群，則 $(G, \circ) \cong (\mathbb{Z}, +)$，其同構函數是

$$\phi(a^k) = k$$

(ii) 設 $(G, \circ)$ 為由 a 生成的 n 階有限循環群，則 $(G, \circ) \cong (\mathbb{Z}_n, +)$，其同構函數是

$$\phi(a^k) = k \mod n$$

其中 $k \mod n$ 代表把 k 除以 n 所得的餘數。

舉例說，根據我們在《感受伽羅瓦：群的基本概念》中對八階二面體群 D_4 (即正方形的對稱變換組成的群) 的討論，容易看到 $\langle R_{90} \rangle (= \{R_{90}, R_{180}, R_{270}, I\})$ 是 D_4 的一個循環子群。現在如果把這個子群單獨抽出來，稱為 ROTATION (因為這個群是由四個旋轉運動組成)，那麼 ROTATION 是由 R_{90} 生成的四階循環群。由此根據「定理 2(ii)」，我們有 ROTATION $\cong \mathbb{Z}_4$，並且其同構函數是

$$\phi_3({R_{90}}^k) = k \mod 4$$

例如我們有 $\phi_3(R_{270}) = \phi_3({R_{90}}^3) = 3 \mod 4 = 3$。此外，根據 (1)，我們知道這個同構函數滿足

$$\phi_3(a \circ b) = \phi_3(a) + \phi_3(b)$$

例如我們有 $\phi_3(R_{270} \circ R_{180}) = \phi_3(R_{270}) + \phi_3(R_{180}) = 3 + 2 = 1$。上述計算結果的直觀意義是，把正方形旋轉 270° 後再旋轉 180°，所得結果等於進行了一次 90° 旋轉。

跟環的情況相似，我們也有以下有關群同態和同構的定理。

定理 3 (第一群同構定理First Isomorphism Theorem for Groups)：設 $\phi : G \to H$ 為群同態，那麼 $G/\mathrm{Ker}(\phi) \cong \mathrm{Im}(\phi)$，以下的 θ 就是 $G/\mathrm{Ker}(\phi)$ 與 $\mathrm{Im}(\phi)$ 之間的同構函數 (在以下定理中，$g \in G$)：

$$\theta(g \circ \mathrm{Ker}(\phi)) = \phi(g) \qquad (3)$$

上述定理要綜合運用《感受伽羅瓦：子群與商群》和本章的定理。由於 ϕ 是從 G 到 H 的同態, 根據本章的「定理 1(iv)」, 可知 $\mathrm{Ker}(\phi)$ 是 G 的正規子群，因此根據《感受伽羅瓦：子群與商群》中的「定理 3」，可知 $G/\mathrm{Ker}(\phi)$ 構成一個群 (即商群)，這個群的元素包括所有形如 $g \circ \mathrm{Ker}(\phi)$ 的陪集 (其中 $g \in G$)。此外, 根據本章的「定理 1(v)」, $\mathrm{Im}(\phi)$ 是 H 的子群。上述定理的要旨是,$G/\mathrm{Ker}(\phi)$ 與 $\mathrm{Im}(\phi)$ 同構,(3) 提供了 $G/\mathrm{Ker}(\phi)$ 與 $\mathrm{Im}(\phi)$ 之間的同構函數。

為讓讀者明白上述定理，我們回顧前述的 $\phi_1 : \mathbb{R} - \{0\} \to \mathbb{R}^+$。根據前面的討論，可知 $\mathrm{Ker}(\phi_1) = \{1, -1\}$ 和 $\mathrm{Im}(\phi_1) = \mathbb{R}^+$。如前所述，$\{1, -1\}$ 是 $\mathbb{R} - \{0\}$ 的正規子群，因此 $(\mathbb{R} - \{0\})/\{1, -1\}$ 構成一個商群，我們在《感受伽羅瓦：子群與商群》中曾討論這個商群，它由所有形如 $n \times \{1, -1\}$(其中 $n \in \mathbb{R} - \{0\}$) 的陪集組成，即

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

現在根據上述定理，我們有以下同構關係：

$$(\mathbb{R} - \{0\})/\{1, -1\} \cong \mathbb{R}^+$$

其中的同構函數可根據 (3) 寫成

$$\theta_1(n \times \{1, -1\}) = \phi_1(n) \qquad (4)$$

利用 ϕ_1 的定義 (2)，可以把上式更具體地寫成

$$\theta_1(n \times \{1, -1\}) = |n| \qquad (5)$$

上式提供了 $(\mathbb{R}-\{0\})/\{1, -1\}$ 與 $\mathbb{R}^+$ 元素之間的一一對應關係,例如 $\{2, -2\}$ 對應著 $2, \{\frac{1}{2}, -\frac{1}{2}\}$ 對應著 $\frac{1}{2}, \{\sqrt{2}, -\sqrt{2}\}$ 對應著 $\sqrt{2}, \{\pi, -\pi\}$ 對應著 π, 等等。

為加深讀者對「定理 3」的了解，讓我們看另一個較複雜的例子，考慮 $(\mathbb{R}/\mathbb{Z}, +)$。由於 $\mathbb{R}$ 是交換群，而 $\mathbb{Z}$ 是其子群，可知 $\mathbb{Z}$ 是 $\mathbb{R}$ 的正規子群，因此根據《感受伽羅瓦：子群與商群》中的「定理 3」，$(\mathbb{R}/\mathbb{Z}, +)$ 構成一個商

群，這個商群由所有形如 $n+\mathbb{Z}$ (其中 $n \in \mathbb{R}$) 的陪集組成，以下是其中某些陪集的例子：

$$\begin{aligned}
\mathbb{Z}\,(=0+\mathbb{Z}) &= \{0, 1, -1, 2, -2, \cdots\} \\
0.6+\mathbb{Z} &= \{0.6, 1.6, -0.4, 2.6, -1.4, \cdots\} \\
0.3737...+\mathbb{Z} &= \{0.3737..., 1.3737..., -0.6262..., 2.3737..., -1.6262..., \cdots\} \\
\cos 1+\mathbb{Z} &= \{\cos 1, \cos 1+1, \cos 1-1, \cos 1+2, \cos 1-2, \cdots\} \\
&= \{0.5403..., 1.5403..., -0.4596..., 2.5403..., -1.4596..., \cdots\}
\end{aligned}$$

上列例子都具有 $n+\mathbb{Z}$ 的形式，其中 $n \in [0,1)$。如果用 $[0,1)$ 以外的正實數作為 n，所得結果如何？請看以下例子：

$$1.6+\mathbb{Z} = \{1.6, 2.6, 0.6, 3.6, -0.4, \cdots\}$$

上述集合等於 $0.6+\mathbb{Z}$。事實上，設 k 為任意正整數，那麼必然有 $k+0.6+\mathbb{Z} = 0.6+\mathbb{Z}$ (這是因為在計算陪集時，k 作為整數會被「吸收」進 $\mathbb{Z}$ 中)。此一結果可以作進一步推廣，設 k 為任意正整數，n 為絕對值小於 1 的任意正實數，則 $k+n+\mathbb{Z} = n+\mathbb{Z}$。

如果用負實數作為 n，所得結果又如何？請看以下例子：

$$-1.4+\mathbb{Z} = \{-1.4, -0.4, -2.4, 0.6, -3.4 \cdots\}$$

上述集合等於 $0.6+\mathbb{Z}$。事實上，對任何負實數 n，我們總能找到一個正整數 k，使得 $k+n>0$，而且 $n+\mathbb{Z} = k+n+\mathbb{Z}$ (例如在上例中，負實數 n 是 -1.4，正整數 k 則是 2 或比 2 大的任何整數)。總上所述，在考慮 $\mathbb{R}/\mathbb{Z}$ 的成員時，只需考慮所有形如 $n+\mathbb{Z}$ 的陪集，其中 $n \in [0,1)$，即

$$\mathbb{R}/\mathbb{Z} = \{n+\mathbb{Z} : n \in [0,1)\}$$

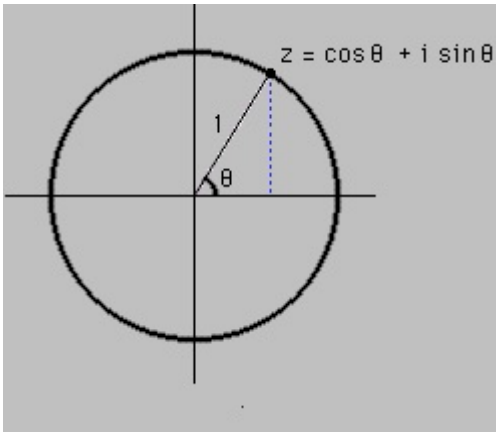
$\mathbb{R}/\mathbb{Z}$ 不僅是一個集合，而且是一個代數結構 (即群)，可以對其成員進行加法，以下是一個計算範例：

$$(0.7+\mathbb{Z}) + (0.8+\mathbb{Z}) = 0.5+\mathbb{Z}$$

直觀地看，$\mathbb{R}/\mathbb{Z}$ 的成員對應著區間 $[0,1)$ 上的實數，例如 $0.7+\mathbb{Z}$ 對應著 0.7，$0.8+\mathbb{Z}$ 則對應著 0.8，而且這些實數的加法是一種「只取其小數部分」的加法，例如 $0.7+0.8$ 在普通加法下的結果是 1.5，但若只取其小數部分，則所得結果是 0.5。上述特殊加法保證 $[0,1)$ 上的兩個實數之和也是 $[0,1)$ 上的實數，即 $\mathbb{R}/\mathbb{Z}$ 在這種特殊加法下封閉。在上述這種「只取其小數部分」的加法下，每個 $[0,1)$ 中的元素都有該區間中的另一個元素作為其加法逆元，例如 0.6 在上述加法下的逆元就是 0.4，這是因為

0.6+0.4 在普通加法下的結果是 1.0, 但若只取其小數部分, 則所得結果是 0。

上述這些 $[0,1)$ 上的實數連同「只取其小數部分」的加法似乎是一個我們以前未曾討論過的數系，但其實我們可以把這些實數看成對應著模為 1 的複數。我們在《感受伽羅瓦：二次方程與複數》中曾指出，複數可被看成平面上的點，而模為 1 的複數則可被看成「單位圓」(unit circle) 圓周上的點。單位圓是指以原點為圓心，半徑為 1 的圓，如下圖所示：



上圖提供了把單位圓圓周上的點表示成複數的公式，設單位圓圓周上的某點與圓心的連線與正 x 軸成夾角 θ (其中 $\theta \in [0, 2\pi)$)，則該點可以表示成以下複數：

$$\cos\theta + i\sin\theta \qquad (6)$$

在上式中，θ 稱為複數的「主幅角」。舉例說，若 $\theta = 0$，所得複數是 $\cos 0 + i\sin 0 = 1$；若 $\theta = \frac{\pi}{2}$，則所得複數是 $\cos\frac{\pi}{2} + i\sin\frac{\pi}{2} = i$，等等。請注意具有 (6) 所示形式的複數都是模為 1 的複數，這是因為根據我們在《感受伽羅瓦：二次方程與複數》中提供的計算複數的模的公式 (即該網頁的公式 (7))，上述複數的模是 $\sqrt{\cos^2\theta + \sin^2\theta} = 1$。

現在如果把區間 $[0,1)$ 上的實數乘大 2π 倍 (即把 $[0,1)$ 變成 $[0,2\pi)$)，把所得結果作為 θ，並代入 (6) 中，便可得到模為 1 的複數。由於 cos 和 sin 函數具有周期性 (其周期為 2π)，即使 $\theta \notin [0,2\pi)$，所得複數會等於某個主幅角屬於 $[0,2\pi)$ 的複數，例如若 $\theta = \frac{5\pi}{2}$，所得複數是 $\cos\frac{5\pi}{2} + i\sin\frac{5\pi}{2} = i$，其結果跟 $\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}$ 一樣。因此，在考慮模為 1 的複數時，只需考慮所有形如 $\cos\theta + i\sin\theta$ 的複數, 其中 $\theta \in [0,2\pi)$, 這種情況跟前述的 $\mathbb{R}/\mathbb{Z}$ 很相似。

模為 1 的複數之間還可進行乘法。利用三角恆等式，我們有以下乘法規律：

$$(\cos\alpha + i\sin\alpha) \times (\cos\beta + i\sin\beta) = \cos(\alpha+\beta) + i\sin(\alpha+\beta) \qquad (7)$$

上式告訴我們, 把兩個主幅角分別為 α 和 β 的複數相乘, 所得結果是主幅角為 $\alpha+\beta$ 的複數。換句話說, 複數的乘法對應著主幅角的加法。此外, 由於 cos 和 sin 函數具有周期性, 上述乘法保證兩個模為 1 的複數的乘積也是模為 1 的複數。舉例說, $(\cos\frac{3\pi}{2}+i\sin\frac{3\pi}{2})\times(\cos\pi+i\sin\pi)=\cos\frac{5\pi}{2}+i\sin\frac{5\pi}{2}=i$。上述結果顯示, 模為 1 的複數在乘法下封閉, 這種情況也跟前述的 $\mathbb{R}/\mathbb{Z}$ 很相似。事實上, 不難證明模為 1 的複數在乘法下構成一個群。

至此讀者應已能猜到, $\mathbb{R}/\mathbb{Z}$ 這個加法群與由模為 1 的複數組成的乘法群存在同構關係, 以下讓我們用「定理 3」來證明這一點。為此, 首先把所有模為 1 的複數組成一個集合, 記作 $\mathbb{T}$, 這個集合在乘法下構成一個群。接著引入以下同態函數 $\phi_4:\mathbb{R}\to\mathbb{T}$：

$$\phi_4(n)=\cos(2n\pi)+i\sin(2n\pi) \qquad (8)$$

上式包含 2π 這個因子, 因為如前所述, 我們要把區間 $[0,1)$ 上的實數乘大 2π 倍。以下讓我們證明上式的確滿足 (1) 所示的條件, 由於這個函數是把 $\mathbb{R}$ 上的加法與 $\mathbb{T}$ 上的乘法聯繫起來, 我們要證明的是, 對任何實數 n、m, 均有 $\phi_4(n+m)=\phi_4(n)\times\phi_4(m)$, 現證明如下：

$$\begin{array}{lll} & \phi_4(n+m) & \\ = & \cos(2(n+m)\pi)+i\sin(2(n+m)\pi) & \text{(根據 (8))} \\ = & \cos(2n\pi+2m\pi)+i\sin(2n\pi+2m\pi) & \\ = & (\cos(2n\pi)+i\sin(2n\pi))\times(\cos(2m\pi)+i\sin(2m\pi)) & \text{(根據 (7))} \\ = & \phi_4(n)\times\phi_4(m) & \text{(根據 (8))} \end{array}$$

接著確定 $\mathrm{Ker}(\phi_4)$ 和 $\mathrm{Im}(\phi_4)$。由於 $\mathbb{T}$ 是乘法群, 其單位元是 1。由於當 $\theta=0,\pm2\pi,\pm4\pi,\cdots$, 則 $\cos\theta+i\sin\theta=1$, 可知當 $n=0,\pm1,\pm2,\cdots$, 則 $\phi_4(n)=1$, 因此 $\mathrm{Ker}(\phi_4)=\mathbb{Z}$。另一方面, 給定 $\mathbb{T}$ 中任意元素 z, 都可找到其主幅角 θ, 由此求 $n=\frac{\theta}{2\pi}$, 便可得到 n 使得 $\phi_4(n)=\cos\theta+i\sin\theta=z$。例如設 $z=-1$, 那麼 z 的主幅角是 π, 接著求 $n=\frac{\pi}{2\pi}=0.5$, 由此可得 $\phi_4(0.5)=-1$。綜合以上討論, 可知 $\mathrm{Im}(\phi_4)=\mathbb{T}$。

把上述結果代入「定理 3」, 便可得到

$$(\mathbb{R}/\mathbb{Z},+)\cong(\mathbb{T},\times)$$

其中的同構函數可根據 (3) 寫成

$$\theta_4(n+\mathbb{Z})=\phi_4(n) \qquad (9)$$

利用 ϕ_4 的定義 (8), 可以把上式更具體地寫成

$$\theta_4(n+\mathbb{Z})=\cos(2n\pi)+i\sin(2n\pi) \qquad (10)$$

上式提供了 $\mathbb{R}/\mathbb{Z}$ 與 $\mathbb{T}$ 元素之間的一一對應關係, 例如 $0.5+\mathbb{Z}$ 對應著 -1 等。

連結至數學專題
連結至周家發網頁