感受伽羅瓦：低次多項式的伽羅瓦群

我們在上一章引入了多項式方程伽羅瓦群的概念，設 f 為域 F 上的多項式，E 為 f 的分裂域，則 f 的伽羅瓦群 $\mathrm{Gal}(f)$ 是指 $\mathrm{Gal}(E:F)$，這個伽羅瓦群的成員是 E 上以 F 全體元素作為不動點的自同構。我們在上一章也曾指出，$\mathrm{Gal}(f)$ 的成員是對 f 的根的排列，因此若 f 是 n 次多項式，則 $\mathrm{Gal}(f)$ 同構於對稱群 S_n 或者 S_n 的某個真子群。

在本章我們將結合對低次 (這裡指一次至四次) 多項式方程的根式解的知識 (請參閱《感受伽羅瓦：二次方程與複數》、《感受伽羅瓦：三次方程的根式解》、《感受伽羅瓦：四次方程的根式解》和《感受伽羅瓦：根與係數的關係》) 以及上一章的內容，討論低次多項式方程的伽羅瓦群，這樣可以加深我們對這些方程的了解。請注意以下討論的多項式都是 $\mathbb{Q}[x]$ 中的多項式。

為方便討論，以下把討論範圍限制於首一多項式，即最高次項的係數等於 1 的多項式，請注意這沒有限制以下討論結果的應用範圍，這是因為任何多項式都可改寫成某個常數與某個首一多項式的乘積，而且這個首一多項式與原來的多項式有相同的根。以 $6x^2-17x+12$ 為例，這個多項式可以改寫成 $6(x^2-\frac{17}{6}x+2)$，其中 $x^2-\frac{17}{6}x+2$ 是首一多項式，而 $6x^2-17x+12$ 與 $x^2-\frac{17}{6}x+2$ 有相同的根，即 $\frac{3}{2}$ 和 $\frac{4}{3}$。

先從最簡單的情況說起，設 f 為一次首一多項式，由於 f 的根必然是有理數，它的分裂域就是 $\mathbb{Q}$。由於在 $\mathbb{Q}$ 上以全體有理數作為不動點的自同構只有一個，即恆等函數 I，因此 $\mathrm{Gal}(f)$ 就是僅包含一個元素的平凡群 $\{I\}$，這個群同構於 S_1。

接著考慮二次首一多項式的情況，我們知道二次方程的根的結構會因應其判別式的值而有所不同。我們在中學時代便已學過二次方程的判別式，但其實判別式此一概念適用於所有一次以上的首一多項式方程，以下是判別式(discriminant) 的普遍定義[1]。設 $f=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 為 n

[1]請注意不同數學家對多項式的判別式提出了不同的定義，以配合不同的需要，因此以下介紹的判別式跟我們在前面某些章節所介紹的判別式不盡相同。

次首一多項式，x_1、...、x_n 為其 n 個根，那麼 f 的判別式 (以下記作 $\Delta(f)$) 定義如下：

$$\Delta(f) = ((x_1 - x_2)\cdots(x_1 - x_n)(x_2 - x_3)\cdots(x_2 - x_n)\cdots(x_{n-1} - x_n))^2 \qquad (1)$$

請注意上述定義並不依賴於 f 的 n 個根的排列次序，這是因為即使把上述乘積中某兩個根的次序對調，雖然所得乘積與原來乘積相差了正負號，但在取平方後此一差異便消失了。例如雖然 $x_1 - x_2$ 與 $x_2 - x_1$ 相差了正負號，但 $(x_1 - x_2)^2$ 卻與 $(x_2 - x_1)^2$ 相等。

此外，判別式 $\Delta(f)$ 還有兩個重要特性，現概括為以下定理。

定理 1：設 f 為首一多項式, $\theta \in \mathrm{Gal}(f)$，則

(i) $\Delta(f) = 0$ 當且僅當 f 有重根。

(ii) $\theta(\Delta(f)) = \Delta(f)$

上述 (i) 的理據是，(1) 中右端等於 0 當且僅當存在至少一對 x_i、x_j 使得 $x_i = x_j$，而若 $x_i = x_j$，那麼 x_i 和 x_j 就是 f 的重根。(ii) 的理據則是，θ 是對 f 的根的排列，因此把 θ 作用於 (1)，所得結果是對該數式中的 x_1、...、x_n 的重新排列。此一重新排列最多只會改變原來乘積的正負號 (例如若把 x_1 和 x_2 對調位置，所得乘積是原來乘積的負值)，在取平方後此一差異即告消失，即把 θ 作用於 (1) 所得結果等於 (1)。

根據 (1)，若 $f = x^2 + bx + c$ 是二次首一多項式，並且 x_1 和 x_2 為其兩個根，則其判別式為

$$\Delta(f) = (x_1 - x_2)^2$$

運用二次方程的求解公式求出 f 的兩個根 x_1 和 x_2 並代入上式，可把上式變成

$$\begin{aligned}\Delta(f) &= \left(\frac{-b + \sqrt{b^2 - 4c}}{2} - \frac{-b - \sqrt{b^2 - 4c}}{2}\right)^2 \\ &= \left(\frac{2\sqrt{b^2 - 4c}}{2}\right)^2 \\ &= b^2 - 4c\end{aligned}$$

上式跟我們在中學時代學到的二次首一多項式的判別式完全相同。

根據二次方程的求解公式，若 $\sqrt{\Delta(f)}$ 是有理數，則 f 是可約多項式，它有兩個相異有理數根或者一個二重有理數根。在此情況下，f 的根全是

有理數，因此其分裂域是 $\mathbb{Q}$，而 $\mathrm{Gal}(f)=\{I\}$。若 $\sqrt{\Delta(f)}$ 不是有理數，則 f 是不可約多項式，它有一對形如 $\frac{1}{2}(-b\pm\sqrt{\Delta(f)})$ 的實數根或共軛複數根。在此情況下，f 的分裂域可以寫成 $\mathbb{Q}(\frac{1}{2}\sqrt{\Delta(f)})$，而 $\mathrm{Gal}(f)$ 包含兩個元素，其中一個是恆等函數 I，另一個則是把 $\frac{1}{2}(-b+\sqrt{\Delta(f)})$ 和 $\frac{1}{2}(-b-\sqrt{\Delta(f)})$ 互相映射為對方的函數，這個函數對應著 S_2 的成員 (12)，因此在此情況下，$\mathrm{Gal}(f)\cong S_2=\{I,(12)\}$。

以 $f_1=x^2+2$ 為例，由於 $\sqrt{\Delta(f_1)}=\sqrt{-8}=2\sqrt{2}i$ 不是有理數，可知 f_1 的分裂域可以寫成 $\mathbb{Q}(\sqrt{2}i)$，並且 $\mathrm{Gal}(f_1)\cong S_2$。上述討論顯示，我們可以根據二次多項式 f 的判別式的值判斷 f 的分裂域，從而判斷 f 的伽羅瓦群，以下將沿用此方法判斷三次和四次多項式的分裂域和伽羅瓦群。

現在設 f 為三次首一多項式，如果 f 在 $\mathbb{Q}$ 上可約，那麼它可被改寫成一個一次因式與一個二次因式的乘積，其中一次因式的根必然是有理數，因此 f 的分裂域和伽羅瓦群取決於其二次因式的分裂域和伽羅瓦群，而這後者可以用以上介紹有關二次多項式的方法求得。

以 $f_2=x^3-x^2+2x-2$ 為例，這個多項式可因式分解為 $(x-1)(x^2+2)$，其中一次因式 $x-1$ 的根是有理數 1，因此 f_2 的分裂域和伽羅瓦群取決於其二次因式 x^2+2。由於這個二次多項式就是上面討論過的 f_1，可知 f_2 的分裂域可以寫成 $\mathbb{Q}(\sqrt{2}i)$，並且 $\mathrm{Gal}(f_2)\cong S_2$。

接下來考慮不可約三次首一多項式的情況，類似二次多項式的情況，這裡要應用這些多項式的判別式。對於一般的三次首一多項式 $f=x^3+bx^2+cx+d$ 而言，其判別式頗為複雜，為此我們可以應用《感受伽羅瓦：三次方程的根式解》中介紹的「契爾恩豪斯變換」，以 $x=y-\frac{b}{3}$ 代入 f，把原來以 x 作為變項的三次首一多項式 f 變換成以 y 作為變項並且其二次項係數為 0 的三次首一多項式 $g=y^3+py+q$。契爾恩豪斯變換不僅可以簡化求解多項式的過程，而且不影響判別式的值，這是以下定理的內容。

定理 2：設 f 為多項式，g 為對 f 進行契爾恩豪斯變換後所得的多項式，則 f 和 g 有相同的判別式。

請注意上述定理適用於任何次數的多項式，以下定理提供經契爾恩豪斯變換後三次多項式的判別式。

定理 3：設 $g=y^3+py+q$ 是二次項係數為 0 的三次首一多項式，則

g 的判別式是[2]

$$\Delta(g) = -4p^3 - 27q^2$$

利用上述判別式，便可用以下定理判斷不可約三次首一多項式的伽羅瓦群。

定理 4：設 g 為不可約三次首一多項式，

(i) 若 $\Delta(g) < 0$，則 $\mathrm{Gal}(g) \cong S_3$。

(ii) 若 $\Delta(g) > 0$ 並且 $\sqrt{\Delta(g)}$ 不是有理數，則 $\mathrm{Gal}(g) \cong S_3$。

(iii) 若 $\Delta(g) > 0$ 並且 $\sqrt{\Delta(g)}$ 是有理數，則 $\mathrm{Gal}(g) \cong A_3$。

上述定理不包含 $\Delta(g) = 0$ 的情況，這是因為根據前面的定理 1(i)，$\Delta(g) = 0$ 當且僅當 g 有重根，但由於 g 是 $\mathbb{Q}$ 上的不可約多項式，g 不可能有重根[3]，因此不可能出現 $\Delta(g) = 0$ 的情況。

接下來讓我們直觀地理解上述定理的內容。如前所述，$\mathrm{Gal}(g)$ 的成員是對 g 的根的排列，在最一般的情況下，$\mathrm{Gal}(g)$ 包含對 g 的根的所有可能排列，即 $\mathrm{Gal}(g) \cong S_3$。但若 g 的根具有一些特殊性質，便會限制 $\mathrm{Gal}(g)$ 的成員對這些根的排列，從而使 $\mathrm{Gal}(g)$ 不同構於 S_3。例如若果 g 的根中有一個 (設為 α) 是有理數，那麼根據伽羅瓦群的定義，$\mathrm{Gal}(g)$ 的任何成員都必須把 α 映射為 α，不可能把 α 映射為 g 的另一個根，正是此一限制使 $\mathrm{Gal}(g)$ 不同構於 S_3。

同樣，在「定理 4(iii)」的情況下，我們有 $\sqrt{\Delta(g)}$ 是有理數，這是一個很特殊的性質，正是此一性質限制了 $\mathrm{Gal}(g)$ 的成員的可能性，從而使 $\mathrm{Gal}(g)$ 不同構於 S_3。由於以上的論述頗抽象，以下用一個實例以作說明，試考慮三次多項式 $g_1 = y^3 - 48y + 64$，有關這個多項式的不可約性質的證明，請參閱本章附錄。根據上面的「定理 3」，可求得 $\Delta(g_1) = 331776$。由於 $\sqrt{331776} = 576$ 是有理數，根據「定理 4(iii)」，可知 $\mathrm{Gal}(g_1) \cong A_3$。

接著讓我們求 g_1 的三個根，看看是甚麼因素令 $\mathrm{Gal}(g_1)$ 不同構於 S_3。運用我們在《感受伽羅瓦：三次方程的根式解》介紹的方法，不難求得 g_1 的三個根是 $8\cos\frac{2\pi}{9}$、$8\cos\frac{8\pi}{9}$ 和 $8\cos\frac{14\pi}{9}$。請注意這三個根中的 $\cos\frac{2\pi}{9}$、$\cos\frac{8\pi}{9}$ 和

[2]請注意下式跟我們在《感受伽羅瓦：三次方程的根式解》介紹的判別式 $\Delta_3 = \frac{q^2}{4} + \frac{p^3}{27}$ 有所不同，其中 $\Delta(g) = -108\Delta_3$，這即是說，$\Delta(g) > 0$ 當且僅當 $\Delta_3 < 0$，並且 $\Delta(g) < 0$ 當且僅當 $\Delta_3 > 0$。正因如此，以下基於 $\Delta(g)$ 正負號所得的結論跟基於 Δ_3 正負號所得的結論相反。

[3]請參閱《感受伽羅瓦：伽羅瓦擴張》中的「定理 3」，請注意 $\mathbb{Q}$ 是特徵等於 0 的域，而根據上述網頁的定義，多項式 g 是可分的當且僅當 g 沒有重根。

$\cos\frac{14\pi}{9}$ 存在以下關係：

$$\begin{aligned}
\cos\frac{14\pi}{9} &= \cos\left(2\pi-\frac{4\pi}{9}\right)\\
&= \cos\frac{4\pi}{9}\\
&= \cos\left(2\times\frac{2\pi}{9}\right)\\
\cos\frac{8\pi}{9} &= \cos\left(4\pi-\frac{28\pi}{9}\right)\\
&= \cos\frac{28\pi}{9}\\
&= \cos\left(2\times\frac{14\pi}{9}\right)\\
\cos\frac{2\pi}{9} &= \cos\left(2\pi-\frac{16\pi}{9}\right)\\
&= \cos\frac{16\pi}{9}\\
&= \cos\left(2\times\frac{8\pi}{9}\right)
\end{aligned}$$

由此可以利用倍角公式 $\cos 2\theta = 2(\cos\theta)^2 - 1$ 寫出這三個數之間的關係如下：

$$\begin{aligned}
\cos\frac{14\pi}{9} &= 2\left(\cos\frac{2\pi}{9}\right)^2 - 1 \qquad (2)\\
\cos\frac{8\pi}{9} &= 2\left(\cos\frac{14\pi}{9}\right)^2 - 1 \qquad (3)\\
\cos\frac{2\pi}{9} &= 2\left(\cos\frac{8\pi}{9}\right)^2 - 1 \qquad (4)
\end{aligned}$$

上述關係顯示 g_1 的分裂域可以寫成 $\mathbb{Q}(\cos\frac{2\pi}{9})$。此外，上述關係也限制了 $\mathrm{Gal}(g_1)$ 的可能性。設 $\theta_1 \in \mathrm{Gal}(g_1)$，並且有 $\theta_1(8\cos\frac{2\pi}{9}) = 8\cos\frac{14\pi}{9}$，即 $\theta_1(\cos\frac{2\pi}{9}) = \cos\frac{14\pi}{9}$。由此根據上述關係，有

$$\begin{aligned}
\theta_1\left(\cos\frac{14\pi}{9}\right) &= \theta_1\left(2\left(\cos\frac{2\pi}{9}\right)^2 - 1\right)\\
&= 2\left(\theta_1\left(\cos\frac{2\pi}{9}\right)\right)^2 - 1
\end{aligned}$$

$$
\begin{aligned}
&= 2\left(\cos\frac{14\pi}{9}\right)^2 - 1 \\
&= \cos\frac{8\pi}{9} \\
\theta_1\left(\cos\frac{8\pi}{9}\right) &= \theta_1\left(2\left(\cos\frac{14\pi}{9}\right)^2 - 1\right) \\
&= 2\left(\theta_1\left(\cos\frac{14\pi}{9}\right)\right)^2 - 1 \\
&= 2\left(\cos\frac{8\pi}{9}\right)^2 - 1 \\
&= \cos\frac{2\pi}{9}
\end{aligned}
$$

根據上述計算結果，我們有

$$\theta_1\left(8\cos\frac{14\pi}{9}\right) = 8\cos\frac{8\pi}{9}$$

$$\theta_1\left(8\cos\frac{8\pi}{9}\right) = 8\cos\frac{2\pi}{9}$$

以上計算了 $\mathrm{Gal}(g_1)$ 一個成員 θ_1 對上述三個根的作用。同理，也可求得 $\mathrm{Gal}(g_1)$ 其餘兩個成員 (以下稱為 θ_2 和 I) 對這三個根的作用，現將 I、θ_1 和 θ_2 對三個根的作用列於下表：

I	$8\cos\frac{2\pi}{9}$	$8\cos\frac{8\pi}{9}$	$8\cos\frac{14\pi}{9}$
θ_1	$8\cos\frac{14\pi}{9}$	$8\cos\frac{2\pi}{9}$	$8\cos\frac{8\pi}{9}$
θ_2	$8\cos\frac{8\pi}{9}$	$8\cos\frac{14\pi}{9}$	$8\cos\frac{2\pi}{9}$

除了上述 I、θ_1 和 θ_2 外，$\mathrm{Gal}(g_1)$ 不可能再有其他成員。現在如對 $8\cos\frac{2\pi}{9}$、$8\cos\frac{8\pi}{9}$ 和 $8\cos\frac{14\pi}{9}$ 分別給予編號 1、2 和 3，那麼根據上表，I、θ_1 和 θ_2 分別對應著 S_3 中的成員 I、(132) 和 (123)，而 $\{I, (123), (132)\}$ 正好構成 S_3 的真子群 A_3，至此讀者應可看到 $\mathrm{Gal}(g_1) \cong A_3$。

接著考慮四次多項式的情況，設 f 為可約四次首一多項式，那麼有兩種可能性，第一種可能性是 f 可被改寫成一個一次因式與一個三次因式的乘積，其中一次因式的根必然是有理數，因此 f 的分裂域和伽羅瓦群取決於其三次因式的分裂域和伽羅瓦群，而這後者可以用以上介紹有關三次多項式的方法求得。

第二種可能性是 f 可被改寫成兩個不可約二次因式的乘積，假設這兩

個二次因式是 g 和 h。根據前面對不可約二次多項式的討論，可知 g 和 h 的分裂域分別是 $\mathbb{Q}(\frac{1}{2}\sqrt{\Delta(g)})$ 和 $\mathbb{Q}(\frac{1}{2}\sqrt{\Delta(h)})$。這時有兩種情況，第一種情況是其中一個分裂域是另一個分裂域的子域，因而可歸併為一個分裂域，這種情況跟普通不可約二次多項式的情況相似，故有 $\mathrm{Gal}(f) \cong \{I, (12)\}$。

以 $f_3 = x^4 - 4x^3 + 3x^2 + 14x + 26$ 為例，這個多項式可因式分解為 $(x^2+2x+2)(x^2-6x+13)$，其中 x^2+2x+2 的分裂域是 $\mathbb{Q}(i)$，$x^2-6x+13$ 的分裂域則是 $\mathbb{Q}(2i)$。由於 $\mathbb{Q}(i)$ 和 $\mathbb{Q}(2i)$ 互為對方的子域[4]，實質上是同一個分裂域，因此 $\mathrm{Gal}(f_3)$ 跟普通不可約二次多項式的伽羅瓦群相同，只有兩個元素，其中一個是恆等函數，另一個則把 i 映射為 $-i$（並且也把 $2i$ 映射為 $-2i$），故有 $\mathrm{Gal}(f_3) \cong \{I, (12)\}$。

第二種情況則是 $\mathbb{Q}(\sqrt{\Delta(g)})$ 和 $\mathbb{Q}(\sqrt{\Delta(h)})$ 這兩個分裂域互不統屬，在此情況下，f 的分裂域是 $\mathbb{Q}(\sqrt{\Delta(g)}, \sqrt{\Delta(h)})$，並且 $\mathrm{Gal}(f) \cong V$，這裡 V 是我們在《感受伽羅瓦：可解群與單純群》中介紹的「克萊因四元群」，是 S_4 的某個真子群：

$$V = \{I, (12)(34), (13)(24), (14)(23)\} \qquad (5)$$

以 $f_4 = x^4 - 5x^2 + 6$ 為例，這個多項式可因式分解為 $(x^2-2)(x^2-3)$，其中 x^2-2 的分裂域是 $\mathbb{Q}(\sqrt{2})$，x^2-3 的分裂域則是 $\mathbb{Q}(\sqrt{3})$。由於 $\mathbb{Q}(\sqrt{2})$ 和 $\mathbb{Q}(\sqrt{3})$ 互不統屬，可知 f_4 的分裂域是 $\mathbb{Q}(\sqrt{2}, \sqrt{3})$。運用我們在《感受伽羅瓦：自同構》中介紹的方法，不難求得 $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q})$ 包含四個成員，可寫成 $\{I, \theta, \phi, \theta\phi\}$，現把這四個成員對 f_4 的四個根 $\sqrt{2}$、$-\sqrt{2}$、$\sqrt{3}$ 和 $-\sqrt{3}$ 的作用列於下表：

I	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{3}$	$-\sqrt{3}$
θ	$-\sqrt{2}$	$\sqrt{2}$	$\sqrt{3}$	$-\sqrt{3}$
ϕ	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{3}$	$\sqrt{3}$
$\theta\phi$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{3}$	$\sqrt{3}$

現在如對 $\sqrt{2}$、$-\sqrt{2}$、$\sqrt{3}$ 和 $-\sqrt{3}$ 分別給予編號 1、2、3 和 4，那麼根據上表，可知 $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q})$ 同構於 S_4 的下列真子群：

$$\{I, (12), (34), (12)(34)\} \qquad (6)$$

上面 (6) 中的子群雖然表面上跟 (5) 中的子群 V 不一樣，但這兩者其實是同構的，只要運用同構函數 Φ_1 把 (6) 中的元素映射為 (5) 中的元素，其中

[4]這是因為 $\mathbb{Q}(i)$ 中任何元素 $a + bi$（其中 $a, b \in \mathbb{Q}$）都可改寫成 $a + \frac{b}{2}(2i)$，即 $\mathbb{Q}(2i)$ 中元素的形式；反過來，$\mathbb{Q}(2i)$ 中任何元素 $a + b(2i)$（其中 $a, b \in \mathbb{Q}$）都可改寫成 $a + (2b)i$，即 $\mathbb{Q}(i)$ 中元素的形式。

$\Phi_1((12)) = (12)(34), \Phi_1((34)) = (13)(24)$，便可證明 (6) 與 (5) 中的兩個子群同構。由此可以得出結論，$\mathrm{Gal}(f_4) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) \cong V$。

接下來考慮不可約四次首一多項式的情況，這裡要應用這些多項式的判別式。如同三次多項式的情況，為簡化一般四次首一多項式 $f = x^4 + bx^3 + cx^2 + dx + e$ 的判別式，我們先用《感受伽羅瓦：四次方程的根式解》介紹的「契爾恩豪斯變換」，以 $x = y - \frac{b}{4}$ 代入 f，把原來以 x 作為變項的四次首一多項式 f 變換成以 y 作為變項並且其三次項係數為 0 的四次首一多項式 $g = y^4 + py^2 + qy + r$。此外，我們還有以下定理。

定理 5：設 $g = y^4 + py^2 + qy + r$ 是三次項係數為 0 的四次首一多項式，則 g 的判別式等於其三次預解式[5] $h = z^3 - 2pz^2 + (p^2 - 4r)z + q^2$ 的判別式。

由於有上述定理，不可約四次首一多項式的伽羅瓦群可以根據該多項式的三次預解式的判別式來判斷，以下是有關定理。

定理 6：設 g 為不可約四次首一多項式，h 為其三次預解式，

(i) 若 h 不可約並且 $\sqrt{\Delta(h)}$ 不是有理數，則 $\mathrm{Gal}(g) \cong S_4$。

(ii) 若 h 不可約並且 $\sqrt{\Delta(h)}$ 是有理數，則 $\mathrm{Gal}(g) \cong A_4$。

(iii) 若 h 可因式分解為三個一次因式 (包括重複的一次因式) 的乘積，則 $\mathrm{Gal}(g) \cong V$。

(iv) 若 h 可因式分解為一個一次因式與一個不可約二次因式的乘積，並且 g 在 $\mathbb{Q}(\sqrt{\Delta(h)})$ 上不可約，則 $\mathrm{Gal}(g) \cong D_4$。

(v) 若 h 可因式分解為一個一次因式與一個不可約二次因式的乘積，並且 g 在 $\mathbb{Q}(\sqrt{\Delta(h)})$ 上可約，則 $\mathrm{Gal}(g) \cong \mathbb{Z}_4$。

在上述定理中，D_4 代表 8 階二面體群，$\mathbb{Z}_4$ 則代表 4 階循環群 (詳見《感受伽羅瓦：群的基本概念》中的介紹)，這兩個群同構於 S_4 的下列真子群：

$$D_4 \cong \{I, (1234), (13)(24), (1432), (12)(34), (13), (14)(23), (24)\} \qquad (7)$$

$$\mathbb{Z}_4 \cong \{I, (1234), (13)(24), (1432)\} \qquad (8)$$

以下讓我們看一些實例，首先考慮 $g_2 = y^4 - 10y^2 + 1$，有關這個多項式的不可約性質的證明，請參閱本章附錄。根據「定理 5」，g_2 的三次預解式是 $h_1 = z^3 + 20z^2 + 96z$。由於 h_1 可以因式分解為 $z(z + 8)(z + 12)$，根據「定

[5]請注意下列三次預解式跟《感受伽羅瓦：根與係數的關係》中介紹的三次預解式相同。

理 6(iii)」，可知 $\mathrm{Gal}(g_2) \cong V$。

另一方面，運用我們在《感受伽羅瓦：根與係數的關係》中介紹的方法，可以求得 g_2 的四個根為 $\sqrt{2}+\sqrt{3}$、$-\sqrt{2}-\sqrt{3}$、$\sqrt{2}-\sqrt{3}$ 和 $-\sqrt{2}+\sqrt{3}$。由於這四個根都可以寫成 $\sqrt{2}+\sqrt{3}$ 的倍數或冪次，例如 $-\sqrt{2}-\sqrt{3} = -(\sqrt{2}+\sqrt{3})$、$-\sqrt{2}+\sqrt{3} = (\sqrt{2}+\sqrt{3})^{-1}$，$g_2$ 的分裂域可以寫成 $\mathbb{Q}(\sqrt{2}+\sqrt{3})$。可是，我們在《感受伽羅瓦：擴張域》中證明了 $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$，而我們在前面又已證明了 $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}) \cong V$，由此可知 $\mathrm{Gal}(g_2) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}) \cong V$，證實了上面根據「定理 6(iii)」所得的結果。

其次考慮 $g_3 = y^4 - 2$，運用艾森斯坦判別法 (即《感受伽羅瓦：因子分解》中的「定理 8」)，容易證明 g_3 是不可約多項式。根據「定理 5」，g_3 的三次預解式是 $h_2 = z^3 + 8z$。這個預解式可以因式分解為 $z(z^2+8)$，其中 z^2+8 是不可約二次多項式。接著根據「定理 3」，可求得 $\Delta(h_2) = -2048$。由於 $\sqrt{\Delta(h_2)} = 32\sqrt{2}i$，我們有 $\mathbb{Q}(\sqrt{\Delta(h_2)}) = \mathbb{Q}(\sqrt{2}i)$。由於 g_3 在 $\mathbb{R}$ 上可因式分解為 $(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x-\sqrt[4]{2}i)(x+\sqrt[4]{2}i)$，把這四個因式如何組合，都不能把 g_3 改寫成 $(x^2+ax+b)(x^2+cx+d)$ (其中 $a,b,c,d \in \mathbb{Q}(\sqrt{2}i)$) 的形式，因此 g_3 在 $\mathbb{Q}(\sqrt{2}i)$ 上不可約，由此根據「定理 6(iv)」，可知 $\mathrm{Gal}(g_3) \cong D_4$。

另一方面，我們曾在《感受伽羅瓦：伽羅瓦理論基本定理》中詳細討論 g_3，指出 g_3 的分裂域是 $\mathbb{Q}(\sqrt[4]{2}, i)$，並且 $\mathrm{Gal}(g_3) = \{I, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}$，其中 $\alpha^4 = I, \beta^2 = I, \beta\alpha = \alpha^3\beta$。讀者可自行驗證，使用同構函數 Φ_2，其中 $\Phi_2(\alpha) = (1234), \Phi_2(\beta) = (12)(34)$，可以證明上述 $\mathrm{Gal}(g_3)$ 與 (7) 中所示的 D_4 同構，即 $\mathrm{Gal}(g_3) \cong D_4$，證實了上面根據「定理 6(iv)」所得的結果。

接著考慮 $g_4 = y^4 - 4y^2 + 2$，運用艾森斯坦判別法，容易證明 g_4 是不可約多項式。根據「定理 5」，g_4 的三次預解式是 $h_3 = z^3 + 8z^2 + 8z$。這個預解式可以因式分解為 $z(z^2+8z+8)$，其中 z^2+8z+8 是不可約二次多項式。為求 $\Delta(h_3)$，我們先用契爾恩豪斯變換將 h_3 改寫成二次項係數等於 0 的三次多項式 $z^3 - \frac{40}{3}z + \frac{448}{27}$。接著根據「定理 3」，可求得這個三次多項式的判別式是 2048。由此根據「定理 2」，可知 $\Delta(h_3) = 2048$。由於 $\sqrt{\Delta(h_3)} = 32\sqrt{2}$，我們有 $\mathbb{Q}(\sqrt{\Delta(h_3)}) = \mathbb{Q}(\sqrt{2})$。由於 g_4 在 $\mathbb{Q}(\sqrt{2})$ 上可以因式分解為 $(y^2-2-\sqrt{2})(y^2-2+\sqrt{2})$，即 g_4 在 $\mathbb{Q}(\sqrt{2})$ 上可約，根據「定理 6(v)」，可知 $\mathrm{Gal}(g_4) \cong \mathbb{Z}_4$。

另一方面，運用 g_4 的上述因式分解，容易求得 g_4 的四個根為 $\sqrt{2+\sqrt{2}}$、$\sqrt{2-\sqrt{2}}$、$-\sqrt{2+\sqrt{2}}$ 和 $-\sqrt{2-\sqrt{2}}$。接著證明這四個根都屬於 $\mathbb{Q}(\sqrt{2+\sqrt{2}})$，首先由於

$$\left(\sqrt{2+\sqrt{2}}\right)^2 - 2 = \sqrt{2} \qquad (9)$$

可知 $\sqrt{2} \in \mathbb{Q}(\sqrt{2+\sqrt{2}})$；其次由於

$$\begin{aligned}
\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} &= \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} \times \frac{\sqrt{2-\sqrt{2}}}{\sqrt{2-\sqrt{2}}} \\
&= \frac{\sqrt{2}\sqrt{2-\sqrt{2}}}{\sqrt{4-2}} \\
&= \sqrt{2-\sqrt{2}} \qquad (10)
\end{aligned}$$

可知 $\sqrt{2-\sqrt{2}} \in \mathbb{Q}(\sqrt{2+\sqrt{2}})$，由此亦可知 $-\sqrt{2+\sqrt{2}}, -\sqrt{2-\sqrt{2}} \in \mathbb{Q}(\sqrt{2+\sqrt{2}})$。上述結果顯示 g_4 的分裂域可以寫成 $\mathbb{Q}(\sqrt{2+\sqrt{2}})$。

請注意上面 (9) 和 (10) 所示的關係大大限制了 $\mathrm{Gal}(g_4)$ 成員的可能性。設 $\phi_1 \in \mathrm{Gal}(g_4)$，並且 $\phi_1(\sqrt{2+\sqrt{2}}) = \sqrt{2-\sqrt{2}}$，由此根據 (9)，有

$$\begin{aligned}
\phi_1(\sqrt{2}) &= \phi_1\left(\left(\sqrt{2+\sqrt{2}}\right)^2 - 2\right) \\
&= \left(\phi_1\left(\sqrt{2+\sqrt{2}}\right)\right)^2 - 2 \\
&= \left(\sqrt{2-\sqrt{2}}\right)^2 - 2 \\
&= -\sqrt{2}
\end{aligned}$$

由此根據 (10)，又有

$$\begin{aligned}
\phi_1\left(\sqrt{2-\sqrt{2}}\right) &= \phi_1\left(\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}\right) \\
&= \frac{\phi_1(\sqrt{2})}{\phi_1(\sqrt{2+\sqrt{2}})} \\
&= \frac{-\sqrt{2}}{\sqrt{2-\sqrt{2}}} \\
&= -\sqrt{2+\sqrt{2}}
\end{aligned}$$

由此還可進一步求得

$$\phi_1\left(-\sqrt{2+\sqrt{2}}\right) = -\sqrt{2-\sqrt{2}}$$

$$\phi_1\left(-\sqrt{2-\sqrt{2}}\right)=\sqrt{2+\sqrt{2}}$$

以上計算了 $\mathrm{Gal}(g_4)$ 一個成員 ϕ_1 對上述四個根的作用。同理，也可求得 $\mathrm{Gal}(g_4)$ 其餘三個成員 (以下稱為 ϕ_2、ϕ_3 和 I) 對這四個根的作用，現將 I、ϕ_1、ϕ_2 和 ϕ_3 對四個根的作用列於下表：

I	$\sqrt{2+\sqrt{2}}$	$\sqrt{2-\sqrt{2}}$	$-\sqrt{2+\sqrt{2}}$	$-\sqrt{2-\sqrt{2}}$
ϕ_1	$\sqrt{2-\sqrt{2}}$	$-\sqrt{2+\sqrt{2}}$	$-\sqrt{2-\sqrt{2}}$	$\sqrt{2+\sqrt{2}}$
ϕ_2	$-\sqrt{2+\sqrt{2}}$	$-\sqrt{2-\sqrt{2}}$	$\sqrt{2+\sqrt{2}}$	$\sqrt{2-\sqrt{2}}$
ϕ_4	$-\sqrt{2-\sqrt{2}}$	$\sqrt{2+\sqrt{2}}$	$\sqrt{2-\sqrt{2}}$	$-\sqrt{2+\sqrt{2}}$

除了上述 I、ϕ_1、ϕ_2 和 ϕ_3 外，$\mathrm{Gal}(g_4)$ 不可能再有其他成員。現在如對 $\sqrt{2+\sqrt{2}}$、$\sqrt{2-\sqrt{2}}$、$-\sqrt{2+\sqrt{2}}$ 和 $-\sqrt{2-\sqrt{2}}$ 分別給予編號 1、2、3 和 4，那麼根據上表，I、ϕ_1、ϕ_2 和 ϕ_3 分別對應著 S_4 中的成員 I、(1234)、(13)(24) 和 (1432)，而 $\{I,(1234),(13)(24),(1432)\}$ 正好構成上面 (8) 所示的 $\mathbb{Z}_4$，由此我們有 $\mathrm{Gal}(g_4)\cong\mathbb{Z}_4$，證實了上面根據「定理 6(v)」所得的結果。

最後考慮 $g_5=y^4+8y+12$，有關這個多項式的不可約性質的證明，請參閱本章附錄。根據「定理 5」，g_5 的三次預解式是 $h_4=z^3-48z+64$，實質上等於前面討論過的 g_1，由此可知 h_4 不可約並且 $\sqrt{\Delta(h_4)}=576$ 是有理數。根據「定理 6(ii)」，可知 $\mathrm{Gal}(g_5)\cong A_4$。

另一方面，運用我們在上面求得的 g_1 的三個根以及《感受伽羅瓦：根與係數的關係》中介紹的方法，可以求得 g_5 的四個根為 $y_1=\frac{1}{2}(\sqrt{-8\cos\frac{2\pi}{9}}+\sqrt{-8\cos\frac{8\pi}{9}}+\sqrt{-8\cos\frac{14\pi}{9}})$、$y_2=\frac{1}{2}(\sqrt{-8\cos\frac{2\pi}{9}}-\sqrt{-8\cos\frac{8\pi}{9}}-\sqrt{-8\cos\frac{14\pi}{9}})$、$y_3=\frac{1}{2}(-\sqrt{-8\cos\frac{2\pi}{9}}+\sqrt{-8\cos\frac{8\pi}{9}}-\sqrt{-8\cos\frac{14\pi}{9}})$ 和 $y_4=\frac{1}{2}(-\sqrt{-8\cos\frac{2\pi}{9}}-\sqrt{-8\cos\frac{8\pi}{9}}+\sqrt{-8\cos\frac{14\pi}{9}})$。

由於在上述四個根中，$8\cos\frac{2\pi}{9}$、$8\cos\frac{8\pi}{9}$ 和 $8\cos\frac{14\pi}{9}$ 被置於根號之下，我們不能使用上面的 (2) — (4) 化簡這四個根之間的關係，故只能把 g_5 的分裂域寫成 $\mathbb{Q}(y_1,y_2,y_3,y_4)$，而無法深入討論其內部結構，因此以下我們只解釋究竟是甚麼因素令 $\mathrm{Gal}(g_5)$ 不同構於 S_4。

根據「定理 5」，$\Delta(g_5)=\Delta(h_4)=\Delta(g_1)=331776$。由於 $\sqrt{\Delta(g_5)}=576\in\mathbb{Q}$，若 $\psi\in\mathrm{Gal}(g_5)$，必有 $\psi(\sqrt{\Delta(g_5)})=\sqrt{\Delta(g_5)}$。但根據 (1)，

$$\sqrt{\Delta(g_5)}=(y_1-y_2)(y_1-y_3)(y_1-y_4)(y_2-y_3)(y_2-y_4)(y_3-y_4)$$

因此 ψ 必須令上式右端的值不變。可是，如果 ψ 是對 $(y_1y_2y_3y_4)$ 的奇排列，則 ψ 並不滿足上述條件。舉例說，如果 ψ_1 是把 y_1 與 y_2 對調但保持 y_3 和 y_4 不變的排列，則 ψ_1 是奇排列，而

$$\begin{aligned}\psi_1(\sqrt{\Delta(g_5)}) &= \psi_1((y_1-y_2)(y_1-y_3)(y_1-y_4)(y_2-y_3)(y_2-y_4)(y_3-y_4))\\ &= (y_2-y_1)(y_2-y_3)(y_2-y_4)(y_1-y_3)(y_1-y_4)(y_3-y_4)\\ &= -(y_1-y_2)(y_1-y_3)(y_1-y_4)(y_2-y_3)(y_2-y_4)(y_3-y_4)\\ &= -\sqrt{\Delta(g_5)}\end{aligned}$$

上述結果顯示 $\psi_1(\sqrt{\Delta(g_5)}) \neq \sqrt{\Delta(g_5)}$，因此 $\psi_1 \notin \Delta(g_5)$。由此可見 $\mathrm{Gal}(g_5)$ 不包含對 $(y_1y_2y_3y_4)$ 的任何奇排列，因此不同構於 S_4，而同構於只包含偶排列的 A_4。請注意如果 $\sqrt{\Delta(g_5)} \notin \mathbb{Q}$，那麼我們便只有 $\psi(\Delta(g_5)) = \Delta(g_5)$ (根據「定理 1(ii)」)，而沒有 $\psi(\sqrt{\Delta(g_5)}) = \sqrt{\Delta(g_5)}$，因此正是 $\sqrt{\Delta(g_5)} \in \mathbb{Q}$ 此一因素使得 $\mathrm{Gal}(g_5)$ 不同構於 S_4。

附錄

本章正文提出了若干個不可約多項式，本附錄提供該等多項式不可約性質的證明。

(1) $g_1 = y^3 - 48y + 64$

先把 g_1 轉化為 $\mathbb{Z}_5[x]$ 中的對應多項式 ${g_1}^* = y^3 + 2y + 4$，由於 ${g_1}^*$ 是三次多項式，若它可約，則必包含至少一個一次因式，即必在 $\mathbb{Z}_5$ 中包含至少一個根。由於在 $\mathbb{Z}_5$ 下，${g_1}^*(0)$、${g_1}^*(1)$、${g_1}^*(2)$、${g_1}^*(3)$ 和 ${g_1}^*(4)$ 都不等於 0，故知 ${g_1}^*$ 在 $\mathbb{Z}_5[x]$ 中不可約。由此根據《感受伽羅瓦：因子分解》中的「定理 7」，可知 g_1 在 $\mathbb{Q}[x]$ 中不可約。

(2) $g_2 = y^4 - 10y^2 + 1$

根據《感受伽羅瓦：因子分解》中的「定理 9」，有理數 $\frac{a}{b}$ 是 g_2 的根當且僅當 $a \mid 1$ 並且 $b \mid 1$，因此 g_2 的可能有理數根包括 ± 1。由於 $g_2(1)$ 和 $g_2(-1)$ 都不等於 0，故知 g_2 沒有有理數根，即 g_2 不能在 $\mathbb{Q}[x]$ 中因式分解為一個一次因式與一個三次因式的乘積。

但我們還要證明 g_2 不能在 $\mathbb{Q}[x]$ 中因式分解為兩個不可約二次因式的乘積，為此，先把 g_2 寫成兩個二次因式的乘積如下 (其中 k、l 和 n 是有理

數)[6]：

$$\begin{aligned} y^4 - 10y^2 + 1 &= (y^2 + ky + l)(y^2 - ky + n) \\ &= y^4 + (-k^2 + l + n)y^2 + (kn - kl)y + ln \end{aligned}$$

從上式左右兩端的各個係數，可得到以下聯立方程：

$$\begin{cases} -k^2 + l + n = -10 & (11) \\ k(n - l) = 0 & (12) \\ ln = 1 & (13) \end{cases}$$

從 (12) 可得 $k = 0$ 或 $n = l$。假設 $k = 0$，則從 (11) 和 (13) 可得二次方程 $l^2 + 10l + 1 = 0$，這個二次方程顯示 l 不可能是有理數。假設 $n = l$，則從 (13) 可得 $l = n = \pm 1$，再從 (11) 可得 $k^2 = 12$ 或 $k^2 = 8$，在這兩種情況下 k 都不可能是有理數。以上討論顯示，k、l 和 n 不可能全是有理數，因此 g_2 不能在 $\mathbb{Q}[x]$ 中分解為兩個不可約二次因式的乘積。總上所述，g_2 在 $\mathbb{Q}[x]$ 中不可約。

(3) $g_5 = y^4 + 8y + 12$

根據《感受伽羅瓦：因子分解》中的「定理 9」，有理數 $\frac{a}{b}$ 是 g_5 的根當且僅當 $a \mid 12$ 並且 $b \mid 1$，因此 g_5 的可能有理數根包括 ± 1、± 2、± 3、± 4、± 6 和 ± 12。由於把上述有理數逐一代入 g_5 的結果都不是 0，故知 g_5 沒有有理數根，即 g_5 不能在 $\mathbb{Q}[x]$ 中分解為一個一次因式與一個三次因式的乘積。

接著證明 g_5 在 $\mathbb{Z}_5[x]$ 中的對應多項式 ${g_5}^* = y^4 + 3y + 2$ 不能分解為兩個二次因式的乘積，為此可以展開所有形如 $(y^2 + ky + l)(y^2 - ky + n)$ 的乘積，看看是否等於 ${g_5}^*$，其中 k、l 和 n 是 $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ 中的成員，$-k$ 代表 k 在 $\mathbb{Z}_5$ 中的逆元 (例如 1 在 $\mathbb{Z}_5$ 中的逆元是 4)。由於 ${g_5}^*$ 的常數項是 2，在上述乘積中，l 和 n 的選擇只能是一個是 1 另一個是 2，或者一個是 3 另一個是 4。舉例說，若取 $k = 0, l = 1, n = 2$，則 $(y^2+1)(y^2+2) = y^4+3y^2+2$，由此可見 ${g_5}^*$ 不能因式分解為 $(y^2 + 1)(y^2 + 2)$。經展開所有可能情況後，便會看到 ${g_5}^*$ 不能分解為兩個二次因式的乘積。但根據《感受伽羅瓦：因子分解》中的「定理 7」，若 g_5 可分解為兩個二次因式的乘積，則 ${g_5}^*$ 必也可分解為兩個二次因式的乘積，由此證明了 g_5 不能分解為兩個二次因式的乘積。總上所述，g_5 在 $\mathbb{Q}[x]$ 中不可約。

連結至數學專題
連結至周家發網頁

[6]以下把兩個二次因式的一次項係數分別設定為 k 和 $-k$，這樣可以確保這兩個二次因式的乘積的三次項係數等於 0，與 g_2 的三次項係數一致。