感受伽羅瓦：根式擴張與根式解

至止我們已介紹伽羅瓦理論的核心內容，本章將介紹伽羅瓦理論的一個重要應用－判斷多項式方程是否存在根式解的問題，為此，須先弄清楚何謂根式解。設 F 為域，E 為其擴張域。如果 $E = F(a_1, \ldots, a_k)$，並且存在正整數 n_1、...、n_k，使得

$$\begin{aligned} a_1^{n_1} &\in F \\ a_2^{n_2} &\in F(a_1) \\ a_3^{n_3} &\in F(a_1, a_2) \qquad (1) \\ &\vdots \\ a_k^{n_k} &\in F(a_1, a_2, \ldots, a_{k-1}) \end{aligned}$$

則 $E : F$ 稱為根式擴張(radical extension)。舉例說，$\mathbb{C} : \mathbb{R}$ 便是根式擴張，這是因為我們有 $\mathbb{C} = \mathbb{R}(i)$，其中 $i^2 = -1 \in \mathbb{R}$，符合上述定義。另外又如 $\mathbb{Q}(\sqrt[3]{5}, \sqrt{1+\sqrt[3]{5}})$ 也是根式擴張，這是因為我們有 $(\sqrt[3]{5})^3 \in \mathbb{Q}$ 並且 $(\sqrt{1+\sqrt[3]{5}})^2 \in \mathbb{Q}(\sqrt[3]{5})$，符合上述定義。

根據上述定義，任何根式擴張都是代數擴張 (請參閱《感受伽羅瓦：代數擴張與超越擴張》的有關定義)。為證明這一點，我們要運用以下定理。

定理 1：若 $E : K$ 和 $K : F$ 是代數擴張，則 $E : F$ 也是代數擴張。

現在考慮 $F(a_1) : F$，任選 $F(a_1)$ 中的元素，這個元素具有 $b_1 a_1 + b_2$ (其中 $b_1, b_2 \in F$) 的形式。這個元素當然是 $F(a_1)$ 的代數元，因為它是 $F(a_1)[x]$ 中多項式方程 $x - (b_1 a_1 + b_2) = 0$ 的根，我們要證明的是這個元素是 F 中的代數元。為此，我們把上述方程轉化為 $F[x]$ 中的方程，如以下步驟所示：

$$\begin{aligned} x - (b_1 a_1 + b_2) &= 0 \qquad (2) \\ x - b_2 &= b_1 a_1 \\ (x - b_2)^{n_1} &= {b_1}^{n_1} {a_1}^{n_1} \\ (x - b_2)^{n_1} - {b_1}^{n_1} {a_1}^{n_1} &= 0 \qquad (3) \end{aligned}$$

請注意由於 $b_1a_1+b_2$ 是 (2) 的根，它也是 (3) 的根。由於根據上述假設，$b_1,b_2\in F$，而根據 (1)，也有 $a_1^{n_1}\in F$，把 (3) 左端展開後可得到 $F[x]$ 中的多項式，由此證得 $b_1a_1+b_2$ 是 $F[x]$ 中多項式方程 (即 (3)) 的根，故為 F 上的代數元，因此 $F(a_1):F$ 是代數擴張。

接著考慮 $F(a_1,a_2):F(a_1)$，任選 $F(a_1,a_2)$ 中的元素，這個元素具有 $c_1a_2+c_2$ (其中 $c_1,c_2\in F(a_1)$) 的形式。利用與上面相似的推理，容易證明 $c_1a_2+c_2$ 是 $(x-c_2)^{n_2}-{c_1}^{n_2}{a_2}^{n_2}=0$ 的根。由於根據上述假設，$c_1,c_2\in F(a_1)$，而根據 (1)，也有 $a_2^{n_2}\in F(a_1)$，故知 $(x-c_2)^{n_2}-{c_1}^{n_2}{a_2}^{n_2}=0$ 是 $F(a_1)[x]$ 中的多項式方程，因此 $c_1a_2+c_2$ 是 $F(a_1)$ 上的代數元，由此證得 $F(a_1,a_2):F(a_1)$ 是代數擴張。

由於我們證明了 $F(a_1,a_2):F(a_1)$ 和 $F(a_1):F$ 都是代數擴張，根據「定理 1」，可知 $F(a_1,a_2):F$ 也是代數擴張。只要繼續運用上述推理思路，便可證明 $F(a_1,\ldots,a_k):F$ 是代數擴張，由此證得以下定理。

定理 2：任何根式擴張都是代數擴張。

從根式擴張我們可以得到一個多項式有根式解的定義。設 f 為域 F 上的多項式，K 為 f 的分裂域 (即包含 F 和 f 所有根的最小的域)。如果存在一個域 E 使得 $K\subseteq E$ 並且 $E:F$ 是根式擴張，我們便說 f 在 F 上有根式解(solvable by radicals)。直觀地說，多項式方程 f 在 F 上有根式解，就是指 f 的所有根都可透過對 F 上元素進行有限次加、減、乘、除和開方運算而得到。

根據上述定義，$\mathbb{C}[x]$ 中任何多項式 f 在 $\mathbb{C}$ 上都有根式解，這是因為根據「代數基本定理」(即《感受伽羅瓦：因子分解》中的「定理 6」)，$\mathbb{C}[x]$ 中任何多項式的所有根都在 $\mathbb{C}$ 中，因此 $\mathbb{C}$ 就是 f 的分裂域，而 $\mathbb{C}:\mathbb{C}$ 是根式擴張，因為 $\mathbb{C}$ 等同於 $\mathbb{C}(1)$，其中 $1^1\in\mathbb{C}$。由此根據上述定義，可知 f 有根式解。直觀地看，由於 f 的每一個根都在 $\mathbb{C}$ 中，我們可透過對 $\mathbb{C}$ 中元素進行零次加、減、乘、除和開方運算而得到 f 的所有根。

不僅如此，$\mathbb{R}[x]$ 中任何多項式 f 在 $\mathbb{R}$ 上都有根式解，這是因為 $\mathbb{R}[x]$ 中的任何多項式都可看成 $\mathbb{C}[x]$ 中的多項式，因此根據「代數基本定理」，$\mathbb{R}[x]$ 中任何多項式的所有根都在 $\mathbb{C}$ 中，由此可知 $\mathbb{C}$ 包含 f 的分裂域，而我們在前面已證明了 $\mathbb{C}:\mathbb{R}$ 是根式擴張。由此根據上述定義，可知 f 有根式解。直觀地看，f 的每一個根要麼是實數，要麼是形如 $a+bi$ (其中 $a,b\in\mathbb{R}$) 的複數。如屬前者，我們可透過對 $\mathbb{R}$ 中元素進行零次加、減、乘、除和開方運算而得到這個根；如屬後者，我們可以先對實數 -1 進行開平方運算得到 i，把 i 與實數 b 相乘，然後再把結果與實數 a 相加，從而得到這個根。

我們還可以借助群的可解性來判斷多項式是否有根式解，為此先要引入

多項式的伽羅瓦群的概念。設 f 為域 F 上的多項式，E 為 f 的分裂域，則 $\mathrm{Gal}(E:F)$ 稱為 f 的伽羅瓦群，記作 $\mathrm{Gal}(f)$。以下是本章的最重要定理。

定理 3：設 F 為特徵為 0 的域，f 為 $F[x]$ 中的多項式，則 f 在 F 上有根式解當且僅當 $\mathrm{Gal}(f)$ 是可解群。

上述定理說明了上一章介紹的「可解群」與多項式方程「根式解」的存在性的密切關係，現在讀者應可明白為何要把上一章中滿足某些特定條件的群稱為可解群。上述定理用到域的「特徵」的概念，我們在《感受伽羅瓦：擴張域》中曾經介紹這個概念，這是指使得 n 個 1 相加之和等於 0 的最小正整數 n，如無這樣的正整數，則規定域的特徵為 0。根據此一定義，$\mathbb{C}$、$\mathbb{R}$ 和 $\mathbb{Q}$ 都是特徵為 0 的域，因此以下我們只討論這幾個域上的多項式是否有根式解的問題。

以下是上述定理在 $\mathbb{C}$ 和 $\mathbb{R}$ 上的應用。設 f 為 $\mathbb{C}[x]$ 中的多項式，如前所述，f 的分裂域就是 $\mathbb{C}$，因此 $\mathrm{Gal}(f)=\mathrm{Gal}(\mathbb{C}:\mathbb{C})=\{I\}$。由於這個群等同於對稱群 S_1，而我們在上一章證明了 S_1 是可解群，由此根據上述定理，可知 f 在 $\mathbb{C}$ 上必有根式解。

現在設 f 為 $\mathbb{R}[x]$ 中的多項式，這有兩種可能性：(i) f 的根全是實數；(ii) f 有至少一個根是 (非實數) 複數。在情況 (i) 下，f 的分裂域是 $\mathbb{R}$，因此 $\mathrm{Gal}(f)=\mathrm{Gal}(\mathbb{R}:\mathbb{R})=\{I\}$。如上段所述，這個群等同於可解群 S_1，由此根據上述定理，可知 f 必有根式解。在情況 (ii) 下，f 的分裂域是 $\mathbb{R}(i)=\mathbb{C}$，這是因為只需把 i 添加到 $\mathbb{R}$ 中並將其擴張成域，便可得到全體複數。因此 $\mathrm{Gal}(f)=\mathrm{Gal}(\mathbb{C}:\mathbb{R})$，而我們在《感受伽羅瓦：自同構》中曾指出 $\mathrm{Gal}(\mathbb{C}:\mathbb{R})=\{I,\bar{}\}$。由於這個群同構於 S_2[1]，而我們在上一章證明了 S_2 是可解群，由此根據上述定理，可知 f 必有根式解。至此證明了在上述情況 (i) 和 (ii) 下，f 在 $\mathbb{R}$ 上都有根式解。

雖然上面證明了 $\mathbb{C}[x]$ 和 $\mathbb{R}[x]$ 中的任何多項式都有根式解，但此一結論沒有很大實質意義。首先，此一結論只告訴我們「存在」這樣的根式解，但完全沒有提供這些根式解的公式或者推導方法。其次，求多項式方程根式解的目的是要透過對某些已知的數進行有限次加、減、乘、除和開方運算來表達方程的根，但我們對實數和 (非實數) 複數所知甚少，我們所熟悉的數絕大多數是有理數以及有理數的開方根，此外還有一些特殊常數 (例如圓周率 π 和虛數單位 i) 和特殊函數 (例如三角函數、指數函數、對數函數等) 的值。但這些加起來只佔全體實數和 (非實數) 複數的一小部分。因此從實用的角度看，在研究多項式的根式解時，應主要以 $\mathbb{Q}[x]$ 中的多項式作為研究對象。

[1]由於 $\bar{}\circ\bar{}=I$，$\bar{}$ 是這個群的生成元，因此這個群與僅包含兩個元素的循環群 S_2 同構。

接下來就讓我們考慮 $\mathbb{Q}[x]$ 中多項式的根式解，首先請注意我們不能像前面那樣運用「代數基本定理」來證明 $\mathbb{Q}[x]$ 中任何多項式 f 在 $\mathbb{Q}$ 上都有根式解，這是因為雖然我們也能運用「代數基本定理」來證明 $\mathbb{C}$ 包含 f 的分裂域，但 $\mathbb{C}:\mathbb{Q}$ 卻不是根式擴張。事實上，由於 $\mathbb{C}$ 包含超越數，$\mathbb{C}:\mathbb{Q}$ 是超越擴張而非代數擴張，因此根據「定理 2」，它不可能是根式擴張。基於上述討論，我們不能一概而論，說 $\mathbb{Q}[x]$ 中的任何多項式都有或沒有根式解, 而是必須分門別類, 就每類多項式應用「定理 3」判斷其是否有根式解。

為應用「定理 3」，須先找出多項式的伽羅瓦群。設有 $\mathbb{Q}[x]$ 中的 n 次多項式 $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ (其中 $a_n, a_{n-1}, \ldots, a_1, a_0 \in \mathbb{Q}$)，$r$ 為 f 的 n 個根中的任何一個，並設 θ 為 $\mathrm{Gal}(f)$ 的成員，即以全體有理數為不動點的自同構，那麼根據自同構的定義，我們有

$$\begin{aligned} 0 &= \theta(0) \\ &= \theta(a_n r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0) \\ &= a_n(\theta(r))^n + a_{n-1}(\theta(r))^{n-1} + \cdots + a_1(\theta(r)) + a_0 \end{aligned}$$

上述計算結果顯示，$\theta(r)$ 是 f 的根。由此可見，$\mathrm{Gal}(f)$ 的成員把 f 的根映射為 f 的根，即 $\mathrm{Gal}(f)$ 的成員是對 f 的根的排列。由於 f 共有 n 個根，因此 $\mathrm{Gal}(f)$ 就是 n 元集合的排列組成的群，這個群可以是包含所有可能排列的 S_n，也可以是 S_n 的某個真子群。

以三次多項式方程 $f_1 = x^3 - 2$ 為例，我們在《感受伽羅瓦：代數擴張與超越擴張》中指出這個多項式的分裂域是 $\mathbb{Q}(\sqrt[3]{2}, \omega_3)$，並在《感受伽羅瓦：伽羅瓦對應》中指出 $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega_3) : \mathbb{Q})$ (即 $\mathrm{Gal}(f_1)$) 就是以下的群：

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega_3) : \mathbb{Q}) = \{I, \gamma, \delta, \delta^2, \gamma\delta, \gamma\delta^2\} \qquad (4)$$

其中 $\gamma(\sqrt[3]{2}) = \omega_3(\sqrt[3]{2})$，$\gamma(\omega_3) = {\omega_3}^2$，$\delta(\sqrt[3]{2}) = {\omega_3}^2(\sqrt[3]{2})$ 以及 $\delta(\omega_3) = \omega_3$。現把 (4) 中六個成員對 f_1 三個根 (即 $\sqrt[3]{2}$、$\omega_3(\sqrt[3]{2})$ 和 ${\omega_3}^2(\sqrt[3]{2})$) 的作用列於下表：

I	$\sqrt[3]{2}$	$\omega_3(\sqrt[3]{2})$	${\omega_3}^2(\sqrt[3]{2})$
γ	$\omega_3(\sqrt[3]{2})$	$\sqrt[3]{2}$	${\omega_3}^2(\sqrt[3]{2})$
δ	${\omega_3}^2(\sqrt[3]{2})$	$\sqrt[3]{2}$	$\omega_3(\sqrt[3]{2})$
δ^2	$\omega_3(\sqrt[3]{2})$	${\omega_3}^2(\sqrt[3]{2})$	$\sqrt[3]{2}$
$\gamma\delta$	${\omega_3}^2(\sqrt[3]{2})$	$\omega_3(\sqrt[3]{2})$	$\sqrt[3]{2}$
$\gamma\delta^2$	$\sqrt[3]{2}$	${\omega_3}^2(\sqrt[3]{2})$	$\omega_3(\sqrt[3]{2})$

從上表可以看到，(4) 中每個成員都把 $\{\sqrt[3]{2}, \omega_3(\sqrt[3]{2}), {\omega_3}^2(\sqrt[3]{2})\}$ 這個集合的成員映射為該集合的成員，即都是對這個集合的排列，而且 (4) 中六個成

員窮盡了對這個集合的全部六種可能排列。

事實上，如對 $\sqrt[3]{2}$、$\omega_3(\sqrt[3]{2})$ 和 ${\omega_3}^2(\sqrt[3]{2})$ 分別給予編號 1、2 和 3，那麼根據上表，γ 的作用是把 1 和 2 對調並使 3 不變，相當於 (12) 這個排列，(4) 中其他元素也各自相當於對稱群 S_3 的某個元素，因此我們可以把 (4) 看成與 S_3 同構。以下列出 S_3 的元素，其元素的排列次序與 (4) 中對應元素的排列次序相同 (即 I 對應著 I、γ 對應著 (12) 等等)：

$$S_3 = \{I, (12), (132), (123), (13), (23)\} \qquad (5)$$

讀者可自行驗證，(4) 與 (5) 中的對應元素滿足同構關係的定義，例如由於 γ 與 (12) 對應並且 δ 與 (132) 對應，我們應有 $\gamma \circ \delta$ 與 $(12) \circ (132)$ 對應，即 $\gamma\delta$ 與 (13) 對應，而事實的確如此。

接著考慮四次多項式方程 $f_2 = x^4 - 2x^2 - 3$，這個多項式的四個根是 $\sqrt{3}$、$-\sqrt{3}$、i 和 $-i$，因此其分裂域是 $\mathbb{Q}(\sqrt{3}, i)$。如前所述，$\mathrm{Gal}(\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q})$ (即 $\mathrm{Gal}(f_2)$) 的成員應是集合 $\{\sqrt{3}, -\sqrt{3}, i, -i\}$ 上的排列，但 $\mathrm{Gal}(\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q})$ 不能包含這個集合上的所有可能排列。例如它不能包含這樣的排列 θ_1，使得 $\theta_1(\sqrt{3}) = i$，這是因為如果存在這樣的 θ_1，那麼便會有

$$3 = \theta_1(3) = \theta_1(\sqrt{3} \times \sqrt{3}) = \theta_1(\sqrt{3}) \times \theta_1(\sqrt{3}) = i \times i = -1$$

但 $3 \neq -1$。由此可以推斷，$\mathrm{Gal}(\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q})$ 的成員只能把 $\{\sqrt{3}, -\sqrt{3}\}$ 中的成員映射為這個集合的成員，並把 $\{i, -i\}$ 中的成員也映射為這個集合的成員，所以只能包括四個成員，以下分別稱為 I、α、β 和 $\alpha\beta$，即

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}) = \{I, \alpha, \beta, \alpha\beta\} \qquad (6)$$

下表列出 (6) 中四個成員對 f_2 四個根的作用：

I	$\sqrt{3}$	$-\sqrt{3}$	i	$-i$
α	$-\sqrt{3}$	$\sqrt{3}$	i	$-i$
β	$\sqrt{3}$	$-\sqrt{3}$	$-i$	i
$\alpha\beta$	$-\sqrt{3}$	$\sqrt{3}$	$-i$	i

現在如對 $\sqrt{3}$、$-\sqrt{3}$、i 和 $-i$ 分別給予編號 1、2、3 和 4，那麼根據上表，α 相當於 (12) 這個排列，其餘類推。因此我們可以把 (6) 看成與以下由 (12) 和 (34) 生成的群同構，以下把這個群記作 $\langle (12), (34) \rangle$(下列元素的排列次序與 (6) 中對應元素的排列次序相同)：

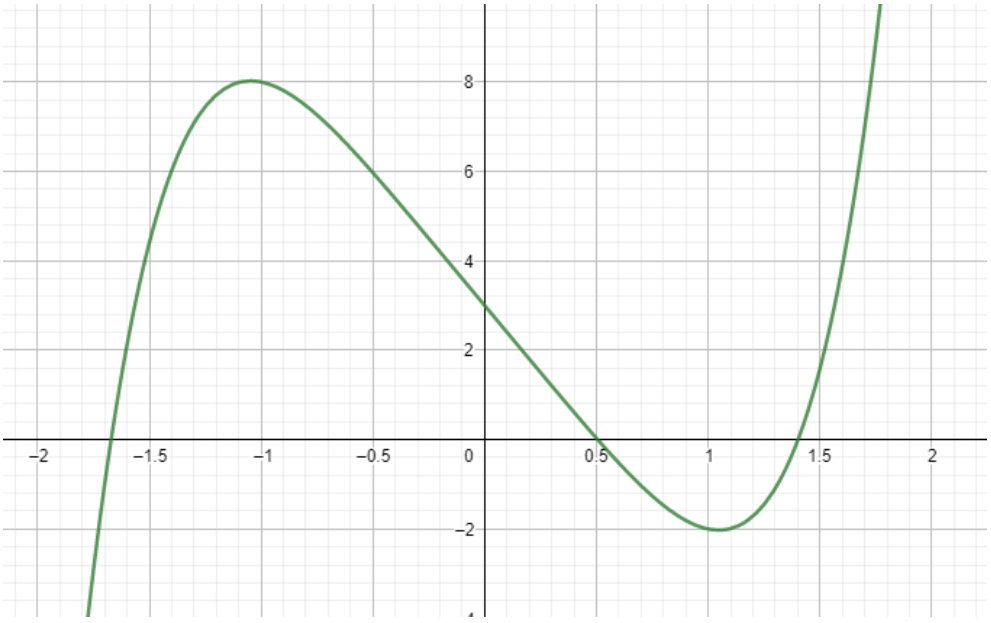
$$\langle (12), (34) \rangle = \{I, (12), (34), (12)(34)\} \qquad (7)$$

請注意 $\langle (12), (34) \rangle$ 是 S_4 的子群。

以上討論顯示，任何 n 次多項式方程的伽羅瓦群都與對稱群 S_n 或其真子群同構，由於我們在上一章已證明了 S_1、S_2、S_3 和 S_4 都是可解群，而根據上一章的「定理 9」，任何可解群的子群都是可解群，因此根據上面的「定理 3」，任何一次、二次、三次和四次多項式都有根式解。事實上，我們在《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》和《感受伽羅瓦：四次方程的根式解》中介紹了求二次、三次和四次多項式方程根式解的一般方法，由此驗證了上述結論。

五次或更高次多項式方程的情況又如何？我們在上一章證明了若 $n \geq 5$，則 S_n 和 A_n 不是可解群。由此根據上面的「定理 3」，可知五次或更高次多項式方程不一定有根式解，但也不能馬上推斷必定存在沒有根式解的五次或更高次多項式方程。為得出這個結論，必須找出這樣的五次或更高次多項式，這些多項式的伽羅瓦群與 S_n、A_n 或其他不可解群同構。

以下讓我們證明五次多項式 $f_3 = x^5 - 6x + 3$ 的伽羅瓦群與 S_5 同構。如把 f_3 的五個根記作 α_1、α_2、α_3、α_4 和 α_5，那麼 f_3 的分裂域可以寫作 $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$，因此 $\mathrm{Gal}(f_3) = \mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) : \mathbb{Q})$。根據前面的討論，這個伽羅瓦群的成員必然是對 $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$ 中元素的排列。現在首先證明這個伽羅瓦群必然包含至少一個對換，為此要證明 f_3 恰好有三個實數根，以下是 f_3 的圖象：



上圖顯示 f_3 至少有三個實數根。事實上，由於 $f_3(-2) = -17$，$f_3(-1) = 8$，$f_3(0) = 3$，$f_3(1) = -2$ 和 $f_3(2) = 23$，而且 f_3 是連續函數，可知 f_3 至少在 -2 與 -1 之間、0 與 1 之間以及 1 與 2 之間有實數根。為證明 f_3 沒有更

多實數根，我們要應用數學分析上的以下定理。

定理 4 (羅爾定理Rolle's Theorem)：若實值函數 f 在閉區間 $[a,b]$ 上連續並在開區間 (a,b) 上可微，並且 $f(a)=f(b)$，則存在 $c\in(a,b)$ 使得 $f'(c)=0$。

由於多項式 f_3 在 $(-\infty,\infty)$ 上連續且可微，故可應用上述定理。根據上述定理，如果 α_1 和 α_2 是 f_3 的實數根 (即 $f_3(\alpha_1)=f_3(\alpha_2)=0$)，則必有至少一個 $c\in(\alpha_1,\alpha_2)$ 使得 ${f_3}'(c)=0$。由此可以推斷，如果 f_3 有至少四個相異實數根，則 ${f_3}'=5x^4-6$ 有至少三個相異實數根。但運用我們在《感受伽羅瓦：二次方程與複數》介紹的方法，容易求得 ${f_3}'$ 只有兩個相異實數根：$\pm\sqrt[4]{\frac{6}{5}}$，因此 f_3 不可能有四個或更多相異實數根。

此外，根據「艾森斯坦判別法」(即《感受伽羅瓦：因子分解》中的「定理 8」)，f_3 在 $\mathbb{Q}$ 上不可約，而如前所述，$\mathbb{Q}$ 是特徵為 0 的域，由此根據《感受伽羅瓦：伽羅瓦擴張》中的「定理 3」，可知 f_3 是可分多項式，即沒有重根的多項式 (請參閱該網頁的相關定義)，由此可知 f_3 的上述三個實數根都不是重根。總括以上討論，可知 f_3 恰好有三個實數根，其餘兩個根都是複數根。由此根據以下定理，

定理 5 (共軛複數根定理Complex Conjugate Root Theorem)：若實係數多項式 f 有複數根 $a+bi$，則 $a-bi$ 也是 f 的根。

可知 f_3 必有一對互為共軛複數的根，因此必有 $^-\in\mathrm{Gal}(\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5):\mathbb{Q})$[2]。把 $^-$ 作用於 f_3 的三個實數根中的任何一個，所得結果仍是該實數根；把 $^-$ 作用於 f_3 的兩個複數根中的任何一個，所得結果是另一個複數根。換句話說，$^-$ 把 f_3 的兩個複數根對調，並保持其餘三個實數根不變，因此可以表示成一個對換，至此證得 $\mathrm{Gal}(\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5):\mathbb{Q})$ 必然包含一個對換。

其次證明 $\mathrm{Gal}(\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5):\mathbb{Q})$ 必然包含至少一個具有單重五循環結構的成員，為此要應用以下定理。

定理 6 (柯西定理Cauchy's Theorem)：設 G 為有限群，p 為正質數，若 $|G|$ 能被 p 整除，則 G 包含一個 p 階元素[3]。

我們在《感受伽羅瓦：代數擴張與超越擴張》中曾經討論 f_3，並指出 (在

[2] $^-$ 代表把複數映射為其共軛複數的函數。我們在《感受伽羅瓦：自同構》中論證了 $^-$ 是自同構，這個自同構以全體實數作為不動點 (因而也以全體有理數作為不動點)，而 $\mathrm{Gal}(\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5):\mathbb{Q})$ 代表 $\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5)$ 上以全體有理數作為不動點的自同構，故有 $^-\in\mathrm{Gal}(\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5):\mathbb{Q})$。

[3] 根據《感受伽羅瓦：群的基本概念》中的定義，群 G 的元素 a 的階就是使 a^n 等於 G 中單位元的最小正整數 n。

下式中，α_1 是 f_3 的任意一個根)：

$$\mathbb{Q}(\alpha_1) = \{a{\alpha_1}^4 + b{\alpha_1}^3 + c{\alpha_1}^2 + d\alpha_1 + e : a, b, c, d, e \in \mathbb{Q}\}$$

從上式可得 $|\mathbb{Q}(\alpha_1) : \mathbb{Q}| = 5$。由此根據《感受伽羅瓦：擴張域》中的「定理 1」，可知 $|\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) : \mathbb{Q}|$ 必能被 5 整除。由此再根據「伽羅瓦理論基本定理」(即《感受伽羅瓦：伽羅瓦理論基本定理》中的「定理 1」) 的 (iv)(a)，可知 $|\mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) : \mathbb{Q})|$ 也必能被 5 整除。由於 5 是正質數，根據上面的「定理 6」，可知 $\mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) : \mathbb{Q})$ 包含一個五階元素。由於在 S_5 中，只有具有單重五循環結構的成員 (例如 (12345)) 才是五階元素,由此可知 $\mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) : \mathbb{Q})$ 必然包含這樣的成員。

最後證明 $\mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) : \mathbb{Q})$ 與 S_5 同構。由於這個伽羅瓦群包含一個對調 f_3 的兩個複數根的對換，如果對這兩個複數根給予編號 1 和 2，可以把這個對換寫成 (12)。此外，由於這個伽羅瓦群包含一個單重五循環，不論在這個五循環中 1 和 2 處於甚麼位置，我們總能通過取這個五循環的適當冪次而得到一個 2 處於緊貼 1 右面位置的五循環，例如如果該五循環是 $(21abc)$，那麼 $(21abc)^4 = (12cba)$。因此透過對 f_3 的三個實數根給予適當編號，我們可以保證 $\mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) : \mathbb{Q})$ 包含著 (12) 和 (12345) 這兩個元素。

從 (12) 和 (12345) 我們逐一生成以下元素，首先我們有

$$\begin{aligned}
(12345) \circ (12) \circ (12345)^{-1} &= (23) \\
(12345) \circ (23) \circ (12345)^{-1} &= (34) \\
(12345) \circ (34) \circ (12345)^{-1} &= (45)
\end{aligned}$$

由此我們有

$$\begin{aligned}
(12) \circ (23) \circ (12) &= (13) \\
(13) \circ (34) \circ (13) &= (14) \\
(14) \circ (45) \circ (14) &= (15)
\end{aligned}$$

由此又有

$$\begin{aligned}
(12) \circ (14) \circ (12) &= (24) \\
(12) \circ (15) \circ (12) &= (25) \\
(13) \circ (15) \circ (13) &= (35)
\end{aligned}$$

以上計算顯示，$\mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) : \mathbb{Q})$ 包含 S_5 中的所有對換。由於我們在《感受伽羅瓦：可解群與單純群》中已指出任何排列都可表示成對

換的複合, 並且提供了把排列改寫成對換複合的公式 (即該網頁的公式 (1)), 因此 $\mathrm{Gal}(\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) : \mathbb{Q})$ 包含 S_5 的所有元素, 即這個伽羅瓦群與 S_5 同構。由於 S_5 不是可解群, 由此根據上面的「定理 3」, 可知 f_3 沒有根式解。

上例顯示我們不能為一般的五次多項式方程尋找根式解。這當然並不代表任何五次或更高次多項式都沒有根式解, 事實上, 任何可約五次多項式都有根式解, 現證明如下。設 f_4 為可約五次多項式, 那麼它可以因式分解為 gk, 其中 g 和 k 為一次、二次、三次或四次多項式。這樣求解 f_4 的過程便變成求解 g 和 k 的過程。根據前面的討論, g 和 k 都有根式解, 因此 f_4 也有根式解。

連結至數學專題
連結至周家發網頁