幾個有名的數學問題(三)
方程式求解問題(上)

康明昌

1. 前言 ……………………………………………… 2
2. Lagrange 預解式 ……………………………………… 4
3. 方程式 $x^n - 1 = 0$ 的根式解 ……………………… 6
4. Galois 預解形與 Galois 群 …………………………… 7
5. Galois 理論 ………………………………………… 11

1. 前言

代數方程式是高中數學教育最基本的一環。事實上，不管時代如何的前進、數學如何的抽象化，方程式的研究一直是數學研究的核心部份。直到今日，多元高次方程式的研究（代數幾何）、Diophantus方程式的研究（代數數論）、微分方程式的研究，仍然是最生氣蓬勃的數學分枝。

遠在北宋仁宗時代（約1050年），中國數學家賈讓已經知道如何把一個正數開 n 次方根，也就是求方程式 $x^n - a = 0$ 的近似根；這個方法，中國數學家稱之為「增乘開方術」。南宋末年秦九韶（1247年）推廣賈讓的方法，得到任意方程式近似根的求法。1804年意大利數學家 P. Ruffini 得到同樣的結果。這個方法在1819年被英國一個中學教師W. G. Horner 重新發現，這就是俗稱的 Horner 方法。

更一般的，我們把數字方程式 $x^n + 3x^{n-1} + \sqrt{2}\, x^{n-3} - 2 = 0$ 推廣成文字方程式 $x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots\cdots + a_{n-1} x + a_n = 0$，其中 a_1，a_2，……，a_n 是沒有任何關係的文字；這種方程式叫做 n 次一般方程式（the general equation of degree n）。請注意，$x^4 + ax^2 + b = 0$ 不是四次一般方程式，因為 x 項的係數為零。如果我們能夠解一般方程式的根，那麼數字方程式的求根問題當然迎刄而解。

根據O. Neugebauer 的說法，巴比倫人在1600～1800 B.C. 已經知道求二次方程式的根。七世紀的印度學者Brahmagupta（約598～？）寫出方程式 $x^2 + ax = b$ 的一

個根的公式 $x=\dfrac{-a+\sqrt{a^2+4b}}{2}$。十二世紀的印度學者Bhaskara（1114～1185年？）更詳盡的討論一次和二次方程式。九世紀的阿拉伯數學家Muhammad ibn Musa al-Khwarizmi（780～850年）在他的書中第一次提出二次方程式的一般解法（註一）。

文藝復興時代意大利數學家發現三次與四次一般方程式的根的公式（約1545年）。方程式 $x^3+qx-r=0$ 的根的公式是

$$x=\sqrt[3]{\frac{r}{2}+\sqrt{\frac{r^2}{4}+\frac{q^3}{27}}}+\sqrt[3]{\frac{r}{2}-\sqrt{\frac{r^2}{4}+\frac{q^3}{27}}}$$ （註二）。

所謂根的公式，就是把代數方程式的根用其係數經過加、減、乘、除開方根表示出來的方法。如果我們可以求得一個（數字或文字）方程式的根的公式，我們就說這個方程式有根式解。

高中代數的Cardano 公式告訴我們，任意三次方程式都有根式解，Ferrari公式告訴我們，任意四次方程式都有根式解（註三）。因此，數學家面對一個最具挑戰性的問題：是不是任意方程式都有根式解？或者，一個更簡單的問題：是不是任意方程式至少都有一個根？

1746年法國數學家 Jean Le Rond D'Alembert發現「代數基本定理」：任意 n 次複數方程式恰有 n 個複數根。D'Alembert的證明其實是錯的，雖然這個定理的敍述是正確的。第一個正確的證明是偉大的Karl Friedrich Gauss 在二十歲（1797年）提出的。此後Gauss又提出另外三種證明。

「代數基本定理」出現之後，根的存在性問題完全解決。接著最自然的問題是，用什麼方式才能把這些根求出來？能不能只用係數的加、減、乘、除、開方根就把這些根表示出來（即「根式解」）？很明顯的，方程式 $x^5+x^4+x^3+x^2+x+1=0$ 與 $x^5+2=0$ 都有根式解（註四）。但是，一般五次方程式是不是有根式解？

十六世紀以來，有許多數學家研究五次一般方程式的根式解問題。在沒有解決這個問題之下，他們轉而探討一些更根本性的問題，例如：

- 根的存在性問題（即「代數基本定理」）。
- 根與係數的關係，根的個數，檢驗重根的方法，檢驗兩個方程式有公解的方法。
- 求數字方程式的近似根。
- 給定某個實係數方程式，並給定一個範圍（例如 0 到 100），估計在此範圍內實數根的數目。
- 因式分解是解數字方程式的第一步。研究因式分解是極爲重要的。第一個問題：對於有理數係數的單變數多項式，如何有效的進行因式分解？第二個問題，多變數多項式能否進行因式分解？第三個問題，因式分解是否有唯一性？

法國數學家 Joseph Louis Lagrange 在1770～1771年綜合前人解方程式的各種方法，歸納出一個一般性的模式。Lagrange 的洞察力在研究方程式根式解的領域打開一條新的道路。沿著Lagrange 指示的方向，Paolo Ruffini（1765～1822年）、Niels Henrick Abel（1802～1829年）、Évariste Galois（1811～1832年）終於解決了方程式根式解的問題。Alexandre Theophile Vandermonde 在1770年提出和Lagrange同樣的觀察，可惜他的結果沒有被當時的人注意。因此，所謂「預解式」的成果就由Lagrange所獨享，後世也稱爲「Lagrange預解式」。

從1799年開始，意大利數學家Ruffini就提出幾種方法，證明一般五次方程式不可能有根式解。Ruffini的證明雖有不少創見，却有許多漏洞，當時的人並不接受他的證明。

1826年挪威數學家Abel 證明：一般五次方程式沒有根式解。Abel 又說，五次以上的一般方程式的討論方法與五次類似。Abel的證明有一個漏洞，經愛爾蘭數學家William Rowan Hamilton（1805～1865年）加以補充說明。因此可以說，Abel 完全解決了一般五次方程式沒有根式解的問題。

但是一般方程式沒有根式解，並不表示所有的數字方程式都沒有根式解。事實上，方程式$2x^2+5=0$有根式解，但是$2x^5-10x+5=0$沒有根式解。法國數學家Galois 在1832年提出任意（數字或文字）方程式有根式解的充分必要條件。Galois 把方程式求解問題轉化成置換群（permutation group）的問題。他在繁複的計算中洞見方程式求解的本質。

Galois 的方法其實只是一個豐富深邃的理論的一個應用。這個理論就是我們習稱的Galois理論。Galois在二十一歲死於決鬥。他在決鬥前夜寫一封給友人的信，再度的簡單解釋Galois 理論的要點，因為當時許多成名的數學家，如S. D. Poisson, S. F. Lacroix，都不能瞭解他的理論。Galois 說，更進一步探討這個理論足夠讓後代的數學家受益良多。所謂方程根式解的問題，可以看做Galois 理論的一個習題。大多數人看到的冰山只是其浮出海面的一角，Galois 理論何嘗不是如此？

1858年法國數學家Charles Hermite 證明五次一般方程式的根可以用其係數經過加、減、乘、除、開方和橢圓函數的組合，表示出來。1880年法國數學家Henri Poincaré發現n次一般方程式的根可以用其係數經過加、減、乘、除、開方和Fuchs 函數的組合，表示出來。這其實是黎曼面理論的均勻化問題（uniformization problem）的應用。

2. Lagrange預解式

考慮三次方程式

$$x^3+qx-r=0 \tag{1}$$

令$x=v+v$，得

$$u^3+v^3+(3uv+q)(u+v)-r=0$$

令$3uv+q=0$，得

$$u^3+v^3-r=0$$

故知u^3與v^3是以下方程式之二根，

$$T^2-rT-\frac{q^3}{27}=0 \tag{2}$$

得

$$\left\{\begin{array}{l} u^3=\dfrac{r}{2}\pm\sqrt{\dfrac{r^2}{4}+\dfrac{q^3}{27}}, \\ v^3=\dfrac{r}{2}\mp\sqrt{\dfrac{r^2}{4}+\dfrac{q^3}{27}} \\ uv=-\dfrac{q}{3},\ x=u+v \end{array}\right.$$

令u_1與v_1各為$\frac{r}{2}+\sqrt{\frac{r^2}{4}+\frac{q^3}{27}}$與$\frac{r}{2}-\sqrt{\frac{r^2}{4}+\frac{q^3}{27}}$的一個三次方根，且$u_1v_1=-\frac{q}{3}$。則

$$x=u_1+v_1,\ wu_1+w^2v_1,\ 或\ w^2u_1+wv_1。$$

$$\left(w=\frac{-1+\sqrt{-3}}{2}\right)$$

以上解法的要點，是把三次方程式(1)變成六次方程式

$$x^6-rx^3-\frac{q^3}{27}=0 \tag{3}$$

這個六次方程式其實是一個偽裝的二次方程式，即(2)式。因此我們把三次方程式的求解問題轉化成二次方程式的求解問題。

方程式(3)是怎樣得到的呢？

令α_1，α_2，α_3是方程式(1)的三根，即$\alpha_1=u_1+v_1$，$\alpha_2=\omega u_1+\omega^2 v_1$，$\alpha_3=\omega^2 u_1+\omega v_1$。方程式(3)的六個根是$u_1$，$\omega u_1$，$\omega^2 u_1$，$v_1$，$\omega v_1$，$\omega^2 v_1$。故得，方程式(3)的六個根是

$$\frac{1}{3}(\alpha_1+\omega\alpha_2+\omega^2\alpha_3),$$

$$\frac{1}{3}(\alpha_1+\omega^2\alpha_2+\omega\alpha_3),$$

$$\frac{1}{3}(\omega\alpha_1+\omega^2\alpha_2+\alpha_3),$$

$$\frac{1}{3}(\omega\alpha_1+\alpha_2+\omega^2\alpha_3),$$

$$\frac{1}{3}(\omega^2\alpha_1+\alpha_2+\omega\alpha_3),$$

$$\frac{1}{3}(\omega^2\alpha_1+\omega\alpha_2+\alpha_3)。$$

Lagrange與Vandermonde高明的地方就在這裡。他們從三次方程式的三個根α_1,α_2,α_3造出一個預解形（resolvent）：$\frac{1}{3}(\alpha_1+\omega\alpha_2+\omega^2\alpha_3)$。在這個預解形中，固定$\alpha_1$，$\alpha_2$，$\alpha_3$的位置，令1，$\omega$，$\omega^2$任意排列，得出3！＝6個數。以這六個數為根的六次方程式就是一種預解式（resolvent）（註五）。預解式是一種解題之鑰。

我們的本意是解方程式(1)。但是如果能事先解出方程式(3)，原來的方程式也就迎刃而解。因此方程式(3)叫做方程式(1)的預解方程式，簡稱預解式。

利用Lagrange預解式的方法，讓我們試試看如何解四次方程式$x^4+ax^3+bx^2+cx+d=0$。令α_1，α_2，α_3，α_4為其四根。

解法1：考慮預解形$\alpha_1+\sqrt{-1}\,\alpha_2-\alpha_3-\sqrt{-1}\,\alpha_4$。

把以上預解形的係數1，$\sqrt{-1}$，-1，$-\sqrt{-1}$任意排列，得出$4!=24$個數。以這24個數為根作出一個預解式。這個預解式是個24次的方程式，其係數是α_1，α_2，α_3，α_4的對稱式，也是1，$\sqrt{-1}$，-1，$\sqrt{-1}$的對稱式。因此這些係數都可以寫成a，b，c，d的整係數多項式。

事實上這個預解式可以分解成兩個12次的多項式的乘積，這兩個12次多項式可以寫成x^4的三次多項式。因為三次方程式有根式解，所以這個預解式也有根式解。因此，$\alpha_1-\alpha_3=\frac{1}{4}\{(\alpha_1+\sqrt{-1}\,\alpha_2-\alpha_3-\sqrt{-1}\,\alpha_4)-\sqrt{-1}(\sqrt{-1}\,\alpha_1+\alpha_2-\sqrt{-1}\,\alpha_3-\alpha_4)-(-\alpha_1-\sqrt{-1}\,\alpha_2+\alpha_3+\sqrt{-1}\,\alpha_4)+\sqrt{-1}(-\sqrt{-1}\,\alpha_1-\alpha_2+\sqrt{-1}\,\alpha_3+\alpha_4)\}$有根式解。同理$\alpha_1-\alpha_2$，$\alpha_1-\alpha_4$也有根式解。所以$4\alpha_1-a=4\alpha_1-(\alpha_1+\alpha_2+\alpha_3+\alpha_4)=(\alpha_1-\alpha_2)+(\alpha_1-\alpha_3)+(\alpha_1-\alpha_4)$有根式解。

因此，只需證明這個預解式有如我們所預料的分解情形。注意，$(x-\alpha_1-\sqrt{-1}\,\alpha_2+\alpha_3+\sqrt{-1}\,\alpha_4)(x-\sqrt{-1}\,\alpha_1+\alpha_2+\sqrt{-1}\,\alpha_3-\alpha_4)(x+\alpha_1+\sqrt{-1}\,\alpha_2-\alpha_3-\sqrt{-1}\,\alpha_4)(x+\sqrt{-1}\,\alpha_1-\alpha_2-\sqrt{-1}\,\alpha_3+\alpha_4)=x^4+$（常數項），且$\{(x-\alpha_1-\sqrt{-1}\,\alpha_2+\alpha_3+\sqrt{-1}\,\alpha_4)(x-\sqrt{-1}\,\alpha_1+\alpha_2+\sqrt{-1}\,\alpha_3-\alpha_4)(x+\alpha_1+\sqrt{-1}\,\alpha_2-\alpha_3-\sqrt{-1}\,\alpha_4)(x+\sqrt{-1}\,\alpha_1-\alpha_2-\sqrt{-1}\,\alpha_3+\alpha_4)\}\{(x-\alpha_1+\alpha_2+\sqrt{-1}\,\alpha_3-\sqrt{-1}\,\alpha_4)(x+\alpha_1+\sqrt{-1}\,\alpha_2-\sqrt{-1}\,\alpha_3-\alpha_4)(x+\sqrt{-1}\,\alpha_1-\sqrt{-1}\,\alpha_2-\alpha_3+\alpha_4)(x-\sqrt{-1}\,\alpha_1-\alpha_2+\alpha_3+\sqrt{-1}\,\alpha_4)\}\{(x-\alpha_1+\sqrt{-1}\,\alpha_2-\sqrt{-1}\,\alpha_3+\alpha_4)(x+\sqrt{-1}\,\alpha_1-\sqrt{-1}\,\alpha_2+\alpha_3-\alpha_4)(x-\sqrt{-1}\,\alpha_1+\alpha_2-\alpha_3+\sqrt{-1}\,\alpha_4)(x+\alpha_1-\alpha_2+\sqrt{-1}\,\alpha_3-\sqrt{-1}\,\alpha_4)\}$的係數是$\alpha_1$，$\alpha_2$，$\alpha_3$，$\alpha_4$的整係數多項式。得證。

解法2：考慮預解形 $y_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$，$y_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$，$y_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$。以 y_1，y_2，y_3 爲三根的方程式係數都是 α_1，α_2，α_3，α_4 的對稱式。故 y_1，y_2，y_3 有根式解（卽，可用 a，b，c，d 經加、減、乘、除、開方根表示出來）。

再考慮預解形 $z_1 = \alpha_1 + \alpha_2 - \alpha_3 - \alpha_4$。因爲 $z_1^2 = (\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4)^2 = (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^2 - 4(\alpha_1\alpha_2 + \alpha_3\alpha_4 + \alpha_1\alpha_3 + \alpha_2\alpha_4 + \alpha_1\alpha_4 + \alpha_2\alpha_3) + 4(\alpha_1\alpha_2 + \alpha_3\alpha_4) = (-a)^2 - 4(y_1 + y_2 + y_3) + 4y_1$，故 z_1 有根式解。

同理 $z_2 = \alpha - \alpha_2 + \alpha_3 - \alpha_4$ 與 $z_3 = \alpha_1 - \alpha_2 - \alpha_3 + \alpha_4$ 也都有根式解。

$\alpha_1 = -\dfrac{a}{4} + \dfrac{1}{4}(z_1 + z_2 + z_3)$ 自然有根式解。

從以上的例子可以看出，只要找出適當的預解形和預解式，就不難求出四次一般方程式的根式解。

預解形是方程式的根的函數。例如，n 次方程式 $x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots\cdots + a_{n-1}x + a_n = 0$ 的 n 個根如果是 α_1，α_2，……，α_n，並且 $\zeta = \cos\dfrac{2\pi}{n} + \sqrt{-1}\sin\dfrac{2\pi}{n}$，則 $\alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3 + \cdots\cdots + \zeta^{n-1}\alpha_n$ 很可能是一個很好的預解形，$\alpha_1 + 2\alpha_2 + 3\alpha_3 + \cdots\cdots + n\alpha_n$ 也可能是一個不壞的預解形，$u_1\alpha_1 + u_2\alpha_2 + u_3\alpha_3 + \cdots\cdots + u_n\alpha_n$ 也是一個預解形（其中任一個 u_i 是 a_1，a_2 ……，a_n 的多項式）。

所謂的預解式就是滿足某一預解形的方程式，並且此方程式的求解問題比原來方程式簡單。

Lagrange曾經考慮五次一般方程式 $x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0$，令其五個根爲 α_1，α_2，α_3，α_4，α_5，並且 $\zeta = \cos\dfrac{2\pi}{5} + \sqrt{-1}\sin\dfrac{2\pi}{5}$。考慮預解形 $\alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3 + \zeta^3\alpha_4 + \zeta^4\alpha_5$，由此得到一個次數爲120的預解式。這個預解式可以表示成 x^5 的24次的方程式。然後呢？Lagrange只好停在這裡。

3. 方程式 $X^n - 1 = 0$ 的根式解

方程式 $x^n - 1 = 0$ 有沒有根式解？方程式 $x^n = a$（$a \neq 1$）有沒有根式解？

令 $\zeta_n = \cos\dfrac{2\pi}{n} + \sqrt{-1}\sin\dfrac{2\pi}{n}$。如果 ζ_n 有根式解（可以用有理數的加、減、乘、除、開方根表示出來），則方程式 $x^n - 1 = 0$ 有根式解：因爲 ζ_n，$(\zeta_n)^2$，$(\zeta_n)^3$，……，$(\zeta_n)^{n-1}$，$(\zeta_n)^n = 1$ 是其所有的根。如果 ζ_n 有根式解，則 $\sqrt[n]{a}$，$\sqrt[n]{a}\,\zeta_n$，$\sqrt[n]{a}(\zeta_n)^2$，……，$\sqrt[n]{a}(\zeta_n)^{n-1}$ 也有根式解。故 $x^n = a$ 有根式解。

若 $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots\cdots p_m^{\alpha_m}$，其中 p_1，p_2，……，p_m 是相異質數。如果 $\zeta_{p_1^{\alpha_1}}$，$\zeta_{p_2^{\alpha_2}}$，……，$\zeta_{p_m^{\alpha_m}}$ 有根式解，則 $\zeta_n = (\zeta_{p_1^{\alpha_1}})\cdots\cdots(\zeta_{p_m^{\alpha_m}})$ 也有根式解。

如果 ζ_p 有根式解，則 $\zeta_{p^l} = \sqrt[p^{l-1}]{\zeta_p}$ 也有根式解。

結論：若 p 是任意質數，且 ζ_p 有根式解。則方程式 $x^n = a$ 也有根式解，其中 n 是任意正整數，a 是任意數。

先看幾個例子，試驗 ζ_p 是否有根式解。

$p = 2$，$\zeta_2 = -1$。

$p = 3$，$\zeta_3 = \dfrac{-1 + \sqrt{-3}}{2}$。

$p = 5$，解方程式

$$x^4+x^3+x^2+x+1=0 \text{。}$$

得 $$x^2+x+1+\frac{1}{x}+\frac{1}{x^2}=0$$

$$\left(x+\frac{1}{x}\right)^2+\left(x+\frac{1}{x}\right)-1=0$$

$$x+\frac{1}{x}=\frac{-1\pm\sqrt{5}}{2}$$

$$x^2-\frac{-1\pm\sqrt{5}}{2}x+1=0$$

$$x=\frac{\sqrt{5}-1\pm\sqrt{-2\sqrt{5}-10}}{4}\,,\quad \frac{-\sqrt{5}-1\pm\sqrt{2\sqrt{5}-10}}{4}$$

故 ζ_5 有根式解。

同理 ζ_7 也有根式解。

Lagrange曾考慮 ζ_{11} 的根式解問題，但是並沒有解決這個問題。Vandermonde却完整的證明了 ζ_{11} 有根式解。Gauss 是第一個證明 ζ_p 有根式解的人，其中 p 是任意質數。以下我們將證明 ζ_{11} 有根式解。事實上，只要具備一點基本的數論的知識，不難將這個證明推廣到 ζ_p 的情形。

我們將證明 ζ_{11} 有根式解。

令 $\zeta=\zeta_{11}$ ，$\alpha=\zeta_{10}$ 。由數學歸納法，可假設 α 有根式解。考慮以下的預解形，

$$t_1=\zeta+\alpha\zeta^2+\alpha^2\zeta^4+\alpha^3\zeta^8+\alpha^4\zeta^5+\alpha^5\zeta^{10}+\alpha^6\zeta^9+\alpha^7\zeta^7+\alpha^8\zeta^3+\alpha^9\zeta^6\,,$$

$$t_2=\zeta+\alpha^2\zeta^2+\alpha^4\zeta^4+\alpha^6\zeta^8+\alpha^8\zeta^5+\alpha^{10}\zeta^{10}+\alpha^{12}\zeta^9+\alpha^{14}\zeta^7+\alpha^{16}\zeta^3+\alpha^{18}\zeta^6\,,$$

……………

$$t_i=\zeta+\alpha^i\zeta^2+\alpha^{2i}\zeta^4+\alpha^{3i}\zeta^8+\alpha^{4i}\zeta^5+\cdots\cdots+\alpha^{9i}\zeta^6\,,$$

……………

$$t_{10}=\zeta+\alpha^{10}\zeta^2+\alpha^{20}\zeta^4+\cdots\cdots+\alpha^{90}\zeta^6 \text{。}$$

可以檢查出，$(t_1)^{10}$ ，$(t_2)^{10}$ ，……，$(t_{10})^{10}$，$t_2(t_1)^8$，$t_3(t_1)^7$，……，$t_9\cdot t_1$，t_{10} 都是 α 的多項式。因此都有根式解。

所以 t_1 ，$t_2=\dfrac{t_2\cdot(t_1)^8}{(t_1)^8}$ ，t_3 ，……，t_{10} 也有根式解。可知 $\zeta=\dfrac{1}{10}(t_1+t_2+\cdots\cdots+t_{10})$ 也有根式解。（註六）

4. Galois預解形與Galois群

在本節我們要從另一個角度來瞭解預解形。我們將定義Galois預解形與Galois群。Galois群是Galois理論的基礎，下一節將介紹Galois 理論。

4.1 體與預解形

定義：若 K 是複數的子集合，如果 K 之內任意兩個元素做加、減、乘、除（0不能做除數），其結果仍然落在 K 之內，並且 K 至少含有兩個不同的元素，則 K 稱爲一個體（ field ）。

定義：若 K 是一個體，α 是一個複數，定義 $K(\alpha)$ 爲 $\left\{\dfrac{f(\alpha)}{g(\alpha)}：f(\alpha)\text{與}g(\alpha)\text{是係數在}K\text{之內的}\alpha\text{的多項式，且}g(\alpha)\neq 0\right\}$。同理，$K(\alpha_1,\cdots\cdots,\alpha_n)=K(\alpha_1,\cdots\cdots,\alpha_{n-1})(\alpha_n)$ 。

定義：若 K 與 L 都是體，且 $K\subset L$ ，則 K 叫做 L 的子體（ subfield ），L 叫做 K 的擴張體（ extension field）。

因爲複數體內有無窮多個超越數，彼此之間並無任何代數關係，我們不妨把 n 變數的有理函數體 $Q(x_1,\cdots\cdots,x_n)$ 看成複數體的子體。（註七）

例 1：方程式 $x^4+x^3+x^2+x+1=0$ 的

根是 $x=\dfrac{\sqrt{5}-1\pm\sqrt{-2\sqrt{5}-10}}{4}$，

$$\frac{-\sqrt{5}-1\pm\sqrt{2\sqrt{5}-10}}{4}\text{。}$$

令$K_0=Q$，$K_1=Q(\sqrt{5})=K_0(\sqrt{5})$，$K_2=Q(\sqrt{-2\sqrt{5}-10})=K_1(\sqrt{-2\sqrt{5}-10})$。$K_1$是$K_0$中某個元素（也就是5）開方得到的，$K_2$是$K_1$中某個元素（卽$-2\sqrt{5}-10$）開方得到的。$\dfrac{\sqrt{5}-1\pm\sqrt{-2\sqrt{5}-10}}{4}$落在$K_2$之內。

例2：三次方程式$x^3+qx-r=0$的根是

$$\alpha_1=\sqrt[3]{\frac{r}{2}+\sqrt{\frac{r^2}{4}+\frac{q^3}{27}}}+\sqrt[3]{\frac{r}{2}-\sqrt{\frac{r^2}{4}+\frac{q^3}{27}}},$$

$$\alpha_2=\omega\cdot\sqrt[3]{\frac{r}{2}+\sqrt{\frac{r^2}{4}+\frac{q^3}{27}}}+\omega^2\cdot\sqrt[3]{\frac{r}{2}-\sqrt{\frac{r^2}{4}+\frac{q^3}{27}}},$$

$$\alpha_3=\omega^2\cdot\sqrt[3]{\frac{r}{2}+\sqrt{\frac{r^2}{4}+\frac{q^3}{27}}}+\omega\cdot\sqrt[3]{\frac{r}{2}-\sqrt{\frac{r^2}{4}+\frac{q^3}{27}}}\text{。}$$

令$K_0=Q(q,r)$，$K_1=Q(q,r,\omega)=K_0(\omega)$，$K_2=K_1\left(\sqrt{\dfrac{r^2}{4}+\dfrac{q^3}{27}}\right)$，$K_3=K_2\left(\sqrt[3]{\dfrac{r}{2}+\sqrt{\dfrac{r^2}{4}+\dfrac{q^3}{27}}}\right)$，$K_4=K_3\left(\sqrt[3]{\dfrac{r}{2}-\sqrt{\dfrac{r^2}{4}+\dfrac{q^3}{27}}}\right)$。每一個$K_i$是$K_{i-1}$的某個元素開方得到的，並且$\alpha_1$，$\alpha_2$，$\alpha_3\in K_4$。

考慮（數字或文字）方程式$x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots\cdots+a_{n-1}x+a_n=0$。令其根爲$\alpha_1$，$\alpha_2$，……，$\alpha_n$。則$\alpha_1$，$\alpha_2$，……，$\alpha_n$有根式解的充分必要條件是，存在某些$K_0=Q(a_1,a_2,\cdots\cdots,a_n)\subset K_1\subset K_2\subset\cdots\cdots\subset K_m$，使得$\alpha_1$，……，$\alpha_n\in K_m$，並且對於任意$i$，$K_i=K_{i-1}(\theta_i)$，其中$(\theta_i)^{l_i}\in K_{i-1}$（$l_i$是由$\theta_i$決定的正整數）。

因此所謂根式解的問題，只不過是體的問題：如果我們能夠找到一個體K，使其包含$Q(\alpha_1,\cdots\cdots,\alpha_n)$，並且$K=K_m$可以由一些子體陸續加入開方根而得（如下圖），則

$$\begin{array}{ccccc}
 & K=K_m & & & \\
\cup & & \cup & & \\
 & & K_{m-1} & & \\
Q(\alpha_1,\cdots,\alpha_n) & & \cup & & \\
 & & \vdots & & \\
\cup & & \cup & & \\
 & & & K_0=Q(a_1,\cdots,a_n) &
\end{array}$$

方程式$x^n+a_1x^{n-1}+\cdots\cdots+a_{n-1}x+a_n=0$有根式解。

首要的問題變成：研究體的結構，研究一個體可能有那些子體，研究那些體可以由子體的元素開方而得到。

如果$K_1=K_0(\theta_1)$，$K_2=K_1(\theta_2)$，……，$K_m=K_{m-1}(\theta_m)$，並且$(\theta_1)^{l_1}=\varphi_0\in K_0$，$(\theta_2)^{l_2}=\varphi_1\in K_1$，……，$(\theta_m)^{l_m}=\varphi_{m-1}\in K_{m-1}$，那麼$\theta_1$，$\theta_2$，……，$\theta_m$就是一組極有用的預解形，而$x^{l_1}-\varphi_0=0$，$x^{l_2}-\varphi_1=0$，……，$x^{l_m}-\varphi_{m-1}=0$各爲其預解式。

4.2　置換群(Permutation group)的定義

在討論Lagrange預解式時，我們常用的手法是把方程式的根任意排列，而得出不同的預解形。例如，令α_1，α_2，α_3是方程式$x^3+qx-r=0$的三根，$\omega=\dfrac{-1+\sqrt{-3}}{2}$，預解形$\theta=\dfrac{1}{3}(\alpha_1+\omega\alpha_1+\omega^2\alpha_2)$；如果有一個排列（permutation），把$\alpha_1$換到$\alpha_2$，把$\alpha_2$換到$\alpha_3$，把$\alpha_3$換到$\alpha_1$，我們把

這個排列記爲

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

其中第二列的數 2，3，1 各爲第一列的 1，2，3 的「影像」。稱之爲 σ，則

$$\sigma=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}。（註八）$$

因此，我們可以把排列 σ 看成是集合 { 1，2，3 } 到其自身的函數。故，$\sigma(1)=2$，$\sigma(2)=3$，$\sigma(3)=1$。

如果我們有兩個排列 σ 與 τ，定義 $\sigma\tau$ 爲 σ 與 τ 的合成函數，即 $\sigma\tau(1)=\sigma(\tau(1))$，$\sigma\tau(2)=\sigma(\tau(2))$，$\sigma\tau(3)=\sigma(\tau(3))$。在這定義下，$\sigma\tau$ 也是一個排列。例如，令

$$\sigma=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}，\tau=\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}，$$

則 $\sigma\tau$ 是以下的排列

$$\sigma\tau=\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}。$$

設 G 是一些由 1，2，3 所做的排列的集合，則 G 叫做置換群，如果對於任意的 σ，$\tau \in G$，$\sigma\tau \in G$ 亦必成立。例如以下的子集都是置換群，

例 1 $$G=\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}\right\}。$$

例 2

$$G=\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right\}。$$

例 3

$$G=\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}。$$

例 4

$$G=\left\{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}。$$

以上的討論可以推廣到 1，2，3，……，n 的排列。

定義：若 σ 把 1，2，3，……，n 排成 p_1，p_2，……，p_n，我們記爲

$$\sigma=\begin{pmatrix} 1 & 2 & 3 \cdots\cdots n \\ p_1 & p_2 & p_3 \cdots p_n \end{pmatrix}。$$

我們可以把 σ 看成是集合 { 1，2，3，……，n } 到其自身的一對一的函數，即 $\sigma(1)=p_1$，$\sigma(2)=p_2$，……，$\sigma(n)=p_n$。若 σ 與 τ 是 1，2，……，n 的兩個排列，定義 $\sigma\tau(i)=\sigma(\tau(i))$；$\sigma\tau$ 也是一個排列。

定義：令 S_n 代表 1，2，……，n 的所有的排列所成的集合。若 G 是 S_n 的子集合，G 叫做一個置換群（ permutation group ），如果對於任意的 σ，$\tau \in G$，$\sigma\tau \in G$ 亦必成立。S_n 本身是一個置換群，S_n 含有 $n!$ 個不同的元素（或排列）。

如果 $\sigma=\begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}$，$\theta=\alpha_1+\omega\alpha_2+\omega^2\alpha_3$，我們可以讓 σ 作用在 θ 之上，也就是，σ 把 $\alpha_1+\omega\alpha_2+\omega^2\alpha_3$ 變成 $\alpha_2+\omega\alpha_3+\omega^2\alpha_1=\omega^2\alpha_1+\alpha_2+\omega\alpha_3$。我們把這個作用記爲

$$\begin{aligned}\sigma\cdot\theta &= \sigma\cdot(\alpha_1+\omega\alpha_2+\omega\alpha_3) \\ &= \alpha_{\sigma(1)}+\omega\alpha_{\sigma(2)}+\omega^2\alpha_{\sigma(3)} \\ &= \omega^2\alpha_1+\alpha_2+\omega\alpha_3\end{aligned}$$

同理，若 $\tau=\begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}$，則 $\tau\cdot\theta=$

$\alpha_{\tau(1)}+\omega\alpha_{\tau(2)}+\omega^2\alpha_{\tau(3)}=\alpha_1+\omega^2\alpha_2+\omega\alpha_3$。

更一般的，若$\sigma\in S_n$，且α_1，……，α_n是方程式$x^n+a_1x^{n-1}+\cdots\cdots+a_n=0$的根，則$\sigma\cdot\alpha_1=\alpha_{\sigma(1)}$，$\sigma\cdot\alpha_2=\alpha_{\sigma(2)}$，……，$\sigma\cdot\alpha_n=\alpha_{\sigma(n)}$，$\sigma\cdot(b_1\alpha_1+b_2\alpha_2+\cdots\cdots+b_n\alpha_n)=b_1\alpha_{\sigma(1)}+b_2\alpha_{\sigma(2)}+\cdots\cdots+b_n\alpha_{\sigma(n)}$，其中$b_1$，$b_2$，……，$b_n$是$a_1$，……，$a_n$的有理係數多項式。

4.3 Galois預解形與Galois群

在本小節與下一節，我們考慮的方程式$x^n+a_1x^{n-1}+\cdots\cdots+a_n=0$是不可約的，因此其根$\alpha_1$，$\alpha_2$，……，$\alpha_n$是相異的$n$個數。這個「不可約」的限制，對於研究根式解的問題，並不產生實質的困擾。

所謂的Galois 預解形就是$Q(\alpha_1,\cdots\cdots,\alpha_n)=Q(a_1,\cdots\cdots,a_n)(\alpha_1,\cdots\cdots,\alpha_n)$之內滿足以下條件的任意元素$\theta$，

(1) $\{\sigma\cdot\theta:\sigma\in S_n\}$是$n!$個相異的數。

(2) α_1，α_2，……，$\alpha_n\in Q(a_1,\cdots\cdots,a_n)(\theta)$。

Galois預解形是Galois定義Galois 群的踏脚石。Galois並沒有證明Galois預解形的存在性。他似乎認爲這個證明太簡單了，不值得大書特書。事實上，這個證明與近世代數課本中「素樸元素(primitive element)的存在性」的證明差不多。我們不妨也假設Galois 預解形的存在性。

例1：方程式$x^4+x^3+x^2+x+1=0$，令其四根爲ζ，ζ^2，ζ^3與ζ^4。則Galois預解式可以取$\theta=\zeta+2\zeta^2+3\zeta^3+4\zeta^4$。

例2：n次一般方程式$x^n+a_1x^{n-1}+\cdots\cdots+a_{n-1}x+a_n=0$，令其$n$個根爲$\alpha_1$，……，$\alpha_n$，則Galois預解式可以取$\theta=\alpha_1+2\alpha_2+3\alpha_3+\cdots\cdots+n\alpha_n$。

現在我們要定義方程式$x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots\cdots+a_{n-1}x+a_n=0$的Galois群。令$\theta$爲其 Galois 預解形。

考慮多項式

$$f(x)=\prod_{\sigma\in S_n}(x-\sigma\cdot\theta)$$

將$f(x)$分解爲係數在$Q(a_1,\cdots\cdots,a_n)$的不可約多項式的乘積，即

$f(x)=f_1(x)\cdots\cdots f_m(x)$，

$f_i(x)\in Q(a_1,\cdots\cdots,a_n)[x]$，

且$f_i(x)$是不可約多項式。

我們可以安排這些$f_i(x)$，使得θ是$f_1(x)=0$的根。令$f_1(x)$的根爲$\theta=\theta_1$，θ_2，……，θ_r。

原來方程式的 Galois 群G定義爲

$$G=\{\sigma\in S_n:\sigma\cdot\theta_i=\theta_{\sigma(i)},\ \{1,2,\cdots\cdots,r\}=\{\sigma(1),\sigma(2),\cdots\cdots,\sigma(r)\}\}。$$

換句話說，$\sigma\in G$的充分必要條件是σ把$\{\theta_1,\cdots\cdots,\theta_r\}$作用到其自身。也就是說，$\sigma$把$f_1(x)$作用到$f_1(x)$。

可以證明，以上的條件可以寫成

$G=\{\sigma\in S_n:f_1(\sigma\cdot\theta)=0\}$。

例1：一般方程式$x^n+a_1x^{n-1}+\cdots\cdots+a_{n-1}x+a_n=0$，令$\alpha_1$，……，$\alpha_n$爲其根，$\theta=\alpha_1+2\alpha_2+\cdots\cdots+n\alpha_n$爲Galois 預解形，則多項式$f(x)=\prod_{\sigma\in S_n}(x-\sigma\cdot\theta)$是不可約多項式，其Galois 群是$S_n$。

例2：方程式$x^4+x^3+x^2+x+1=0$的根爲ζ，ζ^2，ζ^3，ζ^4，令$\theta=\zeta+2\zeta^2+3\zeta^3+4\zeta^4$爲某一個Galois 預解形。我們可以證明(但是這個證明並不十分容易)。

$$f(x)=\prod_{\sigma\in S_4}(x-\sigma\cdot\theta)$$

$= f_1(x) f_2(x) \cdots\cdots f_6(x)$

其中$f_1(x)$，……，$f_6(x) \in Q[x]$是四次不可約多項式，且$f_1(\theta)=0$。並且$f_1(x)=0$的四個根是

$$\begin{aligned}\theta = &\ \zeta + 2\zeta^2 + 3\zeta^3 + 4\zeta^4,\\ &\ \zeta^2 + 2\zeta^4 + 3\zeta + 4\zeta^3,\\ &\ \zeta^3 + 2\zeta + 3\zeta^4 + 4\zeta^2,\\ &\ \zeta^4 + 2\zeta^3 + 3\zeta^2 + 4\zeta。\end{aligned}$$

因此其Galois 群G是

$$G = \{ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \}。$$

5. Galois理論

本節的目的是介紹Galois 理論及其應用。本節的定理來自 Galois 的論文「Mémoire sur les conditions de résolubilité des équations par radicaux」（1831年1月17日）與Galois給友人的信「Lettre à Auguste Chevalier」（1832年5月29日）。大部分的定理都沒有證明，因爲我們並不想寫一本 Galois 理論的課本，我們的目的是介紹Galois 理論的精神。有興趣的讀者不妨參考以下兩本書：H. M. Edwards, Galois theory與E. Artin, Galois theory。在Artin的書，體的擴張與體的自同構群是Galois 理論的核心，學生幾乎看不到有人在解方程式，預解式與預解形也消失了；這是一本典型的近世代數的課本，用近世代數的手法介紹 Galois 理論。

5.1 置換群的簡單性質

令G是一個置換群，H是其子集合，且H不是空集合。如果任取$\sigma, \tau \in H$，而$\sigma\tau$恆落在H之內，則H叫做G的子群（subgroup）。顯然H也是一個置換群。

若H是置換群G的子群，任取$\sigma \in G$，定義$H\sigma = \{ \tau\sigma \in G ; \tau \in H \}$，$\sigma H = \{ \sigma\tau \in G : \tau \in H \}$。請注意，在大部分情況，$H\sigma \neq \sigma H$。但是$H$，$H\sigma$，$\sigma H$ 有同樣多的元素。

定義：若H是置換群G的子群。H是G的一個正則子群（normal subgroup），如果以下條件成立：任取$\sigma \in G$，$H\sigma = \sigma H$恆成立。

若S是一個集合，我們用$|S|$表示S中元素的總數。若H是G的子群，$[G:H]$代表$\dfrac{|G|}{|H|}$。

Lagrange定理：若H是置換群G的子集，則$[G:H]$是一個整數。

證明：很明顯，$G = \bigcup_{\sigma \in G} H\sigma$。

沒有這麼明顯的是，若σ_1，$\sigma_2 \in G$，則$H\sigma_1 = H\sigma_2$或$H\sigma_1 \cap H\sigma_2 = \phi$。（請讀者自己證明。）

因此，$G = \bigcup_{i=1}^{r} H\sigma_i$，並且$H\sigma_i \cap H\sigma_j = \phi$，如果$i \neq j$。

注意，$|H\sigma_i| = |H|$。因此，$|G| = r \cdot |H|$。

5.2 係數擴張時Galois群的變化

請讀者回憶一下，在本文 4.3 小節我們是

怎樣定義Galois群。令方程式 $x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots\cdots+a_{n-1}x+a_n=0$ 的根是 $\alpha_1, \alpha_2, \cdots\cdots, \alpha_n$，$K_0=Q(\alpha_1, \cdots\cdots, \alpha_n)$。取一個Galois預解形 θ，考慮 $f(x)=\prod_{\sigma\in S_n}(x-\sigma\cdot\theta)=f_1(x)\cdot f_2(x)\cdots\cdots f_m(x)$，其中 $f_i(x)\in K_0[x]$，$f_1(\theta)=0$，且 $f_1(x)$ 是不可約的。則方程式 $x^n+ax^{n-1}+\cdots\cdots+a_{n-1}x+a_n=0$ 對於 K_0 的Galois群 $G=\{\sigma\in S_n: f_1(\sigma\cdot\theta)=0\}$。

如果 K 是 K_0 的某個擴張體，那麼原來方程式對於 K_0 的Galois群與對於 K 的Galois群會不會一樣呢？

注意，若 $K_0\subset K_1$，$f_1(x)$ 是 $K_0[x]$ 的不可約多項式，但是 $f_1(x)$ 在 $K[x]$ 之內很可能是可以分解的。例如，x^2+1 在 $Q[x]$ 是不可約，x^2+1 在 $Q(\sqrt{-1})[x]$ 却能分解。

令 $f_1(x)=g_1(x)g_2(x)\cdots\cdots g_l(x)$，其中 $g_i(x)\in K[x]$，$g_1(\theta)=0$ 且 $g_1(x)$ 在 $K[x]$ 是不可約的。考慮

$G=\{\sigma\in S_n: f_1(\sigma\cdot\theta)=0\}$，對於 K_0 的Galois群；

$H=\{\sigma\in S_n: g_1(\sigma\cdot\theta)=0\}$，對於 K 的Galois群。

不難證明，H 是 G 的子群。如果 K_0 與 K 的取法更好的話，G 與 H 的關係還會更清楚，那就是，

定理 1：令方程式 $\phi(x)=0$ 的係數都在體 K 之內，p 是一個質數，且 $\zeta=\cos\frac{2\pi}{p}+\sqrt{-1}\sin\frac{2\pi}{p}\in K$。假設 $L=K(\theta)$，$\theta^p\in K$，並且 G 是方程式 $\phi(x)=0$ 對於 K 的Galois群，H 是方程式 $\phi(x)=0$ 對於 L 的Galois群。則，$G=H$，或 H 是 G 的正則子群且 $[G:H]=p$。

以上定理的逆敘述，其實是正確的。即，

定理 2：令方程式 $\phi(x)=0$ 的係數都在體 K 之內，p 是一個質數，且 $\zeta=\cos\frac{2\pi}{p}+\sqrt{-1}\sin\frac{2\pi}{p}\in K$。若 G 是方程式 $\phi(x)=0$ 對於 K 的 Galois群，H 是 G 的正則子群且 $[G:H]=p$。則存在一個數 u，$u^p\in K$，且 H 是方程式 $\phi(x)=0$ 對於 $K(u)$ 的Galois群。

定理 1 與定理 2 告訴我們，陸續的把 $x^m=a$ 的根加入體 K（這些根都有根式解！），很可能把方程式 $\phi(x)=0$ 對於 K 的Galois群化簡爲 $G=G_0, G_1, G_2, \cdots\cdots, G_s$，其中 G_i 是 G_{i-1} 的正則子群，$[G_{i-1}:G_i]$ 是質數，G_s 只含有一個排列。事實上這個推測剛好是 Galois 研究方程式有根式解的答案。他的結果是，

定理 3：令方程式 $\phi(x)=0$ 的係數都在體 K 之內，G 是方程式 $\phi(x)=0$ 的 Galois群。則 $\phi(x)=0$ 有根式解的充分必要條件是，可以找到置換群 $G=G_0, G_1, G_2, \cdots\cdots, G_s$，其中 G_i 是 G_{i-1} 的正則子群，$[G_{i-1}:G_i]$ 是質數，且 G_s 只含有一個排列。

根據 4.1 的討論，我們把根式解的問題轉變成體的結構（某些體有那些特殊形式的子體）的問題。由定理 1，我們又可把體的結構的問題轉變成群的問題。這就是定理 3 的精神。

如果方程式 $\phi(x)=0$ 沒有根式解，定理3就沒有用了，我們也不能瞭解體 $K(\alpha_1, \cdots\cdots, \alpha_n)$ 的結構（$\alpha_1, \cdots\cdots, \alpha_n$ 是 $\phi(x)=0$ 的根）。事實上，Galois 探討體 $K(\alpha_1, \cdots\cdots, \alpha_n)$ 的更深入的性質。在Galois的探討中，體 $K(\alpha_1, \cdots\cdots, \alpha_n)$ 的性質與Galois 群 G 的性質更加密切。這就是我們在下一小節所要討論的 Galois 理論。

5.3 Galois理論大要

令不可約方程式 $\phi(x)=x^n+a_1x^{n-1}+\cdots\cdots+a_{n-1}x+a_n=0$ 的根爲 α_1,……,α_n,K_0 是包含 $Q(a_1,\cdots\cdots,a_n)$ 的一個體,$K=K_0(\alpha_1,\cdots\cdots,\alpha_n)$,$G$ 是方程式 $\phi(x)=0$ 對於 K_0 的 Galois 群。

若 H 是 G 的任意子群,定義 $K^H=\{u\in K:\sigma\cdot u=u$,$\sigma$ 是 H 的任意元素$\}$。

若 M 是 K 的任意子體,且 $M\supset K_0$,定義 $G(K/M)=\{\sigma\in G:\sigma\cdot u=u$,$u$ 是 M 的任意元素$\}$。

定理4:(Galois 理論的基本定理)

(1) $K^G=K_0$。

(2) 介於 K_0 與 K 之間的所有的體恰與 G 的所有子群成一對一的對應。也就是說,如果 M 是一個體,且 $K_0\subset M\subset K$,則 M 一定是 K^H 的形式,其中 H 是 G 的某個(唯一確定的)子群。反過來說,如果 H 是 G 的任意子群,則 H 一定是 $G(K/M)$ 的形式,其中 M 是 K 的某個子體。

(3) 若 H 是 G 的正則子群,則 K^H 一定可以寫成 $K_0(\beta_1,\cdots\cdots,\beta_m)$ 的形式,其中 β_1,……,β_m 是某個方程 $\phi(x)=0$ 的所有的根,$\phi(x)\in K_0[x]$。反過來說,如果 $\phi(x)\in K_0[x]$,且 β_1,……,β_m 是 $\phi(x)=0$ 的所有的根,則 $G(K/K_0(\beta_1,\cdots,\beta_m))$,是 G 的正則子群。

由定理4,再配合定理1與定理2,很容易證出定理3。

定理4的第(3)部分告訴我們,Lagrange 或其他人所努力尋找的各種預解形(如果有的話),全都是由Galois 群的正則子群所決定。

定理4告訴我們的還不止如此。以前的數學家只想知道 $K_0(\alpha_1,\cdots\cdots,\alpha_n)$ 是否只要把足夠多的開方根加入 K_0 就能得到。他們的目的,對 Galois 來說,只是一個大計劃的一個小項目。Galois 要探討 $K_0(\alpha_1,\cdots\cdots,\alpha_n)$ 的複雜程度;他證明,$K_0(\alpha_1,\cdots\cdots,\alpha_n)$ 的複雜度恰好由 Galois 群 G 的複雜程度表現出來。一個群 G 如果有一連串的子群 $G=G_0$,G_1,……,G_m,其中 $|G_0|$,$|G_1|$,……,$|G_m|$ 是逐次減小且 G_i 是 G_{i-1} 的正則子群,這個群 G 看起來就比較容易處理。一個不可交換群 G,如果除了 G 本身和單位元素之外,沒有其他的正則子群,這種群就不太容易處理;Galois 聲稱,這種群至少要有60個元素。(註九)

從表面上,把體的結構的問題轉變成置換群的問題,似乎把問題簡化了,因爲置換群頂多只有有限個元素,只有有限多種子群。事實上,的確有一些問題從體的角度考慮是非常困難,從置換群的角度來觀察却是不難理解的。

5.4 應 用

利用定理4,Galois 可以證明以下的定理。

定理5:若 p 是一個質數,$\phi(x)=x^p+a_1x^{p-1}+\cdots\cdots+a_{p-1}x+a_p$ 是不可約多項式,α_1,α_2,……,α_p 是 $\phi(x)=0$ 的根。

(1) 方程式 $\phi(x)=0$ 有根式解的充分必要條件是 α_1,α_2,……,$\alpha_p\in Q(a_1,\cdots\cdots,a_p,\alpha_{i_1},\alpha_{i_2})$,其中 i_1,i_2 是 $\{1,2,\cdots\cdots,p\}$ 任意相異的兩個數。

(2) 若 $\phi(x)=0$ 有根式解,則我們把 α_1,……,α_p 適當排列之後,$\sigma\cdot\alpha_i=$

α_{ri+s}，其中σ是Galois 群的任意元素，r與s是隨σ改變的整數，$1 \leqq r \leqq p-1$，$0 \leqq s \leqq p-1$。(如果$ri+s \geqslant p$，則α_{ri+s}表示α_q，其中q是$ri+s$除以p的餘數。)

定理6：五次一般方程式沒有根式解。因此，五次以上的一般方程式也沒有根式解。

證明：由定理5的第(2)部分可知，如果$\phi(x)=0$有根式解，其Galois 群的元素可以由(r,s)決定，$1 \leq r \leq p-1$，$0 \leq s \leq p-1$。因此Galois 群頂多只有$(p-1) \cdot p$個元素。

五次一般方程式如果有根式解，其Galois群頂多只有$4 \cdot 5 = 20$個元素。但是由4.3小節的例子可知，五次一般方程式的Galois 群是S_5，有$5! = 120$個元素。因此五次一般方程式沒有根式解。

若$n > 5$，如果n次一般方程式有根式解，則任意n次方程式都有根式解。因此$x^{n-5}(x^5+a_1x^4+a_2x^3+a_3x^2+a_4x+a_5)=0$也有根式解。但是$x^5+a_1x^4+a_2x^3+a_3x^2+a_4x+a_5=0$是五次一般方程式，沒有根式解。

定理6是N.H. Abel在1826年首先證明的。有了這個定理之後，我們不妨如此說，方程式根式解的領域已沒有多少有意義的問題值得研究。不管我們用如何巧妙的方法導出三次或四次方程式根的公式，在數學上的意義是微乎其微。

Galois 理論的意義至少有兩個。第一，如果把體的結構的問題比做一座高山，從某個角度來看(體的角度)簡直是懸崖峭壁，無處攀援，從變換群的角度來看，山窮水盡之餘却是柳暗花明的世界。這種處理數學問題的手法，以後一再的被數學家借鏡。第二，Galois 理論開創了群論(group theory)的研究。並且Galois 的經驗告訴數學家，研究某個數學結構(集合、群、環、體、向量空間、拓樸空間、微分流型)的變換群(transformation group)，經常有助於瞭解這個數學結構，這就是表現理論(representation theory)何以如此重要的原因。

Nicholas Bourbaki 是二十世紀許多第一流數學家的團體的代稱，他們寫了許多書，其作者都冠以Bourbaki的名字。Bourbaki的「Algebre」(代數學)自然也介紹Galois理論。Bourbaki 認爲，Galois 理論是極重要的數學工具，是從事高深數學研究的人必須具備的基礎知識；Galois理論之中，最重要的是Galois理論的基本定理(定理4)，而所謂根式解的充分必要條件(定理3)只不過是Galois 理論的一個習題罷了。至於五次一般方程式無根式解(定理6)這個定理，在Bourbaki的書中根本沒有出現的資格，因爲Bourbaki認爲那已經是一個死的問題！Bourbaki的論斷是明睿，還是偏頗，那倒是值得我們好好的想想看了。

——本文作者任教於台大數學系——

註 釋

註一：這本書的名字叫「Hisāb al - Jabr wa'l - Muqābalah」，其中al - Jabr 是「移項」的意思，wa'l -Muqābalah 是「消去（同類項）」的意思。因此這本書叫做「移項與消去的科學」。後來 wa'l - Muqābalah 逐漸被遺忘，而 al - Jabr 却變成了Algebra ，這就是拉丁文的algebra（代數）。

註二：請注意這兩個三次方根的取法，我們要取這兩個三次方根，使其乘積爲$-\dfrac{q}{3}$。

註三：三次方程式的根的公式是威尼斯的數學教授Tartaglia（意爲「口吃者」，原名Niccolo Fontanna，1500～1557年）發現的。他告訴米蘭大學的醫學教授Girolamo Cardano(1501～1576年）。Cardano 在1545年出版「大術」（Ars Magna），公開Tartaglia的方法，並且聲明這是Tartaglia發見的，後世却稱爲Cardano公式。Lodovico Ferrari（1522～1565年）是Cardano 的學生。

註四：請參考本文第三節。

註五：有些作者不區分「預解形」與「預解式」，統稱爲 resolvent 。我們爲了說明方便，特加以區分。

註六：請注意，在定義t_1時，我們把$\dfrac{x^{11}-1}{x-1}=0$的十個根作如下的排列：ζ，ζ^2，ζ^4，ζ^8，ζ^5，ζ^{10}，ζ^9，ζ^7，ζ^3，ζ^6。原因是：2是$(Z/11Z)^\times$ 的素根（primitive root）。

在任意質數p時，我們也可取$(Z/pZ)^\times$的素根，然後定義t_1，t_2，……，t_{p-1}。

讀者如果具備近世代數的知識，可以證明$Q(\zeta_p)$與$Q(\zeta_{p-1})$是線性分離（linearly disjoint）。由此可證明t_1^p，t_2^p，……，$(t_{p-1})^p$，$t_2\cdot(t_1)^{p-2}$，$t_3\cdot(t_1)^{p-3}$，……，$t_{p-1}\cdot t_1$，t_p都是$Q(\zeta_{p-1})$的元素（利用Galois 群的作用）。

讀者如果學過Galois 理論，不妨證明$x^p-1=0$對於有理數體的Galois群是$(Z/pZ)^\times$，因此方程式$x^p-1=0$有根式解。

註七：讀者如果不十分瞭解這句話，請接受一件事實：$Q(x_1,\cdots\cdots,x_n)$可以看做複數體的子體，就可以順利的看完本文。有關體與超越數，請參考：康明昌，幾個有名的數學問題(二)：古希臘幾何三大問題（上），第2節與第4節，數學傳播季刊八卷二期，73年6月。

註八：用這種方式介紹排列$\sigma=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$之後，我們就把$\sigma$看成1，2，3的排列，而不再强調$\sigma$是$\alpha_1$，$\alpha_2$，$\alpha_3$ 的排列。如果α_1，α_2，α_3是相異三個數，那麼1，2，3 排列與α_1，α_2，α_3 的排列並沒有什麼區別。如果$\alpha_1=\alpha_2$，强調σ是α_1，α_2，α_3的排列，在說明排列σ時，就不免有些困擾。。如果從開始就假設方程式$x^3+qx-r=0$是不可約，則α_1，α_2，α_3自然是相異的。

註九：群G是不可交換群，如果$\sigma\cdot\tau=\tau\cdot\sigma$在$G$之內並不恆成立。