幾個有名的數學問題(二)：古希臘幾何三大問題(上)

康明昌

1. 前言……………………………………………………………… 2
2. 幾何三大問題簡介………………………………………………… 3
3. 為什麼這些問題無解……………………………………………… 4
4. 超越數簡介………………………………………………………… 6

1.前　言

古希臘人在幾何學的研究開創了一個輝煌的時代。Euclid （歐基里德，約紀元前300年）的「幾何原本」（Elements ）總結了當時希臘數學發展的成果。由於幾千年經驗的累積，人類已經能夠掌握許多幾何知識。如何有效的運用、正確的認識、以及更進一步的發展這些知識，促使希臘人有系統的去整理它們。這個工作的結果，就是「幾何原本」的纂成。「幾何原本」是希臘文明結晶品之一。

「幾何原本」把紛雜的知識變成一個演繹系統，推演出來有條不紊的定理；而這個系統所根據的（也就是沒有加以證明的）只是少數幾個看來相當明顯並且合乎人類經驗的現象。這幾個「不證自明」的現象叫做「公理」（axioms 或 postulates ）；由這些公理出發，Euclid 可以推演出當時人類已經獲得的幾何知識。

幾何作圖是幾何學研究的一個課題。正如希臘人整理「幾何原本」秉持的一貫精神，他們把幾何作圖的「競賽規則」定得清清楚楚。希臘人的幾何作圖只准用（沒有刻劃的）直尺和圓規。據說，在紀元前350年的Menaechmus 曾經建議把拋物線的製圖儀也列入合法的作圖工具，結果（根據Plutarch 的說法）被Plato （柏拉圖）痛斥一頓，Plato 認爲使用陋俗工匠製造的儀器來作圖，是在污辱幾何學。

古希臘人在研究幾何作圖時，有三個問題無法解決，這就是通稱的古希臘幾何三大問題。這些問題直到十九世紀才證明是無解的。所謂無解並不是數學家不能答覆這些問題，而是數學家能夠證明這些作圖問題是辦不到的，就

像一般人能夠證明方程式 $x^2+1=0$ 沒有實數根的情況一樣。

既然這些問題是無解的，那麼幾何學家豈不是沒事幹了？事實恰恰相反，從十八世紀末期以來，幾何三大問題就已經不是幾何學研究的主流；十九世紀幾何學研究的主流是，射影幾何、非歐幾何、微分幾何與代數幾何。因此幾何三大問題的無解並沒有給幾何學家任何衝擊。

如果這麼說的話，幾何三大問題的解決豈不是毫無意義嗎？這也不盡然。幾何三大問題的解決，一方面結束了幾個歷史性懸而未決的問題，更重要的另一面是，它引發了新的問題——也就是超越數的研究。超越數的研究使數學家更熟練的駕馭複數系，更透澈的洞悉複數系的本質。超越數的研究就是數學家通稱的「Diophantine analysis and transcendental number theory」，這是目前數學研究非常熱門、非常重要的一部份。

本文的主題是介紹幾何三大問題與超越數的基本概念，同時也介紹十九世紀幾何學的幾個主要方向。

2.幾何三大問題簡介

古希臘幾何三大問題是，在只准使用（沒有刻劃的）直尺與圓規的限制之下，求解以下的作圖問題

(1)（方圓問題）求作一個正方形，使其面積和半徑爲 1 的圓面積相等；

(2)（倍立方問題）求作一個正立方體，使其體積爲邊長爲 1 的正立方體的 2 倍；

(3)（三等分角問題）三等分任意已知角。

以上問題的 1 是任意選定的單位長度。（註一）。

在歐氏平面幾何學中，我們知道古希臘人能夠做出長度爲任意有理數的線段；他們也能做出長度爲 $\sqrt{2}$、$\sqrt{3}$、$\frac{\sqrt{5}-1}{2}$ 的線段。他們能夠做圓內接（或外切）正五邊形、正六邊形。但是他們始終做不出以上三個作圖問題。因此他們認爲這三個問題一定是非常困難的，以後的歷史證明的確如此。

簡單的分析一下，方圓問題其實是要做出長度爲 $\sqrt{\pi}$ 的線段，倍立方問題是要做出長度爲 $\sqrt[3]{2}$ 的線段。三等分角問題也極爲類似，因爲如果給我們一個角度 θ，$0<\theta<\frac{\pi}{2}$，（假設已經選好單位長度）我們就可以求得 $\cos\theta$，令其爲 α。如果我們能夠求出 $x=\cos\frac{\theta}{3}$，我們就可以做出 $\frac{\theta}{3}$ 的角度。但是，

$$\begin{aligned}\cos\theta &= 4\cos^3\frac{\theta}{3}-3\cos\frac{\theta}{3}\\ &= 4x^3-3x\end{aligned}$$

因此，x 滿足以下方程式：

$$4t^3-3t-\alpha=0$$

其中 $\alpha=\cos\theta$ 是已知線段長度。令

$$f(t)=4t^3-3t-\alpha$$

因

$$f(1)>0, \quad f(0)\leqslant 0$$

$$f\left(-\frac{1}{2}\right)>0, \quad f(-1)<0$$

故知方程式 $4t^3-3t-\alpha=0$ 有三相異實根，x 是唯一的正根。

歸根究底，所謂幾何三大問題無非是，給定一個單位長度；

(1)（方圓問題）求作一個長度爲 $\sqrt{\pi}$ 的線段。

(2)（倍立方問題）求作一個長度爲 $\sqrt[3]{2}$ 的線段。

(3)（三等分角問題）先給長度爲 α 的線段，求作一個長度爲 x 的線段，而 x 滿足 $4x^3-3x-\alpha=0$。

問題既然轉化成這種形式，我們當然要問：到底有那些長度是作得出來的？那些長度是做不出來的？如果我們令

$S=\{r: r$ 是任意實數；在給定單位長度 1 時，我們利用直尺與圓規可以作出長度爲 $|r|$ 的線段$\}$。

那麼，方圓問題與倍立問題變成 $\sqrt{\pi}$ 與 $\sqrt[3]{2}$ 是否在 S 之內。同樣的，令

$T=\{r: r$ 是任意實數；在給定單位長度 1 與另一長度 α 時，我們利用直尺與圓規可以做出長度爲 $|r|$ 的線段$\}$。

很顯然的，S 與 T 都包含有理數，並且 $\sqrt{2}$、$\sqrt{3}$、$\dfrac{\sqrt{5}-1}{2}$、$\sqrt[4]{\sqrt{7}+\sqrt[3]{5}}$ 都落在 S，也落在 T。

由比例定理可知，如果 $a, b\in S$，則 $a\pm b$，ab，$\dfrac{a}{b}\in S$。可知 S 是實數的子集合，並且 S 之內的任意元素做加、減、乘、除之後，仍然落在 S 之內。同理可討論 T。

更重要的，如果 $a\in S$，取 1 與 a 的等比中項，則 $\sqrt{a}\in S$（若 $a>0$）。如果 $a, b\in S$，且 $x^2-ax+b=0$，則

$$x=\frac{a\pm\sqrt{a^2-4b}}{2}\in S\ (\text{若 } a^2-4b>0)$$

。因此，如果一個二次方程式的兩根都是實數，且其係數都在 S，則此二根也在 S。

到底 S 與 T 是什麼樣的集合呢？在討論這個問題之前，我們先給一個定義。

定義 若 U 是複數的一個至少含有兩個元素的子集合，且 U 之內的任意兩個元素做加、減、乘、除（0 不能做除數），其結果仍然落在 U 之內，則 U 稱爲一個體（field）。（註二）

定義 若 $\mathbf{Q}$ 表示所有有理數的集合，u 是任意實數，定義 $\mathbf{Q}(u)=\{\dfrac{f(u)}{g(u)}$：其中 $f(T)$，$g(T)$ 是 $\mathbf{Q}$ 上的多項式，且 $g(u)\neq 0\}$。同理，若 U 是一個體，可定義 $U(u)$。很容易檢查 $U(u)$ 仍然是一個體。利用歸納法，我們把 $\mathbf{Q}(u_1,\cdots,u_n)$ 定義爲 $\mathbf{Q}(u_1,\cdots,u_{n-1})(u_n)$，把 $U(u_1,\cdots,u_n)$ 定義爲 $U(u_1,\cdots,u_{n-1})(u_n)$。

所謂的幾何作圖，無非是保證我們能夠做出直線：$aX+bY=c$ 與圓 $(X-a_1)^2+(Y-b_1)^2=c_1^2$，其中 a, b, c, a_1, b_1, c_1 都是已給定的線段的長度。我們當然可以讓直線與直線相交，直線與圓相交，圓與圓相交。除此之外，我們是無能爲力了。讓直線 $aX+bY=c$ 與圓 $(X-a_1)^2+(Y-b_1)^2=c_1^2$ 彼此相交，其交點座標如果是 (x, y)，則 $x\in\mathbf{Q}(a, b, c, a_1, b_1, c_1)$ 或 $x\in\mathbf{Q}(a, b, c, a_1, b_1, c_1, d)$，其中 $d^2\in\mathbf{Q}(a, b, c, a_1, b_1, c_1)$。（爲什麼？）因此我們證明了以下的定理。

定理：

(1) $r\in S$ 的充分必要條件是存在 $r_1, r_2,\cdots, r_n=r$，使得 $r_{i+1}^2\in\mathbf{Q}(r_1,\cdots,r_i)$，$i=0, 1, 2,\cdots, n-1$。

(2) $r\in T$ 的充分必要條件是存在 $r_1, r_2,\cdots, r_n=r$，使得 $r_{i+1}^2\in\mathbf{Q}(\alpha, r_1,\cdots,r_i)$，$i=0, 1,\cdots, n-1$。

3.爲什麼這些問題無解？

第一節的討論把幾何三大問題變成代數問題。要證明這三個作圖問題只利用直尺與圓規是作不出來的，我們就要證明 $\sqrt{\pi}$，$\sqrt[3]{2}\notin S$，$x\notin T$，其中 $4x^3-3x-\alpha=0$。

先給幾個定義。

定義 令 U 爲一個體，n 個複數 $x_1,\cdots, x_n$ 叫做在 U 上線性獨立（linearly independent over U）的意思是說，以下的關係不可能成立，$u_1x_1+\cdots+u_nx_n=0$，其中 u_i

$\in U$，某些 $u_i \neq 0$。如若不然，$x_1, \cdots, x_n$ 叫做在 U 上線性相依。

例如，1 與 $\sqrt{2}$ 在 $\boldsymbol{Q}$ 上線性獨立，1 與 $\sqrt{2}$ 在 $\boldsymbol{Q}(\sqrt{2})$ 上線性相依。同理，如果把線性獨立的概念推廣到二度空間的向量，那麼兩個向量 $\overrightarrow{OV_1}$ 與 $\overrightarrow{OV_2}$ 在實數 $\boldsymbol{R}$ 上，線性獨立的充分條件是 OV_1V_2 是一個眞正的三角形（沒有退化成線段）。

定義 若 U 與 V 都是體，且 $U<V$，我們要定義 V 相對 U 的維數，記爲〔$V:U$〕。定義：〔$V:U$〕$\geqslant n$ 的意思是說存在 n 個數 $x_1, \cdots, x_n \in V$，且 $x_1, \cdots, x_n$ 在 U 上線性獨立。如果〔$V:U$〕$\geqslant n$，且 $V = Ux_1 + \cdots + Ux_n$，（其中 $x_1, \cdots, x_n$ 在 U 上線性獨立，$Ux_1 + \cdots + Ux_n = \{u_1x_1 + \cdots + u_nx_n$：其中 $u_i \in U\}$），則我們把〔$V:U$〕定爲 n。

例如，〔$\boldsymbol{Q}(\sqrt{2}):\boldsymbol{Q}$〕$=2$

〔$\boldsymbol{Q}(\sqrt[4]{2}):\boldsymbol{Q}$〕$=4$

因爲 $1, \sqrt[4]{2}, \sqrt{2}, \sqrt[4]{8}$ 在 $\boldsymbol{Q}$ 上線性獨立，且 $\boldsymbol{Q}(\sqrt[4]{2}) = \boldsymbol{Q} + \boldsymbol{Q}\sqrt[4]{2} + \boldsymbol{Q}\sqrt{2} + \boldsymbol{Q}\sqrt[4]{8}$，（何故？）（註三）

現在我們可以證明以下幾件事：

(1)若 $u_1, \cdots, u_n$ 是 n 個數，且

$u_{i+1}^2 \in U(u_1, \cdots, u_i)$

$u_{i+1} \notin U(u_1, \cdots, u_i)$

$i = 0, 1, \cdots, n-1$

則 〔$U(u_1, \cdots, u_n):U$〕$=2^n$

(2)若 $u \in S$，則〔$\boldsymbol{Q}(u):\boldsymbol{Q}$〕$=2^n$；若 $u \in T$，則〔$\boldsymbol{Q}(\alpha, u):\boldsymbol{Q}(\alpha)$〕$=2^m$，其中 n 與 m 是非負的整數。

(3)〔$\boldsymbol{Q}(\sqrt{\pi}):\boldsymbol{Q}$〕大於任意正整數。事實上，對於任意正整數 n，$1, \pi, \pi^2, \cdots, \pi^n$ 在 $\boldsymbol{Q}$ 上線性獨立。當然，$1, \pi, \pi^2, \cdots, \pi^n \in \boldsymbol{Q}(\pi) \subset \boldsymbol{Q}(\sqrt{\pi})$。

(4)〔$\boldsymbol{Q}(\sqrt[3]{2}):\boldsymbol{Q}$〕$=3$

(5)〔$\boldsymbol{Q}(\alpha, x):\boldsymbol{Q}(\alpha)$〕$=3$，如果 $4x^3-3x-\alpha=0$，且 $4t^3-3t-\alpha$ 是 $\boldsymbol{Q}(\alpha)$ 上的不可約多項式。（註四）

第(1)的證明，利用數學歸納法，只要注意：1 與 u_{i+1} 在 $U(u_1, \cdots, u_i)$ 上線性獨立，且 $U(u_1, \cdots, u_{i+1}) = U(u_1, \cdots, u_i) + U(u_1, \cdots, u_i)u_{i+1}$。當然還要證明一件事，〔$W:U$〕$=$〔$W:V$〕$\cdot$〔$V:U$〕，如果 $U \subset V \subset W$。

只要利用(1)與上一節的定理，就可得到第(2)。

第(3)是非常困難的，我們還會繼續討論。

第(4)：$1, \sqrt[3]{2}, \sqrt[3]{4}$ 在 $\boldsymbol{Q}$ 上線性獨立，且 $\boldsymbol{Q}(\sqrt[3]{2}) = \boldsymbol{Q} + \boldsymbol{Q}\sqrt[3]{2} + \boldsymbol{Q}\sqrt[3]{4}$。

第(5)：$1, x, x^2$ 在 $\boldsymbol{Q}(\alpha)$ 上線性獨立，且 $\boldsymbol{Q}(\alpha, x) = \boldsymbol{Q}(\alpha) + \boldsymbol{Q}(\alpha)x + \boldsymbol{Q}(\alpha) \cdot x^2$

綜合(2)與(3)，可知 $\sqrt{\pi} \notin S$。

綜合(2)與(5)，可知 $x \notin T$ 的充要條件是多項式 $4t^3-3t-\alpha$ 是 $\boldsymbol{Q}(\alpha)$ 上的不可約多項式。可以證明，當 $\theta = \frac{\pi}{6}, \frac{\pi}{4}, \frac{\pi}{3}$，或不爲零的代數數（見下節），$4t^3-3t-\alpha$ 是 $\boldsymbol{Q}(\alpha)$ 上的不可約多項式。

綜合(2)與(4)，可知 $\sqrt[3]{2} \notin S$。

因此，古希臘幾何三大問題是無解的，得證。

以上的證明，讀者如果還不十分清楚，請參考以下書籍：

F. Klein, Famous problems of elementary geometry ，「凡異出版社」翻印版。

N. Jacobson, Basic Algebra I, Chapter 4, §4.2, 4.12 ，「協進書局」翻印版。

Klein的書寫得明白曉暢，極適合初學者。這本書討論幾何三大問題比本文更詳盡。余介石先生曾翻譯本書，名爲「幾何三大問題」，收在商務印書館人人文庫之內。可惜這本書中譯本字跡模糊，印刷粗陋，極傷目力。

如果讀者具備一些基本的抽象代數的知識

，Jacobson 的書也可以參考。

幾何三大問題在十九世紀才獲得解決。在十九世紀初期法國數學家Évariste Galois（1811～1832年）發明Galois theory 來解決五次或五次以上不可約方程式有沒有根式解的問題。在Galois theory 中，體的擴張（field extension）是一個基本的概念。只要具備體的擴張的幾個基本概念，如維數、有理化分母、維數的相乘性，就可以解決三等分角問題與倍立方問題。1837年 Pierre Laurent Wantzel（1814～1848）提出這兩個問題的解法。幾千年來困擾人類的難題，一夜之間變成一個簡單的習題。

至於方圓問題，因為要證明：對於任意正整數n，1，π，…，π^n 在Q上線性獨立（也就是π是一個超越數，見下節），是一件比較麻煩的事。這件事，直到 1882 年，才由德國數學家Ferdinand Lindemann（1852～1937年）予以證明。

但是天下的事總是禍福相倚，利弊互補的。三等分角問題與倍立方問題的解決，並沒有帶給數學家太多的好處。方圓問題的解決卻替數學家開闢一個新天地,那就是超越數的理論。

4.超越數簡介

一個複數x叫做超越數（transcendental number）的意思是說，對於任何Q上的多項式$f(T)$，若$f(x)=0$，則$f(T)\equiv 0$。否則，就叫做代數數（algehraic numbers）。

不難看出，x是代數數的充分必要條件是〔$Q(x):Q$〕$<\infty$。因為，若〔$Q(x):Q$〕$=n$，則1，x，…，x^{n+1} 不可能在Q上線性獨立。所以可以找到不全為零的有理數$\alpha_0,\alpha_1,\cdots,\alpha_n$，使得$\alpha_0x^{n+1}+\alpha_1x^n+\cdots+\alpha_nx+\alpha_{n+1}=0$。所以$x$是代數數。

所有代數數形成的集合，變成一個體。（證明不是很容易，但是讀者值得自己做做看。）（註五）

如果x是超越數，則$Q(x)$的四則運算和有理函數$Q(T)=\{\frac{f(T)}{g(T)}:f(T),g(T)$是$Q$上的多項式$\}$的四則運算完全一樣，例如$(1+x)(1-x)=1-x^2$。但是如果$x$是代數數，例如$x=\sqrt{2}$，則

$$\begin{aligned}&(1+\sqrt{2})(1-\sqrt{2})\\&=1-(\sqrt{2})^2\\&=1-2\\&=-1\end{aligned}$$

我們可以把$x^2=(\sqrt{2})^2$ 繼續化簡。

超越數和無理數並不一樣。有理數是可以寫成$\frac{q}{p}$型式的數，其中p與q是整數，$p\neq 0$。實數＝有理數$\cup$無理數，複數＝代數數$\cup$超越數，無理數＝無理數中的代數數$\cup$實數中的超越數，實數的代數數＝有理數$\cup$無理數中的代數數。如$\sqrt[3]{2}$是代數數，πi 是超越數，i是代數數而不是實數。

法國數學家Joseph Liouville（1809～1882年）在 1844 年找出第一個超越數出來。Liouville 的方法是根據一個基本的概念：代數數是無法用有理數來高度逼近的。更精確的說，他證明

定理 若實數ξ是一個滿足

$$a_0\xi^n+a_1\xi^{n-1}+\cdots+a_{n-1}\xi+a_n=0$$

的代數數，a_i是整數，$a_0\neq 0$。則必存在一一個正數K，使得 $|\xi-\frac{q}{p}|\ \frac{K}{p^n}$，其中$\frac{q}{p}$是足夠靠近$\xi$的有理數，且$\frac{q}{p}\neq\xi$。

証明 設$f'(T)$是$f(T)$的導函數，其中$f(T)=a_0T^n+a_1T^{n-1}+\cdots+a_{n-1}T+a_n$。找一個正數$M$，使得只要$\xi-1<u<\xi+1$，就會有$|f'(u)|<\frac{1}{M}$。

若$\frac{q}{p}$足夠靠近ξ，使得

$$\xi-1<\frac{q}{p}<\xi+1 \quad 且 \quad f\left(\frac{q}{p}\right)\neq 0$$

則

$$\left|f\left(\frac{q}{p}\right)\right|$$

$$=\frac{|a_0q^n+a_1q^{n-1}p+\cdots+a_{n-1}qp^{n-1}+a_np^n|}{p^n}$$

$$\geqslant\frac{1}{p^n}$$

又 $f\left(\frac{q}{p}\right)$

$$=f\left(\frac{q}{p}\right)-f(\xi)$$

$$=\left(\frac{q}{p}-\xi\right)\cdot f'(\xi_1)$$

其中 $\xi-1<\xi_1<\xi+1$

故 $\left|\xi-\frac{q}{p}\right|=\frac{\left|f\left(\frac{q}{p}\right)\right|}{f'((\xi_1)}>\frac{M}{p^n}$

得證。

利用以上定理，Liouville 指出

$$\xi=0.110001000\cdots$$

$$=\frac{1}{10}+\frac{1}{10^{2!}}+\frac{1}{10^{3!}}+\frac{1}{10^{4!}}$$

$$+\cdots+\frac{1}{10^{n!}}+\cdots$$

是一個超越數。例如，假設ξ滿足一個 57 次的方程數，且$K=1,000$，那麼我們只要取一個有理數η，η是ξ的前 57 項的和，即

$$\eta=\frac{1}{10}+\frac{1}{10^{2!}}+\cdots+\frac{1}{10^{57!}}$$

$$=\frac{q}{10^{57!}}$$

q是某個整數。

則

$$|\xi-\eta|$$

$$=\frac{1}{10^{58!}}+\frac{1}{10^{59!}}+\cdots<2\ \frac{1}{10^{58!}}$$

$$<\frac{1,000}{(10^{57!})^{57}}$$

因此Liouville 定理不成立。故ξ不得不是超越數。

三十年以後，Georg Cantor 利用集合論的方法證明，所有的實數的代數數是可數的（countable）而實數是不可數的（uncountable），因此必有一個超越數存在。

1873 年法國數學家Charles Hermite（1822～1901 年）證明

$$e\left(=\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n\right)$$

是超越數。

1882 年F. Lindemann 利用Hermite的想法，證明π是超越數。事實上Lindemann 證明：若$a\neq 0$是一個代數數，則e^a是一個超越數。取$a=1$，得證e是超越數。取$a=i\pi$，則$e^{i\pi}=\cos\pi+i\sin\pi=1$ 不是超越數，故$i\pi$不是代數數；得證π是超越數。

1900 年David Hilbert（1862～1943 年）在巴黎的國際數學會提出有名的Hilbert 的 23 個問題。他的第七個問題是：如果a與b都是代數數，且$a\neq 0$，1，b是無理數，則a^b是否爲超越數？例如，

$$2^{\sqrt{2}},\ e^{-\pi}=e^{i\pi\cdot i}=(-1)^i,$$

$$e^{i\pi b}=(-1)^b$$

是不是超越數？

在 1934 年，俄國數學家A.O. Gelfond 與德國數學家T. Schneider 分別解決了 Hilbert 第七問題，答案是肯定的。

要證明某些數是超越數並不是很容易的。例如，0.1 2 3 4 5 6 7 8 9 10 11 12… 是不是超越數？（答案：是。）又如：$e+\pi$，e^e，π^π，π^e，$2^{2^{\sqrt{2}}}$，2π，2^e，Euler 常數$\left(=\lim_{n\to\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}-\ln n\right)\right)$是不是超越數？事實上，到現在爲止，我們連這些數是不是無理數都不知道。

由於超越數的研究，數學家連帶的研究，

代數數的對數的線性組合估計值，整係數多項式解的精確範圍，有理數逼近代數數的方式。同時數學家也設計出許多巧妙的方法來討論超越數。Hilbert 在提出第七問題時特別強調，要解決這個問題勢必發見許多新的方法與新的角度來瞭解無理數與超越數的本質。

有關Lindemann 定理的證明，讀者可參考以下資料，

S. Lang Algebra, Appendix, 493～499頁，「美亞書局」翻印版，這裏的證明是採用Gelfond 與Schneider方法。讀者只要具備複變函數的知識就可看懂。並且，就在這裏，Schanuel 猜測第一次出現在衆眼前，Schanuel 猜測幾乎統攝超越數理論中許多主要的定理，如Lindemann n元素定理，Gelfond-Schneider 定理，Baker n元素定理。可惜這個猜測到今天還沒有證明出來。

註 釋

註一 在放鬆這些條件時，例如，假設直尺可以刻劃，三等分角問題就可以進行了。有關這類變化，請參考F. Klein, Famous Problems of elementary geometry，「凡異出版社」翻印本。

註二 唸過抽象代數的人可能對我們在這裏的「體」的定義覺得不夠一般性。在抽象代數中，「體」是具有加法與乘法兩種運算的代數體系，這兩種運算具有某些特殊的性質。我們在這裏給的定義，其實是複數體之內的子體（subfields）的定體。歷史上來看，這種定義或下一個定義$U(u_1, \cdots, u_n)$就是Kronecker 所謂的「domains of rationality」，這是數學家最先瞭解的「體」。

註三 要證明 $\boldsymbol{Q}(\sqrt[4]{2})=\boldsymbol{Q}+\boldsymbol{Q}\sqrt[4]{2}+\boldsymbol{Q}\sqrt{2}+\boldsymbol{Q}\sqrt[4]{8}$

我們只要能夠把分母有理化即可。具體的說，對於任意的多項式

$$g(t)\in\boldsymbol{Q}[t]$$

只要$g(\sqrt[4]{2})\neq 0$，我們都要有辦法把$\dfrac{1}{g(\sqrt[4]{2})}$變成$a+b\sqrt[4]{2}+c\sqrt{2}+d\sqrt[4]{8}$的型式，其中$a$，$b$，$c$，$d$是有理數。因爲$f(t)=t^4-2$ 是$\boldsymbol{Q}$上的不可約多項式，且$f(t)$與$g(t)$互質（否則$f(t)$是$g(t)$的因式，$f(\sqrt[4]{2})=0$，故$g(\sqrt[4]{2})=0$），故可找到多項式$\phi(t)$與$\psi(t)$，使

$$\phi(t)\cdot f(t)+\psi(t)\,g(t)=1$$

以$t=\sqrt[4]{2}$代入，得

$$\frac{1}{g(\sqrt[4]{2})}=\psi(\sqrt[4]{2})$$

利用$(\sqrt[4]{2})^4=2$ 的關係，可以把$\psi(\sqrt[4]{2})$化成

$$a+b\sqrt[4]{2}+c\sqrt{2}+d\sqrt[4]{8}$$

的型式。

註四 令$\alpha=\dfrac{1}{2}$，請讀者證明 $4t^3-3t-\dfrac{1}{2}$是$\boldsymbol{Q}$上的不可約多項式。

註五 若α與β是代數數，則

$$[\boldsymbol{Q}(\alpha,\beta):\boldsymbol{Q}]<\infty$$

今 $\alpha+\beta$，$\alpha\beta\in\boldsymbol{Q}(\alpha,\beta)$

故

$1, \alpha+\beta, (\alpha+\beta)^2, \cdots, (\alpha+\beta)^n$

必定在$\boldsymbol{Q}$上線性相依，其中n是某個正整數。因此$\alpha+\beta$是代數數。或者，令

$$f(t),\ g(t)\in\boldsymbol{Q}[t]$$

且 $f(\alpha)=0$，$g(\beta)=0$

令$\alpha=\alpha_1, \alpha_2, \cdots, \alpha_n$是$f(t)=0$的$n$個根，考慮$h(t)=g(t-\alpha_1)g(t-\alpha_2)\cdots g(t-\alpha_n)$。則$h(\alpha+\beta)=0$，則$h(t)$的係數是$\alpha_1, \alpha_2, \cdots, \alpha_n$ 的對稱多項式，故$h(t)\in\boldsymbol{Q}[t]$。同理請讀者證明$\alpha\beta$ 也是代數數。

（本文作者任敎於台大數學系）