解方程式的故事

王金龍
台大數學系

2012 年 5 月 3 日於建國中學

求解(一元)一次方程式

$$ax = b.$$

解法:

$$x = \frac{b}{a}.$$

Q: 這是什麼意思? 例如 $a = 7$, 如何做出 $b/7$?

Q: 數與量有何差異?

$$\frac{a}{b} = \frac{c}{d} \quad \Longleftrightarrow \quad d = \frac{bc}{a}.$$

求解二次方程式 (巴比倫 2000 BC, 印度, 中國)

$$ax^2 + bx + c = 0.$$

解法:

$$x^2 + \frac{b}{a}x = -\frac{c}{a},$$

$$X^2 = \left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2},$$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Q: 這是什麼意思? 例如 $X^2 = 7, X^2 = d$, 如何做出 X?

求解三次方程式 (義大利 Tartaglia, Cardano 1545)

$$x^3 + ax^2 + bx + c = 0.$$

配三次方: 令

$$X = x + \frac{a}{3},$$

整理得到

$$X^3 + pX + q = 0.$$

其中

$$p = b - \tfrac{1}{3}a^2, \quad q = c - \tfrac{1}{3}ab + \tfrac{2}{27}a^3.$$

Q: 如何進一步消去 pX 項?

設 $X = u + v$ 帶入. 整理得到

$$u^3 + v^3 + q + (3uv + p)(u + v) = 0.$$

可選擇 $v = -p/3u$, 即 $X = u - p/3u$, 得到

$$(u^3)^2 + q(u^3) - \left(\frac{p}{3}\right)^3 = 0.$$

這是 u^3 的二次方程, 因此

$$u^3 = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}.$$

Q: 這是什麼意思? 例如 $u^3 = 2, u^3 = d$, 如何做出 u? 當 $27q^2 + 4p^3 < 0$ 時該如何處理?

求解四次方程式 (Ferrari, Cardano 的學生)

$$x^4 + ax^2 + bx + c = 0.$$

解法: 動態配方法, 引入參數 t,

$$\left(x^2 + \frac{a}{2} + t\right)^2 - \left(2tx^2 - bx - c - \left(\frac{a}{2} + t\right)^2\right).$$

進而要求剩餘項爲 2 次完全平方式, 即

$$b^2 + 8t\left(c + \left(\frac{a}{2} + t\right)^2\right) = 0.$$

這是 t 的 3 次方程, 因此可用 2 次與 3 次方根解出 $t \in \mathbb{R}$.

固定一解 t, 則方程式可轉化成

$$\left(x^2+\frac{a}{2}+t\right)^2=2t\left(x-\frac{b}{4t}\right)^2,$$

即兩個 2 次方程式:

$$x^2+\frac{a}{2}+t=\pm\sqrt{2t}\left(x-\frac{b}{4t}\right).$$

因此, 4 次方程式的根可由其係數 a,b,c 重複使用開 2 次與 3 次方根解出.

Q: 如果 $c>0$, 則 $t<0$. 因此以上 2 次方程式的係數爲複數. 繼續以根公式求解時, 複數的 2 次方根是什麼意思?

複數的 2 次方根還是複數: $(u+vi)^2 = a+bi$ **等價於**

$$u^2 - v^2 = a, \qquad 2uv = b.$$

$$u^4 - au^2 - \frac{b^2}{4} = 0 \quad \Longrightarrow \quad u^2 = \frac{a \pm \sqrt{a^2+b^2}}{2}.$$

不失一般性可假設 $b > 0$**, 則解得**

$$u = \pm\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}}, \qquad v = \pm\sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}.$$

因此 4 次方程的解均可表爲 $\sqrt{A+B\sqrt{C+D\sqrt[3]{E+F\sqrt{G}}}}$ **的組合. 其中** $A,B,C,D,E,F,G \in \mathbb{Q}(a,b,c)$**. 即** **根式解**.

基本問題: 複數如何開 n 次方根? $\sqrt[n]{d} = ?$

根據約定, $i \equiv \sqrt{-1}$ 爲方程式 $x^2 = -1$ 的一個假想解.

$\mathbb{C} := \mathbb{R} + i\mathbb{R}$ 爲 **Euler (尤拉, 1707-1783)** 的複數平面.

$$z = x + yi = r(\cos\theta + i\sin\theta) =: re^{i\theta}.$$

複數乘法的幾何意義:

$$\begin{aligned} & z_1 z_2 \\ &= r_1(\cos\alpha + i\sin\alpha) \times r_2(\cos\beta + i\sin\beta) \\ &= r_1 r_2(\cos\alpha\cos\beta - \sin\alpha\sin\beta + i(\cos\alpha\sin\beta + \sin\alpha\cos\beta)) \\ &= r_1 r_2(\cos(\alpha+\beta) + i\sin(\alpha+\beta)) \\ &= r_1 r_2\, e^{i(\alpha+\beta)}. \end{aligned}$$

對所有 $n \in \mathbb{N}$,

$$z^n = r^n(\cos n\theta + i \sin n\theta) = r^n e^{in\theta}.$$

$$z^n = 1 \quad \Longleftrightarrow \quad \theta = k\frac{2\pi}{n}, \quad k = 0, \cdots, n-1.$$

記 $\zeta = e^{2\pi i/n}$ 爲 **primitive** n 次方根,

$$z^n = d = \rho e^{i\alpha} \quad \Longleftrightarrow \quad z = \sqrt[n]{\rho}\, e^{i\alpha/n}\zeta^k, \quad 0 \le k \le n-1.$$

因此, n 次方程式 $x^n - d = 0$ 恰有 n 個複數解.

Q: 還是老問題, 如何做出 $\sqrt[n]{\rho}$ 以及 $\cos\frac{\alpha}{n} + i\sin\frac{\alpha}{n}$?

複數部份: n 等分角問題.

$$a + bi = \cos n\theta + i \sin n\theta = (\cos\theta + i \sin\theta)^n$$

例如 $n = 3$,

$$a = \cos 3\theta = \cos^3\theta - 3\cos\theta \sin^2\theta = 4\cos^3\theta - 3\cos\theta.$$

這是一個特別的 3 次方程式

$$x^3 - \frac{3}{4}x - \frac{a}{4} = 0.$$

由於 $(\frac{3}{8})^2 - (\frac{a}{12})^3 > 0$, **問題化約爲正數開 2 次及 3 次方根.**

對於一般的 θ **與** n, **必須使用 弧長拉直 的辦法.**

實數 (長度) 開 n 次方根: $x^n = \rho$.

若有 2 次曲線 (圓, 橢圓, 拋物線, 雙曲線) 的製圖器, 則

$$x^3 = \rho \quad \Longleftrightarrow \quad x^2 = \rho y, \qquad xy = 1.$$

對於 3 次方程式 $x^3 + ax^2 + bx + c = 0$ 的實數解, 亦可用

$$-cy = x^2 + ax + b, \qquad xy = 1.$$

對於 4 次方程 $x^4 + ax^2 + bx + c = 0$, 則用

$$x^2 + a + by + cy^2 = 0, \qquad xy = 1.$$

這是橢圓 (或雙曲線) 與雙曲線 $xy = 1$ 的交集.

習題: 設計 2 次曲線 (甚至高次曲線) 的製圖器.

在古希臘, 數的觀念依賴於幾何建構的可能性. 基本方法是對於給定的幾何圖像, 使用圓規與直尺, 建構新圖像.

Elements (原本) 是 Euclid (歐幾里得, 300 BC.) 集大成的創作, 開創與奠定數學公理與證明的基本架構.

他遺留下幾何 (尺規) 作圖三大難題:

1. 三等分角問題:

$$4x^3 - 3x - a = 0, \quad a = \cos\alpha.$$

2. 倍立方問題:

$$x^3 = 2.$$

3. 圓化方問題:

$$x^2 = \pi.$$

記尺規作圖之**數體 (fields)** 序列爲 $F_1 \subset F_2 \subset \cdots$, 其中 $x = a + b\sqrt{w} \in F_k$ 有 $a, b, w \in F_{k-1}$, 但 $\sqrt{w} \notin F_{k-1}$.

若倍立方問題可以尺規作圖達成, 則有 $x^3 = 2$, $x \in F_k$, $x \notin F_{k-1}$, 其中 $F_1 = \mathbb{Q}$, $k \geq 2$ (因爲 $x \notin \mathbb{Q}$). 由

$$0 = x^3 - 2 = (a^3 + 3ab^2w - 2) + (3a^2b + b^3w)\sqrt{w}$$

$$\iff \quad a^3 + 3ab^2w - 2 = 0, \quad 3a^2b + b^3w = 0.$$ 因此,

$$y = a - b\sqrt{w}$$

也是一個解. 但 $y \neq x$, 顯然矛盾.

習題: 應用此論證於三等分角, 及 $\mathbb{Q}$ 的實 n 次方根問題.

十八世紀末, 方程式理論的最根本問題有二:

A. 複數係數的 n 次 $(n \geq 1)$ 多項式方程式

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

是否一定有 **複數根**?

B. 若是, 這 n 個解是否可以表示成一個由係數 $a_0, \cdots, a_{n-1}$ 通過有理運算以及根式

$$+ \quad - \quad \times \quad / \quad \sqrt[k]{}$$

在有限步驟所組成的 **公式** 所得到? 亦即, $f(x) = 0$ 是否一定有 **根式解**?

Gauss (高斯) 在其 1799 年的博士論文證明了A, 即所謂的 代數基本定理. 但所有的證明都要用到分析或拓樸:

證明: 若對於所有的 $z \in \mathbb{C}, f(z) \neq 0$, 則 $|f(z)|$ 有最小值 $m > 0$ (Why?). 假定 $|f(a)| = m$, 對 $z - a$ 展開

$$f(z) = f(a) + c_k(z-a)^k + c_{k+1}(z-a)^{k+1} + \cdots + c_n(z-a)^n,$$

其中 $c_k \neq 0$. 令 $h^k = -f(a)/c_k$. 則對於很小的正數 $t > 0$,

$$\begin{aligned} f(a+th) &= f(a) + c_k h^k t^k + O(t^{k+1}) \\ &= f(a)(1 - t^k) + O(t^{k+1}). \end{aligned}$$

因此 $|f(a+th)| < |f(a)|$, 得到矛盾.

Gauss 決定一生投入數學研究起因於他在 19 歲時 (1796) 找到了 正 n 邊形 能夠以尺規作圖的充分必要條件:

$$n = 2^m p_1 \cdots p_k, \qquad p = 2^{2^s} + 1.$$

當 $s = 0, 1, 2, 3, 4$, Fermat 質數爲 $p = 3, 5, 17, 257, 65537$. 但

$$2^{2^5} + 1 = 641 \times 6700417.$$

對於正 17 邊形, 高斯算出 (算學講話)

$$16\cos\frac{2\pi}{17} = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.$$

臨終前, Gauss 要求將正 17 邊形刻在他的墓碑上.

關於 B: 根式解的可能與否, 是由法國天才數學家 Galois (伽羅瓦 1811-1832) 所完全解決.

- 14 歲: 讀 Legendre (勒襄得) 的幾何原本.
- 15 歲: 讀 Lagrange 分析與方程式的研究論文.
- 16 歲: 考 Ecole Polytechnique 沒上, 進 Ecole Normale.
- 17 歲: 發表論文. 其方程式理論未被 Cauchy 接受.
- 18 歲: 父親自殺. 再考 Ecole Polytechnique 未果.
- 19 歲: 再次投稿於 Fourier (傅立葉) 未果.
  當年法國科學院大獎最後授與了 Abel 與 Jacobi.
- 20 歲: 死於一場政治與愛情因素的決鬥.

1830, 19 歲的 Galois 發明 群 (group) 的觀念與理論.

排列群 (對稱群) S_n: 給定集合 $S = \{1, \cdots, n\}$, 一個排列 $\sigma : S \to S$ 是一個 **1-1 (且 onto)** 函數. 乘法規則

$$\sigma, \tau \in S_n, \qquad \sigma\tau := \sigma \circ \tau.$$

反元素 σ^{-1} 即反函數. 排列由 **交換** 生成, 均有 **循環分解**.

一般而言 $\sigma\tau \neq \tau\sigma$. 例如:

$$(123)(12) = (13), \qquad (12)(123) = (23).$$

例: **循環群 (cyclic group)** $C_k = \{1, \zeta, \cdots, \zeta^{k-1}\}$.

例: 最簡單的非交換群是 **項鏈群 (dihedral group)** D_{2k}.

例: 物理基本粒子之分類依賴其對稱 **李群 (Lie group)**.

考慮 $f(x) \in \mathbb{Q}[x]$ (或一般的 $F[x], F$ 爲某一數體):

$$\begin{aligned} f(x) &= x^n + s_1 x^{n-1} + \cdots + s_{n-1} x + s_n \\ &= (x - x_1) \cdots (x - x_n), \end{aligned}$$

其中 $x_i \in \mathbb{C}$. 令數體 $K = \mathbb{Q}(x_1, \cdots, x_n)$.

Galois 考慮 K 上與四則運算相容的所有可能對稱 (field automorohism), $\sigma : K \to K$.

由於 $\mathbb{Q} \to \mathbb{Q}$ 不會被變動 (Why?), $\sigma f(x) = f(\sigma x)$. 因此 σ 對應到根 $\{x_1, \cdots, x_n\}$ 的一個排列. 即 $\sigma \in S_n$. 稱子群

$$G = \mathrm{Gal}(K/\mathbb{Q}) \subset S_n$$

爲方程式 $f(x) = 0$ 的 Galois 群.

開根號與 **Galois** 群之間具有精確對應:

定理: 如果數體 F 包含 ζ_k, 則

(1) 開根號 $x^k - a = 0$ 的群 G 都是循環群.

(2) 若 $G = C_p$, 其中 p 爲質數, 則逆命題也成立.

一般情形下, **Galois** 發現 **群體 (groups/fields) 關鍵對應**:

$$\mathbb{Q} \subset F_1 \subset F_2 \subset \cdots \subset F_N = K,$$
$$G \supset G_1 \supset G_2 \supset \cdots \supset G_N = \mathbb{1}.$$

我們希望每一次的數體擴張 $F_{k+1} = F_k(\sqrt[n_k]{d_k})$. 這等價於要求每一階段的 **Galois** 群 $G_k := \mathrm{Gal}(K/F_k)$ 滿足

$$G_k \rhd G_{k+1}, \qquad G_k/G_{k+1} \cong \textbf{cyclic group}.$$

其中 $G \supset H$ 能夠進行 **商群** G/H 的操作:

$$G \rhd H \quad \Longleftrightarrow \quad G = \bigcup g_i H, \quad g_i H g_j H = g_i g_j H.$$

即 $g^{-1} H g = H, \forall\, g \in G$. 例如 $S_n \rhd A_n$ (**偶排列**), $D_{2k} \rhd C_k$.

- 不變量觀點: n 次方程式有無窮多種,
- 但是 $G \subset S_n$ 只有有限個可能.
- 因此 **Galois** 群是多項式方程的 **invariants**.

$$S_2 \rhd_2 \mathbb{1}$$

$$S_3 \rhd_2 A_3 \rhd_3 \mathbb{1}$$

$$S_4 \rhd_2 A_4 \rhd_3 K_4 \rhd_2 C_2 \rhd_2 \mathbb{1}$$

$K_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ 爲 **Klein** 的 **4** 元群.

當 $n \geq 5$ 時, $|S_n| = n!$, S_n 的結構急劇變複雜.

引理: $S_5 \rhd A_5$, $|A_5| = 60$ 爲第一個**非交換單群** **(simple group)**. 事實上 $A_n, n \geq 5$ 都是單群.

證明的想法: 如果 $(123) \in A_n$, 則 $(ijk) \in A_n$:

$$(ijk) = g(123)g^{-1}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i & j & k & l & m \end{pmatrix}$$

(可能需要 l, m 使 g 是偶排列). 而 A_n 可由所有 (ijk) 生成.

定理 **(Abel 1824, Ruffini 1799, Galois 1830)**: 一般的 n 次方程式, $n \geq 5$, 沒有根式解. 它們的 Galois 群 $G = S_n$.

Well, the story does not end like that ...

不要只是告訴我這不能!

近代發展 I. 進入微積分的世界: 開根號可表示成

$$\sqrt[n]{a} = e^{\frac{1}{n}\log a} = \exp\left[\frac{1}{n}\int_1^a \frac{dx}{x}\right].$$

或是在 n 等分角的問題裡: 若 $a = \sin\theta$, 則

$$\sin\frac{\theta}{n} = \sin\frac{\sin^{-1} a}{n} = \sin\left[\frac{1}{n}\int_0^a \frac{dx}{\sqrt{1-x^2}}\right].$$

因此, 不妨考慮更一般的 Riemann (黎曼 1850) theta 函數, 以及橢圓積分/週期積分 (elliptic/periods integrals)

$$\vartheta_{\vec{n}}\left[\int_{\Gamma_j} \frac{x^i dx}{\sqrt{F(x)}}\right].$$

這將進入 Abel-Jacobi 理論, 代數幾何學的開始.

Kronecker 1858 ($n = 5$), Hermite 1861 ($n = 5$), Klein 1879, 1884, 1899 ($n \geq 5$, 特殊情形).

定理 1 (Jordan, Thomae 1870, Umemura 1984)

給定多項式 $f(x) \in \mathbb{C}[x]$.
若 n 爲奇數, 令 $F(x) := x(x-1)f(x)$,
若 n 爲偶數, 令 $F(x) := x(x-1)(x-2)f(x)$. 則

$$f\left(\vartheta^4_{1,0;0,0}\vartheta^4_{1,1;0,0} + \vartheta^4_{0,0;0,0}\vartheta^4_{0,1;0,0} - \frac{1}{2}\frac{\vartheta^4_{0,0;1,0}\vartheta^4_{0,1;1,0}}{\vartheta^4_{1,0;0,0}\vartheta^4_{1,1;0,0}}\right) = 0.$$

$\vartheta_* = \vartheta_*(\Omega)$ 是由超橢圓曲線 $y^2 = F(x)$ 的週期積分矩陣 (Ω_{ij}) 所定義的 **Riemann-Segel 模函數** **(modular forms).**

近代發展 II. 利用 symbolic computation 具體實現 Galois 理論. 例如, 用 4 次代換, 5 次方程式可以化簡成

$$f(x) = x^5 + ax + b = 0.$$

考慮 Lagrange–Galois **預解式** (resolvent):

$$f^*(x) = x^6 + 8ax^5 + 40a^2x^4 + 160a^3x^3 + 400a^4x^2 + (512a^5 - 3125b^4)x + (256a^6 - 9375ab^4).$$

定理 2 (Dummit 1991, Hagedorn 2000)

若 $f(x) \in \mathbb{Q}[x]$, 則 $f(x) = 0$ 有根式解充分必要於 $f^*(x) = 0$ 有有理根. 6 次方程式亦有類似方法.

近代發展 III. 多變數聯立方程與數值方法.

Newton's method (牛頓法, 1671):

$$x_{n+1} = N(x_n) := x_n - \frac{f(x_n)}{f'(x_n)}.$$

方程 $f(a) = 0$ 充分必要於 $N(a) = a$. 若 $f(x)$ 是多項式, 則任何一個根 (可爲複數根, 重根) 都會迅速收斂.

對於多變數 $\vec{x} \in \mathbb{C}^n, \vec{y} = F(\vec{x}) \in \mathbb{C}^n$, 亦有

$$\vec{x}_{n+1} = N(\vec{x}_n) := \vec{x}_n - F'(\vec{x}_n)^{-1} F(\vec{x}_n).$$

其中 $F'(\vec{x}_n)$ 是 **Jacobi** 微分矩陣. 牛頓動態系統 N 仍是現代主要的數值解根方法, 但其收斂性尚未被完全理解.

多變數計算宜借助於電腦, 但很容易超越電腦的極限!

例如: $x^3+y^3=1, \qquad x^5+y^5=1.$

MATHEMATICA 或 **MAPLE** 都可以在 **0.1** 秒之內算出所有的 **6** 組非 $0,-1$ 解. (x,y) 均形如

$$(-0.791887+0.755487\sqrt{-1}, -0.0470208+0.998894\sqrt{-1}).$$

但是對 **3** 個變數的情形 **(**假設 $x,y,z\neq 0,-1$**)**

$$x^3+y^3+z^3=1, \quad x^5+y^5+z^5=1, \quad x^7+y^7+z^7=1,$$

電腦永遠跑不停, 或回答有 ∞ 多解. 事實上解恰有 **18** 組.

這些研究深植於現代數學的核心— 代數幾何與數論.

歡迎進入數學的世界

理性思維的最高殿堂

THANK YOU