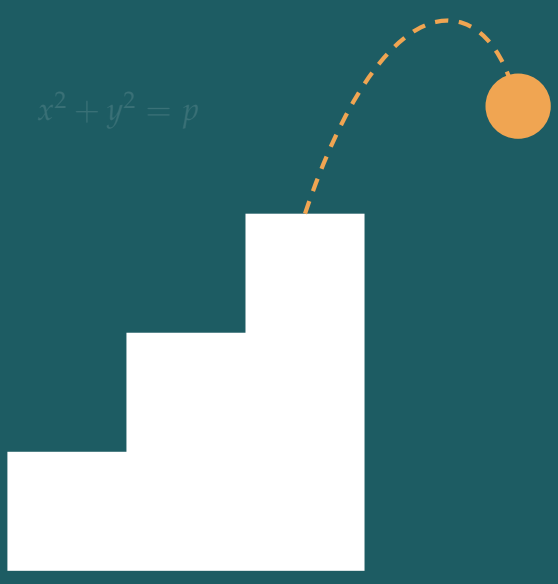
STEP 備試 · 大學數學

# Beyond STEP

第 6 章

## 代數與結構



KEITH McNULTY

# Beyond STEP

以歷屆 STEP 試題為門
走進大學數學

第 6 章

## 代數與結構

Keith McNulty

**Beyond STEP：以歷屆 STEP 試題為門，走進大學數學**

**第 6 章：代數與結構**

本冊是 *Beyond STEP* 全書 13 章中的第 6 章。全書、各章的單行本、每一節的可列印工作紙，以及每一道 STEP 試題的詳細解答，均可在 beyondstep.keithmcnulty.org 免費閱讀及下載。

2026 年 11 月首次於網上發表。

本 PDF 內凡屬作者本人創作的內容，包括正文、解答、插圖、練習及答案，均按照 Creative Commons CC0 1.0 Universal 授權條款貢獻予公有領域：你可以為任何目的複製、改編及分享，毋須徵求許可。詳見 creativecommons.org/publicdomain/zero/1.0。

本書討論的 STEP 試題，版權屬 Cambridge University Press & Assessment 所有。本書並無轉載這些試題：每一題均附連結，通往官方來源的題目，即 STEP Support Programme 的試題資料庫或 OCR 的歷屆試卷。

如有錯漏，歡迎到 github.com/keithmcnulty/step_book_mcnulty 提交 issue 指正。

章

# 6

# 代數與結構

代數中每一個巧妙的技巧背後都有一個結構，而理解這個結構，比掌握多少技巧都更有價值。

**本章內容**


| | | |
|---|---|---|
| **6.1** | 以單位根為根的多項式 | STEP III 2010 |
| **6.2** | 高斯的正十七邊形 | STEP II 1991 |
| **6.3** | 以 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 為根的多項式 | STEP II 2023 |
| **6.4** | 解四次方程 | STEP III 2017 |
| **6.5** | 從公理出發的微分法 | STEP II 1992 |
| **6.6** | 子羣的併集 | STEP II 1988 |
| **6.7** | 四元數羣 | STEP III 1993 |
| **6.8** | 由奇異矩陣組成的羣 | STEP III 1996 |
| **A** | 練習答案 | 第 59 頁 |

# 從方程到結構

數學是給不同事物起相同名字的藝術。

— 龐加萊（Henri Poincaré）

在歷史上的大部分時間裏，代數就是解方程。四千年前，巴比倫人已懂得解二次方程；十六世紀的意大利數學家解決了三次和四次方程；其後近三百年間，五次方程卻令一切嘗試無功而還。到了 1820 至 1830 年代，問題終於有了答案，而這個答案徹底改變了代數。阿貝爾（Niels Henrik Abel）證明了五次方程不存在一般的求根公式，伽羅瓦（Évariste Galois）則確切說明了哪些方程可以求解，他研究的不是方程本身，而是方程各根的對稱性。為此，他必須創造一種全新的數學對象：羣（group）。

從計算答案轉向研究結構，這個轉變正是本章的主題。現代代數問的不再是「解是甚麼？」，而是「這是哪一類對象？它容許哪些運算？」這些問題的答案，既解釋了舊有技巧為何奏效，也解決了單靠技巧永遠無法解決的問題。

## 結構為何重要

以下三個古老的問題，兩千年來令一切嘗試都無功而還：只用直尺和圓規，作出體積為已知立方體兩倍的立方體；三等分任意角；作出正 7 邊形。三者都不可能做到，而在十九世紀找到的證明，靠的並不是巧妙的作圖，而是關於結構的論證：所討論的是尺規所能到達的數所組成的域(field)的次數(degree)(Section 6.3)。同一套理論也解釋了為何正 17 邊形可以作出 (Section 6.2)，以及為何四次方程可解而五次方程不可解 (Section 6.4)。

結構還可以搬到別處去。晶體的對稱、多項式各根的置換（permutation）、三維空間的旋轉、扭計骰的各種轉法，以及橢圓曲線（elliptic curve）上的點，全都滿足羣的公理（axiom）。只要從公理出發把一條定理證明一次，它便在以上所有情況中成立。這種簡約，即龐加萊所說的給「不同事物起相同名字」，正是抽象代數（abstract algebra）如此強大的原因。

## 你在大學會遇到甚麼

在一年級，你會遇到羣（帶有一個運算並滿足三條公理的集合），通常還有環（ring）和域（帶有加法和乘法的集合）。你會證明拉格朗日定理（Lagrange's theorem），即子羣（subgroup）的大小整除羣的大小，並認識置換、對稱羣（symmetry group）和矩陣羣（matrix group）。到了二、三年級，這些內容會引向伽羅瓦理論(Galois theory)，它把域

和羣聯繫起來，回答有關方程和作圖的經典問題；引向表示論（representation theory），它透過矩陣來研究羣；還會引向代數數論（algebraic number theory），Section 1.7 中的想法在那裏會得到嚴格的基礎。本章最後三節講的是羣。羣已不在 STEP 的課程範圍之內（已於 2019 年刪去），但這些題目本身自成一體，每一節都會給出所需的定義。

### 貫穿本章的問題

**三個大問題**

1. **甚麼可以由甚麼構造出來？**從有理數出發，透過開平方根或解方程，可以到達哪些數？又怎樣證明某個數無法到達？
2. **方程的公式為何奏效？**二次、三次和四次方程都有求根公式，背後隱藏的原因是甚麼？到了五次，又有甚麼改變了？
3. **抽象化帶來甚麼？**如果我們只憑對象所遵守的規則來描述它們，會有甚麼結果？

### 本章的想法

| § | 課題 | 想法 |
|---|---|---|
| 6.1 | 分圓多項式（cyclotomic polynomials） | 按階（order）把單位根（roots of unity）分類 |
| 6.2 | 正 17 邊形 | 高斯週期（Gauss periods）：和與積給出二次方程 |
| 6.3 | 最小多項式（minimal polynomials） | 消去根式；次數相乘 |
| 6.4 | 解四次方程 | 對稱函數（symmetric functions）；三次預解式（resolvent cubic） |
| 6.5 | 從公理出發的微分法 | 由規則決定的運算 |
| 6.6 | 子羣的併集（union） | 從羣公理出發作論證 |
| 6.7 | 四元數羣（quaternion group） | 用矩陣表示運算 |
| 6.8 | 由奇異矩陣（singular matrices）組成的羣 | 按字面理解定義 |

### 如何閱讀本章

這些題目當中，有不少可以靠蠻力完成：把所有式子展開、比較係數、逐一檢查每種情況。如有需要，不妨先這樣做。然後回頭想一想，是甚麼令蠻力行得通，背後有沒有結構上的原因。結構上的原因通常較為簡短，總是更具啟發性，而當蠻力再也行不通時，

你需要的正是它。

# 6.1 以單位根為根的多項式

**題目**

**STEP III 2010，第 3 題**

繼續閱讀之前，請先看題目（原題為英文）。題目載於 STEP Support Programme 的試題資料庫：

`step.maths.org/questions/10-s3-q3`

## 引子

$n$ 次單位根（roots of unity），即 $z^n = 1$ 的解，位於正 $n$ 邊形的各個頂點上。但它們並非全都一樣。例如在 12 次單位根之中，1 本身已是一次單位根，$-1$ 是二次單位根，$\mathrm{i}$ 是四次單位根，而十二個之中只有四個，即本原（primitive）的那些，才需要走足十二步方能回到 1。

按所需的步數把單位根分類，再由每一類構造一個多項式，便得到分圓多項式（cyclotomic polynomials，此名源自希臘文，意即「分割圓周」）。它們是 $z^n - 1$ 的基本構件，正如質數是整數的基本構件一樣；高斯（Gauss）的正 17 邊形作圖法（Section 6.2）、單位根篩選法（Section 5.2）以及現代數論中的不少內容，背後都有它們的身影。

## 動筆之前

**想一想** 每個 $n$ 次單位根都滿足 $z^n = 1$。但使它等於 1 的最小正整數次冪，可能小於 $n$。對於四個 4 次單位根 $1$、$\mathrm{i}$、$-1$、$-\mathrm{i}$，這個最小的冪次分別是多少？

$1^1 = 1$，$(-1)^2 = 1$，而 $\mathrm{i}^4 = (-\mathrm{i})^4 = 1$，且沒有更小的冪次可行。所以最小的冪次依次是 1、4、2、4。這個最小的冪次稱為該單位根的階（order），而本原 $n$ 次單位根正是階為 $n$ 的那些單位根。整道題的關鍵事實是：每個單位根都恰好有一個階。

## 逐步解題

### 階段 1　最初的幾個

本原 4 次單位根是 i 和 $-\mathrm{i}$，所以 $\mathrm{C}_4(x) = (x-\mathrm{i})(x+\mathrm{i}) = x^2+1$。 ■

> **想一想**　哪些單位根的階是 1、2、3、5 和 6？（畫出 6 次單位根，並按階把它們分類。）

階為 1：只有 1，所以 $\mathrm{C}_1(x) = x-1$。階為 2：只有 $-1$，所以 $\mathrm{C}_2(x) = x+1$。

階為 3：除 1 以外的三次單位根，即 $\frac{x^3-1}{x-1}$ 的根。所以 $\mathrm{C}_3(x) = x^2+x+1$。

階為 5：除 1 以外的五次單位根，它們是 $\frac{x^5-1}{x-1}$ 的根，所以 $\mathrm{C}_5(x) = x^4+x^3+x^2+x+1$。

階為 6：在六次單位根 $e^{k\pi\mathrm{i}/3}$，$k = 0,\dots,5$ 之中，$k = 0$、3 的階分別是 1、2，而 $k = 2$、4 的階是 3。餘下的是 $e^{\pm\pi\mathrm{i}/3}$，所以

$$\mathrm{C}_6(x) = (x-e^{\mathrm{i}\pi/3})(x-e^{-\mathrm{i}\pi/3}) = x^2 - 2x\cos\tfrac{\pi}{3} + 1 = x^2 - x + 1. \qquad ■$$

### 階段 2　哪個 $n$ 給出 $x^4+1$？

$x^4+1=0$ 的根滿足 $x^4 = -1$，所以 $x^8 = 1$ 但 $x^4 \neq 1$。它們的階整除 8 但不整除 4，所以階是 8。反過來，階為 8 的單位根滿足 $x^8 = 1$，$x^4 \neq 1$，所以 $x^4 = -1$。本原 8 次單位根有四個，$x^4+1$ 的根也有四個，所以 $n = 8$。 ■

### 階段 3　質數

若 $p$ 是質數，則 $p$ 次單位根的階整除 $p$，所以階是 1 或 $p$。因此除 1 以外的每個 $p$ 次單位根都是本原的，而

$$\mathrm{C}_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1. \qquad ■$$

### 階段 4　沒有分圓多項式是另外兩個分圓多項式之積

> **停一停，試一試**　假設 $\mathrm{C}_q = \mathrm{C}_r\mathrm{C}_s$。取 $\mathrm{C}_r$ 的一個根。它的階是多少？這條恆等式對它的階有何說法？由此必然得出甚麼？

$\mathrm{C}_r$ 的每個根（至少有一個，因為 $e^{2\pi\mathrm{i}/r}$ 是本原的）都是 $\mathrm{C}_r\mathrm{C}_s = \mathrm{C}_q$ 的根，所以它的階是 $q$。但它的階同時也是 $r$，而一個單位根只有一個階，所以 $r = q$。於是 $\mathrm{C}_q = \mathrm{C}_q\,\mathrm{C}_s$，又因為 $\mathrm{C}_q$ 不是零多項式，所以 $\mathrm{C}_s = 1$。這是不可能的，因為 $\mathrm{C}_s$ 至少有一個根 $e^{2\pi\mathrm{i}/s}$。所以這樣的 $q$、$r$、$s$ 並不存在。 ■

## 回顧

- **按階分類。**每個單位根都有唯一的階，按階分組便把 $z^n - 1$ 的根分成互不相交的類。
- **用根來定義多項式。**每個 $C_n$ 都是藉着確切指明哪些數是它的根而確定下來的。
- **唯一性帶來不可能性。**第 (iv) 部分只需要一個想法：一個根不可能有兩個不同的階。

## 背後的數學

### 分解 $x^n - 1$

每個 $n$ 次單位根都有某個整除 $n$ 的階 $d$；而當 $d \mid n$ 時，每個階為 $d$ 的 $d$ 次單位根都是 $n$ 次單位根。所以 $x^n - 1$ 的根按階分成若干類，由此得到

$$x^n - 1 = \prod_{d \mid n} C_d(x).$$

例如 $x^6 - 1 = C_1C_2C_3C_6 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$。圖 6.1.1 展示了按這種方式分類的十二個 12 次單位根。本原 $n$ 次單位根的個數，亦即 $C_n$ 的次數，等於 1 至 $n$ 之間與 $n$ 沒有公因數的 $k$ 的個數，也就是歐拉函數（Euler's totient function）$\varphi(n)$。比較兩邊的次數，便得到恆等式 $\sum_{d \mid n} \varphi(d) = n$。

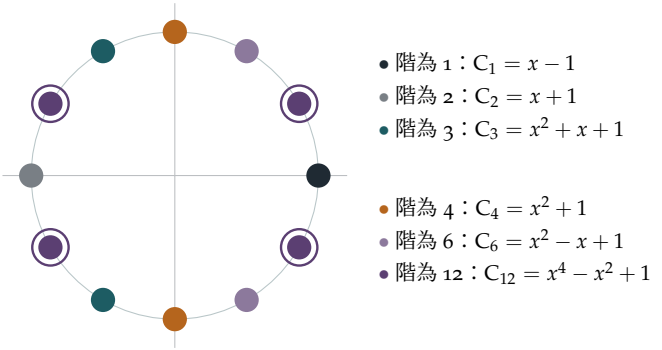



**圖 6.1.1** 十二個 12 次單位根，按階着色。四個本原 12 次單位根（以圓圈標示）是 $C_{12}$ 的根。各類合起來給出 $x^{12} - 1 = C_1C_2C_3C_4C_6C_{12}$，次數為 $1+1+2+2+2+4 = 12$。

### 整數係數，以及一個意外

單看定義並不明顯，但每個分圓多項式的係數都是整數。（利用 $x^n - 1$ 的因式分解和歸納法（induction）：$C_n$ 等於 $x^n - 1$ 除以若干個較早的分圓多項式之積，而以首一（monic）整係數多項式對整係數多項式作長除法，所得係數仍是整數。）在很長一段時間裏，所有已知例子的係數都只有 $0$、$1$ 和 $-1$。第一個例外是 $C_{105}$，它含有 $-2x^7$ 這一項，由 Migotti 於 1883 年發現；$105 = 3 \times 5 \times 7$ 是具有三個相異奇質因數的最小的數。事實上，分圓多項式的係數可以要多大有多大。

### 不可約性

第 (iv) 部分證明了沒有分圓多項式是另外兩個分圓多項式之積。其實更強的結論也成立：$C_n$ 根本不能分解成次數較低的有理係數多項式之積。高斯對 $n$ 為質數的情況證明了這一點（它可由艾森斯坦判別法（Eisenstein's criterion）推出，你會在大學的第一門代數課中遇到），而克羅內克（Kronecker）和戴德金（Dedekind）則證明了一般 $n$ 的情況。正是這種不可約性（irreducibility），使分圓多項式成為與單位根有關的多項式之中的「質數」，它也是單位根的伽羅瓦理論（Galois theory）的起點。

## 思維技巧

**先分類，後構造**

用一個定義明確的不變量（*invariant*），把問題中的對象分成若干類，然後逐類建立結構。

這裏的不變量是單位根的階。由於每個根恰好有一個階，各類互不重疊，於是 $x^n - 1$ 可分解成遍及各類的乘積。同樣的模式（由唯一的不變量得出不相交的分解）也是質因數分解和有限阿貝爾羣（finite abelian groups）分類的基礎。

## 延伸練習

1. **檢查因式分解。**驗證 $(x-1)(x+1)(x^2+x+1)(x^2-x+1) = x^6 - 1$，並驗證 $x^{12} - 1$ 的因式分解如圖 6.1.1 所示。

2. **質數的兩倍。**證明若 $p$ 是奇質數，則 $C_{2p}(x) = C_p(-x)$。就 $p = 3$ 驗證這個結果。

3. **歐拉函數。**證明對於質數 $p$，有 $\varphi(p^k) = p^k - p^{k-1}$，並且 $C_{p^k}(x) = C_p\left(x^{p^{k-1}}\right)$。利用這個結果求 $C_9$。

**4 較長的一題。** 較難 利用 $x^{15}-1 = C_1C_3C_5C_{15}$，證明 $C_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$。

## 延伸閱讀

- **Ian Stewart, *Galois Theory***（CRC Press）。大學本科的標準入門書；分圓多項式和正多邊形在書中很早便出現。
- **Harold Davenport, *The Higher Arithmetic***（Cambridge University Press）。內容包括單位根及其算術性質。
- **Marcus du Sautoy, *Finding Moonshine***（Fourth Estate）。一本講述對稱與羣論的科普讀物，當中包括伽羅瓦的故事。

# 6.2 高斯的正十七邊形

**題目**

**STEP II 1991，第 4 題**

繼續閱讀之前，請先看題目（原題為英文）。題目載於 STEP Support Programme 的試題資料庫：

`step.maths.org/questions/91-s2-q4`

## 引子

1796 年 3 月 30 日，哥廷根（Göttingen）一名十八歲的學生在他的數學日記寫下了第一則記錄，這本日記他此後寫了一輩子。他發現了怎樣用尺規作圖（ruler and compasses construction）作出正 17 邊形。古希臘人早已懂得作出邊數為 3、4、5 和 15 的正多邊形（regular polygon），以及邊數為這些數目反覆加倍的正多邊形，但其後兩千年間，再沒有人添上任何一個新的。高斯（Carl Friedrich Gauss）後來說，正是這項發現令他決心成為數學家，而不是語文學家；相傳他還曾要求在自己的墓碑上刻一個正 17 邊形。

這個作圖法的核心，就是本題的後半部分：四個特定餘弦之和等於 $\frac{\sqrt{17}-1}{4}$，這個數只涉及一個平方根。由平方根構成的長度都可以用尺規作出，而高斯再用三個同類的步驟，就能作出 $\cos\frac{2\pi}{17}$ 本身。

## 動筆之前

? **想一想** 為甚麼一道關於正 17 邊形的題目，第一部分卻是關於 $\cos\frac{2\pi}{5}$ 的？

那是熱身，把同一個想法用在較小的多邊形上。對正五邊形（pentagon）而言，和 $\cos\phi + \cos 2\phi$ 滿足一條有理係數的二次方程（quadratic），所以解一條二次方程就能求出它。對正 17 邊形而言，四個餘弦之和 $z$ 原來也滿足一條二次方程。兩種情況的竅門都是把餘弦相乘，再用 $\cos A\cos B = \frac{1}{2}(\cos(A+B)+\cos(A-B))$ 把乘積變回同一批角的餘弦之和。

## 逐步解題

### 階段 1　正五邊形

**想一想**　展開 $y^2=(\cos\phi+\cos 2\phi)^2$，把每個乘積化為和，再利用 $5\phi=2\pi$ 化簡 $3\phi$ 和 $4\phi$ 這類角。

$$y^2=\cos^2\phi+2\cos\phi\cos 2\phi+\cos^2 2\phi=\tfrac12(1+\cos 2\phi)+(\cos 3\phi+\cos\phi)+\tfrac12(1+\cos 4\phi).$$

由於 $5\phi=2\pi$，有 $\cos 3\phi=\cos(2\pi-2\phi)=\cos 2\phi$ 和 $\cos 4\phi=\cos\phi$。所以

$$y^2=1+\tfrac12(\cos\phi+\cos 2\phi)+(\cos\phi+\cos 2\phi)=1+\tfrac32 y,$$

即 $2y^2=3y+2$。 ■方程 $2y^2-3y-2=(2y+1)(y-2)=0$ 的根是 $y=2$ 和 $y=-\tfrac12$。但 $y=2$ 需要兩個餘弦都等於 $1$，而事實並非如此，所以 $y=-\tfrac12$。 ■

### 階段 2　十七次單位根之和為零

$\sum_{k=0}^{16}\cos k\theta$ 是 $\sum_{k=0}^{16}\omega^k$ 的實部（real part），其中 $\omega=e^{\mathrm{i}\theta}$ 是一個 17 次本原單位根（primitive root of unity）。這個等比級數（geometric series）等於 $\frac{\omega^{17}-1}{\omega-1}=0$。 ■

所以 $\sum_{k=1}^{16}\cos k\theta=-1$。由於 $\cos(17-k)\theta=\cos k\theta$，各項可以兩兩配對，於是

$$\sum_{k=1}^{8}\cos k\theta=-\tfrac12.$$

### 階段 3　把餘弦分成兩組

**想一想**　設 $z=\cos\theta+\cos 2\theta+\cos 4\theta+\cos 8\theta$，並設 $z'$ 為其餘四個餘弦之和 $\cos 3\theta+\cos 5\theta+\cos 6\theta+\cos 7\theta$。$z+z'$ 是多少？

由第 2 階段，$z+z'=-\tfrac12$。如果還能求出 $zz'$，那麼 $z$ 和 $z'$ 就是某條二次方程的兩個根。

**停一停，試一試**　計算 $zz'$。把它展開成 16 個乘積 $\cos a\theta\cos b\theta$，把每個乘積化為兩個餘弦之和，然後數一數 $\cos\theta,\cos 2\theta,\dots,\cos 8\theta$ 各出現多少次。（利用 $\cos k\theta=\cos(17-k)\theta$ 和 $\cos(-k\theta)=\cos k\theta$ 化簡各角。）

每個乘積給出 $\cos a\theta\cos b\theta=\tfrac12(\cos(a+b)\theta+\cos(a-b)\theta)$，所以 $zz'$ 是 32 個餘弦之和的 $\tfrac12$ 倍。逐一考慮 $a\in\{1,2,4,8\}$ 和 $b\in\{3,5,6,7\}$ 的 16 對組合：例如 $a=1$、$b=3$ 給出 $\cos 4\theta$ 和 $\cos 2\theta$；$a=8$、$b=7$ 給出 $\cos 15\theta=\cos 2\theta$ 和 $\cos\theta$。對全部十六對都這樣

做，$\cos\theta,\ldots,\cos 8\theta$ 每一個都恰好出現四次。因此

$$zz' = \tfrac{1}{2}\times 4\times\sum_{k=1}^{8}\cos k\theta = 2\times\left(-\tfrac{1}{2}\right) = -1.$$

#### 階段 4 二次方程

所以 $z$ 和 $z'$ 是 $t^2+\frac{1}{2}t-1=0$ 的兩個根，即 $4t^2+2t-4=0$，其根為 $t=\frac{-1\pm\sqrt{17}}{4}$。哪一個是 $z$？按數值計算，$\cos\theta\approx 0.932$、$\cos 2\theta\approx 0.739$、$\cos 4\theta\approx 0.092$ 和 $\cos 8\theta\approx -0.983$，所以 $z\approx 0.78>0$。因此

$$z=\frac{-1+\sqrt{17}}{4}=-\frac{1-\sqrt{17}}{4}. \qquad \blacksquare$$

## 回顧

- **積化和。**餘弦的積化和公式把 $y^2$ 和 $zz'$ 變成同一批餘弦之和，於是代數運算得以自成一體。
- **和與積給出二次方程。**知道 $z+z'$ 和 $zz'$，就等於知道以 $z$ 和 $z'$ 為根的二次方程。
- **分組要分得對。**把八個餘弦分成 $\{1,2,4,8\}$ 和 $\{3,5,6,7\}$，令每個指標在 $zz'$ 中出現的次數相同。隨意分組是行不通的。

## 背後的數學

#### 高斯週期

為甚麼是 $\{1,2,4,8\}$？以 17 為模（modulo），3 的冪 $3^0,3^1,3^2,\ldots$ 會走遍所有非零剩餘（residue）：

$$1,3,9,10,13,5,15,11,16,14,8,7,4,12,2,6.$$

每隔一個取一個，即 $3^0,3^2,3^4,\ldots$，得出 1、9、13、15、16、8、4、2，以 17 為模就是 $\pm1$、$\pm2$、$\pm4$、$\pm8$：正好是 $z$ 中的角。另一半給出 $\pm3,\pm5,\pm6,\pm7$，即 $z'$ 中的角。高斯把 $\omega^k$ 在這類剩餘類上的和稱為週期（periods）。由於 $17-1=16=2^4$，這些剩餘可以對分四次，而在每一階段，週期都滿足一些二次方程，其係數涉及上一階段的週期。四條二次方程，也就是四個平方根，就從有理數一路通往 $\cos\frac{2\pi}{17}$：

$$\cos\tfrac{2\pi}{17}=\tfrac{1}{16}\Big(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}} \\ +2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}\Big).$$

每一步都只涉及平方根，而平方根可以用尺規作出（利用相似三角形或半圓），所以正 17 邊形是可作圖（constructible）的。

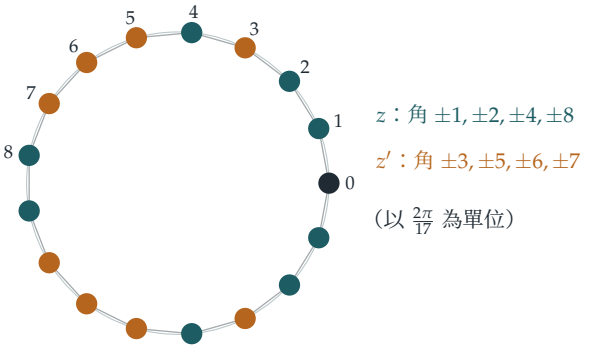



**圖 6.2.1**　正 17 邊形的頂點，按高斯的兩個週期分成兩組。藍綠色頂點位於角 $\pm 1, \pm 2, \pm 4, \pm 8$（以 $\frac{2\pi}{17}$ 為單位），它們的 $x$ 坐標之和是 $2z = \frac{-1+\sqrt{17}}{2}$；琥珀色頂點則給出 $2z' = \frac{-1-\sqrt{17}}{2}$。

### 哪些正多邊形可以作圖？

高斯斷言，而 Pierre Wantzel 在 1837 年證明：正 $n$ 邊形可以用尺規作出，當且僅當 $n$ 是 2 的冪乘以若干個互不相同的費馬質數（Fermat primes）之積，費馬質數即形如 $2^{2^m}+1$ 的質數。已知的費馬質數有 3、5、17、257 和 65537，它們是 Section 1.1 中的費馬數。（費馬（Fermat）猜想所有這類數都是質數，但歐拉（Euler）證明了 $2^{32}+1$ 可被 641 整除，而此後再沒有人找到其他費馬質數。）所以正 257 邊形和正 65537 邊形都可以作圖；十九世紀時，Johann Hermes 花了大約十年時間推算出正 65537 邊形的作圖法，他的手稿現存於哥廷根。正 7 邊形和正 11 邊形不可作圖，因為 7 和 11 不是費馬質數（$7-1=6$ 和 $11-1=10$ 都不是 2 的冪）；正 9 邊形也不可作圖，因為 $9=3^2$ 把費馬質數 3 重複了。Wantzel 的證明用到 Section 6.3 中關於域次數（field degrees）的理論。

## 思維技巧

**計算和與積來求出二次方程**

要求出一個量，可以爲它配上一個自然的夥伴，計算兩者的和與積，再解由此得出的二次方程。

箇中的藝術在於選對夥伴，使和與積都算得出來。這裏的夥伴來自以 17 為模的剩餘的對稱性，而把這個想法重複四次，就得出高斯的作圖法。

## 延伸練習

1 **正七邊形（heptagon）。**試做 STEP II 1995，第 6 題（`step.maths.org/questions/95-s2-q6`）。這道題把高斯將單位根分組的想法用於七次單位根，並求出餘弦之和與正弦之和的準確值。判斷正弦之和的正負號是當中最微妙的一步。

2 **正五邊形。**證明 $\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$，並由此描述一個正五邊形的尺規作圖法。

3 **另一個週期。**用數值驗證 $z' = \cos 3\theta + \cos 5\theta + \cos 6\theta + \cos 7\theta = \frac{-1-\sqrt{17}}{4}$。

4 **生成元（generators）。**證明以 17 為模時，3 的冪給出所有非零剩餘，但 2 的冪卻不然。2 的冪給出哪些剩餘？

## 延伸閱讀

- **Ian Stewart, *Galois Theory***（CRC Press）。當中有一章講述尺規作圖和正 17 邊形。
- **Richard Courant & Herbert Robbins, *What Is Mathematics?***（Oxford University Press）。第 3 章以淺白優美的筆觸介紹作圖問題，包括正 17 邊形。
- **Daniel Kehlmann, *Measuring the World***（Quercus）。一本關於高斯和洪堡（Alexander von Humboldt）的詼諧小說，可作輕鬆讀物。

# 6.3 以 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 為根的多項式

**題目**

**STEP II 2023，第 4 題**

繼續閱讀之前，請先看題目（原題為英文）。題目載於 OCR 提供下載的 2023 年 STEP 試卷（zip 檔案）內的 STEP II 試卷：

`www.ocr.org.uk/Images/707102-2023-past-papers.zip`

## 引子

$\sqrt{2}$ 是 $x^2-2$ 的根，而這是一個整數係數多項式（polynomial）。同樣，$\sqrt{3}$ 是 $x^2-3$ 的根。那麼 $\sqrt{2}+\sqrt{3}$ 是否也是某個整數係數多項式的根？$\sqrt{2}+\sqrt{3}+\sqrt{5}$ 又如何？$\sqrt[3]{2}+\sqrt[3]{3}$ 呢？

凡是整數係數多項式的根，都稱為*代數數*（algebraic number）。這道題透過親手消元（elimination），說明代數數之和仍是代數數。計算所得的次數 4、8、6、9 並非偶然：它們量度每個數有多「複雜」，而這種量度，即*域擴張的次數*（degree of a field extension），正是最終解決古希臘倍立方與三等分角問題的關鍵。

## 動筆之前

**想一想** 要找一個以 $\sqrt{2}$ 為根的多項式，你會把 $x=\sqrt{2}$ 平方，從而消去平方根。若有兩個不同的平方根，怎樣才能逐一消去？

先把其中一個平方根單獨移到一邊再平方，它便會消失；然後把另一個平方根單獨移到一邊，再平方一次。每次平方都可能令次數加倍。整道題的策略就是如此：逐一消去根式（radical）。

## 逐步解題

### 階段 1　兩個平方根

若 $(x-\sqrt{2})^2=3$，則 $x^2-2\sqrt{2}\,x+2=3$，所以 $x^2-1=2\sqrt{2}\,x$。平方便可消去餘下的平方根：$(x^2-1)^2=8x^2$，即

$$x^4-10x^2+1=0. \qquad \blacksquare$$

而 $x=\sqrt{2}+\sqrt{3}$ 滿足 $(x-\sqrt{2})^2=(\sqrt{3})^2=3$，所以 $\mathrm{f}(\sqrt{2}+\sqrt{3})=0$。 $\blacksquare$

### 階段 2　三個平方根

**想一想**　設 $x=\sqrt{2}+\sqrt{3}+\sqrt{5}$，則 $x-\sqrt{5}=\sqrt{2}+\sqrt{3}$ 是 f 的根。把 $\mathrm{f}(x-\sqrt{5})=0$ 寫成 $P(x)+\sqrt{5}\,Q(x)=0$ 的形式。之後怎樣消去 $\sqrt{5}$？

利用 $(x-\sqrt{5})^2=x^2+5-2\sqrt{5}x$ 和 $(x-\sqrt{5})^4=\big(x^2+5-2\sqrt{5}x\big)^2=x^4+30x^2+25-4\sqrt{5}\,x(x^2+5)$ 展開：

$$\mathrm{f}(x-\sqrt{5})=\big(x^4+30x^2+25\big)-4\sqrt{5}\,x(x^2+5)-10\big(x^2+5\big)+20\sqrt{5}\,x+1.$$

合併同類項，得 $P(x)=x^4+20x^2-24$ 和 $Q(x)=-4x^3-20x+20x=-4x^3$。所以 $x^4+20x^2-24=4\sqrt{5}\,x^3$。平方得

$$\big(x^4+20x^2-24\big)^2=80x^6,$$

展開後得

$$\mathrm{g}(x)=x^8-40x^6+352x^4-960x^2+576. \qquad \blacksquare$$

（驗算：$(x^4+20x^2-24)^2=x^8+40x^6+352x^4-960x^2+576$，其中用到 $400-48=352$；再減去 $80x^6$ 便得 g。）

### 階段 3　一個三次方程與一個平方根

**想一想**　若 $x=a+\sqrt{2}$，則 $x-\sqrt{2}$ 是 $t^3-3t+1$ 的根。代入後，把含有 $\sqrt{2}$ 的項與不含它的項分開，然後平方。

$(x-\sqrt{2})^3=x^3-3\sqrt{2}\,x^2+6x-2\sqrt{2}$，所以

$$(x-\sqrt{2})^3-3(x-\sqrt{2})+1=\big(x^3+3x+1\big)-\sqrt{2}\big(3x^2-1\big)=0.$$

因此 $(x^3+3x+1)^2=2(3x^2-1)^2$。展開得 $x^6+6x^4+2x^3+9x^2+6x+1=18x^4-12x^2+2$，所以

$$\mathrm{h}(x)=x^6-12x^4+2x^3+21x^2+6x-1. \qquad \blacksquare$$

同樣的論證對 $b+\sqrt{2}$ 和 $c+\sqrt{2}$ 也成立，因為我們只用到 $a$ 是 $t^3-3t+1$ 的根這一事實。（h 的另外三個根是 $a-\sqrt{2}$、$b-\sqrt{2}$ 和 $c-\sqrt{2}$，它們是在平方時引入的。）

### 階段 4　兩個立方根

**停一停，試一試** 設 $x = \sqrt[3]{2}+\sqrt[3]{3}$。把兩邊立方。你能否把結果用 $x$ 和單獨一個立方根表示？

利用 $(u+v)^3 = u^3+v^3+3uv(u+v)$，取 $u=\sqrt[3]{2}$，$v=\sqrt[3]{3}$：

$$x^3 = 2+3+3\sqrt[3]{6}\,x, \qquad \text{所以} \qquad x^3-5 = 3\sqrt[3]{6}\,x.$$

再立方一次，便消去最後一個立方根：$(x^3-5)^3 = 27\cdot 6\,x^3 = 162x^3$。展開 $(x^3-5)^3 = x^9-15x^6+75x^3-125$，得

$$\mathrm{k}(x) = x^9-15x^6-87x^3-125. \qquad \blacksquare$$

## 回顧

- **逐一消去根式。**把一個根式單獨移到一邊，取適當的次方，然後重複這個步驟。
- **把有理部分與無理部分分開。**把式子寫成 $P+\sqrt{5}\,Q$，再利用 $P^2 = 5Q^2$，是關鍵的一步。
- **平方會帶來額外的根。**每次平方都會引入「共軛」（conjugate）根，例如除了 $a+\sqrt{2}$ 之外還有 $a-\sqrt{2}$。最後得到的多項式以它們全部為根。

## 背後的數學

### 域及其次數

所有形如 $p+q\sqrt{2}$（其中 $p$、$q$ 為有理數）的數所組成的集合 $\mathbb{Q}(\sqrt{2})$，對加、減、乘、除（除數不為零）都封閉：它是一個域（field）。它是 $\mathbb{Q}$ 上的二維「向量空間」（vector space），以 $1, \sqrt{2}$ 為基底（basis），所以我們說它在 $\mathbb{Q}$ 上的*次數*（degree）是 2。添加 $\sqrt{3}$ 便得到 $\mathbb{Q}(\sqrt{2},\sqrt{3})$，其基底為 $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$，次數為 4；再添加 $\sqrt{5}$，次數便是 8（圖 6.3.1）。*塔定律*（tower law）指出，沿着一座域塔往上，次數會相乘。由一個數生成的域，其次數等於該數的*最小多項式*（minimal polynomial）的次數，即該數所滿足的有理係數多項式之中次數最低的一個。可以證明，本題的多項式 f 和 g 都是最小多項式，所以 $\sqrt{2}+\sqrt{3}$ 的次數是 4，而 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 的次數是 8：事實上，單憑 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 這一個數，就足以生成整個 8 次域。

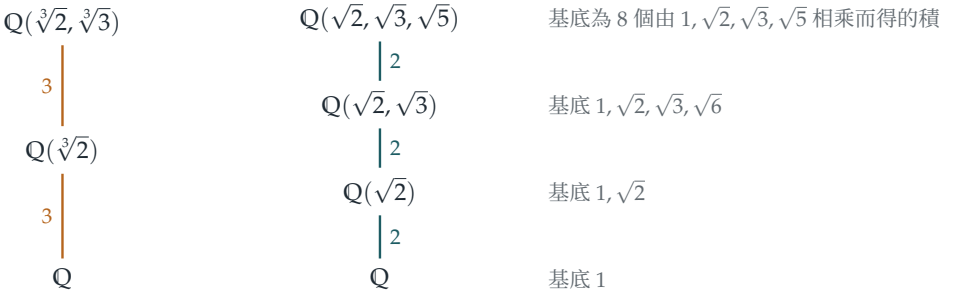



**圖 6.3.1**　域塔。右：每添加一個平方根，次數便加倍，得出 $2\times 2\times 2=8$，即 g 的次數。左：每添加一個立方根，次數便變為三倍，得出 $3\times 3=9$，即 k 的次數。沿着域塔往上，次數會相乘；這條*塔定律*正是證明某些尺規作圖不可能完成的關鍵。

### 倍立方

尺規作圖（ruler-and-compass construction）所能作出的長度，只限於由有理數出發、反覆解一次和二次方程而得到的數。每一步都給出一個次數為 1 或 2 的域擴張，所以根據塔定律，每個可作圖（constructible）的長度都位於一個次數為 2 的冪的域之內，而它本身的次數也是 2 的冪。但 $\sqrt[3]{2}$ 的最小多項式是 $x^3-2$，次數為 3。由於 3 不是 2 的冪，$\sqrt[3]{2}$ 不可作圖，因此約於公元前 430 年提出的提洛島（Delos）問題，即用尺規把立方體的體積加倍，是不可能做到的。旺策爾（Pierre Wantzel）在 1837 年證明了這一點，同時證明了一般的角不可能三等分，並完成了可作圖正多邊形的分類（Section 6.2）。兩千年來的種種嘗試，就此被一個關於次數的論證畫上句號。

### 代數數構成一個域

本題的方法透過例子說明，代數數之和仍是代數數。一般情況則要用線性代數（linear algebra）來證明：若 $\alpha$ 和 $\beta$ 的次數分別為 $m$ 和 $n$，則所有 $\alpha^i\beta^j$（其中 $i<m$，$j<n$）這些數所張成的空間，維數至多為 $mn$，於是 $mn+1$ 個冪 $1,\alpha+\beta,(\alpha+\beta)^2,\ldots$ 必定線性相關（linearly dependent），由此得出一個次數至多為 $mn$ 的多項式。我們得到的次數 $4=2\times 2$、$6=3\times 2$ 和 $9=3\times 3$ 與這個規律完全吻合。*不是*代數數的數稱為*超越數*（transcendental number）；$e$ 和 $\pi$ 都是例子（分別由埃爾米特（Hermite）於 1873 年及林德曼（Lindemann）於 1882 年證明），而林德曼關於 $\pi$ 是超越數的定理，也證明了化圓為方同樣不可能。

## 思維技巧

**先消去，再量度**

要找出一個含根式的式子所滿足的多項式，可把根式逐個單獨移到一邊，再取適當的次方，逐一消去。

然後問一問：次數說明了甚麼？最小多項式的次數是該數的一個不變量（invariant），而比較次數是證明某事不可能的最有力方法之一。

## 延伸練習

1 **本原元（primitive element）。**設 $y=\sqrt{2}+\sqrt{3}$。證明 $y^3=11\sqrt{2}+9\sqrt{3}$，並由此推出 $\sqrt{2}=\frac{1}{2}(y^3-9y)$。因此每個形如 $p+q\sqrt{2}+r\sqrt{3}+s\sqrt{6}$ 的數都可以寫成 $y$ 的多項式。

2 **混合根式。**求一個次數為 6 的整數係數多項式，使它以 $\sqrt{2}+\sqrt[3]{3}$ 為根。

3 **不可約性（irreducibility）。**證明 $x^4-10x^2+1$ 沒有有理根，而且不能寫成兩個整數係數二次式的積。（提示：試用 $(x^2+ax+b)(x^2-ax+c)$。）由此推出 $\sqrt{2}+\sqrt{3}$ 的次數是 4。

4 **三等分角。**證明 $\cos 3\theta=4\cos^3\theta-3\cos\theta$，並由此推出 $\cos 20^\circ$ 是 $8x^3-6x-1=0$ 的根。假設這個三次方程沒有有理根（請自行驗證），解釋為何不能用尺規把 $60^\circ$ 的角三等分。

## 延伸閱讀

- **Ian Stewart, *Galois Theory***（CRC Press）。講述域擴張、塔定律及古典作圖問題，為大學本科生而寫。
- **Richard Courant & Herbert Robbins, *What Is Mathematics?***（Oxford University Press）。第 3 章證明古希臘幾大問題不可能解決，毋須任何預備知識。
- **Robin Hartshorne, *Geometry: Euclid and Beyond***（Springer）。以近世代數處理尺規作圖。

# 6.4 解四次方程

**題目**

**STEP III 2017，第 3 題**

繼續閱讀之前，請先看題目（原題為英文）。題目載於 STEP Support Programme 的試題資料庫：

`step.maths.org/questions/17-s3-q3`

## 引子

每個學生都學過二次方程（quadratic equation）的求根公式。三次方程（cubic）和四次方程（quartic）其實也有公式；這些公式在十六世紀的意大利被發現，其間充滿祕密比試，以及為爭奪發現權而起的激烈爭執。卡爾達諾（Gerolamo Cardano）在 1545 年出版的《大術》（*Ars Magna*）中把兩者一併發表：三次方程的解法來自塔爾塔利亞（Niccolò Tartaglia），而塔爾塔利亞曾要他發誓保密；四次方程的解法則來自他自己的學生費拉里（Lodovico Ferrari）。此後近三百年，數學家一直苦苦尋找五次方程（quintic）的公式，卻始終徒勞無功。

這道題目展示的，正是解開四次方程的那個竅門，而這個竅門背後大有深意。從四個根出發，按三種可能的方式把根兩兩配對，得出三個新的量。這三個量滿足一個三次方程，而三次方程是你解得到的；有了它們，原來的四個根便隨之而來。爲甚麼這個方法行得通？為甚麼四個根可以化約為三個量，五個根卻不能如法炮製？正是這個問題，引領伽羅瓦（Galois）創立了羣論（group theory）。

## 動筆之前

**想一想** 把四件物件 $\alpha, \beta, \gamma, \delta$ 分成兩對，共有多少種分法？

三種：$\{\alpha\beta, \gamma\delta\}$、$\{\alpha\gamma, \beta\delta\}$ 和 $\{\alpha\delta, \beta\gamma\}$（圖 6.4.1）。題目中的三個量 $\alpha\beta + \gamma\delta$ 等等，正好對應這三種配對。把四個根任意重新排列，只會令這三種配對彼此對調，所以這三個量的任何對稱式（symmetric expression），都是四個根的對稱式，因而可以用 $p$、$q$、$r$、$s$ 表示。這就是為甚麼它們滿足一個係數只涉及 $p$、$q$、$r$、$s$ 的三次方程。

## 逐步解題

### 階段 1　欠缺的係數

**想一想**　在三次方程 $y^3 + Ay^2 + By + C = 0$ 中，根之和用 $A$ 表示是甚麼？而 $(\alpha\beta + \gamma\delta) + (\alpha\gamma + \beta\delta) + (\alpha\delta + \beta\gamma)$ 用四次方程的係數表示又是甚麼？

三次方程的根之和是 $-A$。那三個量之和，就是 $\alpha, \beta, \gamma, \delta$ 中兩兩相乘所得全部六個積之和；對四次多項式 $x^4 + px^3 + qx^2 + rx + s$ 而言，這個和是 $q$。所以 $A = -q$。

### 階段 2　具體的三次方程

代入 $p = 0$、$q = 3$、$r = -6$、$s = 10$，三次方程是

$$y^3 - 3y^2 + (0 - 40)y + (120 - 0 - 36) = y^3 - 3y^2 - 40y + 84 = 0.$$

**想一想**　試試 84 的細小因數。

$y = 2$ 給出 $8 - 12 - 80 + 84 = 0$。作除法，得 $y^3 - 3y^2 - 40y + 84 = (y - 2)(y^2 - y - 42) = (y - 2)(y - 7)(y + 6)$。最大的根是 7，所以 $\alpha\beta + \gamma\delta = 7$。 ■

### 階段 3　根的配對

$(\alpha + \beta)(\gamma + \delta) = \alpha\gamma + \alpha\delta + \beta\gamma + \beta\delta$，這是全部六個兩兩之積的和減去 $\alpha\beta + \gamma\delta$，即 $q - 7 = 3 - 7 = -4$。

此外 $\alpha\beta \cdot \gamma\delta = \alpha\beta\gamma\delta = s = 10$。所以 $\alpha\beta$ 和 $\gamma\delta$ 之和為 7，積為 10：它們是 $t^2 - 7t + 10 = (t - 2)(t - 5)$ 的根。由於 $\alpha\beta > \gamma\delta$，得 $\alpha\beta = 5$ 及 $\gamma\delta = 2$。 ■

### 階段 4　解四次方程

**停一停，試一試**　求 $\alpha + \beta$ 和 $\gamma + \delta$。你已知道它們的和（由 $p$ 得出）和它們的積（由第 3 步得出）；要判斷哪個是哪個，就用 $r$。

$\alpha + \beta + \gamma + \delta = -p = 0$ 而 $(\alpha + \beta)(\gamma + \delta) = -4$，所以 $\{\alpha + \beta, \gamma + \delta\} = \{2, -2\}$。係數 $r$ 給出四個三根之積的和：$\alpha\beta\gamma + \alpha\beta\delta + \alpha\gamma\delta + \beta\gamma\delta = -r = 6$。這可以寫成 $\alpha\beta(\gamma + \delta) + \gamma\delta(\alpha + \beta) = 5(\gamma + \delta) + 2(\alpha + \beta)$。若 $\alpha + \beta = 2$，此式等於 $-10 + 4 = -6$；若 $\alpha + \beta = -2$，則等於 $10 - 4 = 6$。所以 $\alpha + \beta = -2$ 及 $\gamma + \delta = 2$。

於是 $\alpha$、$\beta$ 是 $t^2 + 2t + 5 = 0$ 的根，即 $-1 \pm 2\mathrm{i}$；而 $\gamma$、$\delta$ 是 $t^2 - 2t + 2 = 0$ 的根，即

$1 \pm \mathrm{i}$。四個根是

$$x = -1 \pm 2\mathrm{i}, \qquad x = 1 \pm \mathrm{i}. \qquad \blacksquare$$

驗算：$(x^2 + 2x + 5)(x^2 - 2x + 2) = x^4 + 3x^2 - 6x + 10$。

## 回顧

- **對稱函數（symmetric functions）。**每一步都用上了根與係數的關係：根之和與根之積。
- **降低次數。**一個四次方程的問題變成了一個三次方程（即*預解三次方程*（resolvent cubic)），然後再變成兩個二次方程。
- **用盡每一項資料。**$p$ 和 $q$ 給出了各個和與積；$s$ 把 $\alpha\beta$ 和 $\gamma\delta$ 分開；$r$ 則決定了哪一對根配哪一個和。

## 背後的數學

### 這個竅門為何行得通：根的置換

1770 年，拉格朗日（Joseph-Louis Lagrange）追問三次和四次方程的解法為何行得通，並在根的*置換*（permutation）中找到了答案。四個根共有 24 種重新排列的方式。在所有這些排列之下，三個量 $y_1 = \alpha\beta + \gamma\delta$、$y_2 = \alpha\gamma + \beta\delta$、$y_3 = \alpha\delta + \beta\gamma$ 只不過是彼此對調：四個根的每一種重新排列，都引致三種配對的一種重新排列（圖 6.4.1）。所以它們滿足一個 3 次多項式，其係數是各根的對稱式。用現代的語言來說，從對稱羣（symmetric group）$S_4$（全部 24 個置換）到 $S_3$（三種配對的 6 個置換）有一個滿射的羣同態（group homomorphism），這就是四次方程可以化約為三次方程的原因。

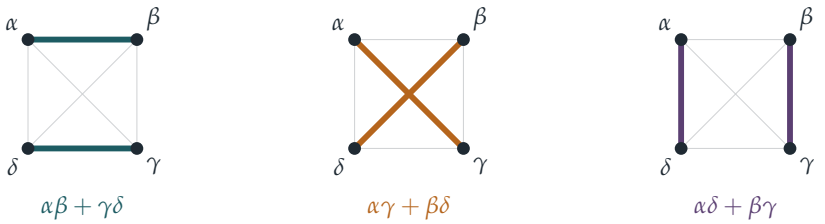



**圖 6.4.1**　把四個根分成兩對的三種方式，以及預解三次方程中與之對應的根。$\alpha, \beta, \gamma, \delta$ 的任何重新排列，都只會令這三幅圖彼此置換，這就是為甚麼那三個量滿足一個三次方程，而其係數可以用四次方程的係數表示。

### 五次方程

對於五個根，拉格朗日嘗試尋找一個類似的量，使它在根的置換之下只取寥寥幾個值，卻找不到有用的。1799 年魯菲尼（Paolo Ruffini）提出證明，1824 年阿貝爾（Niels Henrik Abel）把證明補全，兩人證明了：只用四則運算和根式（radicals），並不存在五次方程的一般求根公式。數年之後，伽羅瓦（Évariste Galois）確切地說明了哪些多項式可以用根式求解：就是那些根的對稱羣能以某種特定方式分解成較簡單部分的多項式。對稱羣 $S_4$ 可以這樣分解（經由 $S_3$ 和更小的羣），但 $S_5$ 不可以，因為它包含一個大小為 60 的「單」（simple）部分，無法再進一步分解。1832 年，伽羅瓦在決鬥中喪生，年僅二十歲；決鬥前一晚，他才匆匆把自己的理論寫下來。這套理論如今是數學學位課程中的瑰寶之一，通常在三年級學到。

### 解三次方程

三次方程本身也可以用類似的竅門求解：把一個缺二次項的三次式（depressed cubic）$x^3 - 3px + q$ 寫成兩個完全立方的組合，從而化約為一個二次方程。這就是練習中那道 2011 年題目所用的方法，它與卡爾達諾公式（Cardano's formula）等價。當三次方程有三個實根時，這條公式在運算途中仍然需要用到複數（complex numbers），正是這個現象迫使數學家認真看待複數（見第 5 章的引言）。

## 思維技巧

> **對稱性化繁為簡**
>
> 如果由根構造出來的一些量，在根被置換時只是彼此置換，那麼它們滿足一個次數較低的多項式，而其係數是你可以計算出來的。
>
> 這是伽羅瓦理論（Galois theory）的種子：透過理解方程各根的對稱性來理解方程本身。

## 延伸練習

1. **驗證三次方程。**驗證 $y_1y_2 + y_2y_3 + y_3y_1 = pr - 4s$，其中 $y_1 = \alpha\beta + \gamma\delta$，餘類推。（展開並利用 $\sum\alpha = -p$、$\sum\alpha\beta\gamma = -r$、$\alpha\beta\gamma\delta = s$。）

2. **把三次式寫成立方之和。**試做 STEP III 2011，第 3 題（`step.maths.org/questions/11-s3-q3`）。這道題把三次式寫成兩個立方的組合來求解，與本節的路線截然不同。請用數值方法核對它的答案。

3 **另一個四次方程。**用本節的方法解 $x^4 - 4x^3 + 7x^2 - 6x + 2 = 0$。（預解三次方程有一個根是細小的整數。）

4 **數算置換。**在 $\alpha, \beta, \gamma, \delta$ 的 24 個置換中，找出所有把配對 $\{\alpha\beta, \gamma\delta\}$ 變回自身的置換。證明這樣的置換共有 8 個。（它們構成 $S_4$ 的一個子羣（subgroup）。）

## 延伸閱讀

- **Mario Livio, *The Equation That Couldn't Be Solved***（Simon & Schuster）。五次方程的故事與羣論的誕生，適合一般讀者。
- **Ian Stewart, *Why Beauty Is Truth: A History of Symmetry***（Basic Books）。從巴比倫人的方程講到伽羅瓦，再到其後的發展。
- **Ian Stewart, *Galois Theory***（CRC Press）。大學本科教科書，其歷史導論所涵蓋的正是本節的內容。

# 6.5 從公理出發的微分法

**題目**

**STEP II 1992，第 4 題**

繼續閱讀之前，請先看題目（原題為英文）。題目載於 STEP Support Programme 的試題資料庫：

`step.maths.org/questions/92-s2-q4`

## 引子

甚麼是微分法（differentiation）？在中學，它是用極限（limit）$\lim_{h\to 0}\frac{f(x+h)-f(x)}{h}$ 來定義的，然後你再學各種法則：和的導數（derivative）等於導數的和、積法則（product rule），諸如此類。這道題把整件事倒轉過來。請把極限完全拋開。假設你對某個運算所知的，就只有它符合和法則、積法則和常數的法則，並且把 $x$ 變成 1。題目要證明的是：這樣的運算必定就是微分，至少對多項式（polynomial）而言是如此。

這是代數學家看微積分的角度：一個運算的特徵在於它所遵從的法則，而不在於某條公式。遵從積法則的運算稱為導子（derivation），它們在代數、幾何和物理中隨處可見。出人意料的是，訓練現代機器學習系統的軟件，內裏用的也是同一個想法。

## 動筆之前

**想一想** 法則 (i) 就是積法則。積法則怎可能告訴你關於常數的任何事情？（試把常數看成一個乘積。）

數 1 等於 $1\times 1$。把積法則應用於 $1\times 1$，便得出 $\Diamond 1$ 與它自身之間的一個關係，從而迫使它等於零。一般而言，處理這類公理（axiom）的竅門，是把它們應用於精心挑選的簡單輸入。

## 逐步解題

### 階段 1　常數

**想一想**　取 $\mathrm{f} = \mathrm{g} = 1$，應用法則 (i)。然後用法則 (iv) 處理其他任何常數。

$\Diamond 1 = \Diamond(1 \cdot 1) = 1 \cdot \Diamond 1 + 1 \cdot \Diamond 1 = 2\Diamond 1$，所以 $\Diamond 1 = 0$。對任意常數 $\lambda$，由法則 (iv) 得 $\Diamond \lambda = \Diamond(\lambda \cdot 1) = \lambda \Diamond 1 = 0$。 ■

### 階段 2　冪

利用法則 (iii)，$\Diamond x^2 = \Diamond(x \cdot x) = x\Diamond x + x\Diamond x = 2x$。於是

$$\Diamond x^3 = \Diamond(x^2 \cdot x) = x\Diamond x^2 + x^2 \Diamond x = x \cdot 2x + x^2 = 3x^2.$$

**停一停，試一試**　用歸納法（induction）證明：對每個正整數 $n$，均有 $\Diamond x^n = nx^{n-1}$。

$n = 1$ 的情況就是法則 (iii)。若 $\Diamond x^n = nx^{n-1}$，則

$$\Diamond x^{n+1} = \Diamond(x^n \cdot x) = x\Diamond x^n + x^n \Diamond x = x \cdot nx^{n-1} + x^n = (n+1)x^n. \qquad \blacksquare$$

### 階段 3　所有多項式

一般的多項式是 $\mathrm{h}(x) = a_0 + a_1 x + \cdots + a_m x^m$。由法則 (ii)（重複應用）和法則 (iv)，

$$\begin{aligned} \Diamond \mathrm{h}(x) &= \Diamond a_0 + a_1 \Diamond x + a_2 \Diamond x^2 + \cdots + a_m \Diamond x^m \\ &= a_1 + 2a_2 x + \cdots + m a_m x^{m-1} = \mathrm{h}'(x). \end{aligned} \qquad \blacksquare$$

## 回顧

- **公理決定運算。**四條法則，完全沒有提及極限，就把 $\Diamond$ 在多項式上的作用完全確定下來。
- **生成元（generator）。**每個多項式都是由常數和 $x$ 經加法和乘法構造出來的。只要知道 $\Diamond$ 對這些基本構件的作用，以及它與這些構造運算如何互動，就能確定它在所有多項式上的作用。
- **沿着構造過程作歸納。**證明的步驟緊隨多項式的構造方式：先以重複相乘得出冪，然後再求和。

## 背後的數學

### 導子

在一個代數系統上，若運算 $D$ 具有可加性（additive），並且滿足積法則 $D(fg) = fD(g) + gD(f)$，便稱為導子。這道題說明，在多項式上，一個把常數變成零的導子完全由 $D(x)$ 決定：事實上 $D(h) = h'(x)\,D(x)$，所以唯一的自由度就是多項式 $D(x)$ 的選擇。法則 (iii) 規定了 $D(x) = 1$。導子遍佈數學各個領域：在幾何中，曲面上的向量場（vector field）可以定義為該曲面上的函數的一個導子（它沿着向量場的方向對函數求導）；在代數中，一個結構的導子量度它的「無窮小對稱」（infinitesimal symmetries）；在物理中，量子力學的交換子（commutator）$[A, B] = AB - BA$ 對每個變元而言都是一個導子。

### 沒有極限的微積分

在極限完全沒有意義的場合，代數式的導數依然行得通。在有限域（finite field）上，例如模質數 $p$ 的算術，並沒有極限可言，但多項式的形式導數（formal derivative）仍由同樣的法則定義，而且仍然能夠偵測重根（repeated root）：多項式 $f$ 有重根，當且僅當 $f$ 與 $f'$ 有公因式。舉例說，我們就是這樣證明當 $p \nmid n$ 時 $x^n - 1$ 沒有重根的；要在有限域上定義 Section 6.1 的分圓多項式（cyclotomic polynomial），就需要這個事實。編碼理論和密碼學也用到同樣的想法。

### 自動微分

以下是一個現代應用。創造一個數 $\varepsilon$，使得 $\varepsilon^2 = 0$ 但 $\varepsilon \neq 0$，然後用對偶數（dual number）$a + b\varepsilon$ 來做算術。這時 $(a + b\varepsilon)(c + d\varepsilon) = ac + (ad + bc)\varepsilon$：$\varepsilon$ 的部分恰好遵從積法則。因此對任何多項式，

$$f(x + \varepsilon) = f(x) + f'(x)\,\varepsilon,$$

而在對偶數 $x + \varepsilon$ 處計算 $f$，就能同時求出函數值和導數，結果完全準確，既不用極限，也沒有因微小差值而產生的捨入誤差（圖 6.5.1）。這稱為*前向模式自動微分*（forward-mode automatic differentiation）。它的近親「反向模式」（reverse mode），就是用來訓練擁有數十億個參數的神經網絡（neural network）的算法（*反向傳播*，backpropagation）：這類系統每學習一次，都是在把積法則和鏈式法則（chain rule）當作導子，一步一步地應用。

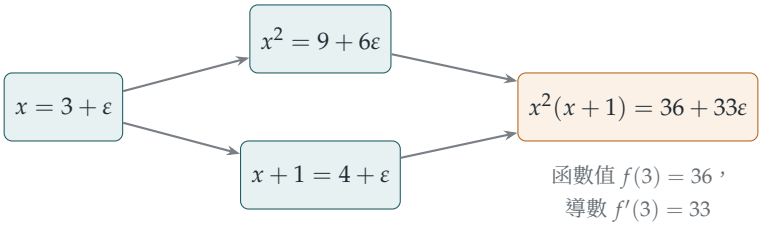



**圖 6.5.1**　用對偶數（$\varepsilon^2 = 0$）對 $f(x) = x^2(x+1)$ 在 $x = 3$ 處作自動微分。每一步都遵從題目中的法則：$(3+\varepsilon)^2 = 9 + 6\varepsilon$，以及 $(9+6\varepsilon)(4+\varepsilon) = 36 + (9+24)\varepsilon$。$\varepsilon$ 的係數就是 $f'(3) = 3\cdot 9 + 2\cdot 3 = 33$，計算結果完全準確。

## 思維技巧

**以性質刻劃對象**

用一個運算所遵從的法則來描述它，然後證明這些法則唯一地確定了它。

這就是公理化方法（axiomatic method），是大學代數的核心。它的威力在於：凡是由公理證明出來的結果，都適用於每一個滿足這些公理的運算，不論那是多項式的微分、曲面上函數的微分，還是某種尚未發明的東西。

## 延伸練習

1. **另一個導子。**假設 $\Diamond$ 滿足法則 (i)、(ii) 和 (iv)，但 $\Diamond x = x$ 而不是 $1$。證明 $\Diamond \mathrm{h}(x) = x\,\mathrm{h}'(x)$。$\Diamond$ 會把 $x^n$ 變成甚麼？

2. **商法則（quotient rule）。**把 $\Diamond$ 推廣到有理函數（rational function）$\mathrm{f}/\mathrm{g}$，並假設法則 (i) 仍然成立。把法則 (i) 應用於 $\mathrm{g}\cdot\frac{\mathrm{f}}{\mathrm{g}} = \mathrm{f}$，從而推導出商法則。

3. **重根。**證明若 $(x-a)^2$ 整除多項式 $\mathrm{f}$，則 $x-a$ 整除 $\mathrm{f}'$。利用這個結果證明 $x^n - 1$ 沒有重根。

4. **對偶數。**設 $f(x) = (x^2+1)^3$，用對偶數計算 $f(2)$ 和 $f'(2)$，並用鏈式法則驗算。

## 延伸閱讀

- **Peter Cameron, *Introduction to Algebra***（Oxford University Press）。大學一年級程度的環、多項式和域，並包括形式導數。

- **Andreas Griewank & Andrea Walther, *Evaluating Derivatives***（SIAM）。自動微分的標準參考書。程度較深。
- **Michael Nielsen, *Neural Networks and Deep Learning***（網上免費閱讀）。第 2 章清楚講解反向傳播。

# 6.6 子羣的併集

**題目**

**STEP II 1988，第 9 題**

繼續閱讀之前，請先看題目（原題為英文）。題目載於 STEP Support Programme 的試題資料庫：

`step.maths.org/questions/88-s2-q9`

## 引子

這是全書最短的題目之一，也是最具大學數學特色的題目之一。它談的是羣（group），即描述對稱的數學語言，問的問題聽起來像個謎題：一個羣能否被它裏面兩個較小的羣完全覆蓋？答案是不能，而證明只有三行。不過三個較小的羣卻可以做到，這倒是出人意表。

羣論（group theory）在 2019 年以前一直屬於 STEP 的課程範圍，如今則是大學一年級的必修內容。這道題只需要用到定義，下文會一一列出；它正好讓你初嘗羣論學者的思考方式：一個簡短而巧妙的論證，除了公理（axiom）之外甚麼都不用。

## 動筆之前

羣是一個集合 $G$，連同一個運算（寫成乘法 $ab$），滿足：

- 運算符合結合律（associative）：$(ab)c = a(bc)$；
- 存在單位元（identity）$e$，對每個 $a$ 都有 $ea = ae = a$；
- 每個 $a$ 都有逆元（inverse）$a^{-1}$，使得 $aa^{-1} = a^{-1}a = e$。

例子：整數（正數、負數和零）在加法下構成羣；非零實數在乘法下構成羣；正方形的旋轉在複合（composition）下構成羣。子羣（subgroup）是 $G$ 的一個子集 $K$，它在同一運算下本身就是一個羣：它包含 $e$，而且若 $a, b \in K$，則 $ab \in K$ 及 $a^{-1} \in K$。

? **想一想** 若 $K$ 是子羣，$a \in K$ 但 $b \notin K$，那麼 $ab$ 可以屬於 $K$ 嗎？

不可以。若 $ab \in K$，則 $b = a^{-1}(ab)$ 是 $K$ 中兩個元素的乘積，因而屬於 $K$。這個小小的觀察就是整個證明。

## 逐步解題

### 階段 1　兩個子羣無法覆蓋

用反證法（proof by contradiction）：假設 $G = G_1 \cup G_2$，但 $G_1$ 和 $G_2$ 都不是整個 $G$。

> **想一想**　由於 $G_1 \neq G$，必有一個元素不在 $G_1$ 之中。它必定在哪裏？$G_2$ 的情況也一樣。現在把這兩個元素相乘。

取 $a \in G$ 使得 $a \notin G_1$；由於每個元素都屬於 $G_1$ 或 $G_2$，故 $a \in G_2$。取 $b \in G$ 使得 $b \notin G_2$；於是 $b \in G_1$。考慮乘積 $ab$。它屬於 $G_1$ 或 $G_2$。

- 若 $ab \in G_1$：由於 $b \in G_1$，$a = (ab)b^{-1} \in G_1$。矛盾。
- 若 $ab \in G_2$：由於 $a \in G_2$，$b = a^{-1}(ab) \in G_2$。矛盾。

無論哪種情況都得出矛盾，所以 $G_1 = G$ 或 $G_2 = G$。 ■

留意我們從未用過 $G$ 是有限羣這個條件。這個結果對所有羣都成立。

### 階段 2　三個子羣卻可以

> **停一停，試一試**　找出一個羣，它是三個子羣的併集（union），而這三個子羣都不是整個羣。（提示：試試一個每個元素都是自己逆元的小羣。）

取克萊因四元羣（Klein four-group）$V = \{e, a, b, c\}$，其運算規則為 $a^2 = b^2 = c^2 = e$ 以及 $ab = ba = c$、$bc = cb = a$、$ca = ac = b$。（具體來說：一個非正方形的長方形的四個對稱，即保持不動、旋轉 $180°$，以及沿兩條對稱軸之一作反射。又或者是由位元 0、1 組成的數對 $(x, y)$，在模 2 加法下構成的羣。）它的三個子羣

$$H_1 = \{e, a\}, \qquad H_2 = \{e, b\}, \qquad H_3 = \{e, c\}$$

各有兩個元素，沒有一個是整個羣，而它們合起來包含了 $V$ 的每一個元素（圖 6.6.1）。 ■

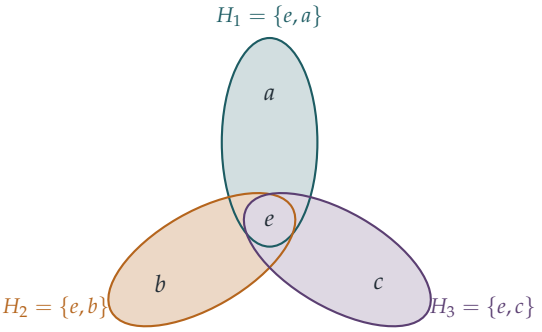



**圖 6.6.1** 克萊因四元羣 $\{e, a, b, c\}$ 是它三個 2 階子羣的併集，這三個子羣只在單位元 $e$ 處重疊。根據題目的第一部分，沒有任何羣可以只是兩個真子羣（proper subgroup）的併集。

## 回顧

- **選出見證元素，再把它們結合。**證明中在每個子羣之外各選一個元素，然後把它們相乘。這種「各取一個再結合」的手法在代數中極為常見。
- **封閉性威力強大。**證明中只用到子羣的一個性質：它們在乘法和取逆元之下封閉（closed）。
- **檢查你真正需要的假設。**題目給了有限這個條件，卻沒有用上。察覺到某個假設並非必要，是理解一個證明的一部分。

## 背後的數學

### 對稱的語言

羣在十九世紀同時從幾個方向出現：伽羅瓦（Galois）對多項式的根的置換（permutation）的研究（Section 6.4）、柯西（Cauchy）關於置換的工作，以及幾何學和晶體學中對對稱的研究。上文那個抽象定義，即凡滿足三條公理的東西都是羣，到該世紀末已經確立。它的威力在於一般性：由公理證明的定理，例如本題中的那一個，同時適用於由數、矩陣、對稱和置換構成的各種羣。今天羣無處不在：在粒子物理學中（標準模型建基於對稱羣）、在化學中（分子的對稱性決定光譜）、在密碼學中（橢圓曲線羣，Section 1.9），以及在扭計骰（Rubik's cube）的解法之中。

### 要用多少個子羣？

這道題引出一個自然的問題：最少要多少個真子羣，它們的併集才是整個羣？根據本題，這個數目永遠不會是 2。1926 年，Gaetano Scorza 證明了一個羣是三個真子羣的併集，當且僅當它以克萊因四元羣為「商羣」（quotient）。1994 年，J. H. E. Cohn 研究了一般的問題，並提出了若干猜想；1997 年，M. J. Tomkinson 證明了沒有任何羣的這個最小數目是七，儘管由 3 到 6 的每個數都會出現。這類問題敘述簡單，卻出奇地微妙，正是羣論的典型。

### 向量空間

類似的論證可以證明，實數上的向量空間（vector space）（例如平面或三維空間）永遠不可能是有限多個真子空間（proper subspace）的併集：平面不是有限多條通過原點的直線的併集。但在有限域（finite field）上卻可以：兩個元素的域上的平面，其實又是克萊因四元羣，它正是其三條直線的併集。

## 思維技巧

**從公理出發論證**

在抽象代數中，你對所處理的對象往往一無所知，只知道它們滿足哪些公理。證明必須只用這些公理。

這迫使論證簡短而乾淨利落，就像本題的論證一樣，也使它們放諸四海皆準。這需要一些時間去適應，而它正是大學一年級代數課中最獨特的體驗之一。

## 延伸練習

1. **驗證這個羣。**寫出克萊因四元羣的乘法表，並驗證各條羣公理。證明它與乘法下的羣 $\{1, i, -1, -i\}$ 並不相同。（提示：哪些元素是自己的逆元？）

2. **循環羣。**若一個羣的每個元素都是某一個元素 $g$ 的冪，則稱它為循環羣（cyclic group）。證明循環羣永遠不是真子羣的併集，不論用多少個。（提示：哪個子羣包含 $g$？）

3. **整數。**直接證明 $(\mathbb{Z}, +)$ 不是子羣 $2\mathbb{Z}$（偶數）和 $3\mathbb{Z}$（3 的倍數）的併集。它是否某兩個真子羣的併集？

**4** **平面上的直線。**較難證明平面 $\mathbb{R}^2$ 不是有限多條通過原點的直線的併集。（提示：每條直線除原點外，最多只包含拋物線 $y = x^2$ 上的一個點。）

## 延伸閱讀

- **M. A. Armstrong, *Groups and Symmetry***（Springer）。一本插圖精美的入門教材，以幾何例子帶動全書。
- **Nathan Carter, *Visual Group Theory***（Mathematical Association of America）。用圖像講解羣，最適合在入讀大學前閱讀。
- **Peter Neumann, Gabrielle Stoy & Edward Thompson, *Groups and Geometry***（Oxford University Press）。牛津大學一年級的經典教材。

# 6.7 四元數羣

**題目**

**STEP III 1993，第 5 題**

繼續閱讀之前，請先看題目（原題為英文）。題目載於 STEP Support Programme 的試題資料庫：

`step.maths.org/questions/93-s3-q5`

## 引子

1843 年 10 月 16 日，哈密頓（William Rowan Hamilton）與妻子沿着都柏林的皇家運河散步時，苦思多年的問題忽然靈光一閃，有了答案。他一直想仿照複數把一對對的數相乘那樣，把三個一組的數相乘，卻屢試屢敗。他突然看出，答案需要的是四個數，而且乘法的次序不可調換：$ij \neq ji$。他把這些法則刻在布魯穆橋（Brougham Bridge）的石頭上：

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{ijk} = -1.$$

這就是四元數（quaternions）。本題用複數對把四元數構造出來，並在其中找到一個只有八個元素、乘法帶點扭曲的小羣。時至今日，每一款電腦遊戲、每一部飛行模擬器、每一套太空船導航系統，都用四元數來描述三維空間中的旋轉。

## 動筆之前

羣的各項定義見 Section 6.6。這裏再補充兩個用語：羣中元素 $g$ 的階（order），是指使 $g^n = e$ 成立的最小正整數 $n$；若兩個羣之間存在一個保持運算的一一對應，則稱這兩個羣同構（isomorphic），也就是說，它們是「換了標籤的同一個羣」。

**想一想** 把數對 $(z_1, z_2)$ 看成代表一個「數」$z_1 + z_2\mathrm{j}$，其中 j 是一個新符號，滿足 $\mathrm{j}^2 = -1$，並且對任意複數 $w$ 有 $\mathrm{j}w = w^*\mathrm{j}$。試用這些法則計算 $(z_1 + z_2\mathrm{j})(w_1 + w_2\mathrm{j})$。得出的是否就是 $\circ$ 的公式？

$(z_1 + z_2\mathrm{j})(w_1 + w_2\mathrm{j}) = z_1w_1 + z_1w_2\mathrm{j} + z_2\mathrm{j}w_1 + z_2\mathrm{j}w_2\mathrm{j} = z_1w_1 + z_1w_2\mathrm{j} + z_2w_1^*\mathrm{j} + z_2w_2^*\mathrm{j}^2$，即 $(z_1w_1 - z_2w_2^*) + (z_1w_2 + z_2w_1^*)\mathrm{j}$。答案是肯定的：運算 $\circ$ 其實就是喬裝了的四元數乘

法。

## 逐步解題

### 階段 1　借助矩陣證明結合律

直接驗證 $(a \circ b) \circ c = a \circ (b \circ c)$，計算十分冗長。其實有更巧妙的方法。

> **想一想**　把 $(z_1, z_2)$ 對應到複矩陣 $M = \begin{pmatrix} z_1 & z_2 \\ -z_2^* & z_1^* \end{pmatrix}$。矩陣乘積 $M(z_1,z_2)\,M(w_1,w_2)$ 的第一行是甚麼？

乘積的第一行是 $(z_1 w_1 - z_2 w_2^*,\ z_1 w_2 + z_2 w_1^*)$，正好是 $(z_1, z_2) \circ (w_1, w_2)$；第二行是 $(-(z_1 w_2 + z_2 w_1^*)^*,\ (z_1 w_1 - z_2 w_2^*)^*)$，所以乘積仍具有同樣的特殊形式。因此 $M(a \circ b) = M(a) M(b)$。矩陣乘法滿足結合律（associativity），而 $M$ 是一對一的（從第一行便可讀出 $z_1$、$z_2$），所以 $\circ$ 滿足結合律。 ∎

### 階段 2　不滿足交換律

$(0,1) \circ (\mathrm{i}, 0) = (0 \cdot \mathrm{i} - 1 \cdot 0,\ 0 \cdot 0 + 1 \cdot \mathrm{i}^*) = (0, -\mathrm{i})$，但 $(\mathrm{i}, 0) \circ (0, 1) = (0, \mathrm{i})$。所以 $\circ$ 不滿足交換律（commutativity）。

四個特殊乘積可由定義直接得出：

$$(z,0) \circ (w,0) = (zw, 0), \qquad (z,0) \circ (0,w) = (0, zw),$$
$$(0,z) \circ (w,0) = (0, zw^*), \qquad (0,z) \circ (0,w) = (-zw^*, 0).$$

### 階段 3　八個元素的羣

用四元數的記法，$A = 1$，$C = \mathrm{i}$，$B = \mathrm{j}$，$D = \mathrm{ij} = \mathrm{k}$，而 $E, G, F, H$ 則分別是它們的相反數。$S_1$ 的每個元素都具有 $(u, 0)$ 或 $(0, u)$ 的形式，其中 $u \in \{1, \mathrm{i}, -1, -\mathrm{i}\}$。

> **想一想**　利用四個特殊乘積，證明 $S_1$ 是封閉的。單位元是甚麼？

由四個特殊乘積可知，兩個形如 $(u, 0)$ 或 $(0, u)$ 的元素相乘，結果仍是這兩種形式之一，其第一個或第二個分量為 $uv$、$uv^*$ 或 $-uv^*$。由於 $\{1, \mathrm{i}, -1, -\mathrm{i}\}$ 在乘法、取共軛及取相反數之下都封閉（closed），乘積仍在 $S_1$ 之內。單位元（identity）是 $A = (1, 0)$：$(1,0) \circ (w_1, w_2) = (w_1, w_2)$，而且 $(w_1, w_2) \circ (1, 0) = (w_1, w_2)$。

> **停一停，試一試**　求出每個元素的階和逆元。

$A$ 的階為 1。$E \circ E = (-1,0) \circ (-1,0) = (1,0)$，所以 $E$ 的階為 2。對於 $C = (\mathrm{i},0)$：$C \circ C = (-1,0) = E$，所以 $C$ 的階為 4，而 $C^{-1} = C^3 = E \circ C = G$。對於 $B = (0,1)$：$B \circ B = (-1 \cdot 1^*, 0) = (-1,0) = E$，所以 $B$ 的階為 4，而 $B^{-1} = F$。同理，$D \circ D = (-\mathrm{i} \cdot \mathrm{i}^*, 0) = (-\mathrm{i} \cdot (-\mathrm{i}), 0) = (-1,0) = E$，所以 $D$ 的階為 4，逆元（inverse）為 $H$。至於 $G$、$F$、$H$，它們分別是 $C$、$B$、$D$ 的逆元，階同樣為 4。總結如下：

| 元素 | $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ |
|---|---|---|---|---|---|---|---|---|
| 逆元 | $A$ | $F$ | $G$ | $H$ | $E$ | $B$ | $C$ | $D$ |
| 階 | 1 | 4 | 4 | 4 | 2 | 4 | 4 | 4 |

既有封閉性和結合律（第 1 步），又有單位元和逆元，$S_1$ 是一個羣。 ■這個羣稱為四元數羣（quaternion group）$Q_8$。

#### 階段 4 一個子羣

$\{A, B, E, F\} = \{1, \mathrm{j}, -1, -\mathrm{j}\}$ 由 $B$ 的各次冪組成：$B^1 = B$，$B^2 = E$，$B^3 = F$，$B^4 = A$。所以它是封閉的，並且包含各元素的逆元：這是一個子羣（subgroup），而且是階為 4 的循環羣（cyclic group）。矩陣 $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ 滿足 $J^2 = -I$，$J^3 = -J$，$J^4 = I$，所以它同樣生成一個階為 4 的循環羣。對應 $B^k \leftrightarrow J^k$ 是一個同構。 ■（事實上，$J$ 正是 $M(0,1)$，即 $B$ 所對應的矩陣。）

## 回顧

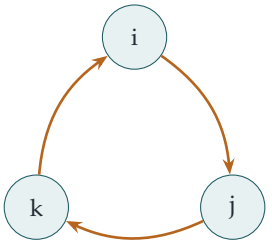
- **用矩陣來表示。**結合律直接驗證起來十分費勁，這裏卻可從矩陣乘法繼承過來。
- **找出公式背後的結構。**古怪的運算。原來就是四元數乘法，看穿了這一點，一切都變得容易。
- **階和逆元刻劃了一個羣。**單看各元素的階，已可見 $Q_8$ 與別不同：一個階為 2 的元素，六個階為 4 的元素。

## 背後的數學

#### 複數之外

實數構成一個一維的數系，在其中可以做加法、乘法和除法；複數則構成一個二維的數系。哈密頓的四元數是四維的，除法依然可行，但乘法不再滿足交換律（圖 6.7.1）。1878 年，弗羅貝尼烏斯（Ferdinand Frobenius）證明了 $\mathbb{R}$、$\mathbb{C}$ 和 $\mathbb{H}$（取自 Hamilton 的首字母）這三者，是實數域上僅有的、乘法滿足結合律的有限維「可除代數」（division

algebras）。如果放棄結合律，但保留一個可乘的大小，即 $|xy| = |x|\,|y|$，一如實數、複數和四元數那樣，那就恰好還多一個：八維的八元數（octonions），由 John Graves 和凱萊（Arthur Cayley）在 1840 年代發現。赫維茲（Adolf Hurwitz）於 1898 年證明，這類數系就只有這四個。（若不設關於大小的條件，還有其他更古怪的非結合可除代數，但 1958 年一條由博特（Raoul Bott）、米爾諾（John Milnor）和 Michel Kervaire 得出的深刻定理指出，任何有限維實可除代數的維數必為 1、2、4 或 8。）




順着箭頭：$\mathrm{ij} = \mathrm{k}$，$\mathrm{jk} = \mathrm{i}$，$\mathrm{ki} = \mathrm{j}$

逆着箭頭：$\mathrm{ji} = -\mathrm{k}$，$\mathrm{kj} = -\mathrm{i}$，$\mathrm{ik} = -\mathrm{j}$

以及 $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1$

**圖 6.7.1**　哈密頓的乘法法則。把 i、j、k 其中兩個順着箭頭方向相乘，得到第三個；逆着箭頭方向相乘，則得到第三個的相反數。$\pm 1, \pm \mathrm{i}, \pm \mathrm{j}, \pm \mathrm{k}$ 這八個元素構成本題的四元數羣 $Q_8$。

### 三維空間中的旋轉

模（modulus）為 1 的四元數描述三維空間的旋轉：繞單位軸 $\mathbf{u}$ 轉過角度 $\theta$ 的旋轉，對應於 $q = \cos\frac{\theta}{2} + \sin\frac{\theta}{2}(u_1\mathrm{i} + u_2\mathrm{j} + u_3\mathrm{k})$，它作用於向量 $\mathbf{v}$（寫成 $v_1\mathrm{i} + v_2\mathrm{j} + v_3\mathrm{k}$）的方式是 $\mathbf{v} \mapsto q\mathbf{v}q^{-1}$。旋轉的複合就是四元數的相乘。這比使用矩陣或角度更有效率，數值上也更穩定，而且避開了「萬向節鎖」（gimbal lock）：那是失去一個自由度的現象，當年阿波羅（Apollo）太空人使用以陀螺儀為本的導航系統時，就不得不設法繞過這個問題。半角 $\frac{\theta}{2}$ 也透露出一點深刻的端倪：旋轉 $360^\circ$ 得到的是 $q = -1$，而不是 1，物理學家在電子的行為（自旋，spin）中正好看到這個事實。

### 四平方和

四元數的模是可乘的，$|pq| = |p||q|$，與複數的模一樣。把它展開寫出，便得到歐拉（Euler）的*四平方恆等式*（four-square identity）：兩個四平方和之積，本身也是一個四平方和。這正是拉格朗日（Lagrange）定理的關鍵一步，該定理指出每個正整數都是四個平方數之和；我們會在 Section 7.8 證明這條定理，它是 Section 1.6 中二平方和結果的四維近親。

## 思維技巧

**把抽象的對象具體地表示出來**

如果一個抽象的運算難以推理，就找一個具體的模型（例如矩陣），讓它在其中變成熟悉的運算。

這樣，結合律之類的性質便不費吹灰之力。這個想法，即把羣表示為矩陣來研究，後來發展成一門龐大而優美的學科：*表示論*（representation theory）。

## 延伸練習

1 **哈密頓的法則。**利用數對，驗證 $C \circ B = D$ 及 $B \circ C = H$，即 $\mathrm{ij} = \mathrm{k}$ 及 $\mathrm{ji} = -\mathrm{k}$。

2 **只有一個階為 2 的元素。**證明 $E = -1$ 是 $Q_8$ 中唯一階為 2 的元素。由此推斷 $Q_8$ 與正方形的對稱羣（它有五個階為 2 的元素）並不同構。

3 **四平方和。**證明 $\det M(z_1, z_2) = |z_1|^2 + |z_2|^2$。利用 $\det(M_1 M_2) = \det M_1 \det M_2$，推斷兩個四平方和之積是一個四平方和。

4 **子羣。**找出 $Q_8$ 的所有子羣。證明除了 $\{A\}$ 之外，每個子羣都包含 $E$，並證明 $Q_8$ 是它三個階為 4 的循環子羣的併集（試與 Section 6.6 比較）。

## 延伸閱讀

- **John Conway & Derek Smith, *On Quaternions and Octonions***（A. K. Peters）。講述四元數和八元數的幾何與算術。程度較深，但引人入勝。
- **John Baez,「The octonions」**，*Bulletin of the American Mathematical Society* 39 (2002)；網上亦可免費閱覽。一篇精彩的綜述；引言部分現在就讀得懂。
- **Andrew Hanson, *Visualizing Quaternions***（Morgan Kaufmann）。講述以四元數處理旋轉，並介紹其在電腦圖像方面的應用。

# 6.8 由奇異矩陣組成的羣

**題目**

**STEP III 1996，第 6 題**

繼續閱讀之前，請先看題目（原題為英文）。題目載於 STEP Support Programme 的試題資料庫：

`step.maths.org/questions/96-s3-q6`

## 引子

每個學生都學過：行列式（determinant）為零的矩陣沒有逆矩陣。那麼，一個由矩陣組成的羣（group），既然其中每個元素都有逆元（inverse），就肯定不可能包含任何奇異矩陣（singular matrix）吧？

其實可以。關鍵在於「逆」這個字。在羣裏，$\mathbf{A}$ 的逆元是指與 $\mathbf{A}$ 結合後得出*該羣的*單位元（identity element）的那個元素，而沒有任何規定說羣的單位元必須是單位矩陣（identity matrix）$\mathbf{I}$。本題構造出一個羣，其中每個矩陣都是奇異的，而單位元本身就是一個行列式為零的矩陣。這一課教我們要按字面去讀定義，也教我們分清抽象結構與我們最初認識它時所見的那個熟悉例子。

## 動筆之前

羣的定義見 Section 6.6。

**想一想** 在第 (i) 部分，單位矩陣 $\mathbf{I}$ 並不是 $\begin{pmatrix} a & a \\ a & a \end{pmatrix}$ 這種形式。那麼 $S$ 的單位元會是甚麼？

它必須是 $S$ 中的某個矩陣 $\mathbf{E}$，使得對 $S$ 中每個 $\mathbf{X}$ 都有 $\mathbf{EX} = \mathbf{XE} = \mathbf{X}$。這個條件只涉及 $\mathbf{E}$ 怎樣作用於這種特殊形式的矩陣，而不是所有矩陣。解方程就可以把它找出來。

## 逐步解題

### 階段 1　封閉性（closure）

以 $\mathbf{M}_a$ 表示四個項全都等於 $a$ 的矩陣。那麼

$$\mathbf{M}_a\mathbf{M}_b = \begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} b & b \\ b & b \end{pmatrix} = \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix} = \mathbf{M}_{2ab},$$

而當 $a, b \neq 0$ 時，$2ab \neq 0$。所以 $S$ 是封閉的。 ■

### 階段 2　羣公理（group axioms）

> **想一想**　矩陣乘法滿足結合律。至於單位元，解 $\mathbf{M}_e\mathbf{M}_a = \mathbf{M}_a$。至於逆元，解 $\mathbf{M}_a\mathbf{M}_b = \mathbf{M}_e$。

結合律（*associativity*）由矩陣乘法繼承而來。單位元：$\mathbf{M}_e\mathbf{M}_a = \mathbf{M}_{2ea} = \mathbf{M}_a$ 對所有 $a$ 成立，當且僅當 $e = \tfrac{1}{2}$；由於公式是對稱的，$\mathbf{M}_a\mathbf{M}_{1/2} = \mathbf{M}_a$ 同樣成立。所以

$$\mathbf{E} = \begin{pmatrix} \tfrac{1}{2} & \tfrac{1}{2} \\ \tfrac{1}{2} & \tfrac{1}{2} \end{pmatrix}$$

是 $S$ 的單位元。逆元：當 $b = \tfrac{1}{4a}$ 時，$\mathbf{M}_a\mathbf{M}_b = \mathbf{M}_{2ab} = \mathbf{M}_{1/2}$，而這個值不為零，所以 $\mathbf{M}_{1/(4a)}$ 是 $\mathbf{M}_a$ 在 $S$ 中的逆元。因此 $S$ 是一個羣。■每個元素的行列式都是 $a^2 - a^2 = 0$。

### 階段 3　奇異性會蔓延

> **停一停，試一試**　假設 $\mathbf{A} \in G$ 是奇異的，並設 $\mathbf{B}$ 為 $G$ 的任意元素。把 $\mathbf{B}$ 寫成一個含有 $\mathbf{A}$ 的乘積，然後取行列式。

以 $\mathbf{A}^{-1}$ 表示 $\mathbf{A}$ 在羣 $G$ 中的逆元（不一定是逆矩陣）。那麼 $\mathbf{C} = \mathbf{A}^{-1}\mathbf{B}$ 屬於 $G$，而且

$$\mathbf{AC} = \mathbf{A}\mathbf{A}^{-1}\mathbf{B} = \mathbf{E}\mathbf{B} = \mathbf{B}.$$

取行列式，得 $\det\mathbf{B} = \det\mathbf{A}\,\det\mathbf{C} = 0$。所以 $G$ 的每個元素都是奇異的。 ■特別地，如果一個矩陣羣中有一個元素作為矩陣是可逆（invertible）的，那麼所有元素都可逆；一個矩陣羣要麼全部可逆，要麼全部奇異。

### 階段 4　一個 $3 \times 3$ 的例子

**想一想** 你能把第 (i) 部分推廣到 $3 \times 3$ 矩陣嗎？或者找一個更簡單的例子，用一個「無視」三個坐標中其中兩個的矩陣？

取

$$G = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} : a \neq 0 \right\}.$$

角上的項分別為 $a$ 和 $b$ 的兩個矩陣，乘積就是角上的項為 $ab$ 的矩陣，所以 $G$ 是封閉的；乘法滿足結合律；單位元是角上的項為 1 的矩陣；角上的項為 $a$ 的矩陣，其逆元是角上的項為 $\frac{1}{a}$ 的矩陣。所以 $G$ 是一個羣，而且每個元素的行列式都是 0。 ■（另一個例子：九個項全都等於 $a \neq 0$ 的 $3 \times 3$ 矩陣，其單位元的所有項都是 $\frac{1}{3}$。）

## 回顧

- **按字面去讀定義。**羣的單位元就是*在該羣之內*起單位元作用的那個元素；它不一定是我們熟悉的那個單位矩陣。
- **解方程求出結構。**$S$ 的單位元和逆元都是靠解方程找出來的，而不是靠猜。
- **行列式具有可乘性。**單憑這一個性質，就說明了奇異性會由一個元素蔓延到所有元素。

## 背後的數學

### 冪等元與隱藏的可逆性

任何矩陣羣的單位元 $\mathbf{E}$ 都滿足 $\mathbf{E}^2 = \mathbf{E}$：它是冪等（*idempotent*）的。從幾何上看，冪等矩陣就是一個投影（*projection*）：它把每個向量映射到某個子空間（subspace）上，而原本已在該子空間內的向量則保持不變。在第 (i) 部分，$\mathbf{E}$ 把平面投影到直線 $y = x$ 上，而每個矩陣 $\mathbf{M}_a$ 都是先投影到這條直線上，然後沿着它以因子 $2a$ 拉伸（圖 6.8.1）。在這條直線上，這個羣的作用是可逆的拉伸；它只是無視了與直線垂直的方向。所以 $S$ 其實就是非零實數的乘法羣（透過 $\mathbf{M}_a \mapsto 2a$），只不過它棲身於平面內的一條直線上。這個結論普遍成立：每個由矩陣組成的羣，經過換基（change of basis）之後，都是一個由可逆矩陣組成的羣，作用於其單位元的像上，其餘位置則以零填充。

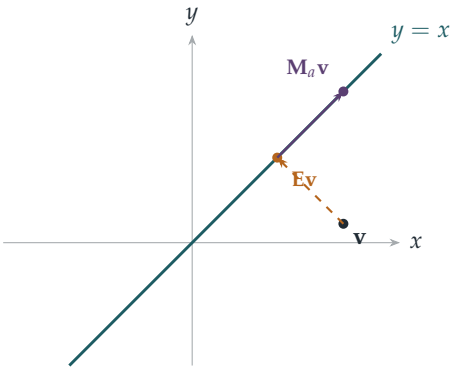



**圖 6.8.1**　第 (i) 部分的矩陣所起的作用。單位元 $\mathbf{E}$ 把每個向量 $\mathbf{v}$ 投影到直線 $y = x$ 上（琥珀色虛線）。每個 $\mathbf{M}_a$ 都先作同樣的投影，然後沿着直線以因子 $2a$ 拉伸（紫紅色；圖中 $2a = \frac{16}{9}$）。在這條直線本身之上，這個羣的作用就是普通的可逆縮放。

### 抽象與具體

人們最早研究的羣都是具體的：置換 (permutation)、對稱、可逆矩陣。抽象的定義 (一個集合連同一個滿足三條公理的運算）是從這些例子中提煉出來的。本題顯示了抽象觀點的價值：$S$ 與非零實數的乘法羣是同構（*isomorphic*）的，即同一個羣換了一身衣服，儘管一個由奇異矩陣組成，另一個由數組成。辨認出兩個外表不同的結構何時「相同」，是代數最核心的技巧之一，而數學家正是藉同構這個概念把這種「相同」說得精確。

## 思維技巧

**質疑對熟悉對象的隱藏假設**

當一個熟悉的對象出現在抽象定義中時，要查清楚定義實際上要求它具備哪些我們熟悉的性質。

「矩陣羣的單位元是 $\mathbf{I}$」聽起來理所當然，卻不是定義的一部分；放下這個假設，就得出了一個真正嶄新的例子。許多新的數學結構，正是這樣靠質疑假設而發現的。

## 延伸練習

1 **一個同構。**證明映射 $\mathbf{M}_a \mapsto 2a$ 是由 $S$ 到非零實數的一一對應（one-to-one correspondence），並且把矩陣乘法變成數的乘法。

2 **不是羣。**證明所有形如 $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ 且 $a \neq 0$ 的矩陣所組成的集合在乘法下封閉，但不是一個羣。（提示：試找單位元。有沒有左單位元？有沒有右單位元？）

3 **冪等元。**求所有滿足 $\mathbf{E}^2 = \mathbf{E}$ 的 $2 \times 2$ 實矩陣 $\mathbf{E}$，並從幾何角度描述它們。

4 **所有項相等。**證明所有項都等於 $a \neq 0$ 的 $n \times n$ 矩陣在乘法下構成一個羣，並求它的單位元。

## 延伸閱讀

- **M. A. Armstrong, *Groups and Symmetry***（Springer）。講述矩陣羣與同構，並附有大量幾何例子。
- **Gilbert Strang, *Introduction to Linear Algebra***（Wellesley-Cambridge）。對投影與冪等矩陣有清晰的講解。
- **Joseph Gallian, *Contemporary Abstract Algebra***（CRC Press）。一本平易近人的入門教材，載有許多不尋常的羣的例子。

# 我們學到了甚麼

本章開首，我們談到代數的重心由解方程轉移到研究結構，並提出了三個問題：甚麼可以由甚麼構造出來？方程的公式為何行得通？抽象化帶來了甚麼好處？以下是本章八道題目所揭示的答案。

### 1. 甚麼可以由甚麼構造出來？

在 Section 6.3 中，我們逐一消去根式（radical），找出 $\sqrt{2}+\sqrt{3}$、$\sqrt{2}+\sqrt{3}+\sqrt{5}$ 和 $\sqrt[3]{2}+\sqrt[3]{3}$ 所滿足的多項式，次數分別為 4、8 和 9。這些次數是不變量（invariant）：它們就是該數所生成的域（field）的次數。由於次數沿着域塔（tower of fields）逐層相乘，凡是可以用平方根得到的數，其次數必為 2 的冪。單憑這一點，便足以證明倍立方不可能做到（$\sqrt[3]{2}$ 的次數是 3），也證明 $60°$ 角不可能三等分。

反過來，Section 6.2 展示了某些東西可以怎樣構造出來。把 17 次單位根（roots of unity）分拆成高斯（Gauss）週期（period）之後，和 $\cos\frac{2\pi}{17}+\cos\frac{4\pi}{17}+\cos\frac{8\pi}{17}+\cos\frac{16\pi}{17}$ 滿足一個二次方程，其根為 $\frac{-1+\sqrt{17}}{4}$；再解三個二次方程便可得到 $\cos\frac{2\pi}{17}$，從而作出正 17 邊形。這兩節的背後，都是 Section 6.1 的分圓多項式（cyclotomic polynomial）：它們是 $x^n-1$ 的基本構件，把單位根按階（order）分類便可得到。

### 2. 方程的公式為何行得通？

Section 6.4 揭示了四次方程（quartic）的祕密：由四個根組成三個量 $\alpha\beta+\gamma\delta$、$\alpha\gamma+\beta\delta$、$\alpha\delta+\beta\gamma$，每個量對應把四個根兩兩配對的一種方法。無論怎樣重新排列這些根，都只會把這三個量互相調換，所以它們滿足一個係數已知的三次方程。先解這個三次方程，再解兩個二次方程，便得出四個根。拉格朗日（Lagrange）看出，這個方法之所以行得通，在於四個物件的置換（permutation）如何作用於那三種配對；伽羅瓦（Galois）則看出，這個方法對五個根失效，是因為五個物件的置換羣（group）之中，有一部分無法再分解。這些公式，其實是羣結構的影子。

### 3. 抽象化帶來了甚麼好處？

最後四節都以物件所遵守的規則來描述物件。

- 在 Section 6.5 中，四條規則（可加性、乘積法則、常數、$\Diamond x=1$）迫使一個運算必然是求導（differentiation），完全不涉及極限。同樣的規則，正是現代軟件中自動微分

（automatic differentiation）的基礎。

- 在 Section 6.6 中，由羣公理（axiom）出發的一個三行論證，一舉對所有羣證明了：沒有任何羣是兩個真子羣（proper subgroup）的併集。
- 在 Section 6.7 中，一個定義在複數對上的古怪運算，原來就是哈密頓（Hamilton）的四元數（quaternion）乘法；用矩陣來表示它，結合律（associativity）便自動成立。
- 在 Section 6.8 中，按字面理解羣的定義，便得出一個由奇異矩陣（singular matrix）組成的羣，它的單位元（identity）並不是單位矩陣，而它「其實」是非零實數羣的化身。

在每一個例子中，抽象的觀點都解釋了一些單靠計算會被掩蓋的東西。

### 4. 代數工具箱

| 方法 | 在哪裏用過 |
|---|---|
| 按唯一的不變量分類 | 按階把單位根分類（6.1） |
| 由和與積得出二次方程 | 高斯週期（6.2）；四次方程（6.4） |
| 積化和差公式 | 正 17 邊形（6.2） |
| 消去根式 | 最小多項式（minimal polynomial）（6.3） |
| 次數與塔定律（tower law） | 作圖的不可能性（6.3） |
| 根的對稱函數（symmetric function） | 三次預解式（resolvent cubic）（6.4） |
| 由公理確定一個運算 | 導子（derivation）（6.5） |
| 由羣公理出發論證 | 子羣的併集（6.6） |
| 矩陣表示（matrix representation） | 四元數（6.7） |
| 同構（isomorphism） | 奇異矩陣羣（6.8） |

### 下一步

- 四元數通往 Section 7.8 的拉格朗日四平方和定理（four-square theorem）。
- 把矩陣視為自有一套規則的代數物件，是第 7 章的主題。
- 像高斯整數（Gaussian integers）這類數系的算術，當中因數分解（factorisation）可能失效，是 Section 1.7 的主題。

#### 如果你想在上大學之前再走遠一點

- **Mario Livio, *The Equation That Couldn't Be Solved***：五次方程、伽羅瓦與羣論的誕生。

- **Nathan Carter, *Visual Group Theory***：用圖像認識羣，是初次接觸的理想讀物。
- **M. A. Armstrong, *Groups and Symmetry***：建基於幾何的大學入門課程。
- **Ian Stewart, *Galois Theory***：留待你準備好了解整個故事的時候。

伽羅瓦在一場決鬥之後去世，年僅二十歲，只留下數十頁手稿，數學界花了幾十年才讀懂。他看出，一個方程最深層的祕密並不在它的係數之中，而在它的解的對稱性之中。這個洞見——給不同的東西起同一個名字，並研究它們共有的結構——如今貫穿整個數學。你已經在多項式、多邊形、四元數和矩陣中見過它發揮作用；到了大學，你幾乎處處都會遇見它。

# 延伸練習答案

以下只是簡短的答案和提示，並非完整解答：這裏只列出結果和關鍵步驟，方便你核對自己的做法。請先認真做過每一道練習，然後才看答案。

## 6.1 以單位根為根的多項式

1. $(x-1)(x+1) = x^2-1$ 而 $(x^2+x+1)(x^2-x+1) = x^4+x^2+1$，兩者之積為 $x^6-1$。同理，$x^{12}-1 = (x^6-1)(x^6+1)$，而 $x^6+1 = (x^2+1)(x^4-x^2+1) = \mathrm{C}_4\mathrm{C}_{12}$。

2. $2p$ 的因數（divisor）為 $1、2、p、2p$，所以 $\mathrm{C}_{2p} = \frac{x^{2p}-1}{(x-1)(x+1)\mathrm{C}_p(x)} = \frac{x^p+1}{x+1}$。另一方面，$\mathrm{C}_p(-x) = \frac{(-x)^p-1}{-x-1} = \frac{x^p+1}{x+1}$，因為 $p$ 是奇數。當 $p=3$ 時：$\mathrm{C}_6 = x^2-x+1 = \mathrm{C}_3(-x)$。

3. 不超過 $p^k$ 而又與 $p^k$ 有公因數的數，就是那 $p^{k-1}$ 個 $p$ 的倍數。本原（primitive）$p^k$ 次單位根是 $x^{p^k}-1$ 的根之中不屬於 $x^{p^{k-1}}-1$ 的根的那些，所以 $\mathrm{C}_{p^k} = \frac{x^{p^k}-1}{x^{p^{k-1}}-1} = \mathrm{C}_p\left(x^{p^{k-1}}\right)$。因此 $\mathrm{C}_9 = x^6+x^3+1$。

4. $\mathrm{C}_{15} = \frac{(x^{15}-1)(x-1)}{(x^3-1)(x^5-1)}$。把 $(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)$ 與題中給出的八次式相乘並展開，驗證結果為 $x^{15}-1$。

## 6.2 高斯的正十七邊形

1. $\eta+\eta'$ 是全部六個非實七次單位根之和，即 $-1$。展開 $\eta\eta'$ 得到九項 $\alpha^{a+b}$，其指數為 $4,6,0,5,0,1,0,2,3$（模 7）：即三個 1，以及每個非實根各出現一次，所以 $\eta\eta' = 3-1 = 2$。因此 $\eta、\eta'$ 就是 $\frac{-1\pm\mathrm{i}\sqrt{7}}{2}$。$\eta$ 的實部給出餘弦之和。它的虛部是 $\sin\frac{2\pi}{7} + \sin\frac{4\pi}{7} - \sin\frac{\pi}{7}$，由於 $\sin\frac{4\pi}{7} = \sin\frac{3\pi}{7} > \sin\frac{\pi}{7}$，這個值為正；所以它等於 $+\frac{\sqrt{7}}{2}$。

2. 設 $\zeta = \mathrm{e}^{2\pi\mathrm{i}/5}$，則兩個週期（period）$\zeta+\zeta^4 = 2\cos\frac{2\pi}{5}$ 和 $\zeta^2+\zeta^3$ 之和為 $-1$，之積為 $-1$，所以它們是 $t^2+t-1=0$ 的根，而其中的正根給出 $\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$。作圖方法：在單位圓內，兩條直角邊為 1 和 $\frac{1}{2}$ 的直角三角形，斜邊長為 $\frac{\sqrt{5}}{2}$；減去 $\frac{1}{2}$ 再取一半，便得 $\cos\frac{2\pi}{5}$。在軸上這個距離處作垂線，它與圓相交於一個與 $(1,0)$ 相鄰的頂點；再用這條弦沿圓周逐步截取。

3. 兩者準確至小數點後五位都是 $-1.28078$。

4. 3 的各次冪依次為 $3,9,10,13,5,15,11,16,14,8,7,4,12,2,6,1$：十六個數全部出現。2 的各次冪在八步之後重複（$2^8 = 256 \equiv 1$），給出 $\{1,2,4,8,9,13,15,16\}$，即模 17 的非零平方數。

### 6.3 以 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 為根的多項式

1. $y^3 = 2\sqrt{2}+6\sqrt{3}+9\sqrt{2}+3\sqrt{3} = 11\sqrt{2}+9\sqrt{3}$，而 $9y = 9\sqrt{2}+9\sqrt{3}$，所以 $y^3 - 9y = 2\sqrt{2}$。於是 $\sqrt{3} = y - \sqrt{2}$ 和 $\sqrt{6} = \sqrt{2}\sqrt{3}$ 也都是 $y$ 的多項式。

2. 設 $x - \sqrt{2} = \sqrt[3]{3}$ 並取立方：$x^3 + 6x - 3 = \sqrt{2}(3x^2+2)$。兩邊平方得 $x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1 = 0$。

3. 可能的有理根只有 $\pm 1$，而兩者都不是根。由於沒有 $x^3$ 項，分解成兩個首一（monic）二次式時必定形如 $(x^2 + ax + b)(x^2 - ax + c)$，其中 $a(c-b) = 0$、$b + c - a^2 = -10$ 及 $bc = 1$。若 $a = 0$，則 $b + c = -10$ 且 $bc = 1$，在整數範圍內不可能；若 $b = c = \pm 1$，則 $a^2 = 12$ 或 $8$，同樣不可能。所以這個四次式不可約（irreducible），而 $\sqrt{2}+\sqrt{3}$ 的次數（degree）為 4。

4. 由棣美弗（De Moivre）定理，$\cos 3\theta = 4\cos^3\theta - 3\cos\theta$；取 $\theta = 20^\circ$，得 $\frac{1}{2} = 4c^3 - 3c$。候選的有理根 $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$ 全都不成立。所以 $\cos 20^\circ$ 的次數為 3，但每個可作圖（constructible）長度的次數都是 2 的冪，因此無法由 $60^\circ$ 作出 $20^\circ$。

### 6.4 解四次方程

1. $y_1y_2 + y_2y_3 + y_3y_1$ 是十二項 $\alpha^2\beta\gamma$（一個根的平方乘以另外兩個根）之和。而 $\left(\sum\alpha\right)\left(\sum\alpha\beta\gamma\right)$ 則是這十二項再加上 $4\alpha\beta\gamma\delta$。所以所求之和為 $(-p)(-r) - 4s$。

2. 比較係數得 $a + b = 1$、$a\alpha + b\beta = 0$ 及 $a\alpha^2 + b\beta^2 = -p$，當 $\alpha \neq \beta$ 時有解，而這正是那兩個條件所保證的：$p \neq 0$ 使關於 $t$ 的方程是真正的二次方程（若 $p = 0$，它會退化成 $-qt = 0$，只有單一個根 0），而 $q^2 \neq 4p^3$ 則使它的判別式（discriminant）$q^2 - 4p^3$ 不為零。對於 $x^3 - 24x + 48$：$p = 8$，$q = 48$，而 $8t^2 - 48t + 64 = 0$ 給出 $\alpha = 2$，$\beta = 4$。於是 $\left(\frac{x-2}{x-4}\right)^3 = -\frac{b}{a} = \frac{\alpha}{\beta} = \frac{1}{2}$，所以 $x - 2 = 2^{-1/3}(x-4)$，整理後即得題中給出的根，$x \approx -5.6946$。

3. 預解三次式（resolvent cubic）為 $y^3 - 7y^2 + 16y - 12 = (y-3)(y-2)^2$。由根 $y = 3$ 得出 $(x^2 - 2x + 1)(x^2 - 2x + 2)$，所以各根為 1（二重根）和 $1 \pm \mathrm{i}$。

4. 在每一對之內可以對換或不對換（4 種選擇），兩對之間也可以互換或不互換（2 種選擇）：恆等置換、$(\alpha\beta)$、$(\gamma\delta)$、$(\alpha\beta)(\gamma\delta)$、$(\alpha\gamma)(\beta\delta)$、$(\alpha\delta)(\beta\gamma)$、$(\alpha\gamma\beta\delta)$ 和 $(\alpha\delta\beta\gamma)$。這與正方形的對稱羣（symmetry group）結構完全相同。

### 6.5 從公理出發的微分法

1. 常數仍然給出 0，而由規則 (i) 及歸納法（induction）可得 $\lozenge x^n = x^{n-1}\lozenge x + x\lozenge x^{n-1} = nx^n$。再由線性（linearity）得 $\lozenge \mathrm{h} = x\mathrm{h}'$。
2. $\lozenge \mathrm{f} = \frac{\mathrm{f}}{\mathrm{g}}\lozenge \mathrm{g} + \mathrm{g}\lozenge\frac{\mathrm{f}}{\mathrm{g}}$，所以 $\lozenge\frac{\mathrm{f}}{\mathrm{g}} = \frac{\mathrm{g}\lozenge \mathrm{f} - \mathrm{f}\lozenge \mathrm{g}}{\mathrm{g}^2}$。
3. 若 $\mathrm{f} = (x-a)^2\mathrm{g}$，則 $\mathrm{f}' = (x-a)\big(2\mathrm{g} + (x-a)\mathrm{g}'\big)$。$x^n - 1$ 的重根（repeated root）必定也是 $nx^{n-1}$ 的根，所以只能是 0；但 0 並不是 $x^n - 1$ 的根。
4. $(2+\varepsilon)^2 + 1 = 5 + 4\varepsilon$，而 $(5+4\varepsilon)^3 = 125 + 300\varepsilon$。所以 $f(2) = 125$ 及 $f'(2) = 300$；用鏈式法則（chain rule）則得 $3(x^2+1)^2 \cdot 2x = 3 \cdot 25 \cdot 4 = 300$。

### 6.6 子羣的併集

1. 設 $V = \{e, a, b, c\}$：$a^2 = b^2 = c^2 = e$，而 $a$、$b$、$c$ 之中任意兩個之積都是第三個。每個元素都是自己的逆元（inverse）。在 $\{1, \mathrm{i}, -1, -\mathrm{i}\}$ 中，i 的逆元是 $-\mathrm{i}$，所以這兩個羣並不相同。
2. 假如 $g$ 屬於某個真子羣（proper subgroup）$H$，那麼 $g$ 的每個冪也都屬於它，於是 $H$ 就是整個羣。
3. 1 既不是偶數，也不是 3 的倍數。更一般地，$\mathbb{Z}$ 是循環羣（cyclic group，由 1 生成），所以根據上一題，它不是任意多個真子羣的並集（union）。
4. 直線 $y = mx$ 與 $y = x^2$ 只相交於 $x = 0$ 和 $x = m$ 兩處，而直線 $x = 0$ 與它只相交於原點。所以 $k$ 條直線最多只能包含 $k$ 個形如 $(t, t^2)$ 而 $t \neq 0$ 的點，但這樣的點有無窮多個。

### 6.7 四元數羣

1. $C \circ B = (\mathrm{i}, 0) \circ (0, 1) = (0, \mathrm{i}) = D$，而 $B \circ C = (0, 1) \circ (\mathrm{i}, 0) = (0, \mathrm{i}^*) = (0, -\mathrm{i}) = H$。
2. $A$ 的階（order）為 1，$E$ 的階為 2；其餘六個元素的平方都是 $E$，所以階為 4。正方形的對稱羣有五個階為 2 的元素（四個反射和一個半周旋轉），所以這兩個羣並不同構（isomorphic）。
3. $\det M = z_1 z_1^* + z_2 z_2^* = |z_1|^2 + |z_2|^2$，這是四個實數平方之和。由於 $M(z)M(w)$ 是 $z \circ w$ 的矩陣，把行列式（determinant）相乘，便可把 $(a_1^2 + \cdots + a_4^2)(b_1^2 + \cdots + b_4^2)$ 寫成 $|u_1|^2 + |u_2|^2$，同樣是四個平方之和。
4. 各子羣為 $\{A\}$、$\{A, E\}$、$\{A, E, C, G\}$、$\{A, E, B, F\}$、$\{A, E, D, H\}$ 和 $Q_8$。除 $A$ 以外，每個元素都有某個冪等於 $E$，所以除 $\{A\}$ 以外的任何子羣都包含 $E$。三個階為 4 的子羣合起來包含了全部八個元素。

### 6.8 由奇異矩陣組成的羣

1. $\mathbf{M}_a\mathbf{M}_b = \mathbf{M}_{2ab}$，而 $2(2ab) = (2a)(2b)$。這個映射是一對一（one-to-one）的，並且映成（onto）全體非零實數。
2. $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix}$，其中 $ac \neq 0$，所以這個集合是封閉（closed）的。每個 $\begin{pmatrix} 1 & e \\ 0 & 0 \end{pmatrix}$ 都是左單位元（left identity）。但若要 $\mathbf{XE} = \mathbf{X}$，其中 $\mathbf{E} = \begin{pmatrix} e & f \\ 0 & 0 \end{pmatrix}$，便需要 $e = 1$ 及 $f = b/a$，而後者取決於 $\mathbf{X}$：所以沒有右單位元，因而沒有單位元，也就不成羣。
3. $\mathbf{0}$、$\mathbf{I}$，以及滿足 $bc = a(1-a)$ 的矩陣 $\begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}$（跡（trace）為 1，行列式為 0）。這些就是把平面沿一條直線的方向投影（projection）到另一條直線上的變換。
4. 所有元素均為 $a$ 的矩陣 $\mathbf{J}_a$ 滿足 $\mathbf{J}_a\mathbf{J}_b = \mathbf{J}_{nab}$。單位元是 $\mathbf{J}_{1/n}$，而 $\mathbf{J}_a$ 的逆元是 $\mathbf{J}_{1/(n^2a)}$。

# Beyond STEP

STEP 是大多數中學生一生中應考過最艱深的數學考試，也是最出色的考試之一：題目簡短、陌生而深刻，當中最精彩的，其實是喬裝了的大學數學小品。

本書精選最有趣的 STEP 試題，由 1987 年首次開考之前的樣本試卷（specimen papers），到 2025 年的試卷，並以每一道題目作為一扇門。每道題目都會仔細解答，沿途提出優秀學生會問的問題，然後帶你穿過這扇門：這個想法從何而來，到了大學會演變成甚麼，以及接下來該讀些甚麼。

本書為正在準備 STEP、有天分又有志投身數學的學生而寫。他們想要的不止是模擬試卷：他們想開始像數學系本科生那樣思考，並一探前方有甚麼正等着自己。

- 共 13 章，涵蓋純數學（pure mathematics）、力學（mechanics）、概率（probability）與統計（statistics）
- 136 道 STEP 歷屆試題，每題均附引導式解答
- 每道題目背後的大學數學
- 附答案的延伸練習，以及延伸閱讀

**全書共 13 章，本冊為第 6 章。** 全書各章及所有詳細解答均可免費閱讀、下載及分享，網址為

**beyondstep.keithmcnulty.org**

文字內容已貢獻予公有領域（CC0 1.0）。STEP 試題 © Cambridge University Press & Assessment。