6.1 以單位根為根的多項式

工作紙

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

提示

請先自行嘗試解題。如果遇到困難，請逐一閱讀提示，每讀完一個便回到題目再試。標有停一停，試一試的提示是關鍵步驟。每個提示之後均留有空位供你演算。

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、i、-1、$-\mathrm{i}$，這個最小的冪次分別是多少？

階段 1 最初幾個

涵蓋：四次單位根，以及第 (i) 部分

想一想 對於四次單位根（roots of unity）1、i、-1、$-\mathrm{i}$，逐一找出使其冪等於 1 的最小正整數指數。哪些是本原根（primitive root）？

停一停，試一試 把 6 次單位根按「使其冪等於 1 的最小指數」分類。對於 $n = 3$ 和 $n = 5$：哪些 n 次單位根不是本原根？用 $x^n - 1$ 除以對應的因式。

階段 2　哪個 n 會給出 x^4+1？

涵蓋：第 (ii) 部分

> **停一停，試一試**　若 $x^4 = -1$，x^8 是多少？已知使其冪等於 1 的最小指數整除 8，但 $x^4 \neq 1$，這個最小指數可以是多少？

階段 3　質數

涵蓋：第 (iii) 部分

> **想一想**　若 p 是質數（prime），p 次單位根的階（order）可以是多少？把你在 $n = 3$ 和 $n = 5$ 時的做法推廣。

階段 4 **沒有分圓多項式是另外兩個分圓多項式之積**

涵蓋：第 (iv) 部分

> **停一停，試一試** 假設 $\mathrm{C}_q = \mathrm{C}_r\mathrm{C}_s$。取 C_r 的一個根：它的階是多少？根據這個恆等式（identity），它的階又是多少？一個單位根只有一個階。

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

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

例如 $x^6 - 1 = \mathrm{C}_1\mathrm{C}_2\mathrm{C}_3\mathrm{C}_6 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$。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 $\sum_{d \mid n} \varphi(d) = n$。

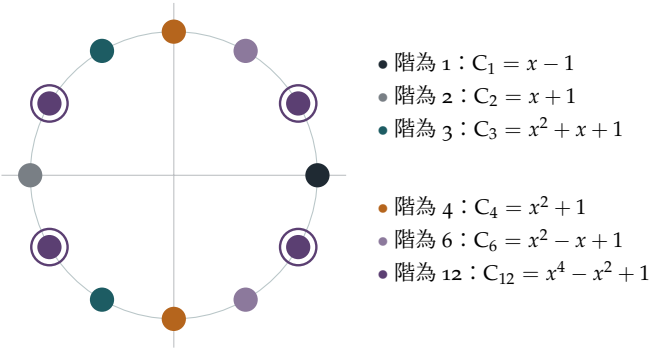

圖 6.1.1　十二個 12 次單位根，按階着色。四個本原 12 次單位根（以圓圈標示）是 C_{12} 的根。各類合起來給出 $x^{12} - 1 = C_1C_2C_3C_4C_6C_{12}$，次數為 $1 + 1 + 2 + 2 + 2 + 4 = 12$。

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。

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 $\mathrm{C}_{p^k}(x) = \mathrm{C}_p\left(x^{p^{k-1}}\right)$。利用這個結果求 C_9。

4 **較長的一題。**較難利用 $x^{15} - 1 = \mathrm{C}_1\mathrm{C}_3\mathrm{C}_5\mathrm{C}_{15}$，證明 $\mathrm{C}_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$。

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。

完整的引導式解答見第 6.1 節：

https://beyondstep.keithmcnulty.org/zh-hant/ch06/cyclotomic.html

每星期一道 STEP 題目，完整講解：The STEP Up，以電郵免費發送，訂閱網址：keithmcnulty.substack.com