分圓多項式

Timo Chang
timo65537@protonmail.com
譯者: 仙女仙女

最後編輯: 2025 年 12 月 25 日

本文中, 我們在 $\mathbb{Q}$ 上爲每個 $n \in \mathbb{N}$ 引入分圓多項式 $\Phi_n(x)$, 並給出各種計算公式. 此外, 我們也將證明 $\Phi_n(x)$ 是任一 n 次本原單位根在 $\mathbb{Q}$ 上的不可約多項式, 且其係數均爲整數.

1 定義與計算

定義 1.1 (分圓多項式) 對每個 $n \in \mathbb{N}$, 定義**第 n 分圓多項式**爲

$$\Phi_n(x) := \prod_{\substack{1\le k\le n\\ \gcd(k,n)=1}} (x - e^{2\pi i k/n}).$$

換言之, 第 n 分圓多項式即爲恰以所有 n 次本原單位根爲根的首一多項式. 注意到 $\deg \Phi_n(x) = \phi(n)$ 爲**歐拉 ϕ 函數**.

命題 1.2 對每個 $n \in \mathbb{N}$,

$$\prod_{d|n} \Phi_d(x) = x^n - 1.$$

比較等式兩側的次數, 可知 $\sum_{d|n} \phi(d) = n$, 這是基礎數論中耳熟能詳的事實. 事實上, 正如下文將要說明的, 這兩條恆等式背後的證明思路可謂殊途同歸, 本質上並無差別. 然而, 若要深入體會命題 1.2 的內涵, 與其鉅細靡遺地鋪陳嚴格證明, 不如先計算一個不會太平凡的例子. 至於一般情形, 其論證完全可以依循相同構想推展, 故留作習題, 請在今晚十二點按時繳交.

例 1.3 以 $n = 6$ 爲例, 欲確認

$$\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = x^6 - 1. \tag{1}$$

首先考慮等式右邊, 令 $\zeta_6 := e^{2\pi i/6}$, 則 $x^6 - 1$ 的六個 6 次單位根爲

$$\{\zeta_6, \zeta_6^2, \zeta_6^3, \zeta_6^4, \zeta_6^5, \zeta_6^6 = 1\} = \{e^{2\pi i/6}, e^{4\pi i/6}, e^{6\pi i/6}, e^{8\pi i/6}, e^{10\pi i/6}, e^{12\pi i/6} = 1\}.$$

另一方面, 依定義 1.1, 可知等式左邊有

$$\begin{aligned}\Phi_1(x) &= (x - e^{2\pi i}),\\ \Phi_2(x) &= (x - e^{2\pi i/2}),\\ \Phi_3(x) &= (x - e^{2\pi i/3})(x - e^{4\pi i/3}),\\ \Phi_6(x) &= (x - e^{2\pi i/6})(x - e^{10\pi i/6}).\end{aligned}$$

注意到 (1) 的兩邊均爲首一多項式, 且有同樣的根, 因此它們必相等.

命題 1.2 的證明中的關鍵觀察如下: 任一 n 次單位根皆爲某個唯一滿足 $d \mid n$ 的 d 次本原單位根, 且反過來, 任一滿足 $d \mid n$ 的 d 次本原單位根必爲 n 次單位根 (比如說, $e^{4\pi i/6} = e^{2\pi i/3}$ 是一個 6 次單位根, 同時也是 3 次本原單位根).

依此方法, 可以證明欲證等式的兩邊恰有完全相同的根. 由於兩者皆爲首一多項式, 該等式遂告成立. 進一步而言, 我們眞正關心的其實是指數上的「分式」, 而此想法類似於證明恆等式

$$\sum_{d|n} \phi(d) = n$$

的其中一種常見方法高度相似.

命題 1.4 對一切 $n \in \mathbb{N}$, $\Phi_n(x)$ 是整係數首一多項式.

證明 對 n 使用歸納法. 歸納基礎顯而易見, 故假設命題對每個 $k = 1, \ldots, n-1$ 均成立. 依命題 1.2, 可知

$$\prod_{d|n} \Phi_d(x) = \Phi_n(x) \cdot \prod_{\substack{d|n\\ d\neq n}} \Phi_d(x) = x^n - 1,$$

所以

$$\Phi_n(x) = x^n - 1 \Big/ \prod_{\substack{d|n\\ d\neq n}} \Phi_d(x). \tag{2}$$

依歸納假設, 在乘積中的每一項均爲整係數首一多項式, 故上述分式的分母當然也是首一多項式. 由長除法, 可推得 $\Phi_n(x) \in \mathbb{Z}[x]$. □

例 1.5 注意到 (2) 式提供了一種計算 $\Phi_n(x)$ 的方法. 舉個例子, 求 $\Phi_8(x)$, 則

$$\Phi_8(x) = \frac{x^8 - 1}{\Phi_1(x)\Phi_2(x)\Phi_4(x)}.$$

依定義 1.1, 有

$$\begin{aligned}\Phi_1(x) &= x - e^{2\pi i} = x - 1,\\ \Phi_2(x) &= x - e^{2\pi i/2} = x + 1,\\ \Phi_4(x) &= (x - e^{2\pi i/4})(x - e^{6\pi i/4}) = (x - i)(x + i) = x^2 + 1,\end{aligned}$$

因此

$$\Phi_8(x) = \frac{x^8 - 1}{(x-1)(x+1)(x^2+1)} = x^4 + 1.$$

不難觀察到: 要使用 (2) 式來計算 $\Phi_n(x)$, 需要先求出 n 的所有眞因數 d 相應的 $\Phi_d(x)$, 但這聽起來很不直接、很沒效率. 因此, 在下面我們將提供 $\Phi_n(x)$ 的另一個公式來解決此問題, 即一個不需要事先知道各 $\Phi_d(x)$ 的表達式 (命題 1.8).

定義 1.6 (莫比烏斯函數) 對每個 $n \in \mathbb{N}$, 定義**莫比烏斯函數** $\mu(n)$ 作

$$\mu(n) = \begin{cases} 1, & n = 1; \\ (-1)^r, & n = p_1 \cdots p_r, \text{ 其中 } p_i \text{ 爲相異質數}; \\ 0, & \text{其他情形}. \end{cases}$$

莫比烏斯函數在數論中無所不在, 並且具有許多優美的性質. 我們即將會用到的工具如下:

引理 1.7 對所有 $n \in \mathbb{N}$,

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1; \\ 0, & n > 1. \end{cases}$$

證明 $n = 1$ 的情形顯而易見, 故考慮 $n > 1$. 將 n 作質因數分解成 $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, 其中各 $\alpha_i \geq 1$, 且 p_i, p_j 相異, 則 n 的每個因數 d 都形如 $d = p_1^{\beta_1} \cdots p_r^{\beta_r}$, 其中每個 i 都滿足 $0 \leq \beta_i \leq \alpha_i$. 從定義 1.6 可看出, 只需考慮所有 i 都滿足 $\beta_i = 0, 1$ 的情形, 因爲否則 $\mu(d) = 0$. 將 n 的這些因數依它們的質因數個數來分組, 有

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_i \mu(p_i) + \sum_{i \neq j} \mu(p_i p_j) + \cdots + \mu(p_1 \cdots p_r) \\ &= 1 + \binom{r}{1}(-1) + \binom{r}{2}(-1)^2 + \cdots + \binom{r}{r}(-1)^r \\ &= (1 + (-1))^r \\ &= 0. \end{aligned}$$

□

命題 1.8 對所有 $n \in \mathbb{N}$,

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

證明 有了引理 1.7 在手, 此公式便能迎刃而解. 注意到

$$\begin{aligned} \prod_{d|n} (x^d - 1)^{\mu(n/d)} &= \prod_{d|n} \left(\prod_{k|d} \Phi_k(x) \right)^{\mu(n/d)} && \text{(命題 1.2)} \\ &= \prod_{d|n} \prod_{k|d} \Phi_k(x)^{\mu(n/d)} \\ &= \prod_{k|n} \Phi_k(x)^{\sum_{d' | \frac{n}{k}} \mu(d')} \\ &= \Phi_n(x) && \text{(引理 1.7)}, \end{aligned}$$

其中或許只有第三個等式需要多加說明. 粗略地說, 我們在做的事情是將該二重乘積中 n 所有固定的因數 k 對應的 $\Phi_k(x)$ 收集起來, 詳言之, 可觀察到對於每個如此的 k,

$$\left\{\frac{n}{d} : d \mid n \text{ 且 } k \mid d\right\} = \left\{d' : d' \mid \frac{n}{k}\right\}.$$

(要是這對你來說還是不甚清楚, 不妨考慮實例: $n = 60$ 及 $k = 6$ 足矣.) □

需要指出, 我們在上述證明簡單使用了**莫比烏斯反演公式**.

例 1.9 來使用命題 1.8 來計算規模稍微大一點的例子: $\Phi_{18}(x)$. 注意到 18 的因數有 $d = 1, 2, 3, 6, 9, 18$, 分別對應

$\mu(18/1)$	$\mu(18/2)$	$\mu(18/3)$	$\mu(18/6)$	$\mu(18/9)$	$\mu(18/18)$
0	0	1	-1	-1	1

故依命題 1.8, 有

$$\Phi_{18}(x) = \frac{(x^3-1)(x^{18}-1)}{(x^6-1)(x^9-1)} = x^6 - x^3 + 1.$$

瞧瞧, 這個公式的優雅之處, 不言而喻. 當 n/d 有平方因子時, 我們就可以從從容容地忽略之.

註記 1.10 依同樣的方法, 我們也可以游刃有餘地計算 (?) 出

$$\begin{aligned}\Phi_{105}(x) = {} & x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} \\ & + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} \\ & + x^{15} + x^{14} + x^{13} + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1.\end{aligned}$$

有趣的是, 105 這個數字其實是使其對應的分圓多項式具有異於 $0, 1, -1$ 的係數的最小正整數[1] (若未留意, -2 是 x^{41} 及 x^7 這兩項的係數), 稱此性質為 $\mathcal{P}$. 於是, 可能會浮現的問題是:

- 什麼導致 105 具有性質 $\mathcal{P}$ (是否有理由)?
- 其它數字如何? 是否能識別出所有滿足 $\mathcal{P}$ 的數?
- 是否有更深層的理由或更深奧的理論和 $\mathcal{P}$ 有關?

2 不可約性

命題 2.1 對所有 $n \in \mathbb{N}$, $\Phi_n(x)$ 在 $\mathbb{Q}[x]$ 中不可約.

[1] 整數數列線上百科 (OEIS): 含有 n 或 $-n$ 爲係數的分圓多項式的最小階數

證明 依高斯引理, 只需證明 $\Phi(x) := \Phi_n(x)$ 在 $\mathbb{Z}[x]$ 中不可約. 設 $\Phi(x) = f(x)g(x)$, 其中 $f(x), g(x) \in \mathbb{Z}[x]$. 由於 $\zeta_n := e^{2\pi i/n}$ 是 $\Phi(x)$ 的一根, 故或者 $f(\zeta_n) = 0$, 或者 $g(\zeta_n) = 0$, 不失一般性, 假設 $f(\zeta_n) = 0$. 而且, 不妨再假設 f 在 $\mathbb{Z}[x]$ 中不可約. 於是, $f(x)$ 是 ζ_n 在 $\mathbb{Q}$ 上的不可約多項式 $\mathrm{Irr}_{\mathbb{Q}}(\zeta_n)(x)$, 我們的目標是證明 $f(x) = \Phi(x)$. 又已有 $f(x) \mid \Phi(x)$, 只需證明

$$\Phi(x) = \prod_{\substack{1\le k\le n\\ \gcd(k,n)=1}} (x - \zeta_n^k) \mid f(x),$$

即欲證對所有滿足 $1 \le k \le n$ 且 $\gcd(k, n) = 1$ 的 k, 有 $f(\zeta_n^k) = 0$.

首先, 考慮 $k = p$ 是質數的情形, 並斷言 $f(\zeta_n^p) = 0$. 事實上, 我們將給出一個稍微更一般的結論: 若對於 n 次本原單位根 ζ 有 $f(\zeta) = 0$, 則對所有不整除 n 的質數 p, 均有 $f(\zeta^p) = 0$.

因 ζ^p 仍是 n 次本原單位根, 故其亦爲 $\Phi(x)$ 的一根, 因此有 $0 = \Phi(\zeta^p) = f(\zeta^p)g(\zeta^p)$. 若 $f(\zeta^p) = 0$, 則不攻自破. 現假設 $g(\zeta^p) = 0$, 將證明這不可能.

設 $h(x) := g(x^p) \in \mathbb{Z}[x]$, 則 $h(\zeta) = g(\zeta^p) = 0$. 另一方面, 一開始我們就假設了 $f(x)$ 不可約, 且在斷言中已經假設 $f(\zeta) = 0$, 這麼一來 $f(x) = \mathrm{Irr}_{\mathbb{Q}}(\zeta)(x)$, 從而 $f(x) \mid h(x)$. 於是, 存在 $a(x) \in \mathbb{Z}[x]$ 滿足 $h(x) = g(x^p) = f(x)a(x)$. 透過對係數取模 p, 有

$$\overline{h}(x) = \overline{g}(x^p) = \overline{g}(x)^p = \overline{f}(x) \cdot \overline{a}(x) \in (\mathbb{Z}/p\mathbb{Z})[x].$$

注意到, 若 $\overline{f}(x)$ 和 $\overline{g}(x)$ 互質, 則 $\overline{f}(x)$ 和 $\overline{g}(x)^p$ 也是, 不合理. 所以 $\overline{f}(x)$ 和 $\overline{g}(x)$ 在 $(\mathbb{Z}/p\mathbb{Z})[x]$ 中有公因子, 不妨設爲 $\overline{d}(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$, 其中 $\deg \overline{d}(x) \ge 1$. 現, 依命題 1.2 及命題 1.4 (參見 (2) 式), 可知在 $\mathbb{Z}[x]$ 中,

$$f(x)g(x) = \Phi(x) \mid x^n - 1.$$

這表示在 $(\mathbb{Z}/p\mathbb{Z})[x]$ 中,

$$\overline{d}(x)^2 \mid \overline{f}(x)\overline{g}(x) = \overline{\Phi}(x) \mid x^n - \overline{1},$$

故存在 $\overline{b}(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ 使得 $x^n - \overline{1} = \overline{d}(x)^2 \cdot \overline{b}(x)$. 對等式兩側求形式導數, 得

$$\overline{n}x^{n-1} = 2\overline{d}(x)\overline{d}'(x) \cdot \overline{b}(x) + \overline{d}(x)^2 \cdot \overline{b}'(x),$$

其非零 (因 $p \nmid n$) 且可被 $\overline{d}(x)$ 整除, 但因 $\overline{d}(x) \mid x^n - \overline{1}$, 故得矛盾.

現已證出, 只要 $f(\zeta) = 0$, 其中 ζ 是 n 次本原單位根, 則對所有不整除 n 的質數 p, 都有 $f(\zeta^p) = 0$, 現要使用這個結論來證明欲證的結果. 設 $1 \le k \le n$, $\gcd(k, n) = 1$, 將 k 作質因數分解成 $k = p_1 \cdots p_r$ (未必相異), 注意到對所有 $i = 1, \ldots, r$, 皆有 $p_i \nmid n$. 因爲 $f(\zeta_n) = 0$, 其中 $\zeta_n = e^{2\pi i/n}$ 是 n 次本原單位根, 且 $p_1 \nmid n$, 所以根據上述斷言, 有 $f(\zeta_n^{p_1}) = 0$. 接著, 因爲 $\zeta_n^{p_1}$ 也是 n 次本原單位根, 且 $p_2 \nmid n$, 所以再依上述斷言, 可得 $f(\zeta_n^{p_1p_2}) = 0$. 反覆進行此論證, 可見

$$0 = f(\zeta_n) = f(\zeta_n^{p_1}) = f(\zeta_n^{p_1p_2}) = \cdots = f(\zeta_n^{p_1\cdots p_r}) = f(\zeta_n^k),$$

而這即爲我們想要的式子. □

註記 2.2 我們也證明了, 對所有 n 次本原單位根 ζ_n, 都有 $\mathrm{Irr}_{\mathbb{Q}}(\zeta_n)(x) = \Phi_n(x)$, 因此體擴張 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ (n **次分圓擴張**) 的次數爲 $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n(x) = \phi(n)$.

註記 2.3 設 A 爲有限體上的多項式環, k 爲其分式體, 我們可分別將 A 和 k 視爲 $\mathbb{Z}$ 和 $\mathbb{Q}$ 的類比. 在此情形下, 也有對應的**卡利茲分圓多項式**的概念, 而本文所討論的一切 (乃至更多結果) 在這個背景下皆有平行的命題, 並且其證明方法本質上也相同. 關於此主題, 讀者可參考 [Pap23, Chapter 7.1].

參考資料

[Pap23] Mihran Papikian. *Drinfeld modules*. Vol. 296. Grad. Texts in Math. Springer Nature Switzerland AG, 2023.