6.1 以单位根为根的多项式

工作纸

题目

STEP III 2010，第 3 题

继续阅读之前，请先看题目（原题为英文）。题目载于 STEP Support Programme 的试题资料库：

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

提示

请先自行尝试解题。如果遇到困难，请逐一阅读提示，每读完一个便回到题目再试。标有“停一停”或“试一试”的提示是关键步骤。每个提示之后均留有空位供你演算。

想一想　每个 n 次单位根都满足 $z^n = 1$。但使它等于 1 的最小正整数次幂，可能小于 n。对于四个 4 次单位根 1、i、-1、$-\mathrm{i}$，这个最小的幂次分别是多少？

阶段 1 最初几个

涵盖：四次单位根，以及第 (i) 部分

想一想 对于四次单位根（roots of unity）1、i、−1、−i，逐一找出使其幂等于 1 的最小正整数指数。哪些是本原根（primitive root）？

停一停，试一试 把 6 次单位根按“使其幂等于 1 的最小指数”分类。对于 $n = 3$ 和 $n = 5$：哪些 n 次单位根不是本原根？用 $x^n - 1$ 除以对应的因式。

阶段 2　哪个 n 会给出 x^4+1?

涵盖：第 (ii) 部分

> **停一停，试一试**　若 $x^4=-1$，x^8 是多少？已知使其幂等于 1 的最小指数整除 8，但 $x^4\neq 1$，这个最小指数可以是多少？

阶段 3　质数

涵盖：第 (iii) 部分

> **想一想**　若 p 是质数（prime），p 次单位根的阶（order）可以是多少？把你在 $n=3$ 和 $n=5$ 时的做法推广。

阶段 4 没有分圆多项式是另外两个分圆多项式之积

涵盖：第 (iv) 部分

> **停一停，试一试** 假设 $C_q = C_r C_s$。取 C_r 的一个根：它的阶是多少？根据这个恒等式（identity），它的阶又是多少？一个单位根只有一个阶。

背后的数学

分解 $x^n - 1$

每个 n 次单位根都有某个整除 n 的阶 d；而当 $d \mid n$ 时，每个阶为 d 的 d 次单位根都是 n 次单位根。所以 $x^n - 1$ 的根按阶分成若干类，由此得到

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

例如 $x^6 - 1 = C_1 C_2 C_3 C_6 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$。图 6.1.1 展示了按这种方式分类的十二个 12 次单位根。本原 n 次单位根的个数，亦即 C_n 的次数，等于 1 至 n 之间与 n 没有公因数的 k 的个数，也就是欧拉函数（Euler's totient function）$\varphi(n)$。比较两边的次数，便得到恒等式 $\sum_{d \mid n} \varphi(d) = n$。

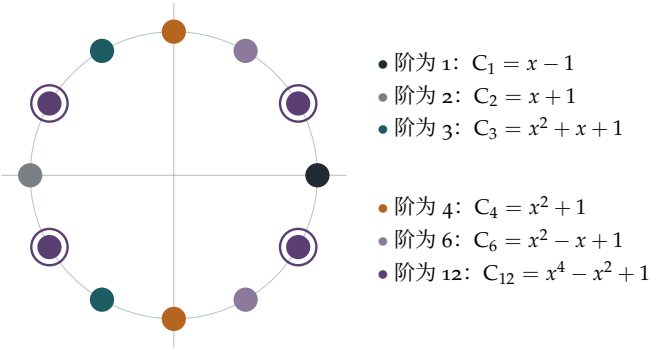

图 6.1.1　十二个 12 次单位根，按阶着色。四个本原 12 次单位根（以圆圈标示）是 C_{12} 的根。各类合起来给出 $x^{12} - 1 = C_1C_2C_3C_4C_6C_{12}$，次数为 $1 + 1 + 2 + 2 + 2 + 4 = 12$。

整数系数，以及一个意外

单看定义并不明显，但每个分圆多项式的系数都是整数。（利用 $x^n - 1$ 的因式分解和归纳法（induction）：C_n 等于 $x^n - 1$ 除以若干个较早的分圆多项式之积，而以首一（monic）整系数多项式对整系数多项式作长除法，所得系数仍是整数。）在很长一段时间里，所有已知例子的系数都只有 0、1 和 -1。第一个例外是 C_{105}，它含有 $-2x^7$ 这一项，由 Migotti 于 1883 年发现；$105 = 3 \times 5 \times 7$ 是具有三个相异奇质因数的最小的数。事实上，分圆多项式的系数可以要多大有多大。

不可约性

第 (iv) 部分证明了没有分圆多项式是另外两个分圆多项式之积。其实更强的结论也成立：C_n 根本不能分解成次数较低的有理系数多项式之积。高斯对 n 为质数的情况证明了这一点（它可由艾森斯坦判别法（Eisenstein's criterion）推出，你会在大学的第一门代数课中遇到），而克罗内克（Kronecker）和戴德金（Dedekind）则证明了一般 n 的情况。正是这种不可约性（irreducibility），使分圆多项式成为与单位根有关的多项式之中的“质数”，它也是单位根的伽罗瓦理论（Galois theory）的起点。

延伸练习

1. **检查因式分解。**验证 $(x-1)(x+1)(x^2+x+1)(x^2-x+1) = x^6 - 1$，并验证 $x^{12} - 1$ 的因式分解如图 6.1.1 所示。

2. **质数的两倍。**证明若 p 是奇质数，则 $C_{2p}(x) = C_p(-x)$。就 $p = 3$ 验证这个结果。

3 **欧拉函数。**证明对于质数 p，有 $\varphi(p^k) = p^k - p^{k-1}$，并且 $C_{p^k}(x) = C_p\left(x^{p^{k-1}}\right)$。利用这个结果求 C_9。

4 **较长的一题。**较难利用 $x^{15} - 1 = C_1C_3C_5C_{15}$，证明 $C_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$。

延伸阅读

- **Ian Stewart, *Galois Theory***（CRC Press）。大学本科的标准入门书；分圆多项式和正多边形在书中很早便出现。
- **Harold Davenport, *The Higher Arithmetic***（Cambridge University Press）。内容包括单位根及其算术性质。
- **Marcus du Sautoy, *Finding Moonshine***（Fourth Estate）。一本讲述对称与群论的科普读物，当中包括伽罗瓦的故事。

完整的引导式解答见第 6.1 节：

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

每星期一道 STEP 题目，完整讲解：The STEP Up，以电子邮件免费发送，订阅网址：keithmcnulty.substack.com