詳細解答

STEP III 1994，第 8 題

純數學 • 四平方和恆等式

STEP III 1994，第 8 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/94-s3-q8

本題在 *Beyond STEP* 第 7.8 節四個平方數中有完整的引導式講解：https://beyondstep.keithmcnulty.org/zh-hant/ch07/four-squares.html

關鍵思路

形如 $\begin{pmatrix} z & w \\ -w^* & z^* \end{pmatrix}$ 的矩陣(matrix)，其行列式(determinant)為 $zz^* + ww^* = |z|^2 + |w|^2$，是四個實數平方之和。若把 a, b, c, d 裝進一個這樣的矩陣，再把 p, q, r, s 裝進另一個，則由 $\det(AB) = \det A \det B$ 便得到左邊。要做的工夫是證明乘積 AB 具有同樣的特殊形式，因為這樣它的行列式也是四個平方之和，而這些平方正是 L_i^2。

解答

準備工作

對複數（complex number）z 和 w，記

$$M(z,w) = \begin{pmatrix} z & w \\ -w^* & z^* \end{pmatrix}, \qquad \det M(z,w) = zz^* - w(-w^*) = |z|^2 + |w|^2.$$

取

$$z_1 = a + b\mathrm{i}, \quad z_2 = c + d\mathrm{i}, \quad z_3 = p + q\mathrm{i}, \quad z_4 = r + s\mathrm{i}.$$

則

$$\det M(z_1, z_2) = a^2 + b^2 + c^2 + d^2, \qquad \det M(z_3, z_4) = p^2 + q^2 + r^2 + s^2.$$

乘積具有相同的形式

乘開得

$$M(z_1, z_2)\, M(z_3, z_4) = \begin{pmatrix} z_1 z_3 - z_2 z_4^* & z_1 z_4 + z_2 z_3^* \\ -z_2^* z_3 - z_1^* z_4^* & -z_2^* z_4 + z_1^* z_3^* \end{pmatrix}.$$

設 $w_1 = z_1 z_3 - z_2 z_4^*$ 及 $w_2 = z_1 z_4 + z_2 z_3^*$，即第一行的兩個元素。由於乘積的共軛（conjugate）等於共軛的乘積，而且 $(z^*)^* = z$，

$$w_1^* = z_1^* z_3^* - z_2^* z_4, \qquad -w_2^* = -z_1^* z_4^* - z_2^* z_3,$$

而這兩個正好就是右下角和左下角的元素。所以

$$M(z_1, z_2)\, M(z_3, z_4) = M(w_1, w_2).$$

想一想 乘積具有這個特殊形狀，為甚麼這樣重要？

對一般的 2×2 複矩陣而言，行列式根本不是平方和。正因為乘積仍然是 $M(w_1, w_2)$ 的形式，它的行列式才是 $|w_1|^2 + |w_2|^2$，從而可拆成四個實數平方。

取行列式

利用 $\det(AB) = \det A \, \det B$，

$$(a^2 + b^2 + c^2 + d^2)(p^2 + q^2 + r^2 + s^2) = \det M(w_1, w_2) = |w_1|^2 + |w_2|^2.$$

餘下只須求出 w_1 和 w_2 的實部（real part）和虛部（imaginary part）：

$$\begin{aligned} w_1 &= (a + b\mathrm{i})(p + q\mathrm{i}) - (c + d\mathrm{i})(r - s\mathrm{i}) \\ &= \big[(ap - bq) + (aq + bp)\mathrm{i}\big] - \big[(cr + ds) + (dr - cs)\mathrm{i}\big] \\ &= (ap - bq - cr - ds) + (aq + bp + cs - dr)\mathrm{i}, \end{aligned}$$

$$\begin{aligned} w_2 &= (a + b\mathrm{i})(r + s\mathrm{i}) + (c + d\mathrm{i})(p - q\mathrm{i}) \\ &= \big[(ar - bs) + (as + br)\mathrm{i}\big] + \big[(cp + dq) + (dp - cq)\mathrm{i}\big] \\ &= (ar - bs + cp + dq) + (as + br - cq + dp)\mathrm{i}. \end{aligned}$$

因此可取

$$L_1 = ap - bq - cr - ds, \qquad L_2 = aq + bp + cs - dr,$$
$$L_3 = ar - bs + cp + dq, \qquad L_4 = as + br - cq + dp,$$

於是 $|w_1|^2 + |w_2|^2 = L_1^2 + L_2^2 + L_3^2 + L_4^2$，得出

$$(a^2 + b^2 + c^2 + d^2)(p^2 + q^2 + r^2 + s^2) = L_1^2 + L_2^2 + L_3^2 + L_4^2.$$

每個 L_i 都是若干項之和，每項的形式為（a, b, c, d 中的一個字母）$\times$（p, q, r, s 中的一個字母），所以它對兩組變數分別都是線性（linear）的，符合題目要求。（答案並不唯一：改變任何 L_i 的正負號，或以不同方式選取 z_j，都會得出其他合用的組合。）

驗算

- 取 $(a, b, c, d) = (1, 2, 3, 4)$ 及 $(p, q, r, s) = (5, 6, 7, 8)$。左邊為 $30 \times 174 = 5220$。由公式得 $(L_1, L_2, L_3, L_4) = (-60, 12, 30, 24)$，而 $3600 + 144 + 900 + 576 = 5220$。
- 設 $c = d = r = s = 0$。則 $L_3 = L_4 = 0$，恆等式(identity)簡化為 $(a^2 + b^2)(p^2 + q^2) = (ap - bq)^2 + (aq + bp)^2$，即由 $|z_1 z_3| = |z_1||z_3|$ 得出的二平方和恆等式。
- 電腦驗算已就八個變數的 20,000 組隨機有理數取值，確認恆等式精確成立，並以數值方式確認了 $M(z_1, z_2)M(z_3, z_4) = M(w_1, w_2)$。

常見錯誤

- 相乘時忘記第二行的共軛，以致破壞了乘積的特殊形式。
- $(c + d\mathrm{i})(r - s\mathrm{i})$ 中的正負號出錯：$-ds\,\mathrm{i}^2$ 一項會變成 $+ds$。

STEP 之外

這就是歐拉(Euler)四平方和恆等式。矩陣 $M(z, w)$ 是哈密頓(Hamilton)四元數(quaternion)的一個具體模型：它們在乘法下封閉（closed），而行列式就是「長度」的平方，具有可乘性(multiplicative)。這個恆等式是拉格朗日(Lagrange)定理(每個正整數都是四個平方之和)證明中的關鍵一步，因為它把問題歸結為質數(prime)的情況。Davenport 的 *The Higher Arithmetic*（一本數論入門經典）涵蓋平方和的課題，而 Needham 的 *Visual Complex Analysis*（以幾何觀點講解複分析）則為二平方和的情況提供幾何直觀。

Beyond STEP 詳細解答：https://beyondstep.keithmcnulty.org/zh-hant/。解答文字採用 CC0 1.0；題目本身版權屬 Cambridge University Press & Assessment 所有（©），本文件不予轉載。由機器從英文翻譯而成；尚未經審閱。