詳細解答

STEP III 1990，第 3 題

純數學 • 群公理與共軛

> **STEP III 1990，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/90-s3-q3

關鍵思路

三個部分都只需用到羣公理（group axioms），而每一部分中有用的一步，都是把一個元素改寫成以另一個元素表示。階（order）為 2 的元素是它自己的逆元（inverse），這使 (i) 變成一行計算。在 (ii) 和 (iii) 中，所用的工具是共軛（*conjugation*）：$x \mapsto c^{-1}xc$ 保持乘積，所以它把冪映到冪。

全文中我們把 $x * y$ 寫作 xy，並以 e 表示單位元（identity）。

解答

第 (i) 部分

元素 x 的階為 2，當且僅當 $x \neq e$ 且 $x^2 = e$；第二個條件即是說 $x^{-1} = x$。所以

$$a^{-1} = a, \qquad b^{-1} = b, \qquad (ab)^{-1} = ab.$$

對任何羣元素，都有 $(ab)^{-1} = b^{-1}a^{-1}$，因為 $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = e$。因此

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba,$$

所以 a 與 b 可交換（commute）。

第 (ii) 部分

首先留意 dc 是 cd 的一個共軛元：

$$c^{-1}(cd)\,c = (c^{-1}c)\,dc = dc.$$

想一想 為甚麼寫成 $dc = c^{-1}(cd)c$ 對處理階有幫助？

因為共軛可以穿過冪。對任何 x 和任何正整數 n，

$$(c^{-1}xc)^n = (c^{-1}xc)(c^{-1}xc)\cdots(c^{-1}xc) = c^{-1}x^n c,$$

因為中間每一對相鄰的 $c\,c^{-1}$ 都互相抵消。取 $x = cd$，便得 $(dc)^n = c^{-1}(cd)^n c$。於是

$$(dc)^n = e \iff c^{-1}(cd)^n c = e \iff (cd)^n = cec^{-1} = e,$$

其中第二步是左乘 c 並右乘 c^{-1}（反方向則乘以 c^{-1} 和 c）。所以滿足 $(cd)^n = e$ 的正整數 n，正好就是滿足 $(dc)^n = e$ 的那些正整數。階就是這樣的 n 中最小的一個，所以 cd 與 dc 的階相同。若不存在這樣的 n，兩者的階都是無限，所以命題在這個情況下同樣成立。

第 (iii) 部分

已知 $c^{-1}bc = b^r$。對正整數 s，用 (ii) 中逐項相消（telescoping）的論證，可得

$$c^{-1}b^s c = (c^{-1}bc)^s = (b^r)^s = b^{sr}.$$

當 $s = 0$ 時同樣成立（兩邊都是 e）。當 s 為負數時，設 $s = -t$，其中 $t > 0$；則 $c^{-1}b^s c = (c^{-1}b^t c)^{-1}$，因為 $(c^{-1}b^t c)(c^{-1}b^{-t}c) = e$。所以

$$c^{-1}b^s c = (b^{tr})^{-1} = b^{-tr} = b^{sr}.$$

因此對每個整數 s，都有 $c^{-1}b^s c = b^{sr}$。

至於第二個結果，我們對 $n \geq 1$ 使用歸納法（induction），並同時處理所有整數 s。$n = 1$ 的情況就是剛才所證明的結果。假設 $c^{-n}b^s c^n = b^{sr^n}$ 對所有整數 s 成立。則

$$\begin{aligned} c^{-(n+1)}\, b^s\, c^{n+1} &= c^{-1}(c^{-n}b^s c^n)c \\ &= c^{-1}\, b^{sr^n}\, c \\ &= b^{(sr^n)r} = b^{sr^{n+1}}, \end{aligned}$$

其中最後一行用了第一個結果，並以整數 sr^n 代替 s。歸納法至此完成，所以 $c^{-n}b^s c^n = b^{sr^n}$ 對所有正整數 n 成立。

想一想 為甚麼我們要特地為負數 s 證明第一個結果？

若 r 是負數（例如在二面體羣（dihedral group）中 $c^{-1}bc = b^{-1}$），則即使 s 是正數，sr^n 也可能是負數，而歸納步驟正是以 sr^n 代替 s 來應用第一個結果。為所有整數 s 證明第一個結果，歸納法便不論 r 的正負都行得通。

驗算

用小的羣來測試。在正方形的對稱羣中，沿兩條對角線的反射及它們的乘積（旋轉半周）的階都是 2，而這兩個反射確實可交換，與 (i) 的預測一致。在 S_3 中，取 $c = (12)$ 和 $d = (13)$：則 cd 和 dc 就是那兩個 3-循環（3-cycle），階都是 3。至於 (iii)，在二面體羣中，反射 c 與旋轉 b 滿足 $c^{-1}bc = b^{-1}$，所以 $r = -1$，而公式預測 $c^{-n}b^s c^n = b^{(-1)^n s}$，這是對的：以同一個反射共軛兩次，等於甚麼也沒有做。我們亦用電腦驗證了全部三個命題，窮舉了 S_4 中所有合適的元素（就 (i) 而言還包括 S_5），以及模 13 之下由映射 $x \mapsto ux + v$ 所組成的羣。

常見錯誤

- 寫成 $(ab)^{-1} = a^{-1}b^{-1}$。次序是會倒轉的；正是這個倒轉令 (i) 得以成立。
- 在 (ii) 中，只證明 $(cd)^n = e \Rightarrow (dc)^n = e$。兩個方向都要證明（或利用對稱性：把 c 和 d 的角色互換），而階為無限的情況亦應提及。
- 在 (iii) 中，以三點省略號代替歸納法，為第二個結果寫出一個所謂的「證明」。

STEP 之外

映射 $x \mapsto c^{-1}xc$ 是這個羣的一個*自同構*（*automorphism*）：它是由 G 到自身的雙射（bijection），並且保持運算，所以它保持元素的階，並把冪映到冪。第 (iii) 部分是*半直積*（*semidirect products*）中的關鍵關係：由 b 和 c 生成並滿足 $c^{-1}bc = b^r$ 的羣，包括二面體羣（$r = -1$）以及模一個質數之下由映射 $x \mapsto ux + v$ 所組成的羣。Allenby 的 *Rings, Fields and Groups*（環、域與羣）對共軛及這些例子有仔細的闡述。

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。