詳細解答

STEP III 1988，第 9 題

純數學 • 群元素的階

> **STEP III 1988，第 9 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/88-s3-q9

關鍵思路

第 (i) 部分其實是帶餘除法（division algorithm）的變相應用：把 N 寫成 n 的倍數加上餘數，而 n 的最小性迫使餘數為零。第 (ii) 部分之所以成立，是因為以 g 作共軛（conjugation）會保持乘積，所以在一串共軛元素的乘積中，夾在中間的每一對 $g^{-1}g$ 都會互相抵消。在第 (iii) 部分，我們反覆以 g 作共軛；由於 $g^5 = e$，做五次之後 h 便回到自身，從而確定 h 的階（order）。

解答

第 (i) 部分

根據帶餘除法，可寫 $N = qn + r$，其中 q 為整數，且 $0 \leq r < n$。（這對任何整數 N 都成立，包括零和負整數。）於是，由於 $g^n = e$，

$$e = g^N = (g^n)^q g^r = e^q g^r = g^r.$$

假如 r 是正數，它便是一個小於 n 而又滿足 $g^r = e$ 的正整數，這與 $n = o(g)$ 是符合此條件的最小正整數這個定義矛盾。因此 $r = 0$，即 $N = qn$，故 n 整除 N。

第 (ii) 部分

$m = 0$：兩邊都等於 e。

$m \geq 1$：我們對 m 使用歸納法（induction）。$m = 1$ 的情況顯然成立。若 $gh^m g^{-1} =$

$(ghg^{-1})^m$，則

$$(ghg^{-1})^{m+1} = (ghg^{-1})^m\,(ghg^{-1}) = (gh^mg^{-1})(ghg^{-1})$$
$$= gh^m(g^{-1}g)hg^{-1} = gh^{m+1}g^{-1},$$

歸納法至此完成。（把乘積 $(ghg^{-1})(ghg^{-1})\cdots(ghg^{-1})$ 全部寫出來，便會逐項相消：中間的每一個 $g^{-1}g$ 都抵消掉。）

$m \le -1$：首先，ghg^{-1} 的逆元（inverse）是 $gh^{-1}g^{-1}$，因為

$$(ghg^{-1})(gh^{-1}g^{-1}) = gh(g^{-1}g)h^{-1}g^{-1} = ghh^{-1}g^{-1} = e.$$

現在寫 $m = -k$，其中 $k \ge 1$。以元素 h^{-1} 代替 h，套用正數情況的結果，得

$$gh^mg^{-1} = g(h^{-1})^kg^{-1} = (gh^{-1}g^{-1})^k = ((ghg^{-1})^{-1})^k = (ghg^{-1})^{-k} = (ghg^{-1})^m.$$

所以這個恆等式對每一個整數 m 都成立。

第 (iii) 部分

先用 $ghg^{-1} = h^2$，再用第 (ii) 部分並取 $m = 2$，

$$g^2hg^{-2} = g\,(ghg^{-1})\,g^{-1} = gh^2g^{-1} = (ghg^{-1})^2 = (h^2)^2 = h^4,$$

正如所求。

同樣的步驟在每一個階段都適用。我們斷言：對所有 $k \ge 0$，$g^khg^{-k} = h^{2^k}$。$k = 0$ 時這顯然成立；若它對 k 成立，則由第 (ii) 部分並取 $m = 2^k$，

$$g^{k+1}hg^{-(k+1)} = g\,(g^khg^{-k})\,g^{-1} = gh^{2^k}g^{-1} = (ghg^{-1})^{2^k} = (h^2)^{2^k} = h^{2^{k+1}}.$$

取 $k = 5$，並利用 $g^5 = e$（因此 $g^{-5} = e$ 亦成立），得

$$h = g^5hg^{-5} = h^{32}, \qquad \text{所以} \qquad h^{31} = e$$

（兩邊乘以 h^{-1} 即得）。

> ? **想一想** 我們知道 $h^{31} = e$。為甚麼由此可知 $o(h)$ 恰好是 31，而不僅僅是不超過 31？

由第 (i) 部分，$o(h)$ 整除 31。由於 31 是質數（prime），$o(h)$ 只能是 1 或 31。但 $o(h) = 1$ 即表示 $h = e$，而題目已說明並非如此。因此

$$o(h) = 31.$$

這樣的羣（group）確實存在，所以題目的條件並無矛盾。考慮 $\{0, 1, \ldots, 30\}$ 上的兩個置換（permutation）：$h(x) = x + 1$ 和 $g(x) = 2x$，運算皆以 31 為模。那麼 $g^5(x) = 32x = x$，而且 $ghg^{-1}(x) = 2(\frac{x}{2} + 1) = x + 2 = h^2(x)$，同時 h 的階確實是 31。

驗算

- 出現質數 31 是合理的：以 g 作共軛，對 h 的各次冪的作用就是「把指數乘以 2」，而加倍五次後必須回到起點，所以 $2^5 \equiv 1$（模 $o(h)$）。換句話說，$o(h)$ 整除 $2^5 - 1 = 31$。
- 我們以置換 $g(x) = 2x$ 和 $h(x) = x + 1$（模 31）作電腦驗算，確認了 $g^5 = e$、$ghg^{-1} = h^2$、$g^k h g^{-k} = h^{2^k}$（$k = 0, \ldots, 5$）以及 $o(h) = 31$。此外，亦在數百個隨機置換上，就 $-12 \leq m \leq 12$ 檢驗了 (i) 和 (ii)。

常見錯誤

- 在 (ii) 中只證明 $m \geq 1$ 的情況。題目說的是任何整數，所以 $m = 0$ 和負數 m 都需要各自的（簡短）論證。
- 直接由 $h^{31} = e$ 斷定 $o(h) = 31$。這只能得出 $o(h) \mid 31$；還需要用到 31 是質數以及 $h \neq e$ 這個條件。

STEP 之外

映射 $x \mapsto gxg^{-1}$ 是 G 的一個自同構（automorphism），即保持結構的雙射（bijection），而第 (ii) 部分正是這個事實的一個推論。第 (iii) 部分是半直積（semidirect product）的一個小例子：由 g 和 h 生成的羣的階是 $5 \times 31 = 155$，而它之所以存在，全賴 2 在模 31 之下的階是 5。這種構造在小階羣的分類中佔有核心地位。若想進一步了解階、共軛和拉格朗日定理（Lagrange's theorem），Allenby 的 *Rings, Fields and Groups*（環、域與羣）是很好的讀物。

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。