详细解答

STEP III 1988，第 9 题

纯数学 · 群元素的阶

> **STEP III 1988，第 9 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/88-s3-q9

关键思路

第 (i) 部分其实是带余除法（division algorithm）的变相应用：把 N 写成 n 的倍数加上余数，而 n 的最小性迫使余数为零。第 (ii) 部分之所以成立，是因为以 g 作共轭（conjugation）会保持乘积，所以在一串共轭元素的乘积中，夹在中间的每一对 $g^{-1}g$ 都会互相抵消。在第 (iii) 部分，我们反复以 g 作共轭；由于 $g^5 = e$，做五次之后 h 便回到自身，从而确定 h 的阶（order）。

解答

第 (i) 部分

根据带余除法，可写 $N = qn + r$，其中 q 为整数，且 $0 \le r < n$。（这对任何整数 N 都成立，包括零和负整数。）于是，由于 $g^n = e$，

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

假如 r 是正数，它便是一个小于 n 而又满足 $g^r = e$ 的正整数，这与 $n = o(g)$ 是符合此条件的最小正整数这个定义矛盾。因此 $r = 0$，即 $N = qn$，故 n 整除 N。

第 (ii) 部分

$m = 0$：两边都等于 e。

$m \ge 1$：我们对 m 使用归纳法（induction）。$m = 1$ 的情况显然成立。若 $gh^m g^{-1} =$

$(ghg^{-1})^m$，则

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

归纳法至此完成。（把乘积 $(ghg^{-1})(ghg^{-1})\cdots(ghg^{-1})$ 全部写出来，便会逐项相消：中间的每一个 $g^{-1}g$ 都抵消掉。）

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

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

现在写 $m = -k$，其中 $k \ge 1$。以元素 h^{-1} 代替 h，套用正数情况的结果，得

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

所以这个恒等式对每一个整数 m 都成立。

第 (iii) 部分

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

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

正如所求。

同样的步骤在每一个阶段都适用。我们断言：对所有 $k \ge 0$，$g^khg^{-k} = h^{2^k}$。$k = 0$ 时这显然成立；若它对 k 成立，则由第 (ii) 部分并取 $m = 2^k$，

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

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

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

（两边乘以 h^{-1} 即得）。

> **想一想** 我们知道 $h^{31} = e$。为甚么由此可知 $o(h)$ 恰好是 31，而不仅仅是不超过 31?

由第 (i) 部分，$o(h)$ 整除 31。由于 31 是质数（prime），$o(h)$ 只能是 1 或 31。但 $o(h) = 1$ 即表示 $h = e$，而题目已说明并非如此。因此

$$o(h) = 31.$$

这样的群（group）确实存在，所以题目的条件并无矛盾。考虑 $\{0, 1, \ldots, 30\}$ 上的两个置换（permutation）：$h(x) = x + 1$ 和 $g(x) = 2x$，运算皆以 31 为模。那么 $g^5(x) = 32x = x$，而且 $ghg^{-1}(x) = 2(\frac{x}{2} + 1) = x + 2 = h^2(x)$，同时 h 的阶确实是 31。

验算

- 出现质数 31 是合理的：以 g 作共轭，对 h 的各次幂的作用就是“把指数乘以 2”，而加倍五次后必须回到起点，所以 $2^5 \equiv 1$（模 $o(h)$）。换句话说，$o(h)$ 整除 $2^5 - 1 = 31$。
- 我们以置换 $g(x) = 2x$ 和 $h(x) = x + 1$（模 31）作电脑验算，确认了 $g^5 = e$、$ghg^{-1} = h^2$、$g^k h g^{-k} = h^{2^k}$（$k = 0, \ldots, 5$）以及 $o(h) = 31$。此外，亦在数百个随机置换上，就 $-12 \le m \le 12$ 检验了 (i) 和 (ii)。

常见错误

- 在 (ii) 中只证明 $m \ge 1$ 的情况。题目说的是*任何整数*，所以 $m = 0$ 和负数 m 都需要各自的（简短）论证。
- 直接由 $h^{31} = e$ 断定 $o(h) = 31$。这只能得出 $o(h) \mid 31$；还需要用到 31 是质数以及 $h \neq e$ 这个条件。

STEP 之外

映射 $x \mapsto gxg^{-1}$ 是 G 的一个*自同构*（automorphism），即保持结构的双射（bijection），而第 (ii) 部分正是这个事实的一个推论。第 (iii) 部分是*半直积*（semidirect product）的一个小例子：由 g 和 h 生成的群的阶是 $5 \times 31 = 155$，而它之所以存在，全赖 2 在模 31 之下的阶是 5。这种构造在小阶群的分类中占有核心地位。若想进一步了解阶、共轭和拉格朗日定理（Lagrange's theorem），Allenby 的 *Rings, Fields and Groups*（环、域与群）是很好的读物。

Beyond STEP 详细解答：https://beyondstep.keithmcnulty.org/zh-hans/。解答文字采用 CC0 1.0；题目本身版权属 Cambridge University Press & Assessment 所有（©），本文件不予转载。由机器从英文翻译而成；尚未经审阅。