详细解答

STEP III 1990，第 3 题

纯数学 · 群公理与共轭

> **STEP III 1990，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/90-s3-q3

关键思路

三个部分都只需用到群公理（group axioms），而每一部分中有用的一步，都是把一个元素改写成以另一个元素表示。阶（order）为 2 的元素是它自己的逆元（inverse），这使 (i) 变成一行计算。在 (ii) 和 (iii) 中，所用的工具是*共轭*（*conjugation*）：$x \mapsto c^{-1}xc$ 保持乘积，所以它把幂映到幂。

全文中我们把 $x * y$ 写作 xy，并以 e 表示单位元（identity）。

解答

第 (i) 部分

元素 x 的阶为 2，当且仅当 $x \neq e$ 且 $x^2 = e$；第二个条件即是说 $x^{-1} = x$。所以

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

对任何群元素，都有 $(ab)^{-1} = b^{-1}a^{-1}$，因为 $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = e$。因此

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

所以 a 与 b 可交换（commute）。

第 (ii) 部分

首先留意 dc 是 cd 的一个共轭元：

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

想一想 为甚么写成 $dc = c^{-1}(cd)c$ 对处理阶有帮助?

因为共轭可以穿过幂。对任何 x 和任何正整数 n，

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

因为中间每一对相邻的 $c\,c^{-1}$ 都互相抵消。取 $x = cd$，便得 $(dc)^n = c^{-1}(cd)^n c$。于是

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

其中第二步是左乘 c 并右乘 c^{-1}（反方向则乘以 c^{-1} 和 c）。所以满足 $(cd)^n = e$ 的正整数 n，正好就是满足 $(dc)^n = e$ 的那些正整数。阶就是这样的 n 中最小的一个，所以 cd 与 dc 的阶相同。若不存在这样的 n，两者的阶都是无限，所以命题在这个情况下同样成立。

第 (iii) 部分

已知 $c^{-1}bc = b^r$。对正整数 s，用 (ii) 中逐项相消（telescoping）的论证，可得

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

当 $s = 0$ 时同样成立（两边都是 e）。当 s 为负数时，设 $s = -t$，其中 $t > 0$；则 $c^{-1}b^s c = (c^{-1}b^t c)^{-1}$，因为 $(c^{-1}b^t c)(c^{-1}b^{-t}c) = e$。所以

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

因此对每个整数 s，都有 $c^{-1}b^s c = b^{sr}$。

至于第二个结果，我们对 $n \geq 1$ 使用归纳法（induction），并同时处理所有整数 s。$n = 1$ 的情况就是刚才所证明的结果。假设 $c^{-n}b^s c^n = b^{sr^n}$ 对所有整数 s 成立。则

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

其中最后一行用了第一个结果，并以整数 sr^n 代替 s。归纳法至此完成，所以 $c^{-n}b^s c^n = b^{sr^n}$ 对所有正整数 n 成立。

想一想 为甚么我们要特地为负数 s 证明第一个结果?

若 r 是负数（例如在二面体群（dihedral group）中 $c^{-1}bc = b^{-1}$），则即使 s 是正数，sr^n 也可能是负数，而归纳步骤正是以 sr^n 代替 s 来应用第一个结果。为所有整数 s 证明第一个结果，归纳法便不论 r 的正负都行得通。

验算

用小的群来测试。在正方形的对称群中，沿两条对角线的反射及它们的乘积（旋转半周）的阶都是 2，而这两个反射确实可交换，与 (i) 的预测一致。在 S_3 中，取 $c = (12)$ 和 $d = (13)$：则 cd 和 dc 就是那两个 3-循环（3-cycle），阶都是 3。至于 (iii)，在二面体群中，反射 c 与旋转 b 满足 $c^{-1}bc = b^{-1}$，所以 $r = -1$，而公式预测 $c^{-n}b^s c^n = b^{(-1)^n s}$，这是对的：以同一个反射共轭两次，等于甚么也没有做。我们亦用电脑验证了全部三个命题，穷举了 S_4 中所有合适的元素（就 (i) 而言还包括 S_5），以及模 13 之下由映射 $x \mapsto ux + v$ 所组成的群。

常见错误

- 写成 $(ab)^{-1} = a^{-1}b^{-1}$。次序是会倒转的；正是这个倒转令 (i) 得以成立。
- 在 (ii) 中，只证明 $(cd)^n = e \Rightarrow (dc)^n = e$。两个方向都要证明（或利用对称性：把 c 和 d 的角色互换），而阶为无限的情况亦应提及。
- 在 (iii) 中，以三点省略号代替归纳法，为第二个结果写出一个所谓的“证明”。

STEP 之外

映射 $x \mapsto c^{-1}xc$ 是这个群的一个*自同构*（*automorphism*）：它是由 G 到自身的双射（bijection），并且保持运算，所以它保持元素的阶，并把幂映到幂。第 (iii) 部分是*半直积*（*semidirect products*）中的关键关系：由 b 和 c 生成并满足 $c^{-1}bc = b^r$ 的群，包括二面体群（$r = -1$）以及模一个质数之下由映射 $x \mapsto ux + v$ 所组成的群。Allenby 的 *Rings, Fields and Groups*（环、域与群）对共轭及这些例子有仔细的阐述。

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。