详细解答

STEP III 1994，第 7 题

纯数学 · 群同构

STEP III 1994，第 7 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/94-s3-q7

关键思路

两个群（group）要同构（isomorphic），就必须共有同构映射（isomorphism）所保持的每一项结构性质。其中最有用的两项，是各元素的阶（order）的清单，以及该群是否可交换（commutative，即阿贝尔群，abelian）。只要列出各元素的阶，已足以把 S_3 和 Z_6 区分开来。要证明两个群确实同构，我们就写出一个明确的双射（bijection），并验证它与运算相容。最后一部分归结为交换性：凡是由复数组成的群都是阿贝尔群，而 S_3 不是。

解答

S_3 和 Z_6 的元素

把三件物件标记为 $1,2,3$，并采用循环记法（cycle notation），由右至左复合，即 $\sigma\tau$ 表示“先做 τ，再做 σ”。六个置换（permutation）列于下表。

S_3 的元素	e	(12)	(13)	(23)	(123)	(132)
阶	1	2	2	2	3	3

对换（transposition）把两件物件互换，做两次便一切还原，所以它的阶是 2。像 (123) 这样的 3-循环把 $1 \to 2 \to 3 \to 1$，要施行三次才能使每件物件回到原位，所以它的阶是 3。

在 $Z_6 = \{0,1,2,3,4,5\}$ 中，单位元（identity）是 0，而 a 的阶是满足 $na \equiv 0 \pmod 6$ 的最小 $n \geq 1$，即 $6/\gcd(a,6)$。

Z_6 的元素	0	1	2	3	4	5
阶	1	6	3	2	3	6

例如，$4+4=8\equiv 2$ 而 $4+4+4=12\equiv 0$，所以 4 的阶是 3。

S_3 和 Z_6 同构吗?

不同构。同构映射 θ 保持元素的阶：若 g 的阶是 n，则 $\theta(g)^k=\theta(g^k)$，而由于 θ 是单射（injective），这个元素是单位元当且仅当 g^k 是单位元。因此，同构的群中，每一种阶的元素数目都相同。但 Z_6 有两个阶为 6 的元素，S_3 却一个也没有，所以两者并不同构。（两者在阶为 2 的元素上也有分别：S_3 有三个，Z_6 只有一个。）

还有第二个理由，我们在最后会再用到。Z_6 是阿贝尔群，因为加法可交换。S_3 则不是：

$$(12)(13)=(132),\qquad (13)(12)=(123).$$

就第一个乘积而言，(13) 把 $1\to 3$，然后 (12) 保持 3 不变，所以 $1\to 3$。同理 $3\to 2$ 及 $2\to 1$。同构映射把可交换的一对元素映到可交换的一对元素，所以非阿贝尔群不可能与阿贝尔群同构。

C_6 与 Z_6 同构

定义 $\phi: Z_6\to C_6$ 为 $\phi(k)=\alpha^k$，其中 $k=0,1,\dots,5$。

- 双射。当 $k=0,\dots,5$ 时，各数 $\alpha^k=\mathrm{e}^{\mathrm{i}k\pi/3}$ 的辐角（argument）为 $0,\frac{\pi}{3},\dots,\frac{5\pi}{3}$。这些是 $[0,2\pi)$ 内互不相同的角，所以这六个值是单位圆上互不相同的点。因此 ϕ 是单射，从而是两个大小同为 6 的集合之间的双射。
- 运算。设 $a,b\in Z_6$，并写 $a+b=6q+r$，其中 $r=(a+b)\bmod 6$。由于 $\alpha^6=\mathrm{e}^{2\pi\mathrm{i}}=1$，

$$\phi(a)\,\phi(b)=\alpha^a\alpha^b=\alpha^{a+b}=(\alpha^6)^q\alpha^r=\alpha^r=\phi\big((a+b)\bmod 6\big).$$

所以 ϕ 把模 6 加法变成复数乘法，它是一个同构映射。因此 $C_6\cong Z_6$。作为核对，α 和 α^5（即 1 和 5 的像）的阶是 6，α^2 和 α^4 的阶是 3，而 $\alpha^3=-1$ 的阶是 2，与 Z_6 的表吻合。

C 有与 S_3 同构的子群吗?

> **想一想** 所有由复数组成的群都共有甚么性质?

它们全都是阿贝尔群。$(\mathbb{C},+)$ 的子群（subgroup）H 是阿贝尔群，因为对所有复数 z,w 都有 $z+w=w+z$。非零复数在乘法下所成的群的子群 H 是阿贝尔群，因为 $zw=wz$。子群沿用大群的同一运算，所以继承了交换性。

现在假设某个这样的 H 有同构映射 $\theta: S_3\to H$。把它应用于上面那对不可交换的元素。由于 H 是阿贝尔群，

$$\theta\big((12)(13)\big)=\theta(12)\,\theta(13)=\theta(13)\,\theta(12)=\theta\big((13)(12)\big),$$

这里以乘法形式书写（若是加法的情况，把乘积换成和即可）。因为 θ 是单射，由此会得出 $(12)(13) = (13)(12)$，而这是错的。所以复数的子群，不论是加法的还是乘法的，都**没有**一个与 S_3 同构。

验算

- 在每个群中，元素的阶都整除 6（拉格朗日定理，Lagrange's theorem）：S_3 中是 $1, 2, 3$，Z_6 中是 $1, 2, 3, 6$。
- 我们用电脑重新计算了 S_3、Z_6 和 C_6 中每个元素的阶，确认了 $(12)(13) \neq (13)(12)$，并对全部 36 对 (a, b) 以数值方法检验了 $\alpha^{(a+b) \bmod 6} = \alpha^a \alpha^b$，误差在 10^{-12} 以内。

常见错误

- 说“两者都有六个元素，所以同构”。大小相同是必要条件，但远远不是充分条件。
- 说 S_3 中阶为 3 的元素是 (12) 和 (13)。对换的阶是 2；只有 3-循环的阶才是 3。
- 在最后一部分，只排除了有限的乘法子群（单位根，roots of unity）。交换性的论证一次过涵盖所有子群，不论有限还是无限、加法还是乘法。

STEP 之外

这道题讲的是不变量（invariant）：同构的群必须共有的性质，例如元素的阶和交换性。事实上，每个阶为 6 的群都与 Z_6 或 S_3 其中之一同构。更一般地，非零复数在乘法下所成的群的任何有限子群都是循环群（cyclic group），所以它是一个由单位根组成的群。这两个结果，你在第一门群论课程的初段就会遇到。Allenby 的 *Rings, Fields and Groups*（环、域与群）写得平易近人，很适合用来阅读这些内容。

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。