详细解答

STEP III 1987，第 9 题

纯数学 · 群的直积

> **STEP III 1987，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/87-s3-q9

关键思路

$G \times H$ 中的一切运算都是逐个坐标进行的，所以每一条群公理（group axiom）以及 $G \times H$ 的每一项性质，都归结为 G 和 H 各自具备同样的性质。至于判断真假的部分，答“真”需要给出一般的证明，而答“假”则只需找出一个确凿的障碍。同构（isomorphic）的群，凡是单靠乘法就能描述的性质都完全一致，例如群的大小和各元素的阶（order）。所以我们就比较这些性质。

解答

以下一律以 e_G 和 e_H 表示 G 和 H 的单位元（identity），并以 g^{-1} 和 h^{-1} 表示在 G 和 H 中的逆元（inverse）。

$G \times H$ 是一个群

我们逐一检查四条公理。

封闭性（*closure*）。若 $g_1, g_2 \in G$ 且 $h_1, h_2 \in H$，则 $g_1 * g_2 \in G$ 且 $h_1 \circ h_2 \in H$，因为 G 和 H 都是封闭的。所以 $(g_1, h_1)(g_2, h_2) = (g_1 * g_2,\ h_1 \circ h_2) \in G \times H$。

结合律（*associativity*）。对任意三个元素，

$$\begin{aligned}((g_1, h_1)(g_2, h_2))(g_3, h_3) &= ((g_1 * g_2) * g_3,\ (h_1 \circ h_2) \circ h_3) \\ &= (g_1 * (g_2 * g_3),\ h_1 \circ (h_2 \circ h_3)) \\ &= (g_1, h_1)((g_2, h_2)(g_3, h_3)),\end{aligned}$$

其中中间一步用到 G 和 H 中的结合律。

单位元。序偶 (e_G, e_H) 满足

$$(e_G, e_H)(g,h) = (e_G * g,\ e_H \circ h) = (g,h),$$

同理 $(g,h)(e_G,e_H) = (g,h)$。所以它是单位元。

逆元。给定 (g,h)，序偶 (g^{-1},h^{-1}) 属于 $G \times H$，并且

$$(g,h)(g^{-1},h^{-1}) = (g * g^{-1},\ h \circ h^{-1}) = (e_G, e_H),$$

而次序倒过来相乘，所得的积同样是 (e_G,e_H)。所以每个元素都有逆元。

四条公理全部成立，所以 $G \times H$ 在这个乘法之下是一个群。

第 (i) 部分：真

若 G 和 H 是阿贝尔群（*abelian group*），则 $G \times H$ 也是。对任意两个元素，

$$(g_1,h_1)(g_2,h_2) = (g_1 * g_2,\ h_1 \circ h_2) = (g_2 * g_1,\ h_2 \circ h_1) = (g_2,h_2)(g_1,h_1),$$

这里用到 G 和 H 中的交换律（commutativity）。

若 $G \times H$ 是阿贝尔群，则 G 和 H 也是。任取 $g_1, g_2 \in G$。由于 $G \times H$ 是阿贝尔群，

$$(g_1 * g_2,\ e_H) = (g_1,e_H)(g_2,e_H) = (g_2,e_H)(g_1,e_H) = (g_2 * g_1,\ e_H).$$

两个序偶相等，其第一个坐标必须相等，所以 $g_1 * g_2 = g_2 * g_1$，即 G 是阿贝尔群。以同样方法使用序偶 (e_G,h_1) 和 (e_G,h_2)，可证明 H 是阿贝尔群。

? **想一想** 为甚么在第二个方向的证明中需要用到单位元 e_H?

我们需要某个第二坐标，才能由 g_1 和 g_2 造出 $G \times H$ 的元素。任何固定的 $h \in H$ 都可以，因为比较时只有第一个坐标起作用。群必定含有单位元，所以 e_H 是一个稳妥的选择，我们确知它存在。

第 (ii) 部分：真

设 $\widetilde{G} = \{(g,e_H) : g \in G\}$，并定义 $\phi\colon G \to \widetilde{G}$ 为 $\phi(g) = (g,e_H)$。

$\widetilde{G}$ 是 $G \times H$ 的子群（subgroup）。它包含单位元 (e_G,e_H)。它对乘积封闭，因为 $(g_1,e_H)(g_2,e_H) = (g_1 * g_2,e_H)$。它对取逆元封闭，因为 $(g,e_H)^{-1} = (g^{-1},e_H)$。

ϕ 是一个同构（isomorphism）。按定义，它映满 $\widetilde{G}$（即满射，onto）。它是一对一的（one-to-one），因为 $(g_1,e_H) = (g_2,e_H)$ 必然推出 $g_1 = g_2$。它保持运算，因为

$$\phi(g_1 * g_2) = (g_1 * g_2,\ e_H) = (g_1,e_H)(g_2,e_H) = \phi(g_1)\phi(g_2).$$

所以 $G \times H$ 包含子群 $\widetilde{G}$，而它与 G 同构。

第 (iii) 部分：假

把两个群都写成加法形式：$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$，运算为模 n 加法。在 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 中，每个元素 $x = (a, b)$ 都满足

$$x + x = (2a, 2b) = (0, 0),$$

所以每个元素的阶都是 1 或 2。相反，在 $\mathbb{Z}_4$ 中，$1 + 1 = 2 \neq 0$，所以 1 的阶是 4。

假设存在同构 $\phi\colon \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$。那么

$$\phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) = (0, 0) = \phi(0),$$

因为由上面的计算可知 $\phi(1) + \phi(1) = (0, 0)$。最后一个等号成立，是因为同构把单位元映到单位元。于是 $\phi(2) = \phi(0)$ 而 $2 \neq 0$，所以 ϕ 不是一对一的，这就产生矛盾。因此 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 与 $\mathbb{Z}_4$ 不同构。（简而言之，$\mathbb{Z}_4$ 是循环群（cyclic group），而 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 不是。）

第 (iv) 部分：假

同构是双射（bijection），所以同构的群有相同数目的元素。现在 $|S_n| = n!$，因为 n 件物件共有 $n!$ 种排列；而 $|G \times H| = |G|\,|H|$，因为每个序偶都是由自由选取的 g 和 h 组成。所以

$$|S_2 \times S_3| = 2! \times 3! = 12, \qquad |S_6| = 6! = 720.$$

两者大小不同，所以 $S_2 \times S_3$ 与 S_6 不同构。

验算

- 对一些细小的例子（例如 $\mathbb{Z}_2 \times \mathbb{Z}_3$、$\mathbb{Z}_2 \times S_3$、$S_3 \times S_3$ 和 $S_2 \times S_3$）逐一穷举检查，可见这个积满足全部四条公理，单位元为 (e_G, e_H)。当且仅当两个因子都是阿贝尔群时，它才是阿贝尔群，而 $g \mapsto (g, e_H)$ 是一个单射（injective）同态（homomorphism）。
- $\mathbb{Z}_2 \times \mathbb{Z}_2$ 中各元素的阶是 $1, 2, 2, 2$，而 $\mathbb{Z}_4$ 中则是 $1, 2, 4, 4$，所以这两个群确实不同。
- 列出 $S_2 \times S_3$ 的元素，共有 12 个，而 S_6 则有 720 个。

常见错误

- 在 (i) 中只证明了“当且仅当”的其中一个方向。逆命题（converse）才是需要技巧的部分，要把 e_H 放在第二个坐标。
- 在 (ii) 中说“G 是 $G \times H$ 的子群”。严格来说，G 连 $G \times H$ 的子集也不是。真正的子群是 $G \times \{e_H\}$，它与 G 同构。

► 在 (iii) 中指出两个群的阶都是 4 便就此打住。大小相等是同构的必要条件，但并非充分条件，所以我们需要找出一个能区分这两个群的性质。

STEP 之外

这就是*直积*（direct product）的构造，是由旧群造出新群的最简单方法。大学第一门群论课的一个重要结果是：每个有限阿贝尔群都是循环群的直积。与此相关的一个事实是：$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ 当且仅当 $\gcd(m,n) = 1$，这正是中国剩余定理（Chinese remainder theorem）在群论中的面貌。第 (iii) 部分就是这个结论不成立的最小例子。想了解更多，可参阅 Allenby 的 *Rings, Fields and Groups*（环、域与群）。

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。