詳細解答

STEP III 1987，第 9 題

純數學 • 群的直積

> **STEP III 1987，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/87-s3-q9

關鍵思路

$G \times H$ 中的一切運算都是逐個坐標進行的，所以每一條羣公理(group axiom)以及 $G \times H$ 的每一項性質，都歸結為 G 和 H 各自具備同樣的性質。至於判斷真假的部分，答「真」需要給出一般的證明，而答「假」則只需找出一個確鑿的障礙。同構（isomorphic）的羣，凡是單靠乘法就能描述的性質都完全一致，例如羣的大小和各元素的階（order）。所以我們就比較這些性質。

解答

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

$G \times H$ 是一個羣

我們逐一檢查四條公理。

封閉性（*closure*）。若 $g_1, g_2 \in G$ 且 $h_1, h_2 \in H$，則 $g_1 * g_2 \in G$ 且 $h_1 \circ h_2 \in H$，因為 G 和 H 都是封閉的。所以 $(g_1, h_1)(g_2, h_2) = (g_1 * g_2,\ h_1 \circ h_2) \in G \times H$。

結合律（*associativity*）。對任意三個元素，

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

其中中間一步用到 G 和 H 中的結合律。

單位元。序偶 (e_G, e_H) 滿足

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

同理 $(g,h)(e_G,e_H) = (g,h)$。所以它是單位元。

逆元。給定 (g,h)，序偶 (g^{-1},h^{-1}) 屬於 $G \times H$，並且

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

而次序倒過來相乘，所得的積同樣是 (e_G,e_H)。所以每個元素都有逆元。

四條公理全部成立，所以 $G \times H$ 在這個乘法之下是一個羣。

第 (i) 部分：真

若 G 和 H 是阿貝爾羣（*abelian group*），則 $G \times H$ 也是。對任意兩個元素，

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

這裏用到 G 和 H 中的交換律（commutativity）。

若 $G \times H$ 是阿貝爾羣，則 G 和 H 也是。任取 $g_1, g_2 \in G$。由於 $G \times H$ 是阿貝爾羣，

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

兩個序偶相等，其第一個坐標必須相等，所以 $g_1 * g_2 = g_2 * g_1$，即 G 是阿貝爾羣。以同樣方法使用序偶 (e_G,h_1) 和 (e_G,h_2)，可證明 H 是阿貝爾羣。

想一想 為甚麼在第二個方向的證明中需要用到單位元 e_H？

我們需要某個第二坐標，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，因為比較時只有第一個坐標起作用。羣必定含有單位元，所以 e_H 是一個穩妥的選擇，我們確知它存在。

第 (ii) 部分：真

設 $\widetilde{G} = \{(g,e_H) : g \in G\}$，並定義 $\phi\colon G \to \widetilde{G}$ 為 $\phi(g) = (g,e_H)$。

$\widetilde{G}$ 是 $G \times H$ 的子羣（subgroup）。它包含單位元 (e_G,e_H)。它對乘積封閉，因為 $(g_1,e_H)(g_2,e_H) = (g_1 * g_2, e_H)$。它對取逆元封閉，因為 $(g,e_H)^{-1} = (g^{-1},e_H)$。

ϕ 是一個同構（isomorphism）。按定義，它映滿 $\widetilde{G}$（即滿射，onto）。它是一對一的（one-to-one），因為 $(g_1,e_H) = (g_2,e_H)$ 必然推出 $g_1 = g_2$。它保持運算，因為

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

所以 $G \times H$ 包含子羣 $\widetilde{G}$，而它與 G 同構。

第 (iii) 部分：假

把兩個羣都寫成加法形式：$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$，運算為模 n 加法。在 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 中，每個元素 $x = (a, b)$ 都滿足

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

所以每個元素的階都是 1 或 2。相反，在 $\mathbb{Z}_4$ 中，$1 + 1 = 2 \neq 0$，所以 1 的階是 4。

假設存在同構 $\phi\colon \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$。那麼

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

因為由上面的計算可知 $\phi(1) + \phi(1) = (0, 0)$。最後一個等號成立，是因為同構把單位元映到單位元。於是 $\phi(2) = \phi(0)$ 而 $2 \neq 0$，所以 ϕ 不是一對一的，這就產生矛盾。因此 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 與 $\mathbb{Z}_4$ 不同構。（簡而言之，$\mathbb{Z}_4$ 是循環羣（cyclic group），而 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 不是。）

第 (iv) 部分：假

同構是雙射（bijection），所以同構的羣有相同數目的元素。現在 $|S_n| = n!$，因為 n 件物件共有 $n!$ 種排列；而 $|G \times H| = |G|\,|H|$，因為每個序偶都是由自由選取的 g 和 h 組成。所以

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

兩者大小不同，所以 $S_2 \times S_3$ 與 S_6 不同構。

驗算

- 對一些細小的例子（例如 $\mathbb{Z}_2 \times \mathbb{Z}_3$、$\mathbb{Z}_2 \times S_3$、$S_3 \times S_3$ 和 $S_2 \times S_3$）逐一窮舉檢查，可見這個積滿足全部四條公理，單位元為 (e_G, e_H)。當且僅當兩個因子都是阿貝爾羣時，它才是阿貝爾羣，而 $g \mapsto (g, e_H)$ 是一個單射（injective）同態（homomorphism）。
- $\mathbb{Z}_2 \times \mathbb{Z}_2$ 中各元素的階是 $1, 2, 2, 2$，而 $\mathbb{Z}_4$ 中則是 $1, 2, 4, 4$，所以這兩個羣確實不同。
- 列出 $S_2 \times S_3$ 的元素，共有 12 個，而 S_6 則有 720 個。

常見錯誤

- 在 (i) 中只證明了「當且僅當」的其中一個方向。逆命題（converse）才是需要技巧的部分，要把 e_H 放在第二個坐標。
- 在 (ii) 中說「G 是 $G \times H$ 的子羣」。嚴格來說，G 連 $G \times H$ 的子集也不是。真正的子羣是 $G \times \{e_H\}$，它與 G 同構。

▶ 在 (iii) 中指出兩個羣的階都是 4 便就此打住。大小相等是同構的必要條件，但並非充分條件，所以我們需要找出一個能區分這兩個羣的性質。

STEP 之外

這就是*直積*（direct product）的構造，是由舊羣造出新羣的最簡單方法。大學第一門羣論課的一個重要結果是：每個有限阿貝爾羣都是循環羣的直積。與此相關的一個事實是：$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ 當且僅當 $\gcd(m,n) = 1$，這正是中國剩餘定理（Chinese remainder theorem）在羣論中的面貌。第 (iii) 部分就是這個結論不成立的最小例子。想了解更多，可參閱 Allenby 的 *Rings, Fields and Groups*（環、域與羣）。

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。