解答例

STEP III 1987、第 9 問

純粋数学 ・ 群の直積

> **STEP III 1987、問 9**
>
> 先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：
>
> step.maths.org/questions/87-s3-q9

鍵となる考え方

$G \times H$ ではすべての演算が成分ごとに行われる。したがって、各群の公理（group axiom）や $G \times H$ の各性質は、G と H それぞれにおける同じ性質に帰着する。真偽を問う小問では、「真」と答えるには一般的な証明が必要であり、「偽」と答えるには確かな反例となる障害が一つあれば十分である。同型（isomorphic）な群は、元の個数や元の位数（order）など、乗法だけを用いて記述できるあらゆる性質が一致する。そこで、それらを比較する。

解答

以下を通じて、e_G と e_H はそれぞれ G と H の単位元（identity）を表し、G と H における逆元（inverse）を g^{-1}、h^{-1} と書く。

$G \times H$ は群である

四つの公理を確かめる。

閉性（*closure*）。$g_1, g_2 \in G$ かつ $h_1, h_2 \in H$ ならば、G と H は閉じているので、$g_1 * g_2 \in G$ かつ $h_1 \circ h_2 \in H$ である。よって $(g_1, h_1)(g_2, h_2) = (g_1 * g_2,\, h_1 \circ h_2) \in G \times H$ である。

結合法則（*associativity*）。任意の三つの元に対して

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

が成り立つ。ここで中央の等号では、G と H における結合法則を用いた。

単位元。 組 (e_G, e_H) は

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

を満たし、同様に $(g,h)(e_G, e_H) = (g,h)$ も満たす。よってこれは単位元である。

逆元。 (g,h) が与えられたとき、組 (g^{-1}, h^{-1}) は $G \times H$ に属し、

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

であり、逆順の積も (e_G, e_H) となる。よってすべての元は逆元をもつ。

四つの公理がすべて成り立つので、$G \times H$ はこの乗法に関して群（group）である。

小問 (i)：真

G と H が可換ならば、$G \times H$ も可換である。 任意の二つの元に対して、G と H における可換性を用いると

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

となる。

$G \times H$ が可換ならば、G と H も可換である。 任意の $g_1, g_2 \in G$ をとる。$G \times H$ は可換（abelian）であるから

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

順序対（ordered pair）が等しいのは第 1 成分が等しいときに限るから、$g_1 * g_2 = g_2 * g_1$ であり、G は可換である。組 (e_G, h_1) と (e_G, h_2) を同様に用いれば、H が可換であることがわかる。

> **考えてみよう** 逆向きの証明で、なぜ単位元 e_H が必要なのだろうか。

g_1 と g_2 から $G \times H$ の元をつくるには、何らかの第 2 成分が必要である。比較で問題になるのは第 1 成分だけなので、固定した $h \in H$ であれば何でもよい。群には必ず単位元が含まれるので、e_H は存在が保証された安全な選択である。

小問 (ii)：真

$\widetilde{G} = \{(g, e_H) : g \in G\}$ とおき、$\phi\colon G \to \widetilde{G}$ を $\phi(g) = (g, e_H)$ で定める。

$\widetilde{G}$ は $G \times H$ の部分群（subgroup）である。実際、単位元 (e_G, e_H) を含む。$(g_1, e_H)(g_2, e_H) = (g_1 * g_2, e_H)$ であるから積について閉じている。$(g, e_H)^{-1} = (g^{-1}, e_H)$ であるから逆元について閉じている。

ϕ は同型写像（isomorphism）である。定義により $\widetilde{G}$ への全射（onto）である。$(g_1, e_H) = (g_2, e_H)$ ならば $g_1 = g_2$ となるから単射（one-to-one）である。また

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

であるから演算を保つ。よって $G \times H$ は G と同型な部分群 $\widetilde{G}$ を含む。

小問 (iii)：偽

両方の群を加法的に表す：$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ は n を法とする加法に関する群である。$\mathbb{Z}_2 \times \mathbb{Z}_2$ では、すべての元 $x = (a, b)$ が

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

を満たすので、すべての元の位数は 1 または 2 である。一方 $\mathbb{Z}_4$ では $1 + 1 = 2 \neq 0$ であるから、1 の位数は 4 である。

同型写像 $\phi\colon \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ が存在したと仮定する。すると

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

となる。ここで、上の計算により $\phi(1) + \phi(1) = (0, 0)$ である。最後の等号は、同型写像が単位元を単位元に写すことによる。こうして $2 \neq 0$ でありながら $\phi(2) = \phi(0)$ となり、ϕ は単射でなく、矛盾である。したがって $\mathbb{Z}_2 \times \mathbb{Z}_2$ は $\mathbb{Z}_4$ と同型**ではない**。（要するに、$\mathbb{Z}_4$ は巡回群（cyclic group）であるが、$\mathbb{Z}_2 \times \mathbb{Z}_2$ はそうではない。）

小問 (iv)：偽

同型写像は全単射（bijection）であるから、同型な群は元の個数が等しい。n 個のものの並べ方は $n!$ 通りあるので $|S_n| = n!$ であり、各組は g と h を自由に選んで得られるので $|G \times H| = |G|\,|H|$ である。よって

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

これらの大きさは異なるので、$S_2 \times S_3$ は S_6 と同型**ではない**。

検算

- 小さな例（$\mathbb{Z}_2 \times \mathbb{Z}_3$、$\mathbb{Z}_2 \times S_3$、$S_3 \times S_3$、$S_2 \times S_3$ など）で総当たりで確かめると、直積は単位元 (e_G, e_H) のもとで四つの公理をすべて満たす。直積が可換となるのは両方の因子が可換であるときに限り、$g \mapsto (g, e_H)$ は単射な準同型写像（homomorphism）である。

- $\mathbb{Z}_2 \times \mathbb{Z}_2$ の元の位数は $1, 2, 2, 2$ であり、$\mathbb{Z}_4$ では $1, 2, 4, 4$ であるから、二つの群は確かに異なる。
- $S_2 \times S_3$ の元を列挙すると 12 個であり、S_6 の 720 個とは異なる。

よくある間違い

- (i) の「必要十分」の一方向だけを証明してしまう。逆向きこそ、第 2 成分に e_H を置く工夫が必要な部分である。
- (ii) で「G は $G \times H$ の部分群である」と述べてしまう。厳密には、G は $G \times H$ の部分集合ですらない。部分群は $G \times \{e_H\}$ であり、これが G と**同型**なのである。
- (iii) で、両方の群の位数がともに 4 であることを指摘して終わりにしてしまう。大きさが等しいことは同型であるための必要条件であって十分条件ではないので、二つの群を区別する性質が必要である。

STEP のその先へ

これは**直積**（direct product）という構成であり、既存の群から新しい群をつくる最も単純な方法である。群論の最初の講義における主要な結果の一つは、すべての有限可換群が巡回群の直積であるというものである。関連する事実として、$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ となるのは $\gcd(m, n) = 1$ のときに限る。これは中国剰余定理（Chinese remainder theorem）の群論的な側面である。小問 (iii) は、これが成り立たない最小の例である。さらに詳しくは、Allenby, *Rings, Fields and Groups*（環・体・群の入門書）を参照のこと。

Beyond STEP 解答集：https://beyondstep.keithmcnulty.org/ja/。解答本文は CC0 1.0 である。問題そのものは © Cambridge University Press & Assessment に帰属し、ここには掲載していない。英語版から機械翻訳したものであり、まだ校閲を経ていない。