代数学 I 第 12 回復習レポート課題解答例

担当：大矢 浩徳 (OYA Hironori)*

問題 1

直積群 $\mathbb{Z}/4\mathbb{Z} \times D_4 \times \mathfrak{S}_3$ の位数を求め，半角数字で入力せよ．

問題 1 解答例. 192 □

問題 1 補足解説. 直積群は集合としては集合の直積なので，

$$\mathbb{Z}/4\mathbb{Z} \times D_4 \times \mathfrak{S}_3 = \{([a]_4, g, \nu) \mid [a]_4 \in \mathbb{Z}/4\mathbb{Z}, g \in D_4, \nu \in \mathfrak{S}_3\}$$

である．よってその位数は，

$$|\mathbb{Z}/4\mathbb{Z} \times D_4 \times \mathfrak{S}_3| = |\mathbb{Z}/4\mathbb{Z}| \cdot |D_4| \cdot |\mathfrak{S}_3| = 4 \cdot 8 \cdot 6 = 192.$$

□

一般に群 $G_1, G_2, \ldots, G_k$ を群としたとき，$G_1, G_2, \ldots, G_k$ の直積集合

$$G_1 \times G_2 \times \cdots \times G_k \coloneqq \{(g_1, g_2, \ldots, g_k) \mid g_1 \in G_1, g_2 \in G_2, \ldots, g_k \in G_k\}$$

に二項演算 $\cdot \colon (G_1 \times G_2 \times \cdots \times G_k) \times (G_1 \times G_2 \times \cdots \times G_k) \to G_1 \times G_2 \times \cdots \times G_k$ を

$$(g_1, g_2, \ldots, g_k) \cdot (h_1, h_2, \ldots, h_k) \coloneqq (g_1h_1, g_2h_2, \ldots, g_kh_k),\ \forall g_i, h_i \in G_i (i = 1, 2, \ldots, k)$$

と定義したものが直積群 $G_1 \times G_2 \times \cdots \times G_k$ である．とくに，$G_1 \times G_2 \times \cdots \times G_k$ の位数は

$$|G_1 \times G_2 \times \cdots \times G_k| = |G_1| \cdot |G_2| \cdots |G_k|$$

である． □

問題 2

G_1, G_2 を群としたとき，写像

$$p \colon G_1 \times G_2 \to G_1,\ (g_1, g_2) \mapsto g_1$$

に関する記述として正しいものを選択せよ．

(1) p は群準同型である．
(2) p は群準同型ではない．
(3) G_1, G_2 の取り方によって，p は群準同型になることもあれば群準同型にならないこともある．

問題 2 解答例. (1) □

問題 2 補足解説. 任意の $g_1, h_1 \in G_1, g_2, h_2 \in G_2$ に対し，

$$p((g_1, g_2) \cdot (h_1, h_2)) = p((g_1h_1, g_2h_2)) = g_1h_1 = p((g_1, g_2))p((h_1, h_2))$$

となるので，p は群準同型である． □

* *e-mail*：hoya@shibaura-it.ac.jp

定義より明らかに p は全射，すなわち $\mathrm{Im}\, p = G_1$ であることにも注意する．

以下に本問で示した性質を含む直積群に関する諸性質をまとめておく (本問の p が以下の pr_1)．全て本問の解答例に書いた程度の短さで証明できるので，証明は各自考えてみてほしい．なお，記号が煩雑になるため避けたが，同様の性質は k 個 $(k \geq 2)$ の群 $G_1, \ldots, G_k$ の直積群 $G_1 \times \cdots \times G_k$ に一般化される．こちらも各自考えてみてもらいたい．

命題

G_1, G_2 を群とし，それぞれの単位元を e_1, e_2 とする．このとき，以下が成立する．

(1) $G_1 \times G_2$ の位数は $|G_1| \cdot |G_2|$ である．

(2) 写像

$$\mathrm{pr}_1 \colon G_1 \times G_2 \to G_1,\ (g_1, g_2) \mapsto g_1,$$
$$\mathrm{pr}_2 \colon G_1 \times G_2 \to G_2,\ (g_1, g_2) \mapsto g_2,$$

はいずれも全射群準同型である．これらは**自然な射影 (canonical projection)** と呼ばれる．

(3) 写像

$$\iota_1 \colon G_1 \to G_1 \times G_2,\ g_1 \mapsto (g_1, e_2),$$
$$\iota_2 \colon G_2 \to G_1 \times G_2,\ g_2 \mapsto (e_1, g_2),$$

はいずれも単射群準同型である．これらは**自然な入射 (canonical injection)** と呼ばれる．

(4)

$$\mathrm{Ker}\, \mathrm{pr}_2 = \mathrm{Im}\, \iota_1 = \{(g_1, e_2) \mid g_1 \in G_1\} \simeq G_1,$$
$$\mathrm{Ker}\, \mathrm{pr}_1 = \mathrm{Im}\, \iota_2 = \{(e_1, g_2) \mid g_2 \in G_2\} \simeq G_2.$$

とくに，$G_1 \simeq \{(g_1, e_2) \mid g_1 \in G_1\}$，$G_2 \simeq \{(e_1, g_2) \mid g_2 \in G_2\}$ は $G_1 \times G_2$ の正規部分群である．

□

問題 3

G を群としたとき，写像

$$m \colon G \times G \to G,\ (g_1, g_2) \mapsto g_1 \cdot g_2$$

に関する記述として正しいものを選択せよ．ただし，$\cdot$ は G における二項演算である．

(1) m は群準同型である．

(2) m は群準同型ではない．

(3) G の取り方によって，m は群準同型になることもあれば群準同型にならないこともある．

問題 3 解答例. (3) □

問題 3 補足解説. $g_1, g_2, h_1, h_2 \in G$ に対し，

$$m((g_1, g_2) \cdot (h_1, h_2)) = m((g_1 h_1, g_2 h_2)) = g_1 h_1 g_2 h_2$$
$$m((g_1, g_2)) m((h_1, h_2)) = g_1 g_2 h_1 h_2$$

となる．よって，m が群準同型となることは任意の $g_1, g_2, h_1, h_2 \in G$ に対し，

$$g_1 h_1 g_2 h_2 = g_1 g_2 h_1 h_2$$

が成り立つことと同値である．上式の両辺に左から g_1^{-1}，右から h_2^{-1} をかけると，

$$h_1 g_2 = g_2 h_1$$

となるので，結局，

$$m \text{ が群準同型} \quad \Leftrightarrow \quad G \text{ が可換群}$$

となる．よって，G が可換群であれば m は群準同型であり，G が非可換群であれば m は群準同型ではない．よって，本問の選択肢においては (3) が当てはまる． □

本問の m は G の二項演算を定める写像であるが，上の解説で述べた通り，二項演算は G が可換の場合を除いては直積群 $G \times G$ から群 G への群準同型というわけではないので注意をしておこう． □

問題 4

加法群 $\mathbb{Z}/120\mathbb{Z}$ と同型な群を<u>全て選択</u>せよ．(ただし，$\mathbb{Z}/n\mathbb{Z}$ という形の群は全て通常の加法群であると考える．以下の問題でも同様．)

(1) $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$
(2) $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$
(3) $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$
(4) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$

問題 4 解答例． (1), (3) □

問題 4 補足解説． 中国式剰余定理 (第 12 回講義資料定理 10.2, 定理 10.3) より，

$$\mathbb{Z}/120\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z},\ [a]_{120} \mapsto ([a]_5, [a]_{24})$$
$$\mathbb{Z}/120\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z},\ [a]_{120} \mapsto ([a]_3, [a]_5, [a]_8)$$

は well-defined な群同型である．ここで，$5, 24$ は互いに素，$3, 5, 8$ はどの 2 つも互いに素であることに注意する．

次に，$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ や $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ が $\mathbb{Z}/120\mathbb{Z}$ と同型でないことを証明しよう．このためには，$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ や $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ が巡回群でないことを示せば十分である．いま，任意の $a, b, c \in \mathbb{Z}$ に対し，

$$\underbrace{([a]_{10}, [b]_{12}) + \cdots + ([a]_{10}, [b]_{12})}_{60\ 個} = ([60a]_{10}, [60b]_{12}) = ([0]_{10}, [0]_{12})$$
$$\underbrace{([a]_2, [b]_3, [c]_{20}) + \cdots + ([a]_2, [b]_3, [c]_{20})}_{60\ 個} = ([60a]_2, [60b]_3, [60c]_{20}) = ([0]_2, [0]_3, [0]_{20})$$

となるので，$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ の各元の位数は全て 60 以下である．特に，位数 120 の元は存在しないので，これらは巡回群ではなく，$\mathbb{Z}/120\mathbb{Z}$ と同型ではない． □

第 12 回講義資料注意 2 で述べたように，一般に $n_1, \ldots, n_k$ の中に互いに素でないような数の組 n_i, n_j $(i \neq j)$ が存在すれば必ず

$$\mathbb{Z}/n_1 \cdots n_k\mathbb{Z} \not\cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$$

となる．証明は上に書いた $\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ や $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ が $\mathbb{Z}/120\mathbb{Z}$ と同型でないことの証明と同様である．ぜひ一般の場合も各自考えてみてほしい． □

問題 5

群同型

$$\phi\colon \mathbb{Z}/55\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$$

であって，$\phi([1]_{55}) = ([1]_5, [1]_{11})$ を満たすものを考える (このような群同型が存在するのは中国式剰余定理より)．このとき，

$$\phi([a]_{55}) = ([2]_5, [4]_{11})$$

を満たす <u>0 以上 54 以下の</u> a を求め，半角数字で入力せよ．

問題 5 解答例. 37 □

問題 5 補足解説. 問題で与えられた ϕ は準同型であることより,

$$\phi([a]_{55}) = ([a]_5, [a]_{11})$$

を満たすので，結局

$$([a]_5, [a]_{11}) = ([2]_5, [4]_{11})$$

を満たす a を求めれば良いことがわかる．この等式は a が 5 で割ると 2 余り，11 で割ると 4 余るということと同値である．そこで，0 以上 54 以下の整数で 11 で割ると 4 余る整数を求めると，これは

$$4,\ 15,\ 26,\ 37,\ 48$$

で全てである．このうち 5 で割って 2 余るものは 37 のみである．よって，求める値は 37. □

$n_1, \cdots, n_k$ がどの 2 つも互いに素なとき，任意の $0 \leq r_i < n_i$ $(i = 1, \ldots, k)$ に対して,

- n_1 で割った余りが r_1
- n_2 で割った余りが r_2

  $\vdots$
- n_k で割った余りが r_k

となるような整数 a を求めよ.

このタイプの問題は中国式剰余定理により mod $n_1 \cdots n_k$ で必ずただ一つ解が存在するのであった (第 12 回講義資料 p.4)．本問も実質的にこのタイプの問題である．本問では 11 で割ると 4 余る 0 以上 54 以下の整数が高々 5 個しかないので全てを列挙して解答を求めた．実際，このように候補が少ない場合はこの方法が確実で早いだろう．ただ，第 12 回講義資料 p.4–6 のコラムで述べた「一般的な解法」もここで復習しておこう.

第 12 回講義資料のコラムで述べた解法:

まず,

$$\phi([a_1]_{55}) = ([1]_5, [0]_{11}), \quad \phi([a_2]_{55}) = ([0]_5, [1]_{11})$$

を満たす $a_1, a_2 \in \mathbb{Z}$ を求める．このためには,

$$5x + 11y = 1 \tag{$*$}$$

を満たす $x, y \in \mathbb{Z}$ を求め,

$$a_1 = 11y, \quad a_2 = 5x$$

とすれば良かった．$(*)$ を満たす $x, y \in \mathbb{Z}$ の一つとして，$(x, y) = (-2, 1)$ が取れるので，結局

$$a_1 = 11, \quad a_2 = -10$$

とすれば良い．このとき,

$$\phi([2 \cdot 11 + 4 \cdot (-10)]_{55}) = 2\phi([11]_{55}) + 4\phi([-10]_{55}) = 2([1]_5, [0]_{11}) + 4([0]_5, [1]_{11}) = ([2]_5, [4]_{11})$$

となるので,

$$\phi^{-1}(([2]_5, [4]_{11})) = [2 \cdot 11 + 4 \cdot (-10)]_{55} = [-18]_{55} = [37]_{55}$$

となる. □

ちなみにこちらの解法で計算した a_1, a_2 を用いれば，上の計算と同じ考え方から一般に

$$\phi^{-1}(([r_1]_5, [r_2]_{11})) = [11r_1 - 10r_2]_{55}$$

であることがわかる. □