代数学 I 第 10 回レポート課題解答例

担当：大矢 浩徳 (OYA Hironori)*

問題 1

G を位数 24 の群とする．全射群準同型 $f\colon G \to \{1,-1\}$ が存在するとき，$\mathrm{Ker}\, f$ の位数を求めよ．(ただし，$\{1,-1\}$ は $\mathbb{R}^\times$ の位数 2 の部分群である.)

問題 1 解答例. 準同型定理より，$G/\ker f \simeq \mathrm{Im}\, f$ であるが，f は全射なので，$\mathrm{Im}\, f = \{1,-1\}$．よって，

$$|G/\ker f| = |\mathrm{Im}\, f| = |\{1,-1\}| = 2.$$

これと Lagrange の定理より，

$$|\mathrm{Ker}\, f| = \frac{|G|}{|G/\ker f|} = \frac{24}{2} = 12.$$

□

問題 1 補足解説. この問題の G および f の具体例は例えば以下のように与えられる：

- $G = \mathbb{Z}/24\mathbb{Z}$．このとき，
$$f\colon \mathbb{Z}/24\mathbb{Z} \to \{1,-1\},\ [m]_{24} \mapsto (-1)^m$$
とすると，これは well-defined な全射群準同型である．　このとき，
$$\ker f = \{[m]_{24} \mid m \in 2\mathbb{Z}\} = \{[0]_{24}, [2]_{24}, [4]_{24}, \dots, [22]_{24}\}$$
となる．
- $G = D_{12}$．このとき，$\sigma \mapsto 1, \tau \mapsto -1$ を満たす全射群準同型
$$f\colon D_{12} \to \{1,-1\}$$
がただ 1 つ存在する．(check してみよ.) このとき，
$$\ker f = \{\sigma^m \mid m \in 2\mathbb{Z}\} = \{e, \sigma, \sigma^2, \dots, \sigma^{11}\}$$
となる．
- $G = \mathfrak{S}_4$．このとき，
$$f = \mathrm{sgn}\colon \mathfrak{S}_4 \to \{1,-1\},\ \sigma \mapsto \mathrm{sgn}(\sigma)$$
は全射群準同型となる．なお，sgn の定義については代数学 I 第 3 回レポート課題解答例を参照のこと．これは，
$$f\left(\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}\right) = f\left(\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}\right) = f\left(\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}\right) = -1$$
を満たす唯一の群準同型 $\mathfrak{S}_4 \to \{1,-1\}$ である．このとき，$\ker f$ の 12 個の元は $\mathfrak{S}_4$ 内の**偶置換**と呼ばれ，$\ker f$ は 4 **次交代群**と呼ばれる．(全く同じ方法で n **次交代群**が定義される.)

□

* *e-mail*：hoya@shibaura-it.ac.jp

問題 2

(1) 39 で割ると 2 余り，119 で割ると 3 余る整数を 1 つ求めよ．

(2) $\mathbb{Z}/4641\mathbb{Z}$ と $\mathbb{Z}/39\mathbb{Z} \times \mathbb{Z}/119\mathbb{Z}$ は同型であることを証明せよ．

問題 2 解答例.

(1)

$$119 = 3 \times 39 + 2 \qquad\qquad 39 = 19 \times 2 + 1$$

より，$1 = 39 - 19 \times 2 = 39 - 19 \times (119 - 3 \times 39) = (-19) \times 119 + 58 \times 39$. これより求める値の 1 つは，

$$2 \times ((-19) \times 119) + 3 \times (58 \times 39) = 2264.$$

$\square$

(2) 写像 $f\colon \mathbb{Z} \to \mathbb{Z}/39\mathbb{Z} \times \mathbb{Z}/119\mathbb{Z}, m \mapsto ([m]_{39}, [m]_{119})$ を考えると，これは加法群の群準同型である．また，

$$\begin{aligned}
\operatorname{Ker} f &= \{m \in \mathbb{Z} \mid [m]_{39} = [0]_{39}, [m]_{119} = [0]_{119}\} \\
&= \{m \in \mathbb{Z} \mid m \in 39\mathbb{Z}, m \in 119\mathbb{Z}\} \\
&= \{m \in \mathbb{Z} \mid m \text{ は 39 の倍数かつ 119 の倍数 }\} \\
&= \{m \in \mathbb{Z} \mid m \text{ は 4641 の倍数 }\} \text{ (39 と 119 は互いに素なので)} \\
&= 4641\mathbb{Z}.
\end{aligned}$$

よって，準同型定理より $\mathbb{Z}/4641\mathbb{Z} \simeq \operatorname{Im} f \subset \mathbb{Z}/39\mathbb{Z} \times \mathbb{Z}/119\mathbb{Z}$ であるが，$\mathbb{Z}/4641$ と $\mathbb{Z}/39\mathbb{Z} \times \mathbb{Z}/119\mathbb{Z}$ はともに位数 4641 なので，$\operatorname{Im} f = \mathbb{Z}/39\mathbb{Z} \times \mathbb{Z}/119\mathbb{Z}$ である．よって，$\mathbb{Z}/4641\mathbb{Z} \simeq \mathbb{Z}/39\mathbb{Z} \times \mathbb{Z}/119\mathbb{Z}$ である． $\square$

問題 2 補足解説. 解答例では写像 $f\colon \mathbb{Z} \to \mathbb{Z}/39\mathbb{Z} \times \mathbb{Z}/119\mathbb{Z}, m \mapsto ([m]_{39}, [m]_{119})$ をまず考えているが，そうではなく $f'\colon \mathbb{Z}/4641\mathbb{Z} \to \mathbb{Z}/39\mathbb{Z} \times \mathbb{Z}/119\mathbb{Z}, [m]_{4641} \mapsto ([m]_{39}, [m]_{119})$ を初めから考えるという解答も見られた．しかし，定義域を初めから割って $\mathbb{Z}/4641\mathbb{Z}$ にする場合，f' が well-defined であることのチェックも必要となる．

この問の設定は 39，119 を任意の互いに素な正の整数 n_1, n_2 に置き換えて一般化できる．特に，以下は**中国剰余定理**と呼ばれる：

> n_1, n_2 を互いに素な正の整数とすると，
>
> $$\pi_{n_1,n_2}\colon \mathbb{Z}/n_1n_2\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z},\ [m]_{n_1n_2} \mapsto ([m]_{n_1}, [m]_{n_2})$$
>
> は well-defined で群同型写像である．

この視点で言えば，(1) は $\pi_{39,119}^{-1}(([2]_{39}, [3]_{119}))$ を求めたということに他ならない ($[2264]_{4641}$ が解である)．

なお，正の整数 n_1, n_2 が互いに素でないとき，

$$\mathbb{Z}/n_1n_2\mathbb{Z} \not\simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$$

である．

理由：n_1 と n_2 の最小公倍数を ℓ とすると，$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ の任意の元 $([m_1]_{n_1}, [m_2]_{n_2})$ は

$$\underbrace{([m_1]_{n_1}, [m_2]_{n_2}) + \cdots + ([m_1]_{n_1}, [m_2]_{n_2})}_{\ell\text{個}} = ([\ell m_1]_{n_1}, [\ell m_2]_{n_2}) = ([0]_{n_1}, [0]_{n_2})$$

を満たす．特に，$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ の元の位数は全て ℓ 以下である．一方，$\mathbb{Z}/n_1n_2\mathbb{Z}$ は位数 n_1n_2 の元 $[1]_{n_1n_2}$ を持つ．今，n_1, n_2 は互いに素でないので，$\ell < n_1n_2$ となるため，$\mathbb{Z}/n_1n_2\mathbb{Z}$ と $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ は同型でない． $\square$