代数学 I 第 12 回本レポート課題解答例

担当：大矢 浩徳 (OYA Hironori)*

問題 1

以下の 2 つの群が同型であるかどうかを判定せよ．

- 加法群 $\mathbb{Z}/4\mathbb{Z}$
- 乗法群 $(\mathbb{Z}/5\mathbb{Z})^{\times}$

問題 1 解答例． 同型である． □

問題 1 補足解説． $(\mathbb{Z}/5\mathbb{Z})^{\times} = \{[1]_5, [2]_5, [3]_5, [4]_5\}$ である (第 3 回講義資料命題 3.4)．いま，

$$[2]_5^2 = [4]_5 \qquad [2]_5^3 = [8]_5 = [3]_5 \qquad [2]_5^4 = [16]_5 = [1]_5$$

となるので，

$$(\mathbb{Z}/5\mathbb{Z})^{\times} = \{[2]_5^k \mid k \in \mathbb{Z}\} = \langle [2]_5 \rangle$$

となる．よって，$(\mathbb{Z}/5\mathbb{Z})^{\times}$ は位数 4 の巡回群となるので，第 12 回講義資料定理 11.2 より，$\mathbb{Z}/4\mathbb{Z}$ と同型である．なお，具体的な同型は巡回群の生成元どうしを対応させれば得られるので，

$$\phi\colon \mathbb{Z}/4\mathbb{Z} \to (\mathbb{Z}/5\mathbb{Z})^{\times},\ [a]_4 \mapsto [2]_5^a$$

で与えられる．なお，実は以下の定理が一般に成立する．

定理

p を素数とする．このとき，ある $[m]_p \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ が存在して，

$$(\mathbb{Z}/p\mathbb{Z})^{\times} = \langle [m]_p \rangle = \{[1]_p, [m]_p, [m^2]_p, \dots, [m_p^{p-2}]\}$$

となる．つまり，$(\mathbb{Z}/p\mathbb{Z})^{\times}$ は位数 $p-1$ の巡回群であり，

$$(\mathbb{Z}/p\mathbb{Z})^{\times} \simeq \mathbb{Z}/(p-1)\mathbb{Z}$$

となる．

この定理で取った $[m]_p$ は $\mathbb{Z}/p\mathbb{Z}$ の**原始根**と呼ばれる．$[2]_5, [3]_5$ は $\mathbb{Z}/5\mathbb{Z}$ の原始根である．

注意．上の定理において p が素数という仮定は重要である．例えば

$$(\mathbb{Z}/12\mathbb{Z})^{\times} = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$$

であるが，$[5]_{12}^2 = [7]_{12}^2 = [11]_{12}^2 = [1]_{12}$ より，位数 4 の元は存在せず，$(\mathbb{Z}/12\mathbb{Z})^{\times}$ は巡回群にはならない．(この群はクラインの 4 元群に同型である．)

□

* *e-mail*: hoya@shibaura-it.ac.jp

問題 2

G を位数 12 の群，G' を位数 6 の群とする．準同型 $\phi\colon G \to G'$ が存在し，像 $\operatorname{Im}\phi$ が G' の正規部分群であると仮定する．$G'/\operatorname{Im}\phi$ の位数が 2 であるとき，$\operatorname{Ker}\phi$ の位数は $\boxed{ア}$ である．$\boxed{ア}$ に入る自然数を半角数字で入力せよ．

問題 2 解答例． ラグランジュの定理より，

$$2 = |G'/\operatorname{Im}\phi| = \frac{|G'|}{|\operatorname{Im}\phi|} = \frac{6}{|\operatorname{Im}\phi|}.$$

となるので，$|\operatorname{Im}\phi| = 3$ である．準同型定理より，

$$G/\operatorname{Ker}\phi \simeq \operatorname{Im}\phi$$

なので，ラグランジュの定理より，

$$3 = |\operatorname{Im}\phi| = |G/\operatorname{Ker}\phi| = \frac{|G|}{|\operatorname{Ker}\phi|} = \frac{12}{|\operatorname{Ker}\phi|}.$$

よって，

$$|\operatorname{Ker}\phi| = 4.$$

□

問題 2 補足解説． 本問の設定の具体例としては以下のようなものが挙げられる．

$$G = \mathbb{Z}/12\mathbb{Z} \quad G' = \mathbb{Z}/6\mathbb{Z}$$

として，

$$\phi\colon \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z},\ [a]_{12} \mapsto [2a]_6.$$

他にももう少し難しい非可換な例として，$G = \mathfrak{A}_4, G' = D_3, \operatorname{Ker}\phi = V$ (クラインの 4 元群) となる ϕ の例も構成することができる．興味がある方は考えてみてほしい． □

問題 3

以下の主張の正誤を判定せよ．

『位数 7 の非可換群は存在しない．』

問題 3 解答例． 正しい． □

問題 3 補足解説． 7 は素数なので，第 12 回講義資料定理 11.3 より位数 7 の非可換群は全て $\mathbb{Z}/7\mathbb{Z}$ と同型である．$\mathbb{Z}/7\mathbb{Z}$ は可換なので，位数 7 の群は全て可換な巡回群となることがわかる． □

問題 4

4 次対称群 $\mathfrak{S}_4$ において，クラインの 4 元群 V と以下の部分群 H を考える．

$$H := \langle (1\ 2\ 3\ 4) \rangle$$

このとき，$\mathfrak{S}_4$ の部分群 HV の位数は $\boxed{ア}$ である．$\boxed{ア}$ に入る自然数を半角数字で入力せよ．なお，自然数なので 2 桁以上の数もあり得ることに注意せよ．

問題 4 解答例． クラインの 4 元群は $\mathfrak{S}_4$ の正規部分群なので (第 10 回講義資料例 4 参照)，第 2 同型定理より，

$$H/(H \cap V) \simeq HV/V. \tag{$*$}$$

ここで，$(1\ 2\ 3\ 4)$ は位数 4 なので，

$$H = \{e,\ (1\ 2\ 3\ 4),\ (1\ 2\ 3\ 4)^2,\ (1\ 2\ 3\ 4)^3\} = \{e,\ (1\ 2\ 3\ 4),\ (1\ 3)(2\ 4),\ (4\ 3\ 2\ 1)\}.$$

よって，

$$H \cap V = \{e, (1\ 3)(2\ 4)\}.$$

さらにラグランジュの定理から，

$$|H/(H\cap V)| = \frac{|H|}{|H\cap V|} = \frac{4}{2} = 2, \qquad |HV/V| = \frac{|HV|}{|V|} = \frac{|HV|}{4}.$$

いま $(*)$ より，

$$|H/(H\cap V)| = |HV/V|$$

なので，

$$2 = \frac{|HV|}{4}$$

よって，$|HV| = 8$. □

問題 4 補足解説. $|H| = 4, |V| = 4$ なので，単純に $|HV| = 4 \times 4 = 16$ としてしまわないように注意しよう．なお，具体的に計算してみると，HV は

$$\{e,\ (1\ 3),\ (2\ 4),\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3),\ (1\ 2\ 3\ 4),\ (4\ 3\ 2\ 1)\}$$

となる． □

問題 5

以下の主張の正誤を判定せよ．
『群 G と $M \subset N$ を満たす G の正規部分群 M, N であって，以下の性質を満たすものの例が存在する；

G/M は可換群であるが G/N は非可換群である

』

問題 5 解答例. 間違い． □

問題 5 補足解説. まず一般に群 G' が可換群のとき，その部分群 N' に対し，剰余群 G'/N' は再び可換群となる (可換群の場合，任意の部分群は正規であることに注意)．実際，任意の $g_1N', g_2N' \in G'/N'$ に対して，

$$g_1N' \cdot g_2N' = g_1g_2N' = g_2g_1N' = g_2N' \cdot g_1N'$$

である．本問の設定では，第 3 同型定理より，

$$G/N \simeq (G/M)/(N/M)$$

となるが, 上で見た性質より G/M が可換群であれば, $(G/M)/(N/M)$ は可換群となるので ($G' = G/M, N' = N/M$ として上の性質を適用すればよい)，ここから G/N も可換群となることがわかる．これより，問題文に書かれているような例は構成できないことがわかる． □