代数学 I 第 11 回復習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 $\mathbb{Z}/6\mathbb{Z}$
- 乗法群 $(\mathbb{Z}/7\mathbb{Z})^\times$

問題 1 解答例. 同型である □

問題 1 補足解説. 7 は素数なので，

$$(\mathbb{Z}/7\mathbb{Z})^\times = (\mathbb{Z}/7\mathbb{Z}) \setminus \{[0]_7\} = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$$

である (第 3 回講義資料命題 2.9 および p.12 参照)．いま，

$$[3]_7^2 = [9]_7 = [2]_7 \qquad [3]_7^3 = [3]_7[2]_7 = [6]_7 \qquad [3]_7^4 = [3]_7[6]_7 = [18]_7 = [4]_7$$
$$[3]_7^5 = [3]_7[4]_7 = [12]_7 = [5]_7 \qquad [3]_7^6 = [3]_7[5]_7 = [15]_7 = [1]_7$$

となるので，

$$(\mathbb{Z}/7\mathbb{Z})^\times = \{[3]_7^k \mid k \in \mathbb{Z}\} = \langle [3]_7 \rangle$$

となる．よって，$(\mathbb{Z}/7\mathbb{Z})^\times$ は位数 6 の巡回群となるので，$\mathbb{Z}/6\mathbb{Z}$ と同型である (第 11 回講義資料定理 9.2)． □

第 11 回講義資料定理 9.2 より，一般に群 G が加法群 $\mathbb{Z}/n\mathbb{Z}$ と同型であることの必要十分条件は G が位数 n の巡回群となることであった．これより，本問は $(\mathbb{Z}/7\mathbb{Z})^\times$ が位数 6 の巡回群であるかどうかを問う問題であると言える．ここまでわかれば，後は $(\mathbb{Z}/7\mathbb{Z})^\times$ を生成する元があるかどうかを探せば良い．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，

$$\phi\colon \mathbb{Z}/6\mathbb{Z} \to (\mathbb{Z}/7\mathbb{Z})^\times,\ [m]_6 \mapsto [3]_7^m$$

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．

この定理で取ったような $[m]_p$ は $\mathbb{Z}/p\mathbb{Z}$ の**原始根**と呼ばれる，上の解答での計算より，$[3]_7$ は $\mathbb{Z}/7\mathbb{Z}$ の原始根であることがわかる．ちなみに，$[5]_7$ も $\mathbb{Z}/7\mathbb{Z}$ の原始根である．

* *e-mail*：hoya@shibaura-it.ac.jp

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．）

□

問題 2

G を位数 10 の群，G' を位数 12 の群，$\phi\colon G \to G'$ を群準同型とする．ある元 $g \in G$ が存在して，

$$\phi(g) \neq e'$$

となるとき，$\operatorname{Ker}\phi$ の位数を求め，半角数字で入力せよ．ここで，e' は G' の単位元である．

問題 2 解答例． 5 □

問題 2 補足解説． $\operatorname{Ker}\phi$ は G の部分群であったので，ラグランジュの定理の系 (第 9 回講義資料系 7.3 (1)) より，$\operatorname{Ker}\phi$ の位数は $|G| = 10$ の約数である．よって，$|\operatorname{Ker}\phi|$ は

$$1, 2, 5, 10$$

のいずれかである．さらに，準同型定理より，

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

なので，

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

よって，ラグランジュの定理より，

$$|\operatorname{Im}\phi| = |G/\operatorname{Ker}\phi| = \frac{|G|}{|\operatorname{Ker}\phi|} = \frac{10}{|\operatorname{Ker}\phi|}$$

なので，$\operatorname{Im}\phi$ の位数は $|\operatorname{Ker}\phi|$ が $1, 2, 5, 10$ であるとき，順に

$$10, 5, 2, 1$$

となる．ここで，$\operatorname{Im}\phi$ は G' の部分群なので，再びラグランジュの定理の系より，$\operatorname{Im}\phi$ の位数は $|G'| = 12$ の約数である．以上の考察より，$\operatorname{Ker}\phi, \operatorname{Im}\phi$ の位数の組み合わせとしてあり得るのは，

(1) $|\operatorname{Ker}\phi| = 5, |\operatorname{Im}\phi| = 2$
(2) $|\operatorname{Ker}\phi| = 10, |\operatorname{Im}\phi| = 1$

のいずれかである．ここで，(2) の場合 $|\operatorname{Ker}\phi| = 10 = |G|$ なので，$\operatorname{Ker}\phi = G$ であるから，全ての $g \in G$ に対して $\phi(g) = e'$ となり，問題文にあるような $g \in G$ の存在に矛盾する．以上より，あり得るのは (1) の場合のみで，求める $\operatorname{Ker}\phi$ の位数は 5 である． □

本問のような状況の具体例としては，

$$\phi\colon D_5 \to \mathbb{Z}/12\mathbb{Z},\ \sigma^k\tau^\ell \mapsto [6\ell]_{12}$$

等がある．このとき，

$$\operatorname{Ker}\phi = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4\}$$

である． □

問題 3

群 G が可換群となるための十分条件となるものを全て選択せよ．

(1) 乗法群 $\mathbb{R}^\times$ からの全射群準同型 $\phi\colon \mathbb{R}^\times \to G$ が存在する．
(2) 群準同型 $\phi\colon G \to G'$ であって，$\operatorname{Im}\phi$ も $\operatorname{Ker}\phi$ も可換群となるものが存在する．
(3) G の位数は 11 である．

問題 3 解答例. (1)，(3) □

問題 3 補足解説.

(1) 全射群準同型 $\phi\colon \mathbb{R}^\times \to G$ が存在すれば，準同型定理より，

$$G = \operatorname{Im}\phi \simeq \mathbb{R}^\times / \operatorname{Ker}\phi$$

となる．ここで任意の $a, b \in \mathbb{R}^\times$ に対し，

$$a \operatorname{Ker}\phi \cdot b \operatorname{Ker}\phi = ab \operatorname{Ker}\phi = ba \operatorname{Ker}\phi = b \operatorname{Ker}\phi \cdot a \operatorname{Ker}\phi$$

となるので，$\mathbb{R}^\times / \operatorname{Ker}\phi$ は可換群である．よって，このとき G も可換群となる．

(2) 例えば 3 次二面体群 D_3 の部分群 $N = \langle \sigma \rangle = \{e, \sigma, \sigma^2\}$ を考えるとこれは正規部分群である (第 9 回講義資料例 6)．このとき，商写像

$$p\colon D_3 \to D_3/N$$

を考えると，これは全射群準同型であり，$\operatorname{Ker} p = N$ である (第 10 回講義資料例 10 参照)．ここで，$\operatorname{Im}\phi = D_3/N$ であるが，これは位数 2 の群なので可換群である (第 9 回講義資料例 9 参照)．よって，このとき $\operatorname{Im}\phi = D_3/N$ も $\operatorname{Ker}\phi = N$ も可換群であるが，D_3 は非可換群である．よって，(2) の条件は G の可換性を一般には導かない．

(3) 11 は素数なので，G の位数が 11 のとき，$G \simeq \mathbb{Z}/11\mathbb{Z}$ である (第 11 回講義資料定理 9.3)．よって，このとき G は可換群となる． □

(1) の解説で述べたのと全く同じ手法で，一般に可換群の剰余群が可換群であることが示される．よって，G が可換群 A からの全射群準同型 $\phi\colon A \to G$ を持つとき，準同型定理から，

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

は可換群である．

(2) の例は n 次二面体群 D_n に一般化される ($n \geq 3$ で D_n は非可換群である)．D_n の部分群 $N = \langle \sigma \rangle = \{e, \sigma, \dots, \sigma^{n-1}\}$ を考えるとこれは正規部分群であり，商写像

$$p\colon D_n \to D_n/N$$

は全射群準同型で $\operatorname{Ker} p = N$ である．このとき，$\operatorname{Im}\phi = D_n/N$ (位数 2) も $\operatorname{Ker}\phi = N$ も可換群である． □

問題 4

4 次対称群 $\mathfrak{S}_4$ の正規部分群

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

を考える．(V はクラインの 4 元群と呼ばれる部分群であった．第 9 回復習レポート課題解答問題 4 補足解説参照．) $\mathfrak{S}_4$ の位数 4 の部分群 H が，

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

を満たすとき，$\mathfrak{S}_4$ の部分群 HV の位数を求めよ．

問題 4 解答例. 8 □

問題 4 補足解説. クラインの 4 元群 V は $\mathfrak{S}_4$ の正規部分群なので，第 2 同型定理より，

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

ここで，ラグランジュの定理より，

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

よって，

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

となるので，HV の位数は $|HV| = 8$. □

$|H| = 4, |V| = 4$ 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，H の具体的な例としては，

$$H = \langle (1\ 2\ 3\ 4) \rangle = \{e, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2)\}$$

が挙げられる．なお，このとき HV を具体的に計算してみると，

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

となる． □

問題 5

G を位数無限の群，N を G の正規部分群とし，N の G における指数 $(G : N)$ は 3 であるとする．M を $M \subset N$ を満たす G の正規部分群とし，G/M の位数が 12 であるとする．このとき，剰余群 N/M の位数を求め，半角数字で入力せよ．

問題 5 解答例. 4 □

問題 5 補足解説. 第 3 同型定理より，

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

である．よって，

$$|(G/M)/(N/M)| = |G/N| = (G : N) = 3.$$

($|G/N| = (G : N)$ は指数の定義である．) ここで，ラグランジュの定理より，

$$|(G/M)/(N/M)| = \frac{|G/M|}{|N/M|} = \frac{12}{|N/M|}$$

なので，

$$\frac{12}{|N/M|} = 3.$$

よって，N/M の位数は $|N/M| = 4$. □

本問のような状況の具体例としては，

$$G = \mathbb{Z}, \quad N = 3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\}, \quad M = 12\mathbb{Z} = \{12k \mid k \in Z\}$$

が挙げられる．このとき，

$$3\mathbb{Z}/12\mathbb{Z} = \{[3k]_{12} \mid k \in \mathbb{Z}\} = \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}$$

である． □