代数学 I 第 3 回復習レポート課題解答例

担当：大矢 浩徳 (OYA Hironori)*

問題 1

$$f\colon \mathbb{Z}/\boxed{ア}\mathbb{Z} \to \mathbb{Z}/\boxed{イ}\mathbb{Z},\ [a]_{\boxed{ア}} \mapsto [2a]_{\boxed{イ}}$$

が well-defined な写像を与えるような $\boxed{ア}$, $\boxed{イ}$ の組み合わせとして正しいものを以下から全て選択せよ.

(1) $\boxed{ア} = 5, \boxed{イ} = 3$
(2) $\boxed{ア} = 4, \boxed{イ} = 8$
(3) $\boxed{ア} = 7, \boxed{イ} = 7$
(4) $\boxed{ア} = 6, \boxed{イ} = 9$
(5) $\boxed{ア} = 9, \boxed{イ} = 6$

問題 1 解答例. (2), (3), (5) □

問題 1 補足解説. (1)–(5) の場合の well-defined 性を順に確かめてみよう．well-defined 性の証明は「定義域の各元の任意の 2 つの表示を取った時に，考えている対応でのそれらの送り先が同じになることを示す」というものである.

(1) $f\colon \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}, [a]_5 \mapsto [2a]_3$ は well-defined ではない (このような対応の写像は定義できない)．なぜなら，$[0]_5 = [5]_5$ であるにも関わらず,

$$f([0]_5) = [0]_3 \neq [1]_3 = [10]_3 = f([5]_5)$$

となるためである.

(2) $f\colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}, [a]_4 \mapsto [2a]_8$ は well-defined である．なぜなら，$[a]_4 = [a']_4$ $(a, a' \in \mathbb{Z})$ であれば，ある $k \in \mathbb{Z}$ が存在して，$a = a' + 4k$ と書けるので,

$$f([a]_4) = [2a]_8 = [2a' + 8k]_8 = [2a']_8 = f([a']_4)$$

となるためである.

(3) $f\colon \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}, [a]_7 \mapsto [2a]_7$ は well-defined である．なぜなら，$[a]_7 = [a']_7$ $(a, a' \in \mathbb{Z})$ であれば，ある $k \in \mathbb{Z}$ が存在して，$a = a' + 7k$ と書けるので,

$$f([a]_7) = [2a]_7 = [2a' + 14k]_7 = [2a']_7 = f([a']_7)$$

となるためである.

(4) $f\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}, [a]_6 \mapsto [2a]_9$ は well-defined ではない (このような対応の写像は定義できない)．なぜなら，$[0]_6 = [6]_6$ であるにも関わらず,

$$f([0]_6) = [0]_9 \neq [3]_9 = [12]_9 = f([6]_6)$$

となるためである.

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

(5) $f\colon \mathbb{Z}/9\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}, [a]_9 \mapsto [2a]_6$ は well-defined である．なぜなら，$[a]_9 = [a']_9$ $(a, a' \in \mathbb{Z})$ であれば，ある $k \in \mathbb{Z}$ が存在して，$a = a' + 9k$ と書けるので，

$$f([a]_9) = [2a]_6 = [2a' + 18k]_6 = [2a']_6 = f([a']_9)$$

となるためである． □

問題 2

加法群 $\mathbb{Z}/60\mathbb{Z}$ における部分群

$$H = \{[36m]_{60} \mid m \in \mathbb{Z}\}$$

の位数を半角数字で入力せよ．

問題 2 解答例. 5 □

問題 2 補足解説.

[解法 1：$36 \times 5 = 180$ が 60 の倍数であることに着目] 任意の整数は $5q + r$ $(q \in \mathbb{Z}, r = 0, 1, 2, 3, 4)$ の形に書けるので，

$$\begin{aligned} H &= \{[36(5q + r)]_{60} \mid q \in \mathbb{Z}, r = 0, 1, 2, 3, 4\} \\ &= \{[180q + 36r]_{60} \mid q \in \mathbb{Z}, r = 0, 1, 2, 3, 4\} \\ &= \{[36r]_{60} \mid r = 0, 1, 2, 3, 4\} \\ &= \{[0]_{60}, [36]_{60}, [72]_{60}, [108]_{60}, [144]_{60}\} \\ &= \{[0]_{60}, [12]_{60}, [24]_{60}, [36]_{60}, [48]_{60}\} \end{aligned}$$

となる．よって，H の位数は 5 である． □

[解法 2：第 3 回講義資料定理 2.2, 2.4 を用いる方法] 第 3 回講義資料定理 2.4 より，

$$\begin{aligned} [k]_{60} \in H = \{[36m]_{60} \mid m \in \mathbb{Z}\} \quad &\Leftrightarrow \quad \text{ある } m_1, m_2 \in \mathbb{Z} \text{ が存在して，} 36m_1 + 60m_2 = k \\ &\Leftrightarrow \quad k \text{ は } \gcd(36, 60) = 12 \text{ の倍数} \end{aligned}$$

となるので，

$$H = \{[12m]_{12} \mid m \in \mathbb{Z}\}.$$

よって，第 3 回講義資料定理 2.2 より，H の位数は $60/12 = 5$ である． □

解法 2 を見るとこの問題は次のように一般化されることがわかる．

定理

n, a を正の整数とする．このとき，加法群 $\mathbb{Z}/n\mathbb{Z}$ における部分群

$$H = \{[am]_n \mid m \in \mathbb{Z}\}$$

の位数は $n/\gcd(a, n)$ である．さらに，

$$H = \{[\gcd(a, n)m]_n \mid m \in \mathbb{Z}\}$$

である．

証明は解法 2 の議論を順に一般的な言葉に直していけば良い．

証明. 第 3 回講義資料定理 2.4 より，

$$\begin{aligned} [k]_n \in H = \{[am]_n \mid m \in \mathbb{Z}\} \quad &\Leftrightarrow \quad \text{ある } m_1, m_2 \in \mathbb{Z} \text{ が存在して，} am_1 + nm_2 = k \\ &\Leftrightarrow \quad k \text{ は } \gcd(a, n) \text{ の倍数} \end{aligned}$$

となるので，

$$H = \{[\gcd(a, n)m]_n \mid m \in \mathbb{Z}\}.$$

よって，第 3 回講義資料定理 2.2 より，H の位数は $n/\gcd(a,n)$ である． □

□

問題 3

$\mathbb{Z}/1829\mathbb{Z}$ において，

$$[100x]_{1829} = [4]_{1829}$$

を満たす 0 以上 1828 以下の自然数 x を半角数字で入力せよ．

問題 3 解答例. 439 □

問題 3 補足解説.

$$[100x]_{1829} = [4]_{1829} \quad \Leftrightarrow \quad \text{ある } m \in \mathbb{Z} \text{ が存在して，} 100x + 1829m = 4$$

なので，$100x + 1829m = 4$ の整数解 (x, m) のうち $0 \leq x \leq 1828$ を満たすものを求めれば良いことがわかる．

ここで，100 と 1829 の最大公約数 $\gcd(100, 1829)$ をユークリッド互除法で求める過程の計算は以下の通りである．

$$1829 = 18 \times 100 + 29 \qquad 100 = 3 \times 29 + 13 \qquad 29 = 2 \times 13 + 3$$
$$13 = 4 \times 3 + 1 \qquad 3 = 3 \times 1 + 0$$

よって，$\gcd(100, 1829) = 1$ であり，ここから $100x' + 1829m' = 1$ を満たす整数の組 (x', m') の 1 つが以下のように求められる．

$$\begin{aligned}
1 &= 13 - 4 \times 3 \\
&= 13 + (-4) \times (29 - 2 \times 13) \\
&= 9 \times 13 + (-4) \times 29 \\
&= 9 \times (100 - 3 \times 29) + (-4) \times 29 \\
&= 9 \times 100 + (-31) \times 29 \\
&= 9 \times 100 + (-31) \times (1829 - 18 \times 100) \\
&= 567 \times 100 + (-31) \times 1829
\end{aligned}$$

つまり，$(x', m') = (567, -31)$ が $100x' + 1829m' = 1$ を満たす整数の組の 1 つである．よって，$100x + 1829m = 4$ の整数解 (x, m) の一つとして，$(567 \times 4, -31 \times 4) = (2268, -124)$ が得られる．よって，$\gcd(100, 1829) = 1$ に注意すると，整数の組 (x, m) に対して，

$$\begin{aligned}
100x + 1829m = 4 &\Leftrightarrow 100(x - 2268) + 1829(y - (-124)) = 0 \\
&\Leftrightarrow \text{ある } m \in \mathbb{Z} \text{ が存在して，} (x - 2268, y + 124) = (-1829m, 100m)
\end{aligned}$$

となるので，$100x + 1829m = 4$ を満たす整数の組は，$(x, m) = (2268 - 1829m, -124 + 100m), m \in \mathbb{Z}$ で全てである．よって，この解の中で $0 \leq x \leq 1828$ を満たすものは，$m = 1$ としたときの $(439, -24)$ である． □

※本問のような問題は検算可能なので，時間があれば検算を行って計算間違いがないか確認を行うこと．

実数の範囲で一次方程式 $100x = 4$ を解くためには両辺を 100 で割ればよかった．$\mathbb{Z}/1829\mathbb{Z}$ の中では，普通の意味で 100 で割ることはできないが，$(x', m') = (567, -31)$ が $100x' + 1829m' = 1$ を満たす整数の組の 1 つであったので，

$$[100]_{1829}^{-1} = [567]_{1829}$$

である．よって，与式の両辺にこれを掛けて

$$[x]_{1829} = [100]_{1829}^{-1}[100]_{1829}[x]_{1829} = [100]_{1829}^{-1}[100x]_{1829} = [567]_{1829} \cdot [4]_{1829} = [2268]_{1829} = [439]_{1829}$$

というようにして求めても良い．$\mathbb{Z}/1829\mathbb{Z}$ の世界においては $[100]_{1829}^{-1}$ を掛けることが “100 で割る” ことに他ならないのである．

また，$100x' + 1829m' = 1$ を満たす整数の組 (x', m') の 1 つを求めるところは拡張ユークリッド互除法で以下のように求めてもよい．

- $1829 = 18 \times 100 + 29$ より，行列 $\begin{pmatrix} 0 & 1 \\ 1 & -18 \end{pmatrix}$ をとる．
- $100 = 3 \times 29 + 13$ より，行列を $\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -18 \end{pmatrix} = \begin{pmatrix} 1 & -18 \\ -3 & 55 \end{pmatrix}$ に更新する．
- $29 = 2 \times 13 + 3$ より，行列を $\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 1 & -18 \\ -3 & 55 \end{pmatrix} = \begin{pmatrix} -3 & 55 \\ 7 & -128 \end{pmatrix}$ に更新する．
- $13 = 4 \times 3 + 1$ より，行列を $\begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} -3 & 55 \\ 7 & -128 \end{pmatrix} = \begin{pmatrix} 7 & -128 \\ -31 & 567 \end{pmatrix}$ に更新する．
- $3 = 3 \times 1 + 0$ より，行列を $\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 7 & -128 \\ -31 & 567 \end{pmatrix} = \begin{pmatrix} -31 & 567 \\ 100 & -1829 \end{pmatrix}$ に更新する．

よって，$\gcd(100, 1829) = 1$ であり，最後の行列の 1 行目から $100x' + 1829m' = 1$ を満たす整数の組 (x', m') の 1 つとして $(x', m') = (567, -31)$ がとれることがわかる (順番注意)． □

問題 4

乗法群 $(\mathbb{Z}/2401\mathbb{Z})^\times$ の位数を半角数字で入力せよ．(Hint：$2401 = 7^4$.)

問題 4 解答例. 2058 □

問題 4 補足解説. 第 3 回講義資料命題 2.11 より，

$$\#(\mathbb{Z}/2401\mathbb{Z})^\times = \varphi(2401) = \#\{m \in \mathbb{N} \mid 1 \leq m \leq 2401, \gcd(m, 2401) = 1\}$$

なので，1 以上 2401 以下の自然数で，2401 と互いに素なものの個数を数えれば良い．$2401 = 7^4$ であるので，自然数 m に対し，

$$\gcd(m, 2401) = 1 \quad \Leftrightarrow \quad m \text{ は } 7 \text{ の倍数ではない}$$

となる．1 以上 2401 以下の 7 の倍数は $2401 \div 7 = 343$ 個あるので，求める値は，

$$\varphi(2401) = 2401 - 343 = 2058.$$

□

本問の解法は 7^4 を一般の素数 p に対する p^k に変えても上手く行くことがわかる．つまり以下の定理が同様に証明される．

定理

p を素数とし，$k \in \mathbb{Z}_{>0}$ とする．このとき，

$$\#(\mathbb{Z}/p^k\mathbb{Z})^\times = \varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

証明. 最初の等式は第 3 回講義資料命題 2.11 である．残りの等式を示す．p は素数なので，自然数 m に対し，

$$\gcd(m, p^k) = 1 \quad \Leftrightarrow \quad m \text{ は } p \text{ の倍数ではない}$$

となる．1 以上 p^k 以下の p の倍数は $p^k \div p = p^{k-1}$ 個あるので，

$$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

□

なお，この定理は実は次のように一般化される．

定理

$n \in \mathbb{Z}_{>0}$ に対し，

$$\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n) = n \prod_{p:\text{ 素数},p|n} \left(1 - \frac{1}{p}\right).$$

ここで，$p \mid n$ は「p が n を割り切る」という意味で，$\prod_{p:\text{ 素数},p|n}$ は「n を割り切る素数 p に渡って積を取る」という記号である ($\sum$ の掛け算バージョン)．

ここではこの定理の証明は行わないが，n と互いに素な自然数を数える時に「n の素因数の倍数を除いていく」という方法を念頭におくと証明をすることができる．この定理を用いれば例えば，以下のような定理も容易に証明できる．

定理

$m, n \in \mathbb{Z}_{>0}$ に対し，$\gcd(m, n) = 1$ であれば，

$$\varphi(mn) = \varphi(m)\varphi(n).$$

この定理と初めの定理を合わせて考えれば，例えば

$$\varphi(12) = \varphi(2^2 \cdot 3) = \varphi(2^2)\varphi(3) = (2^2 - 2)(3 - 1) = 4$$

というような計算も可能になる． □

問題 5

乗法群 $(\mathbb{Z}/9\mathbb{Z})^\times$ の以下の部分集合 H が $(\mathbb{Z}/9\mathbb{Z})^\times$ の部分群となるかどうかを判定せよ．

$$H = \{[1]_9, [4]_9, [7]_9\}$$

問題 5 解答例. 部分群となる □

問題 5 補足解説. $(\mathbb{Z}/9\mathbb{Z})^\times$ が可換群であることに注意すると，

$$[1]_9^2 = [1]_9 \qquad [1]_9[4]_9 = [4]_9 \qquad [1]_9[7]_9 = [7]_9$$
$$[4]_9^2 = [16]_9 = [7]_9 \qquad [4]_9[7]_9 = [28]_9 = [1]_9 \qquad [7]_9[7]_9 = [49]_9 = [4]_9$$

なので，H は二項演算で閉じており，

$$[1]_9^{-1} = [1]_9 \qquad [4]_9^{-1} = [7]_9 \qquad [7]_9^{-1} = [4]_9$$

であるから，H は逆元をとる操作でも閉じている．よって，H は乗法群 $(\mathbb{Z}/9\mathbb{Z})^\times$ の部分群である． □

群 G の部分集合 H が G の部分群であることの必要十分条件は，第 1,2 回講義資料命題 1.5 より，

『H が空でなく，任意の $h, k \in H$ に対し，$h \cdot k \in H$ かつ $h^{-1} \in H$ となること』

であった．部分群であるかどうかの判定についてはこの条件を確認すれば良い．

なお，$[4]_9^3 = [64]_9 = [1]_9$ に注意すると，任意の $k \in \mathbb{Z}$ に対し，$[4]_9^k$ は

$$[4]_9^0 = [1]_9 \qquad [4]_9^1 = [4]_9 \qquad [4]_9^2 = [16]_9 = [7]_9$$

のいずれかに一致することがわかる．よって，

$$H = \{[4]_9^k \mid k \in \mathbb{Z}\}$$

である．これより，任意の $k_1, k_2 \in \mathbb{Z}$ に対し，

$$[4]_9^{k_1}[4]_9^{k_2} = [4]_9^{k_1+k_2} \in H, \qquad ([4]_9^{k_1})^{-1} = [4]_9^{-k_1} \in H$$

となるので，この考え方でも H が $(\mathbb{Z}/9\mathbb{Z})^\times$ の部分群であることがわかる．このように 1 つの元 (ここでは $[4]_9$) から二項演算および逆元を取る操作を何度も繰り返して得られる元を集めてできているような群を**巡回群**と言う．これは今後の講義内でも登場する． □