

# 代数学 I 第 6 回復習レポート課題解答例

担当：大矢 浩徳 (OYA Hironori)\*

## 問題 1

$D_8$  の以下の部分集合  $H$  が  $D_8$  の部分群となるかどうかを判定せよ。

$$H = \{e, \sigma^3, \sigma^6\}$$

ただし、二面体群の元については第 5 回講義資料の記号を用いる。以下の問題でも同様。

問題 1 解答例. 部分群とならない □

問題 1 補足解説.  $\sigma^6 \in H$  であるが,

$$\sigma^6 \sigma^6 = \sigma^{12} = \sigma^4 \notin H$$

である。よって、 $H$  は二項演算で閉じておらず、部分群でない。 □

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、

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

であった。このため、部分群であるかどうかを確かめるときはこの条件を確認すればよい。また、 $D_n$  における二項演算の計算は、以下の  $\sigma, \tau$  に関する関係式を用いて行うのであったということも合わせて思い出そう。

$D_n$  において以下が成立する。

- (1)  $\sigma^n = e$ . したがって、任意の  $k, l \in \mathbb{Z}$  に対し、 $\sigma^{k+ln} = \sigma^k$ .
- (2)  $\tau^2 = e$ . すなわち、 $\tau^{-1} = \tau$ .
- (3) 任意の  $k \in \mathbb{Z}$  に対し、 $\tau \sigma^k = \sigma^{-k} \tau$ .

本問の場合、 $\sigma^8 = e$  となるので、 $\sigma^{12} = \sigma^4$  となる。 □

## 問題 2

$D_6$  において、 $\{\sigma^2, \tau\}$  が生成する部分群  $\langle \{\sigma^2, \tau\} \rangle$  として正しいものを選択せよ。

- (1)  $\{\sigma^2, \tau\}$
- (2)  $\{e, \sigma^2, \tau, \sigma^2 \tau\}$
- (3)  $\{e, \sigma^2, \sigma^4, \tau, \sigma^2 \tau, \sigma^4 \tau\}$
- (4)  $D_6$

問題 2 解答例. (3) □

問題 2 補足解説.  $H = \{e, \sigma^2, \sigma^4, \tau, \sigma^2 \tau, \sigma^4 \tau\}$  とすると、 $H$  の全ての元は  $\sigma^2, \tau$  らに二項演算 (と逆元を取る操作) を繰り返し施すことで得られるので

$$H \subset \langle \{\sigma^2, \tau\} \rangle$$

\* e-mail: hoyo@shibaura-it.ac.jp

である. 一方,  $\{\sigma^2, \tau\} \subset H$  でもあるから, あとは  $H$  が  $D_6$  の部分群であることが示されれば,  $\langle \{\sigma^2, \tau\} \rangle$  が  $\{\sigma^2, \tau\}$  を含む  $D_6$  の部分群の中で最も小さいことにより (第 6 回講義資料命題 5.3),  $H \supset \langle \{\sigma^2, \tau\} \rangle$  の方も示され,  $H = \langle \{\sigma^2, \tau\} \rangle$  がわかる. いま,  $H$  の元らの間の二項演算の結果は以下の表ようになる.

	$e$	$\sigma^2$	$\sigma^4$	$\tau$	$\sigma^2\tau$	$\sigma^4\tau$
$e$	$e$	$\sigma^2$	$\sigma^4$	$\tau$	$\sigma^2\tau$	$\sigma^4\tau$
$\sigma^2$	$\sigma^2$	$\sigma^4$	$e$	$\sigma^2\tau$	$\sigma^4\tau$	$\tau$
$\sigma^4$	$\sigma^4$	$e$	$\sigma^2$	$\sigma^4\tau$	$\tau$	$\sigma^2\tau$
$\tau$	$\tau$	$\sigma^4\tau$	$\sigma^2\tau$	$e$	$\sigma^4$	$\sigma^2$
$\sigma^2\tau$	$\sigma^2\tau$	$\tau$	$\sigma^4\tau$	$\sigma^2$	$e$	$\sigma^4$
$\sigma^4\tau$	$\sigma^4\tau$	$\sigma^2\tau$	$\tau$	$\sigma^4$	$\sigma^2$	$e$

ただし,  $g$  行  $g'$  列に  $gg'$  を書くというルールで表を書いている. この表に現れる元が全て  $H$  の元であることは  $H$  が二項演算で閉じていることを表しており, 各行 (あるいは各列) に単位元  $e$  があることが,  $H$  のそれぞれの元の逆元が  $H$  内に存在することを意味している. これより,  $H$  が  $D_6$  の部分群となることがわかる.  $\square$

### 問題 3

$D_7$  において,  $\{\sigma^2\}$  が生成する部分群  $\langle \sigma^2 \rangle$  として正しいものを選択せよ.

- (1)  $\{\sigma^2\}$
- (2)  $\{e, \sigma^2, \sigma^4, \sigma^6\}$
- (3)  $\{e, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \sigma^6\}$
- (4)  $D_7$

問題 3 解答例. (3)  $\square$

問題 3 補足解説. 一般に群  $G$  とその元  $g$  が与えられたときに,  $g$  が生成する部分群  $\langle g \rangle$  は,

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

となる. 本問の場合,

$$\langle \sigma^2 \rangle = \{\sigma^{2n} \mid n \in \mathbb{Z}\}$$

である. 特に,  $\langle \sigma^2 \rangle$  の元は全て  $\sigma^k$  の形をしていることがわかる. ここで,  $D_7$  においては,

$$\sigma^8 = \sigma, \quad \sigma^{10} = \sigma^3, \quad \sigma^{12} = \sigma^5$$

であることに注意すると, 結局  $D_7$  における  $\sigma^k$  の形の元は全て  $\langle \sigma^2 \rangle$  に含まれることがわかる. よって,

$$\langle \sigma^2 \rangle = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \sigma^6\}$$

である.  $\square$

### 問題 4

2 次一般線形群  $GL_2(\mathbb{R})$  の元  $\begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix} \in GL_2(\mathbb{R})$  の位数を半角数字で入力せよ.

問題 4 解答例. 6  $\square$

問題 4 補足解説. 群  $G$  の元  $g$  に対し,  $g$  の位数  $\text{ord } g$  は  $g^m = e$  を満たす最小の  $m \in \mathbb{Z}_{>0}$  であった (第 6 回講義資料命題 5.5).  $GL_2(\mathbb{R})$  における二項演算は行列の積, 単位元は単位行列であったので,

$$\begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}^m = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

を満たす最小の  $m \in \mathbb{Z}_{>0}$  を求めれば良い。これは直接計算で求めても良いが、少し抽象的に解説してみよう。一般に、

$$R(\theta) := \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

とすると、線形写像  $\mathbb{R}^2 \rightarrow \mathbb{R}^2, \mathbf{v} \mapsto R(\theta)\mathbf{v}$  は  $\mathbb{R}^2$  における反時計回り  $\theta$  回転を表す変換であり、 $R(\theta)$  は**回転行列**と呼ばれるのであった。加法定理により、 $\theta, \theta' \in \mathbb{R}$  に対し、

$$R(\theta)R(\theta') = R(\theta + \theta') \quad (*)$$

が成立する。これは、「 $\theta'$  回転をしてから  $\theta$  回転をすると結果的に  $\theta + \theta'$  回転している」という事実を表している。さて、本問の行列は

$$\begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix} = \begin{pmatrix} \cos(\pi/3) & -\sin(\pi/3) \\ \sin(\pi/3) & \cos(\pi/3) \end{pmatrix} = R(\pi/3)$$

である。よって、(\*) より、 $m \in \mathbb{Z}_{>0}$  に対し、

$$R(\pi/3)^m = R(m\pi/3)$$

となる。これより、 $R(\pi/3)^m$  が単位行列となる  $m \in \mathbb{Z}_{>0}$  は  $m\pi/3$  が  $2\pi$  の整数倍となる  $m$  であり、この中で最小の  $m$  は 6 である。□

#### 問題 5

$\mathfrak{S}_8$  の元

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 5 & 8 & 7 & 4 & 2 & 6 \end{pmatrix}$$

の位数を求めよ。

問題 5 解答例. 15 □

問題 5 補足解説. 問題 4 補足解説で述べたように、位数を求めるためには、

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 5 & 8 & 7 & 4 & 2 & 6 \end{pmatrix}^m = e$$

を満たす最小の  $m \in \mathbb{Z}_{>0}$  を求めれば良い。これは直接計算で求めても良いが、計算が大変なので少し工夫して第 6 回講義資料例 6 の方法で求めてみよう。まず、与えられた元を互いに素な巡回置換の合成として書くと、

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 5 & 8 & 7 & 4 & 2 & 6 \end{pmatrix} = (1\ 3\ 5\ 7\ 2)(4\ 8\ 6)$$

である(この方法について第 4 回講義資料 p.9 を参照)。ここで、互いに素な巡回置換の可換性(第 4 回講義資料命題 3.6)より、

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 5 & 8 & 7 & 4 & 2 & 6 \end{pmatrix}^m = (1\ 3\ 5\ 7\ 2)^m (4\ 8\ 6)^m$$

である。これが単位元  $e$  となるのは  $(1\ 3\ 5\ 7\ 2)^m = e$  かつ  $(4\ 8\ 6)^m = e$  となるときである。前者が成り立つのは、 $m$  が 5 の倍数のとき、後者が成り立つのは  $m$  が 3 の倍数のときなので(第 4 回講義資料命題 3.4)、これらが同時に成り立つのは  $m$  が 15 の倍数のときである。よって、 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 5 & 8 & 7 & 4 & 2 & 6 \end{pmatrix}^m = e$  を満たす正の整数  $m$  で最小のものは 15 である。□

一般に  $\sigma \in \mathfrak{S}_n$  がどの 2 つも互いに素な巡回置換  $\sigma_1, \dots, \sigma_s$  を用いて、

$$\sigma = \sigma_1 \cdots \sigma_s$$

と書けるとき、互いに素な巡回置換の可換性より、各  $m \in \mathbb{Z}$  に対し、

$$(\sigma_1 \cdots \sigma_s)^m = \sigma_1^m \cdots \sigma_s^m$$

が成立する. これが単位元  $e$  となるのは

$$\sigma_1^m = \cdots = \sigma_s^m = e \quad (**)$$

となるときであるが,  $\ell = 1, \dots, s$  に対し,  $\sigma_\ell^m = e$  となるのは,  $m$  が  $\#S(\sigma_\ell)$  の倍数のときなので,  $(**)$  が成り立つのは  $m$  が  $\#S(\sigma_1), \dots, \#S(\sigma_s)$  の最小公倍数  $L$  のときである. よって,

$$\text{ord } \sigma = L$$

である.

□