数学演習 VII・VIII　4 月 25 日分解答[*1]

担当: 柳田伸太郎 (理学部 A 館 441 号室)
yanagida [at] math.nagoya-u.ac.jp
https://www.math.nagoya-u.ac.jp/~yanagida/2019S78.html

3　群論 1 (基本概念)

3.1　群の定義

問題 3.1. 群の 3 条件を確認する.
(結合律) $A=(a_{i,j}), B=(b_{i,j}), C=(c_{i,j}) \in \mathrm{GL}_n(\mathbb{C})$ に対し $(AB)C=A(BC)$ を示せばよい. AB の (i,j) 成分が $\sum_{k=1}^n a_{i,k}b_{k,j}$ となることから, $(AB)C$ の (i,j) 成分は $\sum_{l=1}^n(\sum_{k=1}^n a_{i,k}b_{k,l})c_{l,j}$. 同様に $A(BC)$ の (i,j) 成分は $\sum_{k=1}^n a_{i,k}(\sum_{l=1}^n b_{k,l}c_{l,j})$. $\mathbb{C}$ が環であることから両者は一致する.
(単位元) 単位行列 $I_n \in \mathrm{GL}_n(\mathbb{C})$ は任意の $A \in \mathrm{GL}_n(\mathbb{C})$ に対し $AI_n=I_nA=A$ を満たすので, 今考えている積に関する単位元である.
(逆元の存在) $A \in \mathrm{GL}_n(\mathbb{C})$ の逆行列 $A^{-1} \in \mathrm{GL}_n(\mathbb{C})$ は $AA^{-1}=A^{-1}A=I_n$ を満たす.

問題 3.2. $n=1$ なら可換群であり, $n \geq 2$ なら可換群ではない.

3.2　元の位数, 有限群の位数, 巡回群

問題 3.3. (1) $G \neq \{e\}$ と仮定してよい. 任意の元 $g \in G \setminus \{e\}$ について $\{g^n \mid n \in \mathbb{Z}\}$ を考えると, これは G の部分集合. G は有限集合だから, ある $m,n \in \mathbb{Z}$ が存在して $m \neq n$ かつ $g^m=g^n$. これから $g^{|m-n|}=e$ となり, g の位数は $|m-n|$ 以下である.
(2) $m,n \in \mathbb{Z}$ が互いに素なので, $am+bn=1$ となる $a,b \in \mathbb{Z}$ がある. すると $g=g^{am+bn}=(g^m)^a(g^n)^b=ee=e$.

問題 3.4. $|S_n|=n!$.

問題 3.5. $\zeta_n := \exp(2\pi\sqrt{-1}/n)$ とすれば, $\zeta_n \in G$ でかつ ζ_n の位数は n. また $G=\{\zeta_n^k \mid k=0,1,\dots,n-1\}=\langle\zeta_n\rangle$ となるので, G は位数 n の巡回群.

問題 3.6. 群であることの証明は略. $\mathbb{Z}/n\mathbb{Z}=\langle\overline{1}\rangle$, $\overline{1}$ の位数は n になるので, $\mathbb{Z}/n\mathbb{Z}$ は位数 n の巡回群である.

問題 3.7. (1) x 軸の正の部分の上にある頂点の番号 k $(1 \leq k \leq n)$ に注目して n 通り.
(2) P_n の表が上のときと裏が上のときの各々に対して (1) を適用して, 全部で $2n$ 通り. これらの置き方をそれぞれ (表, k), (裏, k) と書くことにする.
(3) $a^n=1$ と $b^2=1$ は明らか. $ba=a^{-1}b$ は, 例えば (表, 1) が両辺でどの置き方に変わるかを調べれば分かる. 実際, ba によって (表, 1) $\mapsto$ (表, 2) $\mapsto$ (裏, 2) であり, $a^{-1}b$ によって (表, 1) $\mapsto$ (裏, 1) $\mapsto$ (裏, 2) である.
　または a と b を一次変換の行列で表示するか, 複素数の掛け算と複素共役で表して証明できる.
(4) $a^n=1$ より $0 \leq k \leq n-1$ としてよい. このとき (3) の $ba=a^{-1}b$ を繰り返し用いて $ba^k=(ba)a^{k-1}=(a^1b)a^{k-1}=a^{-2}ba^{k-2}=\cdots=a^{-k}b$. また, このとき $(a^kb)^2=a^k(ba^k)b=a^ka^{-k}bb=1$.
(5) $\{1,a,a^2,\dots,a^{n-1},b,ab,a^2b,\dots,a^{n-1}b\} \subset D_n$ は明らかなので, 任意の $g \in D_n$ が a^k または a^kb の形に書けることを示せばよい. ここで g によって置き方 (表, 1) が移った置き方に注目する. g : (表, 1) $\mapsto$ (表, k) のとき $g=a^k$ であり, g : (表, 1) $\mapsto$ (裏, k) のとき $g=a^kb$ である.

[*1] 2019/04/25 版, ver. 0.2.

3.3　部分群, 正規部分群

問題 3.8. まず部分群であることを示す. 単位行列は $\mathrm{SL}_n(\mathbb{C})$ の元である. $A, B \in \mathrm{SL}_n(\mathbb{C})$ なら $\det(AB) = \det A \det B = 1$ より $AB \in \mathrm{SL}_n(\mathbb{C})$. また $A \in \mathrm{SL}_n(\mathbb{C})$ なら $\det(A^{-1}) = (\det A)^{-1} = 1$ より $A^{-1} \in \mathrm{SL}_n(\mathbb{C})$. よって $\mathrm{SL}_n(\mathbb{C})$ は $\mathrm{GL}_n(\mathbb{C})$ の部分群. 次に任意の $A \in \mathrm{SL}_n(\mathbb{C})$ と $B \in \mathrm{GL}_n(\mathbb{C})$ を取ると, $\det(B^{-1}AB) = (\det B)^{-1} \det A \det B = 1$ なので $B^{-1}AB \in \mathrm{SL}_n(\mathbb{C})$. よって $\mathrm{SL}_n(\mathbb{C}) \triangleleft \mathrm{GL}_n(\mathbb{C})$.

問題 3.9.　(1) 問題文中の s_1s_2 の計算を使うと, $s_1s_2s_1$ は

$$s_1s_2s_1 \;=\; (s_1s_2)s_1 \;=\; \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \circ \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

となる. 同様に $s_2s_1s_2$ が次のように計算できて, $s_1s_2s_1 = s_2s_1s_2$ が分かる.

$$s_2s_1s_2 \;=\; s_2(s_1s_2) \;=\; \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} \circ \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

(2) $s_1^2 = s_2^2 = \mathrm{id}$ と (1) の $s_1s_2s_1 = s_2s_1s_2$ から以下のようになるので, s_1s_2 の位数は 3.

$$(s_1s_2)^2 \;=\; (s_1s_2s_1)s_2 \;=\; (s_2s_1s_2)s_2 \;=\; s_2s_1 \neq \mathrm{id}, \quad (s_1s_2)^3 \;=\; (s_1s_2)(s_2s_1) \;=\; \mathrm{id}$$

(3) 部分群は以下の 6 個. このうち可換群なのは S_3 以外の 5 つ. 実際, その 5 つは全て巡回群である.

$$\{\mathrm{id}\}, \quad \{\mathrm{id}, s_1\}, \quad \{\mathrm{id}, s_2\}, \quad \{\mathrm{id}, s_1s_2s_1\}, \quad \{\mathrm{id}, s_1s_2, s_2s_1\}, \quad S_3 \;=\; \{\mathrm{id}, s_1, s_2, s_1s_2s_1, s_1s_2, s_2s_1\}.$$

(これで部分群が尽くされることを示すには, 次のように議論すれば良い:
$s_3 := s_1s_2s_1 = s_2s_1s_2$, $c := s_1s_2$ とおく. $s_2s_1 = c^2$ より $S_3 = \{\mathrm{id}, s_1, s_2, s_3, c, c^2\}$ と書ける.
位数 2 の元は s_1, s_2, s_3 の 3 つ, 位数 3 の元は c, c^2 の 2 つ. これらがそれぞれ生成する部分群は $\{\mathrm{id}, s_1\}$, $\{\mathrm{id}, s_2\}$, $\{\mathrm{id}, s_3\}$, $\{\mathrm{id}, c, c^2\}$ の 4 つ.
部分群 $H \subset S_3$ が位数 2 の異なる 2 元 s, s' を含むと仮定する. 残りの位数 2 の元は s と s' のいくつかの積で書ける. また積 ss' は c または c^2 である. 従って必ず $H = S_3$ となる.
次に部分群 $H \subset S_3$ が位数 2 の元 s と位数 3 の元 t を含むとする. 積 st は位数 2 の元 $s' \neq s$ になるので, 再び s, s' について前の議論を適用して, $H = S_3$ となることが分かる.)

3.4　直積群, 群の同型

問題 3.10. 略.

問題 3.11. 問題 3.5 の群 G の生成元 ζ_n を用いて, 写像 $f : G \to \mathbb{Z}/n\mathbb{Z}$ を $f(\zeta_n^k) := k \bmod n$ で定めると, これは群の同型写像を与える.

問題 3.12. $G := (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ が位数 6 の巡回群であることを示せばよい. $\mathbb{Z}/3\mathbb{Z} = \langle a \rangle$, $\mathbb{Z}/2\mathbb{Z} = \langle b \rangle$ と書く. ただし $a^3 = 1$, $b^2 = 1$. このとき $G = \langle a \rangle \times \langle b \rangle$ の積は $(a^i, b^j) \cdot (a^k, b^l) = (a^{i+k}, b^{j+l})$ と書ける. ここで $\alpha := (a, b) \in \langle a \rangle \times \langle b \rangle$ とおけば $\langle \alpha \rangle = \{1, \alpha, \ldots, \alpha^5\} = G$ が成り立つ. よって G は $\mathbb{Z}/6\mathbb{Z}$ と同型である.

問題 3.13. $\mathbb{Z}/8\mathbb{Z}$ と $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ は可換群である. 一方で, D_4 は可換群ではない. 実際, 問題 3.7 の記号で $ab = ba^{-1} = ba^3 \neq ba$. よって，最初の 2 つの群と D_4 は同型とはならない.

次に, $\mathbb{Z}/8\mathbb{Z}$ と $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ が同型でないこと示す. そのためには $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ が巡回群でないことを示せばよい. 問題 3.12 の解答と同様に $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) = \langle a \rangle \times \langle b \rangle$ と書く. ただし $a^4 = b^2 = 1$ である. このとき, 任意の元 $\alpha = (a^i, b^j) \in \langle a \rangle \times \langle b \rangle$ に対して $\alpha^4 = (a^{4i}, b^{4j}) = (1, 1)$ が成り立つので, 8 乗して初めて単位元になるような元は存在しない. よって $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ は巡回群ではない.

以上です.