# 数学演習 VII・VIII 4 月 26 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

## 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.** (1) 仮定 $ge' = g$ において $g = e$ として $e'e = e$. 一方で単位元の性質 $ge = g$ において $g = e'$ として $e'e = e'$. 従って $e' = e'e = e$.
(2) まず逆元が一意であることに注意する. 実際, $xg = gx = e$ なら $x = xe = x(gg^{-1}) = (xg)g^{-1} = eg^{-1} = g^{-1}$ となって $x = g^{-1}$. まず前半について, 結合律から $(h^{-1}g^{-1}) \cdot (gh) = (gh) \cdot (h^{-1}g^{-1}) = e$ が従うので $h^{-1}g^{-1} = (gh)^{-1}$. 次に後半について, $g^{-1}g = gg^{-1} = e$ から $g$ は $g^{-1}$ の逆元なので $g = (g^{-1})^{-1}$.

**問題 3.3.** $n = 1$ 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 3.4.** (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 3.5.** $|S_n| = n!$.

**問題 3.6.** $\zeta_n := \exp(2\pi\sqrt{-1}/n)$ とすれば, $\zeta_n \in G$ でかつ $\zeta_n$ 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 3.7.** 問題 3.6 の記号 $\zeta_n$ を使うと, 答えは $\zeta_6^k$, $k = 1, 5$.

**問題 3.8.** 問題 3.6 の記号 $\zeta_n$ を使うと, 答えは $\zeta_5^k$, $k = 1, 2, 3, 4$.

**問題 3.9.** 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.

[*1] 2018/04/24 版, ver. 0.1.

**問題 3.10.** (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．
(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 $ba^k = (ba)a^{k-1} = (a^1 b)a^{k-1} = a^{-2}ba^{k-2} = \cdots = a^{-k}b$. また, このとき $(a^k b)^2 = a^k(ba^k)b = a^k a^{-k} bb = 1$.
(5) $\{1, a, a^2, \ldots, a^{n-1}, b, ab, a^2 b, \ldots, a^{n-1}b\} \subset D_n$ は明らかなので, 任意の $g \in D_n$ が $a^k$ または $a^k b$ 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 $g = a^k b$ である．

あるいは，運動は $a, a^{-1}, b, b^{-1}$ の任意回の合成で書けるので, これらが全て $a^i b^j$ の形に書き直せることを (3) を用いて示せばよい.

## 3.3　部分群, 正規部分群

**問題 3.11.** まず部分群であることを示す．$A, B \in \mathrm{SL}_n(\mathbb{C})$ 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 $\mathrm{SL}_n(\mathbb{C}) \triangleleft \mathrm{GL}_n(\mathbb{C})$.

## 3.4　直積群, 群の同型

**問題 3.12.** 略.

**問題 3.13.** 問題 3.6 の群 $G$ の生成元 $\zeta_n$ 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 3.14.** $G := (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ 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 3.15.** $\mathbb{Z}/8\mathbb{Z}$ 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 3.10 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 3.14 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.

## 連絡事項

4/26 のオフィスアワーはお休みさせて頂きます.

以上です.