代数学 I 第 7 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

これまでの講義では様々な群と部分群の例を見てきた．今回からは少し抽象的に群に関する一般論を解説してゆく．抽象度は上がるが，常にこれまで勉強してきたような様々な具体例を頭に浮かべながらついてきてほしい．今回は，群が与えられた時にその部分群を構成する一般的な方法について解説を行う．以下では，群の単位元をしばしば断り無く e と書く．さらに，群の元 g, h に対し，それらの二項演算の結果 gh を与えることを，g と h を「掛ける」という言い方をすることにする．

6.1 自明な部分群

まず，ウォーミングアップとして自明な例を書いておこう．数学において自明な例は面白いものでは無いが，きちんと意識しておくことはいつも大事である．

定義 6.1

G を群とする．このとき，

- 単位元のみからなる G の部分集合 $\{e\}$
- G 自身

はどちらも G の部分群である．これらを G の**自明な部分群**という．

6.2 部分集合の生成する部分群

群 G の部分集合が与えられるとそこから G の部分群を生成することができる．

定義 6.2

S を群 G の任意の部分集合とする．このとき，

$$\langle S\rangle \coloneqq \{g_1^{m_1}\cdots g_k^{m_k} \mid g_i \in S, m_i \in \mathbb{Z}\ (i=1,\dots,k), k \in \mathbb{N}\} (\subset G)$$

とする．言葉で書くと，$\langle S\rangle$ は「S の元とその逆元たちを何度も掛けてできる元全体のなす集合」である．このとき，$\langle S\rangle$ は定義から明らかに二項演算と逆元を取る操作で閉じており，G の部分群となる．これを，S **で生成される部分群**という．
$G = \langle S\rangle$ となるとき，S は G **を生成する**と言い，S を G **の生成系**と言う．また，このとき S の元は**生成元**と呼ばれる．

例えば，S が $S = \{a, b, c\}$ という 3 つの元からなる集合であった場合，$\langle S\rangle$ は

$$e(=a^0),\ a,\ ab^2,\ ac^2b^{-3}a,\ b^4c^{-2}a^{-1}b^2c^4b^2c^{-6}a,\ c^{-2}, \cdots$$

などを全て集めてきてできる集合である．これは二項演算と逆元を取る操作で閉じているということも明らかであろう．例えば，ab^2 と $ac^2b^{-3}a$ を掛けてできる元は $ab^2ac^2b^{-3}a$ なのでやはり $\langle S\rangle$ の元であり，$b^4c^{-2}a^{-1}b^2c^4b^2c^{-6}a$ の逆元 $a^{-1}c^6b^{-2}c^{-4}b^{-2}ac^2b^{-4}$ も $\langle S\rangle$ の元である．

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

命題 6.3

群 G の部分集合 S に対し，$\langle S\rangle$ は S を含む最小の部分群である．

証明. H を S を含む G の部分群としたとき，$\langle S\rangle \subset H$ となることを言えば良い．第 1,2 回講義資料命題 1.5 より，H は二項演算と逆元を取る操作で閉じていることから，H は S の元とその逆元たちを何度も掛けてできる元を全て含んでいる．つまり $\langle S\rangle \subset H$ である． □

以下の命題は群の生成系の例を与える．

命題 6.4

n を 2 以上の整数としたとき，以下が成立する．

(1) n 次対称群 $\mathfrak{S}_n$ は隣接互換のなす集合 $\{(1\ 2), (2\ 3), \ldots, (n-1\ n)\}$ によって生成される．つまり，$\langle\{(1\ 2), (2\ 3), \ldots, (n-1\ n)\}\rangle = \mathfrak{S}_n$ である．

(2) n 次交代群 $\mathfrak{A}_n$ は 3 文字の巡回置換のなす集合 $\{(i\ j\ k) \mid i, j, k$ は相異なる $\{1, \ldots, n\}$ の元 $\}$ によって生成される．つまり，$\langle\{(i\ j\ k) \mid i, j, k$ は相異なる $\{1, \ldots, n\}$ の元 $\}\rangle = \mathfrak{A}_n$ である．

(3) $n+1$ 次二面体群 D_{n+1} は $\{\sigma, \tau\}$ によって生成される．つまり，$\langle\{\sigma, \tau\}\rangle = D_{n+1}$ である．ここで，σ, τ は第 6 回講義資料 5.2 節のものとする．

証明. (1) は第 5 回講義資料定理 4.7 (1) の言い換えであり，(3) は二面体群の定義より明らかである．よって，(2) のみ証明する．i, j, k が相異なる $\{1, \ldots, n\}$ の元のとき，

$$(i\ j\ k) = (i\ j)(j\ k)$$

となるので，第 6 回講義資料定理 5.4 より，

$$\operatorname{sgn}(i\ j\ k) = (-1)^2 = 1$$

である．よって，$S \coloneqq \{(i\ j\ k) \mid i, j, k$ は相異なる $\{1, \ldots, n\}$ の元 $\} \subset \mathfrak{A}_n$．さらに，$\mathfrak{A}_n$ は $\mathfrak{S}_n$ の部分群だったので，命題 6.3 より，$\langle S\rangle \subset \mathfrak{A}_n$．よって，あとは $\mathfrak{A}_n$ の任意の元 σ' が S の元の合成として表されることを証明すればよい．(1) より σ' は隣接互換らの合成として表されるが，第 6 回講義資料定理 5.4 より，そこに用いられる隣接互換の個数は必ず偶数個である．よって，任意の隣接互換 2 つの合成が S の元の合成として表されることを証明すればよい．ここで，

$$(i\ i+1)(j\ j+1) = \begin{cases} e & i = j \text{ のとき}, \\ (i\ i+1\ i+2) & j = i+1 \text{ のとき}, \\ (i+1\ i\ i-1) & j = i-1 \text{ のとき}, \\ (i\ i+1\ j)(j\ j+1\ i+1) & |j-i| \geq 2 \text{ のとき}, \end{cases}$$

となることが直接計算で確かめられる．よって，示すべきことは全て示された． □

注意 1. 3 文字の巡回置換 $(i\ j\ k)$ は本質的には $i < j < k$ となるか $i > j > k$ となるかの 2 通りである（$(i\ j\ k) = (j\ k\ i) = (k\ i\ j)$ であることに注意せよ）．ここで，$i > j > k$ のとき，

$$(i\ j\ k) = (k\ j\ i)^2$$

となるので，$i > j > k$ となる 3 文字の巡回置換 $(i\ j\ k)$ は $i' < j' < k'$ となる巡回置換 $(i'\ j'\ k')$ の合成で得られると言える．よって，命題 6.4 (2) においては生成系 $\{(i\ j\ k) \mid i, j, k$ は相異なる $\{1, \ldots, n\}$ の元 $\}$ を $\{(i\ j\ k) \mid 1 \leq i < j < k \leq n\}$ まで小さくしてもよい．

ここで，部分群に関する基本的な性質も述べておこう．

命題 6.5

G を群とし，$\{H_i \mid i \in I\}$ を G の部分群のなす集合とする（I は部分群を添え字付ける適当な集合で，有限集合であっても無限集合であってもよい）．このとき，これらの部分群の共通集合 $\bigcap_{i\in I} H_i$ も再び G の部分群である．

注意 2. 命題 6.5 の設定で，部分群の和集合 $\bigcup_{i\in I} H_i$ は部分群とはならない．例えば，第 2 回本レポート課題解答問題 1 補足解説 (G_1 についての解説) を参照せよ．$\bigcup_{i\in I} H_i$ を含む最小の部分群を考えるためには $\bigcup_{i\in I} H_i$ で生成される部分群 $\langle \bigcup_{i\in I} H_i \rangle$ を考える必要がある．これはベクトル空間 V の部分空間の集まり $\{W_i \mid i \in I\}$ があった時に，$\bigcap_{i\in I} W_i$ は部分空間となるが，$\bigcup_{i\in I} W_i$ は部分空間とはならないということと対応している．ベクトル空間 V は加法によって群になっていたということを思い出そう (第 1,2 回講義資料例 4).

命題 6.5 の証明. 第 1,2 回講義資料命題 1.4 (3) より，全ての H_i は G の単位元 e を含むので，$e \in \bigcap_{i\in I} H_i$. 特に $\bigcap_{i\in I} H_i$ は空集合ではない．次に $h, k \in \bigcap_{i\in I} H_i$ とすると，第 1,2 回講義資料命題 1.5 より全ての $i \in I$ に対して，

$$hk \in H_i \qquad \text{かつ} \qquad h^{-1} \in H_i.$$

よって，

$$hk \in \bigcap_{i\in I} H_i \qquad \text{かつ} \qquad h^{-1} \in \bigcap_{i\in I} H_i.$$

これより，第 1,2 回講義資料命題 1.5 から，$\bigcap_{i\in I} H_i$ は G の部分群である． □

命題 6.5 を用いると，部分集合 S で生成される部分群 $\langle S \rangle$ は以下のようにも記述できる．この記述は具体計算には向かないが，理論的には重要である．

命題 6.6

群 G の部分集合 S に対し，$\mathscr{S} := \{H \mid H \text{ は } S \text{ を含む } G \text{ の部分群 }\}$ とすると，

$$\langle S \rangle = \bigcap_{H\in\mathscr{S}} H$$

である．

証明. まず，自明な部分群 G は S を含むので，$G \in \mathscr{S}$ であり，$\mathscr{S}$ は空集合ではないことに注意する．さて，命題 6.5 より $\bigcap_{H\in\mathscr{S}} H$ は G の部分群である．ここで，H' を S を含む G の部分群とすると，$H' \in \mathscr{S}$ なので，

$$\bigcap_{H\in\mathscr{S}} H \subset H'$$

である．これより，$\bigcap_{H\in\mathscr{S}} H$ も S を含む最小の部分群となるので，命題 6.3 より，$\langle S \rangle = \bigcap_{H\in\mathscr{S}} H$. □

6.3 群の元の位数，巡回群

群 G の 1 元からなる部分集合 $\{g\}$ で生成される部分群は，定義より

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

となる．これを単に $\langle g \rangle$ と書く．$g^m g^{m'} = g^{m+m'} = g^{m'} g^m$ なので $\langle g \rangle$ は可換群である．

例 1. $n \geq 3$ とし，$D_n = \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \ldots, \sigma^{n-1}\tau\}$ を n 次二面体群とする (第 6 回講義資料 5.2 節と同じ記号を用いる)．このとき，

$$\langle \sigma \rangle = \{\sigma^m \mid m \in \mathbb{Z}\} = \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$$

である．なお，

$$\langle \sigma^{-1} \rangle = \{\sigma^{-m} \mid m \in \mathbb{Z}\} = \{\sigma^m \mid m \in \mathbb{Z}\} = \langle \sigma \rangle.$$

となる．一般に群 G とその元 $g \in G$ に対して，同様の計算により $\langle g \rangle = \langle g^{-1} \rangle$ である．

定義 6.7

群 G の各元 $g \in G$ に対し，G の部分群 $\langle g \rangle$ の位数を g **の位数 (order)** といい，$\operatorname{ord} g$ と書く．

ここで，「位数」という用語が群論において 2 通り現れたことに注意しよう．G の位数 (=G の元の個数) と，G の元 g の位数 (上で定義したもの) という概念があるのである．例 1 で述べたように，一般に $\langle g \rangle = \langle g^{-1} \rangle$ なので，$\operatorname{ord} g = \operatorname{ord} g^{-1}$ である．

例 2. 例 1 における計算より，D_n において，

$$\operatorname{ord} \sigma = \#\langle \sigma \rangle = n$$

である．

例 3. $n \in \mathbb{Z}_{>0}$ とし，整数の剰余類群 $\mathbb{Z}/n\mathbb{Z}$ を考える．$a \in \mathbb{Z}_{>0}$ に対して，

$$\langle [a]_n \rangle = \{ [ma]_n \mid m \in \mathbb{Z} \}$$

である ($\mathbb{Z}/n\mathbb{Z}$ における二項演算は $+$ であったことに注意)．このとき，第 3 回本レポート課題解答問題 3 補足解説に書いた定理により，$\{ [ma]_n \mid m \in \mathbb{Z} \}$ の位数は $n/\gcd(a,n)$ である．よって，

$$\operatorname{ord} [a]_n = n/\gcd(a,n).$$

例えば，

$$\operatorname{ord} [2]_7 = 7, \quad \operatorname{ord} [4]_6 = 3, \quad \operatorname{ord} [8]_{12} = 3$$

である．

群の元 g の位数 $\operatorname{ord} g$ の計算は以下の命題を頭に置いておくと行いやすい．

命題 6.8

群 G の元 g に対し，$\operatorname{ord} g$ は $g^m = e$ となる最小の正の整数 m である．ただし，$g^m = e$ となる正の整数が存在しないとき，$\operatorname{ord} g = \infty$ である．

証明. $\operatorname{ord} g = \#\langle g \rangle < \infty$ のとき，ある $m_1, m_2 \in \mathbb{Z}, m_1 < m_2$ が存在して，

$$g^{m_1} = g^{m_2}$$

となる．このとき，両辺に g^{-m_1} を掛けると，

$$e = g^{m_2 - m_1}$$

なので，$g^m = e$ となる正の整数 m は少なくとも 1 つは存在することがわかる．このうち最小のものを ℓ とすると，

$$\langle g \rangle = \{ g^k \mid k \in \mathbb{Z} \} = \{ e, g, \ldots, g^{\ell - 1} \}$$

である．いま示すべきことは，$\ell = \operatorname{ord} g$ なので，あとは $e, g, \ldots, g^{\ell-1}$ が全て異なる元であることを示せばよい．もし，$g^{k_1} = g^{k_2}$ $(0 \leq k_1 < k_2 \leq \ell - 1)$ となったとすると，両辺に g^{-k_1} を掛けることで，$e = g^{k_2 - k_1}$ となるが，$0 < k_2 - k_1 \leq \ell - 1$ なので，これは ℓ の最小性に矛盾する．よって，$0 \leq k_1 < k_2 \leq \ell - 1$ のとき $g^{k_1} = g^{k_2}$ とはならない．よって，$\ell = \operatorname{ord} g$ であることが示された．

また，上の議論により，$\operatorname{ord} g < \infty$ のとき，$g^m = e$ となる正の整数は存在するので，$g^m = e$ となる正の整数が存在しないのであれば，$\operatorname{ord} g = \infty$ である． □

例 4. 巡回置換 $(i_1\ i_2 \cdots i_k) \in \mathfrak{S}_n$ に対し，

$$(i_1\ i_2 \cdots i_k)^m \neq e \quad (1 \leq m \leq k-1), \qquad (i_1\ i_2 \cdots i_k)^k = e$$

である．(前半は定義より容易にわかる．例えば，i_1 の行き先を考えれば良い．後半は第 5 回講義資料命題 4.4 (2)．) よって，$(i_1\ i_2 \cdots i_k)^m = e$ となる最小の整数は k である．よって，

$$\mathrm{ord}(i_1\ i_2 \cdots i_k) = k. \tag{$*$}$$

一般に $\sigma_1, \ldots, \sigma_s$ をどの 2 つも互いに素な巡回置換とする．このとき，第 5 回講義資料命題 4.6 の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．このことから，$\#S(\sigma_1), \ldots, \#S(\sigma_s)$ の最小公倍数を ℓ とすると，$(*)$ より，

$$\mathrm{ord}(\sigma_1 \cdots \sigma_s) = \ell$$

である．例えば，第 5 回講義資料定理 4.7 の直後で扱った $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 2 & 8 & 7 & 6 & 9 & 1 & 5 & 10 & 3 \end{pmatrix} \in \mathfrak{S}_{10}$ を考えると，

$$\sigma = (1\ 4\ 7)(3\ 8\ 5\ 6\ 9\ 10)$$

であり，$\#S((1\ 4\ 7)) = 3, \#S((3\ 8\ 5\ 6\ 9\ 10)) = 6$ なので，

$$\mathrm{ord}\,\sigma = 6$$

である．実際，$\sigma^6 = (1\ 4\ 7)^6(3\ 8\ 5\ 6\ 9\ 10)^6 = e \cdot e = e$ である．

定義 6.9

群 G においてある $g \in G$ が存在して $G = \langle g \rangle$ となるとき，G を**巡回群 (cyclic group)** といい，g を G の**生成元**という．

6.3 節冒頭の計算より，巡回群は可換群である．また，生成元の取り方は 1 つとは限らない ($\langle g \rangle = \langle g^{-1} \rangle$ なので，g が生成元であれば少なくとも g^{-1} は生成元である)．以下の命題は定義からすぐにわかる．

命題 6.10

群 G の元 g に対し，以下の同値関係が成立する．

(1) $\mathrm{ord}\, g = 1 \Leftrightarrow g = e$.

(2) G が有限群のとき，

$$\mathrm{ord}\, g = \#G \Leftrightarrow G \text{ は巡回群で，} g \text{ はその生成元}$$

例 5. 以下が巡回群，巡回群でないものの例である．

- $n, a \in \mathbb{Z}_{>0}$ を互いに素な整数とする．このとき例 3 での計算より，$\mathrm{ord}[a]_n = n$．特に，$\mathrm{ord}[1]_n = n$．よって，$\mathbb{Z}/n\mathbb{Z} = \langle [a]_n \rangle$ であるので，$\mathbb{Z}/n\mathbb{Z}$ は巡回群であり，$[a]_n$ は $\mathbb{Z}/n\mathbb{Z}$ の生成元である．
- $\mathbb{Z} = \langle 1 \rangle$ であるので，加法群 $\mathbb{Z}$ は巡回群であり，1 は $\mathbb{Z}$ の生成元である．ここで，加法群 $\mathbb{Z}$ においては，二項演算が $+$ であることに注意．$\mathrm{ord}\, 1 = \infty$ である．
- $n \in \mathbb{Z}_{>0}$ に対し，乗法群 $\mathbb{C}^\times$ の部分群 $\mu_n := \{e^{\frac{2m\pi}{n} i} \mid m \in \mathbb{Z}\}$ を考える． このとき，$\mu_n = \langle e^{\frac{2\pi}{n} i} \rangle$ であるので，μ_n は巡回群であり，$e^{\frac{2\pi}{n} i}$ は μ_n の生成元である．$\mathrm{ord}\, e^{\frac{2\pi}{n} i} = n$ である．
- $n \geq 3$ のとき，二面体群 D_n は非可換群なので，D_n は特に巡回群ではない．例 2 より，D_n において，$\mathrm{ord}\,\sigma = n$ である．また，任意の $k = 0, 1, \ldots, n-1$ に対し，

  $$(\sigma^k\tau)(\sigma^k\tau) = \sigma^k(\tau\sigma^k)\tau = \sigma^k(\sigma^{-k}\tau)\tau = \tau^2 = e$$

  となるので，$\mathrm{ord}\,\sigma^k\tau = 2$ である．“正 n 角形の板の対称性” という考え方からすると，各 $\sigma^k\tau$ は適当な対称軸に関する折り返しに対応する (正 n 角形の対称軸は n 本あるので，このような元が計 n 個ある)．

6.4 中心，中心化群

最後に一般の群において考えられる部分群をもう一つ学ぼう．

定義 6.11

群 G に対し，

$$Z(G) \coloneqq \{z \in G \mid zg = gz,\ \forall g \in G\}$$

とする．言葉で書くと，$Z(G)$ は「G の全ての元と可換な元を集めてきてできる集合」である．$Z(G)$ を G の**中心 (center)** と呼ぶ[*1]．
より一般に，S を群 G の任意の部分集合とする．このとき，

$$Z(S) \coloneqq \{z \in G \mid zs = sz,\ \forall s \in S\}$$

とする．言葉で書くと，$Z(S)$ は「S の全ての元と可換な元を集めてきてできる集合」である．$Z(S)$ を G における S **の中心化群 (centralizer)** と呼ぶ．

命題 6.12

群 G とその部分集合 S に対し，S の中心加群 $Z(S)$ は G の部分群である．

証明. まず単位元の定義より $es = s = se,\ \forall s \in S$ なので，$e \in Z(S)$．特に $Z(S)$ は空集合ではない．さらに $z_1, z_2 \in Z(S)$ と任意の $s \in S$ に対し，

$$\begin{aligned}&(z_1z_2)s = z_1(z_2s) = z_1(sz_2) = (z_1s)z_2 = (sz_1)z_2 = s(z_1z_2),\\ &z_1^{-1}s = z_1^{-1}sz_1z_1^{-1} = z_1^{-1}z_1sz_1^{-1} = sz_1^{-1}.\end{aligned}$$

となるので，$z_1z_2, z_1^{-1} \in Z(S)$．よって，二項演算と逆元を取る操作について閉じているので，第 1,2 回講義資料命題 1.5 から，$Z(S)$ は G の部分群である． □

例 6. 一般の群 G に対し，

$$Z(\{e\}) = \{z \in G \mid ze = ez\} = G$$

である．また，G が可換群のとき，任意の部分集合 $S \subset G$ に対して，

$$Z(S) = \{z \in G \mid zs = sz,\ \forall s \in S\} = G$$

となる．

例 7. $\mathbb{K} = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$ のとき，

$$Z(GL_2(\mathbb{K})) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \,\middle|\, a \in \mathbb{K}^\times \right\}$$

である．これは以下のように確かめられる．
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{K})$ で $b \neq 0$ 又は $c \neq 0$ のとき，

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 2a & 2b \\ c & d \end{pmatrix} \neq \begin{pmatrix} 2a & b \\ 2c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

となるので，$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \notin Z(GL_2(\mathbb{K}))$．よって，$Z(GL_2(\mathbb{K}))$ の元は $b = c = 0$ を満たす対角行列．

[*1] $Z(G)$ の Z はドイツ語の Zentrum(中心) に由来．

次に，$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in GL_2(\mathbb{K})$ で $a \neq d$ のとき，

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & d \\ 0 & d \end{pmatrix} \neq \begin{pmatrix} a & a \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

となるので，$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \notin Z(GL_2(\mathbb{K}))$．よって，$Z(GL_2(\mathbb{K}))$ の元は $a = d$ を満たす対角行列，つまり単位行列の定数倍の形をしているもののみ．逆に，単位行列の定数倍が任意の $GL_2(\mathbb{K})$ の元と可換であることは容易にわかるので，結局 $Z(GL_2(\mathbb{K})) = \{aI_2 \mid a \in \mathbb{K}^\times\}$ である．同様の方法で，

$$Z(GL_n(\mathbb{K})) = \{aI_n \mid a \in \mathbb{K}^\times\}$$

であることがわかる (I_n は n 次単位行列)．

例 8. $n \geq 3$ のとき，

$$Z(\mathfrak{S}_n) = \{e\}$$

である．これは以下のように確かめられる．

$\mathfrak{S}_n$ の単位元でない元 $\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ を取ってくると，

(i) ある $k = 1, \ldots, \underline{n-1}$ が存在して，$k \neq i_k$ かつ $k+1 \neq i_k$ となる．

(ii) ある $k = 1, \ldots, \underline{n-1}$ が存在して，

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} = \begin{pmatrix} 1 & \ldots & k-1 & k & \cdots & n-1 & n \\ 1 & \ldots & k-1 & k+1 & \cdots & n & k \end{pmatrix}.$$

のいずれかが成立する (理由を考えよ)．(i) のとき，

$$\left((k\ k+1) \circ \begin{pmatrix} 1 & \cdots & k & \cdots & n \\ i_1 & \cdots & i_k & \cdots & i_n \end{pmatrix}\right)(k) = i_k,$$
$$\left(\begin{pmatrix} 1 & \cdots & k+1 & \cdots & n \\ i_1 & \cdots & i_{k+1} & \cdots & i_n \end{pmatrix} \circ (k\ k+1)\right)(k) = i_{k+1},$$

となるので，

$$(k\ k+1) \circ \begin{pmatrix} 1 & \cdots & n \\ i_1 & \cdots & i_n \end{pmatrix} \neq \begin{pmatrix} 1 & \cdots & n \\ i_1 & \cdots & i_n \end{pmatrix} \circ (k\ k+1).$$

これより，$\begin{pmatrix} 1 & \cdots & n \\ i_1 & \cdots & i_n \end{pmatrix} \notin Z(\mathfrak{S}_n)$．(ii) で $k = 1$ のとき，

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} = (1\ 2\ \cdots\ n)$$

であるが，このとき，n が 3 以上であることに注意すると，

$$((1\ 2) \circ (1\ 2\ \cdots\ n))(2) = 3 \quad ((1\ 2\ \cdots\ n) \circ (1\ 2))(2) = 2$$

より，$(1\ 2) \circ (1\ 2\ \cdots\ n) \neq (1\ 2\ \cdots\ n) \circ (1\ 2)$ なので，$(1\ 2\ \cdots\ n) \notin Z(\mathfrak{S}_n)$．(ii) で $k > 1$ のとき，

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} = (k\ k+1\ \cdots\ n)$$

であるが，このとき，

$$((k-1\ k) \circ (k\ k+1\ \cdots\ n))(k) = k+1 \quad ((k\ k+1\ \cdots\ n) \circ (k-1\ k))(k) = k-1$$

より，$(k-1\ k) \circ (k\ k+1\ \cdots\ n) \neq (k\ k+1\ \cdots\ n) \circ (k-1\ k)$ なので，$(k\ k+1\ \cdots\ n) \notin Z(\mathfrak{S}_n)$．

以上より，$Z(\mathfrak{S}_n)$ に含まれる元は単位元のみである．

一般に群の中心を求める簡単な方法はなく，上のように各群に対して “頑張って” 求める必要がある．