群の交換子全体は交換子群と一致するか？

明治大学理工学部数学科
2010 年度藏野研究室卒業論文
妹川 宜弘
玉城 洸史
蛭川 康治
宮島 謙二

2011 年 2 月 21 日

1　はじめに

この論文では、群の交換子全体が交換子群と一致するかどうかを考察する。

群 G の元で、$xyx^{-1}y^{-1}$ の形の元を交換子という。交換子全体が生成する G の部分群は交換子群と呼ばれる。単位元は交換子であり、交換子の逆元は交換子であることが簡単にわかる。しかし、交換子の積が交換子になるとは限らないので、そのために交換子全体は部分群になるとは限らないのである。

群論の教科書で、いつ交換子全体が交換子群と一致するか？また、どのような時に一致しないか？などが扱われているものはほとんどない。そこで、卒業研究として、このテーマを選ぶことにした。

群の交換子全体が交換子群と一致しない例を構成することは、簡単なことではない。実際、非常に多くの群でこれらは一致するのである。

この論文では、第二章で、二面体群 D_{2n}、一般四元数群 Q_{4n}、n 次対称群 $\mathfrak{S}_n$ と n 次交代群 $\mathfrak{A}_n$ では、交換子全体が交換子群になることを証明する。

最後の第三章で、交換子全体と交換子群が一致しない例を挙げる。それは、教科書 [1] で見つけたものである。ここでは、位数 $4096 = 2^{12}$ の有限群で、そのような例が存在することが示される。実際は、交換子全体と交換子群が一致しない位数が最小の群は位数 96 であるらしいが、そのことは、ここでは証明できない。

2　交換子全体が交換子群と一致する例

非常に多くの群では、交換子全体が交換子群と一致している。この章では、代表的な有限群に対して、そのことを確かめてみる。

この論文を通して使われる記号の定義から始める。

定義 2.1 G は、群であるとする。$x,y \in G$ に対して、

$$[x,y] = xyx^{-1}y^{-1} \in G$$

とおき、これを $x,y \in G$ の交換子という。

G の交換子全体の集合を $C(G)$ とおく。つまり、

$$C(G) = \{[x,y] \mid x,y \in G\}.$$

G の交換子全体で生成された群を $D(G)$ と書き、これを G の交換子群ということにする。つまり、

$$D(G) = \langle C(G) \rangle .$$

最初に、交換子に関する基本性質をまとめておく。

2.1　交換子の基本性質

ここでは、交換子、交換子群に関する基本性質をまとめておく。

この論文を通して、e は単位元であるとする。

事実 2.2 G が群であるとする。

(1) 明らかに、$C(G) \ni e$ である。

(2) G がアーベル群であれば、$C(G) = \{e\}$ である。よって、このとき、$D(G) = C(G) = \{e\}$ が成立する。

(3) 交換子の逆元は交換子である。それは、

$$[x,y]^{-1} = \left(xyx^{-1}y^{-1}\right)^{-1} = yxy^{-1}x^{-1} = [y,x]$$

から従う。つまり、$C(G)$ は逆元で閉じている。

(4) 交換子は、共役で閉じている。つまり、$x,y,z \in G$ に対して、

$$z[x,y]z^{-1} = z\left(xyx^{-1}y^{-1}\right)z^{-1} = (zxz^{-1})(zyz^{-1})(zxz^{-1})^{-1}(zyz^{-1})^{-1} = [zxz^{-1}, zyz^{-1}] \tag{1}$$

が成立する。

H が G の正規部分群であるとする。より一般に、$\alpha \in C(H), z \in G$ に対して、$z\alpha z^{-1} \in C(H)$ であることが、式 (1) と同様にして証明できる。

この事実は、後に、交代群の交換子の計算の際、しばしば使われる。

つまり、$C(G)$ が G の部分群になるかどうかは、積について閉じているかどうかで決まる。

2.2 二面体群

次の定理を証明する。

定理 2.3 二面体群 D_{2n} に対して、$D(D_{2n}) = C(D_{2n})$ が成立する。

二面体群 D_{2n} とは次の 2 つの行列 A, B で生成される群 $<A, B>$ のことである。

$$A = \begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

この 2 つの行列 A, B は $A^n = B^2 = E$, $B^{-1}AB = A^{-1}$ を満たす。これより

$$D_{2n} = \{E, A, A^2, \ldots, A^{n-1}, B, BA, BA^2, \ldots, BA^{n-1}\}$$

となる。

ここで、

$$D(D_{2n}) = <[x, y] \mid x, y \in D_{2n}>$$

を考える。交換子 $[x,y]$ の x と y には A^k か BA^l が入るので、次の 4 つの場合に分けて議論する。

1. $x = A^k, y = A^l$ のとき。
2. $x = A^k, y = BA^l$ のとき。
3. $x = BA^k, y = A^l$ のとき。
4. $x = BA^k, y = BA^l$ のとき。

1 の場合

$[x,y] = xyx^{-1}y^{-1} = A^kA^lA^{-k}A^{-l} = E$

2 の場合

$[x,y] = xyx^{-1}y^{-1} = A^kBA^lA^{-k}(BA^l)^{-1} = A^kBA^lA^{-k}A^{-l}B^{-1} = A^k(BA^{-k}B^{-1}) = A^{2k}$

3 の場合

$[x,y] = xyx^{-1}y^{-1} = BA^kA^l(BA^k)^{-1}A^{-l} = BA^kA^lA^{-k}B^{-1}A^{-l} = (BA^lB^{-1})A^{-l} = A^{-2l}$

4 の場合

$$\begin{aligned}[x,y] = xyx^{-1}y^{-1} &= BA^kBA^l(BA^k)^{-1}(BA^l)^{-1} = BA^kBA^lA^{-k}B^{-1}A^{-l}B^{-1} \\ &= BA^k(BA^lA^{-k}B^{-1})A^{-l}B^{-1} = BA^kA^{k-l}A^{-l}B^{-1} = A^{2(l-k)}\end{aligned}$$

以上のことから

$$D(D_{2n}) =< A^2 >$$

となることが分かる。
　一方、任意の k に対して

$$C(D_{2n}) \ni A^k B A^{-k} B^{-1} = A^{2k}$$

であるので

$$C(D_{2n}) = D(D_{2n})$$

となる。

2.3　一般四元数群

　続いて次の定理を証明する。

定理 2.4　一般四元数群 Q_{4n} に対して、$D(Q_{4n}) = C(Q_{4n})$ が成立する。

　一般四元数群 Q_{4n} は次の 2 つの行列 A, B によって生成される群 $<A, B>$ のことである。

$$A = \begin{pmatrix} e^{\frac{\pi i}{n}} & 0 \\ 0 & e^{-\frac{\pi i}{n}} \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

この 2 つの行列 A, B は $A^n = B^2 = -E$, $B^{-1}AB = A^{-1}$ を満たす。このことから

$$Q_{4n} = \{E, A, \ldots, A^{2n-1}, B, BA, \ldots, BA^{2n-1}\}$$

となる。
　ここで、

$$D(Q_{4n}) = <[x, y] \mid x, y \in Q_{4n}>$$

を考える。次の 4 つの場合に分けて議論する。

1. $x = A^k, y = A^l$ の場合。
2. $x = A^k, y = BA^l$ の場合。
3. $x = BA^k, y = A^l$ の場合。
4. $x = BA^k, y = BA^l$ の場合。

1 の場合
　$[x, y] = xyx^{-1}y^{-1} = A^k A^l A^{-k} A^{-l} = E$
2 の場合
　$[x, y] = xyx^{-1}y^{-1} = A^k B A^l A^{-k} (BA^l)^{-1} = A^k (BA^l A^{-k} A^{-l} B^{-1}) = A^{2k}$
3 の場合
　$[x, y] = xyx^{-1}y^{-1} = BA^k A^l (BA^k)^{-1} A^{-l} = (BA^k A^l A^{-k} B^{-1}) A^{-l} = A^{-2l}$

4 の場合

$$[x,y] = xyx^{-1}y^{-1} = BA^kBA^l(BA^k)^{-1}(BA^l)^{-1} = BA^k(BA^lA^{-k}B^{-1})A^{-l}B^{-1}$$
$$= BA^kA^{k-l}A^{-l}B^{-1} = A^{2(l-k)}$$

以上のことから

$$D(Q_{4n}) =< A^2 >$$

となることが分かる。

一方、任意の k に対して、

$$C(Q_{4n}) \ni A^kBA^{-k}B^{-1} = A^{2k}$$

であるので

$$C(Q_{4n}) = D(Q_{4n})$$

となる。

2.4 対称群と交代群

$\mathfrak{S}_n$ は n 次対称群、$\mathfrak{A}_n$ は n 次交代群であるとする。

定理 2.5 任意の自然数 n に対して、$C(\mathfrak{S}_n) = D(\mathfrak{S}_n)$, $C(\mathfrak{A}_n) = D(\mathfrak{A}_n)$ が成立する。

証明

(i) $n = 1$ のとき。このときは、

$$\mathfrak{S}_1 = \mathfrak{A}_1 = \{e\}$$

であり、共にアーベル群である。よって、事実 2.2 (2) によって、

$$C(\mathfrak{S}_1) = D(\mathfrak{S}_1) = \{e\}$$

$$C(\mathfrak{A}_1) = D(\mathfrak{A}_1) = \{e\}$$

が成立する。

(ii) $n = 2$ のとき。このときは、

$$\mathfrak{S}_2 = \{e, (12)\}, \quad \mathfrak{A}_2 = \{e\}$$

であり、共にアーベル群である。よって、事実 2.2 (2) によって、

$$C(\mathfrak{S}_2) = D(\mathfrak{S}_2) = \{e\}$$

$$C(\mathfrak{A}_2) = D(\mathfrak{A}_2) = \{e\}$$

が成立する。

(iii) $n = 3$ のとき。

$$\mathfrak{A}_3 = \{e, (123), (132)\}$$

である。$\mathfrak{A}_3$ はアーベル群なので、事実 2.2 (2) によって、

$$C(\mathfrak{A}_3) = D(\mathfrak{A}_3) = \{e\}$$

が成立する。

次に、

$$\mathfrak{S}_3 = \{e, (12), (13), (23), (123), (132)\}$$

を扱う。まず、$\mathfrak{A}_3 \subset C(\mathfrak{S}_n)$ となることを証明する。

$$e \in C(\mathfrak{S}_n) \tag{2}$$

$$(12)(13)(12)^{-1}(13)^{-1} = (23)(13) = (123) \in C(\mathfrak{S}_3) \tag{3}$$

$C(\mathfrak{S}_3)$ は共役で閉じている (事実 2.2 の (4)) ので、

$$(23)(123)(23)^{-1} = (132) \in C(\mathfrak{S}_3). \tag{4}$$

(2), (3), (4) より、$\mathfrak{A}_3 \subset C(\mathfrak{S}_n) \subset D(\mathfrak{S}_3)$ が成立する。

一方、$\mathfrak{S}_3$ のすべての交換子は偶置換であるので、

$$C(\mathfrak{S}_3) \subset \mathfrak{A}_3.$$

よって、

$$C(\mathfrak{S}_3) = \mathfrak{A}_3$$

が成立する。故に、

$$D(\mathfrak{S}_3) = <C(\mathfrak{S}_3)> = \mathfrak{A}_3$$

であるので

$$C(\mathfrak{S}_3) = D(\mathfrak{S}_3) = \mathfrak{A}_3$$

が成立する。

注意 2.6 ここで、共役類について説明する。

$\sigma \in \mathfrak{S}_n$ に対して、

$$\sigma = (a_1 \dots a_s)(b_1 \dots b_t) \cdots (c_1 \dots c_u)$$

と表せたとする。このとき、$\tau \in \mathfrak{S}_n$ に対して、

$$\tau\sigma\tau^{-1} = (\tau(a_1) \dots \tau(a_s))(\tau(b_1) \dots \tau(b_t)) \cdots (\tau(c_1) \dots \tau(c_u))$$

が成立する。

$\sigma \in \mathfrak{S}_n$ を共通文字がない巡回置換の積に分解する。それを、改めて、

$$\sigma = (a_1 \dots a_s)(b_1 \dots b_t) \cdots (c_1 \dots c_u)$$

とする。動かない文字は、長さ 1 の巡回置換と思う。このとき、

$$[s, t, \dots, u] \ \ (s + t + \cdots + u = n, \ \ s \geq t \geq \cdots \geq u > 0)$$

を σ の型という。

$\mathfrak{S}_n$ の共役類で、$\mathfrak{A}_n$ に含まれるものは型が、

$[a_1, \dots, a_s]$ $(a_1 + \cdots + a_s = n, \quad a_1 \geq \cdots \geq a_s > 0, \quad a_1, \dots, a_s$の中に偶数が偶数個)

となるものである。

(iv) $n = 4$ のとき。$\mathfrak{S}_4$ の共役類で $\mathfrak{A}_4$ に含まれるものの型は、

$$[3, 1], [2, 2], [1, 1, 1, 1]$$

である。それぞれの型の代表元として、$(123), (12)(34), e$ をとることによって、

$$\mathfrak{A}_4 \subset C(\mathfrak{S}_4)$$

を証明する。

$$\begin{aligned} e &\in C(\mathfrak{S}_4) \\ (12)(13)(12)^{-1}(13)^{-1} &= (23)(13) = (123) \in C(\mathfrak{S}_4) \qquad (5) \\ (12)((13)(24))(12)^{-1}((13)(24))^{-1} &= ((23)(14))((13)(24)) \\ = (12)(34) &\in C(\mathfrak{S}_4) \qquad (6) \end{aligned}$$

$C(\mathfrak{S}_4)$ は共役で閉じている (事実 2.2 の (4)) ので (5), (6) より、型が $[3, 1], [2, 2]$ の元はすべて $C(\mathfrak{S}_4)$ に含まれる。よって、

$$\mathfrak{A}_4 \subset C(\mathfrak{S}_4) \subset D(\mathfrak{S}_4)$$

が成立する。また、交換子はすべて偶置換であるので、

$$D(\mathfrak{S}_4) = < C(\mathfrak{S}_4) > \subset \mathfrak{A}_4$$

である。よって、

$$C(\mathfrak{S}_4) = D(\mathfrak{S}_4) = \mathfrak{A}_4$$

が成立する。

次に、

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$$

という集合を考え、

$$V_4 \subset C(\mathfrak{A}_4)$$

を証明する。V_4 は、$\mathfrak{S}_4$ と $\mathfrak{A}_4$ の正規部分群であることはよく知られている。(そのことは、証明なしで使うことにする。)

$$e \in C(\mathfrak{A}_4) \tag{7}$$

$$\begin{aligned}(234)((13)(24))(234)^{-1}((13)(24))^{-1} &= ((14)(23))((13)(24)) \\ &= (12)(34) \in C(\mathfrak{A}_4)\end{aligned} \tag{8}$$

$C(\mathfrak{A}_4)$ は $\mathfrak{S}_4$ の中での共役で閉じている (事実 2.2 の (4)) ので、

$$(23)(12)(34)(23)^{-1} = (13)(24) \in C(\mathfrak{A}_4) \tag{9}$$

$$(24)(12)(34)(24)^{-1} = (14)(23) \in C(\mathfrak{A}_4). \tag{10}$$

(7), (8), (9), (10) より、

$$V_4 \subset C(\mathfrak{A}_4) \subset D(\mathfrak{A}_4)$$

が成立する。

また、V_4 は、$\mathfrak{A}_4$ の正規部分群であり、剰余群 $\mathfrak{A}_4/V_4$ の位数が 3 だからアーベル群になる。

よって、

$$D(\mathfrak{A}_4) \subset V_4$$

となる。したがって、

$$C(\mathfrak{A}_4) = D(\mathfrak{A}_4) = V_4$$

が成立する。

$n \leq 4$ のときは個別に証明していたが、$n \geq 5$ では、n に関する帰納法によって、$C(\mathfrak{S}_n) = D(\mathfrak{S}_n) = C(\mathfrak{A}_n) = D(\mathfrak{A}_n) = \mathfrak{A}_n$ を示す。

$$\begin{array}{ccccc} C(\mathfrak{S}_n) & \subset & D(\mathfrak{S}_n) & \subset & \mathfrak{A}_n \\ \cup & & \cup & & \\ C(\mathfrak{A}_n) & \subset & D(\mathfrak{A}_n) & & \end{array}$$

が成立する。よって、

$$\mathfrak{A}_n \subset C(\mathfrak{A}_n)$$

を証明すれば十分である。

(v) $n = 5$ のとき、$\mathfrak{S}_5$ の共役類で $\mathfrak{A}_5$ に含まれるものの型は、

$$[5], [3,1,1], [2,2,1], [1,1,1,1,1]$$

である。それぞれの型の代表元として、$(12345), (123), (12)(34), e$ をとることによって、

$$\mathfrak{A}_5 \subset C(\mathfrak{A}_5)$$

を証明する。

$$\begin{aligned}
e &\in C(\mathfrak{A}_5) \\
(13542)(243)(13542)^{-1}(243)^{-1} &= (125)(234) \\
= (12345) &\in C(\mathfrak{A}_5) \qquad (11) \\
(125)(134)(125)^{-1}(134)^{-1} &= (234)(143) \\
= (123) &\in C(\mathfrak{A}_5) \qquad (12) \\
((13)(24))(234)((13)(24))^{-1}(234)^{-1} &= (412)(243) \\
= (12)(34) &\in C(\mathfrak{A}_5) \qquad (13)
\end{aligned}$$

$C(\mathfrak{A}_5)$ は $\mathfrak{S}_5$ の中の共役で閉じている (事実 2.2 の (4))。つまり、(11),(12),(13) より、型が $[5], [3,1,1], [2,2,1]$ の元はすべて $C(\mathfrak{A}_5)$ に含まれる。よって、

$$\mathfrak{A}_5 \subset C(\mathfrak{A}_5)$$

が成立する。以上により、

$$C(\mathfrak{S}_5) = D(\mathfrak{S}_5) = C(\mathfrak{A}_5) = D(\mathfrak{A}_5) = \mathfrak{A}_5$$

が成立することがわかった。

注意 2.7

$$\begin{aligned}
C(\mathfrak{A}_n) &= \{[\sigma, \eta] \mid \sigma, \eta \in \mathfrak{A}_n\} \\
&= \{\sigma\eta\sigma^{-1}\eta^{-1} \mid \sigma, \eta \in \mathfrak{A}_n\} \\
&= \{\sigma\tau \mid \sigma, \tau \in \mathfrak{A}_n,\ \sigma^{-1} \text{ と } \tau \text{ が } \mathfrak{A}_n \text{ の中で共役}\}
\end{aligned}$$

となる。

補題 2.8 $\mathfrak{S}_n$ の元 σ, τ が型 $[a_1 \dots a_s]$ の元とする。

(1) $E(\sigma) \overset{\text{def}}{=} \{\xi \in \mathfrak{S}_n \mid \xi\sigma = \sigma\xi\}$ とする。$\xi_0\sigma\xi_0^{-1} = \tau$ と仮定する。このとき、$\xi_1 \in \mathfrak{S}_n$ に対して、

$$\xi_1\sigma\xi_1^{-1} = \tau \Leftrightarrow \xi_1 \in \xi_0 E(\sigma)$$

が成立する。

(2) $a_1,\ldots,a_s$ は「すべて異なる奇数」ではないと仮定する。このとき、$E(\sigma)$ は、偶置換も奇置換も含む。

(3) σ と τ は同じ型 $[a_1\ldots a_s]$ の元であり、$a_1,\ldots,a_s$ は「すべて異なる奇数」ではないとする。このとき、$\xi\sigma\xi^{-1}=\tau$ を満たす ξ で、偶置換のものも奇置換のものも選ぶことができる。

証明 最初に、(1) を示す。

($\Leftarrow$) $\xi\in E(\sigma)$, $\xi_1=\xi_0\xi$ とする。$\xi_1\sigma\xi_1^{-1}=\xi_0\xi\sigma\xi^{-1}\xi_0^{-1}=\tau$.

($\Rightarrow$) $(\xi_0^{-1}\xi_1)\sigma(\xi_0^{-1}\xi_1)^{-1}=\xi_0^{-1}\xi_1\sigma\xi_1^{-1}\xi_0=\xi_0^{-1}\tau\xi_0=\sigma$. よって、$\xi_0^{-1}\xi_1\in E(\sigma)$. したがって、$\xi_1\in\xi_0E(\sigma)$.

次に (2) を示す。

$e\in E(\sigma)$ より、偶置換を含む。

$\sigma=(12\ldots a_1)(a_1+1,\ldots,a_1+a_2)\cdots$ とする。

- a_1 が偶数とする。このとき、$(12\ldots a_1)\in E(\sigma)$ であり、これは奇置換。
- $a_1=a_2$ が奇数とする。$\xi=(1,a_1+1)(2,a_2+2)\cdots(a_1,a_1+a_2)$ とおくと $\xi\sigma\xi^{-1}=\sigma$ で $\xi\in E(\sigma)$ は奇置換。

したがって、$E(\sigma)$ は偶置換も奇置換も含む。

次に (3) を示す。

(2) によって、$E(\sigma)$ が偶置換も奇置換も含むので、任意の $\xi_0\in\mathfrak{S}_n$ に対して、$\xi_0E(\sigma)$ は偶置換も奇置換も含む。すると、(1) を用いることにより、(3) が証明される。 **証明終**

(vi) $n\geq 6$ のとき。

$[a_1,\ldots,a_s]$ は、$a_1+\cdots+a_s=n$, $a_1\geq\cdots\geq a_s>0$, $a_1,\ldots,a_s$ の中に偶数は偶数個を満たすとする。

$a_s=1$ の場合は、n に関する帰納法により型 $[a_1,\ldots,a_{s-1}]$ の元は $C(\mathfrak{A}_{n-1})$ に含まれることは明らか。このとき、型 $[a_1,\ldots,a_s]$ の元は $C(\mathfrak{A}_n)$ に含まれる。

よって、$a_1\geq\cdots\geq a_s\geq 2$ とする。$a_1,\ldots,a_s$ の順番を入れ替えて、

$$[a_1,\ldots,a_s]\text{が偶置換の型であり、}a_1+\cdots+a_s\geq 5$$

になるように、なるべく細かく分割する。

n に関する帰納法を用いることによって、示すべきケースは、

(1) $[a]$ ($a\geq 5$; 奇数),

(2) $[a, b]$ (a, b; 偶数で、$a + b \geq 6$),

(3) $[a, 3]$ ($a \geq 3$; 奇数),

(4) $[a, b, 3]$ (a, b; 偶数)

であることがわかる。既に示したように、型 $[2, 2]$ の元は $C(\mathfrak{A}_4)$ に含まれることに注意する。

証明 上のそれぞれの場合に分けて証明する。

(1) $[a]$ ($a \geq 5$; 奇数) の場合。$a = 2r + 1$ とする。

(i) r を偶数とする。このとき、

$$(1, 2, \ldots, 2r + 1) = (1, 2, \ldots, r + 1)(r + 1, \ldots, 2r + 1)$$

と分解する。$\sigma = (1, 2, \ldots, r + 1)$, $\tau = (r + 1, \ldots, 2r + 1)$ とすると、型はともに $[r + 1, 1, \ldots, 1]$ (1 は r 個) となる。$\sigma^{-1} = (1,\ r + 1, \ldots, 2)$ も同じ型をもつ。r は 2 以上であるので、補題 2.8 の (3) により、σ^{-1} と τ は $\mathfrak{A}_a$ で共役となり $\sigma\tau \in C(\mathfrak{A}_a)$ となる。

(ii) r を奇数とする。このとき、

$$(1, 2, \ldots, 2r + 1) = (1, 2, \ldots, r,\ 2r + 1,\ r + 1)(r,\ 2r + 1,\ r + 1, \ldots, 2r)$$

と分解する。$\sigma = (1, 2, \ldots, r,\ 2r+1,\ r+1)$, $\tau = (r,\ 2r+1,\ r+1, \ldots, 2r)$ とすると、型はともに $[r + 2, 1, \ldots, 1]$ (1 は $r - 1$ 個) となる。$\sigma^{-1} = (1,\ r + 1,\ 2r + 1,\ r, \ldots, 2)$ も同じ型をもつ。r は 3 以上であるので、補題 2.8 の (3) により、σ^{-1} と τ は $\mathfrak{A}_a$ で共役となり $\sigma\tau \in C(\mathfrak{A}_a)$ となる。

(2) $[a, b]$ (a, b; 偶数) の場合。

注意 2.9 以下で、下の式が使われる。

$$\begin{aligned} & (1, 2, \ldots, 2p)(2p + 1, 2p + 2, \ldots, 2p + q)(1, 2, \ldots, 2p - 2, 2p, 2p + 1) \\ = \ & (1, 3, 5, \ldots, 2p - 1, 2p, 2p + 2, 2p + 3, \ldots, 2p + q, 2p + 1, 2, 4, \ldots, 2p - 2) \end{aligned}$$

(i) $a = 2r$, $b = 2t$, $r > t$ とする。注意 2.9 の式を使えば、$(1, 2, \ldots, 2r) = \alpha\beta\gamma$ と分解できる。ただし、α, β, γ は、それぞれ長さ $2(r - t)$, $2t$, $2(r - t)$ の巡回置換であり、出てくる文字は $1, 2, \ldots, 2r$ に含まれている。また、α と β は、台が交わっていない。すると、

$$(1, 2, \ldots, 2r)(2r + 1, \ldots, 2r + 2t) = \alpha\beta\gamma(2r + 1, \ldots, 2r + 2t)$$

と分解する。$\sigma = \alpha\beta$, $\tau = \gamma(2r + 1, \ldots, 2r + 2t)$ とすると、型は共に $[2(r - t), 2t, 1, \ldots, 1]$ (1 は $2t$ 個) となる。σ^{-1} も同じ型をもつので、補題 2.8 の (3) により σ^{-1} と τ は $\mathfrak{A}_{a+b}$ で共役となり、$\sigma\tau \in C(\mathfrak{A}_{a+b})$ となる。

(ii) $a = b = 2r$, $4r \geq 5$ より、$r \geq 2$ とする。このとき、

$$(1, 2, \ldots, 2r)(2r+1, \ldots, 4r) = (1, 2, \ldots, 2r,\ 2r+1)(2r,\ 2r+1, \ldots, 4r)$$

と分解する。$\sigma = (1, 2, \ldots, 2r,\ 2r+1)$, $\tau = (2r,\ 2r+1, \ldots, 4r)$ とすると、型は共に $[2r+1, 1, \ldots, 1]$ (1 は $2r-1$ 個) となる。σ^{-1} も同じ型をもつので、補題 2.8 の (3) により σ^{-1} と τ は $\mathfrak{A}_{a+b}$ で共役となり $\sigma\tau \in C(\mathfrak{A}_{a+b})$ となる。

(3) $[a, 3]$ ($a \geq 3$; 奇数) の場合。$a = 2t+1$, $p = 2t+2$, $q = 2t+3$, $r = 2t+4$ とする。

(i) t を奇数とする。このとき、

$$\begin{aligned} & (1, 2, \ldots, 2t+1)(p, q, r) \\ = \ & (1, 2, \ldots, t+1)(t+1, \ldots, 2t+1)(p, q)(q, r) \\ = \ & (1, 2, \ldots, t+1)(p, q)(t+1, \ldots, 2t+1)(q, r) \end{aligned}$$

と分解する。$\sigma = (1, 2, \ldots, t+1)(p, q)$, $\tau = (t+1, \ldots, 2t+1)(q, r)$ とすると、型は共に $[t+1, 2, 1, \ldots, 1]$ (1 は $t+1$ 個) となる。σ^{-1} も同じ型をもつので、補題 2.8 の (3) により σ^{-1} と τ は $\mathfrak{A}_{2t+4}$ で共役となり $\sigma\tau \in C(\mathfrak{A}_{2t+4})$ となる。

(ii) t を偶数とする。このとき、

$$\begin{aligned} & (1, 2, \ldots, 2t+1)(p, q, r) \\ = \ & (1, 2, \ldots, t,\ 2t+1,\ t+1)(t,\ 2t+1,\ t+1, \ldots, 2t)(p, q)(q, r) \\ = \ & (1, 2, \ldots, t,\ 2t+1,\ t+1)(p, q)(t,\ 2t+1,\ t+1, \ldots, 2t)(q, r) \end{aligned}$$

と分解する。$\sigma = (1, 2, \ldots, t,\ 2t+1,\ t+1)(p, q)$, $\tau = (t,\ 2t+1,\ t+1, \ldots, 2t)(q, r)$ とすると、型は共に $[t+2, 2, 1, \ldots, 1]$ (1 は t 個) となる。σ^{-1} も同じ型をもつので、補題 2.8 の (3) により σ^{-1} と τ は共役となり $\sigma\tau \in C(\mathfrak{A}_{2t+4})$ となる。

(4) $[a, b, 3]$ (a, b; 偶数) の場合。

(i) $a = 2t$, $b = 2u$, $t > u$, $p = 2t+2u+1$, $q = 2t+2u+2$, $r = 2t+2u+3$ とする。このとき、

$$(*) = (1, 2, \ldots, 2t)(2t+1, \ldots, 2t+2u)(p, q, r)$$

とおく。ここで、(2) より、

$$(1, 2, \ldots, 2t)(2t+1, \ldots, 2t+2u) = \sigma\tau,$$

ただし、$\sigma, \tau \in \mathfrak{A}_{2t+2u}$ であり、σ^{-1} と τ は $\mathfrak{S}_{2t+2u}$ の中で偶置換でも奇置換でも共役にできる (補題 2.8 の (3))。よって、

$$\tau = \xi\sigma^{-1}\xi^{-1} \ (\xi \in \mathfrak{S}_{2t+2u} \setminus \mathfrak{A}_{2t+2u})$$

と書ける。また、

$$(p, q, r) = (p, r, q)^2 = [(p, r, q), (r, q)]$$

となる。ゆえに、

$$\begin{aligned} (*) &= \sigma\xi\sigma^{-1}\xi^{-1}(p, r, q)(r, q)(p, q, r)(q, r) \\ &= \sigma(p, r, q)\xi(r, q)(p, q, r)\sigma^{-1}(q, r)\xi^{-1} \\ &= [\sigma(p, r, q), \xi(r, q)]. \end{aligned}$$

ここで、$\sigma(p, r, q)$ と $\xi(q, r)$ は共に偶置換であるので、$(*)$ は $C(\mathfrak{A}_{a+b+3})$ に含まれる。

(ii) $a = b = 2t$, $p = 4t + 1$, $q = 4t + 2$, $r = 4t + 3$ とする。このとき、

$$\begin{aligned} & (1, 2, \ldots, 2t)(2t + 1, \ldots, 4t)(p, q, r) \\ = \ & (1, 2, \ldots, 2t,\ 2t + 1)(2t,\ 2t + 1, \ldots, 4t)(p, r, q)(p, r, q) \\ = \ & (1, 2, \ldots, 2t,\ 2t + 1)(p, r, q)(2t,\ 2t + 1, \ldots, 4t)(p, r, q) \end{aligned}$$

と分解する。$\sigma = (1, 2, \ldots, 2t,\ 2t{+}1)(p, r, q)$, $\tau = (2t,\ 2t{+}1, \ldots, 4t)(p, r, q)$ とすると、型は共に $[2t + 1, 3, 1, \ldots, 1]$ (1 は $2t - 1$ 個) となる。σ^{-1} も同じ型をもつ。

$t = 1$ の場合、型は $[3, 3, 1]$ より σ^{-1} と τ は (補題 2.8 の (3) により) $\mathfrak{A}_7$ の中で共役となり成立する。

$t \geq 2$ の場合、型は $[2t + 1, 3, 1, \ldots, 1]$ より σ^{-1} と τ は (補題 2.8 の (3) により) $\mathfrak{A}_{4t+3}$ の中で共役となり成立する。 **証明終**

以上より、$n \geq 6$ のとき $\mathfrak{A}_n \subset C(\mathfrak{A}_n)$ が成立するので、

$$C(\mathfrak{S}_n) = D(\mathfrak{S}_n) = C(\mathfrak{A}_n) = D(\mathfrak{A}_n) = \mathfrak{A}_n$$

が成立する。

したがって、任意の自然数 n に対して、$C(\mathfrak{S}_n) = D(\mathfrak{S}_n)$, $C(\mathfrak{A}_n) = D(\mathfrak{A}_n)$ が成立することがわかった。 **証明終**

3　反例

第 2 章では $D(G) = C(G)$ となる例を数多く挙げた。しかし、第 1 章において、この事実には反例が存在することも述べた。第 3 章ではこの反例について述べたい。この反例は、1979 年 P.J.Cassidy によるものである。この反例に関する参考文献 [1] は、法人ポスドクの下元数馬先生に教えていただきました。この場を借りて、深く感謝いたします。

定理 3.1　k を体、R は k 代数、R_1 と R_2 は共に R の中間環、R は環として k 上 R_1 と R_2 で生成されるものとする。このとき、以下の 4 つが成り立つ。

(1)
$$G = \left\{ \begin{pmatrix} 1 & f & h \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix} \middle| \begin{array}{l} f \in R_1 \\ g \in R_2 \\ h \in R \end{array} \right\} \subset GL(3, R)$$
と定義すると、G は $GL(3, R)$ の部分群である。

以下、$(f, g, h) := \begin{pmatrix} 1 & f & h \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix}$ と表すことにする。

(2) G の交換子全体の集合を $C(G)$ とすると、
$$C(G) = \{(0, 0, f_1 g_2 - f_2 g_1) \mid f_1, f_2 \in R_1, g_1, g_2 \in R_2\}$$
である。

(3) G の交換子群を $D(G)$ とすると、
$$D(G) = \{(0, 0, h) \mid h \in R\}$$
である。

(4) $R_1 = k[x]$, $R_2 = k[y]$, $R = k[x, y]$, または、$R_1 = k[x]/(x^3)$, $R_2 = k[y]/(y^3)$, $R = k[x, y]/(x, y)^3$ とする。このとき、$D(G) \neq C(G)$ である。

証明　(1) を証明しよう。まず G が $GL(3, R)$ の演算で閉じていることを示す。

任意に $\begin{pmatrix} 1 & f_1 & h_1 \\ 0 & 1 & g_1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & f_2 & h_2 \\ 0 & 1 & g_2 \\ 0 & 0 & 1 \end{pmatrix} \in G$ をとる。ただし、$f_1, f_2 \in R_1$, $g_1, g_2 \in R_2$, $h_1, h_2 \in R$ である。

$$\begin{pmatrix} 1 & f_1 & h_1 \\ 0 & 1 & g_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & f_2 & h_2 \\ 0 & 1 & g_2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & f_1 + f_2 & h_1 + h_2 + f_1 g_2 \\ 0 & 1 & g_1 + g_2 \\ 0 & 0 & 1 \end{pmatrix}$$

となり、$f_1 + f_2 \in R_1, g_1 + g_2 \in R_2, h_1 + h_2 + f_1 g_2 \in R$ なので、G は $GL(3, R)$ の演算で閉じていることがわかる。以下、

$$(f, g, h) := \begin{pmatrix} 1 & f & h \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix}$$

と表すことにする。すると上の式から、

$$(f_1, g_1, h_1)(f_2, g_2, h_2) = (f_1 + f_2, g_1 + g_2, h_1 + h_2 + f_1 g_2)$$

が成り立つ。あとは G の単位元と逆元の存在を言えばよい。

$(0, 0, 0) \in GL(3, R)$ は 3 次の単位行列であり、任意の $(f, g, h) \in G$ に対して、

$$\begin{aligned} (f, g, h)(0, 0, 0) &= (f + 0, g + 0, h + 0 + f \times 0) \\ &= (f, g, h) \\ (0, 0, 0)(f, g, h) &= (0 + f, 0 + g, 0 + h + 0 \times g) \\ &= (f, g, h) \end{aligned}$$

が成立する。一方、$(f, g, h) \in G$ に対して、$(-f, -g, -h + fg) \in G$ をとれば、

$$\begin{aligned} (f, g, h)(-f, -g, -h + fg) &= (f - f, g - g, h - h + fg - fg) \\ &= (0, 0, 0) \\ (-f, -g, -h + fg)(f, g, h) &= (-f + f, -g + g, -h + fg + h - fg) \\ &= (0, 0, 0) \end{aligned}$$

となる。よってこの元が (f, g, h) の逆元である。

以上のことから G は $GL(3, R)$ の部分群であることがわかった。

次に (2) を証明しよう。$(f_1, g_1, h_1), , (f_2, g_2, h_2) \in G$ を任意にとる。このとき、

$$\begin{aligned} & [(f_1, g_1, h_1), (f_2, g_2, h_2)] \\ = \ & (f_1, g_1, h_1)(f_2, g_2, h_2)(f_1, g_1, h_1)^{-1}(f_2, g_2, h_2)^{-1} \\ = \ & (f_1, g_1, h_1)(f_2, g_2, h_2)(-f_1, -g_1, -h_1 + f_1 g_1)(-f_2, -g_2, -h_2 + f_2 g_2) \\ = \ & (f_1 + f_2, g_1 + g_2, h_1 + h_2 + f_1 g_2)(-f_1, -g_1, -h_1 + f_1 g_1)(-f_2, -g_2, -h_2 + f_2 g_2) \\ = \ & (f_2, g_2, h_2 + f_1 g_2 - f_2 g_1)(-f_2, -g_2, -h_2 + f_2 g_2) \\ = \ & (0, 0, f_1 g_2 - f_2 g_1) \end{aligned}$$

となるので、

$$C(G) = \{(0, 0, f_1 g_2 - f_2 g_1) \mid f_1, f_2 \in R_1, g_1, g_2 \in R_2\}$$

であり (2) が証明できた。

次に (3) を示す。

$$A := \{(0, 0, h) \mid h \in R\}$$

とおく。このとき任意に $(0,0,h_1), (0,0,h_2) \in A$ をとると、

$$(0,0,h_1)(0,0,h_2) = (0,0,h_1+h_2)$$

であることから A は $GL(3,R)$ の部分群であることがわかる。よって $D(G)$ の定義より $D(G) \subset A$ であることがわかる。

次に $D(G) \supset A$ を示す。(2) により $C(G) = \{(0,0,f_1g_2 - f_2g_1) \mid f_1, f_2 \in R_1, g_1, g_2 \in R_2\}$ であることから、任意の $f \in R_1, g \in R_2$ において、$(0,0,fg) \in C(G)$ であり、$D(G)$ はその形の元の有限個の積で表されるので $D(G) \supset A$ が成り立つことがわかる。

最後に (4) を証明する。どちらの場合も同様に証明できるので、前者の場合のみ証明する。

$h(x,y) = x^2 + xy + y^2 \in k[x,y]$ をとり、$(0,0,h(x,y))$ が $C(G)$ に含まれたとしよう。つまり、ある $f_1(x), f_2(x) \in k[x], g_1(y), g_2(y) \in k[y]$ があって、$h(x,y) = f_1(x)g_2(y) - f_2(x)g_1(y)$ とする。

ここで、

$$f_1(x) := \sum_i b_i x^i, \quad f_2(x) := \sum_i c_i x^i$$

とすると、

$$\begin{aligned} h(x,y) &= \sum_i b_i x^i g_2(y) - \sum_i c_i x^i g_1(y) \\ &= \sum_i (b_i g_2(y) - c_i g_1(y))\, x^i \end{aligned}$$

であるから、次のような 3 つの等式を得る。

$$\begin{cases} b_0 g_2(y) - c_0 g_1(y) = y^2 \\ b_1 g_2(y) - c_1 g_1(y) = y \\ b_2 g_2(y) - c_2 g_1(y) = 1 \end{cases}$$

このとき、$k[y]$ を k 上のベクトル空間とみると、3 つの一次独立な元の集合 $\left\{1, y, y^2\right\}$ が 2 つの元の集合 $\{g_1(y), g_2(y)\}$ で張れてしまうことになり矛盾が生じる。

以上のことより、$(0,0,h(x,y))$ は $C(G)$ に含まれないことが示されたので、$D(G) \neq C(G)$ となる。 **証明終**

注意 3.2 p を素数とする。前定理の (4) で、$R_1 = k[x]/(x^3)$, $R_2 = k[y]/(y^3)$, $R = k[x,y]/(x,y)^3$ のケースを考える。k を $k = \mathbb{Z}/p\mathbb{Z}$ とすると、G は有限群となり、その位数は p^{12} である。つまり有限群を用いた反例が作れるということである。特に $p = 2$ とすれば、位数が $2^{12} = 4096$ の反例が作れる。

$D(G) \neq C(G)$ なる有限群で、位数が最小のものは、位数が 96 であることが知られている ([1] の 34 ページ)。

参考文献

[1] Joseph J. Rotman, *An introduction to the theory of groups, Fourth edition*, Graduate Texts in Mathematics, **148**, Springer-Verlag, New York, 1995.