代数学 I 第 14 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

今回は本講義の範囲内では使われ方がわかりにくいかもしれないが，群論においては重要な概念や話題について解説を行う．より進んだ話を学んで行く際に，一度は聞いたことがあった方が良いだろうというような話の詰め合わせである．今回の内容が今後の皆様の進んだ学習の中で役に立てば幸いである．なお，講義内では時間的にとても全てを扱うことはできない．講義の予習としては，13.1 節 (例 3 まで)，13.2 節を読んでいただければ良い．

13.1 可解群

まずは群の可解性について解説する．この性質は群を用いて代数方程式の可解性を調べるというようなことを行う「ガロア理論」と呼ばれる分野で重要な概念となる (第 1,2 回講義資料で少しだけ概要に触れた)．

定義 13.1

G を群とする．各 $g_1, g_2 \in G$ に対し，g_1 と g_2 **の交換子 (commutator of g_1 and g_2)** $[g_1, g_2]$ を，

$$[g_1, g_2] \coloneqq g_1 g_2 g_1^{-1} g_2^{-1}$$

と定義する．さらに，G **の交換子群 (commutator subgroup of G)** $\mathrm{D}(G)$ を，

$$\mathrm{D}(G) \coloneqq \langle \{ [g_1, g_2] \mid g_1, g_2 \in G \} \rangle$$

と定義する．ここで、右辺は交換子全体 $\{[g_1, g_2] \mid g_1, g_2 \in G\}$ の生成する G の部分群である．

注意 1. 各 $g_1, g_2 \in G$ に対し，$[g_1, g_2]^{-1} = (g_1 g_2 g_1^{-1} g_2^{-1})^{-1} = g_2 g_1 g_2^{-1} g_1^{-1} = [g_2, g_1]$ である．これより，$\{[g_1, g_2] \mid g_1, g_2 \in G\}$ は逆元をとる操作では閉じていることがわかるが，一般に二項演算では閉じておらず，これ自体は群にはならない．

命題 13.2

群 G に対し，$\mathrm{D}(G)$ は G の正規部分群である．

命題 13.2 の証明のために，以下の補題を用いる．

補題 13.3

群 G とその部分集合 S に対し、

$$\text{任意の } g \in G \text{ に対して，} gSg^{-1} \subset S$$

が成立するとき，S の生成する G の部分群 $\langle S \rangle$ は G の正規部分群である．

証明. 任意の $\langle S \rangle$ の元 s は

$$s = s_1^{m_1} \cdots s_k^{m_k} \text{ (ただし，} s_1, \ldots, s_k \in S, m_1, \ldots, m_k \in \mathbb{Z}, k \in \mathbb{N}) \tag{13.1}$$

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

と書けるのであった (第 7 回講義資料定義 6.2)．ここで，各 $g \in G$ に対し，

$$\alpha_g \colon G \to G,\ h \mapsto ghg^{-1}$$

と定義すると，これは群同型となるのであった (第 11 回講義資料例 13)．これより，任意の $g \in G$ と上の (13.1) の形の元 s に対して，

$$gsg^{-1} = \alpha_g(s) = \alpha_g(s_1)^{m_1}\alpha_g(s_2)^{m_2}\cdots\alpha_g(s_k)^{m_k}$$

となる．ここで，仮定より $\alpha_g(s_1), \alpha_g(s_2), \ldots, \alpha_g(s_k) \in S$ なので，上式の右辺は再び $\langle S \rangle$ の元であり，$gsg^{-1} \in \langle S \rangle$ である．よって，第 10 回講義資料命題 9.3 (3) の条件が満たされるので，$\langle S \rangle$ は G の正規部分群である． □

命題 13.2 の証明. 補題 13.3 と交換子群の定義より，

$$\text{任意の } g, h_1, h_2 \in G \text{ に対し，} g[h_1, h_2]g^{-1} \in \{[g_1, g_2] \mid g_1, g_2 \in G\}$$

を示せばよいことがわかる (補題 13.3 における S が $\{[g_1, g_2] \mid g_1, g_2 \in G\}$ である)．補題 13.3 の証明中に定義した群同型 α_g を用いると，任意の $g, h_1, h_2 \in G$ に対し，

$$g[h_1, h_2]g^{-1} = \alpha_g([h_1, h_2]) = \alpha_g(h_1h_2h_1^{-1}h_2^{-1}) = \alpha_g(h_1)\alpha_g(h_2)\alpha_g(h_1)^{-1}\alpha_g(h_2)^{-1} = [\alpha_g(h_1), \alpha_g(h_2)]$$

となる．よって，$g[h_1, h_2]g^{-1} \in \{[g_1, g_2] \mid g_1, g_2 \in G\}$ であり，示すべきことは示された． □

命題 13.4

群 G に対し，剰余群 $G/\mathrm{D}(G)$ は可換群となる．また，N を G の正規部分群とし，剰余群 G/N が可換群となるとき，$\mathrm{D}(G) \subset N$ となる．

証明. 任意の $g, h \in G$ に対して，$h^{-1}g^{-1}hg = [h^{-1}, g^{-1}] \in \mathrm{D}(G)$ となるので，$G/\mathrm{D}(G)$ において，

$$g\mathrm{D}(G) \cdot h\mathrm{D}(G) = gh\mathrm{D}(G) = gh[h^{-1}, g^{-1}]\mathrm{D}(G) = gh(h^{-1}g^{-1}hg)\mathrm{D}(G) = hg\mathrm{D}(G) = h\mathrm{D}(G) \cdot g\mathrm{D}(G)$$

となる．よって，$G/\mathrm{D}(G)$ は可換群である．

次に後半の主張を示す．商写像

$$p \colon G \to G/N,\ g \mapsto gN$$

を考える．このとき，p は $\mathrm{Ker}\, p = N$ となる群準同型なので (第 11 回講義資料例 10)，$\mathrm{D}(G) \subset \mathrm{Ker}\, p$ となることを示せばよい．すなわち，任意の $g_1, g_2 \in G$ に対し，

$$p([g_1, g_2]) = eN$$

となることを示せば良い (第 7 回講義資料命題 6.3 も参照のこと)．仮定より，G/N は可換群なので，

$$\begin{aligned} p([g_1, g_2]) = p(g_1g_2g_1^{-1}g_2^{-1}) = p(g_1)p(g_2)p(g_1^{-1})p(g_2^{-1}) &= g_1N \cdot g_2N \cdot g_1^{-1}N \cdot g_2^{-1}N \\ &= g_2N \cdot g_1N \cdot g_1^{-1}N \cdot g_2^{-1}N \\ &= g_2g_1g_1^{-1}g_2^{-1}N = eN. \end{aligned}$$

よって，示すべきことは示された． □

注意 2. 命題 13.4 は言葉で書くと，「$G/\mathrm{D}(G)$ は G を割って可換にするような “最小の割り方” である」ということを述べている．

群 G に対して交換子群 $\mathrm{D}(G)$ を取るという操作は繰り返し行うことができる．つまり，G に対して，

$$\mathrm{D}_0(G) \coloneqq G, \quad \mathrm{D}_1(G) \coloneqq \mathrm{D}(\mathrm{D}_0(G)) = \mathrm{D}(G), \quad \mathrm{D}_2(G) \coloneqq \mathrm{D}(\mathrm{D}_1(G)), \quad \mathrm{D}_3(G) \coloneqq \mathrm{D}(\mathrm{D}_2(G)) \quad \cdots$$

と，各 $k \in \mathbb{Z}_{>0}$ に対して，

$$\mathrm{D}_k(G) \coloneqq \mathrm{D}(\mathrm{D}_{k-1}(G))$$

を満たすように順に定義していくことができる．このとき命題 13.2 より，任意の $k \in \mathbb{Z}_{>0}$ に対して，$\mathrm{D}_k(G)$ は $\mathrm{D}_{k-1}(G)$ の正規部分群となり，命題 13.4 より，剰余群 $\mathrm{D}_{k-1}(G)/\mathrm{D}_k(G)$ は可換群となる．

定義 13.5

群 G がある正の整数 n において，$\mathrm{D}_n(G) = \{e\}$ を満たすとき，G を**可解群 (solvable group)** という．

注意 3. 群 G が可解であるということは，以下の通り G が可換群を “積み上げて” 得られるということを意味している．

G が可解のとき，次の可換群の列が存在する

$$G/\mathrm{D}_1(G)(=\mathrm{D}_0(G)/\mathrm{D}_1(G)),\ \mathrm{D}_1(G)/\mathrm{D}_2(G), \ldots, \mathrm{D}_{n-1}(G)/\mathrm{D}_n(G) = \mathrm{D}_{n-1}(G)/\{e\} \simeq \mathrm{D}_{n-1}(G)$$

例 1. G を可換群とすると，任意の $g_1, g_2 \in G$ に対し，

$$[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1} = g_2 g_1 g_1^{-1} g_2^{-1} = g_2 g_2^{-1} = e$$

となるので，

$$\mathrm{D}_1(G) = \mathrm{D}(G) = \langle e \rangle = \{e\}.$$

よって，G は可解群である．

例 2. n 次二面体群

$$D_n = \{\sigma^k \tau^\ell \mid k = 0, 1 \ldots, n-1, \ell = 0, 1\}$$

を考える ($\sigma^n = e, \tau^2 = e, \sigma^k \tau = \tau \sigma^{-k}$ $(k \in \mathbb{Z})$)．このとき，

$$\begin{aligned}
[\sigma^{k_1}, \sigma^{k_2}] &= \sigma^{k_1} \sigma^{k_2} \sigma^{-k_1} \sigma^{-k_2} = e \\
[\sigma^{k_1}\tau, \sigma^{k_2}] &= \sigma^{k_1} \tau \sigma^{k_2} (\sigma^{k_1}\tau)^{-1} \sigma^{-k_2} = \sigma^{k_1} \tau \sigma^{k_2} \sigma^{k_1} \tau \sigma^{-k_2} = \sigma^{k_1 - k_2 - k_1} \tau^2 \sigma^{-k_2} = \sigma^{-2k_2} \\
[\sigma^{k_1}, \sigma^{k_2}\tau] &= [\sigma^{k_2}\tau, \sigma^{k_1}]^{-1} = (\sigma^{-2k_1})^{-1} = \sigma^{2k_1} \\
[\sigma^{k_1}\tau, \sigma^{k_2}\tau] &= \sigma^{k_1} \tau \sigma^{k_2} \tau (\sigma^{k_1}\tau)^{-1} (\sigma^{k_2}\tau)^{-1} = \sigma^{k_1} \tau \sigma^{k_2} \tau \sigma^{k_1} \tau \sigma^{k_2} \tau = \sigma^{k_1 - k_2} \tau^2 \sigma^{k_1 - k_2} \tau\tau^2 = \sigma^{2(k_1 - k_2)}
\end{aligned}$$

となる．よって，

$$\mathrm{D}_1(D_n) = \langle \{[g_1, g_2] \mid g_1, g_2 \in D_n\} \rangle = \langle \sigma^2 \rangle.$$

とくに，$\mathrm{D}_1(D_n)$ は可換群である．よって，例 1 より，

$$\mathrm{D}_2(D_n) = \mathrm{D}(\mathrm{D}_1(D_n)) = \{e\}.$$

よって，D_n は可解群である．

可解性を調べる際には以下が便利である．

命題 13.6

群 G とその正規部分群 N に対し，以下は同値である．

(1) 群 G は可解である．

(2) 正規部分群 N と剰余群 G/N は共に可解である．

証明. 交換子群の定義より，任意の $k \in \mathbb{Z}_{\geq 0}$ に対し，

$$\mathrm{D}_k(N) \subset \mathrm{D}_k(G) \tag{13.2}$$

となる[*1]．また，$p\colon G \to G/N,\ g \mapsto gN$ を商写像とすると，再び交換子群の定義より，任意の $k \in \mathbb{Z}_{\geq 0}$ に対し，

$$p(\mathrm{D}_k(G)) = \mathrm{D}_k(G/N) \tag{13.3}$$

である[*2]．これらをもとに，(1) と (2) の同値性を証明する．

(1) ⇒ (2) (13.2), (13.3) より，ある $n \in \mathbb{Z}_{>0}$ に対して $\mathrm{D}_n(G) = \{e\}$ となるとき，

$$\mathrm{D}_n(N) \subset \mathrm{D}_n(G) = \{e\}, \qquad \mathrm{D}_n(G/N) = p(\mathrm{D}_n(G)) = p(\{e\}) = \{eN\}$$

より，$\mathrm{D}_n(N) = \{e\}, \mathrm{D}_n(G/N) = \{eN\}$ となるので，定義より $N, G/N$ は共に可解である．

(2) ⇒ (1) G/N が可解であることより，ある $m \in \mathbb{Z}_{>0}$ が存在して，$\mathrm{D}_m(G/N) = \{eN\}$ となる．このとき，(13.3) より，

$$p(\mathrm{D}_m(G)) = \{eN\}$$

となるので，

$$\mathrm{D}_m(G) \subset \operatorname{Ker} p = N.$$

さらに，N が可解であることより，ある $n \in \mathbb{Z}_{>0}$ が存在して，$\mathrm{D}_n(N) = \{e\}$ となるので，13.2 より (G を N，N を $\mathrm{D}_m(G)$ として適用する)，

$$\{e\} = \mathrm{D}_n(N) \supset \mathrm{D}_n(\mathrm{D}_m(G)) = \mathrm{D}_{n+m}(G).$$

これより，$\mathrm{D}_{n+m}(G) = \{e\}$ となるので G は可解である． □

例 3. 例 2 で n 次二面体群 D_n が可解であることを定義通り交換子群を計算して証明したが，命題 13.6 を用いればほぼ計算せずに証明することもできる．まず，D_n の部分群として，

$$N \coloneqq \langle \sigma \rangle = \{e, \sigma, \dots, \sigma^{n-1}\}$$

を考えると，ラグランジュの定理より，

$$(D_n : N) = \frac{|D_n|}{|N|} = \frac{2n}{n} = 2.$$

よって，第 10 回講義資料命題 9.2 より N は D_n の正規部分群であり，剰余群 D_n/N の位数は 2 である．ここで，N は巡回群なので可換であり，D_n/N は素数位数の群であるから巡回群であって可換である (第 9 回講義資料系 8.5)．よって，N も D_n/N も共に可解であるから，命題 13.6 より D_n も可解である．

対称群の可解性は以下のようになっている．

定理 13.7

n 次対称群 $\mathfrak{S}_n$ は $n = 1, 2, 3, 4$ のとき可解，$n \geq 5$ のとき非可解である．

証明. まず, $\mathfrak{S}_1 = \{e\}$ は自明な群なので定義から可解, $\mathfrak{S}_2 = \{e, (1\ 2)\}$ は可換群なので可解である．$\mathfrak{S}_3 = D_3$ であったことを思い出すと (第 6 回講義資料注意 1)，例 2 より $\mathfrak{S}_3$ は可解である．

次に $\mathfrak{S}_4$ を考える．$\mathfrak{S}_4$ にはクラインの 4 元群 V と呼ばれる可換な正規部分群が存在し (第 10 回講義資料例 4)，剰余群 $\mathfrak{S}_4/V$ は $\mathfrak{S}_3$ と同型になるのであった (第 11 解講義資料例 12)．よって，V も $\mathfrak{S}_4/V$ も可解となるので，命題 13.6 より $\mathfrak{S}_4$ は可解である．

最後に $n \geq 5$ のとき $\mathfrak{S}_n$ が非可解であることを示す．まず，相異なる $\{1, \dots, n\}$ の元 i, j, k に対して，

$$[(i\ j), (i\ k)] = (i\ j)(i\ k)(i\ j)^{-1}(i\ k)^{-1} = (i\ j)(i\ k)(i\ j)(i\ k) = (i\ j\ k)$$

[*1] ここでは N の正規性は用いていない．厳密に証明を書きたい場合は例えば数学的帰納法を用いればよい．

[*2] p の全射性と，任意の $g_1, g_2 \in G$ に対し，$p([g_1, g_2]) = [p(g_1), p(g_2)]$ となることに注意せよ．厳密に証明を書きたい場合は例えば数学的帰納法を用いればよい．

となるので，第 7 回講義資料命題 6.4 より，

$$\mathrm{D}(\mathfrak{S}_n) \supset \langle \{(i\ j\ k) \mid i,j,k \text{ は相異なる } \{1,\dots,n\} \text{ の元 }\} \rangle = \mathfrak{A}_n.$$

一方，任意の $\sigma_1, \sigma_2 \in \mathfrak{S}_n$ に対して，

$$\mathrm{sgn}([\sigma_1,\sigma_2]) = \mathrm{sgn}(\sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}) = \mathrm{sgn}(\sigma_1)\,\mathrm{sgn}(\sigma_2)\,\mathrm{sgn}(\sigma_1)^{-1}\,\mathrm{sgn}(\sigma_2)^{-1} = 1$$

となることより，交換子らの合成で得られる元は全て偶置換となる．よって，$\mathrm{D}(\mathfrak{S}_n) \subset \mathfrak{A}_n$．以上より，

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

よって，あとは $\mathrm{D}(\mathfrak{A}_n) = \mathfrak{A}_n$ となることを示せば，任意の $m \in \mathbb{Z}_{>0}$ に対して，

$$\mathrm{D}_{m+1}(\mathfrak{S}_n) = \mathrm{D}_m(\mathrm{D}(\mathfrak{S}_n)) = \mathrm{D}_m(\mathfrak{A}_n) = \mathfrak{A}_n \neq \{e\}$$

となることがわかり，$\mathfrak{S}_n$ が非可解であることが示される．$n \geq 5$ のとき，相異なる $\{1,\dots,n\}$ の元 i,j,k に対して，それらのいずれとも異なる $\ell_1, \ell_2 \in \{1,\dots,n\}, \ell_1 \neq \ell_2$ をとることができ，

$$\begin{aligned}[(i\ j\ \ell_1),(i\ k\ \ell_2)] &= (i\ j\ \ell_1)(i\ k\ \ell_2)(i\ j\ \ell_1)^{-1}(i\ k\ \ell_2)^{-1} \\ &= (i\ j\ \ell_1)(i\ k\ \ell_2)(\ell_1\ j\ i)(\ell_2\ k\ i) \\ &= (i\ j\ k)\end{aligned}$$

となる．よって，

$$\mathfrak{A}_n \supset \mathrm{D}(\mathfrak{A}_n) \supset \langle \{(i\ j\ k) \mid i,j,k \text{ は相異なる } \{1,\dots,n\} \text{ の元 }\} \rangle = \mathfrak{A}_n$$

となるので，$\mathrm{D}(\mathfrak{A}_n) = \mathfrak{A}_n$ である．以上より示すべきことは全て示された． □

定理 13.7 で対称群の可解性が $n \leq 4$ と $n \geq 5$ で変わることを見たが，これは『4 次以下の一般代数方程式にはその係数の加減乗除と根号による解の公式が存在し，5 次以上の一般代数方程式にはそのような公式が存在しない』という事実 (第 1,2 回講義資料定理 1.1) に直接対応している．群論と代数方程式は**ガロア理論**と呼ばれる理論によって関係付けられている．興味のある方は是非ガロア理論を勉強してみてほしい．群における可解性の定義や定理 13.7 の証明は純粋に群論的なものなので，これが代数方程式の可解性と関連しているというのは驚くべきことであろう．

13.2 群の直積・中国式剰余定理

本節では準同型定理の応用として，中国式剰余定理 (Chinese remainder theorem) と呼ばれる定理を解説する．このために重要な群の直積という概念を準備する．

定義 13.8

G_1, G_2 を群とし，それぞれの単位元を e_1, e_2 とする．G_1 と G_2 直積集合

$$G_1 \times G_2 \coloneqq \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$$

に二項演算 $\cdot\colon (G_1 \times G_2) \times (G_1 \times G_2) \to G_1 \times G_2$ を

$$(g_1, g_2) \cdot (h_1, h_2) \coloneqq (g_1h_1, g_2h_2),\ \forall g_1, h_1 \in G,\ g_2, h_2 \in G_2$$

と定義する．この二項演算によって，$G_1 \times G_2$ は再び群となる[*3]．この群を G_1 と G_2 の**直積 (direct product)** という．言葉で書くと，「G_1 と G_2 の直積とは G_1 と G_2 をそれぞれ第 1 成分，第 2 成分だと思って単に並べてできる群」である．$G_1 \times G_2$ の単位元は (e_1, e_2) であり，(g_1, g_2) の逆元は (g_1^{-1}, g_2^{-1}) である．

[*3] チェックは容易なのでここでは省略する．試してみよ．

例 4. $\mathbb{Z}/2\mathbb{Z}$ と $\mathbb{Z}/3\mathbb{Z}$ の直積 $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ を考えてみよう．まず集合としては，

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}=\{([0]_2,[0]_3),([0]_2,[1]_3),([0]_2,[2]_3),([1]_2,[0]_3),([1]_2,[1]_3),([1]_2,[2]_3)\}$$

であり，位数は $|\mathbb{Z}/2\mathbb{Z}|\cdot|\mathbb{Z}/3\mathbb{Z}|=2\cdot3=6$ である．二項演算は

$$([k_1]_2,[k_2]_3)+([\ell_1]_2,[\ell_2]_3)=([k_1]_2+[\ell_1]_2,[k_2]_3+[\ell_2]_3)=([k_1+\ell_1]_2,[k_2+\ell_2]_3)$$

というようにそれぞれの成分ごとに計算される (ここでは直積を考えている群が共に加法群なので直積の二項演算も $+$ で書いた)．例えば，

$$([1]_2,[1]_3)+([0]_2,[2]_3)=([1]_2+[0]_2,[1]_3+[2]_3)=([1]_2,[3]_3)=([1]_2,[0]_3)$$

などとなる．このように直積における二項演算は，それぞれの成分ごとに計算すればよいだけなので特に難しいことはない．

注意 4. 群の直積は 3 つ以上の群についても同様の方法で定義することができる．例えば G_1,G_2,G_3 が群であるとき，G_1,G_2,G_3 の直積集合

$$G_1\times G_2\times G_3\coloneqq\{(g_1,g_2,g_3)\mid g_1\in G_1,g_2\in G_2,g_3\in G_3\}$$

に二項演算 $\cdot\colon(G_1\times G_2\times G_3)\times(G_1\times G_2\times G_3)\to G_1\times G_2\times G_3$ を

$$(g_1,g_2,g_3)\cdot(h_1,h_2,h_3)\coloneqq(g_1h_1,g_2h_2,g_3h_3),\ \forall g_1,h_1\in G,\ g_2,h_2\in G_2,\ g_3,h_3\in G_3$$

と定義するとこれは再び群となる．一般には有限個である必要も無くて，無限個の群の直積も同様に定義できる[*4]．

以下は直積の基本性質である．この命題も証明は容易なので省略する．

命題 13.9

G_1,G_2 を群とし，それぞれの単位元を e_1,e_2 とする．このとき，以下が成立する．

(1) $G_1\times G_2$ の位数は $|G_1|\cdot|G_2|$ である．

(2) 写像

$$\begin{aligned}\mathrm{pr}_1\colon G_1\times G_2\to G_1,\ (g_1,g_2)\mapsto g_1,\\ \mathrm{pr}_2\colon G_1\times G_2\to G_2,\ (g_1,g_2)\mapsto g_2,\end{aligned}$$

はいずれも全射準同型である．これらは**自然な射影 (canonical projection)** と呼ばれる．

(3) 写像

$$\begin{aligned}\iota_1\colon G_1\to G_1\times G_2,\ g_1\mapsto(g_1,e_2),\\ \iota_2\colon G_2\to G_1\times G_2,\ g_2\mapsto(e_1,g_2),\end{aligned}$$

はいずれも単射準同型である．これらは**自然な入射 (canonical injection)** と呼ばれる．

(4)

$$\begin{aligned}\mathrm{Ker}\,\mathrm{pr}_2=\mathrm{Im}\,\iota_1=\{(g_1,e_2)\mid g_1\in G_1\}\simeq G_1,\\ \mathrm{Ker}\,\mathrm{pr}_1=\mathrm{Im}\,\iota_2=\{(e_1,g_2)\mid g_2\in G_2\}\simeq G_2.\end{aligned}$$

とくに，$G_1\simeq\{(g_1,e_2)\mid g_1\in G_1\}$，$G_2\simeq\{(e_1,g_2)\mid g_2\in G_2\}$ は $G_1\times G_2$ の正規部分群である．

ここから，n_1,n_2 が互いに素であるとき，$\mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z}$ が巡回群となることを証明する．これが**中国式剰余定理**の主張である．この主張の整数論的な意味については定理の証明後に解説する．まずは例から見てみよう．

[*4] $\{G_i\}_{i\in I}$ を無限集合 I で添え字付けられた群の族としたとき，その直積は $\prod_{i\in I}G_i$，その元は $(g_i)_{i\in I}$(ただし $g_i\in G_i$) などと書かれる．

例 5. $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ の場合を考えてみよう．$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ における $([1]_2,[1]_3)$ の位数を考えると，

$([1]_2,[1]_3)+([1]_2,[1]_3)=([0]_2,[2]_3)\quad ([0]_2,[2]_3)+([1]_2,[1]_3)=([1]_2,[0]_3)\quad ([1]_2,[0]_3)+([1]_2,[1]_3)=([0]_2,[1]_3)$
$([0]_2,[1]_3)+([1]_2,[1]_3)=([1]_2,[2]_3)\quad ([1]_2,[2]_3)+([1]_2,[1]_3)=([0]_2,[0]_3)$

となるので，$\mathrm{ord}([1]_2,[1]_3)=6$ であり，

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}=\langle([1]_2,[1]_3)\rangle$$

であることがわかる．よって，第 12 回講義資料命題 11.2 より，これは $\mathbb{Z}/6\mathbb{Z}$ と同型であり，具体的な同型写像は

$$\mathbb{Z}/6\mathbb{Z}\xrightarrow{\sim}\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z},\ [a]_6\mapsto([a]_2,[a]_3)$$

で与えられることがわかる (生成元 $[1]_6$ を生成元 $([1]_2,[1]_3)$ にうつした)．次の中国式剰余定理はこの同型の一般化である．

定理 13.10(中国式剰余定理, Chinese remainder theorem)

n_1,n_2 を互いに素な 2 以上の自然数とする．このとき，

$$\mathbb{Z}/n_1n_2\mathbb{Z}\xrightarrow{\sim}\mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z},\ [a]_{n_1n_2}\mapsto([a]_{n_1},[a]_{n_2})$$

は well-defined な群同型となる．特に，$\mathbb{Z}/n_1n_2\mathbb{Z}\simeq\mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z}$ である．

証明. 写像

$$\phi\colon\mathbb{Z}\to\mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z},\ a\mapsto([a]_{n_1},[a]_{n_2})$$

を考える．任意の $a,b\in\mathbb{Z}$ に対し，

$$\phi(a+b)=([a+b]_{n_1},[a+b]_{n_2})=([a]_{n_1},[a]_{n_2})+([b]_{n_1},[b]_{n_2})=\phi(a)+\phi(b)$$

となるので，ϕ は準同型である．また，

$$\begin{aligned}\mathrm{Ker}\,\phi&=\{a\in\mathbb{Z}\mid([a]_{n_1},[a]_{n_2})=([0]_{n_1},[0]_{n_2})\}\\&=\{a\in\mathbb{Z}\mid a\text{ は }n_1\text{と }n_2\text{で割り切れる }\}\\&=\{a\in\mathbb{Z}\mid a\text{ は }n_1n_2\text{で割り切れる }\}\quad(\text{ここで，}n_1\text{と }n_2\text{が互いに素であることを用いた})\\&=\{n_1n_2k\in\mathbb{Z}\mid k\in\mathbb{Z}\}=n_1n_2\mathbb{Z}\end{aligned}$$

これより，準同型定理から，

$$\mathbb{Z}/n_1n_2\mathbb{Z}\xrightarrow{\sim}\mathrm{Im}\,\phi,\ [a]_{n_1n_2}\mapsto([a]_{n_1},[a]_{n_2})$$

は well-defined な群同型になる．ここで，$\mathrm{Im}\,\phi$ は $\mathbb{Z}/n_1n_2\mathbb{Z}$ と同型であることから位数 n_1n_2 の群となるが，一方 $\mathrm{Im}\,\phi$ は位数 n_1n_2 の群である $\mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z}$ の部分群であったので，結局

$$\mathrm{Im}\,\phi=\mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z}$$

となることがわかる．よって，

$$\mathbb{Z}/n_1n_2\mathbb{Z}\xrightarrow{\sim}\mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z},\ [a]_{n_1n_2}\mapsto([a]_{n_1},[a]_{n_2})$$

が同型となることがわかる． □

注意 5. 中国式剰余定理の仮定である「n_1,n_2 は互いに素」は本質的に重要であり，実際 n_1,n_2 が互いに素でないとき必ず

$$\mathbb{Z}/n_1n_2\mathbb{Z}\not\simeq\mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z}$$

となる．例えば，$\mathbb{Z}/60\mathbb{Z}\not\simeq\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$ などとなる．理由を考えてみて欲しい (ヒント：各元の位数に着目せよ)．

注意 6. 中国式剰余定理に現れる $\mathbb{Z}/n_1n_2\mathbb{Z}$ や $\mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z}$ には群だけではなく**環 (ring)** と呼ばれる数学的構造が入る．これは群構造を与える加法 $+$ に加えて，乗法 $\times$ も同時に考えたような構造である (詳しくは「代数学 II」で扱われる)．このとき，$\mathbb{Z}/n_1n_2\mathbb{Z}$ と $\mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z}$ は中国式剰余定理の主張に書いた写像によって環としても同型になる．さらに，中国式剰余定理はより一般の環への拡張もあり，環論の範囲の定理として扱われることが多い．

この定理の “整数論的な意味” を考えてみよう．$\mathbb{Z}/n\mathbb{Z}$ において $[a]_n$ は “a を n で割った余りを見る” というように考えられるのであった．このため，n_1 と n_2 が互いに素のとき，

$$\phi_{n_1.n_2}\colon \mathbb{Z}/n_1n_2\mathbb{Z}\xrightarrow{\sim}\mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z},\ [a]_{n_1n_2}\mapsto([a]_{n_1},[a]_{n_2})$$

という同型が存在するという事実は，

> n_1 と n_2 が互いに素のとき，任意の $0\le r_1<n_1, 0\le r_2<n_2$ に対して，n_1 で割った余りが r_1，n_2 で割った余りが r_2 となるような整数 a が $\bmod n_1n_2$ で必ずただ一つ存在する[*5].

ということに他ならない．$\phi_{n_1.n_2}$ が全単射なので，任意の $0\le r_1<n_1, 0\le r_2<n_2$ に対して，

$$[a]_{n_1n_2}\coloneqq\phi^{-1}_{n_1.n_2}(([r_1]_{n_1},[r_2]_{n_2}))\in\mathbb{Z}/n_1n_2\mathbb{Z} \tag{13.4}$$

が定まり，このとき $\phi_{n_1.n_2}([a]_{n_1n_2})=([r_1]_{n_1},[r_2]_{n_2})$ なので，a は n_1 で割った余りが r_1，n_2 で割った余りが r_2 となるような整数なのである．

コラム：実際に (13.4) の a をどうやって求めるか? (進んで勉強したい方向け)

中国式剰余定理により，(13.4) で定まる a が取れることは保証されているが，どうやってそれを具体的に求めるかと言うと少し工夫が必要である．具体的な計算方法は以下で与えられる．

> n_1 と n_2 を互いに素な整数としたとき，n_1 で割った余りが r_1，n_2 で割った余りが r_2 となるような整数 a を求める $(0\le r_1<n_1, 0\le r_2<n_2)$.
>
> (Step 1) 拡張ユークリッド互除法を用いて $n_1x+n_2y=1$ を満たす整数の組 (x,y) を 1 つ求める (第 3 回講義資料参照)．得られた解を (x_0,y_0) とする．
>
> (Step 2) いま，
>
> $$\begin{aligned}\phi_{n_1.n_2}([n_1x_0]_{n_1n_2})&=([n_1x_0]_{n_1},[n_1x_0]_{n_2})=([n_1x_0]_{n_1},[n_1x_0+n_2y_0]_{n_2})=([0]_{n_1},[1]_{n_2})\\ \phi_{n_1.n_2}([n_2y_0]_{n_1n_2})&=([n_2y_0]_{n_1},[n_2y_0]_{n_2})=([n_1x_0+n_2y_0]_{n_1},[n_2y_0]_{n_2})=([1]_{n_1},[0]_{n_2})\end{aligned}$$
>
> であることに注意すると，
>
> $$\begin{aligned}\phi_{n_1.n_2}([r_2n_1x_0+r_1n_2y_0]_{n_1n_2})&=\phi_{n_1.n_2}([r_2n_1x_0]_{n_1n_2})+\phi_{n_1.n_2}([r_1n_2y_0]_{n_1n_2})\\&=([0]_{n_1},[r_2]_{n_2})+([r_1]_{n_1},[0]_{n_2})=([r_1]_{n_1},[r_2]_{n_2}).\end{aligned}$$
>
> となることがわかるので，
>
> $$\phi^{-1}_{n_1.n_2}(([r_1]_{n_1},[r_2]_{n_2}))=[r_2n_1x_0+r_1n_2y_0]_{n_1n_2}.$$
>
> よって，求める a は $r_2n_1x_0+r_1n_2y_0\pmod{n_1n_2}$.

この方法を用いて 1 つ問題を解いてみよう．

例題

> 39 で割ると 2 余り，119 で割ると 3 余る整数を 1 つ求めよ．

[*5] このような数を求める問題が古代中国の文献『孫子算経』に登場しており，そのことが中国式剰余定理という名前の由来となっている．

解答例.【まず拡張ユークリッド互除法で $39x + 119y = 1$ を満たす整数の組 (x, y) を見つける.】

$$119 = 3 \times 39 + 2 \qquad\qquad 39 = 19 \times 2 + 1$$

より,

$$\begin{aligned} 1 &= 39 - 19 \times 2 \\ &= 39 - 19 \times (119 - 3 \times 39) \\ &= 58 \times 39 + (-19) \times 119 \end{aligned}$$

となるから,$(x_0, y_0) = (58, -19)$ が $39x_0 + 119y_0 = 1$ を満たす整数の組 (x_0, y_0) の 1 つである.
【$(x_0, y_0) = (58, -19), r_1 = 2, r_2 = 3$ として,$r_2(39x_0) + r_1(119y_0)$ を計算】
これより求める値の 1 つは,

$$3 \times (39 \times 58) + 2 \times (119 \times (-19)) = 2264.$$

□

※この解法において,r_1 を n_2y_0 の方に掛けて,r_2 を n_1x_0 の方に掛けないといけないという点は間違えがちである.「この方法でなぜ求まるか」という原理も含めて解法を覚えておくことが望ましい.また,この問題は容易に検算ができるので時間のあるときは検算を行って計算間違いを防ぐと良い.

13.3 共役類・類等式

本節では,群における重要な部分集合として共役類を解説する.共役類の重要性は例えば**表現論 (representation theory)** を学ぶと非常に良く分かる.興味のある方は是非勉強してみて欲しい (以下の注意 8 も参照)[*6].

定義 13.11

G を群とする.第 13 回講義資料例 7 で見たように,写像

$$\psi_{\mathrm{ad}} \colon G \times G \to G,\ (g, h) \mapsto ghg^{-1}$$

は G 上の群 G の作用を与えるのであった (随伴作用と呼ばれた).このとき,各元 $h \in G$ の随伴作用に関する G-軌道

$$K(h) \coloneqq \{ghg^{-1} \mid g \in G\}$$

を h の**共役類 (conjugacy class)** という.

群 G の作用があるとその集合は G-軌道によって軌道分解されることから,G は互いに交わりのない共役類に分割されることがわかる.またこのとき,各 $h \in G$ における固定部分群 G_h は

$$G_h = \{g \in G \mid ghg^{-1} = h\} = \{g \in G \mid gh = hg\} = Z(\{h\})$$

となる (最後は $\{h\}$ の中心化群.第 7 回講義資料定義 6.11 参照).よって,軌道・固定群定理 (第 13 回講義資料定理 12.4) より,

$$|K(h)| = (G : Z(\{h\})) \tag{13.5}$$

となる.特に G を有限群としたとき,共役類の元の個数は必ず $|G|$ の約数である.G を有限群とし,G の共役類への分割

$$G = K(h_1) \cup K(h_2) \cup \cdots \cup K(h_m) \tag{13.6}$$

を考える.このとき,

$$K(e) = \{geg^{-1} \mid g \in G\} = \{e\} \tag{13.7}$$

[*6] 興味のある方は文献を紹介しますので,大矢までご連絡ください.

なので，$h_1 = e$ として良い．すると，(13.5), (13.6), (13.7) より，

$$|G| = |K(h_1)| + |K(h_2)| + \cdots + |K(h_m)| = 1 + \sum_{k=2}^{m} |K(h_k)| = 1 + \sum_{k=2}^{m} (G : Z(\{h_k\})) \tag{13.8}$$

となることがわかる．この等式を**類等式 (class formula)** という．

例 6. 3 次二面体群 $D_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ の共役類を全て求めてみよう．最初に単位元 e の共役類を考えると，(13.7) より，

$$K(e) = \{e\}$$

次に ($K(e)$ に含まれない元であれば何でも良いが)，$\sigma \in D_3$ の共役類を考えると，

$$\begin{aligned} K(\sigma) &= \{\sigma^k \sigma (\sigma^k)^{-1}, (\sigma^k\tau)\sigma(\sigma^k\tau)^{-1} \mid k = 0, 1, 2\} \\ &= \{\sigma, \sigma^{-1}\} = \{\sigma, \sigma^2\}. \end{aligned}$$

次に ($K(e)$，$K(\sigma)$ のいずれにも含まれない元であれば何でも良いが)，$\tau \in D_3$ の共役類を考えると，

$$\begin{aligned} K(\tau) &= \{\sigma^k \tau (\sigma^k)^{-1}, (\sigma^k\tau)\tau(\sigma^k\tau)^{-1} \mid k = 0, 1, 2\} \\ &= \{\tau, \sigma^2\tau, \sigma^4\tau\} = \{\tau, \sigma\tau, \sigma^2\tau\}. \end{aligned}$$

以上で D_3 の全ての元がいずれかの共役類の中に現れたので，D_3 の共役類への分割が

$$D_3 = K(e) \cup K(\sigma) \cup K(\tau)$$

となることがわかる．よって，D_3 の共役類は $K(e)$，$K(\sigma)$，$K(\tau)$ で全てである．(共役類は随伴作用の定める同値関係に関する同値類なので，$\sigma^2 \in K(\sigma)$ であることから，$K(\sigma) = K(\sigma^2)$ などが成立していることに注意する．) 類等式は，

$$6 = |D_3| = |K(e)| + |K(\sigma)| + |K(\tau)| = 1 + 2 + 3$$

となる．

例 7. 対称群の共役類を計算しよう．まず，第 5 回本レポート課題問題 2 で示した以下の命題を頭に入れておくと計算がしやすい．

命題 13.12

n を 2 以上の整数とする．任意の巡回置換 $(i_1\ i_2\ \cdots\ i_k) \in \mathfrak{S}_n$ と $\sigma \in \mathfrak{S}_n$ に対し，

$$\sigma(i_1\ i_2\ \cdots\ i_k)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k))$$

となる．

ではまず $\mathfrak{S}_3$ の共役類を計算してみよう．最初に単位元 e の共役類を考えると，(13.7) より，

$$K(e) = \{e\}$$

次に ($K(e)$ に含まれない元であれば何でも良いが)，$(1\ 2) \in \mathfrak{S}_3$ の共役類を考えると，命題 13.12 より，

$$\begin{aligned} K((1\ 2)) &= \{\sigma(1\ 2)\sigma^{-1} \mid \sigma \in \mathfrak{S}_3\} \\ &= \{(\sigma(1)\ \sigma(2)) \mid \sigma \in \mathfrak{S}_3\} = \{(1\ 2), (1\ 3), (2\ 3)\}. \end{aligned}$$

なお，最後の等式においては，$(i\ j) = (j\ i)$ であったことに注意しよう．次に ($K(e)$，$K((1\ 2))$ のいずれにも含まれない元であれば何でも良いが)，$(1\ 2\ 3) \in \mathfrak{S}_3$ の共役類を考えると，命題 13.12 より，

$$\begin{aligned} K((1\ 2\ 3)) &= \{\sigma(1\ 2\ 3)\sigma^{-1} \mid \sigma \in \mathfrak{S}_3\} \\ &= \{(\sigma(1)\ \sigma(2)\ \sigma(3)) \mid \sigma \in \mathfrak{S}_3\} = \{(1\ 2\ 3), (1\ 3\ 2)\}. \end{aligned}$$

なお，最後の等式においては，$(i\ j\ k) = (j\ k\ i) = (k\ i\ j)$ であったことに注意しよう．

以上で $\mathfrak{S}_3$ の全ての元がいずれかの共役類の中に現れたので，$\mathfrak{S}_3$ の共役類への分割が

$$\mathfrak{S}_3 = K(e) \cup K((1\ 2)) \cup K((1\ 2\ 3))$$

となることがわかる．よって，$\mathfrak{S}_3$ の共役類は $K(e)$，$K((1\ 2))$，$K((1\ 2\ 3))$ で全てである．

コラム：一般の $\mathfrak{S}_n$ の共役類 (進んで勉強したい方向け)

次に一般の $\mathfrak{S}_n$ の場合を考えてみよう．第 5 回講義資料定理 4.7 (2) より，任意の $\mathfrak{S}_n$ の単位元でない元はどの 2 つも互いに素な巡回置換の合成として (順序の違いを除いて) 一意的に書かれるのであった．$\sigma \in \mathfrak{S}_n$ がどの 2 つも互いに素な巡回置換の合成として，

$$\sigma = (i_{1,1}\ i_{1,2}\ \cdots\ i_{1,\ell_1})(i_{1,1}\ i_{2,2}\ \cdots\ i_{2,\ell_2})\cdots(i_{t,1}\ i_{t,2}\ \cdots\ i_{t,\ell_t}),\ \ell_1 \geq \ell_2 \geq \cdots \geq \ell_t$$

と書かれるとき，この巡回置換の長さを並べた $(\ell_1, \ell_2, \ldots, \ell_t)$ を σ の**サイクルタイプ**と呼ぶ (第 5 回本レポート課題問題 2 補足解説参照)．ここで，後の便利さのために，上の表示においては，σ で動かされない数字 k があった時にも (k) という自明な (=単位元に等しい) 巡回置換が合成されていると考えて，常に

$$\ell_1 + \ell_2 + \cdots + \ell_t = n$$

となるようにすることにする．例えば，$\mathfrak{S}_3$ においては，

$$e = (1)(2)(3) \qquad (1\ 2) = (1\ 2)(3) \qquad (2\ 3) = (2\ 3)(1) \qquad (3\ 1) = (3\ 1)(2)$$

というようにする．こうすると，$\mathfrak{S}_3$ の元

$$e, (1\ 2), (2\ 3), (3\ 1), (1\ 2\ 3), (1\ 3\ 2)$$

のサイクルタイプはこの順に，

$$(1,1,1), (2,1), (2,1), (2,1), (3), (3)$$

である．こう見ると，サイクルタイプが同じものをまとめたものが $\mathfrak{S}_3$ の共役類であることに気付けるだろう．実はこの考察は一般の $\mathfrak{S}_n$ で正しい！命題 13.12 を考えれば，サイクルタイプが同じ 2 つの元は適切な $\sigma \in \mathfrak{S}_n$ をとって，左から σ，右から σ^{-1} を掛けることで移りあえることがわかる．(厳密に考えてみよ．上に書いた $\mathfrak{S}_3$ の場合の計算が参考になると思われる．) 逆に左から σ，右から σ^{-1} を掛けるという操作は元のサイクルタイプを変えないこともわかる．これより，以下の定理がわかる．

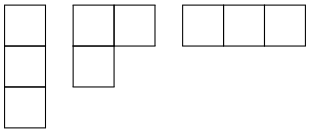
定理 13.13

n を 2 以上の整数とする．このとき，任意の $\sigma \in \mathfrak{S}_n$ に対し，

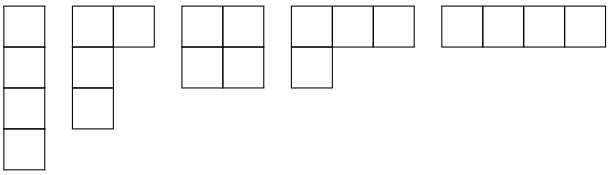
$$K(\sigma) = \{\sigma' \in \mathfrak{S}_n \mid \sigma\text{と}\sigma'\text{のサイクルタイプは等しい}\}$$

となる．特に，$\mathfrak{S}_n$ の共役類と「$\ell_1 + \ell_2 + \cdots + \ell_t = n$ かつ $\ell_1 \geq \ell_2 \geq \cdots \geq \ell_t$ を満たす正の整数の組 $(\ell_1, \ell_2, \cdots, \ell_t)$」は 1 対 1 に対応する．

$\ell_1 + \ell_2 + \cdots + \ell_t = n$ かつ $\ell_1 \geq \ell_2 \geq \cdots \geq \ell_t$ を満たす正の整数の組 $(\ell_1, \ell_2, \cdots, \ell_t)$ は n **の分割**と呼ばれる．n の分割 $(\ell_1, \ell_2, \cdots, \ell_t)$ は，同じ大きさの n 個の正方形 (箱) を各行の正方形の数が上から順に $\ell_1, \ell_2, \cdots, \ell_t$ となるように左上詰めに配置して得られる図を用いて表されることもある．このようにして得られる図を**ヤング図形 (Young diagram)** と呼ぶ．例えば，箱の数が 3 つのヤング図形は



の 3 つあり，順に 3 の分割 $(1,1,1),(2,1),(3)$ に対応する．定理を踏まえると，それぞれに対応して $\mathfrak{S}_3$ の共役類が作れて，$\mathfrak{S}_3$ の共役類は 3 つである．同様に考えると，箱の数が 4 つのヤング図形は



の 5 つあるので，定理 13.13 から $\mathfrak{S}_4$ の共役類は全部で 5 つである[*7]．

群構造を調べる上での類等式の応用例を 1 つ挙げておこう．

定理 13.14

p を素数とする．このとき，位数 p^k(k は 1 以上の整数) の群 G の中心 $Z(G)$ は $Z(G) \neq \{e\}$ となる．つまり，このような群においては必ず単位元以外に全ての元と可換性を持つ元が存在する．

注意 7. 位数が素数 p の自然数べきであるような群を p **群 (p-group)** という．例えば，4 次二面体群 D_4 は位数 $8 = 2^3$ なので，2-群である．

例 8. 4 次二面体群 D_4 においては $Z(D_4) = \{e, \sigma^2\} \neq \{e\}$ となる．

定理 13.14 の証明. 背理法で証明する．もし，$Z(G) = \{e\}$ となるとすると，全ての単位元でない $h \in G$ に対し，

$$K(h) \neq \{h\}$$

となる．なぜなら，$K(h) = \{h\}$ は，共役類の定義から任意の $g \in G$ に対して，$ghg^{-1} = h$ となることを意味するので，このとき，任意の $g \in G$ に対して $gh = hg$ で，$h \in Z(G)$ となるためである．よって，$Z(G) = \{e\}$ のとき全ての単位元でない $h \in G$ に対し，$|K(h)| > 1$ である．一方，(13.5) 直後の考察より，全ての $h \in G$ に対し，$|K(h)|$ は $|G| = p^k$ の約数である．よって，全ての単位元でない $h \in G$ に対し，$|K(h)|$ は p の倍数となる．よって，ある単位元でない $h_2, \ldots, h_m \in G$ が存在して，類等式 (13.8) から

$$p^k = |G| = 1 + \sum_{\ell=2}^{m} |K(h_\ell)| \equiv 1 \mod p$$

となるが，これは矛盾である．以上より，$Z(G) \neq \{e\}$ となる． □

13.4 ケイリーの定理 (やや発展，進んで勉強したい方向け)

本節では，「任意の有限群が実は対称群の部分群として実現できる」というケイリーの定理 (Cayley's theorem) を証明する．まず，準備として，群作用の準同型を用いた言い換えについて説明する．

G を群，X を集合としたとき，以下の命題 13.15 は，

- X 上の G の作用 $G \times X \to X$
- 準同型 $G \to B(X) \coloneqq \{f \colon X \to X \mid f \text{ は全単射 }\}$ (群 $B(X)$ については第 5 回講義資料例 1 参照)

の間に一対一の対応が作れるということを述べている．X 上の G の作用を定めるということは，準同型 $G \to B(X)$ を与えることと等価なのである．

[*7] テトリスのブロックのようだが  や  はヤング図形ではない．

命題 13.15

G を群，X を集合とする．

(1) $G \times X \to X,\ (g,x) \mapsto g \cdot x$ を集合 X 上の群 G の作用とすると，各 $g \in G$ に対し，写像

$$\phi_g \colon X \to X,\ x \mapsto g \cdot x$$

は全単射である．つまり，$\phi_g \in B(X)$ である．さらに，写像

$$\phi \colon G \to B(X),\ g \mapsto \phi_g$$

は準同型である．

(2) 逆に，準同型 $\phi \colon G \to B(X)$ が存在するとき，写像

$$G \times X \to X,\ (g,x) \mapsto g \cdot x \coloneqq \phi(g)(x)$$

は X 上の G の作用を定める．

証明.

(1) ϕ_g の全単射性 各 $g \in G$ に対し，ϕ_g の逆写像が構成できることを示せばよい．各 $x \in X$ に対し，

$$\begin{aligned}(\phi_{g^{-1}} \circ \phi_g)(x) &= \phi_{g^{-1}}(\phi_g(x)) \\ &= g^{-1} \cdot (g \cdot x) \\ &= (g^{-1} \cdot g) \cdot x \quad (\text{作用の定義条件 (2) より}) \\ &= e \cdot x = x \quad (\text{作用の定義条件 (1) より})\end{aligned}$$

となる．全く同様に $(\phi_g \circ \phi_{g^{-1}})(x) = x$．よって，$\phi_{g^{-1}} \circ \phi_g = \phi_g \circ \phi_{g^{-1}} = \mathrm{id}_X$ となる．よって，$\phi_{g^{-1}}$ が ϕ_g の逆写像であり，特に ϕ_g は全単射である．

ϕ が準同型であること 任意の $g_1, g_2 \in G, x \in X$ に対し，

$$\phi(g_1 g_2)(x) = \phi_{g_1 g_2}(x) = (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = \phi_{g_1}(\phi_{g_2}(x)) = (\phi(g_1) \circ \phi(g_2))(x)$$

となるので，$B(X)$ の元として，$\phi(g_1 g_2) = \phi(g_1) \circ \phi(g_2)$．よって，$\phi$ は準同型である．

(2) 作用の定義条件 (1) を満たすこと e を G の単位元とすると，任意の $x \in X$ に対し，

$$e \cdot x = \phi(e)(x) = \mathrm{id}_X(x) = x.$$

ここで，$\phi(e) = \mathrm{id}_X$ は第 11 回講義資料命題 10.2 (1) と群 $B(X)$ の単位元が id_X であることからわかる．

作用の定義条件 (2) を満たすこと 任意の $g, h \in G, x \in X$ に対し，

$$\begin{aligned}gh \cdot x = \phi(gh)(x) &= (\phi(g) \circ \phi(h))(x) \quad (\phi\text{が準同型であることより}) \\ &= \phi(g)(\phi(h)(x)) = g \cdot (h \cdot x).\end{aligned}$$

以上より，(2) の主張で与えられた写像は X 上の G の作用を定める． □

以下が本節の主題であるケイリーの定理 (Cayley's theorem) である．

定理 13.16

G が位数 n の有限群であるとき，単射準同型 $\phi \colon G \to \mathfrak{S}_n$ が存在する．つまり，任意の位数 n の有限群は n 次対称群のある部分群と同型になる．

証明. 第 13 回講義資料例 7 で考えた集合 G 上の群 G の作用

$$\psi_\ell \colon G \times G \to G,\ (g,h) \mapsto gh$$

を考える．ここで，G の元に適当に 1 から順に番号をつけ，集合として G と $\{1,2,\dots,n\}$ を同一視すると，この作用は

$$\psi_\ell \colon G \times \{1,2,\dots,n\} \to \{1,2,\dots,n\}$$

と見ることができる．命題 13.15 (1) より，これに対して準同型

$$\phi \colon G \to B(\{1,2,\dots,n\}) = \mathfrak{S}_n$$

が構成できる．これが単射であることを示せばよい．$g \in \operatorname{Ker}\phi$ とする．このとき，

$$\phi(g) = \mathrm{id}_{\{1,2,\dots,n\}} = \mathrm{id}_G$$

だが，命題 13.15 (1) における ϕ の構成から，これは任意の $h \in G$ に対し，

$$h = \phi(g)(h) = \psi_\ell(g,h) = gh$$

となることを主張している．ここで，$h = e$ ととると (e は G の単位元)，

$$e = ge = g$$

となるので，結局 $g = e$ である．よって，$\operatorname{Ker}\phi = \{e\}$ となり，ϕ は単射である． □

注意 8 (表現．進んで勉強したい方向け)．$\mathbb{K}$ を $\mathbb{Q}, \mathbb{R}$ または $\mathbb{C}$ とする．V を $\mathbb{K}$ 上のベクトル空間とし，

$$GL(V) \coloneqq \{f \colon V \to V \mid f \text{ は全単射線形写像 }\}$$

とする (V 上の**一般線型群**と呼ばれる)．このとき，$GL(V)$ は $B(V)$ の部分群である (チェックせよ)．また，V が n 次元ベクトル空間のとき，V の基底を 1 つ固定すると，$GL(V)$ は $GL_n(\mathbb{K})$ と同一視できるのであった (線形代数 II の内容．線形写像とその表現行列を同一視する)．

このとき，群 G に対し，準同型

$$\rho \colon G \to GL(V)$$

を群 G の V における**線形表現 (linear representation)** という．これは命題 13.15 で見た群準同型と群作用の対応を頭において見ると，G の V 上の “線形な” 作用 $G \times V \to V$ を与えているとも言える．

群 G を 1 つ与えたときに，『どのような線形表現が存在するか・どうすれば線形表現を構成できるか』ということを調べる数学の分野を (群の) **表現論 (representation theory)** という．表現論は様々な数学的手法 (代数・幾何・解析全て！) を用いて研究されており，数学の枠を超えて物理・化学への応用も持つ非常に大きな分野である．興味を持った方は是非進んで勉強してもらいたい[*8]．

1 つ例を挙げておこう．n 次二面体群 $D_n = \{\sigma^k\tau^\ell \mid k = 0,\dots,n-1, \ell = 0,1\}$ を考える．このとき，準同型

$$\rho \colon D_n \to GL_2(\mathbb{R})$$

であって，

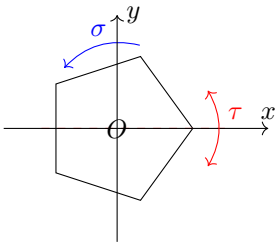
$$\rho(\sigma) = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix} \qquad \rho(\tau) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

を満たすものが存在する．これが定める $\mathbb{R}^2$ 上の D_n の作用は

$$D_n \times \mathbb{R}^2 \to \mathbb{R}^2, \left(\sigma^k\tau^\ell, \begin{pmatrix} x \\ y \end{pmatrix}\right) \mapsto \rho(\sigma^k\tau^\ell) \begin{pmatrix} x \\ y \end{pmatrix}$$

となる．このとき，σ は $\mathbb{R}^2$ の原点を中心とする $2\pi/n$ 回転に対応し，τ は x 軸に関する線対称変換に対応する．n 次二面体群が正 n 角形の対称性であったことを思い出すと，これは自然な作用である．

[*8] 私 (大矢) は代数的な方向から表現論の研究を行っている．もしもこの分野に興味を持った方は，3 年生の研究室配属時に私の研究室を候補に入れていただけると良いだろう．



13.5　シローの定理 (発展，進んで勉強したい方向け)

最後に紹介する定理はシローの定理 (Sylow's theorem) と呼ばれる定理で，群の分類問題を扱う際に非常に便利になる定理である．この定理も群作用を用いて示される．

定理 13.17 (シローの定理)

p を素数，G を有限群とし，G の位数 $|G|$ は p^ℓ では割り切れるが，$p^{\ell+1}$ では割り切れないとする．(ただし ℓ は正の整数．) このとき，任意の $1 \leq k \leq \ell$ に対し，G は位数 p^k の部分群を持つ．

注意 9. 実はこの定理には続きがあり，群の分類問題を扱う上ではそこまで知っているとより良い．興味のある方は是非調べてみてほしい．(例えば，雪江明彦 著「代数学 1 群論入門」(日本評論社) の定理 4.5.7 参照．)

注意 10. シローの定理より，特に G は位数 p^ℓ の部分群をもつことがわかる．これを **p-シロー部分群 (p-Sylow subgroup)** という．

例 9. 6 次二面体群 $D_6 = \{\sigma^k\tau^\ell \mid k = 0, \ldots, 5, \ell = 0, 1\}$ は位数 $12 = 2^2 \cdot 3$ の群なので，シローの定理より，必ず位数 $2, 2^2 = 4, 3$ の部分群をそれぞれ 1 つ以上持つということが言える．実際，それぞれ

$$\langle\tau\rangle = \{e, \tau\}, \quad \{e, \sigma^3, \tau, \sigma^3\tau\}, \quad \langle\sigma^2\rangle = \{e, \sigma^2, \sigma^4\}$$

が例を与えている．$\{e, \sigma^3, \tau, \sigma^3\tau\}$ は D_6 の 2-シロー部分群の例であり，$\{e, \sigma^2, \sigma^4\}$ は D_6 の 3-シロー部分群の例である (実は 3-シロー部分群はこれしかない)．

定理 13.17 の証明. 仮定より，G の位数は $p^\ell n$(ただし，p と n は互いに素) という形で書かれる．ここで，$1 \leq k \leq \ell$ なる k に対し，

$$X \coloneqq \{\{g_1, \ldots, g_{p^k}\} \subset G \mid g_1, \ldots, g_{p^k} \text{は相異なる } G \text{ の } p^k \text{個の元 }\}$$

としたとき，

$$G \times X \to X, (g, \{g_1, \ldots, g_{p^k}\}) \mapsto \{gg_1, \ldots, gg_{p^k}\}$$

は X 上の G の作用を定める (チェックせよ)．このとき，各 $\{g_1, \ldots, g_{p^k}\} \in X$ の固定部分群は定義より，

$$G_{\{g_1,\ldots,g_{p^k}\}} = \left\{g \in G \mid \{gg_1, \ldots, gg_{p^k}\} = \{g_1, \ldots, g_{p^k}\}\right\}$$

である．よってこのとき，各 $g \in G_{\{g_1,\ldots,g_{p^k}\}}$ に対してある $i \in \{1, \ldots, p^k\}$ が定まり，

$$gg_1 = g_i$$

となる．このとき，$g = g_i g_1^{-1}$ となるので，結局

$$G_{\{g_1,\ldots,g_{p^k}\}} \subset \{g_i g_1^{-1} \mid i = 1, \ldots, p^k\}.$$

特に，

$$|G_{\{g_1,\ldots,g_{p^k}\}}| \leq p^k$$

である．ここで，$|G_{\{g_1,\ldots,g_{p^k}\}}| = p^k$ となるものが存在することを示せば，固定部分群 $G_{\{g_1,\ldots,g_{p^k}\}}$ が G の位数 p^k の部分群となり，示すべきことが示される．

ラグランジュの定理より $|G_{\{g_1,\dots,g_{p^k}\}}|$ の値は $|G| = p^\ell n$ の約数なので，$|G_{\{g_1,\dots,g_p\}}| < p^k$ とすると特にこれは $p^{k-1}n$ の約数である．いま各 $\{g_1,\dots,g_{p^k}\} \in X$ に対し，軌道・固定群定理 (第 13 回講義資料系 12.5) から，

$$|G\cdot\{g_1,\dots,g_{p^k}\}| = \frac{|G|}{|G_{\{g_1,\dots,g_{p^k}\}}|} = \frac{p^\ell n}{|G_{\{g_1,\dots,g_{p^k}\}}|}$$

が成立するので，以上の考察から，$|G\cdot\{g_1,\dots,g_p\}|$ は

$$\begin{cases} p^{\ell-k+1}\text{の倍数} & (|G_{\{g_1,\dots,g_{p^k}\}}| < p^k \text{のとき}) \\ p^{\ell-k}n & (|G_{\{g_1,\dots,g_{p^k}\}}| = p^k \text{のとき}) \end{cases}$$

となる．これより，もし $|G_{\{g_1,\dots,g_{p^k}\}}| = p^k$ となる $\{g_1,\dots,g_{p^k}\} \in X$ が存在しないと仮定すると，X を軌道分解したときに元の個数が $p^{\ell-k+1}$ の倍数の軌道で軌道分解されるので，特に $|X|$ は $p^{\ell-k+1}$ の倍数となる．今示したかったことは，$|G_{\{g_1,\dots,g_{p^k}\}}| = p^k$ となるものの存在なので，あとは $|X|$ が $p^{\ell-k+1}$ の倍数でないことを示せば良い．

いま，

$$|X| = {}_{p^\ell n}\mathrm{C}_{p^k} = \frac{p^\ell n(p^\ell n-1)\cdots(p^\ell n-p^k+1)}{p^k(p^k-1)\cdots 1} = p^{\ell-k}n\cdot\frac{(p^\ell n-1)\cdots(p^\ell n-p^k+1)}{(p^k-1)\cdots 1} \tag{13.9}$$

である．ここで，$m\in\mathbb{Z}_{>0}$ に対し，$\ell(m)$ を

$$m \text{ は } p^{\ell(m)} \text{ で割り切れるが } p^{\ell(m)+1} \text{ では割り切れない}$$

という条件で定まる 0 以上の整数とすると，定義より $p^{-\ell(m)}m$ は p で割り切れない整数であり，$m = 1,2,\dots,p^k-1$ のとき $\ell(m) < k$ である．よって，

$$\begin{aligned} &\frac{(p^\ell n-1)\cdots(p^\ell n-p^k+1)}{(p^k-1)\cdots 1} \\ &= \frac{(p^{\ell-\ell(1)}n-p^{-\ell(1)}1)\cdots(p^{\ell-\ell(m)}n-p^{-\ell(m)}m)\cdots(p^{\ell-\ell(p^k-1)}n-p^{-\ell(p^k-1)}(p^k-1))}{(p^{k-\ell(1)}-p^{-\ell(1)}1)\cdots(p^{k-\ell(m)}-p^{-\ell(m)}m)\cdots(p^{k-\ell(p^k-1)}-p^{-\ell(p^k-1)}(p^k-1))}. \end{aligned}$$

ここで，右辺の分子分母の積の各項は整数であることに注意する．このとき，右辺の分子に現れる $(p^{\ell-\ell(m)}n - p^{-\ell(m)}m),\ m=1,\dots,p^k-1$ という形の整数は $p^{\ell-\ell(m)}n$ が p の倍数，$-p^{-\ell(m)}m$ が p で割り切れない整数であることより，p で割り切れない整数である．よって，それらの積である右辺の分子は p で割り切れず，それをさらに整数で割って得られる数である右辺の値は p の倍数ではない．

以上より，$\dfrac{(p^\ell n-1)\cdots(p^\ell n-p^k+1)}{(p^k-1)\cdots 1}$ は p の倍数ではないことが示された．さらに p と n は互いに素であることより，(13.9) から，結局 $|X|$ は $p^{\ell-k+1}$ の倍数ではないことがわかる．よって，示すべきことは全て示された． □