# 代数学 I 第 12 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

今回の講義資料の前半では，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．これは古くから考えられていた整数に関するある種の問題に必ず解があることを保証する定理である (具体的な問題については p.4 を参照)．後半では，可解群について解説を行う．群の可解性は，第 1,2 回講義資料 (p.4) の Galois 理論概観でも少し言及したが，Galois 理論を通じて代数方程式の可解性と直接関連する概念である．しかし，本資料で学ぶように，群の可解性の定義は代数方程式となぜ関係するのか一見わからないような純粋に群論的なものである．興味を持たれた方はぜひ Galois 理論も合わせて勉強してもらいたい．[*1]

## 10.1 群の直積・中国式剰余定理

本節の目標は中国式剰余定理を解説することである．このためにまず群の直積というものを準備する．

**定義 10.1**

$G_1, G_2$ を群とする．$G_1$ と $G_2$ の直積集合

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

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

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

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[*2]．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．
$G_1, G_2$ の単位元をそれぞれ $e_1, e_2$ とすると，$G_1 \times G_2$ 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．

**例 1.** $\mathbb{Z}/2\mathbb{Z}$ 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 $|\mathbb{Z}/2\mathbb{Z}| \cdot |\mathbb{Z}/3\mathbb{Z}| = 2 \cdot 3 = 6$ 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，

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

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

*1 可解群の話 (10.2 節) は時間の都合上，講義内では扱えないかもしれません．とにかく講義で扱われる内容の予習をしたいという方は前半の 10.1 節をしっかり読んでいただければと思います．

*2 チェックは容易なのでここでは省略する．試してみよ．

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．

**例 2.** 5 次対称群 $\mathfrak{S}_5$ の部分群

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c & d & e \end{pmatrix} \;\middle|\; a, b \text{ は } 1, 2 \text{ の並べ替え}, \; c, d, e \text{ は } 3, 4, 5 \text{ の並べ替え} \right\}$$

を考える．これは，$1, 2$ の置換と $3, 4, 5$ の置換を合成することによって得られる $1, 2, 3, 4, 5$ の置換の全体である ($H$ は部分群となることは各自チェックせよ)．このとき，部分群 $H$ は直積群

$$\mathfrak{S}_2 \times \mathfrak{S}_3$$

に同型である．実際，同型写像が

$$\phi \colon \mathfrak{S}_2 \times \mathfrak{S}_3 \to H, \; \left( \begin{pmatrix} 1 & 2 \\ a & b \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ c & d & e \end{pmatrix} \right) \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c+2 & d+2 & e+2 \end{pmatrix}$$

で与えられる．例えば，

$$\phi \left( \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right) \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

というような写像である．$\phi$ が同型写像であることは各自確かめてもらいたいが，$H$ が「$1, 2$ の置換と $3, 4, 5$ の置換を合成することによって得られる $1, 2, 3, 4, 5$ の置換の全体」であることを考えれば，自然に理解できるであろう ($\mathfrak{S}_2 \times \mathfrak{S}_3$ の第 1 成分 $\mathfrak{S}_2$ が $1, 2$ の置換を指定し，第 2 成分 $\mathfrak{S}_3$ が $3, 4, 5$ の置換を指定している)．

注意 1. 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

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

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[*3]．

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．

**例 3.** $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ 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 11 回講義資料定理 9.2 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 $([1]_2, [1]_3)$ にうつす同型写像)．次の中国式剰余定理はこの同型の一般化である．

[*3] $\{G_i\}_{i \in I}$ 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．

**定理 10.2(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，$\phi$ は準同型である．また，

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

これより，準同型定理から，

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

は well-defined な群同型になる．ここで，$\operatorname{Im}\phi$ 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 $\operatorname{Im}\phi$ 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

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

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 2. 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 3. 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．

なお，中国式剰余定理の主張は繰り返し用いることで以下のように一般化できる．

**定理 10.3(中国式剰余定理 (定理 10.2 の拡張))**

$n_1, \cdots, n_k$ をどの 2 つも互いに素な 2 以上の自然数とする ($k \geq 2$)．このとき，

$$\mathbb{Z}/n_1 \cdots n_k\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z},\ [a]_{n_1 \cdots n_k} \mapsto ([a]_{n_1}, \ldots, [a]_{n_k})$$

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

定理 10.2 を繰り返し用いて定理 10.3 を得るというのを例で見ておこう．例えば，$30 = 2 \cdot 3 \cdot 5$ を考える．

$2,3,5$ はどの 2 つも互いに素な 2 以上の自然数である．このとき，まず 2 と $15 = 3 \cdot 5$ は互いに素なので，定理 10.2 より，

$$\mathbb{Z}/30\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z},\ [a]_{30} \mapsto ([a]_2, [a]_{15})$$

は群同型である．ここで，3 と 5 も互いに素なので，定理 10.2 より，

$$\mathbb{Z}/15\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z},\ [a]_{15} \mapsto ([a]_3, [a]_5)$$

も群同型である．これらを組み合わせて，

$$\mathbb{Z}/30\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z},\ [a]_{30} \mapsto ([a]_2, [a]_{15}) \mapsto ([a]_2, [a]_3, [a]_5)$$

は群同型であることがわかる．定理 10.3 はこのような状況を一般に述べたものである．

中国式剰余定理の “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，$n_1, \cdots, n_k$ がどの 2 つも互いに素なとき，

$$\phi_{n_1,\ldots,n_k} \colon \mathbb{Z}/n_1 \cdots n_k\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z},\ [a]_{n_1\cdots n_k} \mapsto ([a]_{n_1}, \ldots, [a]_{n_k})$$

という同型が存在するという事実は，

> $n_1, \cdots, n_k$ がどの 2 つも互いに素なとき，任意の $0 \leq r_i < n_i$ $(i = 1, \ldots, k)$ に対して，
>
> - $n_1$ で割った余りが $r_1$
> - $n_2$ で割った余りが $r_2$
>
> $\vdots$
>
> - $n_k$ で割った余りが $r_k$
>
> となるような整数 $a$ が $\bmod n_1 \cdots n_k$ で必ずただ一つ存在する[*4].

ということに他ならない．$\phi_{n_1,\ldots,n_k}$ が全単射なので，任意の $0 \leq r_i < n_i$ $(i = 1, \ldots, k)$ に対して，

$$[a]_{n_1\cdots n_k} \coloneqq \phi^{-1}_{n_1,\ldots,n_k}(([r_1]_{n_1}, \ldots, [r_k]_{n_k})) \in \mathbb{Z}/n_1 \cdots n_k\mathbb{Z} \tag{10.1}$$

が定まり，このとき

$$([r_1]_{n_1}, \ldots, [r_k]_{n_k}) = \phi_{n_1,\ldots,n_k}([a]_{n_1\cdots n_k}) = ([a]_{n_1}, \ldots, [a]_{n_k})$$

なので，$a$ は $n_i$ で割った余りが $r_i$ $(i = 1, \ldots, k)$ となるような整数なのである．

**コラム：実際に (10.1) 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，(10.1) 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いうことを考えてみる．以下のように考えれば良い；

$n = n_1 \cdots n_k$ とする．まず，各 $i = 1, \ldots, k$ について，

$$\phi_{n_1,\ldots,n_k}([a_i]_n) = ([0]_{n_1}, \ldots, [0]_{n_{i-1}}, [1]_{n_i}, [0]_{n_{i+1}}, \ldots, [0]_{n_k}) \tag{10.2}$$

を満たす $a_i \in \mathbb{Z}$ が求められたとする．すなわち，

$$[a_i]_{n_s} = \begin{cases} [1]_{n_i} & s = i \text{ のとき}, \\ [0]_{n_s} & s \neq i \text{ のとき}, \end{cases}$$

を満たす $a_i \in \mathbb{Z}$ が求められたとする．このとき，(10.1) の $a$ は

$$a = r_1a_1 + \cdots + r_ka_k = \sum_{i=1}^{k} r_ia_i$$

[*4] 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．

で与えられる．なぜなら，各 $s = 1, \ldots, k$ について，

$$\begin{aligned}[a]_{n_s} &= \sum_{i=1,\ldots,k} r_i[a_i]_{n_s} \\ &= r_s[a_s]_{n_s} + \sum_{i=1,\ldots,k;i\neq s} r_i[a_i]_{n_s} \\ &= r_s[1]_{n_s} + \sum_{i=1,\ldots,k;i\neq s} r_i[0]_{n_s} = [r_s]_{n_s}\end{aligned}$$

となるためである．これより，あとは (10.2) を満たす $a_i$ の求め方がわかれば良い．いま，$n_1, \cdots, n_k$ はどの 2 つも互いに素なので，

$$n_i \quad と \quad n/n_i = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k$$

は互いに素な自然数である．よって，第 3 回講義資料系 2.5 から，

$$n_i x_i + (n/n_i) y_i = 1$$

を満たす整数の組 $(x_i, y_i)$ が存在する．なお，このような $(x_i, y_i)$ はユークリッド互除法の計算を逆にたどる，あるいは拡張ユークリッド互除法で求められるのであった．このとき，実は

$$a_i = (n/n_i) y_i$$

とすれば良い．実際，

$$[a_i]_{n_i} = [(n/n_i) y_i]_{n_i} = [n_i x_i + (n/n_i) y_i]_{n_i} = [1]_{n_i}$$

であり，$s \neq i$ であれば，

$$[a_i]_{n_s} = [(n/n_i) y_i]_{n_s} = [n_1 \cdots n_{i-1} n_{i+1} \cdots n_k y_i]_{n_s} = [0]_{n_s}$$

となる．この方法を用いて 1 つ問題を解いてみよう．

**例題**

3 で割ると 2 余り，5 で割ると 3 余り，14 で割ると 10 余る整数を 1 つ求めよ．

**解答例.** $3, 5, 14$ はどの 2 つも互いに素なので，中国式剰余定理により，

$$\phi_{3,5,14} \colon \mathbb{Z}/210\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z},\ [a]_{210} \mapsto ([a]_3, [a]_5, [a]_{14})$$

は同型写像である．まず，

$$\begin{aligned}\phi_{3,5,14}([a_1]_{210}) &= ([1]_3, [0]_5, [0]_{14}), \\ \phi_{3,5,14}([a_2]_{210}) &= ([0]_3, [1]_5, [0]_{14}), \\ \phi_{3,5,14}([a_3]_{210}) &= ([0]_3, [0]_5, [1]_{14}),\end{aligned}$$

を満たす $a_1, a_2, a_3 \in \mathbb{Z}$ を求める．このためには，

$$3x_1 + 5 \cdot 14 y_1 = 3x_1 + 70 y_1 = 1 \tag{10.3}$$
$$5x_2 + 3 \cdot 14 y_2 = 5x_2 + 42 y_2 = 1 \tag{10.4}$$
$$14x_3 + 3 \cdot 5 y_3 = 14x_3 + 15 y_3 = 1 \tag{10.5}$$

を満たす整数の組 $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ を求め，

$$a_1 = 70 y_1, \quad a_2 = 42 y_2, \quad a_3 = 15 y_3$$

とすればよい．そこで (10.3), (10.4), (10.5) を満たす整数の組を 1 つずつ求めると，

$$(x_1, y_1) = (-23, 1), \quad (x_2, y_2) = (17, -2), \quad (x_3, y_3) = (-1, 1).$$

(これらの整数解を求める手順はここでは省略する．第 3 回講義資料 2.3 節を参照のこと．なおこれらの整数解は無限にあるが，1 つ見つければ良い．) よって，

$$a_1 = 70, \quad a_2 = -84, \quad a_3 = 15$$

と取れる．これより，問題の条件を満たす整数 $a$ として，

$$a = 2a_1 + 3a_2 + 10a_3 = 140 + (-252) + 150 = 38$$

が取れる． □

注意 4. この種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．なお例題の条件を満たす整数の全体は，

$$\{38 + 210k \mid k \in \mathbb{Z}\}$$

である．また，上の計算により，3 で割ると $r_1$ 余り，5 で割ると $r_2$ 余り，14 で割ると $r_3$ 余る整数の全体は，

$$\{70r_1 - 84r_2 + 15r_3 + 210k \mid k \in \mathbb{Z}\}$$

である．

## 10.2 可解群

本節では可解群という概念を導入し，対称群の可解性を調べる (定理 10.10).

**定義 10.4**

$G$ 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 5. 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 10.5**

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

命題 10.5 の証明のために，以下の補題を用いる．

**補題 10.6**

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

$$s = s_1^{m_1} \cdots s_k^{m_k} \text{ (ただし, } s_1, \ldots, s_k \in S, m_1, \ldots, m_k \in \mathbb{Z}, k \in \mathbb{N}) \tag{10.6}$$

と書けるのであった (第 6 回講義資料定義 5.2)．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 10 回講義資料例 12)．これより，任意の $g \in G$ と上の (10.6) 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，$\langle S \rangle$ は $G$ の正規部分群である． □

**命題 10.5 の証明.** 補題 10.6 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[*5]．補題 10.6 の証明中に定義した群同型 $\alpha_g$ 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 10.7**

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 10 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．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 6. 命題 10.7 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．

[*5] 補題 10.6 における $S$ が $\{[g_1, g_2] \mid g_1, g_2 \in G\}$ である

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 10.5 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 10.7 より，剰余群 $\mathrm{D}_{k-1}(G)/\mathrm{D}_k(G)$ は可換群となる．

**定義 10.8**

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 7. 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 4.** $G$ 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 5.** $n$ 次二面体群 $D_n$ を考える ($D_n$ の元については第 5 回講義資料の記号を用いる)．このとき，

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

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 4 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 10.9**

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，

$$\mathrm{D}_k(N) \subset \mathrm{D}_k(G) \tag{10.7}$$

となる[*6]．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，

$$p(\mathrm{D}_k(G)) = \mathrm{D}_k(G/N) \tag{10.8}$$

である[*7]．これらをもとに，(1) と (2) の同値性を証明する．

(1) ⇒ (2) (10.7), (10.8) 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，(10.8) 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，(10.7) 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 6.** 例 5 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 10.9 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，これは正規部分群で剰余群 $D_n/N$ の位数はラグランジュの定理より $|D_n|/|N| = 2n/n = 2$ である．ここで，$N$ は巡回群なので可換であり，$D_n/N$ は位数 2 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 7.5)．よって，$N$ も $D_n/N$ も共に可解であるから，命題 10.9 より $D_n$ も可解である．

最後に対称群の可解性について述べよう．

**定理 10.10**

$n$ 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 5 回講義資料注意 1)，例 5 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，剰余群 $\mathfrak{S}_4/V$ は $\mathfrak{S}_3$ と同型になるのであった (第 9 回復習レポート課題問題 4 補足解説参照)．よって，$V$ も $\mathfrak{S}_4/V$ も可解となるので，命題 10.9 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．

$$S \coloneqq \{(i\ j\ k) \mid i, j, k \text{ は相異なる } \{1, \dots, n\} \text{ の元 }\}$$

とし，任意の $m \in \mathbb{Z}_{\geq 0}$ に対し，

$$\mathrm{D}_m(\mathfrak{S}_n) \supset S \tag{10.9}$$

となることを $m$ に関する帰納法で示す．$m = 0$ のときは $\mathrm{D}_0(\mathfrak{S}_n) = \mathfrak{S}_n$ なので (10.9) は自明である．次に，ある $m \in \mathbb{Z}_{\geq 0}$ で $\mathrm{D}_m(\mathfrak{S}_n) \supset S$ であったと仮定する．いま $n \geq 5$ なので，相異なる $\{1, \dots, n\}$ の元 $i, j, k$

[*6] 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．

[*7] $p$ 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．

に対して，それらのいずれとも異なる $\ell_1, \ell_2 \in \{1, \dots, n\}, \ell_1 \neq \ell_2$ をとることができる．すると，仮定より $(i\ j\ \ell_1), (i\ k\ \ell_2) \in S \subset \mathrm{D}_m(\mathfrak{S}_n)$ であり，

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

となる．よって，$(i\ j\ k)$ は $\mathrm{D}(\mathrm{D}_m(\mathfrak{S}_n)) = \mathrm{D}_{m+1}(\mathfrak{S}_n)$ の元であることがわかるので，$\mathrm{D}_{m+1}(\mathfrak{S}_n) \supset S$ も成り立つことが示された．よって，任意の $m \in \mathbb{Z}_{\geq 0}$ に対し，(10.9) が成り立つ．特に，任意の $m \in \mathbb{Z}_{>0}$ に対し，$\mathrm{D}_m(\mathfrak{S}_n) \neq \{e\}$ となるので，このとき $\mathfrak{S}_n$ は非可換である． □

定理 10.10 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 **Galois 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 Galois 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 10.10 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．