# 群論入門これだけ

山上　滋

2012 年 7 月 9 日

おまたせしました、「これだけ」シリーズの群論入門編です。

群論の初歩を半年かけて学びます。「群」の授業は、代数の一部というとらえ方が支配的ですが、幾何学・解析学さらには応用数学全般にまで及ぶ汎用的な形が本来のあるべき姿です。もちろん、内容のある話をするためにはそれなりの予備知識を必要とし、また初歩の内容としては、有限の対象を中心にせざる得ないという事情もありますが、できるだけ代数固有の話題に入り込まないようなものをここでは意図してみました。

最近は、そういった心がけの日本語の本もいくつか目に付くようにはなってきましたが、群に限定したものとなると、まだまだ不足しているという印象です。教える側の意識の問題もあるのでしょう。(教科書として使われない本は出版され難い。)

さてこの教材には多くの「問」が含まれています。これは、いくら証明などの「理屈」を聞いても、実践的な体験なしには身に付かない、という理由からです。一部、難しい問題も入っていますが、大部分は、考えて、あるいは他の本を参考にして、自ら答えに到達できる程度のものです。演習の時間もあることですし、できるだけ多くの問にトライしてみてください。

それと、この教材についてのコメント・要望・間違いの指摘も歓迎します。授業アンケートよりは、よほど効果があるはずです。

参考書としていくつか挙げておきます。


- M.A. Armstrong, Groups and Symmetry, Springer-Verlag, NewYork, 1988
- ドゥージン・チェボタレフスキー「変換群入門」、シュプリンガー・フェアラーク東京 (2000)
- 志賀浩二「群論への３０講」、朝倉書店 (1989)
- 国吉・高橋「群論入門」(新訂版)、サイエンス社 (2001)
- 岩永恭雄「代数学の基礎」、日本評論社 (2002)

- 金子晃「応用代数講義」、サイエンス社 (2006)

古い順に並べてみたのですが、今でも、Armstrong の本はお薦めです。でも、英語がちょっと、という人は、志賀か国吉・高橋あたりが無難でしょうか。岩永は、代数全般について書かれていますが、なかなか愛想の良い本です。副読本としても使えそうです。金子も代数全体の俯瞰によいでしょう。情報系の授業のためということですが、どうして、ここに書いてある内容をしっかり理解できれば、数学科でも通用するかも知れません。ドゥージンの本は、平面幾何学のパズル的問題から微分方程式の対称性にいたるまで、個性的かつ魅力的な内容です。何かを効率的に学習するといった現在の余裕のない風潮とは一線を画するもので正に culture を感じさせてくれます。(Armstrong の本は、最近、翻訳が「対称性からの群論入門」というタイトルでシュプリンガー・ジャパンから出た。)

また、Web で検索すると、かなり立派な代数の「教科書」が公開されていて、貧乏人には有り難い世の中ではあります。そういったものの中には、下手な本よりもよっぽど良く書けているものがあったりして、ここでも「コストと品質は無関係である」というソフトウェア業界の法則(?)が有効のようです。

# 目次

自然数の集合 $\mathbb{N}$ には 0 も含めておくことにする。他に良く使われる集合の記号として、

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}, \quad \mathbb{R} = \text{実数全体}, \quad \mathbb{C} = \text{複素数全体}.$$

# 1 対称性とは

対称性の数学的実例について概観し、次節で与える「群」の概念への動機付けとする。

## 1.1 割り算の数学

自然数 $n \geq 2$ を一つ用意する。勝手な自然数 $a$ を $n$ で割り算してみることにより、

$$a = qn + r$$

となる自然数 $q, r$ で $0 \leq r < n$ となるものが一意的に定まる（割り算の原理)。自然数 $r$ は、$a$ を $n$ で割った**余り**または**剰余** (remainder) と呼ばれる。別の自然数 $a'$ の余りを $r'$ で表わす。もし、$r = r'$ であれば、$a$ と $a'$ は、**n を法として合同** である ($a$ and $a'$ are congruent modulo $n$) と言い、

$$a \equiv a' \mod n$$

という記号で表わす。このとき、$a \equiv a' \mod n \iff a - a'$ が $n$ で割り切れる、となる。そこで、$a, a'$ が整数のときにも、$a - a'$ が $n$ で割り切れる（$n$ の倍数である）という条件を記号 $a \equiv a' \mod n$ で表わすことにする。またこのような数の関係式を**合同式** (congruence) と呼ぶ。

**命題 1.1** (合同式の性質)**.**

$$a \equiv a',\ b \equiv b' \quad \Longrightarrow \quad a \pm b \equiv a' \pm b',\ ab \equiv a'b'.$$

**問 1.** 合同式の性質を確認。

**問 2.** 自然数 $m$ の十進数表示を $a_l \dots a_2 a_1$ とするとき、

$$m \equiv a_1 + a_2 + \cdots + a_l \mod 9.$$

したがって、例えば、

$$271828 \equiv 2+7+1+8+2+8 = 28 \equiv 1 \mod 9.$$

11 を法とした剰余類について類似の計算方法を与えよ。

整数のグループ分けを

$$[r] = \{a \in \mathbb{Z}; a \equiv r\}, \qquad r = 0, 1, \ldots, n-1$$

で定める。各グループを $n$ を法とした**剰余類** (congruence class) と呼ぶ。より一般に、

$$[a] = \{a + kn; k \in \mathbb{Z}\} = a + n\mathbb{Z}$$

とおく。そして、$a$ は剰余類 $[a]$ を代表する、あるいは剰余類の**代表元** (representative) である、といった言い方をする。例えば、[1] も $[-n+1]$ も同じ剰余類を表わすので、剰余類 [1] の代表元として整数 $1-n$ を取ることもできる。

剰余類の集まりを剰余類集合といい、$\mathbb{Z}_n$ なる記号で表わす。$\mathbb{Z}_n$ の各要素（剰余類）は、整数を $n$ で割った余りで区別されるので、剰余類集合 $\mathbb{Z}_n$ は、丁度 $n$ 個の要素からなる集合である。とくに、$n = 2$ の場合の剰余類は、偶数（全体）と奇数（全体）である。

$n = 7$ として、今日、２００４年４月１２日（月)、を基点に $a$ 日後の曜日により、整数 $a$ をグループ分けすると、剰余類と曜日とが１対１に対応する。したがって、今年が閏年であることに注意すれば、去年、２００３年４月１２日の曜日は、

$$366 \equiv 2 \mod 7$$

より、月曜日の２つ前の曜日、すなわち、土曜日であり、来年、２００５年４月１２日の曜日は、

$$365 \equiv 1 \mod 7$$

より、月曜日の一つ後の曜日、すなわち、火曜日であることがわかる。

このように整数の剰余類は、周期的な規則性を表現する上で便利な概念である。より身近な例としては、小学校で習う「時計算」というものがある。１９時の８時間後は何時か、といったあれである。時刻の表示は、２４時間式では２４を法とした、１２時間式では（午前・午後の補助指標を使うにしろ）１２を法とした剰余類に他ならない。この意味で、現代人は、押し並べて剰余類を理解し使いこなしていると言えるだろうか。

剰余類集合は、余りに着目した整数のグループ分けであるが、このグループ同志の和を

$$[a] + [b] = [a+b]$$

によって定義することができる。

**問 3.** 和の定義が、代表元の取り方によらず、剰余類だけで決まること (well-definedness) を確認。

このようにして定められた剰余類同志の和は、通常の数の場合と同様に、結合法則、交換法則をみたす。

$$([a]+[b])+[c]=[a]+([b]+[c]), \qquad [a]+[b]=[b]+[a].$$

さらに、0 を含む剰余類 $[0]=\mathbb{Z}n$ は、$[a]+[0]=[a]=[0]+[a]$ がいつでも成り立つという意味で、零元と呼ばれる。また、整数 $k$ に対して、剰余類 $[a]$ の $k$ 倍を $k[a]=[ka]$ によって定めることができて (well-defined である)、とくに $-[a]=[-a]$ は、

$$[a]+[-a]=[-a]+[a]=[0]$$

をみたすという意味で、$[a]$ の「負数」に相当する剰余類である。

**問 4** (Optional)**.** 素数 $p$ を考える。自然数 $m,n$ について、

$$(m+n)^p \equiv m^p+n^p \mod p$$

であることを示し、これから $m^p \equiv m \mod p$ を導け。

## 1.2 置換と対称式

3 文字 $x,y,z$ の多項式 $f(x,y,z)$ を考える。文字の入れ替えを行うことにより、別の多項式を作り出すことができる。

$$x \leftrightarrow y, \quad f(y,x,z)$$
$$x \to y, y \to z, z \to x, \quad f(y,z,x).$$

どのような文字の入れ替えを行っても変化しない式を**対称式** (symmetric expression) という。例えば、

$$x+y+z, \quad x^2y+y^2z+z^2x+xy^2+yz^2+zx^2$$

などがそうである。対称式どうしを足しても掛けてもやはり対称式が出現する。その意味で、代数計算が可能な集団（環, ring という）を形成している。

対称式の中でも重要なものに**基本対称式** (elementary symmetric polynomial) があり、今の場合、$(t-x)(t-y)(t-z)$ を $t$ の冪で展開した際の係数として定められる。

$$(t-x)(t-y)(t-z)=t^3-(x+y+z)t^2+(xy+yz+zx)t-xyz.$$

この恒等式における $x, y, z$ を 3 次方程式 $t^3 + at^2 + bt + c = 0$ の解（根）を表わしていると見ると、いわゆる根 (解）と係数の関係（Viete の定理）

$$x + y + z = -a, \quad xy + yz + zx = b, \quad xyz = -c$$

が得られる。

以上を一般化して、$n$ 変数の多項式 $f(x_1, \ldots, x_n)$ の文字 $x_1, \ldots, x_n$ を置換 $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$ により入れ替えて得られる多項式 $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ を考えると、あらゆる置換 $\sigma$ に対して $f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ であるものが対称式であり、また、$x_1, \ldots, x_n$ の基本対称式 $s_i(x_1, \ldots, x_n)$ $(i = 1, 2, \ldots, n)$ は、

$$(t - x_1)(t - x_2) \ldots (t - x_n) = \\ t^n - s_1(x_1, \ldots, x_n)t^{n-1} + s_2(x_1, \ldots, x_n)t^{n-2} + \cdots + (-1)^n s_n(x_1, \ldots, x_n)$$

で定められる。

このとき、任意の対称多項式は基本対称式の多項式で表わされることを証明することができる。具体例としては、

$$x^2y + y^2z + z^2x + xy^2 + yz^2 + zx^2 = (x + y + z)(xy + yz + zx) - 3xyz$$
$$x^2 + y^2 + z^2 = (x + y + z)^2 - 2(xy + yz + zx)$$

**問 5.** $x^3 + y^3 + z^3 - 3xyz$ を $x, y, z$ の基本対称式で表わせ。

このように、代数方程式と対称式とは密接な関係にある。代数方程式の代数的解法をこのような根 (root) の入れ替えに関するある種の対称性と結びつけるというアイデアは Lagrange によるもので、ここに Galois 理論の萌芽を見て取ることができる。このような考えに基づく方程式論の研究において Lagrange は次のような問題に遭遇した。

一つの（対称とは限らない）多項式 $f(x_1, \ldots, x_n)$ から出発して、全ての置換 $\sigma$ について $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ を作るとき、異なった式がいくつ得られるか。

Lagrange の発見したことは、次の事実である。

$$G(f) = \{\sigma; f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n)\}$$

とおくとき、得られる多項式の個数は

$$\frac{n!}{|G(f)|}$$

で与えられる。

**問 6.** Lagrange の定理を、

(i) $n=3$, $f=xy$, $f=(x-y)(y-z)(z-x)$ について確かめよ。
(ii) $f=x_2+\cdots+x_n$ について確かめよ。

一般に、$G(f)$ の個数が多いほど $f$ の対称性が高いと考えられる。もう少し正確に述べると、多項式 $f, g$ に対して、$G(f)\subset G(g)$ であるとき、$g$ の対称性は $f$ のそれよりも高い。したがって対称性が最も高いものが対称式である。

**問 7.** $xy+z^2$ と $x^2y+y^2z+z^2x$ の対称性の程度を比較せよ。$n=4$ で、$x_1+x_2$ と $x_1+x_2+x_3^2$ はどちらの対称性が高いか。$n=3$ ではどうか。

## 1.3 図形の対称性

平面の変換とは平面を同じ平面に移す写像のことであり、平面の合同変換とは 2 点間の距離を保つ変換のことである。平面を無限に広がる板と思えば、合同変換とは板を動かしてもとの板に重ねる操作であるとも見なせる。

平面内の図形 $K$ に対して、$K$ を $K$ 自身にぴったり重ねる合同変換が $K$ の対称性を記述していると、以下では考えることにしよう。このような合同変換全体を一つの集合と捉え、図形 $K$ の合同変換群ということにする。合同変換群は恒等変換を必ず含むので空集合になることはないのであるが、恒等変換以外の合同変換がなければ、図形 $K$ の対称性はないに等しいことになる。

例として、三角形 $\triangle ABC$ の対称性を考えよう。対称性の高い順に、

正三角形、二等辺三角形、不等辺三角形

となる。三角形の頂点を $A, B, C$ とし、可能な対称変換（合同変換で三角形 $\triangle ABC$ をそれ自身に写すもの）を頂点の置換で表わせば、

$$\text{正三角形}: \left\{ \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}, \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}, \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} \right.$$
$$\left. \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}, \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}, \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} \right\}.$$

$$\text{二等辺三角形}: \left\{ \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}, \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} \right\}.$$

$$\text{不等辺三角形}：\left\{\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}\right\}.$$

**問 8.** 平面の合同変換を用いて、正方形の対称性、正五角形の対称性について調べる。

**問 9** (Optional)**.** 正六面体の対称性、正四面体の対称性について調べる。

このほかにも対称性は様々な形で姿を見せる。

- 丸い図形は回転対称性をもつ。
- 平行移動での対称性

$$f(x+T)=f(x) \Longrightarrow \text{周期関数} \Longrightarrow \text{フーリエ解析}$$

- 偶関数・奇関数も対称性の一種

$$f(-x)=\pm f(x).$$

- 右手系・左手系も対称性とみなせる。
- 複素共役 $z=x+iy \mapsto \overline{z}=x-iy$ も対称性を表わしている。複素平面における鏡映変換。

# 2 群と部分群

抽象的な定義を述べる前に、群の概念のそもそもの発祥の場となった「置換」について、その性質を確認しておこう。一般に、置換 $\sigma, \tau$ に対してその積 $\sigma\tau$ を写像としての合成で定める：

$$(\sigma\tau)(i)=\sigma(\tau(i)), \qquad 1 \leq i \leq n.$$

また、$\sigma$ の逆写像を $\sigma^{-1}$ という記号で表わして、$\sigma$ の逆置換と呼ぶことにする。

そこで、$n$ 文字の置換全体の集合を $S_n$ で表わせば、$S_n$ においては積が定義できて、写像の合成に由来する結合法則をみたし、さらに 1 に相当する恒等置換 $1_n$ を含み、$\sigma \in S_n$ の逆置換 $\sigma^{-1} \in S_n$ は、関係式 $\sigma\sigma^{-1}=\sigma^{-1}\sigma=1$ を満たしていることがわかる。同様の性質は図形のもつ対称性を表わす合同変換の集まりについても確かめられる。

一方で、周期的な現象の対称性を表わすであろう、$\mathbb{Z}$ や剰余類集合 $\mathbb{Z}_n$ には「和」の演算を考えることができた。

以上、２種類の状況を統一的に扱うために、イギリスの数学者 A. Cayley により 1878 年に導入されたものが次に述べる定義である。

集合 $G$ の 2 つの元 $a, b$ に対して $G$ の元 $a * b$ が定められていて、言い方を換えれば、写像 $G \times G \to G$ が与えられていて（このような写像を二項演算 (binary operation) という）、

(i) **結合法則** (associativity law) $a * (b * c) = (a * b) * c$ が成り立ち、
(ii) すべての $a \in G$ に対して、$e * a = a * e = a$ となるような元 $e \in G$ (**単位元**、unit element、という）が存在し、
(iii) さらに、各 $a \in G$ に対して、$a * a' = a' * a = e$ となる元 $a' \in G$ ($a$ の**逆元**、inverse element、という）が存在する

とき、このような演算の情報をもった集合 $G$ を**群** (group) と称する。

**例 2.1.** 整数全体 $\mathbb{Z}$ は、二項演算 $a * b = a + b$ により群であるが、$a * b = ab$ としたものは群にはならない。逆元の存在が保証されないから。

二項演算の記号はしばしば省略され、単に積の記号 $ab$ で代用される。また、そのときには、逆元を記号 $a^{-1}$ で表すのが普通である。単位元については 1 という書き方も許す。群 $G$ の単位元であることを強調して、$1_G$ という記号を使うこともある。

群の典型的な例は、変換によって与えられる。集合 $X$ に対して、$X$ から $X$ 自身への写像を $X$ における**変換** (transformation) と言う。変換に対しては逆写像という代わりに**逆変換** (inverse transformation) という言い方をする。恒等写像はまた**恒等変換** (identity transformation) とも呼ばれ、$1_X$ という記号も使うことにする。[ここで、写像と合成の復習をすべきである。]

集合 $X$ の変換で逆変換が存在するようなもの全体の集合を $S(X)$ という記号で表し、$S(X)$ の 2 つの元の積を写像の合成によって定めると、$S(X)$ は群となる。これを $X$ の一般変換群 (general transformation group) と呼ぶことにする。

集合 $X$ が大きさ $n$ の有限集合であるとき（とくに、$X = \{1, 2, \ldots, n\}$ であるとき)、$S(X)$ を記号 $S_n$ で表わして、**n 次の対称群** (the symmetric group of degree $n$) と呼ぶ。

上のような定義は、具体例の経験が充分でないと分かり辛いであろう。そもそも、$g \in G$ とは何なのか、それが対称性の記述とどのように結びつくのか、この抽象的な定義だけから読み取ることは困難である。

しかしながら、群の形式的な性質を明らかにする上では都合のよい面もある。例えば、次のようなことである。

**命題 2.2.** 群 $G$ において、単位元は一意的に定まる。(1 という記号は確定した要素を

表わす。）また、$G$ の元 $g$ に対してその逆元も一意的に定まる。（ $g$ の逆元は $g$ だけで決まるので、$g^{-1}$ という表記法を安心して使える。）

*Proof.* こういった、群の定義にまつわる一般的な性質は、抽象的かつ形式的な（代数的ともいう）証明によるものが多く、教える方も教えられる方も楽しいものではない。最も良い方法と思われるものは、（１）取り合えず何も参照せずに考えてみる、それで証明が分かれば良し、分からなければ、（２）教科書の証明を見て感心・納得する、ことである。 □

**問 10.** $(ab)^{-1} = b^{-1}a^{-1}$ である。

**命題 2.3.** 群の有限個の元の積は、順序を保つ限り積を計算する順番によらない。その結果、$a_1a_2 \dots a_n$ といったものが意味をもつ。例えば、

$$(a_1a_2)(a_3a_4) = (a_1(a_2a_3))a_4.$$

*Proof.* これは通常、括弧の数に関する帰納法を使うものであるが、ここでは証明を省略する。後ほど導入される群作用の応用として示すこともできる。下の問を直接確かめるだけでも実用上困らないであろう。 □

**問 11.** ４つの元 $a, b, c, d$ があるとき、積 $abcd$ の計算方法を指示する括弧のつけ方で異なるものは何種類あるか。また、それぞれの計算結果は相互に等しいことを結合法則から導け。

**問 12.** 実数の集合 $\mathbb{R}$ に二項演算を

$$a * b = a + b + \sqrt{5}$$

で定めると群になる。これを示せ。 この「からくり」を説明できるか。

**問 13** (Optional)**.** $a_1 \dots a_n$ に対する勝手な括弧付の結果が、$(\dots((a_1a_2)a_3)\dots)a_n$ に一致することを $n$ についての帰納法で説明せよ。

**定義 2.4.** 群 $G$ の演算が**交換法則** (commutativity law)

$$ab = ba, \qquad a, b \in G$$

をみたすとき**可換群** (commutative group) であるという。可換群でないものを非可換群 (non-commutative group) という。可換群はまた**アーベル群** (abelian group) とも呼ばれる。

可換群においては、演算の記号として積ではなく和の記号＋を使うことも多く、その場合にはとくに**加法群** (additive group) と呼ばれる。加法群においては、単位元は 0 という記号で代用され、名前も零元 (zero element) と呼ばれる。また逆元の代わりに負元の記号 $-a$ が使われる。

一方で、積の形で可換群を表わす場合に、とくに強調して、**乗法群** (multiplicative group) という場合もある。

| | |
|---|---|
| 加法群 | $Z_n$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ |
| 乗法群 | $C_n$, $\mathbb{T}$, $\mathbb{R}_+$, $\mathbb{C}^\times$ |

ここで、

$$C_n = \{z \in \mathbb{C}; z^n = 1\}, \quad \mathbb{T} = \{z \in \mathbb{C}; |z| = 1\}, \quad \mathbb{C}^\times = \mathbb{C} \setminus \{0\}, \quad \mathbb{R}_+ = \text{正の実数全体}$$

である。

**例 2.5.** ベクトル空間は、和の演算に関して加法群である。

**問 14.** 3 次元ベクトル空間での外積（ベクトル積）は、群の演算といえるかどうか。

**定義 2.6.** 群 $G$ は、有限個の要素からなるとき、**有限群** (finite group)、無限の要素からなるとき、**無限群** (infinite group) という。

| | 可換 | 非可換 |
|---|---|---|
| 有限 | $\mathbb{Z}_n$ | 対称群 |
| 無限 | $\mathbb{Z}$ | 変換群 |

無限群はさらに、離散群 (discrete group) と連続群 (continuous group) に区分けすることができる。連続群は、さらにまた、コンパクト群と非コンパクト群に分けられる。

勉強量とともに既知の群の種類が増えるであろう。何種類の群を空で言えるかで、習得度の目安とできるくらいのものである。

再度、多項式の対称性 $G(f)$ を見る。対称性が最も高い場合が対称式で、すなわち、$G(f) = S_n$ となるのであった。それ以外の場合は、$G(f) \subset S_n$ となる。この包含関係は単に集合のそれにとどまらず、群の演算をも共有している。すなわち、$\sigma, \tau \in G(f)$ ならば、$\sigma^{-1}, \sigma\tau \in G(f)$ であり、$G(f)$ は、$S_n$ における群演算を限定的に使用することにより、それ自身群となっている。

この性質を敷衍（ふえん）すると、次の定義に到達する。

**定義 2.7.** 群 $G$ の部分集合 $H$ が、$G$ における積演算を $H$ に限定することにより、それ自身群となっているとき、$H$ は $G$ の**部分群** (subgroup) であるという。すなわち、$a, b \in H$ に対して、$ab \in H$ であり、この二項演算に関して、
(i) $ah = ha$ $(a \in H)$ となる $H$ の単位元 $h \in H$ が存在し、
(ii) $a \in H$ に対して、$H$ の元 $a'$ で、$aa' = h = a'a$ となるものを見つけることができる。

**例 2.8.** 最も大きい部分群として $G$ 自身、最も小さい部分群として $\{1\}$ であるが、この２つは「自明な部分群」として、これら以外の部分群が興味の対象となる。

**例 2.9.** 可換群における部分群。
(i) $n\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{R}$, (ii) $\mathbb{C}_n \subset \mathbb{T}$, (iii) $\mathbb{R}_+ \subset \mathbb{C}^\times$.

**命題 2.10.** 群 $G$ の部分集合 $H \neq \emptyset$ が部分群であるための必要十分条件は、
(i) $a, b \in H \Longrightarrow ab \in H$, (ii) $a \in H \Longrightarrow a^{-1} \in H$
が成り立つことであり、このとき $h = 1$ かつ、$a \in H$ の $H$ での逆元は $a$ の $G$ における逆元 $a^{-1}$ に一致する。

*Proof.* 各自、試みよ。 □

注意 . 群 $G$ の部分集合 $H$ が部分群であるかどうかは、通常は、この２つの性質を調べるとわかる。でたらめな部分集合を取ってきては、こういった性質は期待できないから、部分群となる部分集合は、極めて限定的なものになっている。とは言っても、群 $G$ の部分群を調べるという作業は、$G$ そのものを調べるにも匹敵する内容を含むので、それだけ難しい場合が多い。

**問 15** (Optional)**.** 上の２つの条件は、

$$a, b \in H \Longrightarrow ab^{-1} \in H$$

と同値である。

**問 16.** 群 $G$ の部分群 $H, K$ に対して、$H \cap K$ も部分群である。$H \cup K$ が部分群とならない例を挙げよ。

一般変換群 $S(X)$ の部分群を $X$ の**変換群** (transformation group) という。

**問 17.** 平面の合同変換（２点間の距離を変えない変換）は、

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto T \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a \\ b \end{pmatrix}, \qquad T \text{ は直交行列}$$

の形である。

**例 2.11.** 平面の中の図形 $K$ の合同変換全体は、変換群である。これを $K$ の合同変換群と呼ぶ。

**例 2.12.** 平面における正 $n$ 角形の合同変換群を $n$ 次の**二面体群** (the dihedral group of degree $n$) とよび、$D_n$ という記号で表わす。

**問 18.** 円 $\{(x,y); x^2+y^2=1\}$ の合同変換の形を決定せよ。

**問 19.** $K=\{(x,y); x\in\mathbb{R}, y\in\mathbb{Z}\}$ の合同変換の形を決定せよ。

変換群の中でも重要なものに行列の作る群がある。複素数を成分とする $n$ 次の正方行列で逆行列をもつもの全体 $GL(n,\mathbb{C})$ は、ベクトル空間 $\mathbb{C}^n$ に対する変換群として群になっている。変換の合成が行列の積に対応していることに注意。同様に実数を成分とする $GL(n,\mathbb{R})$ も定義され、$GL(n,\mathbb{C})$ の部分群になっている。これらは、一般線型群 (general linear group) と呼ばれる。

一般線型群 $GL(n,\mathbb{C})$ の部分群を**行列群** (matrix group) と呼ぶことにしよう。例えば、次のようなものが行列群である。

$$\begin{aligned} SL(n,\mathbb{C}) &= \{g\in GL(n,\mathbb{C}); \det(g)=1\} \quad \text{(special linear group)},\\ U(n) &= \{g\in GL(n,\mathbb{C}); g^*g = gg^* = I\} \quad \text{(unitary group)},\\ O(n) &= \{g\in GL(n,\mathbb{R}); {}^t g\, g = g\, {}^t g = I\} \quad \text{(orthogonal group)}. \end{aligned}$$

またこれらを組み合わせた次のようなものも重要である。

$$SU(n) = U(n)\cap SL(n,\mathbb{C}), \qquad SO(n) = O(n)\cap SL(n,\mathbb{R}).$$

**問 20** (Optional)**.** $SO(n)$ と $O(n)$, $SU(n)$ と $U(n)$ の違いを認識せよ。

**問 21.** $SL(n,\mathbb{Z}) = \{g\in SL(n,\mathbb{C}); g$ の成分は整数 $\}$ は、$SL(n,\mathbb{R})$ の部分群である。

群の多くの実例は、変換群の形で与えられる。実は、どのような群も適当な集合に対する変換群とみなせる、という実にコロンブスの卵的な事実がある。これについては、後ほど、群の作用のところで。

**例 2.13.** 部分群にならない例、部分集合をでたらめに選べば即座に得られるのだが注意すべきものとして、次を挙げておこう。

(i) 自然数全体 $\mathbb{N}=\{0,1,\dots\}\subset\mathbb{Z}$（逆元が存在せず)。

(ii) $\mathbb{C}^\times \subset \mathbb{C}$ （群の演算が異なる）。

(iii) 整数を成分とする行列からなる $GL(n,\mathbb{R})$ の部分集合（逆元が存在せず）。

**問 22.** 剰余群 $\mathbb{Z}_n$ 部分集合

$$\mathbb{Z}_n^\times = \{[k] \in \mathbb{Z}_n; \exists l \in \mathbb{Z}, [kl] = 0$$

は、積を演算として群になる。

# 3 群の相互関係

群を自立した対象として扱うことによって、その相互関係の把握が容易になる。

**定義 3.1.** 群 $G$ から群 $G'$ への写像 $\varphi : G \to G'$ で、

$$\varphi(ab) = \varphi(a)\varphi(b), \quad \forall a, b \in G$$

となるものを**準同型** (homomorphism) という。ここで、$ab$ は $G$ における積を表わしているのに対して、$\varphi(a)\varphi(b)$ は $G'$ における積であることに注意。

準同型で全単射であるものを**同型（写像）** (isomorphism) という。

- $\mathbb{Z} \to \mathbb{Z}_n$, $\mathbb{Z} \to C_n$ という全射準同型。
- $\mathbb{Z}_n \cong C_n$ という同型。$SO(2) \cong \mathbb{T}$ という同型。
- $\mathbb{R} \to \mathbb{T}$ という全射準同型。
- $\mathbb{R} \ni t \mapsto e^{at} \in \mathbb{R}_+$ という同型。
- $\det : GL(\mathbb{C}) \to \mathbb{C}^\times$ という全射準同型。
- $\mathrm{sgn} : S_n \to \{\pm 1\} = C_2$ という全射準同型。
- $\mathbb{C}^\times \ni z \mapsto |z| \in \mathbb{R}_+$ という全射準同型。

**命題 3.2.** 準同型 $\varphi : G \to G'$ に対して、

$$\varphi(1_G) = 1_{G'}, \qquad \varphi(g)^{-1} = \varphi(g^{-1}), \quad g \in G$$

が成り立つ。

**問 23.** $G$, $G'$ が加法群である場合に、準同型の定義式および上の関係式はどのような形になるか。

**問 24.** 準同型 $\varphi : G \to G'$ に対して、

$$\ker \varphi = \{g \in G; \varphi(g) = 1_{G'}\}$$

とおくとき、$\varphi$ が単射であることと $\ker \varphi = \{1_G\}$ であることは同値である。

**命題 3.3.** 準同型 $\varphi : G \to G'$ を考える。

(i) $G$ の部分群 $H$ に対して、その像 $\varphi(H) = \{\varphi(h); h \in H\}$ は $G'$ の部分群である。
(ii) $G'$ の部分群 $H'$ に対して、その逆像 $\varphi^{-1}(H') = \{g \in G; \varphi(g) \in H'\}$ は $G$ の部分群である。
(iii) $\varphi$ が同型写像であるとき、その逆写像 $\varphi^{-1} : G' \to G$ も同型写像である。

**問 25.** 準同型の像・逆像についての事実を確認。

**問 26.** 群 $G$ が可換であれば、その像 $\varphi(G)$ は $G'$ の可換な部分群である。($G'$ そのものは可換であるとは限らない。)

**定義 3.4.** 2 つの群 $G$, $G'$ の間に同型写像が存在するとき、$G$ と $G'$ は**同型である** (isomorphic) といい、$G \cong G'$ という記号で表わす。

この場合、2 つの群は同型写像を通じて同一の群構造をもつものと理解される。もっとも、同型であっても、それを保障する同型写像は、一般に一つだけとは限らないので、その違いが問題になる場合には、注意を要する。これが、同型の記号として $=$ ではなく $\cong$ を用いる一つの理由である。

**問 27.** 群の同型性は同値関係である。[ここで同値関係と類別の復習をする。]

**問 28.** $m \neq n$ であるとき、$S_m$ と $S_n$ は同型にならない。何故か。

**例 3.5.** 二面体群 $D_n$ の元（合同変換）に対して、それが引き起こす頂点の集合 $X$ の置換を $\varphi(g)$ で表わせば、$\varphi : D_n \to S(X)$ は単射準同型となり、$D_n$ は、$S_n$ の部分群と同一視される。

**問 29.** $n = 3$ の場合は、$D_3 \cong S_3$ である。$n = 4$ の場合に、$D_4$ を $S_4$ の部分群として具体的に実現してみよ。

**問 30.** $\sigma \in S_n$ に対して $n$ 次の直交行列 $T(\sigma)$ を、$T(\sigma) : e_i \mapsto e_{\sigma(i)}$ で定めると、$T : S_n \to O(n)$ は単射準同型である。

**問 31** (Optional)**.** 直積集合 $\mathbb{R}^2 \times O(2)$ に、積の演算を

$$(a, A) \cdot (b, B) = (a + Ab, AB)$$

で定めたものは、$\mathbb{R}^2$ の合同変換群と同型である。

**問 32** (Optional)**.** $\mathbb{R}$ から $\mathbb{R}$ への連続な準同型は一次式に限ることを示せ。

**問 33** (Optional)**.** $\mathbb{R}$ から $\mathbb{C}^\times$ への準同型で連続であるものは、指数関数に限ることを示せ。

より一般に、$\mathbb{R}$ から $GL(n, \mathbb{C})$ への連続準同型は、行列の指数関数で表わされることが証明できる。

**問 34.** 2 つの集合 $X, Y$ が対等であれば、$S(X) \cong S(Y)$.

# 4 生成元と巡回群

ここでは巡回群と呼ばれる特殊な部分群について調べる。

**命題 4.1.** 群 $G$ の部分群の集まり $\{H_i\}_{i \in I}$ に対して、その共通部分

$$\bigcap_{i \in I} H_i$$

は再び $G$ の部分群となる。

*Proof.* 証明はきわめて形式的であるので、自ら確認すべきである。 □

上の命題より、群 $G$ の部分集合 $S$ に対して、$S$ を含む最小の部分群が存在する。それを $\langle S \rangle$ という記号で表わし、**S から生成された部分群** (the subgroup generated by $S$) と呼ぶ。また、 $G = \langle S \rangle$ であるとき、$G$ は $S$ によって生成される、という。$\langle S \rangle$ を構成的に記述すれば、次のようになる。

$$\langle S \rangle = \{s_1^{\epsilon_1} s_2^{\epsilon_2} \dots s_k^{\epsilon_k}; s_j \in S, \epsilon_j \in \{\pm 1\}\}.$$

**例 4.2.** 二面体群を構成する際の正 $n$ 角形を複素平面の上で考える。また座標を適当に選択して、正 $n$ 角形の中心が原点であり、正 $n$ 角形の頂点が $1 \in \mathbb{C}$ の $n$ 乗根全体 $\{z \in \mathbb{C}; z^n = 1\}$ に一致すると仮定して一般性を失わない。

このとき、二面体群に属する合同変換は、原点を動かさないので、原点の回りの回転であるかまたは原点を通る直線に関する折り返しでなければならない。さらに頂点が頂点に移されるという点を考慮に入れると、回転の角度は $2\pi/n$ の倍数、折り返しの対称軸の実軸と成す角度は、$\pi/n$ の倍数であるとわかる。折り返しの方は、対称軸の角度が $\pi$ だけ違うものは同一の合同変換となっているので、異なるものは $2n$ の半分の $n$ 個だけある。全体として、$|D_n| = 2n$ である。

さて、角度 $2\pi/n$ の回転を $r$ で、実軸に関する折り返しを $s$ という記号で表わすことにすれば、簡単な計算で、$r^k s$ は実軸を正の方向に角度 $\pi k/n$ だけ回転させた直線に関する折り返しを表わしているとわかる。さらに、また

$$srs = r^{-1}, r^n = 1, s^2 = 1$$

もわかるので、$D_n = \langle r, s\rangle$ であり、

$$D_n = \{r^k, r^k s; 0 \le k < n\}$$

となる。

**問 35** (Optional)**.** 隣り合った 2 つの折り返し $s, rs$ によっても生成される。

次に、一つの元 $a \in G$ から生成された部分群 $\langle a\rangle$ の構造について調べてみよう。これを $a$ から生成された**巡回群** (cyclic group) と称する。まずは、記法の準備から。

群 $G$ の演算が積の形で与えられているとして、$a$ の整数冪（べき）を

$$a^n = \begin{cases} a \dots a \ (n \text{ 個の積}) & \text{if } n \ge 1, \\ 1 \quad (G \text{ の単位元}) & \text{if } n = 0, \\ a^{-1} \dots a^{-1} \ (|n| \text{ 個の積}) & \text{if } n \le -1 \end{cases}$$

で定める。先の構成的表示から、$\langle a\rangle = \{a^k; k \in \mathbb{Z}\}$ である。

**命題 4.3.** 指数法則

$$(a^m)^n = a^{mn}, \qquad a^m a^n = a^{m+n}, \qquad m, n \in \mathbb{Z}$$

が成り立つ。

**問 36.** 上の指数法則を確かめよ。

さて、巡回群 $\langle a\rangle$ の構造を調べる作業に戻ろう。二つの場合に分ける：

**場合 1** どのような自然数 $m \ge 1$ に対しても、$a^m \ne 1$ である場合。

この場合には、$\{a^k\}_{k\in\mathbb{Z}}$ が全て異なる元であることが分かる。実際、$a^k = a^l$ とすると、指数法則により $a^{k-l} = 1$ であるが、これは、$a^{|k-l|} = 1$ を意味するので、場合分けの条件から $k - l \neq 0$ では成立しない。すなわち、$k \neq l$ ならば $a^k \neq a^l$ である。

このことと指数法則から、写像 $\mathbb{Z} \ni k \mapsto a^k \in G$ は単射準同型を定め、したがって、その像である $\langle a\rangle$ と $\mathbb{Z}$ とは同型であることがわかる。

**場合２** ある自然数 $m \geq 1$ で $a^m = 1$ となるものがある。

まず、$a^m = 1$ となる自然数 $m \geq 1$ で最小のものを $n$ で表わす。（なぜ、そのような $n$ が存在するか。）そうすると、$1, a, a^2, \ldots, a^{n-1}$ は全て異なる元である。実際、$a^k = a^l$ $(0 \leq k < l < n)$ であったとすると、再び指数法則を使って、$a^{l-k} = 1$ であるので、$1 \leq l - k < n$ に注意すれば、$n$ の最小性に反するからである。この場合には、$a$ を $n$ 乗あるいは $-n$ 乗するたびに単位元 1 に戻るので、写像

$$\mathbb{Z}_n \ni [k] \mapsto a^k \in \langle a\rangle$$

により、$\mathbb{Z}_n$ と $G$ の部分群 $\langle a\rangle$ とは同型であることがわかる。とくに、部分群 $\langle a\rangle$ の元の個数は $n$ である。

**定義 4.4.** 群 $G$ の元 $a$ に対して、$a^m = 1$ となる最小の自然数 $m \geq 1$ を $a$ の**位数** (order) と呼ぶ。$a^m = 1$ となる自然数 $m \geq 1$ が存在しない場合には、$a$ の位数は $\infty$ であると定める。

上の用語を使えば、巡回群 $\langle a\rangle$ の要素の個数 $|\langle a\rangle|$ は $a$ の位数に一致する、とまとめることができる。

**問 37.** 位数 $m$ の元 $a$ と位数 $n$ の元 $b$ が、$ab = ba$ をみたし、$m$ と $n$ が互いに素であるならば、$ab$ の位数は、$mn$ で与えられる。互いに素という条件がない場合はどうか。

**問 38.** 行列

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

の位数について調べよ。

**問 39.** 巡回群 $\mathbb{Z}_n$ において、$[k] \in \mathbb{Z}_n$ $(1 \leq k < n)$ が $\mathbb{Z}_n$ の生成元であるための条件は、$k$ と $n$ が互いに素であることである。

**問 40.** 乗法群 $\mathbb{Z}_n^\times$ $(3 \leq 7)$ の中で巡回群であるものはどれか。

本来、巡回群と呼ぶべきは位数が有限の場合のみであるが、無限位数の場合にも、その

ように呼び習わす習慣ができてしまったようである。(数学者もいい加減なものである。)正しくは、単生成 (singly generated) とでも呼べば良かったのであるが。

さらに言葉は乱れて(?)、$\mathbb{Z}$ と同型な群を無限巡回群、$\mathbb{Z}_n$ と同型な群を有限巡回群と呼ぶこともある。

さて、気を取り直して、$G = \mathbb{Z}$ の場合には、$\langle n \rangle$ は、$n$ の倍数全体の作る部分群に一致するので、

$$\langle n \rangle = n\mathbb{Z} = \{0, \pm n, \pm 2n, \dots\}$$

という記法がよく用いられる。

**命題 4.5.** 加法群 $\mathbb{Z}$ の部分群は、すべて $n\mathbb{Z}$ の形である。さらに、$m\mathbb{Z} \subset n\mathbb{Z}$ となるための必要十分条件は、$m$ が $n$ の倍数であることである。

*Proof.* 部分群 $H$ に対して、$\{k \in H; k > 0\}$ の最小値を $n$ とすると、割り算により、すべての $k \in H$ は $n$ で割り切れる。 □

**系 4.6.** 巡回群の部分群はすべて巡回群である。

*Proof.* 全射準同型 $\mathbb{Z} \to G$ の逆像を考える。 □

**問 41.** $m$, $n$ を自然数とする。$\mathbb{Z}$ の部分群 $m\mathbb{Z}$, $n\mathbb{Z}$ の共通部分を求めよ。

**問 42** (Optional)**.** $\mathbb{T} \cong SO(2)$ の有限部分群は全て $C_n$ の形。$O(2)$ の有限部分群は、$C_n$ または $D_n$ と同型。

最後に、巡回群にまつわる定理を一つ。その前に、言葉の準備を。

**定義 4.7.** 二つの群 $G$, $G'$ があったときにその直積集合 $G \times G'$ は、二項演算 $(a, a')(b, b') = (ab, a'b')$ により群となる。これを $G$ と $G'$ の**直積群** (the direct product of $G$ and $G'$) と呼ぶ。

$G$, $G'$ ともに可換であれば、$G \times G'$ も可換であることに注意。また、加法群の直積は**直和** (direct sum) とも呼ばれ、$G \oplus G'$ という記号でも表わされる。3 個以上の群の直積についても同様である。

**例 4.8.** 長方形の合同変換群は直積群 $\mathbb{Z}_2 \times \mathbb{Z}_2$ と同型である。これは、エチレン $C_2H_4$ の対称性でもある。

**問 43.** $\mathbb{Z}_4$ と $\mathbb{Z}_2 \times \mathbb{Z}_2$ は同型ではない。何故か。

**問 44.** 直積群 $\mathbb{Z}_m \times \mathbb{Z}_n$ が巡回群であるための必要十分条件は、$m$ と $n$ が互いに素であること。とくにこのとき、$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ である。

参考までに、次の定理を挙げておく。証明については、付録参照。

**定理 4.9** (アーベル群の基本定理)**.** 有限集合から生成されたアーベル群は、巡回群の直積と同型である。すなわち、$G \cong \mathbb{Z}^n \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_l}$.

# 5 群作用と軌道空間

変換群の概念を融通無碍（ゆうずうむげ）にしたものに、群作用という考えがあり、群により対称性を統制する上できわめて有用なものである。

多くの群は変換群として実現される。これは言い換えると、群 $G$ から $S(X)$ への単射準同型を与えるといっても同じことである。

一般に、群 $G$ の集合 $X$ における**表現** (representation) とは、準同型写像 $\pi : G \to S(X)$ のことをいう。$X$ がベクトル空間で $\pi(g) : X \to X$ が線型写像である場合を線型表現 (linear representation) という。

さて、表現 $\pi : G \to S(X)$ が与えられた場合に、その情報を次のように代数的演算の形に書き直してみよう。写像 $\lambda : G \times X \to X$ を $\lambda(g, x) = \pi(g)(x)$ で定めると、

$$\lambda(a, \lambda(b, x)) = \lambda(ab, x)$$

$$\lambda(1, x) = x$$

をみたす。

**定義 5.1.** 一般に、群 $G$ と集合 $X$ に対して、写像 $\lambda : G \times X \to X$ で上の 2 つの条件をみたすものが与えられた情況を、群 $G$ が集合 $X$ に**作用する**という。あるいは、$G$ の $X$ への**群作用** (group action) が $\lambda$ によって与えられる、といった言い方をする。

$G \times X$ の要素 $(g, x)$ の群作用による像 $\lambda(g, x)$ は、しばしば、$gx$ のように積の記法で表示される。その略記法に従えば、上の 2 つの条件は、それぞれ、
(i) $a(bx) = (ab)x$ （あたかも結合法則の如し）、
(ii) $1x = x$ （あたかも左単位元の如し）
となり、非常に見やすい。また、作用を受ける集合の要素は、幾何学的意味をもつ場合も多く、しばしば**点** (point) と呼ばれる。

逆に、群作用 $\lambda : G\times X \to X$ が与えられたとき、各 $g \in G$ に対して、写像 $\pi(g) : X \to X$ を $\pi(g) : x \mapsto \lambda(g, x)$ で定めると、結合法則もどきから、$\pi(a) \circ \pi(b) = \pi(ab)$ が得られ、単位元もどきから、$\pi(1) = 1_X$ が得られるので、とくに $\pi(g) \in S(X)$ がわかり、群の準同型写像 $\pi : G \to S(X)$ が復元する。

**問 45.** 群作用から作った $\pi(g) : X \to X$ が全単射であることを確かめよ。

以上により、次がわかった。

**命題 5.2.** 群 $G$ の $X$ への作用を与えることと、群の表現 $G \to S(X)$ を与えることは、同等な内容をもつ。

**問 46.** 写像 $f : X \to Y$, $g : Y \to X$ が $g \circ f = 1_X$ を満たせば、$f$ は単射であり $g$ は全射である。

**問 47.** 上の群作用は、より正確には、左作用と呼ばれるものである。上の議論に倣って、写像 $\rho : X \times G \to X$ の形で右作用の定式化を試みよ。

さらには、両側からの同時作用（双作用という）についても考察してみよ。

群作用の方は、一種の積と思うことにより、準同型の積保存の性質が結合律の形で表現され、代数的計算と調和させることが容易となる。

**例 5.3.** 群 $G$ に対して、$X = G$ と思うことにより、$G$ の $X$ に対する左作用および右作用を

$$G \times X \ni (g, x) \mapsto gx \in X,$$
$$X \times G \ni (x, g) \mapsto xg \in X$$

で定めることができる。これらを $G$ の**正則作用** (regular action) と呼ぶ。

**例 5.4.** 群 $G$ の集合 $X$ への作用が与えられたとする。別に集合 $Y$ を用意して、集合 $X$ から集合 $Y$ への写像全体を $Y^X$ で表わせば、$G$ の $Y^X$ への作用を

$$(gf)(x) = f(g^{-1}x), \qquad g \in G, x \in X$$

で定めることができる。

**問 48.** $S_m$ の写像空間 $Y^{\{1,\dots,m\}}$ への作用を具体的に表示してみよ。

**問 49.** 有限群 $G$ の要素を $\{g_1, g_2, \dots, g_n\}$ と並べておく。このとき、任意の $g \in G$ に対して、$\{gg_1, gg_2, \dots, gg_n\}$ は、もとの $g_1, \dots, g_n$ の並べ替えになっている。これを示せ。

**例 5.5.** $n$ 文字 $x_1, \ldots, x_n$（不定元、indeterminate、という）の多項式 $f(x_1, \ldots, x_n)$ への置換 $\sigma \in S_n$ の左作用を

$$(\sigma f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

によって定める。これが実際、左作用になることは、

$$(\tau(\sigma f))(x_1, \ldots, x_n) = (\sigma f)(x_{\tau(1)}, \ldots, x_{\tau(n)}) = f(x_{\sigma\tau(1)}, \ldots, x_{\sigma\tau(n)}) = ((\tau\sigma)f)(x_1, \ldots, x_n)$$

よりわかる。

- 行列群のベクトル空間への作用。
- 回転群の関数空間への作用。
- $\mathbb{Z}$ の $\mathbb{R}$ への移動作用と、関数空間への作用、周期関数。

こんなもので良いだろう。

**問 50** (Optional)**.** 集合 $X$ に対して、$X$ から二点集合 $\{0, 1\}$ への写像全体と、$X$ の部分集合全体 $2^X$ （$X$ のべき集合という）とは一対一に対応することを復習し、例 5.4 で与えた作用を $G$ の $2^X$ への作用として解釈し直せ。

与えられた作用に対して、$Gx = \{gx \in X; g \in G\}$ の形の部分集合を、(群 $G$ の作用による) $x$ を通る**軌道** (orbit) とよぶ。

有限群の場合には、$G$ の要素を $g_1, \ldots, g_n$ $(n = |G|)$ と列挙することにより、

$$Gx = \{g_1x, g_2x, \ldots, g_nx\}$$

という表示を得る。もちろん、$g_1x, \ldots, g_nx$ が全て異なる点である保障はなく、一般には同じ点が複数含まれることになる。

**例 5.6.** 回転群 $SO(2)$ のユークリッド平面 $\mathbb{R}^2$ への自然な作用に関する軌道は、原点を中心とする同心円である。この例が、「軌道」という用語の由来と思ってよい。正確には、時間変数 $\mathbb{R}$ の作用による軌道というべきであろうが。

**問 51.** 対称群 $S_n$ の集合 $\{1, 2, \ldots, n\}$ への自然な作用を考えるとき、その軌道について調べよ。

**問 52.** 対称群 $S_n$ の べき集合 $2^X$ $(X = \{1, 2, \ldots, n\})$ への自然な作用を定義し、その軌道について調べよ。

軌道の構造を調べる上で重要なのが、**固定部分群** (stabilizer) という $G$ の特殊な部分群である。これは、$X$ の点 $x$ ごとに、

$$G(x) = \{g \in G; gx = x\}$$

で定義される。

注意 . 固定部分群を表わす記号として、$G_x$ を採用しているものも多いが、これだと、手書きの場合 $Gx$ と混乱する恐れがあるので、ここでは使わない。

**例 5.7.** $G = S_n$, $X$ は $n$ 変数の多項式環とし、上で例示した作用に関する固定部分群が Lagrange の扱った場合である。

**問 53.** $G(x)$ が実際に $G$ の部分群であることを確認。

**問 54.** 対称群 $S_4$ の 4 変数の多項式への作用で、

$$G(x_1x_3 + x_2x_4) \cong D_4$$

であることを示せ。

**問 55.** 作用 $G \times X \to X$ に対応する表現を $\pi : G \to S(X)$ で表わすとき、

$$\ker \pi = \{g \in G; \pi(g) = 1_X\} = \bigcap_{x \in X} G(x).$$

ここで、$\ker \pi = \{g \in G; \pi(g) = 1_X\}$ である。

**問 56.** $SO(3)$ の $\mathbb{R}^3$ への自然な作用で、$(0, 0, 1) \in \mathbb{R}^3$ における固定部分群は、 $z$ 軸のまわりの回転全体である。

**問 57** (optional)**.** 実数直線 $\mathbb{R}$ 上の連続関数全体の作る集合 $C$ への加法群 $\mathbb{R}$ の作用を $\lambda(t, f)(x) = f(x - t)$ で定める。このとき, $G(f)$ は、次のいずれかであることを示せ。

$$\mathbb{R}, \qquad \mathbb{R}T \ (T > 0), \qquad \{0\}.$$

**定義 5.8.** 軌道を要素とする集合を**軌道空間** (orbit space) と呼び、記号 $G\backslash X$ で表わす。右作用の場合は、$X/G$ と書く。 すなわち、

$$G\backslash X = \{Gx; x \in X\} \subset 2^X.$$

ここで、2 つの軌道 $Gx$, $Gy$ が等しいとは $X$ の部分集合として等しいことであることに注意する。

**補題 5.9.** 二つの軌道 $Gx, Gy$ に対して、

$$Gx \cap Gy \neq \emptyset \quad \Longrightarrow \quad Gx = Gy.$$

いいかえると、二つの軌道は完全に一致するか、共通部分をもたないかのいずれかである。

*Proof.* 仮に $z \in Gx \cap Gy$ であったとすると、$z = ax = by$ である。これから、$gx = ga^{-1}by \in Gy$ となって、$Gx \subset Gy$ が従う。同様に、$Gy \subset Gx$ も導けるので、$Gx = Gy$. □

**定理 5.10** (軌道分解定理)**.** 作用を受ける集合 $X$ は軌道の分割和で表わされる。

$$X = \bigsqcup_{Gx \in G\backslash X} Gx = \bigsqcup_{O \in G\backslash X} O.$$

**例 5.11.** 置換 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{pmatrix}$ から生成された巡回群 $C = \langle \sigma \rangle$ の作用による軌道分解は、

$$X = \{1, 4, 5\} \sqcup \{3\} \sqcup \{2, 6\}$$

となる。

各軌道ごとに添え字集合 $I$ の元によるラベルをつけて、$\{O_i\}_{i \in I}$ を軌道の過不足のない全体であるとすれば、上の定理は、集合 $X$ が $O_i$ に分割されることを意味する。別の言い方をすると、$X$ の点の間の関係を $x \sim y \iff Gx = Gy$ で定めると、これが同値関係になっていて、各軌道が同値類に対応し、この同値関係による商集合が軌道空間に他ならない、ということである。一方、軌道を指定するのに、軌道 $O_i$ ごとに、$O_i = Gx_i$ となる $x_i \in X$ を選んで指定することもできて、このようにして選出された要素の集まり $\{x_i\}_{i \in I}$ を軌道の**代表系** (representative set) と呼ぶ。$X$ が位相空間で、群 $G$ の作用が同相写像によって与えられる場合には、代表系として $X$ 内の幾何学的図形を選ぶことが多く、その場合には、代表系という代わりに基本領域 (fundamental domain) と称される。

**例 5.12.** $X = \mathbb{R}^2$ 内の独立なベクトル $\{a, b\}$ から生成された部分群 $G = \mathbb{Z}a + \mathbb{Z}b$ による移動作用を考えると、その基本領域として、平行四辺形

$$\{sa + tb; 0 \leq s, t < 1\}$$

を取ることができる。

上の例で、平行四辺形の境界まで含めると、代表系にはならないのであるが、重複する部分は境界に限られるので、平行四辺形の境界を重複する部分を「貼り合わせ」て作られる幾何学的図形（円環面＝ドーナッツの表面）と軌道空間を同一視することができる。こういったとらえ方は、図形の対称性を調べる上で、きわめて重要である。

**問 58.** $O(n)$ の $\mathbb{R}^n$ への自然な作用による軌道は、球面

$$\{(x_1, \ldots, x_n); (x_1)^2 + \cdots + (x_n)^2 = r^2\}$$

であり、軌道の代表系として $\{(0, \ldots, 0, r); r \geq 0\}$ を取ることができる。

**問 59.** $\sigma \in S_5$ から生成された巡回群 $\langle\sigma\rangle$ の $\{1, 2, 3, 4, 5\}$ への作用による軌道が丁度 2 つになるような $\sigma$ の個数を求めよ。

作用 $G \times X \to X$ に対して、$gx = x$ for all $g \in G$ すなわち $G(x) = G$ となる $x \in X$ を**不動点** あるいは**固定点** (fixed point) とよぶ。

**例 5.13.** 作用 $O(n) \times \mathbb{R}^n \to \mathbb{R}^n$ の不動点は原点のみ。作用 $O(n) \times S^{n-1} \to S^{n-1}$ は不動点をもたない。ここで、$S^{n-1} = \{(x_1, \ldots, x_n) \in \mathbb{R}^n; (x_1)^2 + \cdots + (x_n)^2 = 1\}$ は、$n-1$ 次元単位球面を表わす。

不動点と対極の性質として、

$$G(x) = \{1\}$$

となる点 $x$ を自由点 (free point) とよぶことにする。すべての点が自由点であるような作用を**自由作用** (free action) とよぶ。

**例 5.14.** 群 $G$ とその部分群 $H$ に対して、$G$ の左正則作用を $H$ に制限して得られる $H$ の $G$ への作用は、自由作用である。右正則作用の $H$ への制限についても同様である。

**問 60.** $S_n$ の $\{1, \ldots, n\}$ $(n \geq 2)$ への自然な作用は、不動点も自由点ももたない。

**問 61.** $S_m$ の写像空間（＝列空間）$X^{\{1,\ldots,m\}}$ への自然な作用を考えるとき、$f : \{1, \ldots, m\} \to X$ が自由点であるための条件を写像 $f$ の性質として述べよ。

次の補題は後ほど、軌道構造定理として一般化される。

**補題 5.15.** 自由点 $x \in X$ に対して、写像 $G \ni g \mapsto gx \in Gx$ は、$G$ から軌道 $Gx$ の上への全単射を与える。とくに、$G$ が有限群である場合には、軌道 $Gx$ に含まれる点の個数は、$|G|$ に一致する。

**定義 5.16.** 群 $G$ の部分群 $H$ に対して、$H$ の左作用に関する軌道を $H$ の**左剰余類** (left coset)、軌道空間を**左剰余類空間** (left coset space) という。同様に、$H$ の右作用による軌道を**右剰余類** (right coset) 、その軌道空間を**右剰余類空間** (right coset space) と呼ぶ。

左剰余類とは、

$$Hg = \{hg; h \in H\}$$

の形の部分集合のことであり、右剰余類についても同様の表示が可能である。

注意 . 可換群では、左右の剰余類が一致する ($aH = Ha$) ので、単に剰余類と呼ばれる。

**例 5.17.** 群 $\mathbb{Z}$ の部分群 $n\mathbb{Z}$ の剰余類群は、$\mathbb{Z}_n$ の他ならない。

**問 62.** $a, b \in G$ に対して、$aH = bH \iff a^{-1}b \in H$、を示せ。

**問 63** (Optional)**.** 二面体群 $D_n$ の部分群 $\langle s \rangle$ に関する左右の剰余類を求めよ。

**問 64.** $G = S_n$, $H = \langle (1, 2, \ldots, n) \rangle$ とおくとき、$G/H$ と $H\backslash G$ を記述し、それぞれの代表系を 1 つ与えよ。

注意 . 剰余類については、左右の呼び方が逆になっている本も多い。式を見れば即座にわかるので、こういうことに拘らないのが、数学者の流儀でもある。

極端な話、論理的に整合性が取れていれば、どのような用語を使っても構わない、というのがその立場であり、D. Hilbert が椅子とテーブルとカップ（だったかな）からユークリッド幾何を組み立てても一向に構わないと宣言したこと、微分幾何とは notation の違いで不変な量を研究する数学である、などというジョークが出現する背景がこの辺にあるのかも知れない。

用語から記号の使い方まで全て統一しないと気がすまない（というかそうしないと効率が悪いのですね）多くの業界との違いが際立って面白くもあるが。

**命題 5.18.** $G$ の $G/H$ への左作用を

$$G \times G/H \ni (g, aH) \mapsto gaH \in G/H$$

で定めることができる。

一般に、群 $G$ の部分集合 $S$ および $a, b \in G$ に対して、$G$ の部分集合を

$$aS = \{as; s \in S\}, \quad Sb = \{sb; s \in S\}, \quad S^{-1} = \{s^{-1}; s \in S\}$$

で定めると、

$$a(bS) = (ab)S, \quad (Sa)b = S(ab), \quad (aS)b = a(Sb),$$
$$(aS)^{-1} = S^{-1}a^{-1}, \quad (Sb)^{-1} = b^{-1}S^{-1}$$

が成り立つ。

**問 65.** 群の部分集合への作用に関する上の性質を確かめよ。

とくに、$G$ が有限群であるときには、上の補題から、$|gH| = |H|$ となるので、軌道分解定理

$$G = \bigsqcup_{i=1}^{m} g_i H, \qquad m = |G/H|$$

より、$|G| = |G/H|\,|H|$ がわかる。

**定理 5.19** (Lagrange)**.** 有限群 $G$ の部分群 $H$ に対してそれぞれの要素の個数を $|G|, |H|$ で表わせば、$|H|$ は $|G|$ の約数でなければならない。

**系 5.20.** 有限群 $G$ の元 $a$ に対して、その位数は、$|G|$ の約数である。ほぼ同じ言い換えとして、$a^{|G|} = 1$ が成り立つ。

**問 66.** 有限群 $G$ の大きさ $|G|$ が素数であれば、$G$ は巡回群に同型である。

注意 . 上の Lagrange の定理は、部分群の可能性を考えるうえで大きな制約となるのだが、逆は成り立たない。実際、$A_4$ の大きさは 12 であるが、$A_4$ の中に大きさ 6 の部分群は存在しない。同様のことは、5次以上の交代群でも成り立つ。

**定理 5.21** (軌道構造定理)**.** 群 $G$ が集合 $X$ に作用しているとき、$X$ の点 $x$ を通る軌道 $Gx$ に対して、対応

$$G/G(x) \ni gG(x) \mapsto gx \in Gx$$

は、剰余類空間 $G/G(x)$ から軌道 $Gx$ の上への全単射を与える。すなわち、$G$ の固定部分群 $G(x)$ に関する右剰余類と軌道 $Gx$ 内の点とは一対一に対応する。

**系 5.22** (軌道長公式)**.** 有限群の作用においては、軌道 $Gx$ 内の点の個数 $|Gx|$ は、

$$|Gx| = \frac{|G|}{|G(x)|}$$

で与えられる。

注意 . 上の公式は、軌道の大きさと固定部分群の大きさとの間の相反法則と解釈される。

対称群が多項式へ作用する場合の軌道構造定理が、Lagrange 対応に他ならない。

**例 5.23.** 多項式 $f(x_1, x_2, x_3) = x_1x_2^2 + x_2x_3^2 + x_3x_1^2$ に対して、

$$G(f) = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

であるから、その剰余類は

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} G(f), \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} G(f)$$

で与えられる。

一方、$Gf$ の方は、

$$f = x_1x_2^2 + x_2x_3^2 + x_3x_1^2, \quad (12)f = x_1^2x_2 + x_2^2x_3 + x_3^2x_1$$

を構成要素とするので、対応

$$G(f) \mapsto f, \qquad (12)G(f) \mapsto (12)f$$

が求める同型である。

**問 67.** $f(x_1, x_2, x_3) = x_1$ に対して、Lagrange 対応を具体的に与えよ。

**問 68** (optional)**.** (i) $f(x_1, x_2, x_3) = (x_1 + \omega x_2 + \omega^2 x_3)^3$ の軌道に含まれる元を根とする代数方程式を考え、3 次方程式の解の公式を導け。

(ii) $g(x_1, x_2, x_3, x_4) = (x_1 + x_2 - x_3 - x_4)^2$ の軌道に含まれる元を根とする代数方程式を考え、4 次方程式の解が 3 次方程式と 2 次方程式を解くことに帰着されることを示せ。

**問 69.** 有限群 $G = \{g_1, g_2, \ldots, g_n\}$ $(n = |G|)$ が集合 $X$ に作用しているとき、$x \in X$ に対して

$$g_1x, g_2x, \ldots, g_nx$$

の中には、同じ要素が $|G(x)|$ 個ずつ含まれることを確認。

**問 70** (Cauchy)**.** 有限群 $G$ の大きさ $|G|$ が素数 $p$ で割り切れるならば、$G$ は位数 $p$ の元を含む。

$\mathbb{Z}_p$ の集合 $X = \{(g_1, \ldots, g_p) \in G^n; g_1 \ldots g_p = 1\}$ への巡回作用を考え、軌道の大きさを調べる。

**問 71** (Sylow)**.** 有限群 $G$ の大きさ $|G|$ が素数 $p$ の冪（べき） $p^m$ で割り切れ、$p^m$ と $|G|/p^m$ が互いに素であれば、$G$ は大きさが $p^m$ の部分群 (Sylow 部分群という) を含む。

$G$ の大きさ $p^m$ の部分集合（部分群ではない！）全体 $X$ に $G$ を左掛算で作用させて、(i) $X$ の大きさが $p$ の倍数にならないこと、(ii) 大きさが $p$ で割り切れない軌道の存在すること、(iii) その軌道内の点の固定部分群の大きさについて調べる。

Sylow 部分群については、存在の他に、共役作用の下での一意性を示すこともできる。(共役作用については、次節を見よ。)

**問 72.** $S_n$ の任意の部分群 $G$ に対して、多項式 $f \in \mathbb{Z}[x_1, \ldots, x_n]$ で、$G = G(f)$ となるものが存在することを示せ。

# 6 共役類と正規部分群

群 $G$ の $G$ 自身への（左）作用を

$$\mu(g, g') = gg'g^{-1} = g.g'$$

で定めることができる。これを**共役作用** (adjoint action) と呼ぶ。共役作用の軌道を**共役類** (conjugacy class) という。$a \in G$ を含む共役類を $C(a)$ という記号で表わせば、

$$C(a) = \{gag^{-1}; g \in G\}$$

である。

注意 . $G(x)$ は部分群であるが、$C(a)$ は、$a = 1$ でない限り、部分群ではない。

**例 6.1.** 行列群 $GL(n, \mathbb{C})$ における共役類は、行列の固有値の情報でほぼ決定される。対角化不可能である例外については、Jordan 標準形に訴える必要はあるが。

例えば、$GL(2, \mathbb{C})$ においては、すべての元は、次のいずれかの形の行列と共役である。

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}, \qquad \begin{pmatrix} \nu & 1 \\ 0 & \nu \end{pmatrix}.$$

**問 73** (Optional)**.** 二面体群 $D_n$ の共役類について調べよ。

共役作用は、$G$ の部分集合全体にまで拡張することができる。すなわち、$S \subset G$ に対して、

$$g.S = gSg^{-1}.$$

$S$ が部分群であるとき、$gSg^{-1}$ は再び部分群になるので、共役作用は、部分群全体に制限することができる。二つの部分群 $H, K$ が共役作用の元で、同一の軌道に属するとき、$H$ と $K$ は**共役である** (conjugate) という言い方をする。すなわち、 $H = gKg^{-1}$ となる $g \in G$ が存在するとき、$H$ と $K$ とは共役である。

**例 6.2.** 群 $G$ が集合 $X$ に作用しているとき、もし $x$ と $y \in X$ が同一の軌道にあれば、$G(x)$ と $G(y)$ は共役な部分群である。実際、$G(gx) = gG(x)g^{-1}$ である。

共役作用の下で、不動点になっている部分群のことを、**不変部分群** (invariant subgroup) と称する。すなわち、$\forall g \in G, gHg^{-1} = H$ となる部分群のことである。この条件は、$\forall g \in G,\ gH = Hg$ (正規性) と同値であるので、不変部分群というかわりに**正規部分群** (normal subgroup) と呼ばれることが多い。

つぎは、定義から明らかであろうが、不変部分群を調べる上で重宝する事実である。

**命題 6.3.** 不変部分群は、その中に含まれる共役類の分割和になっている。

**問 74.** 部分群に対する性質として、不変性と正規性が同値であることを示せ。

**問 75.** 大きさが偶数の有限群 $G$ の中に、大きさが $|G|/2$ の部分群が存在すれば、それは正規部分群である。

正規部分群というのは、部分群よりもさらに限定的であるが、可換群の場合には一致する。

**例 6.4.** 3 次の対称群 $S_3$ で、

$$N = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

は正規部分群であるが、

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

は不変でない部分群である。

**例 6.5.** 準同型 $\varphi : G \to G'$ に対して、$\varphi^{-1}(1)$ は、$G$ の不変部分群である。これを $\ker \varphi$ と書いて $\varphi$ の**核** (kernel) と呼ぶ。

より一般に、$G'$ の不変部分群 $H'$ に対してその逆像 $\varphi^{-1}(H')$ は $G$ の不変部分群である。

**問 76** (Optional)**.** $H$ が $G$ の不変部分群であっても、その像 $\varphi(H)$ は不変とは限らない。

**問 77** (Optional)**.**

(i) $gHg^{-1} \subset H$ がすべての $g \in H$ で成り立ては、$H$ は正規部分群。
(ii) $H, K$ を正規部分群とすれば、$H \cap K$ も正規部分群。

**問 78** (Optional)**.** 可換群では、すべての部分群は正規部分群であるが、この逆が成り立つかどうか調べよ。（ヒント：４元数群。）

正規部分群 $N$ に対しては、$gN = Ng$ となるので、$g$ の左剰余類と右剰余類は完全に一致する。この意味で、$N\backslash G = G/N$ となる。さらに、$G/N$ における積を

$$(aN)(bN) = (ab)N$$

で定義することができて、$G/N$ は再び群になる。これを $G$ を $N$ で割った **商群** (quotient group) とよぶ。

**問 79.** 上の定義が剰余類の代表元の取り方に依らずに、**うまくいっている** (well-defined) ことを確かめよ。

上の商群の積の定義の仕方から、

$$G \ni g \mapsto gN \in G/N$$

は $G$ から $G/N$ への準同型になっていることがわかる。これを標準的な準同型 (canonical homomorphism) と呼ぶ。

**例 6.6.** $G = \mathbb{Z}$, $N = \mathbb{Z}n$ と取ると、$G/N$ は剰余類群 $\mathbb{Z}_n$ に他ならない。
$G = V$ をベクトル空間、$N = W$ を部分空間とすると、$G/N$ は、商ベクトル空間 $V/W$ の定める加法群と同一視できる。

**定理 6.7** (準同型定理)**.** 与えられた準同型写像 $\varphi : G \to G'$ に対して、$N = \ker\varphi$ とおくと、

$$G/N \ni gN \mapsto \varphi(g) \in \varphi(G)$$

は商群 $G/N$ から $\varphi(G)$ への同型写像を与える。

上の定理で、とくに準同型が全射であるときには、$G'$ は $G$ の商群とみることができる。

**例 6.8.** 同型 $\mathbb{C}^\times/\mathbb{R}_+ \cong \mathbb{T}$ とこれと極表示との関係。さらにまた、円柱・円周との関係。

**問 80.** 同型 $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$ を示せ。

**問 81.** 同型 $O(n)/SO(n) \cong \mathbb{Z}_2$ を示せ。

**問 82** (Optional)**.** 群 $G$ の部分群 $H$ および正規部分群 $N$ に対して、

$$HN = \{hn; h \in H, n \in N\}$$

は $G$ の部分群であること、$H \cap N$ は $H$ の正規部分群であることを確認し、さらに同型 $HN/N \cong H/H \cap N$ を示せ。

**問 83** (Optional)**.** 正規部分群 $N$ が $|G/N| = 2$ であるとき、$G$ の部分群 $H$ に対して、

$$H/(H \cap N) \cong \begin{cases} \mathbb{Z}_2 & \text{if } H \not\subset N, \\ \{1\} & \text{if } H \subset N. \end{cases}$$

これを、$G = S_n$, $N = A_n$ に適用することで、$S_n$ における $\sigma \in A_n$ の共役類 $C(\sigma)$ は、(i) $A_n$ の中でも一つの共役類であるか、(ii) $A_n$ の共役類として同じ大きさの 2 つの部分に分かれるかのいずれかであることを示せ。

**問 84** (Challenging)**.** 同型 $SU(2)/\{\pm 1\} \cong SO(3)$ を示せ。

# 7 対称群の共役類

この節では、$n$ 次の対称群 $S_n$ を専ら扱う。与えられた 2 つの数字 $i \neq j \in \{1, 2, \ldots, n\}$ に対して、$i$ と $j$ を入れ替えてそれ以外の数字はそのままにしておく置換を**互換** (transposition) と呼び、$(ij)$ という記号で表す。$S_n$ の中に互換は、ちょうど $\binom{n}{2} = n(n-1)/2$ 個だけある。とくに隣り合った二文字の互換 $(i\ i+1)$ を基本互換 (elementary transposition) と呼ぶ。基本互換は、$n-1$ 個だけある。

**命題 7.1** (あみだ籤の原理)**.** 対称群 $S_n$ は基本互換 $\{(1\ 2), (2\ 3), \ldots, (n-1\ n)\}$ によって生成される。

*Proof.* $\sigma_i = (i\, i+1)$ とおく。$n$ に関する帰納法による。もし $\sigma \in S_n$ が、$\sigma(n) = i < n$ であれば、$\sigma_{n-1} \ldots \sigma_i \sigma$ は、$n$ を固定し、したがって $S_{n-1}$ の元とみなせるので帰納法の仮定が使える。 □

**問 85.** 置換 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{pmatrix}$ を与えるあみだ籤を具体的に一つ作れ。

置換 $\sigma$ の符号を $\mathrm{sgn}(\sigma)$ で表す。$n$ 次元の基本ベクトルを $e_1, \ldots, e_n$ で表すとき、

$$\mathrm{sgn}(\sigma) = \det(e_{\sigma(1)}, \ldots, e_{\sigma(n)})$$

であることに注意。$\mathrm{sgn}(\sigma) = 1$ であるものを**偶置換** (even permutation) $\mathrm{sgn}(\sigma) = -1$ であるものを**奇置換** (odd permutation) と呼ぶ。互換の符号は $-1$ であるので、偶置換とは、偶数個の互換の積で書ける置換であると言ってもよい。置換に対してその符号を対応させる写像（関数）は、$S_n$ から $\{\pm 1\}$ への準同型になっているので、偶置換全体は、$S_n$ の正規部分群を形成する。これを $n$ 次の**交代群** (the alternating group of degree $n$) とよび、$A_n$ という記号で表す。

**問 86.** 交代群 $A_n$ の要素の数 $|A_n|$ を求めよ。

互換は 2 文字の入れ換えであるが、これを一般化して、$m$ 文字 $j_1, j_2, \ldots, j_m$ に対して

$$j_1 \mapsto j_2,\ \ldots,\ j_{m-1} \mapsto j_m,\ j_m \mapsto j_1$$

であり、これら以外の文字を動かさない置換を $(j_1 j_2 \ldots j_m)$ であらわし、**巡回置換** (cyclic permutation) と称する。$m$ は巡回置換の位数に等しいことに注意。$m$ はまた、巡回置換の長さとも呼ばれる。

与えられた置換 $\sigma$ に対して、$\sigma$ の作用による軌道分解（正確には、$\sigma$ によって生成される巡回群の作用による軌道分解）を考えることで、置換の互いに干渉しない巡回置換による積表示、**サイクル分解** (cycle decomposition) という、を得る。

**例 7.2.**

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 7 & 2 & 6 & 1 & 4 \end{pmatrix} = (1\,5\,6)\,(2\,3\,7\,4).$$

$n$ 次の置換 $\sigma$ のサイクル分解で、長さ $l$ の巡回置換が含まれる個数を $\lambda_l$ で表わす（ただし、$\lambda_1$ は $\sigma$ の不動点の個数を表わす）と、

$$n = \sum_{l=1}^{n} l\lambda_l$$

なる自然数の列 $\lambda_1, \lambda_2, \ldots, \lambda_n$ を得る。これを、

$$\lambda = 1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n}$$

のように表記して、$\sigma$ の**型** (type) と呼ぶ。また、上の式で定まる $n$ を型の大きさといい、$|\lambda|$ で表わす。型の表記においては $\lambda_l = 0$ となる項は、適宜省いてかまわないものとする。

例えば、

$$\sigma = (2)\,(3)\,(6)\,(1\ 9)\,(7\ 11)\,(10\ 8\ 4\ 5)$$

の型は $1^3 2^2 4$ である。

型を視覚的に表示したものにヤング図式がある。与えられた型 $1^{\lambda_1} 2^{\lambda_2} \dots$ に対して、$l$ 個の (小さな) 正方形を横に密着させて並べたものを $\lambda_l$ 行だけ縦に並べて得られる箱型の図形を考え、それらを $l$ の大きい順に上から左端がそろう様に配列したものを**ヤング図式** (Young diagram) という。ヤング図式は $n$ 個の正方形から構成されている。

上で与えた置換の型を表わすヤング図式は、

□ □ □ □
□ □
□ □
□
□
□

のようになる。

**例 7.3.** 1 から 4 までの数字をでたらめに並べるとき、特定の型が得られる確率を求めよ。

**定理 7.4.** 2 つの置換 $\sigma, \tau \in S_n$ が共役であるための必要十分条件は、それらの型が一致することである。

これは次のことから分かる。

**補題 7.5.** 長さ $m$ の巡回置換 $(i_1\, i_2\, \dots\, i_m) \in S_n$ と $n$ 次の置換 $\sigma$ に対して、

$$\sigma(i_1\, i_2\, \dots\, i_m)\sigma^{-1} = (\sigma(i_1)\, \sigma(i_2)\, \dots\, \sigma(i_m))$$

である。

*Proof.* 2 種類の置換の合成 $\sigma(i_i \dots i_m)$, $(\sigma(i_1) \dots \sigma(i_m))\sigma$ が全ての数字の上で同一の対応規則を与えることを見ればよい。 □

対称群 $S_n$ の共役類は、したがって、大きさ $n$ の型の数だけある。この数を $p(n)$ で表わして、$n$ の**分割数** (the partition number of $n$) と呼ぶ。

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $p(n)$ | 1 | 2 | 3 | 5 | 7 | 11 | 15 | 22 | 30 | 42 |

分割数については、次の漸近公式 (Hardy-Ramanujan) が知られている。

$$p(n) \sim \frac{1}{4\sqrt{3}n} e^{\pi\sqrt{2n/3}}.$$

**問 87** (Optional)**.** 分割数の母関数の式、

$$\sum_{n\geq 0} p(n)x^n = \frac{1}{\prod_{l\geq 1}(1-x^l)}$$

を示せ。ただし $p(0) = 1$ とする。

次に、$\sigma \in S_n$ の共役類 $C(\sigma)$ の大きさを、その型 $\lambda$ を使って表わす公式を導こう。そのためには、共役作用に関する固定部分群の大きさがわかれば良い。

上の補題により、共役作用で長さ $l$ の巡回置換はやはり長さ $l$ の巡回置換に移されるので、$l^{\lambda_l}$ の部分は、全体として不変に保たれなければならない。さてこの部分の置換の仕方であるが、巡回部分 $(i_1 i_2 \dots i_l)$ を並べ替えて同一の巡回置換を得るのは、成分の巡回的なずらしだけなので、$l$ 通りの可能性がある。これらは、$\lambda_l$ 個のブロックごとに独立の選べるので全体として $l^{\lambda_l}$ の取り方が可能である。最後に、これら $\lambda_l$ 個の巡回置換は、相互に交換可能であるので、ブロックごとに選んだ配列を再置換することにより、結局 $\lambda_l!$ だけの場合の数が得られる。長さ $l$ の可能性を独立の動かすことにより、固定部分群の大きさは、$\prod_l l^{\lambda_l}\lambda_l!$ で与えられることがわかり、したがって

$$|C(\sigma)| = \frac{n!}{\prod_l l^{\lambda_l}\lambda_l!}$$

である。

**例 7.6.** $\sigma$ が巡回置換であるとき、

$$\lambda_l = \begin{cases} 1 & \text{if } l = n, \\ 0 & \text{otherwise} \end{cases}$$

より $|C(\sigma)| = (n-1)!$ である。

**問 88** (Optional)**.** 1 から $n$ までの数字をでたらめに並べるとき、特定の型が出現する確率を求めよ。

$n = 3, 4, 5$ について、共役類の可能な型とその大きさを求めると、

$n = 3$

$$1^3(1),\ 1^1 2^1(3),\ 3^1(2).$$

$n = 4$

$$1^4(1),\ 1^2 2^1(6),\ 2^2(3),\ 1^1 3^1(8),\ 4^1(6).$$

$n = 5$

$$1^5(1),\ 1^3 2^1(10),\ 1^1 2^2(15),\ 1^2 3^1(20),\ 2^1 3^1(20),\ 1^1 4^1(30),\ 5^1(24).$$

**問 89.** $S_n$ $(n = 3, 4, 5)$ について、共役類の可能な型とその大きさを求めよ。また、各型をヤング図式で表わしてみよ。さらにまた、各共役類の偶奇性についても調べよ。

正規部分群は共役類の和集合であることと、部分群の大きさは約数であるという性質を組み合わせることで、共役類についての分析からから正規部分群についての情報を導くことができる。

**例 7.7.** $S_4$ の自明でない正規部分群は、大きさ $4 = 1 + 3$ と $12 = 1 + 3 + 8$ の 2 種類である。

$S_5$ の自明でない正規部分群は、一つしかなくその大きさは、$60 = 1 + 15 + 24 + 20$ で、実際これは $A_5$ に他ならない。

**問 90** (Optional)**.** 交代群 $A_4$, $A_5$ の共役類について調べよ。$A_4$ の自明でない正規部分群は、一つしかなくその大きさは、4 である。また、$A_5$ の正規部分群は自明なものに限ることを示せ。

多項式 $f(x_1, \ldots, x_n)$ は、$\forall \sigma \in S_n$, $\sigma f = f$ となるとき、**対称式** (symmetric polynomial) また、$\forall \sigma$, $\sigma f = \mathrm{sgn}(\sigma) f$ となるとき、**交代式** (alternating polynomial) と呼ぶ。

交代式で基本的なものが、差積 (difference product)

$$\Delta(x_1, x_2, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j)$$

である。これは、**Vandermonde 行列式**と次の関係で結ばれている。

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{vmatrix} = (-1)^{n(n-1)/2} \Delta(x_1, x_2, \ldots, x_n).$$

**問 91** (Optional)**.** Vandermonde 行列式を差積を使って表わせ。

交代式は差積で割りきれ、割りきった商は対称式になる。

**例 7.8.**

$$\sum_{\sigma \in S_n} \sigma f$$

は対称式で、

$$\sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \sigma f$$

は交代式である。

注意 . 対称群を数ベクトル空間に作用させる際に、例えば、$(z_1, \ldots, z_n) \in \mathbb{C}^n$ に対して、

$$\sigma(z_1, \ldots, z_n) = (z_{\sigma^{-1}(1)}, \ldots, z_{\sigma^{-1}(n)})$$

としなくては左からの作用にならない。これを、関数空間への作用に転化したものを多項式関数などに制限すれば、上で与えた作用と一致することがわかる。

**問 92** (Optional)**.** $S_n$ の元の位数の最大値を求めよ。

# 8 軌道数公式

以下では、群 $G$ が集合 $X$ に（左から）作用している状況を考える。$g \in G$ で動かされない点全体を $X^g$ という記号で表わす。すなわち、

$$X^g = \{x \in X; gx = x\}$$

である。単位元については、$X^1 = X$ であることに注意。

**問 93.** 作用に対応した準同型を $\pi : G \to S(X)$ で表わすとき、

$$\ker \pi = \{g \in G; X^g = X\}$$

を示せ。

**例 8.1.** 対称群 $S_n$ の $X = \{1, 2, \ldots, n\}$ への自然な作用を考える。$n = 5$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$$

とすると、$X^\sigma = \{2, 4\}$ である。

**問 94.** 直交群 $O(2)$ のユークリッド空間 $X = \mathbb{R}^2$ への自然な作用を考える。直交行列 $T$ に対して、

$$X^T = \begin{cases} \text{原点を通る直線} & \text{if } \det(T) = -1, \\ \text{全空間} & \text{if } T = I, \\ \text{原点} & \text{otherwise.} \end{cases}$$

**定理 8.2** (Burnside)**.** 有限群 $G$ が有限集合 $X$ に作用しているとき、その軌道の数（＝軌道空間の大きさ）は、

$$\frac{1}{|G|} \sum_{g \in G} |X^g|$$

に等しい。ここで、

$$X^g = \{x \in X; gx = x\}$$

は $g$ で固定される点全体を表す。

証明に入る前に、軌道長公式を次の形で思い出しておこう。

ひとつの軌道 $O$ に対して、

$$\sum_{x \in O} |G(x)| = |G|$$

である。

*Proof.* 集合

$$Y = \{(g, x) \in G \times X; gx = x\}$$

を 2 つの方法で計算する。ひとつは、$g$ 変数について和を取る方法で、

$$\sum_{g \in G} |X^g|$$

である。

一方、$x$ 変数についての和は、

$$\sum_{x \in X} |G(x)| = \sum_{O \in G \backslash X} \sum_{x \in O} |G(x)|$$

となる。ここで、

$$\sum_{x \in O} |G(x)| = |G|$$

が軌道 $O$ の取り方に無関係に成り立つことに注意すれば、求める公式を得る。 □

**問 95** (Optional)**.** 共役作用において、上の軌道数公式がどうなっているか調べよ。

自然数 $m$ に対して、$X = \{1, 2, \ldots, m\}$ とし、他に、大きさ $n$ の有限集合 $Y$ を用意する。そして、$X$ から $Y$ への写像全体のなす集合 $Z = Y^X$ を考える。集合 $X$ には対称群 $S_m$ が自然に作用しているので、それから引き起こされる形で、集合 $Z$ にも作用している。

さて巡回置換 $\sigma = (1\,2\,\ldots\,m)$ から生成された $S_m$ の部分群を $C$ で表わすと、$C$ もやはり $X$ および $Z$ に作用している。

この状況の解釈として、$X$ は円周を $m$ 等分した弧状の曲線を表わし、$Y$ は色の集合を表わすとすると、$Y$ の中から重複を許して $m$ 回色を取り出し、$X$ の元に対応する円弧を次々と色づけしたものが、$Z$ の元であると思うことができる。

このとき、$C$ の作用は、円周の $m$ 分割を同じく $m$ 分割に移す回転操作と考えることができる。そう思うと、$C$ の作用による $Z$ の軌道空間は、$C$ の回転で移りあえるものを同一視した彩色法の数と解釈される。

まずは、具体的に考えるために $m = 6$ とおいてみる。そうすると、$langle\sigma^l\rangle$ の $X$ への軌道を調べることで、$X^{\sigma^l}$ の表わす彩色の様子は、$l = 1, 5$ の場合は、単色彩色、$l = 2, 4$ の場合は、二色を交互に配色、$l = 3$ の場合は、三色を対点どうしが同色になるように彩色することがわかるので、

$$|Z^{\sigma^l}| = \begin{cases} n & \text{if } l = 1 \text{ or } l = 5, \\ n^2 & \text{if } l = 2 \text{ or } l = 4, \\ n^3 & \text{if } l = 3, \\ n^6 & \text{if } l = 0 \end{cases}$$

となる。これを、軌道数公式に代入すれば、彩色方法の数は、

$$\frac{2n + 2n^2 + n^3 + n^6}{6}$$

であるとわかる。

これを一般化すると次が得られる。

**例 8.3.** 上の状況のもとで、$l$ と $m$ の最大公約数を $(l, m)$ で表わすと、

$$|C\backslash Z| = \frac{1}{m}\sum_{l=1}^{m} n^{(l,m)}$$

となる。

**問 96.** $\sigma^l$ の位数 $o(l)$ は、$m/(l, m)$ で与えられることに注意して、

$$|Z^{\sigma^l}| = n^{m/o(l)} = n^{(l,m)}$$

を導け。

一般の $m$ の場合の分析も同様に可能であるが、簡単のために、$m$ が素数 $p$ である場合を次に調べよう。

さて、$C = \{1, \sigma, \sigma^2, \ldots, \sigma^{p-1}\}$ であるが、$p$ が素数であることに注意すると、$1 \leq l < p$ に対して、$C = \langle \sigma^l \rangle$ であることがわかる。これから、$Z^{\sigma^l}$ に属する彩色は単色でなければならず、結局

$$\left| Z^{\sigma^l} \right| = \begin{cases} n & \text{if } 1 \leq l \leq p-1, \\ n^p & \text{if } l = 0. \end{cases}$$

となる。これを軌道数公式に代入すれば軌道の数 $|C\backslash Z|$ は、

$$\frac{n^p + (p-1)n}{p} = n + \frac{n^p - n}{p}$$

であることがわかる。

次に、以上の配列の問題を空間の中での違いに着目して考えよう。この場合、同一視のための群は、（回転を表わす）巡回群だけでは足りなくて、折り返しの操作も含める必要がある。たとえは、

$$\tau = \begin{pmatrix} 1 & 2 & \ldots & m \\ m & m-1 & \ldots & 1 \end{pmatrix}$$

を加えてみよう。これは $\tau^2 = 1$ の他に

$$\tau\sigma\tau = \sigma^{-1}$$

という関係をみたす。

**問 97.** $\sigma^l\tau$ $(l = 1, \ldots, m-1)$ で $m$ 角形の板を不変にする全ての折り返しが得られる。

これを使えば $\sigma$ と折り返しから生成された群 $G$ は、

$$G = \{1, \sigma, \ldots, \sigma^{m-1}, \tau, \sigma\tau, \ldots, \sigma^{m-1}\tau\}$$

となることがわかる。とくに、$|G| = 2m$ である。

さて、$G$ の作用で移りあるものを同一視した場合の彩色数を求めるために、折り返し $g = \sigma^l\tau$ による $Z^g$ の大きさを求める必要がある。これは、$m$ の偶奇性で様子が異なるので、分けて考える。まず、$m = 2k+1$ が奇数の場合であるが、折り返しは必ず正 $m$ 角形の一頂点と一辺を通るので、その変換で不変な彩色数は、$l$ と関係なく $|Z^g| = n^{k+1}$ となるので、

$$|G\backslash Z| = n^{k+1} + \frac{1}{2m}\sum_{l=1}^{m} n^{(l,m)}$$

となる。

次に、$m = 2k$ が偶数の場合であるが、折り返し $\tau, \sigma^2\tau, \ldots, \sigma^{2m-2}\tau$ は 2 つの辺を通る直線に関するものなので、$|Z^g| = n^k$ となる。一方、$\{\sigma\tau, \sigma^3\tau, \ldots, \sigma^{2k-1}\tau$ の方は、二頂点を通る直線に関する折り返しになっているので、$|Z^g| = n^{k+1}$ となる。以上から、

$$|G\backslash Z| = \frac{n^k(n+1)}{2} + \frac{1}{2m}\sum_{l=1}^{m} n^{(l,m)}$$

となる。

**例 8.4.** $m = 6$ の場合を具体的に書き下してみると、

$$|G\backslash Z| = \frac{1}{12}(n^6 + 3n^4 + 4n^3 + 2n^2 + 2n).$$

さらに具体的に $n = 2$ とすると、１３通り。

**問 98.** 正 6 角形の指輪の 6 辺を 3 色で塗り分ける方法は何通りあるか。

**問 99** (Challenge)**.** 立方体の面を $n$ 種類の色で塗り分けるとき、何種類の本質的に異なった塗り分けが可能か調べよう。

# A　集合と写像

（この付録の文章は、相当「酔っ払って」ます。「独法化」印のカストリを無理やり飲まされ、悪酔いしたのです。今もそう。ご容赦を。）

本文では、集合の記号がふんだんに使われる。とくに、集合を要素とする集合という考え方は、素朴な図形表示による理解では、見過ごされてしまう危険性が高いので、少し、注意点を強調して説明してみよう。有限集合と雖も侮り難しといったところである。（数学者は、とかく無限にばかり目が行きがちで困ったものである。）

集合を表示する際に注意すべきは、同じ要素が複数回並べられていても一つと数える点である。

**問 100.** 次の集合に含まれる要素の数はいくらか。

$$A = \{1, 2, 1, 2, 1, 1\}.$$

次に注意すべきは集合の集合も要素となり得ることである。

**問 101.** 次の集合に含まれる要素の数はいくらか。

$$B = \{1, \{1\}, \{1, 2\}, \{1, \{2\}\}\}.$$

空集合 $\emptyset$ も集合であるので、それを要素とする集合 $\{\emptyset\}$ は空集合でない点である。

**問 102.** 次の集合に含まれる要素の数はいくらか。

$$C = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}\}.$$

さて仕上げとして、集合 $X$ の部分集合を要素とする集合を考えよう。これを $X$ の**べき集合** (power set) と呼び、$2^X$ という記号で表わす。

**問 103.** 有限集合 $X$ に対して、$|2^X| = 2^{|X|}$ であることを、次の公式と併せて示せ。

$$2^n = \sum_{k=0}^{n} {}_nC_k.$$

2つの集合 $X, Y$ （$X = Y$ であっても構わない）の積集合は、$X \times Y$ で表わされる。もう一つ集合 $Z$ があれば、さらに $(X \times Y) \times Z$ という集合を作ることができるが、これは通常、同時積集合 $X \times Y \times Z$ と同一視される（正確には、自然な全単射があるということである)。

上では、集合の同一視のことで神経質に区別したばかりであるのに、ここでは一転して、ある意味でルーズに同一視である。こういう類の「自然な同一視」というものが数学をしていると、意外と多く目にするもので、こういったことが許される根拠も分かってはいるのだが、数学を専門にしている人でも案外無自覚あるいは無邪気に使っていたりする。詳しく知りたければ、Maclane, coherence theorem で検索をかければ色々見つかるであろう。まあ、結果的には、形式的な話ではあるが、結合律は奥が深いということでもある。

さて写像である。定義域と値域に注意しよう。これをいい加減にすると、写像の合成に齟齬をきたすし、ひいては結合法則という有り難い話までたどり着けなくなってしまう。写像の結合法則では、多重合成写像が明確に定義できるため、一般的な結合法則の成立根拠をより明白に把握することができる。

$$(\ldots(f_1 \circ f_2) \circ \cdots \circ f_n) = f_1 \circ f_2 \circ \cdots \circ f_n$$

のことである。

次に単射、全射、全単射が代数的に記述されることは、よいであろうか。

$$f_1 \circ f = f_2 \circ f \Longrightarrow f_1 = f_2$$

といったことである。

逆写像の代数的な特徴づけは、群の公理の逆元の存在そのものである。

全単射は、集合の間に同値関係を導く。同値関係とグループ分け（類別）の対応は素朴なものではあるが、ここまでくると、その深淵さは底なしである。その同値類を集合の濃度という。有限集合の場合には、元の個数に他ならない。これは、ある意味単純な場合であるが、有限集合とて馬鹿にしてはいけない。

再び写像に戻って、順像と逆像である。

$$f(A) = \{f(a) \in Y; a \in A\}, f^{-1}(B) = \{a \in X; f(a) \in B\}$$

よくベルトのような絵が描いてあるあれである。$a \in A$ と $a \subset A$ をうるさく区別しておきながら、何とふしだらなことか。数学者の本質を見る思いがする。彼らは、論理・論理と喚く割には、その行動・生活においては無節操そのものであること多し。

分割和 (disjoint union) の記号

$$A \sqcup B$$

これは良い記号である。二つの世界を峻別する角の存在がすばらしい。角を取って丸く納めるといった不見識は、ここには存在しない。この潔さを堪能すべきである。

分割和を集団に適用すれば、全射との関係が見えてくる。

$$X = \bigsqcup_{i \in I} X_i \iff X = \bigcup_{i \in I} X_i, X_i \cap X_j = \emptyset \text{if } i \neq j$$

なる集合の分割を与えることと、全射 $q : X \to I$ を与えることは同じことだからである。さらにまた、$X$ における同値関係

$$x \sim y \iff q(x) = q(y)$$

と同定することもできる。

さて、こうして三位一体化された同値関係の同値類の作る集合を

$$\overline{X} = \{X_i; i \in I\}$$

で表わそう。これが、同値関係による $X$ の商集合 (quotient set) であり、$I$ の $X$ における実体化でもある。商写像 $x \mapsto \overline{x} \in \overline{X}$ と $q : X \to I$ とは、$\overline{x} = q^{-1}(q(x))$ という関係にあることに注意せよ。

標語的に、集合 $X$ の分割和、同値関係、$X$ で定義された全射像、これらの三位一体性を認識すべきである。

さて、写像 $\overline{X} \to Y$ があれば、商写像との合成により、写像 $X \to Y$ が得られる。逆に、写像 $f : X \to Y$ が、

$$x \sim y \Longrightarrow f(x) = f(y)$$

という性質をみたせば、写像 $\overline{f} : \overline{X} \to Y$ を $\overline{f}(\overline{x}) = f(x)$ によって定めることができる。このような形で記述される写像 $\overline{X} \to Y$ に関して、対応 $\overline{x} \mapsto f(x)$ は**うまくいっている** (well-defined) という言い方をする。すなわち、写像 $f : X \to Y$ が上の一定性の条件を満たしているということである。

# B　有限生成アーベル群

目標は、次の定理である。

**定理 B.1.** 有限生成アーベル群 $G$ は、巡回群の直積（＝直和）に同型である。

$$G \cong \mathbb{Z}^n \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_l}.$$

有限生成という条件から、全射準同型 $\mathbb{Z}^m \to G$ が存在し、その核を $H$ で表わせば、同型 $G \cong \mathbb{Z}^m/H$ が成り立つ（準同型定理)。そこで、$\mathbb{Z}^m$ の部分群 $H$ の構造が問題となる。

まず、$H$ も有限生成であることを示そう。純代数的に処理することも可能であるが、幾何学的直観を活用するために、$\mathbb{Z}^m \subset \mathbb{R}^m$ と埋め込んで考え、$H$ の元から成る $\mathbb{R}^m$ のベクトルの一次独立な集団のうち、極大なもの $\{v_1, \ldots, v_l\}$ を一組取ってくる。このとき、$V = \mathbb{R}v_1 + \cdots + \mathbb{R}v_l$ は、$l$ 次元ベクトル空間で、$\{v_1, \ldots, v_l\}$ は、その基底となる。そこで、$l$ 次元平行体

$$D = \{t_1v_1 + \cdots + t_lv_l; 0 \leq t_j \leq 1\}$$

（これは、$H$ の $\mathbb{R}^m$ への移動作用の基本領域に、境界部分を除いて一致する）を考えると、$D \cap H \subset D \cap \mathbb{Z}^m$ は有限集合となるので、$H$ は有限集合 $D \cap H \cup \{v_1, \ldots, v_l\}$ によって生成されることがわかる。

そこで、$H$ の生成元を改めて $\{a_1, \ldots, a_n\}$ とし、各 $a_j \in \mathbb{Z}^m$ を $m$ 次元縦ベクトルと思って並べて得られる $(m, n)$ 行列を $A$ で表わすと、$H = \{Ax; x \in \mathbb{Z}^n\}$ である。

自由アーベル群 $\mathbb{Z}^n$ の基底とは、$\mathbb{Z}^n$ の元からなる $\mathbb{R}^n$ の基底 $\{e_1, \ldots, e_n\}$ であって、$\mathbb{Z} = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$ となるものと定義する。

**補題 B.2.** $\{x_1, \ldots, x_n\}$ $(x_j \in \mathbb{Z}^n)$ が、$\mathbb{Z}^n$ の基底であるための必要十分条件は、$\det(x_1, \ldots, x_n) = \pm 1$ となることである。

基底の変換を表わす行列をかけることで、$\mathbb{Z}^n$ の自己同型が得られることに注意。

変形のための基本行列のうち、成分が整数から成り行列式の値が $\pm 1$ であるものを $\mathbb{Z}$ 基本行列と呼ぶ。行列 $A$ から出発して行または列に関する $\mathbb{Z}$ 基本変形を繰り返して得られる行列全体を $\mathcal{A}$ と書く。

整数を成分とする行列 $A$ を、$\mathbb{Z}$ 行基本変形、$\mathbb{Z}$ 列基本変形により、対角型に変形することを考える。

$$\mathcal{A}_{1,1} = \{b_{11}; B \in \mathcal{A}\}$$

とし、$\mathcal{A}_{1,1} \cap \mathbb{N}$ の最小値を $d$ とする。このとき、$(1,1)$ を pivot にした掃き出し操作により、1 行目および 1 列目の他の成分は、$d$ の倍数であることがわかるので、掃き出しによって、

$$\begin{pmatrix} d & 0 & \dots & 0 \\ 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \dots & * \end{pmatrix}$$

の形に変形できる。以下同様の方法で、対角型への変形が可能であるとわかる。

$$LAR = \begin{pmatrix} n_1 & 0 & 0 & 0 \\ 0 & \ddots & 0 & \vdots \\ 0 & 0 & n_l & 0 \\ 0 & \dots & 0 & 0 \end{pmatrix}$$

としよう。ここで、$L \in PSL(m,\mathbb{Z})$, $R \in PSL(n,\mathbb{Z})$ であり、左上隅に対角行列が置かれ、残りの成分はすべて 0 である。この表示を使い、次のようにして定理の主張を確かめることができる。

$$\mathbb{Z}^m/H \cong L\mathbb{Z}^m/LH = \mathbb{Z}^m/(n_1\mathbb{Z} \oplus \cdots \oplus n_l\mathbb{Z} \oplus 0^{m-l}) = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_l} \oplus \mathbb{Z}^{m-l}.$$

さて、巡回群は、その位数を素数冪の積に分解することで、$\mathbb{Z}_{p^e}$ の形のものの直和に分解される。したがって、

$$G \cong \mathbb{Z}^n \oplus \mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{e_r}}$$

という表示を得る。ここで、$p_j$ の中には同じ素数が複数回現われても良い。このとき、$n$ および非順序列 $\{p_1^{e_1}, \dots, p_r^{e_r}\}$ の組は、$G$ の同型類の完全不変量となり、型と呼ばれる。

実際、$T = \{g \in G; kg = 0 \text{ for some } k \in \mathbb{N}\}$ とおけば ($T$ を $G$ の torsion subgroup という)、$G/T \cong \mathbb{Z}^n$ という形で $n$ が確定し、さらに型に現れる素数の一つを $p$ とし、$p$ が関

わる指数部分を $(p^{e_1}, p^{e_2}, \dots)$ とすれば、$pT$ のそれは $(p^{e_1-1}, p^{e_2-1}, \dots)$ となるので、帰納法の仮定により指数が 2 以上の部分が確定し、さらに指数 1 の個数は、$\{g \in T; pg = 0\}$ の位数より決定される。また、型が等しい群は、明らかに同型である。

# C Historical Comments

$$Z^3 = c$$

の解は、

$$Z = c^{1/2}\, c^{1/3}\omega, c^{1/3}\omega^2, \qquad \omega = \frac{-1+\sqrt{3}i}{2}, \quad \omega^2 + \omega + 1 = 0.$$

対称式の基本定理：対称多項式式は基本対称式の多項式で書ける。

Lagrange's resolution: 3 次方程式のフォンタナによる解法

$$T^3 + aT^2 + bT + c = 0$$

置き換え $S = T + \frac{a}{3}$ により

$$S^3 + pS + q = 0, \qquad p = b - \frac{1}{3}a^2,\ q = \frac{2}{27}a^3 - \frac{1}{3}ab + c.$$

フォンタナの工夫：$S = U + V$ とおいて書き直すと

$$U^3 + V^3 + q + (U+V)(3UV + p) = 0.$$

そこで、$U, V$ の自由度を利用して、

$$U^3 + V^3 = -q, \qquad UV = -\frac{1}{3}p$$

を課す。$U^3, V^3$ は二次方程式

$$T^2 + qT - \frac{1}{27}p^3 = 0$$

の解。このとき $U^3V^3 = -p^3/27$ であるので三乗根の取り方を調整して、

$$u^3 + v^3 = -q, \qquad uv = -\frac{1}{3}p$$

となるものを取ってくる。このとき、他の解は $(u\omega^2, v\omega)$, $(u\omega, v\omega^2)$ となるので、もとの三次方程式の解として

$$x_1 = -\frac{a}{3} + u + v,$$
$$y_2 = -\frac{a}{3} + u\omega^2 + v\omega,$$
$$z_3 = -\frac{a}{3} + u\omega + v\omega^2$$

を得る（カルダノの公式、1545, Ars Magna）。Lagrange は補助的な量 $u, v$ を解 $x_1, x_2, x_3$ で表してみる。

$$u = \frac{x_1 + x_2\omega + x_3\omega^2}{3},$$
$$v = \frac{x_1 + x_2\omega^2 + x_3\omega}{3}$$

そして $u^3$, $v^3$ がなぜ二次方程式の解になるのかを考える。$u^3$ の中の $x_1, x_2, x_3$ を入れ替えて得られる式は、$u^3$, $v^3$ ですべてであることが二次方程式の出現理由。

$$(T - u^3)(T - v^3)$$

という二次式の係数は、$x_1, x_2, x_3$ の対称式になり、したがってもとの方程式の係数 $a, b, c$ の有理式（今の場合は多項式）で表される。

一般に $x_1, \ldots, x_n$ の有理式 $t_1 = f(x_1, \ldots, x_n)$ の $x_1, \ldots, x_n$ に置換を施して得られる式全体を $t_1, t_2, \ldots, t_m$ とすれば、$m$ 次方程式

$$(T - t_1)(T - t_2)\ldots(T - t_m)$$

の係数は、もとの方程式の係数の有理式でかける。

4 次方程式の解法：$t_1 = (x_1 + x_2)(x_3 + x_4)$, $t_2 = (x_1 + x_3)(x_2 + x_4)$, $t_3 = (x_1 + x_4)(x_2 + x_3)$ を解とする 3 次方程式

$$(T - t_1)(T - t_2)(T - t_3) = 0$$

の係数はもとの方程式の係数の多項式で書ける。そこで、この 3 次方程式をフォンタナの方法で解く。そうすれば、$x_1 + x_2$, $x_3 + x_4$ は二次方程式

$$T^2 - aT + t_1 = 0$$

の解として表され、同様に $x_1 + x_3$, $x_1 + x_4$ の表されるので、

$$x_1 = \frac{(x_1 + x_3) + (x_1 + x_4) - (x_3 + x_4)}{2}$$

も表される。

Nicolo del Fontana, 1465–1526

Gerolamo Cardano, 1501–1576

Viet, 1540–1603

Lagrange, 1736–1813 1770

de Moivre

Vandermonde

Paolo Ruffini, 1799

Abel, 1824,

Galois,

若者よ、汗をかけ、恥をかけ、文字を書け — 佐藤忠良の言葉より