命題 5.8. 全ての（抽象的）群は、群自身に作用するある変換群と同型である。とくに有限群は対称群の部分群と同型である。

Proof. 群 G の左正則作用による。 □

[光学異性体]

正４面体の４つの頂点に数字 $\{1,2,3,4\}$ を対応させることにより、正４面体群は、$X=\{1,2,3,4\}$ に作用する。この作用により正４面体群は、４次交代群 A_4 と同一視できる。

一方、正４面体を正４面体に移す変換を、回転群 $SO(3)$ の要素だけでなく、直交群 $O(4)$ にまで広げて作用を考えると、４次対称群 S_4 を得る。

さて、（４面体の）各頂点に m 種類の原子を配列すると、その可能性は集合 Y^X $(|Y|=m)$ で記述される。この原子配列の集合 Y^X への群 A_4, S_4 の作用による軌道の違いについて調べて見ると、$m\leq 3$ については、どちらの作用でも同一の軌道が得られる一方で、4 種類の原子の配列集合においては、S_4 の作用では推移的になるのに対して、A_4 の作用では、２つの異なる軌道が得られる。この違いが、光学異性体の存在に関する数学的説明となる。より感覚的には、右手系と左手系の違い、でもある。

逆にみると、（結合の仕方も含めて）３種類以下の配列では、正４面体型の光学異性体は出現しない、ということでもある。

6 対称群

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 $(i\ i+1)$ を基本互換と呼ぶ。基本互換は、$n-1$ 個だけある。

命題 6.1 (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。

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

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

であることに注意。$\epsilon(\sigma) = 1$ であるものを偶置換 (even permutation) $\epsilon(\sigma) = -1$ 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** (alternating group) とよび、A_n という記号で表す。

巡回置換 (cyclic permutation or cycle) とサイクル分解 (cycle decomposition)。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、巡回置換と称する。m は巡回置換の位数に等しいことに注意。

与えられた置換 σ に対して、σ の作用による軌道分解（正確には、σ によって生成される部分群の作用による軌道分解）を考えることで、サイクル分解を得る。

共役作用と共役類と分割数、ヤング図形。

群の直積と安定部分群。2 つの群 $G,\ H$ ($G = H$ となっていてもよい）に対して、直積集合 $G \times H = \{(g,h); g \in G, h \in H\}$ に群演算を $(g,h)(g,h) = (gg', hh')$ で定義したものを、G と H の直積群あるいは簡単に**直積** (direct product) という。直積は、複数個の群の場合にも定義できる。n 個の群 $G_1, G_2, \ldots, G_n$ があるとき、その直積集合

$$G_1 \times G_2 \times \cdots \times G_n$$

は自然に群の構造をもつ。

例 6.2. 対称群の直積 $S_m \times S_n$ は、自然に S_{m+n} の部分群とみなせる。もっと一般に、自然数の列 $n_1, n_2, \ldots, n_r$ に対して、

$$S_{n_1} \times S_{n_2} \times \cdots \times S_{n_r} \subset S_{n_1+n_2+\cdots+n_r}$$

となる。

例 6.3. 随伴作用の安定部分群は、サイクル分解に現れる各サイクルから生成される部分群の直積を含む。

例 6.4. クライン群 $\{1, a, b, c\}$ は、$\mathbb{Z}_2 \times \mathbb{Z}_2$ と同型である。

命題 6.5. 交代群 A_n は長さ 3 の巡回置換全体で生成される。

定理 6.6. 5 次以上の交代群 A_n $(n \geq 5)$ は**単純群** (simple group) である、すなわち A_n の正規部分群は、$\{1\}$ かまたは A_n に限る。

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。

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、交代式と呼ぶ。

対称式、交代式。基本対称式。差積と Vandermonde の行列式。

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

とおくと、これは交代式であるので、差積に比例する。

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

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 6.7.

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

は対称式で、

$$\sum_{\sigma \in S_n} \epsilon(\sigma) \sigma f$$

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。

7　アーベル群

群の演算が、$ab = ba$ を常に満たすとき**可換群** (commutative group) あるいは**アーベル群** (abelian group) と呼ぶ。可換群においては、全ての部分群は自動的に正規部分群になるので、この 2 つの概念は一致する。

可換群の代表的な例としてベクトルの和の演算に関するものがあり、この場合は、群の演算は積の記号ではなく和の記号で表される。（群演算を和の記号で表すときには、単位元は、e とかではなく 0 で表す。）このように可換群については、群演算を表すのに、和と積の記号を適宜使い分ける習慣がある。

例として、与えられた自然数 n に対して、$\mathbb{Z}$ の（正規）部分群 $n\mathbb{Z}$ による商群 $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ は和の記号で演算を書くのが普通である。ただし、n が関与しているので、それを明示するために、$n = 7$ の場合であれば、

$$2 + 6 = 1 \mod 7$$

といった書き方をする。

一方、準同型写像 $\mathbb{C}^\times \ni z \mapsto z^n \in \mathbb{C}^\times$ の核としての $\mathbb{C}^\times$ の部分群

$$C_n = \{z \in \mathbb{C}; z^n = 1\}$$

を考えると、1 の原始 n 乗根 ζ （例えば、$\zeta = e^{2\pi i/n}$）を選んでおけば、準同型写像

$$\mathbb{Z} \ni m \mapsto \zeta^m \in C_n$$

の核が $n\mathbb{Z}$ となるので、準同型定理により、

$$\mathbb{Z}_n \ni [m] \mapsto \zeta^m \in C_n$$

という同型（写像）を得る。

もう少し一般的に、群 G の元 a から生成された巡回群 $\langle a\rangle$ を考えると、$\mathbb{Z} \ni m \mapsto a^m \in \langle a\rangle$ という準同型写像を得るので、その核は、$\mathbb{Z}$ の部分群として、$n\mathbb{Z}$ の形（$n = 0, 1, 2, \dots$) になる。$n = 1$ となるのは、$a = e$ の場合で、この自明な場合を排除すれば、準同型定理により

$$\langle a\rangle \cong \begin{cases} \mathbb{Z}_m & \text{if } m \geq 1, \\ \mathbb{Z} & \text{if } m = 0 \end{cases}$$

となる。

$n = 0$ の場合（すなわち $\mathbb{Z}$ と同型な場合）を無限巡回群、$n \geq 2$ の場合（すなわち、$\mathbb{Z}_n$　と同型な場合）を n 次の**巡回群** (cyclic group) という。

例 7.1. 位数が素数の群は、巡回群であり、位数が等しければ全て同型である。

例 7.2. n 次の対称群において、巡回置換

$$(12\dots n) = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix}$$

は n 次の巡回群を生成する。

$\mathbb{Z}_n$ と $\mathrm{Aut}(\mathbb{Z}_n)$。加法群の直和記号。$\mathbb{R}$, $\mathbb{T}$, $\mathbb{Z}$.

オイラーの公式と準同型 $\mathbb{R} \to \mathbb{T}$.

ユークリッド空間 $\mathbb{R}^n$ の基底から生成された部分群を格子群 (lattice) という。$\mathbb{R}^n$ を格子群で割った商群 $\mathbb{R}^n/L \cong \mathbb{T}^n$ はトーラス群と呼ばれる。$\mathbb{Z}^n$ の自己同型群 $\mathrm{Aut}(\mathbb{Z}^n) = GL(n, \mathbb{Z})$.

例 7.3. 有限群 G で、G のすべての元が $g^2 = e$ をみたすものは、$\mathbb{Z}_2$ の直積 $\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ に同型である。

実際、$a, b \in G$ とすると、$(ab)^2 = e$ と $a^{-1} = a$, $b^{-1} = b$ より $ab = ba$ となって、G は可換群。さらに、G の部分群 H と、$a \in G \setminus H$ に対して、$\langle a, H\rangle \cong \langle a\rangle \times H$ が示せるので、帰納法が使える。

次の事実は、ここでは証明しない。「環と加群」または、下の問、参照。

定理 7.4 (アーベル群の基本定理). 有限生成アーベル群は、有限個の巡回群の直積と同型になる。

アーベル群 $\mathbb{Z}$ の有限個の直積 $\mathbb{Z}^n$ と同型な群を自由アーベル群という。自由アーベル群の基底。自由アーベル群の間の準同型 $\mathbb{Z}^n \to \mathbb{Z}^m$ の行列表示。基底の変換と、行列表示の変換。行列表示の標準形。

$$\mathrm{diag}(d_1, d_2, \dots, d_r, 0, \dots, 0), \qquad d_1 | d_2, \dots, d_{r-1} | d_r.$$