

群の概念

高村, 良盛 / Takamura, Y.

(出版者 / Publisher)

法政大学経済学部学会

(雑誌名 / Journal or Publication Title)

The Hosei University Economic Review / 経済志林

(巻 / Volume)

52

(号 / Number)

3・4

(開始ページ / Start Page)

312

(終了ページ / End Page)

288

(発行年 / Year)

1985-03-15

(URL)

<https://doi.org/10.15002/00030462>

群 の 概 念

高 村 良 盛

目 次

1. はじめに
2. 群の定義
 - a 半 群
 - b 群
3. 群の例
 - a 数と行列
 - b 群 表
4. 置換群
 - a 対 称 群
 - b 交 代 群
5. 部分群
 - a 部 分 群
 - b 生 成 系
 - c 巡 回 群
 - d 中心化群
6. む す び

1. はじめに

数学の全体系を支える4つの礎石は、数、集合、関数および群であり、他の数学の諸概念はすべてこれに帰着させられる。他方、数学的な法則の多くのものが、本質的には代数的な法則であり、代数はますます他の数学の分野の基礎となりつつある。数学全体に対して、ますます増大する影響力をもつ、その代数学の基礎こそ、群の概念そのものである。故に、群の概念から研究を始めれば、効率的に現代代数学全般の研究を進めることが

できるであろう¹⁾。

現代代数学は、古典的な代数学は勿論、数学諸分野からの概念を一般化、抽象化して理論を形成してきた。この総合的な現代代数学は、自然科学や社会科学の分析手法として極めて重要な意義をもっているし、これらの科学的認識を向上させるのに役立つであろう。本論文はこの目的のための前進の論理的な第一歩なのである²⁾。

2. 群の定義

a 半群

空でない集合 S に対して、写像 $f: S \times S \rightarrow S$ を S 上の 2 項演算 (binary operation), 代数的演算または略して演算という。 S 上の 2 項演算 $f(a, b)$ を $a * b$ で表す, $a * b$ がつねに S の 1 個の元となるとき, S は演算 $*$ に関して閉じているといい, S を演算 $*$ をもつ代数系 (algebraic system) という。 $a * b = a + b$ と表されるとき加法系 (additive system), $a * b = ab$ と表されるとき乗法系 (multiplicative system) という。しかし, 今後は, 便宜上, 上のような煩わしい記号の区別をさけ, ab でも場合によっては $a + b$ をも意味することにきめておく。なお, ab を積, $a + b$ を和と呼ぶ¹⁾。

演算の定義された集合 S において, 結合法則 (associative law)

$$(ab)c = a(bc) \quad (\forall a, b, c \in S) \quad (2.1)$$

が成り立つとき, S を半群 (semigroup) という。

命題 2.1 半群 S の元 $a_1, a_2, \dots, a_n$ ($n \geq 3$) について配列の順序を固定し, 演算を $n-1$ 回施して得られる S の元は, すべて $(\dots((a_1 a_2) a_3) \dots) a_n$ に等しい。従ってその積を $a_1 a_2 \dots a_n$ と書く。

証明 n に関する帰納法で示す。 $n=3$ のときは (2.1) にほかならない。

1) Alexandroff [A 3], p. 7. van der Waerden [V], pp. 1—2. 奥川 [O 1], まえがき. Allen [A 4], p. 8. 浅野 [A 5], はしがき.

2) 秋月 [A 1], pp. 113—7. Birkhoff [B], pp. 9—10. Queysanne [Q], pp. 7—9.

1) 渡辺 [W], p. 1. Alexandroff [A 3], pp. 56—9.

$n \geq 4$ とし, $n-1$ 個以下の元については成り立つと仮定する. $a_1, \dots, a_n$ に演算を $n-1$ 回施して得られる S の元 a は, $a_1, \dots, a_k$ ($k < n$) に $k-1$ 回演算を施して得られる元 b と, $a_{k+1}, \dots, a_n$ に $n-k-1$ 回演算を施して得られる元 c との積 bc に等しい. 仮定によって $c = (\dots((a_{k+1}a_{k+2})a_{k+3})\dots a_{n-1})a_n$ だから, (2.1)を用いて

$$\begin{aligned} a &= b((\dots((a_{k+1}a_{k+2})a_{k+3})\dots a_{n-1})a_n) \\ &= (b(\dots((a_{k+1}a_{k+2})a_{k+3})\dots a_{n-1}))a_n. \end{aligned}$$

従って, $a = (\dots((a_1a_2)a_3)\dots a_{n-1})a_n = a_1a_2\dots a_n$ ²⁾ ■

半群 S の元 a 自身の n 個の積を a^n で表すと,

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn} \quad (\forall m, n \in \mathbb{N}). \quad (2.2)$$

また, a の n 個の和を na で表すと,

$$ma + na = (m+n)a, \quad n(ma) = (nm)a \quad (\forall m, n \in \mathbb{N}). \quad (2.3)$$

半群 S の元 e は

$ae = a$ ($\forall a \in S$) のとき, e を S の右単位元,

$ea = a$ ($\forall a \in S$) のとき, e を S の左単位元

といい,

$$ae = ea = a \quad (\forall a \in S) \quad (2.4)$$

をみたすとき, S の単位元 (identity, unit element) という, このとき, この半群を単位半群 (monoid) という. S の単位元は存在すればただ 1 つに限る. 実際, e_1 と e_2 を S の単位元とすると, $e_1 = e_1 e_2 = e_2$.

半群 S が単位元をもつとき, $a \in S$ に対して,

$ab = e$ のとき, b を a の右逆元,

$ba = e$ のとき, b を a の左逆元

といい,

$$ab = ba = e \quad (2.5)$$

をみたすとき, $b \in S$ を a の逆元 (inverse element) という. 逆元は存在すれば, ただ 1 つに限る. 実際, b_1 と b_2 を a の逆元とすると,

2) 東郷 [T 2], p. 4. 浅野 [A 5], pp. 3—4. 奥川 [O 1], p. 14.

$$b_1 = b_1 e = b_1 (ab_2) = (b_1 a) b_2 = e b_2 = b_2.$$

a の逆元を a^{-1} で表す. また a^0 で表すこともある. e の逆元は e である. 逆元をもつ元を正則元 (regular element) という. 2 つ以上の正則元の積も正則元である³⁾.

半群 S の元 a, b は $ab = ba$ のとき可換 (commutative) であるといい, S の任意の 2 元が可換のとき, S は可換であるという.

例 2.1 $\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ はいずれも加法に関して半群で, 0 が単位元, 各元 a が逆元 $-a$ をもつ. それらは乗法に関して半群で, 1 が単位元であり, $\mathbf{Z}$ では ± 1 のみが逆元をもち, $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ では 0 以外の各元 a が逆元 $1/a$ をもつ.

例 2.2 $n \geq 2$ として, $\mathbf{R}$ 上の n 次正方行列全体の集合を $M_n(\mathbf{R})$ とすると, $M_n(\mathbf{R})$ は行列の加法に関して可換な半群, 行列の乗法に関して非可換な半群である.

例 2.3 空でない集合 S から S への写像全体の集合 H は, 写像の合成に関して半群である, 実際, $f, g, h \in H$ とすると, 任意の $x \in S$ に対し,

$$\begin{aligned} ((fg)h)(x) &= (fg)(h(x)) = f(g(h(x))) = f((gh)(x)) \\ &= (f(gh))(x). \end{aligned}$$

従って $(fg)h = f(gh)$ ⁴⁾.

b 群

演算をもつ集合 G が半群を作り, さらに, 単位元をもち, G の各元が逆元をもつとき, G は群を作るという. 2. a で述べたように, 群 G の単位元はただ 1 つに限り, それを e で表す. また, 群 G の各元 x はただ 1 つの逆元 x^{-1} をもつ. 単位元 e と逆元 x^{-1} に関して (2.4), (2.5) の条件をゆめめて, つぎのように,

定理 2.2 半群 G が $xe' = x$ ($\forall x \in G$) をみたす元 e' をもち, G の各元 x に対し, $xy = e'$ をみたす $y \in G$ をもつならば, 半群 G は群である.

3) 山田 [Y 2], pp. 11—8. 浅野 [A5], pp. 5—8.

4) 東郷 [T 2], p. 5. 浅野 [A 5], pp. 1—2.

証明 $x \in G$ に対し $xy = e'$ なる $y \in G$ をとると,

$$y = ye' = y(xy) = (yx)y. \quad (1)$$

$yz = e'$ なる $z \in G$ をとり, (1)の右から掛けると,

$$e' = yz = ((yx)y)z = (yx)(yz) = yxe' = yx.$$

故に, y は $xy = yx = e'$ をみたす. これを用いて,

$$e'x = (xy)x = x(yx) = xe' = x$$

となるから, e' は G の単位元であり, 従って y は x の逆元である. よって G は群である. ■

定理 2.2 から右単位元, 右逆元であろうと, 群の定義に支障はおこらないことが分かった. 左単位元, 左逆元の場合も同様である⁵⁾.

群の定義から得られる性質を以下に列挙する.

(1) 群 G では, 簡約法則 (cancellation law)

$$ab = ac \Rightarrow b = c, \quad ba = ca \Rightarrow b = c$$

が成り立つ,

(2) 群 G の 2 元 a, b に対して, $ax = b(ya = b)$ をみたすただ 1 つの $x \in G$ ($y \in G$) がある.

証明 $x = a^{-1}b$ とすると $ax = aa^{-1}b = eb = b$. 逆に $x' \in G$ が $ax' = b$ をみたすならば, 左から a^{-1} を掛けて $a^{-1}ax' = a^{-1}b$, すなわち, $x' = a^{-1}b$. $ya = b$ の場合も, 同様に証明できる. ■

(3) 群 G の任意の元 a に対し

$$aG = G, \quad Ga = G.$$

ただし, aG は $ax (x \in G)$ 全部の集合を示し, Ga は $xa (x \in G)$ 全部の集合を示す. $x \neq y$ ならば, $ax \neq ay$ となるから, aG の元の個数は G の元の個数と等しい. $aG \subset G$ であるが, 元の個数を比較して $aG = G$ となることが分かる. 同様にして $Ga = G$ となる. 性質 (2) で, $ax = b$ となる x が存在することは, $aG = G$ と同値であり, $ya = b$ となる y が存在することは, $Ga = G$ と同値である.

5) 東郷 [T 2], p. 6. 近藤 [K 1], pp. 3-4.

(4) 群 G では $xx=x$ となる元 x は単位元だけである. この元 x を冪等元 (idempotent element) という.

(5) 群 G の元 x, y に対し,

$$(x^{-1})^{-1}=x, \quad (xy)^{-1}=y^{-1}x^{-1} \quad (2.6)$$

証明 x^{-1} を元とすれば, x^{-1} の逆元は x である. よって, $(x^{-1})^{-1}=x$.

つきに, $x^{-1}x=xx^{-1}=e$ と

$$(xy)(y^{-1}x^{-1})=x(yy^{-1})x^{-1}=xex^{-1}=xx^{-1}=e, \quad (y^{-1}x^{-1})(xy)=e$$

から $(xy)^{-1}=y^{-1}x^{-1}$ となる. ■

一般に群 G の元

$$(x_1x_2\cdots x_n)^{-1}=x_n^{-1}x_{n-1}^{-1}\cdots x_1^{-1}.$$

(6) x を群 G の元とすると, 負の整数 n に対して $x^n=(x^{-1})^{|n|}$ と定めると, 式(2.2)はすべての整数 m, n に対して成り立つ⁶⁾.

群 G を, その元の個数が有限のとき, 有限群 (finite group), 無限のとき, 無限群 (infinite group) という. $G=\{e\}$ を自明な群 (trivial group) といい, e と略記することがある. 有限群 G の元の個数を G の位数 (order) といって, $|G|$ で表す.

群 G は可換な半群のとき可換群またはアーベル群 (abelian group) という. アーベル群における演算を表すのに, 乗法の代りに加法 $(x, y) \mapsto x+y$ を用いることが多い. このとき G を加法群 (additive group) という. 単位元を零元 (zero element) といい, 0 で表し, x の逆元を $-x$ で表す. これに対し, 群の演算として乗法を用いたとき乗法群 (multiplicative group) といい, 単位元を 1 で表すこともある⁷⁾.

3. 群 の 例

a 数 と 行 列

例 3.1 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は加法群である. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ から 0 を除いた集合をそ

6) 浅野 [A 5], pp. 9—10. 東郷 [T 2], p. 6.

7) 東郷 [T 2], p. 7. 松坂 [M 1], pp. 46—7. 鈴木 [S 4], pp. 5—6.

それぞれ Q^*, R^*, C^* で表せば, Q^*, R^*, C^* は乗法群である.

例 3.2 絶対値が 1 である複素数の全体は, 乗法に関して群を作る.

証明 絶対値が 1 である任意の複素数は, 極形式 (polar form) で $\alpha = \cos x + i \sin x$ と書けるから, 他に G の元 $\beta = \cos y + i \sin y$ をとると,

$$\alpha\beta = \cos(x+y) + i \sin(x+y), \quad |\alpha\beta| = 1.$$

よって, 積もまた G の元となる.

さらに, $r \in G$ をとれば, 結合法則

$$(\alpha\beta)r = \cos(x+y+z) + i \sin(x+y+z) = \alpha(\beta r)$$

が成り立つ. $1 = \cos 0 + i \sin 0$ は単位元であり, 元 α に対し, G の元

$$\beta = \cos(-x) + i \sin(-x) = \cos x - i \sin x$$

を考えると, $\alpha\beta = 1$. よって, $\beta = \alpha^{-1}$ である. ■

例 3.3 1 の n 乗根 (n -th radical root) ($n \in \mathbb{N}$) の全体は, 次のような乗法に関する位数 n の群を作る. すなわち,

$$G = \left\{ \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \right\} \quad k=0, 1, 2, \dots, n-1.$$

証明 G の任意の 2 元を

$$a = \cos \frac{2p\pi}{n} + i \sin \frac{2p\pi}{n}, \quad b = \cos \frac{2q\pi}{n} + i \sin \frac{2q\pi}{n} \quad 0 \leq p, q \leq n-1$$

するとき,

$$ab = \cos \frac{2(p+q)\pi}{n} + i \sin \frac{2(p+q)\pi}{n} = \cos \frac{2r\pi}{n} + i \sin \frac{2r\pi}{n}$$

$$p+q = nt + r, \quad t: \text{整数} \quad 0 \leq r < n-1$$

となり, $ab \in G$.

結合法則は上の積の右辺の形から明らかに成りたち, 単位元は 1.

$\forall a \in G$ として, $a = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$ に対し, G の元 $b = \cos \frac{2(n-k)\pi}{n} + i \sin \frac{2(n-k)\pi}{n}$ をとると, $ab = ba = 1$. よって, b は a の逆元である. ■

1 の n 乗根の全体は次のようにも表せる.

$$G = [1, z, z^2, \dots, z^{n-1}] \quad \left(z = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \right).$$

特に $n=2$ のとき $\{1, -1\}$, $n=4$ のとき $\{1, i, -1, -i\}$ となる.

例 3.4 $\mathbf{R}$ 上の n 次正則行列 (regular matrix) 全体の集合は, 行列の乗法に関して群をなす.

証明 2つの n 次の行列の積もまた n 次の行列で, 積について結合法則が成り立つ. 単位元は n 次の単位行列 E である. なお, 正則な行列 A に対しては同次なその逆行列 A^{-1} が存在し, $AA^{-1} = A^{-1}A = E$, この両辺の行列式をとると $|AA^{-1}| = |A||A^{-1}| = |E| = 1$. 故に $|A^{-1}| \neq 0$. よって, A^{-1} もまた G の元である. ■

この行列の全体を $\mathbf{R}$ 上の一般線形群 (general linear group) といって, $GL(n, \mathbf{R})$ で表す. 特に行列式が 1 である行列全体の作る群を, $\mathbf{R}$ 上の特殊線形群 (special linear group) といって, $SL(n, \mathbf{R})$ で表す.

例 3.5 $\mathbf{R}$ 上の n 次直交行列 (orthogonal matrix) の全体は, 行列の乗法に関して群を作る.

証明 $\forall R, T \in G$ に対し

$$(RT)'RT = T'R'RT = T'T = E.$$

故に積もまた直交行列である. 行列の積については結合法則が明らかに成り立ち, 単位行列は直交行列であり, これが単位元をなす. 他方, 直交行列の性質から $\forall R \in G$ に対し R' はその逆元である¹⁾. ■

b 群表

有限群を $G = \{a_0, a_1, \dots, a_{n-1}\}$ とする. $a_i a_j = a_k$ ($i, j, k = 0, 1, \dots, n-1$) になるとき, 元 a_i の第 i 行と元 a_j の第 j 列の交点に元 a_k とおいて作った行列を G の群表 ((group table) 或いは乗積表 (multiplication table) という.

例 3.6 Klein の 4 元群 (Klein's four-group) を以下に説明しよう. 位

1) 渡辺 [W], pp. 9—13. 東郷 [T2], p. 7. 近藤 [K1], pp. 5—6. 古屋 [F3], p. 59, 88.

数 4 の可換群を $G = \{a_0, a_1, a_2, a_3\}$ とし, その群表を第 1 表に示す.

表を式に変換すれば,

$$a_0 a_0 = a_0 \quad a_1 a_2 = a_2 a_1 = a_3$$

$$a_0 a_1 = a_1 a_0 = a_1 \quad a_1 a_3 = a_3 a_1 = a_2$$

$$a_0 a_2 = a_2 a_0 = a_2 \quad a_2 a_2 = a_0$$

$$a_0 a_3 = a_3 a_0 = a_3 \quad a_2 a_3 = a_3 a_2 = a_1$$

$$a_1 a_1 = a_0 \quad a_3 a_3 = a_0.$$

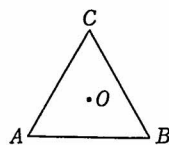
	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_0	a_3	a_2
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_2	a_1	a_0

第 1 表 Klein の 4 元群

この乗法が, 結合法則と交換法則をみたすことは容易に確かめられる. また, 群の任意の元の演算の結果は群の元である. a_0 は単位元であるし, $a_0 a_0 = a_0$, $a_1 a_1 = a_0$, $a_2 a_2 = a_0$, $a_3 a_3 = a_0$ の 4 式をみても, 各元がそれ自身の逆元になっていることが分かる.

第 1 表のように, 群表の対角線上のすべての元が単位元になっているとき, この表は正規 (normal) であるという²⁾.

例 3.7 ユークリッド空間で, 2 点間の距離をかえない点変換を合同変換 (congruent transformation) という. 合同変換の特殊な場合の 1 つに回転 (rotation) がある. それは定点 O のまわりの回転移動であって, 回転の全体は群を作る. これを O を中心とする回転群 (rotation group) と



第 1 図 正三角形

いう. 正三角形 ABC をとり, その中心 O のまわりの, 例えば時計の針と反対の方向へのあらゆる回転を考えよう (第 1 図). この場合, 2 つの回転が, 360° の整数倍だけ異なる場合には, それらは同じものとする.

三角形のあらゆる回転のうち, 三角形をそれ自身に移すのは, 次の 3 つの場合だけである. すなわち, 120° の回転, 240° の回転および三角形のすべての頂点を動かさず, 従って, そのすべての辺をそれ自身に移す零回転

2) Alexandroff [A 3], pp. 22—3. 渡辺 [W], p. 5. 浅野 [A 5], p. 51.

である。2つの回転の積とは、回転をつづけて行うことである。120°の回転と240°の回転の積は360°の回転、すなわち零回転となり、240°の回転を2回行えば120°の回転となる。

いま、零回転を a_0 、120°の回転を a_1 、240°の回転を a_2 で表すと、次の関係が得られる。

$$a_0 a_0 = a_0$$

$$a_1 a_1 = a_2$$

$$a_0 a_1 = a_1 a_0 = a_1$$

$$a_1 a_2 = a_2 a_1 = a_0$$

$$a_0 a_2 = a_2 a_0 = a_2$$

$$a_2 a_2 = a_1.$$

	a_0	a_1	a_2
a_0	a_0	a_1	a_2
a_1	a_1	a_2	a_0
a_2	a_2	a_0	a_1

第2表 正三角形の
回転群表

上の演算が、結合法則と交換法則をみたすことは容易に確かめ得る。任意の回転 a に対し、 $a + a_0 = a_0 + a = a$ となる零回転 a_0 が存在することも明らか。最後に、これら3つの回転にはそれぞれの逆回転が存在する。実際、 $a_0 + a_0 = a_0$ だから、 $-a_0 = a_0$ 、また、 $a_1 + a_2 = a_2 + a_1 = a_0$ だから $-a_1 = a_2$ 、 $-a_2 = a_1$ である。よって、これらの回転は回転群を作る。

以上の回転の積の規則を第2表のように、群表にまとめることができる³⁾。

例 3.8 正方形 $ABCD$ をとり、その中心のまわりの回転で、正方形をそれ自身に移すものを考える。この場合にも、360°の整数倍だけ異なる2つの回転はすべて同じものとする。従って、頂点が4個だから、全部で4つの回転があることになる。すなわち、零回転、90°、180°、270°、それぞれの回転がある。これらの回転を、それぞれ a_0, a_1, a_2, a_3 で表そう。この場合の群表を第3表で示す⁴⁾。

	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_2	a_3	a_0
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_0	a_1	a_2

第3表 正方形回転群表

3) Alexandroff [A 3], pp. 20—2. Allen [A 4], pp. 165—6. 浅野 [A 5], p. 18. 渡辺 [W], pp. 16—7.

4) Alexandroff [A 3], p. 24.

4. 置 換 群

空でない集合 M の自己全単射を、 M における変換 (transformation) と言う。 M における変換の全体は、写像の合成演算として群をなす。この群を M における変換群 (transformation group) という。特に M が有限群の場合、 M における変換、変換群をそれぞれ置換、置換群 (permutation group) という。

a 対 称 群

σ を集合 $M = \{1, 2, \dots, n\}$ の任意の置換とすると、

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \quad (4.1)$$

のように表す。置換は、各各の k に対して $\sigma(k)$ の値が分かれば、完全にきまる。それ故、(4.1) の上の行の数がどういう順に書いてあるかということとは重要ではない。

2つの置換 σ, τ の合成を通常 $\tau\sigma$ と書き、これを乗法、積と呼ぶ。積 $\tau\sigma$ を左合成という。しかし、同じ積を $\sigma\tau$ 、すなわち右合成で表すことも少なくない。2つの置換 σ, τ の積は集合 M に先ず置換 σ を施し、さらに、それに引き続いて、置換 τ を施すことを意味する¹⁾。

命題 4.1 集合 M 上の置換全体には結合法則が成り立つ。

証明 $\sigma^{(1)}$ で i_1 が k_1 で置き換えられ、

$\sigma^{(2)}$ で k_1 が l_1 で置き換えられ、

$\sigma^{(3)}$ で l_1 が m_1 で置き換えられる

とすると、 $\sigma^{(2)}\sigma^{(1)}$ で i_1 が l_1 で置き換えられるから、 $\sigma^{(3)}(\sigma^{(2)}\sigma^{(1)})$ では i_1 が m_1 で置き換えられる。同様に、 $\sigma^{(3)}\sigma^{(2)}$ で k_1 が m_1 で置き換えられるから、 $(\sigma^{(3)}\sigma^{(2)})\sigma^{(1)}$ では i_1 が m_1 で置き換えられる。従って、

$$\sigma^{(3)}(\sigma^{(2)}\sigma^{(1)}) = (\sigma^{(3)}\sigma^{(2)})\sigma^{(1)} \quad \blacksquare$$

1) Alexandroff [A 3], pp. 48—9.

2) Alexandroff [A 3], p. 43.

集合 M の恒等写像を恒等置換 (identity permututation) と呼ぶ, 各置換 σ にはそれぞれ逆写像, すなわち, 逆置換 σ^{-1} が対応する. σ が (4.1) の形をとるならば,

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}. \quad (4.2)$$

位数 n をもつ集合 M 上の置換の全体は群を作ることが分かった. この群を M 上の n 次対称群 (symmetric group of order n) といって, $S_n(M)$, または S_n で表す. 対称群の位数 $|S_n| = n!$. 対称群は可換ではない³⁾.

例 4.1 $M = \{1, 2, 3\}$ の上の全置換を次のようにしする.

$$\begin{aligned} \sigma_0 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & \sigma_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \\ \sigma_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & \sigma_4 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\ \sigma_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} & \sigma_5 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}. \end{aligned}$$

置換の積, 例えば $\sigma_5\sigma_2$ は次のように求める.

$$\begin{aligned} \sigma_5\sigma_2 &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 1 & 3 \\ 2 & 3 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_3. \end{aligned}$$

	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5
σ_0	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	σ_0	σ_3	σ_2	σ_5	σ_4
σ_2	σ_2	σ_4	σ_0	σ_5	σ_1	σ_3
σ_3	σ_3	σ_5	σ_1	σ_4	σ_0	σ_2
σ_4	σ_4	σ_2	σ_5	σ_0	σ_3	σ_1
σ_5	σ_5	σ_3	σ_4	σ_1	σ_2	σ_0

第 4 表 3 次対称群表

与えられた置換に対する逆置換は, 与えられた置換によって動かされたすべての数字を, もとの場所にもどす置換である. 例えば,

$$\begin{aligned} \sigma_3^{-1} &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_4. \end{aligned}$$

3 次の対称群表を第 4 表で示す. 群表

3) 松坂 [M 1], p. 48. 奥川 [O 1], pp. 25—6. 浅野 [A 5], pp. 16—7. 東郷 [T 2], p. 8.

からある置換に対する逆置換を求めるには、左端にその置換がある行をとり、この行で元 σ_0 を探せばよい。すると、その列の上端に、与えられた置換に対する逆置換が出ている。すべての置換の逆置換は次の通りである⁴⁾。

$$\begin{array}{ll} p_0^{-1}=p_0 & p_3^{-1}=p_4 \\ p_1^{-1}=p_1 & p_4^{-1}=p_3 \\ p_2^{-1}=p_2 & p_5^{-1}=p_5. \end{array}$$

b 交代群

集合 $M=\{1, 2, \dots, n\}$ において $i_1, i_2, \dots, i_r$ ($2 \leq r \leq n$) が M の相異なる元で、 M の置換が

$$\begin{aligned} \sigma(i_1) &= i_2, \dots, \sigma(i_{r-1}) = i_r, \quad \sigma(i_r) = i_1, \\ \sigma(k) &= k \quad (\forall k \neq i_1, i_2, \dots, i_r) \end{aligned}$$

のとき、置換 σ を長さ r の巡回置換 (cycle, cyclic permutation) といって、 $(i_1 i_2 \dots i_r)$ で表す。ここで $\sigma(k) = k$ は省略される。すなわち、

$$\sigma = \begin{pmatrix} i_1 & i_2 & \dots & i_{r-1} & i_r \\ i_2 & i_3 & \dots & i_r & i_1 \end{pmatrix} = (i_1 i_2 \dots i_r).$$

$(i_1 i_2 \dots i_r)$ は i_2 から始めて $(i_i i_{i+1} \dots i_r, i_1 \dots i_{i-1})$ と書いても、同じ巡回置換である。特に、長さ 2 の巡回置換を互換 (transposition) という。すなわち、互換 (jk) は

$$(jk) = \begin{pmatrix} j & k \\ k & j \end{pmatrix}.$$

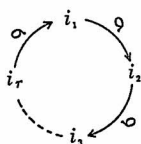
σ を任意の置換とすると、 $i \in M$ に対して、 $\sigma^r(i) = i$ なる最小の r をとり、 $\sigma^m(i) = i_{m+1}$ ($1 \leq m \leq r$) とおくと、 σ は $i_1, i_2, \dots, i_r$ の順に巡回して、巡回置換 $(i_1 i_2 \dots i_r)$ が得られる (第 2 図参照)。

4) Alexandroff [A 3], pp. 39—44.

n 個の文字の対称式とは、 S_n の任意の置換で変わらない多項式のことである。例えば、式 $x_1 + x_2 + x_3$ は、置換

$$b = \begin{pmatrix} 1 & 2 & 3 \\ a_1 & a_2 & a_3 \end{pmatrix}$$

による任意の置換 $a_i = \sigma(i)$ ($i=1, 2, 3$) のもとらす $x_{a_1} + x_{a_2} + x_{a_3}$ と一致するから、それは対称式である。同様に、 $x_1 x_2 + x_2 x_3 + x_3 x_1$, $x_1 + x_2 + x_3$ も対称式である (Alexandroff [A 3], p. 47)。



第2図 巡回

この巡回の中に現れない $j_1 \in M$ をとって、同様に巡回置換 $(j_1 j_2 \cdots j_s)$ が得られる。これを続けて、

$$\sigma = (k_1 k_2 \cdots k_t) \cdots (j_1 j_2 \cdots j_s) (i_1 i_2 \cdots i_r). \quad (4.3)$$

ここで長さ1の巡回置換は省略される⁵⁾。

例 4.2 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 7 & 1 & 6 & 2 \end{pmatrix}$ が与えられたと

き、数字の順次移送を分析すれば、

$$1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 1: \sigma(1)=3, \sigma^2(1)=5, \sigma^3(1)=1,$$

$$2 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 2: \sigma(2)=4, \sigma^2(2)=7, \sigma^3(2)=2,$$

$$6 \xrightarrow{\sigma} 6.$$

よって、

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

巡回置換 $(i_1 i_2 \cdots i_r)$ は

$$(i_1 i_2 \cdots i_r) = (i_1 i_r)(i_1 i_{r-1}) \cdots (i_1 i_2) \quad (4.4)$$

と書けるから、任意の置換は互換の積として表せる。

各置換 σ は幾通りにも互換表示できるが、その因子の個数が偶数になるか、奇数になるかは、各 σ によっていずれか一方にきまる。それぞれの場合、 σ を偶置換 (even permutation)、奇置換 (odd permutation) という。

命題 4.2 置換 $\sigma \in S_n$ を $\Delta = \prod_{1 \leq i < j \leq n} (X_i - X_j)$ に施せば、 $\sigma(\Delta) = (-1)^r \Delta$ となる。ただし $\sigma = \tau_r \cdots \tau_2 \tau_1$ ($\tau_1, \tau_2, \dots, \tau_r$: 互換) とする⁶⁾。

証明 Δ に対する置換は、

$$\sigma(\Delta) = \tau_r(\cdots(\tau_2(\tau_1(\Delta)))\cdots).$$

5) 永尾 [N 1], pp. 30—4. 東郷 [T 2], p. 8.

6) 奥川 [O 1], p. 27.

7) Δ は文字 $X_1, X_2, \dots, X_n$ の差積 (difference-product, Differente) であって、整係数の多項式となる。

置換の実行に先立ち A を分析すれば, A は次の形の因子全体の積に等しい.

$$(i) \quad X_i - X_j \quad (1 \leq i < j \leq n : i \neq p, q : j \neq p, q).$$

$$(ii) \quad (X_i - X_p)(X_i - X_q) \quad (1 \leq i \leq p).$$

$$(iv) \quad (X_p - X_k)(X_k - X_q) \quad (p < k < q).$$

$$(v) \quad (X_p - X_j)(X_q - X_j) \quad (q < j \leq n).$$

$$(vi) \quad X_p - X_q.$$

いま, 任意の互換を $\tau = (pq)$ ($1 \leq p < q \leq n$) とし, これらに τ を作用させるとき, 因子(i)–(v)はいずれも結局は不変に終わり, 因子(vi)だけが $-(X_p - X_q)$ になり, $\tau(A) = -A$ となる. 従って,

$$\sigma(A) = \tau, (\dots(\tau_2(\tau_1(A)))\dots) = (-1)^r A. \blacksquare$$

以上により, 置換 σ の符号 (signum, sign, signature) が次のように定義される⁸⁾.

$$\operatorname{sgn} \sigma = \varepsilon(\sigma) = \begin{cases} +1 & (\sigma: \text{偶置換}) \\ -1 & (\sigma: \text{奇置換}). \end{cases}$$

位数 n なる集合 M に対する, 偶置換の積は偶置換であり, 偶置換の積には結合法則が成り立つ. 恒等置換は偶置換であるから単位元となる. 最後に, 互換 τ に対しては明らかに $\tau^{-1} = \tau$ であるから, 偶置換の逆置換はまた偶置換である. 故に, 偶置換の全体は群をなす. これを n 次交代群 (alternating group of order n) といい, A_n で表す⁹⁾.

命題 4.3 対称群 S_n のうち偶置換と奇置換は同数である.

証明 相異なる偶置換の全体を $\sigma_1, \sigma_2, \dots, \sigma_N$ とする. いま, 1つの互換 τ をとると, $\tau\sigma_1, \tau\sigma_2, \dots, \tau\sigma_N$ は奇置換となり, いずれも相異なる. 他方, 任意の奇置換 ω に対し, $\tau\omega$ は偶置換になるから, どれかの番号 i につい

8) 奥川 [O 1], pp. 27—8. 東郷 [T 2], p. 9. 古屋 [F 3], pp. 29—31. 福井 [F 2], pp. 1—5. 浅野 [A 5], pp. 26—9. Alexandroff [A 3], pp. 48—53. 松坂 [M 2], pp. 167—71.

9) Alexandroff [A 3], pp. 52—4. 矢ヶ部 [Y 1], pp. 255—69.

A は互換 τ により $\tau A = -A$ となるので, 交代式, 詳しくは最簡交代式 (simplest alternating expression) と呼ばれる. なお, A^2 は対称式となる.

て $\tau\omega=\sigma_i$ となる. これに τ を左乗して $\omega=\tau\sigma_i$ が得られるから, $\tau\sigma_1, \tau\sigma_2, \dots, \tau\sigma_N$ は相異なる奇置換の全部である. よって, $|A_n|=|\tau A_n|$. ■

$|S_n|=n!$ であり, $S_n=A_n\oplus\tau A_n$ だから, 上の命題により $|A_n|=n!/2^{10)}$. $\sigma_1, \sigma_2 \in S_n$ に対して

$$(\sigma_1\sigma_2)A=\sigma_1(\sigma_2A)=\varepsilon(\sigma_2)\sigma_1A=\varepsilon(\sigma_1)\varepsilon(\sigma_2)A.$$

故に,

$$\varepsilon(\sigma_1\sigma_2)=\varepsilon(\sigma_1)\varepsilon(\sigma_2).$$

5. 部 分 群

a 部 分 群

群 G の部分集合 H が, それ自身 G における演算によって群をなすとき, H を G の部分群 (subgroup) という. 特に G と異なる G の部分群を G の真部分群 (proper subgroup) という.

例 5.1 加法群 $\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$, 乗法群 $\mathbf{Q}^* \subset \mathbf{R}^* \subset \mathbf{C}^*$ について, 各々はその後にくる群の真部分群である.

例 5.2 $SL(n, \mathbf{R})$ は $GL(n, \mathbf{R})$ の部分群, A_n は S_n の部分群である¹⁾.

例 5.3 対称群 S_3 の位数 2 の部分集合は, すべて $\{p_0, p_i\}$ ($i=1, 2, \dots, 5$) という形をしている. しかし, S_3 の群表 (第 4 表) を検討すれば, 全部で ${}_3C_1=5$ 個の部分集合のうち, $\{p_0, p_1\}$, $\{p_0, p_2\}$ および $\{p_0, p_3\}$ だけが部分群である. 同様にして, 位数 3 の部分群は, 全部で ${}_3C_2=10$ 個の部分集合のうち, $\{p_0, p_3, p_4\}$ だけであることが分かる. 位数 4 の部分群を確かめるには, p_0 を含む 4 つの元からなる ${}_3C_3=10$ 個の部分集合, 位数 5 の場合を確かめるには, p_0 を含む 5 つの元からなる ${}_3C_4=5$ 個の部分集合の全部について調べればよい. しかし, S_3 には位数 4 および 5 の部分群は存在しない (その理由は 4 と 5 が $|S_3|=6$ の約数でないこと, つまり,

10) 奥川 [O 1], p. 28. Alexandroff [A 3], p. 54. 東郷 [T 2], p. 9. 鈴木 [S 4], pp. 283—5.

1) 東郷 [T 2], p. 9.

Lagrange の定理による)²⁾.

定理 5.1 群 G の空でない部分集合 H が G の部分群であるための必要十分条件は,

- a) $x, y \in H \Rightarrow xy \in H$,
- b) $x \in H \Rightarrow x^{-1} \in H$.

証明 H を G の部分群, $x, y \in H$ とする. xy は H における x, y の積と同じであるから $xy \in H$. H の単位元を e' とすると, $e'e' = e'$. G における e' の逆元を左から掛けて $e' = e$. 従って, x^{-1} は H における x の逆元と一致して $x^{-1} \in H$.

逆に a), b) を仮定する. a) によって G における演算は H における演算をひきおこす. H は明らかに結合法則をみたす. $H \neq \emptyset$ だから H の元 x を選ぶと, b) によって $x^{-1} \in H$. 従って, a) により $e = xx^{-1} \in H$. 故に e は単位元である. H が群をなすことが分かった³⁾. ■

定理 5.1 をさらに進めて, つぎの効率化した定理を得る.

定理 5.2 群 G の空でない部分集合 H が G の部分群であるための必要十分条件は,

- c) $x, y \in H \Rightarrow xy^{-1} \in H$.

証明 先ず c) が十分条件であることを証明する. $x \in H \Rightarrow e = xx^{-1} \in H$. よって, $x^{-1} = ex^{-1} \in H$. $x, y \in H \Rightarrow y^{-1} \in H$. 従って $xy = x(y^{-1})^{-1} \in H$. 故に H は定理 5.1 の条件をみたす.

c) が必要条件であることは明らか⁴⁾. ■

群 G の部分集合 A, B に対して, $AB = \{xy | x \in A, y \in B\}$, $A^{-1}\{x^{-1} | x \in A\}$ とする. 特に $A = \{x\}$ または $B = \{y\}$ のとき, AB をそれぞれ xB, Ay で表す. この記法によれば, 先の条件 a), b), c) はそれぞれ $HH \subset H$, $H^{-1} \subset H$, $HH^{-1} \subset H$ となる. $H^{-1} \subset H$ は $H^{-1} = H$ と同値である. また H

2) Alexandroff [A 3], p. 45—6.

3) 東郷 [T 2], pp. 9—10.

4) 東郷 [T 2], p. 10. 浅野 [A 5], p. 37. 都筑 [T 5], p. 22. 松坂 [M 1], pp. 51—2.

が G の部分群ならば $HH=H$, $H^{-1}=H$.

群 G の部分群の任意の集合 $\{H_\lambda | \lambda \in A\}$ に対し, $\bigcap_\lambda H_\lambda$ は G の部分群である. 実際, $\bigcap_\lambda H_\lambda$ は e を含み, 条件 c) をみたす⁵⁾.

b 生成系

S を群 G の空でない部分集合とする. S を含む G の部分群は存在する, 例えば, G 自身である. S を含む G のすべての部分群の共通部分は, S を含む最小の部分群である. これを S の生成する部分群といって, $\langle S \rangle$ で表す. S をその生成系 (generator system) という. このとき, 集合 S は $x_1 x_2 \cdots x_n$ ($n \in N$, $x_i \in S$ または $x_i^{-1} \in S$) の形の元全体から成る集合と一致する. 群 G の部分集合 $S_\lambda (\lambda \in A)$ が与えられたときは, $\langle S_\lambda (\lambda \in A) \rangle$, $\langle S_1, S_2, \dots, S_n \rangle$ または $\langle \bigcup_{i=1}^n S_i \rangle$ で表す. 集合の元から生成される部分群と考えれば $\langle x_1, x_2, \dots, x_n \rangle = \langle \{x_1, x_2, \dots, x_n\} \rangle$ で表す.

ある群のすべての元をとれば, それはその群の自明な生成系となっている. 従って, どんな群にも生成系は存在する⁶⁾.

例 5.4 直交座標系平面における座標 x, y が共に整数であるとする. 点 $P(x, y)$ 全体の集合を G で表す. 次の加法を定める. すなわち, $P_1(x_1, y_1)$, $P_2(x_2, y_2)$ の和とは, $x_3 = x_1 + x_2$, $y_3 = y_1 + y_2$ を座標とする点 $P_3(x_3, y_3)$ であるとする. この加法の定義により集合 G はアーベル群になる. この群の生成系は 2 点 $(0, 1)$, $(1, 0)$ である.

加法群としての複素整数の生成系も上と同様である⁷⁾.

c 巡回群

各元が特定の元 a の累乗 (巾, power) になる群を, a から生成される巡回群 (cyclic group) といい, $\langle a \rangle$ で表し, a を巡回群の生成元 (generator) という. 群 G の元 a から生成される $\langle a \rangle$ は, G の元の集合であって, 巡回部分群と呼ばれる⁸⁾.

5) 東郷 [T 2], p. 10. 都筑 [T 5], pp. 23—4.

6) 東郷 [T 2], p. 10. 鈴木 [S 4], pp. 10—1.

7) Alexandroff [A 3], pp. 77—8.

8) Alexandroff [A 3], p. 70. 浅野 [A 5], p. 20.

$$a^i a^k = a^k a^i = a^{i+k}$$

であるから、巡回群はアーベル群である。

i と j が異なるとき、 a^i と a^j が常に異なるならば、この群は

$$\dots, a^{-2}, a^{-1}, a^0 = e, a, a^2, \dots \quad (5.1)$$

からできる無限巡回群である。そうでない場合には

$$a^h = a^k \quad (h > k)$$

となる h, k が存在する。両辺に a^{-k} を右乗すれば

$$a^{h-k} = e \quad (h-k > 0).$$

いま、 n を $a^n = e$ となる最小の自然数とすれば、元

$$a^0 = e, a, a^2, \dots, a^{n-1} \quad (5.2)$$

はすべて相異なる。

証明 仮りに $a^p = a^q$ $0 \leq p < q \leq n-1$ であるとすると、

$$a^{q-p} = e \quad 0 < q-p \leq n-1.$$

しかるに、 n は $a^n = e$ となる最小の自然数であるから、 $a^p \neq a^q$. ■

i を任意の自然数とすると、整数の除法定理 (division theorem) によって、

$$i = nq + r \quad 0 \leq r < n$$

となる正整数 q, r が存在するから、

$$a^i = a^{nq+r} = (a^n)^q a^r = e a^r = a^r$$

となる。特に $a^i = e$ ならば、 $r=0$ となり、 i は n で割り切れる⁹⁾。

a^i は $e, a, a^2, \dots, a^{n-1}$ のどれかと一致し、これらの n 個の元が位数 n の有限群を作る。この位数を元 a の位数という、位数 n の巡回群を C_n で表す。

9) 松坂 [M 1], p. 5. 浅野 [A 5], pp. 20—1. Alexandroff [A 3], p. 72.

i が負のときも、 $n > 0$ で割ったときの余り r は矢張り正となる。それには次のようにする。 $-i$ は正だから、次の形に表される。

$$-i = q'n + r' \quad q' \geq 0, \quad 0 \leq r' < n$$

すると、

$$i = -q'n - r' = -(q'+1)n + (n-r') \quad 0 \leq n-r' < n.$$

このとき、 $-(q'+1)$ を、負の整数 i を正整数 n で割ったときの商、正整数 $n-r'$ をこのときの余りという。

元 a の位数が n ならば、 $\langle a \rangle$ で (5.1) のように元の無限の列が並んでいるとしても、その全体は (5.2) の無限のくり返しになる¹⁰⁾。実際に計算してみると、

(5.1)の右方に位置する数

$$a^{n+1} = a^n a = a$$

$$a^{n+2} = a^n a^2 = a^2$$

$$\vdots$$

$$a^{2n-1} = a^n a^{n-1} = a^{n-1}$$

$$a^{2n} = e$$

$$a^{2n+1} = a$$

$$\vdots$$

(5.1)の左方に位置する数

$$a^{-1} = a^n a^{-1} = a^{n-1}$$

$$a^{-2} = a^n a^{-2} = a^{n-2}$$

$$\vdots$$

$$a^{-(n-1)} = a^n a^{-(n-1)} = a$$

$$a^{-n} = a^n a^{-n} = a^0 = e$$

$$\vdots$$

	a^0	a	a^2	a^3	$\dots$	a^{n-2}	a^{n-1}
a^0	a^0	a	a^2	a^3	$\dots$	a^{n-2}	a^{n-1}
a	a	a^2	a^3	a^4	$\dots$	a^{n-1}	a^0
a^2	a^2	a^3	a^4	a^5	$\dots$	a^0	a
a^3	a^3	a^4	a^5	a^6	$\dots$	a	a^2
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
a^{n-2}	a^{n-2}	a^{n-1}	a^0	a	$\dots$	a^{n-4}	a^{n-3}
a^{n-1}	a^{n-1}	a^0	a	a^2	$\dots$	a^{n-3}	a^{n-2}

第5表 C_n 群表

例 5.5 n を任意の自然数とすると、位数 n の巡回群は存在する。複素数 $z = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ をとれば、 $z^n = 1$ で $1, z, \dots, z^{n-1}$ が位数 n の巡回群を作るからである¹¹⁾。

位数 n の巡回群表を第5表に示す。この表は実は第2表、第3表と同じ性質をもっている。ということは、巡回群と回転群

は同型 (isomorphic) であるということである¹²⁾。

命題 5.3 巡回群 G の部分群 H は巡回群である。

証明 $G = \langle x \rangle$, $H \neq \{e\}$ とする。 $x^n \in H$ なる最小の正整数 n をとる。 $x^m \in H$ とすると、 $m = nq + r$ $0 \leq r < n$ なる整数 q, r がある。 $x^m = (x^n)^q x^r$ 。従って、 $x^r = (x^n)^{-q} x^m \in H$ 。 n の選び方から $r = 0$ 。従って $m = nq$ 。すな

10) Alexandroff [A 3], p. 73.

11) 浅野 [A 5], p. 21.

12) Alexandroff [A 3], p. 75.

わち $x^m = (x^n)^q$. 故に $H = \langle x^n \rangle^{13)}$. ■

例 5.6 $x_1, x_2, \dots, x_n \in \mathbb{Z}$ の最大公約数 (greatest common divisor) を $\gcd(x_1, x_2, \dots, x_n)$ で表す. 加法群 $\mathbb{Z}$ は 1 を生成元とする巡回群である. $H = \langle x_1, x_2, \dots, x_n \rangle$ とすると, 命題 5.3 によって $H = \langle d \rangle$. このとき $\gcd(x_1, x_2, \dots, x_n) = d$ で $\sum_{i=1}^n m_i x_i$ なる $m_i \in \mathbb{Z}$ $1 \leq i \leq n$ がある.

実際, 各 x_i は H の元として d の倍数である. 故に d は $x_1, x_2, \dots, x_n$ の公約数である. d' を $x_1, x_2, \dots, x_n$ の任意の公約数とすると, $x_i = y_i d'$ $y_i \in \mathbb{Z}$ ($1 \leq i \leq n$). $H = \left\{ \sum_{i=1}^n l_i x_i \mid l_i \in \mathbb{Z} \ (1 \leq i \leq n) \right\}$ であるから,

$$d = \sum_{i=1}^n m_i x_i = \left(\sum_{i=1}^n m_i y_i \right) d'.$$

すなわち d' は d の約数である. 故に $\gcd(x_1, x_2, \dots, x_n) = d^{14)}$.

巡回群 $C_n = \langle a \rangle$ の生成元は 1 つだけとは限らない. それは全部で

$$\varphi(r) \ (1 \leq r \leq n-1, \ r \text{ は } n \text{ と互いに素})$$

である. 位数 n の巡回群の生成元の数は $1, 2, \dots, n$ のうちで, n と素であるものの個数 $\varphi(n)$ に等しい, 自然数の上で定義された関数 φ を Euler 関数という¹⁵⁾.

d 中心化群

群 G の部分集合 M の各元 c ($\forall c \in M$) と可換な G の元全部の集合 $\{x \in G \mid \forall c \in M, cx = xc\}$ は群を作る. これを M の中心化群 (centralizer) といい, $Z_G(M)$ で表す.

証明 $a \in Z(M)$, $b \in Z(M)$ とすれば,

$$ca = ac, \ cb = bc \quad (\forall c \in M).$$

従って,

$$cab = acb = abc \quad (\forall c \in M), \ ab \in Z(M).$$

また, $a \in Z(M)$ ならば, $ca = ac$ ($\forall c \in M$) だから, $a^{-1}c = ca^{-1}$ ($\forall c \in M$)

13) 東郷 [T 2], p. 11. 浅野 [A 5], p. 41.

14) 松坂 [M 1], pp. 9—10. 浅野 [A 5], p. 42. 東郷 [T 2], p. 11.

15) 浅野 [A 5], p. 21. 都筑 [T 5], p. 18.

となり、 $a^{-1} \in Z(M)$ である。故に、 $Z(M)$ は G の部分群を作る。■

特に、 G の中心化群 ($Z(G)$ を G の中心 (center, Zentrum) という。 G の中心は、 G に属するすべての元と個別に可換な元全体からできている。 G の中心に属する元は G の各元と可換だから、互いに可換であり、 G の中心はアーベル群を作る¹⁶⁾。

6. む す び

ささやかな本論文を通じて、数学上重要な作用の体系は群を作っている。或いは、群は数学の対象の所有すべき基本的機能である、ということをかいまみることができた¹⁷⁾。

19世紀前半、Abel, Galois によって築かれた群論は、5次方程式の代数的解法の中で、根の置換の作る群として現われたのが始まりである¹⁸⁾。

その後、合同変換という考え方が拡張されて、幾何学と変換群との関係が明確になり、さらに、Lie による連続群論を通じて、19世紀の終りには数学全般にわたる群の重要性が確立された。その後も群論は急速に進歩したが、特に、最近20年間の有限単純群論の発展振りはまことに目ざましい¹⁹⁾。

各人の群論の探求と理解をまって、各人の群論の応用が可能となる。群論の理解なくして群論の応用をとこなえても、その応用の仕様はない。今日、群論は量子力学、実験計画法、線型経済学などで応用されている。

(1984. 12. 10)

参 考 文 献

秋月康夫

〔A 1〕 軌近代数学の展望，昭年45年。

秋月康夫

〔A 2〕 鈴木通夫共著，高等代数学 I，1970。

16) 東郷 [T 2], p. 11. 浅野 [A 5], pp. 38—9. 鈴木 [S 4], p. 10, pp. 12—3.

1) 秋月 [A 1], pp. 113—4.

2) 矢ヶ部 [Y 1], pp. 6—13. 清水 [S 2], pp. 29—30.

3) 鈴木 [S 4], はしがき。

Alexandroff, P. S.

- [A 3] (translated by Perfect, H. P. and Petersen, G. M.) An introduction to the theory of groups, 1959 (宮本敏夫訳, 群論入門, 1964).

Allen, R. G. D.

- [A 4] Basic mathematics, 1962 (高木秀玄監訳, 経済経営のための基礎数学 上巻, 1963).

浅野啓三

- [A 5] 永尾 汎共著, 群論, 1965.

Birkhoff, G.

- [B] with S. MacLane, A survey of modern algebra, 1941 (奥川光太郎, 辻吉雄訳, 現代代数学概論, 1955).

Fuchs, L.

- [F 1] Abelian group, 1960.

福井常孝

- [F 2] 入江昭二, 前原昭二, 上村外茂男, 宮寺 功, 境正一郎共著, 線型代数学入門, 昭和40年,

古屋 茂

- [F 3] 行列と行列式, 昭和54年.

Hall, M. Jr.

- [H] The theory of groups, 1959.

伊東由文

- [I 1] 初等代数幾何学, 昭和55年.

彌永昌吉

- [I 2] 杉浦光夫共著, 応用数学者のための代数学, 1968.

彌永昌吉

- [I 3] 彌永健一共著, 代数学, 1976.

近藤 武

- [K 1] 群論 I, 1976.

Kurosh, A. G.

- [K 2] General algebra, 1963.

Lang, S,

- [L] Algebraic structure, 1967 (芹沢正三, 大谷正美訳, ラング代数系の構造, 昭和50年).

松坂和夫

- [M 1] 代数系入門, 1976.

松坂和夫

〔M 2〕 線型代数入門, 1980,

永尾 汎

〔N 1〕 群論の基礎, 昭和57年,

中村義作

〔N 2〕 対称図形と群 (数学セミナー 01.84), 1984.

奥川光太郎

〔O 1〕 応用抽象代数学, 昭和49年.

大山 豪

〔O 2〕 有限置換群, 昭和56年.

Pontrjagin, L. C.

〔P〕 Непрерывные Группы, 1954 (柴岡泰光, 杉浦光夫, 宮崎功 訳, 連続群論 上, 1969).

Queysanne, M.

〔Q〕 with Delachet, A, Algèbre moderne (芹沢正三訳, 現代代数学), 1956.

佐武一郎

〔S 1〕 リー群の話, 昭和57年.

清水達雄

〔S 2〕 群 (新初等数学講座, 第6巻, 第3分冊), 昭和31年.

正田健次郎

〔S 3〕 浅野啓三共著, 代数学 I, 1968.

鈴木通夫

〔S 4〕 群論 上, 1977.

淡中忠郎

〔T 1〕 代数学, 昭和36年.

東郷重明

〔T 2〕 代数入門, 昭和58年.

遠山 啓

〔T 3〕 初等整数論, 昭和47年.

都筑俊郎

〔T 4〕 有限群と有限幾何, 1976.

都筑俊郎

〔T 5〕 群論への入門, 昭和58年.

van der Waerden, L.

〔V〕 Moderne algebra, 1937 (銀林 浩訳, 現代代数学 1, 1976).

渡辺哲雄

〔W〕 群論演習，昭和58年．

矢ヶ部巖

〔Y 1〕 ガロアの理論，1983．

山田深雪

〔Y 2〕 半群論入門，昭和51年．