

有限対称系と有限群

ハワイ大学 延沢信雄

結合 $\circ$ を持つ集合 A が次の条件を満たす時, 対称系 (symmetric set) という. (1) $a \circ a = a$, (2) $(a \circ b) \circ b = a$, (3) $(a \circ b) \circ c = (a \circ c) \circ (b \circ c)$. 任意の群 G は $a \circ b = b a^{-1} b$ なる定義により対称系とせられる. 一般にこの結合でせいてなるような群の部分集合は対称系である. 群 G の位数 n なる元のなる集合, また GL_n の中の対称行列のなる集合などはその例である.

対称系 A において, 元 a による右乗法を S_a と表わすと, S_a は位数 n の A の自己同型である. S_a ($a \in A$) で生成された A の自己同型の群を $G(A)$ で, $S_a S_b$ ($a, b \in A$) で生成された $G(A)$ の指数 n の正規部分群を $H(A)$ で表わす. 集合 $S_A = \{S_a \mid a \in A\}$ は対称系 $G(A)$ の部分系 (部分対称系をこうよぶ) で $a \rightarrow S_a$ は A より S_A の上への準同型である. この対応が一対一の時 A は effective という. 以下この文では A は有限で effective な対称系とする. $a \rightarrow S_e S_a$ (e は固定

された一元) は A から $H(A)$ の中への同型写像であることもたしかめられる. A と $H(A)$ との間には密接な関係があり, 一方より他方の構造を論じることが出来る.

1. プーベル対称系とプーベル群

$H(A)$ がプーベル群の時 A をプーベル対称系という. これは A 元 a, b, c に対して $S_a S_b S_c = S_c S_b S_a$ が成立することと同じである. この時 A の二元 a と b に対して, $S_a S_b$ の位数は常に奇数であることを示そう. $S_a S_b$ の位数が $2k$ であると仮定せよ. 任意の元 c に対して, $c(S_a S_b)^k = c$ となる. 何となれば, $d = c(S_a S_b)^k$ とおくと, $S_d = (S_a S_b)^{-k} S_c (S_a S_b)^k = (S_b S_a)^k S_c (S_a S_b)^k = S_c (S_a S_b)^k (S_a S_b)^k = S_c$ となり, $d = c$ となるからである. これは $(S_a S_b)$ の位数が $2k$ という仮定に反する. 次に, 三元 e, a と b に対して, 元 c が存在して $S_a S_e S_b = S_c$ となることを示す. $S_e S_b$ の位数も $2k+1$ とせよ. $I = (S_e S_b)^{2k+1} = (S_e S_b)^k S_e (S_b S_e)^k S_b$ より, $S_b = (S_e S_b)^k S_e (S_b S_e)^k$. 更に, $S_a S_e S_b = (S_a S_e)(S_e S_b)^k S_e (S_b S_e)^k = (S_e S_b)^k S_a (S_b S_e)^k = S_c$. 逆に $c = a(S_b S_e)^k$. また, $S_e S_a$ の位数 m なら $S_a S_e = (S_e S_a)^{m-1} = S_e S_{a'}$ となる元 a' が存在する. 以上より A がプーベルなら, $H(A) = \{S_e S_a \mid a \in A\}$ なることがわかる. 従って $a \rightarrow S_e S_a$ は A と $H(A)$ との同型を与える.

逆に, $H(A) = \{S_e S_a \mid a \in A\}$ なら $H(A)$ はアーベル群であることが次のように分る. $S_e S_a$ と $S_e S_b$ に對して元 C があって, $S_e S_a S_e S_b = S_e S_c$. 逆をとって, $S_b S_e S_a S_e = S_c S_e$. S_e を右と左から乗じて, $S_e S_b S_e S_a = S_e S_c$. 故に $S_e S_a S_e S_b = S_e S_b S_e S_a$ を得る. 更に, 以上の時 A の元 $S_e S_a$ の位数が奇数なることより, $H(A)$ の位数も奇数であることがわかる.

2. 有限等質対称系の可解性

先づ $H(A)$ の位数が奇数であると仮定してみよう. $S_a S_b$ の位数は奇数でそれより $2k+1$ とする. 前の如く, $S_a = (S_b S_a)^k S_b (S_a S_b)^k$ となる. $(S_a S_b)^k = S_b S_c$ となる元 C が存在すること前節の如くに分る. ($S_a S_b$ で生成された巡回部分群を考えるとよい.) 故に, $S_a = (S_b S_c)^{-1} S_b (S_b S_c) = S_c S_b S_c$. 即ち, $a = b S_c$ を得る. 対称系 A において, 任意の二元 a と b に對し常に元 C が存在して, $a = b S_c$ となる時, A は等質 (homogeneous) であるという. $H(A)$ の位数が奇数なら, A は等質であることがわかった. 所で更に重要なことは, この逆が正しいのである. 即ち, A が有限等質対称系ならば $H(A)$ は奇数次の群である. その証明はここには出来ないが, 群論における G. Glauberman の Z^* -定理 が本質的な役割を果すことと言及しておく.

A が有限等質対称系なら、二元 a と b に対し $a = bS_c$ となる元 c は唯一つである。それは、 $x \rightarrow bS_x$ なる対応が A の自身の上への一対一対応であることより明らかである。次に、 B が A の部分系なら B も等質である。それは、上の対応で b を B の一元として、 x を B の元としてとることにより、この対応が B から B の上への一対一対応であることがいえるからである。さて、上で述べた如く、 $H(A)$ の位数は奇数で、有名な Feit-Thompson の定理により、 $H(A)$ は可解群である。このことより A の構造が類似な意味で可解であることの説明を以下に与える。

以下 A は有限等質対称系とする。今 J が $H(A)$ に含まれるような $G(A)$ の正規部分群とする。 $B = eJ$ とすると B が部分系なることは容易に分る。このような部分系を A の正規部分系という。この時 $\bar{A} = \{aJ \mid a \in A\}$ を考えよ。 $(aJ) \circ (bJ) = (aob)J$ なる定義が可能であることは J が $G(A)$ の正規部分群ということより知れる。この乗法に関して、 $\bar{A}$ は対称系となる。これを A の B による商系 A/B であるという。以上で $\bar{A}$ は J によらず B のみで決定されることを示す必要がある。それは、 $a = eS_b$ なる時、 $aJ = bS_b$ であることと、上の結合の定義が元 a と b によらぬことよりわかる。この時 $H(A)$ は $H(A)/J$ の準同型な像となる。従って、特に $H(A)/J$

がアーベルなら, $\bar{A}$ もアーベルなることがわかる. このことより次の定理が成立する. $H(A)$ が可解なことを用いてある.

定理 A も有限等質対称系とする. A の部分系 B_i ($i = 0, 1, \dots, n$) が存在して, $B_0 = A \supset B_1 \supset \dots \supset B_n = (e)$ であり, 各 B_i は B_{i-1} の正規部分系であり, B_{i-1}/B_i はアーベルである.

最後に, 有限等質対称系では有限群論の構造論に類似の理論が可能であることも言及しておく. 即ち, p -群の理論やシローの理論の一部が成立する.

3. 単対称系と単群

ここでは A は等質としなす. しかし, A の部分系 B が正規であるという定義は前の如くにする. そして, A が自分自身又は一点集合以外の正規部分系をもたぬ時, A は単であると言ふことにする. 次の定理を証明しよう.

定理 A が単なら, $H(A)$ は単群であるか, または $G(A)$ で互いに共役な二つの単部分群の直積となる. 更に後者の場合 $o(H(A)) = (o(A))^2$. ($o(A)$ は A の元数)

証明. A も単とせよ. J を $H(A)$ の正規部分群とする. J の $G(A)$ での共役は $S_a J S_a$ のみである. これを J' とする. JJ' は $H(A)$ にふくまれる $G(A)$ の正規部分群である. 故に,

$eJ'J' = e$ であるが, $eJ'J' = A$ である. したがって, A が単純だから $eH(A)$ ($= eG(A)$) は A に一致しなければならない. (注意: A の元 a に対して $aG(A) = a$ になるような A は考えないことにする. 従ってある元 e があり, $eG(A) \neq e$ であるものと仮定しておく.) 既に任意の元 a に対し, $G(A)$ の元 T があり $a = eT$. したがって, $eJ'J' = e$ なら $aJ'J' = eTJ'J' = eJ'J'T = eT = a$ となり, $J'J' = I$. $eJ'J' = A$ なら, 任意の元 a に対し $J'J'$ の元 T' があり, $a = eT'$. この時には, $S_a = T'S_eT'$. この右辺はある $J'J'$ の元 T'' により S_eT'' とかけらる. 既に, $S_eS_a = T'' \in J'J'$. したがって, $H(A)$ は S_eS_a により生成されるから, $J'J' = H(A)$ となる. さて上で, $J \neq I$ なら, $J'J' \neq I$ だから $J'J' = H(A)$ となる. また, $J_0 = J \cap J'$ とおくと, もし $J \neq H(A)$ なら, $J \cap J' \neq H(A)$ だから, $J_0 = I$ となる. これより, $H(A)$ が単純群になり, J と J' の直積になることが分った. この時 J は単純群である. もしそうじゃなかったら, J をその固有な正規部分群とすると, J_1 は $H(A)$ の正規部分群であり, $H(A)$ が J_1 と J_1' の直積になることになり矛盾を生じる. これで定理の前半の証明が終った. さて, $\{S_a \mid a \in A\}$ は, $A = eH(A)$ より, $\{T'S_eT \mid T \in H(A)\}$ であることがわかる. これより, $O(A) = |H(A) : C|$, ことに $C = \{T \in H(A) \mid T'S_e = S_eT\}$. したがって $H(A)$ は単純群にな

く, $H(A) = J \times S_e J S_e$ とする. この時, $C = \{TS_e TS_e \mid T \in J\}$ であることがたしかめうる. 故に $o(C) = o(J)$. 以上により $o(A) = o(J)$, 従って $o(H(A)) = (o(A))^2$ を得る.

4. 原始対称系とその例

A の部分系 B がブロック (置換群の理論から言葉も借りる) であるとは, 任意の $G(A)$ の元 T に対して, $BT = B$ なるか, BT と B は互いに疎であることという. A がそれ自身か又は一点集合以外にブロックを持たない時, A は原始的 (primitive) であるという. $G(A)$ が A の置換群として primitive であるということである. A の正規部分系はブロックであるから, A が原始的なら, A は勿論単純である.

例 1. 互換のなす対称系

n 次の対称群 S_n に含まれるすべての互換のなす集合は対称系をなす. $n \geq 5$ ならこれは原始的であることを示す. B を二元以上含む A のブロックとする. B の二元 $\alpha = (i, j)$ 及び $\beta = (k, l)$ とする. $\beta S_\alpha = \beta$ なら i, j, k, l は凡て異なる. $n \geq 5$ より, これ以外に p がある. $\gamma = (p, i)$ を考える. $\beta S_\gamma = \beta$ より $\beta S_\gamma = B$. 故に $\alpha S_\gamma \in B$. 所で明らかに $\alpha S_\gamma = (p, j)$ でこれが B の元となる. あると, $\gamma' = (p, j)$ とすると, $\gamma = \gamma' S_\alpha$ であるから B は (i, j) ,

(p, i) 及び (p, j) を含む. さて, $\delta = (s, t)$ を任意の互換とすると, S_δ は (i, j) , (p, i) と (p, j) の中少なくとも一つは固定することが分る, 従って $BS_\delta = B$. 容易に分る如く, $A = \alpha G(A)$. (これを, A は transitive ということにする.) 故に, $B = A$ でなければならぬ. A は原始的である. 更に定理の後半より, $H(A)$ が単純群であることが結論される. 勿論 $H(A) = A_n$ (n 次交代群) である.

例2. $\mathbb{Z}_2$ 上のベクトルのなす対称系

$\mathbb{Z}_2$ も = 元 0 と 1 よりなる体とし, V を $\mathbb{Z}_2$ 上の n 次ベクトル空間で内積 (a, b) が与えられているものとする. V の 0 以外のベクトルのなす集合を V^* とする. V^* で結合 $\circ$ を次の如く定義する. $a \circ b = a + (a, b)b$. この時 V^* は対称系をなす. この部分系の中に多くの原始対称系を見つけることが出来ることを示す. V^* の = 元 a と b が, $aS_b \neq a$ なら, $c = aS_b$ とすると, $bS_c = a$ となり, $\{a, b, c\}$ は部分系をなす. ここでは, $\{a, b, c\}$ をサイクルと呼ぶ. 容易とたしかめられるように, $\{a, b, c\}$ がサイクルなら, V^* の任意の元 d に対し S_d は a, b, c の中少なくとも一つは固定する. これよりブロック B がサイクルを含めば, 任意の S_d に対して, $BS_d = B$ であることがいえる. 従って次の判定条件を得る.

判定条件. A は V^* の部分系で transitive なものとする.

A の二元 x と y で $x S_y = x$ ならば, A 元子があり, S_y は x と y の一つを動かして他を固定する, という条件がみたされる時には A は原始的である.

証明は容易であろう. 上の条件の下では, 二元以上を含む A のプロットはサイクルを含むことがわかり, A が transitive よりそれは A のみに限るからである. この判定条件を使って以下種々の原始対称系を得る.

以下, 内積は $(x, y) = \sum_{i,j} x_i y_j$ をとる. これは二次形式 $Q(x) = \sum_{i,j} x_i x_j$ から与えられるものである. n は V の次元, $V_1 = \{x \in V \mid (x, x) \neq 0\}$ と表わす. また, $V^{(i)}$ に i 度 i の成分が 1 で他は 0 となるようなベクトルのなる集合を表わす.

(1) $n=6$. $A = V_1 (= V^{(2)} \cup V^{(3)} \cup V^{(6)})$. A は 36 個の元よりなる原始対称系である. これは, E_6 -型のリー環の正根のなる対称系と同型である. 故に, $H(A) = \Omega_6(\mathbb{Z}, \mathbb{Q})$.

(2) $n=6$. $A = V^*$. A は 63 個の元よりなる原始対称系で, E_7 -型の正根のなる対称系と同型. $H(A) = PS_6(\mathbb{Z}_2)$.

(3) $n=8$. $A = V_1 (= V^{(2)} \cup V^{(3)} \cup V^{(6)} \cup V^{(7)})$. A は 120 個の元よりなる原始対称系で, E_8 -型の正根のなる対称系と同型. $H(A) = \Omega_8(\mathbb{Z}_3, \mathbb{Q})$.

(4) $n=8$. $A=V^*$. A は 255 个の元よりなる, 原始対称系.

(5) $n=10$. $A=V_1$. A は 496 个の元よりなる原始対称系.

(6) $n=10$. $A=V^*$. A は 1023 个の元よりなる原始対称系.

(7) $n=11$. $A=V^{(2)} \cup V^{(6)} \cup V^{(10)}$. A は 528 个の元よりなる原始対称系.

(8) $n=12$. $A=V^{(2)} \cup V^{(6)} \cup V^{(10)}$. A は 1056 个の元よりなる原始対称系.

例3. 有限体上の直交幾何をもつベクトル空間

F を有限体, V を F 上有限次元ベクトル空間で, 正則な直交内積 (a, b) をもつものとする. $(a, a) \neq 0$ なる a を non-isotropic とする. a によって定まる直線を $\bar{a}$ とかく. A を non-isotropic な a によって定まる $\bar{a}$ のなる集合とする: $A = \{ \bar{a} \mid (a, a) \neq 0, a \in V \}$. この時 A に結合 $\circ$ を, $\bar{a} \circ \bar{b} = \bar{c}$, ここで $c = a - 2[(a, b)/(b, b)]b$ により定義すると, A は対称系となる. この時, $\dim V \geq 5$ であるなら, A は原始対称系となる. その証明は, 数頁の紙数を必要とするので, ここでは省略する.

例4. 対称行列のなす対称系

体 F 上の行列式 1 なる n 次の対称行列のなす集合は対称系である. これを $SM_n(F)$ とかく. また, 行列 a と b は $a = \alpha b$ ($\alpha^n = 1$) なる F 元 α がある時同値であるとして, $SM_n(F)$ の同値類のなす集合を $PSM_n(F)$ とかく. これも勿論対称系である. F が有限体で $n \geq 3$ ならば (或は, $F \neq \mathbb{Z}_3$ なら $n \geq 2$ でもよい) $H(SM_n(F)) = SL_n(F) / \{\pm I\}$ 及び $H(PSM_n(F)) = PSL_n(F)$ なることが証明される. n が小さい時, いくつかの例が実際に計算でえられる.

(1) $PSM_3(\mathbb{Z}_2) = SM_3(\mathbb{Z}_2)$ は 28 个の元よりなる原始対称系である.

(2) $PSM_2(\mathbb{Z}_7)$ は 21 个の元よりなる単純対称系ではあるが原始的ではない. 実際に $PSM_2(\mathbb{Z}_7)$ を作ってみることでより, $PSL_2(\mathbb{Z}_7)$ が A_7 の部分群になることが示される.

(3) $SM_4(\mathbb{Z}_2)$. これは互いに共通点をもたぬ二つの部分系の和となる. その中一つは, 凡ての対角線上の元が 0 となるようなもの全体よりなる. そして共にイデアルをなす. さて上にあげた部分系は 28 个の元よりなる原始対称系である. これは S_8 の互換のなす対称系と同型である. このことより, $PSL_4(\mathbb{Z}_2)$ は A_8 と同型という定理が得られる.