数理解析研究所講究録
第308巻 1977年 1-11

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が次の條件をみたす時，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$a\circ b=ba^{-1}b$なる定義により対称系とみられる．一般にこの結合でしじているような群の部分集合は対称系である．群Gの位数2なる元のなす集合，またはGL_nの中の対称行列のなす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2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_aS_b $(a,b\in A)$で生成された$G(A)$の指数2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$a\longrightarrow S_a$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．$a\longrightarrow S_eS_a$（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．アーベル対称系とアーベル群

H(A)がアーベル群の時Aをアーベル対称系という．これはA元a，b，cに対して $S_aS_bS_c=S_cS_bS_a$ 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_aS_b の位数は常に奇数であることを示そう．S_aS_b の位数が2kであると仮定せよ．任意の元cに対して，$c(S_aS_b)^k=c$ となる．何となれば，$d=c(S_aS_b)^k$ とおくと，$S_d=(S_aS_b)^kS_c(S_aS_b)^k$ $=(S_bS_a)^kS_c(S_aS_b)^k=S_c(S_aS_b)^k(S_aS_b)^k=S_c$ となり，$d=c$ となるからである．これは (S_aS_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 $S_aS_eS_b=S_c$ となることを示す．S_eS_b の位数を2k+1とせよ．$I=(S_eS_b)^{2k+1}=(S_eS_b)^kS_e(S_bS_e)^kS_b$ より，$S_b=(S_eS_b)^kS_e(S_bS_e)^k$．故に，$S_aS_eS_b=(S_aS_e)(S_eS_b)^kS_e(S_bS_e)^k(S_eS_b)^kS_a(S_bS_e)^k=S_c$．ここに $c=a(S_bS_e)^k$．また，S_eS_a の位数mなら $S_aS_e=(S_eS_a)^{m-1}=S_eS_{a'}$ となる元a'が存在する．以上よりAがアーベルなら，$H(A)=\{S_eS_a \mid a\in A\}$ となることがわかる．従って $a\to S_eS_a$ はAとH(A)との同型を与える．

逆に，$H(A)=\{S_eS_a \mid a\in A\}$ なら $H(A)$ はアーベル群であることが次のようと分る．S_eS_a と S_eS_b に対して元 C があって，$S_eS_aS_eS_b=S_eS_c$．逆をとって，$S_bS_eS_aS_e=S_cS_e$．S_e を右と左から乗じて，$S_eS_bS_eS_a=S_eS_c$．故に $S_eS_aS_eS_b=S_eS_bS_eS_a$ を得る．更に，以上の時Aての元 S_eS_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

先ず $H(A)$ の位数が奇数であると仮定してみる．S_aS_b の位数は奇数でそれを $2k+1$ とする．前の如く，$S_a=(S_bS_a)^kS_b(S_aS_b)^k$ となる．$(S_aS_b)^k=S_bS_c$ となる元 C が存在することも前の節の如くに分る．（S_aS_b で生成された巡回部分群を考えればよい．）故に，$S_a=(S_bS_c)^{-1}S_b(S_bS_c)=S_cS_bS_c$．即ち，$a=bS_c$ を得る．対称系 A において，任意の二元 a と b に対し常に元 C が存在して，$a=bS_c$ 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，この逆がいえるのである．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．その証明はここでは出来ないが，群論における Glauberman の Z^*-定理 が本質的な役割を果すことを言及しておく．

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，$x \longrightarrow bS_x$ 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 $\bar{A}=\{aJ \mid a\in A\}$ を考える．$(aJ)\circ(bJ)=(a\circ b)J$ 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，$\bar{A}$ は対称系をなす．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．それには，$a=eS_b$ 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，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を有限等質対称系とする．Aの部分系B_i（$i=0,1,\cdots,n$）が存在して，$B_0=A\supset B_1\supset\cdots\supset B_n=(e)$ 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を言及しておく．即ち，p-群の理論やシローの理論の一部が成立する．

3．単純対称系と単純群

ここではAは等質としない．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は単純であるとよぶことにする．次の定理を証明しよう．

定理　Aが単純なら，H(A)は単純群であるか，またはG(A)で互いに共役な二つの単純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を単純とせよ．JをH(A)の正規部分群とする．Jの$G(A)$での共役はS_aJS_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，

$eJJ' = e$ であるか, $eJJ' = A$ である. さて, 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.) 故に任意の元 a に対し, $G(A)$ の元 T があり $a = eT$. さて, $eJJ' = e$ なら $aJJ' = eTJJ' = eJJ'T = eT = a$ となり, $JJ' = I$. $eJJ' = A$ なら, 任意の元 a に対して JJ' 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 JJ' の元 T'' により S_eT'' とかける. 故に, $S_eS_a = T'' \in JJ'$. 所が, $H(A)$ は S_eS_a により生成されるから, $JJ' = H(A)$ となる. さて上で, $J \neq I$ なら, $JJ' \neq I$ だから $JJ' = H(A)$ 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, $H(A)$ が単純群でないなら, J と J' との直積になることが分った. この時 J は単純群である. もしそうでなかったなら, J_1 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' の直積になることになって矛盾を生じる. 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, $\{T^{-1}S_eT \mid T \in H(A)\}$ であることがわかる. これより, $o(A) = |H(A) : C|$, ここに $C = \{T \in H(A) \mid TS_e = S_eT\}$. 故で $H(A)$ は単純群でな

く，$H(A)=J\times S_e JS_e$ とする．この時，$C=\{TS_eTS_e \mid T\in J\}$ 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

Σ の部分系 B がブロック（置換群の理論から言葉を借りる）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をいう．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 に含まれる凡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．$\beta S_\gamma\neq\beta$ より $BS_\gamma=B$．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．すると，$\gamma'=(p,j)$ 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，$\delta=(A,\alpha)$ を任意の互換とすると，S_δ は (i,j)，(p,i) と (p,j) の中少く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，$B=A$ でなければならない．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．Z_2 上のベクトルのなす対称系

Z_2 を二元 0 と 1 よりなる体とし，V を 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^* の二元 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 の中少くも一つは固定する．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．従って次の判定條件を得る．

判定條件. AはV^*の部分系でtransitiveなものとする. Aの二元xとyで$xS_y=x$たらば, A元子があり, S_yはxとyの一つを動かし他を固定する, という條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. 上の條件の下では, 二元以上を含むAのブロック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. この判定條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, $V^{(i)}$にて, i度ベクトルの成分が1で他は0となるようなベクトルのなす集合を表わす.

(1) $n=6$. $A=V_1\ (=V^{(2)}\cup V^{(3)}\cup V^{(6)})$. Aは36ケ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す対称系と同型である. 故に, $H(A)=\Omega_6(Z_2,Q)$.

(2) $n=6$. $A=V^*$. Aは63ケの元よりなる原始対称系で, E_7-型の正根のなす対称系と同型. $H(A)=PS_{p6}(Z_2)$.

(3) $n=8$. $A=V_1\ (=V^{(2)}\cup V^{(3)}\cup V^{(6)}\cup V^{(7)})$. Aは120ケの元よりなる原始対称系で, E_8-型の正根のなす対称系と同型. $H(A)=\Omega_8(Z_2,Q)$.

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

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

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

(7) $n=11$. $A=V^{(3)}\cup V^{(6)}\cup V^{(10)}$. Aは552ケ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ケ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という. aではられる直線を$\bar{a}$とかく. Aをnon-isotropicなaではられる$\bar{a}$のなす集合とする: $A=\{\bar{a}\mid (a,a)\neq 0,\ a\in V\}$. この時$A$に結合$\circ$を，$\bar{a}\circ\bar{b}=\bar{c}$，ここに$c=a-2[(a,b)/(b,b)]b$により定義すると，$A$は対称系をなす. この時，$\dim V\geq 5$であるなら，$A$は原始対称系をなす. 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、$F\neq Z_3$ ならば $n\geq 2$ 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与えられる。

(1) $PSM_3(Z_2)=SM_3(Z_2)$ は28ケの元よりなる原始対称系である。

(2) $PSM_2(Z_7)$ は21ケ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 $PSM_2(Z_7)$ を作ってみることより、$PSL_2(Z_7)$ が A_7 の部分群になることが示される。

(3) $SM_4(Z_2)$。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ケ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、$PSL_4(Z_2)$ は A_8 と同型という定理が得られる。