駆け足で有限群を見てみよう

１９８７年7月　北大での集中講義の記録

イリノイ大学教授　鈴木　通夫　著

Series ♯ 13. July, 1989

HOKKAIDO UNIVERSITY
TECHNICAL REPORT SERIES IN MATHEMATICS

♯ 1: T. Morimoto, Equivalence Problems of the Geometric Structures admitting Differential Filtrations, 14 pages. 1987.
♯ 2: J.L. Heitsch, The Lefshetz Theorem for Foliated Manifolds, 59 pages. 1987.
♯ 3: K. Kubota (Ed.), 第 12 回偏微分方程式論札幌シンポジウム予稿集, 77 pages. 1987.
♯ 4: J.Tilouine, Kummer's criterion over Λ and Hida's Congruence Module, 85 pages. 1987.
♯ 5: Y. Giga (Ed.), Abstracts of Mathematical Analysis Seminar 1987, 17 pages. 1987.
♯ 6: T.Yoshida (Ed.), 1987 年度談話会アブストラクト集 Colloquim Lectures, 96 pages. 1988.
♯ 7: S. Izumiya,G. Ishikawa (Eds.), "特異点と微分幾何 " 研究集会報告集,1988.
♯ 8: K. Kubota (Ed.), 第 13 回偏微分方程式論札幌シンポジウム予稿集, 76 pages. 1988.
♯ 9: Y. Okabe (Ed.), ランジュヴァン方程式とその応用予稿集, 64 pages. 1988.
♯ 10: I. Nakamura (Ed.), Superstring 理論と K3 曲面, 91 pages. 1988.
♯ 11: Y. Kamishima (Ed.), 1988 年度談話会アブストラクト集 Colloquim Lectures, 73 pages. 1989.
♯ 12: G. Ishikawa,S. Izumiya and T. Suwa (Eds.), "特異点論とその応用" 研究集会報告集 Proceedings of the Symposium "Singularity Theory and its Applications," 317 pages. 1989.

はじめに

この講義録は1987年７月に北大でおこなわれた集中講義のノートをもとに、講義では省略した証明や注意を加筆したものである。集中講義の目標は有限群論の特異点にあたる散在単純群を身近な、親しみやすいものにすることであった。そのためもあって、この講義録の第１章 準備にあたる所に「駆け足で有限群を見てみよう」という副題をつけたのがこの講義録の表題となった理由である。短時間では有限群論のほんの一部しか述べることが出来なかったが、散在群の単純性の証明に必要なことはすべて含まれている。Fischer-Griess の "monster" についても詳しく述べることが出来ず残念であるが、その定義に必要な Conway群は詳しく述べてあるから、このあと monster について勉ぶために役立てば幸いである。

この講義録を「北海道大学数学講究録」の一冊として出版することになったのは、北大数学教室の方々、特に都筑、吉田両氏の御好意によるもので厚く御礼申し上げたい。また浅井、竹ケ原、庭崎、船矢、石川、石原、池田の諸君が講義のノートをとり、それをもとに竹ケ原、庭崎両君が整理された由。ここにこれらの方々に厚く御礼申し上げる。

鈴木　通夫

目　次

第１章　準備

本講義録を通して群といえばそれは有限群をさすものとする。群 G の位数を |G| と書く。またｎ次対称群を Σ_n で表す。A が集合 B の部分集合のとき $A \subset B$ と書き、真部分集合のとき $A \subsetneq B$ と書く。N が群 G の正規部分群であることを $N \lhd G$ で表す。また Z(G) で G の中心を表す。

§１ａ　Ｓｙｌｏｗの定理

定理１．１（Sylowの定理）　p を素数、G を群とする。$|G| = m \cdot p^n$、$(m, p) = 1$ ならば次が成り立つ。

(1) 位数が p^n になる部分群が存在する。これを G のSylow p-部分群という。
(2) 二つのSylow p-部分群は共役である。即ち、P_1, P_2 をSylow p-部分群とすると、或る $x \in G$ が存在して $P_1 = x P_2 x^{-1}$ となる。
(3) 任意のｐ-部分群は或るSylow p-部分群に含まれる。
(4) Sylow p-部分群の個数はｐを法として１に合同で、|G| の約数である。

G のSylow p-部分群全体のなす集合を $Syl_p(G)$ と書く。

応用（Frattini論法）　p を素数、N を群 G の正規部分群、P を N のSylow p-部分群とすると、$G = N \cdot N_G(P)$ である。ここで $N_G(P)$ は P の G における正規化群である。

証明　G の任意の元 x に対し、$x P x^{-1} \subset x N x^{-1} = N$ であるから $x P x^{-1}$ も N のSylow p-部分群である。Sylowの定理より、或る $y \in N$ が存在して $y x P x^{-1} y^{-1} = P$ である。$y x \in N_G(P)$ だから $x \in N \cdot N_G(P)$ となり、命題が示された。□

注意　|G| を割る素数全体の集合を $\pi(G)$ と書くと、同形定理より上において $q \in \pi(G)$ ならば $q \in \pi(N)$ または $q \in \pi(N_G(P))$ である。

補題１．２　ｐ を素数、Ｎ を群 Ｇ の正規部分群、Ｐ を Ｇ のSylow ｐ-部分群とすると次が成り立つ。

(1)　Ｎ∩Ｐ は Ｎ のSylow ｐ-部分群である。

(2)　ＮＰ/Ｎ は Ｇ/Ｎ のSylow ｐ-部分群である。

§１ｂ　ｐ-群の基本性質

本節において ｐ は素数とする。次の定理は基本的である。

定理１．３　Ｐ をｐ-群とすると次が成り立つ。

(1)　Ｐ の正規部分群 Ｈ が {1} でないならば Ｈ∩Ｚ(Ｐ) も {1} でない。特に Ｐ≠{1} ならば Ｚ(Ｐ)≠{1} である。

(2)　Ｈ が Ｐ の真部分群ならば $H \subsetneq N_P(H)$ である。

(3)　Ｐ の正規部分群 Ｈ が {1} でないならば $[H,P] \subsetneq H$ である。ここで

$$[H,P] = \langle h\,x\,h^{-1}x^{-1} \mid h \in H, x \in P \rangle$$

である。

この定理よりｐ-群は巾零である（§１ｆ参照）。この応用として次がある。

補題１．４　Ｈ は群 Ｇ の正規部分群で ｐ｜|Ｈ| とする。Ｇ の任意のｐ巾位数の元 ｘ について $H \cap C_G(x) \neq \{1\}$ が成り立つ。

証明　〈ｘ〉はｐ-部分群であるから、定理１．１より Ｇ のSylow ｐ-部分群 Ｐ が存在して 〈ｘ〉⊂Ｐ となる。補題１．２より Ｐ∩Ｈ は Ｈ のSylow ｐ-部分群で、ｐ｜|Ｈ| の仮定より {1} でない。Ｐ∩Ｈ◁Ｐ であるから、定理１．３より (Ｐ∩Ｈ)∩Ｚ(Ｐ)≠{1} を得るが、

$$(P \cap H) \cap Z(P) = H \cap Z(P) \subset H \cap C_G(x)$$

であるから補題が示される。□

定理１．５　Ｐ をｐ-群、Ｘ を Ｐ集合とする。Ｘ の Ｐ-不変元全体を X^P とおけば $|X| \equiv |X^P| \pmod{p}$ となる。

証明　Ｘ の元 ｘ を含むorbitを Ｏ、ｘ の安定部分群を Ｓ とおけば |Ｏ|=|Ｐ:Ｓ| であることに注意すればよい。□

注意　定理１．５の証明法を用いて補題１．４を直接に証明することもできる。

§１ｃ　交換子群

定義　群 G の元 x, y に対し、$[x,y]=xyx^{-1}y^{-1}$ とおく。部分群 X, Y の交換子群 [X, Y] を

$$[X,Y]=\langle [x,y] \mid x\in X, y\in Y\rangle$$

で定め、特に [X, X] を X′ と書く。更にもう一つの部分群 Z に対し、

$$[X,Y,Z]=[[X,Y],Z]$$

とする。[X, Y] = [Y, X] に注意する。

定理１．６ (P. Hallの３部分群定理)　三つの部分群 X, Y, Z について、[X, Y, Z] = [Y, Z, X] = {1} ならば [Z, X, Y] = {1} である。

この応用として次がある。

補題１．７　群 G の部分群 H, K に対し、$[H,K]\subset C_G(H)$ ならば $[H',K]=\{1\}$ である。

証明　仮定より $[H,K,H]\subset[C_G(H),H]=\{1\}$ である。同様に $[K,H,H]=\{1\}$ であるから、定理１．６より $\{1\}=[H,H,K]$ を得る。□

注意　準同形 $f:G\to H$ に対しては $f([X,Y])=[f(X),f(Y)]$ が成り立つ。

§１ｄ　中心積

定義　群 G が部分群 H と K の中心積とは、G = HK かつ [H, K] = {1} が成り立つときにいう。

注意　(1)　G が部分群 H, K の中心積ならば、H も K も正規部分群である。また $Z=H\cap K$ とおくと $Z\subset Z(G)$ で、$G/Z=(H/Z)\times(K/Z)$ となる。

(2) G は部分群 H,K の中心積とする。G の元は H の元と K の元との積で書けるが、その表し方は一意的ではない。いま写像 $f:H\times K\to G$ を

$$f(h,k)=hk,\quad h\in H,k\in K$$

で定めると、f は準同形で、その核は $\{(z,z^{-1})\mid z\in H\cap K\}$ である。

逆に、二つの群 H,K の中心に含まれる部分群 Z_1,Z_2 が同型と仮定する。その同型写像を $g:Z_1\to Z_2$ として $Z=\{(z,g(z^{-1}))\mid z\in Z_1\}$ とおくと $(H\times K)/Z$ は H と K の中心積とみなすことができる。

(3) 直積におけるKrull-Remak-Schmidtの定理の類似は中心積では成り立たない。

例 Q_1,Q_2 を位数8の四元数群とする。即ち $i=1,2$ に対し

$$Q_i=\langle x_i,y_i\mid x_i^2=y_i^2=(x_iy_i)^2\rangle$$

とする。$z_i=x_i^2$ とおくとこれは位数2で、$Z(Q_i)=\langle z_i\rangle$ である。

いま z_1 と z_2 を同一視し、注意(2)の方法で構成される Q_1 と Q_2 の中心積を G とする（各 Q_i は G の部分群とみなす）。一般に、m個の四元数群の中心を同一視して得られる中心積を Q^m と書く。$G=Q^2$ である。

G の部分群 D_1,D_2 を

$$D_1=\langle x_1,y_1y_2\rangle,\quad D_2=\langle y_2,x_1x_2\rangle$$

で定義すると、これらは二面体群である。実際、

$$x_1^4=1,$$
$$(y_1y_2)^2=y_1^2y_2^2=z^2=1,$$
$$(y_1y_2)x_1(y_1y_2)^{-1}=y_1x_1y_1^{-1}=x_1^{-1}$$

であるから D_1 についてはよい。D_2 も同様である。

容易にわかるように $G=D_1D_2$ であり、更に

$$\begin{aligned}y_1y_2\cdot x_1x_2&=y_1x_1\cdot y_2x_2\\&=x_1y_1z\cdot x_2y_2z\\&=x_1x_2\cdot y_1y_2\end{aligned}$$

であるからこれは中心積である。一般に、n個の二面体群の中心を同一視して得られる中心積を D^n と書く。今、我々は $G=Q^2=D^2$ であることを見た。

定義 Q^mD^n という形の中心積として表せる群をextraspecial 2-群という。

P をextraspecial 2-群とすると

(1) $Z(P)=P'$ で、この位数は2

(2) $P/Z(P)$ はelementary abeian 2-群

である。$Q^2=D^2$ だから P は Q^m または Q^mD の形で書ける。

§1e　半単純群

定義　群 G が、次の条件を満たすとき、半単純群(semisimple group)という。

(1)　$G=[G,G]$　　(2)　$G/Z(G)$ が単純群の直積となる。

また群 G が準単純 (quasi-simple) とは、つぎの条件を満たすことをいう。

(1)　$G=[G,G]$　　(2)　$G/Z(G)$ が非可換な単純群となる。

特に (1) は半単純であるが、準単純ではない。

注意　G が半単純ならば $G/Z(G)$ の単純直積因子は非可換単純群である。

定理1.8　半単純な群は、準単純群のいくつかの中心積になる。

証明　G を半単純群とし、$G/Z(G)$ の単純直積因子に対応する G の部分群を $S_1,\cdots,S_r$ とする。このとき S_i の像になる $G/Z(G)$ の部分群を $\overline{S}_i$ とすれば

$$G/Z(G)=\overline{S}_1\times\overline{S}_2\times\cdots\times\overline{S}_r$$

となるので $G=S_1S_2\cdots S_r$ が成り立つ。S_i の正規部分群 Q_i を次のように定義する。即ち、$S_i=Q_iZ(G)$ が成り立ち、その上この等号が成り立つ正規部分群の中で Q_i は極小とする。このとき、Q_i は $Q_i=[Q_i,Q_i]=[S_i,S_i]$ を満たすことを証明しよう。いま $R=[Q_i,Q_i]$ とおけば

$$\overline{R}=[\overline{Q}_i,\overline{Q}_i]=[\overline{S}_i,\overline{S}_i]=\overline{S}_i$$

が成り立つ。よって $S_i=RZ(G)$ となる。ところで $R\subset Q_i$ かつ R は S_i の正規部分群だから Q_i の極小性により $R=Q_i$ を得る。明らかに

$$Q_i=[Q_i,Q_i]\subset[S_i,S_i]。$$

一方、$S_i=Q_iZ(G)$ より

$$S_i/Q_i\simeq Z(G)/Z(G)\cap Q_i。$$

この右辺は可換群だから $Q_i\supset[S_i,S_i]$、よって $Q_i=[S_i,S_i]$。

この等号から Q_i は G の正規部分群であることがわかる。さて

$$Q_i/Q_i\cap Z(G)\simeq S_i/Z(G)=\overline{S}_i$$

は単純群だから Q_i は準単純である。

$i\neq j$ ならば $[Q_i,S_j]\subset Q_i\cap S_j\subset Z(G)$ だから補題1.7により $[Q_i,S_j]=(1)$ を得る。よって $Q=Q_1Q_2\cdots Q_r$ は準単純群 Q_i の中心積である。残っている点は $Q=G$ の証明である。これは $\overline{Q}=\overline{Q}_1\overline{Q}_2\cdots\overline{Q}_r=\overline{S}_1\overline{S}_2\cdots\overline{S}_r=\overline{G}$ より $G=QZ(G)$ を得るから、前と同様に G/Q が可換となり、$Q\supset[G,G]$ が得られ $Q=G$ が証明される。□

補題１．９　Ｇ を半単純な群とすれば、可解な正規部分群は中心に含まれる。

この補題の証明は次の定理よりただちに得られる。

定理１．10 (Krull-Remak-Schmidt)　群 Ｇ は非可換な単純群の直積であるとして

$$G = S_1 \times \cdots \times S_n \qquad S_i : \text{非可換な単純群}$$

とおく。このとき Ｇ の正規部分群 Ｎ は、$S_{i_1} \times S_{i_2} \times \cdots \times S_{i_k}$ という部分積に限る。ここで、$\{S_{i_1}, S_{i_2}, \cdots, S_{i_k}\} = \{S_i \mid [N, S_i] \neq 1\}$ 。

証明　$[N, S_i] \neq 1$ とすると、S_i が単純だから、$[N, S_i] = S_i$ 。従って $S_i \subset N$ となる。また $[N, S_i] = 1$ とすると、$x \in N$ に対し、$x = x_1 \cdots x_j \cdots x_n$ $(x_j \in S_j)$ とおけば、$[x_i, S_i] = [x, S_i] = 1$ となる。これより $x_i \in Z(S_i) = \{1\}$、従って $x_i = 1$ を得る。よって

$$N \subset S_1 \times \cdots \overset{\vee S_i}{\cdots} \cdots \times S_n$$

となる。□

補題１．９の証明　半単純群 Ｇ の可解な正規部分群を Ｎ とする。前のように Ｇ/Ｚ(Ｇ) への像を $\overline{N}$ と書けば、$\overline{N}$ は $\overline{G}$ の正規部分群であるから定理１.10により $\overline{N}$ は $\overline{G}$ の単純直積因子いくつかの積となる。一方、$\overline{N}$ は可解だから単純直積因子を含まない。即ち $\overline{N} = \{1\}$。よって $N \subset Z(G)$ を得る。□

補題１.11　Ｈ と Ｋ は、Ｇ の正規部分群で、共に非可換な単純群の直積と仮定する。このとき ＨＫ も正規で、やはり非可換単純群の直積となる。

証明　$H \cap K$ は Ｈ の正規部分群だから定理１.10より $H = (H \cap K) \times L$、Ｌ は $H \cap K$ に含まれていない単純直積因子の積、となる。また Ｋ は Ｌ を正規化するので Ｌ は ＨＫ の正規部分群である。従って $HK = L \times K$ となるから証明が終わる。□

定理１.12　Ｈ と Ｋ は Ｇ の正規部分群で、共に半単純とする。このとき、ＨＫ もそうである。

証明　$L = HK$ とおく。まず $[L, L] \supset H'K' = HK = L$ となり $L = L'$ がいえる。以下、Ｌ/Ｚ(Ｌ) が非可換単純群の直積であることを示す。

$[H, Z(K)] \subset H \cap Z(K) \subset Z(H)$ だから、補題１．７より

$[H, Z(K)] = [H', Z(K)] = \{1\}$ を得る。即ち、$Z(K) \subset Z(L)$ となる。同様に、$Z(H) \subset Z(L)$ を得る。そこで、$Z = Z(K)Z(H)$ とおく。このとき $Z \subset Z(L)$ で、$L/Z = (HZ/Z)(KZ/Z)$ と書ける。ここで $H \cap Z = Z(H)$ より $HZ/Z = H/H \cap Z = H/Z(H)$ だから、HZ/Z は単純群の直積となる。同様に、KZ/Z も非可換単純群の直積となる。従って補題1.11により L/Z が非可換単純群の直積で $Z = Z(L)$ となる。□

定義　G の中で最大の半単純正規部分群を、$E(G)$ と書く。

補題1.13　群 G の中心による商群が非可換単純群の直積ならば、G は $Z(G)$ と G' の中心積になり G' は半単純である。

証明　$\overline{G} = G/Z(G)$ とおく。定理1.10より $\overline{G} = \overline{G}'$ だから、$G = Z(G)G'$ となり、明らかにこれは中心積である。以下 G' が半単純であることを示す。$\overline{G''} = \overline{G}$ より $G = Z(G)G''$。よって、同形定理により $G/G'' \simeq Z(G)/Z(G) \cap G''$ となり、G/G'' は可換。即ち、$G'' \supset G'$ だから $G'' = G'$ となる。また

$$G/Z(G) \simeq G'/G' \cap Z(G),\quad G' \cap Z(G) \subset Z(G')$$

で、$G/Z(G)$ が非可換単純群の直積だから $G'/Z(G')$ もそうである。□

§1f　巾零群

定義　群 G の部分群 $Z_i(G)$ を

$$Z_0(G) = \{1\},\quad Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$$

で定める。このとき、$Z_0(G) \subseteq Z_1(G) \subseteq \cdots$ を G の昇中心列という。

或る整数 r があって $G = Z_r(G)$ となるとき、G を巾零群という。また $G = Z_r(G)$ となる最小の整数 r を G の巾零級（class）という。

G が class r の巾零群で $r > 0$ ならば、$G/Z(G)$ は class $r-1$ の巾零群である。

定理1.14　G が class 高々 r の巾零群であるための必要十分条件は、$r+1$ 個の交換子群 $[G, \cdots, G]$ が $\{1\}$ となることである。

証明　class が高々１の巾零群は可換群だから定理１.14は　ｒ＝１　のとき成り立つ。そこで　ｒ　に関する帰納法により定理を証明しよう。さて［G,…,G］（Gがｒ個）を　H　とおく。いま　G　が class 高々　ｒ　の巾零群とすれば　$\overline{G}=G/Z(G)$　は class が高々　ｒ－１　の巾零群である。よって帰納法の仮定により

$[\overline{G},\cdots,\overline{G}]$（$\overline{G}$　が　ｒ　個）＝｛1｝　を得る。従って

$$\overline{H}=[\overline{G},\cdots,\overline{G}]=\{1\}$$

となるから　$H\subset Z(G)$、よって　$[H,G]=\{1\}$　となる。即ち、

$$[G,\cdots,G]\text{（G　が　ｒ＋１　個）}=\{1\}\ 。$$

逆に　$[G,\cdots,G]$（G　が　ｒ＋１　個）＝｛1｝　と仮定すれば　$[H,G]=\{1\}$，即ち　$H\subset Z(G)$　を得る。よって　$\overline{G}$　は　$[\overline{G},\cdots,\overline{G}]$（$\overline{G}$　が　ｒ　個）＝｛1｝を満たす。帰納法の仮定により　$\overline{G}$　は class 高々　ｒ－１　の巾零群、よって　G　は class が高々　ｒ　の巾零群となる。□

定理１.15（巾零群の性質）

(1)　巾零群の部分群や商群はまた巾零群。

(2)　もし　Z＝Z(G)　について　G/Z　が巾零ならば、　G　も巾零。

(3)　巾零群の直積はまた巾零。

(4)　H　と　K　を群　G　の巾零な正規部分群とする。このとき、HK　も巾零な正規部分群となる。

証明　(4)のみ証明する。H,K　の class をそれぞれ　c,d　として、c＋d　に関する帰納法で示す。H　の class が　0　であることと　H＝｛1｝　であることは同値だから、c,d＞0　と仮定して証明すれば十分である。

L＝HK　とおく。すると

$$L/Z(H)=(H/Z(H))(KZ(H)/Z(H))$$

であるが、H/Z(H)　は class が　c－１、KZ(H)/Z(H)　は class が高々　d　の巾零群である。従って帰納法の仮定より　L/Z(H)　は巾零である。同様に　L/Z(K)　も巾零である。

いま　Z＝Z(H)∩Z(K)　とおくと、自然な単射

$$L/Z\to(L/Z(H))\times(L/Z(K))$$

が存在するから(1),(3)より　L/Z　は巾零である。さらに　$Z\subset Z(L)$　であることと(1)より　L/Z(L)　も巾零。従って(2)より　L　は巾零である。□

注意　上の証明により HK の class は高々 c＋d となる。実際 c＋d となる例がある（H も K も可換であって、HK が可換にならない例。例えば四元数群）。定理1.15は次の方針で別証明される。いま、A,B,C,D を正規部分群とすれば [A,B] ⊂A∩B、また

$$[AB,C] = [A,C]\,[B,C],\quad [A,CD] = [A,C]\,[A,D]$$

が成り立つ。そこで H,K の class をそれぞれ c,d とすれば
[HK,…,HK]（HK の個数が c＋d＋1）は Π[X,Y,…,Z]（各 X,Y,…,Z は H または K; 全体の個数は c＋d＋1）と一致する。X,Y,…,Z の中に H が c＋1 個あれば

$$[X,Y,\cdots,Z] \subset [H,\cdots,H]\ (H\text{ が }c+1\text{ 個}) = \{1\}\ 。$$

H の個数が高々 c ならば K が少なくとも d＋1 個あるので

$$[X,Y,\cdots,Z] \subset [K,\cdots,K]\ (K\text{ が }d+1\text{ 個}) = \{1\}\ 。$$

よって [HK,…,HK]（HK が c＋d＋1個）＝{1} 。□

定義　群 G の中で最大の巾零正規部分群を F(G) と書き、Fitting 部分群という。

§1g　Generalized Fitting 部分群

定義　集合 Ω が群 G に自己同形として作用しているとき、即ち、Ω の各元 σ に G の自己同形 φ(σ) が対応しているとき、G を Ω群という。特に Ω＝Aut(G) のとき、G の Ω部分群を特性部分群といい、H char G と書く。

前節で定義した E(G) と F(G) は特性部分群である。また

K char H, H char G ならば K char G、

K char H, H◁G ならば K◁G

が成り立つ。

補題1.16　極小のΩ部分群は互いに同形な単純群の直積である。

証明　極小のΩ部分群を M とする。M の極小の正規部分群の一つを S とおく。任意の σ∈Ω について φ(σ) は M の自己同形を引き起こすから、σS＝φ(σ)S はまた M の極小正規部分群である。σ が Ω 全体を動くとき σS の全体は M の正規部分群を生成するが、それは明らかにΩ不変。従って仮定に

より M と一致する。まず $S_1=S$ とおく。$S_1\neq M$ ならば $\sigma S\neq S$ を満たす $\sigma\in\Omega$ があるから、そのような σ をとり $S_2=\sigma S$ とおく。S_2 は極小の正規部分群だから $S_1\cap S_2=\{1\}$。よって $[S_1,S_2]=\{1\}$ が成り立ち $S_1S_2=S_1\times S_2$ は直積となる。もし $S_1S_2\neq M$ ならば ρS が S_1S_2 に含まれないような $\rho\in\Omega$ があるから、その一つをとり $S_3=\rho S$ とおく。前と同様に $S_1S_2S_3=S_1\times S_2\times S_3$ となる。この手段を繰り返していけば $M=S_1\times S_2\times\cdots\times S_r$ となり、各 S_i は S と同形である。$S=S_1$ の正規部分群は M の正規部分群となる。S は極小であるから S は単純群で、補題が証明される。□

定義　$F^*(G)=F(G)E(G)$ を、Generalized Fitting 部分群という。

特に $F^*(G)$ は、G の特性部分群である。また $F^*(G)$ は $E(G)$ と $F(G)$ の中心積である。なぜならば $[F,E]\subset E\cap F\lhd E$ で、$[F,E]$ は巾零、特に可解だから補題1.9より $[F,E]\subset Z(E)$ となる。よって補題1.7より $[F,E]=[F,E']=\{1\}$ である。

定理1.17 (Bender-Gorenstein-Walter)
任意の有限群 G について、$C_G(F^*(G))\subseteq F^*(G)$ が成り立つ。

いま $N\lhd G$とする。$\theta_x:N\longrightarrow N;u\longmapsto xux^{-1}$ とおけば、θ_x は N の自己同形写像となる。$\theta_{xy}=\theta_x\theta_y$ が成り立つから $x\longmapsto\theta_x$ は G から Aut(N) の中への準同形写像となり、その核は $C_G(N)$ である。特に $N=F^*(G)$ とすると、$C_G(F^*(G))=Z(F^*(G))$ だから $G/Z(F^*(G))\subseteq Aut(F^*(G))$となる。このことは、$F^*(G)$ を調べることにより G の構造がかなりわかることを示している。

定理1.17の証明　$F^*=F^*(G)$，$C=C_G(F^*)$ と書く。$F^*\supset C$ でないと仮定して矛盾を導く。まず $Z=F^*\cap C$ とおく。F^* char G より C char G，Z char G となる。仮定より $Z\subseteq H\subset C$，H char G となる極小の部分群 H がある。

H/Z が可換とすると、$Z\subset F^*$ より $Z\subset Z(H)$ だから H は巾零。よって $H\subset F\subset F^*$，$H\subset F^*\cap C=Z$ となり H の定義に矛盾する。

次に、H/Z が非可換とする。H/Z は G/Z の極小Aut(G) 部分群であるから、補題1.16より H/Z は非可換な単純群の直積である。よって $Z=Z(H)$

となり、補題１.13より H は Z と H′ との中心積で H′ は半単純である。
H char G より H′ char G だから、$H' \subset E \subset F^*$。従って $H = ZH' \subset F^*$
となり、前と同じ矛盾がおこる。□

第２章　散在群の歴史的解説

有限群の長年の大問題であった単純群の分類は、1981年２月に完成した。それに依れば、有限単純群は次の４種類に分類される。

１）素数位数の巡回群
２）５次以上の交代群
３）Lie 型の単純群
４）26個の散在群（Sporadic groups）

ここで１）～３）は群を構成する一般的原理があってそれぞれ無限系列をなし４）は系列に入らない例外的な群で26個別々に定義されている。

有限群が本格的に研究され始めたのは、Galois の貢献が大きく、単純群という概念もGalois によってあたえられている。その後 Jordan らによって発展してきた。単純群の分類に関しては1950年代の初め、Brauer のプログラムのもとに第一歩を歩み始め、1960年代になり Feit-Thompsonの定理（奇数位数の群は可解である。）が示された。同じ頃、階数１の Lie型の単純群が分類されるに至ってますます分類の気運が高まっていった。無限系列の単純群は比較的早くから知られていたのに対し、５つの Mathieu群以外の散在群21個は1964年以降に見つかっている。

この章では§２ａで Brauerのプログラムのもとになった Brauer-Fowlerの定理及びThompsonの位数公式を解説する。§２ｂで散在群、特に原始的可移拡大の群と Jankoの群 J_1の構成に関する話題とそれらの単純性を示すための１つ１つの群の難しい性質にふれない多少なりとも統一的で初等的な方法を紹介する。

§２ａ　Brauer-Fowler の定理と Thompson の位数公式

Ｇ は有限群とする。

補題２．１　ｕ，ｖ∈Ｇ　を位数２の元とする。ｗ＝ｕｖ とおけば $uwu^{-1}=w^{-1}$、すなわち〈ｕ，ｖ〉は２面体群で〈ｗ〉は指数２の正規な巡回部分群である。今 ｗ の位数を ｎ とおけば〈ｕ，ｖ〉の位数は ２ｎ、ｎ が奇数ならば ｕ と ｖ は〈ｕ，ｖ〉の中で共役である。

証明　$u=u^{-1}$、$v=v^{-1}$ だから $uwu^{-1}=u(uv)u^{-1}=vu=w^{-1}$ が成り立つ。最後の部分は Sylow の定理から証明できる。直接にも、$(uv)^{2m+1}=1$ とすると $(uv)^{2m}=vu$ だから $(uv)^{m}u(vu)^{m}=(uv)^{2m}u=v$。よって $x=(uv)^{m}$ とおくと $xux^{-1}=v$ となる。□

補題２．１を応用するには群環の言葉で表すのがよい。

Ｚ を整数の環、Γ＝ＺＧ を Ｚ 上の群環とする。特にその中心を考える。Ｇ の共役類を $C_0=\{1\}, C_1, \cdots, C_k$ とし、g_i を C_i の元の中心化群の位数とする。$g=|G|$, $n_i=|C_i|$ とおけば $n_i=g/g_i$ である。Γの中心は $K_i=\sum_{x\in C_i} x$ で生成される、すなわち、

$$Z(\Gamma)=\sum_{i=0}^{k} \mathbb{Z}K_i。$$

いま $C_1, \cdots, C_s$ は位数２の元の共役類全体、Ｍ は $K_1, \cdots, K_s$ のうちｍ個の和とする。$M^2=\sum_{i=1}^{k} a_iK_i$ とおく。M^2 は ｕｖ（ｕ，ｖ は位数２の元）という形の元の和である。そこで ｗ＝ｕｖ（ｕ，ｖ は位数２の元）とおく。$w\in C_i$ とすれば a_i は ｗ を ｕｖ という形にかく仕方の数である。$w^2=1$ ならば、$uwu^{-1}=w$ より、a_i は $C_G(w)-\{w\}$ に含まれ Ｍの中に現れる元の数以下となる。したがって $1\leqq i\leqq s$ ならば $a_i\leqq g_i-2$。一方、$i>s$ ならば $w\neq w^{-1}$。ところで $uwu^{-1}=w^{-1}=u'wu'^{-1}$ のとき $u^{-1}u'\in C_G(w)$。したがって ｕｖ＝ｗ を満たし Ｍ の中に現れる元 ｕ，ｖ の組は高々 $|C_G(w)|$ だから、$a_i\leqq g_i$ となる。

いま ｕｖ という形の元で位数≧３のものを含む共役類を $C_{s+1}, \cdots, C_t$ とおけば、$a_i=0$（$i>t$）である。特に $M=K_{i_0}$（$1\leqq i_0\leqq s$）とすると、

$$M^2=n_{i_0}K_0+\sum_{i=0}^{t} a_iK_i。$$

M は n_{i_0}個の元の和だから、この式の右辺は $n_{i_0}^2$ 個の和となる。したがって

$$n_{i_0}^2 = n_{i_0} + \sum_{i=1}^{t} a_i n_i$$

となる。いま、G が非可換単純群とすれば $g_i < g\ (i \geqq 1)$ である。
$h = \max\{g_1, \cdots, g_t\}$ とおけば $g_i \leqq h\ (1 \leqq i \leqq t)$、特に $g_{i_0} \leqq h$ である。$a_i \leqq g_i$ かつ $\sum_{i=1}^{t} n_i < g$ だから上の式より

$$g/g_{i_0} \cdot (g/g_{i_0} - 1) < hg \quad 。$$

したがって　$g/h < g_{i_0}^2 + g_{i_0}/h \leqq g_{i_0}^2 + 1$ となり、
$g/h \leqq g_{i_0}^2$ を得る。この式から G は指数が高々 $g_{i_0}^2$ の部分群を含んでいることがわかる。したがって G は $\Sigma_j\ (j \leqq g_{i_0}^2)$ の部分群と考えられる。

以上をまとめると、位数２の元 t を含む非可換単純群の位数は $C_G(t)$ の位数により定まるある定数 N を越えない。$C_G(t)$ の構造が与えられればそのような位数２の元を含む単純群は有限個しかない。これが Brauer-Fowler の定理で、Brauer のプログラムのもととなる。

以下 G は任意の有限群として、記号はいままでのものを用いる。
$1 \leqq i < j \leqq s$ とし $K_i K_j = \Sigma a_k K_k$ を考える。この時 $u \in C_i$ と $v \in C_j$ は共役でないから、前述の補題２．１より uv の位数は偶数である。そこで uv の巾のうち位数２の元がある。いま集合

$$\{(u, v) \in C_i \times C_j \mid uv \text{ の巾が } C_k \text{ に入る } (1 \leqq k \leqq s)\}$$

を考え、その元数を a_{ijk} とかく。このとき

$$n_i n_j = \sum_{k=1}^{s} a_{ijk} n_k$$

を得る。$u \in C_i, v \in C_j$ に対して uv の巾が　$t \in C_k$ になるとすると、u, v は共に $C_G(t)$ に含まれる。したがって a_{ijk} は $C_G(t)$ の構造及びその位数２の元が G のどの共役類に含まれるかが分かれば計算できる。上の式より

$$g/g_i \cdot g/g_j = \Sigma a_{ijk} \cdot g/g_k$$

を得、したがって　$g = g_i g_j \Sigma a_{ijk}/g_k$ となる。

これが Thompson の位数公式と呼ばれるものである。

§２ｂ　散在群の単純性の初等的証明

ここでは26個の散在群を次の４つの型に分けて、主として最初の２つの型についての統一的証明法を解説する。

Ⅰ）与えられた群の原始的可移拡大として定義される群

Ⅱ）位数２の元の中心化群の構造が与えられた上で定義される群

Ⅲ）Fisher群　M(22), M(23), M(24)′　（３互換の共役類から定義される群）

Ⅳ）Conway群　・1, ・2, ・3　(Leech lattice の自己同型群から定義される群)

（１）　Ⅰ)型の群の統一的な証明

まずⅠ)型に含まれる散在群の構成について簡単に解説する。G が H の原始的可移拡大であるとは、G が或る集合 Ω の上の原始的置換群で、１点の安定化群が H となる事である。Ⅰ)型には次の10個の散在群がふくまれる。

＊ Mathieu群 $M_{24}, M_{23}, M_{22}, M_{12}, M_{11}$

これらの群は1860年代に発表された多重可移群で、次の可移拡大の系列がある。

$$M_{12} \supset M_{11} \supset M_{10} (= A_6 \cdot 2)$$
$$M_{24} \supset M_{23} \supset M_{22} \supset M_{21} = PSL(3,4)$$

Mathieu群以外のⅠ)型の群はすべて階数３の原始的可移群である。

＊ Jankoの２番目の群 J_2

Jankoがこの単純群が存在するであろうと発表してまもなく、M. Hallが次数100の可移群として計算機を用いて構成した。その後すぐに 100個の点からなるグラフの自己同型の作る群として計算機なしで構成された（鈴木，Tits）。

＊ Higman-Sims群 HS

HigmanとSimsがHallと類似の方法を用いてM_{22} の次数100の可移拡大を構成した。M_{24} の３つの置換表現（次数１, 22, 77）から頂点の数が 100のグラフを作り、そのグラフの自己同型群が頂点の集合の上に可移に作用することを証明した。

＊ 鈴木群 S

鈴木はHigman-Simsと同様な方法を用いて階数３の可移拡大の系列

$$PSL(2,7) \subset PSU(3,3) \subset J_2 \subset G_2(4) \subset S$$

を構成し散在鈴木群 S を発見した（ここで $G_2(4)$ は４元体上で定義されるG_2型のChevalley群）。

＊ McLaughlin群 M^C

上の鈴木群の系列は $A_6 \subset PSL(3,4) \subset PSU(4,3)$ という階数３の可移拡大の類似として構成されたものであるが、McLaughlinはこの系列で PSU(4,3) をさらに可移拡大して散在単純群 M^C が得られることを証明した。

＊ Rudvalis群 Ru

RudvalisがTits群の階数３の原始的可移拡大の存在する可能性のあることを発表した。その群が存在すれば位数２の中心をもつ中心拡大があり、その中心拡大は28次元の表現をもつことが証明された。その後Conway-Walesは28次元空間のベクトルを用いて頂点の数が4060のグラフを構成し、その自己同型のつくる群として Ru の中心拡大を構成した。

以上がⅠ)型の散在群である。J_2 にはじまる階数３の原始的可移拡大の群の次数と安定化群を表にしておく。

群	次数	安定化群
J_2	$2^2 \cdot 5^2$	PSU(3,3)
HS	$2^2 \cdot 5^2$	M_{22}
S	$2 \cdot 3^4 \cdot 11$	$G_2(4)$
M^C	$5^2 \cdot 11$	PSU(4,3)
Ru	$2^2 \cdot 5 \cdot 7 \cdot 29$	Tits群

さてⅠ)型の散在群の単純性の一般的証明法は次の補題による。

補題２.２　G はｎ次の原始置換群で、一点の安定化群は単純であると仮定する。このとき一般には G は単純群である。例外の場合は G が位数 n の極小正規部分群を含む。特に n は単純群の位数の巾となる。

証明　G が作用しているｎ元集合を X とし、その一点 $x_0 \in X$ を定める。x_0 の安定化群を H とおく。即ち $H = \{\sigma \in G \mid \sigma(x_0) = x_0\}$。G が原始置換群という仮定は、G が X 上可移で、H が G の極大部分群であることと同値である。

G が単純でないと仮定し、G の真の正規部分群の一つを N とする。まず N が H に含まれていないことを示そう。そこで $N \subset H$ と仮定する。G は可移だから、任意の $x \in X$ に対して $\tau(x_0) = x$ を満たす $\tau \in G$ がある。任意の $\rho \in N$ について $\tau^{-1} \rho \tau \in N$。よって $N \subset H$ という仮定から

$\tau^{-1}\rho\,\tau(x_0)=x_0$、即ち　$\rho\,\tau(x_0)=\tau(x_0)$

を得る。よって $\rho(x)=x$ がすべての $x\in X$ について成り立つ。従って $\rho=1$。これより $N=\{1\}$ となり、N が真の正規部分群という仮定に反する。よって N は H に含まれていない。この場合 HN は H より真に大きい部分群となる。ところで H は G の極大部分群だから $HN=G$ を得る。

次に $H\cap N$ を考える。これは H の正規部分群であるから、H が単純群であるという仮定により $H\cap N=H$ または $H\cap N=\{1\}$ を得る。ところで $H\cap N=H$ ならば $H\subset N$ だから $N=HN=G$ となり、N が G の真の正規部分群という仮定に矛盾する。よって $H\cap N=\{1\}$。

上のことから G の真の正規部分群 N は $G=HN$ および $H\cap N=\{1\}$ を満たす。同形定理から $G/N\simeq H$，$|N|=n$ を得る。H が G の極大部分群だから N が G の極小正規部分群であることがわかる。補題1.16により N は互いに同形な単純群いくつかの直積となる。よって n は或る単純群の位数の巾となる。□

例えばHSについてこの補題をあてはめる。$n=100$ で M_{22} は単純群だから、HSが単純でないとすると、位数$100=2^2\cdot5^2$ または $10=2\cdot5$ の単純群が存在することになり矛盾が起こる。同様に、I)型の散在群で階数3の原始置換群であるものについても $n>100$ ならば素数11または29について Sylowの定理を適用すれば位数nの単純群が存在しない事がわかる。

M_{24}, M_{22}, M_{12} についても位数nの単純群が存在しないことが証明される。M_{23} の場合は位数23の正規部分群を含まない事を示さねばならないが、それは容易に証明される。M_{11} については補題2.2の仮定を満たさないので単純性の証明は異なるが、補題2.2による方法は統一的証明という観点からみて、ほぼ満足すべき証明法であろう。

（2）　Ⅱ）型の群の統一的証明

Brauer-Fowler の定理にもとづく Brauer のプログラムの中で、単純群の位数２の元の中心化群となる群はどういう群かという問題が起こった。その問題を調べていくうちに例外となる場合が起こって来た。そのうち一番最初に現れた例外の場合は Jankoの群J_1である。$G=J_1$ の位数２の元 t の中心化群は $C_G(t)=\langle t\rangle \times A_5$ となっている。中心化群としてこのような群を考えたのは次の理由による。1955年にChevalley群がはっきり定義された後、Steinberg群，鈴木群，Ree群，Tits群が現れ1960年始めにはLie型の単純群は全部現れた。その中でG_2 型の Ree群の位数２の元の中心化群は

$$C_G(t)=\langle t\rangle \times PSL(2,3^n)$$

となっている。そこで可換な Sylow２-群をもつ単純群 G があって位数２の元の中心化群が $C_G(t)=\langle t\rangle \times PSL(2,q)$（q は奇素数）となっているとする。このとき $q>5$ ならばqは３の巾で、G は Ree群と非常によく似ている。この場合 G が実際 Ree群と一致することはずっと後になって証明された。$q=5$ のときが例外の場合で、このときに J_1 が現れた。実際 Janko は GL(7,11) の部分群として J_1 を書き上げた。

Ⅱ）型の散在群と位数２の元 t の中心化群 $C_G(t)$ を表にしておく。

単純群		$C_G(t)$
Janko群	J_1	$\langle t\rangle \times A_5$
〃	$J_3(J_2)$	$2^{4+1}A_5$
〃	J_4	$2^{12+1}(3M_{22}\cdot 2)$
Held群	He	$2^{6+1}PSL(3,2)$
Lyons群	Ly	$2A_{11}$
O'Nan群	ON	$4PSL(3,4)\cdot 2$
Fischer群	F_2	$2({}^2E_6(2))\cdot 2$
Thompson群	F_3	$2^{8+1}A_9$
原田群	F_5	$2HS\cdot 2$
Monster	F_1	$2F_2$; $(2^{24+1}(\cdot 1))$

ここで $Y=2^{2n+1}X$ とは、Y が extraspecial ２-群 E（$|Z(E)|=2$，$|E/Z(E)|=2^{2n}$）を正規部分群としてもち、$E=F^*(Y)$、さらにその剰余群が X と同型となることを表す。$Y=mX$ とは X は単純群で、$Y=[Y,Y]$，$Y/Z(Y)\cong X$，$Z(Y)$ は位数mの巡回群であることを表す。$Y=X\cdot 2$ とは Y が X を指数２の正規部分群としてもち Y は位数２の巡回群と X の直積でないことを示す。また $mX\cdot 2$ は $(mX)\cdot 2$ を表す。

さて次の性質をもつ散在群 G を第２種の散在群と呼ぶ。位数２の元ｔを含み、

1) $\langle t^G \rangle = G$、 2) $C_G(t)$ が上の表に出てくる構造をもつ。

Ⅱ）型の散在群の単純性を証明するための補題は次である。

補題２．３ G の位数は４で割り切れるとする。G に含まれる或る位数２の元ｔについて以下の条件が成り立つとする。

(1) $C_G(t) \triangleright H \neq \{1\} \Rightarrow t \in H$, (2) $G = \langle t^G \rangle$

このとき G は単純である。

この補題を F_1 にあてはめる。補題２．３の条件(１)を満たす事をいえば F_1 が単純であることが証明される。ところで、$2F_2$ がｔを含まない正規部分群 D をもつとすると $2F_2 = D \times \langle t \rangle$ となり $2F_2 = (2F_2)'$ に矛盾する。中心化群が F_5 の場合のような構造を持つときも同様の証明法で単純性が示せる。

F_3 の場合は、$K = 2^{8+1}A_9$の正規部分群 H について $E \cap H \neq \{1\}$ とする (E はextraspecial ２群).このとき $E \cap H$ は E の正規部分群だから１でない Z(E) の元を含むが $\langle t \rangle = Z(E)$ より $t \in H$ となる。$H \cap E = \{1\}$ とすると $H \subset C_K(E)$ となるが、$C_K(E) = Z(E) \subset E$ であることより矛盾が起こる。よって F_3 が(１)を満たすことがいえ単純性が証明された。

他のⅡ）型の散在群についても上の場合と同様な方法で(１)を満たす事がいえ単純性が証明される。

補題２．３の証明 N を G の正規部分群とする。

１）|N| を偶数とする。位数２の元ｔを含む G の Sylow ２-群を Q とすると $Q \cap N$ は N の Sylow ２-群だから {1}でない。一方 $Q \triangleright Q \cap N$ より定理１．３(1)から $Q \cap N \cap Z(Q) \neq \{1\}$。したがって

$$C_G(t) \triangleright N \cap C_G(t) \supset N \cap Z(Q) \neq \{1\} .$$

仮定(１)より $t \in N$ だから $G = \langle t^G \rangle = N$ を得る。

２）|N| を奇数とする。また $N \neq \{1\}$ とする。このとき条件 (1) より $C_G(t) \cap N = \{1\}$、よって Burnside の補題により N の各元 x について

$$t x t^{-1} = x^{-1} (\neq x)$$

が成り立ち、特に N は可換群となる。よって $G/C_G(N)$ を Aut(N) の中に埋め込むと、ｔは -1 に対応している。-1 は Aut(N) の中心に含まれるから $G \triangleright \langle t, C_G(N) \rangle$ となる。$|\langle t, C_G(N) \rangle|$ は偶数だから１)により G と一致する。一方 $C_G(N) \neq G$ より$|C_G(N)|$ は偶数でなく４が|G| の約数であることに矛盾する。□

最後に、Ⅲ)型の散在群について M(22) と M(23) は補題２．３を使って単純性が証明される。M(24)′は別で、M(24)′が M(24) の唯一の真の正規部分群であることから証明される（M(24)′は M(23) の原始的可移拡大だから、補題２．２が適用されるが、この場合はSylowの定理だけでは単純性は証明されない）。Ⅳ)型の群については第４章で単純性が証明される。

第２章のしめくくりとして26個の散在群の位数を表にしておく。

散在群	位数
M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
J_2	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$
J_3	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$
J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$
HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$
S	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
M^C	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$
Ru	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$
He	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$
Ly	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$
ON	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$
・1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$
・2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
・3	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$
M(22)	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$
M(23)	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$
M(24)	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
F_2	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$
F_3	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$
F_5	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$
F_1	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$

第３章　散在群の構成　M_{24}（Conway の方法）

まず、$SL_2(23)=\{\sigma\in M_2(\mathbb{F}_{23}) \mid \det\sigma=1\}$ を考える。これは、23元体 $\mathbb{F}_{23}$ の上の２次の正方行列で行列式が１のもの全体である。この群の中心で割った商群、即ち

$$L=L_2(23)=SL_2(23)/\{\pm I\}$$

を L とおく。計算する際には $SL_2(23)$ の中で σ と $-\sigma$ を同一視して考えればよい。$SL_2(23)$ は、

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} x' \\ y' \end{pmatrix} \qquad x,y,x',y'\in\mathbb{F}_{23}$$

により、２次元の $\mathbb{F}_{23}$ 上のベクトル空間に作用する。この作用は可移ではなく、また０を除いて考えても２重可移ではないので、それよりは射影直線 Ω 上に作用させる方がよい。ここで射影直線というのは、２次元のベクトル空間上の１次元部分空間全体のことである。つまり、

$$\begin{pmatrix} x \\ y \end{pmatrix}\neq 0 \text{ に対して, } \begin{pmatrix} x \\ y \end{pmatrix}\text{と}\begin{pmatrix} ax \\ ay \end{pmatrix}\ (a\neq 0)$$

を同一視することによって得られる同値類の集合が射影直線 Ω である。いま、

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix},\quad \begin{pmatrix} x \\ 1 \end{pmatrix} \qquad x\in\mathbb{F}_{23}$$

で代表される元をそれぞれ ∞，x と表すことにすれば、

$$\Omega=\{\infty,0,1,\cdots,22\}$$

であり、この24個の点上に L が作用する。

ここで実際に L の作用する様子を見てみる。

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}=\begin{pmatrix} a \\ c \end{pmatrix}\ \text{より}\ \infty\longmapsto\begin{cases} \infty & (c=0) \\ a/c & (c\neq 0) \end{cases}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ 1 \end{pmatrix}=\begin{pmatrix} ax+b \\ cx+d \end{pmatrix}\ \text{より}\ x\longmapsto\begin{cases} \infty & (cx+d=0) \\ \dfrac{ax+b}{cx+d} & (cx+d\neq 0) \end{cases}$$

となる。従って射影直線上の点の L による作用は、

$$x\longmapsto\frac{ax+b}{cx+d}$$

と一次分数変換の形で書ける。（ここで、分母が０のときは ∞，また $x=\infty$ のときは $\dfrac{a+d/x}{c+b/x}=\dfrac{a}{c}$ と約束する。）

命題３．１　Ｌ は Ω の上に２重可移に作用する。

証明　$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ は ∞，０を $\begin{pmatrix} a \\ c \end{pmatrix}$，$\begin{pmatrix} b \\ d \end{pmatrix}$ で代表される元にうつす。射影直線上の相異なる２点は一次独立なベクトル２つで表現されるからＬは２重可移である。□

注意　これは別にベクトル空間が２次元でなくとも一般に、

$$SL_n(\mathbb{F}_q)=\{\sigma\in M_n(\mathbb{F}_q)\mid \det\sigma=1\}$$

を n-1 次元の射影空間に作用させると２重可移になる。

あとの計算に便利なようにＬの中に３つの特別な元を定める。

$$\alpha\leftrightarrow\begin{pmatrix}1&1\\0&1\end{pmatrix}\qquad \alpha:\infty\mapsto\infty,\ x\mapsto x+1,$$

$$\beta\leftrightarrow\begin{pmatrix}5&0\\0&14\end{pmatrix}\qquad \beta:\infty\mapsto\infty,\ x\mapsto 2x,$$

$$\gamma\leftrightarrow\begin{pmatrix}0&1\\-1&0\end{pmatrix}\qquad \gamma:\infty\leftrightarrow 0,\ x\mapsto -1/x\ (x\neq 0,\infty)。$$

$\gamma\alpha\gamma^{-1}=\begin{pmatrix}1&0\\-1&1\end{pmatrix}$ ということから　$L=\langle\alpha,\beta,\gamma\rangle$　とわかる。

次に Ω を Q と N とに分解する。

Q＝平方元の全体＝{0，1，2，3，4，6，8，9，12，13，16，18}，

N＝Ω－Q＝{∞，5，7，10，11，14，15，17，19，20，21，22}，

Q'＝Q－{0}，N'＝N－{∞}。

$\mathbb{F}_{23}$ では $2=5^2$ であるので、βQ＝Q。β の位数は11だから次の事が成り立つ。

命題３．２　〈β〉 は Q'，N'上可移に作用する。

Ω 上の置換 δ を

$$\delta(x)=\begin{cases} x^3/9 & (x\in Q)\\ 9x^3 & (x\in N)\end{cases}$$

で定義する。すなわち、

$$\delta=(\infty)(3)(1\ \ 18\ \ 4\ \ 2\ \ 6)(5\ \ 21\ \ 20\ \ 10\ \ 7)$$
$$(0)(15)(22\ \ 14\ \ 17\ \ 11\ \ 19)(9\ \ 12\ \ 8\ \ 16\ \ 13)。$$

上の記号において上段の元 a の下は $-a^{-1}$ である。

M＝〈α，β，γ，δ〉 とおく。以下 M が M_{24} と同形になることを示す。

命題３．３　M は Ω 上５重可移になる。

証明　$\alpha^2\delta = (\infty)(0\ \ 2\ \ 8\ \ 18\ \ 6\ \ 3\ \ 5)$
$(4)(1\ \ 20\ \ 12\ \ 10\ \ 9\ \ 14\ \ 19)$
$(7)(11\ \ 21\ \ 22\ \ 16\ \ 15\ \ 17\ \ 13)$

となり、$\alpha^2\delta$ は $(1^3 7^3)$ 型の元である。

まず M は命題３．１より２重可移である。そこで２点の安定化群を考えるとそれは $(1^2 11^2)$ 型と $(1^3 7^3)$ 型の元をもつので残りの22点の上に可移になる。よって M は３重可移である。

３点の安定化群は，$(1^3 7^3)$ 型および $(1^4 5^4)$ 型の元を含むので前と同様に４重可移になる。

さて、あとは５重可移性であるが、ここで計算により

$$\alpha^2\gamma\delta = (\infty\ \ 2\ \ 21\ \ 10\ \ 15\ \ 5\ \ 14\ \ 6\ \ 1\ \ 16\ \ 9\ \ 0)(3\ \ 17\ \ 4\ \ 13\ \ 7\ \ 11\ \ 8\ \ 12\ \ 22\ \ 20\ \ 18\ \ 19)$$

となるから $(\alpha^2\gamma\delta)^3$ は (4^6) 型である。よって４点集合の安定化群は (4^6) 型および $(1^4 5^4)$ 型の元を含むから他の20点上に可移，すなわち M は５点集合上に可移に作用している。

５点集合を１つ決めると，その上に 5 cycle となるものがある。ここで

$$\alpha\delta = (\infty)(21)(3\ \ 4)(11\ \ 20)(0\ \ 1\ \ 19)(2\ \ 7\ \ 6)(5\ \ 22\ \ 15\ \ 16\ \ 14\ \ 18)(8\ \ 17\ \ 12\ \ 9\ \ 13\ \ 10)$$

と計算できるので $(\alpha\delta)^3$ は $(1^8 2^8)$ 型である。すなわち与えられた５点集合上に互換の形で働く元がある。よって M は与えられた５点集合上に Σ_5 をひきおこす。したがって M は５重可移である。□

ここで Ω の部分集合をその特性関数で表し、それを２元体上の24次元ベクトル空間 V の元とみることにより Ω の部分集合を V の元と同一視する。次に

$$N_\infty = \Omega,\ N_0 = N,\ N_i = \{n - i \mid n \in N'\} \cup \{\infty\}$$

とおき、$\{N_\infty, N_0, N_1, \cdots, N_{22}\}$ が生成する V の部分空間を $\mathcal{C}$ と表す。
V から $\mathcal{C}$ への写像 φ を

$$\varphi(S) = \sum_{i \in S} N_i \qquad (S \subset \Omega)$$

で定義する。

このとき $\varphi(\{i\}) = N_i$ $(i \in \Omega)$ だから $\mathcal{C} = \mathrm{Im}\,\varphi$ である。

注意　ここで、$\alpha N_i = N_{i-1}$，$\alpha N_\infty = N_\infty$，$\beta N_i = N_{2i}$，$\beta N_\infty = N_\infty$ であるから α も β も $\mathcal{C}$ を不変にしている。

S,T を Ω の部分集合とすると、V の元として $S+T=S\cup T-S\cap T$、$2N_i=0$ であるから $\varphi(S+T)=\varphi(S)+\varphi(T)$ となる。よって φ は V から $\mathcal{C}$ の上への準同形である。

命題3.4　$\dim\mathcal{C}=12$, $\mathcal{C}=\ker\varphi$ で $\{N_\infty, N_i(i\in Q')\}$ は$\mathcal{C}$の基になる。

証明　$\dim\mathcal{C}=k$ とすると、$\dim\ker\varphi=24-k$ である。

まず $\mathcal{C}\subset\ker\varphi$ を証明する。すなわち、

$$\varphi(N_i)=0 \quad (i\in\Omega)$$

を示せばよい。$\varphi(N_\infty)=\sum_{i\in\Omega} N_i$ の右辺において∞は24回現れる。また $0,1,2,\cdots,22$ はそれぞれ12回現れる。よって

$$\varphi(N_\infty)=0。$$

$\varphi(\{i\})=N_i$, $\varphi(\alpha S)=\alpha^{-1}\varphi(S)$ だから$\varphi(N_i)$ $(i\in\Omega-\{\infty\})$ のかわりに $\varphi(N_0)$を計算すればよい。

$\varphi(N_0)=\sum_{i\in N} N_i$ の右辺において $\infty,0$は12回現れる。N' において1は N' の元の差として5通りに表される。つまり $1\in N_i$ となる $i\in N$ は6通りある。$\varphi(N_0)$ はβ不変だからすべての0でない平方元は6回現れる。また、非平方元も6回現れる。よって、

$$\varphi(N_0)=0 \quad 。$$

ゆえに $\mathcal{C}\subset\ker\varphi$ である。これより、$k=\dim\mathcal{C}\leqq\dim\ker\varphi=24-k$。従って $k\leqq12$ となる。

あとは $\langle N_\infty, N_i(i\in Q')\rangle$ の中に12個の一次独立な元が存在することを確かめればよい。実際、最後に並ぶ0の数が添数と共に増えていくようなベクトルの列、例えば

$$B_0=N_\infty,\ B_1=N_1,\ \cdots,\ B_4=N_4,\ B_5=N_\infty+N_1+N_6,\cdots$$

が構成できる。従って $\{N_\infty, N_i(i\in Q')\}$ は $\mathcal{C}$ の基である。□

注意　$\mathcal{C}$ の次元が12以上であることは、次のようにしてもわかる。

$D_1=\varphi(\{\infty, 4, 8, 9\})$とおくと、

$$N_4=\{\infty, 1, 3, 6, 7, 10, 11, 13, 15, 16, 17, 18\}$$
$$N_8=\{\infty, 2, 3, 6, 7, 9, 11, 12, 13, 14, 20, 22\}$$
$$N_9=\{\infty, 1, 2, 5, 6, 8, 10, 11, 12, 13, 19, 21\}$$

より $D_1=\{0, 1, 2, 3, 4, 7, 10, 12\}$ を得る。$D_{i+1}=\alpha^i(D_1)$ とおけば $D_i\in\mathcal{C}$ であり、やはり最後に並ぶ0の数を考えて $\{N_\infty, D_1, D_2, \cdots, D_{11}\}$ は一次独立である。

命題３．５　M は $\mathcal{C}$ を不変にする。

証明　まず、$\gamma^2=\delta^5=1$，$\gamma\delta=\delta\gamma$ より $M=\langle\alpha,\beta,\gamma\delta\rangle$ である。
α,β は $\mathcal{C}$ を不変にしており、

$$\gamma\delta(N_\infty)=N_\infty$$

であるから、あとは $\gamma\delta(N_i)\in\mathcal{C}$ $(i\in Q')$ を示せばよい。
命題３．２より $N_i=\beta^j(N_1)$ だから $\gamma\delta(N_i)=\gamma\delta\beta^j(N_1)$ であり、
ここで $\delta\beta\delta^{-1}=\beta^3$ であるから、

$$\left\{\begin{array}{l}\text{なぜならば}\\ \delta\beta:x\mapsto 2x\mapsto\left\{\begin{array}{l}(2x)^3/9\\ 9(2x)^3\end{array}\right.\\ \beta^3\delta:x\mapsto\left\{\begin{array}{l}x^3/9\\ 9x^3\end{array}\right.\mapsto\left\{\begin{array}{l}8x^3/9=(2x)^3/9\\ 8\cdot 9x^3=9(2x)^3\end{array}\right.\end{array}\right.$$

$\gamma\delta\beta\delta^{-1}\gamma^{-1}=\beta^{-3}=\beta^8$。よって $\gamma\delta\beta^j(N_1)=\beta^{8j}(\gamma\delta(N_1))$ となる。
結局、$\gamma\delta(N_1)\in\mathcal{C}$ を示せばよい。$S=\{\infty,6,8,13,16,18\}$ とすると、
$\gamma\delta(N_1)=\varphi(S)\in\mathcal{C}$ である（各自チェックされたい）。□

さて、$\mathcal{C}_n=\{x\in\mathcal{C}\mid|x|=n\}$，$\mathcal{D}=\mathcal{C}_8$ とおく。

定義３．６　P を v 点からなる集合、B を P の k 点集合全体の部分集合とする。$D=(P,B)$ が $t-(v,k,\lambda)$ デザインであるとは、P の任意の t 点に対して、それを含む B の元の数が λ 個になっているときをいう。

定理３．７　$\mathcal{D}$ は $5-(24,8,1)$ デザインである。

注意　$\lambda=1$ のとき、即ち $t-(v,k,1)$ デザインを Steiner system という。
特に $4-(11,5,1)$，$5-(12,6,1)$，$3-(22,6,1)$，$4-(23,7,1)$，
$5-(24,8,1)$ デザインは一意的に定まることが知られていて、これらは Witt system と呼ばれる。これらの自己同形群は順に M_{11}，M_{12}，M_{22}，M_{23}，M_{24} である。
（詳しくは大山豪「有限置換群」、永尾汎「群とデザイン」を参照のこと。）

この定理を証明するために補題をいくつか用意する。

補題３．８　$S,T\in\mathcal{C}$ ならば、$S\cap T$ は偶数個の元を含む。

証明　$S,T\in V$ に対し内積を考えると、

$$|S\cap T|\equiv(S,T)\pmod 2$$
$$=\begin{cases}0 & (\text{共通部分の数が偶数個})\\ 1\end{cases}$$

であるから、$S,T\in\mathcal{C}$ ならば $(S,T)=0$ となることを示せばよい。つまり $(N_i,N_j)=0$ を示せばよいのであるが、$\mathcal{C}$ の内積は α,β で不変だから $i\neq\infty$ なら α を使って０に戻せば、$(N_i,N_j)=(N_0,N_{j-i})$ となる。特に $j\neq 0,\infty$ なら β で不変なことより、j を１などの決まったものにうつすことができる。従って $(N_0,N_1),(N_0,N_{-1}),(N_\infty,N_i)$ が０になることをいえばよい。$(N_\infty,N_i)=0$ は明らかである。他は実際に計算すればよい。□

補題３．９　$S\in\mathcal{C}$ ならば $|S|$ は４で割り切れる。

証明　$\mathcal{C}'=\{S\in\mathcal{C}\mid |S|\equiv 0\pmod 4\}$ $(\subset\mathcal{C})$ とおくと、$\mathcal{C}'$ は V の部分空間になる。なぜならば、$|S+T|=|S|+|T|-2|S\cap T|$ で、$|S|,|T|$ は４で割り切れ、補題３．８より $2|S\cap T|$ も４で割り切れるので $|S+T|$ も４で割り切れるからである。

また、明らかに $\mathcal{C}$ の生成元は $N_\infty,N_i\in\mathcal{C}'$ であるから、$\mathcal{C}'=\mathcal{C}$ となる。よって補題は証明された。□

補題３．10　$S\in\mathcal{C}$ ならば $|S|\neq 4$。

証明　$|S|=4$ と仮定する。$S=\{a,b,c,d\}$ とすれば M は $\mathcal{C}$ を不変にし、M は５重可移（４重可移でよい）であるから M の元で S を $S'=\{a,b,c,e(\neq d)\}\in\mathcal{C}$ にうつすものが存在する。$S+S'\in\mathcal{C}$ であるが、$|S+S'|=2$ であり、これは補題３．９に反する。□

定理３．７の証明　５点集合 $U=\{a_0,a_1,a_2,a_3,a_4\}$ を考える。M は５重可移であるから、$\sigma\{i\}=a_i$ $(i=0,\cdots,4)$ となるような $\sigma\in M$ が存在する。ここで $D_1=\{0,1,2,3,4,7,10,12\}$ をとれば、$\sigma(D_1)$ は U を含む８点集合である。

$B,B'\in\mathcal{D}$ がともに U を含むとする。すると $|B+B'|\leqq 6$ である。ところが $B+B'\in\mathcal{C}$ だから、補題３．９，３．10より $B=B'$ となる。よって $\mathcal{D}$ は 5-$(24,8,1)$ デザインである。□

前に注意した通り、5-(24, 8, 1) デザイン $\mathcal{S}$ は一意的に定まるデザインで、

$$\mathrm{Aut}(\mathcal{S}) = M_{24}$$

である。従って $M \subset M_{24}$ であるが、以下これが一致することを示す。

M は5重可移であり、5点の安定化群の中に $(1^8 2^8)$ 型の元（位数2の元）が存在し、$(\alpha\delta)^2$ は $(1^6 3^6)$ 型であるから、5点の安定化群の位数は最低でも6なので、$|M| \geqq 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 6$ である。

また $|M_{24}| = 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$ だから $|M_{24} : M| \leqq 8$ である。ところが M_{24} の中には指数8以下の部分群は含まれていない。実際、指数8以下の部分群が存在すれば、M_{24} が単純であることより、M_{24} から高々8次の対称群の中への同形が存在してしまうが、これは $|M_{24}| > |\Sigma_8|$ であることに矛盾する。したがって、$M = M_{24}$ でなければならない。

注意　$\mathcal{C}$ は Golay code である。Hamming distance

$$d(x, y) = \#\{x_i \neq y_j \mid x = (x_1, \cdots, x_n),\ y = (y_1, \cdots, y_n)\}$$

を考えれば $\mathcal{C}$ の minimum distance は8である。よって3個の誤りが訂正できる符号である。

第4章　Conway群

Ω, $\mathcal{C}$, $\mathcal{D}$ $(=\mathcal{C}_8)$ は前章の通りとする。

$\mathbb{R}^{24}$ を24次元ユークリッド空間とし、$(\ ,\ )$ をその標準内積、$\{v_\infty, v_0, v_1, \cdots, v_{22}\}$ を一つの正規直交系とする。ここで各 v_i の添数 i は Ω の元とみる。Ω の部分集合 D に対し、$\mathbb{R}^{24}$ の元 V_D を

$$v_D = \sum_{d\in D} v_d$$

で定め、整数環 $\mathbb{Z}$ 上の二つの lattice を次で定義する。

$$\Lambda = \langle\ 2v_D \mid D\in\mathcal{D}\ \rangle_{\mathbb{Z}}\ ,$$

$$\Lambda = \langle\ \Lambda,\ v_\Omega - 4v_\infty \rangle_{\mathbb{Z}}\ .$$

この Λ を Leech lattice と呼ぶ。Λ の部分集合 Λ_m $(m\geqq 0)$ を

$$\Lambda_m = \{x\in\Lambda \mid (x,x)=16m\}$$

で定義する。

さて $\mathcal{D}$ は 5-(24, 8, 1) デザインであったから、そのブロックの数は

$${}_{24}C_5 \,/\, {}_8C_5 = 759$$

である。また $|\mathcal{C}| = 2^{12}$ であるから、与えられた長さをもつ $\mathcal{C}$ の元の個数は次のようになる。

元の長さ	0	8	12	16	24
元の個数	1	759	2576	759	1

補題4.1　$\mathcal{D}$ は $\mathcal{C}$ を生成する。

証明　$D_1 = \{0,1,2,3,4,7,10,12\}\in\mathcal{D}$ であったから、

$$\alpha^n(D_1)\in\mathcal{D}\quad (n=0,1,\cdots,10)$$

であり、これらは一次独立である。これに $\mathcal{D}$ の元

$$B = N_\infty + D_2 + D_3 + D_4 + D_5 + D_7 + D_{10} + D_{11}$$
$$= \{\infty, 0, 2, 4, 5, 6, 10, 11\}$$

を加えて $\mathcal{C}$ の基が得られる。□

命題４．２　Ω の中に４点集合 T を任意にとる。このとき六つの４点集合 $T_0=T, T_1, \cdots, T_5$ が存在して次を満たしている。

$$\Omega = T_0 \cup T_1 \cup \cdots \cup T_5 ,$$

$$T_m \cup T_n \in \mathcal{L} \ (m \neq n) , \quad T_m \cap T_n = \phi \ (m \neq n) 。$$

この分割は T により一意的に定まる。これを T の定める６×４分割という。

証明　T に含まれない元 x を定めると、$T \cup \{x\}$ を含むブロックが一意的に定まる。従って Ω の分割 $T, T_1, \cdots, T_5$ が存在して、$T \cup T_n$ $(n=1, \cdots, 5)$ が丁度 T を含むブロックになる。このとき $m \neq n$ ならば

$$T_m \cup T_n = (T \cup T_m) + (T \cup T_n)$$

は $\mathcal{L}$ の元である。□

補題４．３　$x = \sum_{i \in \Omega} x_i v_i$ $(x_i \in \mathbb{R})$ に対して、x が Δ の元であることと、x が次の３条件を満たすこととは同値である。

(1)　どの x_i も整数で、しかも偶数である。

(2)　$\sum_{i \in \Omega} x_i$ は16の倍数である。

(3)　$S(x) = \{ i \in \Omega \mid x_i \not\equiv 0 \pmod 4 \}$ とおくと、これは $\mathcal{L}$ の元。

証明　Δ_0 を上の３条件を満たす Δ の元全体とする。$x \in \Delta$ ならば、すべての $i \in \Omega$ に対して $x_i \equiv 0 \pmod 2$ であるから、Δ_0 の元 x, y に対し

$$S(x+y) = S(x) + S(y) \in \mathcal{C}$$

が成り立つ。従って Δ_0 は Δ の部分群である。ところが Δ の生成元は Δ_0 に含まれるから $\Delta = \Delta_0$ となり、Δ の元は上の３条件を満たす。

逆の証明のために、次の三つのことを示す。尚、v_D $(D \subset \Omega)$ を (D) とも書くことにする（(i)なども同様）。

(4.4)　Ω の４点集合 T をとれば $4 v_T \in \Delta$ である。

証明　T の定める６×４分割を $T = T_0, T_1, \cdots, T_5$ とすると、

$$4 \cdot (T) = 2 \cdot (T \cup T_1) + 2 \cdot (T \cup T_2) - 2 \cdot (T_1 \cup T_2)$$

は Δ の元である。□

(4.5)　$i, j \in \Omega$、$i \neq j$ ならば $4 v_i - 4 v_j \in \Delta$ である。

証明　二つの４点集合 $T = \{i, a, b, c\}, U = \{j, a, b, c\}$ をとれば、(4.4) より $4 \cdot (i) - 4 \cdot (j) = 4 \cdot (T) - 4 \cdot (U) \in \Delta$ となる。□

(4.6) $i \in \Omega$ ならば $16v_i \in \Lambda$ である。

証明　i を含まない4点集合 T をとれば (4·5) より

$$16\cdot(i)-4\cdot(T)=\sum_{j\in T}(4\cdot(i)-4\cdot(j)) \in \Lambda$$

で、また (4.4) より $4\cdot(T)$ も Λ の元であるから命題が成り立つ。□

補題4.3の逆の証明　$x=\sum_{i\in\Omega}x_i v_i$ が三条件を満たしているとする。

$S(x)\in\mathcal{C}$ で、$\mathcal{C}=\langle\mathcal{D}\rangle$ だから、$S(x)=\Sigma D_j$ ($\{D_j\}\subset\mathcal{D}$) と表せる。

そこで

$$y=x+\Sigma\, 2\cdot(D_j)$$

とおくと、y の v_i に関する係数 y_i はすべて4で割り切れる。また

$\sum_{i\in\Omega}y_i\equiv 0 \pmod{16}$ である。従って(4.5),(4.6)より

$$y=\sum_{i\in\Omega}y_i(v_i-v_\infty)+(\sum_{i\in\Omega}y_i)v_\infty \in \Lambda$$

となり、$x\in\Lambda$ を得る。□

Leech lattice Λ についても同様のことが成り立つ。

定理4.7　$x=\sum_{i\in\Omega}x_i v_i$ ($x_i\in\mathbb{R}$) に対して、x が Λ の元であることと、x が次の3条件を満たすこととは同値である。

(1)　x_i ($i\in\Omega$) はすべて偶数、またはすべて奇数である。

(2)　整数nに対して $S(x,n)=\{i\in\Omega \mid x_i\equiv n \pmod 4\}$ とおくと、これは $\mathcal{C}$ の元である。

(3)　$\sum_{i\in\Omega}x_i\equiv 4m \pmod 8$ である。ここで m は x_i が偶数のとき0、x_iが奇数のとき1である。

証明　補題4.3と同様に、上の3条件を満たす Λ の元全体は Λ の部分群をなし、Λ の生成元が3条件を満たすから、Λ の元も3条件を満たす。

逆に x が3条件を満たすとする。整数 n に対して $y=x+n(v_\Omega-4v_\infty)$ おき、y_i を v_i に関する係数、整数 k を $\sum_{i\in\Omega}x_i=4m+8k$ で定めると

$$\sum_{i\in\Omega}y_i=4m+8k+20n=4(m+2k+n)+16n,$$

$$y_i\equiv m+n \pmod 2$$

である。そこで n を $m+n\equiv 0 \pmod 2$, $m+2k+n\equiv 0 \pmod 4$ となるようにとれば $\sum_{i\in\Omega}y_i\equiv 0 \pmod{16}$, y_i は偶数 ($i\in\Omega$) となる。更に各 $i\in\Omega$ につ

いて $y_i \not\equiv 0 \pmod 4$ と $x_i \not\equiv -n \pmod 4$ とは同値だから y_i が4で割り切れない添数 i の集合は $\mathcal{C}$ の元である（条件(2)）。従って補題4.3より $y \in \Lambda$ を得るから、$x \in \langle \Lambda, v_\Omega - 4v_\infty \rangle = \Lambda$ である。□

Λ の元を基底 $\{v_i\}$ に関する係数で分類してみよう。まず、次を示す。

(4.8) $x \in \Lambda$ ならば (x, x) は16の倍数である。

証明　$S, T \in \mathcal{S}$ に対し

$$(2v_S, 2v_T) = 4 \cdot |S \cap T| \equiv 0 \pmod 8,$$

$$(2v_S, v_\Omega - 4v_\infty) = \begin{cases} 8 \cdot 2 = 16 & (\infty \notin S), \\ -3 \cdot 2 + 7 \cdot 2 = 8 & (\infty \in S), \end{cases}$$

$$(v_\Omega - 4v_\infty, v_\Omega - 4v_\infty) = (-3)^2 + 23 \cdot 1 = 32$$

である。従って、$x, y \in \Lambda$ ならば (x, y) は8の倍数である。故に (x, x) が16の倍数となるような $x \in \Lambda$ の全体は Λ の部分群を作る。ところが Λ の生成元 z について $(z, z) = 32$ だから、この部分群は Λ に一致する。□

注意　これより $\Lambda_m = \{x \in \Lambda \mid (x, x) = 16m\}$ という定義には意味がある。

$\Lambda_1 \cup \Lambda_2$ の元の型とその個数をすべて求めよう。いま $\Lambda_1 \cup \Lambda_2$ の元 $x = \sum_{i \in \Omega} x_i v_i$ $(x_i \in \mathbb{R})$ が与えられたとする。

(1)　x_i がすべて奇数の場合

$24 \leqq \sum_{i \in \Omega} x_i^2$ より $\sum_{i \in \Omega} x_i^2 = 32$ である。従って或る $k \in \Omega$ が存在して

$$x = \left(\sum_{i \neq k} \pm v_i\right) \pm (-3) v_k \qquad (-3, 1^{23}) \text{ 型}$$

である。ここで $-3 \equiv 1 \pmod 4$ に注意すると、前定理より上式の‘±’において‘−’をとる添数 i の集合は $\mathcal{C}$ の元である。よってこの型の元は $24 \cdot 2^{12}$個ある。

(2)　x_i がすべて偶数の場合

$D = \{i \in \Omega \mid x_i \not\equiv 0 \pmod 4\}$ とおく。定理よりこれは $\mathcal{C}$ の元である。

まず $D \neq \phi$ のときを考える。$|D| \geqq 8$、$|x_i| \geqq 2$ $(i \in D)$ より $D \in \mathcal{S}$、$\sum_{i \in \Omega} x_i^2 = 32$ を得る。従って

$$x = \sum_{i \in D} \pm 2 v_i \qquad (2^8) \text{ 型}$$

である。ここで‘−’がk個あるとすると、前定理4.7(3)を用いて

$$0 \equiv \sum_{i \in \Omega} x_i = 2 \cdot (8 - k) - 2k \pmod 8$$

となる。故に k は偶数で、この型の元は $759\cdot 2^7$ 個ある。

次に $D=\phi$ のときを考える。$\sum_{i\in\Omega} x_i \equiv 0 \pmod 8$ より

$$x=\pm 4v_i \pm 4v_j \quad (i\neq j) \qquad (4^2) \text{ 型}$$

であり、‘－’は自由にとれるからこの型の元は ${}_{24}C_2\cdot 2^2$ 個ある。

特に Λ_1 は空集合である。Λ_3, Λ_4 についても同様に元の型とその元数を求めることができる（下表において各項目は、元の型、元数、備考の順である）。

Λ_2 （元数：$2^4\cdot 3^3\cdot 5\cdot 7\cdot 13=196,560$）

(4^2)	${}_{24}C_2\cdot 2^2$	
(2^8)	$759\cdot 2^7$	‘－’は偶数個
$(-3,1^{23})$	$24\cdot 2^{12}$	‘－’は$\mathfrak{C}$の元の上

Λ_3 （元数：$2^{12}\cdot 3^2\cdot 5\cdot 7\cdot 13=16,773,120$）

$(4,2^8)$	$2\cdot 16\cdot 759\cdot 2^7$	-2は奇数個
(2^{12})	$2576\cdot 2^{11}$	-2は偶数個
$(5,1^{23})$	$24\cdot 2^{12}$	
$(-3^3,1^{21})$	${}_{24}C_3\cdot 2^{12}$	

Λ_4 （元数：$2^4\cdot 3^7\cdot 5^3\cdot 7\cdot 13=48\times 8,292,375$）

(8)	$2\cdot 24$	
$(6,2^7)$	$759\cdot 8\cdot 2^7$	非零係数は$\mathfrak{H}$の元の上、‘－’は奇数個
(4^4)	${}_{24}C_4\cdot 2^4$	
$(4^2,2^8)$	$2^2\cdot {}_{16}C_2\cdot 759\cdot 2^7$	± 2は$\mathfrak{H}$の元の上、-2は偶数個
$(4,2^{12})$	$2576\cdot 2^{11}\cdot 12\cdot 2$	± 2は$\mathfrak{C}_{12}$の元の上、-2は奇数個
(2^{16})	$759\cdot 2^{15}$	± 2は$\mathfrak{C}_{16}$の元の上、-2は偶数個
$(5,-3^2,1^{21})$	$24\cdot {}_{23}C_2\cdot 2^{12}$	‘－’は$\mathfrak{C}$の元の上
$(-3^5,1^{19})$	${}_{24}C_5\cdot 2^{12}$	‘－’は$\mathfrak{C}$の元の上

定義　24次の直交群の部分群 $\mathrm{Aut}(\Lambda)$ を ・0 と書く。

補題4.9　・0 の元を正規直交系 $\{v_i \mid i \in \Omega\}$ を用いて行列表示すれば、各成分は有理数でその分母は8の約数とできる。

証明　$\sigma \in$ ・0 とする。各 $i \in \Omega$ について $8v_i \in \Lambda$ であるから、$8\sigma(v_i)$ は $\{v_j\}$ の整係数一次結合である。□

ここでいくつかの記号を導入する。$T \subset \Omega$ に対し符号変換 ε_T を

$$\varepsilon_T : v_i \mapsto \begin{cases} v_i & (i \notin T) \\ -v_i & (i \in T) \end{cases}$$

で定め、$E = \{\varepsilon_T \mid T \in \mathcal{C}\}$ とおく。$\varepsilon_S \cdot \varepsilon_T = \varepsilon_{S+T}$ より E は直交群の部分群である。また M_{24} の元 π は $\mathbb{R}^{24}$ の座標変換 $(v_i \mapsto v_{\pi(i)})$ を引き起こす。これも π と書く。$\pi, \rho \in M_{24}$ ならば

$$(\varepsilon_S \pi) \cdot (\varepsilon_T \rho) = \varepsilon_{S+\pi(T)} \cdot \pi\rho$$

が成り立つから M_{24} は E を正規化する。そこで $N = E \cdot M_{24}$ とおくとこれは半直積で、・0 の部分群であることがわかる。

以下、$N \neq$ ・0 となることを示す。

注意　N の元は $\{v_i\}$ を用いると単項行列として表示される。

補題4.10　$\lambda \in$ ・0 が或る $i, j \in \Omega$ について $\lambda(v_i) = \pm v_j$ となっていれば、$\lambda \in N$ である。

証明　λ の行列表示は、直交変換であることも考えあわせると

$$\begin{array}{c} \\ j \end{array} \begin{array}{c} \begin{array}{ccc} & i & \end{array} \\ \begin{pmatrix} * & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} & * \\ 0 \cdots 0 & \pm 1 & 0 \cdots 0 \\ * & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} & * \end{pmatrix} \end{array}$$

の形である。$k \in \Omega$, $k \neq i$ に対し、$4\lambda(v_i + v_k) \in \Lambda_2$ は上の行列の第 i 列と第 k 列の和の4倍になっている。ところが Λ_2 の元は $(-3, 1^{23}), (2^8), (4^2)$ 型のいずれかだから、これは (4^2) 型である。したがって λ は単項行列で、

$$\lambda = \varepsilon_T \cdot \pi \quad (\pi \text{ は } \Omega \text{ の置換}, T \text{ は } \Omega \text{ の部分集合})$$

と表せる。$\pi \in M_{24}$, $T \in \mathfrak{C}$ がいえれば補題が示される。

$D \in \mathfrak{D}$ に対し、$\lambda(2v_D) = 2\varepsilon_T(v_{\pi(D)}) \in \Lambda$ は (2^8) 型である。よって $\pi(D) \in \mathfrak{D}$ となり、$\pi \in \mathrm{Aut}(\mathfrak{D}) = M_{24}$ を得る。また、

$$\lambda(v_\Omega - 4v_\infty) = \varepsilon_T(v_\Omega - 4v_{\pi(\infty)}) \in \Lambda_2$$

は $(-3, 1^{23})$ 型で、'$-$' は T の上でおこる。よって $T \in \mathfrak{C}$ である。□

定理4.11 ・$0 \neq N$ である。

証明 Ω の4点集合 T を任意にとり、T の定める6×4分割を $T = T_0, T_1, \cdots, T_5$ とする。4次の正方行列 P を

$$\frac{1}{2}\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix}$$

で定める。また Ω の元を $T_0, T_1, \cdots, T_5$ の順に適当に並べ、それに対応するように v_i $(i \in \Omega)$ も並べる。そして $\mathbb{R}^{24}$ の一次変換 θ をこの基底に関して次で定める。

$$\begin{array}{c} \\ T_0 \\ \cdot \\ \cdot \\ \cdot \\ T_5 \end{array}\begin{array}{c} \begin{array}{cccccc} T_0 & & \cdots & & & T_5 \end{array} \\ \begin{pmatrix} P & & & & & \\ & P & & & 0 & \\ & & P & & & \\ & & & P & & \\ & 0 & & & P & \\ & & & & & P \end{pmatrix} \end{array}$$

即ち、θ は対角ブロックだけが P の行列である。θ は単項行列でないから N の元ではないが、・0 の元に近いことが以下でわかる。

$D \in \mathfrak{D}$ に対し $\theta(2v_D)$ を調べる。$S, S' \in \mathfrak{D}$ ならば $|S \cap S'|$ は 0,2,4,8 のどれかだから、D の元の $\{T_i\}$ へ分配されるしかたは (4^2), (2^4), $(3, 1^5)$型のいずれかである。一方、

$$(2,2,2,2)P = (-2,-2,-2,-2)$$
$$(2,2,0,0)P = (0,0,-2,-2)$$
$$(2,2,2,0)P = (-1,-1,-1,-3)$$
$$(2,0,0,0)P = (1,-1,-1,-1)$$

であるから、分配の型と $\theta(2v_D)$ の型の関係は次のようになる。

分配の型	$\theta(2v_D)$ の型
(4^2)	$(-2,-2,-2,-2)^2(0,0,0,0)^4\in\Lambda_2$
(2^4)	$(0,0,-2,-2)^4(0,0,0,0)^2\in\Lambda_2$
$(3,1^5)$	$(-1,-1,-1,-3)(1,-1,-1,-1)^5\notin\Lambda_2$

$(3,1^5)$ 型の場合、符号のついた添数の集合は $\mathcal{C}$ の元ではない。しかし θ の定義において、いずれかの P を一つだけ -P に替えると $\theta(2v_D)\in\Lambda_2$ となる。例えば、もとの θ に対する $\theta(2v_D)$ は

$$\dot{-1}\ \dot{-1}\ \dot{-1}\ -3\ |\ \dot{1}\ -1\ -1\ -1\ |\ \cdots\ |\ \dot{1}\ -1\ -1\ -1$$

の形（ここで・は D の元を添数にもつことを意味する）で、先頭の P を -P に替えると

$$\dot{1}\ \dot{1}\ \dot{1}\ -(-3)\ |\ \dot{1}\ -1\ -1\ -1\ |\ \cdots\ |\ \dot{1}\ -1\ -1\ -1$$

となり、これは Λ_2 にはいる。また、

$$\theta(v_\Omega-4v_\infty)=(-3\ \ 1\ \ 1\ \ 1)(-1\ -1\ -1\ -1)^5$$

であるが、これも θ に上の変形を施せばやはり Λ_2 にはいる。従ってこの変形された θ は ・0 の元であるが、N の元ではない。□

注意　定理における変形された θ に対し、実は ・0＝$\langle\theta,N\rangle$ であることが証明できる。

ところで、定理の P に対し $(4,0,0,0)P=(2,-2,-2,-2)$ である。従って Λ_2 の (4^2) 型の元は・0 の元によって (2^8) 型に移すことができる。(2^8) 型の元は $(-3,1^{23})$ 型に移せたが、$(-3,1^{23})$ 型の負号は $\mathcal{C}$ の元の添数上にのっているので、E の元で負号を全てはずすことができ、さらに M_{24} の元で -3 を最初にもってくることができる。

$$(4^2)\to(2^8)\to(-3,1^{23})\to(-3,1,\cdots,1)。$$

よって ・0 は Λ_2 上可移に作用している。

また、Λ_3,Λ_4 上にも可移に作用していることが、同様に示される。（Λ_2 の $(-3,1^{23})$ 型の役割を、Λ_3 では $(5,1^{23})$ 型が担う。Λ_4 では (2^{16}) 型が N で可移でなく、少し複雑になる。）

さて $8v_\infty \in \Lambda_4$ だから $|\cdot 0| = |\Lambda_4| \cdot |8v_\infty$ の安定化群$|$ である。ところが補題4.10より $8v_\infty$ の $\cdot 0$ における安定化群は N における安定化群に一致し、また N は（8）型の元の上に可移に作用している。（8）型の元は48個で、また $E \simeq \mathfrak{C}$ だから $|N| = 2^{12} \cdot |M_{24}|$ である。従って

$$|\cdot 0| = (|\Lambda_4|/48) \cdot 2^{12} \cdot |M_{24}| = 2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$$

を得る。

定義　三つの群 $\cdot 1, \cdot 2, \cdot 3$ を

$\cdot 1 = \cdot 0/\{\pm 1\}$

$\cdot 2 = \Lambda_2$ の元の $\cdot 0$ における安定化群

$\cdot 3 = \Lambda_3$ の元の $\cdot 0$ における安定化群

で定める。

これらの位数は $|\cdot 0|$ より計算できる。以下、これらが単純群であることを示す。

第3章で M_{24} の元 α, β が次のように定義されていた。

$$\alpha(x) = x+1, \quad \beta(x) = 2x \quad (x \in \Omega - \{\infty\}),$$

$$\alpha(\infty) = \beta(\infty) = \infty \quad 。$$

そこで $G = \cdot 0$, $A = \langle \alpha \rangle$ とおく。$|A| = 23$ で、A は G の Sylow 23-部分群である。

<u>補題4.12</u>　$C_G(\alpha) = \langle -1 \rangle \times A$ である。

証明　巡回置換として $\alpha = (\infty)(0\ \ 1\ \cdots\ 22)$ だから、$\alpha \in G$ とみたときの行列表示の固有値は1の23乗根で、1の重複度は2、その他の根の重複度は1である。そこで

$$u = v_\infty, \quad w = v_0 + v_1 + \cdots + v_{22}$$

とおけば、$\langle u, w \rangle$ は α の固定点全体の作る部分空間になる。

さて、$C_G(\alpha)$ は $\langle u, w \rangle$ に作用している。$\tau \in C_G(\alpha)$ に対して、

$$\tau(u) = au + bw, \qquad a, b \in \mathbb{R}$$

とおけば、$(au + bw, au + bw) = (u, u) = 1$ だから $a^2 + 23b^2 = 1$ である。一方、補題4.9より $8a, 8b$ は整数だから $64a^2 + 23 \cdot 64b^2 = 64$ の各項は負でない整数である。よって $a = \pm 1$, $b = 0$ であり、補題4.10より $\tau \in N$ がわかる。従って、

$$C_G(\alpha) = C_N(\alpha) = C_E(\alpha) \cdot C_{M_{24}}(\alpha) = \langle -1 \rangle \times A$$

を得る。□

さて、$N_G(A)/C_G(A) \leqq Aut(A)$ だが $Aut(A)$ は位数22の巡回群である。補題4.12より $|C_G(A)| = 2 \cdot 23$ だから $|N_G(A)|$ は $11 \cdot 2 \cdot 23$ か $22 \cdot 2 \cdot 23$ のいずれかである。ところが Sylow の定理より $|G : N_G(A)| \equiv 1 \pmod{23}$ であるから $|G|$ と比較して $|N_G(A)| = 2 \cdot 11 \cdot 23$ を得る。更に $\beta \in N_G(A)$ であるから

$$N_G(A) = \langle -1 \rangle \times \langle \alpha, \beta \rangle$$

である。また $Z(G) \subseteq C_G(A)$ より $Z(G) = \{\pm 1\}$ もわかる。

定理4.13　$G = \cdot 0$ の正規部分群 H が $\langle -1 \rangle$ を含めば、$H = \langle -1 \rangle$ または $H = G$ である。

証明　まず $|H| \equiv 0 \pmod{23}$ と仮定する。P を H の Sylow 23-部分群とすると P は A と共役だが H は正規だから $A \subseteq H$ である。第1章 Frattini 論法より $G = N_G(A) \cdot H$ である。ところが $\langle \alpha, \beta \rangle \subset M_{23}$ で、M_{23} は単純だから $\langle A^{M_{23}} \rangle = M_{23}$ である。よって

$$N_G(A) = \langle -1 \rangle \times \langle \alpha, \beta \rangle \subset \langle -1 \rangle \times M_{23} \subset \langle -1, A^G \rangle \subset H$$

となり、故に $G = H$ である。

次に $|H| \not\equiv 0 \pmod{23}$ と仮定する。まず H が2-群であることを示す。

$|H|$ を割る素数 p に対し、H の Sylow p-部分群 P をとる。前と同様に $G = N_G(P) \cdot H$ だから $|N_G(P)|$ は23で割り切れる。γ を $N_G(P)$ の位数23の元とすると、γ は A の元と共役だから $C_G(\gamma) = \langle -1 \rangle \times \langle \gamma \rangle$ となる。従ってもし $p \neq 2$ ならば γ は P 上 1 以外に固定点をもたず、$|P| \equiv 1 \pmod{23}$ となるはずである。しかし G の位数から、これは不可能である。

以上より H は2-群で、$C_H(\gamma) = \langle -1 \rangle$ である。よって $|H| \equiv 2 \pmod{23}$ で $|H| \leqq 2^{22}$ だから $|H| = 2$ または $|H| = 2^{12}$ である。そこで $|H| = 2^{12}$ と仮定する。

G の位数13の元 σ をとり $|C_H(\sigma)| = 2^a$ とおく。$a \geqq 1$、$2^{12} \equiv 2^a \pmod{13}$ であるから $a = 12$ である。ところがこれは、$C_G(H)$ が G の正規部分群で、$|C_G(H)| \equiv 0 \pmod{13}$ を意味する。上でみたように $G = C_G(H)$ でなければならないが、$\alpha \notin C_G(H)$ であるからこれは矛盾である。故に $H = \langle -1 \rangle$ である。□

以上の議論は $\cdot 2, \cdot 3$ の単純性の証明にも適用できる。このとき $\langle \alpha, \beta \rangle \subset M_{23} \subset \cdot 2, \cdot 3$ であること、及び $-1 \notin \cdot 2, \cdot 3$ に注意する。証明の手順は以下の通りである。

(1) ・2 の場合

$|H| \equiv 0 \pmod{23}$ のときは定理と同様に、$\alpha \in H$ と M_{23} の単純性より ・2＝H となる。

$|H| \not\equiv 0 \pmod{23}$ のときも同様に H は2-群となる。そこで $H \neq \{1\}$ と仮定すると $|H| = 2^{11}$、$C_G(H) = H$ が導かれ、H は基本可換群となる。しかしこれは

$$G/H \subseteq Aut(H) = SL(11, 2)$$

において、左辺の位数が5で割れるのに反し、右辺は割れないという矛盾を引き起こす。

(2) ・3 の場合

$|H| \equiv 0 \pmod{23}$ のときは定理と同様である。

$|H| \not\equiv 0 \pmod{23}$ のときも定理と同様に、H の Sylow p-群 P に対し $|P| \equiv 1 \pmod{23}$ となるはずだが、・3 の位数からこれはありえない。

【文献について】

M_{24} については前述のように

永尾　汎　　群とデザイン　　岩波書店

大山　豪　　有限置換群　　裳華房

を参照されたい。第3章は

Conway, J.H.　Three lectures on exceptional groups.

"Finite Simple Groups"　Academic Press　1971

による。第2章以下については

鈴木　通夫　　有限単純群　　紀伊国屋書店

も参照。