平成14年度　学位論文

Mathieu群とConway群について

兵庫教育大学大学院　学校教育研究科
教科・領域教育専攻　自然系コース
Ｍ０１１８６Ｂ　岸　　本　　章

目 次

0章　序

本論文では 1861 年, Emile Mathieu によって発見された Mathieu 群 M_{24} と, 1969 年, Conway によって発見された Conway 群 $\cdot 0$ について考察する. 特に Mathieu 群 M_{24} についてはその 5 重可移性, および単純性を導き, Conway 群 $\cdot 0$ については, その剰余群, 部分群として 3 つの単純群 $\cdot 1$, $\cdot 2$, $\cdot 3$ が現れること, M_{24} を部分群に含むことなどを示す.

有限単純群は

(1)　素数位数の可換な単純群

(2)　5 次以上の交代群

(3)　Lie 型の単純群

(4)　26 個の散在型の単純群

に分類され, (1), (2), (3) は無限系列として現れる. 無限系列に属さない 26 個の単純群は散在型単純群と呼ばれる. Mathieu の単純群 M_{24}, M_{23}, M_{22}, M_{12}, M_{11}, および Conway の単純群 $\cdot 1$, $\cdot 2$, $\cdot 3$ は散在型単純群に分類される. なお本論文では小さい次数の Mathieu 群 M_{12}, M_{11} は扱わない.

Mathieu 群, Conway 群の構成 (construction) には Steiner system S(5,8,24) が重要な役割を演じる. 一般に Steiner system $S(t, m, n)$ とは n 個の元からなる有限集合 Ω とそのべき集合 $P(\Omega)$ の部分集合 $\mathbb{B}$ の組 $(\Omega, \mathbb{B})$ で次の条件をみたすものである. ただし t, m, n は $t < m < n$ をみたす自然数である.

(1)　$X \in \mathbb{B} \implies |X| = m$

(2)　Ω の任意の t 個の元を含む $\mathbb{B}$ の元が唯 1 つ存在する.

$t \geq 4$ である Steiner system は十数個しか知られておらず, $t \geq 6$ である Steiner system は 1 つも見つかっていない. この論文では 23 元体上の 1 次元射影空間 Ω 上に Binary Golay Code を構成し, その 8 点集合 $\mathbb{O}$ を取り出すことにより Steiner system $(\Omega, \mathbb{O})$ を導

く. Binary Golay Code は対称差を加法とする 2 元体上のベクトル空間 $P(\Omega)$ の 12 次元部分空間で $\mathbb{O}$ により生成される.

S(5,8,24) は同型の意味で一意に定まり, その自己同型群が M_{24} である. また M_{24} の部分群として 21, 22, 23 次の Mathieu 群 M_{21}, M_{22}, M_{23} が現れる. なお M_{24} は 5 重可移であり, M_{23} は 4 重可移である. 実際に対称群, 交代群以外に 6 重可移群は存在せず, 対称群, 交代群以外の 4, 5 重可移群は Mathieu 群のみである.

Conway 群 $\cdot 0$ は Leech lattice を不変にする 24 次元ユークリッド空間 $\mathbb{R}^{24}$ の直交変換のなす群として定義される. Leech lattice は 1967 年, J. Leech が sphere packing との関連で発見した $\mathbb{R}^{24}$ の格子である. Leech lattice は Binary Golay Code を用いて定義される. 従って M_{24} が自然に作用し $\cdot 0$ の真部分群となる. $\cdot 0$ の中心による剰余群 $\cdot 1$ は単純群である. また長さが $4\sqrt{2}$ および $4\sqrt{3}$ のベクトルの固定群として単純群 $\cdot 2$ および $\cdot 3$ が現れる.

本論文では Ω および $\mathbb{O}$ への作用を通して M_{24} の構造を, また Leech lattice への作用を通して $\cdot 0$ の構造を明らかにする.

以下, 論文の構成について述べる.

1 章では Mathieu 群と Conway 群を考察する上で必要となる群論の基本事項について述べる. また有限集合 Ω の部分集合全体からなるべき集合 $P(\Omega)$ が対称差を加法とする 2 元体上のベクトル空間の構造を持つことを示す.

2 章では Mathieu 群, Conway 群を構成する際必要となる Steiner system S(5,8,24) と Binary Goley Code について述べる. §2.1 では Binary Golay Code を定義し, Binary Golay Code から S(5,8,24) が得られることを示す. また 23 元体上の 1 次元射影空間上に Binary Golay Code を構成し, S(5,8,24) の存在を導く. §2.2 では S(5,8,24) の構造を調べる. 任意の S(5,8,24) である $(\Omega, \mathbb{B})$ に対して, Ω の 4 点集合への分割は, どの 2 つの和も octad であるとき sextet と呼ばれる. octad と sextet の 4 点集合との交わりの個数が 3 つの型に分類されることを示す. また Ω の元をある条件をみたすように 4×6 行列に配置した M-行列の概念を導入し, 関連する 6 つの sextet を定義する. 更に $P(\Omega)$ の部分空間 $\langle \mathbb{B} \rangle$ が Binary Golay Code であることを示し, 得られた Binary Golay Code から $(\Omega, \mathbb{B})$ が復元できることを示す. これより S(5,8,24) と Binary Golay Code が同義であることが導かれる. §2.3 では 2 つの M-行列が与えられたとき, (i, j) 成分を (i, j) 成分に対応させる写像が Steiner system としての同型であることを示す. また, これより S(5,8,24) が一意に定まることを導く.

3 章では Mathieu 群を定義し, その単純性および多重可移性を示す. また $(\Omega, \mathbb{O})$ への

作用から生じる種々の作用が原始的であることを導く. §3.1 では $(\Omega, \mathbb{O})$ の自己同型群として 24 次の Mathieu 群 M_{24} を定義し, それが M-順列上正則であることを示す. これより M_{24} が Ω 上 5 重可移であることが導かれ, $1, 2, 3$ 点の固定群として M_{23}, M_{22}, M_{21} が得られる. また octad C の固定群 H を C に作用させたときの核を N とするとき H/N が A_8 に同型であること, N が位数 16 の基本アーベル群で C の補集合に正則に作用することを示す. 更に M_{24} の位数 2 の元の Ω 上の置換の型が $1^8 2^8$ または 2^{12} のいずれかになること, $1^8 2^8$ 型の元がすべて共役であることを示す. §3.2 では M_{24} の $\mathbb{O}$ への作用が原始的であることを示す. これより M_{23}, M_{22}, M_{21} の $\mathbb{O}$ の部分集合への原始的な作用が導かれる. またそれらの作用の 1 点の固定群の構造を明らかにし, M_{21}, M_{22}, M_{23} において位数 2 の元が互いに共役であることを導く. 最後に, これらの結果と 鈴木の判定法により, Mathieu 群 M_{22}, M_{23}, M_{24} の単純性を導く. なお Mathieu 群の構成にはいくつかの方法が知られている ([2, 3]).

4 章では Leech lattice Λ, および, それを不変にする直交変換のなす群として Conway 群 $\cdot 0$ を定義し, その剰余群, 部分群として Conway の単純群 $\cdot 1$, $\cdot 2$, $\cdot 3$ が現れることを示す. §4.1 では Leech lattice Λ を定義し, Λ に含まれる 長さ $4\sqrt{2}$, $4\sqrt{3}$, 8 のベクトルの型と個数を決定する. また $\Lambda/2\Lambda$ の, 長さ 8 のベクトルを含む剰余類に長さ 8 のベクトルからなる $\mathbb{R}^{24}$ の直交基底が含まれることを示す. §4.2 では Binary Golay Code と M_{24} から Λ を不変にする単項行列のなす Monomial group が自然に定まることを示し, 長さ $4\sqrt{3}$ 以下のベクトルの集合を軌道に分割する. また長さ 8 のベクトルからなる直交基底から得られる正規直交基底に関する Λ のベクトルの成分表示が Leech lattice の 3 条件をみたすことを示す. §4.3 では Conway 群 $\cdot 0$, $\cdot 1$, $\cdot 2$, $\cdot 3$ を定義し, それらの位数を決定するとともに, $\cdot 1$, $\cdot 2$, $\cdot 3$ の単純性を導く. なお Λ の長さ $4\sqrt{2}$ のベクトルに対応する $\mathbb{R}^{24}$ の点を中心とする半径 $2\sqrt{2}$ の球は原点を中心とする半径 $2\sqrt{2}$ の球に接する. その個数 196560 は 24 次元空間において, 1 つの球に接する同一半径の球の最大個数 (kissing number) であることが知られている ([4, §7.4]).

なお, 本論文を書くに際し, 主として参考にした文献は近藤武氏による講義録 [1] である.

最後にこの論文の作成にあたり 2 年間懇切丁寧にご指導いただいた松山 廣先生, ご助言いただいた濱中 裕明先生, および数学科の諸先生方に心から感謝申し上げます.

1章　準備

この章では Mathieu 群と Conway 群を考察する上で必要となる群論の基本事項について述べる. また有限集合 Ω の部分集合全体からなるべき集合 $P(\Omega)$ が対称差を加法とする 2 元体上のベクトル空間の構造を持つことを示す. なお定理の証明は一部を除いて省略し, 参考文献を明記した.

本論文では, 自然数全体の集合を $\mathbb{N}$, 整数全体の集合を $\mathbb{Z}$, 実数全体の集合を $\mathbb{R}$ と表すことにする. また「A ならば B である」ことを「$A \implies B$」, 「A と B が同値である」ことを「$A \iff B$」と表すことがある.

1.1　基本概念

- $a, b, c \in \mathbb{Z}$ が $a = bc$ をみたすとき, b は a を割るといい $b \mid a$ と表す. また, このとき b を a の約数, a を b の倍数という. なお a, b に共通な約数を公約数, 公約数の中で最大のものを最大公約数といい, $gcd(a, b)$ と表す. $gcd(a, b) = 1$ であるとき, a と b は互いに素であるという.

- 2 以上の自然数 n で, 約数が ± 1 と $\pm n$ のみであるようなものを素数という. 2 以上の自然数は素数の積として一意的に表される.

- 自然数 n に対して 整数 a, b が $n \mid a - b$ をみたすとき $a \equiv b \pmod{n}$ と表し, n を法として a は b に合同であるという.

- 集合 X の元の個数を $|X|$ で表し X の size ということにする. また size が有限である集合を有限集合という.

- 集合 G に 2 項演算 $\cdot$ が定義され次の条件をみたすとき G を群という.

  (1)　任意の $a, b, c \in G$ に対して $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ が成り立つ.

  (2)　ある元 $e \in G$ が存在して, 任意の $a \in G$ に対して $a \cdot e = e \cdot a = a$ が成り立つ.

  (3)　任意の $a \in G$ に対して $a \cdot a^{-1} = a^{-1} \cdot a = e$ をみたすような $a^{-1} \in G$ が存在する.

以下 $a \cdot b$ を ab と略記し，a と b の積という．

(2) をみたすみたす e は一意に定まり，G の単位元と呼ばれる．また, 任意の $a \in G$ に対して (3) をみたす a^{-1} は一意に定まり, a の逆元と呼ばれる．以下, この論文では特に断らない限り, 単位元を 1 で表すことにする．

- 群 G に対して $|G|$ を G の位数という．位数が有限の群を有限群, 位数が無限の群を無限群という．

- 群 G の元 a に対して, $a^n = 1$ となる自然数 n が存在するとき, そのような自然数の中で最小のものを a の位数といい, $o(a)$ または $|a|$ と表す．

- 群 G の任意の $a, b \in G$ が $ab = ba$ をみたすとき, G をアーベル群または可換群という．可換群でないとき非可換群という．

  アーベル群は演算記号を加法 $+$ で表し, 加法群と呼ばれることがある．このとき 2 元の積 $a + b$ を a, b の和という．また単位元を 0, a の逆元を $-a$ と表す．

- 集合 R に 2 つの演算, 加法 $+$ と乗法が定義されていて次の条件をみたすとき R を環という．

  (1) R は加法について加法群である．

  (2) R の任意の元 a, b, c に対して $(ab)c = a(bc)$ が成り立つ．

  (3) R の元 1 で, R の任意の元 a に対して $a1 = 1a = a$ をみたすものが存在する．

  (4) R の任意の元 a, b, c に対して $a(b + c) = ab + ac$, $(a + b)c = ac + bc$ が成り立つ．

  (5) $1 \neq 0$ である．

- R の任意の元 a, b に対して $ab = ba$ が成り立つとき R を可換環という．

- 可換環 K の 0 でない任意の元 a に対して $a \cdot a^{-1} = a^{-1} \cdot a = 1$ をみたすような $a^{-1} \in R$ が存在するとき K を体という．a に対して $a^{-1} \in K$ は一意に定まり a の逆元という．以下 $K^* = K - \{0\}$ と表すことにする．

- 自然数 n を法とする合同関係 $\equiv$ は $\mathbb{Z}$ 上の同値関係である．このときの同値類を剰余類といい, 剰余類全体を $\mathbb{Z}/n\mathbb{Z}$ と表す．整数 a, b を含む剰余類を $\overline{a}$, $\overline{b}$ と表し, その和, 積を $\overline{a+b}$, $\overline{ab}$ と定めると, これらは well-defined で, この和と積により $\mathbb{Z}/n\mathbb{Z}$ は可換環となる．特に n が素数 p のとき $\mathbb{Z}/p\mathbb{Z}$ は体となり, p 元体と呼ばれる．この論文では p 元体を $\mathbb{F}_p$ と表し, その元を $0, 1, 2, ..., p-1$ と記す．$\mathbb{F}_p{}^*$ は巡回群である ([8, Chapter 2, Theorem 2.18]).

1.2 群論の基本事項

定義 群 G の部分集合 $H \neq \emptyset$ が次の条件をみたすとき, G の部分群であるといい $H \leq G$ と表す.

(1) $H \ni a, b$ に対して $ab \in H$

(2) $H \ni a$ に対して $a^{-1} \in H$

$\{1\} \leq G$, $G \leq G$ である. 以下 $\{1\}$ を単に 1 と表す. また $H \leq G$ かつ $H \neq G$ のとき $H < G$ と表す.

定理 ([6, Chapter 2, Corollary 2.3]) 部分群の共通部分は部分群である.

H を G の部分群とする. $H < G$ であり, $H < M < G$ となる M が存在しないとき H を G の極大部分群という. また $H > 1$ であり, $H > M > 1$ となる M が存在しないとき H を G の極小部分群という.

群 G の部分集合を X, X を含む部分群すべてのなす集合 $\mathcal{H}$ とおき, $\langle X \rangle = \bigcap_{H \in \mathcal{H}} H$ を X によって生成される部分群という. 以下 $\langle \{a, b, c, \cdots\} \rangle$ を単に $\langle a, b, c, \cdots \rangle$ と表す.

群 G に対して $G = \langle x \rangle$ をみたす $x \in G$ が存在するとき, G を巡回群, x を G の生成元という.

定理 ([6, Chapter 2, Lemma 2.8]) a を群 G の元とする. $o(a)$ が有限のとき $|\langle a \rangle| = o(a)$ が成り立つ

定義 n が自然数のとき, $1, 2, ..., n$ の中で n と互いに素なものの個数を $\Phi(n)$ と表し, Φ をオイラー関数という.

位数 n の巡回群には位数 n の元が $\Phi(n)$ 個存在する ([6, Chapter 2, p.17, Theorem 2.10]). 特に巡回群の位数が素数 p のとき, 位数 p の元は $\Phi(p) = p - 1$ 個ある.

群 G と $H \leq G$ に対して $Ha = \{ha \mid h \in H\}$ とおき H の G における a を含む (右) 剰余類, または (右)coset という. 剰余類の個数 $|\{Hg \mid g \in G\}|$ を H の G における指数といい $|G : H|$ と表す. このとき次の定理が成り立つ.

定理 1.1 (Lagrange の定理,[6, Chapter 2,Theorem 2.23]) G が有限群のとき部分群 H に対して $|G| = |H| \cdot |G : H|$ が成り立つ.

上の定理より, G が有限群のとき, 部分群 H の位数は G の位数の約数である. 従って $a \in G$ に対して $< a >$ の位数が $o(a)$ であることから, $o(a)$ は $| G |$ の約数である. 特に次が成り立つ.

定理 **([6, Chapter 2,Corollary 2.24])** 有限群 G の元 a に対して $a^{|G|} = 1$ が成り立つ.

g を群 G の元とする. $x \in G$ に対して $x^g = g^{-1}xg$, $S \subseteq G$ に対して $S^g = \{x^g \mid x \in S\}$ とおき, x^g を x の g による共役, S^g を S の g による共役という.

定義 群 G の部分群 H が G の任意の元 g に対して $H^g = H$ をみたすとき, G の正規部分群であるといい $H \lhd G$ と表す.

任意の群 G において 1, G は G の正規部分群である. また指数 2 の部分群は正規部分群であることが容易に示される ([6, Chapter 2, Problem 2.6]).

群 G の部分集合 X, Y に対して, 積を $XY = \{xy | x \in X, y \in Y\}$ と定める. H, K が群 G の部分群であっても HK は 必ずしも部分群とはならないルこれについて次の定理が成り立つ.

定理 **([6, Chapter 2, Lemma 2.18])** H, K は群 G の部分群とする. HK が部分群である条件は $HK = KH$ が成り立つことである.

群 G の正規部分群 H の剰余類全体のなす集合を G/H と表すと, H の剰余類 Hx, Hy に対して $(Hx)(Hy) = Hxy$ が成り立つ ([6, Chapter 2,Corollary 2.24]). これより G/H に 2 項演算が定義される. これについて次の定理が成り立つ.

定理 **([6, Chapter 2, Theorem 2.27])** $H \lhd G$ のとき H の剰余類全体 G/H は $(Hx)(Hy) = Hxy$ なる演算により群をなす. ただし $x, y \in G$ である.

G/H を G の H による剰余群という. G/H の単位元は H であり, Hx の逆元は Hx^{-1} である. なお以下において Hx を $\overline{x}$ と表すことがある.

定義 群 $G \neq 1$ の正規部分群が 1, G のみであるとき G を単純群という.

群 G の元 a に対して

$$C_G(a) = \{g \in G \mid ag = ga\}$$

と定め a の中心化群という. $C_G(a)$ は G の部分群である ([6, Chapter 2, Lemma 2.12]). また $X \subseteq G$ に対して

$$C_G(X) = \bigcap_{x \in X} C_G(x)$$

を X の中心化群という. 特に $C_G(G)$ を $Z(G)$ と表し G の中心という. G の中心は G の可換な正規部分群である. 更に, 群 G の空でない部分集合 X に対して

$$N_G(X) = \{g \in G \mid X^g = X\}$$

と定め X の正規化群という. $N_G(X)$ も G の部分群である ([6, Chapter 2, Lemma 2.29]).

$x, y \in G$ に対し, $[x, y] = x^{-1}y^{-1}xy$ と定め x と y の交換子という. また $H, K \leq G$ に対して

$$[H, K] = \langle \{\, [h, k] \mid h \in H, k \in K \,\} \rangle$$

と定める. 特に $[H, H]$ を H' と表し H の交換子部分群という.

定理 ([6, Chapter 3, Theorem 3.10, Corollary 3.12]) 群 G の交換子部分群を G' とする. このとき G の部分群 N について次は同値である.

(1) $N \geq G'$

(2) $N \lhd G$ かつ G/N はアーベル群.

群の集合への作用

G は群, X は空でない集合とする. $g \in G$, $x \in X$ に対して $x \cdot g \in X$ が定まり, 次の条件をみたすとき G は X に (右から) 作用するという.

(1) 任意の $x \in X$ と $g, h \in G$ に対して $(x \cdot g) \cdot h = x \cdot (gh)$ が成り立つ.

(2) 任意の $x \in X$ に対して $x \cdot 1 = x$ が成り立つ.

以下, この論文では $x \cdot g$ を x^g と表すことにする. また G が X に (右から) 作用するとき X を (右) $G-$ set ということにする.

X が $G-$ set のとき

$$\{\, g \in G \mid \text{任意の } x \in X \text{ に対して } x^g = x \,\}$$

は G の正規部分群になる ([6, Chapter 4, Corollary 4.3]). これをこの作用の核という.

X の相異なる n 個の元の任意の 2 組 $a_1, ..., a_n$ と $b_1, ..., b_n$ に対して $(a_i)^g = b_i$ となる $g \in G$ が存在するときこの作用は n 重可移であるという. $n = 1$ のとき単に可移といい, $n \geq 2$ のとき多重可移という.

X の n 個の元からなる任意の部分集合 Y, Z に対して $Y^g = Z$ となる $g \in G$ が存在するとき, この作用は n-homogeneous であるという.

$x \in X$ に対して $\mathcal{O}_x = \{x^g \mid g \in G\}$ とおき x を含む $(G-)$ 軌道, または $(G-)$orbit という. また $G_x = \{g \in G \mid x^g = x\}$ とおき, x の固定群という. 可移であり, $G_x = 1$ である作用を正則な作用という. $y = x^g$ のとき $G_y = (G_x)^g$ であるから, この定義は x の選び方によらない.

$N \lhd G$ のとき, $g \in G$, $a \in N$ に対して $a \cdot g = a^g = g^{-1}ag$ と定めると G の N への作用が得られる. このとき $G_a = C_G(a)$ であり, 作用の核は $C_G(N)$ である.

定理 1.2 ([8, Chapter 9, Lemma 9.5]) G は群, $X\,(\geq 3)$ は $G-$ *set* とする. このとき次は同値である. ただし r は 2 以上の整数であるとする.

(1) G が X 上 r 重可移である.

(2) 任意の $x \in X$ に対して G_x が $X - \{x\}$ 上 $r-1$ 重可移である.

定理 1.3 ([8, Chapter 3, Theorem 3.19]) $x \in X$ に対して $|\mathcal{O}_x| = |G : G_x|$ が成り立つ.

$\emptyset \neq \Delta \subseteq X$ が, 任意の $g \in G$ に対し $\Delta^g = \Delta$ または $\Delta^g \cap \Delta = \emptyset$ をみたすとき, Δ を block という. 1 つの元からなる部分集合, および X 自身は block である. これらを自明な block という. 自明でない block をもたない作用を原始的な作用という.

線形群

体 K 上のすべての n 次正方行列からなる集合を $M(n, K)$ とし

$$GL(n, K) = \{A \in M(n, K) \mid |A| \neq 0\}, \quad SL(n, K) = \{A \in M(n, K) \mid |A| = 1\}$$

とおく．ただし $|A|$ は A の行列式である． $GL(n,K)$ は行列の乗法について群をなし，$SL(n,K) \lhd GL(n,K)$ が成り立つ． $GL(n,K)$ を一般線形群, $SL(n,K)$ を特殊線形群という．また

$$L_n(K) = SL(n,K)/Z(SL(n,K))$$

を射影特殊線形群という．$L_n(K)$ は $PSL(n,K)$ と表されることもある．

$K = \mathbb{F}_q$ のとき $GL(n,K)$, $SL(n,K)$, $L_n(K)$ をそれぞれ $GL(n,q)$, $SL(n,q)$, $L_n(q)$ と表すことがある．

$$O(n) = \{A \in M(n,\mathbb{R}) \mid A \cdot {}^tA = {}^tA \cdot A = E\}$$

は $GL(n,\mathbb{R})$ の部分群である．$O(n)$ を n 次直交群という．ただし ${}^tA$ は A の転置行列，E は n 次単位行列である．

定理 1.4 ([8, Chapter 8, Theorems 8.5, 8.8, 8.11])

$$|GL(n,q)| = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (q^i - 1), \quad |SL(n,q)| = q^{\frac{n(n-1)}{2}} \prod_{i=2}^{n} (q^i - 1)$$

が成り立つ．更に $d = gcd(n, q-1)$ とすると

$$|L_n(q)| = \frac{1}{d} q^{\frac{n(n-1)}{2}} \prod_{i=2}^{n} (q^i - 1)$$

が成り立つ．

定理 1.5 $L_2(q) = \langle \overline{\alpha_a}, \overline{\beta}, \overline{\gamma} \mid a \in \mathbb{F}_q \rangle$ が成り立つ．ここで

$$\alpha_a = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, \ a \in \mathbb{F}_q, \quad \beta = \begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix}, \quad \gamma = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

であり，b は乗法群 $\mathbb{F}_q^*$ の生成元である．また $x \in SL(2,q)$ に対して $\overline{x}$ は x を含む剰余類を表す．

Proof $H = \langle \alpha_a, \beta, \gamma \mid a \in \mathbb{F}_q \rangle$ とおき，$H = SL(2,q)$ を示せばよい． $H \subseteq SL(2,q)$ は明らかであるから，任意に $\sigma = \begin{bmatrix} x & y \\ z & u \end{bmatrix} \in SL(q)$ を選び $\sigma \in H$ を示せばよい．

$z = 0$ のときは

$$\sigma = \begin{bmatrix} x & y \\ 0 & x^{-1} \end{bmatrix} = \begin{bmatrix} 1 & xy \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x & 0 \\ 0 & x^{-1} \end{bmatrix} \in H$$

が成り立つ. 次に $z \neq 0$ とする. $xu - yz = 1$ より $y - z^{-1}xu = -z^{-1}$ であることに注意すれば

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & -z^{-1}x \\ 0 & 1 \end{bmatrix} \sigma = \begin{bmatrix} -z & -u \\ 0 & -z^{-1} \end{bmatrix}$$

を得る. 前述の結果とあわせて

$$\begin{bmatrix} -z & -u \\ 0 & -z^{-1} \end{bmatrix}, \qquad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \qquad \begin{bmatrix} 1 & -z^{-1}x \\ 0 & 1 \end{bmatrix} \in H$$

が得られるので $\sigma \in H$ が成り立つ. よって $H = SL(2, q)$, 従って $\overline{H} = L_2(q)$ が示された. ∎

体 K 上の n 次元ベクトル空間 V の 0 でない元 a, b に対して $a = kb$ となる $0 \neq k \in K$ が存在するとき $a \sim b$ であると定めると $\sim$ は $V - \{0\}$ 上の同値関係になる. ここで

$$[a] = \{\, b \in V \mid b \sim a \,\}, \qquad PG(n-1, K) = \{\, [a] \mid a \in V\,, a \neq 0 \,\}$$

とおき, $PG(n-1, K)$ を $n-1$ 次元射影空間という. さて $SL(n, K)$ の n 次元ベクトル空間 V への作用から $PG(n-1, K)$ への作用が定まるが, この作用の核は $Z(SL(n, K))$ である. 従って $L_n(K) = SL(n, K)/Z(SL(n, K))$ は $PG(n-1, K)$ に作用する. これについて次の定理が成立する.

定理 1.6 ([8, Chapter 9, Theorem 9.45]) $n \geq 2$ のとき $L_n(K)$ の $PG(n-1, K)$ への作用は 2 重可移である.

この論文で必要なのは $n = 2$ の場合のみである.

定理 1.7 $L_2(q)$ の $\Omega = PG(1, K)$ への作用は 2 重可移である.

Proof $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ を任意の 0 でない $\begin{bmatrix} a \\ b \end{bmatrix}$ に移す $SL(2, q)$ の元が存在することから $L_2(q)$ は

Ω 上可移である. 次に $L_2(q)$ における $\infty = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ の固定群を H とおくと

$$H = \left\{ \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix} \middle| \, a, b \in \mathbb{F}_q, a \neq 0 \right\}$$

である. 任意の $b \in {\mathbb{F}_q}^*$ に対して

$$\begin{bmatrix} a^{-1} & ab \\ 0 & a \end{bmatrix} : \begin{bmatrix} 0 \\ 1 \end{bmatrix} \longmapsto \begin{bmatrix} b \\ 1 \end{bmatrix}$$

であるから H は $\Omega - \{\infty\}$ 上可移である. ゆえに $L_2(q)$ は 2 重可移である. ∎

準同型定理

G, H は群であるとする. 写像 $f : G \mapsto H$ で $f(ab) = f(a)f(b)$ $(a, b \in G)$ をみたすものを G から H への準同型写像という. 特に f が全単射であるとき同型写像と呼ぶ. また G から H への同型写像があるとき G と H は同型であるといい $G \simeq H$ と表す. 準同型写像 $f : G \mapsto H$ に対して

$$ker(f) = \{\, x \in G \mid f(x) = 1 \,\}, \qquad Im(f) = \{\, f(x) \mid x \in G \,\}$$

とおき, $ker(f)$, $Im(f)$ をそれぞれ f の核, 像という. $ker(f) \lhd G$, $Im(f) \leq H$ であることに注意されたい.

群 G から G への同型写像を G の自己同型という. G のすべての自己同型からなる集合を $Aut(G)$ と表す. また $g \in G$ から定まる自己同型 $G \ni x \mapsto x^g \in G$ を (g による) 内部自己同型という. 内部自己同型全体のなす集合を $Inn(G)$ と表す. $Aut(G)$, $Inn(G)$ は写像の合成について群をなし, $Aut(G)$ を G の自己同型群, $Inn(G)$ を G の内部自己同型群という. このとき $Inn(G) \lhd Aut(G)$ が成り立つ ([8, Chapter 7, Theorem 7.1]).

定理 1.8 ([8, Chapter 7, Lemma 7.2]) G が位数 n の巡回群であるとき $Aut(G)$ は位数 $\Phi(n)$ のアーベル群である. 特に n が素数 p のときは位数 $p-1$ の巡回群である.

定理 1.9 ([8, Chapter 7, Theorem 7.1]) $H \leq G$ とする. このとき $N_G(H)/C_G(H)$ は $Aut(H)$ の部分群に同型である.

定理 1.10 (準同型定理,[8, Chapter 2, Theorem 2.24]) $\varphi : G \mapsto H$ が準同型のとき $G/ker(\varphi) \simeq Im(\varphi)$ が成り立つ.

$N \lhd G$ のとき任意の $H \leq G$ に対して $NH = HN$ が成り立つ. 従って NH は定理より部分群である.

定理 1.11 ([8, Chapter 2, Theorem 2.26]) $N \lhd G$, $H \leq G$ のとき $NH/N \simeq H/H \cap N$ が成り立つ.

Sylowの定理

定理 1.12 ([8, Chapter 4, Lemma 4.11, Theorems 4.12, 4.14]) 有限群 G の位数を n, p を n の素因数とする. このとき次が成り立つ.

(1) $p^a \mid n$ かつ $p^{a+1} \nmid n$ となる a に対して G は位数 p^a の部分群 P を含む. P を G の *Sylow* p-部分群という.

(2) G のすべての *Sylow* p-部分群の集合を $Syl_p(G)$ とおくと, G は共役をとる操作で $Syl_p(G)$ に可移に作用する.

(3) $|Syl_p(G)| \equiv 1 \pmod{p}$ である.

定理 1.13 ([8, Chapter 4, Theorem 4.2]) G の位数が素数 p で割り切れるならば G に位数 p の元が存在する.

次の定理は Conway 群の単純性の証明に必要となる.

定理 1.14 (Frattini Argument,[8, Chapter 4, Theorem 4.18]) 有限群 G の正規部分群 N の *Sylow* p -部分群 P について $G = N_G(P)N$ が成り立つ.

p-群

位数が素数 p のべきである有限群を p-群という. 次の 2 つの定理は Conway 群の単純性の証明の中で用いられる.

定理 1.15 有限群 G の部分群 H の正規化群 $N_G(H)$ の元 α の位数が素数 p のべきであるとき $|H| \equiv |C_H(\alpha)| \pmod{p}$ が成り立つ.

Proof　$P = \langle \alpha \rangle$ とすると $P \leq N_G(H)$ である. 従って P の H への共役による作用を考えることができる. ここで

$$C_H(\alpha) = \{h \in H \mid \text{任意の } x \in P \text{ に対して } h^x = h\}$$

であるから $H = C_H(\alpha)$ ならば明らかに $|H| \equiv |C_H(\alpha)| \pmod{p}$ が成り立つ. 従って $H \neq C_H(\alpha)$ とする. $x \in C_H(\alpha)$ を含む orbit $\mathcal{O}_x$ については $|\mathcal{O}_x| = 1$ が成り立つ. 一方 $x \in H - C_H(\alpha)$ に対しては $|\mathcal{O}_x| = |P : P_x|$, $P_x < P$ より $|\mathcal{O}_x| \equiv 0 \pmod{p}$ となる. 従って $|H| \equiv |C_H(\alpha)| \pmod{p}$ が成り立つ. ∎

定理 1.16 ([8, Chapter 4,Theorem 4.4]) P を有限 p -群, $N > 1$ を P の正規部分群とすると $N \cap Z(P) > 1$ が成り立つ. 特に $|P| > 1$ ならば $Z(P) > 1$ である.

置換群

集合 X から X への全単射全体を S_X で表す. $\sigma \in S_X$ に対して $x \in X$ の σ による像を x^σ と表すことにする. このとき $\sigma, \tau \in S_X$ に対して, その合成 $\sigma\tau$ が $x^{\sigma\tau} = (x^\sigma)^\tau$ $(x \in X)$ で定義され, この写像の合成を積として S_X が群をなす. S_X を X 上の対称群という. 群 G が集合 X に作用することと, 準同型 $G \to S_X$ が存在することとは同値である. S_X の元は X 上の置換, または変換と呼ばれる. 特に X の元の順列 $(x_1, \ldots, x_n)$ に対して

$$(x_1, \ldots, x_n)^\sigma = (x_1^\sigma, \ldots, x_n^\sigma)$$

と定める. また $|X| = n$ のとき S_X を S_n と表し n 次対称群という. n 次の置換群とは S_n の部分群をいう. S_n は X 上 n 重可移に作用し, $|S_n| = n!$ をみたす.

次の条件をみたす $\sigma \in S_X$ を n-cycle といい $\sigma = (x_1, x_2, \ldots, x_n)$ と表す.

(1)　$1 \leq i < n$ のとき ${x_i}^\sigma = x_{i+1}$ かつ ${x_n}^\sigma = x_1$

(2)　$y \in X - \{x_1, x_2, \ldots, x_n\}$ のとき $y^\sigma = y$

2-cycle を互換という. 共通元を持たない 2 つの cycle は disjoint であるという.

定理 1.17 ([8, Chapter 1,Theorems 1.1,1.2]) すべての置換は *disjoint* な *cycle* の積として一意的に表すことができる.

置換 σ を, 1-cycle も含めて disjoint な cycle の積に分解したとき a_i-cycle が b_i 個現れたとする. このとき σ を $a_1^{b_1}a_2^{b_2}\cdots$ 型の置換という.

定理 1.18 ([8, Chapter 1,Theorem 1.7]) すべての置換は互換の積に分解できる. また互換の積にあらわれる互換の個数の偶奇は分解の仕方によらず一定である.

偶数個の互換の積である置換を偶置換, 奇数個の互換の積である置換を奇置換という. S_n に含まれるすべての偶置換の集合は部分群をなす. これを A_n と表し交代群という. $n \geq 2$ のとき $|S_n : A_n| = 2$ であり, $A_n \lhd S_n$ が成り立つ ([6, Chapter 6, Corollary 6.10]).

定理 1.19 ([8, Chapter 3,Theorem 3.11]) $n \geq 5$ のとき A_n は単純群である.

直積

$H, K \lhd G$ が $G = HK$, $H \cap K = 1$ をみたすとき G は H と K の直積であるといい $G = H \times K$ と表す. $G = H \times K$ のとき $x \in H$ と $y \in K$ に対して

$$x^{-1}y^{-1}xy = (x^{-1}y^{-1}x)y = x^{-1}(y^{-1}xy) \in H \cap K$$

が成り立つ. 従って $x^{-1}y^{-1}xy = 1$ より $xy = yx$ を得る. すなわち H の元と K の元は可換である. また $xy = uv$, $x, u \in H$, $y, v \in K$ とすると

$$u^{-1}x = vy^{-1} \in H \cap K$$

となり $x = u$, $y = v$ が得られる. 従って $G = H \times K$ のとき G の元は一意的に xy $(x \in H, y \in K)$ と表される.

同様にして有限個の群 H_1,...,H_n の直積 $H_1 \times \cdots \times H_n$ も定義される.

可換な有限 p -群で各元の位数が p であるものは, 位数が素数 p の巡回群いくつかの直積である. このような群を基本アーベル p-群と呼ぶ.

$H \lhd G$, $K \leq G$ が $G = HK$, $H \cap K = 1$ をみたすとき G は H と K の半直積であるといい $G = H.K$ と表す. またこのとき K を H の補群という. 半直積 $G = H.K$ の場合

も直積のときと同様にして G の元が一意的に xy $(x \in H, y \in K)$ と表されることが証明される.

べき零群, 可解群

G を有限群とする. 部分群列 $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ で, 任意の i に対して $G_i \lhd G_{i+1}$ かつ G_{i+1}/G_i がアーベル群となるものが存在するとき G を可解群という. また, 任意の i に対して $G_i \lhd G$ かつ $G_{i+1}/G_i \leq Z(G/G_i)$ となる部分群列 $1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$ が存在するとき G をべき零群という.

次の定理は定義より明らかである (証明略).

定理 1.20 べき零群は可解群である.

定理 1.21 ([8, Chapter 5,Theorem 5.33]) 有限 p -群はべき零群である.

$N \lhd G$ であり $1 < M < N$ をみたす G の正規部分群 M が存在しないとき N を G の極小正規部分群という.

定理 1.22 ([6, Chapter 8, Lemma 8.6]) G を有限群, N を G の可解な極小正規部分群とする. このとき, N は基本アーベル p-群である.

定理 1.22 の証明は [8, Chapter 5,Theorem 5.24] の証明を修正して得ることもできる. なお, 上の 3 つの定理は 3 章で必要となる.

$\mathbb{Z}$ 加群

L を加法群, R を可換環とする. $R \times L \ni (a, x)$ に対して L の元 ax が定まり, 次が成り立つとき L を R 加群という. ただし $a, b \in R$, $x, y \in L$ である.

(1) $(ab)x = a(bx)$

(2) $a(x + y) = ax + ay$

(3) $(a + b)x = ax + bx$

(4)　R の単位元 1 に対して $1x = x$

アーベル群 G の元 a と整数 n に対して

$$na = \begin{cases} \overbrace{a + a + \cdots + a}^{n\text{ 個}} & n > 0 \text{ のとき} \\ 0 & n = 0 \text{ のとき} \\ \underbrace{(-a) + (-a) + \cdots + (-a)}_{-n\text{ 個}} & n < 0 \text{ のとき} \end{cases}$$

と定めることにより G を $\mathbb{Z}$ 加群とみなすことができる.

R を環とし L を R 加群とする. $u_1, u_2, \cdots, u_n \in L$ が存在して, 任意の $x \in L$ が

$$x = a_1u_1 + a_2u_2 + \cdots + a_nu_n\,, \qquad a_1, a_2, \ldots, a_n \in R$$

と一意的に表されるとき L を自由 R 加群, $u_1, u_2, \ldots, u_n$ を R 基底という.

以下, 自由 $\mathbb{Z}$ 加群を単に自由加群ということにする. 自由加群 L の基底をなす元の個数は基底の選び方によらず一定である ([8, Chapter 10, Theorem 10.14]). これを L の階数という.

定理 1.23 ([8, Chapter 10, Theorem 10.18]) 階数 n の自由加群の部分加群は階数が高々 n の自由加群である.

K が体のとき K 加群 V は常に自由 K 加群となり, K 上のベクトル空間と呼ばれる. その階数は基底の選び方によらず一定で, これを V の次元といい $\dim V$ と表す. 以下, これらを含め, 線型代数学の基本事項は既知とする.

鈴木の判定法

次の定理は鈴木の判定法と呼ばれ, 3 章で Mathieu 群の単純性を示すのに用いられる.

定理 1.24 (鈴木) 有限群 G の位数 2 の元 t が

$$G = \langle t^G \rangle \tag{1.1}$$

$$C_G(t) \rhd U \neq 1 \text{ ならば } U \cap t^G \neq \emptyset \tag{1.2}$$

をみたすとする. このとき G は単純群であるか, 指数 2 で奇数位数のアーベル部分群をもつ. ただし $t^G = \{t^g \mid g \in G\}$ である.

Proof G が単純群でないと仮定する. このとき $1 < K < G$ をみたす正規部分群 K が存在する.

まず $C_K(t) = 1$ を示す. そのために $C_K(t) \neq 1$ と仮定して矛盾を導く. $K \lhd G$ より $C_K(t) \lhd C_G(t)$ を得る. 従って (1.2) より $C_K(t) \cap t^G$ はある t^g を含み, $K \lhd G$ であることから $t \in K$ を得る. このとき $t^G \subseteq K$ となるので(1.1) より $G = K$ となり, $K < G$ と仮定したことに矛盾する. 従って $C_K(t) = 1$ を得る.

次に K の位数が偶数であるとする. 任意の $x \in K - \{1\}$ について $x \neq x^t$ と仮定すると $K - \{1\}$ が $\{x, x^t\}$ のペアに分割され, $|K|$ が偶数であることに矛盾する. 従って $x = x^t$ となる元 $x \in K - \{1\}$ が存在する. このとき $C_K(t) \neq 1$ となり, 前述のことに矛盾する. 従って K の位数は奇数である.

ここで写像 f を

$$f : K \ni x \longmapsto x^{-1}x^t \in K$$

と定める. いま $f(x) = f(y)$ とすると $x^{-1}x^t = y^{-1}y^t$ より $xy^{-1} = (xy^{-1})^t$ となるので $xy^{-1} = 1$, すなわち $x = y$ を得る. よって f は単射である. K は有限集合であるから f は全単射である. 従って K の任意の元 g は $g = x^{-1}x^t$ という形に一意的に表される. これより

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

が得られる. またこのとき任意の $x, y \in K$ に対して

$$x^{-1}y^{-1}xy = x^t y^t xy = (xy)^t xy = (xy)^{-1}xy = 1$$

となり $x^{-1}y^{-1}xy = 1$ より $xy = yx$ が得られるので K はアーベル群である.

一方 $t \notin C_G(K)$ より $G > C_G(K) \geq K > 1$ が成り立つ. また $K \lhd G$ より $C_G(K) \lhd G$ であるから, 上述の K を $C_G(K)$ で置き換えることにより $C_G(K)$ も奇数位数のアーベル群であることが導かれる.

さて定理 1.9 より $G/C_G(K)$ は $Aut(K)$ の部分群に同型である． $G/C_G(K) \ni \bar{t}$ は K の各元をその逆元に移す自己同型であるから $G/C_G(K)$ の中心に含まれる． 従って $< t > C_G(K) \lhd G$ が成り立つので(1.1) より $< t > C_G(K) = G$ を得る. 以上で指数が 2 である奇数位数のアーベル群 $C_G(K)$ の存在が示された. ∎

補題 1.25 次の条件が成り立てば定理 1.24 の(1.2) がみたされる.

$$\begin{array}{l} G \text{ の位数 } 2 \text{ の元は互いに共役で, 位数 } 2 \text{ の元 } t \text{ に対して } C_G(t) \text{ は} \\ \text{奇数位数の正規部分群 } (\neq 1) \text{ をもたない.} \end{array} \tag{1.3}$$

Proof $C_G(t) \rhd U \neq 1$ とすると(1.3) より U は偶数位数となる. 従って位数 2 の元 $u \in U$ が存在する. 位数 2 の元は互いに共役であるから $u = t^g$ となる $g \in G$ が存在する. ゆえに $u \in U \cap t^G$ となり(1.2) がみたされる. ∎

べき集合 $\mathbf{P}(\Omega)$

以下, Ω は有限集合で $|\Omega| = n$ をみたすとする． Ω の部分集合全体のなす集合族を Ω のべき集合と呼び, $P(\Omega)$ と表す． $X, Y \in P(\Omega)$ に対し, 対称差 $X + Y$ を

$$X + Y = (X \cup Y) - (X \cap Y)$$

と定義する. Ω の元を $\{a_1, a_2, \cdots, a_n\}$ と番号付け, 2 元体 $\mathbb{F}_2$ 上の n 次元ベクトル空間を V とすると, 1 対 1 対応

$$V \ni \mathbf{x} = (x_1, \ldots, x_n) \longleftrightarrow X = \{\, a_i \mid x_i = 1 \,\} \in P(\Omega)$$

が得られる. ここで $\mathbf{x} \leftrightarrow X$, $\mathbf{y} \leftrightarrow Y$ のとき $\mathbf{x} + \mathbf{y} \leftrightarrow X + Y$ となる. これより $P(\Omega)$ は自然に $\mathbb{F}_2$ 上の n 次元ベクトル空間と見なされる. また, $P(\Omega)$ を位数 2^n の基本アーベル 2 -群とみなすこともできる.

定理 1.26 $P(\Omega)$ は $\mathbb{F}_2$ 上の n 次元ベクトル空間である. また $P(\Omega)$ は対称差を演算として, 位数 2^n の基本アーベル 2-群をなす.

Ω 上の対称群 S_Ω の元 σ は明らかに $(X + Y)^\sigma = X^\sigma + Y^\sigma$ をみたす. 従って $P(\Omega)$ の線型変換を誘導する. これより $S_\Omega \leq GL(n, 2)$ とみなすことができる.

定理 1.27 Ω の偶数個の元からなる部分集合全体の集合 $P_0(\Omega)$ は $P(\Omega)$ の部分群をなす.

Proof $\emptyset \in P_0(\Omega)$ より $P_0(\Omega)$ は空でない. また $P_0(\Omega) \ni X, Y$ に対して $|X+Y| = |X|+|Y|-2|X\cap Y|$ は偶数であるので $X+Y \in P_0(\Omega)$ が成り立つ. 更に $-X = X \in P_0(\Omega)$ となるから $P_0(\Omega)$ は $P(\Omega)$ の部分群である. ∎

定理 1.28 $X, Y \in P(\Omega)$ であり, $|X|$, $|Y|$ が 4 の倍数であるとする. このとき $|X+Y|$ が 4 の倍数であることと $|X\cap Y|$ が偶数であることとは同値である.

Proof $|X+Y| = |X|+|Y|-2|X\cap Y|$ より明らかである. ∎

定理 1.29 $X, Y, Z \in P(\Omega)$ であり, $|X\cap Z|$, $|Y\cap Z|$ が偶数ならば $|(X+Y)\cap Z|$ も偶数である.

Proof $X\cap Z, Y\cap Z \in P_0(\Omega)$ より

$$(X+Y)\cap Z = (X\cap Z)+(Y\cap Z) \in P_0(\Omega)$$

が得られる. ∎

定理 1.30 $A_1, A_2, \ldots, A_n$ を $P(\Omega)$ の元とする. $|A_i|$ が 4 の倍数で, 任意の $1 \le i \ne j \le n$ に対して $|A_i \cap A_j|$ が偶数であるとする. このとき $A_1, A_2, \ldots, A_n$ から 任意の k 個 $A_{i_1}, \ldots, A_{i_k}$ を選んでできる和 $A_{i_1} + A_{i_2} + \cdots + A_{i_k}$ の元の個数は 4 の倍数である.

Proof $|A_1+A_2+\cdots+A_n|$ が 4 の倍数であることを示せば十分である. n についての帰納法で示す. $n=1$ のときは明らかに成り立ち, $n=2$ のときは定理 1.28 より成り立つ. 次に $n \ge 3$ として n より小さい場合には成り立つと仮定する. ここで $X = A_1+\cdots+A_{n-2}$, $Y = A_{n-1}$, $Z = A_n$ とおく. 帰納法の仮定より $|X|$, $|X+Y|$, $|X+Z|$, $|Y+Z|$ は 4 の倍数である. 従って定理 1.28 より $|X\cap Y|$, $|X\cap Z|$ は偶数となり, 定理 1.29 より $|X\cap(Y+Z)|$ が偶数となる. よって定理 1.28 より $|X+Y+Z|$ は 4 の倍数である. ∎

2章　S(5,8,24)

この章では Mathieu 群, Conway 群を構成する際必要となる Steiner system S(5,8,24) と Binary Goley Code について述べる. §2.1 では Binary Golay Code を定義し, Binary Golay Code から S(5,8,24) が得られることを示す. また 23 元体上の 1 次元射影空間上に Binary Golay Code を構成し, S(5,8,24) の存在を導く. §2.2 では S(5,8,24) の構造を調べる. 任意の S(5,8,24) である $(\Omega, \mathbb{B})$ に対して, Ω の 4 点集合への分割は, どの 2 つの和も octad であるとき sextet と呼ばれる. octad と sextet の 4 点集合との交わりの個数が 3 つの型に分類されることを示す. また Ω の元をある条件をみたすように 4×6 行列に配置した M-行列の概念を導入し, 関連する 6 つの sextet を定義する. 更に $P(\Omega)$ の部分空間 $\langle \mathbb{B} \rangle$ が Binary Golay Code であることを示し, 得られた Binary Golay Code から $(\Omega, \mathbb{B})$ が復元できることを示す. これより S(5,8,24) と Binary Golay Code が同義であることが導かれる. §2.3 では 2 つの M-行列が与えられたとき, (i, j) 成分を (i, j) 成分に対応させる写像が Steiner system としての同型であることを示す. また, これより S(5,8,24) が一意に定まることを導く.

2.1　S(5,8,24) とその存在

まず Steiner system を定義する. Ω を $|\Omega| = n$ をみたす有限集合とする. $\mathbb{B} \subseteq P(\Omega)$ が次の (1), (2) をみたすとき $(\Omega, \mathbb{B})$ を Steiner system といい $S(t, m, n)$ と表す. ただし t, m, n は自然数で $t < m < n$ をみたすものとする.

(1)　$X \in \mathbb{B} \implies |X| = m$

(2)　Ω の任意の t 個の元を含む $\mathbb{B}$ の元が唯 1 つ存在する.

$m = n$ のときは $\mathbb{B} = \{\Omega\}$ とおけば任意の $t \leq n$ に対して条件 (1),(2) がみたされる. また $t = 1$ のときは Ω の分割 $\Omega = B_1 \cup \cdots \cup B_r$ を $|B_1| = \cdots = |B_r|$ となるように選び

$\mathbb{B} = \{ B_1, ..., B_r \}$ とおけば条件 (1),(2) がみたされる. 条件 $t < m < n$ を付加すると (1),(2) をみたすものを見つけるのは容易でない. 現在でも $t \geq 4$ である Steiner system は十数個しか知られておらず, $t \geq 6$ である Steiner system は 1 つも見つかっていない. 以下 Mathieu 群と深く関わり合う Steiner system S(5,8,24) について考察するので $|\Omega| = 24$ と仮定するこのとき定理 1.26 より $P(\Omega)$ は $\mathbb{F}_2$ 上の 24 次元ベクトル空間である. なお Steiner system $(\Omega, \mathbb{B})$ において Ω の元を点と呼ぶことにする.

Binary Goley Code

$\mathbb{F}_2$ 上の 24 次元ベクトル空間 $P(\Omega)$ の部分空間 Γ が

$$\Gamma \ni X \neq \emptyset \quad \Longrightarrow \quad |X| \geq 8 \tag{2.1}$$

をみたすとする. ここで

$$\mathbb{O} = \{ X \in \Gamma \;\big|\; |X| = 8 \}$$

とおく. さて Ω のある 5 点を含む $\mathbb{O}$ の元が 2 個あったとして, それらを X, Y とする. このとき

$$|X + Y| = |X| + |Y| - 2\,|X \cap Y| \leq 6$$

となり(2.1) に反する. 従って Ω の任意の 5 点に対して, それを含む $\mathbb{O}$ の元は高々 1 個である.

補題 2.1 上で定めた Γ, $\mathbb{O}$ について次の (1), (2), (3) が成り立つ.

(1) $|\mathbb{O}| \leq 759$

(2) $\dim \Gamma \leq 12$

(3) $\dim \Gamma = 12 \iff |\mathbb{O}| = 759$

Proof (1) Ω の 5 点集合を含む $X \in \mathbb{O}$ は高々 1 個であることに注意して集合

$$\left\{ (T, X) \;\middle|\; |T| = 5,\, X \in \mathbb{O}\,, T \subseteq X \right\}$$

の個数を 2 通りに数えると

$$\binom{8}{5} \cdot |\mathbb{O}| \;\leq\; \binom{24}{5} \cdot 1$$

を得る. 従って $|\mathbb{O}| \leq 759$ が成り立つ. ここで等号が成立するのは Ω のすべての 5 点集合に対して, それを含む $\mathbb{O}$ の元が存在する場合に限ることを注意しておく.

(2)　商空間 $P(\Omega)/\Gamma$ において X, Y が同じ剰余類に入るとき, すなわち $X - Y \in \Gamma$ のとき $X \equiv Y \pmod{\Gamma}$ と表すことにする. いま $X \neq Y$ が $|X| \leq 3, |Y| \leq 4$ をみたすとする. このとき $X + Y \neq \emptyset$ であり

$$|X + Y| = |X| + |Y| - 2\,|X \cap Y| \leq 7$$

より $X \not\equiv Y \pmod{\Gamma}$ が成り立つ. これより 3 点以下の集合は $P(\Omega)/\Gamma$ の異なる剰余類に属する. また 3 点以下の集合を含む剰余類は 4 点集合を含まない.

また $|X| = |Y| = 4$ のとき $X \equiv Y \pmod{\Gamma}$ となるのは $X \cap Y = \emptyset$ かつ $|X + Y| = 8$ のときに限る. これより 4 点集合 X を含む $\mathbb{O}$ の元は高々 $\frac{(24-4)}{4} = 5$ 個であるから X と同じ剰余類に含まれる 4 点集合は X を含めて高々 6 個である. 従って

$$|\,P(\Omega)/\Gamma\,| \;\geq\; 1 + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} + \frac{1}{6} \cdot \binom{24}{4} \tag{2.2}$$

となるので $|P(\Omega)/\Gamma| \geq 2^{12}$ が得られる. ここで $|P(\Omega)| = 2^{24}$ であることから $|\Gamma| \leq 2^{12}$, 従って $\dim \Gamma \leq 12$ を得る. ここで等号が成立すれば 4 点集合を含む剰余類には 6 個の 4 点集合が存在することになる.

(3)　まず $|\mathbb{O}| = 759$ と仮定する. このとき (1) の証明中で注意したことから任意の 5 点に対して, それを含む $\mathbb{O}$ の元が唯 1 つ存在する. 従って任意の 4 点に対して, それを含む $\mathbb{O}$ の元が 5 個存在する. これより $P(\Omega)/\Gamma$ において 4 点集合 X と同じ剰余類に含まれる 4 点集合は丁度 6 個ある. さて $|X| \geq 5$ のときは X の 5 点を含む $C \in \mathbb{O}$ を選ぶと

$$|X + C| = |X| + |C| - 2\,|X \cap C| \leq |X| - 2$$

となるので, これを繰り返して $|X + Y| \leq 4$ となるような $Y \in \Gamma$ を得る. このとき $Z = X + Y$ とおくと $|Z| \leq 4$, かつ $X + Z = Y \in \Gamma$ をみたす. 従って X は 4 点以下の集合 Z と同じ剰余類に入る. これよりすべての剰余類が 4 点以下の集合を含むことがわかる. ゆえに

$$|\,P(\Omega)/\Gamma\,| \;\leq\; 1 + \binom{24}{1} + \binom{24}{2} + \binom{24}{3} + \frac{1}{6} \cdot \binom{24}{4}$$

が成立する. これと (2.2) より $|P(\Omega)/\Gamma| = 2^{12}$, すなわち $\dim \Gamma = 12$ を得る.

次に $\dim\Gamma = 12$ と仮定して $|\mathbb{O}| = 759$ を導く. $|P(\Omega)/\Gamma| = 2^{12}$ より任意の 4 点を含む $C \in \mathbb{O}$ は丁度 5 個存在する. 従って

$$\left\{ (Y, C) \,\middle|\, |Y| = 4\,, Y \subseteq C\,, C \in \mathbb{O} \right\}$$

を 2 通りに計算すると

$$\binom{8}{4} \cdot |\mathbb{O}| = \binom{24}{4} \cdot 5$$

が得られる. よって $|\mathbb{O}| = 759$ が示された. ∎

系 2.2 *$dim\Gamma = 12$ のとき $\Gamma = \langle \mathbb{O} \rangle$ が成り立つ.*

Proof　補題 2.1 (3) より $|\mathbb{O}| = 759$ である. ここで $\Delta = \langle \mathbb{O} \rangle$ とおくと $\Delta \subseteq \Gamma$ であることから Δ は(2.1) をみたす. 従って Γ についての上述の結果は Δ に対しても成り立つ. $\mathbb{O} \subseteq \Delta$ であるので補題 2.1 (3) を適用すると $\dim\Delta = 12$ を得る. 従って $\Delta = \Gamma$ が成り立つ. ∎

24 点集合 Ω のべき集合 $P(\Omega)$ の部分空間 Γ で, 条件(2.1) と $\dim\Gamma = 12$ をみたすものを Ω 上の Binary Goley Code という. Γ が Binary Goley Code のとき $|\mathbb{O}| = 759$ が成り立つ. 従って補題 2.1 (1) の証明のなかで注意したように Ω の任意の 5 点を含む $\mathbb{O}$ の元がただ 1 つ存在する. すなわち $(\Omega, \mathbb{O})$ は Steiner system S(5,8,24) をなす.

Binary Goley Code の存在

ここでは 23 元体 $\mathbb{F}_{23}$ 上の 1 次元射影空間を Ω とおく. $|\Omega| = 24$ である. ここで次の同一視を行う.

$$\Omega \ni \begin{bmatrix} a \\ 1 \end{bmatrix} \quad \longleftrightarrow \quad a \in \mathbb{F}_{23}\,, \qquad \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \longleftrightarrow \quad \infty$$

これにより $\Omega = \{\infty\} \cup \mathbb{F}_{23}$ とおくことができる. 定理 1.7 により $L_2(23)$ は Ω に 2 重可移に作用する. さて $i \in \mathbb{F}_{23}$ に対して $\infty + i = \infty$ と定め

$$Q = \{\, x^2 \mid x \in \mathbb{F}_{23} \,\}\,, \quad N = \Omega - Q\,, \quad N_i = \{\, n + i \mid n \in N \,\}\ (i \in \mathbb{F}_{23})\,, \quad N_\infty = \Omega$$

として, $P(\Omega)$ の部分空間 Γ を $\Gamma = \langle N_i \mid i \in \Omega \rangle$ と定める. 以下 Γ が Binary Goley Code であることを示す.

$$Q = \{0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$$
$$N = \{\infty, 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$$

であることから次の補題を得る.

補題 2.3 $N = \{\infty, -x^2 \mid x \in \mathbb{F}_{23}^*\}$ である.

補題 2.4 $L_2(23)$ は Ω に 3-*homogeneous* に作用する.

Proof　$L_2(23)$ が Ω の 3 点集合上可移であることを示せばよい. Ω の 3 点集合 $\{\alpha, \beta, \gamma\}$ を任意に選ぶと定理 1.7 より $L_2(23)$ は Ω 上 2 重可移であるから (α, β) を $(\infty, 0)$ に移す $\bar{g} \in L_2(23)$ が存在する. $\bar{g} : \gamma \mapsto y$ とする. ここで $\mathbb{F}_q^*$ の生成元を a として

$$g_0 = \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix}$$

とおく. $g_0 \in SL(2, 23)$ であり, $\bar{g_0}$ は ∞ と 0 を固定する. また $\Omega - \{\infty, 0\}$ における $\langle \bar{g_0} \rangle$ -orbit は

$$\{\, a^{2i}\, y \mid i \in \mathbb{Z} \,\}, \qquad \{\, -a^{2i}\, y \mid i \in \mathbb{Z} \,\}$$

の 2 つで, 1 と -1 は異なる軌道に属する. これより $L_2(23)$ は任意の 3 点集合を $\{\infty, 0, 1\}$ か $\{\infty, 0, -1\}$ に移す. 一方

$$g_1 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$$

とすると $\bar{g_1} \in L_2(23)$ であり, $\bar{g_1}$ は 0 を固定し, 1 を ∞ に, ∞ を -1 に移す. 従って $\bar{g_1}$ は $\{\infty, 0, 1\}$ を $\{\infty, 0, -1\}$ に移す. 以上で任意の 3 点集合が $\{\infty, 0, -1\}$ に移されることが示された. よって $L_2(23)$ は 3-homogeneous である. ∎

補題 2.5 $L_2(23)$ の各元の Ω における固定点は高々 2 個である.

Proof　$SL(2,23)$ の元 $A=\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ を任意に選ぶ．$\bar{A}$ が ∞ を固定するとする．このとき $c=0$ である．更に $x\in\mathbb{F}_{23}$ を固定すると

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} x \\ 1 \end{bmatrix}=\begin{bmatrix} ax+b \\ d \end{bmatrix}$$

より $ax+b=dx$ が成り立つ．このような x は高々 1 個であるから $\bar{A}$ によって固定される点は高々 2 個である．

次に $\bar{A}$ が ∞ を固定しないとする．このとき $c\neq 0$ である．$x\in\mathbb{F}_{23}$ を固定するとすると

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} x \\ 1 \end{bmatrix}=\begin{bmatrix} ax+b \\ cx+d \end{bmatrix}$$

より $ax+b=cx^2+dx$ が成り立つ．このような x は高々 2 個であるから $\bar{A}$ によって固定される点は高々 2 個である． ∎

補題 2.6 $X\in\Gamma$ のとき $|X|$ は 4 の倍数である．

Proof　$X\in\Gamma$ を任意に選ぶと $X=N_{a_1}+N_{a_2}+\cdots+N_{a_k}$ と表される．ただし $a_i\in\Omega$ である．ここで $|N_\infty|=24$ であるから $|X|$ が 4 の倍数であることと $|X+N_\infty|$ が 4 の倍数であることとは同値である．従って, 必要ならば X を $X+N_\infty$ で置き換えることにより $a_1,\ldots,a_k$ の中に ∞ が含まれていないとしてよい．

以下 k についての帰納法を用いて示す．　$k=1$ のとき, 任意の $a\in\mathbb{F}_{23}$ に対して $|N_a|=|N|=12$ であるから $|X|$ は 4 の倍数である．$k=2$ のとき $X=N_{a_1}+N_{a_2}$ と表される．ここで $N_{a_1}+N_{a_2}$ を $-a_1$ 平行移動すると $N+N_{a_2-a_1}$ が得られる．従って $|N+N_{a_2-a_1}|$ が 4 の倍数であることを示せばよい．$b=a_2-a_1$ とおき $|N+N_b|$ が 4 の倍数であることを示すことにする．$b=0$ のときは明らかに成り立つので $b\neq 0$ とする．$\infty\neq z\in N\cap N_b$ に対して $z=-x^2=-y^2+b$ をみたす $x,y\in\mathbb{F}_{23}^*$ が存在する．ここで $(y-x)(y+x)=b$ であることから $y-x$ は $\mathbb{F}_{23}^*$ の元である．逆に $\mathbb{F}_{23}^*$ の任意の元 c に対して方程式 $\begin{cases} y-x=c \\ y+x=\frac{b}{c} \end{cases}$ より $(y-x)(y+x)=b$ をみたす x,y が定まる．従って $(y-x)(y+x)=b$ の解 (x,y) は 22 組あるが, そのうち $x\neq 0$ かつ $y\neq 0$ となるのは 20 組である．ここで 4 組 $(\pm x,\pm y)$ は同一の x^2, y^2 に対応することから $|N\cap N_b|$ は $\frac{20}{4}$ に ∞ の 1 を加えればよい．よって $|N\cap N_b|=\frac{20}{4}+1$ を得る．これは偶数であるから定理 1.28 より $|N+N_b|$ は 4 の倍数である．

次に $k > 2$ とし, $k-1$ 以下では成り立っているものとする.

$$Y = N_{a_1} + \cdots + N_{a_{k-1}}\,, \qquad Z = N_{a_1} + \cdots + N_{a_{k-2}}$$

とすると $|N_{a_k}|$ が 4 の倍数であり, また帰納法の仮定より $|Y|$ も 4 の倍数であるので, 定理 1.28 より $|Y \cap N_{a_k}|$ が偶数であることを示せばよい. 一方, 帰納法の仮定より $|Z + N_{a_k}|$, $|N_{a_{k-1}} + N_{a_k}|$ は 4 の倍数である. 従って定理 1.28 より $|Z \cap N_{a_k}|$, $|N_{a_{k-1}} \cap N_{a_k}|$ は偶数である. このとき定理 1.29 より

$$|(Z + N_{a_{k-1}}) \cap N_{a_k}| = |Y \cap N_{a_k}|$$

は偶数である. 以上で k の場合も成り立つので, $|X|$ が 4 の倍数であることが示された. ∎

補題 2.7 $L_2(23)$ の任意の元 σ に対して $\Gamma^\sigma = \Gamma$ が成り立つ.

Proof　定理 1.5 より $L_2(23) = \langle\, \bar{\alpha_a}, \bar{\beta}, \bar{\gamma} \mid a \in \mathbb{F}_{23} \,\rangle$ が成り立つ. ただし

$$\alpha_a = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}\,,\ a \in \mathbb{F}_{23}\,, \quad \beta = \begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix}, \quad \gamma = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

であり, b は乗法群 $\mathbb{F}_{23}^*$ の生成元である. $\Gamma = \langle N_i \mid i \in \Omega \rangle$ であるから $N_i^{\alpha_a}$, N_i^β, N_i^γ がすべて Γ に含まれることを示せばよい. $i = \infty$ のときは $N_\infty = \Omega$ より $N_\infty = N_\infty^{\alpha_a} = N_\infty^\beta = N_\infty^\gamma$ であるから, すべて Γ に含まれる. 次に $x \in \Omega$, $x \neq \infty$ とすると

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ 1 \end{bmatrix} = \begin{bmatrix} x+a \\ 1 \end{bmatrix}, \qquad \begin{bmatrix} b & 0 \\ 0 & b^{-1} \end{bmatrix} \begin{bmatrix} x \\ 1 \end{bmatrix} = \begin{bmatrix} bx \\ b^{-1} \end{bmatrix} = \begin{bmatrix} b^2 x \\ 1 \end{bmatrix}$$

および $\infty^{\alpha_a} = \infty^\beta = \infty$ であることから

$$N_x^{\alpha_a} = \{\, (n+x)^{\alpha_a} \mid n \in N \,\} = \{\, n + x + a \mid n \in N \,\} = N_{x+a} \in \Gamma$$

と

$$N_x^\beta = \{\, (n+x)^\beta \mid n \in N \,\} = \{\infty\} \cup \{\, b^2 n + b^2\, x \mid n \in N - \{\infty\} \,\} = N_{b^2 x} \in \Gamma$$

が得られる. 一方

$$\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \text{および} \quad \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} -x^2 \\ 1 \end{bmatrix} = \begin{bmatrix} -1 \\ -x^2 \end{bmatrix} = \begin{bmatrix} \left(\frac{1}{x}\right)^2 \\ 1 \end{bmatrix}$$

より $N_0^\gamma = Q = N_0 + N_\infty \in \Gamma$ が成り立つ. また

$$\begin{aligned} N_{-1} &= \{\infty, 4, 6, 9, 10, 13, 14, 16, 18, 19, 20, 21\} \\ N_0 &= \{\infty, 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\} \\ N_1 &= \{\infty, 0, 6, 8, 11, 12, 15, 16, 18, 20, 21, 22\} \\ (N_{-1})^\gamma &= \{0, 5, 6, 7, 8, 10, 12, 14, 16, 17, 18, 19\} \end{aligned}$$

であることから $(N_{-1})^\gamma = N_0 + N_1$ を得る. これより $x \notin Q$ のとき $x = -s,\ \ s = b^{2j}$, $t = s^{-1}$ として $\beta\gamma = \gamma\beta^{-1}$ に注意すれば

$$\begin{aligned} N_x^\gamma &= (N_{-s})^\gamma = (N_{-b^{2j}})^\gamma = (N_{-1})^{\beta^j\gamma} = (N_{-1})^{\gamma\beta^{-j}} \\ &= (N_0 + N_1)^{\beta^{-j}} = N_0^{\beta^{-j}} + N_1^{\beta^{-j}} \\ &= N_0 + N_{b^{-2j}} = N_0 + N_t \in \Gamma \end{aligned}$$

が得られる. 更に $\bar{\gamma}^2 = \bar{1}$ であるから

$$N_{-s} = (N_{-s}^\gamma)^\gamma = N_0^\gamma + N_t^\gamma = N_0 + N_\infty + N_t^\gamma$$

となるので

$$N_t^\gamma = N_\infty + N_0 + N_{-s} \in \Gamma$$

を得る. すなわち $x = t = b^{-2j} \in Q$ のときも $N_x^\gamma \in \Gamma$ が得られた. ∎

補題 2.8 $\emptyset \neq X \in \Gamma$ ならば $|X| \geq 8$ となる.

Proof　定理 1.4 より $|L_2(23)| = 6072$ となり 3 で割り切れる. 従って定理 1.13 により $L_2(23)$ には位数 3 の元 σ が存在する. また補題 2.5 より $L_2(23)$ の各元は Ω に固定点を高々 2 個しかもたないので σ は Ω に固定点をもたない. よって σ は 8 個の 3 -cycle の積 $\sigma = (i, j, k)(\cdots)(\cdots)\cdots$ に分解できる.

さて Γ に $|X| < 8$ となる $X \neq \emptyset$ が存在すると仮定する. このとき 補題 2.6 より $|X| = 4$ が成り立つ. また補題 2.4 より $X = \{i, j, k, h\}$ としてよい. このとき補題 2.7 より $X^\sigma = \{i, j, k, h^\sigma\} \in \Gamma$ である. ここで σ が固定点を持たないことから $h^\sigma \neq h$ となるが, $\Gamma \ni X + X^\sigma = \{h, h^\sigma\}$ となり補題 2.6 に反する. 以上で補題が証明された. ∎

定理 2.9 $\dim \Gamma = 12$ である. 従って Γ は *Binary Golay Code* である.

Proof　$0 \leq i \leq 10$ に対して $X_i = N_{-2+i} + N_i + N_{2+i} + N_{-3+i}$ とすると

$$X_0 = \{0,1,2,3,4,7,10,12\} \qquad X_1 = \{1,2,3,4,5,8,11,13\}$$
$$X_2 = \{2,3,4,5,6,9,12,14\} \qquad X_3 = \{3,4,5,6,7,10,13,15\}$$
$$X_4 = \{4,5,6,7,8,11,14,16\} \qquad X_5 = \{5,6,7,8,9,12,15,17\}$$
$$X_6 = \{6,7,8,9,10,13,16,18\} \qquad X_7 = \{7,8,9,10,11,14,17,19\}$$
$$X_8 = \{8,9,10,11,12,15,18,20\} \qquad X_9 = \{9,10,11,12,13,16,19,21\}$$
$$X_{10} = \{10,11,12,13,14,17,20,22\}$$

が得られる. ここで $\mathcal{X} = \{X_i \mid 0 \leq i \leq 10\} \cup \{\Omega\}$ とおく. いま

$$a_0X_0 + a_1X_1 + \cdots + a_{10}X_{10} + a_{11}\Omega = \emptyset$$

が成り立つと仮定する. ただし $a_i \in \mathbb{F}_2$ $(0 \leq i \leq 11)$ である. このとき $\mathcal{X}$ の元で ∞ を含むものが Ω のみであることから $a_{11} = 0$ を得る. 次に $\mathcal{X} - \{\Omega\}$ の元で 22 を含むものが X_{10} のみであるので $a_{10} = 0$ を得る. 更に $\mathcal{X} - \{X_{10}, \Omega\}$ の元で 21 を含むものが X_9 のみであるので $a_9 = 0$ を得る. 以下同様にして $a_0 = a_1 = \cdots = a_{11} = 0$ が得られる. ゆえに $\mathcal{X}$ は 1 次独立である. よって $\dim \Gamma \geq 12$ であるが, 補題 2.8 より Γ は(2.1) をみたすので補題 2.1 (2) が適用できる. よって $\dim \Gamma = 12$ が成り立つ. Γ が Binary Goley Code であることは定義から明らかである. ∎

Γ に含まれるすべての 8 点集合のなす集合を $\mathbb{O}$ とすると $(\Omega, \mathbb{O})$ は S(5,8,24) である. これより次の定理を得る.

定理 2.10 S(5,8,24) が存在する.

2.2　S(5,8,24) の構造

以下 $(\Omega, \mathbb{B})$ は S(5,8,24) であるとして, $\mathbb{B}$ の元を octad と呼ぶことにする. また Ω の 5 点 $a_1, \ldots, a_5$ を含む octad を $C(a_1, \ldots, a_5)$ と表すことにする. octad という用語, および $C(a_1, \ldots, a_5)$ なる記号はこの論文を通じて頻繁に利用される. なお $(\Omega, \mathbb{B})$ が Binary Golay Code から得られたものであるかどうかは (この段階では) 断定できないことを注意しておく.

補題 2.11 $|\mathbb{B}| = 759$ である.

Proof　Ω の任意の 5 点集合に対して, それを含む octad が丁度 1 個であることに注意して集合

$$\{\,(X,C)\,\big|\,|X|=5, X\subseteq C, C\in\mathbb{B}\,\}$$

の元の個数を 2 通りに計算すると

$$\binom{24}{5}\cdot 1=\binom{8}{5}\cdot|\mathbb{B}|$$

が得られる. これより $|\mathbb{B}|=759$ が導かれる. ∎

$1\leq n\leq 4$ とする. Ω の n 点集合を任意に選び S とし, S を含む octad の個数を N とする. $\Omega-S$ から $5-n$ 点を選ぶと S とその $5-n$ 点を合わせた 5 点集合を含む octad が 1 つ定まることに注意して集合

$$\{\,(X,C)\,\big|\,X\cap S=\emptyset, |X|=r, X\cup S\subseteq C, C\in\mathbb{B}\,\}$$

の元の個数を 2 通りに計算すると

$$\binom{8-n}{5-n}\cdot N=\binom{24-n}{5-n}\cdot 1$$

が得られる. これより $n=0,1,2,3,4$ に対して, それぞれ $N=759, 253, 77, 21, 5$ となる. さて次の表 2.1 の上から $k+1$ 行目の右端の数は Ω の k 点を含む octad の個数を表す. ただし $0\leq k\leq 8$ とし, k 点はある octad に含まれるようなものを選ぶことにする.

							759									
						506		253								
					330		176		77							
				210		120		56		21						
			130		80		40		16		5					
		78		52		28		12		4		1				
	46		32		20		8		4		0		1			
30		16		16		4		4		0		0		1		
30		0		16		0		4		0		0		0		1

表 2.1

上の表の $k+1$ 行目の右から $j\,(\geq 1)$ 番目の数は Ω の点 $a_1,\ldots,a_k$ に対して $a_1,\ldots,a_{j-1}$ を含まず, $a_j,\ldots,a_k$ を含む octad の個数を表す. たとえば上から 3 行目は, 右から順に a_1,a_2 を含む octad が 77 個, a_1 を含まず, a_2 を含む octad が 176 個, a_1,a_2 を含まない octad が 330 個あることを表している. さて Ω の $k+1$ 点 $a_1,\ldots,a_{k+1}$ を含む octad の個数と $a_1,\ldots,a_k$ を含み, a_{k+1} を含まない octad の個数の和が $a_1,\ldots,a_k$ を含む octad の個数

になることより次の表 2.1 の $k+1$ 行の右端と $k+2$ 行の右端から $k+2$ 行の右から 2 番目の数が得られる. 同様にしてその他の数も得られる. 表 2.1 の 最下行より次の定理を得る.

補題 2.12 $X, Y \in \mathbb{B}$ に対して $|X \cap Y|$ は 0, 2, 4 または 8 である.

補題 2.13 (Todd) $X, Y \in \mathbb{B}$ が $|X \cap Y| = 4$ をみたすとき $X + Y \in \mathbb{B}$ である.

Proof $X = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8\}$, $Y = \{x_1, x_2, x_3, x_4, y_5, y_6, y_7, y_8\}$ とおき $X + Y$ が $\mathbb{B}$ に含まれないと仮定する. ここで $Z = C(x_5, x_6, x_7, x_8, y_5)$ とすると $|Z \cap X| \geq 4$ かつ $Z \neq X$ であるから, 補題 2.12 より $|Z \cap X| = 4$ となり $x_1, x_2, x_3, x_4 \notin Z$ を得る. これより $1 \leq |Z \cap Y| \leq 4$ が導かれる. いま $|Z \cap Y| = 4$ とすると $\mathbb{B} \ni Z = \{x_5, x_6, x_7, x_8, y_5, y_6, y_7, y_8\} = X + Y$ となり仮定に反する. 従って補題 2.12 より $|Z \cap Y| = 2$ となる. 以下 $Z \cap Y = \{y_5, y_6\}$ とおく.

$W = C(x_5, x_6, x_7, x_8, y_7)$ とおくと, 同様にして $|W \cap Y| = 2$ が得られる. いま $y_5 \in W \cap Y$ とすると $W \cap Z \ni x_5, x_6, x_7, x_8, y_5$ より, $Z = W$ となり $Z \cap Y = \{y_5, y_6\}$ としたことに矛盾する. $y_6 \in W \cap Y$ としても同様に矛盾が生じる. 従って $W \cap Y = \{y_7, y_8\}$ である.

次に $U = C(x_5, x_6, x_7, y_5, y_7)$ とおく. X, Z, W が y_5, y_7 のいずれかを含まないことから $U \neq X, Y, Z, W$ が成り立つ. 補題 2.12 より $|U \cap X| = 4$ である. $x_8 \in U$ ならば $U = Z$ となり 矛盾が生じるので $x_8 \notin U$ である. 従って x_1, x_2, x_3, x_4 のいずれかが U に含まれる. 一般性を失うことなく $x_1 \in U$ としてよい. このとき $|U \cap Y| \geq 3$ となるが $U \neq Y$ であるから $|U \cap Y| = 4$ が成り立つ. x_2, x_3, x_4 のいずれかが U に含まれると $|U \cap X| \geq 5$ より $U = X$ となり矛盾が生じる. また $y_6 \in U$ ならば $|U \cap Z| \geq 5$ より $U = Z$ となり矛盾が生じる. $y_8 \in U$ と仮定しても $|U \cap W| \geq 5$ より $U = W$ となり矛盾が生じる. いずれの場合も矛盾が生じたので $X + Y \in \mathbb{B}$ が示された. ∎

sextet

Ω に含まれる 6 つの 4 点集合 $S = \{T_1, T_2, T_3, T_4, T_5, T_6\}$ が次の条件をみたすとき sextet という. また各 T_i を sextet の成分という.

(1) $i \neq j$ ならば $T_i \cap T_j = \emptyset$

(2) $\Omega = T_1 \cup T_2 \cup T_3 \cup T_4 \cup T_5 \cup T_6$

(3)　任意の $i \neq j$ に対して $T_i \cup T_j$ は octad である.

定理 2.14 Ω の任意の 4 点集合 T_0 を成分とする *sextet*が一意に存在する.

Proof　表 2.1 より T_0 を含む octad は 5 個存在する. それらを C_1, C_2, C_3, C_4, C_5 とおく. ここで $T_i = C_i - T_0$ とおくと $|T_i| = 4$ が成り立つ $(1 \leq i \leq 5)$.

$i \neq j$ のときは $C_i \cap C_j = T_0$ より $T_i \cap T_j = \emptyset$ が得られる. これより

$$|T_0 \cup T_1 \cup T_2 \cup T_3 \cup T_4 \cup T_5| = 24$$

となることから $\Omega = T_0 \cup T_1 \cup T_2 \cup T_3 \cup T_4 \cup T_5$ が成り立つ.

また $i \neq 0$ のときは T_i の定め方より $T_0 \cup T_i = C_i$ は octad である. $i \neq j$ が共に 0 でないときは $T_i \cup T_j = C_i + C_j$ となることから補題 2.13 より $T_i \cup T_j$ は octad である. 以上で $\{T_i\}_{0 \leq i \leq 5}$ が sextet であることが示された. また T_0 を含む octad が 5 個であるから T_0 を成分とする sextet が一意に定まることは明らかである. ∎

定理 2.15 $\{T_k\}_{0 \leq k \leq 5}$ が *sextet, C* が *octad* のとき 6 個の整数 $|C \cap T_k|$ は次のいずれかをみたす.

(1)　4 が 2 個, 0 が 4 個.

(2)　3 が 1 個, 1 が 5 個.

(3)　2 が 4 個, 0 が 2 個.

Proof　$|C \cap T_k|_{0 \leq k \leq 5}$ の最大値が 1 以下ならば $|C| \leq 6$ となり矛盾が生じる. 従って $|C \cap T_k|$ の最大値は 2, 3 または 4 である.

最大値が 4 のとき $|C \cap T_i| = 4$, $C \cap T_j \neq \emptyset$ となる $i \neq j$ が存在する. このとき $T_i \cup T_j \in \mathbb{B}$ かつ $|C \cap (T_i \cup T_j)| \geq 5$ であるから $C = T_i \cup T_j$ が成り立つ. 従ってこの場合 $|C \cap T_k|_{0 \leq k \leq 5}$ は 4 が 2 個, 0 が 4 個である.

最大値が 3 であるとして $|C \cap T_i| = 3$ とする. いま $|C \cap T_j| \geq 2$ となる $j \neq i$ が存在すると仮定する. このとき $|C \cap (T_i \cup T_j)| \geq 5$ となり $C = T_i \cup T_j$ が得られ, $|C \cap T_i| = 3$ であることに矛盾する. 従って $j \neq i$ に対して $|C \cap T_j| \leq 1$ である. よってこの場合は 3 が 1 個, 1 が 5 個である.

最大値が 2 であるとして $|C \cap T_i| = 2$ とする. いま $|C \cap T_j| = 1$ となる $i \neq j$ が存在すると仮定すれば $|C \cap (T_i \cup T_j)| = 3$ となり補題 2.12 に矛盾する. よってこの場合は 2 が 4 個, 0 が 2 個である. ∎

以下 octad と sextet の交わりが上の定理の (1),(2),(3) のいずれになるかにより, $[4^2 0^4]$ 型, $[3^1 1^5]$ 型, $[2^4 0^2]$ 型と呼ぶことにする.

次に任意の sextet に対して 3 つの型が起こり得ることを示す.

$S = \{T_i \mid 0 \leq i \leq 5\}$ を sextet として $T_i = \{a_i, b_i, c_i, d_i\}$ とおく. このとき $T_0 \cup T_1$ は octad であり, S との交わりは $[4^2 0^4]$ 型である.

$C = C(a_0, a_1, a_2, a_3, a_4)$ とおく. C の残りの 3 点がどの成分に含まれても $|C \cap T_i| = 1$ となる i が存在する. 従って この場合は $[3^1 1^5]$ 型である.

$C = C(a_0, b_0, a_1, b_1, a_2)$ とおく. $|C \cap T_0| \geq 2$, $|C \cap T_1| \geq 2$, $|C \cap T_2| \geq 1$ であるから $[4^2 0^4]$ 型, $[3^1 1^5]$ 型ではあり得ない. 従ってこの場合は $[2^4 0^2]$ 型である.

M-行列

Ω の部分集合 X に対して X を含む octad が存在するとき X は special であるという. special でないとき non-special であるという. また $\{x_1, x_2, x_3, x_4, x_5, x_6\}$ が non-special であり, $\{x_2, x_3, x_4, x_5, x_6, x_7\}$ が special であるような 7 点順列 $(x_1, x_2, x_3, x_4, x_5, x_6, x_7)$ を $(\Omega, \mathbb{B})$ の M-順列, または単に M-順列という.

補題 2.16 *non-special な* $X = \{x_1, x_2, x_3, x_4, x_5, x_6\}$ *に対して* $X_i = X - \{x_i\}$, X_i *を含む octad を* $X(i)$, $T_i = (X(i) - X_i) \cup \{x_i\}$ *とおく* $(1 \leq i \leq 6)$. *このとき* $\{T_i\}_{1 \leq i \leq 6}$ *は sextet である.*

Proof X が non-special であるから $x_i \notin X(i)$ である. 従って $|T_i| = |X(i)| - |X_i| + 1 = 4$ が成り立つ. また $i \neq j$ のとき $x_i \in X(j)$ より $X(i) \neq X(j)$ となる. ここで $X_i \cap X_j \subseteq X(i) \cap X(j)$, $|X_i \cap X_j| = 4$ より $X_i \cap X_j = X(i) \cap X(j)$ を得る. よって $X(i) \cap X(j) = \{x_k \mid k \neq i, j\}$ が得られる. これより $T_i \cap T_j = \emptyset$ が導かれる. 元の個数を考えると $\Omega = T_1 \cup T_2 \cup \cdots \cup T_6$ が得られる. 一方 $i \neq j$ のとき $T_i \cup T_j = X(i) + X(j)$, $|X(i) \cap X(j)| = |X_i \cap X_j| = 4$ であるから, 補題 2.13 より $T_i \cup T_j$ は octad である. よって $\{T_i\}_{1 \leq i \leq 6}$ は sextet である. ∎

以下本論文を通じて non-special な $X = \{x_1, x_2, x_3, x_4, x_5, x_6\}$ に対して $X(i)$ は上の補題で定めた octad を表すものとする.

次に M-行列の概念を導入する. M-行列とは Ω の元を成分とする 4×6 行列であり, octad が特別な位置に配置されたものである. 次節で Steiner system $S(5, 8, 24)$ の一意性を示すのに必要となる. 定義の前に記号などを準備する.

$$\mathbf{M} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & a_{26} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & a_{36} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} & a_{46} \end{bmatrix}$$

とおき 8 点集合 $\mathbf{M}(1), \ldots, \mathbf{M}(8)$ を

$$\begin{aligned}
\mathbf{M}(1) &= \{a_{12}, a_{13}, a_{14}, a_{15}, a_{16}, a_{21}, a_{31}, a_{41}\} \\
\mathbf{M}(2) &= \{a_{11}, a_{12}, a_{13}, a_{14}, a_{21}, a_{22}, a_{23}, a_{24}\} \\
\mathbf{M}(3) &= \{a_{11}, a_{12}, a_{13}, a_{14}, a_{31}, a_{32}, a_{33}, a_{34}\} \\
\mathbf{M}(4) &= \{a_{11}, a_{12}, a_{13}, a_{14}, a_{41}, a_{42}, a_{43}, a_{44}\} \\
\mathbf{M}(5) &= \{a_{13}, a_{14}, a_{15}, a_{16}, a_{23}, a_{24}, a_{25}, a_{26}\} \\
\mathbf{M}(6) &= \{a_{13}, a_{14}, a_{15}, a_{16}, a_{33}, a_{34}, a_{35}, a_{36}\} \\
\mathbf{M}(7) &= \{a_{13}, a_{14}, a_{15}, a_{16}, a_{43}, a_{44}, a_{45}, a_{46}\} \\
\mathbf{M}(8) &= \{a_{11}, a_{12}, a_{13}, a_{24}, a_{31}, a_{35}, a_{41}, a_{46}\}
\end{aligned}$$

と定める (これらを行列の位置で表したものを p.93 の付録に記す).
更に $1 \leq i \neq j \leq 6$ に対して

$$\mathbf{M}(ij) = \{a_{1i}, a_{2i}, a_{3i}, a_{4i}, a_{1j}, a_{2j}, a_{3j}, a_{4j}\}$$

と定める. $\mathbf{M}(ij)$ は i 列と j 列の和である.

定義 2.17 Ω の元を次の条件をみたすように 4×6 行列 $\mathbf{M}$ に配置したものを $(\Omega, \mathbb{B})$ の *M*-行列, または単に *M*-行列という.

(0) 任意の $1 \leq i \neq j \leq 6$ に対して $\mathbf{M}(ij)$ は *octad* である.

(1) 8 つの 8 点集合 $\mathbf{M}(1)$, ... , $\mathbf{M}(8)$ は *octad* である.

M-行列において $(a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}, a_{21})$ が M-順列であることを注意しておく. 次に M-行列になるように Ω の点を配置できることを示す.

定理 2.18 *M*-行列は存在する.

Proof $C \in \mathbb{B}$, $x_1 \notin C$, $x_2, x_3, x_4, x_5, x_6, x_7 \in C$ を選ぶと $(x_1, x_2, x_3, x_4, x_5, x_6, x_7)$ は M-順列になる. 補題 2.16 より sextet $S = \{T_i\}_{1 \le i \le 6}$ と octad $X(i)$, 5 点集合 X_i が得られる $(1 \le i \le 6)$. ここで

$$a_{1i} = x_i\,, \qquad T_i = \{a_{1i}, a_{2i}, a_{3i}, a_{4i}\} \qquad (1 \le i \le 6)$$

をみたすように Ω の点を配置したものを $\mathbf{M}$ とおく. $x_7 \in X(1)$ より $a_{21} = x_7$ であるとしてよい.

さて $\mathbf{M}(ij) = T_i + T_j$ であるから任意の $1 \le i \ne j \le 6$ に対して $\mathbf{M}(ij)$ は octad である. 従って定義 2.17 の条件 (0) がみたされる.

$\mathbf{M}(1) = X(1)$ であるから $\mathbf{M}(1)$ は octad である. 次に $\mathbf{M}(2), \cdots, \mathbf{M}(8)$ が octad になるように a_{ij} を並べ換える. ただし, 同じ列内で並べ替えるときは $\mathbf{M}(ij)$ が octad であることに影響はない.

$D(b) = C(a_{11}, a_{12}, a_{13}, a_{14}, a_{21})$ とおく. このとき $X(1) \ne D(b)$, $|X(1) \cap D(b)| \ge 4$ より $|X(1) \cap D(b)| = 4$ を得る. 従って $a_{15}, a_{16}, a_{31}, a_{41} \notin D(b)$ が成り立つ. 定理 2.15 より $D(b)$ と S との交わりは $[2^4 0^2]$ 型となるから $D(b)$ の残りの 3 点を列を変えないように a_{22}, a_{23}, a_{24} の位置に移せば $\mathbf{M}(2) = D(b)$ が octad となる. また, このとき $\mathbf{M}(1)$ が octad であることに変わりはない.

$D(c) = C(a_{11}, a_{12}, a_{13}, a_{14}, a_{31})$ とおく. $|X(1) \cap D(c)| = |\mathbf{M}(2) \cap D(c)| = 4$ より, S との交わりは $[2^4 0^2]$ 型となるので $a_{15}, a_{16}, a_{21}, a_{22}, a_{23}, a_{24}, a_{41} \notin D(c)$ である. $D(c)$ の残りの 3 点を列を変えないように a_{32}, a_{33}, a_{34} の位置に移せば $\mathbf{M}(3) = D(c)$ が octad となる. また, このとき $\mathbf{M}(1)$, $\mathbf{M}(2)$ が octad であることに変わりはない. 一方

$$\mathbf{M}(4) = \big((\mathbf{M}(2) + \mathbf{M}(3)) + \mathbf{M}(12)\big) + \mathbf{M}(34)$$

であるので補題 2.13 により $\mathbf{M}(4)$ も octad である.

$D(e) = C(a_{13}, a_{14}, a_{15}, a_{16}, a_{23})$ とおく. $|X(3) \cap D(e)| = 4$ より $a_{11}, a_{12}, a_{33}, a_{43} \notin D(e)$ を得る. 従って S との交わりは $[2^4 0^2]$ 型である. $3 \le |D(e) \cap \mathbf{M}(2)| \le 6$ より $|D(e) \cap \mathbf{M}(2)| = 4$ となるので $a_{24} \in D(e)$ である. $D(e)$ の残りの 2 点を列を変えないように a_{25}, a_{26} の位置に移せば $\mathbf{M}(5) = D(e)$ が octad となる. また, このとき $\mathbf{M}(1)$, ... , $\mathbf{M}(4)$ が octad であることに変わりはない.

$D(f) = C(a_{13}, a_{14}, a_{15}, a_{16}, a_{33})$ とおく. $|X(3) \cap D(f)| = 4$ より $a_{11}, a_{12}, a_{23}, a_{43} \notin D(f)$ を得る. 従って S との交わりは $[2^4 0^2]$ 型である. ここで $3 \le |D(f) \cap \mathbf{M}(3)| \le 6$ よ

り $|D(f)\cap\mathbf{M}(3)|=4$ となるから $a_{34}\in D(f)$ でなければならない. 一方 $|\mathbf{M}(5)\cap D(f)|=4$ であることより $a_{25},a_{26}\notin D(f)$ が成り立つ. 従って $D(f)$ の残りの 2 点を列を変えないように a_{35}, a_{36} の位置に移せば $\mathbf{M}(6)=D(f)$ が octad となる. このとき $\mathbf{M}(1)$, ... , $\mathbf{M}(5)$ が octad であることに変わりはない. また

$$\mathbf{M}(7)=\big((\mathbf{M}(5)+\mathbf{M}(6))+\mathbf{M}(34)\big)+\mathbf{M}(56)$$

であるので補題 2.13 より $\mathbf{M}(7)$ も octad である.

$D(h)=C(a_{11},a_{12},a_{13},a_{31},a_{41})$ とおく. $|D(h)\cap\mathbf{M}(1)|=4$ より $a_{21},a_{14},a_{15},a_{16},\notin D(h)$ が成り立つ. このとき S との交わりは $[3^11^5]$ 型となるから, 残りの 3 点は $4,5,6$ 列の 2〜4 行にある. 一方 $|\mathbf{M}(2)\cap D(h)|=4$ より $a_{24}\in D(h)$ を得る. また $|\mathbf{M}(5)\cap D(h)|=2$ または 4 であるが, $|\mathbf{M}(5)\cap D(h)|=4$ とすると $a_{23}\in D(h)$ となり $[3^11^5]$ 型であることに矛盾する. よって $|\mathbf{M}(5)\cap D(h)|=2$ である. 同様にして $|\mathbf{M}(6)\cap D(h)|=2$ を得る. 以上から残る 2 点は $\{a_{35},a_{46}\}$ または $\{a_{36},a_{45}\}$ である. 前者の場合 $D(h)=\mathbf{M}(8)$ は octad である. 後者の場合 5 列と 6 列を交換する, すなわち a_{i5} と a_{i6} を交換することにより $D(h)=\mathbf{M}(8)$ とできる. この並べ換えにより $\mathbf{M}(1)$, ..., $\mathbf{M}(7)$, $\mathbf{M}(ij)$ が octad で あることに変わりはない.

以上で M-行列の条件をみたすように Ω の点を配置することができた. ∎

定理 2.19 *M*-順列 $(x_1,x_2,x_3,x_4,x_5,x_6,x_7)$ に対して x_i を $(1,i)$ 成分とし $(1\le i\le 6)$, x_7 を $(2,1)$ 成分とする *M*-行列が一意に定まる.

Proof $\mathbf{M}$, $\mathbf{N}$ を題意をみたす 2 つの M-行列として $\mathbf{M}$, $\mathbf{N}$ の (i,j) 成分をそれぞれ a_{ij},a'_{ij} とおく. このとき $a_{1i}=a'_{1i}=x_i$ $(1\le i\le 6)$, $a_{21}=a'_{21}=x_7$ が成り立つ. また $\mathbf{M}(k)$, $\mathbf{M}(ij)$ に対応する $\mathbf{N}$ の octad を $\mathbf{N}(k)$, $\mathbf{N}(ij)$ と表すことにする.

$i>1$ のとき octad $\mathbf{M}(1)+\mathbf{M}(1i)$ と $\mathbf{N}(1)+\mathbf{N}(1i)$ は 5 点を共有するので一致する. 従って

$$\{a_{2i},a_{3i},a_{4i}\}=\{a'_{2i},a'_{3i},a'_{4i}\}$$

が成り立つ. またこれより $\mathbf{M}(ij)=\mathbf{N}(ij)$ が得られる. 一方

$$\mathbf{M}(2)=C(x_1,x_2,x_3,x_4,x_7)=\mathbf{N}(2)$$

より

$$\{a_{22},a_{23},a_{24}\}=\{a'_{22},a'_{23},a'_{24}\}$$

を得る. 以上から

$$a'_{22} \in \{a_{22}, a_{32}, a_{42}\} \cap \{a_{22}, a_{23}, a_{24}\}$$

となり $a'_{22} = a_{22}$ が成り立つ. 同様にして $a'_{23} = a_{23}$, $a'_{24} = a_{24}$ が得られる.

次に

$$\mathbf{M}(5) = C(a_{13}, a_{14}, a_{15}, a_{16}, a_{23}) = C(a'_{13}, a'_{14}, a'_{15}, a'_{16}, a'_{23}) = \mathbf{N}(5)$$

となるので $\{a_{25}, a_{26}\} = \{a'_{25}, a'_{26}\}$ が得られるが, 上と同様にして $a'_{25} = a_{25}$, $a'_{26} = a_{26}$ が得られる. 一方

$$\mathbf{M}(8) = C(a_{11}, a_{12}, a_{13}, a_{31}, a_{41}) = C(a'_{11}, a'_{12}, a'_{13}, a'_{31}, a'_{41}) = \mathbf{N}(8)$$

が成り立つことから $a'_{35} = a_{35}$, $a'_{46} = a_{46}$ が得られ, これより $a'_{45} = a_{45}$, $a'_{36} = a_{36}$ も得られる. 更に

$$\mathbf{M}(6) = C(a_{13}, a_{14}, a_{15}, a_{16}, a_{35}) = C(a'_{13}, a'_{14}, a'_{15}, a'_{16}, a'_{35}) = \mathbf{N}(6)$$

より $a'_{33} = a_{33}$, $a'_{34} = a_{34}$ を得る. 同様にして $\mathbf{M}(7) = \mathbf{N}(7)$, $\mathbf{M}(3) = \mathbf{N}(3)$, $\mathbf{M}(4) = \mathbf{N}(4)$ から残りの成分の一致することが導かれる. 以上で $\mathbf{M} = \mathbf{N}$ が示された. ∎

Sextet $\mathbf{S_0}$〜$\mathbf{S_5}$

$\mathbf{M} = [a_{ij}]$ を M-行列として, 後節で必要となる 6 つの sextet S_0, ..., S_5 の $\mathbf{M}$ での配置を求める (これらの sextet $S_0, S_1, \cdots, S_5$ を M-行列に表したものを付録 p.94 に示す). 定理 2.14 より 4 点集合から sextet が定まることを想起されたい. なお, 以下において sextet $S_k = \{T_i\}_{1 \le i \le 6}$ の成分 T_i, T_j の和である octad を $S_k(i, j)$ と表すことにする.

($\mathbf{S_0}$) $\mathbf{M}$の 1 列 $T_1 = \{a_{11}, a_{21}, a_{31}, a_{41}\}$ によって定まる sextet を $S_0 = \{T_i\}_{1 \le i \le 6}$ とする. T_1 が M-行列の第 1 列なので $\mathbf{M}(ij)$ が octad になることから各列が sextet の成分になる.

($\mathbf{S_1}$) $T_1 = \{a_{11}, a_{22}, a_{32}, a_{42}\}$ によって定まる sextet を $S_1 = \{T_i\}_{1 \le i \le 6}$ とする. $T_1 \subseteq \mathbf{M}(12)$ より $T_2 = \{a_{12}, a_{21}, a_{31}, a_{41}\}$, $T_2 \subseteq \mathbf{M}(1)$ より $T_3 = \{a_{13}, a_{14}, a_{15}, a_{16}\}$ が定まる. ここで T_3 を含む octad $\mathbf{M}(5)$, $\mathbf{M}(6)$, $\mathbf{M}(7)$ から $T_{i+2} = \{a_{i3}, a_{i4}, a_{i5}, a_{i6}\}$ $(2 \le i \le 4)$ が得られる.

(**S_2**) $T_1 = \{a_{11}, a_{12}, a_{21}, a_{22}\}$ によって定まる sextet を S_2 とする. $\mathbf{M}(12), \mathbf{M}(2)$ が T_1 を含む octad であることから $T_2 = \{a_{31}, a_{32}, a_{41}, a_{42}\}$, $T_3 = \{a_{13}, a_{14}, a_{23}, a_{24}\}$ が定まる. $\mathbf{M}(34)$, $\mathbf{M}(5)$ が T_3 を含む octad であることから $T_4 = \{a_{33}, a_{34}, a_{43}, a_{44}\}$, $T_5 = \{a_{15}, a_{16}, a_{25}, a_{26}\}$ が得られる. 従って残りの $T_6 = \{a_{35}, a_{36}, a_{45}, a_{46}\}$ も定まる.

(**S_3**) $T_1 = \{a_{11}, a_{12}, a_{31}, a_{32}\}$ によって定まる sextet を S_3 とする. $\mathbf{M}(12)$, $\mathbf{M}(3)$ が T_1 を含む octad であることから $T_2 = \{a_{21}, a_{22}, a_{41}, a_{42}\}$, $T_3 = \{a_{13}, a_{14}, a_{33}, a_{34}\}$ が定まる. $\mathbf{M}(34)$, $\mathbf{M}(6)$ が T_3 を含む octad であることから $T_4 = \{a_{23}, a_{24}, a_{43}, a_{44}\}$, $T_5 = \{a_{15}, a_{16}, a_{35}, a_{36}\}$ が定まり, 残りの $T_6 = \{a_{25}, a_{26}, a_{45}, a_{46}\}$ も定まる.

(**S_4**) $T_1 = \{a_{11}, a_{12}, a_{31}, a_{41}\}$ で定まる sextet を S_4 とする. $\mathbf{M}(12)$, $\mathbf{M}(8)$ が T_1 を含む octad であることから $T_2 = \{a_{21}, a_{22}, a_{32}, a_{42}\}$, $T_3 = \{a_{13}, a_{24}, a_{35}, a_{46}\}$ が定まる. $\mathbf{M}(8) + S_2(3,6)$, $\mathbf{M}(8) + (\mathbf{M}(35) + S_3(4,6))$ が T_1 を含む octad であるから $T_4 = \{a_{14}, a_{23}, a_{36}, a_{45}\}$, $T_5 = \{a_{15}, a_{26}, a_{33}, a_{44}\}$ が定まり, 残りの $T_6 = \{a_{16}, a_{25}, a_{34}, a_{43}\}$ も定まる.

(**S_5**) 最後に sextet S_5 を $T_1 = \{a_{11}, a_{12}, a_{21}, a_{31}\}$ で定まるものとする. $\mathbf{M}(12)$ が T_1 を含む octad であることから $T_2 = \{a_{22}, a_{32}, a_{41}, a_{42}\}$ が定まる. $D = C(a_{11}, a_{12}, a_{13}, a_{21}, a_{31})$ とすると $|\mathbf{M}(12) \cap D| = 4$ である. 従って S_0 との交わりは $[3^1 1^5]$ 型となる. 更に $\mathbf{M}(1)$, $\mathbf{M}(2)$, $\mathbf{M}(3)$, $\mathbf{M}(8)$ と D との交わりが 4 点になるので 4 列の D の元は a_{44} である. $\mathbf{M}(5), \mathbf{M}(6)$ と D の交わりが 2 点になることから第 5, 6 列の元は a_{25}, a_{36} である. 従って $T_3 = \{a_{13}, a_{25}, a_{36}, a_{44}\}$ を得る. また $D + ((\mathbf{M}(5) + \mathbf{M}(6)) + \mathbf{M}(34)), D + (\mathbf{M}(5) + \mathbf{M}(46))$ が T_1 を含む octad であるから $T_4 = \{a_{14}, a_{26}, a_{35}, a_{43}\}$, $T_5 = \{a_{15}, a_{23}, a_{34}, a_{46}\}$ が定まり, 残りの $T_6 = \{a_{16}, a_{24}, a_{33}, a_{45}\}$ も定まる.

さて M-行列が与えられたとき, $1 \leq i \leq 3$ に対して $2i-1, 2i$ 列の和集合としてできる octad を第 i Brick ということにする. ここで 3 次の置換 σ の $\mathbf{M}$ への作用を定義する. σ は brick 内での位置は変えず 3 個の Brick を置き換えるものとする. 例えば $\sigma = (1,2)$ は $\mathbf{M}(1) = \{a_{12}, a_{13}, a_{14}, a_{15}a_{16}, a_{21}, a_{31}, a_{41}\}$ に対して, 第 3 Brick の元 a_{15}, a_{16} を固定し, 第 1 Brick にある元 $a_{12}, a_{21}, a_{31}, a_{41}$ を第 2 Brick での同じ位置に, すなわち $a_{14}, a_{23}, a_{33}, a_{43}$ の位置に移す. また第 2 Brick にある元 a_{13}, a_{14} を第 1 Brick の同じ位置, すなわち a_{11}, a_{12} の位置に移す. 従って $\mathbf{M}(1)^\sigma = \{a_{11}, a_{12}, a_{23}, a_{33}, a_{43}, a_{14}, a_{15}a_{16}\}$ が得られる. なお $\mathbf{M}(ij)^\sigma$ が octad であることは明らかである.

定理 2.20 (M-行列の対称性) *M-*行列 $\mathbf{M}$ に 3 次の置換 σ を上で定めたように作用させるとする. このとき $\mathbf{M}(i)^\sigma$ は *octad*である $(1 \leq i \leq 8)$. 特に *M-*行列の *Brick*を置換しても *M-*行列である.

Proof　$\mathbf{M}(1)^\sigma$ は $\mathbf{M}(1)$, $X(3)$, $X(5)$ のいずれかであるので octad である. ただし $X(i)$ については補題 2.16 を参照されたい.　$\mathbf{M}(2)^\sigma$, $\mathbf{M}(5)^\sigma$ は sextet S_2 の成分の和となるので octad である. $\mathbf{M}(3)^\sigma$, $\mathbf{M}(6)^\sigma$ は sextet S_3 の成分の和となるので octad である. $\mathbf{M}(4) = \mathbf{M}(2) + \mathbf{M}(3) + \mathbf{M}(12) + \mathbf{M}(34)$ より

$$\mathbf{M}(4)^\sigma = \mathbf{M}(2)^\sigma + \mathbf{M}(3)^\sigma + \mathbf{M}(12)^\sigma + \mathbf{M}(34)^\sigma$$

となるが, 補題 2.13 より $\mathbf{M}(4)^\sigma$ も octad である. 同様に $\mathbf{M}(7) = \mathbf{M}(5) + \mathbf{M}(6) + \mathbf{M}(34) + \mathbf{M}(56)$ より $\mathbf{M}(7)^\sigma$ も octad である.　$\mathbf{M}(8)^\sigma$ は σ に応じて $\mathbf{M}(8)$ に $\mathbf{M}(13) + \mathbf{M}(2)$,$\mathbf{M}(7)$, $\mathbf{M}(15) + S_2(1,5)$, $S_3(2,4) + \mathbf{M}(2)$,　$\mathbf{M}(35) + S_2(3,5)$ を加えることによって得られる. 従って前と同様に $\mathbf{M}(8)^\sigma$ も octad である. ∎

S(5,8,24) と Binary Goley Code

次に $(\Omega, \mathbb{B})$ が S(5,8,24) であるとき $P(\Omega)$ の部分空間 $\langle \mathbb{B} \rangle$ が Binary Goley Code であることを示す.

補題 2.21　$A, B \in \mathbb{B}$ が $A \cap B = \emptyset$ をみたすとき $\Omega - (A \cup B) \in \mathbb{B}$ である.

Proof　$\Omega - (A \cup B) \notin \mathbb{B}$ と仮定して矛盾を導く.　$\Omega - (A \cup B) = \{u_1, u_2, \ldots, u_8\}$ とおく.　$C = C(u_1, u_2, u_3, u_4, u_5)$ とすると仮定より $C \neq \Omega - (A \cup B)$ であるから C は A または B と交わる.　B と交わる場合も同様であるから, 以下 $C \cap A \neq \emptyset$ とする. このとき $1 \leq |C \cap A| \leq 3$ より $|C \cap A| = 2$ が成り立つ. 従って $0 \leq |C \cap B| \leq 1$ より $|C \cap B| = 0$ を得る. ここで $u_1, u_2, \ldots, u_6 \in C$, $u_7, u_8 \notin C$ とする.

次に $D = C(u_1, u_2, u_3, u_4, u_7)$ とおく.　$|C \cap D| = 4$ となるので $u_5, u_6 \notin D$ である.　C と同様に $|D \cap (\Omega - (A \cup B))| = 6$ が得られるので $u_8 \in D$ が成り立つ. 更に $E = C(u_1, u_2, u_3, u_5, u_7)$ とおく. このときも $|E \cap (\Omega - (A \cup B))| = 6$ が得られることから u_4, u_6, u_8 のいずれかは E に含まれる. ここで $u_4 \in E$ または $u_6 \in E$ とすると $E = C$ となり矛盾が生じる. また $u_8 \in E$ の場合も $E = D$ となり, 矛盾が生じる. 以上で $\Omega - (A \cup B) \in \mathbb{B}$ が示された. ∎

定理 2.22　任意の $A \in \mathbb{B}$ に対して $\Omega - A = B + C$ となる $B, C \in \mathbb{B}$ が存在する.

Proof　表 2.1 より $A \cap B = \emptyset$ をみたす $B \in \mathbb{B}$ が存在する. 補題 2.21 より $C = \Omega - (A \cup B) \in \mathbb{B}$ が成り立つ. これより $\Omega - A = B + C$ が得られる. ∎

上の定理の B, C が $B \cap C = \emptyset$ をみたすことを注意しておく.

octad A, B が $|A \cap B| = 2$ をみたすとき $A + B$ を dodecad という.

補題 2.23 *dodecad は octad を含まない.*

Proof　A, B, C を octad, $A + B$ を dodecad とし, $A + B \supseteq C$ と仮定する. $A \cap B$ は 2 点集合であり, $A \cap B \not\subseteq C$ が成り立つので $C \neq A, B$ である. 従って $|C \cap A|$, $|C \cap B|$ はともに 4 以下である. 仮定よりこれらの和は 8 となるので $|C \cap A| = |C \cap B| = 4$ が成り立つ. このとき補題2.13 より $C + A$, $C + B$ は octad である. 一方

$$A = \{a_1, a_2, a_3, a_4, a_5, a_6, c_1, c_2\}, \qquad B = \{b_1, b_2, b_3, b_4, b_5, b_6, c_1, c_2\}$$

とおき $C = \{a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4\}$ とすると $C + A = \{a_5, a_6, c_1, c_2, b_1, b_2, b_3, b_4\}$ より $|B \cap (C + A)| = 6$ となり, 矛盾が生じる. ∎

補題 2.24 *A, B が octad で $A + B$ が dodecad であるとき $\Omega - (A + B)$ も dodecad である.*

Proof

$$A = \{a_1, a_2, a_3, a_4, a_5, a_6, c_1, c_2\}, \qquad B = \{b_1, b_2, b_3, b_4, b_5, b_6, c_1, c_2\}$$

とおく. $A_1 = \{a_1, a_2, a_3, a_4\}$ によって定まる sextet を $S = \{A_i\}_{1 \leq i \leq 6}$ とおく. ここで $A_2 = \{a_5, a_6, c_1, c_2\}$ としてよいから $|A_1 \cap B| = 0$, $|A_2 \cap B| = 2$ より S と B の交わりは $[2^4 0^2]$ 型である. 従って $|A_i \cap B| = 2$ となる $i \geq 3$ が 3 個存在する. 従って

$$A_3 = \{d_1, d_2, d_3, d_4\},\ A_4 = \{b_1, b_2, b_1', b_2'\},\ A_5 = \{b_3, b_4, b_3', b_4'\},\ A_6 = \{b_5, b_6, b_5', b_6'\}$$

とおくことができる. このとき

$$C = B + (A_5 \cup A_6) = \{b_1, b_2, c_1, c_2, b_3', b_4', b_5', b_6'\}$$

は octad であり,

$$D = C + (A_2 \cup A_4) = \{a_5, a_6, b_1', b_2', b_3', b_4', b_5', b_6'\}$$

も octad になる. 従って

$$D + (A_2 \cup A_3) = \{c_1, c_2, d_1, d_2, d_3, d_4, b_1', b_2', b_3', b_4', b_5', b_6'\} = \Omega - (A + B)$$

が成り立つことから $\Omega - (A + B)$ は dodecad である. ∎

定理 2.25 $\langle \mathbb{B} \rangle = \{\Omega\} \cup \{\emptyset\} \cup \{X | X \text{ は } octad\} \cup \{\Omega - X | X \text{ は } octad\} \cup \{Y | Y \text{ は } dodecad\}$ である.

Proof

$$G = \{\Omega\} \cup \{\emptyset\} \cup \{X | X \text{ は octad}\} \cup \{\Omega - X | X \text{ は octad}\} \cup \{Y | Y \text{ は dodecad}\}$$

とおく. 補題 2.24 より dodecad の補集合は dodecad であるから, G の任意の元 X に対して X の補集合 $\Omega - X$ が G に含まれることを注意しておく. 以下 $G = \langle \mathbb{B} \rangle$ を示す.

まず $G \subseteq \langle \mathbb{B} \rangle$ を示す. octad A に対して $A + A = \emptyset$ となるから $\emptyset \in \langle \mathbb{B} \rangle$ である. また定理 2.22 より $\Omega - A = B + C$ をみたす octad B, C が存在することから, octad の補集合, および $\Omega = A + B + C$ は $\langle \mathbb{B} \rangle$ に含まれる. 定義により dodecad は 2 つの octad の和であるから $\langle \mathbb{B} \rangle$ に含まれる. 以上で $G \subseteq \langle \mathbb{B} \rangle$ が示された.

次に $\langle \mathbb{B} \rangle \subseteq G$ を示す. そのためには G が $P(\Omega)$ の部分加群であることを示せばよい. なぜならば $\langle \mathbb{B} \rangle$ は $\mathbb{B}$ を含む最小の部分加群であるが, G も $\mathbb{B}$ を含む部分加群となり $\langle \mathbb{B} \rangle \subseteq G$ が導かれるからである. G が $P(\Omega)$ の部分加群であることを示すためには $-X = X \in G$ に注意すれば, 任意の $X, Y \in G$ に対して $X + Y \in G$ が成り立つことを示せばよい. 任意の $X, Y \in G$ に対して $X + Y \in G$ が成り立つことを示すためには, 任意の $X \in G$ と任意の octad A に対して $X + A \in G$ を示せばよい. なぜならば, このとき任意の $X, Y \in G$ に対して $Y = A_1 + \cdots + A_s$ と octad の和に表せば

$$X \in G \Rightarrow X + A_1 \in G \Rightarrow (X + A_1) + A_2 \in G \Rightarrow (X + A_1 + A_2) + A_3 \in G \Rightarrow \cdots$$

より $X + A_1 + \cdots + A_s = X + Y \in G$ が導かれるからである. 以下, 任意の $X \in G$ と任意の octad A に対して $X + A \in G$ を示すことにする.

$X = \emptyset$ または $X = \Omega$ のとき $X + A \in G$ は明らかに成り立つ. また X が octad のときは $|X \cap A| = 0, 2, 4, 8$ であることに従って, $X + A$ は octad の補集合, dodecad, octad, $\emptyset$ になるので $X + A \in G$ が成り立つ.

X が octad の補集合であるときは $X = \Omega + B$ となる octad B が存在し, $X + A = \Omega + A + B$ となるが, $A + B \in G$ であるからその補集合 $\Omega + A + B$ も G に含まれる. 従って $X + A \in G$ が成り立つ.

最後に X が dodecad であるとする. このとき $X = B + C$ となる octad B, C が存在する. また補題 2.24 より $\Omega + X = D + E$ となる octad D, E が存在する. $|A \cap B| = 0, 2, 4, 8$ であるが $|A \cap B| = 8$ のときは $A = B$ となり $X + A = C \in G$ が成り立つ. $|A \cap B| = 4$

のときは $A+B$ が octad となるから $X+A=(A+B)+C\in G$ が成り立つ. $|A\cap B|=0$ のときは $A+B$ が octad の補集合となるから $A+B=\Omega+F$ となる octad F が存在し, このとき $X+A=(A+B)+C=\Omega+F+C\in G$ が成り立つ. 従って $|A\cap B|=2$ であるとしてよい. 同様にして $|A\cap C|=2$ であるとしてよい. また $X=\Omega+D+E$ より $|A\cap D|=|A\cap E|=2$ であるとしてよい. ここで $A\cap B=\{a_1,a_2\}$ とおく. 今 $a_1\in B\cap C$ とすると $|A\cap(B+C)|<4$ より $|A\cap D|=|A\cap E|=2$ であったことに矛盾する. よって $a_1\notin C$ である. 同様にして $a_2\notin C$ が得られる. また

$$A\cap D=\{a_3,a_4\},\quad A\cap C=\{a_5,a_6\},\quad A\cap E=\{a_7,a_8\}$$

とおくと, 同様にして

$$a_3,a_4\notin E,\quad a_5,a_6\notin B,\quad a_7,a_8\notin D$$

が得られる. 特にこれらの a_i は互いに異なる. さて $T_1=\{a_1,a_2,a_3,a_4\}$ で定まる sextet を $\{T_i\}_{1\le i\le 6}$ とする. $T_2=\{a_5,a_6,a_7,a_8\}$ としてよい. ここで $|A\cap B|=2$ より $T_1\cap B=\{a_1,a_2\}$ が得られることから B と $\{T_i\}$ の交わりは $[2^40^2]$ 型である. 同様に C と $\{T_i\}$ との交わりも $[2^40^2]$ 型である. sextet は 6 個であるから, ある T_k は $|T_k\cap B|=|T_k\cap C|=2$ をみたす. このとき $A=T_1+T_2=T_1+T_k+T_k+T_2$, $|B\cap(T_1+T_k)|=4$, $|C\cap(T_2+T_k)|=4$ となるので $B+T_1+T_k$, $C+T_2+T_k$ は octad である. よって

$$X+A=B+C+A=B+C+T_1+T_k+T_k+T_2=(B+T_1+T_k)+(C+T_k+T_2)\in G$$

が成り立つ. ∎

$\langle\mathbb{B}\rangle$ は $P(\Omega)$ の部分空間で定理 2.25 より $\langle\mathbb{B}\rangle\ni X$, $X\neq\emptyset$ のとき $|X|\ge 8$ をみたし, 補題 2.11 より $|\mathbb{B}|=759$ が成り立つ. 従って $\langle\mathbb{B}\rangle$ は Binary Goley Code で, $\mathbb{B}$ はその 8 点集合全体のなす集合に一致する. 逆に Binary Goley Code Γ が与えられたとき §2.1 で示したように, その 8 点集合全体のなす集合を $\mathbb{B}$ とすると $(\Omega,\mathbb{B})$ は S(5,8,24) である. このとき系 2.2 より $\Gamma=\langle\mathbb{B}\rangle$ が成り立つ.

すなわち S(5,8,24) から Binary Golay Code が得られ, その Binary Golay Code から元の S(5,8,24) が復元される. 逆に Binary Golay Code から S(5,8,24) が得られ, その S(5,8,24) から元の Binary Golay Code が復元される.

以下 $\Gamma=\langle\mathbb{B}\rangle$, すべての dodecad の集合を $\mathbb{D}$ とおく. $\dim\Gamma=12$ より

$$|\mathbb{D}|=2^{12}-(2+759+759)=2576$$

が成り立つ.

系 2.26 $\Gamma = \langle \mathbb{D} \rangle$ である.

Proof　$\mathbb{D} \subseteq \Gamma$ であることから $\langle \mathbb{D} \rangle \subseteq \Gamma$ が得られる. 従って $\Gamma \subseteq \langle \mathbb{D} \rangle$ を示せばよいが $\Gamma = \langle \mathbb{B} \rangle$ より $\mathbb{B} \subseteq \langle \mathbb{D} \rangle$ を示せばよい.

任意に $C \in \mathbb{B}$ を選び $C \in \langle \mathbb{D} \rangle$ を示そう.

$$\mathbb{D} = \{D_1, D_2, \ldots\ldots, D_{2576}\}$$

とする. ここで

$$\mathbb{D}' = \{D_1 + C, D_2 + C, \ldots\ldots, D_{2576} + C\}$$

とおくと, $\mathbb{D}' \subseteq \Gamma$ かつ $|\mathbb{D}| = |\mathbb{D}'| = 2576$ が成り立つ. 一方 $|\Gamma| = 2^{12} = 4096 < 2 \cdot 2576$ であることから $\mathbb{D} \cap \mathbb{D}' \neq \emptyset$ である. 従って $D \in \mathbb{D} \cap \mathbb{D}'$ に対して $D = C + D'$ をみたす dodecad D' が存在する. このとき $C = D + D'$ であるから $C \in \langle \mathbb{D} \rangle$ が得られる. よって $\mathbb{B} \subseteq \langle \mathbb{D} \rangle$ が成り立つ. ∎

定理 2.27 (Binary Goley Code の自己共役性) Γ を Ω 上の *Binary Goley Code,* $\mathbb{B}$ を *octad* の集合とする. $X \in P(\Omega)$ に対して, 次は同値である.

(1)　$X \in \Gamma$ である.

(2)　任意の $C \in \mathbb{B}$ に対して $|X \cap C| \equiv 0 \pmod 2$ が成り立つ.

Proof　$X \in \Gamma$ とする. このとき任意の $C \in \mathbb{B}$ に対して $X + C \in \Gamma$ であるから $|X|$, $|C|$, $|X + C|$ は 4 の倍数である. 従って定理 1.28 より $|X \cap C|$ は偶数である.

逆に $X \in P(\Omega)$ が, 任意の $C \in \mathbb{B}$ に対して $|X \cap C| \equiv 0 \pmod 2$ をみたすとする. ここで $1 \leq |X| \leq 7$ と仮定すると表 2.1(p.30) より $|X \cap C| \equiv 1 \pmod 2$ となる octad C が存在することになり矛盾が生じる. よって $|X| \leq 7$ ならば $X = \emptyset \in \Gamma$ が成り立つ.

次に $|X| = n \geq 8$ とする. このとき $|X \cap C_1| \geq 5$ となる octad C_1 を選ぶと

$$|X + C_1| = |X| + |C_1| - 2|X \cap C_1| \leq n - 2$$

を得る. 定理 1.29 より任意の $C \in \mathbb{B}$ に対して $|(X + C_1) \cap C| \equiv 0 \pmod 2$ をみたすことに注意されたい. ここで $|X + C_1| \geq 8$ であれば, $|(X + C_1) \cap C_2| \geq 5$ となる octad C_2 を

選ぶと

$$|X + C_1 + C_2| = |X + C_1| + |C_2| - 2|(X + C_1) \cap C_2| \leq n - 4$$

を得る. 同様にして octad C_i を適当に選べば

$$\left| X + \sum_{i=1}^{k} C_i \right| \leq 7$$

とできる. また $X + \sum_{i=1}^{k} C_i$ が定理の条件 (2) をみたすので, 前述の結果より

$$X + \sum_{i=1}^{k} C_i = \emptyset \quad \Longrightarrow \quad X = \sum_{i=1}^{k} C_i \in \Gamma$$

が得られる. ∎

2.3 S(5,8,24) の一意性

この節では Steiner system S(5,8,24) が唯一つであること, すなわち S(5,8,24) はすべて同型であることを示す. ここで Steiner system $(\Omega, \mathbb{B})$ と $(\Omega', \mathbb{B}')$ が同型であるとは, 同型写像, すなわち全単射 $\sigma : \Omega \to \Omega'$ で $\mathbb{B}^\sigma = \mathbb{B}'$ となるものが存在するときにいう. ただし

$$\mathbb{B}^\sigma = \{\, B^\sigma \mid B \in \mathbb{B} \,\}$$

である. 以下, 任意の Steiner system S(5,8,24), $(\Omega, \mathbb{B})$ と $(\Omega', \mathbb{B}')$ が同型であることを示す.

定理 2.18 より $(\Omega, \mathbb{B})$, $(\Omega', \mathbb{B}')$ から M-行列 **M**, **M**' が得られる.

$$\mathbf{M} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & a_{26} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & a_{36} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} & a_{46} \end{bmatrix}, \quad \mathbf{M}' = \begin{bmatrix} a'_{11} & a'_{12} & a'_{13} & a'_{14} & a'_{15} & a'_{16} \\ a'_{21} & a'_{22} & a'_{23} & a'_{24} & a'_{25} & a'_{26} \\ a'_{31} & a'_{32} & a'_{33} & a'_{34} & a'_{35} & a'_{36} \\ a'_{41} & a'_{42} & a'_{43} & a'_{44} & a'_{45} & a'_{46} \end{bmatrix}$$

$(\Omega, \mathbb{B})$ と $(\Omega', \mathbb{B}')$ が同型であることを示すには, 写像 $\sigma : \Omega \ni a_{ij} \longmapsto a'_{ij} \in \Omega'$ が $\mathbb{B}^\sigma = \mathbb{B}'$ をみたすことを示せばよい.

M の第 1 Brick を Ω_8 とおく.

$$\Omega_8 = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \\ a_{41} & a_{42} \end{bmatrix}$$

である. また Ω_8 の偶数個の元からなる部分集合全体を $P_0(\Omega_8)$ とし,

$$X_0 = \{a_{12}, a_{22}, a_{32}, a_{42}\}, \quad X_1 = \{a_{21}, a_{31}, a_{41}, a_{12}\}, \quad X_2 = \{a_{31}, a_{41}, a_{32}, a_{42}\}$$

$$X_3 = \{a_{21}, a_{41}, a_{22}, a_{42}\}, \quad X_4 = \{a_{21}, a_{22}, a_{32}, a_{42}\}, \quad X_5 = \{a_{41}, a_{22}, a_{32}, a_{42}\}$$

とする (付録 p.94).

補題 2.28 $\Delta = \{\Omega_8, X_0, X_1, \ldots, X_5\}$ は $P_0(\Omega_8)$ の基底をなす.

Proof　$P_0(\Omega_8)$ は 7 次元であるから, Δ が 1 次独立であることを示せばよい.

$$c\,\Omega_8 + c_0\,X_0 + c_1\,X_1 + c_2\,X_2 + c_3\,X_3 + c_4\,X_4 + +c_5\,X_5 = \emptyset$$

と仮定する. このとき a_{11} を含むのは Ω_8 のみであるから $c = 0$ である. 同様に a_{ij} の係数を計算すると

$$c_0 + c_1 = 0,\ \ c_1 + c_3 + c_4 = 0,\ \ c_0 + c_3 + c_4 + c_5 = 0,\ \ c_1 + c_2 = 0,\ \ c_0 + c_2 + c_4 + c_5 = 0$$

$$c_1 + c_2 + c_3 + c_5 = 0, \qquad c_0 + c_2 + c_3 + c_4 + c_5 = 0$$

が得られる. これより $c_0 = c_1 = c_2 = c_3 = c_4 = c_5 = 0$ を得る. ∎

以下 $\Delta = \{\Omega_8, X_0, X_1, \ldots, X_5\}$ とおく. p.37で示したように, M-行列 $\mathbf{M}$ に対して S_i は sextet をなす (付録 p.94). $\mathbf{M}$' に対しても S_i に対応する分割 S_i' は sextet をなす. 一方 $X_i \in \Delta$ は $(\Omega, \mathbb{B})$ の sextet S_i の成分である (付録 p.94). 従って $X_i^\sigma \in \Delta^\sigma$ は $(\Omega', \mathbb{B}')$ の sextet の成分である. これより次の補題を得る.

補題 2.29 $C \cap \Omega_8 \in \Delta$ をみたす $C \in \mathbb{B}$ について $C^\sigma \in \mathbb{B}'$ が成り立つ.

以下

$$\Omega_8^* = \{\, S \subseteq \Omega_8 \mid C \cap \Omega_8 = S \text{ となる } C \in \mathbb{B} \text{ は } C^\sigma \in \mathbb{B}' \text{ をみたす} \,\}$$

とおく. 上の補題より $\Delta \subseteq \Omega_8^*$ が成り立つ. また $S \in \Omega_8^*$, $|S| = 4$ ならば $S + \Omega_8 \in \Omega_8^*$ が成り立つことを注意しておく.

補題 2.30 $C \in \mathbb{B}$ が次の条件をみたすとする.

- $|C \cap \Omega_8| = 2$ または 4
- $|D_1| = 4$, $|D_2| = 2$ または 4, である $D_1, D_2 \in \Omega_8^*$ で $C \cap \Omega_8 = D_1 + D_2$ をみたすものが存在する.

このとき $C_i \cap \Omega_8 = D_i$ $(i = 1, 2)$ かつ $C = C_1 + C_2$ となる $C_1, C_2 \in \mathbb{B}$ が存在する. 特に $C^\sigma \in \mathbb{B}'$ が成り立つ.

Proof $C = \{a_1, a_2, \ldots, a_8\}$, $C' = C \cap \Omega_8$ とおく. また D_1 を成分とする sextet を $\{P_i\}_{1 \le i \le 6}$ とおく. ただし $P_1 = D_1$ とする. ここで Ω_8 が octad なので $P_2 = \Omega_8 - P_1$ としてよい. 以下 C', D_2 の元の個数によって場合分けし, 補題の結論をみたす $C_1, C_2 \in \mathbb{B}$ が存在することを示す.

$|C'| = |D_2| = 4$ の場合. $D_1 = \{a_1, a_2, b_1, b_2\}$, $D_2 = \{a_3, a_4, b_1, b_2\}$ とおくことができる. $\{P_i\}$ と C との交わりは $[2^4 0^2]$ 型であるから $|P_3 \cap C| = 2$ としてよい. このとき $C_1 = P_1 + P_3$ は octad であり, $|C \cap C_1| = 4$ より $C_2 = C + C_1$ も octad である. また $C_2 \cap \Omega_8 = D_2$ となるので C_1, C_2 が求める octad である.

$|C'| = 4$, $|D_2| = 2$ の場合. $D_1 = \{a_1, a_2, a_3, b_1\}$, $D_2 = \{a_4, b_1\}$ とおくことができる. $\{P_i\}$ と C との交わりは $[3^1 1^5]$ 型である. このとき $C_1 = P_1 + P_3$, $C_2 = C + C_1$ とすると $|C \cap C_1| = 4$ より C_2 は octad で $C_2 \cap \Omega_8 = D_2$ をみたす. 従って C_1, C_2 が求める octad である.

$|C'| = 2$, $|D_2| = 4$ の場合. $D_1 = \{a_1, b_1, b_2, b_3\}$, $D_2 = \{a_2, b_1, b_2, b_3\}$ とおくことができる. $\{P_i\}$ と C との交わりは $[3^1 1^5]$ 型であるから $|P_3 \cap C| = 3$ としてよい. このとき $C_1 = P_1 + P_3$, $C_2 = C + C_1$ とすると $|C \cap C_1| = 4$ より C_2 は octad で $C_2 \cap \Omega_8 = D_2$ をみたす. 従って C_1, C_2 が求める octad である.

$|C'| = |D_2| = 2$ の場合. $D_1 = \{a_1, a_2, b_1, b_2\}$, $D_2 = \{b_1, b_2\}$ とおくことができる. $\{P_i\}$ と C との交わりは $[2^4 0^2]$ 型であるから $|P_3 \cap C| = 2$ としてよい. このとき $C_1 = P_1 + P_3$, $C_2 = C + C_1$ とすると $|C \cap C_1| = 4$ より C_2 は octad で $C_2 \cap \Omega_8 = D_2$ をみたす. 従って C_1, C_2 が求める octad である.

以上で $C_i \cap \Omega_8 = D_i$ $(i = 1, 2)$ かつ $C = C_1 + C_2$ となる $C_1, C_2 \in \mathbb{B}$ の存在が示された. ここで $D_i \in \Omega_8^*$ より $C_i^\sigma \in \mathbb{B}'$ が成り立つ. 一方

$$C^\sigma = (C_1 + C_2)^\sigma = C_1^\sigma + C_2^\sigma$$

より $C^\sigma \in \mathbb{B}'$ が得られる. ∎

定理 2.31 $C \in \mathbb{B}$ ならば $C^\sigma \in \mathbb{B}'$ である.

Proof $C = \mathbf{M}(ij)$ のときは明らかに $C^\sigma \in \mathbb{B}'$ であるから, 以下 $C \neq \mathbf{M}(ij)$ と仮定する. 定理2.20 より $\mathbf{M}$ の Brick を置換しても $(\Omega.\mathbb{B})$ の M-行列であるから $C \cap \Omega_8 \neq \emptyset$ と仮定してよい. 以下 $C' = C \cap \Omega_8$ とおく. $C \neq \mathbf{M}(ij)$ より $|C'| = 2$ または 4 である. 従って, 補題2.28 より

$$C' = D_1 + D_2 + \cdots + D_r$$

となる $D_i \in \Delta$ が存在する. $r = 1$ のときは 補題2.29 より $C^\sigma \in \mathbb{B}'$ が成り立つ. よって $r \geq 2$ としてよい. またある i について $D_i = \Omega_8$ であれば $j \neq i$ である D_j に対して $D_j + \Omega_8 \in \Omega_8^*$ $|D_j + \Omega_8| = 4$ が成り立つ. このことより

$$C' = D_1 + D_2 + \cdots + D_k\,, \quad D_i \in \Omega_8^*\,, \quad |D_i| = 4$$

と表されることがわかる. 以下 k についての帰納法で $C = C_1 + C_2 + \cdots + C_k$ かつ $C_i \cap \Omega_8 = D_i$ をみたす $C_i \in \mathbb{B}$ が存在することを示す. このとき $C_i^\sigma \in \mathbb{B}'$ より

$$C^\sigma = (C_1 + C_2 + \cdots + C_k)^\sigma = C_1^\sigma + C_2^\sigma + \cdots + C_k^\sigma \in \mathbb{B}'$$

が得られ, 定理が証明される.

$k = 1$ のときは Ω_8^* の定義より $C_1 = C$ とすれば成り立つ. 以下 $k > 1$ とし, k より小さいときには成立すると仮定する. ここで

$$E = D_2 + D_3 + \cdots + D_k$$

とおく. $C' = D_1 + E$ である.

$|E| = 0$ のときは

$$D_2 = D_3 + \cdots + D_k\,, \quad D_i \in \Omega_8^*\,, \quad |D_i| = 4$$

となる. 従って $C_2 \cap \Omega_8 = D_2$ となる任意の $C_2 \in \mathbb{B}$ に対して, 帰納法の仮定より $C_2 = C_3 + \cdots + C_k$ かつ $C_i \cap \Omega_8 = D_i$ をみたす $C_i \in \mathbb{B}$ が存在する. このとき $C_1 = C$ とすれば $C = C_1 + C_2 + \cdots + C_k$ かつ $C_i \cap \Omega_8 = D_i$ が成り立つ.

$|E| = 2$ または 4 とする. このとき $E = C_E \cap \Omega_8$ となる任意の octad C_E に対して, 帰納法の仮定より $C_E = C_2 + \cdots + C_k$ かつ $C_i \cap \Omega_8 = D_i$ をみたす $C_i \in \mathbb{B}$ が存在する. これ

より

$$C_E^\sigma = C_2^\sigma + \cdots + C_k^\sigma$$

が成り立つことから $C_E^\sigma \in \mathbb{B}'$ となる. 従って $E \in \Omega_8^*$ が得られる. $C' = D_1 + E$ であるので補題 2.30 より $C = C_1 + C_0$, $C_1 \cap \Omega_8 = D_1$, $C_0 \cap \Omega_8 = E$ をみたす $C_1, C_0 \in \mathbb{B}$ が存在する. この C_0 に対して, 再び帰納法を適用して

$$C_0 = C_2 + \cdots + C_k\,, \quad C_i \cap \Omega_8 = D_i$$

をみたす $C_i \in \mathbb{B}$ が存在する. このとき $C_1, ..., C_k$ が求める octad である.

最後に $|E| = 6$ または 8 とする. このとき $D_1' = D_1 + \Omega_8$, $D_2' = D_2 + \Omega_8$ とすると $|D_i'| = 4$ かつ $D_i' \in \Omega_8^*$ である. また

$$C' = D_1' + D_2' + D_3 + \cdots + D_k\,, \quad |D_i'| = 4$$

が成り立つ. ここで $|D_2' + \cdots + D_k| = 0$ または 2 となるので, 前と同様にして

$$C = C_1' + C_2' + C_3 + \cdots + C_k\,, \;\; C_1' \cap \Omega_8 = D_1'\,, \;\; C_2' \cap \Omega_8 = D_2'\,, \;\; C_i \cap \Omega_8 = D_i$$

をみたす $C_1', C_2', C_3, \ldots, C_k \in \mathbb{B}$ が存在する. 従って $C_1 = C_1' + \Omega_8$, $C_2 = C_2' + \Omega_8$ とおけば $C_1, C_2, \ldots, C_k$ が求める octad である.

以上で定理が証明された. ∎

定理 2.31 より次の定理が得られる.

定理 2.32 2 つの Steiner system S(5,8,24) を任意に選び $(\Omega, \mathbb{B})$, $(\Omega', \mathbb{B}')$ とする. このとき, これらから得られる M-行列をそれぞれ $\mathbf{M} = [a_{ij}]$, $\mathbf{M}' = [a'_{ij}]$ とすると, 写像 $\sigma : \Omega \ni a_{ij} \longmapsto a'_{ij} \in \Omega'$ は $(\Omega, \mathbb{B})$ から $(\Omega', \mathbb{B}')$ への同型を与える. 特に Steiner system S(5,8,24) はすべて互いに同型である.

3章　Mathieu群

この章では Steiner system S(5,8,24), $(\Omega, \mathbb{O})$ の自己同型群として Mathieu 群を定義し, その単純性および多重可移性を示す. また $(\Omega, \mathbb{O})$ への作用から生じる種々の作用が原始的であることを導く. §3.1 では $(\Omega, \mathbb{O})$ の自己同型群として 24 次の Mathieu 群 M_{24} を定義し, それが M-順列上正則であることを示す. これより M_{24} が Ω 上 5 重可移であることが導かれ, $1, 2, 3$ 点の固定群として M_{23}, M_{22}, M_{21} が得られる. また octad C の固定群 H を C に作用させたときの核を N とするとき H/N が A_8 に同型であること, N が位数 16 の基本アーベル群で C の補集合に正則に作用することを示す. 更に M_{24} の位数 2 の元の Ω 上の置換の型が $1^8 2^8$ または 2^{12} のいずれかになること, $1^8 2^8$ 型の元がすべて共役であることを示す. §3.2 では M_{24} の $\mathbb{O}$ への作用が原始的であることを示す. これより M_{23}, M_{22}, M_{21} の $\mathbb{O}$ の部分集合への原始的な作用が導かれる. またそれらの作用の 1 点の固定群の構造を明らかにし, M_{21}, M_{22}, M_{23} において位数 2 の元が互いに共役であることを導く. 最後に, これらの結果と 鈴木の判定法により, Mathieu 群 M_{22}, M_{23}, M_{24} の単純性を導く.

3.1　Mathieu 群 $\mathbf{M_{24}}$

以下, この章を通じて $(\Omega, \mathbb{O})$ は Steiner system S(5,8,24) を表すものとする.

定義 3.1 24 次の *Mathieu* 群 M_{24} を次のように定める.

$$M_{24} = \{\, \sigma \in S_\Omega \mid \mathbb{O}^\sigma = \mathbb{O} \,\}$$

ただし $\mathbb{O}^\sigma = \{B^\sigma \mid B \in \mathbb{O}\}$ である.

M-順列 (p.33) を任意に 2 つ選び

$$(x_1, x_2, x_3, x_4, x_5, x_6, x_7)\,, \quad (y_1, y_2, y_3, y_4, y_5, y_6, y_7)$$

とする. これらに対して定理 2.19 より 2 つの M-行列 $\mathbf{M}$, $\mathbf{M}$' が定まる.

$$\mathbf{M} = \begin{bmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_7 & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \end{bmatrix}, \quad \mathbf{M}' = \begin{bmatrix} y_1 & y_2 & y_3 & y_4 & y_5 & y_6 \\ y_7 & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \end{bmatrix}$$

このとき定理 2.32 より $\mathbf{M}$ の (i,j) 成分を $\mathbf{M}$' の (i,j) 成分に移す写像は $(\Omega, \mathbb{O})$ から $(\Omega, \mathbb{O})$ への同型 (自己同型) となる. この自己同型を σ とすると, 定義より $\sigma \in M_{24}$ である. 従って M_{24} は M-順列全体のなす集合の上に可移に作用する. 一方, 定理 2.19 より M-行列は M-順列から一意に定まることから, 1 つの M-順列を固定する $(\Omega, \mathbb{O})$ の自己同型は恒等変換に限る. すなわち M_{24} は M-順列全体のなす集合の上に正則 (p.9) に作用する. 特に M_{24} の位数は M-順列の個数に等しい.

一方 Ω の任意の 5 点順列 $(x_1, x_2, \ldots, x_5)$ に対して $C = C(x_1, x_2, \ldots, x_5)$ とおき, $x_6 \in C$, $x_0 \in \Omega - C$ を選ぶと, M-順列 $(x_0, x_1, \ldots, x_6)$ が得られる. 逆に, 任意の M-順列がこのようにして得られることから, M_{24} の位数はこのような選び方の総数 24·23·22·21·20·3·16 に一致する. 以上より次の定理を得る.

定理 3.2 M_{24} は $(\Omega, \mathbb{O})$ の M-順列全体のなす集合の上に正則に作用する. 特に $|M_{24}| = 244823040 = 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 3 \cdot 16$ である.

任意の 5 点順列を任意の 5 点順列に移す M_{24} の元が存在することから, 次の系が得られる.

系 3.3 M_{24} は Ω 上 5 重可移に, $\mathbb{O}$ 上可移に作用する.

$\mathbf{M_{24}}$ の $\mathbb{O}$ への作用

次に M_{24} の $\mathbb{O}$ への作用を考える. $\mathbb{O} \ni C$ の固定群を $H = H(C)$ とおく.

$$H(C) = \{\, \sigma \in M_{24} \mid C^\sigma = C \,\}$$

である. H は C に作用するが, その核を $N = N(C)$ とおく.

補題 3.4 H は C 上 6 重可移に作用する.

Proof　C から 2 つの 6 点順列 $(x_1, \ldots, x_6)$, $(y_1, \ldots, y_6)$ を任意に選ぶ. このとき $x_0 \in \Omega - C$ に対して $M_1 = (x_0, x_1, \ldots, x_6)$, $M_2 = (x_0, y_1, \ldots, y_6)$ は M-順列である. 従って定理 3.2 よ

り $M_1^\sigma = M_2$ をみたす $\sigma \in M_{24}$ が存在する. ここで

$$(x_1, \ldots, x_6)^\sigma = (y_1, \ldots, y_6)$$

が成り立つので $\sigma \in H$ である. ゆえに H は C 上 6 重可移である. ∎

補題 3.5 H は $\Omega - C$ 上 2 重可移に作用する.

Proof $\Omega - C \ni y_1, y_2$, $C \ni x_1, x_2, x_3$ を任意に選ぶ. $C_1 = C(x_1, x_2, x_3, y_1, y_2)$ とおくと $|C \cap C_1| = 4$ が成り立つ. ここで $C \cap C_1 = \{x_1, x_2, x_3, x_4\}$, $x_0 \in C - C_1$ とすると M-順列 $M_1 = (x_0, x_1, x_2, x_3, x_4, y_1, y_2)$ が得られる. 同様にして任意の $y_1', y_2' \in \Omega - C$ と x_1, x_2, x_3 とから M-順列 $M_2 = (x_0', x_1, x_2, x_3, x_4', y_1', y_2')$ が得られる. 定理 3.2 より $M_1^\sigma = M_2$ をみたす $\sigma \in M_{24}$ が存在する. ここで

$$x_0, x_0', x_1, x_2, x_3, x_4, x_4' \in C$$

であるから $C^\sigma = C$ かつ $(y_1, y_2)^\sigma = (y_1', y_2')$ が成り立つ. よって H は $\Omega - C$ 上 2 重可移である. ∎

H の $\Omega - C$ への作用が, 実際は 3 重可移であることを補題 3.11 で証明する.

補題 3.6 N は $\Omega - C$ 上正則に作用する.

Proof $\sigma \in N$ が $\Omega - C$ の点 y を固定すると仮定する. このとき C の任意の 6 点 x_i $(1 \leq i \leq 6)$ を選んでできる M-順列 $(y, x_1, x_2, x_3, x_4, x_5, x_6)$ は σ によって固定される. 従って $\sigma = 1$ が成り立つ. ゆえに $N \ni \sigma \neq 1$ は $\Omega - C$ に固定点をもたない.

一方, 補題 3.4 より H が C 上 6 重可移であることから H/N の 位数は $\dfrac{8!}{2!}$ の倍数である. 従って H/N の S_8 における指数は 1 または 2 である. 定理 1.19 より A_8 は単純群であるから指数 2 の部分群を持たない. これより H/N は A_8 または S_8 と同型であることがわかる. 一方, 系 3.3 より M_{24} は $\mathbb{O}$ 上可移であるから 定理 1.3 より $|M_{24} : H| = 759$ が成り立つ. 従って

$$|N| = \frac{|M_{24}|}{|M_{24} : H||H : N|} = \begin{cases} 8, & H/N \simeq S_8 \\ 16, & H/N \simeq A_8 \end{cases}$$

が得られる. これより $H/N \simeq A_8$ のとき N は $\Omega - C$ 上可移, 従って正則となる. 以下 N が $\Omega - C$ 上可移でないとして矛盾を導くことにする. このとき $H/N \simeq S_8$, すなわち

$|N| = 8$ であることから $\Omega - C$ は 2 つの N-orbit $\mathcal{O}_1$, $\mathcal{O}_2$ に分割される. $H/N \simeq S_8$ より H には位数 5 の元 α が存在する. $x \in \Omega - C$, $g \in N$ に対して

$$(x^g)^\alpha = x^{g\alpha} = x^{\alpha(\alpha^{-1}g\alpha)}$$

となるので α は x を含む N-orbit を x^α を含む N-orbit に移す. すなわち α は N-orbit の置換を引き起こすが, N-orbit は $\mathcal{O}_1$ と $\mathcal{O}_2$ のみであるから, それらを固定する. 従って α は $\mathcal{O}_1$, $\mathcal{O}_2$ に作用し, それぞれ少なくとも 3 個の固定点をもつ. 固定点から任意に 5 点を選び, それを含む octad を C' とすると α は C' の点をすべて固定する. これは $N(C')$ の位数が 8 であることに矛盾する. よって補題が証明された. ∎

系 3.7 $|N| = 16$ および $H/N \simeq A_8$ である.

定理 3.8 H を $\Omega - C$ へ作用させたときの 1 点の固定群を A とする. このとき $H = NA$, $N \cap A = 1$, $A \simeq A_8$ が成り立つ.

Proof　H における $y \in \Omega - C$ の固定群を A とする. N が $\Omega - C$ に正則に作用することから $A \cap N = 1$ かつ $H = AN$ が成り立つ. ここで $N \lhd H$ に注意して定理 1.11 を適用すると

$$A_8 \simeq H/N \simeq AN/N \simeq A/A \cap N \simeq A$$

が得られる. ∎

$A = H_y$ を上の定理の通りとし, $A < B \leq H$ をみたす部分群 B が存在したと仮定する. B は y を固定しない元 τ を含む. $y^\tau = z$ とおく. H は $\Omega - C$ に 2 重可移に作用するので, 定理 1.2 より A は $\Omega - C - \{y\}$ に可移に作用する. 従って $\Omega - C - \{y\}$ の任意の w に対して $z^\lambda = w$ をみたす $\lambda \in A$ が存在する. このとき $y^{\lambda^{-1}\tau\lambda} = w$ が成り立つ. $\lambda^{-1}\tau\lambda \in B$ より, B は $\Omega - C$ に可移に作用する. 従って $|B : A| = 16 = |H : A|$ となり $H = B$ を得る. すなわち A は H の極大部分群 (p.6) である.

系 3.9　A は H の極大部分群である.

系 3.10 N は位数 2^4 の基本アーベル群である.

Proof　N は位数 16 の 2-群であるから, 定理 1.21 よりべき零群, 従って定理 1.20 より可解群となる. 一方 A が極大部分群であることから N は極小正規部分群である. よって定理 1.22 より N は基本アーベル群である. ∎

補題 3.11 $A_8 \simeq L_4(2)$ である. また H は $\Omega - C$ に 3 重可移に作用する.

Proof　N が位数 2^4 の基本アーベル群なので $\mathbb{F}_2$ 上の 4 次元ベクトル空間とみなすことができる. さて A の 元 λ に対して

$$f_\lambda \ : \ N \ni x \longmapsto x^\lambda \in N$$

と定めると, f_λ は N の自己同型となり, $f_\lambda \in GL(4,2)$ が得られる. ここで写像

$$A \ni \lambda \longmapsto f_\lambda \in GL(4,2)$$

は準同型であり, その核は $\Omega - C$ のすべての点を固定する A の元である. $\Omega - C$ は octad を含むから核は 2-群である. 一方, 定理 1.19 より A は単純群であるから核は 1 となる. 従って A は $GL(4,2)$ の部分群に同型であるが $|A| = |A_8| = |GL(4,2)|$ より $A \simeq A_8 \simeq GL(4,2)$ を得る. ここで $GL(4,2) = L_4(2)$ であることから $A_8 \simeq L_4(2)$ が成り立つ.

また $N - \{1\}$ を $PG(3,2)$ とみなすと定理 1.6 より $A \simeq L_4(2)$ は $N - \{1\}$ に 2 重可移に作用する. A は H の $\Omega - C$ への作用の 1 点の固定群であるから, 定理 1.2 より H は $\Omega - C$ 上 3 重可移である. ∎

補題 3.12 M_{24} の元 $\sigma \neq 1$ が Ω の 6 点 $x_1, x_2, \ldots, x_6$ を固定するとき, 次が成り立つ.

(1)　6 点が *special* ならば σ は $1^8 2^8$ 型の置換で, 固定点の集合は *octad* をなす.

(2)　6 点が *non-special* ならば σ は $1^6 3^6$ 型の置換である.

特に M_{24} の元 $(\neq 1)$ の固定点は高々 8 個である.

Proof　$X = \{x_1, x_2, \ldots, x_6\}$ とおく. X が special のとき $C = C(x_1, x_2, \ldots, x_5)$ とすると $x_6 \in C$ かつ $C^\sigma = C$ が成り立つ. 従って $\sigma \in H = H(C)$ である. 一方, 系 3.7 より σ は C 上偶置換として作用することから $\sigma \in N = N(C)$ が導かれる. 更に系 3.10 より $o(\sigma) = 2$ となり, 補題 3.6 より $\Omega - C$ に固定点をもたないことがわかる. ゆえに σ は $1^8 2^8$ 型であり, 固定点の集合は octad C である.

X が non-special のとき, 補題 2.16 のように各 $1 \leq i \leq 6$ に対して X_i, octad $X(i)$, sextet $\{T_i = (X(i) - X_i) \cup \{x_i\}\}$ を定める. このとき σ が $x_1, x_2, \ldots, x_6$ を固定することから X_i, $X(i)$ を固定する $(1 \leq i \leq 6)$. 従って $T_i^\sigma = T_i$ が成り立つ. 定理 3.2 より σ が $x_1, x_2, \ldots, x_6$ 以外に固定点をもてば $\sigma = 1$ となることから, σ は $1^6 3^6$ 型である. ∎

$\mathbf{M} = [a_{ij}]$ を $(\Omega, \mathbb{O})$ から得られる 1 つの M-行列とする. また $X(i)$ は p.33 の補題 2.16 で, $\mathbf{M}(ij)$, $\mathbf{M}(i)$ は p.34 の定義 2.17 で, $S_k(n,m)$ は p.37 で定めたものとする.

さて

$$(a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}, a_{21}), \quad (a_{12}, a_{11}, a_{13}, a_{14}, a_{15}, a_{16}, a_{22})$$

が M-順列になるので定理 3.2 より

$$(a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}, a_{21})^{\sigma} = (a_{12}, a_{11}, a_{13}, a_{14}, a_{15}, a_{16}, a_{22})$$

となる $\sigma \in M_{24}$ が唯 1 つ存在する. ここで $X(1)^{\sigma} = X(2)$, $X(i)^{\sigma} = X(i)$ $(3 \leq i \leq 6)$, $\mathbf{M}(2)^{\sigma} = \mathbf{M}(2)$ が成り立つことから $(a_{22}, a_{23}, a_{24})^{\sigma} = (a_{21}, a_{23}, a_{24})$ が成り立ち

$$(a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}, a_{21})^{\sigma^2} = (a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}, a_{21})$$

が得られる. よって σ の位数は 2 である. また

$$\{a_{31}, a_{41}\}^{\sigma} = \{a_{32}, a_{42}\}, \ \{a_{32}, a_{42}\}^{\sigma} = \{a_{31}, a_{41}\}, \ \{a_{2i}, a_{3i}, a_{4i}\}^{\sigma} = \{a_{2i}, a_{3i}, a_{4i}\} \ (3 \leq i \leq 6)$$

も導かれる. 一方 $\mathbf{M}(5)^{\sigma} = \mathbf{M}(5)$ となるので $(a_{25}, a_{26})^{\sigma} = (a_{25}, a_{26})$ が成り立つ. 更に定理 3.8 より σ は $X(i)$ 上で偶置換であるから $(a_{3i}, a_{4i})^{\sigma} = (a_{4i}, a_{3i})$ となる $(3 \leq i \leq 6)$. 以上から $\mathbf{M}(3)^{\sigma} = \mathbf{M}(4)$ となり

$$(a_{31}, a_{41}, a_{32}, a_{42})^{\sigma} = (a_{42}, a_{32}, a_{41}, a_{31})$$

を得る. 従って

$$\sigma = (a_{11}, a_{12})(a_{21}, a_{22})(a_{31}, a_{42})(a_{41}, a_{32})(a_{33}, a_{43})(a_{34}, a_{44})(a_{35}, a_{45})(a_{36}, a_{46})$$

が示された. 以下, この置換を $\sigma_2(1)$ とおく. 同様に

$$\begin{aligned}
(a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}, a_{21})^{\sigma_2(2)} &= (a_{11}, a_{13}, a_{12}, a_{14}, a_{15}, a_{16}, a_{21}) \\
(a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}, a_{21})^{\sigma_2(3)} &= (a_{11}, a_{12}, a_{14}, a_{13}, a_{15}, a_{16}, a_{21}) \\
(a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}, a_{21})^{\sigma_2(4)} &= (a_{11}, a_{12}, a_{13}, a_{15}, a_{14}, a_{16}, a_{21}) \\
(a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}, a_{21})^{\sigma_2(5)} &= (a_{11}, a_{12}, a_{13}, a_{14}, a_{16}, a_{15}, a_{21}) \\
(a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}, a_{21})^{\sigma_3(1)} &= (a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}, a_{31})
\end{aligned}$$

をみたす置換がそれぞれ唯 1 つ存在する. これらの置換は

$\sigma_2(2)$ については $\mathbf{M}(1)$, $\mathbf{M}(2)$, $X(4)$, $\mathbf{M}(3)$, $X(2)$, $\mathbf{M}(8)$, $X(5)$, $X(6)$ への作用,

$\sigma_2(3)$ については $\mathbf{M}(1)$, $X(2)$, $\mathbf{M}(2)$, $X(3)$, $\mathbf{M}(3)$, $\mathbf{M}(4)$, $\mathbf{M}(5)$, $X(5)$, $X(6)$ への作用,

$\sigma_2(4)$ については $\mathbf{M}(1), \mathbf{M}(8)$, $X(6), X(3), \mathbf{M}(7), \mathbf{M}(5), X(2)$ への作用と $|\mathbf{M}(3)^{\sigma_2(4)} \cap \mathbf{M}(3)|$ により,

$\sigma_2(5)$ については $\mathbf{M}(1)$, $X(2)$, $X(3)$, $X(4)$, $\mathbf{M}(2)$, $\mathbf{M}(5)$, $X(5)$, $\mathbf{M}(6)$ への作用,

$\sigma_3(1)$ については 補題 3.12 と $X(i)$ への作用,

によってその形が定まる. 以上から次の定理を得る.

定理 3.13 $\mathbf{M} = [a_{ij}]$ を $(\Omega, \mathbb{O})$ の M-行列とする. このとき M_{24} は次の置換を含む.

$$\sigma_2(1) = (a_{11}, a_{12})(a_{21}, a_{22})(a_{31}, a_{42})(a_{41}, a_{32})(a_{33}, a_{43})(a_{34}, a_{44})(a_{35}, a_{45})(a_{36}, a_{46})$$
$$\sigma_2(2) = (a_{12}, a_{13})(a_{22}, a_{23})(a_{31}, a_{41})(a_{32}, a_{43})(a_{42}, a_{33})(a_{34}, a_{44})(a_{25}, a_{45})(a_{26}, a_{36})$$
$$\sigma_2(3) = (a_{13}, a_{14})(a_{23}, a_{24})(a_{31}, a_{41})(a_{32}, a_{42})(a_{33}, a_{44})(a_{43}, a_{34})(a_{35}, a_{45})(a_{36}, a_{46})$$
$$\sigma_2(4) = (a_{14}, a_{15})(a_{44}, a_{45})(a_{31}, a_{41})(a_{22}, a_{42})(a_{23}, a_{33})(a_{24}, a_{35})(a_{34}, a_{25})(a_{26}, a_{36})$$
$$\sigma_2(5) = (a_{15}, a_{16})(a_{25}, a_{26})(a_{31}, a_{41})(a_{32}, a_{42})(a_{33}, a_{43})(a_{34}, a_{44})(a_{35}, a_{46})(a_{45}, a_{36})$$
$$\sigma_3(1) = (a_{21}, a_{31}, a_{41})(a_{22}, a_{32}, a_{42})(a_{23}, a_{33}, a_{43})(a_{24}, a_{34}, a_{44})(a_{25}, a_{35}, a_{45})(a_{26}, a_{36}, a_{46})$$

これらを M-行列に表したものを付録 (p.95) に記す. 定理 3.13 より, M_{24} が $1^8 2^8$ 型, および $1^6 3^6$ 型の元を含むことがわかる. また $\sigma_2(1)\sigma_2(3)\sigma_2(5)$ は 2^{12} 型の元である. 次の定理は次節で Mathieu 群の単純性を証明する際に必要となる.

定理 3.14 位数 2 の元は $1^8 2^8$ 型または 2^{12} 型である. また $1^8 2^8$ 型の元はすべて共役である.

Proof $\sigma \in M_{24}$ は位数が 2 で, 固定点 x をもつとする. 固定点の個数は高々 8 個なので σ の cycle 分解は少なくとも 8 個の互換を含む. その中の 3 個を $(y_1, y_2)(y_3, y_4)(y_5, y_6)$ とする. ここで $C_1 = C(x, y_1, y_2, y_3, y_4)$ とおくと $C_1^\sigma = C_1$ となる. 従って $\sigma \in H(C_1) - N(C_1)$ となるので σ は C_1 に偶置換として作用する. 従って $C_1 - \{y_1, y_2, y_3, y_4\}$ の元はすべて固定される. 特に y_5, y_6 は C_1 に含まれない. $C_2 = C(x, y_1, y_2, y_5, y_6)$ とすると $C_2 - \{y_1, y_2, y_5, y_6\}$ の元もすべて固定される. 一方 $|C_1 \cap C_2| = 4$ となることから σ の固定点は 6 点以上ある. 従って補題 3.12 より σ は $1^8 2^8$ 型である. また $1^8 2^8$ 型の元の固定点のなす octad を系 3.3 により, octad C に一致させることができる. 更に $H(C)$ が $N(C) - \{1\}$ 上 2 重可移であるから $N(C) - \{1\}$ の元は $H(C)$ で共役である. ゆえに $1^8 2^8$ 型の元は互いに共役である. ∎

次に 4 章で Conway 群の単純性を示す際に必要となる Sylow 23-部分群の正規化群について考察する. 以下 α を M_{24} の位数 23 の元とする. α の置換の型は $1^1 23^1$ となり, Ω の 1 点を固定することに注意されたい.

補題 3.15 $\langle\alpha\rangle$ の中心化群は $\langle\alpha\rangle$ 自身である. すなわち $C_{M_{24}}(\alpha) = \langle\alpha\rangle$ が成り立つ.

Proof $K = C_{M_{24}}(\alpha)$ とする. 明らかに $\langle\alpha\rangle \leq K$ が成り立つから $K \leq \langle\alpha\rangle$ を示せばよい. $K \ni \gamma$ を任意に選ぶ. α の固定点を x とすると

$$(x^\gamma)^\alpha = x^{\gamma\alpha} = x^{\alpha\gamma} = (x^\alpha)^\gamma = x^\gamma$$

より x^γ も α の固定点である. α の固定点は x のみであるから $x^\gamma = x$ が成り立つ.

$y^\gamma = y$ となる $y \neq x$ が存在すると仮定する. $\langle\alpha\rangle$ は $\Omega - \{x\}$ 上可移であるから x と異なる任意の $z \in \Omega$ に対して $y^{\alpha^r} = z$ となる整数 r が存在する. このとき

$$z^\gamma = (y^{\alpha^r})^\gamma = y^{\alpha^r\gamma} = y^{\gamma\alpha^r} = (y^\gamma)^{\alpha^r} = y^{\alpha^r} = z$$

となることから $\gamma = 1 \in \langle\alpha\rangle$ が成り立つ.

さて $\Omega - \{x\}$ から任意に y を選ぶと $\langle\alpha\rangle$ が $\Omega - \{x\}$ 上可移であるから $y^{\alpha^m} = y^\gamma$ となる整数 m が存在する. このとき $y^{\gamma\alpha^{-m}} = y$ であるから上述のことより $\gamma\alpha^{-m} = 1$ が成り立つ. 従って $\gamma = \alpha^m \in \langle\alpha\rangle$ を得る. 以上で $K \leq \langle\alpha\rangle$ が示された. ∎

補題 3.16 $|N_{M_{24}}(\langle\alpha\rangle)| = 11 \cdot 23$ である. また M_{24} の元 β で 位数が 11 かつ $\alpha^\beta = \alpha^2$ をみたすものが存在する.

Proof $\langle\alpha\rangle$ は M_{24} の Sylow 23-部分群であるから, 定理 1.3 と定理 1.12 より

$$|M_{24} : N_{M_{24}}(\langle\alpha\rangle)| \equiv 1 \pmod{23}$$

が成り立つ. また定理 1.9 と補題 3.15 より $N_{M_{24}}(\langle\alpha\rangle)/C_{M_{24}}(\langle\alpha\rangle) = N_{M_{24}}(\langle\alpha\rangle)/\langle\alpha\rangle$ は $Aut(\langle\alpha\rangle)$ の部分群と同型である. 従って, 定理 1.8 より $|N_{M_{24}}(\langle\alpha\rangle) : C_{M_{24}}(\langle\alpha\rangle)|$ は 22 の約数になる. 以上から $|N_{M_{24}}(\langle\alpha\rangle)| = 11 \cdot 23$ が得られる.

また $\beta \in N_{M_{24}}(\langle\alpha\rangle)$ を位数 11 の元とする. このとき $\alpha^\beta = \alpha^k$ となる自然数 k $(2 \leq k \leq 22)$ が存在する. $\alpha = \alpha^{\beta^{11}} = \alpha^{k^{11}}$ となることから

$$k = 2, 3, 4, 6, 8, 9, 12, 13, 16, 18$$

を得る. いずれの場合も, それぞれ $n = 1, 7, 6, 5, 4, 9, 10, 8, 3, 2$ とすると $k^n \equiv 2 \pmod{23}$ が成り立つ. β^n を改めて β とすると $\alpha^\beta = \alpha^2$ が成り立つ. ∎

補題 3.17 補題 3.16 をみたす β に対して $N_{M_{24}}(\langle\alpha\rangle) = \langle\alpha, \beta\rangle$ が成り立つ.

Proof $\langle\alpha, \beta\rangle \leq N_{M_{24}}(\langle\alpha\rangle)$ は明らかに成り立つ. また補題 3.16 より $N_{M_{24}}(\langle\alpha\rangle)$ は位数 $11 \cdot 23$ である. 一方, 位数 11, 23 の元を含むことから $\langle\alpha, \beta\rangle$ の位数は $11 \cdot 23$ の倍数である. 従って $N_{M_{24}}(\langle\alpha\rangle) = \langle\alpha, \beta\rangle$ が成り立つ. ∎

3.2 Mathieu 群の単純性

Ω の元 a_1, a_2, a_3 を任意に選んで固定し

$$M_{24-t} = \{\sigma \in M_{24} \mid a_i^\sigma = a_i\}, \quad \mathbb{O}(t) = \{C \in \mathbb{O} \mid a_1, \ldots, a_t \in C\} \quad (1 \leq t \leq 3)$$

とおく. ただし $\mathbb{O}(0) = \mathbb{O}$ とする. M_{24} の 5 重可移性により M_{24-t} の構造は a_1, a_2, a_3 の選び方によらない. これらの群 M_{21}, M_{22}, M_{23} も Mathieu 群 と呼ばれる.

M_{24} が Ω 上 5 重可移であることから M_{24-t} は $\Omega - \{a_1, \ldots, a_t\}$ 上 $(5-t)$ 重可移となる. また $\mathbb{O}(t) \ni C_1, C_2$ に対して

$$C_1 - \{a_1, \ldots, a_t\} \ni x_1, ..., x_{5-t} \quad を \quad y_1, ..., y_{5-t} \in C_2 - \{a_1, \ldots, a_t\}$$

に移す M_{24} の元 σ が存在し, $C_1^\sigma = C_2$ となることから次の定理を得る.

定理 3.18 M_{24-t} は $\mathbb{O}(t)$ 上可移である $(t = 0, 1, 2, 3)$.

以下, M_{24-t} が $\mathbb{O}(t)$ に原始的に作用することを示す.

$C \in \mathbb{O}(t)$ を不変にする M_{24-t} の部分群 $H(C) \cap M_{24-t}$ を $H_t(C)$ とおく.

$$H_t(C) = \{\sigma \in M_{24-t} \mid C^\sigma = C\}$$

である. また octad C と $a, b, c, d \in C$ に対して

$$\mathbb{O}_{ab}^C = \left\{D \in \mathbb{O} \mid D \cap C = \{a, b\}\right\}$$
$$\mathbb{O}_{abcd}^C = \left\{D \in \mathbb{O} \mid D \cap C = \{a, b, c, d\}\right\}$$

とおく.

補題 3.19 a,b,c,d は *octad* C_0 の元であるとする. このとき $N(C_0)$ は $\mathbb{O}_{ab}^{C_0}$ に正則に, $\mathbb{O}_{abcd}^{C_0}$ に可移に作用する.

Proof $N(C_0)$ は $H(C_0)$ を C_0 に作用させたときの核であったことを想起されたい (p.50). $N(C_0)$ の元は a,b,c,d をすべて固定するので $\mathbb{O}_{ab}^{C_0}$, $\mathbb{O}_{abcd}^{C_0}$ に作用する. さて $C \in \mathbb{O}_{ab}^{C_0}$ を任意に選び, $N(C_0) \ni \sigma \neq 1$ が C を固定すると仮定する. 前節の結果から σ は位数 2 で $C - C_0$ に固定点を持たない. 従って σ は $C - C_0$ 上互換 3 個の積となるが, これは $H(C)/N(C) \simeq A_8$ であることに反する. よって C を固定する $N(C_0)$ の元は 1 のみである. 従って $|N(C_0)| = 16$ より, $\mathbb{O}_{ab}^{C_0}$ における $N(C_0)$-orbit の size は 16 となるが, 表 2.1(p.30) の最下行より $|\mathbb{O}_{ab}^{C_0}| = 16$ となるので $N(C_0)$ が $\mathbb{O}_{ab}^{C_0}$ 上可移, 従って正則に作用することがわかる.

次に $C \in \mathbb{O}_{abcd}^{C_0}$ とし, $S = \{\sigma \in N(C_0) \mid C^\sigma = C\}$ とおく. S は $C - C_0$ 上に S_4 の部分群で位数が 2 のべきの基本アーベル群として作用する. 従って $|S| \leq 4$ を得る. これより $\mathbb{O}_{abcd}^{C_0}$ 上の $N(C_0)$-orbit の size は 4 以上となるが, 表 2.1(p.30) の最下行より $|\mathbb{O}_{abcd}^{C_0}| = 4$ となるので $N(C_0)$ が $\mathbb{O}_{ab}^{C_0}$ に可移に作用することがわかる. ∎

系 3.20 M_{24} は *dodecad* 全体のなす集合 $\mathbb{D}$ に可移に作用する.

Proof dodecad D_1, D_2 に対して

$$D_1 = A_1 + B_1\,, \qquad D_2 = A_2 + B_2$$

をみたす octad A_i, B_i が存在する. M_{24} は $\mathbb{O}$ 上可移であるから, $A_1^\sigma = A_2$ をみたす $\sigma \in M_{24}$ が存在する. ここで $B_3 = B_1^\sigma$ とおく. $H(A_2)$ は A_2 上 2 重可移であるから $(B_3 \cap A_2)^\lambda = B_2 \cap A_2$ となる $\lambda \in H(A_2)$ が存在する. $B_4 = B_3^\lambda$ とおく. $B_2 \cap A_2 = \{a,b\}$ とおくと, 補題 3.19 より $N(A_2)$ は $\mathbb{O}_{ab}^{A_2}$ 上可移であるから $B_4^\rho = B_2$ となる $\rho \in N(A_2)$ が存在する. このとき

$$A_1^{\sigma\lambda\rho} = A_2^{\lambda\rho} = A_2\,, \quad B_1^{\sigma\lambda\rho} = B_3^{\lambda\rho} = B_4^\rho = B_2 \quad \Longrightarrow \quad D_1^{\sigma\lambda\rho} = D_2$$

となるので, 系が証明された. ∎

$\Omega = C_1 \cup C_2 \cup C_3$ をみたす $C_1, C_2, C_3 \in \mathbb{O}$ に対して $\mathbf{T} = \{C_1, C_2, C_3\}$ を Trio と呼び, C_1, C_2, C_3 を Trio $\mathbf{T}$ の成分ということにする.

補題 3.21 M_{24} は *Trio* 全体のなす集合上可移である.

Proof　M_{24} が $\mathbb{O}$ 上可移であることから, 任意の octad C に対して $H(C)$ が C を成分とする Trio 全体の上に可移であることを示せばよい.

$y \in \Omega - C$ の $H(C)$ における固定群を A とすると, 定理 3.8 より $A \simeq A_8$ なので C 上 $3^1 5^1$ 型の置換 $\rho \in A$ が存在する. ここで ρ^5 は位数 3 であり, 6 点以上の固定点を持つことから補題 3.12 より, non-special な 6 点を固定し, Ω 上 $1^6 3^6$ 型である. 従って ρ^5 の $\Omega - C$ での固定点は y のみである. また ρ^3 は位数 5 であるから, その固定点は 5 点以下であり, Ω 上 $1^4 5^4$ 型である. 従って ρ^3 の $\Omega - C$ での固定点は y のみである. 以上から ρ は $\Omega - C$ 上 $1^1 15^1$ 型である.

さて定理 2.22 より C を成分とする Trio $\{C, C_1, C_2\}$ が存在する. $y \in C_1$ であるとしてよい. $\Omega - C$ 上 ρ^3 が $1^1 5^3$ 型, ρ^5 が $1^1 3^5$ 型であるから, $\langle\rho\rangle$ における C_1 の固定群は 1 である. 従って

$$\{C_1, C_2\}^{\rho^k} \qquad (k = 0, 1, 2, .., 14)$$

には C と共有点をもたない octad 30 個すべてが現れる (p.30, 表 2.1). C を成分とする Trio は $\{C, C_1^{\rho^k}, C_2^{\rho^k}\}$ $(k = 0, 1, 2, .., 14)$ でつくされるので, $H(C)$ が可移に作用することがわかる. ∎

群 G が X に作用するとき G-orbit は block である. 従って G の作用が原始的ならば, その作用は可移である. また x の固定群 G_x は G の極大部分群である. なぜならば, $G_x < M < G$ となる部分群 M が存在すれば X の部分集合

$$\{x^\sigma \mid \sigma \in M\}$$

が自明でない block となり, 矛盾が生じるからである.

定理 3.22 M_{24} の $\mathbb{O}$ 上への作用について次が成り立つ.

(1) M_{24-t} は $\mathbb{O}(t)$ 上原始的に作用する. 従って $H_t(C_0)$ は M_{24-t} の極大部分群である.

(2) $H_t(C_0) = N(C_0)A(t)$, $N(C_0) \cap A(t) = 1$, $A(t) \simeq A_{8-t}$ をみたす $A(t) \leq H_t(C_0)$ が存在する.

Proof　a_1, a_2, a_3 を含む octad を任意に選び C_0 とする. また $k = 0, 2, 4$ に対して

$$\mathbb{O}_k = \{C \in \mathbb{O} \mid |C \cap C_0| = k\}$$

とおく. まず $t=0$ として M_{24} の $\mathbb{O}$ への作用における, C_0 の固定群 $H(C_0)$ の軌道を求めることにする. 表 2.1 より

$$|\mathbb{O}_0| = 30, \quad |\mathbb{O}_2| = 16 \cdot \binom{8}{2} = 448, \quad |\mathbb{O}_4| = 4 \cdot \binom{8}{4} = 280,$$

が成り立つ. 補題 3.19 を用いて $\mathbb{O}$ を $H(C_0)$-orbit へ分割すると

$$\mathbb{O} = \{C_0\} \cup \mathbb{O}_0 \cup \mathbb{O}_2 \cup \mathbb{O}_4 \quad \Longrightarrow \quad 759 = 1 + 30 + 448 + 280$$

が得られる. ここで C_0 を含む block が存在すれば, その size は $1, 30, 448, 280$ の和となるが, 759 を割り切るのは 1, 759 のみであるから, 自明でない block は存在しない. よって M_{24} の $\mathbb{O}(0) = \mathbb{O}$ への作用は原始的である. また, 前述のことから $H(C_0) = H_0(C_0)$ は M_{24} の極大部分群である.

次に $t=1$ として M_{23} の $\mathbb{O}(1)$ への作用における C_0 の固定化群 $H_1(C_0)$ の軌道を求める.

$$|\mathbb{O}(1) \cap \mathbb{O}_2| = 16 \cdot \binom{7}{1} = 112, \quad |\mathbb{O}(1) \cap \mathbb{O}_4| = 4 \cdot \binom{7}{3} = 140$$

が成り立つことから

$$\mathbb{O}(1) = \{C_0\} \cup (\mathbb{O}(1) \cap \mathbb{O}_2) \cup (\mathbb{O}(1) \cap \mathbb{O}_4) \quad \Longrightarrow \quad 253 = 1 + 112 + 140$$

が得られる. ここで C_0 を含む block が存在すれば, その size は $1, 112, 140$ の和となるが, 253 を割り切るのは 1, 253 のみであるから, 自明でない block は存在しない. よって M_{23} の $\mathbb{O}(1)$ への作用は原始的で, $H_1(C_0)$ は M_{23} の極大部分群である.

$t=2$ の場合も同様にして M_{22} の $\mathbb{O}(2)$ への作用における C_0 の固定化群 $H_2(C_0)$ の軌道を求めれば

$$|\mathbb{O}(2) \cap \mathbb{O}_2| = 16, \quad |\mathbb{O}(2) \cap \mathbb{O}_4| = 4 \cdot \binom{6}{2} = 60,$$

より

$$\mathbb{O}(2) = \{C_0\} \cup (\mathbb{O}(2) \cap \mathbb{O}_2) \cup (\mathbb{O}(2) \cap \mathbb{O}_4) \quad \Longrightarrow \quad 77 = 1 + 16 + 60$$

が得られ, 作用の原始的であること, $H_2(C_0)$ が M_{22} で極大であることが導かれる.

$t=3$ の場合も同様にして M_{21} の $\mathbb{O}(3)$ への作用における C_0 の固定化群 $H_3(C_0)$ の軌道を求めれば

$$|\mathbb{O}(3) \cap \mathbb{O}_4| = 4 \cdot 5 = 20$$

より

$$\mathbb{O}(3) = \{C_0\} \cup (\mathbb{O}(3) \cap \mathbb{O}_4) \quad \Longrightarrow \quad 21 = 1 + 20$$

が得られ, 作用の原始的であること, $H_3(C_0)$ が M_{21} で極大であることが導かれる. 以上で (1) が示された.

定理 3.8 より $\Omega - C_0$ の 1 点 y の固定群を A とすれば

$$H(C_0) = N(C_0)A, \quad N(C_0) \cap A = 1, \quad H(C_0)/N(C_0) \simeq A \simeq A_8$$

が成立する. $N(C_0) \leq M_{21}$ であるから $A(t) = M_{24-t} \cap A$ とおけば $H_t(C_0) \rhd N(C_0)$ であり

$$H_t(C_0) = N(C_0)A(t), \quad N(C_0) \cap A(t) = 1, \quad H_t(C_0)/N(C_0) \simeq A(t) \simeq A_{8-t}$$

が成り立つ. よって (2) も示された. ∎

定理 3.23 $t = 1, 2, 3$ のとき M_{24-t} の位数 2 の元は互いに共役である.

Proof C_0 は前と同様 a_1, a_2, a_3 を含む octad であるとする. M_{24-t} の位数 2 の元 σ を選ぶと, 定理 3.14 より σ は Ω 上 $1^8 2^8$ 型であり, その固定点の集合は $a_1, .., a_t$ を含む octad である. M_{24-t} は $\mathbb{O}(t)$ 上可移であるから σ^τ の固定点が C_0 となるような $\tau \in M_{24-t}$ が存在する. これより M_{24-t} の位数 2 の元は $N(C_0)$ の元に共役である. 従って $N(C_0)$ の任意の位数 2 の元 σ_1, σ_2 が $H_t(C_0) = M_{24-t} \cap H(C_0)$ で共役であることを示せばよい. σ_1, σ_2 を disjoint な互換の積として表すと

$$\sigma_1 = (b_1, b_2) \cdots\cdots, \qquad \sigma_2 = (c_1, c_2) \cdots\cdots,$$

であるとする. ここで b_1, b_2, c_1, c_2 が $\Omega - C_0$ の点であることを注意しておく.

さて $C_1 = C(a_1, a_2, a_3, b_1, b_2)$ とする. このとき $|C_0 \cap C_1| = 4$ となることから $x_1 \in C_0 \cap C_1, x_1 \neq a_i$, が存在する. 従って $x_0 \in C_0 - C_1$ を適当に選ぶと $M_1 = (x_0, x_1, a_1, a_2, a_3, b_1, b_2)$ は M-順列になる. 同様に $x_0' \in C_0 - C_1$, $x_1' \in C_0 \cap C_1$ を適当に選ぶと M-順列 $M_2 = (x_0', x_1', a_1, a_2, a_3, c_1, c_2)$ が得られる. M_1 を M_2 に移す M_{24} の元を ρ とする. 明らかに

$\rho \in M_{24-t} \cap H(C_0) = H_t(C_0)$ である. ここで

$$\begin{aligned}(x_0', x_1', a_1, a_2, a_3, c_1, c_2)^{\sigma_1^\rho} &= (x_0', x_1', a_1, a_2, a_3, c_1, c_2)^{\rho^{-1}\sigma_1\rho} \\ &= (x_0, x_1, a_1, a_2, a_3, b_1, b_2)^{\sigma_1\rho} \\ &= (x_0, x_1, a_1, a_2, a_3, b_2, b_1)^{\rho} \\ &= (x_0', x_1', a_1, a_2, a_3, c_2, c_1) \\ &= (x_0', x_1', a_1, a_2, a_3, c_1, c_2)^{\sigma_2}\end{aligned}$$

が成り立つ. M-順列を固定するのは恒等置換のみであるから $\sigma_1^\rho = \sigma_2$ が成り立つ. よって σ_1, σ_2 は $H_t(C_0)$ で共役である. ゆえに M_{24-t} の位数 2 の元は互いに共役である. ∎

上の証明の中で次の系が示されていることに注意されたい.

系 3.24 $N(C_0)$ の位数 2 の元は $H_t(C_0)$ で互いに共役である.

C を a_1, a_2, a_3 を含む octad とし, $\sigma \in N(C)$ を位数 2 の元とする. また定理 3.22 と同様に $H_t(C) = N(C)A(t)$, $A(t)$ の $\Omega - C$ での固定点を y とする.

補題 3.25 $A(3)$ は $\Omega - C - \{y\}$ に可移に作用する.

Proof $\Omega - C$ から b_1, b_2 を選び $C_1 = C(a_1, a_2, a_3, b_1, b_2)$ とおく. このとき, $|C \cap C_1| = 4$ となることから $x_0 \in C - C_1$, $x_1 \in C \cap C_1$ を適当に選べば $M_1 = (x_0, x_1, a_1, a_2, a_3, b_1, b_2)$ が M-順列となる. 同様に $b_1', b_2' \in \Omega - C$ に対して M-順列 $M_2 = (x_0', x_1', a_1, a_2, a_3, b_1', b_2')$ が得られる. このとき $M_1^\rho = M_2$ となる $\rho \in M_{24}$ が存在し, $(b_1, b_2)^\rho = (b_1', b_2')$ をみたす. 一方 $a_1^\rho = a_1$, $a_2^\rho = a_2$, $a_3^\rho = a_3$, $C^\rho = C$ であることから $\rho \in H_3(C)$ である. 従って $H_3(C)$ は $\Omega - C$ に 2 重可移に作用する. よって定理 1.2 より $A(3)$ は $\Omega - C - \{y\}$ に可移に作用する. ∎

補題 3.26 $C_{M_{24}}(N(C)) = N(C)$ が成り立つ.

Proof C が $N(C)$ の固定点全体に一致することから, 任意の $\tau \in C_{M_{24}}(N(C))$ に対して C^τ は $N(C)^\tau = N(C)$ の固定点全体に一致する. 従って $C^\tau = C$ が成り立つ. これより $C_{M_{24}}(N(C)) \leq H(C)$ が得られる.

今 $C_{M_{24}}(N(C)) \supsetneq N(C)$ と仮定すると $C_{M_{24}}(N(C)) \cap A \neq 1$ が成り立つ. ただし $H(C) = N(C)A$ であり, A は $\Omega - C$ の点 y を固定するとする. このとき任意の $\sigma \in N(C)$

と $a \in C_{M_{24}}(N(C)) \cap A$ に対して

$$(y^\sigma)^a = y^{\sigma a} = y^{a\sigma} = (y^a)^\sigma = y^\sigma$$

が成り立つので y^σ は $C_{M_{24}}(N(C)) \cap A$ によって固定される. 一方 $N(C)$ が $\Omega - C$ 上可移であることから $C_{M_{24}}(N(C)) \cap A$ は $\Omega - C$ のすべての点を固定する. 9 点以上固定するのは恒等置換のみであるからこれは $C_{M_{24}}(N(C)) \cap A \neq 1$ に矛盾する. よって補題が証明された. ∎

定理 3.27 $N(C)$ の位数 2 の元 σ に対して $C_{M_{24-t}}(\sigma) \leq H_t(C)$ が成り立つ. 更に $C_{M_{24-t}}(\sigma) \cap A(t) = B(t)$ とおけば $C_{M_{24-t}}(\sigma) = N(C)B(t)$ が成り立つ. また $C_{M_{24-t}}(\sigma)$ は 1 以外に奇数位数の正規部分群をもたない.

Proof C が $\sigma \in N(C)$ の固定点全体に一致することから, 任意の $\tau \in C_{M_{24-t}}(\sigma)$ に対して C^τ は σ^τ の固定点全体に一致する. $\sigma^\tau = \sigma$ より $C^\tau = C$ が得られる. 従って $C_{M_{24-t}}(\sigma) \leq H_t(C)$ が成り立つ.

$H_t(C)$ における $\Omega - C \ni y$ の固定群を $A(t)$ とすると $H_t(C) = N(C)A(t)$ である. $N(C) \leq C_{M_{24-t}}(\sigma)$ より

$$C_{M_{24-t}}(\sigma) = N(C)\left(A(t) \cap C_{M_{24-t}}(\sigma)\right)$$

が成り立つ. 従って $C_{M_{24-t}}(\sigma) \cap A(t) = B(t)$ とおけば $C_{M_{24-t}}(\sigma) = N(C)B(t)$ が得られる.

さて $P \lhd C_{M_{24-t}}(\sigma)$ をみたす奇数位数の部分群 P が存在したと仮定する. ここで $a \in P$, $\sigma \in N(C)$ に対して

$$[a,\sigma] = a^{-1}\sigma^{-1}a\sigma = a^{-1}(\sigma^{-1}a\sigma) \in P, \qquad [a,\sigma] = a^{-1}\sigma^{-1}a\sigma = (a^{-1}\sigma^{-1}a)\sigma \in N(C)$$

が成り立つ. $N(C)$ が 2-群であるから $P \cap N(C) = 1$ となるので

$$[a,\sigma] \in P \cap N(C) \implies a^{-1}\sigma^{-1}a\sigma = 1 \implies a\sigma = \sigma a$$

が得られる. 従って P の元と $N(C)$ の元は可換になる. 補題 3.26 より $P \leq N(C)$ となるが, P が奇数位数, $|N(C)| = 16$ であることより $P = 1$ が得られる. ∎

ここで $G = H.K$ が半直積を表すことを想起されたい (p.15). また σ は $N(C)$ の位数 2 の元とし, $B(t)$ は定理 3.27 で定めた通りとする.

補題 3.28 $B(0) \simeq 2^3.L_3(2)$ が成り立つ. ただし 2^3 は位数が 2^3 の基本アーベル群を表す.

Proof $N(C)$ が位数 2^4 の基本アーベル群であることから $\mathbb{F}_2$ 上の 4 次元ベクトル空間とみなすことができる. A の元 a は共役をとる作用で次の $N(C)$ の線型変換を引き起こす.

$$N(C) \ni \sigma \longmapsto \sigma^a \in N(C)$$

補題 3.11 より a にこの線型変換を対応させる写像は A から $L_4(2)$ への同型写像である. σ を含む基底を 1 つ選び $\{\sigma, \sigma_1, \sigma_2, \sigma_3\}$ とする. この基底に関する $N(C)$ の線型変換 f の行列 F を

$$(f(\sigma), f(\sigma_1), f(\sigma_2), f(\sigma_3)) = (\sigma, \sigma_1, \sigma_2, \sigma_3)\, F$$

で定める. $B(0)$ は A における σ の固定群であることから

$$B(0) \simeq \left\{ \left[\begin{array}{cccc} 1 & x_1 & x_2 & x_3 \\ 0 & & & \\ 0 & & \mathbf{X} & \\ 0 & & & \end{array} \right] \;\middle|\; x_i \in \mathbb{F}_2, \quad \mathbf{X} \in L_3(2) \right\}$$

となる. ここで

$$V = \left\{ \left[\begin{array}{cccc} 1 & x_1 & x_2 & x_3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right] \;\middle|\; x_i \in \mathbb{F}_2 \right\}, \qquad G = \left\{ \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & & & \\ 0 & & \mathbf{X} & \\ 0 & & & \end{array} \right] \;\middle|\; \mathbf{X} \in L_3(2) \right\}$$

とおけば $V \simeq 2^3$, $G \simeq L_3(2)$ であるから $B(0) \simeq 2^3.L_3(2)$ が成り立つ. ∎

以下において V は上の証明中で定めたものとする. 定理3.22 より $C_{M_{24}}(\sigma) \simeq N(C).(V.L_3(2))$ が成り立ち, $P = N(C)V$ とおけば $P \lhd C_{M_{24}}(\sigma)$ となる.

補題 3.29 $Z(P) = \langle \sigma \rangle$ が成り立つ.

Proof $Z(P) \leq C_P(N(C))$ であるが, 補題 3.26 より $Z(P) \leq N(C)$ が得られる. 従って V のすべての元と可換な $N(C)$ の元を求めればよい. $a \in V$, $\rho \in N(C)$ に対して a に対応

する行列を A とし,

$$A = \begin{bmatrix} 1 & x_1 & x_2 & x_3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \rho = b_0\sigma + b_1\sigma_1 + b_2\sigma_2 + b_3\sigma_3 = (\sigma, \sigma_1, \sigma_2, \sigma_3) \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

とおくと

$$\rho^a = \begin{bmatrix} b_0 + x_1b_1 + x_2b_2 + x_3b_3 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

となる. これより任意の $a \in V$ に対して $\rho^a = \rho$ となる ρ は 0 と σ のみであることがわかる. ゆえに $Z(P) = \langle\sigma\rangle$ である. ∎

補題 3.30 $C_{M_{24}}(\sigma) \rhd U \neq 1$ ならば $\sigma \in U$ が成り立つ.

Proof $C_{M_{24}}(\sigma) \rhd U \neq 1$ と仮定する. $P \cap U = 1$ であるとすれば $C_{M_{24}}(\sigma) \rhd P$ より U は P の元と可換となり, 補題 3.26 より $U \leq N(C)$ が得られ, 矛盾が生じる. 従って $P \cap U \neq 1$ が成り立つ. 一方, P は 2-群であり, $P \cap U \lhd P$ であることから, 定理 1.16 より $(P \cap U) \cap Z(P) > 1$ が得られる. よって $\sigma \in P \cap U \leq U$ が示された. ∎

定理 3.31 $t = 0, 1, 2, 3$ に対し M_{24-t} は単純群である.

Proof 鈴木の判定法を適用し, $t = 0$ の場合は定理 1.24 の条件(1.1) と(1.2), $t = 1, 2, 3$ の場合は条件(1.1) と補題 1.25 の条件(1.3) をみたすことを示す. このとき M_{24-t} の位数が 4 の倍数であることから M_{24-t} の単純性が得られる. 以下 σ は前と同様に $1^8 2^8$ 型の置換とし, その固定点からなる octad を C, $a_1, a_2, a_3 \in C$ とする.

まず $G = M_{24-t}$ とおき $G = \langle\sigma^G\rangle$ を示す. $N(C)$ の位数 2 の元はすべて σ の共役であるから $N(C) \leq \langle\sigma^G\rangle$ が成り立つ. また $A(t) \simeq A_{8-t}$ は単純群であり, 位数 2 の元で生成されるが $A(t)$ の位数 2 の元は固定点をもつから $1^8 2^8$ 型で σ と共役である. 従って $A(t) \leq \langle\sigma^G\rangle$ を得る. 以上で $H_t(C) \leq \langle\sigma^G\rangle$ が示された. 次に C と異なる $C_1 \in \mathbb{O}(t)$ で a_1, a_2, a_3 を含むものを選ぶ. このとき $|C \cap C_1| = 4$ であるから $C \cap C_1 = \{a_1, a_2, a_3, a_4\}$ とおく. $N(C_1)$ は $\mathbb{O}^{C_1}_{a_1a_2a_3a_4}$ に可移に作用するから $C^\tau \neq C$ をみたす $\tau \in N(C_1)$ が存在する. $\tau \in \sigma^G$ かつ $\tau \notin H_t(C)$ であるから $H_t(C) \subsetneq \langle\sigma^G\rangle$ が成り立つ. 一方, 定理 3.22 より

$H_t(C)$ は $G = M_{24-t}$ の極大部分群であるから $G = \langle \sigma^G \rangle$ を得る. よって G は条件(1.1) をみたすことが示された.

$t = 0$ のときは補題 3.30 より条件(1.2) が成り立つ. また $t = 1, 2, 3$ のときは定理 3.23 と定理 3.27 より条件(1.3) が成り立つ. ゆえに $G = M_{24-t}$ は単純群である. ∎

M_{24}, M_{23}, M_{22} は Mathieu の単純群と呼ばれる. なお M_{21} は $PSL(3, 4)$ に同型であることが知られている. また $1 < M_{24} \cap A_{24} \lhd M_{24}$ であるが, M_{24} が奇置換を含めば $M_{24} \cap A_{24} \neq M_{24}$ となり定理 3.31 に矛盾する. 従って M_{24} のすべての元は偶置換である.

4章　Conway群

4 章では Leech lattice Λ, および, それを不変にする 24 次元ユークリッド空間 $\mathbb{R}^{24}$ の直交変換のなす群として Conway 群 $\cdot 0$ を定義し, その剰余群, 部分群として Conway の単純群 $\cdot 1$, $\cdot 2$, $\cdot 3$ が現れることを示す. なお Leech lattice は 1967 年, J. Leech が sphere packing との関連で発見した $\mathbb{R}^{24}$ の格子である.

§4.1 では Leech lattice Λ を定義し, Λ に含まれる 長さ $4\sqrt{2}$, $4\sqrt{3}$, 8 のベクトルの型と個数を決定する. また $\Lambda/2\Lambda$ の, 長さ 8 のベクトルを含む剰余類に長さ 8 のベクトルからなる $\mathbb{R}^{24}$ の直交基底が含まれることを示す. §4.2 では Binary Golay Code と M_{24} から Λ を不変にする単項行列のなす Monomial group が自然に定まることを示し, 長さ $4\sqrt{3}$ 以下のベクトルの集合を軌道に分割する. また長さ 8 のベクトルからなる直交基底から得られる正規直交基底に関する Λ のベクトルの成分表示が Leech lattice の 3 条件をみたすことを示す. §4.3 では Conway 群 $\cdot 0$, $\cdot 1$, $\cdot 2$, $\cdot 3$ を定義し, それらの位数を決定するとともに, $\cdot 1$, $\cdot 2$, $\cdot 3$ の単純性を導く.

4.1　Leech lattice

以下 $\mathbb{R}^{24}$ は 24 次ユークリッド空間とし, そのベクトルを行ベクトルで表すことにする. すなわち

$$\mathbb{R}^{24} = \{\, (x_1, x_2, \cdots, x_{24}) \mid x_i \in \mathbb{R} \,\}$$

である. ベクトル $\mathbf{x} = (x_1, \ldots, x_{24})$ と $\mathbf{y} = (y_1, \ldots, y_{24})$ に対して

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=i}^{24} x_i\, y_i\,, \qquad \|\mathbf{x}\| = \langle \mathbf{x}, \mathbf{x} \rangle = \sum_{i=i}^{24} x_i^2$$

と定める. $\langle \mathbf{x}, \mathbf{y} \rangle$ はユークリッド空間における通常の内積である. 第 i 座標が 1 であり, その他の座標が 0 である基本ベクトルを $\mathbf{e}_i$ と表す $(1 \le i \le 24)$. 更に $\Omega = \{1, 2, \ldots, 24\}$ と

おき, Γ を Ω 上の Binary Goley Code, $(\Omega, \mathbb{O})$ を Γ から定まる S(5,8,24) とする. Ω の部分集合 T に対して $\mathbf{e}_T = \sum_{i \in T} \mathbf{e}_i$ とおく.

定義 4.1 座標が整数である $\mathbb{R}^{24}$ のベクトル $\mathbf{x} = (x_1, ..., x_{24})$ で, 次の条件をみたすもの全体からなる集合を *Leech lattice* といい Λ と表す.

$$x_1 \equiv x_2 \equiv \cdots\cdots \equiv x_{24} \pmod 2 \tag{4.1}$$

$$\sum_{i=1}^{24} x_i = \begin{cases} 0 \pmod 8, & x_i \equiv 0 \pmod 2 \text{ のとき} \\ 4 \pmod 8, & x_i \equiv 1 \pmod 2 \text{ のとき} \end{cases} \tag{4.2}$$

$$m = 0, 1, 2, 3 \text{ に対して } \{i \mid x_i \equiv m \pmod 4\} \in \Gamma \text{ が成り立つ} \tag{4.3}$$

成分が整数である $\mathbb{R}^{24}$ のベクトル全体のなす集合を $\mathbb{Z}^{24}$ と表すと $\mathbb{Z}^{24}$ は $\mathbf{e}_1, ..., \mathbf{e}_{24}$ を $\mathbb{Z}$ 基底とする階数 24 の自由加群で, $\Lambda \subseteq \mathbb{Z}^{24}$ が成り立つ.

補題 4.2 Λ は $\mathbb{Z}^{24}$ の部分加群である.

Proof $\mathbf{x} \in \Lambda$ に対して $-\mathbf{x}$ が(4.1), (4.2), (4.3) をみたすのは明らかである. また $\mathbf{x}, \mathbf{y} \in \Lambda$ に対して $\mathbf{x} + \mathbf{y}$ が (4.1), (4.2) をみたすことも明らかである. 従って $\mathbf{x} + \mathbf{y}$ が(4.3) をみたすことを示せばよい.

$x_i \equiv y_j \equiv 0 \pmod 2$ のとき

$$D = \{i \mid x_i \equiv 0 \pmod 4\}, \qquad E = \{i \mid y_i \equiv 0 \pmod 4\}$$

とおくと $D, E \in \Gamma$ より

$$\{i \mid x_i + y_i \equiv 2 \pmod 4\} = D + E \in \Gamma, \quad \{i \mid x_i + y_i \equiv 0 \pmod 4\} = \overline{D + E} \in \Gamma$$

となるので(4.3) が成り立つ. $x_i \equiv y_j \equiv 1 \pmod 2$ のときも同様である.

$x_i \equiv 0,\ y_j \equiv 1 \pmod 2$ のときは

$$D' = \{i \mid x_i \equiv 0 \pmod 4\}, \qquad E' = \{i \mid y_i \equiv 1 \pmod 4\}$$

とおくと $D', E' \in \Gamma$ より

$$\{i \mid x_i + y_i \equiv 3 \pmod 4\} = D' + E' \in \Gamma, \quad \{i \mid x_i + y_i \equiv 1 \pmod 4\} = \overline{D' + E'} \in \Gamma$$

となるので(4.3)が成り立つ. $x_i \equiv 1,\ y_j \equiv 0 \pmod 2$ のときも同様である. ∎

Λ は階数 24 の自由加群 $\mathbb{Z}^{24}$ の部分加群であるから, 定理 1.23 より階数が高々 24 の自由加群である. 一方 $8\mathbf{e}_i$ は明らかに Λ に含まれるから

$$\{\,(x_1, x_2, \cdots, x_{24}) \mid x_i \in \mathbb{Z}\,, x_i \equiv 0 \pmod 8\,\}$$

は $8\mathbf{e}_1, ..., 8\mathbf{e}_{24}$ を基底とする自由加群で, Λ の部分加群である. その階数 24 は Λ の階数以下であることから Λ の階数は 24 である.

一般に $\mathbb{R}^n$ の部分加群 L が階数 n の自由加群で, $\mathbb{R}^n$ の $\mathbb{R}$ 基底を含むとき, $\mathbb{R}^n$ の格子 (lattice) と呼ばれる. 従って Λ は $\mathbb{R}^{24}$ の格子である.

以下, 整数 $a, b, c, \ldots$ に対して

$$p = \big|\{\, i \mid x_i = a \,\}\big|,\quad q = \big|\{\, i \mid x_i = b \,\}\big|,\quad r = \big|\{\, i \mid x_i = c \,\}\big|, \ldots\ldots$$

であるようなベクトル $\mathbf{x}$ を $(a^p.b^q.c^r\ldots.)$ 型のベクトルと呼ぶ.

補題 4.3 $D \in \Gamma$ ならば $2\mathbf{e}_D \in \Lambda$ が成り立つ. また次の型のベクトルはすべて Λ に含まれる.

$$(-3^1.1^{23}),\quad (8^1.0^{23}),\quad (-4^1.4^1.0^{22}),\quad (4^2.0^{22})$$

Proof　$D \in \Gamma$ のとき, ベクトル $2\mathbf{e}_D$ は明らかに(4.1), (4.3) をみたす. また $|D|$ が 4 の倍数であるから, 成分の和は 8 の倍数になり(4.2) もみたす. 従って $2\mathbf{e}_D \in \Lambda$ が成り立つ.

$(-3^1.1^{23})$ 型のベクトル $\mathbf{x}$ は成分がすべて奇数で $\sum_{i=1}^{24} x_i = 20 \equiv 4 \pmod 8$, および $\{i \mid x_i \equiv 1 \pmod 4\} = \Omega \in \Gamma$ をみたすことから Λ に含まれる. また $(8^1.0^{23})$ 型のベクトルが Λ に含まれることは上に注意した通りである.

$(-3^1.1^{23})$ 型のベクトルは適当な i により $-4\mathbf{e}_i + \mathbf{e}_\Omega$ と表される. これより, 任意の $i \neq j$ に対して

$$-4\mathbf{e}_i + \mathbf{e}_\Omega,\ -4\mathbf{e}_j + \mathbf{e}_\Omega \in \Lambda \implies -(-4\mathbf{e}_i + \mathbf{e}_\Omega) + (-4\mathbf{e}_j + \mathbf{e}_\Omega) = 4\mathbf{e}_i - 4\mathbf{e}_j \in \Lambda$$
$$4\mathbf{e}_i - 4\mathbf{e}_j\,,\ 8\mathbf{e}_j \in \Lambda \implies 4\mathbf{e}_i - 4\mathbf{e}_j + 8\mathbf{e}_j = 4\mathbf{e}_i + 4\mathbf{e}_j \in \Lambda$$

が成り立つので $(-4^1.4^1.0^{22})$ 型, および $(4^2.0^{22})$ 型のベクトルも Λ に含まれる. ∎

補題 4.4 Λ は $(2^8.0^{16})$, $(-3^1.1^{23})$ 型のベクトルで生成される.

Proof $(-3^1.1^{23})$ 型のベクトルを $\mathbf{y}_i = -4\mathbf{e}_i + \mathbf{e}_\Omega$ $(1 \le i \le 24)$ とし

$$\Lambda_0 = \langle\ 2\mathbf{e}_C,\ \mathbf{y}_i \mid C \in \mathbb{O},\ 1 \le i \le 24\ \rangle$$

とおく. $\Lambda_0 \subseteq \Lambda$ は明らかに成り立つので $\Lambda \subseteq \Lambda_0$ を示せばよい. Trio $\{C_1, C_2, C_3\}$ を 1 つ選べば

$$2\mathbf{e}_{C_1} + 2\mathbf{e}_{C_2} + 2\mathbf{e}_{C_3} = 2\mathbf{e}_\Omega \in \Lambda_0$$

が得られ, これより

$$2\mathbf{e}_\Omega - 2\mathbf{y}_i = 8\mathbf{e}_i \in \Lambda_0$$

も得られる. また補題 4.3 の証明と同様にして $4\mathbf{e}_i - 4\mathbf{e}_j \in \Lambda_0$ が得られる.

さて 任意の $\mathbf{a} = (a_1, ..., a_{24}) \in \Lambda$ を選び $\mathbf{a} \in \Lambda_0$ が成り立つことを示す. 各 a_i が奇数であれば $\mathbf{a} + \mathbf{y}_1$ と置き換えることにより, a_i はすべて偶数であるとしてよい. 更に $\mathbf{a}$ に適当に $4\mathbf{e}_1 - 4\mathbf{e}_k$ の整数倍を加えることにより, 第 2〜 24 成分が 0 または 2 であるとしてよい.

ここで

$$D = \{i \mid a_i \equiv 2 \pmod 4\}$$

とおく. $\mathbf{a} \in \Lambda$ より $D \in \Gamma$ である. $D = \emptyset$ のとき, 第 2〜 24 成分はすべて 0 である. $D = \Omega$ のときは $\mathbf{a} - 2\mathbf{e}_\Omega$ の第 2〜 24 成分はすべて 0 である. D が octad のときは $\mathbf{a} - 2\mathbf{e}_D$ の第 2〜 24 成分はすべて 0 である. D が octad の補集合のときは $D = C_1 \cup C_2$ と表されるので, $\mathbf{a} - 2\mathbf{e}_{C_1} - 2\mathbf{e}_{C_2}$ の第 2〜 24 成分はすべて 0 である. D が dodecad のときは $D = C_1 + C_2$ と表されるので, $\mathbf{a} - 2\mathbf{e}_{C_1} - 2\mathbf{e}_{C_2}$ とすると第 2〜 24 成分は高々 2 成分で -4 になることを除いて, すべて 0 である. 従って適当な $-4\mathbf{e}_1 + 4\mathbf{e}_k$ を加えることにより第 2〜 24 成分をすべて 0 になるようにできる.

以上から $\mathbf{a}$ の第 2〜 24 成分はすべて 0 であるとしてよい. このとき a_1 は 8 の倍数であるから $\mathbf{a}$ は $8\mathbf{e}_1$ の整数倍に一致する. よって $\mathbf{a} \in \Lambda_0$ が示された. ∎

補題 4.5

(1) 任意の $\mathbf{x}, \mathbf{y} \in \Lambda$ に対して $\langle \mathbf{x}, \mathbf{y} \rangle \in 8\mathbb{Z}$ が成り立つ.

(2) 任意の $\mathbf{x} \in \Lambda$ に対して $\|\mathbf{x}\| \equiv 0 \pmod{16}$ が成り立つ. ただし $\|\mathbf{x}\| = 16$ をみたす $\mathbf{x} \in \Lambda$ は存在しない.

(3) 任意の $\mathbf{x} \in \Lambda$ に対して $\langle \mathbf{z}, \mathbf{x} \rangle \in 8\mathbb{Z}$ をみたす $\mathbf{z} \in \mathbb{R}^{24}$ は Λ に含まれる.

Proof　$\mathbf{x}, \mathbf{y} \in \Lambda$ を任意に選ぶ. 補題 4.4 より

$$\mathbf{x} = x_1\mathbf{a}_1 + \cdots + x_{24}\mathbf{a}_{24}\,, \qquad \mathbf{y} = y_1\mathbf{b}_1 + \cdots + y_{24}\mathbf{b}_{24} \quad (x_i, y_j \in \mathbb{Z})$$

と表すことができる. ただし $\mathbf{a}_i$, $\mathbf{b}_j$ は $(2^8.0^{16})$ 型, または $(-3^1.1^{23})$ 型のベクトルである. ここで

$$\langle \mathbf{x}, \mathbf{y} \rangle = \langle x_1\mathbf{a}_1 + \cdots + x_{24}\mathbf{a}_{24},\ y_1\mathbf{b}_1 + \cdots + y_{24}\mathbf{b}_{24} \rangle = \sum_{i,j} x_i y_j \langle \mathbf{a}_i, \mathbf{b}_j \rangle$$

が成り立つ. 従って (1) を示すには $\mathbf{a}$, $\mathbf{b}$ が $(-3^1.1^{23})$ 型または $(2^8.0^{16})$ 型のとき $\langle \mathbf{a}, \mathbf{b} \rangle$ が 8 の倍数であることを示せばよい.

$\mathbf{a}$, $\mathbf{b}$ が共に $(2^8.0^{16})$ 型のとき $\mathbf{a} = 2\mathbf{e}_C$, $\mathbf{b} = 2\mathbf{e}_D$ とおく. ただし $C, D \in \mathbb{O}$ である. このとき補題 2.12 より $|C \cap D|$ は偶数である. 従って $\langle \mathbf{a}, \mathbf{b} \rangle = 4\,|C \cap D|$ は 8 の倍数である.

$\mathbf{a}$, $\mathbf{b}$ が共に $(-3^1.1^{23})$ 型のとき $\mathbf{a} = -4\mathbf{e}_i + \mathbf{e}_\Omega$, $\mathbf{b} = -4\mathbf{e}_j + \mathbf{e}_\Omega$ とする. このとき

$$\langle \mathbf{a}, \mathbf{b} \rangle = \begin{cases} 32\,, & i = j \\ 16\,, & i \neq j \end{cases}$$

となり, $\langle \mathbf{a}, \mathbf{b} \rangle$ は 8 の倍数である.

$\mathbf{a}$ が $(2^8.0^{16})$ 型, $\mathbf{b}$ が $(-3^1.1^{23})$ 型のとき $\mathbf{a} = 2\mathbf{e}_C$ $(C \in \mathbb{O})$, $\mathbf{b} = -4\mathbf{e}_j + \mathbf{e}_\Omega$ とする. このときも

$$\langle \mathbf{a}, \mathbf{b} \rangle = \begin{cases} 8\,, & j \in C \\ 16\,, & j \notin C \end{cases}$$

となり $\langle \mathbf{a}, \mathbf{b} \rangle$ は 8 の倍数である. $\mathbf{a}$ が $(-3^1.1^{23})$ 型, $\mathbf{b}$ が $(2^8.0^{16})$ 型のときも同様である. 以上で (1) が示された.

次に $\mathbf{x}$ を前と同様とすると

$$\begin{aligned} \langle \mathbf{x}, \mathbf{x} \rangle &= \langle x_1\mathbf{a}_1 + \cdots + x_{24}\mathbf{a}_{24},\ x_1\mathbf{a}_1 + \cdots + x_{24}\mathbf{a}_{24} \rangle \\ &= \sum_{i,j} x_i x_j \langle \mathbf{a}_i, \mathbf{a}_j \rangle \\ &= \sum_{i=1}^{24} x_i^2 \langle \mathbf{a}_i, \mathbf{a}_i \rangle + \sum_{i<j} 2x_i x_j \langle \mathbf{a}_i, \mathbf{a}_j \rangle \end{aligned}$$

が成り立つ. 上式の第 2 項は $\langle \mathbf{a}_i, \mathbf{a}_j \rangle$ が 8 の倍数であることから 16 の倍数である. 一方 $\langle \mathbf{a}_i, \mathbf{a}_i \rangle$ は $\mathbf{a}_i$ が $(2^8.0^{16})$ 型または $(-3^1.1^{23})$ 型のいずれの場合も 32 である. 従って $\langle \mathbf{x}, \mathbf{x} \rangle$ は 16 の倍数である. また $\mathbf{u} = (u_1, ..., u_{24}) \in \Lambda$ が

$$\langle \mathbf{u}, \mathbf{u} \rangle = u_1^2 + \cdots + u_{24}^2 = 16$$

をみたすとすると, u_i の中に 0 が含まれることになるので, すべての u_i は偶数である. ある i について $u_i = \pm 4$ となるならば, 第 i 成分以外はすべて 0 となり, $\sum_i u_i = \pm 4 \not\equiv 0 \pmod 8$ より矛盾が得られる. 従って u_i は 0 または ± 2 である. このときも $u_i \equiv 2 \pmod 4$ となる i が 4 個のみで, Leech lattice の条件(4.3) をみたさない. よって $\langle \mathbf{u}, \mathbf{u} \rangle = 16$ をみたすベクトル $\mathbf{u}$ は Λ に存在しない. 以上で (2) が示された.

最後に任意の $\mathbf{x} \in \Lambda$ に対して $\langle \mathbf{z}, \mathbf{x} \rangle \in 8\mathbb{Z}$ をみたす $\mathbf{z} = (z_1, \ldots, z_{24}) \in \mathbb{R}^{24}$ が Λ に含まれることを示す. $8\mathbf{e}_i \in \Lambda$ より

$$\langle \mathbf{z}, 8\mathbf{e}_i \rangle = 8z_i \in 8\mathbb{Z}$$

が成り立つ. 従って $z_i \in \mathbb{Z}$ が得られる. 次に $i \neq j$ として

$$\langle \mathbf{z}, 4\mathbf{e}_i - 4\mathbf{e}_j \rangle = 4(z_i - z_j) \in 8\mathbb{Z}$$

より $z_i \equiv z_l \pmod 2$ が得られるので定義 4.1 の(4.1) がみたされる. また

$$\langle \mathbf{z}, -4\mathbf{e}_1 + \mathbf{e}_\Omega \rangle = -4z_1 + \sum_i z_i \in 8\mathbb{Z}$$

より $\sum_i z_i \equiv 4z_1 \pmod 8$ が成り立つ. 従って(4.2) もみたされる.

さて, 必要ならば $\mathbf{z}$ を $\mathbf{z} - 4\mathbf{e}_1 + \mathbf{e}_\Omega$ で置き換えることにより $\mathbf{z}$ の成分は偶数であるとしてよい. ここで

$$D = \{i \mid z_i \equiv 2 \pmod 4\} \notin \Gamma$$

と仮定すると, 定理 2.27 より $|C \cap D|$ が奇数となる octad C が存在する. このとき

$$\langle \mathbf{z}, 2\mathbf{e}_C \rangle \equiv \sum_{i \in C \cap D} 2z_i \equiv \sum_{i \in C \cap D} 4 \equiv 4|C \cap D| \equiv 4 \pmod 8$$

より $\langle \mathbf{z}, 2\mathbf{e}_C \rangle \notin 8\mathbb{Z}$ となり仮定に反する. よって $D \in \Gamma$ が成り立ち, (4.3) もみたされるので $\mathbf{z} \in \Lambda$ が示された. ∎

以下 $n = 2, 3, 4$ に対して Λ_n を次のように定める.

$$\Lambda_2 = \left\{\mathbf{x} \in \Lambda \;\middle|\; \|\mathbf{x}\| = 32\right\}, \quad \Lambda_3 = \left\{\mathbf{x} \in \Lambda \;\middle|\; \|\mathbf{x}\| = 48\right\}, \quad \Lambda_4 = \left\{\mathbf{x} \in \Lambda \;\middle|\; \|\mathbf{x}\| = 64\right\}$$

Λ_n のベクトル $\mathbf{x} = (x_1, \ldots, x_{24})$ は $\sum_{i=1}^{24} {x_i}^2 = 16n$ をみたす. Λ_n に属するベクトル $\mathbf{x}$ に対して $(|x_1|, \ldots, |x_{24}|)$ の型を絶対値型ということにし, まずこれを決定する. なお絶対値型は便宜上大きい順に並べることにする. 以下 $\max\{|x_i|\} = |x_m|$ とおく.

Λ_2 のベクトル $\mathbf{x} = (x_1, \ldots, x_{24})$ は $\sum_{i=1}^{24} {x_i}^2 = 32$ をみたす. 従って $|x_i| < 6$ が得られる.

$|x_m| = 5$ のときは $\sum_{i \neq m} {x_i}^2 = 7$ となり, ある x_i が 0 となる. 従って, この場合(4.1) をみたさない.

$|x_m| = 4$ のときは $\sum_{i \neq m} {x_i}^2 = 16$ となる. この場合 $(4^2.0^{22})$ 型, $(-4^1.4^1.0^{22})$ 型, $(-4^2.0^{22})$ 型ベクトルなど, 絶対値型が $(4^2.0^{22})$ となるものに 3 条件(4.1), (4.2), (4.3) をみたすベクトルがある. 一方, 成分に ± 2 が現れる絶対値型が $(4^1.2^4.0^{19})$ であるベクトルは(4.3) をみたさない.

$|x_m| = 3$ のときは $\sum_{i \neq m} {x_i}^2 = 23$ となる. x_m のほかに ± 3 を成分に持てば, ある x_i が 0 となり(4.1) をみたさない. 従って絶対値型が $(3^1.1^{23})$ となるが, 実際 $(-3^1.1^{23})$ 型ベクトルなどが 3 条件をみたす.

$|x_m| = 2$ のときは絶対値型が $(2^8.0^{16})$ となるベクトルで 3 条件をみたすものがある.

以上から Λ_2 のベクトルの絶対値型は $(2^8.0^{16})$, $(3^1.1^{23})$, $(4^2.0^{22})$ のいずれかである. Λ_3, Λ_4 も同様にしてベクトルの絶対値型が決定できる (詳細略).

補題 4.6

(1) Λ_2 のベクトルの絶対値型は $(2^8.0^{16})$, $(3^1.1^{23})$, $(4^2.0^{22})$ である.

(2) Λ_3 のベクトルの絶対値型は $(2^{12}.0^{12})$, $(3^3.1^{21})$, $(4^1.2^8.0^{15})$, $(5^1.1^{23})$ である.

(3) Λ_4 のベクトルの絶対値型は次のいずれかである.

$$(2^{16}.0^8), (3^5.1^{19}), (4^4.0^{20}), (4^2.2^8.0^{14}), (4^1.2^{12}.0^{11}), (5^1.3^2.1^{21}), (6^1.2^7.0^{16}), (8^1.0^{23})$$

以下, 絶対値型が $(2^8.0^{16})$ であるベクトル全体のなす集合を Λ_2^2, $(2^{12}.0^{12})$ であるベクトル全体のなす集合を Λ_3^2 と表す. 一般に Λ_n のベクトルで, 絶対値型の最初の数が k であるもの全体のなす集合を Λ_n^k と表すことにする. ただし $(4^4.0^{20})$ 型のベクトル全体のなす集合は $\Lambda_4^{4^4}$ と, $(4^2.2^8.0^{14})$ 型のベクトル全体のなす集合は $\Lambda_4^{4^2}$ と, $(4^1.2^{12}.0^{11})$ 型のベクトル全体のなす集合は $\Lambda_4^{4^1}$ と表すことにする.

次に集合 Λ_n^k の size を求めることにする. Λ_2^2 のベクトルの絶対値型は $(2^8.0^{16})$ である. 実際 $\{i \mid x_i = 2\}$ が octad である $(2^8.0^{16})$ 型のベクトル $\mathbf{x}$ は Λ_2^2 に含まれる. ここで成分の 2 を -2 に置き換えても(4.1), (4.3) はみたされる. (4.2) をみたすためには偶数個の 2 を -2 に置き換えればよい. 8 点集合の偶数個の元からなる部分集合は 2^7 個 あり, octad が 759 個であるから $|\Lambda_2^2| = 759 \cdot 2^7$ が得られる.

Λ_3^4 は絶対値型が $(4^1.2^8.0^{15})$ のベクトルのなす集合であり, 実際 $\{i \mid x_i \equiv 2 \pmod 4\}$ が octad である $(4^1.-2^1.2^7.0^{15})$ 型のベクトル $\mathbf{x}$ は Λ_3^4 に含まれる. -2 は奇数個あればよい. 4 は octad 外のどの位置にあってもよく, -4 に置き換えてもよい. 従って

$$|\Lambda_3^4| = 759 \cdot 16 \cdot 2 \cdot 2^{7\cdot} = 759 \cdot 2^{12}$$

が成り立つ. その他の場合も同様の計算をすることにより, 次の補題が得られる (計算略).

補題 4.7 Λ_n および Λ_n^k の *size* は次のようになる.

$\lvert\Lambda_2\rvert = 196560,$	$\lvert\Lambda_3\rvert = 16773120,$	$\lvert\Lambda_4\rvert = 398034000$	
$\lvert\Lambda_2^2\rvert = 759 \cdot 2^7,$	$\lvert\Lambda_2^3\rvert = 24 \cdot 2^{12},$	$\lvert\Lambda_2^4\rvert = \binom{24}{2} \cdot 2^2$	
$\lvert\Lambda_3^2\rvert = 2576 \cdot 2^{11},$	$\lvert\Lambda_3^3\rvert = \binom{24}{3} \cdot 2^{12},$	$\lvert\Lambda_3^4\rvert = 759 \cdot 2^{12},$	$\lvert\Lambda_3^5\rvert = 24 \cdot 2^{12}$
$\lvert\Lambda_4^2\rvert = 759 \cdot 2^{15},$	$\lvert\Lambda_4^3\rvert = \binom{24}{5} \cdot 2^{12},$	$\lvert\Lambda_4^{4^4}\rvert = \binom{24}{4} \cdot 2^4,$	$\lvert\Lambda_4^{4^2}\rvert = 759 \cdot \binom{16}{2} \cdot 2^9$
$\lvert\Lambda_4^{4^1}\rvert = 2576 \cdot 12 \cdot 2^{12},$	$\lvert\Lambda_4^5\rvert = 759 \cdot 2^{15},$	$\lvert\Lambda_4^6\rvert = 759 \cdot 2^{10},$	$\lvert\Lambda_4^8\rvert = 24 \cdot 2$

ここで Λ_2 のベクトルに対応する $\mathbb{R}^{24}$ の点は原点からの距離が $4\sqrt{2}$ である. これらの点を中心とする半径 $2\sqrt{2}$ の球は原点を中心とする半径 $2\sqrt{2}$ の球に接する. その個数 196560 は 24 次元空間において, 1 つの球に接する同一半径の球の最大個数 (kissing number) であることが知られている ([4, §7.4]).

さて $2\Lambda = \{2\mathbf{x} \mid \mathbf{x} \in \Lambda\}$ とおくと, 2Λ は Λ の部分加群である. Λ は階数が 24 の自由加群であるから $\underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{24\text{ 個}}$ と同型であり, 2Λ はその部分群 $\underbrace{2\mathbb{Z} \times \cdots \times 2\mathbb{Z}}_{24\text{ 個}}$ に同型である. 従って

$$\Lambda/2\Lambda \simeq (\mathbb{Z} \times \cdots \times \mathbb{Z})/(2\mathbb{Z} \times \cdots \times 2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$$

となるので $\Lambda/2\Lambda$ は位数が 2^{24} の基本アーベル 2-群である. ここで

$$L_8 = \big\{\mathbf{x} \in \Lambda \;\big|\; \|\mathbf{x}\| \leq 64\big\} = \{\mathbf{0}\} \cup \Lambda_2 \cup \Lambda_3 \cup \Lambda_4$$

とおき $\Lambda/2\Lambda$ の各剰余類に含まれる L_8 の元について調べることにする. 2Λ の $\mathbf{0}$ と異なるベクトル $2\mathbf{x}$ について $\|2\mathbf{x}\| = 4\|\mathbf{x}\| \geq 128$ となることから $L_8 \cap 2\Lambda = \{\mathbf{0}\}$ が成り立つ. また $\mathbf{x} - (-\mathbf{x}) = 2\mathbf{x} \in 2\Lambda$ より $\mathbf{x}$ と $-\mathbf{x}$ は同じ剰余類に含まれる. 以下 $L_8 - \{\mathbf{0}\}$ をペア $\{\pm\mathbf{x}\}$ に分割しておく. 今, ある剰余類に 2 つの異なるペア $\{\pm\mathbf{x}\}$ と $\{\pm\mathbf{y}\}$ が含まれたとする. 必要ならば $\mathbf{y}$ を $-\mathbf{y}$ で置き換えることにより $\langle\mathbf{x}, \mathbf{y}\rangle \geq 0$ であるとしてよい. $\mathbf{x} - \mathbf{y} \in 2\Lambda$ より $\mathbf{x} - \mathbf{y} = 2\mathbf{z}$ となる $\mathbf{z} \in \Lambda$ が存在するので, $\mathbf{z} \neq \mathbf{0}$ に注意すれば

$$128 \leq 4\|\mathbf{z}\| = \|2\mathbf{z}\| = \|\mathbf{x} - \mathbf{y}\| = \|\mathbf{x}\| + \|\mathbf{y}\| - 2\langle\mathbf{x}, \mathbf{y}\rangle \leq 128$$

より $\|\mathbf{x}\| = \|\mathbf{y}\| = 64$, $\langle\mathbf{x}, \mathbf{y}\rangle = 0$ が得られる. これより $\Lambda_2 \cup \Lambda_3$ に含まれるペアは互いに異なる剰余類に属し, 同じ剰余類に含まれる異なるペアは直交する Λ_4 のペアである. 一方, 互いに直交する $\mathbf{0}$ でないベクトルの集合は 1 次独立であるから, 同じ剰余類に属するペアは 24 個以下である. 補題 4.7 から

$$\big|\,\Lambda/2\Lambda\,\big| \geq 1 + \frac{|\Lambda_2|}{2} + \frac{|\Lambda_3|}{2} + \frac{|\Lambda_4|}{48} \geq 2^{24}$$

を得るが $|\Lambda/2\Lambda| = 2^{24}$ より

$$\big|\,\Lambda/2\Lambda\,\big| = 1 + \frac{|\Lambda_2|}{2} + \frac{|\Lambda_3|}{2} + \frac{|\Lambda_4|}{48}$$

が成り立つ. 従って $\Lambda/2\Lambda$ の 2Λ 以外の各剰余類には L_8 の元が含まれ, それらは $\Lambda_2 \cup \Lambda_3$ に含まれるペアであるか, 互いに直交する Λ_4 に含まれる 24 個のペアである. 以上をまとめて次の定理を得る.

定理 4.8 $\Lambda/2\Lambda$ の剰余類について次のいずれかがなり立つ.

(1) $\mathbf{0}$ を含む.

(2) $\Lambda_2 \cup \Lambda_3$ に含まれるペアを 1 つ含む.

(3) 互いに直交する Λ_4 に含まれる 24 個のペアを含む.

以下において, 互いに直交する Λ_4 に含まれる 24 個のペアを含む剰余類全体を $\Lambda_4/2\Lambda$ と表すことにする.

4.2 Monomial group

24 次直交変換群 (p.10)

$$O(24) = \{\, U \in M(24,\mathbb{R}) \,\big|\, U \cdot {}^tU = E \,\}$$

の元 U は $\mathbb{R}^{24}$ に次のように作用するものとする.

$$U \,:\, \mathbb{R}^{24} \ni (x_1, ..., x_{24}) \longmapsto (x_1, ..., x_{24})\, U \in \mathbb{R}^{24}$$

$D \subseteq \Omega$ に対して $\mathbf{e}_i^{\varepsilon_D} = \begin{cases} -\mathbf{e}_i, & i \in D \\ \mathbf{e}_i, & i \notin D \end{cases}$ で定まる線型変換 ε_D は $O(24)$ に含まれ, $D_1, D_2 \subseteq \Omega$ に対して $\varepsilon_{D_1}\varepsilon_{D_2} = \varepsilon_{D_1+D_2}$ が成り立つ. また $\pi \in M_{24}$ に対して $\mathbf{e}_i^{\sigma_\pi} = \mathbf{e}_{i^\pi}$ で定まる線型変換 σ_π も $O(24)$ に含まれ, 写像

$$M_{24} \ni \pi \longmapsto \sigma_\pi \in O(24)$$

は単射準同型となる. 以下, その像を M_{24} と同一視し, σ_π を π, $\mathbf{e}_i^{\sigma_\pi} = \mathbf{e}_i^{\pi}$ と表すことにする.

補題 4.9 $D \in \Gamma$ ならば $\Lambda^{\varepsilon_D} = \Lambda$ である. また $\pi \in M_{24}$ ならば $\Lambda^{\pi} = \Lambda$ である

Proof　まず $D \in \Gamma$ のときに $\Lambda^{\varepsilon_D} = \Lambda$ が成り立つことを示す. 上で注意したように $D_1, D_2 \subseteq \Gamma$ に対して $\varepsilon_{D_1}\varepsilon_{D_2} = \varepsilon_{D_1+D_2}$ が成り立つ. 従って $C \in \mathbb{O}$ に対して $\Lambda^{\varepsilon_C} = \Lambda$ が成り立つことを示せばよい. また補題 4.4 より Λ は $(2^8.0^{16})$ 型および $(-3^1.1^{23})$ 型のベクトルで生成される. 従って, これらのベクトルの ε_C による像が Λ に含まれることを示せば $(\varepsilon_C)^2 = 1$ より

$$\Lambda^{\varepsilon_C} \subseteq \Lambda \quad\Longrightarrow\quad (\Lambda^{\varepsilon_C})^{\varepsilon_C} \subseteq (\Lambda)^{\varepsilon_C} \quad\Longrightarrow\quad \Lambda \subseteq \Lambda^{\varepsilon_C}$$

となり $\Lambda = \Lambda^{\varepsilon_C}$ が得られる.

$\mathbf{x} = (x_1, \ldots, x_{24})$ が $(2^8.0^{16})$ 型のとき $\mathbf{x}^{\varepsilon_C} = (x'_1, \ldots, x'_{24})$ は明らかに(4.1) をみたす. また $2 \equiv -2 \pmod 4$ に注意すれば(4.3) も成り立つ. 一方

$$D = \{i \mid x_i \equiv 2 \pmod 4\}, \qquad |D \cap C| = r$$

とおくと, r は偶数である. ここで $x_i \equiv 0 \pmod 4$ のとき $-x_i \equiv x_i \pmod 8$ であり, $x_i \equiv 2 \pmod 4$ のとき $-x_i \equiv x_i + 4 \pmod 8$ であることに注意すれば

$$\sum_{i=1}^{24} x_i' \equiv 4r + \sum_{i=1}^{24} x_i \equiv \sum_{i=1}^{24} x_i \equiv 0 \pmod 8$$

を得る. 従って(4.2) もみたされるので $\mathbf{x}^{\varepsilon_C} \in \Lambda$ が示された.

次に $\mathbf{x} = (x_1, \ldots, x_{24})$ が $(-3^1.1^{23})$ 型とする. このときも $\mathbf{x}^{\varepsilon_C}$ は明らかに(4.1) をみたす. また $-1 \equiv 3, -3 \equiv 1 \pmod 4$ より

$$\{i \mid x_i' \equiv 3 \pmod 4\} = C \in \Gamma$$

となるので(4.3) も成り立つ. また $-x_i \equiv x_i + 6 \pmod 8$ であることに注意すれば

$$\sum_{i=1}^{24} x_i' \equiv \sum_{i=1}^{24} x_i + 6 \cdot 8 \equiv 4 \pmod 8$$

を得る. 従って(4.2) もみたされるので $\mathbf{x}^{\varepsilon_C} \in \Lambda$ が成り立つ. よって $\Lambda^{\varepsilon_C} = \Lambda$ が示された.

さて $\pi \in M_{24}$ とする. π は座標を置換する変換であるから $\mathbf{x} \in \Lambda$ が $(2^8.0^{16})$ 型のとき $\mathbf{x}^\pi$ も $(2^8.0^{16})$ 型である. また π は $\mathbb{O}$ を不変にするので

$$\{i \mid x_i = 2\} \in \mathbb{O} \quad \Longrightarrow \quad \{i \mid x_i = 2\}^\pi \in \mathbb{O}$$

より $\mathbf{x}^\pi \in \Lambda$ が導かれる. $\mathbf{x} \in \Lambda$ が $(-3^1.1^{23})$ 型のときも $\mathbf{x}^\pi$ は $(-3^1.1^{23})$ 型となり, -3 はどの位置にあっても(4.3) がみたされるので $\mathbf{x}^\pi \in \Lambda$ が成り立つ. よって $\Lambda^\pi = \Lambda$ が示された. ∎

$D_1, D_2 \in \Gamma$ に対して $\varepsilon_{D_1}\varepsilon_{D_2} = \varepsilon_{D_1+D_2}$ が成り立つことから $\langle \varepsilon_D \mid D \in \Gamma \rangle$ は Binary Golay Code と同型になる. 従って, 位数 2^{12} の基本アーベル群である. 以下 $\langle \varepsilon_D \mid D \in \Gamma \rangle$ を 2^{12} と表す. また ε_Ω はすべての成分を -1 倍するので, 以下, 単に -1 と表す.

定義 4.10 $M_o = \langle \varepsilon_D, \pi \mid D \in \Gamma, \pi \in M_{24} \rangle$ とおき, M_o を *Monomial group* という.

M_o の元は単項行列 (monomial matrix), すなわち各行各列に 0 でない成分が 1 つある行列である. 任意の $D \in \Gamma, \pi \in M_{24}$ に対して

$$\varepsilon_D{}^\pi = \varepsilon_{D^\pi} \tag{4.4}$$

が成り立つ. これより $2^{12} \lhd M_o$ が成り立つ. また $2^{12} \cap M_{24} = 1$ であるので M_o は 2^{12} と M_{24} の半直積 $2^{12}.M_{24}$ である.

さて Ω の任意の点 a を含む octad を 1 つ選び C とする. C の a と異なる 2 点 b, c に対して $D \cap C = \{a, b\}$, $E \cap C = \{a, c\}$ をみたす octad D, E が存在する. このとき $C \cap D \cap E = \{a\}$ となることから $M_{24} \ni \pi$ が C, D, E を固定すれば $a^\pi = a$ が成り立つ. これよりすべての octad を固定する M_{24} の元は単位元に限ることがわかる. 一方 2^{12} のすべての元と可換な M_{24} の元は(4.4) よりすべての $D \in \Gamma$ を固定することになり, 単位元に限る. 従って $C_{M_o}(2^{12}) \cap M_{24} = 1$ が得られる. ここで 2^{12} がアーベル群であることより,

$$C_{M_o}(2^{12}) = 2^{12}.\left(C_{M_o}(2^{12}) \cap M_{24}\right) = 2^{12}$$

が成り立つ.

補題 4.11 $C_{M_o}(2^{12}) = 2^{12}$ が成り立つ.

M_{24} の位数 23 の元 σ は Ω 上 23-cycle であり, $\emptyset$, Ω 以外の Γ の元を固定しないので $C_{2^{12}}(\sigma) = \{1, -1\}$ が成り立つ. これより σ を (共役をとる操作で) 2^{12} に作用させると size 1 の軌道が 2 個で, それ以外の軌道は size 23 である. 従って 2^{12} の位数 2^n の部分群 V が $V^\sigma = V$ をみたせば $2^n \equiv 1$ または 2 (mod 23) が成り立ち, $n = 0, 1, 11, 12$ を得る. $n = 0, 1, 12$ のとき V はそれぞれ 1, $\langle -1 \rangle$, 2^{12} である.

定理 4.12 M_o の正規部分群は M_o, 2^{12}, $\langle -1 \rangle$, 1 のみである.

Proof M_o, 2^{12}, 1 は M_o の正規部分群である. また任意の $\pi \in M_{24}$ に対して

$$(-1)^\pi = (\varepsilon_\Omega)^\pi = \varepsilon_{\Omega^\pi} = \varepsilon_\Omega = -1$$

より $\langle -1 \rangle \lhd M_o$ も成り立つ.

次に M_o の正規部分群 M で $M \leq 2^{12}$ かつ $M \neq 2^{12}, \langle -1 \rangle, 1$ であるものが存在したと仮定する. このとき上述のことから $|M| = 2^{11}$ が成り立つ. 一方 p.42 で示したように dodecad は 2576 個あり

$$2576 + 2^{11} > 2^{12}$$

であるから, ある dodecad D に対して $\varepsilon_D \in M$ が成り立つ. このとき, 系 3.20 と (4.4) より, 任意の dodecad E に対して $\varepsilon_E \in M$ が成り立ち, $\Gamma = \langle \mathbb{D} \rangle$ であるから $M = 2^{12}$ となり矛盾が生じる. 従って M_o の正規部分群 M で 2^{12} に含まれるのは 2^{12}, $\langle -1 \rangle$, 1 に限る.

$1 \neq M \lhd M_o$, $M \not\leq 2^{12}$ をみたす部分群 M が存在したと仮定すると $2^{12}M/2^{12}$ は単純群 $M_o/2^{12} \simeq M_{24}$ の正規部分群 $(\neq 1)$ であるから $2^{12}M = M_o$ が成り立つ. $2^{12} \leq M$ ならば $M = M_o$ である. $2^{12} \not\leq M$ とすると前述の結果から $2^{12} \cap M = 1$ または $2^{12} \cap M = \langle -1 \rangle$ が成り立つ. $2^{12} \cap M = 1$ のときは $M \leq C_{M_o}(2^{12})$ となり, 補題 4.11 より $C_{M_o}(2^{12}) = 2^{12}$ であることに矛盾する. 従って $2^{12} \cap M = \langle -1 \rangle$ が成り立つ. このとき

$$[M, 2^{12}] \leq M \cap 2^{12} = \langle -1 \rangle$$

となり, M の元による内部自己同型は $2^{12}/\langle -1 \rangle$ のすべての剰余類を固定する. $M/\langle -1 \rangle \simeq M_{24}$ より M は位数 23 の元 σ を含むが, σ は 2^{12} のすべての元を固定することになる. これは $C_{M_o}(2^{12}) = 2^{12}$ に矛盾する. よって $2^{12} \not\leq M$ は起こり得ず $M \not\leq 2^{12}$ のとき $M = M_o$ となる. 以上で定理が証明された. ∎

定理 4.13 $\sigma \in O(24)$ が $\Lambda^\sigma = \Lambda$ かつ $\mathbf{e}_i{}^\sigma = \mathbf{e}_j$ をみたすならば $\sigma \in M_o$ が成り立つ.

Proof $\sigma \in O(24)$ が $\Lambda^\sigma = \Lambda$ かつ $\mathbf{e}_i{}^\sigma = \mathbf{e}_j$ をみたすとする. $1^\rho = i$, $j^\tau = 1$ となる ρ, $\tau \in M_{24}$ を用いて $\sigma_0 = \rho\sigma\tau$ とおくと $\mathbf{e}_1{}^{\sigma_0} = \mathbf{e}_1$ が成り立つ. ここで $\sigma_0 \in M_o$ を示せば, $M_{24} \leq M_o$ より $\sigma \in M_o$ が得られる.

以下 σ_o を改めて σ とおき $\sigma \in M_o$ を示すことにする.

$$\sigma = \begin{bmatrix} x_{11} & x_{12} & x_{13} & \cdots & x_{1,24} \\ x_{21} & y_2 & y_3 & \cdots & y_{24} \\ x_{31} & z_2 & z_3 & \cdots & z_{24} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{24,1} & \cdot & \cdot & \cdots & \cdot \end{bmatrix}$$

とおくと $\mathbf{e}_1{}^\sigma = \mathbf{e}_1$ より

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \end{pmatrix} \begin{bmatrix} x_{11} & x_{12} & x_{13} & \cdots & x_{1,24} \\ x_{21} & y_2 & y_3 & \cdots & y_{24} \\ x_{31} & z_2 & z_3 & \cdots & z_{24} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{24,1} & \cdot & \cdot & \cdots & \cdot \end{bmatrix} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

が成り立つ. これより $(x_{11}, x_{12}, ..., x_{1,24}) = (1, 0, ..., 0)$ を得る. また $\sigma \in O(24)$ より σ の 1 行ベクトルが $2 \sim 24$ 行のベクトルと直交することから

$$\sigma = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & y_2 & y_3 & \cdots & y_{24} \\ 0 & z_2 & z_3 & \cdots & z_{24} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdot & \cdot & \cdots & \cdot \end{bmatrix}$$

が得られる. ここで

$$\sum_{i=2}^{24} {y_i}^2 = \sum_{i=2}^{24} {z_i}^2 = 1, \qquad \sum_{i=2}^{24} y_i z_i = 0$$

が成り立つことに注意されたい. さて第 1 成分が 4 である $(4^2.0^{22})$ 型のベクトルの σ による像は $(4, ...)$ と表されるが, 長さが $4\sqrt{2}$ であることから Λ_2 に含まれる. 従って補題 4.6 より第 1 成分が 4 である絶対値型が $(4^2.0^{22})$ のベクトルである. 従って $i \neq 1$ とすると, 適当な j により

$$(4\mathbf{e}_1 + 4\mathbf{e}_i)^\sigma = (4\mathbf{e}_1)^\sigma + (4\mathbf{e}_i)^\sigma = 4\mathbf{e}_1 \pm 4\mathbf{e}_j$$

と表される. これより任意の $i \neq 1$ に対して $\mathbf{e}_i^\sigma = \pm\mathbf{e}_j$ となる. よって σ は各行各列に ± 1 が 1 つある単項行列である. 従って $\sigma = \sigma_1\sigma_2$ と成分がすべて 1 である単項行列 (置換行列) σ_1 と成分が ± 1 である対角行列 σ_2 との積として表される. さて C を任意の octad とすると

$$\Lambda \ni 2\mathbf{e}_C \overset{\sigma}{\longmapsto} \mathbf{y} = (y_1, ..., y_{24}) \in \Lambda, \quad \{i \mid y_i \equiv 2 \pmod 4\} = C^{\sigma_1}$$

となる. これより C^{σ_1} は octad となる. C は任意であったから $\sigma_1 \in M_{24}$ が成り立つ. 一方

$$\sigma_2 = \begin{bmatrix} z_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & z_{24} \end{bmatrix}, \qquad D = \{i \mid z_i = -1\}$$

とおくと $\sum_{i=1}^{24} y_i \equiv 0 \pmod 8$ であるためには $|D \cap C^{\sigma_1}|$ が偶数でなければならない. C は任意の octad であったことから D と任意の octad との交わりが偶数個になる. 従って定理 2.27 より $D \in \Gamma$ を得る. ゆえに $\sigma_2 = \varepsilon_D \in M_o$ が成り立つ. 以上で $\sigma = \sigma_1\sigma_2 \in M_o$ が示された. ∎

定理 4.14 $\sigma \in O(24)$ が $\Lambda^\sigma = \Lambda$ かつ $(\Lambda_2^4)^\sigma = \Lambda_2^4$ をみたすならば $\sigma \in M_o$ である.

Proof　$\sigma \in O(24)$ が $\Lambda^\sigma = \Lambda$ かつ $(\Lambda_2^4)^\sigma = \Lambda_2^4$ をみたすとする. ここで

$$\mathbf{a} = (4, 4, 0, \ldots, 0), \quad \mathbf{b} = (4, -4, 0, \ldots, 0)$$

とおく. このとき $\mathbf{a}^\sigma$, $\mathbf{b}^\sigma$ は絶対値型が $(4^2.0^{22})$ のベクトルである. 従って適当な $\pi \in M_{24}$ と適当な octad C を選べば

$$\mathbf{a}^{\sigma\pi\varepsilon_C} = (4, 4, 0, \ldots, 0)^{\sigma\pi\varepsilon_C} = (4, 4, 0, \ldots, 0)$$

とすることができる. 例えば適当な $\pi \in M_{24}$ により $\mathbf{a}^{\sigma\pi} = (4, -4, 0, \ldots, 0)$ となった場合は 1 を含まず 2 を含む octad C を選べばよい. さて $\sigma\pi\varepsilon_C \in M_o$ を示せば $\sigma \in M_o$ が得られるので, 最初から $\mathbf{a}^\sigma = \mathbf{a}$ であるとしてよい. $\mathbf{a}$ と $\mathbf{b}$ は直交するので $\mathbf{b}^\sigma$ は $\mathbf{a}$ と直交する. 従って, 必要ならば σ を, 適当な M_{24} の元 π' と, 適当な octad C' による $\varepsilon_{C'}$ との積 $\sigma\pi'\varepsilon_{C'}$ で置き換えることにより, $\mathbf{b}^\sigma$ は次のいずれかの型のベクトルであるとしてよい.

$$\mathbf{b} = (4, -4, 0 \ldots, 0), \qquad -\mathbf{b} = (-4, 4, 0 \ldots, 0), \qquad (0, 0, 4, 4, \ldots, 0)$$

$\mathbf{b}^\sigma = \mathbf{b}$ のときは

$$(8\mathbf{e}_1)^\sigma = (\mathbf{a} + \mathbf{b})^\sigma = \mathbf{a}^\sigma + \mathbf{b}^\sigma = \mathbf{a} + \mathbf{b} = 8\mathbf{e}_1$$

となり $\mathbf{e}_1^\sigma = \mathbf{e}_1$ を得る. ゆえに定理 4.13 より $\sigma \in M_o$ が得られる. $\mathbf{b}^\sigma = -\mathbf{b}$ のときも同様に

$$(8\mathbf{e}_1)^\sigma = (\mathbf{a} + \mathbf{b})^\sigma = \mathbf{a}^\sigma + \mathbf{b}^\sigma = \mathbf{a} - \mathbf{b} = 8\mathbf{e}_2$$

より $\mathbf{e}_1^\sigma = \mathbf{e}_2$ が得られ, 定理 4.13 より $\sigma \in M_o$ が導かれる.

さて $\mathbf{b}^\sigma = (0, 0, 4, 4, \ldots, 0)$ と仮定する. $\mathbf{a}$, $\mathbf{b}$ と直交する絶対値型が $(4^2.0^{22})$ のベクトルの個数と $\mathbf{a}$, $\mathbf{b}^\sigma$ と直交する絶対値型が $(4^2.0^{22})$ のベクトルの個数とは一致する. ここで $\mathbf{a}$, $\mathbf{b}$ と直交する絶対値型が $(4^2.0^{22})$ のベクトルは ± 4 が第 3 成分以下にあるので, $4 \cdot \binom{22}{2} = 924$ 個ある. 一方 $\mathbf{a}$, $\mathbf{b}^\sigma$ と直交する絶対値型が $(4^2.0^{22})$ のベクトルは $4 + 4 \cdot \binom{20}{2} = 764$ 個で $764 \neq 924$ となり, 矛盾が生じる. よって $\mathbf{b}^\sigma = \pm\mathbf{b}$ となり, $\sigma \in M_o$ が成り立つ. ∎

M_o の元は座標の置換と ± 1 倍の操作の合成であるから, ベクトルの絶対値型を不変にする. 従って Λ_k^n は M_o により固定される.

補題 4.15 次の集合は M_o-*orbit*である.

$$\Lambda_2^2, \quad \Lambda_2^3, \quad \Lambda_2^4, \quad \Lambda_3^2, \quad \Lambda_3^3, \quad \Lambda_3^4, \quad \Lambda_3^5$$

Proof　Λ_k^n は M_o により固定されるので, M_o が Λ_k^n 上可移であることを示せばよい.

Λ_2^2 は絶対値型が $(2^8 0^{16})$ のベクトルの集合である. octad を 1 つ選び C とする. 任意の $\mathbf{x} \in \Lambda_2^2$ に対して $\sigma \in M_o$ が存在して $\mathbf{x}^\sigma = 2\mathbf{e}_C$ とできることを示せばよい.

$$\mathbf{x} = (x_1, \ldots, x_{24}), \qquad D = \{i \mid x_i \equiv 2 \pmod 4\}$$

とおく. このとき適当な $\pi \in M_{24}$ により $D^\pi = C$ とできる.

$$\mathbf{x}^\pi = \mathbf{y} = (y_1, \ldots, y_{24}), \quad E = \{i \mid y_i = -2\}$$

とおく. $|E \cap C| \leq 4$ のときは octad C' を $C' \cap C = E \cap C$ となるように選べば

$$\mathbf{x}^{\pi\varepsilon_{C'}} = \mathbf{y}^{\varepsilon_{C'}} = 2\mathbf{e}_C$$

が得られる. $|E \cap C| = 8$ のときは

$$\mathbf{x}^{\pi\varepsilon_C} = \mathbf{y}^{\varepsilon_C} = 2\mathbf{e}_C$$

が成り立つ. $|E \cap C| = 6$ のときは C との交わりが $C - E \cap C$ である octad F を選び, 得られる dodecad $D' = F + C$ から

$$\mathbf{x}^{\pi\varepsilon_{D'}} = \mathbf{y}^{\varepsilon_{D'}} = 2\mathbf{e}_C$$

が導かれる. 以上で M_o が Λ_2^2 上可移に作用することが示された.

次に, 任意の $\mathbf{x} \in \Lambda_2^3$ を $(-3, 1, \ldots, 1)$ に移す M_o の元が存在することを示す. $\mathbf{x}$ の ± 3 を第 1 成分になるように M_{24} の元で移す. 次に 1 を含む octad C から得られる ε_C を作用させれば $\mathbf{y} = (-3, y_2, \ldots, y_{24})$ なる形のベクトルに移すことができる. ここで

$$D = \{i \mid y_i \equiv 3 \pmod 4\} = \{i \mid y_i = -1\}$$

とおけば $D \in \Gamma$ より ε_D を作用させて $(-3, 1, \ldots, 1)$ に移すことができる. よって M_o は Λ_2^3 上可移である.

Λ_2^4 については定理 4.14 の証明中でも述べたように絶対値型が $(4^2.0^{22})$ である任意のベクトルを $(4,4,0,\dots,0)$ に移す M_o の元が存在する. 従って M_o は Λ_2^4 上可移である.

Λ_3^2 は絶対値型が $(2^{12}0^{12})$ のベクトルのなす集合である. dodecad を 1 つ選び D とする. 任意の $\mathbf{x} \in \Lambda_3^2$ が M_o の元によって $2\mathbf{e}_D$ に移されることを示せばよい.

$$\mathbf{x} = (x_1, \dots, x_{24}), \qquad E = \{i \mid x_i \equiv 2 \pmod 4\}$$

とおくと E は dodecad である. 系 3.20 より $E^\pi = D$ となる $\pi \in M_{24}$ が存在する. ここで

$$\mathbf{x}^\pi = \mathbf{y} = (y_1, \dots, y_{24}), \qquad F = \{i \mid y_i = -2\}$$

とおき, 必要ならば ε_D を作用させることにより $|F| = 0, 2, 4, 6$ であるとしてよい. $|F| = 0$ ならば $\mathbf{x}^\pi = 2\mathbf{e}_D$ である. $|F| = 6$ で F が special のときは F を含む octad C_1 と, ある octad C_2 により $D = C_1 + C_2$ と表される. このとき ε_{C_1} を作用させると $2\mathbf{e}_D$ に移る. $|F| = 4$ のときは F を含む octad C_3 と, ある octad C_4 により $D = C_3 + C_4$ と表される. ここで F を含む sextet と C_4 の交わりが $[2^40^2]$ 型となることから D との交わりが F となる octad C が存在する. 従って ε_C を作用させて $2\mathbf{e}_D$ に移すことができる. $|F| = 2$ のときは $D = C_5 + C_6$, $F \subseteq C_5$ となる octad C_5, C_6 が存在する. ここで ε_{C_5} を作用させると $|F| = 4$ の場合に帰着される. $|F| = 6$ で F が non-special のときも D との交わりが F の 4 点である octad C を選び ε_C を作用させて $|F| = 2$ の場合に帰着させることができる. 以上で M_o が Λ_3^2 上可移であることが示された.

Λ_3^3 は 絶対値型が $(3^3.1^{21})$ のベクトルのなす集合である. 任意の $\mathbf{x} \in \Lambda_3^3$ が M_o の元により $\mathbf{a} = (-3,-3,-3,1,\dots,1)$ に移されることを示せばよい. M_{24} は Ω 上 5 重可移であるから適当な $\pi \in M_{24}$ により $\mathbf{x}$ の ± 3 を $1 \sim 3$ 成分に移すことができる. 更に, 表 2.1(p.30) からわかるように $1, 2, 3$ の “3 点を含む octad”, “2 点を含み, 他の 1 点を含まない octad”, “1 点を含み, 他の 2 点を含まない octad” が存在するから, そのような octad を C とすれば $\pi\varepsilon_C$ により $\mathbf{x}$ は

$$\mathbf{y} = (-3,-3,-3,\dots\dots)$$

に移される. ここで

$$\mathbf{y} = (y_1, \dots, y_{24}), \qquad D = \{i \mid y_i \equiv 3 \pmod 4\} = \{i \mid y_i = -1\}$$

とおけば $D \in \Gamma$ が成り立つ. 従って ε_D を作用させれば $\mathbf{a}$ に移すことができる. よって M_o は Λ_3^3 上可移である.

Λ_3^4 は 絶対値型が $(4^1.2^8.0^{15})$ のベクトルのなす集合である. octad を 1 つ選び C とする.

$$\mathbf{a} = 2\mathbf{e}_C - 4\mathbf{e}_r + 4\mathbf{e}_s = (a_1, \ldots, a_{24}), \quad r \in C,\ s \notin C$$

とおく. 任意の $\mathbf{x} \in \Lambda_3^4$ が M_o の元により $\mathbf{a}$ に移されることを示せばよい.

$$\mathbf{x} = (x_1, \ldots, x_{24}), \qquad D = \{i \mid x_i \equiv 2 \pmod 4\}$$

とおくと D は octad である. 従って $\pi \in M_{24}$ により $D^\pi = C$ とできる. ここで

$$\mathbf{x}^\pi = \mathbf{y} = (y_1, \ldots, y_{24}), \qquad E = \{i \mid y_i = -2\}$$

とおく. $|E|$ は奇数であるから $\{r\} + E$ は偶数個の元を含む. 従って前と同様に M_o の元の作用で $C - (\{r\} + E)$ の成分はそのままにして, $\{r\} + E$ の成分を -1 倍することができる. このとき $\mathbf{y}$ が $\mathbf{z} = (z_1, ..., z_{24})$ に移ったとすると

$$i \in C \quad \Longrightarrow \quad z_i = a_i$$

が成り立つ. 更に, $N(C)$ が $\Omega - C$ 上可移であるから $\mathbf{z}$ の s 成分が 4 であるようにできる. このとき $\mathbf{z} = \mathbf{a}$ となる. よって M_o は Λ_3^4 上可移である.

Λ_3^5 は 絶対値型が $(5^1.1^{23})$ のベクトルのなす集合である. $\mathbf{a} = (5, 1, \ldots, 1)$ とおく. 任意の $\mathbf{x} \in \Lambda_3^5$ が M_o の元により $\mathbf{a}$ に移されることを示せばよい. 適当な $\pi \in M_{24}$ により $\mathbf{x}^\pi$ の第 1 成分が ± 5 となるようにできる. また必要ならば 1 を含む octad を C として ε_C を作用させて $\mathbf{x}$ が

$$\mathbf{y} = (5, \ldots\ldots) = (y_1, \ldots, y_{24})$$

に移されたとしてよい. ここで $E = \{i \mid y_i \equiv 3 \pmod 4\}$ とおくと $E \in \Gamma$ であるから ε_E を作用させて $\mathbf{y}$ を $\mathbf{a}$ に移すことができる. よって M_o は Λ_3^5 上可移である. 以上で補題が証明された. ∎

定理 4.16 $\Lambda_4/2\Lambda$ の剰余類に含まれる直交基底から定まる正規直交基底を適当に選べば, その正規直交基底に関する Λ のベクトルの座標は定義 4.1 の 3 条件をみたす.

Proof　定理 4.8 より $\Lambda_4/2\Lambda$ の剰余類には $\mathbb{R}^{24}$ の直交基底が存在する. 今, その 1 つを $\mathbf{a}_1, \ldots, \mathbf{a}_{24}$ とし $\mathbf{u}_i = \frac{1}{8}\mathbf{a}_i$ と定めると $\mathbf{u}_1, \ldots, \mathbf{u}_{24}$ は正規直交基底である. 以下, 必要ならば $\mathbf{u}_1, \ldots, \mathbf{u}_{24}$ を置換し, また $\mathbf{u}_i$ を $-\mathbf{u}_i$ に置き換えることにより, Λ のベクトルの $\mathbf{u}_1, \ldots, \mathbf{u}_{24}$ に関する座標が定義 4.1 の 3 条件をみたすようにできることを示す. なお, この証明中, 座

標はすべて $\mathbf{u}_1, \ldots, \mathbf{u}_{24}$ に関する座標であるとし, ベクトルの型もこの座標に関するものとする.

$\mathbf{x} \in \Lambda$ の座標を $(x_1, \ldots, x_{24})$ とすると

$$\mathbf{x} = x_1\mathbf{u}_1 + \cdots + x_{24}\mathbf{u}_{24}\,, \qquad x_i = \langle \mathbf{x}, \mathbf{u}_i \rangle$$

であるが, 補題 4.5 より $\langle \mathbf{x}, \mathbf{a}_i \rangle$ は 8 の倍数である. 従って

$$x_i = \langle \mathbf{x}, \mathbf{u}_i \rangle = \langle \mathbf{x}, \tfrac{1}{8}\,\mathbf{a}_i \rangle = \frac{1}{8}\,\langle \mathbf{x}, \mathbf{a}_i \rangle \in \mathbb{Z}$$

が得られる. また $\pm\mathbf{a}_i$ $(1 \le i \le 24)$ が $\Lambda/2\Lambda$ の同じ剰余類に属することから $\mathbf{a}_i \pm \mathbf{a}_j \in 2\Lambda$ が成り立つ. これより $\mathbf{a}_i - \mathbf{a}_j = 2\mathbf{y}$ とおけば $\mathbf{y} \in \Lambda$ であることから

$$x_i - x_j = \langle \mathbf{x}, \mathbf{u}_i - \mathbf{u}_j \rangle = \frac{1}{8}\,\langle \mathbf{x}, \mathbf{a}_i - \mathbf{a}_j \rangle = 2\left(\frac{1}{8}\,\langle \mathbf{x}, \mathbf{y} \rangle\right) \in 2\mathbb{Z}$$

となる. よって $x_i \equiv x_j \pmod 2$ が得られ, (4.1) の成り立つことが示された.

座標が偶数である Λ のベクトルのなす集合を L_0 とおくと, 明らかに L_0 は Λ の部分加群である. ここで $\mathbf{x} \in L_0$ に対して

$$C_{\mathbf{x}} = \{i \mid x_i \equiv 2 \pmod 4\} \quad \text{とおき} \quad \Gamma' = \langle\, C_{\mathbf{x}} \mid \mathbf{x} \in L_0 \,\rangle \le P(\Omega)$$

と定める. $\mathbf{x}, \mathbf{y} \in L_0$ に対して $C_{\mathbf{x}+\mathbf{y}} = C_{\mathbf{x}} + C_{\mathbf{y}}$ が成り立つことから, 任意の $C \in \Gamma'$ に対して $C = C_{\mathbf{x}}$ となる $\mathbf{x} \in L_0$ が存在する. また $\mathbf{a}_i$, $\frac{1}{2}(\mathbf{a}_i \pm \mathbf{a}_j) \in \Lambda$ より, 座標の型が $(\pm 8^1.0^{23})$ および $(\pm 4. \pm 4.0^{22})$ であるベクトルが L_0 に存在する.

空でない $C \in \Gamma'$ を任意に選び, $\mathbf{x} \in L_0$ を $C = C_{\mathbf{x}}$ をみたすベクトルとする. また $|C| = n$ とおく. 座標の型が $(\pm 8^1.0^{23})$, $(\pm 4. \pm 4.0^{22})$ である L_0 のベクトルを $\mathbf{x}$ に適当に加減して得られる $\mathbf{y}$ について, $C = C_{\mathbf{y}}$ が成り立ち, $i \in C$ ならば $|y_i| = 2$, $i \notin C$ ならば $|y_i| = 0$ となるようにできる. 一方, 補題 4.5 より $32 \le \|\mathbf{y}\| = 4n$ となるので $n \ge 8$ が成り立つ. 従って

$$\mathbb{O}' = \left\{\, C \in \Gamma' \,\middle|\, |C| = 8 \,\right\}$$

とおくと 補題 2.1 より $\dim \Gamma' \le 12$, $|\mathbb{O}'| \le 759$ が成り立つ. 以下, Γ' が Binary Golay Code であることを示す.

上述のことから $\|\mathbf{x}\| = 32$ かつ $x_i \equiv 0 \pmod 2$ をみたすベクトル $\mathbf{x} = (x_1, \ldots, x_{24}) \in \Lambda$ の絶対値型は $(2^8.0^{16})$ または $(4^2.0^{22})$ である. $(4^2.0^{22})$ 型のベクトルの存在はすでに示し

た. それらは $4\cdot\binom{24}{2}$ 個ある. 一方 $(2^8.0^{16})$ 型のベクトルの総数は $759\cdot 2^8$ 以下である. これら以外に $\|\mathbf{x}\|=32$ となるベクトルが存在しないとすると

$$4\cdot\binom{24}{2}+759\cdot 2^8=195408<196560$$

となり補題 4.7 に矛盾する. 従って Λ に $\|\mathbf{x}\|=32$ かつ $x_i\equiv 1 \pmod 2$ となるベクトルが存在する. このようなベクトル $\mathbf{x}$ の絶対値型は $(3^1.1^{23})$ である.

さて, 必要ならば適当に $\mathbf{u}_i$ を $-\mathbf{u}_i$ に置き換えて, Λ に (-3.1^{23}) 型のベクトル $\mathbf{a}$ が存在するとしてよい. ベクトル $\mathbf{x}$ の絶対値型が $(3^1.1^{23})$ であるとし, $C_{\mathbf{x}}=\{i\mid x_i\equiv 1 \pmod 4\}$ とおくと $\mathbf{x}+\mathbf{a}\in L_0$ より $C_{\mathbf{x}}=C_{\mathbf{x}+\mathbf{a}}\in\Gamma'$ を得る. 逆に $D=C_{\mathbf{x}}\in\Gamma'$ となる, 絶対値型が $(3^1.1^{23})$ である $\mathbf{x}$ は, $i\in D$ のとき $y_i=1$, $i\notin D$ のとき $y_i=-1$ と定め, 更に, ある 1 を -3 で置き換えるか, ある -1 を 3 で置き換えることにより得られる. ここで D の選び方は高々 $|\Gamma'|$ 通り, ± 3 に置き換えるのは 24 通りであるから, 絶対値型が $(3^1.1^{23})$ であるベクトルの個数は高々 $24\cdot|\Gamma'|$ 個である.

また Λ に (-3.1^{23}) 型のベクトル $\mathbf{a}$ が存在することと補題 4.5 より, $(2^8.0^{16})$ 型のベクトルで座標に -2 を奇数個含むものは存在しない. よって $(2^8.0^{16})$ 型のベクトルは高々 $759\cdot 2^7$ 個である. $|\Gamma'|\le 2^{12}$ より $\|\mathbf{x}\|=32$ となるベクトルの個数は

$$24\cdot 2^{12}+4\cdot\binom{24}{2}+759\cdot 2^7=196560$$

以下となるが, 補題 4.7 より $\|\mathbf{x}\|=32$ となるベクトルの個数は 196560 個存在する. 従って $(3^1.1^{23})$ 型のベクトルが $24\cdot 2^{12}$ 個存在することになり, $|\Gamma'|=2^{12}$ が得られ $\dim\Gamma'=12$ が成り立つ. これより Γ' は Binary Golay Code で, $(\Omega,\mathbb{O}')$ は S(5,8,24) である. 定理 2.32 より $\sigma\in S_{24}$ で $\mathbb{O}^\sigma=\mathbb{O}'$ をみたすものがある. このとき $\mathbf{u}_{1^\sigma},\dots,\mathbf{u}_{24^\sigma}$ と正規直交基底を置換すれば (4.1), (4.3) が成り立つ.

さて絶対値型が $(2^8.0^{16})$ であるベクトルは -2 を座標に偶数個含み, (4.2) をみたす. また絶対値型が $(3^1.1^{23})$ であるベクトルも (4.2) をみたす. 補題 4.4 の証明と同様にして Λ は $(-3^1.1^{23})$ 型, $(2^8.0^{16})$ 型のベクトルで生成されることが示される. $(-3^1.1^{23})$ 型, $(2^8.0^{16})$ 型のベクトルが (4.2) をみたすので Λ の任意のベクトルが (4.2) をみたす. 以上で定理が証明された. ∎

4.3 Conway 群

Leech lattice Λ を不変にする $O(24)$ の元全体のなす部分群を $\cdot 0$ と表し, Conway 群という.

$$\cdot 0 = \{\sigma \in O(24) \mid \Lambda^\sigma = \Lambda\}$$

である. 補題 4.9 と定義 4.10 より $M_o \leq \cdot 0$ が成り立つ.

補題 4.17 $\cdot 0$ は $\Lambda_4/2\Lambda$ に可移に作用する.

Proof $\cdot 0$ が $\Lambda/2\Lambda$ に作用することは明らかである. またベクトルの長さを不変にするので $\Lambda_4/2\Lambda$ に作用する. 定理 4.16 より, $\Lambda_4/2\Lambda$ の剰余類から適当に正規直交基底 $\mathbf{u}_1, \ldots, \mathbf{u}_{24}$ を選べば, この基底に関する Λ のベクトルの座標が定義 4.1 の 3 条件をみたす. このとき $\mathbf{e}_i^\sigma = \mathbf{u}_i$ となる $\sigma \in O(24)$ を選ぶと Λ^σ は $\mathbf{u}_1, \ldots, \mathbf{u}_{24}$ に関する座標が定義 4.1 の 3 条件をみたすベクトル全体のなす集合であるから $\Lambda \leq \Lambda^\sigma$ が成り立つ. 一方, 定理 4.16 の証明中で示したように Λ は $(-3^1.1^{23})$ 型, および $(2^8.0^{16})$ 型のベクトルをすべて含み, Λ^σ がそれらで生成されることから $\Lambda = \Lambda^\sigma$ が得られ, $\sigma \in \cdot 0$ を得る. ゆえに正規直交基底 $\mathbf{e}_i$ を $\mathbf{u}_i$ に移す $\cdot 0$ の元が存在する. $\mathbf{u}_i$ は任意の剰余類から選べるから $\cdot 0$ は $\Lambda_4/2\Lambda$ に可移に作用する. ∎

定理 4.18 $|\cdot 0| = 2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$ である.

Proof 明らかに $\Lambda_4/2\Lambda$ の $8\mathbf{e}_i$ を含む剰余類を固定する $\cdot 0$ の部分群は M_o である. 従って

$$|\cdot 0| = \frac{|\Lambda_4|}{48} \cdot |M_o|$$

が成り立つ. 従って補題 4.7 と $|M_o| = 2^{12} \cdot |M_{24}|$ より

$$\begin{aligned} |\cdot 0| = \frac{|\Lambda_4|}{48} \cdot |M_o| &= \frac{398034000}{48} \cdot 2^{12} \cdot 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 3 \cdot 16 \\ &= 8315553613086720000 = 2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23 \end{aligned}$$

を得る. ∎

次に任意の 4 点集合 T から $\cdot 0$ の元 $\xi_T \notin M_o$ が定まることを示す. T を成分とする sextet を S として, まず η_S を

$$\mathbf{e}_j{}^{\eta_S} = \mathbf{e}_j - \frac{1}{2}\mathbf{e}_{U_j} \qquad (U_j \text{ は } j \text{ を含む } S \text{ の成分})$$

をみたす線型変換とする. このとき $\eta_S \in O(24)$ であることは容易に確かめられる. ここで $\xi_T = \eta_S\varepsilon_T$ とおくと $\xi_T \in O(24)$ かつ $\xi_T \notin M_o$ は明らかであるが, $\xi_T \in \cdot 0$ となることを示そう. 以下, $\mathbf{M}$ は T を第 1 列, S の T 以外の成分を $2 \sim 6$ 列とする M-行列の 1 つであるとする. このような M-行列がいくつか存在することに注意されたい.

C を octad として $(2^8.0^{16})$ 型のベクトル $\mathbf{x} = 2\mathbf{e}_C$ の ξ_T による像を考える. C と S との交わりが $[4^20^4]$ 型のとき $\mathbf{x}^{\eta_S}$ は $(-2^8.0^{16})$ 型のベクトルである. このとき $\mathbf{x}^{\xi_T}$ は $(-2^8.0^{16})$ 型, または $(-2^4.2^4.0^{16})$ 型のベクトル $\mathbf{y}$ となり, $\{i \mid y_i \equiv 2 \pmod 4\} = C$ より, Λ に含まれる. S との交わりが $[3^11^5]$ 型のとき $\mathbf{x}^{\eta_S}$ は $(-3^1.-1^{18}.1^5)$ 型のベクトルである. このとき $\mathbf{x}^{\xi_T}$ は $(3^1.1^8.-1^{15})$ 型, または $(-3^1.1^7.-1^{16})$ 型のベクトル $\mathbf{y}$ であり, $\{i \mid y_i \equiv 1 \pmod 4\}$ は $|C \cap S_1| = 3$ のとき C であり, $|C \cap S_i| = 3$ $(i \neq 1)$ のとき $C + \mathbf{M}(1i)$ である. ゆえに $\mathbf{x}^{\xi_T}$ は Λ に含まれる. S との交わりが $[2^40^2]$ 型のとき $\mathbf{x}^{\eta_S}$ は $(-2^8.0^{16})$ 型のベクトルである. このとき $\mathbf{x}^{\xi_T}$ は $(-2^8.0^{16})$ 型, または $(-2^6.2^2.0^{16})$ 型のベクトル $\mathbf{y}$ である. ここで $|C \cap S_i| = 2$ となる i を i_1, i_2, i_3, i_4 とおくと, $\{i \mid y_i \equiv 2 \pmod 4\}$ は $C + \mathbf{M}(i_1i_2) + \mathbf{M}(i_3i_4)$ となるので, $\mathbf{x}^{\xi_T} \in \Lambda$ を得る.

$\mathbf{x}$ が $(-3^1.1^{23})$ 型のベクトルのとき $\mathbf{x}^{\eta_S}$ は $(-3^1.1^3.-1^{20})$ 型のベクトルである. このとき $\mathbf{x}^{\xi_T}$ は $(3^1.-1^{23})$ 型, または $(-3^1.1^7.-1^{16})$ 型のベクトル $\mathbf{y}$ となり, $\{i \mid y_i \equiv 1 \pmod 4\}$ は $\emptyset$ または $\mathbf{M}(1j)$ となり Λ に含まれる. 従って $\mathbf{x}$ が $(-3^1.1^{23})$ 型のベクトルのとき $\mathbf{x}^{\xi_T} \in \Lambda$ が成り立つ.

以上の結果と補題 4.4 より $\Lambda^{\xi_T} \leq \Lambda$ が得られる. また $\Lambda_2^{\xi_T}$ は長さ $4\sqrt{2}$ のベクトルを 196560 個含むので Λ_2 に一致する. 一方 Λ^{ξ_T} は Λ_2 で生成される Λ の部分加群であるから Λ に一致する. ゆえに $\Lambda^{\xi_T} = \Lambda$ となるので $\xi_T \in \cdot 0$ が示された.

定理 4.19 $\cdot 0$ は Λ_2, Λ_3 に可移に作用する.

Proof $\cdot 0$ の元はベクトルの長さを変えないので Λ_2, Λ_3 を不変にする. 従って Λ_2, Λ_3 は $\cdot 0$-orbit に分割される. まず Λ_2 が $\cdot 0$-orbit であること, すなわち $\cdot 0$ が Λ_2 上可移であることを示す. 補題 4.15 より $\Lambda_2 = \Lambda_2^2 \cup \Lambda_2^3 \cup \Lambda_2^4$ は Λ_2 の M_o-orbit への分割である. 従って 3 つの軌道に属するベクトルが $\cdot 0$ の元で移りあうことを示せばよい.

C を octad として $\mathbf{x} = 2\mathbf{e}_C$ とおくと $\mathbf{x} \in \Lambda_2^2$ である. $|C \cap T| = 3$ となるように 4 点集合 T を選ぶと, 上で示したように $\mathbf{x}^{\xi_T} \in \Lambda_2^3$ が得られる. 従って Λ_2^2 と Λ_2^3 は同じ $\cdot 0$-orbit に含まれる. ここで

$$|\Lambda_2^2| + |\Lambda_2^3| = 759 \cdot 2^7 + 24 \cdot 2^{12} = 195456 = 2^7 \cdot 3 \cdot 509$$

は $|\cdot 0|$ を割り切らないので定理 1.3 より $\Lambda_2^2 \cup \Lambda_2^3$ は $\cdot 0$-orbit でない. よって $\Lambda_2^2 \cup \Lambda_2^3$ を含む $\cdot 0$-orbit は Λ_2 となる.

次に $\cdot 0$ が Λ_3 上可移であること, すなわち Λ_3 が $\cdot 0$-orbit であることを示す. 補題 4.15 より $\Lambda_3 = \Lambda_3^2 \cup \Lambda_3^3 \cup \Lambda_3^4 \cup \Lambda_3^5$ は Λ_3 の M_o-orbit への分割である. 従って 4 つの軌道に属するベクトルが $\cdot 0$ の元で移りあうことを示せばよい.

4 点集合 T から定まる sextet を $S = \{S_i \mid 1 \leq i \leq 6\}$ とおく. ただし $S_1 = T$ とする. S_i を i 列とする M-行列を $\mathbf{M}$, $D = \mathbf{M}(1) + \mathbf{M}(56)$ とおく. D は dodecad であり, $\mathbf{x} = 2\mathbf{e}_D$ とおくと $\mathbf{x} \in \Lambda_3^2$ である. このとき $\mathbf{x}^{\xi_T}$ は $(-3^2.3^1.1^6.-1^{15})$ 型のベクトルとなる. 従って $\mathbf{x}^{\xi_T} \in \Lambda_3^3$ が得られ, Λ_3^2 と Λ_3^3 は同じ $\cdot 0$-orbit に含まれる.

octad C を $1 \leq j \leq 4$ のとき $|C \cap S_j| = 2$ となるように選び, $i \in S_5$, $j \in S_1$ として $\mathbf{x} = 4\mathbf{e}_i - 4\mathbf{e}_j + 2\mathbf{e}_C$ とおく. $\mathbf{x} \in \Lambda_3^4$ である. このとき $\mathbf{x}^{\xi_T}$ は $(-2^{10}.2^2.0^{12})$ 型であるから $\mathbf{x}^{\xi_T} \in \Lambda_3^2$ が成り立つ. 従って Λ_3^2 と Λ_3^4 は同じ $\cdot 0$-orbit に含まれる.

$\mathbf{x} = 4\mathbf{e}_1 + \mathbf{e}_\Omega$ とおくと $\mathbf{x} \in \Lambda_3^5$ である. このとき $\mathbf{x}^{\xi_T}$ は $(3^3.-1^{21})$ 型であるから $\mathbf{x}^{\xi_T} \in \Lambda_3^3$ が成り立つ. 従って Λ_3^5 と Λ_3^3 は同じ $\cdot 0$-orbit に含まれる. 以上で $\cdot 0$ が Λ_3 上可移であることが示された. ∎

定義 4.20 $\cdot 0$ の Λ_2 への作用の 1 点の固定群を $\cdot 2$, Λ_3 への作用の 1 点の固定群を $\cdot 3$ とおく. また $\cdot 1 = \cdot 0/\langle -1 \rangle$ とおき, $\cdot 1, \cdot 2, \cdot 3$ を $\cdot 0$ とあわせて *Conway* 群と呼ぶ.

定理 4.19 より $\cdot 2, \cdot 3$ は固定点の選び方によらない. 以下 $\cdot 2$ の Λ_2 における固定点を $\mathbf{u}_2 = -4\mathbf{e}_1 + \mathbf{e}_\Omega$, $\cdot 3$ の Λ_3 における固定点を $\mathbf{u}_3 = 4\mathbf{e}_1 + \mathbf{e}_\Omega$ とする.

-1 が $\mathbf{u}_2, \mathbf{u}_3$ を固定しないことから $-1 \notin \cdot 2$ および $-1 \notin \cdot 3$ が成り立つ. また M_o の部分群 M_{24} の元で $\mathbf{e}_1$ を固定するもの全体を M_{23} と同一視すると, M_{23} が $\mathbf{u}_2, \mathbf{u}_3$ を固定するので $M_{23} < \cdot 2$, $M_{23} < \cdot 3$ が成り立つ. これらを補題として述べておく.

補題 4.21 $-1 \notin \cdot 2$ および $-1 \notin \cdot 3$ が成り立つ. また $M_{23} < \cdot 2$, $M_{23} < \cdot 3$ が成り立つ.

定理 4.18 と定理 4.19 から $|\cdot 0 : \cdot 2| = |\Lambda_2|$, $|\cdot 0 : \cdot 3| = |\Lambda_3|$ が成り立つので, 次の定理が得られる.

補題 4.22 $\cdot 1, \cdot 2, \cdot 3$ の位数は次のようになる.

$$|\cdot 1| = 2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$$
$$|\cdot 2| = 2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$$
$$|\cdot 3| = 2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$$

以下 M_o の部分群 M_{24} の元で $\mathbf{e}_1$ を固定する位数 23 の元を α とし, $A = \langle\alpha\rangle$ とおく. 補題 3.17 より $N_{M_{24}}(\langle\alpha\rangle) = \langle\alpha, \beta\rangle$ をみたす位数 11 の元 β が存在する. ここで $\mathbf{e}_1^{\beta} = \mathbf{e}_1$ であることを注意しておく.

補題 4.23 $G = \cdot 0$ とする. このとき次が成り立つ.

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

Proof $\sigma \in C_G(\alpha)$ を任意に選ぶ.

$$\alpha = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{bmatrix} \text{ と表されるので } \sigma = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \text{ とおくと}$$

$$\alpha\,\sigma = \sigma\,\alpha \quad \text{より} \quad \sigma = \begin{bmatrix} \pm 1 & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{bmatrix} \text{ が成り立つ.}$$

従って ${\mathbf{e}_1}^{\sigma} = \pm\mathbf{e}_1$ となるので定理 4.13 より $\sigma \in M_o$ または $(-1)\cdot\sigma \in M_o$ が成り立つが, $-1 \in M_o$ より, いずれの場合も $\sigma \in M_o$ が得られる.

$M_o = 2^{12}.M_{24}$ であるから $\sigma = ab$ $(a \in 2^{12}, b \in M_{24})$ と一意的に表される. ここで

$$\sigma^{\alpha} = \sigma \implies a^{\alpha} = a\,,\ b^{\alpha} = b \implies a\alpha = \alpha a\,,\ b\alpha = \alpha b$$

となることから $\sigma \in C_{2^{12}}(\alpha).C_{M_{24}}(\alpha)$ より $C_G(\alpha) = C_{2^{12}}(\alpha).C_{M_{24}}(\alpha)$ が導かれる. 補題 3.15 より $C_{M_{24}}(\alpha) = A$ である. また任意の $\varepsilon_D \in 2^{12}$ に対して $\varepsilon_D^{\alpha} = \varepsilon_{D^{\alpha}}$ となることから $a = \pm 1$ を得る. よって $C_G(\alpha) = \langle -1\rangle \times A$ が示された.

さて $A \in Syl_{23}(G)$ であるから $|G : N_G(A)| \equiv 1 \pmod{23}$ が成り立つ. 一方定理 1.8, 定理 1.9 より $N_G(A)/C_G(A)$ が $Aut(A)$ の部分群で, $Aut(A)$ は位数 22 の巡回群であ

るから, $|N_G(A) : C_G(A)|$ は $|Aut(A)| = 22$ の約数である. $|N_G(A) : C_G(A)| = 22$ とすると $|G : N_G(A)| \equiv 12 \pmod{23}$ となるので $|N_G(A) : C_G(A)| = 11$ である. 従って $|N_G(A)| = 2 \cdot 23 \cdot 11$ となり, $N_G(A) = \langle -1 \rangle \times \langle \alpha, \beta \rangle$ を得る. ∎

定理 4.24 $\cdot 1$ は単純群である.

Proof $G = \cdot 0$ とおき, G の部分群 H で $\langle -1 \rangle \lneq H \lhd G$ をみたすものは G に限ることを示せばよい.

$|H|$ が 23 の倍数であるとき, G の Sylow 23-部分群はすべて H に含まれるので $A \leq H$ が成り立つ. 従って $M_{24} \cap H \neq 1$ となり, M_{24} の単純性より $M_{24} \leq H$ が得られる. このとき補題 4.23 より $N_G(A) \leq \langle -1 \rangle \times M_{24} \leq H$ となることから, Frattini argument(定理 1.14) より

$$G = HN_G(A) \leq H \cdot H = H$$

が得られ, $G = H$ が導かれる.

$|H|$ が 23 の倍数でないとき $|H|$ の素因数 p を任意に選び $P \in Syl_p(H)$ とする. Frattini argument を適用すると $G = HN_G(P)$ となるので $|N_G(P)|$ は 23 の倍数である. 従って P を適当な共役に置き換えることにより $\alpha \in N_G(P)$ であるとしてよい. 一方, 補題 4.23 より $C_G(\alpha) = \langle -1 \rangle \times A$ が成り立つ. ここで p が奇数とすると $C_P(\alpha) = 1$ より, 定理 1.15 を適用すれば

$$|P| \equiv | C_P(\alpha) | \equiv 1 \pmod{23}$$

が得られる. G の位数は $2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$ であり

$$3^k \not\equiv 1 \ (1 \leq k \leq 9), 5^k \not\equiv 1 \ (1 \leq k \leq 4), 7^k \not\equiv 1 \ (1 \leq k \leq 2), 11 \not\equiv 1, 13 \not\equiv 1 \pmod{23}$$

となり, このような P は存在し得ない. ゆえに H は 2-群である. このとき $C_H(\alpha) = \langle -1 \rangle$ となり, 定理 1.15 より $|H| \equiv 2 \pmod{23}$ が得られるが, 2 以上 2^{22} 以下の 2 のべきでこれをみたすのは 2 と 2^{12} のみである. $H \neq \langle -1 \rangle$ と仮定しているので $|H| = 2^{12}$ となる. さて $\langle -1 \rangle \leq C_G(H) \lhd G$ であるが, $\alpha \notin C_G(H)$ であるから $|C_G(H)|$ は 23 の倍数でない. 従って H の場合と同様にして $C_G(H) = \langle -1 \rangle$ または $|C_G(H)| = 2^{12}$ が得られる. ここで位数 13 の元 $\theta \in G$ に対して

$$1 \equiv |H| \equiv |C_H(\theta)| \pmod{13}$$

が成り立つことと, $-1 \in C_H(\theta)$ とから $|C_H(\theta)| = 2^{12}$ が得られる. よって $\theta \in C_G(H)$ となり, $|C_G(H)| = 2$ または 2^{12} であることに矛盾が生じる. 以上で $H = G$ が示された. ∎

定理 4.25 $\cdot 2$ は単純群である.

Proof $G = \cdot 2$ として $1 \lneq H \lhd G$ をみたす H が G に限ることを示せばよい. $|H|$ が 23 の倍数のときは $A \leq H$ より $G = HN_G(A)$ が得られる. 一方, 補題 4.21 より $M_{23} \leq G$ であるが, $M_{23} \cap H \neq 1$ と M_{23} の単純性から $M_{23} \leq H$ を得る. ここで $-1 \notin G$ より $N_G(A) = \langle \alpha, \beta \rangle \leq M_{23}$ となることから

$$G = H\, N_G(A) \leq H\, M_{23} = H$$

より $H = G$ が得られる.

$|H|$ が 23 の倍数でないとする. $|H|$ の素因数 p に対して $P \in Syl_p(H)$ とおくと $G = HN_G(P)$ となる. 必要ならば P を適当な共役で置き換えることにより $\alpha \in N_G(P)$ であるとしてよい. 一方, $-1 \notin G$ より $C_G(\alpha) = A$ となるので $C_P(\alpha) = 1$ が成り立つ. よって

$$|P| \equiv 1 \pmod{23}$$

を得るが, これをみたすのは $|P| = 2^{11}$ のみである. 従って $|H| = 2^{11}$ が成り立つ. 位数が 23 の倍数でない正規部分群 $(\neq 1)$ の位数は 2^{11} であることが示されたので $H = C_G(H)$ かつ H は G の極小正規部分群である.

さて $G/C_G(H) \leq Aut(H) = GL(11, 2)$ より G/H は $GL(11, 2)$ の部分群に同型である. 補題 4.22 より $|G/H|$ は 5^3 で割り切れ, 定理 1.4 より $|GL(11, 2)|$ は 5^3 で割り切れない. よって矛盾が得られたので G の正規部分群 $(\neq 1)$ の位数は 23 の倍数となり, G に一致することが示された. ∎

定理 4.26 $\cdot 3$ は単純群である.

Proof $G = \cdot 3$ として $1 \lneq H \lhd G$ をみたす H が G に限ることを示せばよい. $|H|$ が 23 の倍数のときは $A \leq H$ より $G = HN_G(A)$ が得られ, 定理 4.25 の証明と同様にして $H = G$ が得られる. $|H|$ が 23 の倍数でないとすると, $|H|$ の素因数 p に対して $P \in Syl_p(H)$ とおくと, 定理 4.25 の証明と同様にして

$$|P| \equiv 1 \pmod{23}$$

が導かれるが, これをみたす $|P|$ は存在しない. よって矛盾が得られ, 定理が証明された. ∎

以上で $\cdot 1, \cdot 2, \cdot 3$ の単純性が示された.

付録

M-行列を定義する octad

定義 2.17 で用いた 8 つの 8 点集合の元の位置を行列内の ∘ で表すと次のようになる.

$$\mathbf{M}(1) = \begin{bmatrix} & \circ & \circ & \circ & \circ & \circ \\ \circ & & & & & \\ \circ & & & & & \\ \circ & & & & & \end{bmatrix} \quad \mathbf{M}(2) = \begin{bmatrix} \circ & \circ & \circ & \circ & & \\ \circ & \circ & \circ & \circ & & \\ & & & & & \\ & & & & & \end{bmatrix}$$

$$\mathbf{M}(3) = \begin{bmatrix} \circ & \circ & \circ & \circ & & \\ & & & & & \\ \circ & \circ & \circ & \circ & & \\ & & & & & \end{bmatrix} \quad \mathbf{M}(4) = \begin{bmatrix} \circ & \circ & \circ & \circ & & \\ & & & & & \\ & & & & & \\ \circ & \circ & \circ & \circ & & \end{bmatrix}$$

$$\mathbf{M}(5) = \begin{bmatrix} & & \circ & \circ & \circ & \circ \\ & & \circ & \circ & \circ & \circ \\ & & & & & \\ & & & & & \end{bmatrix} \quad \mathbf{M}(6) = \begin{bmatrix} & & \circ & \circ & \circ & \circ \\ & & & & & \\ & & \circ & \circ & \circ & \circ \\ & & & & & \end{bmatrix}$$

$$\mathbf{M}(7) = \begin{bmatrix} & & \circ & \circ & \circ & \circ \\ & & & & & \\ & & & & & \\ & & \circ & \circ & \circ & \circ \end{bmatrix} \quad \mathbf{M}(8) = \begin{bmatrix} \circ & \circ & \circ & & & \\ & & & \circ & & \\ \circ & & & & \circ & \\ \circ & & & & & \circ \end{bmatrix}$$

sextet S_i

sextet S_i に対し,M-行列の i の位置で T_i の元を表すと次のようになる.

$$S_0 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix} \quad S_1 = \begin{bmatrix} 1 & 2 & 3 & 3 & 3 & 3 \\ 2 & 1 & 4 & 4 & 4 & 4 \\ 2 & 1 & 5 & 5 & 5 & 5 \\ 2 & 1 & 6 & 6 & 6 & 6 \end{bmatrix}$$

$$S_2 = \begin{bmatrix} 1 & 1 & 3 & 3 & 5 & 5 \\ 1 & 1 & 3 & 3 & 5 & 5 \\ 2 & 2 & 4 & 4 & 6 & 6 \\ 2 & 2 & 4 & 4 & 6 & 6 \end{bmatrix} \quad S_3 = \begin{bmatrix} 1 & 1 & 3 & 3 & 5 & 5 \\ 2 & 2 & 4 & 4 & 6 & 6 \\ 1 & 1 & 3 & 3 & 5 & 5 \\ 2 & 2 & 4 & 4 & 6 & 6 \end{bmatrix}$$

$$S_4 = \begin{bmatrix} 1 & 1 & 3 & 4 & 5 & 6 \\ 2 & 2 & 4 & 3 & 6 & 5 \\ 1 & 2 & 5 & 6 & 3 & 4 \\ 1 & 2 & 6 & 5 & 4 & 3 \end{bmatrix} \quad S_5 = \begin{bmatrix} 1 & 1 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 6 & 3 & 4 \\ 1 & 2 & 6 & 5 & 4 & 3 \\ 2 & 2 & 4 & 3 & 6 & 5 \end{bmatrix}$$

$\triangle$ の元

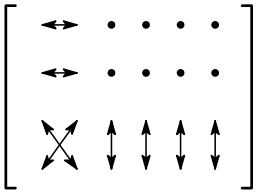
Δ の元 $X_0, X_1, \cdots, X_5$ の元を $\circ$ で表し, 行列に表すと次のようになる.

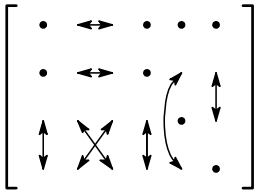
$$X_0 = \begin{bmatrix} & \circ & \\ & \circ & \\ & \circ & \\ & \circ & \end{bmatrix} \quad X_1 = \begin{bmatrix} & & \circ \\ \circ & & \\ \circ & & \\ \circ & & \end{bmatrix} \quad X_2 = \begin{bmatrix} & & \\ & & \\ \circ & & \circ \\ \circ & & \circ \end{bmatrix}$$

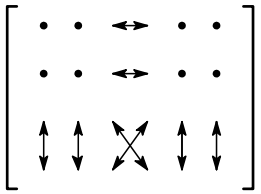
$$X_3 = \begin{bmatrix} & & \\ \circ & & \circ \\ & & \\ \circ & & \circ \end{bmatrix} \quad X_4 = \begin{bmatrix} & & \\ \circ & & \circ \\ & \circ & \\ & \circ & \end{bmatrix} \quad X_5 = \begin{bmatrix} & & \\ & \circ & \\ & \circ & \\ \circ & & \circ \end{bmatrix}$$

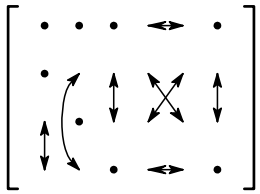
M_{24} の元

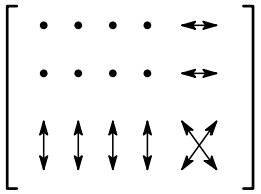
M_{24} の元をいくつかを M-行列に表す.

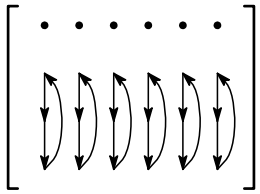
$\sigma_2(1) =$ 

$\sigma_2(2) =$ 

$\sigma_2(3) =$ 

$\sigma_2(4) =$ 

$\sigma_2(5) =$ 

$\sigma_3(1) =$ 

Λ_n^k の元の個数

ベクトル $(x_1, x_2, \cdots, x_{24})$ に対する集合 $\{i|x_i = k\}$ と Binary Goley Code との関連と k の値を () 内に示す. ただし $\{i|x_i \equiv m \pmod 4\}$ が Ω と $\emptyset$ になるときは単に Ω と記す.

(1) $|\Lambda_2| = 196560$

1. $|\Lambda_2^2| = 759 \cdot 2^7$
   ($\pm 2, \mp 2$ の集合が octad)
   - $(\pm 2^8.0^{16})$ が 759 個
   - $(\pm 2^6. \mp 2^2.0^{16})$ が $759 \cdot \begin{pmatrix} 8 \\ 2 \end{pmatrix}$ 個
   - $(2^4. - 2^4.0^{16})$ が $759 \cdot \begin{pmatrix} 8 \\ 4 \end{pmatrix}$ 個
2. $|\Lambda_2^3| = 24 \cdot 2^{12}$
   - $(\mp 3^1. \pm 1^{23})$ が 24 個 (Ω)
   - $(\mp 3^1. \pm 1^{15}. \mp 1^8)$ が $759 \cdot 16$ 個 (∓ 1 の集合が octad)
   - $(\mp 3^1. \pm 1^{11}. \mp 1^{12})$ が $2576 \cdot 12$ 個 (∓ 1 の集合が dodecad)

- $(\mp 3^1.\pm 1^7.\mp 1^{16})$ が $759\cdot 8$ 個 ($\mp 3, \pm 1$ の集合が octad)

3. $|\Lambda_2^4| = \begin{pmatrix} 24 \\ 2 \end{pmatrix} \cdot 2^2$ (Ω)
   - $(\pm 4^2.0^{22})$ が $\begin{pmatrix} 24 \\ 2 \end{pmatrix}$ 個
   - $(4^1.-4^1.0^{22})$ が $24\cdot 23$ 個

(2) $|\Lambda_3| = 16773120$

1. $|\Lambda_3^2| = 2576\cdot 2^{11}$
   ($\pm 2, \mp 2$ の集合が dodecad)
   - $(\pm 2^{12}.0^{12})$ が 2576 個
   - $(\pm 2^{10}.\mp 2^2.0^{12})$ が $2576\cdot \begin{pmatrix} 12 \\ 2 \end{pmatrix}$ 個
   - $(\pm 2^8.\mp 2^4.0^{12})$ が $2576\cdot \begin{pmatrix} 12 \\ 4 \end{pmatrix}$ 個
   - $(2^6.-2^6.0^{12})$ が $2576\cdot \begin{pmatrix} 12 \\ 6 \end{pmatrix}$ 個

2. $|\Lambda_3^3| = \begin{pmatrix} 24 \\ 3 \end{pmatrix} \cdot 2^{12}$
   - $(\mp 3^3.\pm 1^{21})$ が $\begin{pmatrix} 24 \\ 3 \end{pmatrix}$ 個 (Ω)
   - $(\mp 3^3.\pm 1^{13}.\mp 1^8)$ が $759\cdot \begin{pmatrix} 16 \\ 3 \end{pmatrix}$ 個 (∓ 1 の集合が octad)
   - $(\mp 3^3.\pm 1^9.\mp 1^{12})$ が $2576\cdot \begin{pmatrix} 12 \\ 3 \end{pmatrix}$ 個 (∓ 1 の集合が dodecad)
   - $(\mp 3^3.\pm 1^5.\mp 1^{16})$ が $759\cdot \begin{pmatrix} 8 \\ 3 \end{pmatrix}$ 個 ($\mp 3, \pm 1$ の集合が octad)
   - $(\mp 3^2.\pm 3^1.\pm 1^{14}.\mp 1^7)$ が $759\cdot \begin{pmatrix} 16 \\ 2 \end{pmatrix}\cdot 8$ 個 ($\pm 3, \mp 1$ の集合が octad)
   - $(\mp 3^2.\pm 3^1.\pm 1^{10}.\mp 1^{11})$ が $2576\cdot \begin{pmatrix} 12 \\ 2 \end{pmatrix}\cdot 12$ 個 ($\pm 3, \mp 1$ の集合が dodecad)
   - $(\mp 3^2.\pm 3^1.\pm 1^6.\mp 1^{15})$ が $759\cdot \begin{pmatrix} 8 \\ 2 \end{pmatrix}\cdot 16$ 個 ($\mp 3, \pm 1$ の集合が octad)

3. $|\Lambda_3^4| = 759 \cdot 2^{12}$
   ($\pm 2, \mp 2$ の集合が octad)
   - $(\pm 4^1. \pm 2^7. \mp 2^1.0^{15})$ が $759 \cdot 16 \cdot 8$ 個
   - $(\pm 4^1. \pm 2^5. \mp 2^3.0^{15})$ が $759 \cdot 16 \cdot \begin{pmatrix} 8 \\ 3 \end{pmatrix}$ 個
   - $(\pm 4^1. \pm 2^3. \mp 2^5.0^{15})$ が $759 \cdot 16 \cdot \begin{pmatrix} 8 \\ 3 \end{pmatrix}$ 個
   - $(\pm 4^1. \pm 2^1. \mp 2^7.0^{15})$ が $759 \cdot 16 \cdot 8$ 個
4. $|\Lambda_3^5| = 24 \cdot 2^{12}$
   - $(\pm 5^1. \pm 1^{23})$ が 24 個 (Ω)
   - $(\pm 5^1. \pm 1^{15}. \mp 1^8)$ が $759 \cdot 16$ 個 (± 1 の集合が octad)
   - $(\pm 5^1. \pm 1^{11}. \mp 1^{12})$ が $2576 \cdot 12$ 個 (± 1 の集合が dodecad)
   - $(\pm 5^1. \pm 1^7. \mp 1^{16})$ が $759 \cdot 8$ 個 ($\pm 5, \pm 1$ の集合が octad)

(3) $|\Lambda_4| = 398034000$

1. $|\Lambda_4^2| = 759 \cdot 2^{15}$
   (0 の集合が octad)
   - $(\pm 2^{16}.0^8)$ が 759 個
   - $(\pm 2^{14}. \mp 2^2.0^8)$ が $759 \cdot \begin{pmatrix} 16 \\ 2 \end{pmatrix}$ 個
   - $(\pm 2^{12}. \mp 2^4.0^8)$ が $759 \cdot \begin{pmatrix} 16 \\ 4 \end{pmatrix}$ 個
   - $(\pm 2^{10}. \mp 2^6.0^8)$ が $759 \cdot \begin{pmatrix} 16 \\ 6 \end{pmatrix}$ 個
   - $(2^8. - 2^8.0^8)$ が $759 \cdot \begin{pmatrix} 16 \\ 8 \end{pmatrix}$ 個
2. $|\Lambda_4^3| = \begin{pmatrix} 24 \\ 5 \end{pmatrix} \cdot 2^{12}$
   - $(\pm 3^5. \mp 1^3. \pm 1^{16})$ が $759 \cdot \begin{pmatrix} 8 \\ 3 \end{pmatrix}$ 個 ($\pm 3, \mp 1$ の集合が octad)
   - $(\pm 3^5. \mp 1^7. \pm 1^{12})$ が $2576 \cdot \begin{pmatrix} 12 \\ 5 \end{pmatrix}$ 個 (± 1 の集合が dodecad)

- $(\pm 3^5.\mp 1^{11}.\pm 1^8)$ が $759\cdot\begin{pmatrix}16\\5\end{pmatrix}$ 個 (± 1 の集合が octad)
- $(\pm 3^5.\mp 1^{19})$ が $\begin{pmatrix}24\\5\end{pmatrix}$ 個 (Ω)
- $(\pm 3^4.\mp 3^1.\pm 1^7.\mp 1^{12})$ が $759\cdot 8\cdot\begin{pmatrix}16\\4\end{pmatrix}$ 個 ($\mp 3, \pm 1$ の集合が octad)
- $(\pm 3^4.\mp 3^1.\pm 1^{11}.\mp 1^8)$ が $2576\cdot 12\cdot\begin{pmatrix}12\\4\end{pmatrix}$ 個 ($\mp 3, \pm 1$ の集合が dodecad)
- $(\pm 3^4.\mp 3^1.\pm 1^{15}.\mp 1^4)$ が $759\cdot 16\cdot\begin{pmatrix}8\\4\end{pmatrix}$ 個 ($\pm 3, \mp 1$ の集合が octad)
- $(\pm 3^3.\mp 3^2.\pm 1^6.\mp 1^{13})$ が $759\cdot\begin{pmatrix}8\\2\end{pmatrix}\cdot\begin{pmatrix}16\\3\end{pmatrix}$ 個 ($\mp 3, \pm 1$ の集合が octad)
- $(\pm 3^3.\mp 3^2.\pm 1^{10}.\mp 1^9)$ が $2576\cdot\begin{pmatrix}12\\2\end{pmatrix}\cdot\begin{pmatrix}12\\3\end{pmatrix}$ 個 ($\mp 3, \pm 1$ の集合が dodecad)
- $(\pm 3^3.\mp 3^2.\pm 1^{14}.\mp 1^5)$ が $759\cdot\begin{pmatrix}16\\2\end{pmatrix}\cdot\begin{pmatrix}8\\3\end{pmatrix}$ 個 ($\pm 3, \mp 1$ の集合が octad)

3. $|\Lambda_4^{4^4}| = \begin{pmatrix}24\\4\end{pmatrix}\cdot 2^4$ （ Ω ）
   - $(\pm 4^4.0^{20})$ が $\begin{pmatrix}24\\4\end{pmatrix}$ 個
   - $(\pm 4^3.\mp 4^1.0^{20})$ が $24\cdot\begin{pmatrix}23\\3\end{pmatrix}$ 個
   - $(4^2.-4^2.0^{20})$ が $\begin{pmatrix}24\\2\end{pmatrix}\begin{pmatrix}22\\2\end{pmatrix}$ 個

4. $|\Lambda_4^{4^2}| = 759\cdot\begin{pmatrix}16\\2\end{pmatrix}\cdot 2^9$
   ($\pm 2, \mp 2$ の集合が octad)
   - $(\pm 4^2.\pm 2^8.0^{14})$ が $759\cdot\begin{pmatrix}16\\2\end{pmatrix}$ 個
   - $(\pm 4^2.\pm 2^6.\mp 2^2.0^{14})$ が $759\cdot\begin{pmatrix}16\\2\end{pmatrix}\begin{pmatrix}8\\2\end{pmatrix}$ 個

- $(\pm 4^2.\pm 2^4.\mp 2^4.0^{14})$ が $759\cdot\begin{pmatrix}16\\2\end{pmatrix}\begin{pmatrix}8\\4\end{pmatrix}$ 個
- $(\pm 4^2.\pm 2^2.\mp 2^6.0^{14})$ が $759\cdot\begin{pmatrix}16\\2\end{pmatrix}\begin{pmatrix}8\\2\end{pmatrix}$ 個
- $(\pm 4^2.\mp 2^8.0^{14})$ が $759\cdot\begin{pmatrix}16\\2\end{pmatrix}$ 個
- $(\pm 4^1.\mp 4^1.\pm 2^8.0^{14})$ が $759\cdot 16\cdot 15$ 個
- $(\pm 4^1.\mp 4^1.\pm 2^6.\mp 2^2.0^{14})$ が $759\cdot 16\cdot 15\cdot\begin{pmatrix}8\\2\end{pmatrix}$ 個
- $(4^1.-4^1.2^4.-2^4.0^{14})$ が $759\cdot 16\cdot 15\cdot\begin{pmatrix}8\\4\end{pmatrix}$ 個

5. $|\Lambda_4^{4^1}|=2576\cdot 12\cdot 2^{12}$
   ($\pm 2,\mp 2$ の集合が dodecad)
   - $(\pm 4^1.\pm 2^{11}.\mp 2^1.0^{11})$ が $2576\cdot 12\cdot 12$ 個
   - $(\pm 4^1.\pm 2^9.\mp 2^3.0^{11})$ が $2576\cdot 12\cdot\begin{pmatrix}12\\3\end{pmatrix}$ 個
   - $(\pm 4^1.\pm 2^7.\mp 2^5.0^{11})$ が $2576\cdot 12\cdot\begin{pmatrix}12\\5\end{pmatrix}$ 個
   - $(\pm 4^1.\pm 2^5.\mp 2^7.0^{11})$ が $2576\cdot 12\cdot\begin{pmatrix}12\\5\end{pmatrix}$ 個
   - $(\pm 4^1.\pm 2^3.\mp 2^9.0^{11})$ が $2576\cdot 12\cdot\begin{pmatrix}12\\3\end{pmatrix}$ 個
   - $(\pm 4^1.\pm 2^1.\mp 2^{11}.0^{11})$ が $2576\cdot 12\cdot 12$ 個
6. $|\Lambda_4^5|=759\cdot 2^{15}$
   - $(\pm 5^1.\pm 3^2.\pm 1^{15}.\mp 1^6)$ が $759\cdot 16\cdot\begin{pmatrix}8\\2\end{pmatrix}$ 個 ($\pm 3,\mp 1$ の集合が octad)
   - $(\pm 5^1.\pm 3^2.\pm 1^{11}.\mp 1^{10})$ が $2576\cdot 12\cdot\begin{pmatrix}12\\2\end{pmatrix}$ 個 ($\pm 3,\mp 1$ の集合が dodecad)
   - $(\pm 5^1.\pm 3^2.\pm 1^7.\mp 1^{14})$ が $759\cdot 8\cdot\begin{pmatrix}16\\2\end{pmatrix}$ 個 ($\pm 5,\pm 1$ の集合が octad)
   - $(\pm 5^1.\pm 3^1.\mp 3^1.\pm 1^{14}.\mp 1^7)$ が $759\cdot 8\cdot 16\cdot 15$ 個 ($\pm 3,\mp 1$ の集合が octad)
   - $(\pm 5^1.\pm 3^1.\mp 3^1.\pm 1^{10}.\mp 1^{11})$ が $2576\cdot 12\cdot 12\cdot 11$ 個 ($\pm 3,\mp 1$ の集合が dodecad)

- $(\pm 5^1.\pm 3^1.\mp 3^1.\pm 1^6.\mp 1^{15})$ が $759\cdot 16\cdot 8\cdot 7$ 個 ($\pm 5, \mp 3, \pm 1$ の集合が octad)
- $(\pm 5^1.\mp 3^2.\pm 1^{13}.\mp 1^8)$ が $759\cdot 16\cdot \begin{pmatrix} 15 \\ 2 \end{pmatrix}$ 個 (∓ 1 の集合が octad)
- $(\pm 5^1.\mp 3^2.\pm 1^9.\mp 1^{12})$ が $2576\cdot 12\cdot \begin{pmatrix} 11 \\ 2 \end{pmatrix}$ 個 (∓ 1 の集合が dodecad)
- $(\pm 5^1.\mp 3^2.\pm 1^5.\mp 1^{16})$ が $759\cdot 8\cdot \begin{pmatrix} 7 \\ 2 \end{pmatrix}$ 個 ($\pm 5, \mp 3, \pm 1$ の集合が octad)

7. $|\Lambda_4^6| = 759\cdot 2^{10}$
   ($\pm 6, \pm 2, \mp 2$ の集合が octad)
   - $(\pm 6^1.\pm 2^6.\mp 2^1.0^{16})$ が $759\cdot 8\cdot 7$ 個
   - $(\pm 6^1.\pm 2^4.\mp 2^3.0^{16})$ が $759\cdot 8\cdot \begin{pmatrix} 7 \\ 3 \end{pmatrix}$ 個
   - $(\pm 6^1.\pm 2^2.\mp 2^5.0^{16})$ が $759\cdot 8\cdot \begin{pmatrix} 7 \\ 2 \end{pmatrix}$ 個
   - $(\pm 6^1.\mp 2^7.0^{16})$ が $759\cdot 8$ 個
8. $|\Lambda_4^8| = 24\cdot 2$ (Ω)
   - $(8^1.0^{23}), (-8^1.0^{23})$ が 24 個

References

[1] 近藤 武, Mathieu 群と Conway 群 (講義録), 1996.

[2] 佐伯 陽, 有限置換群の研究, 1982 年度兵庫教育大学修士論文.

[3] 永尾 汎, 群とデザイン, 岩波書店, 1974.

[4] I. Anderson, A first course in combinatorial mathematics, 2nd edition, Oxford, 1989.

[5] J. H. Conway, *A group of order 8315553613086720000*, Bull. London Math. Soc., 1 (1969), 79-88.

[6] I. M. Isaacs, Algebra, Brooks/Cole, 1994.

[7] J. Leech, *Notes on sphere packing*, Can. J. Math., 19 (1967), 251-267.

[8] J. J. Rotman, An introduction to the theory of groups, Springer-Verlag, 1995.