

Conway 群の単純性の初等的証明

イリノイ大学 鈴木通夫 (Michio Suzuki)

はじめに Conway 群は Leech 格子の自己同形のつくる群から導かれる散在群である。Conway 群は $\cdot 0, \cdot 1, \cdot 2, \cdot 3$ と四つ定義されるが, $\cdot 1$ 以下の三つの群は単純であることが知られている。(しかし文献に証明がのっているのは $\cdot 1$ についてだけである。)

ここではこれらの Conway 群が単純であることと初等的にかゝ Conway 群の性質のうち, 定義から比較的直ちに導かれる性質だけを用いて証明する方法を述べよう。この方法によれば三つの Conway 群 $\cdot 1, \cdot 2, \cdot 3$ に対して同一の方法を用いて, 同じようにして単純性を証明することができる。

§1 Conway 群と Leech 格子

よく知られていることであるが, まず Leech 格子の定義から始めよう。24次元の Euclid 空間に正規直交系 $\{v_i\}$

をとる。添数の集合を

$$\Omega = \{1, 2, \dots, 24\}$$

とおき, Ω の部分集合 I について

$$[I] = \sum_{i \in I} v_i$$

と定義する.

\mathcal{E} を binary Golay code とし \mathcal{E} の元を Ω の部分集合と考える. Ω の部分集合全体のつくる集合 V に対称差により加法を定義すれば, V は 2 元体上の 24 次元ベクトル空間となり, よく知られているように \mathcal{E} は V の 12 次元部分空間となる. また \mathcal{E} の元で 8 点からなるものの全体の集合を \mathcal{D} とおけば, \mathcal{D} は $5(24, 8, 1)$ デザインであって \mathcal{E} は \mathcal{D} が生成する V の部分空間と一致する. さて Leech 格子 Λ は

$$2[\mathcal{D}] \quad (\mathcal{D} \in \mathcal{D})$$

および

$$u_2 = -3v_1 + v_2 + \dots + v_{24} = -4v_1 + [\Omega]$$

から生成される格子群である.

この定義から次の命題の成り立つことが容易に証明される.

(1.1) 正規直交系 $\{v_i\}$ について元 $\sum x_i v_i$ ($x_i \in \mathbb{Z}$) が Leech 格子 Λ に属するための条件は

(i) 係数 x_i がすべて偶数で和 $\sum x_i$ は 8 で割り切れるか,

または x_i がすべて奇数で和 $\sum x_i$ が 8 と法として 4 に合同である,

(ii) 係数を法 4 で考えた時, x_i が与えられた剰余類 1 にはいる添数の集合は \mathcal{C} の元である.

以下 Leech 格子を Λ と表わす. そして

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

とおく. ここで (x, y) は通常の内積である. (1.1) を用いて次の命題が証明される.

(1.2) Λ は Λ_m の合併集合となる. $\Lambda_0 = \{0\}$, $\Lambda_1 = \text{空集合}$,

$$u_2 = -4v_1 + [\Omega] \in \Lambda_2,$$

$$u_3 = 4v_1 + [\Omega] \in \Lambda_3,$$

$$8v_i \in \Lambda_4.$$

また $|\Lambda_2|$, $|\Lambda_3|$, $|\Lambda_4|$ が計算される.

24 次元の直交群の元のうち Leech 格子 Λ を不変にするものの全体のつくる部分群を $\cdot O$ と表わす.

§2 Conway 群 $\cdot O$ の性質

いま code \mathcal{C} の元 X について

$\varepsilon_X: v_i \mapsto -v_i \ (i \in X), v_j \mapsto v_j \ (j \notin X)$
 と符号変換 ε_X と定義すれば, ε_X は直交群の元であるが,
 (1.1) から容易にわかるように ε_X は $\cdot O$ の元である. また
 Mathieu群 M_{24} の元 π に対して

$$v_i \mapsto v_{\pi(i)}$$

という座標変換を対応させれば, これも $\cdot O$ の元となる. こ
 れで M_{24} が $5(24, 8, 1)$ デザインの自己同形群であること
 が用いられる (大山: 有限置換群 参照). このように

$$M_{24} \subset \cdot O$$

と考えられる. そこで \mathcal{E} の元に対応する符号変換の全体を
 E とおけば, E は位数 2^{12} の基本可換群である. M_{24} は E と
 不変にするから $N = EM_{24}$ は $\cdot O$ の部分群であるが, 次の
 Conway の主定理

$$(2.1) \quad \cdot O \neq N = EM_{24}$$

が成り立つ. このことから次の結果を得る.

(2.2) 群 $\cdot O$ は Λ_2 上可移 (= 作用する). 同様に $\cdot O$ は Λ_3
 上にも, Λ_4 上にも可移 (= 作用する).

群・ O の中で N の元は次の性質により特長づけられる。

(2.3) 群・ O の元 σ がある添数 i について $\sigma(v_i) = \pm v_j$ を満足すれば σ は N の元である。

この命題の系として Λ_4 の一点 $8v_i$ の安定化群は N の部分群であることが証明される。この系と (1.2) における $|\Lambda_4|$ の値から、(2.2) を用いて $\cdot O$ の位数が計算される。

$$|\cdot O| = 2^{22} 3^9 5^4 7^2 11 \cdot 13 \cdot 23.$$

次の命題が重要である。

(2.4) 群・ O の各元は正規直交系 $\{v_i\}$ により 24 次元の直交行列により表現される。行列の各成分は有理数でその分母は 8 の約数である。

証明 前半は明らかである。後半は $\sigma \in \cdot O$ ならば

$$\sigma(8v_i) \in \Lambda$$

であるから明らかである。 \square

§3. Conway 群 $\cdot 1, \cdot 2, \cdot 3$ の定義

まず次の命題が成り立つ。

(3.1) 群 $\cdot 0$ の中心は恒等写像 I と $-I$ からなっている。

そこで Conway 群 $\cdot 0$ の中心による商群を $\cdot 1$ と表わす。

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

群 $\cdot 0$ の中で Λ_2 の元 $u_2 = -4v_1 + [\Omega]$ の安定化群を $\cdot 2$, Λ_3 の元 $u_3 = 4v_1 + [\Omega]$ の安定化群を $\cdot 3$ と表わす。(2.2) および (1.2) から $\cdot 2, \cdot 3$ の位数が計算できる。

$$(3.2) \begin{cases} |\cdot 1| = 2^{21} 3^9 5^4 7^2 \cdot 11 \cdot 13 \cdot 23 \\ |\cdot 2| = 2^{18} 3^6 5^3 7 \cdot 11 \cdot 23 \\ |\cdot 3| = 2^{10} 3^7 5^3 7 \cdot 11 \cdot 23 \end{cases}$$

こゝで次の性質と注意しておこう。

(3.3) 群 $\cdot 2$ も $\cdot 3$ も $-I$ を含んでいない。また

$$M_{23} \subset \cdot 2, \quad M_{23} \subset \cdot 3.$$

証明 前半は明らか。後半も $\cdot 2, \cdot 3$ と定義する元 u_2, u_3 の形から明らかである。 \square

§4 位数 23 の元 α

M_{24} の中には, 1 と固定し残りの 2 から 24 までは巡回的に動かす元 α がある. また:

$$\beta \alpha \beta^{-1} = \alpha^2$$

をみたす位数 11 の元 β もある. $Z \mid 2 \langle \alpha \rangle = A$ とおけば次の命題が成り立つ. $\therefore \langle \alpha, \beta \rangle \subset M_{23} \subset M_{24}$.

(4.1) M_{24} の中で A の正規化群は $\langle \alpha, \beta \rangle$ である. また α の中心化群は A と一致する.

単純性の証明に必要な命題は次のようになる.

命題 4.2 $G = \cdot O$ とおき $\alpha, \beta \in G$ の元とみる. この時次式が成り立つ. ($A = \langle \alpha \rangle$ とおく.)

$$C_G(\alpha) = \langle -I \rangle \times A, \quad N_G(A) = \langle -I \rangle \times \langle \alpha, \beta \rangle.$$

証明 α を表現する行列の固有値は 1 の 23 乗根で, そのうち 1 の重複度は 2, その他の根の重複度は 1 である. \therefore α の不変元のつくる部分空間は 2 次元

$$u = v_1, \quad w = v_2 + v_3 + \cdots + v_{24}$$

により生成される. いま $\sigma \in C_G(\alpha)$ とすれば

$$\sigma(u) = au + bw$$

となる. $t=3$ で $\sigma(u)$ の長さは 1 だから $a^2 + 23b^2 = 1$.
 一方, (2.4) により a, b は分母が 8 の約数である有理数だから $b=0$ となる. したがって $\sigma(v_1) = \pm v_1$, (2.3) により $\sigma \in N$ を得る. これから $C_G(\alpha) = \langle -I \rangle \times A$ が得られる.

よって $A = \langle \alpha \rangle$ は G のシロ-群だから ($\cdot 0$ の位数参照)

$$|G : N_G(A)| \equiv 1 \pmod{23}.$$

また $|N_G(A) : C_G(A)|$ は 22 の約数となる. これから

$$|N_G(A) : C_G(A)| = 11$$

を得て命題 4.2 が証明される. \square

§5 Conway 群の単純性

次の良く知られた一般的な補題が必要となる.

(5.1) G は任意の有限群, H を G の正規部分群, P を H のシロ-群とする. この時

$$G = HN_G(P)$$

が成り立つ. 群 G の位数 $|G|$ を割り切る任意の素数 p について p は H の位数を割り切るか, または $N_G(P)$ の位数を割り切る.

(これは Frattini 論法とよばれる一般原理である.)

まず Conway 群 $\cdot 1$ の単純性を証明しよう.

命題 A Conway 群 $\cdot 0$ を G とおき, H を G の正規部分群で $-I$ を含むものとする. この時 $G=H$, または $H=\langle -I \rangle$. すなわち Conway 群 $\cdot 1 = \cdot 0 / \langle -I \rangle$ は単純である.

証明 部分群 H の位数が 23 で割れるか, 割れないかに応じて $\tau = \tau$ の場合に分ける. §4 で定めた元 α, β をとり, それらを G の元とみる.

(1) $|H|$ が 23 で割れる場合. H のシロ-23 群の一つを A_0 とする. $A = \langle \alpha \rangle$ は G のシロ-群だから A_0 と G の中で共役. よって $A = g A_0 g^{-1} \subset g H g^{-1} = H$ となり, A は H のシロ-群となる. よって (5.1) により

$$G = H N_G(A)$$

が成り立つ. ところで命題 4.2 により

$$N_G(A) = \langle -I \rangle \times \langle \alpha, \beta \rangle \subset \langle -I, M_{23} \rangle$$

となる. 仮定により $-I \in H$. さらに M_{23} は単純群だから α の共役元により生成されている. $\alpha \in H$ であるから α の共役元はすべて H に含まれる. よって $M_{23} \subset H$, すなわち

$$N_G(A) \subset \langle -I, M_{23} \rangle \subset H$$

を得る. $G = H N_G(A)$ だから $G = H$ となる.

(2) $|H|$ が 23 で割り切れない場合. H の位数を割る素数 p をとり, H のシロ p 群を P とおく. (5.1) により

$$G = HN_G(P)$$

かつ $N_G(P)$ の位数が 23 で割り切れる. いま $N_G(P)$ に含まれている位数 23 の元の α_0 とおけば, α_0 は A の元と共役だから命題 4.2 を用いて

$$C_G(\alpha_0) = \langle -I \rangle \times \langle \alpha_0 \rangle$$

を得る. $\Sigma = 2$ p が奇数ならば $C_P(\alpha_0) = \{1\}$. よって

$$|P| \equiv 1 \pmod{23}$$

を得る. しかし G の位数とみれば, これから $P = \{1\}$ となり矛盾が得られる. したがって $p = 2$. すなわち H の位数は 2 のべきである. この時は

$$|H| \equiv 2 \pmod{23}$$

($C_H(\alpha_0) = \langle -I \rangle$ である). よって $|H| = 2$ または 2^{12} .

$|H| = 2$ ならば $H = \langle -I \rangle$. $\Sigma = 2$ $|H| = 2^{12}$ と仮定し

て矛盾を導こう. H と共に $C_G(H)$ は G の正規部分群で $-I \in C_G(H)$. よって $C_G(H)$ は 2 群である.

一方, $C_G(H)$ は 2 群ではないことを示そう. G は位数 13 の元 θ を含む. $\Sigma = 2$

$$|H| \equiv |C_H(\theta)| \pmod{13}.$$

$\Sigma = 2$ $|C_H(\theta)| = 2^m$ とおけば $m \geq 1$. よって

$$2^{12} \equiv 2^m \pmod{13}$$

より $m=12$ を得る. これは $\theta \in C_G(H)$ を示すから $C_G(H)$ が 2 群であることに矛盾する.

これより $H = \langle -I \rangle$ または $H = G$ が証明されたから, Conway 群 $\cdot 1 = \cdot 0 / \langle -I \rangle$ は単純群である. \square

命題 B Conway 群 $\cdot 2$ および $\cdot 3$ は共に単純である.

証明 $G = \cdot 2$ または $\cdot 3$ とし H と G の正規部分群 $H \neq \{1\}$ と仮定する. $H = G$ と証明すればよい. 前命題の証明と同様に二つの場合に分ける.

(1) $|H|$ が 23 で割れる場合. 前と同様に $A \subset H$ とする. この場合 (3.3) により $-I \notin G$ しか $M_{23} \subset G$. よって

$$N_G(A) = \langle \alpha, \beta \rangle \subset M_{23}$$

となるから前と同様に $H = G$ を得る.

(2) $|H|$ が 23 で割れない場合. H の位数を割る素数 p ととり H のシロ- p 群の一つを P とする. この場合 p の奇偶にかかわらず

$$|P| \equiv 1 \pmod{23}$$

を得る. $|G|$ の形から $|P| = 2^{11}$ となる. よって $G = \cdot 3$ の場合は $|H| = 1$ となる ($| \cdot 3 |$ は 2^{11} で割れない). そこで $G = \cdot 2$, $|H| = 2^{11}$ の場合に矛盾を導けばよい.

H は 2 群だから $C_G(H) \supseteq Z(H) \neq \{1\}$. $C_G(H)$ も G の正規部分群だから $C_G(H) = H$, すなわち H は (基本) 可換群である. そゝで $G/H \hookrightarrow \text{Aut } H = GL(11, 2)$ となる. ところが G/H の位数は 5^3 で割れるが $GL(11, 2)$ の位数は 5^3 では割り切れない. これは矛盾である. \square

Conway 群の場合も位数 2 の元の中心化群の構造が既知とすれば, 他の方法により単純性と言明することが出来る. これについては福井における代数シンポジウム 4 (昭和 62 年) の報告集に書く予定である.

文献

M_{24} については 大山: 有限置換群 (裳華房)

Conway 群については Conway: Bull. London Math. Soc. 1 (1969) または Finite Simple Groups Acad. Press (1971) の第 7 章. なお T. M. Thompson の本 (MAA の Carus 叢書 21) にも解説がのっている.