「代数的組合わせ論および群論」

研究集会報告集

（伊藤昇先生還暦記念）

1985年1月9日〜11日

於　大阪市立大学文化交流センター

序

この報告集は１９８５年１月９日〜１１日の３日間大阪市立大学文化交流センターで開催された「代数的組合わせ論および群論」研究集会における講演内容をまとめたものである（ただしKantor 氏の分はこれに先立って行なわれた阪大での研究会の講演内容である）。

副題にもあるように伊藤昇先生（現甲南大学教授）の還暦を記念するという意味もあって講演テーマは氏の研究歴を反映するかの如く多彩となり、出席者は１２０名近くあった。プログラムを作成して下さった大山豪氏、および本報告集のため伊藤先生の研究業績等の紹介をして下さった木村浩氏に感謝いたします。

講演者の旅費等の経費ならびにこの報告集の出版費は昭和５９年度科学研究費（総合研究Ａ、研究代表者　都筑俊郎）によるものである。

１９８５年２月

津　島　行　男

目　　　次

伊藤昇先生の還暦に寄せて

愛媛大学・理　木　村　　　浩

昨年４月に伊藤先生は、還暦をお迎えになりました。お元気で数学の研究に御活躍中でいらっしゃることは、誠におめでたいとお喜び申し上げます。
お祝いのシンポジウムが開かれ、その報告集に先生の紹介を書くように北大都筑教授より言われ、その任ではないと思いつつ引き受けてしまいました。先生との開きがあまりにも大きすぎ、数学的業績の正しい評価が出来ないであろうと考えながら書いています。足りない所誤っている所等は、この文を読んでくだださった各位が御加筆、御訂正してくだされぱと勝手に期待しています。

伊藤先生は、１９２４年４月１１日東京都墨田区で生まれ、第三高等学校、名古屋大学を卒業後、名古屋大学大学院をへて１９５１年４月、名古屋大学助手に、２年後に講師になられました。その後北大に４年間在籍し、その間約１年半西ドイツへ留学されました。
１９５９年４月名大教養部教授、１９６４年８月理学部教授になられ、1968年に退職されました。１９６６年〜１９８２年までイリノイ大学シカゴサークル教授であられました。
現在は、イリノイ大学名誉教授であり、また甲南大学理学部教授として研究に励んでいらっしゃいます。

伊藤先生の仕事は、論文リストを見ればわかるように、有限群に関するもの、またそれに関したデザインやHadamard行列に関するものが多い。１９６０年前後より単純群の分類問題が急に動きだし、その一翼をになったのが先生です。J. Thompsonの出現が大きいのは勿論であるが、置換群に関しての伊藤先生、鈴木通夫先生（イリノイ大教授）、W. Feitの仕事が大きく寄与している。
H. Zassenhausが１９３６年に「３点を動かす元は単位元だけである」２重可移群の分類を始めた。いわゆるZassenhaus群である。彼は、このような群で３重可移なものを決定した。１９６０年Feitは例外指標の理論を用いて次のことを示している。

「Zassenhaus 群の degree は、ある素数 p と自然数 m があって p^m+1 である。」更に正則正規部分群を含む場合を研究した。残りの場合 p＝2 のときが鈴木先生であり、p が奇数の時が伊藤先生であった。鈴木先生はこの場合にいわゆる Suzuki 群を発見したのである。

伊藤先生の場合は、知られていた群であったが、これによって Zassenhaus 群の分類は終ったのである。

この仕事が多くの伊藤先生の論文の中で最も有名なものの1つであることは確かであろう。証明を述べるのが目的ではないのでふれない。しかし読まれた方はお気付きのことと思うが、先生の仕事の進め方、或いは問題の見つめ方がよく表われているように思います。

私なりに感じている先生の数学に対する情熱を記してみたい。これはまったく個人的感じ方であり、従って先生御自身からこんなものではないとお叱りを受けるかもしれないが、お祝いの文であるのに免じてお許しをいただきたい。私が名古屋大学教養部にいた頃、都筑先生の勧め(おだて？)に乗って Zassenhaus, Feit, Suzuki, Ito の論文を読み、自分の仕事をしなければと思い、種になる論文として見つけたのが伊藤先生のものでした。それを少し拡張して先生にお送りしたところ、シカゴから数日おきに手紙をいただきました。もっと一般的になりそうだとか、御自身がその仕事をなさったときのことなどが書いてありました。それ以来御指導を受けております。常に数学を考えられ、シカゴでは夜でもよく電話をいただきました。次を考えようとしていると、次の電話があり、改めて尊敬し、自分も頑張らねばと思ったものです。確か三高の時にラグビーをやっておられたと聞きましたが、とり組んだ問題に対してラグビーの様に突進なさるのが伊藤先生ではないでしょうか。

シンポジウムを機会に津島氏がお祝いのパーティーを計画してくれました。その席でも還暦などの祝いは10年後でよいとおっしゃっていました。多分これからもラグビーのように突き進んでいくことでしょう。「今年も誰にでもわかる定理を作ります」と述べられました。これこそ先生の数学観を表わしている言葉だと思います。

最後になりましたが、富美子夫人の人柄も先生の数学的生き方を表わしてい

るような気がします。ということは、夫人の功も大きかったことでしょう。個人的にも大変お世話になりました。是非機会を作って夫人とも話してみられることをおすすめ致します。

なお現在は、デザイン特にHadamard行列に興味を持たれ、その方面の仕事も沢山なさっています。

これからも、お元気で御活躍されることでしょう。

List of mathematical papers of Noboru Ito
(up to 1984)

[1] (with Nagata, Masayoshi) Note on groups of automorphisms. Kôdai Math. Sem. Rep., no.3 (1949), 37-39.

[2] Note on p-groups. Nagoya Math. J. 1 (1950), 113-116.

[3] Remarks on factorizable groups. Acta. Sci. Math. Szeged 14 (1951), 83-84.

[4] Note on (LM)-groups of finite orders. Kôdai Math. Sem. Rep. 1951 (1951), 1-6.

[5] A theorem on the alternating group $\mathfrak{A}_n$ ($n \geqq 5$). Math. Japonicae 2 (1951), 59-60.

[6] On the degrees of irreducible representations of a finite group. Nagoya Math. J. 3 (1951), 5-6.

[7] Some studies on group characters. Nagoya Math. J. 2 (1951), 17-28.

[8] On the characters of soluble groups. Nagoya Math. J. 3 (1951), 31-48.

[9] On a theorem of L. Rédei an J. Szép concerning p-groups. Acta Sci. Math. Szeged 14 (1952), 186-187.

[10] Remarks on O. Grün's paper "Beiträge zur Gruppentheorie.III." Math. Nachr. 6 (1952), 319-325.

[11] Note on A-groups. Nagoya Math. J. 4 (1952), 79-81.

[12] On Π-structures of finite groups. Tohoku Math. J. (2) 4 (1952), 172-177.

[13] On the factorizations of the linear fractional group $LF(2,p^n)$.

Acta Sci. Math. Szeged 15 (1953), 79-84.

[14] On a theorem of H. F. Blichfeldt. Nagoya Math. J. 5 (1953), 75-77.

[15] On finite groups with given conjugate types. I. Nagoya Math. J. 6 (1953), 17-28.

[16] Note on S-groups. Proc. Japan Acad. 29 (1953), 149-150.

[17] On monomial representations of finite groups. Osaka Math. J. 6 (1954), 119-127.

[18] (with Bertram Huppert) Über die Auflösbarkeit faktorsierbarer Gruppen. II. Math. Z. 61 (1954), 94-99.

[19] On the number of isomorphic classes of nonnormal subgroups in a finite group. Acta Sci. Math. Szeged 16 (1955), 9-11.

[20] On primitive permutation groups. Acta Sci. Math. Szeged 16 (1955), 207-228.

[21] Über das Produkt von zwei abelschen Gruppen. Math. Z. 62 (1955), 400-401.

[22] Über eine zur Frattini-Gruppe duale Bildung. Nagoya Math. J. 9 (1955), 123-127.

[23] Über die Frattini-Gruppe einer endlichen Gruppe. Proc. Japan Acad. 31 (1955), 327-328.

[24] (with Jenö Szép) Über die Faktorisation von Gruppe. Acta Sci. Math. Szeged, 16 (1955), 229-231.

[25] Über das Produkt von zwei zyklischen 2-Gruppen. Publ. Math. Debrecen 4 (1956), 517-520.

[26] (et Ôhara, Akiko) Sur les groupes factorisables par deux 2-

groupes cycliques. I. Cas où leur groupe des commutateurs est cyclique. Proc. Japan Acad. 32 (1956), 736-740.

[27] II. Cas où leur groupe des commutateurs n'est pas cyclique. Proc. Japan Acad. 32 (1956), 741-743.

[28] (Und Szép, J.) Über nichtauflösbare endliche Gruppen. Acta Sci. Math. Szeged 17 (1956), 76-82.

[29] Normalteiler mehrfach transitiver Permutationsgruppen. Math. Z. 70 (1958), 165-173.

[30] Über den kleinsten p-Durchschnitt auflösbarer Gruppen. Arch. Math. 9 (1958), 27-32.

[31] Zur Theorie der Permutationsgruppen vom Grad p. Math. Z. 74 (1960), 299-301.

[32] Faktorisierung endlicher auflösbarer Gruppen. Math. Z. 74 (1960), 392-413.

[33] Über die Gruppen $PSL_n(q)$, die eine Untergruppe von Primzahlindex enthalten. Acta Sci. Math. (Szeged) 21 (1960), 206-217.

[34] Zur Theorie der transitiven Gruppen vom Grad p. II. Math. Z. 75 (1960/61), 127-135.

[35] On a class of doubly transitive permutation groups. Illinois J. Math. 6 (1962), 341-352.

[36] A note on transitive permutation groups of degree p. Osaka Math. J. 14 (1962), 213-218.

[37] On transitive simple permutation groups of degree 2p. Math. Z. 78 (1962), 453-468.

[38] On transitive simple groups of degree 3p. Nagoya Math. J. 21 (1962), 123-158.

[39] A note on $SL_r(q)$. Arch. Math. 13 (1962), 331-333.

[40] (with Jenö Szép) Über die Quasinormalteiler von endlichen Gruppen. Acta Sci. Math. Szeged 23 (1962), 168-170.

[41] Transitive permutation groups of degree p = 2q+1, p and q being prime numbers. Bull. Amer. Math. Soc. 69 (1963), 165-192.

[42] A note on transitive permutation groups of degree p = 2q+1, p and q being prime numbers. J. Math. Kyoto Univ. 3 (1963), 111-113.

[43] Transitive permutation groups of degree p = 2q+1, p and q being prime numbers. II. Trans. Amer. Math. Soc. 113 (1964), 454-487.

[44] Transitive permutation groups of degree p = 2q+1, p and q being prime numbers. III. Trans. Amer. Math. Soc. 116 (1965), 151-166.

[45] Un teorema sui gruppi transitivi di grado primo. Rend. Sem. Mat. Univ. Padova 35 (1965), 132-133.

[46] Über die Darstellungen der Permutationsgruppen von Primzahlgrad. Math. Z. 89 (1965), 196-198.

[47] On doubly transitive groups of degree n and order 2(n-1)n. Nagoya Math. J. 27 (1966), 409-417.

[48] On transitive permutation groups of Fermat prime degree. Proc. Internat. Conf. Theory of Groups (Canberra, 1965), pp. 191-202. Gordon and Breach, New York, 1967.

[49] On permutation groups of prime degree p which contain (at least) two classes of conjugate subgroups of index p. Rend Sem. Mat.

Univ. Padova 38 (1967), 287-292.

[50] On a class of doubly, but not triply transitive permutation groups. Arch. Math. (Basel) 18 (1967), 564-570.

[51] On a conjecture of J. S. Frame. Nagoya Math. J. 30 (1967), 79-81.

[52] On uniprimitive permutation groups of degree 2p. Math. Z. 102 (1967), 238-244.

[53] A theorem on Jordan groups, in "Theory of finite groups" Benjamin (1969), 47-48.

[54] Note on the characters of solvable groups. Nagoya Math. J. 39 (1970), 23-28.

[55] On permutation groups of prime degree p which contain at least two classes of conjugate subgroups of index p. II. Nagoya Math. J. 37 (1970), 201-208.

[56] On finite groups with given conjugate types.II. Osaka J. Math. 7 (1970), 231-251.

[57] On finite groups with given conjugate types. III. Math. Z. 117 (1970), 267-271.

[58] On factorizable groups. Representation theory of finite groups and related topics (Proc. Sympos. Pure Math., Vol.XXI, Univ. Wisconsin, Madison, Wis., 1970), pp. 77-83. Amer. Math. Soc., Providence, R. I., 1971.

[59] A theorem of factorizable groups. Acta Sci. Math. (Szeged) 33 (1972), 49-52.

[60] Simple groups of conjugate type rank 4. J. Algebra 20 (1972),

226-249.

[61] Normal subgroups of quadruply transitive permutation groups. Hokkaido Math. J. 1 (1972), 1-6.

[62] A note on transitive permutation groups of degree 2p. Commemoration volumes for Prof. Dr. Akitsugu Kawaguchi's seventieth birthday, Vol. III. Tensor (N.S.) 26 (1972), 105-106.

[63] Simple groups of conjugate type rank +5. Finite groups '72 (Proc. Gainesville Conf., Univ of Florida, Gainesville, Fla., (1972), pp. 84-97. North-Holland Math. Studies, Vol.7, North-Holland, Amsterdam, 1973.

[64] Simple groups of conjugate type rank 5. J. Math. Kyoto Univ. 13 (1973), 171-190.

[65] On factorizable groups. Symposia Mathematica, Vol. XIII (convegno di Gruppi e loro Rappresentazioni, INDAM, Roma, Dicembre, 1972), pp.357-366. Academic Press, London, 1974.

[66] On t-designs. Proc. International Symp. on Theory of Groups (1974), Sapporo, 69-73.

[67] On tight 4-designs. Osaka J. Math. 12 (1975), 493-522.

[68] On Wielandt number of transitive permutation groups of prime degree. Acta Math. Acad. Sci. Hungar. 26 (1975), 267-274.

[69] Corrections and supplements to "On tight 4-designs". (Osaka J. Math. 12 (1975), 493-522). Osaka J. Math. 15 (1978), 693-697.

[70] On a conjecture of C. W. Norman. I. J. Combin. Theory Ser. A 27 (1979), 85-99.

[71] (with Enomoto, Hikoe and Noda, Ryuzaburo) Tight 4-designs. Osaka J. Math. 16 (1979), 39-43.

[72] Hadamard matrices with "doubly transitive" automorphism groups. Arch. Math. (Basel) 35 (1980), 100-111.

[73] Note on Hadamard matrices of Pless type. Hokkaido Math. J. 9 (1980), 129-134.

[74] A note on symmetric codes over GF(3). Hokkaido Math. J. 9 (1980), 138-139.

[75] Symmetry codes over GF(3). J. Combin. Theory Ser. A 29 (1980), 251-253.

[76] (with Leon, Jeffrey S. and Longyear, Judith Q.) Classification of 3-(24,12,5) designs and 24-dimensional Hadamard matrices. J. Combin. Theory, Ser. A 31 (1981), 66-93.

[77] Note on Hadamard matrices of type Q. Studia Sci. Math. Hung. 16 (1981), 389-393.

[78] Doubly regular tournaments of Szekeres type. J. Aust. Math. Soi., Ser. A 32 (1982),399-404.

[79] (with Leon, Jeffrey S.) A Hadamard matrix of order 36. J. Combin. Theory, Ser. A 34 (1983), 244-247.

[80] On a certain class of connected symmetric trivalent graphs. Math. J. Okayama Univ. 25 (1983), 145-152.

[81] On a conjecture of Kiyasu Zen'iti. Mem. Konan Univ. 30 (1983), 1-5.

[82] On a family of conjugacy classes graph. Mem. Konan Univ. 31

(1984), 105-112.

[83] (with Kimura, Hiroshi) Studies on Hadamard matrices with "2-transitive" automorphism groups. J. Math. Soc. Japan 36 (1984), 63-73.

Contractible Edges in 3-connected Graphs

Kiyoshi Ando

Department of Fundamental Sciences

Nippon Ika University

Kawasaki, 211 Japan

Hikoe Enomoto

Akira Saito

Department of Information Science

Faculty of Science

University of Tokyo

Hongo, Bunkyo-ku, Tokyo, 113 Japan

ABSTRACT

In [5], Thomassen proved that every 3-connected graph of order at least five has an edge whose contraction results in a 3-connected graph. We call such an edge a contractible edge and study the distribution of contractible edges in 3-connected graphs. As a consequence, we prove that every 3-connected graph has at least $\left\lceil \frac{|G|}{2} \right\rceil$ contractible edges and determine the graphs which attain the equality.

In this paper, we only consider finite simple graphs. In [5], Thomassen gave a simple proof to Kuratowski's criterion for graphs to be planar. In his proof, he used the following theorem as a tool for an induction argument.

Theorem A. (Thomassen [5]) *Every 3-connected graph of order at least five has an edge whose contraction results in a 3-connected graph.*

In this paper, we call an edge whose contraction results in a 3-connected graph *a contractible edge*, and study the distribution of contractible edges in 3-connected graphs. As a consequence, we prove that every 3-connected graph of order $p \geq 5$ has at least $\left\lceil \frac{p}{2} \right\rceil$ contractible edges and determine the extremal graphs.

Let G be a graph. We denote by $V(G)$ and $E(G)$ the set of vertices and the set of edges, respectively. We write $\Gamma_G(x)$ for the set of vertices adjacent to x in G, $d_G(x)$ for the degree of x in G, and $|G|$ for the order of G. For $S \subset V(G)$, $\Gamma_G(S) = \bigcup_{x \in S} \Gamma_G(x)$ and $G-S$ is the subgraph of G induced by $V(G)-S$. If $G-S$ has at least two connected components, we call S a cutset of G. Furthermore, S is called a least cutset if $|S| = \kappa(G)$, where $\kappa(G)$ is the connectivity of G. We denote by $C(G)$ the set of least cutsets of G. Let $E_c(G)$ be the set of contractible edges of G. An edge which is not contractible is called non-contractible. For $x \in V(G)$, $E(x)$ is the set of edges which are incident with x. Notation not defined here can be found in [1].

Lemma 1. *Let G be a 3-connected graph of order at least five and $x \in V(G)$. Suppose $d_G(x)=3$, say $\Gamma_G(x)=\{a,b,c\}$. If both xb and xc are non-contractible, then b and c are adjacent and $d_G(b)=d_G(c)=3$.*

Proof. Since the edge xc is non-contractible, there exists $S \in C(G)$ such that $x,c \in S$. Since $d_G(x)=3$, $G-S$ has exactly two connected components, say A and B. We may assume $a \in A$ and $b \in B$. Similarly, there exists $T \in C(G)$ such that $x,b \in T$ and $G-T$ has exactly two connected components. Let C and D be the components of $G-T$ and assume $c \in C$ and $a \in D$. Let

$$X_1=(A\cap T)\cup(S\cap T)\cup(S\cap D)$$

and

$$X_2=(B\cap T)\cup(S\cap T)\cup(S\cap C).$$

Assume $A\cap T=\phi$. Since $A\cap D\neq\phi$ ($a\in A\cap D$), X_1 is a cutset of G. On the other hand, since $A\cap T=\phi$, $|S|=3$ and $c\in S\cap C$, we have $|X_1|\leq 2$. This contradicts the assumption that G is 3-connected. Hence we have $A\cap T\neq\phi$. Since $|T|=3$, we have $|A\cap T|=1$, $S\cap T=\{x\}$ and $B\cap T=\{b\}$. By a similar argument as above, we have $|S\cap D|=1$ and $S\cap C=\{c\}$.

Next assume $B\cap C\neq\phi$. Then X_2 is a cutset of G. Since $|X_2|=3$, $X_2\in C(G)$. However, since $d_G(x)=3$, $\Gamma_G(x)\cap B\cap C=\phi$. Hence $X_2-\{x\}$ is also a cutset of G. This is a contradiction. Hence we have $B\cap C=\phi$. Similarly, we have $A\cap C=B\cap D=\phi$ and hence $B=\{b\}$ and $C=\{c\}$. Then $\Gamma_G(b)=S$ and $\Gamma_G(c)=T$. This implies the desired properties. ▪

Let

$$U_i=\{x\in V(G)\mid d_G(x)=3,|E(x)\cap E_c(G)|=i\}\quad(i=0,1,2,3)$$

and

$$W_i=\{x\in V(G)\mid d_G(x)\geq 4,|E(x)\cap E_c(G)|=i\}\quad(i\geq 0).$$

Obviously, $V(G)=(\bigcup_{i=0}^{3}U_i)\cup(\bigcup_{i\geq 0}W_i)$.

Theorem 2. *Let G be a 3-connected graph of order at least five. Then each vertex of degree three has a contractible edge incident with it.*

Proof. The theorem says $U_0=\phi$. In order to prove it, we assume $U_0\neq\phi$, say $x\in U_0$, and $\Gamma_G(x)=\{a,b,c\}$. Since xa and xb are non-contractible, $ab\in E(G)$ and $d_G(a)=d_G(b)=3$ by Lemma 1. Similarly, we have bc, $ca\in E(G)$ and $d_G(c)=3$. Hence G is a complete graph of order four. This is a contradiction. ▪

For a 3-connected graph G and $x\in V(G)$, we define $\Gamma^{(1)}(x)$ and $\Gamma^{(2)}(x)$ by

$$\Gamma^{(1)}(x)=\{y\in\Gamma_G(x) \mid xy \text{ is contractible }\}$$

and

$$\Gamma^{(2)}(x)=\{y\in\Gamma_G(x) \mid xy \text{ is non-contractible }\}.$$

For $y\in\Gamma_G(x)$, let $C_x(y)=\{K\in C(G) \mid x,y\in K\}$ and $C_x=\bigcup_{y\in\Gamma^{(2)}(x)} C_x(y)$.

Theorem 3. *Let G be a 3-connected graph of order at least five, $x\in V(G)$, and $X\subset V(G)$. Suppose $\Gamma^{(1)}(x)\subset X$, $d_G(x)\geq 4$, and there exists $S\in C_x$ such that $G-S$ has a connected component which is disjoint from X. Then $(\Gamma^{(2)}(x)-X)\cap U_2\neq\phi$.*

Proof. Define

$$C'_x=\{S\in C_x \mid G-S \text{ has a connected component } A \text{ such that } A\cap X=\phi\}.$$

By the assumption $C'_x\neq\phi$. For each $S\in C'_x$, let A_S be the smallest component which is disjoint from X. We choose S such that $|A_S|$ is minimum. Let $B_S=V(G)-(S\cup A_S)$. Since $S\in C(G)$ and $x\in S$, $\Gamma_G(x)\cap A_S\neq\phi$. Let $a\in\Gamma_G(x)\cap A_S$.

Since $A_S\cap X=\phi$, $a\in\Gamma^{(2)}(x)$. Let $T\in C_x(a)$ and let C be a connected component of $G-T$ and $D=V(G)-(T\cup C)$. Let

$$X_1=(S\cap C)\cup(S\cap T)\cup(A_S\cap T)$$

and

$$X_2=(S\cap C)\cup(S\cap T)\cup(B_S\cap T).$$

First we claim that $S\cap C\neq\phi$. Assume $S\cap C=\phi$. Since $a\in A_S\cap T$, $|X_2|\leq 2$. If $B_S\cap C\neq\phi$, then X_2 is a cutset of G, contradicting the assumption that G is 3-connected. Hence $B_S\cap C=\phi$. Since $B_S\cap C=S\cap C=\phi$, $C=A_S\cap C\neq\phi$. Then X_1 is a cutset of G. Since $X_1\subset T$ and $T\in C(G)$, $X_1=T$. Since $A_S\cap C\subsetneq A_S$, $T\in C'_x$. This contradicts the minimality of A_S. Thus we have $S\cap C\neq\phi$. By the same argument as above, $S\cap D\neq\phi$. Since $|S|=3$ and $x\in S\cap T$, $|S\cap C|=|S\cap T|=|S\cap D|=1$.

Next we claim that $B_S\cap T\neq\phi$. Assume the contrary. Then $B_S\cap C\neq\phi$ or $B_S\cap D\neq\phi$. We may assume $B_S\cap C\neq\phi$. Then X_2 is a cutset of G and $|X_2|\geq 3$.

However, since $B_S \cap T=\phi$, $|X_2|=2$, a contradiction. Hence $B_S \cap T\neq\phi$. Since $a\in A_S \cap T$, we have $|B_S \cap T|=1$ and $A_S \cap T=\{a\}$.

Assume $A_S \cap C\neq\phi$. Then $X_1\in C'_x$. However, $G-X_1$ has a connected component which is a subset of $A_S \cap C$. This contradicts the minimality of A_S. Therefore, we have $A_S \cap C=\phi$. Similarly, we have $A_S \cap D=\phi$, and hence $A_S=\{a\}$. Obviously, $\Gamma_G(a)=S$ and $d_G(a)=3$.

Let $y\in S-\{x\}$ and assume the edge ay is non-contractible. Then by Lemma 1, $d_G(x)=3$, contradicting the assumption that $d_G(x)\geq 4$. Hence $ay\in E_c(G)$. This implies $a\in U_2$. ▪

Corollary 4. *Let G be a 3-connected graph of order at least five and $x\in W_1$. Then* $|\Gamma^{(2)}(x)\cap U_2|\geq 2$.

Proof. Let $\Gamma^{(1)}(x)=\{x'\}$. Let $y\in\Gamma^{(2)}(x)$ and $S_1\in C_x(y)$. Since $|G|\geq 5$, $G-S_1$ has a component which does not contain x'. Now by applying Theorem 3 to $X=\Gamma^{(1)}(x)=\{x'\}$, we obtain $\Gamma^{(2)}(x)\cap U_2\neq\phi$. Let $a_1\in\Gamma^{(2)}(x)\cap U_2$ and $S_2\in C_x(a_1)$. Then $G-S_2$ has a component which does not contain x'. Again applying Theorem 3 to $X=\{x',a_1\}$, we have $(\Gamma^{(2)}(x)-\{a_1\})\cap U_2\neq\phi$, and the result follows. ▪

Corollary 5. *Let G be a 3-connected graph of order at least five and $x\in W_0$. Then* $|\Gamma^{(2)}(x)\cap U_2|\geq 3$.

Proof. Since $x\in W_0$, $\Gamma^{(1)}(x)=\phi$. First applying Theorem 3 to $X=\phi$, we obtain $\Gamma^{(2)}(x)\cap U_2\neq\phi$. Let $b_1\in\Gamma^{(2)}(x)\cap U_2$ and $S_1\in C_x(b_1)$. Then no component of $G-S_1$ contains b_1. By applying the theorem to $X=\{b_1\}$, we infer $(\Gamma^{(2)}(x)-\{b_1\})\cap U_2\neq\phi$. Let $b_2\in(\Gamma^{(2)}(x)-\{b_1\})\cap U_2$ and $S_2\in C_x(b_2)$. Then $G-S_2$ has a component which does not contain b_1. By the theorem, $(\Gamma^{(2)}(x)-\{b_1,b_2\})\cap U_2\neq\phi$. Let $b_3\in(\Gamma^{(2)}(x)-\{b_1,b_2\})\cap U_2$. Then $\{b_1,b_2,b_3\}\subset\Gamma^{(2)}(x)\cap U_2$. ▪

By Corollaries 4 and 5, the following theorem immediately follows.

Theorem 6. *Let G be a 3-connected graph of order at least five. Then* $|U_2| \geq 2|W_1| + 3|W_0|$.

Now using Theorems 2 and 6, we obtain a lower bound of $|E_c(G)|$.

Theorem 7. *Let G be a 3-connected graph of order at least five. Then*

(1) $|E_c(G)| \geq \left\lceil \frac{|G|}{2} \right\rceil$.

(2) *Equality holds in* (1) *if and only if G satisfies the following two conditions.*

(2-1) *G is 3-regular.*

(2-2) *Each vertex of G lies on a triangle.*

Proof.

(1) By Theorem 2, $V(G) = (\bigcup_{i=1}^{3} U_i) \cup (\bigcup_{i\geq 0} W_i)$. By the definitions of U_i and W_i, $2|E_c(G)| = \sum_{i=1}^{3} i|U_i| + \sum_{i\geq 0} i|W_i|$. Using Theorem 6,

$$\begin{aligned} 2|E_c(G)| &\geq \sum_{i=1}^{3} |U_i| + 2|W_1| + 3|W_0| + 2|U_3| + \sum_{i\geq 1} i|W_i| \\ &= \sum_{i=1}^{3} |U_i| + \sum_{i\geq 0} |W_i| + 2|W_0| + 2|W_1| + |W_2| + 2|U_3| + \sum_{i\geq 3} (i-1)|W_i| \\ &\geq |G| + 2|W_0| + 2|W_1| + |W_2| + 2|U_3| + 2\sum_{i\geq 3} |W_i| . \qquad \text{(A)} \end{aligned}$$

Therefore, we have the desired inequality.

(2) Let G be a 3-connected graph satisfying (2-1) and (2-2). Define $E_0 \subset E(G)$ by

$E_0 = \{e \in E(G) \mid e \text{ lies on a triangle of } G\}$.

By contraction of $e \in E_0$, we have a vertex of degree two. Thus all members of E_0 are non-contractible. Furthermore, $|E_0 \cap E(x)| \geq 2$ for all $x \in V(G)$ by (2-2). Thus we have $|E_0| \geq |G|$. Since G is 3-regular, $|E(G)| = \frac{3}{2}|G|$. Hence

$$|E_c(G)| \leq |E(G) - E_0| \leq \frac{3}{2}|G| - |G| = \frac{1}{2}|G|$$

and by (1), $|E_c(G)| = \frac{1}{2}|G|$.

Next we prove the converse. First we claim that $|G|$ is even. Assume that $|G|$ is odd. Then G cannot be 3-regular, and hence $\bigcup_{i\geq 0} W_i \neq \phi$. Also we have $2|E_c(G)|=|G|+1$. By (A), $\bigcup_{i\neq 2} W_i=\phi$, which implies $W_2\neq\phi$, and $U_3=\phi$. Hence $V(G)=U_1\cup U_2\cup W_2$. Then

$$|U_1|+|U_2|+|W_2|+1=|G|+1=2|E_c(G)|=|U_1|+2|U_2|+2|W_2|$$

yielding $|U_2|+|W_2|=1$. Since $W_2\neq\phi$, $|W_2|=1$ and $U_2=\phi$. Let $W_2=\{x\}$ and $\Gamma^{(2)}(x)=\{x_1,x_2\}$. Since $x_1\in U_1$, x_1 has two non-contractible edges, one of which is xx_1. Thus we have $d_G(x)=3$ by Lemma 1. This contradicts the assumption that $x\in W_2$. Thus $|G|$ is even.

Since $|G|$ is even, $|G|=2|E_c(G)|$. By (1), $\bigcup_{i\geq 0} W_i=\phi$ and $U_3=\phi$. Therefore, G is 3-regular and $V(G)=U_1\cup U_2$. Then $|G|=|U_1|+|U_2|$ and $2|E_c(G)|=|U_1|+2|U_2|$. This implies $U_2=\phi$ and $V(G)=U_1$. Let $x\in V(G)$ and $\Gamma^{(2)}(G)=\{y,z\}$. By Lemma 1, $yz\in E(G)$ and x lies on a triangle induced by $\{x,y,z\}$. •

Let G be an n-connected graph and $F\subset E(G)$. Suppose $|F|=n$ and F is independent. Lovász [4] and Woodall [6] independently conjectured that, if n is even or $G-F$ is connected, then G has a cycle containing all edges of F. The conjecture is proved by Lovász [4] for $n\leq 3$, and recently for $n=4$ by Kaneko [2].

Now, as an example of an application of Theorem 7, we give an alternate proof to the conjecture for $n=3$.

Proposition 8. (Lovász [3, section 6 problem 67], [4]) *Let G be a 3-connected graph and $F\subset E(G)$. Suppose $|F|=3$, F is independent and $G-F$ is connected. Then G has a cycle which contains all edges of F.*

Proof. Let $F=\{f_1,f_2,f_3\}$ and $f_i=a_ib_i$ $(i=1,2,3)$. Assume the contrary and let G be a counterexample. We take $|G|$ as small as possible. Since $|F|=3$ and F is independent, $|G|\geq 6$ and hence $|E_C(G)|\geq 3$. If $|E_C(G)|=3$, we can easily infer that $G \cong K_2 \times K_3$ by Theorem 7 (2), where K_n is a complete graph of order n. However, the proposition is true for $K_2 \times K_3$. Hence $G \not\cong K_2 \times K_3$ and $|E_C(G)| \geq 4$. Let $e \in E_C(G)-F$ and $e=xy$. Let G' be a graph obtained from G by contraction of e and z be the vertex obtained by identifying x and y. Let f_i' be an edge which results from f_i by the contraction and let $f_i'=a_i'b_i'$. Let $F'=\{f_1', f_2', f_3'\}$. Since F is independent in G, $|F'|=3$. Suppose F' is not independent. Then we may assume $a_1'=a_2'=z$. Let $G''=G'-z+b_1'b_2'$. Then G'' is a 2-connected graph and G'' has a cycle C'' containing $b_1'b_2'$ and $a_3'b_3'$. From C'', we can easily construct a cycle in G containing all edges of F. However, this is a contradiction. Hence F' is independent. Next assume $G'-F'$ is connected. Then G' has a cycle C' which contains all edges of F'. From C', we can also construct a cycle C in G which contains all edges of F, contradicting the assumption. Therefore, $G'-F'$ is not connected.

Since G' is 3-connected, $G'-F'$ has exactly two components, say D_1' and D_2'. Let D_i be the set of vertices of G corresponding to D_i' $(i=1,2)$. We may assume $a_i \in D_1$ and $b_i \in D_2$ $(i=1,2,3)$. Since $G-F$ is connected, we may assume $a_1=x$, $y \in D_1$, and $yb_1 \in E(G)$. Since F is independent, $|D_1| \geq 3$ and $|D_2| \geq 3$.

Suppose D_2-b_1 is disconnected. Then for some component K of D_2-b_1, $|K \cap \{b_2, b_3\}| \leq 1$. This contradicts the assumption that G is 3-connected. Hence D_2-b_1 is connected. Next assume D_1 has a cutvertex c. Then for some component K' of D_1-c, $|\Gamma_G(K') \cap D_2| \leq 1$. This is also a contradiction. Hence D_1 is 2-connected.

Since D_2-b_1 is connected, there exists a path P_2 in D_2-b_1 which joins b_2 and b_3. Since D_1 is 2-connected, there exists a path P_1 in D_1 which joins a_2 and a_3 and contains an edge a_1y. From P_1-a_1y, P_2, F and an edge yb_1 we can construct a cycle C containing all edges of F. This is a final contradiction and the proof is complete. •

Acknowledgement. The authors would like to thank Professor Yoshimi Egawa for helpful discussions.

References.

[1] M. Bezhad, G. Chartrand and L. Lesniak-Foster, Graphs and Digraphs, Prindle, Weber & Schmidt, Boston MA, 1979.

[2] A. Kaneko, private communication.

[3] L. Lovász, Combinatorial Problems and Exercises, North-Holland, Amsterdam, 1979.

[4] L. Lovász, Problem 5, *Period. Math. Hungar.* 4 (1974), 82.

[5] C. Thomassen, Planarity and duality of finite and infinite graphs, *J. Combinatorial Theory Ser.* B 29 (1980) 244-271.

[6] D.R. Woodall, Circuits containing specified edges, *J. Combinatorial Theory Ser.* B 22 (1977) 274-278.

平方位数の translation plane について

大阪大学教養部　　平峰 豊

1. Introduction.

translation plane についての研究は、新しい plane を構成すること, collineation group の一般的性質を調べること, 既知の plane を その collineation group のもつ性質（置換群的な または 抽象群として）から特徴付けること, など を中心として行われている。とくに新しい plane の構成については、最近、非デザルグ的 plane の無限列が次々と見つかっているが、その大部分は translation plane である。その中でも、Kernel 上 2次元のものとして構成されているものが圧倒的に多い。Kernel 上 2次元のものでまだ知られていないものもかなりあるだろうと予想されるので、この最小次元の場合でさえ完全な分類にはまだ多くの困難があるというのが現状であるように思う。

2. Translation plane, spread, spread set. ([4])

$K = GF(q)$, $V = V(2n, q)$ とする。V のいくつ

かの n 次元 K-部分空間の集合 $\mathcal{S}$ が次の2条件をみたすとき V の <u>*spread*</u> という。

(1) $W_1, W_2\ (\neq) \in \mathcal{S} \longrightarrow W_1 \cap W_2 = 0$

(2) $\bigcup_{W \in \mathcal{S}} W = V$

(定義より $|\mathcal{S}| = (q^{2n}-1)/(q^n-1) = q^n+1$)

与えられた spread $\mathcal{S}$ に対して次のように affine plane が構成され これにより射影平面が定まる。

点 : V の q^{2n} 個のベクトル全体

直線 : $q^{2n}+q^n$ 個の剰余類 $W+v\ (W \in \mathcal{S},\ v \in V)$ 全体

Incidence : 集合としての包含関係.

この affine plane を $\mathcal{S}$ により定まる(<u>Kernel 上 n 次元の</u>) <u>*translation plane*</u> といい. <u>$\pi(\mathcal{S})$</u> で表わす。

$\mathcal{S}$ の2元 W_1, W_2 は $V = W_1 \oplus W_2$ をみたすから. 基底を W_1, W_2 からとることにすれば. $\mathcal{S}$ は次の2元を含むと仮定することができる。

$\{(0, y) \mid 0=(0,0,\cdots,0) \in V(n,q),\ y \in V(n,q)\}$ ($=V(\infty)$ と書く)

$\{(x, 0) \mid 0=(0,0,\cdots,0) \in V(n,q),\ x \in V(n,q)\}$ ($=V(0)$ と書く)

$W \in \mathcal{S}$ が. $W \neq V(\infty), V(0)$ とすれば. $W \cap V(\infty) = W \cap V(0) = 0$ であるから 適当な $M \in GL(n,q)$ をとれば. $W = \{(x, xM) \mid x \in V(n,q)\}$ と書ける。

Wを簡単に $y=xM$ と書く. $V(0)$は $y=0$, $V(\infty)$は $x=0$ と表わされる. $\Sigma=\{M \mid y=xM$は$\mathcal{S}$の元$\}$ とおくとき, これは次の (i) (ii) をみたす。

(i) $GL(n,q)\cup\{0\}\supset\Sigma\ni 0$, $|\Sigma|=q^n$

(ii) $M, N\in\Sigma$, $M\neq N \rightarrow \det(M-N)\neq 0$

((i)は定義より, (ii)は spread の条件(1) よりでる)

逆に $GL(n,q)\cup\{0\}$ の部分集合 Σ が上の(i)(ii)を満たすとき, <u>spread set</u> という。Σ から自然に spread が構成できる。これを <u>$\mathcal{S}(\Sigma)$</u> と書く。

π を V 上で定義された translation plane とする。$V=V(2n,q)$とし, 記号は今までと同じにとるとき, $R=\{\sigma_v \mid \sigma_v(x)=x+v\ (\forall x\in V(n,q)),\ v\in V(n,q)\}$ はπの自己同型群に含まれ明らかに V上 regular に作用する。 $\mathrm{Aut}(\pi)\triangleright R$ が知られている。従って $\mathrm{Aut}(\pi)=R\cdot(\mathrm{Aut}\,\pi)_0$ 。 ここで$(\mathrm{Aut}\,\pi)_0$は 0の stabilizer であり これを <u>$C(\pi)$</u> と書き, πの <u>translation complement</u> という。 次が知られている。([4]): $C(\pi)\leq \Gamma L(n,q)$, $\mathrm{Aut}(\pi)=R\cdot C(\pi)$(半直積)。

<u>$LC(\pi)$</u>$=C(\pi)\cap GL(n,q)$ とおき <u>linear translation complement</u> という。

3. Kernel 上2次元の translation plane

以下では前節で $n=2$ の場合について考える。spread set Σ ($\subset GL(2,q)\cup O$) の任意の元を $M=\begin{pmatrix} x & y \\ f & g \end{pmatrix}$ とするとき、spread set の定義の(ii)より f, g は x, y だけで unique に定まる。従って $K\times K \longrightarrow K$ なるある写像 f, g があって、$\Sigma=\left\{\begin{pmatrix} x & y \\ f(x,y), & g(x,y) \end{pmatrix} \;\middle|\; x, y\in K\right\}$ の形に書ける。

例1. $q\equiv 1 \pmod 2$ とし x^2-u が K 上既約となるように $u\in K$ を選ぶ。このとき $\Sigma=\left\{\begin{pmatrix} x & y \\ uy & x \end{pmatrix} \;\middle|\; x, y\in K\right\}$ とおけば、Σ は spread set となる。$\Sigma \simeq GF(q^2)$ で Σ により定まる plane はデザルグ平面である。

例2. $r, s\in K$ で x^2-rx-s は K 上既約であるとする。

$$f(x,y)=\begin{cases} 0 & (y=0) \\ -\dfrac{x^2-rx-s}{y} & (y\neq 0) \end{cases}, \quad g(x,y)=\begin{cases} x & (y=0) \\ -x+r & (y\neq 0) \end{cases}$$

により f, g を定め、$\Sigma=\left\{\begin{pmatrix} x & y \\ f(x,y), & g(x,y) \end{pmatrix} \;\middle|\; x, y\in K\right\}$ とおけば、Σ が spread set であることが容易に確かめられる。これにより得られる plane が Hall plane

(と同型) であることも確かめられる。また $P = \left\{ \begin{pmatrix} T & 0 \\ 0 & T \end{pmatrix} \middle| \, T = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}, t \in K \right\}$ とおけば、

P は spread $\mathcal{S}(\Sigma)$ を不変にすることが直接計算により容易に分かるので、$P \le LC(\pi)$, $(\pi = \pi(\Sigma))$ である。つまり $q \mid |LC(\pi)_{V(0), V(\infty)}|$ (☆)

4. Hall plane の一般化

一般に $C(\pi)$ は V のベクトル 0 を固定するので $\mathcal{S}$ の置換を引起している。$C(\pi)$ の部分群が $\mathcal{S}$ の2元以上を固定しているとき autotopism group という。前節の (☆) より Hall plane は order q の linear autotopism group をもつ。

注: π により定まる projective plane を π^* とするとき $C(\pi) \le Aut(\pi^*)$ とみることができるが、$C(\pi)$ の無限遠直線 $l_\infty (\in \pi^*)$ への作用は $C(\pi)$ の $\mathcal{S}$ への作用と完全に同一である。

次に $\tilde{\Phi}_K$ と Φ_K を定義する。K から K への写像を $h(x)$, $K^\# = K - \{0\}$ から K への写像 $r(y)$, $s(y)$ をとり

$$f(x,y) = \begin{cases} h(x) & (y=0) \\ -\dfrac{x^2 - r(y)x - s(y)}{y} & (y \ne 0) \end{cases}, \quad g(x,y) = \begin{cases} x & (y=0) \\ -x + r(y) & (y \ne 0) \end{cases}$$

とおく。

これが次の条件をみたすとする。

(1) $x \in K$, $y_1, y_2 (\neq) \in K^{\#} \longrightarrow f(x, y_1) \neq f(x, y_2)$

(2) $K = f(x, K^{\#}) \cup h(x) \quad \forall x \in K$

(3) $h(0) = h(1) = 0$

このような (r, s, h) の全体を $\widetilde{\Phi}_K$ と表わす。$\widetilde{\Phi}_K$ の元で h が零写像となるものの全体を Φ_K で表わす。

$\sigma = (r, s, h) \in \widetilde{\Phi}_K$ に対して

$$\Sigma_\sigma = \left\{ \begin{pmatrix} x & y \\ f(x,y) & g(x,y) \end{pmatrix} \middle| x, y \in K \right\}$$ とおく。この時

<u>補題</u>　Σ_σ は spread set である。

前節(☆)をみたすような translation plane は次の定理のようにのべることができる。

<u>定理</u>　π を Kernel $K = GF(q)$ 上 2次元の plane とする。π が order q の linear autotopism group をもつための必要十分条件は $\pi \cong \pi(\Sigma_\sigma)$ となるような $\sigma \in \widetilde{\Phi}_K$ が存在することである。

order q の linear autotopism group をもつ plane が Hall plane 以外にも最近いくつかみつけられている。

(a) Hall plane of order q^2 : $r(y) = c$, $s(y) = d$, $h(x) = 0$, ただし $c, d \in K$, $x^2 - cx - d$ は K 上既約。

(b) Narayana Rao - Satyanarayana により構成された

plane : $q=5^{2n+1}$, $r(y)=3y^{-1}$, $s(y)=-3y^{-2}$

$h(x)=0$ ([5])

(c) Cohen-Ganley により構成された plane : [1]

(1) $q=p^n$, $p>2$, $r(y)=0$, $s(y)=k y^{1-p^m}$,

$k \notin \{t^2 \mid t \in K\}$, $0 \leqq m < n$, $h(x)=0$

(2) $q \equiv -1 \pmod 6$, $r(y)=3y^{-1}$, $s(y)=-3y^{-2}$,

$h(x)=0$

(3) $q \equiv \pm 3 \pmod{10}$, $r(y)=5y^{-2}$, $s(y)=-5y^{-4}$,

$h(x)=0$.

この表記法でみれば (C) の (2) は次のように拡張できることが容易に分かる。

<u>補題</u> $q \equiv -1 \pmod 3$, $r(y)=3y^{-1}$, $s(y)=-3y^{-2}$

$h(x)=0$ (つまり $q=2^{\text{巾}}$ にも拡張できる)

とおけば $(r, s, h) \in \Phi_K$.

無限列というわけではないが Φ_K の元を作ることができる:

q の値が小さいときに $(r, s, 0) \in \Phi_K$ の可能なものをマイコンを用いて調べることができる。この方法で得たものがいくつかあるが、そのうち $r(y)$, $s(y)$ の式が比較的簡単なものをいくつか書くと (a) $q=7$, $r(x)=4x^5+6x^4$, $s(x)=6x^5+3x^4$

$+6x^3+4x^2+3$ ($\tilde{b}$) $q=11$, $r(x)=5x^9+6x^7+9x^6+2$, $s(x)=3x^9+5x^8+6x^7+9x^6+4x^5+10x^4+9x^3+2x^2+9$ ($\tilde{c}$) $q=11$, $r(x)=2x^9+6x^8+4x^7+3x^6+8$

$s(x)=5x^9+x^8+8x^6+10x^5+x^4+2x^3+10x^2+10$

これらも何か無限列の一部であろうと考えられるが今のところよく分からない。([2] [3])

先の例 (a) (b) (c) の plane はすべて $\mathcal{S}$ 上に長さ q^2-q の orbit をもつ linear autotopism group を $LC(\pi)$ の subgroup として含んでいる。ここで次のことが言える。

<u>定理</u> $\pi=\pi(\mathcal{S})$ を kernel $K=GF(q)$ 上 2次元の translation plane とする。π の linear autotopism group で $\mathcal{S}$ 上長さ q^2-q の orbit をもつものがあれば $\pi\cong\pi(\Sigma_\sigma)$ $^\exists\sigma\in\Phi_K$ である。ここで $\sigma=(r,s,0)$ は $r(y)=ay^n$, $s(y)=by^{2n}$, $a,b\in K$, $0\leq n<q-1$ の形のものである。

<u>注</u>: 上の定理は a,b,n の可能性をすべて決定していない。たぶん先の (a) (b) (c) にあげたものと補題でのべたものに尽きるのではないかと思われるが

証明はされていない。　　　　また $(\hat{a}),(\hat{b}),(\hat{c})$ などの例を含めて考えても $h(x) \neq 0$ なる (r, s, h) の例は知られていない。$\widetilde{\Phi}_K = \Phi_K$ と予想される。

問題 1. $\{a, b, n\}$ をすべて決定せよ。

問題 2. $\widetilde{\Phi}_K = \Phi_K$ を示せ。(つまり $h=0$ を示せ)

文献

[1] S.D. Cohen and M.J. Ganley : Some classes of translation planes, preprint

[2] Y. Hiramine : A generalization of Hall quasi-fields, to appear

[3] Y. Hiramine : On translation planes of order q^2 which admit an autotopism group having an orbit of length q^2-q, to appear

[4] H. Lüneburg : Translation planes, Springer-Verlag, Berlin-Heidelberg-New York, 1980.

[5] M.L. Narayana Rao and K. Satyanarayana : A new class of square planes, J. Combin. Theory Ser. A 35 (1983), 33-42.

28次のアダマール行列

愛媛大　理　木村浩
愛媛大　教育　大森博之

2-(27, 13, 6) デザインで 3個のブロックの共通元の個数は高々5である事は容易にわかりますが、今それが5である場合のデザインを計算機を用いて構成する事を前回の研究集会[1]で報告しましたが、その方法によりますとあまりにもたくさんのデザインが出来すぎて(おそらく数十万個)、分類が不可能と思われます。

今回は上記の方法によってデザインの9行(ブロック)までを決定する過程の間にデザインをアダマール行列にうめこみ、アダマール行列として同値なものを除くという方法により類別する事を考えます。

1° 2-(27, 13, 6) デザインの点の集合 $\Omega=\{1,2,\cdots,27\}$ のいくつかの部分集合を

$A_1=\{1,2,\cdots,5\}$, $A_2=\{6\}$, $A_3=\{7\}$, $A_4=\{8\}$,
$A_5=\{9,10,\cdots,14\}$, $A_6=\{15,16,\cdots,20\}$, $A_7=\{21,\cdots,26\}$

$A_8=\{27\}$とおきます。 また第i番目のブロックをB_iとします。この時条件をみたすデザインは一般性を失う事はなく $B_1=A_1\cup A_2\cup A_3\cup A_5$, $B_2=A_1\cup A_2\cup A_4\cup A_6$, $B_3=A_1\cup A_3\cup A_4\cup A_7$ とする事が出来ます。

2° 4番目以降のブロックBの決定の仕方は、$|B\cap B_i|=13$ $(i=1,2,3)$ より $|B\cap A_i|=x_i$ $(1\leq i\leq 8)$ とすると 下記の表のように 8組の解が得られますが、それぞれの解の組を pattern 1 ~ pattern 8 と名付けます。そして4番目以降のブロックの内 pattern i のブロックの個数を y_i とすると 解は下記の表のようになります。

X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8		
3	0	0	0	3	3	3	1	---	PATTERN 1
2	0	0	1	4	3	3	0	---	PATTERN 2
2	0	1	0	3	4	3	0	---	PATTERN 3
2	1	0	0	3	3	4	0	---	PATTERN 4
2	0	1	1	3	3	2	1	---	PATTERN 5
2	1	0	1	3	2	3	1	---	PATTERN 6
2	1	1	0	2	3	3	1	---	PATTERN 7
1	1	1	1	3	3	3	0	---	PATTERN 8

Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8
4	3	3	3	3	3	3	2

3° 2°の結果をふまえてデザインを以下のように配置する事にします。 $B_4\sim B_7$ に Pattern 1 $B_8\sim B_9$ に Pattern 8, $B_{10}\sim B_{12}$ に Pattern 2 $B_{13}\sim B_{15}$ に Pattern 7,

$B_{16} \sim B_{18}$ に Pattern 3　$B_{19} \sim B_{21}$ に Pattern 6,
$B_{22} \sim B_{24}$ に Pattern 4　$B_{25} \sim B_{29}$ Pattern 5. を
それぞれ y_i $(1 \leq i \leq 8)$ 個 もってくる事にします。
その理由は, $\Omega - \{A_2 \cup A_3 \cup A_4 \cup A_8\} \ni P$ に
対し
$$\sum_{j=4}^{7} |\{P\} \cap B_j| = \begin{cases} \sum_{j=19}^{22} |\{P\} \cap B_j| + 2 & \text{if } P \in A_1 \\ \sum_{j=19}^{10} |\{P\} \cap B_j| + 1 & \text{if } P \notin A_1 \end{cases}$$
及び $i = 1, 2, 3$ に対し
$$\sum_{j=6(i+1)-2}^{6(i+1)} |\{P\} \cap B_j| = \begin{cases} \sum_{j=6i+7}^{6i+9} |\{P\} \cap B_j| + 1 & \text{if } P \in A_{i+4} \\ \sum_{j=6i+9}^{6i+9} |\{P\} \cap B_j| & \text{if } P \notin A_{i+4} \end{cases}$$
なる関係式が成立し デザインが存在する為の必要条件を与えているからです。

4° $A^* = A_1 \times (\bigcup_{i=4}^{9} B_i)$ とします。この時デザインの存在性により また同値なものを除くと 一般性を失う事なく A^* は下記の5通りに類別出来ます。それを Type 1 ～ Type 5 と名付けます。しかし Type 4 及び Type 5 から来るデザインは 下記の理由により Type 1 ～ Type 3 に帰着出来る事がわかります。例えば Type 5 から出来るデザイン D についていえば, D の結合行

列と 0行 0列の成分がすべて1をもつアダマール行列 H にうめこみます。そして 0列と1列を入れかえ 0列を normalize した後のアダマール行列の 0行 0列を取り除いて再びデザイン D に変換すると，D の最初の3つのブロックの会合数は5で更に A^* の状態は下の Figure となります。ここで Figure に点の置換 $\begin{pmatrix} 1&2&3&4&5 \\ 2&1&3&4&5 \end{pmatrix}$ 及びブロックの置換 $\begin{pmatrix} B_4&B_5&B_6&B_7&B_8&B_9 \\ B_4&B_8&B_9&B_7&B_6&B_5 \end{pmatrix}$

を施す事により Type 2 と同じになります。同じような方法により Type 4 から出来るデザインを転置したものは Type 5 から導き出せる事がわかります。Type 1～Type 3 については，上のような考え方では，一方から他方へ移る事はありません。

```
 TYPE 1          TYPE 2          TYPE 3
1 2 3           1 2 3           1 2 3
    3 4 5       1     4 5         2   4 5
  2   4 5       1   3   5         2 3 4
1     4 5       1 2   4         1     4 5
        5       1                     4
      4         1                 2

 TYPE 4          TYPE 5          FIGURE
1 2 3           1 2 3           1 2 3
1     4 5           3 4 5         2
1     4 5           3 4 5         2
1 2 3           1 2   4         1 2   4
1                     4           2 3   5
1                   3             2   4 5
```

5° Type 1 ～ Type 3 の各々について $(\bigcup_{i=5}^{7} A_i) \times (\bigcup_{j=4}^{9} B_j)$ の部分を決定していくのですが，その場合 A^* の Automorphism によるブロックの入れかえ，$A_i \times (\bigcup_{j=4}^{9} B_j)$ の compliment をとり $\{A_i \times (\bigcup_{j=4}^{9} B_j)\}$ $(i=5,6,7)$ の中での入れかえ，更にデザインをアダマール行列にうめこみ，0行と i行 $(i=1,2,3)$ を入れかえ normalize したあと再びデザインに変換する等の方法により場合を分けると結局 $\Omega \times (\bigcup_{j=4}^{9} B_j)$ は Type 1 のものが 20通り，Type 2 のものが 37通り，Type 3 のものが 54通りに分類出来る事がわかります。

6° 一般に位数 n のアダマール行列 H（その成分を +，− とする）に対し H の任意の $4 \times n$ 小行列の各列に + の個数が偶数か奇数によりそれぞれ $1, -1$ を対応させ 1の総和を M とすると M は 4の倍数である事がわかります。$M = 4m$ とするとアダマールの性質より一般性を失う事なく $0 \leqq m \leqq [\frac{n}{8}]$ とする事が出来ます。この m を 'キャス数'(?) と呼ぶ事にします。

所で 5° のそれぞれの場合についてデザインを求めるのですが，それらが同値（アダマール行列の意

味で）か否かの判定に対し上述のキヤス数を用いて判定する事を考えます。
28次のアダマール行列の場合 3行を固定した時残り25行のうち1行をつけ加えて，そのキヤス数がmの行の個数を $K_m(28)$ とすると
$\{K_1(28)=1,\ K_3(28)=24\}$ 又は $\{K_2(28)=3,\ K_3(28)=22\}$
のいずれかとなります。更に28次のアダマール行列の2行を固定した時残り26行から2行選んで出来る ${}_{26}C_2$ 個のキヤス数のうち，キヤス数が1となる行の組は唯一組という事がわかります。そこで5°で求めたデザインをアダマール行列(H)にうめこみ，Hの各行に対してキヤス数が1となるものの分布を求め，その分布によってデザインを分類する事にします。
その手法によりますと現在の所少くとも300個以上の同値でない（アダマール行列の意味で）デザインが存在する事がわかっています。

[1] 代数的組み合せ論の研究（1983年）報告集 P.96−101

Distance-Regular Graphs with Fixed Valency

伊藤達郎（上越教育大学）

Γを distance-regular graphs (DRG)，kとdをそれぞれ valency と diameter とする。Γは ordinary n-gon ではない ($k \geq 3$) と仮定する。

予想　ある関数fが存在して、$d < f(k)$。特にkを固定すると、valency kの DRG は有限個。

distance-transitive graphs に関して、この予想は正しい (Cameron-Praeger-Saxl-Seitz [2])。Cameron 達の証明は本質的に単純群の分類を使用しているが、elementary な証明が最近 Weiss によってなされたそうである。DRG に関して、この予想の証明をいくつかの steps に分けて、坂内英一氏（オハイオ州立大学）と共に試みている。

Γの intersection matrix を

$$B = \begin{pmatrix} 0 & c_1 & & & \\ k & a_1 & \ddots & & \\ & b_1 & \ddots & c_{d-1} & \\ & & \ddots & a_{d-1} & c_d \\ & & & b_{d-1} & a_d \end{pmatrix}$$

とする。valency k を固定すれば、$c_i + a_i + b_i = k$ より、相異なる columns $\begin{pmatrix} c_i \\ a_i \\ b_i \end{pmatrix}$ は有限個しかない。よく知られた不等式 $k = b_0 \geq b_1 \geq b_2 \geq \cdots \geq b_{d-1} \geq 1$, $1 = c_1 \leq c_2 \leq \cdots \leq c_d \leq k$ より

$$\begin{pmatrix} c_{s+1} \\ a_{s+1} \\ b_{s+1} \end{pmatrix} = \begin{pmatrix} c_{s+t} \\ a_{s+t} \\ b_{s+t} \end{pmatrix} \Rightarrow \begin{pmatrix} c_{s+1} \\ a_{s+1} \\ b_{s+1} \end{pmatrix} = \begin{pmatrix} c_{s+\nu} \\ a_{s+\nu} \\ b_{s+\nu} \end{pmatrix} \quad (1 \leq \nu \leq t)$$

が成立するので、columns の sequence $\begin{pmatrix} c_i \\ a_i \\ b_i \end{pmatrix}$ は

$$\overbrace{\begin{matrix} 1 & \cdots & 1 \\ 0 & \cdots & 0 \\ k-1 & \cdots & k-1 \end{matrix}}^{t_0\text{個}} \quad \overbrace{\begin{matrix} c_{t_0+1} & \cdots & c_{t_0+1} \\ a_{t_0+1} & \cdots & a_{t_0+1} \\ b_{t_0+1} & \cdots & b_{t_0+1} \end{matrix}}^{t_1\text{個}} \quad \overbrace{\begin{matrix} \cdots\cdots \\ \cdots\cdots \\ \cdots\cdots \end{matrix}}^{t_2\text{個}} \quad \begin{matrix} \cdots\cdots \\ \cdots\cdots \\ \cdots\cdots \end{matrix}$$

ここで $\begin{pmatrix} 1 \\ 0 \\ k-1 \end{pmatrix} \neq \begin{pmatrix} c_{t_0+1} \\ a_{t_0+1} \\ b_{t_0+1} \end{pmatrix} \neq \cdots\cdots$

という形をしている。予想を証明するには、各々の t_i が

kの関数で bound されることを示せばよい。Ivanov [4] は、各々の t_i が t_0 と k の関数で bound されることを示した(従って diameter d も、t_0 と k の関数で bound される)。これが DRG の diameters の評価に関して知られている最も良い結果である。

技術的理由により、はじめにあげた予想の証明を次のような steps に分ける。

<u>Step 1</u>　$c_i = b_i$ なる columns $\begin{pmatrix} c_i \\ a_i \\ b_i \end{pmatrix}$ の個数を k の関数で bound する。

<u>Step 2</u>　valency 3 の DRG、および valency 4 の bipartite DRG の diameters を bound する。
(valency 3 の (bipartite) DRG は分類済 Ito [3]。)

<u>Step 3</u>　bipartite DRG の diameters を k の関数で bound する。

<u>Step 4</u>　一般の場合。

ここでは Step 1 をとりあつかう。

<u>定理</u> (Bannai - Ito [1])

$$\begin{bmatrix} c_s \\ a_s \\ b_s \end{bmatrix} \neq \begin{bmatrix} c_{s+1} \\ a_{s+1} \\ b_{s+1} \end{bmatrix} = \begin{bmatrix} c_{s+t} \\ a_{s+t} \\ b_{s+t} \end{bmatrix} \qquad (s \geq 1)$$

とする。$c_{s+1} = b_{s+1}$ ならば、t は k の関数で bound される。

<u>証明の概略</u> (1) $c_i = c$, $a_i = a$, $b_i = b$ とおく ($c = b$)。A を Γ の adjacency matrix とする。A の second largest eigenvalue θ に注目する (largest eigenvalue は valency k)。まず

$$k - b - c + 2\sqrt{bc}\cos\frac{3\pi}{t+1} < \theta$$

を示す。$b = c$ より $t \to \infty$ のとき $\theta \to k$ となる。

(2) θ の A における重複度を $m(\theta)$ とすると、Biggs の公式 $m(\theta) = n \Big/ \left(\sum_{i=0}^{d} v_i(\theta)^2 / v_i(k) \right)$ (ここで n は Γ の点の数, $v_i(x)$ は次の漸化式により定まる i 次の多項式: $v_0(x) = 1$, $v_1(x) = x$, $b_{i-1} v_{i-1}(x) + a_i v_i(x) + c_{i+1} v_{i+1}(x) = x\, v_i(x)$) を使って

$$m(\theta) < (k^2+sk)\left(\frac{v_s(k)}{v_s(\theta)}\right)^2$$

が容易に示せる。次に s に independent な $\varepsilon=\varepsilon(k,t)>0$ が存在して、

$$\left|\frac{v_s(k)}{v_s(\theta)}\right| < k^{\varepsilon} \qquad \text{for } k-\frac{1}{2k}<\theta<k$$

かつ $\lim_{t\to 0}\varepsilon = 0$ を示す。以上より $t>t_0(k)$ のとき $m(\theta)$ はほぼ k^2+sk で bound されることが分る。

(3) 一方 Terwilliger [5] の結果とその改良（girth 3 の場合）により、

$$m(\theta) > 2\left(\frac{k}{2}\right)^{\left[\frac{s}{2}\right]} - 1.$$

これを (2) でおめた upper bound と比較して、$t>t_0(k)$ なら s は k の関数で bound され、従って Ivanov [4] の結果によっても k の関数で上から bound される。

References

1. Bannai E. and Ito T., On Distance-Regular Graphs with Fixed Valency, submitted to Graphs and Combinatorics.

2. Cameron P.J., Praeger C.E., Saxl J. and Seitz G.M., On the Sims Conjecture and Distance-Transitive Graphs, Bull. London Math. Soc., 15 (1983), 499–506.

3. Ito T., Bipartite Distance-Regular Graphs of Valency Three, Linear Alg. Appl., 46 (1982), 195–213.

4. Ivanov A.A., Bounding the Diameter of a Distance-Regular Graph, Soviet Math. Dokl., 28 (1983), 149–152.

5. Terwilliger P., Eigenvalue Multiplicities of Highly Symmetric Graphs, Discrete Math., 41 (1982), 295–302

An Analogue of t-Designs in the Association Schemes of Alternating Bilinear Forms

宗政 昭弘

P. Delsarte は彼の学位論文 [4] において、design の概念を任意の association scheme に拡張した。これは、Johnson scheme における普通の t-(v,k,λ) design の自然な一般化になっている。また、知られている (P and Q)-polynomial association scheme のほとんどについては、design の幾何的意味が知られている。

§1 では、Delsarte による design の代数的定義を説明するために、有限群を例にとる。§2 では、§1で述べたことを distance-regular graph について並行した議論をして、(P and Q)-polynomial association scheme とその t-design の定義を与える。§3 では、known (P and Q)-polynomial association scheme での t-design の幾何的意味について、過去に知られていた結果と、今回得られた結果を述べる。

§1. 置換群の transitive subset

Gを有限群，$C_0=\{1\}, C_1, \cdots, C_d$をその共役類，$\chi_0 = 1_G, \chi_1, \ldots, \chi_d$を既約指標とする。また，$H$を$G$の部分群とし，$G/H$上の$G$の置換表現に現われる$G$の既約指標を$\chi_0, \chi_1, \cdots, \chi_t$となるように番号をつけておく。$G$の部分集合$Y$に対して

$$a_i = \frac{1}{|Y|}|\{(x,y)\in Y\times Y \mid xy^{-1}\in C_i\}| \quad (0\le i\le d)$$

とおき，$a=a_Y=(a_0,\cdots,a_d)$をYの <u>inner distribution</u> という。Yが部分群なら，$a_i=|Y\cap C_i|$である。次に，QをGの character table を転置したもの，すなわち，$Q_{ij}=\chi_j(a_i)$ $(a_i\in C_i)$とおく。Yの <u>dual inner distribution</u> を$\hat{a}=\hat{a}_Y=\frac{1}{|Y|}a_YQ$で定義する。容易に$\hat{a}_0=1$がわかる。例えば，$Y=H$とすると，$\hat{a}_i=(\chi_i|_H, 1_H)_H=(\chi_i, 1_H^G)_G$となるから初めに仮定したことから，$\hat{a}_i\ne 0$ $(i=1,\cdots,t)$ $\hat{a}_i=0$ $(i=t+1,\cdots,d)$となる。それでは，$\hat{a}_Y=(1,\overbrace{0\cdots 0}^{t},*)$となる$Y$はどのようなものだろうか。つまり，dual inner distributions が，ある意味で直交する（すなわち$(\hat{a}_H)_i(\hat{a}_Y)_i=0$ $(i=1,2,\cdots d)$）Yを求めよという問題である。この問題は，Enomoto-Ito の Lemma として，伊藤[8]

の中で解決されている。その結果は、

"$\hat{a}_Y = (1, \overbrace{0 \cdots 0}^{t}, *, \cdots *)$　if and only if

Y は transitive set on G/H."

ただし、ここで、G の subset Y が <u>transitive</u> とは、

"$\forall \alpha, \beta \in G/H \quad \exists y \in Y \quad \alpha^y = \beta$"

だけではなくて、

☆ "$\forall \alpha, \beta \in G/H \quad |\{y \in Y \mid \alpha^y = \beta\}|$ は α, β によらず

一定 (>0)"

を意味する。Y が部分群ならば上の2つの条件は同値となる。また、☆は次の条件と同値である。

"$\forall x, y \in G \quad |Y \cap H| = |Y \cap xHy|$"

$\hat{a}_Y$ の成分は、既約指標 $\chi_0, \chi_1, \cdots, \chi_d$ で parametrize されているので、$(a_Y)_i = 0 \quad i = 1, \cdots, t$ となる Y を、$\{\chi_1, \chi_2, \ldots, \chi_t\}$- design という。これが、Delsarte の design の定義の特別な場合である。既約指標の並べ方を初めに決めているので、$\{\chi_1, \cdots, \chi_t\}$-design のことを t-design と言う訳にはいかない。しかし、§2 では、もっと良い状況 (Q-polynomial association scheme) を設定して t-design を考える。

§2. Distance-regular graphs と (P and Q)-polynomial association scheme

$\Gamma=(X,R)$ を distance-regular graph とする。(定義については、例えば Biggs [2]) ここで、X は頂点の集合、$R\subset X\times X$ は辺の集合とする。グラフ Γ における距離を ∂ で表し、

$$R_i=\{(x,y)\in X\times X \mid \partial(x,y)=i\} \qquad i=0,1,\cdots,d=\mathrm{diam}\,\Gamma$$

とおく。このとき $(X,\{R_i\}_{i=0,\cdots,d})$ は symmetric association scheme になる。(cf [1]) R_i の adjacency matrix を A_i とすると、A_i は A_1 の i 次多項式で表わされることが知られている：$A_i=v_i(A_1)$, $\deg v_i=i$。また、A_1 は相異なる $d+1$ 個の固有値 $\theta_0=$ valency of Γ, $\theta_1,\ldots,\theta_d$ をもつことも知られている。固有値 θ_i の重複度を m_i とおく。さて、有限群の character table に対応する行列 Q を定義しよう。Q の (i,j) 成分 Q_{ij} を $Q_{ij}=m_j v_i(\theta_j)/k_i$, ただし、$k_i=|R_i|/|X|$, と定義する。

注) Q は second eigenmatrix と呼ばれ、任意の association scheme について定義できる。特に、有限群には association scheme の構造を入れることができて、その

とき定義されるQはcharacter tableと"ほぼ"同じものになる。詳しくは [1, §2.7] 参照。

さて、Qの列はA_1の固有値θ_jによってparametrizeされているが、さらに、条件

(*) $\theta_1, \cdots \theta_d$ をてきとうに並べたとき、Qの第j列はQの第1列のj次多項式になる。

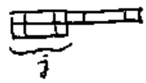
を満たすものを考える。Distance-regular graphであって、(*)を満たすものを <u>(P and Q)-polynomial association scheme</u> という。(*)はあまり強い条件ではなく、実際、次のような予想もある。([1], P.312])

<u>予想</u> Primitive distance-regular graph で diameterが十分大きければ (*)は必ず満たされる。

<u>例</u> Johnson scheme $J(v, k)$.

$X = \binom{\Omega}{k}$, ただし $|\Omega| = v \geq 2k$. $X \ni x, y$ が adjacent $\Leftrightarrow$ $|x \cap y| = k-1$ とする。このとき graph X は、Ω上の対称群S_vによってdistance-transitiveで、$\partial(x, y) = i \Leftrightarrow |x \cap y| = k - i$, diameter $= k$ である。従って adjacency matrices の生成する algebra は、Hecke環 $\mathcal{H}(S_v, S_k \times S_{v-k})$ と同型である。A_1 の固有値

$\theta_0, \cdots \theta_d$ は $\mathcal{H}(S_v, S_k \times S_{v-k})$ の表現と対応していて、それらはまた、S_v の置換表現 $S_v/S_k \times S_{v-k}$ の既約成分と対応している。この対応を通して、

$\theta_j \longleftrightarrow$ 

により θ_j の番号付けを与える。(右辺は S_v の既約表現に対応する Young 図形である。) このとき条件(*)が満たされる。従って $J(v,k)$ は (P and Q)-polynomial association scheme になる(詳しい証明は [1, §3.2] 参照)

前おきが長くなったが、(P and Q)-polynomial association scheme について §1 にならって議論を展開しよう。
$(X, \{R_i\}_{0\le i\le d})$ を (P and Q)-polynomial association scheme. すなわち、(X, R_1) が distance-regular graph で(*)をみたすとする。X の部分集合 Y に対して、

$$a_i = \frac{1}{|Y|}\left|\{(x,y)\in Y\times Y \mid \partial(x,y)=i\}\right| = \frac{1}{|Y|}\left|(Y\times Y)\cap R_i\right|$$

とおき、$a = a_Y = (a_0, \cdots, a_d)$ を Y の <u>inner distribution</u> という。Y の <u>dual inner distribution</u> を $\hat{a} = \hat{a}_Y = \frac{1}{|Y|} aQ$ で定義する。我々の目的は、§1 にあったような有限群の、部分群と、transitive subset に対応するものを、知られている (P and Q)-polynomial association scheme について

見つけることである。

<u>例</u> Johnson scheme $J(v,k)$ (k=diameter)

$X=\binom{\Omega}{k}$ の部分集合Z_tを次のように定義する. $T\in\binom{\Omega}{t}$ を固定し. $Z_t=\{x\in X \mid x\supset T\}$。このとき、$Z_t$の dual inner distribution が $(1,\overbrace{*,\cdots,*}^{t},0\cdots 0)$ $(*\neq 0)$ となることは. 直接計算によって確かめられる（Qの成分は知られている [1, §3.2]） それでは. $\hat{a}_Y=(\hat{a}_0,\cdots \hat{a}_d)$ が $\hat{a}_i=0$ $(i=1,\cdots,t)$ となるYはどのようなものだろうか。この答は. 次の定義と定理から導びかれる。

<u>定義</u> $(X,\{R_i\}_{i=0,\cdots,d})$を association scheme とする。Xの2つの部分集合Y, Zの dual inner distributions を $\hat{a}_Y=((\hat{a}_Y)_i)$ $\hat{a}_Z=((\hat{a}_Z)_i)$ とおく。このとき

YとZは design orthogonal $\underset{def}{\Longleftrightarrow}$ $(\hat{a}_Y)_i(\hat{a}_Z)_i=0$ $(i=1,\cdots,d)$

<u>定理</u> (Delsarte [6], Roos [10]) $(X,\{R_i\}_{i=0,\cdots,d})$ を association scheme, Y, Z を Xの部分集合とする。$\{R_i\}_{i=0,\cdots,d}$ がある X上の置換群Gの、$X\times X$ 上の orbitであると仮定する。このとき. Y, Zが design orthogonal

$$\Longleftrightarrow |Y\cap Z|=|Y\cap gZ| \quad \forall g\in G$$

Johnson scheme が distance-transitive であることから定理の仮定はみたされ $G=S_v$, $\{g\mathfrak{Z}_t \mid g\in G\}=\{\{x\in X \mid x\supset T\} \mid T\in\binom{\Omega}{t}\}$ となることから、次の定理を得る。

<u>定理</u> Johnson scheme $J(v,k)$ の部分集合 Y の dual inner distribution $\hat{a}=(\hat{a}_0,\cdots,\hat{a}_d)$ が $\hat{a}_i=0$ $(i=1,2,\cdots,t)$ となる必要十分条件は、Y が t-(v,k,λ) design のブロックの集合となることである。

この定理は、Delsarte [4] によって初めて証明された。

<u>定義</u> $(X,\{R_i\}_{i=0,\cdots,d})$ を (P and Q)-polynomial association scheme とする。X の部分集合 Y が t-design であるとは、Y の dual inner distribution $\hat{a}=(\hat{a}_0,\cdots,\hat{a}_d)$ が、$\hat{a}_i=0$ $(i=1,\cdots,t)$ のときをいう。

前定理より、この定義は、Johnson scheme での普通の意味の t-design の拡張になっている。

§3. Known (P and Q)-polynomial association scheme における t-design の幾何的意味

この § では、§2 で述べた t-design の抽象的な定義を幾何的に言い換えることを考える。Known (P and Q)-polynomial association scheme のうちで、t-design の幾何的意味がわかっているものは次のとおりである。

1. Johnson scheme　$X = \binom{\Omega}{k}$　$|\Omega| = v \geq 2k$

　$X \supset Y$ が t-design $\Leftrightarrow$ Ω の $^\forall t$ 点部分集合に対して、それを含む Y の元の数は一定数 λ

2. q-analogue of Johnson scheme. $v \geq 2k$ とし $X = \left[{V \atop k} \right] = \{V$ の k 次元部分空間全体$\}$, ただし、V は v 次元ベクトル空間 $/ GF(q)$。$X \ni x, y$ が adjacent $\Leftrightarrow \dim(x \cap y) = k-1$

　$X \supset Y$ が t-design $\Leftrightarrow$ V の $^\forall t$-次元部分空間に対して、それを含む Y の元の数は一定数 λ。

3. Dual Polar Spaces　V: ベクトル空間 $/ GF(q)$ で非退化な symplectic or hermitian or quadratic form が定義されているとする。$X = \{V$ の極大全等方的部分空間$\}$ とし、$X \ni x, y$ が adjacent $\Leftrightarrow \dim(x \cap y) = \dim x - 1$

$X \supset Y$ が t-design $\Leftrightarrow$ V の $^\forall t$ 次元全等方的部分空間に対し

それを含む Y の元の数は一定数入。

4. Hamming scheme $H(n,q)$　$X = F^n$　$|F| = q$　とし．

$X \ni x, y$ が adjacent $\Leftrightarrow$ x, y の成分がただ一個所で異なる。

$X \supset Y$ が t-design $\Leftrightarrow$ Y は orthogonal array of strength t

すなわち $\{1, 2, \cdots, n\}$ の $^\forall t$ 点部分集合 $\{i_1, \cdots, i_t\}$

と F の $^\forall t$-tuple $(a_1, \cdots, a_t)$ に対して $y_{i_j} = a_j$

$(j = 1, \cdots, t)$ となる $y = (y_i) \in Y$ の数は一定数入。

5. Association scheme of bilinear forms　V, W を $GF(q)$ 上の d, m 次元ベクトル空間 $(d \leq m)$ とし．$X = \{ \gamma : V \times W \to GF(q) \mid \gamma$ は bilinear$\}$ とおく。

$X \ni \gamma, \delta$ が adjacent $\Leftrightarrow$ $\mathrm{rank}(\gamma - \delta) = 1$

$X \supset Y$ が t-design $\Leftrightarrow$ V の $^\forall t$ 次元部分空間 U と $^\forall$bilinear

form $\delta : U \times W \to GF(q)$ に対して．

δ の拡張となっている $\gamma \in Y$ の数は一定数入。

以上 1.−5. の t-design の意味づけは、Delsarte [5] によって開発された方法、X を semi-lattice に埋め込む、という方法で、具体的には伊藤 [8] による。しかし、次に掲げる 6.−8. はこの方法ではうまくいかない。

6. Association scheme of alternating bilinear forms.

V：n次元ベクトル空間 / $GF(q)$. $X = \{V$上の alternating forms$\}$.

$X \ni \gamma, \delta$ が adjacent $\Leftrightarrow$ $\mathrm{rank}(\gamma - \delta) = 2$

7. Association scheme of hermitian bilinear forms

V：n次元ベクトル空間 / $GF(q^2)$ $X = \{V$上の hermitian forms$\}$

$X \ni \gamma, \delta$ が adjacent $\Leftrightarrow$ $\mathrm{rank}(\gamma - \delta) = 1$

8 Association scheme of quadratic forms

V：n次元ベクトル空間 / $GF(q)$ $X = \{V$上の quadratic forms$\}$

$X \ni \gamma, \delta$ が adjacent $\Leftrightarrow$ $\mathrm{rank}(\gamma - \delta) = 1$ or 2 ただし この rankについては [1, P.309] を見よ。

このうち、6.については、§2 の Delsarte, Roos の定理を用いることにより次の結果が得られた。

<u>定理</u> (Munemasa [9]) X：association scheme of alternating bilinear forms on V. $X \supset Y$ について次は同値.

(1) Y は t-design

(2) $^\forall U$：$2t$次元のVの部分空間と$^\forall \delta$：U上の alternating formに対して δの拡張となっている $\gamma \in Y$の数は一定

(3) (2) において $\dim U = 2t+1$ とおいたもの.

6. については、$GL(V)$ と $\gamma \mapsto \gamma+\delta$ $(\gamma, \delta \in X)$ で生成されるX上の置換群によって distance-transitive になっているので、この定理の証明は、

$$Z_{2t} = \{\gamma \in X \mid \gamma|_U = 0\} \qquad \dim U = 2t$$

$$Z_{2t+1} = \{\gamma \in X \mid \gamma|_{U'} = 0\} \qquad \dim U' = 2t+1$$

の dual inner distribution $\hat{a} = (\hat{a}_0, \cdots, \hat{a}_d)$ $d = [\frac{n}{2}]$ が $\hat{a}_i \neq 0$ $(i=1,\cdots t)$, $\hat{a}_i = 0$ $(i=t+1,\cdots,d)$ を示すことに帰着される。(これが言えれば §2 の Delsarte, Roos の定理を使える。)

7. 8 については、今のところ t-design の意味づけは知られていない。しかし、7 については、6 とほぼ同様の方法で意味づけができるものと期待している。8 については、distance-transitive でないため、§2 の Delsarte, Roos の定理が適用できない。(例 1.－7. はすべて distance-transitive である。)

REFERENCES

1. E.Bannai and T.Ito, "Algebraic Combinatorics I, Association Schemes", Benjamin/Cummings, Menlo Park, California, 1984.
2. N.L.Biggs, "Algebraic Graph Theory", Cambridge Univ. Press, Cambridge,1974.
3. A.M. Cohen, A synopsis of known ditance-regular graphs with large diameters, Mathematisch Centrum report ZW165.81, Amsterdam, 1981.
4. P.Delsarte, An algebraic approach to the association schemes of coding theory, Philips Research Reports Supplements, No.10 (1973).
5. ——, Association schemes and t-designs in regular semilattices, J. of Combinatorial Theory (A) 20,(1976).
6. ——, Pairs of vectors in the space of an association scheme, Philips Research Reports 32 (1977), 373-411.
7. —— and J.M.Goethals, Alternating bilinear forms over GF(q), J. of Combinatorial Theory (A) 19 (1975), 26-50.
8. 伊藤達郎 , Codes and designs in association schemes, 代数的組合せ論シンポジウム報告集, 岡山大学 (1983).
9. A.Munemasa, An analogue of t-designs in the association schemes of alternating bilinear forms, preprint.
10. C.Roos, Designs and anti-designs in association schmes, Delft Progress Reports, Delft Univ., the Netherlands, 1982.

球面の配列

筑波大数学系　八牧宏美

"同じ大きさの球を空間にどの程度密に重複することなく配列できるか？"と云う問題は非常にむずかしく3次元以上については一般的な解答は得られていないようである。格子配列とよばれる特殊な配列に限っても最密な配列は Lagrange, Gauss, Korkine-Zolotareff, Blichfeldt によって8次元以下の場合に知られているにすぎない。それらは $Z_1, L_2, D_3, D_4, D_5, E_6, E_7, E_8$ と呼ばれるものである。(添字は対応する次元を表わす。）　一般の配列では1次元では Z_1 が2次元では L_2 が最密な配列であることが Rogers などによって示されている。3次元については1958年 Rogers が球は空間の .7796 を越えては配列できないことを証明した。この結果は 1/4 世紀余り最良の評価を与えるものであった。さて

$$\beta = 243\sqrt{2}\left(5\tan^{-1}\sqrt{3} - 5\tan^{-1}\sqrt{2} + \tan^{-1}11\sqrt{3} - \tan^{-1}11\sqrt{2}\right)/208$$

とおく。この値はおよそ .7784 である。最近

Lindsey は次の結果を得た。

<u>定理</u>: 3辺の長さ l, m, n の直方体の内部に配列できる単位球の体積と直方体の体積の比は

$$\beta(l+2)(m+2)(n+2)/lmn$$

を越えることはできない。

$l, m, n \longrightarrow \infty$ のとき上の値は β に収束するのでこの定理は Rogers の結果を26年ぶりに大巾に改良したことになる。 3次元空間で実際に知られている最大密度は .7405 程度である。 従って Lindsey の結果の改良ならびに高次元への拡張が考えられるが現状では極めて困難なことのように思われる。

参考文献

1. H.S.M. Coxeter, Twelve Geometric Essays, Southern Illinois Univ. Press, 1968.
2. J.H. Lindsey, Sphere packing in R^3, Preprint.
3. C.A. Rogers, Packing and Covering, Cambridge Univ. Press, 1964.
4. N.J.A. Sloane, The packing of spheres, Scientific American 250, 116-125.

有限群における非平方元について

富蘭 平太 (巴里大)

$\Gamma = GF(p^s)$の時、affine 変換群を考えよう:

$\{ax+b : a, b \in \Gamma, a \neq 0\} = A(s,p)$.

$A(s,p)$ の p-sylow 部分群は、$T_s = \{x+b : b \in \Gamma\}$ である。$T_s \triangleleft A(s,p)$ と、T_s は elementary abelian だから、$1 \neq c \in T_s$ について、$x^p = c$ $x \in A(s,p)$ は解をもたない。

任意の群 G に対して、$N_p(G) = \{g \in G : x^p = g \ \ x \in G$ が解をもたない$\}$、とする。また、$n_p(G) = |N_p(G)|$ とする。すると、$N_p(A(s,p)) = \{x+b : 0 \neq b \in \Gamma\}$ と $n_p(A(s,p)) = p^s - 1 < \sqrt{|A(s,p)|} = \sqrt{p^s(p^s-1)}$ である。$p \nmid |G|$ のとき明らかに $n_p(G) = 0$ である。

三年程前、E. Bertram [1] は $A(s,2)$ を除いてすべての偶数位数の有限群 G に対して、$n_2(G) > \sqrt{|G|}$ が成り立つと予想しました。

定理. Gを有限可解群とする。$p \mid |G|$, $G \not\cong A(s,p)$ $(s = 0, 1, \cdots)$ とすると、$n_p(G) > \sqrt{|G|}$である。

証明. $|G|$ に関する帰納法で証明する。

Case 1. Gのある正規部分群Nがあって$p \mid |G:N|$のとき。
明らかに、$g\in G$, $gN\in N_p(G/N)$ならば、$g\in N_p(G)$。
従って $n_p(G)\geq |N|n_p(G/N)$となる。もし、$n_p(G/N)>\sqrt{|G/N|}$ならば、$n_p(G)>|N|\sqrt{|G/N|}>|G|$となる。また、
もし $n_p(G/N)\leq\sqrt{|G/N|}$ならば 帰納法の仮定によって、
$G/N\cong A(s,p)$。すなわち、ある $s\geq 1$ に対して $|G/N|=p^s(p^s-1)$, $n_p(G/N)=p^s-1$ である。$|N|=d$とおく。このとき $|G|=dp^s(p^s-1)$, $n_p(G)\geq d(p^s-1)$である。これより、$n_p(G)>\sqrt{|G|}$ をえる。

Case 2. Gのすべての正規部分群Nに対してpが$|G:N|$を割りきらないとき。
NをGの極小正規部分群とする。$p \mid |G|$なので $p \mid |N|$。
従って、$|N|=p^s$, Nは elementary abelian である。($\because G$:可解)
$p\nmid |G:N|$なのでNはGのp-Sylow部分群である。Hallの定理によってGは位数$|G:N|$の部分群Mを含む。すなわち$G=NM$である。明らかに$(N-\{1\})\subset N_p(G)$が成り立つ。もし$|M|<|N|-1$ならば、$|G|\leq p^s(p^s-2)$, 従って
$n_p(G)\geq p^s-1>\sqrt{|G|}$である。次に、$|M|\geq|N|-1$とする。
Mの$N-\{1\}$への作用: $n^m=m^{-1}nm$, $1\neq n\in N$ $m\in M$, を考える。$1\neq n\in N$ に対してnの固定部分群は$C_M(n)=$

$C_G(n)\cap M$ である。n の軌道の長さは $|M:C_M(n)|$ $\leqq |N|-1$. 従って $|C_M(n)|\geqq |M|/(|N|-1)$ となる。
$m\in C_M(n)$ ならば、nm の位数は m の位数の p 倍である。
G には、位数が p^2 の倍数である元はないから、$nm\in N_p(G)$ である。よって

$$n_p(G)\geqq \sum_{n\in N-1} |C_M(n)| \geqq (p^s-1)\left\lceil\frac{|M|}{|N|-1}\right\rceil \geqq |M|。$$

従って、もし $|M|>|N|$ ならば、$|M|>\sqrt{|G|}$ だから上の不等式より $n_p(G)>\sqrt{|G|}$ となる。M は p 群でないから、$|M|\neq |N|$ で、前に仮定したように $|M|\geqq |N|-1$ である。
よって、残っている場合は $|M|=|N|-1=p^s-1$ のときでしかも上の不等式で等号が成立する場合：$|C_M(n)|=1$, のときである。すなわち、M が $N-1$ 上正則に作用しているときである。$N-1\ni n$ を固定して、$N-1$ に乗法を $n^m * n^{m'} = n^{mm'}$ で定義する。加法は N のもとの群演算を考えると、N は体になる。(例えば、右分配法則は、$(n^{m_1}n^{m_2})*n^m=(m_1^{-1}nm_1m_2^{-1}nm_2)*n^m$
$=m^{-1}m_1^{-1}nm_1(mm^{-1})m_2^{-1}nm_2m = n^{m_1m}n^{m_2m}$.)
$|N|=p^s$ だから、ここに定義された体は $GF(p^s)$ で、従ってMは巡回群である。よって $G\cong A(s,p)$ □

参考文献

[1] E. Bertram, Solvability of the equation $x^2 = g$ in finite groups (manuscript, 1981)

(v, k, λ) グラフ

甲南大理 伊藤昇

1. 対称デザインの基本的な性質を代数的グラフのなかで考察しようというのが目的である．

v, k, λ を正整数で，$v > 2k$，$\lambda(v-1) = k(k-1)$ を満足し，さらに v が偶数ならば，$n = k - \lambda$ は平方数，v が奇数ならば，$nX^2 + (-1)^{\frac{v-1}{2}}\lambda Y^2 = Z^2$ が自明でない整数解を持つようなものとする．

V でサイズ v の ± 1 ベクトル全部の集合を示す．V は成分毎の乗法で位数 2^v の基本可換 2 群を作る．$(\ ,\ )$ で普通の内積を示す．そのとき V を頂点集合とするグラフ $\tilde{\Gamma} = \tilde{\Gamma}(v, k, \lambda)$ をつぎのように定義する：2 頂点 α，β は $(\alpha, \beta) = v - 4n$ のとき隣接である．

内積はベクトルの成分位置上の対称群 S，ベクトルの成分のサイン変更群 $\tilde{R}$ について不変であるから，$\tilde{\Gamma}$ は頂点可移な正則グラフである．さらに V の単位元，全 1 ベクトルを J で示すと，J に隣接している頂点の集合 $D_1(J)$ は -1 の個数が $2n$ に等しい $\binom{v}{2n}$ 個のベクトル全部からできており，S が J を固定しながら可移に働らくので，$\tilde{\Gamma}$ は対称な $\binom{v}{2n}$-正則グラフである．

頂点αの重さ$w(\alpha)$をαの-1に等しい成分の個数と定義する．重さ偶数の頂点全部はVの指数2の部分群Eを作る．このとき$\langle D_1(J)\rangle$はEに等しく，$\tilde{\Gamma}$のJをふくむ連結成分$\Gamma=\Gamma(v,k,\lambda)$の頂点集合が$E$である．$D_1(J)$は$E$の共役類の合併集合であるから，$\Gamma$は共役類グラフであり，$\Gamma$のスペクトラムは$E$の既約指標を使って計算出来る（[1], [2]）．

2．Γについて最も興味を持つのは，クリーク数c，即ちΓの極大完全部分グラフの位数の集合の最大値である．Γと$\tilde{\Gamma}-\Gamma$は同型なグラフであることに注意する．

命題1．$c \leqq v+1$．等号は$v-4n$がvを整除するときにかぎるが，さらにそのとき$v<4n$となる．

証明（[2]）．$\{\alpha_1, \dots \alpha_v, \beta\}$を完全部分グラフとし，$A=(\alpha_1, \dots, \alpha_v)^T$とおくと，$AA^T = 4nI_v+(v-4n)J_v$，ここで$I_v$, J_vはサイズvの単位行列，全1行列である．$\det(AA^T) = (v-2k)^2(4n)^{v-1}$であるから，$A$は可逆で，$\{\alpha_1, \dots, \alpha_v\}$は$\mathbb{R}_v$の基である．$\beta=b_1\alpha_1+\dots+b_v\alpha_v$とおくと，内積の計算から，$\beta=b_1(\alpha_1+\dots+\alpha_v)$, $b_1\{v+(v-4n)(v-1)\}=v-4n$

を得る. ここで $v = 4n$ ならば, $b_1 = 0$ であり, $c \leqq v$ となる. $v \neq 4n$ とすると, β が $\alpha_1, \dots, \alpha_v$ で一意的に決まるから, ともかく $c \leqq v+1$ である. $c = v+1$ とすると, β が ± 1 ベクトルだから b_1 の既約分数型は $\pm \frac{1}{l}$, l は正整数の形であり, $(v-4n)(\pm l - v + 1) = v$, 即ち $v - 4n$ は v を整除する. さらに l の最大値は v であるから, $v < 4n$ も明らかである.

命題2. $c = v+1$ のときは $v = 2k+1$, 即ち v, k, λ はアダマールデザインのパラメータとなる.

証明. 命題1から, $v = a(4n - v)$, a は正整数とおける. $n(v-1) = k(v-k)$ であるから, $\frac{k(v-k)}{v-1} = \frac{(a+1)v}{4a}$, 整理して, $v^2 - \frac{4a}{a+1}kv + \frac{4a}{a+1}k^2 = v$ を得る. $x^2 - \frac{4a}{a+1}kx + \frac{4a}{a+1}k^2$ の最小値は $\frac{4a}{(a+1)^2}k^2$ であるから, $\frac{4a}{(a+1)^2}k^2 \leqq v = \frac{4an}{a+1}$, したがって $\frac{k^2}{a+1} \leqq n = k - \lambda$, 即ち $k \leqq a$ を得る. $a \geqq k > n$ であるから, $4(a-1) > v$ である. したがって $4(a-1) > a(4n - v)$ であり, $4n - v = b$, $1 \leqq b \leqq 3$ を得る. $n(v-1) = k(v-k)$ であるから, $(v+b)(v-1) = 4k(v-k)$,

したがって $b>1$ なら $(v-2k)^2<0$ となってしまう．それで $b=1$, $v=4n-1$．ふたたび，$n(v-1)=k(v-k)$ から $(k-2n)(k-2n+1)=0$．$v>2k$ であるから，$k=2n-1$，即ち $v=2k+1$ である．

注意1．アダマールデザインのパラメータのときにだけ，$c=v+1$ となり得ることは，アダマールデザインが沢山存在することを指示しているように思われる．

3．Dを対称 (v,k,λ) デザインとする．Dをインシデンス行列と同一視する．ただし 0，1 は 1，−1 におきかえる．それでDの各ブロックの −1 成分の個数は k である．記述の便宜上 $v>2k+1$ と仮定し，アダマールデザインのときは別に考へる（[3]）．そうすると $\tilde{\Gamma}$ のなかでは，Dは重さ k の頂点から出来ているクリークと定義される．

さて対称デザインは $|\alpha_i\wedge\alpha_j|=\lambda$, $1\leq i\neq j\leq v$ を満足する v 個のブロック（k-部分集合）の集合として特徴づけられる．

命題3．対称 (v,k,λ) デザインDが存在するとすると，$|\alpha_i\wedge\alpha_j|=n$, $1\leq i\neq j\leq v-1$ を満足する

$v-1$個の$2n$-部分集合で，対称デザインに完成できないものが存在する．

証明．Dのブロックαのk個の成分のサインを変更しαをJに移動する．α以外のブロックでは-1から1に変更されるのがλ個，1から-1に変更されるのが$k-\lambda$個ある．したがってα以外のブロックの集合は，k，λが$2n$，nとなる$v-1$個のブロックの集合となる．もしこれが対称デザインに完成されると，$n(v-1)=2n(2n-1)$から，$v=4n-1$，即ちアダマール補デザインとなる．このときDがアダマールデザインであることは見易い．

注意2．アダマールデザインのパラメータのときは，$v-6$個のブロックの集合はアダマールデザインに完成できるというVerheidenの定理（[4]）があることは特記に値しよう．

$\boxed{\text{問1}}$ $\tilde{\Gamma}$で$c=v$が成立するとき，Dも存在するであろうか．

4．W_lで重さlの頂点全部の集合，$D_i(J)$でJから距離iにある頂点全部の集合を示す．$D_i(J)$はSに対して不変であるから，$D_i(J)\cap W_l\neq\phi$ならば，$D_i(J)\supseteq W_l$

である．明らかに $D_1(J)=W_{2n}$．

つぎにはじめ $2n$ 個の成分が -1 という重さ $2n$ の頂点を $J(2n)$ とし，$J(2n)$ と隣接している頂点 α $(\neq J)$ の重さ $w(\alpha)$ を求めると，$1\leq a\leq \mathrm{Min}(2n, v-2n)$ という自然数 a について $w(\alpha)=2a$ となり，またそのような $2a$ を重さとする α で $J(2n)$ と隣接しているものがあることはすぐわかる．

命題4．Γ の直径は $v\leq 4n+1$ のときそのときにかぎり2に等しい．

証明．まず $v\geq 2k+1$ とすると，$v\geq 4n-1$ であることは見易い．それで $v=4n+1$，$4n$，$4n-1$ のときをしらべればよく，それはやさしい．

$v\geq 4n$ ならば $D_2(J)=\bigcup_{\substack{1\leq i\leq 2n\\ i\neq n}} W_{2i}$ である．∂ で $\tilde{\Gamma}$ の距離を示す．$\sigma\in\tilde{R}$ とすると，$(\alpha, \beta)=(\sigma(\alpha), \sigma(\beta))$，したがって $\partial(\alpha, \beta)=\partial(\sigma(\alpha), \sigma(\beta))$ である．

命題5．$2(d-1)n+2\leq v\leq 2dn+1$，$d\geq 3$ とすると Γ の直径は d に等しい．

とくに射影平面のパラメータ $v=n^2+n+1$，$k=n+1$，$\lambda=1$ のときには n が偶数なら $v=$

$2\left(\frac{n}{2}\right)n+n+1$ と書けるから Γ の直径は $\frac{n}{2}+1$，
n が奇数なら $v=2\left(\frac{n+1}{2}\right)+1$ と書けるから Γ の直径は $\frac{n+1}{2}$ に等しい．

5．$v=4n$ のとき，Γ はアダマールグラフなのでスペクトラムは既に計算されている（[3]）．このときのデザイン D は $k=2n-\sqrt{n}$，$\lambda=n-\sqrt{n}$ というパラメータを持つが，RHデザインと呼ぼう．RH は正則（行和，列和がそれぞれ一定）アダマール行列を意味する．Feit の定理により対称デザインの自己同型対応（キイ）は $\frac{v}{2}$ 個よりも多い固定点を持たないが，$\frac{v}{2}$ 個の固定点を持つものが存在するのは RHデザインにかぎる（[5]）．$\boxed{\text{問 1}}$ に関し，このとき $C=v$ は位数 $4n$ のアダマール行列の存在と同じであり，デザインの存在は正則アダマール行列のそれであることを注意したい．

さて $\sigma(i,j)$，$i\neq j$，で i，j 成分だけが -1 という頂点を示すと，$\{\sigma(1,2),\sigma(1,3),\cdots,\sigma(1,v)\}$ が E の極小生成系になる．E の指標 $\chi(1,j)$ を
$\chi(1,j)\left(\sigma(1,i)\right)=\delta_{ij}$（クロネッカのデルタ）
で定義すると，$\{\chi(1,2),\chi(1,3),\cdots,\chi(1,v)\}$ が E の指標群 $\chi(E)$ の極小生成系になる．$D_1(J)$ の頂点

は $\sigma(1,2)\sigma(1,3)\cdots\sigma(1,2n)$ という形のもの $\binom{v-1}{2n-1}$ 個と，$\sigma(1,2)\sigma(1,3)\cdots\sigma(1,2n)\sigma(1,2n+1)$ という形のもの $\binom{v-1}{2n}$ 個，あわせて $\binom{v}{2n}$ 個である．

スペクトラムの計算の仕方は[2]のときと全く同じである．$\chi(1,2)\chi(1,3)\cdots\chi(1,r)$ の形の指標から得られる固有値を $\lambda(r)$ とおく．その様な形の指標の個数は $\binom{v-1}{r-1}$ である．そして

$$\lambda(r)=\binom{v}{2n}-2\sum_{i=1}^{[\frac{r}{2}]}\binom{r-1}{2i-1}\binom{v-r+1}{2n-2i+1}$$

である．これから $\lambda(r)=\lambda(v-r+2)$ が出て来るから，$1\leq r\leq\left[\frac{v+2}{2}\right]$ としてよく，そうしたうえでの重複度は $\binom{v-1}{r-1}+\binom{v-1}{v-r+1}=\binom{v}{r-1}$ に等しい．ただし，$v=2r-2$ のときは2で割るものとする．

スペクトラムが計算されると，Hoffman, Wilf による Γ の染色数についての限界が得られるのであるが([2])，このような"良い"グラフについては，Frankl と Rödl によってはるかに良い結果が得られている([6])．

6．染色数については，コセット染色数([2])の方が取り扱いやすいし，染色数の実際の値に近い様に思われる：E の部分群 C で空グラフを誘導するものを色部分群と呼ぶと，E の C によるコセットの個数だけ色を用意

するとEの染色が得られる．

$\boxed{\text{問 2}}$ Eの極大色部分群を分類せよ．

Frankleはもっと一般な定式化が可能であることを示しているが(私信)，この様な場合が本質的であろうと今のところ思っている．

7．自己同型群の決定など，当然出来るであろう問題もいろいろあるが，次にまわしたい．

文献

[1] N. Ito, The spectrum of a conjugacy class graph of a finite group, to appear in Math. J. Okayama Univ.

[2] N. Ito, On a family of conjugacy classes graph, Mem. Kōnan Univ. 31 (1984), 105-112.

[3] N. Ito, Hadamard graphs, to appear in Graphs and Combinatorics.

[4] E. Verheiden, Integral and rational completions of combinatorial matrices, JCTA 25 (1978), 267-276.

[5] E. S. Lander, Symmetric designs: an

algebraic approach (1983), LMSLNS 74.
[6] P. Frankl and V. Rödl, Forbidden intersections, to appear

Leech lattice の sublattice のテータ関数.

東大 教養　近藤 武
〃　田坂 隆士

標題の lattice のテータ関数の計算を実行し，ある程度，満足の行く結果が得られた．これについて，計算の方法を述べ，結果の一部分を報告します．結果の完全な記録は，別に論文に書いておるので (to appear)，それを参照して下さい．

1. テータ関数.

二変数 x, q の関数 $\theta(x,q)$ を

$$(1)\qquad \theta(x,q)=\sum_{n\in\mathbb{Z}} x^n q^{n^2}\,,\qquad (x\neq 0)$$

と定義する．容易に判るように，(1) の右辺は $x\neq 0$, $|q|<1$ のとき収束する．以下，$x\neq 0$, $0<|q|<1$ の場合を主として考える．即ち $q=0$ の場合は，容易に判るので，そのことに対する注意はあまりしない．

このような関数 $\theta(x,q)$ を考えた動機は，勿論 Jacobi

の4種類のテータ関数 $\vartheta_\alpha(v,\tau)$ $(1\leq\alpha\leq4)$ による。 たとえば、$z=e^{\pi i v}$, $q=e^{\pi i\tau}$ ($\mathrm{Im}\,\tau>0$) と置くとき、

$$\vartheta_1(v,\tau)=i\sum_{n=-\infty}^{\infty}(-1)^n q^{(\frac{2n-1}{2})^2}z^{2n-1}$$

であるから、

$$\vartheta_1(v,\tau)=iz^{-1}q^{\frac{1}{4}}\theta(-z^2q^{-1},q)=-izq^{\frac{1}{4}}\theta(-z^2q,q)$$

となる。 他の $\vartheta_\alpha(v,\tau)$ に対しても同様な表示が得られる。 特に Jacobi の theta zero $\theta_\alpha(\tau)=\vartheta_\alpha(0,\tau)$ に対しては

$$(2)\qquad \theta_3(\tau)=\sum q^{n^2}=\theta(1,q)$$

$$(3)\qquad \theta_2(\tau)=\sum q^{(n+\frac{1}{2})^2}=q^{\frac{1}{4}}\theta(q,q)$$

$$(4)\qquad \theta_4(\tau)=\sum(-1)^n q^{n^2}=\theta(-1,q)=\theta(1,-q)$$

となる。 尚 $\vartheta_1(0,q)=0$ であるから、

$$(5)\qquad \theta(-q,q)=0$$

となる。 この式は直接簡単に判る。 ここで

$$\rho_0(\tau)=\sum q^{(n+\frac{1}{4})^2},\qquad \rho_1(\tau)=\sum q^{(n+\frac{1}{4})^2}\cdot(-1)^n$$

と置くと、

$$(6)\qquad \rho_0(\tau)=q^{\frac{1}{16}}\theta(q^{\frac{1}{2}},q),\qquad \rho_1(\tau)=q^{\frac{1}{16}}\theta(-q^{\frac{1}{2}},q)$$

となる。 これらの関数 $\rho_0(\tau)$, $\rho_1(\tau)$ は lattice のテータ関数を計算するとき必要となる。 なお、自然数 α に対し、$q^{1/\alpha}=e^{\pi i\tau/\alpha}$ と定義する。

さて，Jacobi のテータ関数 $\vartheta_\alpha(v,\tau)$ に対しては多種多様な公式がある。それらをまとめると，ゆうに1冊の本（100ページ以上）が出来るであろう。その一つの原因は4種類もの関数を考えるところにあると考える。もっとも，$\cos x=\sin(\frac{\pi}{2}-x)$ だから，三角関数は $\sin x$ だけで十分であると結論すると，大変不自由なことになる。しかし，三角関数の公式集の複雑さは，上記の関数の導入にも一つの原因があると考える。

式(1)で定義されるテータ関数 $\theta(x,q)$ に対しても，色々な公式がある。しかしそれらは以下の5種類に分類することが出来ます[3]。（さらに言えば，すべての公式はこの5種類の公式から導びけるのではないかと，思っているけど，実際はどうか判からない）。即ち

0) 自明な公式。

I) Schröter の公式。

II) Jacobi の三重積定理。

III) テータ関数の変換公式。

IV) エータ関数 $\eta(\tau)$，もっと広く無限積 $T(x,q)$ $\left(=\prod_{n=1}^{\infty}(1-xq^n)\right)$ に対して成立する公式。

と分ける。以下これらについて簡単に説明しよう。

自明な公式と言うのは，定義(1)から判るように，

(7) $\theta(-x,-q) = \theta(x,q)$

(8) $\theta(x^{-1},q) = \theta(x,q)$

(9) $\theta(xq^2,q) = \frac{1}{xq}\theta(x,q) = \frac{q}{xq^2}\theta(x,q)$

となる。これら，およびこれらの簡単な演算を自明な公式と言う。なお式(9)は $\sum x^n q^{2n} q^{n^2} = \frac{1}{xq}\sum x^{(n+1)} q^{(n+1)^2}$ より判るのであるが，これは関数 $\theta(x,q)$ の擬二重周期性を表わす重要な公式である。

次にSchröterの公式であるが，自然数 α に対し，$n = \alpha m + \rho$ $(0 \le \rho < \alpha)$ と書き，式(1)を見れば，

Lemma 1. 自然数 α に対し，

(10) $$\theta(x,q) = \sum_{\rho=0}^{\alpha-1} x^{\rho} q^{\rho^2} \theta(x^{\alpha} q^{2\alpha\rho}, q^{\alpha^2})$$

が成立する。

次に自然数 α,β に対し，積 $\theta(x,q^{\alpha})\theta(y,q^{\beta})$ を考察すると，

Lemma 2. 自然数 α,β に対して，

(11) $$\theta(x,q^{\alpha})\,\theta(y,q^{\beta}) = \sum_{\rho=0}^{\alpha+\beta-1} y^{\rho} q^{\beta\rho^2} \theta(xyq^{2\beta\rho}, q^{\alpha+\beta})\,\theta(x^{-\beta}y^{\alpha}q^{2\alpha\beta\rho}, q^{\alpha\beta(\alpha+\beta)})$$

が成立する。

これらの二つをSchröterの公式と言う。証明は

いずれも初等的に出来る。 本書では式(11)をSchröterの公式と言う。 この式は複雑なだけで、あまり役に立たない様に見えるが、式の右辺の各項を自明な公式等を使って整理すると、α, β, x, y を具体的な値にしたとき、非常に簡明な公式が得られるのである。 以下其の二三例を作って見よう。 先ず(10)において、$\alpha=2$, $x=\pm 1$ か $\pm q$ とすると、

$$\theta(1,q)=\theta(1,q^4)+q\theta(q^4,q^4),$$
$$\theta(-1,q)=\theta(1,q^4)-q\theta(q^4,q^4)$$
$$\theta(q,q)=\theta(q^2,q^4)+q^2\theta(q^6,q^4)=2\theta(q^2,q^4)$$
$$0=\theta(-q,q)=\theta(q^2,q^4)-q^2\theta(q^6,q^4)$$

を得る。 これは、$q=e^{\pi i z}$ と置き、式(2)—(6)を見れば、

(T1) $\theta_3(z)=\theta_3(4z)+\theta_2(4z)$, $\theta_4(z)=\theta_3(4z)-\theta_2(4z)$

(T2) $\theta_2(z)=2\rho_0(4z)$

であることを示している。 次に(11)において、$\alpha=\beta=1$ $y=\pm x$ と置くと、

$$\theta(x,q)^2=\theta(x^2,q^2)\theta(1,q^2)+xq\,\theta(x^2q^2,q^2)\,\theta(q^2,q^2)$$
$$\theta(x,q)\theta(-x,q)=\theta(-x^2,q^2)\,\theta(-1,q^2)$$

を得る。 さらに $x=\pm 1$ か $\pm q$ とすることにより、

倍角公式 (Duplication formulas):

(T3) $$\theta_2(z)^2 = 2\theta_2(2z)\theta_3(2z)$$

(T4) $$\theta_3(z)^2 = \theta_3(2z)^2 + \theta_2(2z)^2$$

(T5) $$\theta_4(z)^2 = \theta_3(2z)^2 - \theta_2(2z)^2$$

(T6) $$\theta_3(z)\theta_4(z) = \theta_4(2z)^2$$

が導かれる。これから、重要な公式

(T7) $$\theta_3(z)^4 = \theta_2(z)^4 + \theta_4(z)^4$$

を得る。さらに $\alpha=3$, $\beta=1$ のとき、

(T8) $$\theta_3(3z)\theta_3(z) = \theta_2(3z)\theta_2(z) + \theta_4(3z)\theta_4(z)$$

等を示すのも容易である。すなわち、両辺の各項を式(11)を使って比べればよいのである。

次に(II),(III),(IV)について簡単に述べよう。

(12) $$T(x, q) = \prod_{n=1}^{\infty}(1 - xq^n)$$

という無限積は、任意の x に対し、$|q|<1$ のとき絶対収束する。これを使うと、Jacobi の triple product theorem は、

(13) $$\theta(x, q) = T(1, q^2)\, T\left(-\frac{x}{q}, q^2\right)\cdot T\left(\frac{-1}{xq}, q^2\right)$$

と表わされる。ここで x の値を特殊化すると、$\theta_3(z)$, $\theta_2(z)$, $\theta_4(z)$ の無限積表示が得られる。特に Dedekind のエータ関数 $\eta(z)$ は、

(14) $\quad \eta(z) = q^{\frac{1}{12}}\, T(1, q^2) = q^{\frac{1}{12}} \prod_{n=1}^{\infty} (1 - q^{2n})$

であるが、

$$\theta(-q, q^3) = T(1, q^6)\, T(q^{-2}, q^6)\, T(q^{-4}, q^6) = T(1, q^2)$$

であるから、

(15) $\quad \eta(z) = q^{\frac{1}{12}}\, \theta(-q, q^3)$

を得る。 次に、テータ公式は、一応

(16) $\quad \theta(e^{\gamma}, e^{\delta}) = \kappa\, \theta(e^{\alpha}, e^{\beta})$

(17) $\quad \kappa = e^{\alpha^2/4\beta} \cdot \sqrt{\frac{-\beta}{\pi}}$

と定式化して置く。 但し $\alpha, \beta \in \mathbb{C}$, $\mathrm{Re}\,\beta < 0$ であり $\beta\delta = \pi^2$, $\alpha^2\delta + \gamma^2\beta = 0$ (ie $\delta = \pi^2/\beta$, $\gamma = \pm\frac{\pi i \alpha}{\beta}$) である。 なお $\mathrm{Re}\left(\sqrt{\frac{-\beta}{\pi}}\right) > 0$ とする。 これから、$T(e^{\alpha}, e^{\beta})$ に対する変換公式を作れる筈であるが、よく判らない。 最後に (IV) に対するコメントであるが、これは主として、無限積 $T(x, q)$ に対して成立する公式を意味する。 特に Schöten type の計算をすると色々な公式が得られる。 また、$I = \prod(1 - q^{2n})$, $J = \prod(1 + q^{2n})$, $K = \prod(1 + q^{2n-1})$, $L = \prod(1 - q^{2n-1})$ とするとき、

(18) $\quad JKL = 1$

と言う公式も (IV) に入る。~~[illegible]~~.

2. Leech lattice

Leech lattice Λ とは, 正値な階数 24 の even unimodular lattice で, squared length 2 の vector を含まないものを言う. こう言う lattice は同型を除いて唯一つであり, 非常に対称性に富んだ lattice で, その自己同型群は Conway の $\cdot 0$ と言う有名な群である. この群 $\cdot 0$ は自然に 24 次の Mathieu 群 M_{24} を含んでいるのは容易に判るし, 以下の構成法からもすぐ導ける.

集合 Ω を 24 点からなる集合とし, Ω の点で index をもつベクトルの系 $\{e_i : i \in \Omega\}$ は

(19) $$l(e_i, e_j) = 2\delta_{ij}$$

をみたすとする. 但し $l(x,y)$ は $\mathbb{R}^{\Omega} = \sum \mathbb{R} e_i$ 内のユークリッド内積であり, $l(x) = l(x,x)$ はベクトル x の squared length をあらわす. lattice $L = \sum \mathbb{Z} e_i$ は even lattice であり, その判別式は 2^{24} である. そして集合 Ω 上のコード $\mathcal{H} \subset P(\Omega)$ (Ω の部分集合全体 $P(\Omega)$ は対称差 $X+Y = X \cup Y - X \cap Y$ に関してアーベル群となすが, その部分群(または部分集合) $\mathcal{H}$ を Ω 上のコードと言う) に対して,

(20) $$L(\mathcal{H}) = \bigcup_{X \in \mathcal{H}} \left(\tfrac{1}{2} e_X + L \right)$$

と置く。 但し $X \subset \Omega$ に対し

(21) $$e_X = \sum_{i \in X} e_i$$

と略記する。 なお (20) の右辺は部分集合 $\frac{1}{2}e_X + L$ の disjoint sum であり、 $\frac{1}{2}e_X + \frac{1}{2}e_Y = \frac{1}{2}e_{X+Y} + e_{X \cap Y}$ に注意すると、 $\mathcal{H}$ が $P(\Omega)$ の部分群ならば、 $L(\mathcal{H})$ は lattice となる。 さらに、 $\mathcal{H}$ が self-dual ($\mathcal{H} = \mathcal{H}^\circ$) なら、 $L(\mathcal{H})$ は unimodular ($L(\mathcal{H})^\circ = L(\mathcal{H}^\circ) = L(\mathcal{H})$) であり、 $\mathcal{H}$ が even ($\forall X \in \mathcal{H} \rightarrow |X| \equiv 0 \pmod 4$) なら、 $L(\mathcal{H})$ は even lattice である。 そこで Golay code $\mathcal{G} \subset P(\Omega)$ ($\mathcal{G}$ は、4元集合を含まない even self-dual code over Ω として特徴づけられる) に対し、 lattice $L(\mathcal{G})$ は squared length 2 のベクトルを 48 個 ($\pm e_i ; i \in \Omega$) 持つだけような even unimodular lattice である。 squared length 4 のベクトル $y = e_{i_0} + \frac{1}{4}e_\Omega \in \frac{1}{2} L(\mathcal{G})$ に対し、 $K_y = \{ z \in L(\mathcal{G});\ (y, z) \in \mathbb{Z} \}$ と置くと、

$$\overline{K}_y = K_y + \mathbb{Z}y = K_y \cup \{ y + K_y \}$$

は even unimodular lattice であることが容易に示せる。 点 $i_0 \in \Omega$ は適当な一点である。 $e_i \notin K_y$ であるから、 $\overline{K}_y$ は squared length 2 のベクトルを含まないことが判る。 すなわち、 $\overline{K}_y$ は Leech lattice Λ と同型で、

lattice K_y を具体的に計算することにより,

(22) $$\Lambda = \bigcup_{x\in g}\left\{\left(\tfrac12 e_x + L_0\right)\cup\left(\tfrac14 e_\Omega + \tfrac12 e_x + L_1\right)\right\}$$

という Leech lattice Λ の表示を得る。但し $\delta=0$ or 1 に対し, $L_\delta = \{\sum x_i e_i \in L : \sum x_i \equiv \delta \pmod 2\}$ である。この表示 (22) は, Conway [1] の Lecture 3 の Th 2 における lattice Λ の descriptions (i), (ii), (iii) に相当する。

集合 Ω 上の置換 $m\in S_{24}$ に対し, $(e_i)^m = e_{i^m}$ $(i\in\Omega)$ と置くと, m は自然に $\mathbb{R}^\Omega$ 及び L 等に作用する。容易に判るように, m が lattice Λ を不変にするには, コード $g\subset P(\Omega)$ を不変にしなければならない。即ち, $m\in M_{24}$ (Golay code g を不変にする S_{24} の部分群) となる。逆に $m\in M_{24}$ は, Λ の各ベクトルに

(23) $$\left(\tfrac12 e_x + \sum x_i e_i\right)^m = \tfrac12 e_{x^m} + \sum x_i e_{i^m},$$

(24) $$\left(\tfrac14 e_\Omega + \tfrac12 e_x + \sum y_i e_i\right) = \tfrac14 e_\Omega + \tfrac12 e_{x^m} + \sum y_i e_{i^m}.$$

と作用し, lattice Λ を不変にすることが判る。

なお, $S\subset\Omega$ に対し, ε_S を $(e_i)\varepsilon_S = e_i$ (if $i\in S$) or $-e_i$ (if $i\notin S$) と置くと, $2^{12}\cdot M_{24} = \{ m\varepsilon_x : m\in M_{24}, x\in g\}$ の各元は Λ を不変にする。$2^{12}\cdot M_{24}$ 以外の元 $\rho\in\cdot O$ を見出すことから, Conway の仕事が始まった。

3. Invariant sublattices とそのテータ関数.

先ず、ユークリッド空間 $\mathbb{R}^n$ 内の点集合 $\mathfrak{X}$ のテータ関数 $\Theta(z,\mathfrak{X})$ を、$q=e^{\pi i z}$ と置き、

$$(25)\qquad \Theta(z,\mathfrak{X}) = \sum_{x\in\mathfrak{X}} q^{l(x)}$$

と定義する。但し、$\mathrm{Im}\, z>0$、即ち $|q|<1$ と仮定し、右辺が収束する場合のみを考える。また $l(x)$ は原点 0 と点 x の間の squared length である。例えば、$\mathfrak{X}$ が可算でないと、(25) の右辺は定義出来ないし、discrete でないと、(25) の右辺は発散する。もっと一般に、各点 $x\in\mathfrak{X}$ に weight $w(x)\in\mathbb{R}$ が定まっているとき、

$$(26)\qquad \Theta(z,\mathfrak{X}:w) = \sum w(x)\, q^{l(x)}$$

を weighted theta 関数と言う。もし weight $w(x)$ の値が有限種類ならば、$\Theta(z,\mathfrak{X}:w)$ は"普通の"テータ関数の組み合せで表わされる。明らかに、

$$(27)\qquad \Theta(z,\mathfrak{X})+\Theta(z,\mathfrak{Y}) = \Theta(z,\mathfrak{X}\cup\mathfrak{Y})+\Theta(z,\mathfrak{X}\cap\mathfrak{Y})$$

であり、集合 $\mathfrak{X}$, $\mathfrak{Y}$ が $\mathbb{R}^n$ 内の互いに直交する(線形)部分空間に含まれているとき、即ち $\mathfrak{X}\perp\mathfrak{Y}$ ならば、

$$(28)\qquad \Theta(z,\mathfrak{X}\times\mathfrak{Y}) = \Theta(z,\mathfrak{X})\,\Theta(z,\mathfrak{Y})$$

となる。たとえば、標準的距離を持つ $\mathbb{Z}\subset\mathbb{R}$ に対して、

$$\Theta(z,\mathbb{Z}) = \sum_{n\in\mathbb{Z}} q^{n^2} = \theta_3(z)$$

となる。また $\frac{1}{2}+\mathbb{Z}=\{n+\frac{1}{2} : n\in\mathbb{Z}\}$, $\frac{1}{4}+\mathbb{Z}$ に対し、

$$\Theta(z,\tfrac{1}{2}+\mathbb{Z}) = \sum q^{(n+\frac{1}{2})^2} = \theta_2(z),$$

$$\Theta(z,\tfrac{1}{4}+\mathbb{Z}) = \rho_0(z)$$

となる。また図形の対称性から、$\Theta(z,(-\frac{1}{4})+\mathbb{Z})=\rho_0(z)$ etc を得る。一方 $\theta_4(z)$ および $\rho_1(z)$ は weighted theta 関数となっている。(式(2)～(6)を参照)。

明らかに、$\mathbb{Z}^N$ のテータ関数は $\theta_3(z)^N$ であり、D_N 型の lattice $(\mathbb{Z}^N)_0=\{x\in\mathbb{Z}^N : \sum x_i\equiv 0(2)\}$ のテータ関数は $\frac{1}{2}\{\theta_3(z)^N+\theta_4(z)^N\}$ である。同様に、

(29) $$E_4(z)=\frac{1}{2}\{\theta_2(z)^8+\theta_3(z)^8+\theta_4(z)^8\},$$

(30) $$\Theta^{(p)}(z)=\theta_3(pz)\theta_3(z)+\theta_2(pz)\theta_2(z),$$

と置くと、$E_4(z)$ は even unimodular lattice E_8 のテータ関数であり、$p\equiv 3\ (\mathrm{mod}\ 4)$ のとき、$\Theta^{(p)}(z)$ は虚2次体 $\mathbb{Q}(\sqrt{-p})$ の整数環の(自然な metric に関する)テータ関数である。

さて、元 $m\in M_{24}$ を、S_{24} の元と考え

(31) $$m=(U_1)(U_2)\cdots(U_s)$$

と言う m の cycle 分解を考える。但し $\{U_i : 1\le i\le s\}$ は集合 Ω の disjoint sum decomposition をなす Ω の部分集合達であり、(U_i) は集合 U_i 上のある巡回置換を

表わす. 即ち 適当な順序で, $U_i = \{\alpha_1, \alpha_2, \cdots, \alpha_t\}$ と書いたとき, $(U_i) = (\alpha_1 \alpha_2 \cdots \alpha_t)$ となっている.

このとき, 元 m の“共役”類 を

$$(32) \qquad m = |U_1||U_2| \cdots |U_\rho|.$$

と表わすと, 二三の類を除いて, 共役類を一意的に表し, 例外の類は, m 又は m^{-1} の類を表すことになる.

式(31)で与えられる置換 m に対し, 式(23)および(24)により, m で不変なベクトル全体の なす invariant sublattice Λ_m を決定するのは, 少々複雑だけど, むつかしいことではない。 このとき, m で不変なコード $\mathcal{G}_m = \{X \in \mathcal{G} : Xm = X\}$ が重要であるが, これは, Todd [3] の表を検討することにより, 決定出来る. 結局 invariant lattice Λ_m のテータ関数

$$\Theta_m(z) = \Theta(z, \Lambda_m)$$

は, $\theta_3(z)$, $\theta_4(z)$, $\theta_2(z)$, $P_0(z)$ および $P_1(z)$ (もっとくわしく, $\theta_3(pz)$, $\theta_4(qz)$, etc ($p, q \in \mathbb{N}$)) の有理係数の斉次多項式として表わされる. これらを, 保角公式および, 式(29),(30) で与えられる $E_4(z)$, $\Theta^{(p)}(z)$ 等を使って整理すると, 次の例で与えるように, 扱いやすい表示が得られる.

4. Examples.

A) $m = 1^{24}$（単位元）.

$$\Theta_m(z) = E_4(z)^3 - 720\,\Delta(z)$$

但し，$\Delta(z) = \eta(z)^{24} = 2^{-8}\,\theta_1'(z)^8$.

B) $m = 1^8 2^8$,

$$\Theta_m(z) = E_4(2z)^2 + \frac{15}{256}\,\theta_2(z)^{16}$$

$$= \left\{\tfrac{1}{2}\left(\theta_3(z)^4 + \theta_4(z)^4\right)\right\}^4 - \frac{3}{8}\left(\theta_2(z)\,\theta_4(2z)\right)^8$$

C) $m = 2^{12}$,

$$\Theta_m(z) = \frac{1}{2}\left(\theta_3(2z)^{12} + \theta_2(2z)^{12} + \theta_4(2z)^{12}\right)$$

$$= \theta_3(2z)^{12} - \frac{3}{2}\,\theta_1'(2z)^4$$

D) $m = 1^6 3^6$,

$$\Theta_m(z) = \Theta^{(3)}(2z)^6 - \frac{9}{4}\left(\theta_1'(z)\,\theta_1'(3z)\right)^2$$

E) $m = 3^8$,

$$\Theta_m(z) = E_4(3z).$$

F) $m = 1^3 7^3$,

$$\Theta_m(z) = \Theta^{(7)}(2z)^3 - \frac{3}{2}\,\theta_1'(z)\,\theta_1'(7z)$$

以上のように，各 type の元に，相当きれいな表示が得られる。なお

$$\theta_1'(z) = \theta_2(z)\,\theta_3(z)\,\theta_4(z) = 2\,\eta(z)^3 \tag{33}$$

と云う略記法を使っている。

前記の例 D or F をみれば，

$$m = 1^4 \cdot 5^4$$

のときも，簡単な表示が得られそうな筈なのだが，色々な理由（たとえば $p \not\equiv 3 \bmod 4$）のため，この場合だけは，$q = e^{\pi i z}$ の巾級数として，別な取り扱いを必要とした．

References.

(1) Conway, J.H. Three lectures on exceptional groups. p215–247 of Finite simple groups. edited by M.B. Powell and G. Higman 1971.

(2) Conway - Norton. Monstrous moonshine. Bull. Lon. Math. Soc. 11 (1979) p 308–339.

(3) Todd, N.J. A presentation of the Mathieu group M_{24} as a collineation group. Ann. Math Pure Appl. 71 (1966) p 199–238.

(4) Kondo, T - Tasaka, T : The theta functions of sublattices of the Leech lattice. (to appear)

一般四元数型Hadamard行列

東京女子大・文理　山田美枝子

§1. 序.

2^{s+1}位一般四元数群とn(奇数)位巡回群の半直積Gが有理整数環$\mathbf{Z}$上につくる群環$\mathbf{Z}G$において、そのある元の右正則表現行列が$2^{s+1}n$次Hadamard行列になるとき、これを一般四元数型Hadamard行列と呼ぶことにする。周知のPaley type I行列から生ずるHadamard行列はある特別な一般四元数型Hadamard行列にSeidel同値となる。一般四元数群の位数が最小、すなわち$s=2$の場合には伊藤のtype QのHadamard行列[1]となり、さらにその場合で成分行列が対称のものはWilliamson行列[5]となる。1972年にR. J. TurynはWilliamson行列のある無限系列を発見した[3]が、1980年に山本–山田によりこれらは有限体の相対的Gaussの和より構成されることがわかった[6, 9]。

ここでは一般四元数型Hadamard行列について、いくつかの新しい無限系列を構成する。$s\geq 2$を固定しておくと、

$2^s n-1$ が素数巾の場合に対応して $2^s n$ 次一般四元数型Hadamard行列の n に関する無限系列が構成できる．特に $s=2$ の場合には $4n$ 次Hadamard行列になる．$2n-1$ が素数巾の場合には $8n$ 次の n に関する無限系列が構成できる．どちらもTuryn型Williamson行列の場合と同様に相対的Gaussの和がその構成にあたって大きな役割を果している。

また一般四元数型Hadamard行列が存在する時、その倍次数の一般四元数型Hadamard行列を構成することができ、n が一定ならばこれから２の巾倍 $2^s n$ に関する無限系列ができる。

最後の節で24次の一般四元数型Hadamard行列を例にあげそれらをすべて求めて同値類にわける．その結果１つを除いて他の類の構成の原理がわかる。

§2. 一般四元数型Hadamard行列の定義

群 G を 2^{s+2} 位一般四元数群 Q_s と n (奇数) 位巡回群 $Z_n=\{\zeta\}$ の半直積とする．すなわち

$$\rho^{2^s}=-1,\quad j^2=-1,\quad j\rho j^{-1}=\rho^{-1},$$
$$\rho\zeta\rho^{-1}=\zeta,\quad j\zeta j^{-1}=\zeta^{-1},\quad \zeta^n=1$$

で定義される群とする。

Zは有理整数環，$L=H\cup Hj$ は G の半系，ただし $H=\{\rho^k\zeta^\ell\}$ $k=0,\cdots,2^s-1$, $\ell=0,\cdots,n-1$ とし．L を基底とする群環 ZG の右正則表現を考える。ただし中心 $1,-1$ を Z の $1,-1$ と一致させる．すなわち $\xi\in ZG$ に対し．

$$\begin{pmatrix} \xi \\ \zeta\xi \\ \vdots \\ \zeta\rho\xi \\ \vdots \\ \zeta^{n-1}\rho^{2^s-1}\xi \\ j\xi \\ \zeta j\xi \\ \vdots \\ \zeta\rho j\xi \\ \vdots \\ \zeta^{n-1}\rho^{2^s-1}j\xi \end{pmatrix} = R(\xi)\begin{pmatrix} 1 \\ \zeta \\ \vdots \\ \zeta\rho \\ \vdots \\ \zeta^{n-1}\rho^{2^s-1} \\ j \\ \zeta j \\ \vdots \\ \zeta\rho j \\ \vdots \\ \zeta^{n-1}\rho^{2^s-1}j \end{pmatrix}$$

なる行列 $R(\xi)$ を対応させる．詳しく書くと

$$\xi=\sum_{k=0}^{2N-1}\sum_{\ell=0}^{n-1}a_{k,\ell}\zeta^\ell\rho^k+\sum_{k=0}^{2N-1}\sum_{\ell=0}^{n-1}b_{k,\ell}\zeta^\ell\rho^k j=\alpha+\beta j,$$

$$N=2^{s-1},\quad a_{k,\ell},\ b_{k,\ell}\in Z,$$

の右正則表現行列は

$$R(\xi)=\begin{pmatrix} \mathfrak{a} & \mathfrak{b} \\ -\mathfrak{b}^* & \mathfrak{a}^* \end{pmatrix},$$

$$\mathfrak{a}=\begin{pmatrix} A_0 & A_1 & A_2 & \cdots & A_{2N-1} \\ -A_{2N-1} & A_0 & A_1 & \cdots & A_{2N-2} \\ -A_{2N-2} & -A_{2N-1} & A_0 & \cdots & A_{2N-3} \\ & & & \ddots & \\ -A_1 & -A_2 & -A_3 & \cdots & A_0 \end{pmatrix},\quad \mathfrak{b}=\begin{pmatrix} B_0 & B_1 & B_2 & \cdots & B_{2N-1} \\ -B_{2N-1} & B_0 & B_1 & \cdots & B_{2N-2} \\ -B_{2N-2} & -B_{2N-1} & B_0 & \cdots & B_{2N-3} \\ & & & \ddots & \\ -B_1 & -B_2 & -B_3 & \cdots & B_0 \end{pmatrix}$$

である。ただし $A_k=\sum_{l=0}^{n-1} a_{k,l}T^l$, $B_k=\sum_{l=0}^{n-1} b_{k,l}T^l$ は n 次巡回

行列, $T=\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ & & & & \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}$ は n 次基本巡回行列である。

$\xi=\alpha+\beta j$ に対しその共役元 $\bar{\xi}$ を $\bar{\xi}=\bar{\alpha}-\beta j$, $\bar{\alpha}=\tau(\alpha)$

で定義する。τ は $\rho\to\rho^{-1}$, $\zeta\to\zeta^{-1}$ から得られる $\mathbf{Z}G$ の自己

同型写像である。このときノルムは $N(\xi)=\xi\bar{\xi}=\alpha\bar{\alpha}+\beta\bar{\beta}$

である。また一般に $N(\xi\eta)=N(\xi)N(\eta)$ が成立つ。さらに

$R(\bar{\xi})=R(\xi)^*$ であり

$$R(\xi)R(\xi)^*=R(\xi)R(\bar{\xi})=R(\xi\bar{\xi})=\begin{pmatrix} aa^*+bb^* & \\ & aa^*+bb^* \end{pmatrix}$$

である。

我々は一般四元数型 Hadamard 行列を次のように定義する。

__定義__ 群環 $\mathbf{Z}G$ の元 $\xi=\sum_{k=0}^{2N-1}\sum_{l=0}^{n-1} a_{k,l}\zeta^l\rho^k+\sum_{k=0}^{2N-1}\sum_{l=0}^{n-1} b_{k,l}\zeta^l\rho^k j$ が

① $a_{k,l}$, $b_{k,l}$ $(0\leqq k\leqq 2N-1,\ 0\leqq l\leqq n-1)$ は 1 または -1,

② $N(\xi)=\xi\bar{\xi}=2^{s+1}n=4nN$,

を満足する時、ξ の右正則表現行列 $R(\xi)$ は $2^{s+1}n=4nN$ 次

Hadamard 行列となる。これを一般四元数型 Hadamard 行列と呼

ぶ。また、

①′ $a_{kk}=0$, a_{kl} $(k\neq l)$, b_{kl} は 1 または -1,

②′ $N(\xi)=\xi\bar{\xi}=2^{s+1}n-1=4nN-1$,

を満足する時 $R(\xi)$は $2^{s+1}n-1=4nN-1$ 次C行列となる.

これを一般四元数型C行列と呼ぶ。

前述の $\mathfrak{a}$, $\mathfrak{b}$ を用いて言いかえると

① $\mathfrak{a}$の対角線上の元はすべて 1（またはすべて -1）、他の元は 1 または -1, $\mathfrak{b}$の元も 1 または -1,

② $\mathfrak{a}\mathfrak{a}^*+\mathfrak{b}\mathfrak{b}^*=2^{s+1}nI=4nNI$,

を満足する時、$R(\xi)$を一般四元数型Hadamard行列と呼ぶ。

①′ $\mathfrak{a}$の対角線上の元が0、他の元は 1 または -1, $\mathfrak{b}$の元も 1 または -1,

②′ $\mathfrak{a}\mathfrak{a}^*+\mathfrak{b}\mathfrak{b}^*=(2^{s+1}n-1)I=(4nN-1)I$,

を満足する時、$R(\xi)$を一般四元数型C行列と呼ぶ.

$R(\xi)$が一般四元数型Hadamard行列となるための条件をその成分行列A_k, B_kを使って詳しく表わすと.

$$\begin{cases} \displaystyle\sum_{k=0}^{2N-1} A_k A_k^* + \sum_{k=0}^{2N-1} B_k B_k^* = 4nNI, \\ \displaystyle -\sum_{k=0}^{\nu-1}\left(A_k A^*_{2N-\nu+k} + B_k B^*_{2N-\nu+k}\right) + \sum_{k=0}^{2N-\nu-1}\left(A_k^* A_{k+\nu} + B_k^* B_{k+\nu}\right) = 0, \quad (1\leq\nu\leq 2N-1) \end{cases}$$

となる。

特に $N=1$ の一般四元数型Hadamard行列では

$$\begin{cases} A_0A_0^* + A_1A_1^* + B_0B_0^* + B_1B_1^* = 4nI, \\ A_0A_1^* - A_1A_0^* + B_0B_1^* - B_1B_0^* = 0 \end{cases}$$

となり、伊藤の type Q Hadamard行列[1]に他ならない。この場合で A_0, A_1, B_0, B_1 が対称であるとすると最初の条件式だけが残る。これはWilliamson等式でそれが成立するとWilliamson行列が構成される。

よく知られているPaley type 1 行列について次が言える[10]。

<u>定理1</u>　Paley type 1 行列は　$\mathfrak{a}$ が skew symmetric, $B_{2N-\ell-1} = -B_\ell^*$ $(\ell=0,\cdots,N-1)$ であるような一般四元数型C行列に Seidel 同値である。ただし Seidel 同値とは、同じ番号の行と列に -1 をかけること、行と列に同じ置換をほどこすことによって得られる行列を同値とみなすものである。

§3. 一般四元数型Hadamard行列の無限系列

相対的Gaussの和について、次の定理が重要である。

<u>定理2</u>　q:素数巾, $K=GF(q^t)$, $t\geqq 2$, $F=GF(q)$, F^*:F の乗法群, S_K:K からの絶対スプール, S_F:F からの絶対スプール, $S_{K/F}$:K から F へのスプール, χ:K の指標

で$\bar{F}$に制限した時単位指標でないもの，$\tau_K(\chi)=\sum_{\alpha\in K}\chi(\alpha)\zeta_p^{S_K\alpha}$：

Kでの Gaussの和，$\tau_{\bar{F}}(\chi)=\sum_{\alpha\in\bar{F}}\chi(\alpha)\zeta_p^{S_{\bar{F}}\alpha}$：$\bar{F}$での Gaussの和，ただし $\zeta_p=e^{\frac{2\pi i}{p}}$ とすると．相対的Gaussの和 $\vartheta_\chi=\frac{\tau_K(\chi)}{\tau_{\bar{F}}(\chi)}$ は，

$$\vartheta_\chi=\sum_{\alpha \bmod \bar{F}^*}\chi(\alpha)\bar{\chi}(S_{K/\bar{F}}\alpha),$$

の形に書くことができ，

$$\vartheta_\chi\overline{\vartheta_\chi}=q^{t-1}.$$

（証明）[6, 7, 9]参照．

この定理を使って 2^sが固定されたとき次数$2^s n$の nに関する無限系列を与える次の定理を得る．

<u>定理3</u>　q：素数中，$q+1=2^s n$，n：奇数，$s\geqq 2$，$K=GF(q^2)$，$\bar{F}=GF(q)$，η：Kの生成元．$\rho=\zeta_{2^{s+1}}$：1の原始2^{s+1}乗根，$\omega=\zeta_n$：任意の1のn乗根，$\chi=\chi_{2^{s+1}}\cdot\chi_n$，$\chi_{2^{s+1}}(\eta)=\rho$，$\chi_n(\eta)=\omega$でKの指標$\chi$を$\bar{F}$に制限したとき平方剰余指標となる、とすれば．$\chi$に属する相対的Gaussの和

$$\vartheta_\chi=\alpha+\beta\rho^n,\quad \alpha,\beta\in Z[\rho^2,\omega]$$

に対し、$\alpha\pm i+\beta j$ の右正則表現行列は$2^s n$次一般四元数型Hadamard行列となる．

（証明）定理2から、ψを$\bar{F}$の平方剰余指標とすると，

$$\vartheta_x=\sum_{m=0}^{g}\chi(\eta^m)\overline{\chi}(S_{K/k}\eta^m)=\sum_{m=0}^{g}\psi(S_{K/k}\eta^m)\rho^m\omega^m$$

である。mの偶数、奇数によって分けて

$$\vartheta_x=\sum_{m=0}^{\frac{g-1}{2}}\psi(S_{K/k}\eta^{2m})\rho^{2m}\omega^{2m}+\left(\sum_{m=0}^{\frac{g-1}{2}}\psi(S_{K/k}\eta^{2m+n})\rho^{2m}\omega^{2m}\right)\rho^n$$

を得る。

$$\alpha=\sum_{m=0}^{\frac{g-1}{2}}\psi(S_{K/k}\eta^{2m})\rho^{2m}\omega^{2m},\quad \beta=\sum_{m=0}^{\frac{g-1}{2}}\psi(S_{K/k}\eta^{2m+n})\rho^{2m}\omega^{2m}\in \mathbf{Z}[\rho^2,\omega]$$

とおくと

$$\overline{\vartheta}_x=\sum_{m=0}^{g}\psi(S_{K/k}\eta^m)\rho^{-m}\omega^{-m}=\sum_{m=0}^{g}(-1)^m\psi(S_{K/k}\eta^m)\rho^m\omega^m=\alpha-\beta\rho^n$$

から、$\overline{\alpha}=\alpha$, $\overline{\beta\rho^n}=-\beta\rho^n$;

$$\begin{aligned}\vartheta_x\overline{\vartheta}_x&=(\alpha+\beta\rho^n)(\overline{\alpha}+\overline{\beta}\,\overline{\rho}^n)=\alpha\overline{\alpha}+\beta\rho^n\overline{\beta\rho^n}+\alpha\overline{\beta}\,\overline{\rho}^n+\beta\overline{\alpha}\rho^n\\&=\alpha\overline{\alpha}+\beta\overline{\beta}+\alpha(-\beta\rho^n)+\alpha\beta\rho^n=\alpha\overline{\alpha}+\beta\overline{\beta}=g\end{aligned}$$

を得る。$\alpha\pm i+\beta j$ の基底$\{\rho^k\zeta^i,\ \rho^k\zeta^i j\}$, $0\leq k\leq 2^s-1$, $0\leq i\leq n-1$ に関する係数はすべて±1で、$N(\alpha\pm i+\beta j)=g+1$ より $\alpha\pm i+\beta j$ の右正則表現行列は $2^s n$ 次一般四元数型Hadamard行列となる。

この定理で $s=2$ とおくと $4n$次一般四元数型Hadamard行列の無限系列が得られる。

ϑ_xのかわりに $X=\alpha+\beta\rho^n$, $\alpha,\beta\in Z[\rho^2,\zeta_n]$, 基底Lによる X の係数は$\pm1$, $N(X)=2^s n$ となる X が存在するものとすれば $\Gamma=\alpha+\beta j$ とおいて Γは$2^s n$次一般四元数型

Hadamard行列を生成する。しかし、このようなXを円周$2^{s+1}n$等分体でみつける問題は整数論において研究が行われているが（H.B. Mann, S. Chowla 等）、一般には大変難しい問題のようである。

<u>定理3の系</u>　定理3のα, βに対し

$$\mu = (\alpha - i + \beta \rho^{n} j)(1 - j) = (1-j)(\vartheta_{\chi} + i j)$$

の右正則表現行列は$2^{s+1}n$次一般四元数型Hadamard行列となる。特に$s=1$とおくとTuryn型Williamson行列となる。

（注意）定理3では$s \geq 2$としたがそれはHadamard行列の位数が4の倍数であるためで、系では2倍になっているので$s=1$における相対的Gaussの和を使うことができる。

同じように相対的Gaussの和を使って次のような無限系列が得られる。

<u>定理4</u>　g：素数巾，$g+1=2n$，n：奇数，$K=GF(g^2)$，$F=GF(g)$，η：Kの生成元，$\rho=\zeta_8$：1の原始8乗根，ζ_n：任意の1のn乗根，$\chi=\chi_8 \cdot \chi_n$，$\chi_8(\eta)=\rho$，$\chi_n(\eta)=\zeta_n$：Kの指標でFに制限したとき原始4乗剰余指標となる，

とする。χに属する相対的Gaussの和ϑ_χに対し

$$\gamma = (\vartheta_\chi + \rho^t j)(1+i)(1+j), \quad t=1,3,5,7$$

の右正則表現行列は$8n$次一般四元数型Hadamard行列となる。

ただし、$\vartheta_\chi + \rho^t j$, $1+i$, $1+j$のかける順を変えてもよい。

(証明) $$\vartheta_\chi = \sum_{m=0}^{8} \overline{\chi}(S_{K/F}\eta^m)\rho^m \zeta_n^m$$

$$= \sum_{m=0}^{n-1} \{\overline{\chi}(S_{K/F}\eta^{8m}) + \rho\,\overline{\chi}(S_{K/F}\eta^{8m+n})\}\zeta_n^m$$

で、$\vartheta_\chi \cdot \overline{\vartheta_\chi} = 8$を満たす。

$$\Gamma = (\vartheta_\chi + \rho j)(1+i)(1+j)$$

$$= \vartheta_\chi(1+i) - \rho + \rho^3 + (\vartheta_\chi(1+i) + \rho - \rho^3)j$$

とおく($t=3,5,7$のとき、およびかける順をかえても同様に証明できるのでここでは省く)。$\vartheta_\chi(1+i)$の展開で$m=0$なるζ^m、すなわち1の係数は$\overline{\chi}(S_{K/F}1)(1+i) = \pm1\pm\rho^2$で、$m\neq0$なる$\zeta^m$の係数は$\pm1\pm\rho\pm\rho^2\pm\rho^3$である。従って$\Gamma$を基底$\{\rho^k\zeta^l, \rho^k\zeta^l j\}$, $0\leq k\leq3$, $0\leq l\leq n-1$で表わす時各係数は±1となり、

$$N(\gamma) = N(\vartheta_\chi + \rho j)N(1+i)N(1+j) = 8+1\cdot2\cdot2 = 4(8+1)$$

を満足する。これより定理が証明される。

また、$2^s n$次一般四元数型Hadamard行列が存在すれば次のようにその位数を倍にすることができる。

<u>定理5</u>　群環 ZG の元 $\xi=\alpha+\beta j$ の右正則表現行列が $2^s n$ 次一般四元数型Hadamard行列となるとき、ρ を1の原始 2^{s+1} 乗根とすると

$$\gamma=(\alpha+\beta j)(1+\rho^t j),\quad t=1,3,5,7,\cdots,2^s-1$$

の右正則表現行列は $2^{s+1}n$ 次一般四元数型Hadamard行列となる。ただし、$\alpha+\beta j$, $1+\rho^t j$ のかける順をかえてもよい。

(証明)　$\gamma=(\alpha+\beta j)(1+\rho j)=\alpha-\beta\rho+(\beta+\alpha\rho)j$

とおく ($t=3,5,7,\cdots,2^s-1$ のとき及びかける順をかえても同様に証明できるのでここでは省く)。$\alpha+\beta j$ が $2^s n$ 次一般四元数型Hadamard行列となることから、$\alpha-\beta\rho$, $\beta+\alpha\rho$ の $\{\rho^k\xi^l\}$, $0\leqq k\leqq 2^s-1$, $0\leqq l\leqq n-1$ に対する係数は ±1 で、

$$N(\gamma)=N(\alpha+\beta j)N(1+\rho j)=2^s n\cdot 2=2^{s+1}n$$

を満足する。

従って前の定理3、4から得られる $4n$, $8n$ 次一般四元数型Hadamard行列を出発点として 2^s に関する無限系列を構成することができる。

§4. 24次一般四元数型Hadamard行列

24次一般四元数型Hadamard行列をすべて求めた。それを

以下の変形

$$① \ \xi \to \xi^{\sigma}, \quad \sigma \in \mathrm{Aut}\,G,$$

$$② \ \xi \to \alpha\xi, \quad \alpha \in G,$$

を次々に施して移りあうものを同値とし分類した（①は Seidel 同値を与える）。その結果類の転置を除き8個の類に分かれる。これらの類の構成の原理を表で示す。定理3, 4から直接に構成されるもの以外は次の定理6を使って12次一般四元数型Hadamard行列から構成できることがわかる。

<u>定理6</u>　$\alpha = a_0 + a_1\rho + a_2\rho^2 + a_3\rho^3$, ρ：1の原始8乗根, ζ_n：任意の1のn乗根, $a_i\ (i=0,\cdots,3) \in Z[\zeta_n]$ に対し,

$$f(\alpha) = \bar{a}_0 a_2 + \bar{a}_1 a_3 - \bar{a}_2 a_0 - \bar{a}_3 a_1, \quad g(\alpha) = \bar{a}_0 a_1 + \bar{a}_1 a_2 + \bar{a}_2 a_3 - \bar{a}_3 a_0,$$

$$\sigma_3 : \rho \to \rho^3, \qquad \sigma_5 : \rho \to \rho^5 = -\rho, \qquad \sigma_7 : \rho \to \rho^7 = -\rho^3,$$

とおくと

$$\alpha\bar{\alpha} = a_0\bar{a}_0 + a_1\bar{a}_1 + a_2\bar{a}_2 + a_3\bar{a}_3 + f(\alpha)\rho^2 + g(\alpha)\rho + \overline{g(\alpha)}\,\bar{\rho}.$$

・$f(\alpha) = 0$, すなわち $a_0 + a_2 i + a_1 j + a_3 ij$ が $4n$ 次一般四元数型 Hadamard行列ならば

$$\alpha + \alpha^{\sigma_5} j, \quad \alpha + \bar{\alpha}^{\sigma_5} j \ \text{が}$$

・$f(\alpha) = 0$, $g(\alpha) = \overline{g(\alpha)}$ ならば, さらに

$\alpha + \alpha^{\sigma_3} j$, $\alpha + \bar{\alpha}^{\sigma_3} j$ が

・$g(\alpha) = 0$ ならば

$$\alpha + \alpha^{\sigma_3} j, \quad \alpha + \alpha^{\sigma_7} j, \quad \alpha + \bar{\alpha}^{\sigma_3} j, \quad \alpha + \bar{\alpha}^{\sigma_7} j$$

が $8n$ 次一般四元数型 Hadamard 行列を生成する。

24次一般四元数型 Hadamard 行列の同値類とその構成の原理	
▶ $\omega = 1$ のときの固有値が $(3,1,1,1)(3,-1,1,-1)$ で $\omega \neq 1$ のときの固有値が	
① $(0,-2,-2,-2)(0,2,-2,2)$ のとき	12次 Williamson 行列から定理6, σ_5 により変形
② $(0,-2,-2\omega,-2)(0,2,-2\omega,2)$ のとき	定理3, $g=11$ の12次一般四元数型 Hadamard 行列から定理6, σ_5 により変形
③ $(0,-2,-2\omega,-2)(0,2,-2\omega^2,2)$ のとき	定理3, $g=11$ の12次一般四元数型 Hadamard 行列から定理6, $\bar{\sigma}_5$ により変形
▶ $\omega = 1$ のときの固有値が $(3,1,1,-1)(3,-1,1,1)$ で $\omega \neq 1$ のときの固有値が	
④ $(0,-2,-2,2)(0,2,-2,-2)$ のとき	12次 Williamson 行列から定理6 σ_5 により変形
⑤ $(0,-2,-2\omega,2)(0,2,-2\omega,-2)$ のとき	定理3, $g=11$ の12次一般四元数型 Hadamard 行列から定理6, σ_5 により変形
⑥ $(0,-2,-2\omega^2,2\omega)(0,2\omega,-2\omega^2,-2)$ のとき	定理4, $g=5$

▶ $\omega=1$ のときの固有値が $(3,3,-1,1)(1,1,-1,1)$ で $\omega\neq 1$ のときの固有値が	
⑦ $(0,\ 0,\ 2\omega,\ -2)(-2\omega^2,\ -2,\ 2,\ -2\omega)$ のとき	定理 3, $q=23$
⑧ $(0,\ 0,\ 2,\ -2)(-2\omega,\ -2\omega^2,\ 2,\ -2)$ のとき	?

（記号の説明） $(\alpha_0, \alpha_1, \alpha_2, \alpha_3)(\beta_0, \beta_1, \beta_2, \beta_3)$ は左から成分行列 $A_0, A_1, A_2, A_3, B_0, B_1, B_2, B_3$ の各行列の固有値を示す。ω は 1の原始3乗根.

参 考 文 献

[1] N. Ito, Note on Hadamard matrices of type Q, *Studia Scientiarum Mathematicarum Hungarica* **16** (1981), 389-393.

[2] S. Lang, *Cyclotomic Fields*, Springer, New York, 1978.

[3] R. J. Turyn, An infinite class of Williamson matrices, *J. Combinatorial Theory, Ser. A* **12** (1972), 319-321.

[4] W. D. Wallis, A. P. Street and J. S. Wallis, *Combinatorics: Room squares, sum-free sets, Hadamard matrices*, Lecture Notes in Math. vol. **292**, Springer, New York, 1972.

[5] J. Williamson, Hadamard's determinant theorem and sum of four squares, *Duke Math. J.* **11** (1944), 65-81.

[6] 山田美枝子, Turyn型 Williamson行列について、京都大学数理解析研究所講究録 **404** (1980), 101-116.

[7] 山田美枝子, 有限体のガウスの和とそのアダマール行

列への応用，昭和58年度文部省科学研究費総合A「代数的整数論」研究集会報告集，1983，9-30.

[8] K. Yamamoto, On a generalized Williamson equation, Colloquia Mathematica Societatis János Bolyai **37** (1983).

[9] K. Yamamoto and M. Yamada, Williamson Hadamard matrices and Gauss sums, J. of Math. Soc. Japan **37** (1985), in print.

[10] M. Yamada, Hadamard matrices of generalized quaternion type, to appear.

268次のHadamard行列について

名工大 情報 澤出和江

1. n次のHadamard行列（以下，略してH－行列と書きます）とは，成分がすべて±1で，相異なる行（列）が直交している$n \times n$行列です。$4|n$のとき，n次H-行列は常に存在するらしいという有名な予想がありますが，これまで多くの人々によってH－行列の無限系列や特定の次数のH－行列が発見されており，現在なお未解決の問題とは言えこの予想は確かなようです．92次がBaumert, Golomb-Hallによって1962年に，188次と236次がTurynによってそれぞれ1973年と1974年に発見された後，268（$=4 \cdot 67$）次のH－行列がこれまで存在が確認されていない最小次数のH－行列でしたが，昨年12月8日に計算機を使ってこの行列を構成することができましたので報告致します。

2. まず，この構成に必要な幾つかの行列を定義します。

定義1．$p\times p$ $(0,\pm1)$－行列 $A=(a_{ij})$，$B=(b_{ij})$，$C=(c_{ij})$，$D=(d_{ij})$ は次の３つの条件を満たすとき，p次のT－行列という。

(i) A, B, C, D は巡回行列である，

(ii) $|a_{ij}|+|b_{ij}|+|c_{ij}|+|d_{ij}|=1$ $\quad (1\leqslant i, j\leqslant p)$，

(iii) $AA^T+BB^T+CC^T+DD^T=pI_p$．

「T－行列」の名は，この行列を初めに考案したR. J. Turyn のイニシャル『T』を取って付けたものと思われます。

定義2．$r\times r$ 対称 (±1)－行列 W_i $(i=1,2,3,4)$ は次の２つの条件を満たすとき，r次のWilliamson行列という．

(i) $W_iW_j=W_jW_i$ $\quad (1\leqslant i, j\leqslant 4)$，

(ii) $W_1^2+W_2^2+W_3^2+W_4^2=4rI_r$．

また，$M\otimes N$を行列MとNのテンソル積とし，$S=(s_{ij})$ はp次基本的逆巡回行列：

$$s_{ij}=\begin{cases}1 & i+j\equiv1 \pmod p \text{ のとき}\end{cases}$$

とします．この行列Sと，上で定義したT－行列A，B，C，Dおよび Williamson 行列 W_i ($i=1,2,3,4$)を使って行列X，Y，Z，VとRを次のように定義します：

$$R = S \otimes I_r,$$
$$X = A \otimes W_1 + B \otimes W_2 + C \otimes W_3 + D \otimes W_4,$$
$$Y = -A \otimes W_2 + B \otimes W_1 + C \otimes W_4 - D \otimes W_3,$$
$$Z = -A \otimes W_3 - B \otimes W_4 + C \otimes W_1 + D \otimes W_2,$$
$$V = -A \otimes W_4 + B \otimes W_3 - C \otimes W_2 + D \otimes W_1.$$

問題のH－行列の構成には次の定理が重要です。

定理（Turyn［7］，Cooper-Wallis［1］）．T－行列A，B，C，Dと Williamson 行列 W_1, W_2, W_3, W_4 があれば，上のように定義された行列X，Y，Z，V，Rに対して行列

$$\begin{pmatrix} X & YR & ZR & VR \\ -YR & X & -V^TR & Z^TR \\ -ZR & V^TR & X & -Y^TR \\ -VR & -Z^TR & Y^TR & X \end{pmatrix}$$

は，4pr次の Hadamard 行列になる。

証明．直接計算により容易に証明できる。

上の定理で，$r=1$ として得られる $4p$ 次の H－行列は一般に Goethals－Seidel 型 H－行列と呼ばれています。この定理を使えば，268 次の H－行列を構成することは，$r=1$，$W_1=W_2=W_3=W_4=1$ に取って，67 次の T－行列を構成することに帰着されます。

3．$U=(u_{ij})$ は p 次基本的巡回行列：

$$u_{ij}=\begin{cases}1 & j\equiv i+1 \pmod p \text{ のとき，}\\ 0 & \text{その他}\end{cases}$$

とします．T－行列を構成する4つの行列 A, B, C, D は巡回行列ですから，U の多項式として表わせます。

p を素数で $p\equiv 1 \pmod 3$ と仮定します．すると，$p=\alpha^2+3\beta^2$，$\alpha\equiv 1 \pmod 3$ として（β の符号を無視すれば）一意的に表わせます。γ を p の原始根，w を $\bmod p$ で $w^3\equiv 1$ かつ $w\not\equiv 1$ を満たす数と仮定します．そして，巡回群 $\{I_p, U, \ldots, U^{p-1}\}$ の自己同型 $\varphi: U\to U^w$ のもとで，A は不変で，B, C, D は巡回的に置換されるような T－行列 A, B, C, D を考えます。このような T－

行列を w 型T－行列と呼ぶことにします．67 は素数 $\equiv 1 \pmod 3$ ですから，67 次 w 型T－行列の存在する可能性があるわけです．$e=(p-1)/3$，$h=e/2$，$\Omega=\{0,1,\ldots,e-1\}$，$A_+, A_-, B_+, B_-$ を Ω の分割，$\delta(i)$ $(i\in\Omega)$ を値 0，1 または 2 を取るものとすると，w 型T－行列は一般に次のような形で表わせます．

$$\begin{cases} A = I_p + \sum_{i\in A_+}(U^{\gamma^i}+U^{w\gamma^i}+U^{w^2\gamma^i}) - \sum_{i\in A_-}(U^{\gamma^i}+U^{w\gamma^i}+U^{w^2\gamma^i}) \\ B = \sum_{i\in B_+} U^{w^{\delta(i)}\gamma^i} - \sum_{i\in B_-} U^{w^{\delta(i)}\gamma^i} \\ C = \varphi(B) \\ D = \varphi(C) \end{cases}$$

一方，U から 1 の原始 p 乗根 ζ への対応によって，T－行列は円周 p 等分体の整数と対応させることができます．A, B, C, D に対応する整数は $a(\zeta)$，$b(\zeta)$，$c(\zeta)$，$d(\zeta)$ ですから，定義 1 の (iii) は

$$a(\zeta)\overline{a(\zeta)} + b(\zeta)\overline{b(\zeta)} + c(\zeta)\overline{c(\zeta)} + d(\zeta)\overline{d(\zeta)}$$

$$= |a(\zeta)|^2 + |b(\zeta)|^2 + |c(\zeta)|^2 + |d(\zeta)|^2 = p \qquad (1)$$

となります．T－行列探索時の数値計算には，(1) 式を使います．

4．$p=67$ に固定すると，$e=22$，$h=11$，$\Omega=\{0,$

$1,\ldots,21\}$，$a(1)=\alpha=-8$ より $\#A_+ + 3 = \#A_-$，$b(1)=c(1)=d(1)=\beta=\pm 1$ より $\#B_+ \pm 1 = \#B_-$ ですが複号は，B，C，D を -1 倍する操作で反転し，T－行列になる事実は変りませんから，$b(1)>0$，$\#B_+ - 1 = \#B_-$ に固定します。すると，$\#A_+$, $\#A_-$, $\#B_+$, $\#B_-$ の分布は10通り：

	<1>	<2>	<3>	<4>	<5>	<6>	<7>	<8>	<9>	<10>
$\#A_+$	9	8	7	6	5	4	3	2	1	0
$\#A_-$	12	11	10	9	8	7	6	5	4	3
$\#B_+$	1	2	3	4	5	6	7	8	9	10
$\#B_-$	0	1	2	3	4	5	6	7	8	9

が考えられ，その中で解が最も多く存在しそうな分布は <9> と <10> ですが，探索時間を適当に短縮できて，しかも解が得られそうな条件が必要です。$p<67$, $p\equiv 7 \pmod{12}$，すなわち $p=7, 19, 31, 43$ の場合について調べた結果，$p=67$ の場合前者の濃度分布 <9> に対して，$A_+=\{h\}$，$B_+ \ni 0$，0 と h 以外の Ω の要素はすべて i と $e-i$ で対になって，A_-, B_+, B_- にそれぞれ属するという条件を付けた上で，B_+ の要素をすべて偶数にしても解が得られる望みはあると判断し，探索してみました。探索方法は，計算時間を極力減らしたい為，p進近似による判定条件［9, 4］を使って，整数計算だけで解の候補を約 $1/67$ にふるいおとし，更に倍精度の cos，sin 近

似計算で約 1/200 におとし，最終的に (1)式の左辺を展開して，係数比較により解をもとめるというものです。上の条件のもとで探索の試行回数は約8億通り，計算時間は約40時間（使用計算機は往年の名計算機 HITAC 8000 シリーズの1つ H-8450 です）。残念ながら，B+の要素は全て偶数という条件では解が得られませんでしたが，この条件を少し変えて得られた解が次のようです。この解から，どのような条件に変えたのかは明らかだと思います。

$$A = I + X(11) - X(2) - X(20) - X(3) - X(19),$$

$$\begin{aligned} B = {} & X(0,0)+X(13,2)+X(9,2)+X(4,0)+X(18,0)+X(10,2)+X(12,1)+X(6,0)+X(16,2) \\ & -X(8,0)-X(14,2)-X(7,1)-X(15,2)-X(1,1)-X(21,0)-X(5,1)-X(17,2), \end{aligned}$$

$$\begin{aligned} C = {} & X(0,1)+X(13,0)+X(9,0)+X(4,1)+X(18,1)+X(10,0)+X(12,2)+X(6,1)+X(16,0) \\ & -X(8,1)-X(14,0)-X(7,2)-X(15,0)-X(1,2)-X(21,1)-X(5,2)-X(17,0), \end{aligned}$$

$$\begin{aligned} D = {} & X(0,2)+X(13,1)+X(9,1)+X(4,2)+X(18,2)+X(10,1)+X(12,0)+X(6,2)+X(16,1) \\ & -X(8,2)-X(14,1)-X(7,0)-X(15,1)-X(1,0)-X(21,2)-X(5,0)-X(17,1), \end{aligned}$$

ここで，$0 \leqq i \leqq 21$，$0 \leqq j \leqq 2$ に対し

$$X(i) = U^{2^i} + U^{37 \cdot 2^i} + U^{29 \cdot 2^i},$$

$$X(i,j) = U^{37^j 2^i},$$

もっと簡単に書くと，

$$A = I+U^{30}+U^{38}+U^{66}$$
$$-U^{4}-U^{8}-U^{12}-U^{13}-U^{14}-U^{17}-U^{24}-U^{26}-U^{28}-U^{31}-U^{42}-U^{49}$$

$$B = U+U^{15}+U^{16}+U^{22}+U^{40}+U^{41}+U^{53}+U^{64}+U^{65}$$
$$-U^{7}-U^{11}-U^{39}-U^{44}-U^{45}-U^{46}-U^{52}-U^{55}$$

$$C = \varphi(B)$$

$$D = \varphi(C)$$

上の結果と先の定理により，r次Williamson行列が存在すれば，$268 \cdot r$次のH－行列が存在することがわかります。

また，TurynはH－行列の構成に非常に有用な2つの配列，すなわちBaumert－Hall配列とBaumert－Hall－Welch配列（定義については，[1]または[7]を参照）の中，後者とT－行列の存在を仮定して，前者の存在を示す重要な定理（[1, Theorem 4.79.]）を考えました。これまでに知られているBaumert－Hall－Welch配列は，5次[8]と9次[3]の2つだけですが，Turynの定理と先の結果を使って，335（$=5 \cdot 67$）次と603（$= 9 \cdot 67$）次のBaumert－Hall配列が構成できることになります。そして，r次Williamson行列が存在すれば，$335 \cdot r$次および$603 \cdot r$次のH－行列が存在することがわかりま

す。

以上の結果から，存在未確認のH－行列の最小次数は412（＝4·103）になることを明記して報告を終ります。

文　献

[1] A.V. Germita and J. Seberry, Orthogonal designs, Lecture Notes in Pure and Applied Mathematics, vol. 45, Dekker, 1979.

[2] M. Hall, Jr., Combinatorial theory, Blaisdel Waltham, Mass., 1967.

[3] 小野貴生・沢出和江，36次のBaumert-Hall-Welch配列，数学，36-2 (1984), 76-78.

[4] K. Sawade, Hadamard matrices of order 100 and 108, Bull. of Nagoya Institute of Technology 29, (1977), 147-153.

[5] 沢出和江，ある特殊なT－行列について，京都大学数理解析研究所講究録，429 (1981), 85-98.

[6] K. Sawade, A Hadamard matrix of order 268, Graphs and Combinatorics, (to appear).

[6] R.J. Turyn, Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compressions and surface wave encodings, J. Combinatorial Theory, Ser. A, 16 (1974), 313-333.

[8] W.D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis, Combinatorics: Room squares, sum-free sets, Hadamard matrices, Lecture Notes in Math., vol. 292, Springer, New York, 1972.

[9] K. Yamamoto, An explicit formula of the norm residue symbol in a local number field, Science Reports of Tokyo Woman's Christian College, 24-28 (1972), 302-334.

二重可移群に関係した可換代数

阪教大・教育　鈴 木 寛

1° 導入

常に次を仮定する。

仮定 (1) G : $\Omega=\{1,2,\cdots,m\}$ 上の二重可移群。

(2) $G_{\{1,2\}}$ は 軌道を3つもつ, i.e., $\{1,2\}\cup\Omega_{12}^{1}\cup\Omega_{12}^{2}$.

ここで $|\Omega_{12}^{t}|=r_t$, $\Omega_{ij}^{t}=(\Omega_{12}^{t})^{g}$ 但し $\{1^g, 2^g\}=\{i,j\}$

$g\in G$ とするとき.

(3) $k\in\Omega_{ij}^{t}\Leftrightarrow i\in\Omega_{jk}^{t}\Leftrightarrow j\in\Omega_{ki}^{t}$　　$t=1,2.$

注 (1) Ω_{ij}^{t}: well-defined, i.e., g のとり方によらない。

(2) $\Omega_{ij}^{t}=\Omega_{ji}^{t}$

(3) $r_1\neq r_2$ ならば, (3)は, (1), (2) から出る。

定義 (1). $A(c_1,c_2)$: 次元 n の $\mathbb{C}$ 上の代数で基底

$\{x_1,\cdots,x_n\}$ 上. 次の式で定義されたもの。

$$x_ix_i=(c_1r_1+c_2r_2)x_i$$

$$x_i x_j = c_1 \sum_{k\in\Omega_{ij}^1} x_k + c_2 \sum_{k\in\Omega_{ij}^2} x_k \qquad 1\le i\neq j\le n$$

(2) $\mathcal{A}_1(c_1, c_2)$：次元 $n-1$ の $\mathbb{C}$ 上の代数で基底 $\{e_1,\cdots,e_{n-1}\}$ 上．次の式で定義されたもの。

$$e_i e_i = (c_1 r_1 + c_2 r_2) e_i$$

$$e_i e_j = c_1 \sum_{k\in\Omega_{ij}^1} e_k + c_2 \sum_{k\in\Omega_{ij}^2} e_k \qquad 1\le i\neq j\le n-1$$

但し．$e_n := -(e_1+\cdots+e_{n-1})$ とする。

(3) $\mathcal{A}$：代数のとき．$\mathrm{Aut}\mathcal{A}=\{\sigma\in GL(\mathcal{A}) \mid x^\sigma y^\sigma=(xy)^\sigma, x,y\in\mathcal{A}\}$ とし．$H\le \mathrm{Aut}\mathcal{A}$ のとき．$\mathcal{A}$ を H-不変という。

(4) $\mathbb{C}[\Omega]$ を．$\{x_1,\cdots,x_n\}$ を基底とする置換加群．$\delta = x_1+\cdots+x_n$ とし．$\mathbb{C}[\Omega]=V=V_0+V_1$．ただし $V_0=\langle\delta\rangle$，$V_1=\{\sum\lambda_i x_i \mid \sum\lambda_i=0\}$ とする。V_0, V_1 は．G-不変でかつ既約である。

この定義と．仮定のもとで．次の定理 A, B, C が成立する。

<u>定理 A.</u> $\mathcal{A}_1$ を V_1 上の G-不変な代数とすると．$c_1, c_2\in\mathbb{C}$ で．$\mathcal{A}_1=\mathcal{A}_1(c_1,c_2)$ をみたすものが存在する。ここで．$e_i=x_i-\frac{1}{n}\delta$ である。逆に．任意の c_1, c_2 $(\in\mathbb{C})$ について．$\mathcal{A}_1(c_1,c_2)$ は G-不変である。

<u>定理 B</u>　$\mathcal{A}=\mathcal{A}(c_1, c_2)$　$c_1r_1+c_2r_2\neq 0$ とする。この時、次が成り立つ。

(1)　V_0, V_1 は $\mathrm{Aut}\,\mathcal{A}$－不変である。

(2)　V_0, V_1 は $\mathcal{A}$ のイデアルで、かつ $e_i=x_i-\frac{1}{n}\delta$ と置くことにより、$\mathcal{A}|V_1=\mathcal{A}_1(c_1, c_2)$ となる。

(3) 制限写像 $\mathrm{Aut}\,\mathcal{A}\to GL(V_1)$ は、自然に、次の同型をひきおこす。　$\mathrm{Aut}\,\mathcal{A}\simeq\mathrm{Aut}\,\mathcal{A}_1(c_1, c_2)$.

<u>定理 C</u>　$\mathcal{A}=\mathcal{A}(c_1, c_2)$ 又は $\mathcal{A}_1(c_1, c_2)$ とする。この時、次の (i)～(v) のいずれかが成立する。

(i)　$\mathrm{Aut}\,\mathcal{A}$　は　Σ_n の部分群に同型である。

(ii)　$r_1=r_2=2(p_{11}^1+1)$, $p_{12}^1=p_{22}^1=p_{11}^2=p_{12}^2=p_{11}^1+1=p_{22}^2+1$

ここで　$p_{ij}^k=|\Omega_{12}^i\cap\Omega_{1t}^j|$　　$t\in\Omega_{12}^k$

(iii)　$c_1r_1+c_2r_2=0$

(iv)　$c_1^2r_1+c_2^2r_2=0$

(v)　$c_1r_1+c_2r_2\neq 0$ かつ、$c_1/(c_1r_1+c_2r_2)$ は、(G, Ω) だけから決まる 4次の多項式 $f(x)\in\mathbb{Z}[X]$ の根である。

<u>注</u> (1)　G が仮定をみたす Σ_n の部分群のうち極大

ならば，定理C (i) かつ $c_1 \neq c_2$ であれば，$\mathrm{Aut}A = G$ が得られる。

(2) (v)にあらわれる多項式 $f(x)$ の最高次の係数が，$r_2^2(p_{11}^1 - p_{11}^2) - 2r_1r_2(p_{12}^1 - p_{12}^2) + r_1^2(p_{22}^1 - p_{22}^2)$ であり，これが 0 となることと，(ii) とが同値。

(3). $f(x)$ は，$|\Omega_{ij}^t \cap \Omega_{k\ell}^s|$，$i,j,k,\ell (*)$ と p_{ij}^k によって決まる。p_{ij}^k は，簡単に求まるが，$|\Omega_{ij}^t \cap \Omega_{k\ell}^s|$ をすべて決定し，$f(x)$ を具体的に計算するのは大変であるので，簡単な計算方法を見つける事が望まれる。

(4). $|\Omega_{12}^1 \cap \Omega_{ij}^1| = |\Omega_{1i}^1 \cap \Omega_{2j}^1|$ がすべての $i,j\ (\neq 1,2)$ について成立する時，(*)をみたすということにする。(*)を満たせば，$f(x)$ は p_{ij}^k だけで書ける。

この方面で，今迄に知られている結果は，次の通りである。

(1) [HARADA] $\mathrm{Aut}\,A_1(c,c) = \Sigma_n$ ただし $c \neq 0$.

(2) [NARANG] $\mathrm{Aut}\,A_1(\frac{1}{r_1}, 0) = P\Gamma L(n,q)$ ただし，$(G,\Omega) = (P\Gamma L(n,q), \mathbb{P}^{n-1}(q))$ で $n \geq 3$，自然な二重可移表現である。

2° 証明

定義 $H \leq GL(W)$ とする。

(1) $\mathcal{L}(W^r;W)=\{\Theta : W\times\overset{r}{\cdots}\times W\to W \quad r\text{-重線型}\}$

$\mathcal{L}^S(W^r;W)=\{\Theta\in\mathcal{L}(W^r;W) \mid \Theta:\text{対称}\}$

(2) $\mathcal{L}(W^r;\mathbb{C})=\{\Theta : W\times\overset{r}{\cdots}\times W\to \mathbb{C} \quad r\text{-重線型}\}$

$\mathcal{L}^S(W^r;\mathbb{C})=\{\Theta\in\mathcal{L}(W^r;\mathbb{C}) \mid \Theta:\text{対称}\}$

(3) $\Theta\in\mathcal{L}(W^r;W)$ の時

$\mathrm{Aut}\,\Theta=\{\sigma\in GL(W) \mid \Theta(u_1^\sigma,\cdots,u_r^\sigma)=\Theta(u_1,\cdots,u_r)^\sigma\}$

(4) $\Theta\in\mathcal{L}(W^r;\mathbb{C})$ の時

$\mathrm{Aut}\,\Theta=\{\sigma\in GL(W) \mid \Theta(u_1^\sigma,\cdots,u_r^\sigma)=\Theta(u_1,\cdots,u_r)\}$

(5) Θ : H-不変 $\Leftrightarrow$ $\mathrm{Aut}\,\Theta\geq H$.

(6) $\mathcal{L}\in\{\mathcal{L}(W^r;W),\mathcal{L}^S(W^r;W),\mathcal{L}(W^r;\mathbb{C}),\mathcal{L}^S(W^r;\mathbb{C})\}$

とする時. $\mathcal{L}_H=\{\Theta\in\mathcal{L} \mid \mathrm{Aut}\,\Theta\geq H\}$

$\mathcal{L}^S(W^2;W)$ の元と可換代数は. 自然に対応している事に注意しておく。

これらの記号のもとで. まず. 次の二つの補題が. 成り立つ。一つ目の補題の証明は容易であるが. 二つ目の補題の証明には. 現在のところ. BENDER の "Strongly Embedded" の結果が用いられている。

補題1 (1) $\dim \mathcal{L}^S(V_1^3;\mathbb{C})_G \leq \dim \mathcal{L}^S(V_1^2;V_1)_G = 2$

(2). $G \leq H \leq \Sigma_n$. $H_{\{1,2\}}$ が $\Omega-\{1,2\}$ 上可移ならば. $\mathcal{L}^S(V_1^2;V_1)_H = \langle \Theta_S \rangle$ で Θ_S は $A_1(c,c)$ $c \neq 0$ を定義する。

補題2 (EGAWA-SUZUKI) $\mathcal{L}^S(V_1^3;\mathbb{C})_{\Sigma_n} = \langle \theta^S \rangle \leq \mathcal{L}^S(V_1^3;\mathbb{C})_G$ かつ. $\mathrm{Aut}\,\theta^S \cong \mathbb{Z}_3 \times \Sigma_n$ である.

定義 (1) $S \in \mathcal{L}(V^1;\mathbb{C})$. $S(\sum \lambda_i x_i) = \sum \lambda_i$

(2) $B \in \mathcal{L}^S(V^2;\mathbb{C})$, $B(\sum \lambda_i x_i, \sum \mu_i x_i) = \sum \lambda_i \mu_i$

以下に. 定理 C′ の証明の概要を記す。

$c_1 r_1 + c_2 r_2 \neq 0$ とする. $\mathrm{Aut}\,A_1(c_1 c_2) = \mathrm{Aut}\,A_1(c_1/a, c_2/a)$ ($c_1 r_1 + c_2 r_2 = a$) だから. $c_1 r_1 + c_2 r_2 = 1$ と仮定してよい。

$\mathcal{L}^S(V_1^3;\mathbb{C})_{\mathrm{Aut}A_1} \leq \mathcal{L}^S(V_1^3;\mathbb{C})_G \geq \mathcal{L}^S(V_1^3;\mathbb{C})_{\Sigma_n} = \langle \theta^S \rangle$

で. $\mathcal{L}^S(V_1^3;\mathbb{C})_G$ の次元は. 補題1より 2以下だから.

$m = \dim \mathcal{L}^S(V_1^3;\mathbb{C})_{\mathrm{Aut}A_1}$ とすると. 三つの場合に分かれる。ここで $A_1 = A_1(c_1, c_2)$.

● Case 1 $m = 0$

あとで定義される $\Theta_0 \in \mathcal{L}^s(V_1^3;\mathbb{C})_{\mathrm{Aut}A_1}$ が 0 となることより．$c_1^2 r_1 + c_2^2 r_2 = 0$ すなわち．Case(iv) が得られる。

◎ Case 2　$m=2$.

$\mathcal{L}^s(V_1^3;\mathbb{C})_{\mathrm{Aut}A_1} = \mathcal{L}^s(V_1^3;\mathbb{C})_G \geq \mathcal{L}^s(V_1^3;\mathbb{C})_{\Sigma_n} = \langle \Theta^s \rangle$

より．Θ^s が $\mathrm{Aut}A_1$-不変。補題2より．

$$\mathrm{Aut}A_1 \leq \mathrm{Aut}\,\Theta^s \cong Z_3 \times \Sigma_n$$

が得られ．Case (i) が得られる。

◎ Case 3　$m=1$

$c_1^2 r_1 + c_2^2 r_2 \neq 0$ と仮定することによって得られる．$0 \neq \Theta_0 \in \mathcal{L}^s(V_1^3;\mathbb{C})_{\mathrm{Aut}A_1}$ と．これもあとに作り方を示す $\Theta_1 \in \mathcal{L}^s(V_1^3;\mathbb{C})_{\mathrm{Aut}A_1}$ が．相似であることより．$\exists \lambda \in \mathbb{C}-\{0\}$ s.t. $\Theta_1 = \lambda\Theta_0$. さらに．この等式をみたすには．高々4次の多項式 $f(x)$ があって．$f(c_1)=0$ となることが示され．Case (ii) と (v) が得られる.

従って．以下に．Θ_0, Θ_1 を構成するのに用いられ．かつ．定理B を証明するのにも有効な補題と．その応用の仕方を記す。

<u>補題3.</u> $\Theta \in \mathcal{L}(V^{r+1}; V)$ とする時.

$$\delta(\Theta)(u_1, \cdots, u_r) = \mathrm{Tr}(\Theta(u_1, \cdots, u_r, *))$$
$$= \sum_{i=1}^{n} B(\Theta(u_1, \cdots, u_r, x_i), x_i)$$

で $\delta(\Theta)$ を定義すると. $\delta(\Theta) \in \mathcal{L}(V^r; \mathbb{C})$ であり,

$\mathrm{Aut}\,\Theta \leq \mathrm{Aut}\,\delta(\Theta)$ が成り立つ。

<u>補題3. の応用</u>

(1). $\Theta(u_1, u_2, u_3, u_4) = (u_1 u_2)(u_3 u_4)$ として補題を用い $\delta(\Theta) = \Theta_0'$ とおくと. $\Theta_0' \in \mathcal{L}^S(V^3; \mathbb{C})_{\mathrm{Aut}A}$. 上記の Θ_0 は Θ_0' を V_1 上に制限したものである。

(2) $\Theta(u_1, u_2, u_3, u_4) = u_1(u_2(u_3 u_4))$ として補題を用い $\delta(\Theta) = \Theta_1'$ とおくと. $\Theta_1' \in \mathcal{L}^S(V^3, \mathbb{C})_{\mathrm{Aut}A}$. 上記の Θ_1 は. Θ_1' を V_1 上に制限したものである。

(3) $\Theta(u_1, u_2) = u_1 u_2$ のとき $\delta(\Theta) = S$

(4) $\Theta(u_1, u_2, u_3) = u_1(u_2 u_3)$ のとき $\delta(\Theta)$ は. 対称二次形式.

(3) より. $\mathrm{Ker}\,S$ である V_1 が $\mathrm{Aut}A$-不変である事(定理B参照) が得られ. 直接必要ではないが. (4) から B も $\mathrm{Aut}A$-不変であることが示される。

3° 例

(1) $G = P\Gamma L(m, q)$ $m \geqslant 3$ $\Omega = \mathbb{P}^{m-1}(q)$ とすると. $n = (q^m - 1)/(q-1)$, $r_1 = q-1$, $r_2 = q^{m-1} + \cdots + q^2$ で. $r_1 \neq r_2$ であるから. 仮定がみたされる。又. この時. $p_{11}^1 = q-2$ で. 性質(*)もみたされていることが示せるので. $f(x)$ も計算でき. 定理C が Narang の結果を含むこともわかる。

(2). $G = PSL(2, 11)$ $G = \langle \alpha, \beta, \gamma \rangle$

$\alpha = (0\,1\,2\,3\,4\,5\,6\,7\,8\,9\,X)$ $\beta = (0)(1\,3\,9\,5\,4)(2\,6\,7\,X\,8)$

$\delta = (0)(19)(26)(3)(45)(78)(X)$

この時は. $r_1 = 3$, $r_2 = 6$ $p_{11}^1 = 0$ で 仮定. 性質(*)共にみたされる。

(3). $G = Co.3$ $n = 276$, $r_1 = 112$, $r_2 = 162$, $p_{11}^1 = 30$ で仮定はみたされているが, 性質(*) は成立しない。

(4) $G = Sp(2m, 2)$ は二つのタイプがあり. $\varepsilon = \pm 1$ $n = 2^{m-1}(2^m + \varepsilon)$, $r_1 = 2(2^{m-1} - \varepsilon)(2^{m-2} + \varepsilon)$, $r_2 = 2^{2m-2}$ $p_{11}^1 = 2^{2m-3} + \varepsilon 2^{m-1} - 3$. $m \geqslant 3$ のとき仮定はみたされる

が、性質(ヵ) はみたされていない。

以上が、定理が有効に用いられる例である 以下に、定理が使えない例を記す。

(5) 三重可移群、V_1 上の 代数 からできるものはすべて $A_1(c,c)$ つまり 自己同型群はいつも Σ_n.$(c\neq 0)$ したがって、高次の多重線型写像か、他の表現を用いなければ、不可能, $PSL(2,q)$ $(q\equiv -1\ (4))$ も同様.

(6) $PSL(2,q)$ $(q\equiv +1\ (4))$ 定理Cの (ii) がおこる。この場合は、他の方法で、示される可能性がある.

(7) A_7 $n=15$. $A_7 < A_8 = PSL(4,2)$ なので、仮定をみたすものの中で極大でないため、代数の自己同型は A_8 を含んでしまい、(5) の場合と似ている。

(8) HS, $PSU(3,q)$, ${}^2G_2(q)$ いずれも $G_{\{1,2\}}$ の軌道の数が、多い。(但し HS は4)。定理を直接は使えないが、上記証明の手法を用いて、これらの群を

自己同型群にもつ可換代数の存在は示せるかもしれない。いずれにせよ、二重可移群から自然にできる代数の自己同型群を考察するには、この場合(8)が興味深そうである。

可換代数の自己同型群の研究は、また散発的にしかなされていないが、一つの代数の自己同型群を考えるのに今のところ必ず一つは新しいアイディアを必要とし、現在は道具を揃えるのが本質的に思われる。

Block代数の直既約な商環について

北大. 理学部　池田　正

有限群の modular 表現論において．群 G の block B は G-algebra とみなされる場合や．$G\times G$-加群とみなされる場合がある。(c.f. [1], [5])．しかし．この2つの場合．block B が interior G-algebra になっていることが本質的である。このノートでは．block の場合をやや一般化した interior G-algebra の $G\times G$-加群として持つ性質を調べることを中心におく。

今．Gを有限群とし．pを素数、kを標数がpの代数的閉体、eをkGの中心的原始巾等元とし．$B=kGe$をそれに対応する block とする。Bはeを単位元とする k-algebra となる。

このノートでは k-algebra はすべて．k上有限次な単位元をもつものとし．k-algebra 上の加群は．すべて k上有限次な右加群とする。

1°. Interior G-algebras.

Aを k-algebra とし，ρを kG から A への k-algebra homomorphism とした時，対 (A, ρ) を interior G-algebra とよぶ。Gの部分群 H に対し，Hによって共役作用で固定される部分環を $A^H = \{a \in A \mid \rho(h^{-1})a\rho(h)$ for $^\forall h \in H\}$ とする。もし $A^G = Z(A)$（Aの中心）が local ring となるとき，(A, ρ)を local interior G-algebra とよび，また，もし，homomorphism ρ が"上へ"の写像であるとき，(A, ρ)を epimorphic interior G-algebra とよぶ。

(A, ρ)を local interior G-algebra とし，Hを G の部分群とした時，トレース写像 $\mathrm{Tr}_H^G : A^H \longrightarrow A^G$ を $a \longmapsto \sum \rho(g^{-1})a\rho(g)$，但し gは Gの右 H-coset の代表系を動く，で定義する。$\mathrm{Tr}_H^G(A^H) = A_H^G$ は A^G の両側イデアルになる。そこで，1を Aの単位元として，$A_H^G \ni 1$ となる Gの部分群 H 全体の極小部分群を，local interior G-algebra (A, ρ)の defect 群とよぶ。defect 群は G-共役を除いて一意的に定り，更に Gの p-部分群 になる。

<u>例1</u>　Vを直既約な kG-加群とする。$E_V = \mathrm{End}_k(V)$，ρを Vに対応する kG から E_Vへの表現とする。このとき

(E_V, ρ) は local interior G-algebra となる。更に、この場合の defect 群は、加群 V の vertex $(= vtx_G V)$ と一致する。また、もし V が既約 kG-加群のとき、(E_V, ρ) は epimorphic かつ local interior G-algebra となる。

<u>例2</u>　$B = kGe$ を G の block とする。$\rho : kG \longrightarrow B$ を $x \longmapsto xe$ とすると、(B, ρ) は epimorphic & local interior G-algebra となる。この際の defect 群は、古典的な block の defect 群と一致する。

(A, ρ) を local interior G-algebra とし、B を G の block とする。もし $\rho(B) \neq 0$ のとき、(A, ρ) は block B に属するという。

(A, ρ) を interior G-algebra とした時、k-algebra A は、次のように $k(G \times G)$-加群になる：$a \in A$, $(g, h) \in G \times G$ として、$a \cdot (g, h) = \rho(g^{-1}) a \rho(h)$。以下、しばしば、$A$ をこのように $k(G \times G)$-加群とみなす。したがって例1のようにして、$E_A = \mathrm{End}_k(A)$ として、E_A は interior $G \times G$-algebra となっている。

(A, φ) を interior G-algebra とし、H を G の部分群とした時、次の k-algebra homomorphisms Ψ_H, Φ_H を次のように定義する。

$$\begin{array}{cccc} \Psi_H : \mathrm{End}_{G\times H}(A) = (E_A)^{G\times H} & \longrightarrow & A^H \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ f & \longmapsto & f(1) \end{array}$$

$$\begin{array}{cccc} \Phi_H : A^H & \longrightarrow & \mathrm{End}_{G\times H}(A) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ b & \longmapsto & (a \longmapsto ab) \end{array}$$

次の補題はセクション 2 で利用される。

<u>補題1</u>　上の記号の下で、

(1) $\mathrm{End}_{G\times G}(A) \underset{\Phi_G}{\overset{\Psi_G}{\rightleftarrows}} A^G \longrightarrow 0$ は split する。

(2) (A, φ) が epimorphic interior G-algebra ならば、

$\mathrm{End}_{G\times G}(A) \xrightarrow[\sim]{\Psi_G} A^G$ となる。

(3) 次の図式は可換になる。

$$\begin{array}{ccc} \mathrm{End}_{G\times G}(A) & \xleftarrow{\ \Phi_G\ } & A^G \\ \Big\uparrow {\scriptstyle \mathrm{Tr}_{G\times H}^{G\times G}} & & \Big\uparrow {\scriptstyle \mathrm{Tr}_H^G} \\ \mathrm{End}_{G\times H}(A) & \xleftarrow[\ \Phi_H\ ]{} & A^H \end{array}$$

(証明) (1) 定義より明らか。

(2) Ψ_G が injective のみ示せば十分。 $f, g \in \mathrm{End}_{G\times G}(A)$ として、$\Psi_G(f) = \Psi_G(g)$ とする。すると $f(1) = g(1)$。また $G\times G$-作用の定義より、$x \in kG$ として、$f(\rho(x)) = \rho(x)f(1)$、$g(\rho(x)) = \rho(x)g(1)$ 故に ρ が surjection から $f = g$ となる。

(3) 定義より容易。 //

<u>系2</u> (A, ρ) が epimorphic interior G-algebra のとき、A が直既約 $k(G\times G)$-加群となるための必要十分条件は、(A, ρ) が local interior G-algebra となることである。

2°. vertex of $k(G\times G)$-module A

このセクションでは、次の定理を証明する。

<u>定理A</u> (A, ρ) を epimorphic & local interior G-algebra とし、その defect 群を D とする。この時、

$$D^{\Delta} \leq_{G\times G} \mathrm{vtx}_{G\times G} A \leq_{G\times G} D\times D$$

が成立する。但し、$D^{\Delta} = \{(d, d) \in D\times D \mid d \in D\}$ である。

定理Aを示すため、次のよく知られた2つの補題を準備する。

VをkG-加群とし、HをGの部分群とする。VのHの作用で固定されるVの部分空間を$V^H=\{v\in V \mid vh=v,\ h\in H\}$とし、トレース写像 $\mathrm{Tr}_H^G: V^H \longrightarrow V^G$ を $v \longmapsto \sum_g vg$, 但し gはHの右-cosetの代表を動く、として $V(P)= V^P/\sum_{Q<P}\mathrm{Tr}_Q^P(V^Q)$ とおく，但し PはGのp-部分群とする。

__補題3__ ([2] (1.3))　V: kG-加群で、PをGのp-部分群とする。今Vが H-projective であると、$P \not\leq_G H$ ならば、$V(P)=0$ となる。

(証明)　[2] を参照して下さい。　//

__補題4__　Vを直既約 kG-加群で $\mathrm{vtx}_G V=P$ とする。今 Gのp-部分群 Q に対し V_Q の直既約直和因子 W で $\mathrm{vtx}_Q W=Q$ をみたすものがあれば、$Q\leq_G P$ となる。

(証明)　Mackey 分解より容易.　//

(定理Aの証明)　まず $vtx_{G\times G}A \leq_{G\times G} D\times D$ を示す。

そのためには、$k[G\times G]$-加群 A が $D\times D$-projective となることを示せばよい。補題1の(3)より、

$$\Phi_G(A_D{}^G) = Tr_{G\times D}{}^{G\times G}(\Phi_D(A^D)) \subset (E_A)_{G\times D}{}^{G\times G}$$

が成立する。(A,P) の defect 群が D より $1 \in A_D{}^G$ で $\Phi_G(1) = id_A$ となるから、$id_A \in (E_A)_{G\times D}{}^{G\times G}$ となる。

Higman の判定条件より、A は $G\times D$-projective となる。全く同様に A は $D\times G$-projective となる。故に Mackey 分解より G のある元 g に対し、A は $D\times D^g$-projective となり、これより明らかに A は $D\times D$-projective になる。

次に $D^\Delta \leq_{G\times G} vtx_{G\times G}A$ を示す。$k[G\times G]$-加群 A を G^Δ に制限して、$k[G^\Delta]$-加群とみてみる。Broué - Puig の defect 群の特徴付けより、$A(D) \neq 0$ である。故に、補題2より、$A\downarrow_{G^\Delta}$ の直既約直和因子 V で、$D^\Delta \leq_{G^\Delta} vtx_{G^\Delta}V$ となるものが存在する。以下 $vtx_{G^\Delta}V = Q^\Delta$ とおく。vertex の定義より、$V\downarrow_{Q^\Delta}$ の直既約直和因子 W で、$vtx_{Q^\Delta}W = Q^\Delta$ となるものが存在し、従って、結局、$A\downarrow_{Q^\Delta}$ の直既約直和因子 W で、$vtx_{Q^\Delta}W = Q^\Delta$ となるものが存在する。Q^Δ は p-部分群より、補題3より $Q^\Delta \leq_{G\times G} vtx_{G\times G}A$ となり、故に $D^\Delta \leq_{G\times G} vtx_{G\times G}A$ が成立する。　#

系5 (Green) $B=kGe$ を G の block とし, D をその defect 群とする。この時, $vtx_{G\times G}B=D^{\Delta}$ が成立する。

(証明) 定理 A より, $k[G\times G]$-加群 B が D^{Δ}-projective を いえば十分である。$k_{G^{\Delta}}$ を自明な $k[G^{\Delta}]$-加群とした時, 明らかに, B は $(k_{G^{\Delta}})^{\uparrow G\times G}$ の直既約直和因子である。一方定理 A より, B は, $D\times D$-projective であるから, Mackey 分解より, ある G の元 g があって, B は, $(G^{\Delta})^{(1,g)}\cap D\times D$ -projective になる。故に, B は $G^{\Delta}\cap(D\times D)^{(1,g^{-1})}$-projective となり, $G^{\Delta}\cap(D\times D)^{(1,g^{-1})}\leq D^{\Delta}$ より, B は D^{Δ}-projective になる。 ||

3°. Characterization of block with vertex.

定理 A における一つの等号, $vtx_{G\times G}A=D^{\Delta}$ がいつ成立するかという問いに対し, シンポジウムでは, 特殊な場合のみ示したが, 次の一般的な結果を, 最近得た。

定理 B (A,φ) を block B に属する, epimorphic & local interior G-algebra とし, その defect 群を D とする。今, $vtx_{G\times G}A=D^{\Delta}$ と仮定すると, homomorphism φ を $B=kGe$ に

制限した写像 $\rho|_B : B \longrightarrow A$ に対し $\rho|_B$ は k-algebra としての同型になる。特に (A, ρ) の defect 群 D は、block B の defect 群と同型になる。

(証明) (A, ρ) は block B に属する epimorphic & local interior G-algebra より、$\rho(B) = A$ となる。故に、$\dim_k A = \dim_k B$ を示せば十分である。

今、kG の原始中等元 f で $\rho(f) \neq 0$ となるものをとってくる。まず、右 A-加群 $\rho(f)A$ を自然に右 kG-加群とみたものに対して、$\rho(f)A \simeq fk[G]$ となることを示す。そのため、$vtx_{G\times G} A = D^\Delta$ より A は G^Δ-projective 従って、A を $1\times G$ に制限した加群 $A\downarrow_{1\times G}$ は projective になることに注意する。これより、A を正則右 A-加群とみたものを自然に右 $k[G]$-加群とみたものは projective $k[G]$-加群となる。$\rho(f)A$ は A-加群として、A の直既約直和因子より、$k[G]$-加群とみても直既約直和因子となる。故に $\rho(f)A$ は projective $k[G]$-加群である。ところが、ρ の制限 $\rho|_{fk[G]} : fk[G] \twoheadrightarrow \rho(f)A$ は right $k[G]$-module homomorphism となる。よって $\rho(f)A$ が projective より、$k[G]$-加群として、$\rho(f)A$ は、$fk[G]$ の直和因子となる。f が原始中等元より、$k[G]$-加群として $\rho(f)A \simeq fk[G]$ となる。

次に $V_1, V_2, \cdots, V_s$ を既約 A-加群全体とする。各 V_i から自然に作られる既約 $k[G]$-加群を $W_1, W_2, \cdots, W_s$ とする。このように順序をつけて、B に属する既約 $k[G]$-加群全体を $W_1, W_2, \cdots, W_s, W_{s+1}, \cdots, W_t$ とする。更に、各 W_i に対応する P.I.M を $f_i k[G]$ とする。今 $\rho(f_i) = f_i'$ とおくと、前の議論より

$$1 \leq i \leq s \text{ に対し、} \quad f_i' A \simeq f_i k[G]$$
$$i > s \text{ に対し} \quad f_i' = 0$$

となる。今、上の index の順序にしたがって、A の Cartan 行列を $C_A = (c_{ij}')$、B の Cartan 行列を $C_B = (c_{ij})$ とする。すると

$$f_i' A \longleftrightarrow \bigoplus_{j=1}^{s} c_{ij}' V_j$$
$$f_i k[G] \longleftrightarrow \bigoplus_{j=1}^{t} c_{ij} W_j$$

となる。$1 \leq i \leq s$ に対し $f_i' A \simeq f_i k[G]$ より、$1 \leq i, j \leq s$ に対して、$c_{ij}' = c_{ij}$ で、$1 \leq i \leq s$, $j > s$ に対し、$c_{ij} = 0$ となる。即ち、

$$C_B = \begin{pmatrix} C_A & * \\ 0 & * \end{pmatrix}$$

が成立する。

ところが、C_B は対称行列より、

$$C_B = \begin{pmatrix} C_A & 0 \\ 0 & * \end{pmatrix}$$

となる。ところが [4] Th 16.7 より、C_B は indecomposable であるから、$t = s$ で、$C_A = C_B$ となる。今 $1 \leq i \leq s$ に対して、$\dim_k V_i = \dim_k W_i$, $\dim_k f_i' A = \dim_k f_i k[G]$ が成立している。

ところが、右 A-加群として、

$$A_A \cong \bigoplus_{i=1}^{s} (\dim_k V_i)\, f_i' A$$

となり、また、

$$B_{k[G]} \cong \bigoplus_{i=1}^{s} (\dim_k W_i)\, f_i\, k[G]$$

となることから、 $A_A \simeq B_{k[G]}$ となり、特に

$$\dim_k A = \dim_k B$$

が成立する。故に $\rho|_B : B \xrightarrow{\sim} A$ となる。 $\|$

$k[G\times G]$-加群 $k[G]$ は、明らかに置換加群より $k[G]^*_{G\times G}$ と $k[G]_{G\times G}$ は同型になる。よって定理 B から、次の系をえる。

<u>系6</u> $k[G]$の直既約な両側イデアル I に対し、$\mathrm{vtx}_{G\times G} I$ が G° に含まれていれば、I は G の block イデアルとなる。

(Reference)

[1] J. L. Alperin - B. W. Burry , Block theory with modules , J. Alg. 65 , 225 - 233 , (1980)

[2] M. Broué , On Scott module and p-permutation module , preprint

[3] M. Broué - L. Puig , Charcters and local structure in G-algebras, J. Alg. 63 , 306 - 317 (1980)

[4] W. Feit , The Representation Theory of Finite Groups, North-Holland (1982)

[5] J. A. Green, Some remarks on defect groups, Math. Z 107, 133 - 150 (1968)

On p-blocks with abelian defect groups

熊本大学　理学部
渡辺アツミ

abelian defect group をもついくつかの p-block の構造とくに通常既約指標の様子について述べる。M. Broué と L. Puig [4] で構成された一般指標(もしくは interior G-algebra として群環をとったときの結果を用いた。1節で(interior G-algebra としての)群環から構成される一般指標について述べる。

1. Broué - Puig の一般指標

p を素数, K を p 進体の代数閉包, $\mathcal{O}$ を K の付値環, $\mathfrak{p}$ を $\mathcal{O}$ の極大イデアルとする。さらに G を有限群, B を G の block とする。B の defect group を D, $C_G(D)$ における B の root の一つを b とする。

定義1. Q を G の p-部分群, b_Q を $b_Q{}^G = B$ である $C_G(Q)$ の block とするとき, (Q, b_Q) を (B, G)-Brauer pair という。$Q = \langle\pi\rangle$ (巡回群) のとき

には (B,G) − Brauer element といい，$(\pi,*)$ と書く（(B,G) − Brauer element は R. Brauer [1] における subsection である）.

定義 2. (B,G) − Brauer pair (Q,b_Q), (R,b_R) に対して (i) Q は R の正規部分群である (ii) $b_Q^{RC_G(Q)} = b_R^{RC_G(Q)}$ が満たされるとき (Q,b_Q) は (R,b_R) において normal といい，$(Q,b_Q) \triangleleft (R,b_R)$ と書く.

定義 3. (B,G) − Brauer pair の series (Q_0,b_0), (Q_1,b_1), ……, (Q_n,b_n) が存在して

$(Q,b_Q) = (Q_0,b_0) \triangleleft (Q_1,b_1) \triangleleft \cdots\cdots (Q_{n-1},b_{n-1}) \triangleleft (Q_n,b_n)$

$= (R,b_R)$

となるとき (Q,b_Q) は (R,b_R) に含まれるといい，$(Q,b_Q) \subset (R,b_R)$ と書く. Brauer element $(\pi,*)$ に対して $(\pi,*) \subset (R,b_R)$ のときには $(\pi,*) \in (R,b_R)$ と書く.

maximal (B,G) − Brauer pair は $(D,b)^x$, $x \in G$ で与えられる.

χ を B の通常既約指標，π を G の p − 元とする. $C_G(\pi)$ の任意の p − 正則元 ρ に対して

$$\chi(\pi\rho) = \sum_{\varphi} d(\chi,\pi,\varphi)\varphi(\rho)$$

と書ける，但し φ は $C_G(\pi)$ の modular 既約指標で $d(\chi,\pi,\varphi)$ は χ の φ に関する一般分解定数である．

(π, b) を (B,G) − Brauer element とする．$\chi^{(\pi,b)}$ を次の式で定義される G の類関数とする（[1]）．

$$
\begin{cases}
\chi^{(\pi,b)}(\pi\rho) = \sum_{\varphi\in b} d(\chi,\pi,\varphi)\varphi(\rho) & (\rho\in (C_G(\pi))_{p'}), \\
\chi^{(\pi,b)}(x) = 0 & \text{if } x_p \text{ is not conjugate to } \pi
\end{cases}
$$

但し x_p は x の p 部分である．このとき，R を (B,G) − Brauer element の共役類の完全代表系とすると

$$
\chi = \sum_{(\pi,b)\in R} \chi^{(\pi,b)}.
$$

定義4．R の各元は $(D,\mathcal{b})$ に含まれているとする．

(i) D の一般指標 η に対して

$(\pi,b)\in S$, $(\pi,b)^g\in(D,\mathcal{b})$ $(g\in G)$ ならば $\eta(\pi)=\eta(\pi^g)$

が満たされているとき η は $(G,\mathcal{b})$ − stable であるという．

(ii) B の通常既約指標 χ と $(G,\mathcal{b})$ − stable な D の一般指標 η に対して

$$
\chi*\eta = \sum_{(\pi,b)\in R} \eta(\pi)\chi^{(\pi,b)}
$$

とおく．

定理（Broué − Puig）$\chi*\eta$ は B に associate される G の一般指標である．

これを用いて M. Broué - L. Puig [3] において nilpotent block の構造が明らかにされた。

2. 準備

以下 B の defect group D は abelian と仮定する。このとき $(\pi, *) \in (D, b)$ ならば $\pi \in D$ かつ $* = b^{C_G(\pi)}$。さらに R. Brauer [2] より $\pi_1, \pi_2 \in D$ に対して $(\pi_1, b^{C_G(\pi_1)})$ と $(\pi_2, b^{C_G(\pi_2)})$ が $(G-)$ 共役であることと π_1, π_2 が $T(b)$-共役であることは同値である。但し $T(b)$ は b の $N_G(D)$ における inertia group である。従って S を D の $T(b)$-共役類の完全代表系とすると $\{(\pi, b^{C_G(\pi)}) \mid \pi \in S\}$ は (B, G)- Brauer element の共役類の完全代表系をなす。また η を $T(b)$-不変な D の一般指標とするとき η は (G, b)-stable になる。よってこのとき

$$\chi * \eta = \sum_{\pi \in S} \eta(\pi)\, \chi^{(\pi, b)}.$$

D の一次指標 μ に対して μ と $T(b)$-共役な指標の和を η_μ と書く。η_μ は $T(b)$-不変である。Λ を D の一次指標の $T(b)$-共役類の完全代表系とする。

補題 1. χ を B の height 0 の通常既約指標

とする．Bの任意の通常既約指標χ'に対してΛの元μが存在して　$(\chi', \chi * \eta_\mu) \neq 0$．

λを$T(b)$－不変なDの一次指標とするとき，Bの任意の通常既約指標χに対して　$\chi*\lambda$の内積$(\chi*\lambda, \chi*\lambda)$は$1$に等しい．従って$\chi*\lambda$は$B$の通常既約指標である．

eをBのinertia indexとする．$e = |T(b) : C_G(D)|$である．$e=1$のときBのmodular既約指標の個数$\ell(B)$は1に，通常既約指標の個数$k(B)$はDの位数$|D|$に等しいことが知られている．よってこのときはχをBの通常既約指標の一つとすれば，Bの通常既約指標は$\chi*\lambda$，λはDの一次指標，で尽くされる．

πを$C_G(\pi) \cap T(b) = C_G(D)$を満たす$D$の元とする．このとき$b^{C_G(\pi)}$のinertia indexは$1$に等しい．$b^{C_G(\pi)}$の一意的に存在するmodular既約指標を$\varphi^{(\pi)}$で表わすことにする．

補題２．π_1, π_2を$C_G(\pi_i) \cap T(b) = C_G(D)$を満たす$D$の元とする．このとき次のことが成立する．

$$\exists \gamma = \pm 1 \ \text{s.t.} \ d(\chi, \pi_1, \varphi^{(\pi_1)}) \equiv \gamma d(\chi, \pi_2, \varphi^{(\pi_2)})$$

(mod $\mathfrak{p}$) for all $\chi \in B$.

3 $e = 2$ or 3 のとき

定理 1. $e = 2$ or 3 とする. $D_1 = D \cap C_G(T(b))$, $D_2 = [T(b), D]$ とおくと $D = D_1 \times D_2$. Λ_1 を D_1 の一次指標の全体, Λ_2 を D_2 の自明でない一次指標の $T(b)$-共役類の完全代表系とする. $|D_2| \geqq p^2$ ならば次のことが成立する.

(i) $\ell(B) = e$, $k(B) = |D_1|\left(e + \frac{|D_2|-1}{e}\right)$. さらに B の通常既約指標は $\chi_1, \cdots, \chi_e$; χ_μ, $\mu \in \Lambda_2$; $\chi_1 * \lambda, \cdots, \chi_e * \lambda$, $\lambda \in \Lambda_1$; $\chi_\mu * \lambda$, $\lambda \in \Lambda_1$, $\mu \in \Lambda_2$ で与えられる.

(ii) $\exists\, \varepsilon_1, \cdots, \varepsilon_e = \pm 1$ s.t.

$$\chi_\mu^{(1,B)} = \sum_{i=1}^{e} \varepsilon_i \chi_i^{(1,B)} \quad \text{for all } \mu \in \Lambda_2.$$

(iii) π を $C_G(\pi) \cap T(b) = C_G(D)$ を満たす D の元とする.

$$\exists\, \gamma_\pi = \pm 1 \quad \text{s.t}$$

$$d(\chi_i, \pi, \varphi^{(\pi)}) = \gamma_\pi \varepsilon_i$$

$$d(\chi_\mu, \pi, \varphi^{(\pi)}) = \gamma_\pi \eta_\mu(\pi)$$

for all $i = 1, \cdots, e$ and $\mu \in \Lambda_2$.

証明の概略. $|G|$ に関する帰納法による.

補題2と条件 $|D_2| \leq p^2$ より

$$d(\chi_1, \pi, \varphi^{(\pi)}) = \pm 1 \quad \text{for all } \pi \in S - D_1$$

を満たす $\chi_1 \in B$ が存在する。χ_1 は height 0 の指標である。

χ_1 に対して以下の内積に関する関係式が成立する。

$\mu \in \Lambda_2$ に対して

$$(\chi_1 * \eta_\mu, \chi_1) = e - 1$$

$$(\chi_1 * \eta_\mu, \chi_1 * \eta_\mu) = e^2 - e + 1.$$

$\mu, \mu' \in \Lambda_2$ に対して $\mu \neq \mu'$ ならば

$$(\chi_1 * \eta_\mu, \chi_1 * \eta_{\mu'}) = e^2 - e.$$

これらの関係式より $e = 2$ のときには

(1) $$\chi_1 * \eta_\mu = \chi_1 + \delta_2 \chi_2 + \delta \chi_\mu$$

for all $\mu \in \Lambda_2$, 但し $\delta_2, \delta = \pm 1$, $\chi_2, \chi_\mu \in B$,

$e = 3$ のときには

(2) $$\chi_1 * \eta_\mu = 2\chi_1 + \delta_2 \chi_2 + \delta_3 \chi_3 + \delta \chi_\mu$$

for all $\mu \in \Lambda_2$, 但し $\delta_2, \delta_3, \delta = \pm 1$, $\chi_\mu \in B$,

を導くことができる。$\lambda \in \Lambda_1$ に対して

$$\chi_1 * \eta_{\lambda\mu} = (\chi_1 * \eta_\mu) * \lambda$$

が成立することに注意すれば 補題1より B の通常既約指標は $\chi_1, \cdots, \chi_e$; χ_μ, $\mu \in \Lambda_2$; $\chi_1 * \lambda, \cdots, \chi_e * \lambda$, $\lambda \in \Lambda_1$; $\chi_\mu * \lambda$, $\lambda \in \Lambda_1$, $\mu \in \Lambda_2$ でつくされる。帰納法

の仮定と公式 $k(B)=\sum_{\pi\in S} l(\mathfrak{b}^{G(\pi)})$ より得られた指標が相異なることと $l(B)=e$ がわかる．(ii) 及び (iii) は (1) 又は (2) と一般分解定数についての性質から導かれる．

注意　定理1は B が principal block，D が巡回群，D が G において normal，又は G が p-可解群のときは，条件 $(|D_2|\leqq p^2)$ なしに成立する．

4.　inertia index が 4 又は 5 の principal block

この節では B は principal block とする．D は G のシロー p-部分群で，$T(\mathfrak{b})=N_G(D)$．

定理2．$N_G(D)/C_G(D)$ は位数4の巡回群とする；$N_G(D)/C_G(D)=\langle t\rangle$．$D_1=C_D(t)$，$D_2=[\langle t\rangle, C_D(t^2)]$，$D_3=[\langle t^2\rangle, D]$ とおく．$D=D_1\times D_2\times D_3$ である．このとき $k(B)=|D_1|\left(4+2\times\frac{|D_2|-1}{2}+\frac{|D_3|-1}{4}+2\times\frac{|D_2|-1}{2}\times\frac{|D_3|-1}{4}\right)$ かつ $l(B)=4$．

なお B の通常既約指標は次の通りである．Λ_1 を D_1 の一次指標の全体，Λ_i を D_i の自明でない

一次指標の $N_G(D)$ 一共役類（$\langle t\rangle$ -orbit に一致する）の代表系とする，$i=2,3$．このとき $\{\lambda, \lambda\mu_2, \lambda\mu_3, \lambda\mu_2\mu_3, \lambda\mu_2^{-1}\mu_3 \mid \lambda\in\Lambda_1, \mu_2\in\Lambda_2, \mu_3\in\Lambda_3\}$ は D の一次指標の $N_G(D)$ 一共役類の代表系をなす．μ_2, μ_3 を Λ_2, Λ_3 の任意の元とする．

$$1_G * \eta_{\mu_2} = 1_G + \varepsilon_2\chi_2 - \varepsilon_2\chi_{\mu_2},$$

$$1_G * \eta_{\mu_3} = 3\cdot 1_G + \varepsilon_2\chi_2 + \varepsilon_3\chi_3 + \varepsilon_4\chi_4 + \varepsilon\chi_{\mu_3},$$

$$1_G * \eta_{\mu_2\mu_3} = 2\cdot 1_G + 2\varepsilon_2\chi_2 - \varepsilon_2\chi_{\mu_2} + \varepsilon_{\mu_2}\chi'_{\mu_2} + \delta_{\mu_2}\chi_{\mu_2\mu_3},$$

$$1_G * \eta_{\mu_2^{-1}\mu_3} = 2\cdot 1_G + 2\varepsilon_2\chi_2 - \varepsilon_2\chi_{\mu_2} + \varepsilon_{\mu_2}\chi'_{\mu_2} + \delta_{\mu_2}\chi_{\mu_2^{-1}\mu_3}$$

但し $\varepsilon, \varepsilon_i, \varepsilon_{\mu_2}, \delta_{\mu_2} = \pm 1$，$\chi_2, \chi_3, \chi_4, \chi_{\mu_2}, \chi_{\mu_3}, \chi'_{\mu_2}, \chi_{\mu_2\mu_3}, \chi_{\mu_2^{-1}\mu_3} \in B$．

定理3　$N_G(D)/C_G(D)$ は位数4の基本可換群とする；$N_G(D)/C_G(D)=\{1, t_1, t_2, t_3\}$ とおく．$D=D_0\times D_1\times D_2\times D_3$，$D_0=C_D(N_G(D))$，$D_0\times D_i=C_D(t_i)$ $(i=1,2,3,)$ である．$k(B)=|D_0|\left(4+2\sum_{i=1}^{3}\frac{|D_i|-1}{2}+\frac{|D_1|-1}{2}\times\frac{|D_2|-1}{2}+\frac{|D_1|-1}{2}\times\frac{|D_3|-1}{2}+\frac{|D_2|-1}{2}\times\frac{|D_3|-1}{2}+2\times\frac{|D_1|-1}{2}\times\frac{|D_2|-1}{2}\times\frac{|D_3|-1}{2}\right)$ かつ $\ell(B)=4$．

上の場合通常既約指標は次のようになっている．Λ_0 を D_0 の一次指標の全体，Λ_i を D_i の

自明でない一次指標の $N_G(D)$－共役類の代表系とする，$i=1,2,3$．このとき $\{\lambda,\ \lambda\mu_1,\ \lambda\mu_2,\ \lambda\mu_3,\ \lambda\mu_1\mu_2,\ \lambda\mu_1\mu_3,\ \lambda\mu_2\mu_3,\ \lambda\mu_1\mu_2\mu_3,\ \lambda\mu_1^{-1}\mu_2\mu_3 \mid \lambda\in\Lambda_0,\ \mu_i\in\Lambda_i\ (i=1,2,3)\}$ は D の一次指標の $N_G(D)$－共役類の代表系をなす．μ_i を Λ_i の任意の元とする，$i=1,2,3$．

$$1_G*\eta_{\mu_i} = 1_G+\varepsilon_i\chi_i-\varepsilon_i\chi_{\mu_i} \qquad (i=1,2,3),$$

$$\begin{aligned}1_G*\eta_{\mu_1\mu_2} = {} & 1_G+\varepsilon_1\chi_1-\varepsilon_1\chi_{\mu_1}+\varepsilon_2\chi_2-\varepsilon_2\chi_{\mu_2}-\varepsilon_3\chi_3\\ & +\delta_1\chi'_{\mu_1}+\delta_2\chi'_{\mu_2}+\delta_{12}\chi_{\mu_1\mu_2},\end{aligned}$$

$$\begin{aligned}1_G*\eta_{\mu_1\mu_3} = {} & 1_G+\varepsilon_1\chi_1-\varepsilon_2\chi_2+\varepsilon_3\chi_3-\varepsilon_3\chi_{\mu_3}-\varepsilon_1\chi_{\mu_1}\\ & +\delta_1\chi'_{\mu_1}+\delta_3\chi'_{\mu_3}+\delta_{13}\chi_{\mu_1\mu_3},\end{aligned}$$

$$\begin{aligned}1_G*\eta_{\mu_2\mu_3} = {} & 1_G-\varepsilon_1\chi_1+\varepsilon_2\chi_2-\varepsilon_2\chi_{\mu_2}+\varepsilon_3\chi_3-\varepsilon_3\chi_{\mu_3}\\ & +\delta_2\chi'_{\mu_2}+\delta_3\chi'_{\mu_3}+\delta_{23}\chi_{\mu_2\mu_3},\end{aligned}$$

$$1_G*\eta_{\mu_1\mu_2\mu_3} = -\sum_{i=1}^{3}\varepsilon_i\chi_{\mu_i}+\sum_{i=1}^{3}\delta_i\chi'_{\mu_i}+\delta\chi_{\mu_1\mu_2\mu_3},$$

$$1_G*\eta_{\mu_1^{-1}\mu_2\mu_3} = -\sum_{i=1}^{3}\varepsilon_i\chi_{\mu_i}+\sum_{i=1}^{3}\delta_i\chi'_{\mu_i}+\delta\chi_{\mu_1^{-1}\mu_2\mu_3},$$

但し $\varepsilon_i,\ \delta_i,\ \delta_{ij},\ \delta=\pm1$，$\chi_{\mu_i},\ \chi'_{\mu_i},\ \chi_{\mu_i\mu_j},\ \chi_{\mu_1\mu_2\mu_3},\ \chi_{\mu_1^{-1}\mu_2\mu_3}\in B$．．

定理4．$|N_G(D):C_G(D)|=5$ とする．$D_1=C_D(N_G(D))$，$D_2=[N_G(D),D]$ とおく．$k(B)=|D_1|\left(5+\frac{|D_2|-1}{5}\right)$ かつ

$\ell(B) = 5$.

上の場合，D_2 の自明でない一次指標の $N_G(D)$-共役類の代表系 Λ_2 の任意の元 μ に対して

$$1_G * \eta_\mu = 4\cdot 1_G + \sum_{i=2}^{5} \varepsilon_i \chi_i + \varepsilon \chi_\mu$$

が成立する，但し $\varepsilon_i, \varepsilon = \pm 1$, $\chi_i, \chi_\mu \in B$.

文献

[1] R. Brauer: On blocks and sections in finite groups II, Amer. J. Math. 90 (1968), 895-925.

[2] ――――: On the structures of blocks of characters of finite groups, Lecture Notes in Math. 372, Springer, Berlin, 103-130.

[3] M. Broué - L. Puig: A Frobenius theorem for blocks, Inventiones Math. 56 (1980), 117-128

[4] ――――: Characters and local structures in G-algebras, J. Algebra, 63 (1980), 306-317.

A short proof of 2-local solvable

愛知教育大　林　誠

極度に長く，超難解な有限単純群の分類定理の簡明化の第一歩として，"すべての 2-局所部分群が可解な有限単純群の分類定理"の平易化（従って，N-群の分類定理を含む）の説明が本稿の目的です。

復習も兼ねて，定義から始めることにします。

G を有限群とするとき，

$O_2(G) :=$ G の最大の正規 2-部分群；

$O(G) :=$ G の最大の正規 $2'$-部分群；

$H \subseteq G \ (H \subset G) \Leftrightarrow H$ は G の（真）部分群；

G の部分群 X に対して，$\langle X \rangle :=$ X で生成される部分群；

$O^2(G) := \langle x \in G \ ; \ x$ は $2'$-元 $\rangle$；

G が p-群のとき，$\Omega_1(G) = \langle x \in G \ ; \ x^p = 1 \rangle$；

$N \subseteq G$ が G の 2-局所部分群 $\Leftrightarrow$ G のある 2-部分群 $T (\neq 1)$ に対して，$N = N_G(T)$；

$Syl_p(G) = \{ G$ の p-Sylow 群全体 $\}$；

最後に，$S \subseteq G$ に対して，Gが'S-既約'$\Leftrightarrow$
GのSを含む極大部分群は唯一つ。

仮定A. G^*を群，SをG^*の有限2-部分群，G_1, G_2をG^*の有限可解部分群で次の条件をみたすとする。

(A.1) $S \in Syl_2(G_1) \cap Syl_2(G_2)$;

(A.2) G_1, G_2 は S-既約;

(A.3) $S = O_2(G_1)(O^2(G_2) \cap S) = O_2(G_2)(O^2(G_1) \cap S)$;

(A.4) $G_i \neq O(G_i) N_{G_i}(S)$, $i = 1, 2$;

(A.5) Sは単位元以外に$\langle G_1, G_2 \rangle$の正規部分群を含まない。

仮定Aの下での従来(近年)の主な結果：

[1] Goldschmidt [4]：$|G_i : S| = 3$, $i = 1, 2$ ならば15個の相異なる(G_1, G_2)の同型類類があり，それ等は完全に決定される。特に，$|S| \leq 2^7$.

[2] 五味[6]，Fan [2]：$|G_i : S| = p_i$ (素数), $i = 1, 2$ ならば，[1] の他に，${}^2F_4(2)$ と ${}^2F_4(2)'$ 型 (後述) が加わる。

[3] 五味-田中 [7]：G_iの$2'$-Hall部分群が巡回群で$O(G_i) = 1$, $i = 1, 2$ ならば上記に限る。${}^2F_4(2)$, ${}^2F_4(2)$-型は一意。

定理 A.[10] 仮定 A の下で次の何れかが起こる。

(1) G_i の $2'$-Hall は巡回 3-群, $i=1,2$;

(2) (G_1, G_2 を適当に入れかえて)

(2.1) $G_1/O_{2',2}(G_1) \simeq \Sigma^3$, $G_2/O_{2',2}(G_2) \simeq \mathbb{Z}_5 \rtimes \mathbb{Z}_4$;

(2.2) $2^{11} \leq |S| \leq 2^{12}$, $|(O^2(G_1) \cap S)(O^2(G_2) \cap S)| = 2^{11}$;

(2.3) $|\Omega_1 Z(S)| = 2$, $\Omega_1 Z(S) \leq Z(G_2)$;

(2.4) G_1 は $O_2(G_1)$ 内に 4 個の non-central chief factors をもつ;

(2.5) G_2 は $O_2(G_2)$ 内に 2 個の non-central chief factors をもつ。$O_2(G_2)$ の巾零 class は 3。

定理 A (2.2) で, $|S| = 2^{11}$ のとき, (G_1, G_2) は ${}^2F_4(2)'$-型, $|S| = 2^{12}$ のとき (G_1, G_2) は ${}^2F_4(2)$-型 という。

従って, $\boxed{2}$, $\boxed{3}$ と定理 A より,

系 A. 仮定 A の下で (G_1, G_2) の同型類 (15+2 個) はすべて決定される。

ここで注目したいのは, $\boxed{1}$, $\boxed{2}$ 及び筆者の手法がる様かなり異なっていることである。現在のところ, それぞれに長短がある。

問題1. $\boxed{1}$, $\boxed{2}$, 定理A を統一的に扱えて, 更に非可解を扱うにも有効な手段を見出せ。

例1. $G^* = GL_3(2)$, $S = \left\{ \begin{bmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{bmatrix} \in G^* \right\}$,

$G_1 = \left\{ \begin{bmatrix} * & * & * \\ * & * & * \\ & & 1 \end{bmatrix} \in G^* \right\}$, $G_2 = \left\{ \begin{bmatrix} 1 & * & * \\ & * & * \\ & * & * \end{bmatrix} \in G^* \right\}$

とおくと, 仮定Aを満たす。

例1. $G^* = GL_3(2) \wr \Sigma^2$ (wreath product) とおくと, 上の例から, 容易に G^* が $(A.3)$ を除く仮定Aを満たす (G_1, G_2) をもつことが分かる。$(A.3)$ はこの様な trivial な例を除く条件である。しかし, 次の問題が解かれることが望ましい。

問題2. 仮定$(A.3)$を $(A.3')$ $S = O_2(G_1)O_2(G_2)$ に弱めよ。

暫く, G^* をすべての 2-局所部分群が可解な有限単純群で $S^* \in Syl_2(G^*)$ とする。

定理 B. (Gorenstein-Lyon [8])。G^* は次の何れかに同型である。

(I) $L_2(q)$, q: odd (>5), A_7, M_{11}, $U_3(3)$;

(II) ${}^2F_4(2)'$;

(III) $L_2(2^n)$, $U_3(2^n)$, $Sz(2^{2n-1})$, $(n \geq 2)$.

こゝで，G^* が (I) に含まれるとき，G^* は標数2型でないか，或は，$\boxed{1}$ の 15 cases に含まれる部分群の組 (G_1, G_2) をもつ。G^* が (II) のときは勿論 G^* は ${}^2F_4(2)'$-型の (G_1, G_2) の組をもつ。G^* が (III) に含まれるときは，$\mathrm{Syl}_2(G^*) \ni {}^\forall S^*, T^* (\neq)$ に対して $S^* \cap T^* = 1$ である。

$\boxed{\cdot}$ 逆に，(G_1, G_2) が $\boxed{1}$ の 15 cases か ${}^2F_4(2)'$, ${}^2F_4(2)$ 型に含まれて，$\mathrm{Syl}_2(G_1) \subseteq \mathrm{Syl}_2(G^*)$ であれば，比較的容易に（文献を引用する式での意）G^* が (I) か (II) の群であることが分かる。また，G^* が strongly embedded 部分群をもつ (i.e. $S^* \subseteq H^*$ で ${}^\forall g \in G^* - H^*$ に対して，$|H^* \cap H^{*g}|$ が odd なる $H^* (\subset G^*)$ が存在する) ならば G^* が (III) の群になることが分かる (c.f. [1]。実は，H^* が可解のときは [1] も不要)。

$S \subseteq S^*$ に対して，$\mathfrak{F}(S) = \{H \subseteq G^* ;\ S \in Syl_2(H)$, H は S-既約で $H \neq N_H(S)O(H)\}$, $\mathfrak{F}^*(S) = \{H \in \mathfrak{F}(S) ;\ H \subseteq H^*$ for some $H^* \in \mathfrak{F}(S^*)\}$ とおく。

補題 1（五味，一）．$S \subseteq S^*$, $S \neq 1$ に対して，

(1) $O_2(\langle H, N_{G^*}(S)\rangle) \neq 1$.

(2) $S \triangleleft S^*$ ならば $\langle \mathfrak{F}(S)\rangle = \langle \mathfrak{F}^*(S)\rangle$。

$\boxed{\cdot}$：補題 1(1) より，G^* が標数 2-型として，$O_2(\langle \mathfrak{F}(S^*)\rangle) \neq 1$ ならば G^* が strongly embedded 部分群をもつことが分かる。

一方，[9, §5] の論法を用いて，次が得られる．

補題 2．$\forall H, K \in \mathfrak{F}(S^*)$ に対して，$O_2(\langle H, K\rangle) \neq 1$ ならば $O_2(\langle \mathfrak{F}^*(S^*)\rangle) \neq 1$.

$\boxed{\cdot}$, $\boxed{\cdot}$ と補題 2 より，G^* を標数 2-型として，（定理 B を示すには）次の定理 B′ を示せばよい。

定理 B′．$H, K \in \mathfrak{F}(S^*)$ に対して，$O_2(\langle H, K\rangle) = 1$ ならば (H, K) は仮定 A（即ち，$(A.3)$）を満たす。

定理 B′ の対偶をとれば，ここで定理 B が本質的に定理 A（型）の問題に置きかわっていることに注意して頂きたい。この例は，五味-田中氏が $\boxed{2}$, $\boxed{3}$ を用いて [11] の証明の簡略化に成功したことにもみられる [5]。

これ以後は定理Aの証明の論法を必要とするので，ひとまずその概略に移り，然る後 再び定理Bの証明に戻ります。次の定義は Glauberman [3] を真似たもので定理Aの証明に重要な役割を課します。

定義： Sを有限2-群，tを非負整数とする。$X, Y \subseteq S$ に対して，$V \in \omega_t(X,Y) \Longleftrightarrow$ VはY-不変なXの部分群で $[V,L,L]=1$ を満たすYの任意の基本可換群Lに対し，Vの生成元 $\{v_i ; i \in I\}$（Lにdepend）を $|[v_i, L]| \leq 2^t$ $(\forall i \in I)$ と選べる。

$N_{-1}=S$ とおき，以下帰納的に $N_i=\langle \omega_t(S, N_{i-1}) \rangle$，$i=0,1,2,\cdots$，$N^\infty(\omega_t ; S)=\bigcap_{i\ \mathrm{odd}} N_i$ と定義する。

$N^\infty(\omega_t ; S)$ は次の性質をもつ.

$(N^\infty.1)$ $S \neq 1$ ならば $N^\infty(\omega_t ; S) \neq 1$

$(N^\infty.2)$ $N^\infty(\omega_t ; S) \subseteq T \subseteq S$ ならば $N^\infty(\omega_t ; T)=N^\infty(\omega_t ; S)$.

従って，仮定Aの下で $G \in \{G_1, G_2\}$ に対して，

$(N^\infty.3)$ $N^\infty(\omega_t ; S) \subseteq O_2(G)$ ならば $N^\infty(\omega_t ; S) \triangleleft G$

$(N^\infty.4)$ $M \in \omega_t(S,S)$ で $|[M,x]| \geq 2^{t+1}$ for $\forall x \in S-O_2(G)$ ならば $N^\infty(\omega_t ; S) \triangleleft G$。

補題3. Gを有限可解群，$S\in Syl_2(G)$，MをGの極小正規2-部分群とするとき，$M\in\omega_1(S,S)$。従って(№4)より，もし，$|[M,x]|\geq 2^2$ for $\forall x\in S-O_2(G)$ ならば $N^\infty(\omega_1;S)\lhd G$。

補題4. 補題3の条件の下で，$M=\prod_{i=1}^{r} M_i$ (M_iは$O(G/C_G(M))$に関するMの Wedderburn component) $J=N_G(M_1)/C_G(M_1)$，$2^\delta=\min.\{|[M,x]|;x\in S-O_2(G)\}$とおく。$[M,G]\neq 1$とするとき，(1) $\delta=1$なら$|M_1|=2^2$で$J\simeq\Sigma^3$，(2) $\delta=2$なら(1)の他，$|M_1|=2^4$で$J\subsetneq \mathbb{Z}_5\rtimes\mathbb{Z}_4$ or $|M_1|=2^6$で$J\subsetneq Aut\,U_3(2)$，(3) $\delta=3$なら，(1),(2)の他$|M_1|=2^6$で$J\simeq\mathbb{Z}_7\rtimes\mathbb{Z}_2$ or $\mathbb{Z}_9\rtimes\mathbb{Z}_2$。

さて，定理Aの証明の概略に入ります。仮定(A.5)より(番号を付けかえて) $[\Omega_1 Z(S),G_1]\neq 1$としてよい。$M$を$G_1$の極小正規2-部分群で$[M,G_1]\neq 1$とする。$M_0=M$，$M_1=M^{G_2}$，$M_2=M^{G_2G_1}$，$M_3=M^{G_2G_1G_2}$，… とおく。もし，$M_3\subsetneqq O_2(G_1)$ならば，$O_2(G_1)=C_S(M)$より，$[M_2,M_2]=[M^{G_2G_1},M^{G_2G_1}]=[M^{G_2G_1G_2},M]^{G_2G_1}=1$。従って，$M_2$は基本可換群。同様に，もし$M_n\subsetneqq O_2(G_1)$ならば$M_{[\frac{n}{2}]}$は基本可換群。

従って，定理Aを示すには，次の性質(P.1)，(P.2)をもつ(小さな)整数nの存在を云えばよい。

(P.1) もし，M_nが可換ならばSの(単位元でない)部分群で$\langle G_1, G_2\rangle$で正規となるものがある。

(P.2) もし，$M_n \subsetneqq O_2(G_1)\cap O_2(G_2)$ならば$G_1$と$G_2$の構造が決まる。

実際，我々の証明において，常に$n \leqq 5$にとれる。

定義：$G\in\{G_1, G_2\}$と$x\in S$に対して，

$\prod|[O_2(G)/-, x]| := \prod_{i=0}^{r}|[B_i/B_{i+1}, x]|$，ここで

$1 = B_r \subseteq B_{r-1} \subseteq \cdots \subseteq B_1 \subseteq B_0 = O_2(G)$は$G$の chief factors. (c.f. Jordan-Hörder's Th.).

また，$n.n.c._G(O_2(G))$でGの$O_2(G)$内の non-central chief factor の個数を表すことにする。

補題5. ((P.2)の解答). 仮定Aの下で$X_1, X_2\in\{G_1, G_2\}$とする。MをX_1の正規2-群，$Z = C_M(X_1)$，$y_i\in G^*$，$1\leq i\leq n$とし，$y = y_1\cdots y_n$とおく。

(a) $[M, O_2(X_1)]\subseteqq Z$；

(b) $M^y \subsetneqq S$で$M^y O_2(X_2)/O_2(X_2)$は基本可換群。

このとき，$\prod |[O_2(X_2)/\text{-}, x]| \leq \prod_{i=1}^{n} |S:S\cap S^{y_i}| \times |S/O_2(X_1)|$
$\times |S:O_2(X_1)(S\cap O_2(X_2)^{y^{-1}})|^{-1} \times |S:O_2(X_2)(S\cap S^{y})|^{-1}$
for all $x \in M^{y}$.

補題 4.5 により，$M^{y} \nsubseteq O_2(X_2)$ なるとき，$n.n.c._{X_2}(O_2(X_2))$ の評価 と，X/Y を X_2 の $O_2(X_2)$ 内の non-central chief factor としたとき，$X_2/C_{X_2}(X/Y)$ の（大体の）構造 求められ，従って，X_2 が定まる。(A.3) の条件等により，X_1 の方も調べがつく。

次に，M_n が基本可換群のとき，比較的小さい t に対して，$M_n \in \omega_t(S,S)$ となることは，次の補題から分かる。

補題 6. G を有限（可解）群，$S \in Syl_2(G)$，M を S の正規基本可換群，$Z \subseteq C_M(S)$ とする。

(a) $|Z| \leq 2$ で $Z \neq 1$ ならば $C_M(S) = Z$;

(b) $S = C_S(M/Z)(O^2(G)\cap S)$;

(c) $[M,S,S] \nsubseteq Z$;

(d) M^G は可換。

このとき，(1) $[M^G, L, L] = 1$ なる任意の $L \subseteq S$ に対して，$|L/L\cap O_2(G)| \leq 2$。従って，$M \in \omega_t(S,S)$ ならば

$M^G \in \omega_{t+1}(S,S)$。

(2) $\prod |[M^G/-, x]| \geq |M/Z_{|Z|}(S) \cap M|$ for all $x \in S - O_2(G)$.

実際，補題6で $G = G_2$, $Z = 1$ とおくと，仮定(A.3)より，$S = O_2(G_1)(O^2(G_2) \cap S) = C_S(M)(O^2(G_2) \cap S)$。また，$M$ が G_1-既約，G_1 が S-既約で $C_S(M) = O_2(G_1)$ より (c) の仮定 $\Leftrightarrow$ $|S/O_2(G_1)| > 2$。

補題7. G_2 は次の条件を満たす基本可換正規2-群 N をもつ。$Z^* = C_N(G_2)$ とおく。

(1) $|Z^*| \leq 2$ で $Z^* \neq 1$ ならば $Z^* = C_N(S)$

(2) N/Z^* は G_2-既約。

実は，補題7が成立しない場合もあるが，そのときは，補題5等を用いて，$\boxed{1}$ の15 cases の一つが起ることが示される。補題7より，G_1 と G_2，M と N を入れかえて補題5,6が適当できる。以上の議論($+\alpha$)だけからも $|S/O_2(G_1)|$ or $|S/O_2(G_2)| = 2$ が分かる。
以下は [10] を見て頂くとして，再び定理Bの

証明に戻ります。定理 B′（の対偶）より，$H, K \in \mathfrak{F}(S^*)$ で $O_2(\langle H, K\rangle) = 1$ を満たすものがあるとしてよい。このとき，(H, K) は仮定 A を満たさないとしてよい。このとき定理 A より，$\boxed{\because}$ H, K 何れかの Hall $2'$-部分群は巡回群でない。

$S_* = (O^2(H)\cap S)(O^2(K)\cap S)$，$H_* = O^2(H)S_*$，$K_* = O^2(K)S_*$ とおく。$\boxed{\because}$ と $\boxed{1}$ の 15 cases 及び $^2F_4(2)^{(1)}$-型の pair の構造より次を得る。

補題 8. $S \subseteq S^*$，$H_0, K_0 \in \mathfrak{F}(S)$ で $H = \langle H_0, S^*\rangle$，$K = \langle K_0, S^*\rangle$ 且つ，H_0, K_0 の Hall $2'$-部分群が cyclic ならば $O_2(\langle H_0, K_0\rangle) \neq 1$.

補題 8 より，

補題 9. H 及び K の Hall $2'$-部分群は non-cyclic.

補題 10. (1) $S_*/S_*\cap O_2(H)$ 及び $S_*/S_*\cap O_2(K)$ は基本可換群.

(2)（H_* と K_* を適当に入れかえて）H_*, K_* はそれぞれ基本可換正規部分群 M, N で次の性質を有するものをもつ：

(2.1) $M = \prod_{i \in I} M_i$, $N = \langle N_i ; i \in J \rangle$;
(2.2) S は $\{M_i ; i \in I\}$, $\{N_i ; i \in J\}$ を permute する;
(2.3) $S_* \subseteq (\bigcap_{i \in I} N_S(M_i)) \cap (\bigcap_{i \in J} N_S(N_i))$。

M の存在は補題4 を用い，N の存在は本質的に補題7と同じ。これより，$\boxed{::}$: $H_* = \langle H_\alpha ; H_\alpha / O_2(H_\alpha)$ は dihedral, $\alpha \in A \rangle$, $K_* = \langle K_\beta ; K_\beta / O_2(K_\beta)$ は dihedral $\beta \in B \rangle$ となる。次の補題の証明は，(1) を示した後は，補題3 と $(N^\infty.4)$ の帰結である。

補題 10. G を G^* の可解部分群，$S \subseteq S^*$, $H_0, K_0 \in \mathfrak{F}(S)$ とする。(a) $G = \langle H_0, K_0 \rangle$ で $O(G) = 1$;
(b) $[\Omega_1 Z(S), H_0] \neq 1$;
(c) $|S^* : S| \leq 2^3$;
(d) $(O^2(K_0) \cap S) O_2(H_0) / O_2(H_0)$ は基本可換群 $(\neq 1)$。

このとき，(1) $S \in Syl_2(G)$.
(2) $N^\infty(\omega_1 ; S) \triangleleft K$。
(3) 次の何れかが起る。
(3.1) $N^\infty(\omega_1 ; S) \triangleleft \langle H_0, K_0 \rangle$; or
(3.2) $[\Omega_1 Z(S), K] \neq 1$。

これより，$\forall \alpha \in A, \beta \in B$ に対して，
$\#\{i \in I; [M_i, O^2(K_\beta)] \neq 1\} \geqq 4$, $\#\{i \in J; [N_i, O^2(H_\alpha)] \neq 1\} \geq 4$。従って，$M^* = \langle M^{K_\beta}; \beta \in B \rangle$, $N^* = \langle N^{H_\alpha}; \alpha \in A \rangle$ とおくとき，

⚄: $|[M^*, y]| \geq 2^4$, $|[N^*, x]| \geq 2^4$ for $\forall x \in S - O_2(H)$, $y \in S - O_2(K)$。

更に，M^*, N^*が可換であることを示して，$M \in \omega_1(S_*, S_*)$, $N \in \omega_2(S_*, S_*)$, $|S_*/S_* \cap O_2(H_\alpha)| = |S_*/S_* \cap O_2(K_\beta)| = 2$ より，

⚅: $M^*, N^* \in \omega_3(S_*, S_*)$。

⚄, ⚅ と $(N^\infty.4)$ より，$N^\infty(\omega_3; S_*) \lhd \langle H_\alpha, K_\beta; \alpha \in A, \beta \in B \rangle$ 即ち，$N^\infty(\omega_3; S_*) \lhd \langle H, K \rangle$ となり最終的矛盾を得る。

参考文献

1. Bender, Math. Z. 104 (1968).
2. Fan, Amalgams of prime index, to appear.
3. Glauberman, Math. Z. 117 (1970).
4. Goldschmidt, Ann. of Math. 111 (1980).
5. 五味，J. Fac. Sci. Univ. Tokyo 32 (1985).

6. —, Pairs of groups having a common 2-subgroup of prime indices, to appear.

7. —-田中, On pairs of groups having a common 2-subgroup of odd indices, to appear.

8. Gorenstein-Lyons, J. Alg. 38 (1976).

9. Hayashi, Pacific J. Math. 84 (1979).

10. — , On a normal 2-subgroup of a pair of finite groups, to appear.

11. Janko, J. Alg. 21 (1972).

散在型単純群における極大部分群問題

東大 理　吉荒(よしあら) 聡(さとし)

§1 問題意識

1981年頃, 次の定理の証明が完成したと報告された。

定理. 非可換有限単純群は次のいずれかである。

(i) n次交代群 ($n \geqq 5$)

(ii) Lie型の群

(iii) 26個の散在型単純群 (sporadics)

リストを見れば, その(i)はWeyl群 S_n の交換子群であり, (ii)は複素数体上の単純Lie群の有限体版であって, いずれもBuilding (thinなものも許す)と呼ばれる広く代数群一般に付随した幾何構造上にchamber transitiveに作用する。つまり, 有限群であることの特殊性は(iii)の26個のsporadicsに集約されている。

従ってこれらsporadicsの数学的実態を明確にすると共に, buildingを一般化した幾何構造の存在を模索する必要があろう。すなわち, 次の問題が考えられる。

問題 1. Sporadicsの良い数学的記述を与えよ。
(簡潔で数学的に定義された対象の自己同型群 etc. として)

問題 2. Sporadicsに属する(必ずしも有限でない)幾何を, (coset geometryのような)群の言葉を使わずに, 色々与えよ。その中

にbuildingの一般化といえるものがあるか？

<u>問題3.</u> 先の幾何の良い公理による特徴付けを与えよ。

またこれを通じてsporadicsを特徴付けよ。

問題1,2の解決の為には、sporadicsの群としての構造を決めるのが基本的作業となろう。従って次が解かれるべきである。

<u>問題4.</u> sporadic G に対し、G のmaximal subgroupsの G－共役類の完全代表系を決定せよ。

問題1〜3が群論以外の広い数学的素養と、全く新しい発想を必要とする（と予想される）のに対し、問題4は完全に有限群論内の問題であり、取り組むのは気楽である。しかし乍ら、local theory中心であった在来の有限群の議論で処理しきれない部分があり（結局それも§3で見る如く、local subgp.中の効率的計算という問題に帰着されるが）問題4の完全解決は難しく面倒である。

以下、§2ではsporadicの紹介を兼ねて問題4に対する成果を示し、§3では証明上の難点をsporadic simple gp. O'NSを例にとり解説する。

結論を先にいえば、<u>問題4はほぼ解かれており</u>、残っているものについては現在の方法のままでは（多分）computerの使用を本質的に用いる<u>甚大な計算が必要</u>となるであろう。従って、今後は問題1〜3の解決に精力が注がれるべきである。

§2 問題4に関する成果

26個のsporadicsのうち，最もorderの大きいものはFischer-Griess Monsterと呼ばれ，F_1と記される。F_1のsubgroupのfactor group（section）として得られるsporadicsの事をHappy familyとよぶ。J_1というsporadicsがHappy familyに属するか否かは未解決のおだがそれを除くと，Happy familyは20個のsporadicsからなり，4つのsubfamilyに別けられる。それを以下，仮にMathieu家，Conway家，Fischer家，Monster家と呼ぼう。（cf. 後の表）

Mathieu家は最も由緒ある家柄で（Sylowの定理より古く前世紀にMathieuが発見したという）M_{24}を頭に，M_{23}，M_{22}，M_{12}，M_{11}の5人のメンバーから成り，"群とデザイン"（永尾先生）及び"有限置換群"（大山先生）等の名著によって，その名もかなり広く一般の知る所となっている。

Conway家はLeech latticeと呼ばれる24次元のeven unimodular latticeのautomorphism gp $\cdot 0$のcenterによるfactor gp. $\cdot 1$を頭にそのsection $\cdot 2$，$\cdot 3$，HS，M^c；Suz，J_2の7人のメンバーから成り，いずれもLeech latticeを通じて（あるいはその適当なversionを通じて）良い数学的記述を持っている。

以上両家の頭である$\cdot 1$とM_{24}は深い関係にあり，Leech latticeとGolay codeの関連を通じ，$\cdot 1$はM_{24}から見易く導かれる。（cf. Conway [1]）したがって両家は問題1に対しかなり満足すべき

答えを有するHappy familyのメンバーである。しかし、残る2つの家族は満足すべき記述を持っていない。

<u>Monster家</u>は、F_1とそのあるorder 2, 3, 5 および7の元の中心化群のsectionとして得られる F_2, F_3, F_5 および He の5人のメンバーを持つ。GriessはF_1と関連して、ある196884次元のvector space 上にnon-associativeな可換代数の構造を入れ、その自己同型の中にF_1を構成している。最近Lepowskyら[2]が affine Lie alg. と関連して、このalg.をより数学的に構成している。それでもこの対象(及び証明)はわかりづらい。(cf. 先年の岩手大シンポ.報告集、また Tits [3])

<u>Fischer家</u>は F_1のある order 3の元のcentralizerのsectionであるF_{24}'を頭に、そのsection F_{23}, F_{22} の3人からなる。もともとこれは3-transpositionを持つ群の研究から、Fischer [4]が あるグラフの自己同型群として見出したものなが このグラフもわかりづらい。しかもM_{24}とF_{24}は密接な関係があるにもかかわらず<u>M_{24}からF_{24}をdirectに構成する方法は知られていない</u>。

さて以上のHappy family に対し、F_1にsectionとして入っていない、5個or 6個の sporadics を<u>Pariah</u>とよぶ。それは、orderの小さい順から；(J_1), J_3, Rud, O'NS, Ly, J_4 であり、J_1が O'NSのsubgroupであることを除き、お互いの間にいかなるsectionとしての包含関係もない。これら"お山の大将"であるpariah達も、よい数学

的記述を持たない。J_1, Rud および J_4は,もともとの構成から

$J_1 \leqq G_2(11)$, Rudの2-cover $\leqq GL_{28}(\mathbb{C})$, $J_4 \leqq GL(112, 2)$

であり, J_3, O'NS, Lyはそれぞれある次元の置換表現をcomputerを用いてあたえることにより作られた。最近,後2者は線型群として(しかしやはりcomputerを部分的に用いて)構成されたらしい。(Wilsonの手紙による。)

すなわち, $Ly \leqq GL_{125}(5)$, O'NSの3-cover $\leqq GL_{45}(7)$.

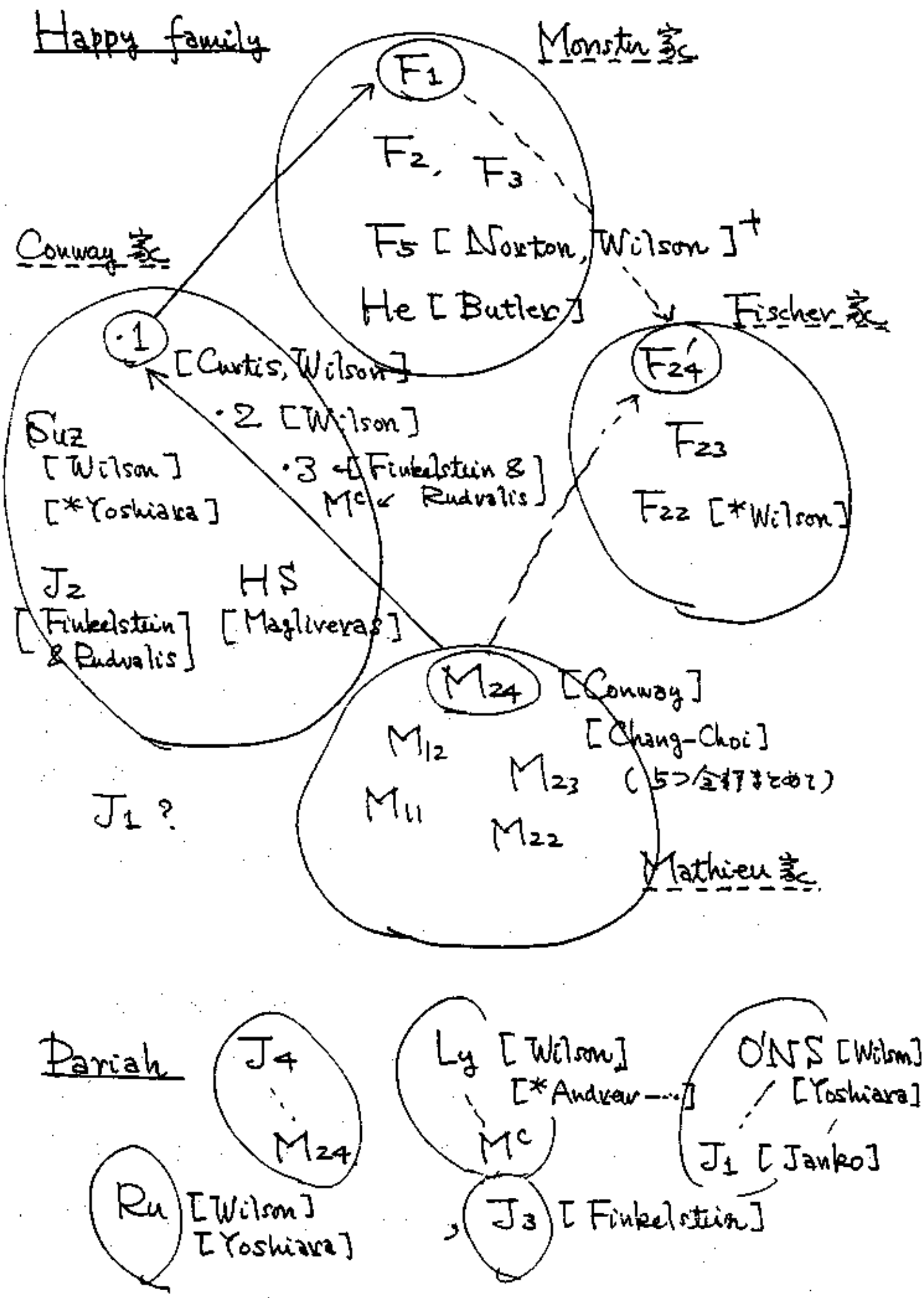
J_3に関しては $J_3 \leqq GL_{85}(\mathbb{Q}(\sqrt{-3}, \sqrt{-11}))$のみならず(Frohardt)この形で構成されたかどうかは知らない。なおWeissはJ_3をあるグラフの自己同型として作っている。

さて,これら26個のsporadicsにたいする問題4への成果が次ページの表にまとめてある。群の欄の[ ]中に,対応する群の極大部分群を完全決定した人の名及び部分決定した人の名(*を付す)が記されている。[ ], [ ]とかかれているのは独立に行なわれたことを示し, [,]は2人の仕事を併せて解かれた事を示す。

次ページの表によれば,問題4が未解決なsporadicsは次の7つである。F_{22}, F_{23}, F_{24}', J_4, F_3, F_2, F_1.

この中で, F_{22}, F_{23}は2,3年がかりで頑張れば出来るかも知れないが,あとのものは問題1にたいするよほどうまい解答が与えられない限り, computerを用いても難しかろう。(computerをフルに用いて精力的な仕事を行っているWilsonも半ばあきらめているようである。)

問題4への成果



†: Nortonが決めたらしいが，証明がなくなってしまったのをWilsonが証明し直しているという。

§3 証明の難点 ― 構成問題 ―

Gをsporadic simple groupとし，Mをその極大部分群，NをMのminimal normal subgroupとすれば，Nはcharacteristically simple，すなわち互いに同型な（可換も許す）単純群の直積，であり，$N=N_G(M)$である。従って問題4の解決は自然に次のStepsに分けられる。

Step1　可換なN，すなわちelementary abelian subgroup Nを共役を除いて分類し，そのGにおける正規化群を求めよ。

Step2　Gが実際に含むnon-abelian char. simple group Nをきっちり決定せよ。

Step3　Step2で得られたNを共役を除いて分類し，そのGにおけるnormalizerを求めよ。

Step4　Step1，3で得られたGのsubgroupsの共役を除いた包含関係を調べよ。

（残ったものが求める完全代表系である。）

Step1は面倒なだけで頑張ればなんとかなる。Step4はStep1〜3が解決すれば容易である。Step2及び3が難関である。

特に Step 2 では次の作業を行なわねばならない。

与えられた非可換単純群 X に対して，

"X と同型な G の部分群が存在するか？"

no

存在しない事を証明せよ。

yes

"従来から知られている G の部分群で，
X と同型な部分群を含むものがあるか？"

yes

その事実を指摘せよ。

no

☆ $\boxed{X\text{ と同型な部分群を構成せよ。}}$

この☆が全体を通じて最も難しい。(elementary abelian group はあらためて構成してみせる必要がないので，Step 1 は易しいのである。) しかも☆の構成を下手に行なうと Step 3 が非常に難しくなる。X と同型な G の部分群の共役類分割が自然に見えてくるような構成が望ましい。また，Step 3 は一般にはかなり面倒であり，しばしば computer が使用されるようである。

Pariah のひとつである O'Nan-Sims の群を例にとってこの点を解説しよう。この群も問題1に対する良い答を持たないが，一応次の形で定義する。

<u>定義</u>. 次のpresentationを持つ2-group P を2-Sylow群に持つ有限単純群 G をO'Nan-Simsの群とよぶ。

$$P = \left\langle \begin{array}{l} v_1, v_2, v_3 \\ s,\ t \end{array} \middle| \begin{array}{l} v_i^4 = t^2 = [v_i, v_j] = 1 \ (1 \le i, j \le 3) \\ s^4 = v_1 v_3;\ v_1^s = v_2,\ v_2^s = v_3, \\ v_3^s = v_1 v_2^{-1} v_3\ ;\ v_1^t = v_3^{-1}, \\ v_2^t = v_2^{-1},\ v_3^t = v_1^{-1} \end{array} \right\rangle$$

<u>定理</u>. (Sims-Andrilli) O'Nan-Simsの群 G は存在し, 同型を除いて唯一つである。また $|\mathrm{Aut}\,G : G| = 2$ である。

O'Nan [5] は $|G| = 2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$ を示し, すべての素数 p にたいする G のmaximal p-local subgps. の大体を記述し, G のcharacter tableも決定した。また $\mathrm{Aut}\,G - G$ は唯一つのinvolutionの共役類を持ち, involution $\sigma \in \mathrm{Aut}\,G - G$ に対し, $C_G(\sigma) \cong J_1$ であることも示した。

筆者は[5]における情報のみを用い, computerを全く使わずに次の結果を得た。

<u>定理</u>. ([6]) O'Nan-Simsの単純群 G の極大部分群の共役類は13個あり, その代表系は次の如し。

(A) 2個の2-local groups	index
(i) $(Z_4 \cdot L_3(4)) \rtimes Z_2$	2,857,239

(ii)	$(Z_4 \times Z_4 \times Z_4)\cdot L_3(2)$	42,858,585
(B)	2個の 3-local groups	
(iii)	$((E_9 \rtimes Z_4) \times A_6)\cdot Z_2$	17,778,376
(iv)	$E_{81} \rtimes (2^{1+4}_{-} \cdot D_{10})$	17,778,376
(C)	9個の non-local groups	
(v),(vi)	$L_3(7) \rtimes Z_2$ (2つの共役類)	122,760
(vii)	J_1	2,624,832
*(viii),(ix)	$L_2(31)$ (2つの共役類)	30,968,784
*(x),(xi)	M_{11} (〃)	58,183,776
*(xii),(xiii)	A_7 (〃)	182,863,296

この中で * を付したものは従来その存在が知られていなかった為，新たに構成した部分群である。上に見る如くこれらの部分群の index は非常に大きい。

さて，問題は 単純群 G における proper simple gp. X をどのように構成するか；であるが，現在 3つの方法が考えられる。

(i) Gがうまい幾何的構造 Ω に作用している場合；例えば 1点の stabilizer 等，X に幾何学的意味を付して存在を示す。

(ii) Xの適当な subgroup A, B で $\langle A, B\rangle = X$ をみたすべきものの存在をまず示しておき，Gの non-trivial irreducible character χ で $(\chi|_A, 1) + (\chi|_B, 1) > (\chi|_{A\cap B}, 1)$ をみたすものを見つける。すると，

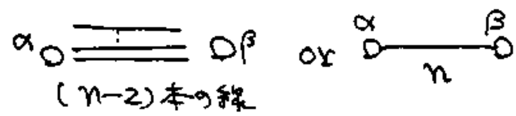
$\langle A,B\rangle$はGのproper subgroupとなる。(Brauer trick) そのあと、$X\cong\langle A,B\rangle$を示す。

(iii) Xの適当なpresentation $\langle x_i\ (i=1\sim m) \mid \overset{\text{relations}}{r_j}\ (j=1\sim n)\rangle$ を使って、Gが実際にこのrelation $\tilde{r}_j$を満す元$\tilde{x}_i$を含むことを示す。(Xはsimpleだから、$\langle \tilde{x}_i\rangle\cong X$となる。)

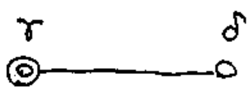
O'Nan-Simsの群の場合、(i)は目指す幾何を知らないから使えないし、(ii)が適用できる(すなわちうまいXが存在する)のはindexの最小の$L_3(7)\rtimes Z_2$のみである。従って(iii)が使われた。

この過程で$L_2(11)$, M_{11}の興味深いpresentationが得られた。それを表すため次の記号を用意する。([6], §4)

記号. ◎はorder 3の元を表し、○はinvolutionを表す。次のルールでこれらを結ぶ。



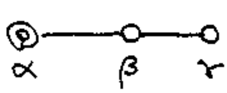
$\overset{\text{def.}}{\Longleftrightarrow}$ $o(\alpha\beta)=n$



$\underset{\text{def.}}{\Longleftrightarrow}$ $o(\gamma\delta)=3$ $\left(\Leftrightarrow \begin{array}{l} o(\gamma^{-1}\delta)=o(\delta\gamma) \\ =o(\delta\gamma^{-1})=3 \end{array}\right)$

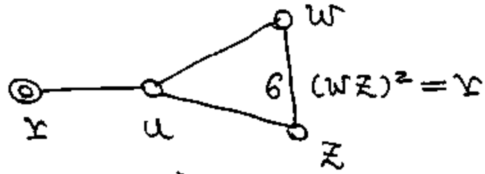
$\underset{\text{def.}}{\Longleftrightarrow}$ $o(\gamma\delta)=2$ $\left(\Leftrightarrow \gamma^{\delta}=\gamma^{-1} \Leftrightarrow \begin{array}{l} o(\gamma^{-1}\delta)=o(\delta\gamma) \\ =o(\delta\gamma^{-1})=2. \end{array}\right)$

また、これらの他にrelationがあるときは関連するedgeに添えて表す。

例えば $\langle \alpha,\beta,\gamma \mid$ 

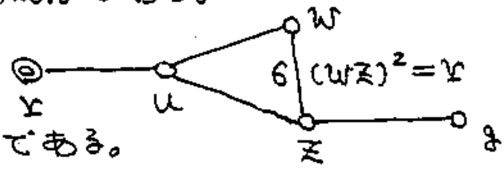
$\rangle$ はA_5のpresentationである。

Lemma.

(i) $\langle x, u, w, z \mid$ 

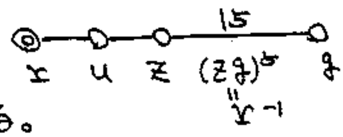
$\rangle$

は $L_2(11)$ の presentation である。

(ii) $\langle x, u, w, z, g \mid$ 

$\rangle$

は M_{11} の presentation である。

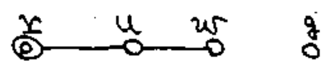
(iii) (Perkel [7]) $\langle x, u, z, g \mid$ 

$\rangle$

は $L_2(31)$ の presentation である。

このpresentationを用いて, M_{11}, $L_2(31)$ と同型な部分群は次の様に構成される。

まず, G は J_1 に同型な部分群 J を含んでいた。J_1 は $L_2(11)$ と同型な群を含むから J の元 x, u, w, z で Lemma (i) の relation を満すものがある。そこで Lemma (ii) を見れば次の集合

$\mathcal{S} := \{ g \in G \mid g$: involution, 

$\}$

$= \{ g \in C_G(u) \cap C_G(w) \mid g$: involution, $x^g = x^{-1} \}$

を調べる事が重要である。うまい具合に $C_G(u) \cap C_G(w)$ は小さい local subgroup だから, この群の中の元の様子はかなりよくわかる。そこで, 次がわかる。

Lemma. $|\mathcal{S}| = 4$ であり, 2つの $\mathcal{S}$ の元 g_1, g_2 に対しては $g = g_i$ $(i=1,2)$ として lemma の (ii) の relation が満たされ, のこり2つの $g_3, g_4 \in \mathcal{S}$ は $g = g_i$ $(i=3,4)$ として lemma (iii) の relation が成立つ

特にGはM_{11}, $L_2(31)$と同型な部分群を含む。

これでM_{11}, $L_2(31)$に対する構成問題☆は解決した。しかも、実はGの$L_2(11)$と同型な部分群は互いに共役な事が示せるので、M_{11}中$L_2(11)$が互いに共役な事と併せて、G中のM_{11}と同型な群は上のlemmaの記号で$\langle x, u, z, w, g_1\rangle$ or $\langle x, u, z, w, g_2\rangle$のいずれかと共役になる事もわかり、(この2つは$G$-共役でない。)$M_{11}$に対するStep 4も解決する。$L_2(31)$についても同様である。

A_7の構成はもう少し注意深く生成元を選ばねばならぬが、presentation $\langle \alpha, \beta, \gamma, \delta, \varepsilon \mid \overset{\alpha}{\circledcirc}\!-\!\overset{\beta}{\circ}\!-\!\overset{\gamma}{\circ}\!-\!\overset{\delta}{\circ}\!-\!\overset{\varepsilon}{\circ} \rangle$をやはり利用する。

presentationの形が良く、relationをcheckする際にlocal subgroupの中からpick upすれば済んだという点が成功の原因のように思われる。

文　献

1. Conway, J., Three lectures on exceptional groups, in: G. Higman and M. Powell, Finite Simple Groups, Oxford, 1969; Academic Press, London, 1971, pp. 215-247.

2. Frenkel, B., Lepowsky, J., and A. Meurman, A natural representation of the Fischer-Griess Monster with the modular function J as character, Proc, Natl. Acad. Sci. USA

vol. 81, pp. 3256–3260, May 1984

3. Tits, J., On R. Griess' "Friendly Giant", Invent. Math. 78, pp. 491–499 (1984)

4. Fischer, B., Finite groups generated by 3-transpositions, Univ. of Warwick (preprint)

5. O'Nan, M., Some evidence for the existence of a new simple group, Proc. London Math. Soc. 32 (1976), pp. 421–479.

6. Yoshiara, S., The maximal subgroups of the sporadic simple group of O'Nan, to appear in J. of the Fac. Sci, the Univer. of Tokyo, Sec. IA, Vol 33.

7. Perkel, M., A characterization of PSL2(31) and its geometry, Canad. J. Math., 32 (1980), 155–164.

Indecomposable modules と blocks

大阪市大　理　河合浩明

Gを有限群，Fを標数 $p(>0)$ の代数的閉体，Mを defect group Dをもつ G の block Bに属する既約 FG-加群とする。その時，次のことが知られている。

MがBにおいて height 0 をもつ $\Longleftrightarrow$ i) DがMの vertex
ii) Mの D-source のF上の次元は p と素

（Knörr [5] 参照）

ここでは，次のことを目標とする。

I　右辺の condition ii) を満す直既約加群について調べる。

II　右辺の condition i) ii) を満す直既約加群の restriction と block induction (correspondence) の間の関係を調べる。そしてそれらの事実を基に blocks に関するいくつかの結果（すでに知られている）を導く。

notation：Rは標数0のcomplete discrete valuation ring，Fをそのresidue class fieldとする。さらにRのqoutient fieldはGの任意の部分群のsplitting fieldであると仮定する。$\mathcal{O}$はR又はFを表わすとする。任意の$\mathcal{O}G$-加群Mは$\mathcal{O}$上finitely generated，freeであるright $\mathcal{O}G$-加群であるとする。Mが直既約の時，$vx(M)$はMのvertexを表わす。他の加群Nに対し，$N|M$はNがMの直和因子に同型であることを意味するさらにNが直既約であるとき"NはMのcomponentである"と言うことにする。nを自然数としてp^mがnを割り切る最大p-巾であるとき，$m=\nu(n)$と書く。最後にGのblock Bに対し，$\delta(B)$はBのdefect groupを表わす。

I Sources with $\mathcal{O}$-rank prime to p

Mを直既約$\mathcal{O}G$-加群とする。我々は次のcondition を考える。

$$(*) \qquad p \nmid \mathrm{rank}_{\mathcal{O}} V \quad \text{for a source } V \text{ of } M$$

次のことはよく知られていることであるが便利であるので証明なしに記しておく。

<u>補題 1.1</u>　M を vertex Q をもつ直既約 $\mathcal{O}G$-加群，V を直既約 $\mathcal{O}Q$-加群とする．この時

V が M の Q-source $\Longleftrightarrow$ $V \mid M_Q$，Q が V の vertex

<u>定理 1.2</u>　H を G の部分群．M を vertex Q をもち，(*) を満す直既約 $\mathcal{O}G$-加群　P を $\{Q^x \cap H \mid x \in G\}$ の maximal member とする。この時，M_H の component で P を vertex としてもち，(*) を満足するものが存在する．

∵）$P = Q^a \cap H$ $(a \in G)$ とする，V を M の Q^a-source とするとき，V_P の component W で $p \nmid \mathrm{rank}_{\mathcal{O}} W$ となるものが存在する。その時 Green's Theorem より $vx(W) = P$ となる。$W \mid M_P$ としてよいので N を $W \mid N_P$ となる M_H の component とするとき，$P \leq_H vx(N) \subseteq_H Q^x \cap H$ for some $x \in G$ となる。従って P の maximality より $vx(N) =_H P$ となる．さらに補題 1.1 より W は N の P-source である．

次に condition (*) に関する2つの注意を与える.

注意 1.3 cyclic vertex をもつ直既約 FG-加群は (*) を満す。

(non-cyclic defect group をもつ block の中に (*) を満す非同型な直既約FG加群は infinite 存在する)

注意 1.4 F を代数的閉体と仮定する。

直既約 $\mathcal{O}G$-加群 M に対して.

$\nu(\mathrm{rank}_{\mathcal{O}} M) = \nu(|G : vx(M)|) \Rightarrow$ M は (*) を満す

定理 1.2 の応用として，次の結果が得られる。

Corollary 1.5 H を G の正規部分群，M を既約 FG-加群 そして N を M_H の既約成分とする.

その時. $\nu(\dim_F M) = \nu(|G : vx(M)|) \Rightarrow \nu(\dim_F N) = \nu(|H : vx(N)|)$

又 (*) を満す代表的な module の一つとして，Scott module と呼ばれるもの ([2] 参照) がある。この module に関して定理 1.2 に対応する一つの結果を証明なしに記しておく。この定理は奥山氏によって suggest された。

<u>定理 1.6</u>　H を G の部分群，S を vertex Q をもつ Scott G-module，P を $\{Q^x \cap H \mid x \in G\}$ の maximal member とする。S' を vertex P をもつ Scott H-modle とする時，$S' \mid S_H$ となる。

Ⅱ　Block theory への応用．

block induction と modules の induction - restriction の間の関係において，次の事実は重要である．

<u>定理 2.1</u>（Nagao - Green）　H を G の部分群 M を G の block B に属する直既約 の G - 加群とする．N を M_H の component，b を N が属する H の block とする．そのとき

$$H \geq C_G(\mathrm{vx}(N)) \Rightarrow b^G \text{ は define され，} b^G = B$$

H を G の部分群，b を H の block とする．$C_G(\delta(b)) \subseteq H$ である時，Brauer に従って b を H の G - admissible block と呼ぶことにする。（この時 b^G は define される）次の定理は奥山氏によって suggest された．

<u>定理 2.2</u>　b を H の G-admissible block とする。M を $B=b^G$ に属する直既約 $\mathcal{O}G$-加群で $vx(M)=_G \delta(B)$，(*) を満足するものとする。その時 M_H の component N で b に属し，$vx(N)=_H \delta(b)$，(*) を満足するものが存在する。

∵) $|\delta(B)|/|\delta(b)|$ に関する帰納法で証明する

$|\delta(B)|=|\delta(b)|$ の場合，渡辺〔6〕において次のことが示されている：$^\forall$直既約 $\mathcal{O}G$-加群 $M\in B$ に対して $^\exists M_H$ の component N s.t. $N\in b$，$vx(N)=_G vx(M)$。さらに補題 1.1 を用いれば，定理の主張は成立する。そこで $|\delta(B)|>|\delta(b)|$ とする。$\hat{b}$ を $T=\delta(b)C_G(\delta(b))$ における b の root とする　$H_1=N_G(\delta(b))$ $b_1=\hat{b}^{H_1}$ とおくとき，Brauer's first main theorem と仮定より $|\delta(b_1)|>|\delta(b)|$ となる。そこで帰納法の仮定より M_{H_1} の comp. N_1 で b_1 に属し，$vx(N_1)=_H \delta(b_1)$，(*) を満すものが存在する。ところで $T\lhd H_1$ より b_1 は $\hat{b}$ を cover する。そこで定理 1.2 は $(N_1)_T$ の comp. $\hat{N}$ で $\hat{b}$ に属し，$vx(\hat{N})=_{H_1} \delta(b_1)\cap T$ となるものが存在することを示す。ところで $vx(\hat{N})\subseteq\delta(b)\subseteq\delta(b_1)$ である。

故に $vx(\hat{N}) = \delta(b)$ となる。N を $\hat{N} \mid N_T$ となる M_H の component とするならば 定理 2.1 より $N \in b$ さらに $\hat{N} \mid N_T$ より $\delta(b)$ は N の vertex となり 補題 1.1 を適用することにより N は (*) を満すことが示される。

定理 2.1 と定理 2.2 において $M = I_G$ (trivial $\mathcal{O}G$ module) をとることによって次の事実が示される。

<u>系 2.3</u> (Brauer's third main theorem)

b を G の部分群の G-admissible block とする。

b^G : principal $\Leftrightarrow$ b : principal

以後の結果を導くとき，F は代数的閉体と仮定してよい。

<u>系 2.4</u> (Alperin and Burry) Q を G の p-部分群とし，H を G の部分群で $H \geq QC_G(Q)$ とする。B を G の block そして P を $\{\delta(B)^x \cap H \mid x \in G, \delta(B)^x \cap H \geq Q\}$ の maximal member とする。その時

$\exists$ H の block b s.t. $b^G = B$, $\delta(b) =_H P$

∵) M を B に属する height 0 の既約 FG-加群とする。その時 $\nu(\dim_F M) = \nu(|G : vx(M)|)$ をして $\delta(B)$ が M の vertex となる。定理 1.2 と注意 1.4 より，P を vertex としてもつ M_H の component N が存在する b を N を含む block とするならば，$C_G(P) \subseteq H$ より定理 2.1 から b^G は define され，$b^G = B$ となる。さらに P の極大性より P は b の defect group となる。

H を G の正規部分群とする。G の block B が H の block b を cover しているとする。この時次の事実はよく知られている。

i) B に属する任意の既約 FG-加群 M に対して $\exists$ 既約 FH-加群 N s.t. $N \mid M_H$

ii) b に属する任意の既約 FH-加群 N に対して $\exists$ 既約 FG-加群 M s.t. $N \mid M_H$

この事実と定理 1.2 より次の結果を示すことができる

<u>系 2.5</u> (Knörr) H を G の正規部分群，G の block B が H の block b を cover しているとする。この時 $\delta(b) =_G \delta(B) \cap H$

Corollary 1.5 と Corollary 2.5 より

<u>Corollary 2.6</u>　H を G の正規部分群，B を G の block として φ を B に属する G の既約 Brauer 指標とする。この時

φ : height 0 $\Rightarrow$ φ_H の任意の既約成分はその属する block において height 0

— Reference —

[1] J. L. Alperin and D. W. Burry : Block theory with modules, J. Algebra 65 (1980), 225-233.

[2] D. W. Burry : Scott modules and lower defect groups, Comm. Algebra (17) 10 (1982), 1855-1872.

[3] J. A. Green : On the Brauer homomorphism, J. London Math. Soc. (2) 17 (1978), 58-66.

[4] R. Knörr : Blocks, vertices and normal subgroups, Math. Z. 148 (1976), 53-60.

[5] ________ : On the vertices of irreducible modules, Ann. of Math. (2) 110 (1979), 487-499.

[6] A. Watanabe : Relations between blocks of a finite group and its subgroup, J. Algebra, 78 (1982), 282-291.

Some Recent Results Concerning Designs and Planes

William M. Kantor *

University of Oregon, Eugene, OR 97403, USA

This short paper surveys some recent results made possible by the classification of finite simple groups.

1. 2-transitive designs

During the period 1960-1975 there was a great deal of research activity concerning designs $\mathcal{D}$ whose automorphism group $G = \mathrm{Aut}\ \mathcal{D}$ is 2-transitive on points. The results obtained are surveyed in detail in [15]. One of the leaders in this area was Noboru Ito, whose beautiful results [6-11] greatly influenced my research.

During that period it had been hoped that the study of designs might lead to a classification of 2-transitive groups — or, at least, of multiply transitive ones. However, the relatively little work in this direction after 1975 reflected the difficulty of this prolem. Finally, it became apparent that 2-transitive groups would be classified only when all finite simple groups were.

There is now a list of (finite!) 2-transitive groups (e.g., in [16], based on results of Maillet, Curtis-Kantor-

*The preparation of this paper was supported by the JSPS.

Seitz, Huppert, Hering, and folklore in the case of the sporadic simple groups). One very easy consequence of this list is the folowing

Theorem 1 ([17]). If $\mathcal{D}$ is a symmetric design with a 2-transitive automorphism group, then $\mathcal{D}$ or its complementary design is a projective space, the 11-point Hadamard design, the 176-point design for the Higman-Sims group, or the 2^{2n}-point design whose (1,-1) incidence matrix is the 2n-fold tensor power of $\begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}$, $n \geq 2$.

This theorem and the next one completely settle problems studied at length by Ito and myself:

Theorem 2 ([16]). If $\mathcal{D}$ is a design with $\lambda = 1$ and $k > 2$ whose automorphism group is 2-transitive on points, then $\mathcal{D}$ is one of the following: an affine or projective space; the unital ($v = q^3 + 1$, $k = q+1$) associated with $PSU(3,q)$ or ${}^2G_2(q)$; an affine plane with 3^4 or 3^6 points; or one of two designs having $v = 3^6$ and $k = 3^2$.

The two designs with 3^6 points were discovered by Hering (unpublished). Recent special cases of Theorem 2 are found in [2,4,19]. The proof of Theorem 2 is very easy when G has no regular normal subgroup. In fact, the only delicate part of the proof occurs when G is assumed to be solvable.

There is an analogue of Theorem 2 for t-designs with $\lambda = 1$ having a t-transitive group. In a somewhat similar direction, Theorem 2 immediately produces a classification of all designs with $\lambda = 1$ and $k>2$ whose automorphism group G is transitive on ordered triangles of points. Recently, Li [20] extended this to deal with tansitivity on unordered triangles.

More generally, consider a geometric lattice L. In [16], it was noted that Theorem 2 produces a classification of all such L for which Aut L is transitive on ordered bases. While the corresponding problem for unordered bases remains open, involved arguments in Li [20] settle the cases of dimension 2 or 3.

On the other hand, it is very easy to deduce from Theorem 2 the classification of all t-designs with $\lambda = 1$ whose automorphism group is t-homogeneous on points (see [3] for the case $t = 2$).

Another open problem (somewhat related to Theorem 1) is a classification of all Hadamard matrices whose automorphism group is 2-transitive on rows. This is another important problem studied by Ito [12-14].

2. Projective planes

The first, best and most important result concerning 2-transitive designs was the Ostrom-Wagner Theorem [22], which dealt with the case of projective planes. The proof given 25 years ago is elegant, and led to many other significant results. In particular, Theorem 2 in no way influences the beauty or strength of that fundamental result.

Attempts to generalize the Ostrom-Wagner Theorem began almost immediately after its publication. While there were several directions in which generalizations were studied, the one that concerns us here involves transitivity on flags (incident point-line pairs).

Conjecture A. If π is a finite projective plane such that $G = \mathrm{Aut}\ \pi$ is flag-transitive, then π is desarguesian.

According to a result of Higman-McLaughlin [5], if $\mathcal{D}$ is a design with $\lambda = 1$ and $G \leq \mathrm{Aut}\ \mathcal{D}$ is flag-transitive, then G is primitive on the points of $\mathcal{D}$. Therefore, Conjecture A would follow from

Conjecture B. If π is a finite projective plane such that $G = \mathrm{Aut}\ \pi$ is primitive on points, then π is desarguesian.

These conjectures remain open. The following results handle the group theoretic cases of the conjecture.

Theorem 3 ([18]). Let π be a finite projective plane such that $G = \mathrm{Aut}\ \pi$ is primitive on points (or, less generally, is transitive on flags). If the stabilizer of some flag is not 1, then π is desarguesian.

When the stabilizer of each flag is just 1, π is a difference set plane. If π has order n then the number n^2+n+1 of points is a prime, either $|G| = n^2+n+1$ or G is a Frobenius group, and Conjectures A and B reduce to questions about $\mathbb{Z}_p$. Thus, the open cases of the conjectures are very much not group theoretic.

The proof of Theorem 3 begins with three observations: G is primitive on points, the number n^2+n+1 of points is odd, and G can be assumed to have a simple normal subgroup. All primitive permutation groups of odd degree having a nonsporadic simple normal subgroup were determined in [18]. (Independently, the same result was obtained in [21]. Also independently, the sporadic case was completely handled in [1].) The list of such primitive groups is very long. It contains all maximal parabolic permutation representations of characteristic 2 groups of Lie type, alternating or symmetric groups acting on subsets of a fixed size or on partitions into blocks of equal size, classical groups on orbits of subspaces or on suitable direct sum decompositions of the vector space into subspaces of equal dimension, and so on.

The proof of Theorem 3 then degenerates into a long and tedious case by case elimination of the possibilities in this long list. The main tools involve subplanes. In particular, one can assume that n is a square, $n = m^2$, and that all involutions in G fix exactly m^2+m+1 points. Unfortunately, I was not able to find a uniform approach, and many separate tricks were used.

3. Open problems

The proof of Theorem 3 suggests further problems, such as the following two.

(a) Determine all flag-transitive designs $\mathcal{D}$ with $\lambda = 1$ and v odd but not a prime power. This is related to both sections 1 and 2. By [5], G is primitive on points. One can assume that $G = \mathrm{Aut}\,\mathcal{D}$ has a simple normal subgroup. Then the results in [1,18,21] provide a very long list of possible permutation groups to be checked. Unlike the case in Theorem 3, there is no reason to expect involutions to be well-behaved. Nevertheless, the question seems feasible. Its solution may even produce a better approach to Theorem 3.

(b) Show that if π is finite affine plane and $G = \mathrm{Aut}\,\pi$ is point-primitive then π must be a translation plane. If the plane has order n then there are n^2 points. A standard argument of Ostrom and Wagner [22] settles the case of even n. When n is odd, it is easy to reduce to the situation in which G has a simple normal subgroup. Once again, the results in [1,18,21] produce a long list of primitive groups to check. One can assume that each involution fixes exactly n points. Nevertheless, I have not been able to check the list. The difference between this situation and that of Theorem 3 concerns the action on lines: G was line-transitive in Theorem 3 whereas here G can have many line-orbits of various sizes.

References

1. M. Aschbacher, Overgroups of Sylow subgroups in sporadic groups (to appear).

2. G. Cherlin, L. Harrington and A. Lachlan, $\aleph_0$-categorical $\aleph_0$-stable structure (to appear).

3. A. Delantsheer and J. Doyen (to appear).

4. M.Hall,Jr., Steiner triple systems with a doubly transitive automorphism group (to appear).

5. D. G. Higman and J. E. McLaughlin, Geometric ABA-groups, Ill. J. Math. 5 (1961) 382-397.

6. N. Ito, Uber die Gruppen $PSL_n(q)$, die eine Untergruppe von Primzahlindex erhalten, Acta Sci. Math. (Szeged) 21 (1961) 206-217.

7. N. Ito, On a class of doubly, but not triply transitive permutation groups, Arch. Math. 18 (1967) 564-570.

8. N. Ito, On permutation groups of prime degree p which contain (at least) two classes of conjugate subgroups of index p, Rend. Sem. Mat. Padova 38 (1967) 287- 292.

9. N. Ito, On permutation groups of prime degree p which contain at least two classes of conjugate subgroups of index p, II, Nagoya Math. J. 37 (1970) 201-208.

10. N. Ito, A theorem on Jordan groups, in "Theory of finite groups", Benjamin, New York 1969, pp.47-48.

11. N. Ito, On Wielandt number of transitive permutation groups of prime degree, Acta Math. Acad. Sci. Hungar. 26 (1975) 267-274.

12. N. Ito, Hadamard matrices with "doubly transitive" automorphism groups, Arch. Math. 35 (1980) 100-111.

13. N. Ito and J. S. Leon, An Hadamard matrix of order 36, JCT(A) 34 (1983) 244-247.

14. N. Ito and H. Kimura, Studies on Hadamard matrices with "2-transitive" autmorphism groups, J. Math. Soc. Japan 36(1984) 63-73.

15. W. M. Kantor, 2-transitive designs, in "Proc. Comb. Conf.", Reidel, Dordrecht 1975, pp 44-97.

16. W. M. Kantor, Homogeneous designs and geometric lattices (to appear in JCT(A)).

17. W. M. Kantor, Classification of 2-transitive symmetric designs (to appear in Graphs and Comb.: An Asian Journal).

18. W. M. Kantor, Primitive permutation groups of odd degree, and an application to finite projective planes (submitted).

19. J. D. Key and E. E. Shult, Steiner triple systems with doubly transitive automorphism groups : A corollary to the classificaiton theorem for finite simple group, JCT(A) 36 (1984) 105-110.

20. Hui-Ling Li (to appear).

21. M. Liebeck and J. Saxl, The primitive prmutation groups of odd degree (to appear).

22. T. G. Ostrom and A. Wagner, On projective and affine planes with transitive collineation groups, Math. Z. 71 (1959) 186-199.