Witt システム覚書

岩　崎　史　郎

§1　はじめに

'24' や '12' は日常生活によく出てくる数である——1日は24時間，1年は24節気，二十四の瞳；1年は12ヵ月，12支，12平均律音階，十二指腸，十二単，…….

この小文では，24や12と関連した不思議な世界—— Witt システム——の一端を論じたい．Witt システムは有限幾何の一種であって，全部で5つあり，$\boldsymbol{W}_{24}$, $\boldsymbol{W}_{23}$, $\boldsymbol{W}_{22}$, $\boldsymbol{W}_{12}$, $\boldsymbol{W}_{11}$ と表される．ここに $\boldsymbol{W}_v$ は，v 個の点の上の幾何であることを示す．各 $\boldsymbol{W}_v$ には，M_v で表される Mathieu 群という有限単純群が自然に作用しており，両者は相俟って我々を魅了してやまない不思議で豊かな世界を形成する．(5つの Witt システム，Mathieu 群のうち，$\boldsymbol{W}_{24}$, M_{24} はそれぞれ他の4つを含むと考えてよく，特に重要である．) Witt システムと Mathieu 群は，ある意味で極めて例外的な存在であって，特殊で独自の美しい不思議な性質を持ちながら (持つゆえに?)，群論・組合せ論において，Mathieu 群以外のいくつかの重要な単純群の構成にも本質的にかかわっているなど，種々の面で大きな役割を演じている．また，数学の他分野，符号理論や整数論 (保型関数)，更に広い意味では物理の (超) 弦理論などともかかわってきているらしく，このシステム・群は普遍的な存在あるいは大いなる世界への不思議な扉・裂け目といってもよいように思われる．このことはいくつかのことを連想させる——特殊な数でありながら，数学の至る所に顔を出し，普遍的な特殊ともいえる π (円周率), e (自然対数の底), i (虚数単位)．また，

「特殊を生き生きと捉えればそのまま普遍となる」という Goethe の言葉や,「幾分 strangeness を持たないようなすばらしい美は存在しない」という F. Bacon の言葉などを. あるいは, 原則から例外を説明するのが普通であるが, 逆に例外から原則を説明する方が本質に迫ることがあるという考え方を.

5つの Mathieu 群は 1861・73年 E. Mathieu によって発見されたが, それらを実際に構成して確固たる存在証明を与え, それらが単純群であること, 更に対応する5つの Witt システムを構成し, その存在と一意性を示したのは E. Witt である (1938年 [9], [10]). 以来, 多くの人によって Mathieu 群と Witt システムに関する興味深い研究がなされてきたが, まだ研究が十分とは言いがたい面も少なからずあり, その不思議な正体は満足のいくほど十分には把握されていないように思われる. (R. T. Curtis は 1976年 [2] で, MOG=Miracle Octad Generator という文字通り魔法のような概念を導入して $\boldsymbol{W}_{24}$, M_{24} の注目すべき研究をしたが, MOG という名前からも Witt システム・Mathieu 群の神秘さがうかがえよう.)

この小文の目的は, Witt システムについて簡単に紹介し, その魅力の一端に触れながら, その正体が少しでもよく分かるように Witt システムの自然な透明化をめざし, 従来の研究より一層単純で初等的かつ統一的な一つのアプローチを試みることである. 特に, (MOG の代わりに) '差型' または '代表ブロック' という概念を導入して, 5つの ($\boldsymbol{W}_{22}$ 以外の4つというべきか) システムの全てのブロックを統一的・具体的に記述する簡単な一つの方法と, 3つの大きなシステム $\boldsymbol{W}_{24}$, $\boldsymbol{W}_{23}$, $\boldsymbol{W}_{22}$ の一意性の新しい証明の概略を与える. 詳しくは [3], [4] を参照されたい.

§2 準備

定義 1 t, v, k, λ を一定の自然数とし, $v \geqq k \geqq t$ とする. S を v 個の点の集合, $\boldsymbol{B}$ を S の部分集合からなるある集合として, 次がみたされているとする.

(1) $\boldsymbol{B}$ の元は全て, S の k 個の点からなる部分集合である ($\boldsymbol{B}$ の各元を**ブロック**という).

(2) S の t 個の任意の点に対し，それらを含むブロックの個数は，t 個の点のとり方によらず一定で λ である.

このとき，S と $\boldsymbol{B}$ の組 $\boldsymbol{D}=(S, \boldsymbol{B})$ を $\boldsymbol{t}-(\boldsymbol{v}, \boldsymbol{k}, \boldsymbol{\lambda})$ **デザイン**，あるいは t, v, k, λ を**パラメーター**とする **t-デザイン**という.（デザインというのは，S の点全体がブロックによって，パラメーターの値が示すようにきれいに‘配置’されているという意味であろう.）

特に $\lambda=1$ のとき，即ち $t-(v, k, 1)$ デザインを Steiner **システム**という. このシステムでは，任意の t 個の点 $a_1, \cdots\cdots, a_t$ に対し，それらを含むブロックがただ1つ定まるが，それを $a_1, \cdots\cdots, a_t$ の定めるブロックといい，

$$\langle a_1, \cdots\cdots, a_t\rangle$$

で表すことにする.

次のことは容易に証明され，よく知られている.

結果1 (たとえば永尾 [8], p. 14). $\boldsymbol{D}=(S, \boldsymbol{B})$ を $t-(v, k, \lambda)$ デザインとするとき，$0\leqq s\leqq t$ なる任意の整数 s に対して，s 個の任意の点を含むブロックの個数は

$$\lambda_s=\lambda\binom{v-s}{t-s}\Big/\binom{k-s}{t-s}=\lambda\frac{(v-s)(v-s-1)\cdots\cdots(v-t+1)}{(k-s)(k-s-1)\cdots\cdots(k-t+1)}$$

である. 特に，ブロックの個数は

$$|\boldsymbol{B}|=\lambda_0=\lambda\binom{v}{t}\Big/\binom{k}{t}.$$

定義 2 $t-(v, k, \lambda)$ デザイン $\boldsymbol{D}=(S, \boldsymbol{B})$ とその1点 $a\in S$ に対して，$S'=S\setminus\{a\}, \boldsymbol{B}'=\{B\setminus\{a\}\,|\,a\in B\in \boldsymbol{B}\}$ とおくと，明らかに $\boldsymbol{D}_a=(S', \boldsymbol{B}')$ は $(t-1)-(v-1, k-1, \lambda)$ デザインとなるが——$\boldsymbol{D}_a$ は $\boldsymbol{D}$ のブロックの中で a を含むものだけを考え，それから a をとり除いてえられる $\boldsymbol{D}$ の部分デザインともいうべきもの——，$\boldsymbol{D}_a$ を点 a に関する $\boldsymbol{D}$ の**内部構造**または**導来デザイン**という. 逆に，t-デザイン $\boldsymbol{D}$ に対し，$(t+1)$-デザイン D^* が存在して $\boldsymbol{D}$ が $\boldsymbol{D}^*$ の1点に関する内部構造になっているとき，$\boldsymbol{D}$ は**拡大可能**であるという. また，このような $\boldsymbol{D}^*$ を $\boldsymbol{D}$ の**拡大**という.

定義 3　$\boldsymbol{D}=(S, \boldsymbol{B}), \boldsymbol{D}'=(S', \boldsymbol{B}')$ を2つの t-デザインとする．全単射 $\sigma: S \longrightarrow S'$ が $\boldsymbol{B}^{\sigma}(=\{B^{\sigma}|B \in \boldsymbol{B}\})=\boldsymbol{B}'$ をみたすとき，即ち $\boldsymbol{D}$ のブロックを $\boldsymbol{D}'$ のブロックにうつすとき，σ を $\boldsymbol{D}$ から $\boldsymbol{D}'$ への**同型写像**という．このような同型写像が存在するとき，$\boldsymbol{D}$ と $\boldsymbol{D}'$ とは**同型**であるという．特に，$\boldsymbol{D}$ から $\boldsymbol{D}$ への同型写像，即ち S 上の置換 σ で $\boldsymbol{B}^{\sigma}=\boldsymbol{B}$ をみたすものを $\boldsymbol{D}$ の**自己同型**という．$\boldsymbol{D}$ の自己同型の全体は写像の積に関して群をなすが，それを $\boldsymbol{D}$ の（**全**）**自己同型群**といい，Aut $\boldsymbol{D}$ と書く．

さて，t-デザインに関する基本的な問題として次のようなものがある．

存在・構成の問題：どんな t, v, k, λ の値に対して t-(v, k, λ) デザインは存在するか？　実際にデザインを構成せよ．

一意性の問題：t-(v, k, λ) デザインが存在するとき，（どんな場合に，）それは（同型を度外視すれば）パラメーターのみによって一意に定まるか？　即ち，同じパラメーターをもつデザインは，（どんな場合に）同型か？

存在と一意性の問題は常に数学の基本問題であるが，上の2つの問題と関連して

拡大問題：どんなデザインが拡大可能か？　与えられたデザインの拡大を決定せよ．

上の3つの問題の一般的解決は難しいが，Steiner システムについてこの問題を少し述べてみる．

q（素数巾）個の元からなる有限体 F_q 上の affine 平面，射影平面の点全体を点集合とし，直線全体をブロック集合として自然に，それぞれ $2-(q^2, q, 1)$, $2-(q^2+q+1, q+1, 1)$ デザインという Steiner システムができる．これらのデザインをそれぞれ $\boldsymbol{AG}(2, q), \boldsymbol{PG}(2, q)$ で表すことにする．（一般に，$n \geqq 2$ を自然数として，$2-(n^2, n, 1), 2-(n^2+n+1, n+1, 1)$ デザインをそれぞれ**位数** n **の affine 平面**，**射影平面**という．）従って，Steiner システムは古典的な affine 平面・射影平面を一般化した概念であるといえよう．

$t \geqq 3$ なる Steiner システムでは，著名なものとして $5-(24, 8, 1), 4-(23, 7, 1), 3-(22, 6, 1)$; $5-(12, 6, 1), 4-(11, 5, 1)$ デザインがある．このようなパ

ラメーターをもったデザインは（同型を度外視して）それぞれ一意的に存在することを Witt [10] が証明したが，それらはそれぞれ $\boldsymbol{W}_{24}$, $\boldsymbol{W}_{23}$, $\boldsymbol{W}_{22}$；$\boldsymbol{W}_{12}$, $\boldsymbol{W}_{11}$ と表され，今日 **Witt システム**と呼ばれている．（ちなみに，デザインは存在しても一意に定まるとは限らない．たとえば位数 9 の射影平面で，$PG(2,9)$ と同型でないものが存在する．）Witt システムの自己同型群が Mathieu 群である：$M_{24}=\mathrm{Aut}\ \boldsymbol{W}_{24}$, $M_{23}=\mathrm{Aut}\ \boldsymbol{W}_{23}$, $M_{12}=\mathrm{Aut}\ \boldsymbol{W}_{12}$, $M_{11}=\mathrm{Aut}\ \boldsymbol{W}_{11}$ (M_{22} は $\mathrm{Aut}\ \boldsymbol{W}_{22}$ の指数 2 の部分群)．

Witt システムの発見の直接の動機は知らないが，Witt システムは射影平面・affine 平面の拡大問題を考えると，自然に，しかし例外的に登場する．

結果 2 (Hughes, 1965, たとえば [8], p. 46, p. 143). $PG(2,q)$ が拡大可能ならば，$q=2$ または 4.

結果 3 (Kantor [5], 1974). $AG(2,q)$ は常に拡大可能であるが，2 回拡大可能ならば，$q=2,3$ または 13.

上の結果はもっと一般的な形でパラメーター間の整除関係などを調べることによって証明されているが，前者では，$q=2$ のときは 1 回だけ，$q=4$ のときは 3 回だけ（も）拡大できて大きな Witt システムが得られる：

$$PG(2,4)\xrightarrow{\text{拡大}}\boldsymbol{W}_{22}\xrightarrow{\text{拡大}}\boldsymbol{W}_{23}\xrightarrow{\text{拡大}}\boldsymbol{W}_{24}\longrightarrow\text{拡大不可能}$$

後者では，$q=2$ のときは何回でも拡大できるが，それは $k=t$ という自明なデザインの無限列にすぎない．$q=13$ のときは拡大できても 2 回までであるが，不明のようである．$q=3$ のときは，3 回だけ拡大できて小さな Witt システムが得られる：

$$AG(2,3)\xrightarrow{\text{拡大}}\boldsymbol{W}_{10}\xrightarrow{\text{拡大}}\boldsymbol{W}_{11}\xrightarrow{\text{拡大}}\boldsymbol{W}_{12}\longrightarrow\text{拡大不可能}$$

同じように，特殊線型群 $PSL(n,q)$ の拡大問題などを考察すると，例外的に Mathieu 群が飛び出してくるが，省略する．

それにしてもなぜ，このような例外的な隙間があって，この隙間から（あのようなパラメーターや次数をもって）Witt システムや Mathieu 群というものが噴出してくるのであろうか？　このシステム・群の存在は有限群論の中の色々な不思議な例外的現象ともつながっていて，その根は広く深いように思われ

る．たとえば，v 次の対称群 S_v，交代群 A_v の自己同型群は $v=6$ のとき例外的な現象が起るが，このことと Mathieu 群の存在とは関係があるようである．逆に，Mathieu 群の中で見ると，群の奇妙な同型性などが自然に見えてくることもある．たとえば，A_6 と $PSL(2,9)$ の同型，A_8 と $PSL(4,2)$ の同型は，M_{24} の中で見るとどちらも，1つの部分群の2通りの姿（表現）であるということが分かる．

さて，t-デザインは群における次のような概念と関係がある．

定義 4　S を v 個の点の集合，G を S 上の置換群とする．S から t 個の元の順列 $(a_1, a_2, \cdots\cdots, a_t)$, $(b_1, b_2, \cdots\cdots, b_t)$〔$t$ 個の元からなる部分集合 $\{a_1, a_2, \cdots\cdots, a_t\}$, $\{b_1, b_2, \cdots\cdots, b_t\}$〕を2つ任意にとったとき，一方を他方にうつす G の元が存在するならば，即ち $a_i^\sigma=b_i (i=1, 2, \cdots\cdots, t)$〔$\{a_1^\sigma, a_2^\sigma, \cdots\cdots, a_t^\sigma\}=\{b_1, b_2, \cdots\cdots, b_t\}$〕をみたす $\sigma\in G$ が存在するならば，G は S 上 **t 重可移**〔**t 斉次**〕であるという．（定義から明らかに，t 重可移群は t 斉次である．）

v 次の対称群 S_v は v 重可移，v 次の交代群 A_v は $v-2$ 重可移であるが，t の大きな t 重可移または t 斉次置換群は高い対称性をもつ群といってよいであろう．Mathieu 群をそれぞれの Witt システムの点集合上の置換群とみると，M_{24}, M_{12} は5重可移，M_{23}, M_{11} は4重可移，M_{22} は3重可移であり，交代群以外の単純群で高い多重性をもつのは Mathieu 群だけであって，ここにも Mathieu 群の特異性が現われている．（実際，Mathieu はある種の多重可移群を決定しようとして，Mathieu 群を発見したようである．）

ところで，一般に，t 斉次置換群から t-デザインが自然に次のように構成される．

結果 4（たとえば Lane [7]）．v, k, t を一定の自然数で $v\geqq k\geqq t$ とし，S を v 個の点の集合，G を S 上の t 斉次置換群とする．S の k 個の点からなる部分集合 A を任意に1つとり，$A^G=\{A^\sigma | \sigma\in G\}$ とおくと，$\boldsymbol{D}=(S, A^G)$ は $t-(v, k, \lambda)$ デザインである．ここに

$$\lambda=|G:G_{(A)}|\binom{k}{t}\Big/\binom{v}{t}$$

($G_{(A)}=\{\sigma\in G|A^\sigma=A\}$) である.

どんなGとAに対して，$\boldsymbol{D}=(S, A^G)$ は興味あるデザインとなるのだろうか？ この問題の特別の場合を次の節で考える.

§3 ある無限系列の3-デザインと W_{12}, W_{24} の構成

本節では次の記号を用いる.

q: 素数巾 >7, $q\equiv-1 \pmod 4$.

F_q: q 個の元からなる有限体.

$\Omega=\Omega(q)=\{\infty\}\cup F_q$: F_q 上の射影直線.

$Q=\{x^2|x\in F_q\setminus\{0\}\}$.

$i\in F_q$ に対し

$Q_i=Q+i(=\{x+i|x\in Q\})$: Q の i による平行移動,

$U_i=\{i\}\cup Q_i=U_0+i(=\{x+i|x\in U_0\})$.

$G=PSL(2, q)=\{x\mapsto(ax+b)/(cx+d)|a, b, c, d\in F_q, ad-bc\in Q\}$.

$A, B\subset\Omega$ に対し

$A\triangle B=(A\setminus B)\cup(B\setminus A)$: A, B の対称差.

$\bar{A}=\Omega\setminus A=\Omega\triangle A$.

$q\equiv-1 \pmod 4$ よりGはΩ上3斉次の置換群となることが分かるが，これから自然に，§2の結果4を用いて3-デザインが構成される:

任意の $A\subset\Omega, |A|=k\geqq 3$ に対し，Ωを点集合，A^G をブロック集合として，(Ω, A^G) は $3-(q+1, k, \lambda)$ デザインとなる．ここに

$$\lambda=|G: G_{(A)}|\binom{k}{3}\Big/\binom{q+1}{3}$$

このデザイン (Ω, A^G) を以下 $\boldsymbol{D}(q, A)$ で表すことにする.

前節の最後に述べた

問題: どんなqと$A\subset\Omega$に対して，$\boldsymbol{D}(q, A)$ は興味あるデザインとなるか？

を考えよう．$A=U_0$ のときは，次の結果が得られる（証明略).

定理 1 (i) $\boldsymbol{D}(q, U_0)$ は $3-(q+1, (q+1)/2, (q+1)(q-3)/8)$ デザインで

あって，そのブロック集合は

$$U_0{}^G=\{U_i|i\in F_q\}\cup\{\bar{U}_i|i\in F_q\}$$
$$\cup\{U_i\triangle U_j(=\bar{U}_i\triangle\bar{U}_j)|i\neq j\in F_q\}$$
$$\cup\{U_i\triangle\bar{U}_j(=\bar{U}_i\triangle U_j=\overline{U_i\triangle U_j})|i\neq j\in F_q\}\qquad(\text{直和})$$

である．特に，$\boldsymbol{D}(q, U_0)$ が 4-デザインとなるのは $q=11$ のときのみで，実は

(ii)　(Beth[1])　$\boldsymbol{D}(11, U_0)$ は $5-(12, 6, 1)$ デザインである．

上の定理の (i) が示すように，$\boldsymbol{D}(q, U_0)$ のブロックは高々 2 つの $U_i, \bar{U}_i$ $(i\in F_q)$ の△による結合である．3つ以上の結合を考えるため，$U_i, \bar{U}_i(i\in F_q)$ の△による有限個の結合の全体を $\boldsymbol{U}(q)$ とすると，次のことが分かる．

(1)　$q\equiv-1(\mathrm{mod}\ 24)$ ならば，任意の $A\in\boldsymbol{U}(q), A\neq\phi, \Omega$ に対し，$8\leqq|A|\equiv 0(\mathrm{mod}\ 4)$ である．特に

(2)　$q=23$ のときは，$|A|=8, 12$ または 16 である．$|A|=8$ なる A として，たとえば

$$U_0\triangle U_1\triangle U_4=\{0, 4, 13, 14, 18, 19, 20, 22\}$$

がある．

定理 1 (ii) と同様な証明により次を得る．

定理 2　$\boldsymbol{D}(23, U_0\triangle U_1\triangle U_4)$ は $5-(24, 8, 1)$ デザインである．

以上の大半は既に知られているようであるが，こうしてある意味で統一的に——$\boldsymbol{D}(q, A)$ において適当な q と A をとることによって，あるいは $U_i, \bar{U}_i$ の対称差と群 $G=PSL(2, q)$ を通して—— 2 つの Witt システム $\boldsymbol{W}_{12}=\boldsymbol{D}(11, U_0)$, $\boldsymbol{W}_{24}=\boldsymbol{D}(23, U_0\triangle U_1\triangle U_4)$ を構成することができた．§2 の結果 2 と 3 の後でも見たように，大きなシステム $\boldsymbol{W}_{24}$, $\boldsymbol{W}_{23}$, $\boldsymbol{W}_{22}$ と小さなシステム $\boldsymbol{W}_{12}$, $\boldsymbol{W}_{11}$ とは，ある意味で異質であるといえる．従って，それらを統一的に扱おうとするのは無意味ではない．この統一化は次節で更に強められる．

§4　差型と代表ブロック

§3 の記号の他に，本節では次の記号を固定して用いる．

$$\boldsymbol{W}_{12}=\boldsymbol{D}(11,U_0),\ \boldsymbol{W}_{11}=(\boldsymbol{W}_{12})_\infty;$$

$$\boldsymbol{W}_{24}=\boldsymbol{D}(23,U_0\triangle U_1\triangle U_4),\ \boldsymbol{W}_{23}=(\boldsymbol{W}_{24})_\infty,\ \boldsymbol{W}_{22}=(\boldsymbol{W}_{23})_0.$$

(ここに $(\boldsymbol{W}_v)_a$ は，$\boldsymbol{W}_v$ の点 a に関する内部構造を表す.)

§2 の結果1より，これらのブロックの個数はそれぞれ，$132=12\cdot 11$, $66=6\cdot 11$; $759=33\cdot 23$, $253=11\cdot 23$, $77=11\cdot 7$ である.

これら Witt システムの全てのブロックを統一的かつ簡潔に記述するために，差型（差輪）または代表ブロックという概念を導入しよう．そのために以下，$q=11$ または 23 として，$\Omega(q)$ の元の間に

$$\infty<0<1<2<\cdots\cdots<q-1$$

という全順序を入れておくことにする.

定義 5　$\Omega(q)$ の部分集合

$$A=\{a_1,a_2,\cdots\cdots,a_k\}\quad(a_1<a_2<\cdots\cdots<a_k)$$

に対し，次のような $\tilde{A}$ を A の**差型**または**差輪**という:

$\infty<a_1$ なら

$$\begin{aligned}\tilde{A}&=(a_2-a_1,a_3-a_2,\cdots\cdots,a_k-a_{k-1},a_1-a_k)\\&=(a_3-a_2,a_4-a_3,\cdots\cdots,a_1-a_k,a_2-a_1)\\&=\cdots\cdots\\&=(a_1-a_k,a_2-a_1,\cdots\cdots,a_{k-1}-a_{k-2},a_k-a_{k-1})\end{aligned}$$

$\infty=a_1$ なら

$$\begin{aligned}\tilde{A}&=(\infty,a_3-a_2,a_4-a_3,\cdots\cdots,a_k-a_{k-1},a_2-a_k)\\&=(\infty,a_4-a_3,a_5-a_4,\cdots\cdots,a_2-a_k,a_3-a_2)\\&=\cdots\cdots\\&=(\infty,a_2-a_k,a_3-a_2,\cdots\cdots,a_{k-1}-a_{k-2},a_k-a_{k-1}).\end{aligned}$$

また，Witt システム $\boldsymbol{W}_v$ のブロックの差型の全体

$$\tilde{\boldsymbol{W}}_v=\{\tilde{B}\mid B:\ \boldsymbol{W}_v\ のブロック\}$$

を $\boldsymbol{W}_v$ の**差型**または**差輪**とよぶ．$d\in\tilde{\boldsymbol{W}}_v$ に対し，$\tilde{B}=d$ なる $\boldsymbol{W}_v$ のブロック B を1つ定めておき，それを差型 d に対応（属）する**代表ブロック**という.

定理 3　(i) $\boldsymbol{W}_v(v=12,11,24,23)$ の差型と代表ブロックは表1のとおりである.

(ii)　$\boldsymbol{W}_{12}$, $\boldsymbol{W}_{11}$($\boldsymbol{W}_{24}$, $\boldsymbol{W}_{23}$) のブロックは全て，代表ブロックを体 F_{11}(F_{23})

表 1

	差型		代表ブロック		個数
W_{12}	(∞,1,1,1,6,2)	(∞,1,1,2,3,4)	{∞,0,1,2,3,9}	{∞,0,1,2,4,7}	12
	(∞,1,1,3,1,5)	(∞,1,2,1,4,3)	{∞,0,1,2,5,6}	{∞,0,1,3,4,8}	
	(∞,1,2,2,2,4)	(∞,1,3,2,3,2)	{∞,0,1,3,5,7}	{∞,0,1,4,6,9}	
	(1,1,1,1,2,5)	(1,1,1,4,1,3)	{0,1,2,3,4,6}	{0,1,2,3,7,8}	
	(1,1,2,1,3,3)	(1,1,3,2,2,2)	{0,1,2,4,5,8}	{0,1,2,5,7,9}	
	(1,1,4,2,1,2)	(1,2,2,1,2,3)	{0,1,2,6,8,9}	{0,1,3,5,6,8}	
W_{11}	(1,1,1,6,2)	(1,1,2,3,4)	{0,1,2,3,9}	{0,1,2,4,7}	6
	(1,1,3,1,5)	(1,2,1,4,3)	{0,1,2,5,6}	{0,1,3,4,8}	
	(1,2,2,2,4)	(1,3,2,3,2)	{0,1,3,5,7}	{0,1,4,6,9}	
W_{24}	(∞,1,1,1,2,9,3,6)	(∞,1,1,4,1,12,2,2)	{∞,0,1,2,3,5,14,17}	{∞,0,1,2,6,7,19,21}	33
	(∞,1,1,6,3,1,6,5)	(∞,1,1,7,1,5,5,3)	{∞,0,1,2,8,11,12,18}	{∞,0,1,2,9,10,15,20}	
	(∞,1,2,1,7,8,1,3)	(∞,1,2,3,2,2,3,10)	{∞,0,1,3,4,11,19,20}	{∞,0,1,3,6,8,10,13}	
	(∞,1,2,4,2,7,2,5)	(∞,1,3,2,3,3,5,6)	{∞,0,1,3,7,9,16,18}	{∞,0,1,4,6,9,12,17}	
	(∞,1,3,6,4,4,3,2)	(∞,1,4,4,2,2,8,2)	{∞,0,1,4,10,14,18,21}	{∞,0,1,5,9,11,13,21}	
	(∞,1,4,5,2,4,3,4)		{∞,0,1,5,10,12,16,19}		
	(1,1,1,1,3,3,2,11)	(1,1,1,5,7,1,3,4)	{0,1,2,3,4,7,10,12}	{0,1,2,3,8,15,16,19}	
	(1,1,1,10,5,2,1,2)	(1,1,2,1,4,9,1,4)	{0,1,2,3,13,18,20,21}	{0,1,2,4,5,9,18,19}	
	(1,1,2,2,2,6,6,3)	(1,1,2,7,4,2,4,2)	{0,1,2,4,6,8,14,20}	{0,1,2,4,11,15,17,21}	
	(1,1,3,1,6,1,2,8)	(1,1,3,2,4,5,4,3)	{0,1,2,5,6,12,13,15}	{0,1,2,5,7,11,16,20}	
	(1,1,4,4,6,1,1,5)	(1,1,7,3,2,2,5,2)	{0,1,2,6,10,16,17,18}	{0,1,2,9,12,14,16,21}	
	(1,1,8,1,2,1,5,4)	(1,2,2,3,1,3,8,3)	{0,1,2,10,11,13,14,19}	{0,1,3,5,8,9,12,20}	
	(1,2,2,5,1,4,3,5)	(1,2,3,1,8,2,3,3)	{0,1,3,5,10,11,15,18}	{0,1,3,6,7,15,17,20}	
	(1,2,3,6,2,4,1,4)	(1,2,4,1,3,3,7,2)	{0,1,3,6,12,14,18,19}	{0,1,3,7,8,11,14,21}	
	(1,2,6,1,7,2,2,2)	(1,3,1,5,3,4,3,3)	{0,1,3,9,10,17,19,21}	{0,1,4,5,10,13,17,20}	
	(1,3,2,1,4,2,5,5)	(1,3,4,4,1,6,2,2)	{0,1,4,6,7,11,13,18}	{0,1,4,8,12,13,19,21}	
	(1,5,2,1,6,3,3,2)	(2,2,4,2,3,2,3,5)	{0,1,6,8,9,15,18,21}	{0,2,4,8,10,13,15,18}	
W_{23}	(1,1,1,2,9,3,6)	(1,1,4,1,12,2,2)	{0,1,2,3,5,14,17}	{0,1,2,6,7,19,21}	11
	(1,1,6,3,1,6,5)	(1,1,7,1,5,5,3)	{0,1,2,8,11,12,18}	{0,1,2,9,10,15,20}	
	(1,2,1,7,8,1,3)	(1,2,3,2,2,3,10)	{0,1,3,4,11,19,20}	{0,1,3,6,8,10,13}	
	(1,2,4,2,7,2,5)	(1,3,2,3,3,5,6)	{0,1,3,7,9,16,18}	{0,1,4,6,9,12,17}	
	(1,3,6,4,4,3,2)	(1,4,4,2,2,8,2)	{0,1,4,10,14,18,21}	{0,1,5,9,11,13,21}	
	(1,4,5,2,4,3,4)		{0,1,5,10,12,16,19}		

$W_{12}=D(11,\ U_0)$, $W_{11}=(W_{12})_\infty$; $W_{24}=D(23,\ U_0\triangle U_1\triangle U_4)$, $W_{23}=(W_{24})_\infty$.

の元で平行移動することによって得られる．（たとえば，W_{24} の $759=33\cdot 23$ 個の全ブロックは，33個の代表ブロックを F_{23} の元で平行移動して得られる．）

証明の概略．まず，W_{12} と W_{24} の差型を直接計算で出す．たとえば W_{24}

の場合,

$$U=U_0\triangle U_1\triangle U_4,\ G=PSL(2,23)\ni\tau:\ x\mapsto -1/x$$

とすると,直接計算によって

$$\begin{aligned}\boldsymbol{W}_{24}\ \text{のブロック集合}\ &=U^G\\ &=\{aU+b,\ a(U+b)^\tau+c\,|\,a\in Q;\ b,c\in F_{23}\},\\ \widetilde{\boldsymbol{W}}_{24}&=\{\widetilde{aU},\ \widetilde{aU^\tau},\ \widetilde{a(U+6)^\tau}\,|\,a\in Q\}\end{aligned}$$

を得る.この $\widetilde{\boldsymbol{W}}_{24}$ の元を具体的に書き表したのが表1における $\boldsymbol{W}_{24}$ の差型である.また,$\widetilde{\boldsymbol{W}}_{24}$ の表の中で∞を含むものは11個あり,それらから∞をとり除けば $\widetilde{\boldsymbol{W}}_{23}$ の表が得られる.次に容易に分かるように,B,C を $\boldsymbol{W}_v$ のブロックとするとき,$\tilde{B}=\tilde{C}$ であるための必要十分条件は $B=C+i$ なる $i\in F_q$ ($v=12,11$ のときは $q=11$, $v=24,23$ のときは $q=23$) が存在すること,即ち,B,C は F_q の元による平行移動で互いにうつれることである.このことに注意すれば,差型から代表ブロックと (ii) の主張が直ちに得られる. □

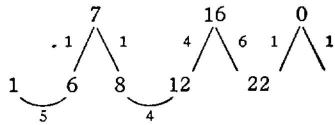
差型の利点あるいは応用について述べよう.

(1) 上の定理でみたように,差型あるいは代表ブロックは,Witt システム $\boldsymbol{W}_{12}$, $\boldsymbol{W}_{11}$, $\boldsymbol{W}_{24}$, $\boldsymbol{W}_{23}$ の全てのブロックを統一的・具体的に記述する簡単な方法を与えているといえる.($\boldsymbol{W}_{22}$ はやや異質である.$\boldsymbol{W}_{22}$ の差型は77個 ($\boldsymbol{W}_{22}$ のブロックの個数) もあって無意味であるが,$\boldsymbol{W}_{22}$ の全てのブロックも $\boldsymbol{W}_{23}$ の11個の代表ブロックを F_{23} の適当な7個の元で平行移動すれば得られる.)

(2) $\boldsymbol{W}_{12}$, $\boldsymbol{W}_{24}$ ($\boldsymbol{W}_{11}$, $\boldsymbol{W}_{23}$) の与えられた5 (4) 個の点に対し,それらを含むブロックはただ1つ定まるが,そのブロックを具体的に見つけるのはそれほどたやすいとはいえない.しかし,差型を用いるとすぐ見つけることができる.このことを $\boldsymbol{W}_{24}$ の場合について述べる.たとえば,与えられた5点を $A=\{1,6,8,12,22\}$ とすると,$\tilde{A}=(5,2,4,10,2)$ である.$\boldsymbol{W}_{24}$ の差型表から,その適当な部分和が $\tilde{A}$ であるようなものを探すと,ただ1つの差型

$$(\underbrace{1,1}_{2},4,\underbrace{4,6}_{10},\underbrace{1,1}_{2},5)$$

が見つかる．従って，求めるブロックは



即ち $\{0, 1, 6, 7, 8, 12, 16, 22\}$ である．

差型の利点・応用は他にもいくつかあるが省略し，$\boldsymbol{W}_{24}$，$\boldsymbol{W}_{23}$，$\boldsymbol{W}_{22}$ の一意性を示すのにも役立つことを次節で述べる．

§5　$\boldsymbol{W}_{24}$，$\boldsymbol{W}_{23}$，$\boldsymbol{W}_{22}$ の一意性

Witt システムの一意性の証明はいくつか知られているが，その殆どは射影平面・affine 平面の細かな性質や符号理論などを使っているようであり，またそのような知識を使っていなくても，システムを統一的に扱って証明しているとは言いがたいように思われる．ここでは，$\boldsymbol{W}_{24}$，$\boldsymbol{W}_{23}$，$\boldsymbol{W}_{22}$ の場合だけであるが，その一意性——全ての $5-(24, 8, 1)$, $4-(23, 7, 1)$, $3-(22, 6, 1)$ デザインはそれぞれ同型である——を，上のような知識を一切使わない単純で初等的な方法によって，統一的に証明できることを大まかに述べる．

規約：本節では，$\boldsymbol{W}_{24}$，$\boldsymbol{W}_{23}$，$\boldsymbol{W}_{22}$ をそれぞれ，任意の $5-(24, 8, 1)$, $4-(23, 7, 1)$, $3-(22, 6, 1)$ デザインとする．

我々の証明で使うのは，（背後では差型が重要な役割を演じているが，論理的には）次のようなブロックの交叉に関する性質（Block Intersection Property ＝BIP）のみである．

BIP：$\boldsymbol{W}_v$ の任意の異なるブロック　B, C に対し，

$$|B\cap C|=\begin{cases}0, 2 \text{ または } 4 & (v=24 \text{ のとき})\\ 1 \text{ または } 3 & (v=23 \text{ のとき})\\ 0 \text{ または } 2 & (v=22 \text{ のとき})\end{cases}$$

である．

この性質の証明は全く初等的で，$\boldsymbol{W}_v$ のパラメーターのみから容易に導くこ

とができる.

一般に，デザインの一意性を示すために，次の簡単な命題——点とブロックの命名による方法——が有効である.

命題 与えられたパラメーター t, v, k, λ をもつ任意の t-(v, k, λ) デザイン $\boldsymbol{D}$ に対し，その全ての点とブロックを命名するある定まった方法——正確に述べると，その方法に従えば，$\boldsymbol{D}$ の全ての点を $1, 2, \cdots\cdots, v$ と名づけることができ，$\boldsymbol{D}$ の各ブロックに属する点は全て $1, 2, \cdots\cdots, v$ で明示することができる——があれば，t-(v, k, λ) デザインは（存在するとしても）一意的である.

証明 $\boldsymbol{D}=(S, \boldsymbol{B}), \boldsymbol{D}'=(S', \boldsymbol{B}')$ を任意の 2 つの t-(v, k, λ) デザインとする. 仮定から，ある一定の命名法で，$\boldsymbol{D}$ と $\boldsymbol{D}'$ の全ての点に名前をつけ，全てのブロックを明示することができる. i と名づけられた S, S' の点そのものをそれぞれ a_i, a_i' ; $I=\{i_1, i_2, \cdots\cdots, i_k\}$ と表された $\boldsymbol{B}, \boldsymbol{B}'$ のブロックそのものをそれぞれ B_I, B_I' とする. $B_I=\{a_{i_1}, a_{i_2}, \cdots\cdots, a_{i_k}\}$, $B_I'=\{a_{i_1}', a_{i_2}', \cdots\cdots, a_{i_k}'\}$ であるから，全単射 $\sigma: S \longrightarrow S'$ を $a_i^\sigma=a_i'$ で定義すると，$B_I^\sigma=B_I'$ 従って $\boldsymbol{B}^\sigma=\boldsymbol{B}'$ となり，σ は $\boldsymbol{D}$ から $\boldsymbol{D}'$ への同型写像となっている. □

この命題に基づいて $\boldsymbol{W}_v$ の一意性を示すためには，$\boldsymbol{W}_v$ のパラメーターのみを用いてできる

（I） $\boldsymbol{W}_v$ の全ての点を命名する方法（点の命名法）と

（II） $\boldsymbol{W}_v$ の全てのブロックを明示する方法（全ブロックの書き上げ法）と

を提示すればよい. この（I）と（II）は，$v=24, 23, 22$ のときは同一の仕方で，殆ど同時に，BIP のみを用いて提示できるというのが我々の証明の方針である.（I）と（II）は関連していて，点の命名（I）をするとき，同時にいくつかのブロックも明示的に定まる（つまり，それらのブロックはどんな点からなるか具体的に表せる）のであるが，実はこれらのブロックが全てのブロックを生成（増殖）していくということを示すのが方法（II）である.

（I） **点の命名法**:

(i) 任意の $\boldsymbol{W}_{22}$ に対し，ある一定の方法に従って，全ての点に $1, 2, \cdots\cdots,$

22 という名前をつけることができ，同時に $\boldsymbol{B}_1$ (1 を含む 21 個のブロック) と，1 を含まないあるブロック A を明示することができる．

(ii)　任意の $\boldsymbol{W}_{23}$ に対し，ある一定の方法に従って，全ての点に 0, 1, 2, ……, 22 という名前をつけることができ，同時に $\boldsymbol{B}_{0,1}$(0, 1 を含む 21 個のブロック) と，$0 \in A \not\ni 1, 1 \in A' \not\ni 0$ なるブロック A, A' を明示することができる．

(iii)　任意の $\boldsymbol{W}_{21}$ に対し，ある一定の方法に従って，全ての点に ∞, 0, 1, 2, ……, 22 という名前をつけることができ，同時に $\boldsymbol{B}_{\infty,0,1}$(∞, 0, 1 を含む 21

表 2

	∞	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	BIP
B_1	○	○	○	○	○		○									○			○						
A'	●̲	×	●̲	●̲	●̲	●̲	×	○								×	○		×	○					×-B_1
B_2	●	●̲	●	●	×	●	×	(×)							○	×	(×)	○	×	(×)				○	×-B_1, A'
A	●	●	×	●	●	●	×	(×)		○	○				×	×	(×)	×	×	(×)			○	×	×-B_1, B_2, A'
B_3	●	●	●	×	●	●	×	(×)		×	×		○		×	×	(×)	×	×	(×)	○	○	×	×	×-B_1, B_2, A, A'
B_4	●	●	●	●	×	×	×	(■̲)	○̲	△	△		×		×	×	(□)	×	×	(□)	●̲	×	▲̲	×	×-B_1, B_2, B_3; △-A; □-A'
B_5	●	●	●	×	●	×	×	●	×	■̲	□̲	○̲	×		▲̲	×	(×)	△	×	(×)	×	×	×	△	×-B_1, B_3, B_4, A'; △-B_2; □-A
B_6	●	●	●	×	×	●	△	●	×	×	▼	×	×	○̲	×	△	(×)	×	▲̲	(×)	×	×	×	×	×-B_2, B_3, B_4, B_5, A'; △-B_1; ▼-A
B_7	●	●	●	●	×	×	×	×	×	●	×	×	▲̲	▼	×	×	(□̲)	×	×	(■̲)	×	△̲	×	×	×-B_1, B_2, B_4, B_5, A; ▼-B_6; △-B_3; □-A'
B_8	●	●	●	×	●	×	×	×	▼	×	●	×	×	×	×	×		▲̲	×	▼	×	×	×	△̲	×-B_1, B_3, B_5, B_6, A; △-B_2; ▼-B_4, B_7
B_9	●	●	●	×	×	●	▲̲	×	●	▼	×		×	×	×	△̲	(▼)	×	×	×	×	×	×	×	×-B_2, B_3, B_4, B_6, B_8; △-B_1; ▼-A, A'

B_1 以外の $\boldsymbol{W}_{24}$ (それぞれ $\boldsymbol{W}_{23}$, $\boldsymbol{W}_{22}$) の各ブロックは 5 (4, 3) 個の● ('∞', '∞, 0' を除く) で定められるものとし，そのブロックの残りの 3 点は ○, ▲, ■または▼て表されている．

＿はその点の命名が完了したことを表す．

×はそのブロックがその点を含まないことを表す．

( ) はそのブロックと A' との共通部分の影響を表す (A' は $\boldsymbol{W}_{22}$ では不要である)．

表 3

	∞	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	BIP
B_{10}	●	●	●	●	×	×	×	×	×	×	▼	▼	×	×	×	×	▼	×	×	×	×	▼	×	×	×-B_1, B_2, B_4, B_7
B_{11}	●	●	●	×	●	×	×	×	×	×	×	×	×	▼	×	×	▼	×	×	×	×	×	▼	▼	×-B_1, B_3, B_5, B_8
B_{12}	●	●	●	×	×	●	×	×	×	×	×	▼	×	×	×	▼	×	×	×	▼	×	×	▼	×	×-B_2, B_3, B_6, B_9
B_{13}	●	●	●	×	×	×	×	×	×	●	●	×	×	×	×	▼	×	×	×	×	▼	×	×	▼	×-A, B_5, B_6, B_7, B_8, B_9, B_{10}
B_{14}	●	●	●	×	×	×	×	×	×	●	×	×	×	×	×	×	×	▼	▼	×	×	▼	▼	×	×-B_5, B_7, B_9, B_{13}
B_{15}	●	●	●	×	×	×	▼	×	×	×	●	×	▼	×	▼	×	×	×	×	×	×	×	▼	×	×-B_6,B_8,B_{10}, B_{13}
B_{16}	●	●	●	×	×	×	●	●	×	×	×	×	×	×	×	×	×		×	▼	×	▼	×	▼	×-B_1, B_4, B_5, B_6, B_9, B_{15} ; ▼-B_3, B_7, B_{11}
B_{17}	●	●	●	×	×	×	●	×	×	×	×	▼	×	▼	×	×	×	▼	×	×	▼	×	×	×	×-B_1, B_9, B_{15}, B_{16}
B_{18}	●	●	●	×	×	×	×	●	×	×	×	×	▼	×	×	▼	▼	▼	×	×	×	×	×	×	×-B_4, B_5, B_6, B_{16}
B_{19}	●	●	●	×	×	×	×	×	▼	×	×	●	▼	×	×	×	×	×	▼	×	×	×	×	▼	×-B_5, B_{10}, B_{12}, B_{17}
B_{20}	●	●	●	×	×	×	×	×	●	×	×	×	×	▼	▼	▼	×	×	×	×	×	▼	×	×	×-B_4, B_8, B_9, B_{19}
B_{21}	●	●	●	×	×	×	×	×	×	×	×	×	×	×	●	×	▼	×	▼	▼	▼	×	×	×	×-B_2, B_5 B_{15}, B_{20}
A''	×	●	●	●	●	●	×	×	▼	×	×	▼	×	▼	×	×	×	×	×	×	×	×	×	×	×-A', A, B_1, B_2, B_3

W_{24} (それぞれ W_{23}, W_{22}) の各ブロックは 5 ないし 4 (4 ないし 3,3 ないし 2) 個の● ('∞', '∞, 0' を除く) を含むものとして定められ，そのブロックの残りの 3 ないし 4 個の点は▼で表されている．
×はそのブロックかその点を含まないことを表す．
(A'' は W_{24} のみに必要)

個のブロック) と，$\{\infty, 0\} \subset A \not\ni 1$, $\{1, \infty\} \subset A' \not\ni 0$, $\{0, 1\} \subset A'' \not\ni \infty$ をみたすブロック A, A', A'' を明示することができる．

証明の概略　証明は表 2, 3 にまとめられているが，3 つとも殆ど同様にできるので，(iii) の場合を簡単に述べる．W_{24} の任意のブロックを 1 つとって B_1

と呼び，B_1 に属する8個の点を全体として '$\infty, 0, 1, 2, 3, 5, 14, 17$' と名づける(全体としての命名で，個々にはまだ命名されない)．B_1 の中と外から任意に点を1つずつとり，それぞれ '∞', '4' と名づける．$B_1 \setminus \{\infty\}$ の任意の3点をとって，個々に '1', '2', '3' と名づけ，$A'=\langle\infty, 1, 2, 3, 4\rangle$ とおく．BIP より $B_1 \cap A'=\{\infty, 1, 2, 3\}$ であるが，$A' \setminus \{\infty, 1, 2, 3, 4\}$ の3点を全体として '6, 15, 18' と名づける．$B_1 \setminus \{\infty, 1, 2, 3\}=\{0, 5, 14, 17\}$ の任意の1点を '0' と名づけ，$B_2=\langle\infty, 0, 1, 2, 4\rangle$ とおく．BIP より $B_2 \cap B_1=\{\infty, 0, 1, 2\}$, $B_2 \cap A'=\{\infty, 1, 2, 4\}$ であるから，B_2 を定める5点以外の B_2 の残りの3点は $A' \cup B_1$ の外にあり，その3点を全体として '13, 16, 22' と名づける．$A=\langle\infty, 0, 2, 3, 4\rangle$, $B_3=\langle\infty, 0, 1, 3, 4\rangle$ とおき，上と同様に考えると，A, B_3 を定める5点以外の残りの3点は，それぞれ $A' \cup B_1 \cup B_2$, $A \cup A' \cup B_1 \cup B_2$ の外にあることが分かるので，全体として '8, 9, 21', '11, 19, 20' と名づける．$\{11, 19, 20\}$ の中の1点を任意にとって '19' と名づけ，$B_4=\langle\infty, 0, 1, 2, 19\rangle$ とおく．BIP より B_4 と B_1, B_2, B_3 との共通部分が分かるが，それから $B_4 \cap A=\{\infty, 0, 2, x\}$ (x は 8, 9, 21 のうちのどれか) ということが分かるので，x を '21' と名づける．以下ほぼ同じようにして，ブロック $B_5, \cdots\cdots, B_9$ が明示的に表され，$\boldsymbol{W}_{24}$ の全ての点に1つずつ名前をつける作業が完了する．以上のことは表2にまとめられている．この表のブロックから BIP のみを用いて，$B_{10}, \cdots\cdots, B_{21}, A''$ が次々に自動的に明示される(表3)．　□

注意　上の証明では，ブロック $B_1, \cdots\cdots, B_9, A, A'$ に属する点にどのような名前をつけるかが大事であるが，名づけ方は差型に基づいている．つまり，上の証明は論理的には BIP のみを用いてなされているが，背後では差型を使っている．

(II)　全ブロックの書き上げ法(ブロックの増殖法):

$\boldsymbol{W}_{24}$ の場合を簡単に述べる．(I) の (iii) で得られた $\infty, 0, 1$ を含む21個のブロックと3つのブロック A, A', A'' から残りの全ブロックが次々と増殖されていくことを証明するのであるが，以下例示するにとどめる．$\boldsymbol{W}_{24}$ の任意の5点，たとえば $\infty, 0, 2, 3, 6$ の定めるブロックを X として，X の残りの3点が

具体的に決まることを示す．$A_1=\langle\infty, 0, 1, 2, 3\rangle$, $A_2=\langle\infty, 0, 1, 2, 6\rangle$, $A_3=\langle\infty, 0, 1, 3, 6\rangle$，更に $A_4=\langle\infty, 0, 1, 6, 4\rangle$ とおくと，表2から $A_1=B_1$, $A_2=B_4$, $A_3=B_5$, $A_4=B_6$ となる．BIP によってXと A, A_1, A_2, A_3 との共通部分を考えると，$X\cap A_4$ は 12 を含まなければならないことが分かる．$A_5=\langle\infty, 0, 1, 12, 5\rangle$, $A_6=\langle\infty, 0, 1, 12, 14\rangle$ とおくと，表3から $A_5=B_{17}$, $A_6=B_{20}$ となる．上と同様にして，$X\cap A_5$ は 16 を，$X\cap A_6$ は 20 を含まなければならないことが分かり，結局Xの残りの3点は 12, 16, 20 である． □

§6 おわりに

(1) 上の一意性の証明で見たように，$\boldsymbol{W}_{22}$ では10個のブロック $B_1, \cdots\cdots, B_9, A$ が，$\boldsymbol{W}_{23}$, $\boldsymbol{W}_{24}$ では A' をつけ加えた11個のブロックが全ての点に名前をつけて，全ブロックを生成・増殖していく．その様子はなんともおもしろい――$B_1, \cdots\cdots, B_9$ だけでは増殖能力は弱いが，それらと異質な $A, (A')$ が加わると能力は一挙に高まり，全ブロックを増殖するのである．従って，これら 10; 11個のブロックを $\boldsymbol{W}_{22}$; $\boldsymbol{W}_{23}$, $\boldsymbol{W}_{24}$ の**命名ブロック**，**増殖ブロック**，**生成ブロック**，**基底ブロック**あるいは**決定ブロック**などと呼んでもよいであろう．

(2) 説明は省くが，上の一意性の証明は，(§3で述べた $PSL(2, 23)$ を用いる方法とは別に) $\boldsymbol{W}_{22}$, $\boldsymbol{W}_{23}$, $\boldsymbol{W}_{24}$ の構成・存在証明も同時に与えていることを注意しておく．

(3) $\boldsymbol{W}_{12}$, $\boldsymbol{W}_{11}$ では，BIP が $\boldsymbol{W}_{22}$, $\boldsymbol{W}_{23}$, $\boldsymbol{W}_{24}$ のようにきれいでないため，今のところ上のような仕方では，一意性の証明はできていない．

(4) これまでに見たように，差型という概念は，Witt システム (の全ブロック) を統一的・具体的に記述する簡単な方法を与え，$\boldsymbol{W}_{22}$, $\boldsymbol{W}_{23}$, $\boldsymbol{W}_{24}$ の (存在と) 一意性を示すのにも有効であって，Witt システムの透明化に幾分かは役立つと思われる．しかし，差型も Curtis の MOG [2] も，その正体が筆者にはまだよく分からない．差型に現われる数列はどのような規則で並んでいるのだろうか？ MOG や差型を決定または control している，より本質的な何かがあるのだろうか？

(5)　これまで，Witt システム $\boldsymbol{W}_v$, Mathieu 群 M_v の魅力の一端を述べてきたが，v の値はなぜ 11, 12, 22, 23, 24 であって，他の数ではないのだろうか？　ある観点から選ばれたこれらの数（特に 24）に特別深い意味があるだろうか？　あるとすれば，なぜだろうか？（別の観点から見れば別の数が重視され，それぞれの数がそれぞれの観点から意味のある存在となるであろうか？それとも，重要な視点あるいは種々の視点から見て特別に意味のある数があり，24 はそのような数の 1 つなのであろうか？）24 と 23, 12 とは一緒に登場することがあり，また 5−(24, 8, 1) デザイン $\boldsymbol{W}_{24}$ のように，24 とともに 8 という数もよく出てくる．これらの数の間に不思議なつながりがあって，豊饒な世界が展開されていくのだろうか？　‘24’ という数の奥深さと広がりを，山田 [11]，吉田 [12]，近藤 [6] などは興味深く，また夢多く展開している．ともあれ，各数は一様に存在しているのではなく，豊かな個性や色々な度合いの微妙なつながり・関係があって豊饒な世界を形成しており，「万物は数なり」という Pythagoras の世界観は今でも生きているといってもよいであろうか．

参考文献

[1]　T. Beth, Some remarks on D. R. Hughes' construction of M_{12} and its associated designs, in 'Finite geometries and designs', London Math. Soc. Lect. Note Ser. 49, 22—30, Camb. Univ. Press, 1981

[2]　R. T. Curtis, A new combinatorial approach to M_{24}, Math. Proc. Camb. Phil. Soc. 79 (1976), 25—42.

[3]　S. Iwasaki, An elementary and unified approach to the Mathieu-Witt systems, J. Math. Soc. Japan 40 (1988), 393—414.

[4]　———, 同 II : The uniqueness of $\boldsymbol{W}_{22}$, $\boldsymbol{W}_{23}$, $\boldsymbol{W}_{24}$, (submitted).

[5]　W. M. Kantor, Dimension and embedding theorems for geometric lattices, J. Comb. Th. (A), 17 (1974), 173—195.

[6]　近藤武，有限単純群の分類定理，数学セミナー 1990年4月号，27—31，日本評論社．

[7]　R. N. Lane, t-designs and t-ply homogeneous groups, J. Comb. Th. 10 (1971), 106—118.

[8]　永尾汎，群とデザイン，岩波，1974.

[9] E. Witt, Die 5-fach transitiven Gruppen von Mathieu, Abh. Math. Sem. Univ. Hamburg, 12 (1938), 256—264.

[10] ———, Über Steinersche Systeme, 同上, 265—275.

[11] 山田裕理, ある種のエータ積の乗法性について, 一橋大学研究年報, 自然科学研究 26(1987), 73—114.

[12] 吉田知行, 24 の不思議, 「Dynkin 数学」研究集会報告集, 1—28, 筑波大学, 1987,

(一橋大学教授)