デザイン覚書

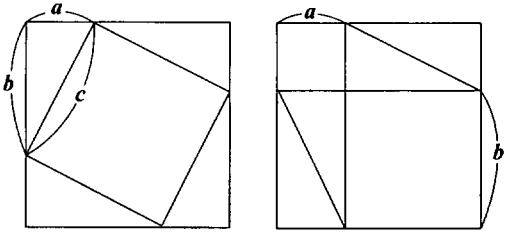
岩崎史郎

1 はじめに

デザイン（design）といえば，服飾などのことを連想し，数学を思い浮かべる人は少ないであろう．しかしこの小文では，数学におけるデザイン理論をごく簡単に紹介し，筆者が最近得た結果をも簡単に記すことにしたい．

Designは‘図案’とか‘設計’とか‘計画’などと訳されることが多いが，この小文におけるような意味では，通常‘**配置**’と訳される．集合の元が何らかの意味でうまく配置されると，不思議で魅力的な現象がしばしば生じる——たとえば，いろいろな生命現象は分子の特殊な配置・結びつきから生じるといえるであろうし，そもそも‘配偶者’というのは，大勢の男女の中から‘偶然に？　配置された者’という意味に解することもできよう．（もっとも辞典によれば，‘配’はそばにくっついた人＝つれあい，‘偶’は2で割り切れる偶数の偶で，対とか似た者どうしということらしく，配も偶も似通った意味のようであるが．）よい文章・詩には，的確に選ばれた言葉が的確に配置されている．日常生活において，配置の問題はいろいろとあろう——家・部屋の中で家具はどのように配置すれば過ごしやすいか；店では品物をどのように配置すれば，客が品物を選びやすく，売上げを伸ばすことができるだろうか等等．

中学・高校の数学から身近な例をとってみよう．たとえばピタゴラスの定理は図形の配置という面から証明することができる——1つの正方形の中に，4つの合同な直角三角形（直角をはさむ2辺の長さはa, bで，斜辺の長さは



c とする）の置き方・配置を左図から右図のように変えるだけで証明されたことになる．（正方形の中から 4 つの合同な直角三角形を取り除いた図形の面積は，左図では c^2，右図では a^2+b^2 で，両者は等しいから，$a^2+b^2=c^2$.）

$S=1+2+3+\cdots+99+100$ の値を求める場合も，私達は左から順に加えていくというような愚かなことはせず，通常は数を逆に並べ替えて（数の配置を変えて）$S=100+99+\cdots+2+1$ を作り，それをはじめの式に縦に加えて

$$2S = (1+100)+(2+99)+\cdots+(99+2)+(100+1) = 101\times 100,$$

$$\therefore S = 101\times 100/2 = 5050.$$

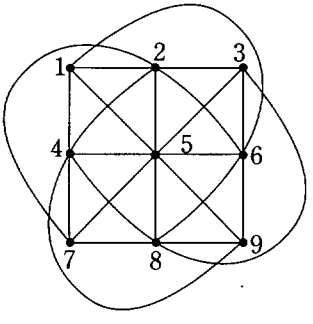
というようにやる．

では，次の問題はどうだろうか．

ある会社が守衛を何人か雇って，1 組 3 人ずつのチームで 2 時間交代の見回りを終日行いたいという．しかも次の条件を満たすようにするには，守衛を何人雇って，どのように配置すればよいか？

（i）　どの 2 人も 1 日 1 回だけ顔を合わせるようにチームを作る．

（ii）　どの人も 1 日 8 時間労働となるようにチームを作る．



まず，各チーム 2 時間交代であるから，終日（24 時間）では 24/2＝12 チーム作らなければならないが，結論を言うと，守衛は 9 人雇い，3 人ずつからなる 12 チームの編成を左図のようにすれば――9 人は数字 1, 2, …, 9 で表され，3 人からなる各チームは 3 つの数字を結んだ線で表されている――，上の条件 (i) と (ii) がともに満たされる．条件 (i) を

満たすことは，たとえば1と2（1と6）が顔を合わすチームは{1,2,3}（{1,6,8}）だけであることなどからわかる．条件（ii）を満たすことは，どの点も丁度4つのチームに含まれる（たとえば，1を含むチームは{1,2,3}, {1,4,7}, {1,5,9}, {1,6,8}）から，どの人も1日に2時間×4＝8時間見回りをすることからわかる．

このような配置の問題を，数学ではデザイン理論として一般にどのように扱っているかを簡単に述べ，筆者が最近得た結果をも紹介するのがこの小文の目的である．ここで主に用いるのは，足し算・引き算・掛け算・割り算だけの四則演算であるが，演算が行われる舞台は実数全体のような無限集合ではなく，有限個の元からなる有限体である．以下，q（qは素数べき）個の元からなる有限体を$GF(q)$で表す．有限体の知識を持ち合わせていない読者は，qが素数のときだけを考え，そのときは$GF(q)=\{0,1,2,\cdots,q-1\}$であって，その中で加減乗除が自然に自由にできるようになっていると思えばよい．（ただし，$GF(q)$の各数rは通常の整数そのものではなく，qで割ると余りがrとなるような任意の整数あるいはそのような整数全体を表す．したがってたとえば，$q+2=3q+2=-q+2=2$; $q=2q=0$; $q-1=-1,\cdots$）そしてこれらの数同士の加減乗は各数rを通常の整数と思って行ってよいが，その計算結果が通常の整数としては$0,1,2,\cdots,q-1$の中にない場合は，それをqで割った余りをとることにする．そうすると，$GF(q)$の中で加減乗除が自由にできる（たとえば，$q=3, GF(3)=\{0,1,2\}$では，$1+2=3=0, 2\cdot 2=4=1$であり，したがって$1\div 2=1/2=2$である）．以下では，ベクトル空間とか射影空間とか置換群などといった言葉も出てくるが，そのような概念に不慣れな人は適当な本（たとえば永尾［12］）で補うか，そのようなところは気にしないで読み流して頂きたい．ともかく有限体$GF(q)$を用いて，デザインという整然とした有限幾何（点全体が有限個で，各直線も有限個の点からなっているような幾何）を作る——いわば**加減乗除（だけ）で絵を描く**——のがねらいである．

2　定義，よく知られている事柄・例

この小文でいうデザインの数学的定義は次のとおりである．

定義1　t,v,k,λ は正の整数であって $v>k>t$ であるとし，2つの有限集合 Ω と $\boldsymbol{B}$ が次の条件を満たすものとする．

(1)　Ω は v 個の元からなる．（Ω の各元を**点**という．）

(2)　$\boldsymbol{B}$ の元はどれも，Ω の k-部分集合（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．）

(3)　Ω の t 個の任意の点に対して，それらを含むブロックの個数は，t 個の点の取り方によらず一定であって λ である．

このとき，Ω と $\boldsymbol{B}$ の組 $(\Omega,\boldsymbol{B})$ を t-(v,k,λ) **デザイン**，あるいは t,v,k,λ を**パラメーター**にもつ t-**デザイン**という．（デザインとよばれるのは，集合の元がブロックという部分集合の系にきれいに――どんな t 個の元に対しても上の条件を満たすようにきれいに，いわば対称度 t という正則性をもって――整然と配置されているという意味合いであろう．）

t-(v,k,λ) デザインというとき，その点の個数 $v:=|\Omega|$ は表に出ていてもブロックの個数 $b:=|\boldsymbol{B}|$ は表に出ていない．それは，容易に示される次のよく知られた命題から，b が t,v,k,λ で表されるからである．（以下に引用される命題や例，その証明について，その多くは永尾［12］等を見られたい．）

命題1　$(\Omega,\boldsymbol{B})$ が t-(v,k,λ) デザインであるとき，次が成り立つ．

(1)　$0\leq i\leq t$ なる任意の整数 i に対して，i 個の点を含むブロックの個数 λ_i は，i 個の点の取り方によらず一定で

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

で与えられる．特にブロックの個数 $b:=|\boldsymbol{B}|$ は

$$b=\lambda_0=\lambda\binom{v}{t}\Big/\binom{k}{t}=\lambda\frac{v(v-1)\cdots(v-t+1)}{k(k-1)\cdots(k-t+1)}.$$

(2)　$1\leq i\leq t$ なる任意の整数 i に対して，$(\Omega, \boldsymbol{B})$ は i-(v, k, λ_i) デザインである．簡単にいえば，t-デザインは $(t-1)$-, $(t-2)$-, …, 2-, 1- デザインでもある．

定義から自然に考えられるデザイン理論の基本課題の一つは

存在・構成の問題　どんなパラメーター t, v, k, λ の値に対して，t-(v, k, λ) デザインは存在するか？　興味深い t-(v, k, λ) デザインを実際に構成せよ．

命題1は証明も内容も簡単ではあるが，なかなか有効である．たとえば，デザインが存在するためのパラメーターをかなり規定する：命題1 (1) における λ_i は勿論整数であるから，t-(v, k, λ) デザインが存在するならば，パラメーター t, v, k, λ の間には少なくとも (1) のどの λ_i の右辺も整数となるような整除関係がある．したがって，ある λ_i の右辺が整数でないような t-(v, k, λ) デザインは存在しない．

前節の終りに述べた守衛の問題の解の一部（守衛の雇用人数は9人）も，命題1によって次のように得られる．守衛を v 人雇うとし，3人ずつの各チームをブロックと考え，ブロックの総数（1日の全チーム数）を b とすると，この問題は次のようなデザインの問題となる：条件 (i) を満たすような守衛の配置は，2-$(v, 3, 1)$ デザインで $b=12$ となるものを作ることであり，条件 (ii) を満たす——どの人も2時間交代で1日8時間労働というのは，どの人も1日 $8/2=4$ チームに加わること——ような守衛の配置は，1-$(v, 3, 4)$ デザインで $b=12$ となるものを作ることである．したがって命題1 (1) によって，(i) の場合は $12=1\cdot v(v-1)/3(3-1)$ から，(ii) の場合は $12=4\cdot v/3$ から v が求まり，どちらの場合も $v=9$ で，守衛は9人雇えばよいことがわかる．さらに次のこともわかる．条件 (i) を満たすような守衛の配置は 2-$(9, 3, 1)$ デザインであり，これは命題1から 1-$(9, 3, 4)$ デザインでもある

から，条件（ii）も満たしている．2-(9, 3, 1) デザインの具体的な作り方は前節の終りに述べた図のとおりであるが，これは次の例1のアフィン平面の1つである．

よく知られているデザインの代表的な例を以下いくつかあげる．

デザインの例.

（例1，2では，$n\geq 2$ で $1\leq i\leq n-1$ とする．）

例1　$AG(n,q)$ を有限体 $GF(q)$ 上の n 次元アフィン空間（すなわち $GF(q)$ 上の n 次元ベクトル空間 V の元全体），$\boldsymbol{B}_i$ を $AG(n,q)$ の i 次元部分空間（すなわち V の i 次元部分ベクトル空間を平行移動したもの）全体の集合とすると，その組 $\boldsymbol{AG}_i(n,q):=(AG(n,q),\boldsymbol{B}_i)$ は $2\text{-}(q^n,q^i,N_{i-1}(n-1,q))$ デザインである．ここに

$$N_r(m,q)=\frac{(q^m-1)(q^{m-1}-1)\cdots(q^{m-r+1}-1)}{(q^r-1)(q^{r-1}-1)\cdots(q-1)}$$

（$=GF(q)$ 上の m 次元ベクトル空間の r 次元部分ベクトル空間全体の個数）．特に $\boldsymbol{AG}_1(2,q)$ は $2\text{-}(q^2,q,1)$ デザインで，位数 q の**アフィン平面**とよばれる．$\boldsymbol{AG}_1(2,3)$ は 2-(9, 3, 1) デザインで，守衛問題の解を与えている．

例2　$PG(n,q)$ を有限体 $GF(q)$ 上の n 次元射影空間（すなわち $GF(q)$ 上の $n+1$ 次元ベクトル空間 V の1次元部分ベクトル空間全体の集合），$\boldsymbol{B}_i$ を $PG(n,q)$ の i 次元部分空間（すなわち V の $i+1$ 次元部分ベクトル空間に含まれる1次元部分ベクトル空間の集合）全体の集合とすると，その組 $\boldsymbol{PG}_i(n,q):=(PG(n,q),\boldsymbol{B}_i)$ は $2\text{-}\left(\frac{q^{n+1}-1}{q-1},\frac{q^{i+1}-1}{q-1},N_{i-1}(n-1,q)\right)$ デザインである．

特に，$\boldsymbol{PG}_1(n,q)$ は $2\text{-}\left(\frac{q^{n+1}-1}{q-1},q+1,1\right)$ デザイン，$\boldsymbol{PG}_1(2,q)$ は $2\text{-}(q^2+q+1,q+1,1)$ デザインで，$\boldsymbol{PG}_1(2,q)$ は位数 q の**射影平面**とよばれる．また，$\boldsymbol{PG}_{n-1}(n,q)$ は $2\text{-}\left(\frac{q^{n+1}-1}{q-1},\frac{q^n-1}{q-1},\frac{q^{n-1}-1}{q-1}\right)$ デザイン，$\boldsymbol{PG}_{n-1}(n,2)$ は $2\text{-}(2^{n+1}-1,2^n-1,2^{n-1}-1)$ デザインである．

上の例からわかるように，デザインはアフィン幾何や射影幾何などの古典

幾何の流れに沿った自然な概念であるといってよい．なお，上にあげた例は全て2-デザインであるが，2-デザインについての一般的な事実と例を少し述べておく．

命題2　**(Fisher の不等式)**

2-(v, k, λ) デザインでは常に，

$$b(\text{ブロックの個数}) \geq v(\text{点の個数})$$

が成り立つ．

上で特に等号 $b=v$ が成り立つ場合は，**対称的** 2-デザインとよばれる．(このとき命題1の記号を用いると，$\lambda_1=k, \lambda_2=\lambda$ であり，$\lambda_1-\lambda_2=k-\lambda$ をこのデザインの位数という．) 対称的2-デザインの例として，例2の $\boldsymbol{PG}_1(2, q), \boldsymbol{PG}_{n-1}(n, q)$ などがあるが，典型例として，2-$(q^2+q+1, q+1, 1)$ デザイン $\boldsymbol{PG}_1(2, q)$ を一般化した次のような（一般の）射影平面とアダマール2-デザインがある．

定義2　n を $n\geq 2$ なる整数として，

(1)　2-$(n^2+n+1, n+1, 1)$ デザインを位数 n の**射影平面**という．

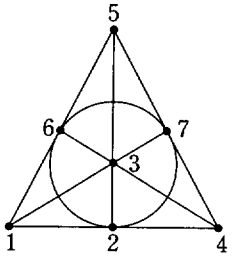
(2)　2-$(4n-1, 2n-1, n-1)$ デザインを位数 n の**アダマール(Hadamard) 2-デザイン**という．

(この2つのデザインは，命題1より b, λ_1 がわかり，どちらも位数が $\lambda_1-\lambda_2=n$ の対称的2-デザインである．)

例3　次はアダマール2-デザインである．

(1)　$\boldsymbol{PG}_{n-1}(n, 2)$

(2)　q は素数べきで，$q-1=2m$ (m は奇数) であるとし，有限体 $GF(q)$ の0でない平方数の全体を $Q:=(GF(q)\backslash\{0\})^2$ とする．$GF(q)$ を点集合とし，Q を平行移動したものをブロックとして作った組 $(GF(q), \{Q+i \mid i\in$



$GF(q)\}$) は 2-$(q,(q-1)/2,(q-3)/4)$ デザインである．このデザインを **Paley デザイン**という．

射影平面とアダマール 2-デザインが注目される理由の一つは，次のことが成り立つからである：位数 n の対称的 2-(v,k,λ) デザインにおいては，$v\geq k+2$ ならば，

$$4n-1\leq v\leq n^2+n+1.$$

ここで等号が成り立つのは，右等号の場合は射影平面，左等号の場合はアダマール 2-デザイン（およびそれらの補構造とよばれるもの）である．特に左右の等号が同時に成り立つのは，$n=2$ の場合で対称的 2-(7, 3, 1) デザイン——位数 2 の射影平面 $\boldsymbol{PG}_1(2,2)$——である．このデザインは最も有名な有限幾何の一つで，上のように図示される．（7 点の作る幾何で，各ブロックは 3 点からなり，直線ともよばれる．この図は，[3] のような有限幾何関係の本の表紙に象徴的に描かれていることがある．）7 つの点は $\{1,2,\cdots,7\}$ で表され，各ブロック（＝直線）は 3 点を結んだ線で表されている．すなわち，直線は全部で 7 つあって，$\{1,2,4\}$, $\{2,3,5\}$, $\{3,4,6\}$, $\{4,5,7\}$, $\{5,6,1\}$, $\{6,7,2\}$, $\{7,1,3\}$（見かけ上 $\{6,7,2\}$ は円，他は直線）である．この図から，このデザイン＝射影平面 $\boldsymbol{PG}_1(2,2)$ においては任意の 2 直線は必ず 1 点で交わり，平行線が存在しないことが見てとれる．したがってこれは，最も簡単な非ユークリッド幾何のモデルになっている．なお，ここでは詳しく述べるゆとりがないが，この図あるいは射影平面 $\boldsymbol{PG}_1(2,2)$ を適当に補うと誤り訂正符号というもののもっとも簡単なモデルができる．誤り訂正符号というのは，通信の途中で発生した誤り——たとえば，火星・木星・土星などの宇宙探査機から送られてくるデータは途中でいろいろな障害のために，地上で受信する時は発信時のものと違っていることがよく起るが，そのような誤りを見つけ，正しく訂正するものである．実は，有限体 $GF(q)$ はこのような符号理論をはじめ応用面でも非常に活躍している．今の例でいえば，宇宙探査

機は惑星のようすを普通のカメラで写すわけにはいかないから，映像の情報は有限体を用いた数値情報として符号化されて送信され，地上で受信された情報は誤り訂正符号によって誤りを正しく訂正され，画像処理技術によって普通の写真になるのである．

なお上では，不等式 '$4n-1 \leq v \leq n^2+n+1$' における等号の場合を述べたが，中間の場合：$4n-1 < v < n^2+n+1$ の対称的 2-デザインでも興味深い例がある．たとえば，後述の W_{24} から作られる対称的 2-$(176, 50, 14)$ デザインは，その自己同型群が Higman-Sims の単純群であることがわかり，注目される（Lander [11]）．

t-デザインに関する一般的な注目すべき結果としては，次のこと——任意の t に対して，t-デザインが存在する——が知られている：

命題 3　（Teirlinck [14]）t は任意の正整数とし，$v \geq t+1$ であって $v-t$ が $(t+1)!^{(2t+1)}$ で割れれば，t-$(v, t+1, (t+1)!^{(2t+1)})$ デザインが存在する．

これは非常に興味深い結果であるが，惜しむらくは $\lambda=(t+1)!^{(2t+1)}$ の値が大きすぎることである（任意の t に対して，λ の値が小さい t-デザインの存在証明が望まれる）．

λ の値が最も小さいとき，すなわち $\lambda=1$ のときは特に注目され，

定義 3　t-$(v, k, 1)$ デザインを**シュタイナー・システム**（Steiner system）という．

これは，t 個の点を通る（含む）ブロックはただ一つである幾何であるから，2 点を通る直線はただ一つであるという通常の幾何の自然な一般化になっている．因みに数学史（たとえば，カジョリ [10]，高木 [13]）によれば，Steiner（1796-1863）は誠に異色な数学者であったようである——スイスの貧しい農家に生まれ，14 歳まで教育を受けず，一字も書くことができなかったが，18 歳のとき Pestalozzi の学校に入り，数学に興味を持ち始めた．

この学校を出てからベルリンに赴き，学校教師や家庭教師（Humboldt家の家庭教師をしたのは，その後の幸運につながった）をしながら，数学の研究を続けた．彼はAbelとともに，その頃Crelleが発刊した有名な数学雑誌の有力な寄稿者として高く評価され，ついに彼のためにベルリン大学に幾何学の講座が創設されるに至り，終生その職にあった．経歴だけでなく，研究・教育の仕方も異色のようであった——直観力に秀でた彼は，しだいに図を描かずに幾何学が研究できるようになり，幾何学の講義のときも図を描かなかったので聴講者を面くらわせたようである．

シュタイナー・システムの例.

(1)　2-$(n^2+n+1, n+1, 1)$ デザイン，すなわち射影平面.

(2)　2-$(n^2, n, 1)$ デザイン，すなわち**アフィン平面.**

$t \geq 3$ の有名な例として，1938年Wittによって構成された

(3)　**ヴィット（Witt）・システム**または**マシュー（Mathieu）・デザイン**とよばれる次の5つのデザイン：

$$3\text{-}(22, 6, 1), 4\text{-}(23, 7, 1), 5\text{-}(24, 8, 1); 4\text{-}(11, 5, 1), 5\text{-}(12, 6, 1).$$

これらはそれぞれ $W_{22}, W_{23}, W_{24}; W_{11}, W_{12}$ と表される．これらがマシュー・デザインともよばれるのは，それらがマシュー群という対応する5つの単純群の作用する幾何学的場になっているからである．

近年構成された $t=5$ の例として，

(4)　Denniston [5] 等による

5-(28, 7, 1) デザインや5-$(v, 6, 1)$ デザイン（$v=24, 48, 72, 84, 108, 132, 168$）.

実はこれまでに知られている $t=5$ のシュタイナー・システム，すなわち5-$(v, k, 1)$ デザインの v の値は全て，$v=q+1$（q は素数べきで，$q+1$ は4の倍数）という形をしている．なお，$t \geq 6$ なるシュタイナー・システムは知られていない．

上の例 (3) で述べたヴィット・システムとマシュー群は色々な意味で注

目され，我々を魅了してやまない．それらは近年の散在型単純群を構成する際にも本質的に用いられ，特異な不思議さを持って色々な所に現れることなどから，その不思議なありようの根源を解明することは，有限群論・有限幾何の大きな課題の一つであると思われる．その正体をいくらかでも解明するために，たとえば，Curtis は [4] で MOG＝Miracle Octad Generator という文字通り魔法のような概念を，私も [6] で‘差型’あるいは‘代表ブロック’という概念を導入した（[7]）．

t-デザインを構成するにはいろいろな方法があるが，強力な一つとして t 斉次な置換群を用いる簡単な方法がある．

定義 4　v, t は正の整数であって $v \geq t$ とする．Ω を v 個の元からなる集合とし，G を Ω 上の置換群とする．Ω の任意の 2 つの t-部分集合（t 個の元からなる部分集合）$\{a_1, a_2, \cdots, a_t\}, \{b_1, b_2, \cdots, b_t\}$ に対し，一方を他方に移す G の元 σ が存在するとき，すなわち $\{a_1^\sigma, a_2^\sigma, \cdots, a_t^\sigma\} = \{b_1, b_2, \cdots, b_t\}$ なる $\sigma \in G$ が存在するとき，G は Ω 上 **t 斉次**であるという．

v 次の対称群 S_v は v 斉次，v 次の交代群 A_v は $v-2$ 斉次であるが，t の値が大きな t 斉次置換群は対称性の高い群といってよいであろう．

一般に，t 斉次置換群から t-デザインが次のように自然に簡単に構成される．

命題 4　**（t 斉次置換群 → t-デザイン）**

t, v, k は正の整数であって $v > k > t$ であるとし，Ω を v 個の元からなる集合，G を Ω 上の t 斉次置換群とする．Ω の k-部分集合 A を任意に 1 つとり，それを G の元全体で動かしてできる集合を $A^G = \{A^\sigma \mid \sigma \in G\}$ とすると，組 (Ω, A^G) は t-(v, k, λ) デザインである．ただし

$$\lambda = |G : G_A| \binom{k}{t} \Big/ \binom{v}{t}, \qquad G_A = \{\sigma \in G \mid A^\sigma = A\} : G \text{ における } A \text{ の固定部分群}$$

である.

この簡単な原理から自然に考えられる問題は：

Ω 上のどんな t 斉次置換群 G と k-部分集合 A に対して，(Ω, A^G) は興味深いデザインとなるだろうか？

命題4の方法による t-デザインの構成問題は，G の部分群 G_A を決める問題に帰着するから，G の部分群が全てわかっている場合は，群論の問題としては面白いものではない．しかし，デザインの問題としては面白いものと思われる．なぜなら，G が簡単でありふれた群（G の部分群も全てわかっている）であっても，A をうまくとると，（興味ある）新しいデザイン (Ω, A^G) が得られることがあるからである．このようにして最近得られたいくつかの新しいデザインを次節で述べる.

3　ある無限系列の2-デザインと3-デザインの構成

以下，q は奇素数べきで，$GF(q)$ を q 個の元からなる有限体とし，Ω を $GF(q)$ 上の射影直線とする：$\Omega = \{\infty\} \cup GF(q)$.

G として Ω 上に自然に作用する一次分数変換群

$$PGL(2,q) := \{x \mapsto (ax+b)/(cx+d) \mid a,b,c,d \in GF(q)\,;\, ad-bc \neq 0\}$$

または特殊一次分数変換群

$$PSL(2,q) := \{x \mapsto (ax+b)/(cx+d) \mid a,b,c,d \in GF(q)\,;\, ad-bc \in Q\}$$

をとる．ここで，Q は $GF(q)$ の0でない平方数の全体である：

$$Q := \{x^2 \mid x \neq 0 \in GF(q)\}.$$

Ω の任意の部分集合 A（ただし $|A|>3$ または2）に対して

$$\tilde{\boldsymbol{D}}(q,A) := (\Omega, A^{PGL(2,q)})$$

$$\boldsymbol{D}(q,A) := (\Omega, A^{PSL(2,q)})$$

とおく．$PGL(2,q)$ は Ω 上の3斉次置換群であるから，命題4によって $\tilde{\boldsymbol{D}}(q,A)$ は3-デザインである．また，$PSL(2,q)$ は Ω 上に

$q-1=2m$（m は奇数）のときは3斉次に，

$q-1=2^e m$ ($e\geq 2, m$ は奇数) のときは2斉次に
作用することがわかるから，命題4より $\boldsymbol{D}(q, A)$ はそれぞれ3-デザインまたは2-デザインとなる.

問題 Ω のどのような部分集合 A (と q) に対して，$\tilde{\boldsymbol{D}}(q, A)$ または $\boldsymbol{D}(q, A)$ は興味あるデザインとなるか.

$q-1=2m$ (m は奇数) のときは，$A=\{\infty\}\cup Q$ にとると，次の結果が得られる.

結果I ([6]) $q-1=2m$ (m は奇数) で $q>7$ のとき，$\boldsymbol{D}(q, \{\infty\}\cup Q)$ は $3\text{-}(q+1, (q+1)/2, (q+1)(q-3)/8)$ デザインである. そしてこのデザインのブロックは全て具体的に記述することができる.

この証明は，単純群 $PSL(2, q)$ の部分群が全てわかっているから難しくない.

このデザインは次の意味で興味深いものと思われる.

(i) 先の例3で述べたPaleyデザインに1点 $\{\infty\}$ を加えて，それをある意味で拡大した形のデザインとなっている (ただし，Paleyデザインの通常の意味での拡大——その定義は省く——ではない)：実際，$G=PSL(2, q)$ とおくと，$\boldsymbol{D}(q, \{\infty\}\cup Q)$ の点集合は $\Omega=\{\infty\}\cup GF(q)$，ブロック集合は $(\{\infty\}\cup Q)^G$ であるが，Paleyデザインの点集合は $GF(q)$，ブロック集合は $\{Q+i \mid i\in GF(q)\}=Q^{G_\infty}$ である (ここに，$G_\infty=\{\sigma\in G \mid \infty^\sigma=\infty\}=\{x\mapsto ax+b \mid a\in Q, b\in GF(q)\}$: G における ∞ の固定部分群).

(ii) $\boldsymbol{D}(q, \{\infty\}\cup Q)$ が4-デザインとなるのは $q=11$ のときで，$\boldsymbol{D}(11, \{\infty\}\cup Q)$ は実は $5\text{-}(12, 6, 1)$ デザイン $\boldsymbol{W}_{12}$ である. したがって，$\boldsymbol{D}(q, \{\infty\}\cup Q)$ は $\boldsymbol{W}_{12}$ を含む無限系列の3-デザインである. (因みに，AssmusとKey [1] は任意の整数 $m\geq 3$ に対して，$3\text{-}(22, 6, 1)$ デザイン $\boldsymbol{W}_{22}$ を含む無

限系列の興味深い 3-$((4^m+2)/3, 6, 1)$ デザインを構成した.）

(iii)　$q=23$ のとき，A として $\boldsymbol{D}(23, \{\infty\}\cup Q)$ のブロックの形を少し変えた8個の元からなる集合をとると，$\boldsymbol{D}(23, A)$ は 5-$(24, 8, 1)$ デザイン $\boldsymbol{W}_{24}$ になる.

このように A（と q）を適当にうまくとれば，$\boldsymbol{D}(q, A)$ は興味深いデザインになっていると思われる.

次に，$q-1=2^e m$（$e\geq 2, m$ は奇数）の場合を考える．上の結果Iでは $A=\{\infty\}\cup Q=\{\infty\}\cup(GF(q)\backslash\{0\})^2$ にとったから，その続きとして今度の場合自然に考えられるのは A が $\{\infty\}\cup(GF(q)\backslash\{0\})^{2^i}$ という形をしているときであろう．次の結果はこのような流れのなかで得られたものである.

結果II　([8], [9])　$q-1=2^e m$（$e\geq 2, m$ は奇数）とし，各 $i, 1\leq i\leq e$ に対し，

$$E_i=\{\infty\}\cup(GF(q)\backslash\{0\})^{2^i}, \qquad k=1+(q-1)/2^i$$

とおくと，例外を除き（例外の記述は略す）

$\tilde{\boldsymbol{D}}(q, E_i)$ は 3-$(q+1, k, k\cdot(k-2))$ デザイン，

$\boldsymbol{D}(q, E_i)$ は 2-$(q+1, k, k\cdot(q-1)/2)$ デザインである.

上のデザイン $\tilde{\boldsymbol{D}}(q, E_i)$，$\boldsymbol{D}(q, E_i)$ が興味深いものであるかどうかわからないが，これまでに得られているデザインの表には見当たらない——たとえば，パラメーターが $\tilde{\boldsymbol{D}}(29, E_1)$，$\tilde{\boldsymbol{D}}(29, E_2)$，$\boldsymbol{D}(29, E_2)$ と同じ値のデザインの存在が [2] の表では空白になっている——から，新しい無限クラスのデザインと思われる．こうして結果I・IIからわかるように，A として $\Omega=\{\infty\}\cup GF(q)$ の部分集合を適当にとり，それを一次分数（加減乗除の最も簡単な形）変換で動かすだけでいろいろなデザインが得られる.

なお，上の結果I，IIは T. Meixner 氏のおかげで次のような形に一般化できた（[9]）.

結果 III ([9]) q は素数べきとし，$d>1$ を $q-1$ の任意の約数とする．有限体 $GF(q)$ の 0 以外の元全体 $GF(q)\backslash\{0\}$ は巡回乗法群をなすが，その位数 d の部分群を U とし，$A=\{\infty\}\cup U$ とおく．このとき，$PGL(2,q), PSL(2,q)$ における A の固定部分群が決まり，3-デザイン $\tilde{\boldsymbol{D}}(q,A)$ と 2-デザイン $\boldsymbol{D}(q,A)$ のパラメーターも決まる．

次に

問題 結果 II における 2-デザイン $\boldsymbol{D}(q,E_i)$ は 3-デザインになりうるか？そうなるのはどんな場合か？

という問題を考える．$\boldsymbol{D}(q,E_i)$ が 3-デザインになりうるのは，命題 1 のパラメーター間の整除関係から $i=e$ の場合に限ることがすぐわかる．しかしその場合でも，$\boldsymbol{D}(q,E_e)$ は 3-デザインになるときとそうでないときがある．たとえば，$\boldsymbol{D}(29,E_2)$ は 3-デザインになるが，$\boldsymbol{D}(37,E_2)$ はそうならないことが確かめられる．これは考えているうちにわかってきたのであるが，単に群の問題ではなく，整数論とも関係する微妙な問題で，解決するには有限体のかなり詳しい性質を知る必要が起きてきた．

以下，有限体 $GF(q)$ の 0 以外の元全体を $F:=GF(q)\backslash\{0\}$ とし，これまでのようにその平方数の全体を $Q:=F^2$ とし，非平方数の全体を $N:=F\backslash Q$ とする．F は巡回乗法群であるから，その生成元の 1 つを α として，$\{\infty,0,1\}$, $\{\infty,0,\alpha\}$ を含む $\boldsymbol{D}(q,E_e)$ のブロックの個数をそれぞれ λ_0,λ_1 とすると，$\boldsymbol{D}(q,E_e)$ が 3-デザインになるのは $\lambda_0=\lambda_1$ の場合に限ることが容易にわかる．ところがこの λ_0,λ_1 の値を計算するのに，$GF(q)$ のある部分集合が $GF(q)$ の平方数・非平方数をどのくらい含むか知る必要があり，特に

$$q_0:=|(F^{2^e}-1)\cap Q|,\qquad n_0:=|(F^{2^e}-1)\cap N|$$

の値についての情報が必要である．

$m=5$ または 7 のときは次の結果が得られた．

結果 IV ([8]) $q-1=2^e m$ $(e\geq 2)$ で，$m=5$ または 7 とする．

(1)　$q_0\neq 0$ かつ $n_0\neq 0 \implies \lambda_0=\lambda_1$.

(2)　$m=5$ で，$q_0\neq 0$ かつ $n_0\neq 0 \Longrightarrow \boldsymbol{D}(q, E_e)$ は 3-$(q+1, 6, 12)$ デザイン.

(3)　$m=7$ で，$q_0\neq 0$ かつ $n_0\neq 0 \Longrightarrow \boldsymbol{D}(q, E_e)$ は 3-$(q+1, 8, 24)$ デザイン.

(4)　$m=5$ のとき

$q_0\neq 0$ かつ $n_0\neq 0 \iff 5$ は $GF(q)$ の4乗数ではない.

具体的にはたとえば

q	29	41	113	449	641
$q-1$	$2^2\cdot 7$	$2^3\cdot 5$	$2^4\cdot 7$	$2^6\cdot 7$	$2^7\cdot 5$

においては，実際確かに $q_0\neq 0$ かつ $n_0\neq 0$ であるから，対応する $\boldsymbol{D}(q, E_e)$ は3-デザインになる．特に $\boldsymbol{D}(29, E_2)$ は 3-$(30, 8, 24)$ デザインで，[2] の表の1つの空白を埋める．なお $q=37$，$q-1=2^2\cdot 9$ のときは，$q_0\neq 0$ かつ $n_0\neq 0$ であるが，$\lambda_0\neq\lambda_1$ であるから，$\boldsymbol{D}(37, E_2)$ は3-デザインではない.

なお結果IVの (2)，(3) で，6，12；8，24という数が出てくるが，これらの数はヴィット・システム $\boldsymbol{W}_{12}$, $\boldsymbol{W}_{24}$ のパラメーターにも出てきて注目されており，なぜそうあちこちにひょっこり顔を出すのですか？　と訊きたい思いにかられる.

さて，上の考察から自然に次の問題が出てくる.

問題　'$q_0\neq 0$ かつ $n_0\neq 0$' はどんな場合に成り立つか？　言い換えると，$q-1=2^e m$ ($e\geq 2, m$ は奇数) である有限体 $GF(q)$ において，0以外の 2^e 乗元を1だけ平行移動した全体 $F^{2^e}-1$（これは m 個の元からなる）に，平方数と非平方数が極端に片寄らずに分布するのはどんな場合か？

明らかに，$F\supset F^2=Q\supset F^{2^2}\supset\cdots\supset F^{2^e}$ であるから

$$(Q-1)\cap Q\supset (F^{2^2}-1)\cap Q\supset\cdots\supset (F^{2^e}-1)\cap Q$$

$$(Q-1)\cap N\supset (F^{2^2}-1)\cap N\supset\cdots\supset (F^{2^e}-1)\cap N.$$

q が素数なら，整数論における平方剰余の相互律などをうまく使うと

$|(Q-1)\cap Q|=(q-1)/4-1$,　　$|(Q-1)\cap N|=(q-1)/4$　や

$(F^{2^2}-1)\cap Q \neq \phi$ $(m\geq 5)$, すなわち

上の2つの集合系列の左側の大きな集合は空集合ϕではないということは何とか導けるが, どのような場合に右側の一番小さな集合も空集合ϕではないのか? というのが今の問題である. この問題は, 次のようにも表される: 方程式

$$x^{2^e}-1=y^2, \qquad x^{2^e}-1=\alpha y^2$$

のいずれも, 有限体$GF(q)$において解$x\neq 0$, $y\neq 0$を持つのはどのような場合か?

上の問題に関して, 久保田富雄先生からいくつかの御親切なコメントを戴いた. 特にmが大きいとき, "$m\geq 2^e+2$の場合は, $q_0\neq 0$かつ$n_0\neq 0$である" ということの証明をお送り戴いた. その証明はJacobi和を巧妙に用いた実に見事なもので, 証明の一つのあるべき姿をかいま見る思いであった (先生のお話では, このような証明のしかたはGaussが既に行っていた節があるとのことである). しかし残念なら, 結果IVで問題としているのは$m=5,7$のようにmが小さい場合である.

$m=5$のとき, この問題は結果IV(4)からもわかるように, 有限体$GF(q)$において与えられた元が4乗数 ($GF(q)$の元xによってx^4と書ける数) であるかどうかをいかに判定するかという問題とも自然にかかわってくる. この4乗数判定問題は, Gauss, Eisensteinによって既に著しい結果が得られているということも久保田先生に教えて頂いた. その結果によると, たとえば$q=40961$, $q-1=2^{13}\cdot 5$の場合は, 5は$GF(q)$において4乗数であることがわかり, したがって結果IV(4)より, $q_0=0$または$n_0=0$である. この問題は, Jacobi和などともつながったり, さらに有限体$GF(q)$におけるn乗数判定問題, 類体論という整数論の深い理論ともつながったりするためか, 久保田先生の他, 伊藤昇, 白谷克己, 中原徹, 山田美枝子等の諸先生にも関心を寄せて頂いたり, お教え頂いた. この場を借りて厚く御礼申し上げたい.

4　おわりに

前節の結果IIの後で述べたように，有限体 $GF(q)$ に無限遠点∞を加えた射影直線 $\Omega=\{\infty\}\cup GF(q)$ の部分集合 A を適当にとり，それを一次分数（加減乗除の最も簡単な形）変換で動かすだけでいろいろなデザインを得たが，（無限遠点∞を含めた）足し算・引き算・掛け算・割り算という最も初等的・素朴な演算だけでこのような世界が描かれることに，改めて（的確な場における）四則演算の持つ威力といったものを感じ驚かされる．そのような驚きは，双曲的非ユークリッド幾何のモデルが複素平面上の円の内部や上半平面という場の上に一次分数変換群を作用させて得られること――もっともこのモデルをきちんと議論するためには，四則演算だけでなく，何を直線と考えるかということや，積分のような極限操作も必要であるが――や一次分数変換群で不変な保型関数のことなども思い出すと，いっそう深まっていく．

そして前節の終りで述べたように，加減乗除（だけ）で作られた結果IIにおける2-デザインが3-デザインになりうるかどうかきめ細かく調べようとして，自然に整数論の深い理論につながっていってしまったことにも，数学における地下水のようなつながりを感じないわけにはいかない．

また有限体 $GF(q)$ は，2節の対称的2-$(7, 3, 1)$ デザイン＝射影平面 $\boldsymbol{PG}_1(2, 2)$ のところでちょっと触れたように，符号理論などの応用面でも重要な役割を演じているが，これらのことも思い合わせると，加減乗除の織り成す世界の豊富さに感じ入るばかりである．

参考文献

[1] E. F. Assmus, Jr. and J. D. Key, On an finite class of Steiner systems with $t=3$ and $k=6$, J. Comb. Theory, Ser. A 42 (1986), 55-60.

[2] Y. M. Chee, C. J. Colbourn and D. L. Kreher, Simple t-designs with $v\leq 30$, ARS Comb. 29 (1990), 193-258.

[3] C. J. Colbourn and J. H. Dinitz (eds.), The CRC handbook of combinato-

rial designs, CRC Press, 1996.

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

[5] R. H. F. Denniston, Some new 5-designs, Bull. London Math. Soc. 8 (1976), 263-267.

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

[7] ———, Witt システム覚書, 一橋論叢第 104 巻第 3 号 (1990), 1-19, 日本評論社.

[8] ———, Infinite families of 2-and 3-designs with parameters $v=p+1$, $k=(p-1)/2^i+1$, where p odd prime, $2^e \top (p-1), e\geq 2, 1\leq i\leq e$, J. Comb. Designs 5 (1997), 95-110.

[9] ———and T. Meixner, A remark on the action of $PGL(2, q)$ and $PSL(2, q)$ on the projective line, Hokkaido Math. J. 26 (1997), 203-209.

[10] カジョリ, 小倉金之助補訳, 初等数学史 (1970 年に共立全書として, 現在は共立出版社から復刻).

[11] E. S. Lander, Symmetric designs : an algebraic approach, London Math. Soc. Lect. Note Ser. 74 (1983), Cambridge Univ. Press.

[12] 永尾汎, 群とデザイン, 岩波, 1974.

[13] 高木貞治, 近世数学史談 (1933 年に第 1 版. 現在は岩波文庫または共立出版社から復刻).

[14] L. Teirlinck, Non-trivial t-designs without repeated blocks exist for all t, Disc. Math. 65 (1987), 301-311.

(一橋大学教授)