魔円陣と有限幾何

秋山 茂樹

1　魔円陣

魔円陣を説明するには実例を見るのが一番分かりやすい。図 1 のように 5 つの数字 1, 3, 10, 2, 5 が輪になっているとしよう。

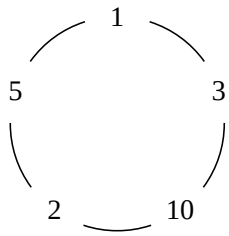

図 1: 大きさ 5 の魔円陣

すると面白いことに、この輪の連続する数の和により 1 から 21 までの数を全て無駄なく表すことができる。

$$1,\ 2,\ 3,\ 1+3,\ 5,\ 5+1,\ 2+5,\ 2+5+1,\ 5+1+3,\ 10,\ 2+5+1+3,$$
$$10+2,\ 3+10,\ 1+3+10,\ 3+10+2,\ 1+3+10+2,\ 10+2+5,$$
$$10+2+5+1,\ 5+1+3+10,\ 3+10+2+5,\ 1+3+10+2+5$$

一般に n 個の自然数で輪を作るとき、連続する整数をとり出すための切れ目の入れ方は $n(n-1)$ あり、切らないで全ての数を使うことも考えると n^2-n+1 個の整数が作れる。この輪が大きさ n の魔円陣であるとは、1 から n^2-n+1 の自然数を全て無駄なく作れるようにしたものの事である。上の例は大きさ 5 の魔円陣[1]である。先を読む前に、この程度の大きさの魔円陣を自力でいろいろ作ってみることを勧めたい。手でやってみれば大きさ $3,4,5,6$ ぐらいは作れる（かもしれない）。さて大きさ 7 はどうだろう。いろいろやってもなかなか出来ない。実は大きさ 7 の魔円陣は存在しないのである。

近代代数学の始祖のガロアは若くして決闘で死んでしまうが、勝ち目のない決闘に持ち込まされた理由として出所不明のうわさ話がある ([5])。パリ近

[1]以下の話の都合で $n \geq 3$ とする。二つの数字 $1,2$ の組も大きさ 2 の魔円陣となるが、これは面白くない。

郊のある池の周囲に 307 本の木が植えられている。彼は 18 人の兵士に各自木を選んで、どの二人の兵士間の木で計った間隔を、全て異なるようにせよと命じた。これは 18 の大きさの魔円陣を作る問題である。それが余りに難しいので不興を買ったのが決闘の一因というのである。話が出来すぎていて、かなり怪しい。しかしこのような妙な噂があるくらいだから、問題自体はかなり以前から知られているものなのだろう。

私自身もかなり以前に故岩堀長慶先生の集中講義で出題されたのを聞いたことがある。しかし不真面目な聴衆であったので面白さが分からなかった。そのため、すっかり忘れていた。ごく最近になって同じ問題を知人に問われ、初めて真面目に考える機会を得た。しかし、なんだか手のつけようもない。同僚の宮本雅彦先生に立ち話で聞いたところ、宮本先生も当時、岩堀先生に聞き、なんと自分で解いたというのである。頂いた一ページに満たない解答を見て驚いた。初等的な問題に見えるが、数学の未解決問題と繋がっている実に奥深い問題だったのである。本稿ではこの解答をもとに分かりやすく解説を試みることにしよう。かなり以前に本誌で扱われたことがあるが詳しい解説はないようである ([7, 8])。

本稿の目標をはっきりさせよう。魔円陣が作れる大きさは

$$3, 4, 5, 6, 8, 9, 10, 12, 14, 17, 18, 20, 24, 26, \ldots$$

という数列[2]になる。読者のみなさんは規則を見つけることができるだろうか。数字を見て類推できる人は整数ファンであろう。これが本稿の目標である未解決問題である。

予想 1. 魔円陣の大きさは素数の冪に 1 を加えたものである。

先に結論だけを述べると大きさが素数の冪プラス 1 の場合は有限射影平面を用いる方法により具体的に魔円陣を構成できる。それ以外の構成方法があるかはいまだに分からない。5 章を参考にしてほしい。

この原稿を読んでコメントをくださった宮本雅彦先生、藤田尚昌先生に深く感謝いたします。

2 有限射影平面

ユークリッド幾何学は 5 つの公理で記述されることがよく知られている。「直線 L とその上にない点 p があるとき、p を通り L と交わらない直線がただ一つ引ける」という平行線公準を他のものに置き換えた幾何学は非ユークリッド幾何学と呼ばれており様々な例が知られている。数学セミナーの読者の多くは聞いたことがあるだろう。たとえば射影幾何学は、大雑把にいえば

[2] 全ての場合を計算機で調べることが可能なのは、現在でも大きさ 20 位までで、それ以降は場合の数が多すぎ難しいらしい。[8] に工夫されたプログラムがある。

ユークリッド幾何学に無限遠点を加えることにより平行線を排除し、二直線は必ず交わるようにしたものである。このようにすることで面倒な例外の記述はなくなり理論体系が分かりやすくなる。

有限幾何とはこのような公理を満たす対象を有限集合で実現したものである。魔円陣の記述に必要なものは有限射影平面で、その公理はとても単純である。有限集合 P とその部分集合の族 E を考え P の元の事を点、E の元のことを直線と呼ぶ。直線 L が点 p を通るとは p が L に含まれることとし、直線の交点は集合としての共通部分を意味する。(P, E) が次の公理を満たすとき有限射影平面であるという。

1. 二つの点を通る直線はただ一つ存在する。
2. 二つの直線はただ一つの点で交わる。
3. 非自明な四角形が存在する。

最後の公理はつまらない場合を排除するためのものである。非自明な四角形とは、P の四点で、どの三点も同一直線上にないもののことをいう。

例 1.

$$\begin{aligned} P &= \{1,2,3,4,5,6,7\}, \\ E &= \{\{1,3,7\},\{2,4,1\},\{3,5,2\},\{4,6,3\},\{5,7,4\},\{6,1,5\},\{7,2,6\}\} \end{aligned}$$

を考えよう。二直線は必ず一点で交わっていること、二つの点を通る直線がただ一つ存在することを確かめてほしい。この有限射影平面は図 *2* のように図示でき *Fano* 平面と呼ばれている。非常に高い対称性を持つことで有名である。

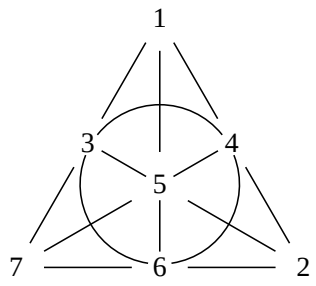

図 2: Fano 平面

上記の三つの公理から自然数 n が存在して、直線および点の個数は共に $n^2 + n + 1$ で各点を通る直線の個数および各直線上の点の個数はどちらも

$n+1$ でなければならないことが容易に導ける。この数 n の事を有限射影平面の位数という。

有限射影平面を構成するもっとも容易な方法は、ユークリッド空間から作られる射影平面の方法を模倣することである。

実射影平面は原点を通る直線を同一の「点」、原点を通る平面のことを「直線」であると考えて構成する。線形代数の言葉では一次元部分空間を「点」、二次元部分空間を「直線」とするのだ。視点が原点にあることを想像しよう。このとき原点を通る直線は点に見え、原点を通る平面は直線に見える。このような「射影」を実体と考えるのが射影幾何である。地球から星を眺めると同方向にある星は一点に見えるし黄道は一直線に見える。このような気分で考えれば射影幾何を想像するのは難しくない。

有限幾何を構成するには、係数を実数から有限の数体系に置き換える必要がある。つまり実数体を有限体に置き換えれば有限射影平面が出来上がる。有限体の簡単な例として $\{0,1\}$ だけからなる二元体を考える。足し算は

$$0+0=0,\ 0+1=1,\ 1+0=1,\ 1+1=0$$

掛け算は

$$0\times 0=0,\ 0\times 1=0,\ 1\times 0=0,\ 1\times 1=1$$

とする。0 を偶数、1 を奇数を思えば分かりやすい。二元体上の射影平面とは定数倍がこの場合 1 しかないから結局 (x,y,z) が全て零でないような元の全体で $2^3-1=7$ 点ある。二点 $(x_1,y_1,z_1),(x_2,y_2,z_2)$ を通る「直線」とは、

$$\{u(x_1,y_1,z_1)+v(x_2,y_2,z_2)\ |u,v\in\{0,1\}\}$$

という集合であり、

$$\{(x_1,y_1,z_1),(x_2,y_2,z_2),(x_1+x_2,y_1+y_2,z_1+z_2)\}$$

の三点である。このようにして 7 本の直線が作られる。これが例 1 の有限射影平面である。よく理解するため (x,y,z) と $\{1,2,3,4,5,6,7\}$ の一対一対応を作ってみるとよい。この場合、位数 $n=2$ の射影平面ができたことになる。点と直線の数は $1+2+2^2=7$ となっている。有限射影平面の位数という言葉は、この有限体の位数から来ているものと思う。4 章でも述べるが有限体の位数は素数の冪となることがよく知られている。

興味深いことに有限射影平面はこのような有限体から作られるものだけではない。射影幾何が有限体から作られたものであることはデザルグ性というある種の作図の性質で特徴づけられるが、有限射影平面の中にはデザルグ性を満たさないものが存在することが知られている。（非デザルグ平面）それにも関わらず、今まで発見された有限射影平面の位数は全て素数の冪である。そこで次の予想がなされている。

予想 2. 有限射影平面の位数は素数の冪である。

これは有限射影幾何の基本問題で、これを中心として現在も様々な研究が進んでいる。一般的な結果として Bruck-Ryser の定理がある。有限射影平面の位数が 4 で割って 1 または 2 余るならば、二つの整数の平方の和で表せる。このことより位数 $6, 14$ の有限射影平面は存在しない。この定理の証明は、初等整数論をうまく用いるもので面白い ([2, 1])。予想 2 は直交するラテン方陣の個数の関する予想で言い換えることができ ([6])、位数 6 の有限射影平面が存在しないことは、オイラーの 36 士官の問題に解がないことからも導かれる。位数 10 の射影平面が存在するかは長期にわたって未解決であったが、1989 年に存在しないことの計算機援用証明 (Lam-Thiel-Swiercz) が見つかった。位数 $12, 15, 18, 20$ の射影平面が存在するかどうかは現時点で知られていない。

3 巡回平面

予想 1, 2 の形を眺め、点の個数などを比べると魔円陣の問題は有限射影幾何と関連があるのではないかと想像ができるだろう。実は魔円陣と巡回平面という特別な有限射影平面が一対一に対応するのである。

位数 n の巡回平面とは、位数 n^2+n+1 の巡回群を推移的な自己同型群としてもつ有限射影平面のことである。言葉が難しいが内容は簡単である。7 で割った余りを $\{1, 2, 3, 4, 5, 6, 7\}$ で表す[3]とき前章の例 1 の E は

$$E = \{\{1+k, 3+k, 7+k\} \mid k = 1, 2, 3, 4, 5, 6, 7\}$$

とも書ける。つまり

$$\begin{aligned} \{1+1, 3+1, 7+1\} &= \{2, 4, 1\}, \\ \{1+2, 3+2, 7+2\} &= \{3, 5, 2\}, \\ &\vdots \end{aligned}$$

のように 7 で割ったあまりで直線が巡回的に出てきている。このような番号付けが可能な有限射影平面を巡回平面というのである。

次の定理が私が宮本先生に頂いた解答である。専門家以外にはほとんど知られていないと思う。次の 4 章にあるような魔円陣構成に関連した記述は文献に散見されるが、このような切り口の文献[4]は見つからなかった。詳しく証明を書いておこう。

[3]魔円陣との関連の記述を簡単にするため、余り 0 の場合にはその代わりに 7 と書くことにする。

[4]Singer[9] に類似の記述がみられるが、完全差集合の形で書いており巡回平面についての記述はない。

定理 1. 大きさ $n+1$ の魔円陣と位数 n の巡回平面は一対一[5]に対応する。

証明。 大きさ n+1 の魔円陣から位数 n の巡回平面を構成しよう。$(a_0, a_1, a_2, \ldots, a_n)$ を魔円陣に現れる自然数列とする。以下、上の説明のように n^2+n+1 で割った余りを $\{1, 2, \ldots, n^2+n+1\}$ の完全剰余系で考えることにする。つまり足したり引いたりしたあと n^2+n+1 で割った余りを考えるのだが、0 のときは n^2+n+1 とする。このとき

$$\begin{aligned} P &= \{1, 2, \ldots, n^2+n+1\}, \\ E &= \left\{\{a_0+k, a_0+a_1+k, \ldots, a_0+a_1+\cdots+a_n+k\} \mid k \in \{1, 2, \ldots, n^2+n+1\}\right\} \end{aligned}$$

とする。このとき (P, E) は有限射影平面であることを確かめよう。以下では $a_{n+1} = a_0, a_{n+2} = a_1, \ldots$ のように a_i のインデックス i は $n+1$ で割った剰余と考える。二点 $x, y \in \{1, 2, \ldots, n^2+n+1\}$ について $x < y$ とすれば魔円陣なので $y-x = a_i + a_{i+1} + \cdots + a_j$ と書ける。$k = x - (a_0 + a_1 + \cdots + a_{i-1})$ と置くと

$$x = a_0 + a_1 + \cdots + a_i + k, \quad y = a_0 + a_1 + \cdots + a_j + k \tag{1}$$

となるので x, y を含む E の元が見つかった。i と j の間に 0 が含まれる場合には (1) の表示の中に a_0 が二回現れるが $a_0 + a_1 + \cdots + a_n = n^2+n+1$ であるので問題は生じない。従って二点を通る直線は必ず存在する。逆に (1) という表示があったとすると魔円陣の定義より $y-x$ を計算すれば i, j は一意にさだまり k もきまるので、二点を通る直線ははただ一つである。交わらない二直線があったとする。各直線上には $n+1$ の点があるのでそれらを結ぶ直線全体を考えると異なる直線が $(n+1)^2$ できてしまい E の個数より多くなってしまう。したがって二直線は必ず交わる。二点を通る直線が唯一なので二直線の交点もただ一つである。各直線には三点以上の点があるので非自明な四角形があることもわかる。

逆に位数 n の巡回平面 (P, E) から大きさ $n+1$ の魔円陣を作ろう。

$$E = \left\{\{b_0+k, b_1+k, \ldots, b_n+k\} \mid k \in \{1, 2, \ldots, n^2+n+1\}\right\}$$

とかけるが大小の順に並べ直し $b_0 < b_1 < \cdots < b_n$ が成立するとしよう。このとき $b_1 - b_0, b_2 - b_1, \ldots, b_n - b_{n-1}, b_0 - b_n$ のように隣合う数の差を順にならべた輪を作ると魔円陣となることを示す。ここで最後の $b_0 - b_n$ は負であるが n^2+n+1 で割った剰余系を考えるので、自然数として書けば

$$b_1 - b_0, \ldots, b_n - b_{n-1}, b_0 - b_n + n^2 + n + 1$$

となる。したがって、まず全ての数の和は n^2+n+1 であり、この円陣の連続する数の和は n^2+n+1 以下の自然数である。従って 1 から n^2+n の自

[5] ここでは同型を考慮しない。5 章参照のこと

然数が魔円陣の連続する数の和で書けることを n^2+n+1 での剰余で考えて示せばよい。(P,E) は射影平面なので 1 以上 n^2+n までの自然数 k について直線

$$\{b_0, b_1, \ldots, b_n\}$$

と

$$\{b_0+k, b_1+k, \ldots, b_n+k\}$$

は一点で交わる。つまり $b_i = b_j + k$ が成り立つ i, j が存在する。$j > i$ ならば j を順に減らして

$$k = b_j - b_i = (b_j - b_{j-1}) + \cdots + (b_{i+1} - b_i),$$

$i > j$ ならば b_k のインデックス k を $n+1$ で割った剰余と考えて i を順に増加させていくと、途中に b_0 を挟んで

$$k = b_j - b_i = (b_{i+1} - b_i) + (b_{i+2} - b_{i+1}) + \cdots + (b_j - b_{j-1})$$

という表示が得られる。したがって、1 から n^2+n+1 の自然数は円陣の連続する数の和で表せる。1 章で述べたようにサイズ $n+1$ の円陣では最大で $(n+1)^2-(n+1)+1 = n^2+n+1$ 個の数しか作れないので、このような連続する数の和としての表現はただ一通りである。これで証明は終了した。

4 原始根

定理 1 により魔円陣を構成する問題は巡回平面を求める問題に帰着されたが、有限体から構成される有限射影平面は巡回平面なのだろうか。この問題は Singer [9] によって解かれた。

以下を理解するには有限体の基礎的な知識が必要である。本稿ではこれにページを割けないが、多くの代数学の初歩の教科書に載っている事柄である。ご存知の読者も多いと思う、

まずそもそも体とは、加減乗除の出来る対象を抽象化したものである。有限体とは有限集合で体の公理を満たすときにいう。任意の有限体 F に対して、素数 p (標数) が定まり、F は p^e 個の元からなる。有限体は p^e が同じなら同型となるのでこれを F_{p^e} とか、$GF(p^e)$ とも書く。有限体の事をガロア体と呼ぶこともある。F_{p^e} の零を除く p^e-1 個の元は積に関して巡回群をなす。この巡回群の生成元のことを原始根という。有限体から構成される有限射影平面は、F_{p^e} 上の三次元ベクトル空間において一次元部分空間の全体を「点」、二次元部分空間の全体を「直線」とみなしたものであった。F_{p^e} の三次拡大で得られる有限体 $F_{p^{3e}}$ を F_{p^e} 上の三次元ベクトル空間とみなせば、$F_{p^{3e}}$ の原始根の積が自然な自己同型を引き起こす。原始根の位数は $p^{3e}-1$ であるが、各「点」は F_{p^e} の零でない定数倍しても同一なので引き起こされ

る自己同型の位数は $(p^{3e}-1)/(p^e-1) = p^{2e}+p^e+1$ となる。つまり原始根の積の作用により、位数 $p^{2e}+p^e+1$ の有限射影平面の自己同型が導かれる。したがって巡回平面となる。具体的に計算してみよう。

例 2. $p=2, e=1$ としてみると F_{2^3} の元は F_2 上の多項式の全体を x^3+x^2+1 で割った[6]余りとして出てくる二次の多項式の集合となる。原始根として $g = x+1$ がとれることが分かり、順に冪を取っていくと

$$g = x+1, g^2 = x^2+1, g^3 = x, g^4 = x^2+x, g^5 = x^2+x+1, g^6 = x^2, g^7 = 1$$

となる。1 と x で張られる部分空間 $\{1, x, x+1\}$ が射影平面の直線である。この g の冪をみると $\{7,3,1\}$ となる。大小の順に並べて $\{1,3,7\}$、これに g を書けると $\{2,4,1\}, \{3,5,2\}, \ldots$ という順で例 *1* で述べた巡回平面が再構成できる。これによって大きさ 3 の魔円陣 $(3-1, 7-3, 1-7) = (2,4,1)$ が出来た。

大きさが 3 の魔円陣ではありがたみを感じないかもしれない。

例 3. $p=17, e=1$ とする。F_{17^3} は F_{17} 係数の多項式の全体を x^3+3x^2+1 で割った余りの集合である。原始根はここでも $x+1$ でよく、同じように 1, x で生成される射影直線を原始根の冪で表すと

$$\{1, 3, 27, 42, 46, 62, 74, 99, 137, 187, 201, 218, 223, 231, 241, 252, 301, 307\}$$

となる。原始根の位数は 17^3-1 まであるが、射影直線は $17^2+17+1 = 307$ しかない。実際 $(x+1)^{307} = 14$ となってこれは射影平面では 1 と同じ点であり、ここで循環する。したがって大きさ 18 の魔円陣として

$$(2, 24, 15, 4, 16, 12, 25, 38, 50, 14, 17, 5, 8, 10, 11, 49, 6, 1)$$

が出来た。これが *1* 章のガロア *(?)* の問題の一つの解である。確かにこの答えは簡単には見つかりそうにない。

5 関連する未解決問題

前節までの記述により魔円陣の問題は巡回平面の分類問題に帰着し、特に大きさが素数冪プラス 1 の場合には有限体の原始根を用いて魔円陣が簡単に構成されることが分かった。

では巡回平面は位数が素数冪のときしか存在しないのだろうか。また、素数冪のときには、有限体から作られるもの以外のものはあるのだろうか。実はどちらも未解決である。

[6] F_2 係数の既約多項式ならなんでもよい

有限射影平面一般と比べると巡回平面のほうが分かっていることは多い。最新の結果によると、位数 $2,000,000,000$ までの巡回平面の位数は素数冪である。(Baumert and Gordon)。41 未満の位数の巡回平面は同型、従って有限体から作られるもののみである (Hall, Bruck, Huang-Schmidt [4])。定理 1 を組み合わせると、予想 1 の反例となる魔円陣があるとすれば 20 億以上の大きさとなる。また有限体から作れない魔円陣があるとすれば最低でも大きさは 42 である。

大きさが与えられたとき魔円陣はいくつあるだろう。ここでは魔円陣は回転したり裏返したものも同じと考える。巡回平面が 4 章の方法で得られたとして、定理 1 における巡回平面と魔円陣の対応では原始根の取り方を考慮していない。巡回平面への数字の貼り付け方により別の魔円陣が出来ることがある。フロベニウス準同型 $x \to x^p$ は位数 $3e$ の巡回平面の同型を引き起こし、これによってできる魔円陣は同じである。裏返しも考慮にいれると、F_{p^e} の 3 次拡大から魔円陣が $\phi(p^{2e}+p^e+1)/6e$ 個できる。それらは全て異なると予想[7]される ([9])。ここで $\phi(m)$ はオイラーの関数、すなわち $1, 2, \ldots, m$ のなかで m と互いに素なものの個数である。もしも、全ての巡回平面が有限体から作られるならば、この式が大きさ $1+p^e$ の魔円陣の個数の公式となるだろう。大きさ 3, 5 の魔円陣は一つしかないが、4 では $\phi(13)/6 = 2$ 個、18 は $\phi(307)/6 = 51$ 個ある。

有限体を用いない新しい魔円陣の構成方法が見つかれば数学上の大発見となるだろう。歴史的な未解決問題であるが、見かけは初等的で楽しい。読者も挑戦してみてはいかがだろうか？

参考文献

[1] S. Ball and Z. Weiner, An Introduction to Finite Geometry, http://www-ma4.upc.es/ simeon/IFG.pdf

[2] R.H. Bruck and H.J. Ryser, The nonexistence of certain finite projective planes, Canadian J. Math. 1, (1949). 88-93.

[3] 平峰豊, 有限射影平面概観, 数理解析研究所講究録 **1214** 巻 (2001) pp. 46-61.

[4] Y. Huang and B. Schmidt, Uniqueness of some cyclic projective planes, Des. Codes Cryptogr. **50** (2009) pp. 253-266.

[5] D.A. James, Magic Circles, Mathematics Magazine, **54**-3 (1981) pp.122-125,

[7]解決済みか否か筆者にはわからなかった。

[6] G.L. Mullen, A candidate for the "next Fermat problem", Math. Intelligencer 17 (1995), no. 3, 18-22.

[7] 島内剛一, λ 倍取りゲーム, 数学セミナー **1** (1982) 10-14.

[8] 下林山稔, パソコンで魔円陣を, 数学セミナー **7** (1987) 55-59.

[9] J. Singer, A Theorem in Finite Projective Geometry and Some Applications to Number Theory,Trans. Amer. Math. Soc., **43**-3 (1938), pp.377-385.