数理物質科学研究科

幾何学概論IIB

教育研究科

幾何学B

有限幾何学
(配付資料)

田崎博之

2014年度

目 次

第1章　アフィン平面

1.1　体上のアフィン平面

定義 1.1.1 加法 $+$ と乗法 $\cdot$ という二種類の演算が定義された集合 F が次の条件を満たすとき、F を**体**という。

(1) 加法の結合法則が成り立つ。すなわち $(a+b)+c=a+(b+c) \quad (a,b,c \in F)$.

(2) 加法の単位元 0 が存在する。すなわち $a+0=0+a=a \quad (a \in F)$.

(3) 加法の逆元が存在する。すなわち、任意の $a \in F$ に対してある $b \in F$ が存在して $a+b=b+a=0$ が成り立つ。

(4) 加法は可換である。すなわち $a+b=b+a \quad (a,b \in F)$.

(5) 乗法の結合法則が成り立つ。すなわち $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad (a,b,c \in F)$.

(6) 乗法の単位元 1 が存在する。すなわち $a \cdot 1 = 1 \cdot a = a \quad (a \in F)$.

(7) 乗法の逆元が存在する。すなわち、0 ではない任意の $a \in F$ に対してある $b \in F$ が存在して $a \cdot b = b \cdot a = 1$ が成り立つ。

(8) 乗法は可換である。すなわち $a \cdot b = b \cdot a \quad (a,b \in F)$.

(9) 加法と乗法の分配法則が成り立つ。すなわち $a \cdot (b+c) = a \cdot b + a \cdot c \quad (a,b,c \in F)$.

注意 1.1.2 (3) における a の加法の逆元 b は a に対して一意的に定まることがわかる。これを $-a$ で表す。(7) における a の加法の逆元 b は a に対して一意的に定まることがわかる。これを a^{-1} で表す。

例 1.1.3 実数の全体 $\mathbf{R}$ と複素数の全体 $\mathbf{C}$ は通常の加法と乗法に関して体になる。

例 1.1.4 体の定義 (定義 1.1.1) より、体には加法の単位元 0 と乗法の単位元 1 は必ず存在する。この二元 $0,1$ だけからなる体が存在することを示しておこう。0 と 1 の性質からこれらの加法と乗法は次の表のように定まる。

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

逆に上の表によって加法と乗法を定めると、$\{0,1\}$ は体になることがわかる。この体を $\boldsymbol{F}_2$ で表す。

定義 1.1.5 F を体とする。積 $F^2 = F \times F = \{(x, y) \mid x, y \in F\}$ を体 F 上の**アフィン平面**と呼ぶ。

F が実数 $\mathbf{R}$ の場合、$\mathbf{R}^2$ は高校数学でも学ぶ座標平面と同じものである。F が $\boldsymbol{F}_2$ の場合、$\boldsymbol{F}_2^2 = \{(0,0), (1,0), (0,1), (1,1)\}$ は4個の点からなる有限集合である。

体 F と自然数 n に対して積集合 $F^n = \{(x_1, \ldots, x_n) \mid x_i \in F\}$ を考えることができ、実数 $\mathbf{R}$ や複素数 $\mathbf{C}$ の場合と同様に体 F 上の線形代数を F^n で展開できる。F の元を係数に持つ連立一次方程式や行列式の議論も実数や複素数の場合と同様に行うことができる。

定義 1.1.6 体 F の元 a, b, c をとる。ただし、a, b の少なくとも一方は0ではないと仮定する。このとき、F^2 の部分集合 $\{(x, y) \in F^2 \mid ax + by + c = 0\}$ を**直線**と呼ぶ。

F が実数 $\mathbf{R}$ の場合、上で定義した直線は高校数学で学ぶ座標平面 $\mathbf{R}^2$ の直線と同じものである。F が $\boldsymbol{F}_2$ の場合、直線は以下の6個である。

$$\{(x, y) \in \boldsymbol{F}_2^2 \mid 1x + 0y + 0 = 0\} = \{(0,0), (0,1)\},$$
$$\{(x, y) \in \boldsymbol{F}_2^2 \mid 1x + 0y + 1 = 0\} = \{(1,0), (1,1)\},$$
$$\{(x, y) \in \boldsymbol{F}_2^2 \mid 0x + 1y + 0 = 0\} = \{(0,0), (1,0)\},$$
$$\{(x, y) \in \boldsymbol{F}_2^2 \mid 0x + 1y + 1 = 0\} = \{(0,1), (1,1)\},$$
$$\{(x, y) \in \boldsymbol{F}_2^2 \mid 1x + 1y + 0 = 0\} = \{(0,0), (1,1)\},$$
$$\{(x, y) \in \boldsymbol{F}_2^2 \mid 1x + 1y + 1 = 0\} = \{(0,1), (1,0)\}.$$

$\boldsymbol{F}_2^2$ の直線の全体には、$\boldsymbol{F}_2^2$ の4点から2点を選ぶすべての組み合せが現れている。

座標平面 $\mathbf{R}^2$ の点と直線については次が成り立つ。

(1) 異なる二点 p, q に対して、p と q を含む直線がただ一つ存在する。

(2) 直線 l と点 p に対して、p を含み l と平行な直線がただ一つ存在する。

(3) 一つの直線に含まれない三点が存在する。

上記の座標平面の点と直線の性質は一般の体上のアフィン平面の点と直線の性質に拡張できる。そのためには、体上のアフィン平面の二つ直線が平行であることを定義しておく必要がある。

定義 1.1.7 体上のアフィン平面の二つ直線が一致するかまたは交わらないとき、これら二つの直線は**平行**であるという。

定理 1.1.8 体上のアフィン平面の点と直線について次が成り立つ。

(1) 異なる二点 p, q に対して、p と q を含む直線がただ一つ存在する。

(2) 直線 l と点 p に対して、p を含み l と平行な直線がただ一つ存在する。

(3) 一つの直線に含まれない三点が存在する。

定理 1.1.8 の証明の概略　アフィン平面を定める体を F とする。
(1) 異なる二点を $p = (x_0, y_0), q = (x_1, y_1)$ とする。

$$(*) \quad (y_0 - y_1)x + (x_1 - x_0)y + (x_0y_1 - y_0x_1) = 0$$

の定める直線は (x_0, y_0) と (x_1, y_1) を含むただ一つの直線になる。

注意 1.1.9 上の証明では直線を定める $(*)$ を天下りに与えた。F の元を成分に持つ行列式を利用するとこれは以下のように導くことができる。(x_0, y_0) と (x_1, y_1) を含む直線は存在するならば、その直線を定める

$$(**) \quad ax + by + c = 0$$

の係数 a, b, c は

$$ax_0 + by_0 + c = 0, \quad ax_1 + by_1 + c = 0$$

を満たす。さらに $(**)$ が定める直線の任意の点 (x, y) はもちろん $(**)$ を満たす。これら三つの等式

$$\begin{aligned} xa + yb + c &= 0, \\ x_0a + y_0b + c &= 0, \\ x_1a + y_1b + c &= 0 \end{aligned}$$

を a, b, c に関する方程式と考えると、a, b の少なくとも一方は 0 ではない解が存在することになり、

$$\begin{vmatrix} x & y & 1 \\ x_0 & y_0 & 1 \\ x_1 & y_1 & 1 \end{vmatrix} = 0$$

が成り立つ。この行列式を展開すると $(*)$ が現れる。

(2) p が l に含まれる場合、p を含み l と平行な直線は l だけである。そこで、p が l に含まれない場合を考える。

$$ax + by + c = 0$$

が l を定めているとする。$p = (x_0, y_0)$ とおくと、

$$ax + by - ax_0 - by_0 = 0$$

が定める直線が p を含み l と平行なただ一つの直線になる。
(3) 体 F は加法の単位元 0 と乗法の単位元 1 を持ち、これらは異なる。アフィン平面の二点 $(0, 0)$ と $(0, 1)$ は、

$$1x + 0y + 0 = 0$$

が定める直線に含まれる。(1) より、これら二点を含む直線は、この直線だけである。$(1, 0)$ は上の直線には含まれない。したがって、三点 $(0, 0), (0, 1), (1, 0)$ は一つの直線には含まれない。

1.2 公理的扱い

前節では、体からアフィン平面とそこでの直線を定め、そのアフィン平面の点と直線の性質を扱った。この節では前節の定理 1.1.8 の性質を満たす集合の中の部分集合の集りについて考え、これを体上のアフィン平面の幾何学の一般化として扱う。

定義 1.2.1 集合 A の部分集合の集まり $L(A)$ が次の条件を満たすとき、A を**アフィン平面**と呼び、$L(A)$ の各元を A の**直線**と呼ぶ。

(1) A の異なる二点 p, q に対して、p と q を含む $L(A)$ の元がただ一つ存在する。

(2) $L(A)$ の元 l と A の点 p に対して、p を含み l と平行な $L(A)$ の元がただ一つ存在する。(平行の定義は次の定義 1.2.2 にある。)

(3) $L(A)$ の一つの元に含まれない A の三点が存在する。

定義 1.2.2 アフィン平面の二つ直線が一致するかまたは交わらないとき、これら二つの直線は**平行**であるという。

定理 1.1.8 より、体上のアフィン平面はこの節で定義したアフィン平面である。アフィン平面の直線やその平行性の定義についても矛盾はない。アフィン平面の異なる二点 p, q を含む直線はただ一つ存在するので、その直線を pq と書くことにする。

命題 1.2.3 アフィン平面の二つの直線について次のいずれか一つが成り立つ。

(1) 二つの直線は等しい。

(2) 二つの直線は一点で交わる。

(3) 二つの直線は交わらない。

命題 1.2.4 アフィン平面の二つ直線が平行であるという関係は同値関係である。

証明 推移律を証明すればよい。直線 l_0 は直線 l_1 に平行であり、直線 l_1 は直線 l_2 に平行であると仮定する。l_0 と l_2 が交わらなければ平行になる。そこで、l_0 と l_2 が交わる場合を考える。l_0 と l_2 の交点を p とする。l_0 は p を含み l_1 と平行である。l_2 も p を含み l_1 と平行である。定義 1.2.1 の (2) より l_0 と l_2 は一致する。特に l_0 と l_2 は平行である。

命題 1.2.5 アフィン平面の一つの直線には含まれない 3 点に対して、1 点を付け加えその中のどの 3 点も一つの直線には含まれないようにできる。

証明 一つの直線に含まれない三点を p, q, r とする。定義 1.2.1 の (2) より p を含み直線 qr と平行な直線 l が存在する。同様に r を含み直線 pq に平行な直線 m が存在する。このとき、l と m は平行ではないことを示す。もし l と m が平行ならば、l は qr と平行であり m は pq と平行だから、命題 1.2.4 より qr と pq は平行になる。これらは q で交わるので一致する。よって、p, q, r は一つの直線 $pq = qr$ に含まれ、p, q, r のとり方に矛盾する。したがって、l と m は平行ではない。命題 1.2.3 より l と m は一点 s で交わる。s は pq に含まれず、qr にも含まれない。よって、p, q, r, s は異なる 4 点になる。最初の定め方より p, q, r は一つの直線には含まれない。q, r, s は一つの直線には含まれない。p, q, s も一つの直線には含まれない。最後に p, r, s も一つの直線には含まれないことを示す。もし p, r, s が一つの直線に含まれるとすると、この直線は l に一致する。これは l と qr が点 r で交わることになり、l と qr が平行であることに反する。以上より p, q, r, s の中のどの 3 点も一つの直線には含まれない。

系 1.2.6 アフィン平面にはある 4 点が存在して、その中のどの 3 点も一つの直線には含まれない。

証明 定義 1.2.1 の (3) より一つの直線に含まれない三点 p, q, r が存在する。これに命題 1.2.5 を適用すればよい。

命題 1.2.7 アフィン平面のどの点についても、その点を含む直線は二つ以上ある。

証明 アフィン平面の任意の点 a をとる。系 1.2.6 よりある 4 点が存在して、その中のどの 3 点も一つの直線には含まれない。この 4 点のうち一つは a に一致する可能性もあるが、a とは異なり一つの直線には含まれない 3 点をとることができる。その 3 点を p, q, r とする。

命題 1.2.8 アフィン平面のどの直線も二つ以上の点を含む。

証明 アフィン平面の任意の直線 l をとる。系 1.2.6 の 4 点を p, q, r, s とする。l がこれらのうちの 2 点を含めば証明は終わるので、1 点のみを含む場合を考える。l が p, q, r を含まないと仮定してよい。p, q, r は一つの直線には含まれないので、pq, qr, rp のどの二つも平行ではない。よってこれらのうちで l と平行になるものは高々一つである。そこで、l と平行ではないものを m, n とする。l と m の交点を a とし、l と n の交点を b とする。m と n は l に含まれない点を交点に持つので、もし a と b が一致するならば m と n は異なる二点で交わることになり、m と n は一致する。これは定め方に反するので、a と b は等しくない。したがって、l は二点を含む。

命題 1.2.9 一つのアフィン平面のどの二つの直線の間にも全単射が存在する。

証明 二つの直線を l, m とする。まず、l, m が平行な場合を考える。$l = m$ のときは証明することはないので、l と m が異なる場合を考えればよい。l の点 p と m の点 q をとる。直線 pq と l は平行ではない。もし平行なら pq と l は一致し l と m も一致することになる。同様に pq と m も平行ではない。p, q を利用して、全単射 $\phi : l \to m$ を構成する。l の点 x に対して x を含み直線 pq と平行な直線 n をとる。pq と m は平行ではないので、命題 1.2.4 より m と n も平行ではない。命題 1.2.3 より m と n は一点で交わる。この交点を $\phi(x)$ とする。m の点に対して ϕ の構成法と同様の議論を行えば、l の点が定まり ϕ の逆写像を定めることがわかる。したがって、ϕ は全単射である。

次に、l, m が平行ではない場合を考える。このときは、命題 1.2.3 の (2) が成り立ち、l, m は一点で交わる。l, m の交点を r で表す。命題 1.2.8 より l は r 以外の点 p を含み、m は r 以外の点 q を含む。l, m が平行ではないことから、p, q, r は一つの直線には含まれない。この三点 p, q, r を利用して、全単射 $\phi : l \to m$ を構成する。l の点 x に対して x を含み直線 pq と平行な直線 n をとる。pq と m は平行ではないので、命題 1.2.4 より n と m も平行ではない。命題 1.2.3 より n と m は一点で交わる。この交点を $\phi(x)$ とする。これにより、写像 $\phi : l \to m$ が定まる。

m の点に対して ϕ の構成法と同様の議論を行えば、l の点が定まり ϕ の逆写像を定めることがわかる。したがって、ϕ は全単射である。

1.3 有限アフィン平面

定義 1.3.1 アフィン平面の直線が n 個の点からなるとき、このアフィン平面を n 次アフィン平面と呼ぶ。命題 1.2.9 より、n 次アフィン平面のどの直線も n 個の点からなる。

命題 1.3.2 n 次アフィン平面の一点を含む直線のすべては $n+1$ 本ある。

命題 1.3.3 n 次アフィン平面の一本の直線と平行な直線のすべては n 本ある。

命題 1.3.4 n 次アフィン平面の点のすべては n^2 個である。

命題 1.3.5 n 次アフィン平面の直線のすべては $n(n+1)$ 本である。

命題 1.3.6 n 次アフィン平面の平行直線の同値類の個数は $n+1$ である。

第2章　有限体

2.1　有限体の基本定理

元の個数が有限個の体を**有限体**という。

定理 2.1.1 有限体の元の個数は素数の冪になり、逆に素数の冪の元を持つ体は存在し、同型を除いて一意的である。

元の個数が q の体は同型を除いて一意的に定まるので、$\boldsymbol{F}_q$ と書く。

定義 2.1.2 加法 $+$ と乗法 $\cdot$ という二種類の演算が定義された集合 R が定義 1.1.1 の (7) 以外の条件を満たすとき、R を**環**という。

通常は上の定義は可換環の定義であるが、この講義では可換環しか扱わないので、単に環と呼ぶことにする。

定義 2.1.3 環 R の部分集合 S が次の条件を満たすとき、S を R の**部分環**という。

(1) 加法に関して閉じている。すなわち $s+t \in S \quad (s,t \in S)$.

(2) R の加法の単位元 0 を S が含む。

(3) 加法の逆元が存在する。すなわち、任意の $a \in S$ に対してある $b \in S$ が存在して $a+b=b+a=0$ が成り立つ。

(4) 乗法に関して閉じている。すなわち $st \in S \quad (s,t \in S)$.

このとき、R の演算の制限によって S の演算を定めると S は環になる。部分環 S がさらに $s \in S,\, r \in R \Rightarrow sr \in S$ を満たすとき、S を R の**イデアル**という。

例 2.1.4 整数の全体 $\mathbf{Z}$ は通常の加法と乗法に関して環になるが、体ではない。非負整数 n に対して $n\mathbf{Z} = \{nz \mid z \in \mathbf{Z}\}$ は $\mathbf{Z}$ のイデアルになる。逆に $\mathbf{Z}$ のイデアルはこの形に限られることがわかる。

命題 2.1.5 環 R が体であるための必要十分条件は、R が $\{0\}$ と自分自身以外のイデアルを持たないことである。

定義 2.1.6 R を環とし、I を R のイデアルとする。R の二元 r, r' に対して $r-r' \in I$ のときに $r \equiv r' (\mathrm{mod} I)$ と表し、二元の間の I に関する合同関係を定める。すると、この合同関係は同値関係になる。さらに、R の加法と乗法はこの同値類の全体に加法と乗法を誘導し、同値類の全体は環になる。この同値類全体の成す環を R/I で表し、R の I による**剰余環**と呼ぶ。この同値類を**剰余類**という。

定義 2.1.7 環のイデアルが包含関係に関して極大であるとき、**極大イデアル**と呼ぶ。すなわち、環 R のイデアル I が極大イデアルであるとは、$I \subset J \subset R$ となるイデアル J が I と R 以外にはないことである。

命題 2.1.8 環 R のイデアル I について、剰余環 R/I が体であるための必要十分条件は、I が R の極大イデアルになることである。

命題 2.1.9 整数環 $\mathbf{Z}$ のイデアルは例 2.1.4 より非負整数 n によって $n\mathbf{Z}$ と表せる。非負整数 m, n に対して以下が成り立つ。

(1) $m\mathbf{Z} = n\mathbf{Z} \Leftrightarrow m = n$

(2) $m\mathbf{Z} \subset n\mathbf{Z} \Leftrightarrow n$ は m を割り切る

(3) $n\mathbf{Z}$ は極大イデアル $\Leftrightarrow n$ は素数

系 2.1.10 素数 p に対して剰余環 $\mathbf{Z}/p\mathbf{Z}$ は体になる。したがって、$\boldsymbol{F}_p = \mathbf{Z}/p\mathbf{Z}$ である。

例 2.1.11 $\boldsymbol{F}_3 = \mathbf{Z}/3\mathbf{Z}$ より、加法と乗法は次の表のように定まる。

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

例 2.1.12 $\boldsymbol{F}_5 = \mathbf{Z}/5\mathbf{Z}$ より、加法と乗法は次の表のように定まる。

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

例 2.1.13 $\boldsymbol{F}_7 = \mathbf{Z}/7\mathbf{Z}$ より、加法と乗法の表もつくることができる。

2.2 多項式環の剰余体としての構成

定義 2.2.1 F を体とする。x を変数とし F の元を係数とする多項式

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \quad (a_i \in F)$$

の全体を $F[x]$ で表す。$F[x]$ の元の加法と乗法を通常の多項式の場合と同様に定義すれば、$F[x]$ は環になる。この環の構造を持つ $F[x]$ を F 上の**多項式環**と呼ぶ。上記の多項式 $f(x)$ の係数が $a_0 \neq 0$ を満たすとき、n を $f(x)$ の**次数**といい、$n = \deg f, \deg f(x)$ と書く。$F[x]$ の元としての 0 の次数は $-\infty$ と定める。

通常の多項式の次数と同様に以下が成り立つ。

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$$
$$\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$$

ここで、非負整数 n に対して $n + (-\infty) = -\infty$, $-\infty < n$ と約束しておく。

定義 2.2.2 正の次数の多項式 $f(x) \in F[x]$ に対して、

$$f(x) = g(x)h(x) \quad (\deg g(x) >, \deg h(x) > 0)$$

を満たす二つの多項式 $g(x), h(x) \in F[x]$ が存在するとき、$f(x)$ は**可約**であるといい、可約ではないとき**既約**であるという。

定理 2.2.3 体 F 上の多項式環 $F[x]$ のイデアル I が極大イデアルための必要十分条件は、ある既約多項式 $f(x)$ が存在して $I = f(x)F[x]$ となることである。

定理 2.2.4 素数 p と自然数 n に対して、$\boldsymbol{F}_p[x]$ において $x^{p^n} - x$ を割る既約多項式 $f(x)$ が存在して、有限体 $\boldsymbol{F}_{p^n}$ は $\boldsymbol{F}_p[x]/f(x)\boldsymbol{F}_p[x]$ に同型になる。

例 2.2.5 $\boldsymbol{F}_4$ は定理 2.2.4 の $p = 2$, $n = 2$ の場合に対応する。$x^4 - x$ を因数分解して、既約多項式 $x^2 + x + 1 \in \boldsymbol{F}_2[x]$ を見つけることができる。

$$\boldsymbol{F}_4 = \boldsymbol{F}_2[x]/(x^2 + x + 1)\boldsymbol{F}_2[x] = \{[0], [1], [x], [x + 1]\}$$

となる。加法と乗法は次の表のように定まる。

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[x+1]$	$[1]$
$[x+1]$	$[0]$	$[x+1]$	$[1]$	$[x]$

0 以外の各行各列に 1 があることから乗法の逆元の存在を直接確かめることもできる。

例 2.2.6 $\boldsymbol{F}_8$ は定理 2.2.4 の $p=2$, $n=3$ の場合に対応する。

$$x^8-x=x(x^7-1)=x(x-1)(x^6+x^5+x^4+x^3+x^2+x+1).$$

ここで

$$(x^3+x+1)(x^3+x^2+1)=x^6+x^5+x^4+x^3+x^2+x+1$$

となるので、

$$x^8-x=x(x-1)(x^3+x+1)(x^3+x^2+1)$$

を得る。$x^3+x+1, x^3+x^2+1\in\boldsymbol{F}_2[x]$ が既約多項式であることを示す。$\boldsymbol{F}_2[x]$ の定数項の消えない一次式のすべては $x+1$ であり、定数項の消えない二次式のすべては x^2+1, x^2+x+1 である。これらの積のすべては、

$$(x+1)(x^2+1)=x^3+x^2+x+1,\quad (x+1)(x^2+x+1)=x^3+1$$

である。x^3+x+1, x^3+x^2+1 はこれらのどれにも一致しないので既約多項式である。x^3+x+1 の定めるイデアルによる剰余環を考える。

$$\begin{aligned}&\boldsymbol{F}_2[x]/(x^3+x+1)\boldsymbol{F}_2[x]\\&=\{[0],[1],[x],[x+1],[x^2],[x^2+1],[x^2+x],[x^2+x+1]\}\end{aligned}$$

が成り立つ。加法と乗法は次の表のように定まる。ただし、剰余類を表す $[\cdot]$ は省略する。

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

0 以外の各行各列に 1 があることから乗法の逆元の存在を直接確かめることもできる。

例 2.2.7 $\boldsymbol{F}_9$ は定理 2.2.4 の $p=3$, $n=2$ の場合に対応する。

$$\begin{aligned}x^9-x&=x(x^8-1)=x(x^4-1)(x^4+1)=x(x^2-1)(x^2+1)(x^4+1)\\&=x(x-1)(x+1)(x^2+1)(x^4+1).\end{aligned}$$

ここで

$$(x^2+x+2)(x^2+2x+2)=x^4+1$$

となるので、

$$x^9-x=x(x-1)(x+1)(x^2+1)(x^2+x+2)(x^2+2x+2)$$

を得る。$x^2+1, x^2+x+2, x^2+2x+2 \in \boldsymbol{F}_3[x]$ が既約多項式であることを示す。x の係数が 1 であり定数項が消えない一次式のすべては $x+1, x+2$ である。これらの積のすべては

$$(x+1)^2=x^2+2x+1, \quad (x+1)(x+2)=x^2+2, \quad (x+2)^2=x^2+x+1$$

である。x^2+1, x^2+x+2, x^2+2x+2 はこれらのどれにも一致しないので既約多項式である。x^2+1 の定めるイデアルによる剰余環を考える。

$$\begin{aligned}&\boldsymbol{F}_3[x]/(x^2+1)\boldsymbol{F}_3[x]\\&=\{[0],[1],[2],[x],[x+1],[x+2],[2x],[2x+1],[2x+2]\}\end{aligned}$$

が成り立つ。加法と乗法は次の表のように定まる。ただし、剰余類を表す $[\cdot]$ は省略する。

$+$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

$\cdot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+1$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

0 以外の各行各列に 1 があることから乗法の逆元の存在を直接確かめることもできる。

2.3 有限体上のアフィン平面

命題 2.3.1 体 $\boldsymbol{F}_q$ 上のアフィン平面 $\boldsymbol{F}_q^2$ は q 次アフィン平面になり、点のすべては q^2 個、一点を含む直線のすべては $q+1$ 本、一本の直線と平行な直線のすべては q 本、直線のすべては $q(q+1)$ 本である。

$\boldsymbol{F}_2$ 上のアフィン平面の直線の全体は、1.1 節で求めた。他の体上のアフィン平面の直線の全体も求める。平行な直線の族の中には原点 $(0,0)$ を含む直線がただ一つ存在する。そこで、$(0,0)$ を含む直線をすべて求め、次にそれぞれについて平行な直線の族を求めることにより、直線の全体を記述する。

例 2.3.2 $\boldsymbol{F}_3$ 上のアフィン平面の直線の全体について考える。$(0,0)$ を含む直線のすべては、

$$
\begin{aligned}
l_1 \qquad & \{(x,y) \in \boldsymbol{F}_3^2 \mid 1\cdot x + 0\cdot y = 0\} = \{(0,0),(0,1),(0,2)\},\\
l_2 \qquad & \{(x,y) \in \boldsymbol{F}_3^2 \mid 0\cdot x + 1\cdot y = 0\} = \{(0,0),(1,0),(2,0)\},\\
l_3 \qquad & \{(x,y) \in \boldsymbol{F}_3^2 \mid 1\cdot x + 1\cdot y = 0\} = \{(0,0),(1,2),(2,1)\},\\
l_4 \qquad & \{(x,y) \in \boldsymbol{F}_3^2 \mid 2\cdot x + 1\cdot y = 0\} = \{(0,0),(1,1),(2,2)\}
\end{aligned}
$$

である。l_1 と平行な直線のすべてと l_2 と平行な直線のすべての記述は簡単なので省略する。l_1 と平行な直線のすべては

$$
\begin{aligned}
&\{(x,y) \in \boldsymbol{F}_3^2 \mid 1\cdot x + 0\cdot y = 0\} = \{(0,0),(0,1),(0,2)\},\\
&\{(x,y) \in \boldsymbol{F}_3^2 \mid 1\cdot x + 0\cdot y = 1\} = \{(1,0),(1,1),(1,2)\},\\
&\{(x,y) \in \boldsymbol{F}_3^2 \mid 1\cdot x + 0\cdot y = 2\} = \{(2,0),(2,1),(2,2)\}.
\end{aligned}
$$

l_2 と平行な直線のすべては

$$
\begin{aligned}
&\{(x,y) \in \boldsymbol{F}_3^2 \mid 0\cdot x + 1\cdot y = 0\} = \{(0,0),(1,0),(2,0)\},\\
&\{(x,y) \in \boldsymbol{F}_3^2 \mid 0\cdot x + 1\cdot y = 1\} = \{(0,1),(1,1),(2,1)\},\\
&\{(x,y) \in \boldsymbol{F}_3^2 \mid 0\cdot x + 1\cdot y = 2\} = \{(0,2),(1,2),(2,2)\}.
\end{aligned}
$$

l_3 と平行な直線のすべては

$$
\begin{aligned}
&\{(x,y) \in \boldsymbol{F}_3^2 \mid 1\cdot x + 1\cdot y = 0\} = \{(0,0),(1,2),(2,1)\},\\
&\{(x,y) \in \boldsymbol{F}_3^2 \mid 1\cdot x + 1\cdot y = 1\} = \{(0,1),(1,0),(2,2)\},\\
&\{(x,y) \in \boldsymbol{F}_3^2 \mid 1\cdot x + 1\cdot y = 2\} = \{(0,2),(1,1),(2,0)\}.
\end{aligned}
$$

l_4 と平行な直線のすべては

$$
\begin{aligned}
&\{(x,y) \in \boldsymbol{F}_3^2 \mid 2\cdot x + 1\cdot y = 0\} = \{(0,0),(1,1),(2,2)\},\\
&\{(x,y) \in \boldsymbol{F}_3^2 \mid 2\cdot x + 1\cdot y = 1\} = \{(0,1),(1,2),(2,0)\},\\
&\{(x,y) \in \boldsymbol{F}_3^2 \mid 2\cdot x + 1\cdot y = 2\} = \{(0,2),(1,0),(2,1)\}.
\end{aligned}
$$

例 2.3.3 $\boldsymbol{F}_4$ 上のアフィン平面の直線の全体について考える。$\boldsymbol{F}_4$ の元を剰余類を表す記号 $[\cdot]$ を省略し、さらに $x+1$ を y で表すことにすると、例 2.2.5 より加法と乗法の表は次のようになる。

$+$	0	1	x	y
0	0	1	x	y
1	1	0	y	x
x	x	y	0	1
y	y	x	1	0

$\cdot$	0	1	x	y
0	0	0	0	0
1	0	1	x	y
x	0	x	y	1
y	0	y	1	x

直線を表す方程式の変数は X, Y で表すことにする。$(0,0)$ を含む直線のすべては、

$$
\begin{aligned}
l_1 \qquad & \{(X,Y) \in \boldsymbol{F}_4^2 \mid 1\cdot X + 0\cdot Y = 0\} = \{(0,0),(0,1),(0,x),(0,y)\},\\
l_2 \qquad & \{(X,Y) \in \boldsymbol{F}_4^2 \mid 0\cdot X + 1\cdot Y = 0\} = \{(0,0),(1,0),(x,0),(y,0)\},\\
l_3 \qquad & \{(X,Y) \in \boldsymbol{F}_4^2 \mid 1\cdot X + 1\cdot Y = 0\} = \{(0,0),(1,1),(x,x),(y,y)\},\\
l_4 \qquad & \{(X,Y) \in \boldsymbol{F}_4^2 \mid x\cdot X + 1\cdot Y = 0\} = \{(0,0),(1,x),(x,y),(y,1)\},\\
l_5 \qquad & \{(X,Y) \in \boldsymbol{F}_4^2 \mid y\cdot X + 1\cdot Y = 0\} = \{(0,0),(1,y),(x,1),(y,x)\}
\end{aligned}
$$

である。l_1 と平行な直線のすべてと l_2 と平行な直線のすべての記述は簡単なので省略する。l_3 と平行な直線のすべては

$$
\begin{aligned}
&\{(X,Y) \in \boldsymbol{F}_4^2 \mid 1\cdot X + 1\cdot Y = 0\} = \{(0,0),(1,1),(x,x),(y,y)\},\\
&\{(X,Y) \in \boldsymbol{F}_4^2 \mid 1\cdot X + 1\cdot Y = 1\} = \{(0,1),(1,0),(x,y),(y,x)\},\\
&\{(X,Y) \in \boldsymbol{F}_4^2 \mid 1\cdot X + 1\cdot Y = x\} = \{(0,x),(1,y),(x,0),(y,1)\},\\
&\{(X,Y) \in \boldsymbol{F}_4^2 \mid 1\cdot X + 1\cdot Y = y\} = \{(0,y),(1,x),(x,1),(y,0)\}.
\end{aligned}
$$

l_4 と平行な直線のすべては

$$
\begin{aligned}
&\{(X,Y) \in \boldsymbol{F}_4^2 \mid x\cdot X + 1\cdot Y = 0\} = \{(0,0),(1,x),(x,y),(y,1)\},\\
&\{(X,Y) \in \boldsymbol{F}_4^2 \mid x\cdot X + 1\cdot Y = 1\} = \{(0,1),(1,y),(x,),(y,0)\},\\
&\{(X,Y) \in \boldsymbol{F}_4^2 \mid x\cdot X + 1\cdot Y = x\} = \{(0,x),(1,0),(x,1),(y,y)\},\\
&\{(X,Y) \in \boldsymbol{F}_4^2 \mid x\cdot X + 1\cdot Y = y\} = \{(0,y),(1,1),(x,0),(y,x)\}.
\end{aligned}
$$

l_5 と平行な直線のすべては

$$
\begin{aligned}
&\{(X,Y) \in \boldsymbol{F}_4^2 \mid y\cdot X + 1\cdot Y = 0\} = \{(0,0),(1,y),(x,1),(y,x)\},\\
&\{(X,Y) \in \boldsymbol{F}_4^2 \mid y\cdot X + 1\cdot Y = 1\} = \{(0,1),(1,x),(x,0),(y,y)\},\\
&\{(X,Y) \in \boldsymbol{F}_4^2 \mid y\cdot X + 1\cdot Y = x\} = \{(0,x),(1,1),(x,y),(y,0)\},\\
&\{(X,Y) \in \boldsymbol{F}_4^2 \mid y\cdot X + 1\cdot Y = y\} = \{(0,y),(1,0),(x,x),(y,1)\}.
\end{aligned}
$$

第3章　いろいろな方陣

3.1　ラテン方陣

定義 3.1.1 0 から $n-1$ までの自然数を成分とする n 次正方行列のどの行にもどの列にも重複がないとき、この行列を n **次ラテン方陣**と呼ぶ。

行列の用語を使ってラテン方陣を定義したが、通常はその行列の成分をます目に入れたものをラテン方陣とよ呼ぶ。たとえば、

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \rightarrow \quad \begin{array}{|c|c|} \hline 0 & 1 \\ \hline 1 & 0 \\ \hline \end{array}$$

と書く。

例 3.1.2 n 次ラテン方陣を次のようにつくることができる。第 1 行目に $0, 1, \ldots, n-1$ を並べ、第 2 行目に第 1 行目の最後の $n-1$ を最初に移動させ他の数字は右に一つずつ移動させる。この操作を繰り返すことにより n 次ラテン方陣を得る。逆に数字を左に一つずつ移動させることによっても n 次ラテン方陣を得る。

命題 3.1.3 有限体 $\boldsymbol{F}_n$ 上のアフィン平面 $\boldsymbol{F}_n^2$ の x 軸または y 軸に平行でない直線と平行な直線族に対して、0 から $n-1$ までの自然数を同じ直線にある点には同じ値を入れ、異なる直線には異なる値を入れると、ラテン方陣になる。

例 3.1.4 1.1 節より $\boldsymbol{F}_2^2$ の x 軸または y 軸に平行でない直線と平行な直線族から上に挙げた 2 次ラテン方陣が定まる。

例 3.1.5 例 2.3.2 の記号を流用する。l_1 は y 軸であり l_2 は x 軸である。l_3 と平行な直線の 1 番目の直線の点に 0、2 番目の直線の点に 1、3 番目の直線の点に 2 を入れたラテン方陣と、l_4 と平行な直線から同様にして得られるラテン方陣は次のとおり。

2	0	1
1	2	0
0	1	2

2	1	0
1	0	2
0	2	1

例 3.1.6 例 2.3.3 の記号を流用する。l_3, l_4, l_5 のそれぞれと平行な直線族から得られるラテン方陣は次のとおり。

3	2	1	0
2	3	0	1
1	0	3	2
0	1	2	3

3	1	0	2
2	0	1	3
1	3	2	0
0	2	3	1

3	0	2	1
2	1	3	0
1	2	0	3
0	3	1	2

右の二つのラテン方陣は対角線においても重複がない。

3.2 オイラー方陣

定義 3.2.1 二つのラテン方陣 $A = (a_{ij})$ と $B = (b_{ij})$ 0 から $n-1$ までの自然数の組を成分とする n 次正方行列 (a_{ij}, b_{ij}) のすべての成分が互いに異なるとき、A と B は**直交する**といい、この行列 (a_{ij}, b_{ij}) を n **次オイラー方陣**と呼ぶ。

例 3.2.2 例 3.1.2 で得た同じ次数の二つのラテン方陣は、n が奇数のときは直交し、n が偶数のときは直交しないことがわかる。$n = 3, 5$ の場合は以下のとおりである。

$(0,0)$	$(1,1)$	$(2,2)$
$(2,1)$	$(0,2)$	$(1,0)$
$(1,2)$	$(2,0)$	$(0,1)$

$(0,0)$	$(1,1)$	$(2,2)$	$(3,3)$	$(4,4)$
$(4,1)$	$(0,2)$	$(1,3)$	$(2,4)$	$(3,0)$
$(3,2)$	$(4,3)$	$(0,4)$	$(1,0)$	$(2,1)$
$(2,3)$	$(3,4)$	$(4,0)$	$(0,1)$	$(1,2)$
$(1,4)$	$(2,0)$	$(3,1)$	$(4,2)$	$(0,3)$

例 3.2.3 例 3.1.5 で得た二つのラテン方陣から定まる数の組の方陣

$(2,2)$	$(0,1)$	$(1,0)$
$(1,1)$	$(2,0)$	$(0,2)$
$(0,0)$	$(1,2)$	$(2,1)$

はオイラー方陣になる。

第一成分の $0, 1, 2$ をコーヒー、紅茶、ココアに対応させ、第二成分の $0, 1, 2$ を S, M, L に対応させると、上オイラー方陣は次のようになる。

ココア L	コーヒー M	紅茶 S
紅茶 M	ココア S	コーヒー L
コーヒー S	紅茶 L	ココア M

この方陣の各行と各列に異なる飲み物と異なるサイズが並んでいる。

3.3 魔方陣

定義 3.3.1 0 から $n^2 - 1$ までの自然数のすべてを成分とする n 次正方行列のどの行の成分の和もどの列の成分の和も等しいとき、この行列を n **次魔方陣**と呼ぶ。

通常はさらに対角線の成分の和も等しいという条件を加えたものを魔方陣と呼ぶが、ここでは若干弱い条件で魔方陣を定義している。

命題 3.3.2 n 次オイラー方陣の各成分 (a_{ij}, b_{ij}) を n 進数とみなして

$$a_{ij}b_{ij} = a_{ij}n + b_{ij}$$

に置き換えると魔方陣になる。さらにラテン方陣 (a_{ij}) と (b_{ij}) の対角線においても重複がないならば、オイラー方陣から得られた魔法陣の対角線の成分の和も等しい。

証明 n 次オイラー方陣の性質より、オイラー方陣から作られた方陣の第 i 行の成分の和は

$$\begin{aligned}\sum_{j=0}^{n-1} a_{ij}b_{ij} &= \sum_{j=0}^{n-1}(a_{ij}n + b_{ij}) = n\sum_{j=0}^{n-1} j + \sum_{j=0}^{n-1} j = (n+1)\sum_{j=0}^{n-1} j \\ &= \frac{1}{2}(n-1)n(n+1).\end{aligned}$$

よって、すべての行の成分の和は等しい。同様にすべての列の和も同じ値に等しいことがわかる。

さらにラテン方陣 (a_{ij}) と (b_{ij}) の対角線においても重複がないならば、上記の行や列の場合と同様に、オイラー方陣から得られた魔法陣の対角線の成分の和も等しいことがわかる。

例 3.3.3 例 3.2.2 の 3 次オイラー方陣から定まる魔方陣とそれを 10 進数で表したものは

00	11	22
21	02	10
12	20	01

0	4	8
7	2	3
5	6	1

である。

例 3.2.3 の 3 次オイラー方陣から定まる魔方陣とそれを 10 進数で表したものは

22	01	10
11	20	02
00	12	21

8	1	3
4	6	2
0	5	7

である。

例 3.2.3 で構成したラテン方陣の対角線の成分が 1 になるように変えると、対角線の成分の和も等しい魔方陣になる。

2	0	1
1	2	0
0	1	2

2	1	0
1	0	2
0	2	1

$\rightarrow$

1	2	0
0	1	2
2	0	1

0	2	1
2	1	0
1	0	2

これら二つのラテン方陣から定まるオイラー方陣、それから定まる魔方陣とそれを 10 進数で表したものは

$(1,0)$	$(2,2)$	$(0,1)$
$(0,2)$	$(1,1)$	$(2,0)$
$(2,1)$	$(0,0)$	$(1,2)$

10	22	01
02	11	20
21	00	12

3	8	1
2	4	6
7	0	5

となり、対角線の和も等しいことがわかる。

例 3.3.4 例 3.1.6 の後の二つの 4 次ラテン方陣から定まるオイラー方陣をもとに構成した魔方陣とそれを 10 進数で表したものは

33	10	02	21
22	01	13	30
11	32	20	03
00	23	31	12

15	4	2	9
10	1	7	12
5	14	8	3
0	11	13	6

この魔方陣は例 3.1.6 で示した対角線においても重複がない二つのラテン方陣から作られているため、命題 3.3.2 より対角線の成分の和も等しい。

例 3.3.5 例 3.2.2 の 5 次オイラー方陣から定まる魔方陣とそれを 10 進数で表したものは

00	11	22	33	44
41	02	13	24	30
32	43	04	10	21
23	34	40	01	12
14	20	31	42	03

0	6	12	18	24
21	2	8	14	15
17	23	4	5	11
13	19	20	1	7
9	10	16	22	3

定義 3.3.6 (魔方陣のテンソル積) p 次魔方陣 (a_{ij}) と q 次魔方陣 (b_{kl}) の**テンソル積**を、p 次魔方陣の (i,j) 成分の場所に q 次魔方陣の (k,l) 成分 b_{kl} を $b_{kl}+a_{ij}q^2$ に入れ換えた方陣をはめ込んだのものとして定める。

命題 3.3.7 魔方陣のテンソル積は魔方陣である。

例 3.3.8 例 3.3.3 の最後に構成した 3 次魔方陣

3	8	1
2	4	6
7	0	5

とそれ自身とのテンソル積は

30	35	28	75	80	73	12	17	10
29	31	33	74	76	78	11	13	15
34	27	32	79	72	77	16	9	14
21	26	19	39	44	37	57	62	55
20	22	24	38	40	42	56	58	60
25	18	23	43	36	41	61	54	59
66	71	64	3	8	1	48	53	46
65	67	69	2	4	6	47	49	51
70	63	68	7	0	5	52	45	50

となる。これは 9 次魔方陣である。

3.4 魔方陣の存在

定理 3.4.1 n 次アフィン平面から互いに直交する $n-1$ 個のラテン方陣を構成できる。

定理 3.4.2 互いに直交する $n-1$ 個のラテン方陣から n 次アフィン平面を構成できる。

この節では自然数 n に対して n 次魔方陣が存在するかどうかについて考える。2 次魔方陣が存在しないことはすぐにわかるので、$n \geq 3$ の場合を考えればよい。上記の定理と有限体の基本定理から、n が素数の冪で 3 以上であれば n 個の元を持つ有限体が存在し、さらに直交する n 次ラテン方陣が存在する。したがって、n 次オイラー方陣が存在し、n 次魔方陣が存在することがわかる。

n が奇数のとき、例 3.2.2 よりオイラー方陣が存在し、n 次魔方陣も存在する。これより、偶数次の魔方陣が存在するかどうかが問題になる。偶数 n は

$$n = 2^a b \qquad (a \geq 1,\ b : \text{奇数})$$

と表すことができる。$a \geq 2$ ならば、有限体 $\boldsymbol{F}_{2^a}$ のアフィン平面から 2^a 次魔方陣を構成でき、b 次魔方陣とのテンソル積から $n = 2^a b$ 次魔方陣を構成できる。以上より $a = 1$ の場合が残る。すなわち奇数 b に対して $n = 2b$ 次の魔方陣が存在する

かという問題が残る。b は奇数だから $b = 2c + 1$ と表すことができ、$n = 4c + 2$ となる。

オイラーは1782年に $n = 4c + 2$ を次数に持つオイラー方陣は存在しないことを予想した。1900年頃にG. Tarryは6次オイラー方陣が存在しないことを証明した。その後、このオイラーの問題は長い間解かれていなかったが、1959年にR. C. Bose, S. S. ShrikhandeとE. T. Parkerによって、$n = 4c + 2 \geq 10$ の場合にはオイラー方陣は存在するという形で解決された。

3次以上の魔方陣は6次以外では存在することが以上でわかる。6次オイラー方陣は存在しないが、これだけでは6次魔方陣が存在しないかどうかはわからない。実は次に示すように6次魔方陣は存在することが知られている。

0	1	2	33	34	35
30	31	14	3	22	5
29	28	27	8	7	6
11	10	9	26	25	24
23	19	21	20	4	18
12	16	32	15	13	17

したがって、次の定理を得る。

定理 3.4.3 $n \geq 3$ に対して n 次魔方陣は存在する。

第4章　アフィン平面の応用

4.1　実験計画法

ある作物の収穫量に関する実験を次のように計画する。光量、温度、湿度、肥料それぞれ三つの条件 $0, 1, 2$ において収穫する実験を行う。

三つの光量の条件、三つの温度の条件、三つの湿度の条件、三つの肥料のそれぞれを異なる組合せで実験を行うと、

$$3^4 = 81$$

通りの実験を行う必要がある。

例 3.3.3 の最後に構成した 3 次オイラー方陣

$(1,0)$	$(2,2)$	$(0,1)$
$(0,2)$	$(1,1)$	$(2,0)$
$(2,1)$	$(0,0)$	$(1,2)$

を利用して実験の数を大幅に減らすことが可能になる。上記オイラー方陣の各行に光量の条件を対応させる。各列に温度の条件を対応させ、オイラー方陣の各成分の第一成分を湿度の条件、第二成分を肥料の条件に対応させる。これによって、9 種類の実験を行う。たとえば、場所 $(0,0)$ に対応する実験は、第 0 行であるため光量の条件は 0、第 0 列であるため温度の条件は 0、オイラー方陣の成分は $(1,0)$ であるため湿度の条件は 1、肥料の条件は 0 である。

オイラー方陣の各場所 (i,j) に対応する実験の作物の収穫量を C_{ij} で表す。このとき、光量の条件 $0, 1, 2$ の収穫量は

$$\frac{C_{00}+C_{01}+C_{02}}{3}, \quad \frac{C_{10}+C_{11}+C_{12}}{3}, \quad \frac{C_{20}+C_{21}+C_{22}}{3}$$

とみなせる。なぜなら、温度の条件は三種類の平均になっているため、これらの収穫量は温度に依存しない。また、湿度の条件も三種類の平均になっているため、これらの収穫量は湿度にも依存しない。さらに、肥料の条件も三種類の平均になっているため、これらの収穫量は肥料にも依存しない。したがって、上の三つの量を比較することで、$0, 1, 2$ のどの光量の条件の収穫量が多いかがわかる。

温度の条件 $0, 1, 2$ の収穫量は

$$\frac{C_{00}+C_{10}+C_{20}}{3}, \quad \frac{C_{01}+C_{11}+C_{21}}{3}, \quad \frac{C_{02}+C_{12}+C_{22}}{3}$$

とみなせる。なぜなら、光量の条件は三種類の平均になっているため、これらの収穫量は光量に依存しない。また、湿度の条件も三種類の平均になっているため、これらの収穫量は湿度にも依存しない。さらに、肥料の条件も三種類の平均になっているため、これらの収穫量は肥料にも依存しない。したがって、上の三つの量を比較することで、$0, 1, 2$ のどの温度の条件の収穫量が多いかがわかる。

湿度や肥料についてもこれらの条件が同じものの収穫量の平均をとることにより同様に考えることができる。

4.2 対戦相手組合せ問題

3 人で行うゲームを 9 人の参加者で行うときの対戦相手の組合せを考える。すべての対戦の組合せを考えると

$$\binom{9}{3} = \frac{9 \cdot 8 \cdot 7}{3!} = 84$$

通りになる。

$\boldsymbol{F}_3$ 上のアフィン平面 $\boldsymbol{F}_3^2$ の直線を利用して、任意の二人が必ず対戦する組合せは数を減らすことができる。$\boldsymbol{F}_3^2$ の各点を 9 人の参加者に対応させる。3 人の対戦は $\boldsymbol{F}_3^2$ の 3 点部分集合を考えることになる。$\boldsymbol{F}_3^2$ の直線も対戦と考えることができる。$\boldsymbol{F}_3^2$ の直線の全体は、12 本の直線からなる。任意の二点を含む直線が存在することは、直線全体が定める対戦の組合せでは任意の二人が対戦することに対応する。12 は上の 84 よりは小さいが、9 から 2 を選ぶ組合せ数 36 よりも小さい。

4 人で行うゲームを 16 人の参加者で行うときの対戦相手の組合せを考える。すべての対戦の組合せを考えると

$$\binom{16}{4} = \frac{16 \cdot 15 \cdot 14 \cdot 13}{4!} = 1820$$

通りになる。

$\boldsymbol{F}_4$ 上のアフィン平面 $\boldsymbol{F}_4^2$ の直線を利用して、任意の二人が必ず対戦する組合せは数を減らすことができる。$\boldsymbol{F}_4^2$ の各点を 16 人の参加者に対応させる。4 人の対戦は $\boldsymbol{F}_4^2$ の 4 点部分集合を考えることになる。$\boldsymbol{F}_4^2$ の直線も対戦と考えることができる。$\boldsymbol{F}_4^2$ の直線の全体は、20 本の直線からなる。任意の二点を含む直線が存在することは、直線全体が定める対戦の組合せでは任意の二人が対戦することに対応する。