平成24年度　　学 位 論 文

ライツアウトパズルの解析
―有限体上の線形代数の応用として―

兵庫教育大学大学院　　学校教育研究科
教科・領域教育学専攻　　自然系コース
Ｍ１０１７７Ｂ　　中原諒太

目 次

はじめに

研究の目的

本論文では数学分野の基礎である線形代数の応用, 特に行列を利用した研究について記している.

線形代数は様々な分野の基礎であり, 数学分野だけでなく, 理学・工学を問わず多くの場面で応用されている. つまり線形代数は数学を学ぶ上では必要不可欠である. しかし, 昨今高校での行列の扱いは極端に縮小されている. 学習指導要領改訂により, 2012 年度から行列は教科「数学活用」でのみ取り扱うこととなった. しかし, 数学活用は多くの高校で開講されていなかったり, 履修者がほとんどいないことから, 事実上取り扱われていない状態である.

確かに行列は線形代数の基礎であるがゆえに, 高校数学の範囲ではどうしても計算方法に重きをおかれてしまう. 行列の計算はそれまでに習っていた計算方法と大きく違い, 分かりにくい上に, その学習に面白さと意味を見出しにくいことも否めない. それが現在のように行列の扱いが縮小されたことの理由の一端であろう.

筆者自身も高校で行列は学習したものの, 知識としては計算方法を知っている程度のものであったし, 大学でも線形代数を詳しく学んでこなかった. しかしながらこの論文作成を通して, 線形代数・行列がどのように応用されるのか, どのように便利なのか, どのような意味を持つのかなどを, 身近で理解しやすい応用例を用いて, 初めて学ぶことができた.

このように身近で親しみやすい題材を通した線形代数の応用として, ライツアウトパズルの解析を行うのが本論文の目的である.

研究の内容

本論文の最終目標はライツアウトパズルの解析である. ライツアウトパズルとそれに類似したパズルはいくつかあるが, その中でも有名なもの

は5 × 5の格子状に並んだライトが, ランダムに点灯または消灯しており, そのライトに触れると, そのライトとそのライトの上下左右についているライトの点灯・消灯が切り替わるというルールの下, いくつかのライトに触れて全て消灯させることを目的としたパズルである. 日本では1995年に株式会社タカラから発売された. 今では, インターネット上に様々な類似ゲームが存在している.

このライツアウトパズルの構造は, 初等的な線形代数の概念に置き換えることができ, ベクトル空間や行列の概念を用いて解析を行うことができる. また, 本来ライツアウトパズルは長方形のグリッド状になっているもの (ただし, 製品化されているもののほとんどは正方形のグリッド状) であるが, 長方形のグリッド状に限らず, 一般的なグラフ上でのライツアウトパズルを考察することもできる. このライツアウトパズルを本論文上ではσゲームという.

長方形のグリッド, もしくは一般的なグラフ上のσゲームにおいて, 任意の状態にある操作を加えて, 全て0の状態にすることができるとき, このグリッド・グラフをσ可移であるということにする. 特に長方形のグリッドに関しては, そのグリッドがσ可移かどうかを決定するのが1つの主要なテーマである.

論文の構成

第1章では, 体・ベクトル空間・線型写像・行列・行列式・内積空間を定義している. 本論文で扱う$\mathbb{F}_p$については, さまざまな点で実数と異なった性質を持っているので, その点に注意しながら定義を行った. 第2章では実際の例を提示しながら, 一般的なグラフ上のライツアウトパズルについて解析 (σゲームの解析) を行った. 各頂点に順番を付け, 各頂点にボタンとライトがついているものとし, ライトの状態とボタンの操作を$\mathbb{F}_2$の元$0, 1$と対応付けをした. さらに, それを縦に並べ, 頂点の状態や操作をベクトルと同一視した. また, それぞれの頂点がどの頂点とつながっているかを表す隣接行列を定義し, 一般的なグラフ上のσゲームを行列とベクトルの積に帰着させた. その結果, 一般的なグラフ上のσゲームがどのようなときにσ可移であるかを, 特性写像と呼ばれるある線型写像の全射性に帰着できることがわかった. さらに, いかなるグラフであっても, 全てのライトが点灯した状態からであれば, 全てのライトを消灯させた状態にすることができるという定理を得た.

第3章では, 本来のライツアウトパズルの形に戻って, $m \times n$ の長方形グリッド $P_{m,n}$ におけるライツアウトパズルを考えた. この章では, 長方形のグリッド上の頂点の状態を行列と同一視して考える. ゲームのルールに基づいて, 各頂点の操作と状態を行列で表し, $P_{m,n}$ が σ 可移であるかどうかを mn 次元のベクトル空間上の線型写像 σ と関係付けた. これを, ある行列の固有多項式の行列の計算と関係付けることにより, ある m 次 (または n 次) の行列の正則性に帰着できた.

本稿の最後では, 実際に $1 \leq n \leq 11 (n \neq 6, 10)$ の範囲で具体的に m がどういった条件のときに解法を持つかを行列式の計算によって求めた.

第1章　$\mathbb{F}_p$上の線形代数

一般に高校では, $\mathbb{R}$ 係数のベクトル空間を扱い, 大学ではそれに加えて $\mathbb{C}$ 係数のベクトル空間を扱うことが多い. しかし, ベクトル空間は係数が体になっていればよく, 係数体は $\mathbb{R}, \mathbb{C}$ に限らない. 本論文では有限体 $\mathbb{F}_p$ 上のベクトル空間を考える.

1.1　体 $\mathbb{F}_p$

定義 1.1.1 集合 S 上に同値関係 $\sim$ があるとする. S の元 x に対して, $C(x) = \{y \in S | y \sim x\}$ を, x の定める**同値類**という. このとき x を $C(x)$ の**代表元**という.

集合 S に同値関係 $\sim$ が与えられているとき, 同値類 C_1, C_2 に対して $C_1 \cap C_2 = \phi$ もしくは $C_1 = C_2$ が成り立つ. よって, 集合 S 上の全ての異なる同値類 $C_a (a \in A)$ を考えると, $C_i \cap C_j = \phi (i \neq j,\ i, j \in A)$ かつ, $\bigcup_{a \in A} C_a = S$ となる.

定義 1.1.2 S 上の同値関係 $\sim$ に対する全ての同値類の集合, つまり $\{C(x) | x \in S\}$ を S の $\sim$ による**商集合**といい, $S/\sim$ と表す.

定義 1.1.3 n を正の整数とし, $\mathbb{Z}$ 上の同値関係 $\sim$ を次のように定める. すなわち $x, y \in \mathbb{Z}$ に対して

$$x \sim y \Leftrightarrow \text{ある } k(\in \mathbb{Z}) \text{ が存在して } x - y = nk$$

とする. 実際, この $\sim$ は同値関係であり, このとき $\mathbb{Z}/\sim$ を $\mathbb{Z}/n\mathbb{Z}$ と表す. また, $x \in \mathbb{Z}$ の定める同値類 $C(x) = \{y \in \mathbb{Z} | y = x + nk, k \in \mathbb{Z}\}$ を $\overline{x}$ と表す.

例 1.1.4 $\mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ である. また, $\overline{-2} = \overline{3} = \overline{8}$ である.

定義 1.1.5 集合 R が2つの演算 $+$（加法）と $\cdot$（乗法）を持ち, 次を満たすとき, R を (**可換**) **環** という.

1. 任意の元 $x, y, z \in R$ に対して $x + (y + z) = (x + y) + z$ および $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ が成り立つ.
2. 任意の元 $x, y \in R$ に対して $x + y = y + x$ および $x \cdot y = y \cdot x$ が成り立つ.
3. ある元 $0 \in R$ が存在して, 任意の元 $x \in R$ に対して $x + 0 = x$ となる.
4. ある元 $1 \in R$ が存在して, 任意の元 $x \in R$ に対して $x \cdot 1 = x$ となる.
5. 任意の元 $x \in R$ に対して, ある元 $x' \in R$ が存在して, $x + x' = 0$ が成り立つ.
6. 任意の元 $x, y, z \in R$ に対して $x \cdot (y + z) = x \cdot y + x \cdot z$ が成り立つ.

環の元 x, y に対して, $xy = yx$ が成り立たないような非可換環も存在するが, 本論文では非可換環は考えないので, 以後環といえば全て可換環のこととする. また, 通常は環の乗法の記号 $\cdot$ は省略する.

定義 1.1.6 環 R 上の元 x に対し, ある元 $x' \in R$ が存在して, $xx' = 1$ が成り立つとき, x を**単元**といい, x' を x の**逆元**という.

命題 1.1.7 m を正の整数とするとき, $\mathbb{Z}/m\mathbb{Z}$ 上に加法と乗法を次のように

$$\overline{a}\,\overline{b} = \overline{ab} \qquad (a, b \in \mathbb{Z})$$

$$\overline{a} + \overline{b} = \overline{a + b} \qquad (a, b \in \mathbb{Z})$$

と定めると, 演算の結果は代表元の取り方によらず well-defined である.

証明　$\overline{a} = \overline{a'}, \overline{b} = \overline{b'}$ のとき, $\overline{ab} = \overline{a'b'}, \overline{a + b} = \overline{a' + b'}$ であることを示す.

ある $s, t \in \mathbb{Z}$ が存在して, $a' = a + sm, b' = b + tm$ とすると,

$$\begin{aligned} a'b' &= (a + sm)(b + tm) \\ &= ab + m(at + bs) + stm^2 \\ &= ab + m(at + bs + stm) \end{aligned}$$

$at+bs+stm$ は整数なので, $\overline{ab}=\overline{a'b'}$ となる. さらに,

$$\begin{aligned} a'+b' &= (a+sm)+(b+tm) \\ &= (a+b)+(sm+tm) \\ &= (a+b)+m(s+t) \end{aligned}$$

$s+t$ は整数なので, $\overline{a+b}=\overline{a'+b'}$ となる. ゆえに well-defined である. □

m を正の整数とすると, 上記の加法, 乗法により $\mathbb{Z}/m\mathbb{Z}$ は環になる. 実際, 定義 1.1.5 と $\mathbb{Z}$ 上の和, 積の性質から, $\mathbb{Z}/m\mathbb{Z}$ が環であることはほとんど自明である.

定義 1.1.8 環 R において, 0 以外の任意の元 x が逆元を持つとき, R を **体** という.

$\mathbb{Q},\mathbb{R},\mathbb{C}$ は通常の加法, 乗法により体であることは容易に分かる. しかしこれ以外にも体は存在する. 特に次の定理に示すように, 有限集合である体も存在する.

定理 1.1.9 p を素数とすると, $\mathbb{Z}/p\mathbb{Z}$ は体になる.

証明　$\mathbb{Z}/p\mathbb{Z}$ の $\overline{0}$ 以外の任意の元 $\bar{a}$ をとる. $\mathbb{Z}/p\mathbb{Z}=\{\overline{0},\cdots,\overline{p-1}\}$ なので, a は $1,\cdots,p-1$ のどれかであるとしてよい. このとき $\bar{a}\bar{b}=\overline{1}$ となる $\overline{b}\in\mathbb{Z}/p\mathbb{Z}$ が存在すればよい. つまり, $1\leq a\leq p-1$ となる整数 a に対して, $ab-pn=1$ となる $b,n\in\mathbb{Z}$ が存在すればよい.

今, p は素数なので, a は p と互いに素である. したがって, a と p の最大公約数は 1 であるので, ユークリッドの互除法を用いれば, $ax+py=1$ となる $x,y\in\mathbb{Z}$ が存在することが分かる. ここで $b=x,n=-y$ とすれば, $ab-pn=1$ であるから, $\bar{a}\bar{b}=\overline{1}$ となり, $\bar{a}$は $\mathbb{Z}/p\mathbb{Z}$ の単元となる. よって $\mathbb{Z}/p\mathbb{Z}$ は体である. □

以後, $\mathbb{Z}/p\mathbb{Z}$ を $\mathbb{F}_p$ と表すこととし, $\mathbb{F}_p$ の元 $\bar{a}(a\in\mathbb{Z})$ を単に a と表記する.

1.2　ベクトル空間

本論文では, 体 $\mathbb{F}_p$ 上のベクトル空間を考えるわけだが, まずは一般の体 $\mathbb{K}$ 上のベクトル空間と, そこで成り立つ性質について述べる.

定義 1.2.1 集合Vが次の2つの演算を持ち,以下の性質を満たすとき,Vを$\mathbb{K}$上の**ベクトル空間**という.

演算1: Vの2つの元$\boldsymbol{x},\boldsymbol{y}$に対して,$V$の元$\boldsymbol{x}+\boldsymbol{y}$を定める演算(ベクトルの和)

演算2: $\mathbb{K}$の元kとVの元$\boldsymbol{x}$に対して,Vの元$k\boldsymbol{x}$を定める演算(スカラー倍)

性質

1. 任意の元$\boldsymbol{x},\boldsymbol{y},\boldsymbol{z}\in V$に対し,$(\boldsymbol{x}+\boldsymbol{y})+\boldsymbol{z}=\boldsymbol{x}+(\boldsymbol{y}+\boldsymbol{z})$および$\boldsymbol{x}+\boldsymbol{y}=\boldsymbol{y}+\boldsymbol{x}$が成り立つ.
2. ある元$\boldsymbol{0}\in V$が存在して,任意の元$\boldsymbol{x}\in V$に対して$\boldsymbol{x}+\boldsymbol{0}=\boldsymbol{x}$となる.
3. 任意の元$\boldsymbol{x}$に対して,ある元$\boldsymbol{x'}\in V$が存在して,$\boldsymbol{x}+\boldsymbol{x'}=\boldsymbol{0}$となる.
4. $1,0\in\mathbb{K}$と任意の元$\boldsymbol{x}\in V$に対し,$1\cdot\boldsymbol{x}=\boldsymbol{x}$および$0\cdot\boldsymbol{x}=\boldsymbol{0}$が成り立つ.
5. 任意の元$k,l\in\mathbb{K}$および$\boldsymbol{x}\in V$に対して,$(kl)\boldsymbol{x}=k(l\boldsymbol{x})$が成り立つ.
6. 任意の元$k,l\in\mathbb{K}$および$\boldsymbol{x},\boldsymbol{y}\in V$に対して,$(k+l)\boldsymbol{x}=k\boldsymbol{x}+l\boldsymbol{x}$および$k(\boldsymbol{x}+\boldsymbol{y})=k\boldsymbol{x}+k\boldsymbol{y}$が成り立つ.

以後,定義1.2.1と同様に,ベクトル空間の元は太字,スカラー($\mathbb{K}$の元)は通常の文字で表すこととする.

例 1.2.2 n個の$\mathbb{K}$の元の組の集合$\mathbb{K}^n=\{(a_1,\cdots,a_n)|a_1,\cdots,a_n\in K\}$において,$\mathbb{K}^n\ni(a_1,\cdots,a_n),(b_1,\cdots,b_n)$と$\lambda\in\mathbb{K}$に対し,

$$(a_1,\cdots,a_n)+(b_1,\cdots,b_n)=(a_1+b_1,\cdots,a_n+b_n)$$

$$\lambda(a_1,\cdots,a_n)=(\lambda a_1,\cdots,\lambda a_n)$$

という演算を定義すると,$\mathbb{K}^n$は$\mathbb{K}$上のベクトル空間である.

ここでは,$\mathbb{K}^n$の元を,$\mathbb{K}$の元を横にn個並べた横ベクトルとして表したが,以後,$\mathbb{K}^n$の元を,$\mathbb{K}$の元を縦にn個並べた縦ベクトルとして扱うこともある.

定義 1.2.3 ベクトル空間Vの$\emptyset$でない部分集合WがVの**部分空間**であるとは以下が成り立つことである.

1. $\boldsymbol{a}, \boldsymbol{b} \in W$のとき, $\boldsymbol{a}+\boldsymbol{b} \in W$が成り立つ.
2. $\boldsymbol{a} \in W$のとき, 任意の$\mathbb{K}$の元λに対し$\lambda\boldsymbol{a} \in W$が成り立つ.

定理 1.2.4 ベクトル空間Vの部分集合Wにおいて, 次の2つは同値である.

1. WがVの部分空間である.
2. 任意の元$\boldsymbol{a}, \boldsymbol{b} \in W$と, 任意の元$\lambda, \mu \in \mathbb{K}$に対し$\lambda\boldsymbol{a}+\mu\boldsymbol{b} \in W$が成り立つ.

証明　Wが部分空間であるとすると, $\mathbf{a}, \mathbf{b} \in \mathbf{W}$のとき, $\lambda\boldsymbol{a}, \mu\boldsymbol{b} \in W$である. Wは部分空間なので, $\lambda\boldsymbol{a}, \mu\boldsymbol{b} \in W$のとき, $\lambda\boldsymbol{a}+\mu\boldsymbol{b} \in W$となる.

逆に, $\mathbb{K}$の元λ, μに対し, $\lambda\boldsymbol{a}+\mu\boldsymbol{b} \in W$が成り立つとき, $\lambda=\mu=1$とすれば定義1.2.3の1を得る. $\mu=0$とすれば定義1.2.3の2を得る. よって逆も成り立つ. □

定理 1.2.5 $\mathbb{K}$上のベクトル空間Vの元$\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$に対して, Vの部分集合Wを,

$$W = \{\lambda_1\boldsymbol{a}_1 + \cdots + \lambda_m\boldsymbol{a}_m \in \mathbb{K}^n \mid \lambda_1, \cdots, \lambda_m \in \mathbb{K}\}$$

とおくとき, WはVの部分空間になる.

証明　Wの元$\boldsymbol{x}, \boldsymbol{y}$をそれぞれ

$$\boldsymbol{x} = \lambda_1\boldsymbol{a}_1 + \cdots + \lambda_m\boldsymbol{a}_m(\lambda_i \in \mathbb{K})$$

$$\boldsymbol{y} = \mu_1\boldsymbol{a}_1 + \cdots + \mu_m\boldsymbol{a}_m(\mu_i \in \mathbb{K})$$

とすると, $\mathbb{K}$の元λ, μに対して

$$\lambda\boldsymbol{x}+\mu\boldsymbol{y} = (\lambda\lambda_1+\mu\mu_1)\boldsymbol{a}_1 + \cdots (\lambda\lambda_m+\mu\mu_m)\boldsymbol{a}_m \in W$$

となるので, WはVの部分空間となる. □

定義 1.2.6 上記のWを$\boldsymbol{a}_1,\cdots,\boldsymbol{a}_m$によって**生成される部分空間**といい，$\langle \boldsymbol{a}_1,\cdots,\boldsymbol{a}_m\rangle$と表す．また，$\mathbb{K}$上のベクトル空間$V$とその元$\boldsymbol{a}_1,\cdots,\boldsymbol{a}_m$に対して，$V=\langle \boldsymbol{a}_1,\cdots,\boldsymbol{a}_m\rangle$のとき，$\boldsymbol{a}_1,\cdots,\boldsymbol{a}_m$は$V$を**生成する**ともいう．

定義 1.2.7 $\mathbb{K}$上のベクトル空間Vにおいて，Vの元$\boldsymbol{a}_1,\cdots,\boldsymbol{a}_m$が，$\mathbb{K}$上**一次独立**であるとは次が成り立つことである．

- $\lambda_1\boldsymbol{a}_1+\cdots+\lambda_m\boldsymbol{a}_m=\boldsymbol{0}$ならば$\lambda_1=\cdots=\lambda_m=0$ $(\lambda_1,\cdots,\lambda_m\in\mathbb{K})$

例えば1つのベクトル，$\boldsymbol{x}$が一次独立であるとは，$\lambda\boldsymbol{x}=\boldsymbol{0}$のとき，$\lambda=0$となることである．したがって，$\boldsymbol{x}\neq\boldsymbol{0}$であることに等しい．

また，Vの元$\boldsymbol{a}_1,\cdots,\boldsymbol{a}_m$が，$\mathbb{K}$上**一次従属**であるとは次が成り立つことである．実際，一次従属であるとは，一次独立であることの否定となっている．

- $\mathbb{K}$の元$\lambda_1,\cdots,\lambda_m$で，$\lambda_1,\cdots,\lambda_m$のどれかは0でなく，$\lambda_1\boldsymbol{a}_1+\cdots+\lambda_m\boldsymbol{a}_m=\boldsymbol{0}$を満たすものが存在する．

$\boldsymbol{a},\boldsymbol{a}_1,\cdots,\boldsymbol{a}_m$において，$\boldsymbol{a}$が$\boldsymbol{a}_1,\cdots,\boldsymbol{a}_m$のそれぞれのスカラー倍の和$\boldsymbol{a}=\lambda_1\boldsymbol{a}_1+\cdots+\lambda_m\boldsymbol{a}_m$で表されるとき，$\boldsymbol{a}$は$\boldsymbol{a}_1,\cdots,\boldsymbol{a}_m$の**一次結合**で表されるという．

定理 1.2.8 自然数m,nに対し，$m<n$のとき，$\mathbb{K}$上のベクトル空間Vの元$\boldsymbol{x}_1,\cdots,\boldsymbol{x}_{\boldsymbol{n}}$が一次独立ならば，$\boldsymbol{x}_1,\cdots,\boldsymbol{x}_{\boldsymbol{m}}$も一次独立である．

証明　$\lambda_1\boldsymbol{x}_1+\cdots+\lambda_m\boldsymbol{x}_{\boldsymbol{m}}=\boldsymbol{0}$とすると，

$$\lambda_1\boldsymbol{x}_1+\cdots+\lambda_m\boldsymbol{x}_{\boldsymbol{m}}+0\boldsymbol{x}_{\boldsymbol{m+1}}+\cdots+0\boldsymbol{x}_{\boldsymbol{n}}=\boldsymbol{0}$$

である．$\boldsymbol{x}_1,\cdots,\boldsymbol{x}_{\boldsymbol{n}}$は一次独立なので，$\lambda_1=\cdots=\lambda_m=0$である．ゆえに$\boldsymbol{x}_1,\cdots,\boldsymbol{x}_{\boldsymbol{m}}$は一次独立である．　□

定理 1.2.9 $\mathbb{K}$上のベクトル空間Vにおいて，Vの元$\boldsymbol{a}_1,\cdots,\boldsymbol{a}_m$が一次従属であることは，$\boldsymbol{a}_1,\cdots,\boldsymbol{a}_m$のうちのどれかが他のベクトルの一次結合で表されることと同値である．

証明　$\boldsymbol{a}_1,\cdots,\boldsymbol{a}_m$が一次従属であるとすれば，$\lambda_1\boldsymbol{a}_1+\cdots+\lambda_m\boldsymbol{a}_m=\boldsymbol{0}$において，$\lambda_1,\cdots,\lambda_m$のどれかが0でないものが存在する．ここで，順番を入れ替えて$\lambda_1\neq0$としてよい．$\lambda_1\boldsymbol{a}_1$を移項して

$$-\lambda_1\boldsymbol{a}_1=\lambda_2\boldsymbol{a}_2+\cdots+\lambda_m\boldsymbol{a}_m$$

両辺を $-\lambda_1$ で割ると,

$$\boldsymbol{a}_1 = -\left(\frac{\lambda_2}{\lambda_1}\boldsymbol{a}_2 + \cdots + \frac{\lambda_m}{\lambda_1}\boldsymbol{a}_m\right)$$

となり, $\boldsymbol{a}_1$ が $\boldsymbol{a}_2, \cdots, \boldsymbol{a}_m$ の一次結合で表される.

逆に, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ のうちのどれかが他のベクトルの一次結合で表されるとき, 定義 1.2.7 より, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ が一次従属であることは明らかである. □

定義 1.2.10 $\mathbb{K}$ 上のベクトル空間 V において, V の元 $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ が V の**基底**であるとは, 以下の2つの条件が成り立つことである.

1. $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ が一次独立である.
2. $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ が V を生成する.

例 1.2.11 $\mathbb{K}^n$ の中で, i 番目の成分が 1 で, それ以外の成分が 0 であるベクトル $\boldsymbol{e}_i$ を考えると, 集合 $\{\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n\}$ は $\mathbb{K}^n$ の基底になる. これを**標準基底**という.

定理 1.2.12 $\mathbb{K}$ 上のベクトル空間 V において, V の元 $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ が基底のとき, V の任意の元 $\boldsymbol{a}$ は, $\boldsymbol{a} = \lambda_1\boldsymbol{a}_1 + \cdots + \lambda_m\boldsymbol{a}_m$ と一意的に表される.

証明　$\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ は基底であるので, V の任意の元 $\boldsymbol{a}$ が $\boldsymbol{a} = \lambda_1\boldsymbol{a}_1 + \cdots + \lambda_m\boldsymbol{a}_m$ と表されることは明らかである. よって, 以下に表示の一意性を示す. ここで, $\boldsymbol{a}$ が

$$\boldsymbol{a} = \lambda_1\boldsymbol{a}_1 + \cdots + \lambda_m\boldsymbol{a}_m$$

$$\boldsymbol{a} = \mu_1\boldsymbol{a}_1 + \cdots + \mu_m\boldsymbol{a}_m$$

と表されたとすると, 両辺の差をとって,

$$(\lambda_1 - \mu_1)\boldsymbol{a}_1 + \cdots + (\lambda_m - \mu_m)\boldsymbol{a}_m = \boldsymbol{0}$$

となる. $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ は一次独立なので, $\lambda_1 - \mu_1 = \cdots = \lambda_m - \mu_m = 0$ である. ゆえに $\lambda_i = \mu_i$ となり, 一意性が示された. □

定理 1.2.13 $\mathbb{K}$ 上のベクトル空間 V において, V の元 $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_r$ が一次独立でかつ $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ の一次結合で表されるとき, 以下が成り立つ.

1. $r < m$

2. $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ の順序をうまくとりなおすと

$$\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_m \rangle = \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_r, \boldsymbol{a}_{r+1}, \cdots, \boldsymbol{a}_m \rangle$$

が成り立つ.

証明　(STEP1)

まず, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ の順を適当に入れかえると

$$\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_m \rangle = \langle \boldsymbol{b}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_m \rangle$$

となることを示す.

$\boldsymbol{b}_1$ は $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ の一次結合で表されるので, $\mathbb{K}$ の元 λ_i を用いて,

$$\boldsymbol{b}_1 = \lambda_1 \boldsymbol{a}_1 + \cdots + \lambda_m \boldsymbol{a}_m \tag{1.1}$$

と表される. 定理 1.2.8 より $\boldsymbol{b}_1$ は一次独立なので $\boldsymbol{b}_1 \neq \boldsymbol{0}$ である. したがって $\lambda_1, \cdots, \lambda_m$ のうち少なくとも一つは 0 でない λ_i が存在する. ここで, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ の順番を入れ替えて $\lambda_1 \neq 0$ としてよいので, 式 (1.1) の $\boldsymbol{a}_1$ と $\boldsymbol{b}_1$ を移項して両辺を $-\lambda_1$ で割ると,

$$\boldsymbol{a}_1 = \frac{1}{\lambda_1}\boldsymbol{b}_1 + \left(-\frac{\lambda_2}{\lambda_1}\right)\boldsymbol{a}_2 + \cdots + \left(-\frac{\lambda_m}{\lambda_1}\right)\boldsymbol{a}_m$$

となる. ゆえに $\boldsymbol{a}_1$ は $\boldsymbol{b}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_m$ の一次結合で表される. つまり, $\boldsymbol{a}_1 \in \langle \boldsymbol{b}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_m \rangle$ であるので,

$$\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_m \rangle \subset \langle \boldsymbol{b}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_m \rangle$$

となる.

一方 $\boldsymbol{b}_1$ は $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ の一次結合で表されるので, $\langle \boldsymbol{b}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_m \rangle$ の任意の元は $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ の一次結合で表せる. よって

$$\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_m \rangle \supset \langle \boldsymbol{b}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_m \rangle$$

となる. ゆえに

$$\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_m \rangle = \langle \boldsymbol{b}_1, \boldsymbol{a}_2, \cdots, \boldsymbol{a}_m \rangle$$

である.

(STEP2)

$k < m$ となる k に対して,

$$\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_m \rangle = \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_k, \boldsymbol{a}_{k+1}, \cdots, \boldsymbol{a}_m \rangle \tag{1.2}$$

が成り立つとき, $\boldsymbol{a}_{k+1}, \cdots, \boldsymbol{a}_m$ の順をうまくとれば,

$$\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_m \rangle = \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_{k+1}, \boldsymbol{a}_{k+2}, \cdots, \boldsymbol{a}_m \rangle \tag{1.3}$$

となることを (STEP1) と同様の方法で示す.

まず, $\boldsymbol{b}_{k+1}$ も $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ の一次結合で表されるので, 式 (1.2) より $\boldsymbol{b}_{k+1}$ は $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_k, \boldsymbol{a}_{k+1}, \cdots, \boldsymbol{a}_m$ の一次結合でも表される. よって, $\mathbb{K}$ の元 μ_i を用いて,

$$\boldsymbol{b}_{k+1} = \mu_1 \boldsymbol{b}_1 + \cdots + \mu_k \boldsymbol{b}_k + \mu_{k+1} \boldsymbol{a}_{k+1} \cdots + \mu_m \boldsymbol{a}_m \tag{1.4}$$

となる. $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_{k+1}$ は一次独立なので, $\mu_{k+1}, \cdots, \mu_m$ の中に, 少なくとも一つは 0 でない $\mu_l (k+1 \leq l \leq m)$ が存在する. $\boldsymbol{a}_{k+1}, \cdots, \boldsymbol{a}_m$ の順番を入れ替えて, $\mu_{k+1} \neq 0$ とすると, (STEP1) と同様にして

$$\boldsymbol{a}_{k+1} = \left(-\frac{\mu_1}{\mu_{k+1}}\right) \boldsymbol{b}_1 + \cdots + \left(\frac{1}{\mu_{k+1}}\right) \boldsymbol{b}_{k+1} + \left(-\frac{\mu_{k+2}}{\mu_{k+1}}\right) \boldsymbol{a}_{k+2} + \cdots + \left(-\frac{\mu_m}{\mu_{k+1}}\right) \boldsymbol{a}_m$$

と表される. つまり $\boldsymbol{a}_{k+1} \in \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_{k+1}, \boldsymbol{a}_{k+2} \cdots, \boldsymbol{a}_m \rangle$ であり, $\boldsymbol{a}_i (i = 1, \cdots, k)$ は式 (1.2) より $\boldsymbol{a}_i \in \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_k, \boldsymbol{a}_{k+1} \cdots, \boldsymbol{a}_m \rangle$ なので

$$\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_m \rangle \subset \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_{k+1}, \boldsymbol{a}_{k+2} \cdots, \boldsymbol{a}_m \rangle$$

となる.

一方式 (1.4) より $\boldsymbol{b}_{k+1}$ は $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ の一次結合で表されるので, 式 (1.2) と合わせて考えれば, $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_{k+1}, \boldsymbol{a}_{k+2} \cdots, \boldsymbol{a}_m$ は $\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_m \rangle$ に含まれる. よって,

$$\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_m \rangle \supset \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_{k+1}, \boldsymbol{a}_{k+2} \cdots, \boldsymbol{a}_m \rangle$$

となる. ゆえに

$$\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_m \rangle = \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_{k+1}, \boldsymbol{a}_{k+2} \cdots, \boldsymbol{a}_m \rangle$$

となり, 式 (1.3) が示された.

(STEP3)

ここで$r > m$とすると,

$$\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_m \rangle = \cdots = \langle \boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_{m-1}, \boldsymbol{a}_m \rangle = \langle \boldsymbol{b}_1, \boldsymbol{b}_2, \cdots, \boldsymbol{b}_m \rangle$$

となるまで(STEP2)の操作を繰り返せる. $\boldsymbol{b}_{m+1}$も$\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$の一次結合で表されるので,

$$\boldsymbol{b}_{m+1} \in \langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_m \rangle = \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_m \rangle$$

となり, $\boldsymbol{b}_{m+1}$が$\boldsymbol{b}_1, \cdots, \boldsymbol{b}_m$の一次結合で表されることになる. これは$\boldsymbol{b}_1, \cdots, \boldsymbol{b}_r$が一次独立であることに矛盾する. よって$r \leq m$となり, 主張の1が示された.

$r \leq m$より, 以上の操作をr回繰り返すと

$$\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_m \rangle = \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_r, \boldsymbol{a}_{r+1}, \cdots, \boldsymbol{a}_m \rangle$$

となり, 主張の2が示された. □

定理 1.2.14 $\mathbb{K}$上のベクトル空間Vにおいて, 2組の基底$\{\boldsymbol{a}_1, \cdots, \boldsymbol{a}_r\}$, $\{\boldsymbol{b}_1, \cdots, \boldsymbol{b}_s\}$が存在するとき, $r = s$である.

証明　$\boldsymbol{a}_1, \cdots, \boldsymbol{a}_r$は$V$の基底であり, Vを生成するので, $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_s \in \langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_r \rangle$である. したがって, 定理1.2.13より$s \leq r$となる.

同様に, $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_s$は$V$の基底であり, Vを生成するので, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_r \in \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_s \rangle$である. よって, 定理1.2.13より$r \leq s$となる.

以上より, $r = s$となる. □

定理1.2.14より, 基底を構成するベクトルの個数は, 基底の取り方によらず常に一定である. そこで, これを用いて以下を定める.

定義 1.2.15 $\mathbb{K}$上のベクトル空間Vにおいて, 基底のベクトルの個数を**次元**といい, $\dim V$と表す.

一般のベクトル空間Vにおいて常に基底が存在するとは限らないが, 以下の定理より$\mathbb{K}^n$の部分空間Wには常に基底が存在する.

定理 1.2.16 $\mathbb{K}^n$の部分空間Wに対して, Wの基底が存在する.

証明　$\mathbb{K}^n$上には標準基底$\{\boldsymbol{e}_1, \cdots, \boldsymbol{e}_n\}$が存在する. $\mathbb{K}^n$の一次独立なベクトル$\boldsymbol{a}_1, \cdots, \boldsymbol{a}_r$は$\boldsymbol{a}_1, \cdots, \boldsymbol{a}_r \in \langle \boldsymbol{e}_1, \cdots, \boldsymbol{e}_n \rangle$なので, 定理1.2.13より

$r \leq n$ である. よって, $\mathbb{K}^n$ の部分空間 W 内の一次独立なベクトルはいくらでも多くとることはできず, W 内に一次独立なベクトルの最大個数が存在する. この一次独立なベクトルを $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_m$ とする. これが基底であることを示す.

$\boldsymbol{b}_1, \cdots, \boldsymbol{b}_m$ は一次独立なベクトルの最大個数であるので, 任意の $\boldsymbol{b} \in W$ に対し, $\boldsymbol{b}, \boldsymbol{b}_1, \cdots, \boldsymbol{b}_m$ は従属である. よって $\lambda_0\boldsymbol{b} + \lambda_1\boldsymbol{b}_1 + \cdots + \lambda_m\boldsymbol{b}_m = \boldsymbol{0}$ において, 少なくとも1つは0でない $\lambda_i (\in \mathbb{K})$ が存在する. ここで, $\lambda_0 = 0$ とすると, $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_m$ が一次独立であることに矛盾するので, $\lambda_0 \neq 0$ である. ゆえに $\boldsymbol{b} = -\dfrac{1}{\lambda_0}(\lambda_1\boldsymbol{b}_1 + \cdots + \lambda_m\boldsymbol{b}_m)$ となり, $\boldsymbol{b} \in \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_m \rangle$ である. よって, $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_m$ は一次独立かつ W を生成するので, W の基底となる. □

系 1.2.17 V が $\mathbb{K}$ 上の有限次元のベクトル空間なら, V の部分空間 W にも基底は存在して, $\dim W \leq \dim V$ が成り立つ.

次元が有限で係数体が有限体であるとき, 以下に示すようにベクトル空間は有限集合である.

定理 1.2.18 $\mathbb{K}$ は $\#\mathbb{K} = p$ の有限体とする. $\mathbb{K}$ 上の次元 k のベクトル空間 V において, $\#V = p^k$ が成り立つ. ただし有限集合 X に対して, $\#X$ は X の元の個数のことである.

証明　V の基底を $\boldsymbol{x}_1, \cdots, \boldsymbol{x}_k$ とすると, V の任意の元 $\boldsymbol{y}$ は $\boldsymbol{y} = \lambda_1\boldsymbol{x}_1 + \cdots + \lambda_k\boldsymbol{x}_k$ $(\lambda_i \in \mathbb{K})$ と一意的に表される. したがって, V の元の個数は λ_1 から λ_k の組み合わせで決まる. $\lambda_i \in \mathbb{K}$ は p 通り考えられるので, 組み合わせ方は p^k 個である. □

1.3　線型写像

先に述べたように本論文では $\mathbb{F}_p$ 上の線形代数を扱うが, この節で述べる線型写像の性質は, 一般の体 $\mathbb{K}$ でも成り立つものである.

定義 1.3.1 $\mathbb{K}$ 上のベクトル空間 V, W と, V から W への写像 f について, f が**線型写像**であるとは, 以下の2つを満たすことである.

- V の元 $\boldsymbol{x}, \boldsymbol{y}$ について, $f(\boldsymbol{x} + \boldsymbol{y}) = f(\boldsymbol{x}) + f(\boldsymbol{y})$ が成り立つ.

- $\mathbb{K}$の元kとVの元$\boldsymbol{x}$に対して$f(k\boldsymbol{x}) = kf(\boldsymbol{x})$が成り立つ.

定義 1.3.2 2つのベクトル空間V, Wにおいて, VからWの線型写像で, 全単射であるものが存在するとき, VとWはベクトル空間として**同型**であるといい, $V \cong W$と表す.

定義 1.3.3 fを$\mathbb{K}$上のベクトル空間VからWへの線型写像とする. このとき, Wの元$\boldsymbol{y}$のうち, ある元$\boldsymbol{x} \in V$に対して$\boldsymbol{y} = f(\boldsymbol{x})$となるものの集合を$f$の**像**といい, $\mathrm{Im}f$と表す.

また, $f(\boldsymbol{x}) = \boldsymbol{0}$となるような$V$の元$\boldsymbol{x}$の集合を$f$の**核**といい, $\mathrm{Ker}f$と表す.

定理 1.3.4 $\mathbb{K}$上のベクトル空間をV, W, fをVからWへの線型写像とする. このとき, $\mathrm{Ker}f, \mathrm{Im}f$はそれぞれ$V, W$の部分空間になる.

証明　$\mathrm{Ker}f$の任意の元$\boldsymbol{a}, \boldsymbol{b}$と$\mathbb{K}$の元$\lambda, \mu$に対し,

$$f(\lambda\boldsymbol{a} + \mu\boldsymbol{b}) = f(\lambda\boldsymbol{a}) + f(\mu\boldsymbol{b}) = \lambda f(\boldsymbol{a}) + \mu f(\boldsymbol{b}) = \lambda\boldsymbol{0} + \mu\boldsymbol{0} = \boldsymbol{0}$$

となり, $\lambda\boldsymbol{a} + \mu\boldsymbol{b}$は$\mathrm{Ker}f$の元である. よって$\mathrm{Ker}f$は$V$の部分空間である.

また, $\mathrm{Im}f$の任意の元$\boldsymbol{x}, \boldsymbol{y}$に対し, $\boldsymbol{x} = f(\boldsymbol{c}), \boldsymbol{y} = f(\boldsymbol{d})$となる$\boldsymbol{c}, \boldsymbol{d} \in V$をとれば, $\mathbb{K}$の元λ, μに対して

$$\lambda\boldsymbol{x} + \mu\boldsymbol{y} = \lambda f(\boldsymbol{c}) + \mu f(\boldsymbol{d}) = f(\lambda\boldsymbol{c}) + f(\mu\boldsymbol{d}) = f(\lambda\boldsymbol{c} + \mu\boldsymbol{d})$$

となる. $f(\lambda\boldsymbol{c} + \mu\boldsymbol{d})$は$\mathrm{Im}f$の元であるので, $\lambda\boldsymbol{x} + \mu\boldsymbol{y}$も$\mathrm{Im}f$の元である. ゆえに$\mathrm{Im}f$は$W$の部分空間である. □

定理 1.3.5 $\mathbb{K}$上のベクトル空間V, W, 及びVからWへの線型写像fについて, $\dim(\mathrm{Im}f) + \dim(\mathrm{Ker}f) = \dim V$が成り立つ.

証明　$\dim(\mathrm{Im}f) = r$, $\dim(\mathrm{Ker}f) = s$とし, $\mathrm{Im}f$の基底を$\boldsymbol{c}_1, \cdots, \boldsymbol{c}_r$とする. また, Vの元で$f(\boldsymbol{a}_i) = \boldsymbol{c}_i$となるような$\boldsymbol{a}_1, \cdots, \boldsymbol{a}_r$をとる. $\mathrm{Ker}f$の基底を$\boldsymbol{b}_1, \cdots, \boldsymbol{b}_s$としたとき, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_r, \boldsymbol{b}_1, \cdots, \boldsymbol{b}_s$が$V$の基底であることを示せばよい.

まずは$\boldsymbol{a}_1, \cdots, \boldsymbol{a}_r, \boldsymbol{b}_1, \cdots, \boldsymbol{b}_s$が一次独立であることを示す. $\mathbb{K}$の元λ_i, μ_jに対して

$$\lambda_1\boldsymbol{a}_1 + \cdots + \lambda_r\boldsymbol{a}_r + \mu_1\boldsymbol{b}_1 + \cdots + \mu_s\boldsymbol{b}_s = \boldsymbol{0} \tag{1.5}$$

とする. 両辺に f を施して

$$f(\lambda_1 \boldsymbol{a}_1 + \cdots + \lambda_r \boldsymbol{a}_r + \mu_1 \boldsymbol{b}_1 + \cdots + \mu_s \boldsymbol{b}_s) = f(\boldsymbol{0})$$

f は線型写像なので,

$$\lambda_1 f(\boldsymbol{a}_1) + \cdots + \lambda_r f(\boldsymbol{a}_r) + \mu_1 f(\boldsymbol{b}_1) + \cdots + \mu_s f(\boldsymbol{b}_s) = \boldsymbol{0}$$

となる. ここで, $f(\boldsymbol{b}_1), \cdots, f(\boldsymbol{b}_s)$ はそれぞれ $\boldsymbol{0}$ であるので,

$$\lambda_1 \boldsymbol{c}_1 + \cdots + \lambda_r \boldsymbol{c}_r = \boldsymbol{0}$$

となる. $\boldsymbol{c}_1, \cdots, \boldsymbol{c}_r$ は $\mathrm{Im}f$ の基底なので $\lambda_1 = \cdots = \lambda_r = 0$ である. これを式 (1.5) に代入して

$$\mu_1 \boldsymbol{b}_1 + \cdots + \mu_s \boldsymbol{b}_s = \boldsymbol{0}$$

となる. $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_s$ は $\mathrm{Ker}f$ の基底なので $\mu_1 = \cdots = \mu_s = 0$ である. ゆえに $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_r, \boldsymbol{b}_1, \cdots, \boldsymbol{b}_s$ は一次独立である.

次に $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_r, \boldsymbol{b}_1, \cdots, \boldsymbol{b}_s$ が V を生成していることを示す. V の任意の元 $\boldsymbol{x}$ に対して, $\boldsymbol{y} = f(\boldsymbol{x})(y \in W)$ とおくと,

$$f(\boldsymbol{x}) = \boldsymbol{y} = \lambda_1 \boldsymbol{c}_1 + \cdots + \lambda_r \boldsymbol{c}_r$$

と表せる. ここで $\boldsymbol{z} = \boldsymbol{x} - (\lambda_1 \boldsymbol{a}_1 + \cdots + \lambda_r \boldsymbol{a}_r)$ とおいて, 両辺に f を施すと,

$$f(\boldsymbol{z}) = \boldsymbol{y} - (\lambda_1 \boldsymbol{c}_1 + \cdots + \lambda_r \boldsymbol{c}_r) = \boldsymbol{0}$$

となり, $\boldsymbol{z}$ は $\mathrm{Ker}f$ の元であることがわかる. ゆえに $\boldsymbol{z}$ は

$$\boldsymbol{z} = \mu_1 \boldsymbol{b}_1 + \cdots + \mu_s \boldsymbol{b}_s$$

と表すことができる. したがって $\boldsymbol{x}$ は

$$\boldsymbol{x} = \lambda_1 \boldsymbol{a}_1 + \cdots + \lambda_r \boldsymbol{a}_r + \mu_1 \boldsymbol{b}_1 + \cdots + \mu_s \boldsymbol{b}_s$$

となり, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_r, \boldsymbol{b}_1, \cdots, \boldsymbol{b}_s$ は V を生成している.

以上より, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_r, \boldsymbol{b}_1, \cdots, \boldsymbol{b}_s$ は V の基底となる. □

1.4　行列

定義 1.4.1 成分が体 $\mathbb{K}$ の元である $m \times n$ の行列全体の集合を $M_{m,n}(\mathbb{K})$ と表す. また成分が $\mathbb{K}$ の元である $n \times n$ の行列全体の集合を $M_n(\mathbb{K})$ と表す.

定義 1.4.2 行列 $A \in M_n(\mathbb{K})$ において, $AB = BA = E$ (E : 単位行列) となるような $B \in M_n(\mathbb{K})$ が存在するとき, 行列 A は**正則である**といい, B を A の**逆行列**という. また, B を A^{-1} と表す.

定義 1.4.3 行列 $A \in M_{m,n}(\mathbb{K})$ に対して

1. 1 つの行に 0 でない数をかける.
2. 1 つの行に $\mathbb{K}$ の元 k をかけたものを他の行に加える.
3. 2 つの行を入れ替える.

のいずれかを行って新しい $m \times n$ 行列を得る操作を**行基本変形**という. また, 行を列にかえて,

1. 1 つの列に 0 でない数をかける.
2. 1 つの列に $\mathbb{K}$ の元 k をかけたものを他の列に加える.
3. 2 つの列を入れ替える.

のいずれかを行って新しい $m \times n$ 行列を得る操作を**列基本変形**という. 行基本変形と列基本変形を合わせて**基本変形**という.

定義 1.4.4 単位行列 $E \in M_n(\mathbb{K})$ に行基本変形を 1 度だけ行ったものを**基本行列**という. 容易に分かるように, 単位行列 E に列基本変形を 1 度施すことは, 行基本変形を 1 度施すことと同じである.

また, $A \in M_n(\mathbb{K})$ に対し, A に行基本変形を 1 度施すことは, 左から基本行列をかけることと等しく, A に列基本変形を 1 度施すことは, 右から基本行列をかけることと等しい.

また, 基本行列が正則であることも容易に確かめられる.

定義 1.4.5 $M_{m,n}(\mathbb{K})$ 上の 2 項関係$\sim$を以下のように定める.

$A, B \in M_{m,n}(\mathbb{K})$ に対し, A に行基本変形と列基本変形を有限回行って B にできるとき, $A \sim B$ とする.

定義 1.4.5 で定めた関係〜は, 容易に確かめられるように同値関係である.

定義 1.4.6 $m \times m$ の単位行列を E_m, $m \times n$ の零行列を $O_{m,n}$ とし, $m \times n$ の次のような行列

$$\begin{pmatrix} E_r & O_{r,n-r} \\ O_{m-r,r} & O_{m-r,n-r} \end{pmatrix}$$

を ${F_r}^{m,n}$ と表す.

定理 1.4.7 任意の $m \times n$ 行列 $A \in M_{m,n}(\mathbb{K})$ に対し, ある整数 $r(0 \leq r \leq m, n)$ があって, $A \sim {F_r}^{m,n}$ が成り立つ. つまり, m 次の基本行列の積 P と n 次の基本行列の積 Q を用いて, $PAQ = {F_r}^{m,n}$ と変形できる.

証明　行列 A に基本行列を右や左からかけることと, 行列 A に基本変形を行うことは同じなので, A に基本変形を行って ${F_r}^{m,n}$ にできればよい. 仮に A が零行列だとすると, P, Q は単位行列であればよく, $r = 0$ である.

そこで, A は零行列でないとする. このとき行や列を入れ替える基本変形を行い $(1,1)$ 成分を $a_{11} \neq 0$ とできる. 第 1 列を $\dfrac{1}{a_{11}}$ 倍して, $(1,1)$ 成分を 1 にする. この行列の第 1 行と第 1 列のスカラー倍を他の行や列に加える基本変形を行い, 第 1 行と第 1 列の a_{11} 以外の成分を全て 0 にすることができる.

このとき, A を変形した後の新たな行列 A' は

$$A' = \left(\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A'' & \\ 0 & & & \end{array}\right)$$

と表される. この A' の第 2 行から第 n 行の範囲で行基本変形, 第 2 列から第 m 列の範囲で列基本変形を行うことを考えると, 第 1 行と第 1 列には影響がないので, 上記のような基本変形は A' の基本変形と一致する. これを繰り返し, 残された行列の部分が零行列になるか, 無くなるまで行うと ${F_r}^{m,n}$ に変形することができる. □

定理 1.4.8 行列 $A, B \in M_{m,n}(\mathbb{K})$ を $A = (\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n), B = (\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ と n 個の m 次元縦ベクトルに分けて考える. このとき, A に基本変形を有限回行って B にできるならば,

$$\dim\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_n\rangle = \dim\langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\rangle \tag{1.6}$$

である.

証明　まず, B が A に列基本変形を1回行った行列である場合に式 (1.6) が正しいことを示す.

1. $\lambda \boldsymbol{a}_i = \boldsymbol{b}_i (\lambda \neq 0)$ とすると, $(\boldsymbol{a}_1, \cdots, \lambda\boldsymbol{a}_i, \cdots, \boldsymbol{a}_n) = (\boldsymbol{b}_1, \cdots, \boldsymbol{b}_i, \cdots, \boldsymbol{b}_n)$ となる. ここで, i でない任意の k に対して $\boldsymbol{a}_k = \boldsymbol{b}_k$, i に対して $\boldsymbol{a}_i = \dfrac{1}{\lambda}\boldsymbol{b}_i$ が成り立つ. ゆえに $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n \in \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\rangle$ よって $\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_n\rangle \subset \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\rangle$ が成り立つ. 逆の包含関係も同様である. したがって $\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_n\rangle = \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\rangle$ が成り立つ.

2. $\boldsymbol{a}_i + \lambda\boldsymbol{a}_j = \boldsymbol{b}_i (\lambda \neq 0)$ とすると, $(\boldsymbol{a}_1, \cdots, \boldsymbol{a}_i + \lambda\boldsymbol{a}_j, \boldsymbol{a}_{i+1}, \cdots, \boldsymbol{a}_n) = (\boldsymbol{b}_1, \cdots, \boldsymbol{b}_i, \boldsymbol{b}_{i+1}, \cdots, \boldsymbol{b}_n)$ となる. 1. と同様に, i でない任意の k に対して $\boldsymbol{a}_k = \boldsymbol{b}_k$, i に対して $\boldsymbol{a}_i = \boldsymbol{b}_i - \lambda\boldsymbol{b}_j$ が成り立つ. ゆえに $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n \in \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\rangle$ よって $\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_n\rangle \subset \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\rangle$ が成り立つ. 逆の包含関係も同様である. したがって $\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_n\rangle = \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\rangle$ が成り立つ.

3. $(\boldsymbol{a}_1 \cdots \boldsymbol{a}_j\ \boldsymbol{a}_i \cdots \boldsymbol{a}_n) = (\boldsymbol{b}_1 \cdots \boldsymbol{b}_i\ \boldsymbol{b}_j \cdots \boldsymbol{b}_n)$ とする. i, j でない任意の k に対して $\boldsymbol{a}_k = \boldsymbol{b}_k$, i に対して $\boldsymbol{a}_i = \boldsymbol{b}_j$, j に対して $\boldsymbol{a}_j = \boldsymbol{b}_i$ が成り立つ. ゆえに $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n \in \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\rangle$ よって $\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_n\rangle \subset \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\rangle$ が成り立つ. 逆の包含関係も同様である. したがって $\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_n\rangle = \langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\rangle$ が成り立つ.

よって, B が A に列基本変形を有限回行った行列である場合も正しい.

次に, $B = (\boldsymbol{b}_1, \cdots, \boldsymbol{b}_n)$ に行基本変形を行って $C = (\boldsymbol{c}_1, \cdots, \boldsymbol{c}_n)$ となるとき, $\dim\langle \boldsymbol{b}_1, \cdots, \boldsymbol{b}_n\rangle = \dim\langle \boldsymbol{c}_1, \cdots, \boldsymbol{c}_n\rangle$ となることを示す.

今, $m \times m$ の基本行列の積 P を用いて $C = PB$ と表せるとする. このとき, 基本行列は正則なので, P も正則である. まず, $\langle \boldsymbol{b}_1 \cdots \boldsymbol{b}_n\rangle$ の基底を $\boldsymbol{v}_1 \cdots \boldsymbol{v}_r$ とする. このとき, $P\boldsymbol{v}_1 \cdots P\boldsymbol{v}_r$ が $\langle \boldsymbol{c}_1 \cdots \boldsymbol{c}_n\rangle$ の基底であればよい.

まず $P\boldsymbol{v}_i \in \langle \boldsymbol{c}_1 \cdots \boldsymbol{c}_n\rangle$ を示す. $C = PB$ より

$$\boldsymbol{c}_i = P\boldsymbol{b}_i$$

であり, また $\boldsymbol{v}_i \in \langle \boldsymbol{b}_1 \cdots \boldsymbol{b}_n\rangle$ より,

$$\boldsymbol{v}_i = \lambda_1\boldsymbol{b}_1 + \cdots + \lambda_n\boldsymbol{b}_n$$

と表すことができる. よって

$$\begin{aligned} P\boldsymbol{v_i} &= \lambda_1 P\boldsymbol{b}_1 + \cdots + \lambda_n P\boldsymbol{b}_n \\ &= \lambda_1 \boldsymbol{c}_1 + \cdots + \lambda_n \boldsymbol{c}_n \end{aligned}$$

より, $P\boldsymbol{v_i} \in \langle \boldsymbol{c}_1 \cdots \boldsymbol{c}_n \rangle$ である.

次に $P\boldsymbol{v_i}$ が $\langle \boldsymbol{c}_1 \cdots \boldsymbol{c}_n \rangle$ を生成することを示す. $\boldsymbol{v}_1 \cdots \boldsymbol{v}_r$ が $\langle \boldsymbol{b}_1 \cdots \boldsymbol{b}_n \rangle$ を生成するので, 各 $\boldsymbol{b}_i$ は, $\boldsymbol{b}_i = \lambda_1 \boldsymbol{v}_1 + \cdots + \lambda_r \boldsymbol{v}_r$ の形に表せる. つまり, $\boldsymbol{c}_i = P\boldsymbol{b}_i = \lambda_1 P\boldsymbol{v}_1 + \cdots + \lambda_r P\boldsymbol{v}_r$ となる. したがって, $P\boldsymbol{v}_1 \cdots P\boldsymbol{v}_r$ は $\langle \boldsymbol{c}_1 \cdots \boldsymbol{c}_n \rangle$ を生成する.

最後に $P\boldsymbol{v}_1 \cdots P\boldsymbol{v}_r$ が一次独立であることを示す. ある係数 $\lambda_1, \cdots, \lambda_r \in \mathbb{K}$ に対して, $\lambda_1 P\boldsymbol{v}_1 + \cdots + \lambda_r P\boldsymbol{v}_r = \boldsymbol{0}$ とする. 両辺に P^{-1} を左からかければ, $\lambda_1 \boldsymbol{v}_1 + \cdots + \lambda_r \boldsymbol{v}_r = \boldsymbol{0}$ となる. $\boldsymbol{v}_1 \cdots \boldsymbol{v}_r$ は基底なので一次独立である. ゆえに $\lambda_1 = \cdots = \lambda_r = 0$ となり, $P\boldsymbol{v}_1 \cdots P\boldsymbol{v}_r$ は一次独立である. したがって $P\boldsymbol{v}_1 \cdots P\boldsymbol{v}_r$ は $\langle \boldsymbol{c}_1 \cdots \boldsymbol{c}_n \rangle$ の基底である. □

系 1.4.9 任意の行列 $A \in M_{m,n}(\mathbb{K})$ に対して, $A \sim {F_r}^{m,n}, A \sim {F_{r'}}^{m,n}$ ならば, $r = r'$ である.

証明　i 番目の成分が 1 で, それ以外の成分が 0 のベクトルを $\boldsymbol{e}_i$ とおくと, $A \sim {F_r}^{m,n}$ より, $\dim\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_n \rangle = \dim\langle \boldsymbol{e}_1 \cdots \boldsymbol{e}_r\ \boldsymbol{0} \cdots \boldsymbol{0} \rangle = r$ である.

同様に $A \sim {F_{r'}}^{m,n}$ より, $\dim\langle \boldsymbol{a}_1, \cdots, \boldsymbol{a}_n \rangle = \langle \boldsymbol{e}_1 \cdots \boldsymbol{e}_{r'}\ \boldsymbol{0} \cdots \boldsymbol{0} \rangle = r'$ である. したがって定理 1.4.8 より $r = r'$ である. □

定義 1.4.10 行列 $A \in M_{m,n}(\mathbb{K})$ に対し, $A \sim {F_r}^{m,n}$ となるとき, r を A の**階数**といい, $\operatorname{rank} A$ と表す. これは, $A = (\boldsymbol{a}_1 \cdots \boldsymbol{a}_n)$ と表したときの $\dim\langle \boldsymbol{a}_1 \cdots \boldsymbol{a}_n \rangle$ に等しい.

定理 1.4.11 行列 $A \in M_{m,n}(\mathbb{K})$ で表される線型写像 $f : \mathbb{K}^n \to \mathbb{K}^m$, $f(\boldsymbol{x}) = A\boldsymbol{x}$ に対して, $\dim(\operatorname{Im} f) = \operatorname{rank} A$ が成り立つ.

証明　$A = (\boldsymbol{a}_1 \cdots \boldsymbol{a}_n)$ とするとき,

$$\operatorname{Im} f = \{A\boldsymbol{x} | \boldsymbol{x} \in \mathbb{K}^n\} = \{\boldsymbol{a}_1 x_1 + \cdots + \boldsymbol{a}_n x_n | x_i \in \mathbb{K}\} = \langle \boldsymbol{a}_1 \cdots \boldsymbol{a}_n \rangle$$

となる. したがって $\dim(\operatorname{Im} f) = \dim\langle \boldsymbol{a}_1 \cdots \boldsymbol{a}_n \rangle = \operatorname{rank} A$ となる. □

次の補題は容易に確認できる. そのことから定理 1.4.13 が得られる.

補題 1.4.12 基本行列を転置すると基本行列である.

定理 1.4.13 行列 $A \in M_{m,n}(\mathbb{K})$ に対して, $\mathrm{rank}\, A = \mathrm{rank}\, {}^tA$ が成り立つ.

証明　$\mathrm{rank}\, A = r$ とする. このとき, 基本行列 $S_i(i = 1, \cdots, a), T_j(j = 1, \cdots, b)$ を用いて

$$S_a \cdots S_1 \, A \, T_1 \cdots T_b = {F_r}^{m,n} \tag{1.7}$$

と表せる. 式 (1.7) の両辺を転置すると,

$${}^tT_b \cdots {}^tT_1 \, {}^tA \, {}^tS_a \cdots {}^tS_a = {}^t{F_r}^{m,n} = {F_r}^{n,m}$$

となる. 命題 1.4.12 より, 基本行列の転置は基本行列なので, $\mathrm{rank}\, {}^tA = r = \mathrm{rank}\, A$ である　□

命題 1.4.14 行列 $A, B \in M_n(\mathbb{K})$ において, A, B が正則であるとき,

$$(AB)^{-1} = B^{-1}A^{-1}$$

が成り立ち, AB も正則である.

証明　$C = B^{-1}A^{-1}$ とすると, $ABC = CAB = E$ が成り立つので, C は確かに AB の逆行列である. したがって $(AB)^{-1} = B^{-1}A^{-1}$ である.　□

また, 行列の正則性と, 行列の階数には次のような関係がある.

定理 1.4.15 行列 $A, B \in M_n(\mathbb{K})$ において, 以下は同値である.

1. A が正則である.
2. $\mathrm{rank}\, A = n$ である.

証明　まず, A が正則ならば $\mathrm{rank}\, A = n$ であることを示す. 定理 1.4.7 より, A に基本行列の積 S, T を左右からかけることで $SAT = F_m$ とすることができる. 基本行列は正則なので, $m < n$ とすると,

$$AT = S^{-1}F_m = \left(\begin{array}{ccc|c} & \cdots & & 0 \\ \vdots & \ddots & \vdots & \vdots \\ & \cdots & & 0 \end{array}\right) \tag{1.8}$$

となる. 仮定より, A は正則であり, T は基本行列の積なので, このとき定理 1.4.14 より, AT は正則である. しかし, 式 (1.8) が成り立つと, どんな n 次正方行列を左から AT にかけても, その積となる行列の一番右の縦ベクトルは $\mathbf{0}$ となるので, これは AT が正則であることに矛盾する. したがって $m = n$ である.

次に, rank $A = n$ ならば A が正則であることを示す. rank $A = n$ より, A に基本行列の積 $P_n \cdots P_1, Q_1 \cdots Q_n$ を左右からかけると

$$P_n \cdots P_1 A Q_1 \cdots Q_n = F_n = E$$

となる. 基本行列は正則なので,

$$A = P_1^{-1} \cdots P_n^{-1} Q_n^{-1} \cdots Q_1^{-1}$$

となり, 定理 1.4.14 より, A は正則である. □

定理 1.4.16 行列 $A, B \in M_n(\mathbb{K})$ において, A, B が正則であることと, AB が正則であることは同値である.

証明　A, B が正則ならば AB が正則であることは定理 1.4.14 で示したので, AB が正則ならば A, B が正則であることを示す.

B が正則でないとすると, rank$B = m < n$ とすることができる. 定理 1.4.7 より $B \sim F_m$ なので, B は基本行列の積 S, T を用いて $B = SF_mT$ と表される. したがって $AB = ASF_mT$ となり, 両辺に右から T^{-1} をかけると,

$$ABT^{-1} = ASF_m = \left(\begin{array}{ccc|c} & \cdots & & 0 \\ \vdots & \ddots & \vdots & \vdots \\ & \cdots & & 0 \end{array}\right)$$

となり, 定理 1.4.15 の証明と同様に, ABT^{-1} が正則であることに矛盾する. ゆえに rank$B = n$ であり, B は正則である. 同様に A も正則である. □

定理 1.4.17 行列 A を $A \in M_n(\mathbb{K})$ として, 写像 $f : \mathbb{K}^n \to \mathbb{K}^n$ を $f(\boldsymbol{x}) = A\boldsymbol{x}$ と定めると, 以下は同値である.

1. $\dim(\mathrm{Ker} f) = 0$ である.
2. A が正則である.

証明　定理 1.3.5 より, $\dim \mathrm{Ker} f = 0$ であることは, $\dim \mathrm{Im} f = n$ であることと同値である. また, 定理 1.4.11 より, これは $\mathrm{rank}\, A = n$ と同値で, A が正則であるということを示している. よって上記の 2 つは同値である. □

1.5　行列式

この節では行列式について述べる. 実数の行列の行列式については多くの線形代数の本に書かれている. しかしここでは $\mathbb{F}_p$ を成分とする行列の行列式について述べる. 多くのことは実数の行列と同じ証明で済むので, 必要な部分のみ強調して記す. その他の部分は参考文献 [2] の pp.79-80 を参照されたい.

定義 1.5.1　n 次対称群を S_n とする. このとき, $\sigma \in S_n$ に対して, 順列 $\sigma(1), \sigma(2), \cdots, \sigma(n)$ の中で大きい数が左側に現れるようなペア, つまり $i < j$ かつ $\sigma(i) > \sigma(j)$ となる (i, j) の個数を**逆転数**という. また, $(-1)^{(\sigma\text{の逆転数})}$ を $\mathrm{sgn}(\sigma)$ と表す.

定義 1.5.2　行列 $A = (a_{ij}) \in M_n(\mathbb{F}_p)$ において,

$$\sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

を A の**行列式**といい, $\det A$ と表す.

以下, 補題 1.5.3 から補題 1.5.9 までは, 実数行列と全く同じ証明のため, 証明は割愛する.

補題 1.5.3　行列 $A \in M_n(\mathbb{F}_p)$ において,

$$\det A = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \cdots a_{\sigma(n)n}$$

である.

補題 1.5.4　$c \in \mathbb{F}_p$ とする. 行列 $A \in M_n(\mathbb{F}_p)$ において, A の第 i 行を c 倍した行列を A' とすると, $\det A' = c \det A$ が成り立つ.

補題 1.5.5　$c \in \mathbb{F}_p$ とする. 行列 $A \in M_n(\mathbb{F}_p)$ において, A の第 i 列を c 倍した行列を A' とすると, $\det A' = c \det A$ が成り立つ.

補題 1.5.6 行列 $A \in M_n(\mathbb{F}_p)$ において, A の第 i 行と第 j 行を入れ替えた行列を A' とすると, $\det A = -\det A'$ が成り立つ.

補題 1.5.7 行列 $A \in M_n(\mathbb{F}_p)$ において, A の第 i 列と第 j 列を入れ替えた行列を A' とすると, $\det A = -\det A'$ が成り立つ.

補題 1.5.8 行列 $A \in M_n(\mathbb{F}_p)$ を, n 個の横ベクトルに分けて考えて,

$$A = \begin{pmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_m \end{pmatrix}$$

とする. また, A と第 i 行以外等しく, 第 i 行が $\boldsymbol{a}_i'$ である行列を A', A と第 i 行以外等しく, 第 i 行が $\boldsymbol{a}_i + \boldsymbol{a}_i'$ である行列を A'' とすると,

$$\det A'' = \det A + \det A'$$

が成り立つ.

補題 1.5.9 行列 $A \in M_n(\mathbb{F}_p)$ を, n 個の縦ベクトルに分けて考えて,

$$A = (\boldsymbol{a}_1 \cdots \boldsymbol{a}_n)$$

とする. また, A と第 j 列以外等しく, 第 j 列が $\boldsymbol{a}_j'$ である行列を A', A と第 j 列以外等しく, 第 j 列が $\boldsymbol{a}_j + \boldsymbol{a}_j'$ である行列を A'' とすると,

$$\det A'' = \det A + \det A'$$

が成り立つ.

補題 1.5.10 については, $\mathbb{F}_2$ の場合に注意を要するので, 以下に示す. 以下, 補題 1.5.10 の証明の中では, 偶置換・奇置換の性質を用いるが, これについては既知とする. 詳しくは参考文献 [2] の pp.79-80 を参照されたい.

補題 1.5.10 行列 $A \in M_n(\mathbb{F}_p)$ を, n 個の横ベクトルに分けて考えて,

$$A = \begin{pmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_n \end{pmatrix}$$

とする. このとき, ある $\boldsymbol{a}_i, \boldsymbol{a}_j (1 \leq i \leq j \leq n)$ について, $\boldsymbol{a}_i = \boldsymbol{a}_j$ ならば, $\det A = 0$ である.

証明　もし, $p \neq 2$ ならば, 実数行列のときと同様に, 補題1.5.6より, A の $\boldsymbol{a}_i$ と $\boldsymbol{a}_j$ を入れ替えると $\det A$ は -1 倍となるので $\det A = -\det A$ が得られる. ゆえに $2\det A = 0$ となるので, $\mathbb{F}_p \ni 2 \neq 0$ より, $\det A = 0$ が得られる.

$p = 2$ のとき, つまり $\mathbb{F}_2$ 上においては $-1 = 1$ であるので, 上記の $\det A = -\det A$ から $\det A = 0$ を結論づけることができない. そこで別の方法で示す. まず, $-1 = 1$ より, 行を入れ替えても行列式は変わらないから, $\boldsymbol{a}_1 = \boldsymbol{a}_2$ として考えてもよい. このとき, $\tau = (1,2)$ を用いて, 行列式を表す和 $\sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$ を, σ が偶置換となる部分和と, σ が奇置換となる部分和に分けて考える.

$$\det A = \det \begin{pmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_m \end{pmatrix} = \sum_{\substack{\sigma \in S_n \\ \mathrm{sgn}(\sigma) = 1}} \mathrm{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} + \sum_{\substack{\sigma \in S_n \\ \mathrm{sgn}(\sigma) = 1}} \mathrm{sgn}(\sigma\cdot\tau) a_{1\sigma\cdot\tau(1)} a_{2\sigma\cdot\tau(2)} \cdots a_{n\sigma\cdot\tau(n)} \tag{1.9}$$

と表される. 上記のように $\mathbb{F}_2$ 上においては $-1 = 1$ なので, σ によらず $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\sigma\cdot\tau) = 1$ である. $\tau(1) = 2, \tau(2) = 1$ なので, 式 (1.9) は, 偶置換の集合 A_n を用いて,

$$\det A = \sum_{\sigma \in A_n} a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} + \sum_{\sigma \in A_n} a_{1\sigma(2)} a_{2\sigma(1)} \cdots a_{n\sigma(n)}$$

となる. $a_{1i} = a_{2i}$ なので,

$$\begin{aligned} \det A &= \sum_{\sigma \in A_n} a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} + \sum_{\sigma \in A_n} a_{2\sigma(2)} a_{1\sigma(1)} \cdots a_{n\sigma(n)} \\ &= \sum_{\sigma \in A_n} a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} + \sum_{\sigma \in A_n} a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} \\ &= 2 \sum_{\sigma \in A_n} a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} \end{aligned}$$

となる. $\mathbb{F}_2$ 上では $2 = 0$ であるので $\det A = 0 \in \mathbb{F}_2$ となり, 示された. □

補題 1.5.11 行列 $A \in M_n(\mathbb{F}_p)$ を, n 個の縦ベクトルに分けて考えて,

$$A = (\boldsymbol{a}_1 \cdots \boldsymbol{a}_n)$$

とする. このとき, ある $\boldsymbol{a}_i, \boldsymbol{a}_j (1 \leq i \leq j \leq n)$ について, $\boldsymbol{a}_i = \boldsymbol{a}_j$ ならば, $\det A = 0$ である.

証明　証明は補題 1.5.10 と同様である. □

以上の補題 1.5.4 から補題 1.5.11 より, 次の定理が成り立つ.

定理 1.5.12 行列 $A \in M_n(\mathbb{F}_p)$ において, $\det A \neq 0$ であるならば, A を基本変形した行列 A' も $\det A' \neq 0$ である.

定理 1.5.12 を用いることで, 行列式と行列の正則性の, 次に示す関係が証明される.

定理 1.5.13 行列 $A \in M_n(\mathbb{F}_p)$ において, 以下は同値である.

1. $\det A \neq 0$ である.
2. A は正則である.

証明　まず, 1. ならば 2. であることを示す. $\det A \neq 0$ とすると, A を基本変形しても行列式は 0 ではない. よって, $A \sim F_m$ とすると, $\det F_m \neq 0$ である. したがって, $F_m = E$ であるので, $\operatorname{rank} A = n$ である. ゆえに定理 1.4.15 より A は正則である.

次に, 2. ならば 1. であることを示す. A を正則とすると定理 1.4.15 より $\operatorname{rank} A = n$ である. したがって, $A \sim E$ であり, $\det E \neq 0$ なので $\det A \neq 0$ である. □

1.6　内積空間

ここまで一般のベクトル空間における基底, 次元や線型写像について述べてきたが, それらは係数が一般の体であっても成り立つ概念や性質であった. しかし以下で扱う内積空間に関する概念や命題の中には, $\mathbb{F}_p$ 上のベクトル空間では成り立たないものもある. それも併せて述べていく.

定義 1.6.1 $\mathbb{K}$ 上のベクトル空間 V において, $V \times V$ から $\mathbb{K}$ への写像 $(,)$ を考える. つまり V の2元 $\boldsymbol{x}, \boldsymbol{y}$ に対して, $\mathbb{K}$ の元 $(\boldsymbol{x}, \boldsymbol{y})$ が対応しているとする. この写像 $(,)$ が以下を満たすとき, 写像 $(,)$ を**双線型形式**という.

1. $(\boldsymbol{a}+\boldsymbol{b}, \boldsymbol{c}) = (\boldsymbol{a}, \boldsymbol{c}) + (\boldsymbol{b}, \boldsymbol{c}) \qquad (\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in V)$
2. $(\boldsymbol{a}, \boldsymbol{b}+\boldsymbol{c}) = (\boldsymbol{a}, \boldsymbol{b}) + (\boldsymbol{a}, \boldsymbol{c}) \qquad (\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in V)$
3. $(\lambda\boldsymbol{a}, \boldsymbol{b}) = \lambda(\boldsymbol{a}, \boldsymbol{b}) \qquad (\boldsymbol{a}, \boldsymbol{b} \in V, \lambda \in \mathbb{K})$
4. $(\boldsymbol{a}, \lambda\boldsymbol{b}) = \lambda(\boldsymbol{a}, \boldsymbol{b}) \qquad (\boldsymbol{a}, \boldsymbol{b} \in V, \lambda \in \mathbb{K})$

定義 1.6.2 $\mathbb{K}$ 上のベクトル空間 V において, 双線型形式 $(,)$ が対称, すなわち $(\boldsymbol{a}, \boldsymbol{b}) = (\boldsymbol{b}, \boldsymbol{a})$ を満たすとき, 写像 $(,)$ を**対称双線型形式**という.

定義 1.6.3 実数体上のベクトル空間 V 及び V 上の対称双線型形式 $(,)$ に対して, 任意の V の元 $\boldsymbol{a}(\neq \boldsymbol{0})$ が $(\boldsymbol{a}, \boldsymbol{a}) > 0$ を満たすとき, この対称双線型形式は**正定値**であるという. 正定値という用語は一般の体上のベクトル空間ではなくて, 実数上のベクトル空間で定義されていることに注意されたい.

定義 1.6.4 $\mathbb{R}$ 上のベクトル空間 V 上の対称双線型形式 $(,)$ が正定値のとき, $(,)$ を**内積**という. 内積であるような対称双線型形式は, V の元 $\boldsymbol{a}, \boldsymbol{b}$ に対して, $(\boldsymbol{a}, \boldsymbol{b})$ ではなく, $\langle \boldsymbol{a}, \boldsymbol{b} \rangle$ とかいて区別する.

例えば $\mathbb{F}_3$ の元では $2 = -1$ のように正負の区別がなく, 正定値性は定義できない. したがって, まずは $\mathbb{R}$ 上のベクトル空間における内積について述べる.

定義 1.6.5 内積をもつ $\mathbb{R}$ 上のベクトル空間 V の元 $\boldsymbol{a}$ に対して, $||\boldsymbol{a}||$ を $\sqrt{\langle \boldsymbol{a}, \boldsymbol{a} \rangle}$ と定義する. これを $\boldsymbol{a}$ の**長さ**という. また, V の元 $\boldsymbol{a} \neq \boldsymbol{0}$ に対して, $\boldsymbol{b} = \dfrac{1}{||\boldsymbol{a}||}\boldsymbol{a}$ とおくと, $\boldsymbol{b}$ は長さが1となる. この $\dfrac{1}{||\boldsymbol{a}||}\boldsymbol{a}$ を $\boldsymbol{a}$ の**正規化**という.

定義 1.6.6 $\mathbb{R}^n$ の元 $\boldsymbol{a} = (a_1, \cdots, a_n), \boldsymbol{b} = (b_1, \cdots, b_n)$ に対し, $\langle \boldsymbol{a}, \boldsymbol{b} \rangle = \sum_{i=1}^{n} a_i b_i$ と定めると, $\langle , \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ は内積となる. この $\langle , \rangle$ を**標準内積**という.

高校までで扱ってきたベクトル空間の内積は標準内積である. 本論文で扱う内積は標準内積とは限らず, ここでは一般的な内積について述べる.

定義 1.6.7 内積を持つ$\mathbb{R}$上のベクトル空間Vと, Vの元$\boldsymbol{a}, \boldsymbol{b}$において, $\langle \boldsymbol{a}, \boldsymbol{b} \rangle = 0$のとき, $\boldsymbol{a}, \boldsymbol{b}$は**直交する**といい, $\boldsymbol{a} \perp \boldsymbol{b}$と表す.

定義 1.6.8 $\mathbb{R}$上のベクトル空間Vにおいて, Vの元$\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$が**正規直交系**であるとは以下を満たすことである.

- $||\boldsymbol{a}_1|| = \cdots = ||\boldsymbol{a}_m|| = 1$
- $\boldsymbol{a}_i \perp \boldsymbol{a}_j \qquad (1 \leq i, j \leq m, i \neq j)$

定理 1.6.9 $\mathbb{R}$上のベクトル空間Vにおいて, 正規直交系をなすベクトルは一次独立である.

証明　Vの元$\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$を正規直交系とする. $\mathbb{K}$の元λ_iに対し$\lambda_1 \boldsymbol{a}_1 + \cdots + \lambda_m \boldsymbol{a}_m = \boldsymbol{0}$とする. 両辺について$\boldsymbol{a}_i$と内積をとると,

$$\lambda_1 \langle \boldsymbol{a}_1, \boldsymbol{a}_i \rangle + \cdots + \lambda_i \langle \boldsymbol{a}_i, \boldsymbol{a}_i \rangle + \cdots + \lambda_m \langle \boldsymbol{a}_m, \boldsymbol{a}_i \rangle = \langle \boldsymbol{0}, \boldsymbol{a}_i \rangle$$

となるが, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$は正規直交系なので

$$0 + \cdots + \lambda_i ||\boldsymbol{a}_i||^2 + \cdots + 0 = 0$$

となる. $||\boldsymbol{a}_i||^2 \neq 0$より, $\lambda_i = 0$である. iが1からmのどれであってもこの式は成り立つので$\lambda_1 = \cdots = \lambda_m = 0$である. ゆえに$\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$は一次独立である. □

定義 1.6.10 $\mathbb{R}$上のベクトル空間Vにおいて, Vの元$\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$が正規直交系かつ基底であるとき, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$を$V$の**正規直交基底**という.

定理 1.6.11 有限次元の$\mathbb{R}$上のベクトル空間Vは常に正規直交基底をもつ.

証明　$\dim V = m$として, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$を$V$の1つの基底とする. $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$を用いて新たに直交する基底$\boldsymbol{b}_1, \cdots, \boldsymbol{b}_m$を次のように作る.

$$\boldsymbol{b}_1 = \boldsymbol{a}_1$$

$$\boldsymbol{b}_2 = \boldsymbol{a}_2 - \frac{\langle \boldsymbol{b}_1, \boldsymbol{a}_2 \rangle}{\langle \boldsymbol{b}_1, \boldsymbol{b}_1 \rangle} \boldsymbol{b}_1$$

$$\boldsymbol{b}_3 = \boldsymbol{a}_3 - \frac{\langle \boldsymbol{b}_2, \boldsymbol{a}_3 \rangle}{\langle \boldsymbol{b}_2, \boldsymbol{b}_2 \rangle} \boldsymbol{b}_2 - \frac{\langle \boldsymbol{b}_1, \boldsymbol{a}_3 \rangle}{\langle \boldsymbol{b}_1, \boldsymbol{b}_1 \rangle} \boldsymbol{b}_1$$

$$\vdots$$

$$\boldsymbol{b}_m = \boldsymbol{a}_m - \frac{\langle \boldsymbol{b}_{m-1}, \boldsymbol{a}_m \rangle}{\langle \boldsymbol{b}_{m-1}, \boldsymbol{b}_{m-1} \rangle} \boldsymbol{b}_{m-1} - \cdots - \frac{\langle \boldsymbol{b}_1, \boldsymbol{a}_m \rangle}{\langle \boldsymbol{b}_1, \boldsymbol{b}_1 \rangle} \boldsymbol{b}_1$$

とすると, $\boldsymbol{b}_k$ は $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_k$ の一次結合で表すことができる. このとき, $\boldsymbol{b}_k$ が $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_{k-1}$ と直交することを $k \geq 2$ に関する帰納法で示す.

$k = 2$ のとき,

$$\begin{aligned}
\langle \boldsymbol{b}_2, \boldsymbol{b}_1 \rangle &= \langle \boldsymbol{a}_2 - \frac{\langle \boldsymbol{b}_1, \boldsymbol{a}_2 \rangle}{\langle \boldsymbol{b}_1, \boldsymbol{b}_1 \rangle} \boldsymbol{b}_1, \boldsymbol{b}_1 \rangle \\
&= \langle \boldsymbol{a}_2, \boldsymbol{b}_1 \rangle - \frac{\langle \boldsymbol{b}_1, \boldsymbol{a}_2 \rangle}{\langle \boldsymbol{b}_1, \boldsymbol{b}_1 \rangle} \langle \boldsymbol{b}_1, \boldsymbol{b}_1 \rangle \\
&= \langle \boldsymbol{a}_2, \boldsymbol{b}_1 \rangle - \langle \boldsymbol{b}_1, \boldsymbol{a}_2 \rangle \\
&= 0
\end{aligned}$$

となり, $\boldsymbol{b}_2$ は $\boldsymbol{b}_1$ と直交する.

$k = 1, \cdots, l-1$ まで正しいとして, $k = l$ のとき正しいことを示す. $l > i$ に対して,

$$\begin{aligned}
\langle \boldsymbol{b}_l, \boldsymbol{b}_i \rangle &= \langle \boldsymbol{a}_l - \frac{\langle \boldsymbol{b}_{l-1}, \boldsymbol{a}_l \rangle}{\langle \boldsymbol{b}_{l-1}, \boldsymbol{b}_{l-1} \rangle} \boldsymbol{b}_{l-1} - \cdots - \frac{\langle \boldsymbol{b}_i, \boldsymbol{a}_l \rangle}{\langle \boldsymbol{b}_i, \boldsymbol{b}_i \rangle} \boldsymbol{b}_i - \cdots - \frac{\langle \boldsymbol{b}_1, \boldsymbol{a}_l \rangle}{\langle \boldsymbol{b}_1, \boldsymbol{b}_1 \rangle} \boldsymbol{b}_1, \boldsymbol{b}_i \rangle \\
&= \langle \boldsymbol{a}_l, \boldsymbol{b}_i \rangle - \frac{\langle \boldsymbol{b}_{l-1}, \boldsymbol{a}_l \rangle}{\langle \boldsymbol{b}_{l-1}, \boldsymbol{b}_{l-1} \rangle} \langle \boldsymbol{b}_{l-1}, \boldsymbol{b}_i \rangle - \cdots - \frac{\langle \boldsymbol{b}_1, \boldsymbol{a}_l \rangle}{\langle \boldsymbol{b}_1, \boldsymbol{b}_1 \rangle} \langle \boldsymbol{b}_1, \boldsymbol{b}_i \rangle \\
&= \langle \boldsymbol{a}_l, \boldsymbol{b}_i \rangle - \frac{\langle \boldsymbol{b}_i, \boldsymbol{a}_l \rangle}{\langle \boldsymbol{b}_i, \boldsymbol{b}_i \rangle} \langle \boldsymbol{b}_i, \boldsymbol{b}_i \rangle \\
&= \langle \boldsymbol{a}_l, \boldsymbol{b}_i \rangle - \langle \boldsymbol{b}_i, \boldsymbol{a}_l \rangle \\
&= 0
\end{aligned}$$

$\boldsymbol{b}_1, \cdots, \boldsymbol{b}_m$ の作り方から, $\boldsymbol{b}_k$ は $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_k$ の一次結合で表せる. ここで $\boldsymbol{b}_k = \boldsymbol{0}$ とすると,

$$\boldsymbol{b}_k = \boldsymbol{a}_k - \frac{\langle \boldsymbol{b}_{k-1}, \boldsymbol{a}_k \rangle}{\langle \boldsymbol{b}_{k-1}, \boldsymbol{b}_{k-1} \rangle} \boldsymbol{b}_{k-1} - \cdots - \frac{\langle \boldsymbol{b}_1, \boldsymbol{a}_k \rangle}{\langle \boldsymbol{b}_1, \boldsymbol{b}_1 \rangle} \boldsymbol{b}_1 = \boldsymbol{0}$$

となり, $\boldsymbol{a}_k$ が $\boldsymbol{b}_{k-1}, \cdots, \boldsymbol{b}_1$ の一次結合で表される. すると, $\boldsymbol{a}_k$ が $\boldsymbol{a}_{k-1}, \cdots, \boldsymbol{a}_1$ の一次結合で表せるので, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_k$ が V の基底であることに矛盾する. よって, $\boldsymbol{b}_k \neq \boldsymbol{0}$ かつ, $1 \leq i \leq k-1$ において $\boldsymbol{b}_k \perp \boldsymbol{b}_i$ となる. ここで, $k = 1, \cdots, l$ に対して $\boldsymbol{c}_k = \dfrac{1}{\sqrt{\langle \boldsymbol{b}_k, \boldsymbol{b}_k \rangle}} \boldsymbol{b}_k$ とすると, $||\boldsymbol{c}_k|| = 1$ で, $\boldsymbol{c}_1, \cdots, \boldsymbol{c}_m$ は互いに直交する. つまり $\boldsymbol{c}_1, \cdots, \boldsymbol{c}_m$ は正規直交系で, 定理 1.6.9 より $\boldsymbol{c}_1, \cdots, \boldsymbol{c}_m$ は一次独立である. $\dim V = m$ より, $\boldsymbol{c}_1, \cdots, \boldsymbol{c}_m$ は正規直交基底になる. □

定義 1.6.12 $\mathbb{R}$ 上のベクトル空間 V の部分空間 W と V の元 $\boldsymbol{a}$ において, W の任意の元 $\boldsymbol{b}$ に対し, $\boldsymbol{a} \perp \boldsymbol{b}$ となるとき, $\boldsymbol{a}$ は W と**直交する**といい, $\boldsymbol{a} \perp W$ と表す.

命題 1.6.13 $\mathbb{R}$ 上のベクトル空間 V の部分空間 W に対し, $W^\perp$ を $W^\perp = \{\boldsymbol{x} \in V | \boldsymbol{x} \perp W\}$ と定めると, $W^\perp$ はベクトル空間になる.

証明　$\boldsymbol{a}, \boldsymbol{b}$ を $W^\perp$ の元, λ, μ を $\mathbb{K}$ の元とする. $\boldsymbol{a}, \boldsymbol{b}, \lambda, \mu$ に対して, $\lambda\boldsymbol{a} + \mu\boldsymbol{b}$ が $W^\perp$ の元になっていることを示す. 実際, W の任意の元 $\boldsymbol{c}$ に対して,

$$\langle \lambda\boldsymbol{a} + \mu\boldsymbol{b}, \boldsymbol{c} \rangle = \lambda\langle \boldsymbol{a}, \boldsymbol{c} \rangle + \mu\langle \boldsymbol{b}, \boldsymbol{c} \rangle = 0$$

となるから, $\lambda\boldsymbol{a} + \mu\boldsymbol{b}$ は W と直交する. ゆえに $\lambda\boldsymbol{a} + \mu\boldsymbol{b}$ は $W^\perp$ の元である. □

定義 1.6.14 上記の $W^\perp$ を W の**直交補空間**という.

命題 1.6.15 $\mathbb{R}$ 上のベクトル空間 V の部分空間 W, W' に対して以下が成り立つ.

1. $W + W' = \{\boldsymbol{a} + \boldsymbol{a}' | \boldsymbol{a} \in W, \boldsymbol{a}' \in W'\}$ と定めると, $W + W'$ は V の部分空間になる.
2. $W \cap W'$ は V の部分空間である.

証明　まず 1. を示す. W の元 $\boldsymbol{a}, \boldsymbol{b}$ 及び W' の元 $\boldsymbol{a}', \boldsymbol{b}'$ と $W + W'$ の元 $\boldsymbol{a} + \boldsymbol{a}', \boldsymbol{b} + \boldsymbol{b}'$ 及び $\mathbb{R}$ の元 λ, μ に対して,

$$\lambda(\boldsymbol{a} + \boldsymbol{a}') + \mu(\boldsymbol{b} + \boldsymbol{b}') = (\lambda\boldsymbol{a} + \mu\boldsymbol{b}) + (\lambda\boldsymbol{a}' + \mu\boldsymbol{b}') \in W + W'$$

となり, $W + W'$ は V の部分空間である.

次に2.を示す. $W \cap W'$ の元 $\boldsymbol{a}, \boldsymbol{b}$ と $\mathbb{R}$ の元 λ, μ に対して, $\boldsymbol{a}, \boldsymbol{b}$ は W の元なので, $\lambda\boldsymbol{a} + \mu\boldsymbol{b} \in W$ となる. また, $\boldsymbol{a}, \boldsymbol{b}$ は W' の元なので, $\lambda\boldsymbol{a} + \mu\boldsymbol{b}$ は W' の元である. したがって $\lambda\boldsymbol{a} + \mu\boldsymbol{b}$ は $W \cap W'$ の元になるため, $W \cap W'$ は V の部分空間になる. □

定理 1.6.16 $\mathbb{R}$ 上のベクトル空間 V の部分空間 W, W' に対して W と W' の共通部分 $W \cap W'$ が $W \cap W' = \{\boldsymbol{0}\}$ ならば, $W + W'$ の任意の元 $\boldsymbol{x}$ は W の元 $\boldsymbol{a}$ と W' の元 $\boldsymbol{a'}$ を用いて $\boldsymbol{x} = \boldsymbol{a} + \boldsymbol{a'}$ と一意的に表せる.

証明　$W + W'$ の任意の元 $\boldsymbol{x}$ が W の元 $\boldsymbol{a}$ と W' の元 $\boldsymbol{a'}$ を用いて $\boldsymbol{x} = \boldsymbol{a} + \boldsymbol{a'}$ と表されることは $W + W'$ の定義より明らかである.

そこで, $\boldsymbol{x}$ が2通りに表されたとすると, W の元 $\boldsymbol{a}, \boldsymbol{b}$ と W' の元 $\boldsymbol{a'}, \boldsymbol{b'}$ に対して, $\boldsymbol{x} = \boldsymbol{a} + \boldsymbol{a'} = \boldsymbol{b} + \boldsymbol{b'}$ とできる. これを変形すれば

$$\boldsymbol{a} - \boldsymbol{b} = \boldsymbol{b'} - \boldsymbol{a'}$$

となる. $\boldsymbol{a} - \boldsymbol{b}$ は W の元, $\boldsymbol{b'} - \boldsymbol{a'}$ は W' の元であるので, $\boldsymbol{a} - \boldsymbol{b}, \boldsymbol{b'} - \boldsymbol{a'}$ はそれぞれ $W \cap W'$ の元である.

今, $W \cap W' = \{\boldsymbol{0}\}$ なので $\boldsymbol{a} - \boldsymbol{b} = \boldsymbol{b'} - \boldsymbol{a'} = \boldsymbol{0}$ となる. ゆえに $\boldsymbol{a} = \boldsymbol{b}, \boldsymbol{a'} = \boldsymbol{b'}$ となり, 一意性が示された. □

定義 1.6.17 $\mathbb{R}$ 上のベクトル空間 V の部分空間 W, W' に対して, $W \cap W' = \{\boldsymbol{0}\}$ のとき, $W + W'$ のことを $W \oplus W'$ と表し, W と W' の**直和**という.

定理 1.6.18 有限次元の $\mathbb{R}$ 上のベクトル空間 V と V の部分空間 W に対して, $V = W \oplus W^{\perp}$ が成り立つ.

証明　まずは $V = W + W^{\perp}$ であることを示す. W の次元を m とし, W の正規直交基底を $\{\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m\}$ とする. V の任意の元 $\boldsymbol{a}$ に対して,

$$\boldsymbol{b} = \sum_{i=1}^{m} \langle \boldsymbol{a}, \boldsymbol{a}_i \rangle \boldsymbol{a}_i, \qquad \boldsymbol{c} = \boldsymbol{a} - \sum_{i=1}^{m} \langle \boldsymbol{a}, \boldsymbol{a}_i \rangle \boldsymbol{a}_i$$

とおく. このとき $\boldsymbol{a} = \boldsymbol{b} + \boldsymbol{c}$ で, $\boldsymbol{b} \in W$ は自明であるので, $\boldsymbol{c} \in W^{\perp}$ を示す. $\boldsymbol{c}$ と $\boldsymbol{a}_j$ と内積をとると,

$$\begin{aligned}\langle \boldsymbol{c}, \boldsymbol{a}_j \rangle &= \langle \boldsymbol{a} - \sum_{i=1}^{n} \langle \boldsymbol{a}, \boldsymbol{a}_i \rangle \boldsymbol{a}_i, \boldsymbol{a}_j \rangle \\ &= \langle \boldsymbol{a}, \boldsymbol{a}_j \rangle - \sum_{i=1}^{n} \langle \boldsymbol{a}, \boldsymbol{a}_i \rangle \langle \boldsymbol{a}_i, \boldsymbol{a}_j \rangle \\ &= \langle \boldsymbol{a}, \boldsymbol{a}_j \rangle - \langle \boldsymbol{a}, \boldsymbol{a}_j \rangle \langle \boldsymbol{a}_j, \boldsymbol{a}_j \rangle \\ &= 0\end{aligned}$$

となる. ゆえに W の任意の元 $\boldsymbol{x} = \lambda_1 \boldsymbol{a}_1 + \cdots + \lambda_m \boldsymbol{a}_m (\lambda_i \in \mathbb{R})$ に対し, $\langle \boldsymbol{c}, \boldsymbol{x} \rangle = \langle \boldsymbol{c}, \lambda_1 \boldsymbol{a}_1 + \cdots + \lambda_m \boldsymbol{a}_m \rangle = 0$ となり, $\boldsymbol{c}$ は $W^\perp$ の元であることが示された.

次に $W \cap W^\perp = \{\boldsymbol{0}\}$ を示す. $\boldsymbol{a}$ を $W \cap W^\perp$ の元とすると, $\boldsymbol{a} \in W$ かつ $\boldsymbol{a} \in W^\perp$ であるから $\langle \boldsymbol{a}, \boldsymbol{a} \rangle = 0$ となる. したがって $\boldsymbol{a} = \boldsymbol{0}$ であるので, $W \cap W^\perp = \{\boldsymbol{0}\}$ である.

ゆえに $V = W \oplus W^\perp$ である. □

定理 1.6.19 内積をもつ $\mathbb{R}$ 上の有限次元ベクトル空間 V の部分空間 W を考える. このとき, V の正規直交基底 $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n$ で, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ が W の正規直交基底かつ, $\boldsymbol{a}_{m+1}, \cdots, \boldsymbol{a}_n$ が $W^\perp$ の正規直交基底となるものが存在する.

証明　$\boldsymbol{a}'_1, \cdots, \boldsymbol{a}'_m$ を W の基底とする. $\boldsymbol{a}'_1, \cdots, \boldsymbol{a}'_m$ に $\boldsymbol{a}'_{m+1}, \cdots, \boldsymbol{a}'_n$ を加えた n 個のベクトルで V の基底にできる. $\boldsymbol{a}'_1, \cdots, \boldsymbol{a}'_n$ を定理1.6.11 の証明のように正規直交化して $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n$ を得ると, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_n$ は $\mathbb{R}^n$ の正規直交基底で, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ は $\boldsymbol{a}'_1, \cdots, \boldsymbol{a}'_m$ の一次結合で表されるので, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ は W の正規直交基底である. そして, $\boldsymbol{a}_{m+1}, \cdots, \boldsymbol{a}_n$ は $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ に直交するので, $\boldsymbol{a}_{m+1}, \cdots, \boldsymbol{a}_n$ は $W^\perp$ に含まれる. あとは $\boldsymbol{a}_{m+1}, \cdots, \boldsymbol{a}_n$ が $W^\perp$ の基底であればよい. $\boldsymbol{a}_{m+1}, \cdots, \boldsymbol{a}_n$ はそれぞれ直交するので一次独立である. $W^\perp$ の元 $\boldsymbol{y}$ を $\boldsymbol{y} = \lambda_1 \boldsymbol{a}_1 + \cdots + \lambda_n \boldsymbol{a}_n$ とすると, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ と $\boldsymbol{a}_i (1 \leq i \leq m)$ はそれぞれ直交するので $\langle \boldsymbol{y}, \boldsymbol{a}_i \rangle = \lambda_i = 0$ となる. ゆえに $\boldsymbol{y} = \lambda_{m+1} \boldsymbol{a}_{m+1} + \cdots + \lambda_n \boldsymbol{a}_n$ となり, $\boldsymbol{a}_{m+1}, \cdots, \boldsymbol{a}_n$ は $W^\perp$ を生成し, $W^\perp$ の基底である. □

定理1.6.19 より, 次が直ちに成り立つ.

系 1.6.20 $\mathbb{R}^n$ の部分空間 W に対し, $\dim W + \dim W^\perp = n$ が成り立つ.

ここまで $\mathbb{R}$ 上のベクトル空間での内積について述べてきたが, $\mathbb{F}_p$ には正や負といった概念がなく, 正定値性が意味をもたないので, $\mathbb{F}_p$ 上のベクトル空間では定義 1.6.4 の内積が定義できない. ただし, 標準内積であれば, ${\mathbb{F}_p}^n$ 上で類似物を考えることは可能である.

定義 1.6.21 $\mathbb{F}_p$ 上のベクトル空間 ${\mathbb{F}_p}^n$ において, ${\mathbb{F}_p}^n$ の元 $\boldsymbol{x} = (x_1, \cdots, x_n)$, $\boldsymbol{y} = (y_1, \cdots, y_n)$ に対し, $\mathbb{F}_p$ の元 $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$ を

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_{i=1}^{n} x_i y_i \in \mathbb{F}_p$$

と定める. このときこの対称双線型形式を ${\mathbb{F}_p}^n$ 上の**標準内積**という.

例えば, ${\mathbb{F}_2}^2$ の元 $(1,1)$ について, 自分自身との標準内積をとると,

$$\langle (1,1), (1,1) \rangle = 1^2 + 1^2 = 0$$

となり, $\boldsymbol{a} \neq \boldsymbol{0}$ でも $\langle \boldsymbol{a}, \boldsymbol{a} \rangle = 0$ になりうるから, 標準内積とは言っても正定値性に類する性質は成り立たない. このように $\mathbb{F}_p$ 上では, 自分自身との内積がベクトルの"大きさ" をうまく表さず, まして $\mathbb{R}$ 上のときのように平方根をとれないので, 標準内積から直接ベクトルの大きさを定義することができない.

さらに, 上記の例で, ベクトル $(1,1)$ は自分自身との内積が 0 なので, 実数係数のときと同じように"直交"の定義を使うと, 自分自身と"直交"してしまい, 通常の幾何学的なイメージの"直交"とはかけはなれた性質を持つことになる. しかしながらここではあえて $\mathbb{F}_p$ 上においての"直交"や"直交補空間"を以下のように定義する.

定義 1.6.22 $\mathbb{F}_p$ 上のベクトル空間 ${\mathbb{F}_p}^n$ の元 $\boldsymbol{x}, \boldsymbol{y}$ において, 標準内積 $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0$ となるとき, $\boldsymbol{x}, \boldsymbol{y}$ は**直交する**という.

${\mathbb{F}_p}^n$ の部分空間 W に対し, W の任意の元 $\boldsymbol{x}$ と直交するようなベクトルの集合を $W^{\perp}$ とする.

${\mathbb{F}_p}^n$ 上においても, 上記のように直交するという概念は定義できたが, 内積から大きさを定義できないので, 正規直交基底のような概念は使えない.

また, ${\mathbb{F}_2}^2$ の元 $(1,1)$ によって生成される部分空間 $\langle (1,1) \rangle$ を W とすると, $(1,1)$ と $(1,1)$ の ${\mathbb{F}_2}^2$ 上の標準内積は $\langle (1,1), (1,1) \rangle = 0$ となり, $(1,1)$ は $(1,1)$ と直交することになる. つまり, $W \cap W^{\perp} \neq \boldsymbol{0}$ となりうるので, $\mathbb{R}$ 上のベクトル空間のときと違い, W と $W^{\perp}$ は直和にならない. にもかか

わらず, 次に述べるように, $\mathbb{F}_p$ 上のベクトル空間 ${\mathbb{F}_p}^n$ の部分空間 W において, $\mathbb{R}^n$ のときと同じように $\dim W + \dim W^{\perp} = n$ が成り立つ. ただし, 正規直交基底は使えないので, $\mathbb{R}$ 係数のベクトル空間のときとは別の方法で以下に示す.

定理 1.6.23 $\mathbb{F}_p$ 上のベクトル空間 ${\mathbb{F}_p}^n$ の部分空間 W において, $\dim W + \dim W^{\perp} = n$ が成り立つ.

証明　W の基底を $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ とする. このとき, $\boldsymbol{x}$ が $W^{\perp}$ の元であることは, $1 \leq i \leq m$ に対して, $\boldsymbol{a}_i \perp \boldsymbol{x}$ となることと同値である. つまり, $\langle \boldsymbol{a}_i, \boldsymbol{x} \rangle = 0\ (i = 1, \cdots, m)$ となることが $\boldsymbol{x} \in W^{\perp}$ となるための必要十分条件である. ここで $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ を横ベクトルと考えて, これら $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m$ を縦に並べた行列を A, つまり

$$A = \begin{pmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_m \end{pmatrix}$$

とすると, $\langle \boldsymbol{a}_i, \boldsymbol{x} \rangle = 0\ (i = 1, \cdots, m)$ となることは,

$$A\boldsymbol{x} = \begin{pmatrix} \boldsymbol{0} \\ \vdots \\ \boldsymbol{0} \end{pmatrix}$$

となることと同値である. つまり ${\mathbb{F}_p}^n$ から ${\mathbb{F}_p}^m$ の写像 $f(\boldsymbol{x}) = A\boldsymbol{x}$ を考えると, $\boldsymbol{x} \in W^{\perp}$ であることは, $\boldsymbol{x}$ が $\mathrm{Ker}f$ の元であることと同値である. つまり, $W^{\perp} = \mathrm{Ker}f$ であり, $\dim W^{\perp} = \dim(\mathrm{Ker}f)$ が成り立つ.

また, このとき写像 g を $g : {\mathbb{F}_p}^m \to {\mathbb{F}_p}^n$, $g(\boldsymbol{y}) = {}^tA\boldsymbol{y}$ とすると,

$$\begin{aligned} W &= \langle \boldsymbol{a}_1 \cdots \boldsymbol{a}_m \rangle \\ &= \{ y_1\boldsymbol{a}_1 + \cdots + y_m\boldsymbol{a}_m | y_i \in \mathbb{F}_p \} \\ &= \left\{ (\boldsymbol{a}_1 \cdots \boldsymbol{a}_m) \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix} \middle| y_i \in \mathbb{F}_p \right\} \\ &= \{ {}^tA\boldsymbol{y} | \boldsymbol{y} \in {\mathbb{F}_p}^m \} \\ &= \mathrm{Im}g \end{aligned}$$

となる. 定理 1.4.11 と定理 1.4.13 より, $\dim(\mathrm{Im}g) = \mathrm{rank}\,{}^tA = \mathrm{rank}\,A = \dim(\mathrm{Im}f)$ であるから, $\dim W = \dim(\mathrm{Im}f)$ である.

一方, 定理 1.3.5 より $\dim(\mathrm{Im}f) + \dim(\mathrm{Ker}f) = n$ なので, $\dim W + \dim W^{\perp} = n$ が示された. □

系 1.6.24 $\mathbb{F}_p$ 上のベクトル空間 ${\mathbb{F}_p}^n$ の部分空間 W において, $(W^{\perp})^{\perp} = W$ が成り立つ.

証明　まず, $(W^{\perp})^{\perp} \supset W$ を示す. W の任意の元 $\boldsymbol{x}$ は, W の直交補空間 $W^{\perp}$ と直交するので, $\boldsymbol{x} \perp W^{\perp}$ である. したがって, $\boldsymbol{x}$ は $W^{\perp}$ の任意の元と直交するので, $\boldsymbol{x} \in (W^{\perp})^{\perp}$ となる. ゆえに $(W^{\perp})^{\perp} \supset W$ が示せた. また, 定理 1.6.23 より,

$$\dim W + \dim W^{\perp} = n$$

$$\dim W^{\perp} + \dim (W^{\perp})^{\perp} = n$$

が成り立つから,

$$\dim W = \dim (W^{\perp})^{\perp}$$

が得られる. $(W^{\perp})^{\perp}$ と W は次元が等しく, $(W^{\perp})^{\perp} \supset W$ の包含関係が成り立っているので, $(W^{\perp})^{\perp} = W$ が成り立つ. □

$\mathbb{R}$ 上のベクトル空間のときとは証明が異なるが, このように $\mathbb{F}_p$ 上のベクトル空間 ${\mathbb{F}_p}^n$ の部分空間 W においても, $\dim W + \dim W^{\perp} = n$ がいえる. しかし, 先に述べたように, ${\mathbb{F}_p}^n$ 上でのベクトルの"直交"は, 我々が通常思い浮かべる"直交"とは違う性質をもっていることに注意されたい.

第2章　σゲームについて

本論文では, ライツアウトパズルの解析を目標としている. ライツアウトパズルとそれに類似したパズルはいくつかあるが, その中でも有名なものは5 × 5の格子状に並んだライトをある法則に従って全て消灯させることを目的としたパズルである. 日本では1995年に株式会社タカラから発売された. 今では, インターネット上に様々な類似ゲームが存在している. 当初はライトの状態はonかoffの2つだったが, 消灯→赤→青→消灯のように, 複数の色に変わっていくライツアウトパズルも存在する. 以下, 基本となるライツアウトパズルについて説明する.

まず, たて, よこの長さが$m-1, n-1$の長方形を単位正方形に分割して, その格子点に$m \times n$個の点をとった長方形のグリッドを考える. このとき, このグリッドを$P_{m,n}$と表すことにする. 図2.1は$P_{5,6}$である.

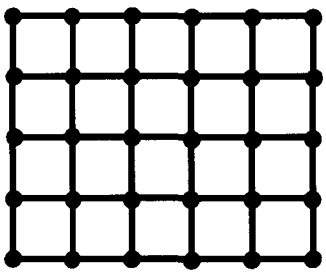

図 2.1: 5 × 6の長方形のグリッド

この$P_{m,n}$における各格子点にボタンとライトがついており, 各ライトはonかoffの2つの状態をとるとする. また, あるボタンを押すと, その点のライト及び, その点と縦と横に1つの辺でつながった点のライトのonとoffが切り替わるようになっている. 一般的にライツアウトパズルは, い

くつかのライトがonの状態から始め,最終的に全てのライトをoffにすることが目標である.

2.1　グラフ上のσ ゲーム

ライツアウトパズルは長方形のグリッドで考えるものであるが,各ライトの状態はonとoffの2つのままで,グリッドの形を変えることで,もっと一般化したパズルが考えられる.そのためにまずグラフという概念を述べる.

定義 2.1.1 **頂点集合**とよばれる有限集合V及び,Vの2つの元からなる対の集合Eを考える.Eの元は順を考えないVの元の組と考えることもできる.このときVとEの組のことをV上の**グラフ**といい$G=(V,E)$と表す.

グラフ$G=(V,E)$において,Vの元をGの**頂点**,Eの元をGの**辺**という.Eの元eがVの2元x,yからなる対であるとき,辺eはxとyを**つなぐ**といい,$e=(x,y)$と表す.またこのとき,辺eは頂点x,yに**接続している**,x,yはeの**端点**ともいう.ただし,(x,y)と(y,x)は区別しない.また,xとyをつなぐ辺があるとき,xとyは**隣接する**という.

例 2.1.2 $V=\{1,2,3,4,5\}$, $E=\{(1,2),(2,3),(3,4),(1,4),(1,5)\}$ とすると,$G=(V,E)$はグラフの例である.

$G=(V,E)$に対して,Vの元を平面にとり,Eの各元$e=(x,y)$に対して,xとyに対応する平面上の点を結んだ図でグラフGを表すことが多い.例2.1.2のグラフを図にすると図2.2のようになる.またこの章のはじめに述べた長方形のグリッド$P_{m,n}$もグラフの1つと考えられる.

このとき,定義2.1.1でのグラフの定義から,辺は必ず異なる2点を結び,2点を結ぶ辺は1つしかないことに注意する.(このようなグラフを特に**単純グラフ**ということもある.)

ここでライツアウトを一般化したパズルである一般グラフ$G=(V,E)$の上のσ ゲーム(参考文献[1])について説明する.単純グラフにおいて,頂点集合Vの各元,つまり各頂点にボタンとライトがついているとする.今後,"頂点vのボタンを押す" ということを,単に"頂点vを押す"ということとする.同様に,"頂点vのライトの状態"を"頂点vの状態"ということとする.

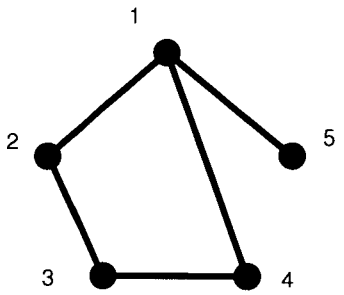

図 2.2: グラフの例

頂点には on と off の 2 つの状態があり, 頂点を押すことで, いくつかの頂点の on と off が切り替わる. 実際, 1 つの頂点 v を押すと, その頂点とその頂点に隣接している頂点の on と off が切り替わる. このとき, いくつかの頂点が on の状態を初期状態として, いくつかの頂点を押して, 全ての頂点を off にすることを考える. 与えられた初期状態から全てを off にすることができるか, また可能であるならどの頂点を押せばよいかを考える問題をこのグラフ G 上の **σ ゲーム**という.

図 2.3 の状態を例に説明する. ●を頂点が off の状態, ○を頂点が on の状態とする. この状態で頂点 3 を押したとすると, グラフは図 2.4 の状態になる.

こういったルールの中で, 適当な初期状態（各頂点の on と off が指定された状態）から全ての頂点を消灯させることが, このゲームの目的である. なお, 重要なのはどの頂点を押すかであって, 頂点を押す順番は関係がない. また, 同じ頂点を 2 回押すと直前の状態に戻ることから, 一つの頂点を 2 回押すことは意味をなさないことがわかる.

今後 σ ゲームについて数学的に解析していく.

A を集合, F を体とするとき, A から F への写像全体の集合を $map(A, F)$ と表す. グラフ $G = (V, E)$ に対して, $C_G = map(V, \mathbb{F}_2)$ とおく. C_G の各元 f は各頂点を $\mathbb{F}_2$ の元に対応させる写像になっている.

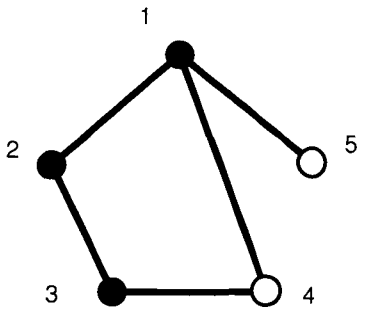

図 2.3: 頂点 3 を押す前

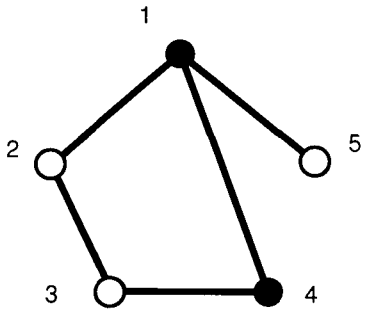

図 2.4: 頂点 3 を押した後

今後は $\mathbb{F}_2$ の元を用いて, 各頂点を押す・押さない, 各頂点の on・off の状態を以下のように表す.

定義 2.1.3 グラフ G の各頂点の on・off が指定されているものをグラフ G の**状態**という. 頂点集合 V において, V の各元 v_i の頂点が on の状態を $1 \in \mathbb{F}_2$, off の状態を $0 \in \mathbb{F}_2$ と表す. つまりグラフの状態は, 各頂点に $\mathbb{F}_2$ の 0 または 1 を対応させることに他ならないので, グラフ G の状態は C_G の元で表される.

定義 2.1.4 グラフ G の各頂点を押す行為及び押さない行為をグラフ G の**操作**という. 頂点集合 V において, V の各元 v_i を押す操作を $1 \in \mathbb{F}_2$, 押さない操作を $0 \in \mathbb{F}_2$ と表す. つまり, グラフ全体の各頂点を押すか押さないかは, 各頂点に $\mathbb{F}_2$ の 0 または 1 を対応させることに他ならないので, グラフ G の上の σ ゲームの操作は C_G の元で表される.

2.2　奇点定理

この節では後に用いる, グラフに関する基本的な補題や定理について述べる.

定義 2.2.1 グラフ $G=(V,E)$ の頂点 $x \in V$ において, x に接続している辺の本数を x の**次数**といい, $\deg x$ と表す.

補題 2.2.2 (握手補題) グラフ $G=(V,E)$ において,

$$\sum_{x \in V} \deg x = 2(\#E)$$

が成り立つ.

証明　V と E の直積集合 $V \times E$ をとり, その部分集合 A を

$$A = \{(x,e) | x \text{ が } e \text{ の端点 }\}$$

とおく. このとき, A の元を頂点 v ごとに考えると,

$$A = \coprod_{v \in V} \{(v,e) | e \text{ は } v \text{ を端点にもつ }\}$$

である. したがって,

$$\#A = \sum_{v \in V} \deg v \tag{2.1}$$

が成り立つ.

また, A の元を辺 l ごとに考えると,

$$A = \coprod_{l \in E} \{(v,l) | v \text{ は } l \text{ の端点 }\}$$

である. したがって,

$$\#A = \sum_{l \in E} 2 = 2(\#E) \tag{2.2}$$

が成り立つ. 式 (2.1),(2.2) より,

$$\sum_{v \in V} \deg v = 2(\#E)$$

が成り立つ. □

定理 2.2.3 (奇点定理) 任意のグラフ $G=(V,E)$ において, $\#\{x \in V | \deg x \text{ が奇数 }\}$ は偶数となる.

証明　A, B を頂点集合 V の以下に示す部分集合とする.

$$A = \{a \in V | \deg a \text{が偶数}\}$$

$$B = \{b \in V | \deg b \text{が奇数}\}$$

このとき, 補題 2.2.2 より,

$$\sum_{a \in A} \deg a + \sum_{b \in B} \deg b = \sum_{x \in V} \deg x = 2(\#E) \equiv 0 \pmod 2 \tag{2.3}$$

が成り立つ. また, A の任意の元 a は $\deg a \equiv 0 \pmod 2$ であり, B の任意の元 b は $\deg b \equiv 1 \pmod 2$ である. よって式 (2.3) より,

$$0 \equiv \sum_{b \in B} \deg b \equiv \sum_{b \in B} 1 \equiv \#B \pmod 2$$

が得られる. ゆえに $\#B$ は偶数である. □

2.3　σ ゲームと線型写像

C_G 上に次のような演算を考える.

1. $f, g \in C_G = map(V, \mathbb{F}_2)$ に対して, $f + g : V \to \mathbb{F}_2$ を

$$(f + g)(a) = f(a) + g(a)$$

と定める.

2. C_G の元 f と $\mathbb{F}_2$ の元 k に対して, $kf : V \to \mathbb{F}_2$ を

$$(kf)(a) = k(f(a))$$

と定める.

このような演算を定めると, C_G はベクトル空間になる.

ここで, 特に V の頂点に $v_1, \cdots, v_n$ というような順番があるとする. このとき C_G の元 f を, $f(v_1), \cdots, f(v_n)$ を縦に並べたベクトル

$$\boldsymbol{x} = \begin{pmatrix} f(v_1) \\ \vdots \\ f(v_n) \end{pmatrix} \in {\mathbb{F}_2}^n \tag{2.4}$$

と対応させると, この写像は線型写像で, C_G と ${\mathbb{F}_2}^n$ との間の全単射となる. したがってこの対応はベクトル空間の同型である. 以下この章では, グラフの頂点には常に順番があるとして, C_G の元 f を式 (2.4) に表す ${\mathbb{F}_2}^n$ の元 $\boldsymbol{x}$ と同一視することにする.

定義 2.3.1 グラフ $G=(V,E)$ において, 頂点全体に順番がついているとし, その頂点集合を $V=\{v_1,v_2,\cdots,v_n\}$ とする. このとき, $\mathbb{F}_2$ の元を成分とする次のような $n\times n$ 行列 $A=(a_{ij})$ を考える. すなわち, v_i と v_j が隣接しているとき $a_{ij}=1\in\mathbb{F}_2$, v_i と v_j が隣接していないとき $a_{ij}=0\in\mathbb{F}_2$ とする. また, 対角成分 $a_{ii}=0$ とする. これは, グラフ G のどの頂点間が隣接しているかを表す行列となっている. この行列を**隣接行列**という.

定理 2.3.2 グラフ $G=(V,E)$ において, 頂点集合 V に $\{v_1,\cdots,v_n\}$ という順番があるとする. このとき, ${\mathbb{F}_2}^n\cong C_G$ の元 $\boldsymbol{x},\boldsymbol{y}$ に関し, 状態 $\boldsymbol{x}$ が操作 $\boldsymbol{y}$ によって新たな状態 $\boldsymbol{x'}$ になったとすると, 操作後の状態 $\boldsymbol{x'}$ は隣接行列 A を用いて

$$\boldsymbol{x'}=\boldsymbol{x}+\boldsymbol{y}+A\boldsymbol{y}$$

と表される.

証明　操作後の頂点 v_i の状態について考える. v_i が最終的に 0 か 1 かは初期状態 $\boldsymbol{x}$ における v_i の状態と, v_i を押すか否かと, v_i に隣接している頂点 v_j がいくつ押されるかで決まる. 実際,

$$\boldsymbol{x}=\begin{pmatrix} f(v_1)\\ \vdots\\ f(v_n)\end{pmatrix}$$

$$\boldsymbol{y}=\begin{pmatrix} g(v_1)\\ \vdots\\ g(v_n)\end{pmatrix}$$

となる $f,g\in C_G=map(V,\mathbb{F}_2)$ をとると, 操作後の v_i の状態 $h(v_i)$ は

$$h(v_i)=f(v_i)+g(v_i)+\sum_{v_i\text{と隣接している }v_j} g(v_j) \tag{2.5}$$

と表すことができる. 隣接行列 $A=(a_{ij})$ を用いて, 式 (2.5) の最後の項の和を頂点全体についての和に書き直すと,

$$\begin{aligned} h(v_i) &= f(v_i)+g(v_i)+\sum_{j=1}^{n} a_{ij}g(v_j) \\ &= f(v_i)+g(v_i)+(a_{i1}g(v_1)+\cdots+a_{in}g(v_n)) \end{aligned}$$

となる. したがって, 操作後の状態を表すベクトルを $\boldsymbol{x}'$ とすると,

$$\boldsymbol{x}'=\begin{pmatrix} h(v_1) \\ \vdots \\ h(v_n) \end{pmatrix}=\begin{pmatrix} f(v_1) \\ \vdots \\ f(v_n) \end{pmatrix}+\begin{pmatrix} g(v_1) \\ \vdots \\ g(v_n) \end{pmatrix}+A\begin{pmatrix} g(v_1) \\ \vdots \\ g(v_n) \end{pmatrix}$$

となる. つまり,

$$\boldsymbol{x}'=\boldsymbol{x}+\boldsymbol{y}+A\boldsymbol{y}$$

と表される. □

定理 2.3.2 より, 次のことが分かる. $\mathbb{F}_2{}^n$ では $\boldsymbol{x}=-\boldsymbol{x}$ なので, $\boldsymbol{x}$ を移項して,

$$\boldsymbol{x}'+\boldsymbol{x}=(E+A)\boldsymbol{y}\quad (E: n\text{ 次単位行列}) \tag{2.6}$$

が得られる. つまり, $\boldsymbol{x}$ から $\boldsymbol{x}'$ への変化が可能であるかどうかは, $\boldsymbol{x}+\boldsymbol{x}'=(E+A)\boldsymbol{y}$ を満たすようなベクトル $\boldsymbol{y}$ が存在するかどうかで決まるので, これは $\boldsymbol{x}$ と $\boldsymbol{x}'$ の差だけで決まる. したがって $\boldsymbol{x}=\boldsymbol{0}$ の場合に可能かどうかが判別できれば, 任意の 2 つの状態について, それらの状態間の変化が可能かどうかが判別できる. したがって, 以後 $\boldsymbol{0}$ から $\boldsymbol{x}$ ($\boldsymbol{x}$ から $\boldsymbol{0}$) への変化が可能かどうかを考える.

式 (2.6) より, $\boldsymbol{0}$ の状態からある操作を加えて $\boldsymbol{x}$ に変化することが可能であることは, $\boldsymbol{x}=(A+E)\boldsymbol{y}$ となる $\mathbb{F}_2{}^n$ の元 $\boldsymbol{y}$ が存在することと同値である. つまり, $A+E$ が表す線型写像 $\sigma:\mathbb{F}_2{}^n\longrightarrow\mathbb{F}_2{}^n$ に対して, $\boldsymbol{x}$ が $\mathrm{Im}\,\sigma$ の元であれば, $\boldsymbol{0}$ から $\boldsymbol{x}$ への変化が可能である.

これをまとめると次の定理が得られる.

定理 2.3.3 状態 $\boldsymbol{0}$ からある状態 $\boldsymbol{x}$ に, 適当な操作 $\boldsymbol{y}$ を加えて変化することが可能であるための必要十分条件は, $(A+E)$ が表す線型写像 $\sigma:\mathbb{F}_2{}^n\to\mathbb{F}_2{}^n$ に対して, $\boldsymbol{x}$ が $\mathrm{Im}\,\sigma$ の元であることである.

この σ は σ ゲームの解析上重要な役割を果たすので, 名称を定めておく.

定義 2.3.4 グラフ $G=(V,E)$ における頂点集合を $V=\{v_1,\cdots,v_n\}$, 隣接行列を $A\in M_n(\mathbb{F}_2)$ とする. このとき, $A+E(E:n$ 次単位行列) が表す $C_G\cong {\mathbb{F}_2}^n$ から $C_G\cong {\mathbb{F}_2}^n$ への線型写像 σ を G 上の σ ゲームの**特性写像**ということにする.

定理 2.3.3 より, 次の定理が得られる.

定理 2.3.5 グラフ G 上の σ ゲームにおいて, 次は同値である.

1. 任意の状態 $\boldsymbol{x}\in C_G$ に対して σ ゲームの操作で $\mathbf{0}$ から $\boldsymbol{x}$ へと変化できる.
2. 2つの状態 $\mathbf{0},\boldsymbol{x}$ が σ ゲームの操作で移り合うなら, $\mathbf{0}$ から $\boldsymbol{x}$ へ移すための操作 $\boldsymbol{y}\in C_G$ は唯一つである.
3. $\mathbf{0}$ を $\mathbf{0}$ へと移すような操作 $\boldsymbol{y}\in C_G$ は $\boldsymbol{y}=\mathbf{0}$ に限る.

証明　まず, 条件 1. について考える. 任意の状態 $\boldsymbol{x}\in C_G$ に対して σ ゲームの操作で $\mathbf{0}$ から $\boldsymbol{x}$ へと変化できることは, 任意の状態 $\boldsymbol{x}\in C_G$ に対して $\boldsymbol{x}=(A+E)\boldsymbol{y}$ となる ${\mathbb{F}_2}^n$ の元 $\boldsymbol{y}$ が存在することと同値であるので, これは $\operatorname{Im}\sigma$ が C_G 全体であることを示している. したがって, 条件 1. は $\dim\operatorname{Im}\sigma$ が n であることと同値である.

また, $\boldsymbol{y}$ が $\mathbf{0}$ を $\mathbf{0}$ へ移す操作であるということは, $\sigma(\boldsymbol{y})=\mathbf{0}$ であることと同値である. つまり, $\boldsymbol{y}$ は $\operatorname{Ker}\sigma$ の元である. 条件 3. は, そのような $\boldsymbol{y}$ は $\mathbf{0}$ に限ることを述べており, これは $\operatorname{Ker}\sigma=\{\mathbf{0}\}$ を示している. したがって, 条件 3. は $\dim\operatorname{Ker}\sigma=0$ であることと同値である. ゆえに, 定理 1.3.5 より, 条件 1. と条件 3. が同値であることがわかる.

次に条件 2. と条件 3. が同値であることを示す. $\mathbf{0}$ から $\mathbf{0}$ に移すことは, 何もしないという操作によって可能である. よって条件 2. を仮定すると, $\mathbf{0}$ を $\mathbf{0}$ へと移すような操作 $\boldsymbol{y}\in C_G$ は $\boldsymbol{y}=\mathbf{0}$ に限ることになり, 条件 3. が得られる.

また, 条件 3. を仮定すると, 上記より $\dim\operatorname{Ker}\sigma=0$ である. このとき, $C_G\ni\boldsymbol{x}$ に対し, $\mathbf{0}$ を $\boldsymbol{x}$ へ移す操作 $\boldsymbol{y},\boldsymbol{y'}$ があったとする. このとき $\boldsymbol{x}=\sigma(\boldsymbol{y})=\sigma(\boldsymbol{y'})$ であるから, $\sigma(\boldsymbol{y})=\sigma(\boldsymbol{y'})$ である. これより $\sigma(\boldsymbol{y}-\boldsymbol{y'})=\mathbf{0}$ が得られる. $\operatorname{Ker}\sigma=\mathbf{0}$ より, $\boldsymbol{y}-\boldsymbol{y'}=\mathbf{0}$ である. したがって, $\boldsymbol{y}=\boldsymbol{y'}$ であり, $\boldsymbol{x}$ から $\mathbf{0}$ へ移すための操作 $\boldsymbol{y}\in C_G$ は唯一つである. □

例 2.3.6 図 (2.5),(2.6) に示すグラフ G,G' 上の σ ゲームを例にとって上記の結果を考察する.

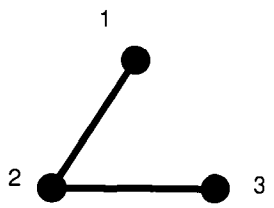

図 2.5: グラフ G

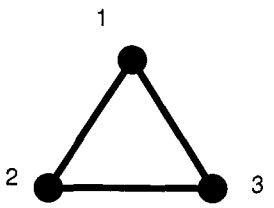

図 2.6: グラフ G'

このグラフ G, G' の頂点集合 V はともに $V = \{1, 2, 3\}$ であり, G の辺の集合 E は $E = \{(1, 2), (2, 3)\}$, G' の辺の集合 E' は $E' = \{(1, 2), (2, 3), (3, 1)\}$ である. また, G, G' 上の σ ゲームの特性写像をそれぞれ $\sigma, \sigma' : {\mathbb{F}_2}^3 \to {\mathbb{F}_2}^3$ とする. このグラフ G, G' の隣接行列 A, A' はそれぞれ

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad A' = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

である. したがって, 隣接行列 A, A' と単位行列 E の和は

$$A + E = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad A' + E = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

となる.

この行列 $A + E, A' + E$ に基本変形を行い, それぞれの行列の rank を求める.

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \xrightarrow[\text{第 1 列を加える}]{\text{第 2 列に}} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \xrightarrow[\text{第 2 列を加える}]{\text{第 3 列に}} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

$$\xrightarrow[\text{第 3 列を加える}]{\text{第 1 列に}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \xrightarrow[\text{第 3 列を入れ替える}]{\text{第 2 列と}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

よって, このグラフ G の特性写像 σ を表す行列 $A+E$ の rank は 3 であることがわかった. したがって, このグラフの $\dim \mathrm{Im}\,\sigma$ は 3 であり, どんな状態でも $\mathbf{0}$ にすることができ, その方法は唯一であることがわかる.

また, グラフ G の特性写像 σ' を表す行列 $A'+E$ の rank は明らかに 1 であり.

$$\mathrm{Im}\,\sigma = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle$$

である. 実際, 状態 $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ と $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ のみが, $\mathbf{0}$ にできる状態であり, その他の状態からは $\mathbf{0}$ にすることができないことが分かる.

2.4　All1 ゲーム

σ ゲームは様々なグラフにおいて様々な初期状態から考えられるので, 例 2.3.6 の G' のように, 中には目的の状態にできないこともある. しかし, 一般グラフ上の σ ゲームでは, いかなるグラフであっても, 全ての頂点が 1 の状態から, 全ての頂点を 0 の状態にすることが可能であることが知られている. 全ての頂点が 0 の状態から 1 の状態にできるならば, 全ての頂点が 1 の状態から 0 の状態にすることは可能であるので, 今後, 全ての頂点が 0 の状態から全ての頂点を 1 にすることを考える. これを **All 1 ゲーム**と呼ぶことにする. この節では,All 1 ゲームについて考察する.

補題 2.4.1 $\langle , \rangle$ を $\mathbb{K}^n$ 上の標準内積とし, 行列 $P \in M_n(\mathbb{K})$ をとる. $\mathbb{K}^n$ の元 $\boldsymbol{x}, \boldsymbol{y}$ に対して,

$$\langle {}^tP\boldsymbol{x}, \boldsymbol{y} \rangle = \langle \boldsymbol{x}, P\boldsymbol{y} \rangle$$

が成り立つ.

証明　$\mathbb{K}^n$ 内のベクトルを縦ベクトル, つまり $n \times 1$ 行列と考える. このとき, $\mathbb{K}^n \ni \boldsymbol{x}$ に対して ${}^t\boldsymbol{x}$ は $1 \times n$ 行列, つまり横ベクトルとなり, ${}^t\boldsymbol{x}\boldsymbol{y}$ は 1×1 行列となるが, 1×1 行列を $\mathbb{K}$ の元と同一視すれば, $\langle , \rangle$ は $\mathbb{K}^n$ 上の標準内積なので, $\langle \boldsymbol{x}, \boldsymbol{y} \rangle = {}^t\boldsymbol{x}\boldsymbol{y}$ となる.

したがって,

$$\begin{aligned}\langle {}^tP\boldsymbol{x}, \boldsymbol{y}\rangle &= {}^t({}^tP\boldsymbol{x})\boldsymbol{y} \\ &= ({}^t\boldsymbol{x}P)\boldsymbol{y} \\ &= {}^t\,\boldsymbol{x}(P\boldsymbol{y}) \\ &= \langle \boldsymbol{x}, P\boldsymbol{y}\rangle\end{aligned}$$

となる. □

以下, グラフ G の頂点に順番があると仮定して, 式 (2.4) の対応で $C_G \cong \mathbb{F}_2{}^n$ と考え, C_G に標準内積を考える.

補題 2.4.2 グラフ G 上の特性写像 σ において, $C_G \cong \mathbb{F}_2{}^n$ の元 $\boldsymbol{x}, \boldsymbol{y}$ に対して,

$$\langle \boldsymbol{x}, \sigma(\boldsymbol{y})\rangle = \langle \sigma(\boldsymbol{x}), \boldsymbol{y}\rangle$$

が成り立つ.

証明　$\sigma(\boldsymbol{x})$ は, 隣接行列 A と単位行列 E を用いて, $\sigma(\boldsymbol{x}) = (A+E)\boldsymbol{x}$ と表される. A は隣接行列なので, $A = {}^tA$ であることに注意すると, 補題 2.4.1 より,

$$\begin{aligned}\langle \boldsymbol{x}, \sigma(\boldsymbol{y})\rangle &= \langle \boldsymbol{x}, (A+E)\boldsymbol{y}\rangle \\ &= \langle {}^t(A+E)\boldsymbol{x}, \boldsymbol{y}\rangle \\ &= \langle (A+E)\boldsymbol{x}, \boldsymbol{y}\rangle \\ &= \langle \sigma(\boldsymbol{x}), \boldsymbol{y}\rangle\end{aligned}$$

となる. □

命題 2.4.3 C_G の元 $\boldsymbol{z}$ をとる. C_G の任意の元 $\boldsymbol{x}$ に対して $\langle \boldsymbol{x}, \boldsymbol{z}\rangle = 0$ ならば, $\boldsymbol{z} = \boldsymbol{0}$ である.

証明　命題の対偶 : $z \neq \boldsymbol{0}$ ならば, $\langle \boldsymbol{x}, \boldsymbol{z}\rangle \neq 0$ となるような $\boldsymbol{x} \in C_G$ が存在することを示す. $\boldsymbol{z} \neq \boldsymbol{0}$ なので, $\boldsymbol{z} = (z_1, \cdots, z_n)$ とすると, 少なくとも 1 つは $z_i = 1$ となる成分 z_i が存在する. このとき, i 番目の成分だけが 1 であるベクトル $\boldsymbol{x}$ をとると, $\langle \boldsymbol{x}, \boldsymbol{z}\rangle = 1 \neq 0$ が成り立つ. したがって, 対偶が示された. □

補題 2.4.4 グラフ G 上の特性写像を σ とする．このとき，

$$(\mathrm{Im}\,\sigma)^{\perp} = \mathrm{Ker}\,\sigma$$

が成り立つ．

証明　$\boldsymbol{y}$ を $(\mathrm{Im}\,\sigma)^{\perp}$ の元とする．これは，C_G の任意の元 $\boldsymbol{x}$ に対して，

$$\langle \sigma(\boldsymbol{x}), \boldsymbol{y} \rangle = 0$$

となることと同値である．また補題2.4.2より，これは C_G の任意の元 $\boldsymbol{x}$ に対して，

$$\langle \boldsymbol{x}, \sigma(\boldsymbol{y}) \rangle = 0$$

となることと同値である．

命題2.4.3より，C_G の任意の元 $\boldsymbol{x}$ に対して $\langle \boldsymbol{x}, \sigma(\boldsymbol{y}) \rangle = 0$ となることの必要十分条件は，$\sigma(\boldsymbol{y}) = \boldsymbol{0}$ なので，$\boldsymbol{y}$ は $\mathrm{Ker}\,\sigma$ の元である．ゆえに $(\mathrm{Im}\,\sigma)^{\perp} = \mathrm{Ker}\,\sigma$ である．　□

定理 2.4.5 有限グラフ $G = (V, E)$ において，σ を G 上の特性写像とする．$C_G \cong {\mathbb{F}_2}^n$ の元 $\boldsymbol{x}$ に対して次は同値である．

1. $\boldsymbol{x} = \sigma(\boldsymbol{y})$ となる $\boldsymbol{y} \in C_G$ が存在する．
2. $\boldsymbol{x} \perp \mathrm{Ker}\,\sigma$ となる．

証明　$\boldsymbol{x} = \sigma(\boldsymbol{y})$ となることは，$\boldsymbol{x} \in \mathrm{Im}\,\sigma$ と同値なので，$\mathrm{Im}\,\sigma = (\mathrm{Ker}\,\sigma)^{\perp}$ を示せばよい．

補題2.4.4より，$(\mathrm{Im}\,\sigma)^{\perp} = \mathrm{Ker}\,\sigma$ である．両辺の直交補空間を考えると $((\mathrm{Im}\,\sigma)^{\perp})^{\perp} = (\mathrm{Ker}\,\sigma)^{\perp}$ となる．系1.6.24より，$((\mathrm{Im}\,\sigma)^{\perp})^{\perp} = \mathrm{Im}\,\sigma$ なので，$(\mathrm{Ker}\,\sigma)^{\perp} = \mathrm{Im}\,\sigma$ である．

□

定義 2.4.6 $G = (V, E)$ をグラフとし，$\#V = n$ とする．このとき，$f \in C_G = map(V, \mathbb{F}_2)$ に対して

$$V' = \{v \in V | f(v) = 1\}$$

とし，E' を V' の頂点同士をつなぐ辺の集合とすると，(V', E') も1つのグラフとなる．このグラフを $\mathrm{sub}(f) = (V', E')$ と表す．また，G 上の頂点集合 V に順番があるとして，$C_G \cong {\mathbb{F}_2}^n$ の同型で f が $\boldsymbol{x} \in {\mathbb{F}_2}^n$ に移るとすれば，上記の V' の元の個数 $\#V'$ は $\boldsymbol{x}$ の成分に1がいくつあるかを表す．このときの $\#V'$ を $\#\boldsymbol{x}$ とも表す．

補題 2.4.7 グラフ $G=(V,E)$ 上の σ ゲームを考える. このとき, C_G の元 $\boldsymbol{x}$ に対し, $\sigma(\boldsymbol{x})=\mathbf{0}$ ならば, $\#\boldsymbol{x}$ は偶数である.

証明　V に順番があるとして, $map(V,\mathbb{F}_2)\cong {\mathbb{F}_2}^n$ の対応で, $\sigma(\boldsymbol{x})=\mathbf{0}$ となる $\boldsymbol{x}$ に対応する $f\in map(V,\mathbb{F}_2)$ を考え, $\mathrm{sub}(f)=(V',E')$ とする. $\sigma(\boldsymbol{x})=\mathbf{0}$ なので, V' の頂点を全て押したとき, 全て0の状態は全て0の状態へ移る. つまり V' の頂点を1つずつ押していくとき, 任意の頂点は偶数回変化する. ゆえに各頂点 $v\in V'$ は, V' の奇数個の頂点とつながっている. したがって, グラフ $\mathrm{sub}(f)$ の中で $\deg v$ は全て奇数であるので, 奇点定理より, $\#\boldsymbol{x}=\#V'\equiv 0 \pmod 2$ が得られる. □

定理 2.4.8 任意のグラフ $G=(V,E)$ の σ ゲームにおいて, 全ての頂点が0の状態から, 全てを1の状態にする操作が存在する.

証明　$\#V=n$ とし, $C_G\cong {\mathbb{F}_2}^n$ の中の全ての頂点が1の状態のベクトルを $\mathbf{1}$ と表す. このとき, $\mathrm{Ker}\,\sigma$ の任意の元 $\boldsymbol{x}$ に対して, $\boldsymbol{x}$ と $\mathbf{1}$ の内積 $\langle \boldsymbol{x},\mathbf{1}\rangle$ は,

$$\langle \boldsymbol{x},\mathbf{1}\rangle = \#\boldsymbol{x} \pmod 2$$

である. 今, $\sigma(\boldsymbol{x})=\mathbf{0}$ なので, 補題2.4.7より, $\#\boldsymbol{x}$ は偶数であり,

$$\langle \boldsymbol{x},\mathbf{1}\rangle = 0$$

が得られる. したがって, $\mathbf{1}$ は $(\mathrm{Ker}\,\sigma)^{\perp}$ の元である. だから定理2.4.5より, $\mathbf{1}\in \mathrm{Im}\,\sigma$ である. よって, $\mathbf{1}=\sigma(\boldsymbol{y})$ となるような $\boldsymbol{y}\in C_G$ が存在し, この $\boldsymbol{y}$ は $\mathbf{0}$ を $\mathbf{1}$ に移す操作である. □

第3章　長方形グリッドのσゲーム

第2章では一般グラフ上のσゲームについて考察した. 第3章では, 本来のライツアウトパズルの形に戻って, $P_{m,n}$におけるライツアウトパズルを考える. 長方形のグリッド$P_{m,n}$において, m,nがどんな条件を満たせば, σゲームのルールで任意の状態から全ての頂点を0の状態にできるのかを調べていく.

3.1　$P_{m,n}$上の特性写像

この章では, 第2章と同様に$C_{P_{m,n}}$を考えて, 状態や操作を$C_{P_{m,n}}$の元で表す. 以下, $C_{P_{m,n}}$を簡単に$C_{m,n}$と表すことにする. 第2章ではグラフGの頂点に順番をつけることにより, C_Gを$\mathbb{F}_2{}^{\#V}$内のベクトルと対応させて考えたが, 第3章では以下の方法によって$C_{m,n}$の元を別の形で捉える.

$P_{m,n}$の上からi番目, 左からj番目の頂点を(i,j)と表す. すると, $P_{m,n}$の頂点集合は$\{1,\cdots,m\}\times\{1,\cdots,n\}$となり, $f\in C_{m,n}=map(V,\mathbb{F}_2)$は$f:\{1,\cdots,m\}\times\{1,\cdots,n\}\to\mathbb{F}_2$となる. このとき, fを

$$X=\begin{pmatrix} f(1,1) & \cdots & f(1,n) \\ \vdots & & \vdots \\ f(m,1) & \cdots & f(m,n) \end{pmatrix}\in M_{m,n}(\mathbb{F}_2)$$

という行列Xと対応させると, この写像は$\mathbb{F}_2$上の線型写像で, $C_{m,n}$と$M_{m,n}(\mathbb{F}_2)$との間の全単射となる. したがってこの対応は$\mathbb{F}_2$上のベクトル空間の同型である. 以下, この章では$C_{m,n}$の元を上記のように行列と同一視することする. この同一視では, 全ての頂点が0となる状態は零行列Oで表される.

定義 3.1.1 $\sigma:C_{m,n}\to C_{m,n}$を次のように定める. $C_{m,n}\cong M_{m,n}(\mathbb{F}_2)$の元$A=(a_{ij})$に対して, $C_{m,n}\cong M_{m,n}(\mathbb{F}_2)$の元$B=(b_{ij})$を

$$b_{ij}=a_{ij}+a_{i-1,j}+a_{i+1,j}+a_{i,j-1}+a_{i,j+1}\in\mathbb{F}_2$$

とし, $\sigma(A)=B$ とする. ただし, $a_{0j}, a_{m+1,j}, a_{i0}, a_{i,n+1}$ は0とする. この対応が線型写像となることは容易に確かめられる.

定理 3.1.2 $C_{m,n} \cong M_{m,n}(\mathbb{F}_2)$ の元 X, Y に対して, 状態 $X=(x_{ij})$ に操作 $Y=(y_{ij})$ を加えた状態 $X'=(x'_{ij})$ は

$$X' = X + \sigma(Y)$$

となる.

証明　σ ゲーム上では, 頂点 x_{ij} の操作後の状態 x'_{ij} は, 操作前の状態と, 頂点 (i,j) を押すかどうか及び, 頂点 (i,j) に隣接している頂点をいくつ押すかで決まってくるので, 各頂点に対して

$$x'_{ij} = x_{ij} + y_{i,j} + y_{i-1,j} + y_{i+1,1} + y_{i,j-1} + y_{i,j+1}$$

が成り立つ. ただし, $y_{0j}, y_{m+1,j}, y_{i0}, y_{i,n+1}$ は0である. したがって, $X' = X + \sigma(Y)$ である. □

定理3.1.2と定理2.3.3を比べると, 定義3.1.1で定めた写像 σ は σ ゲームにおける特性写像と同じ性質をもっていることが分かる. 実際, 定義2.3.4では C_G を $\mathbb{F}_2{}^{\#V}$ と同一視して特性写像 σ を考えたが, この定義3.1.1の σ は $C_{P_{m,n}}$ を $M_{m,n}(\mathbb{F}_2)$ と同一視して特性写像を書き下したものとなっている. よって, この定義3.1.1の σ を $P_{m,n}$ 上の σ ゲームの特性写像と呼ぶことにする.

グラフ $P_{m,n}$ 上の特性写像を σ とすると, 状態 O からある状態 X に, 適当な操作 Y を加えて変化することが可能であるということは, $O+\sigma(Y)=X$ となることと同値である. よって, 状態 O からある状態 X に, 適当な操作 Y を加えて変化することが可能であるための必要十分条件は, X が $\mathrm{Im}\,\sigma$ の元であることである.

定義 3.1.3 $P_{m,n}$ 上の σ ゲームにおいて, 任意の状態 X にある操作 Y を加えて状態 O への遷移が可能であるとき, $P_{m,n}$ は**σ 可移**であるということにする.

定理 3.1.4 グラフ $P_{m,n}$ 上の特性写像を σ とする. このとき, 以下は同値である.

1. $\dim(\mathrm{Ker}\,\sigma)=0$ である.

2. $P_{m,n}$はσ可移である.

証明　2.の, $C_{m,n} \cong M_{m,n}(\mathbb{F}_2)$の任意の元$X$に対して, OからXにできるということは, $C_{m,n} \cong M_{m,n}(\mathbb{F}_2)$の任意の元$X$に対して, ある操作$Y$があって, $\sigma(Y) = X$を満たすことと同値である. つまり$\mathrm{Im}\,\sigma$が$C_{m,n}$全体となることと同値である. ゆえに$\dim(C_{m,n}) = \dim(\mathrm{Im}\,\sigma)$であり, 定理1.3.5より, $\dim(\mathrm{Ker}\,\sigma) = 0$であることと同値である. □

定理 3.1.5 グラフ$P_{m,n}$上の特性写像をσとする. $\dim(\mathrm{Ker}\,\sigma) = d$とすると, 以下が成り立つ.

1. σゲームの操作で状態Oから遷移できるXの個数は$C_{m,n}$全体の$\dfrac{1}{2^d}$で, $\dfrac{2^{mn}}{2^d}$個である.
2. 状態Oから遷移できるようなXに対し, OをXに移す操作Yの個数は2^d個である.

証明　まず1.を示す. まず, $\dim(C_{m,n}) = mn$である. $\dim(\mathrm{Ker}\,\sigma) = d$なので, 定理1.3.5より, $\dim(\mathrm{Im}\,\sigma) = mn - d$である. ゆえに, $\mathrm{Im}\,\sigma$の元の個数は$2^{mn-d} = \dfrac{2^{mn}}{2^d}$個である.

次に2.を示す. 状態Oから状態XできるようなXに対して, OをXに移す操作$Y \in C_{m,n}$は, $O + \sigma(Y) = X$となるようなYの総数である. ここで, OをXに移す操作の1つをY_0とすると, $\sigma(Y_0) = X$である. Y_0にある操作Zを加えて

$$\sigma(Y_0 + Z) = X \tag{3.1}$$

となるような操作Zについて調べる. σは線型写像なので, 式(3.1)は$\sigma(Y_0) + \sigma(Z) = X$と同値である. $\sigma(Y_0) = X$なので, これは$\sigma(Z) = O$を意味する. つまりZは$\mathrm{Ker}\,\sigma$の元である. よって, 集合$\{Y_0 + Z | Z \in \mathrm{Ker}\,\sigma\}$が, $\sigma(Y) = X$となるY全体である. 以上より, 状態Oを状態Xに移すような操作Yの個数は$\dim(\mathrm{Ker}\,\sigma) = d$より, 2^d個である. □

定理3.1.4及び3.1.5から, σゲームにおいては, $\mathrm{Ker}\,\sigma$の次元が分かれば, 状態Oから状態Xに変化できないようなXがあるかどうか, また何通りの操作があるかが分かることになる.

そこで, 第3章の次節以降では, $\mathrm{Ker}\,\sigma$の次元を調べることを目標とする.

3.2　Kerσについて

定義 3.2.1 $A_m \in M_m(\mathbb{F}_2)$を以下のような行列とする.

$$A_m = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 \end{pmatrix}$$

定理 3.2.2 σを$P_{m,n}$上のσゲームの特性写像とする. このとき, $C_{m,n} \cong M_{m,n}(\mathbb{F}_2)$の元$X$に対して,

$$\sigma(X) = A_m X + X A_n + X$$

が成り立つ.

証明　$X \in M_{m,n}(\mathbb{F}_2)$について, $A_m X$は,

$$A_m X = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \\ x_{m1} & \cdots & x_{mn} \end{pmatrix}$$

と表されるので, $A_m X = B = (b_{ij})$とすると, b_{ij}成分は

$$b_{ij} = (0 \cdots 0\,1\,0\,1\,0 \cdots 0) \begin{pmatrix} x_{1j} \\ \vdots \\ x_{ij} \\ \vdots \\ x_{mj} \end{pmatrix} = x_{i-1,j} + x_{i+1,j}$$

である.

同様にXA_nを具体的に考えると,

$$XA_n = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \\ x_{m1} & \cdots & x_{mn} \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 & \ldots & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & \ldots & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \ldots & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \ldots & 0 & 1 & 0 \end{pmatrix}$$

なので, $XA_n = B' = (b'_{ij})$とすると, b'_{ij}成分は

$$b'_{ij} = (x_{i1} \cdots x_{ij} \cdots x_{in}) \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} = x_{i,j-1} + x_{i,j+1}$$

である. したがって, $\sigma(X) = B + B' + X = A_m X + XA_n + X$が成り立つ. □

定理 3.2.3 $X \in M_{m,n}(\mathbb{F}_2) \cong C_{m,n}$に対して, Xを縦ベクトルに分けて$X = (\boldsymbol{x}_1 \cdots \boldsymbol{x}_n)$とする. このとき, 以下は同値である.

1. Xが$\mathrm{Ker}\,\sigma$の元である.
2. $\boldsymbol{x}_0 = \boldsymbol{x}_{n+1} = \boldsymbol{0}$とおくと, $\boldsymbol{x}_0, \boldsymbol{x}_1 \cdots \boldsymbol{x}_n, \boldsymbol{x}_{n+1}$が漸化式

$$\boldsymbol{x}_i = (A_m + E)\boldsymbol{x}_{i-1} + \boldsymbol{x}_{i-2} \quad (2 \leq i \leq n+1)$$

を満たす.

証明　Xが$\mathrm{Ker}\,\sigma$の元であるということは,

$$(A_m + E)X + XA_n = O_{m,n} \tag{3.2}$$

であることと同値である. $\mathbb{F}_2$上には正負の区別がないので, 式(3.2)は

$$(A_m + E)X = XA_n \tag{3.3}$$

と同値である. $(A_m+E)X$ を, n 個の m 次元縦ベクトルに分けて考えると,

$$(A_m+E)X=(A_m+E)(\boldsymbol{x}_1\cdots\boldsymbol{x}_n)=((A_m+E)\boldsymbol{x}_1\cdots(A_m+E)\boldsymbol{x}_n)$$

であり, XA_n についてもやはり n 個の縦ベクトルに分けて考えると,

$$XA_n=(\boldsymbol{x}_1\cdots\boldsymbol{x}_n)\begin{pmatrix}0&1&0&\ldots&0&0&0\\1&0&1&\ldots&0&0&0\\0&1&0&\ldots&0&0&0\\\vdots&\vdots&\vdots&\ddots&\vdots&\vdots&\vdots\\0&0&0&\ldots&0&1&0\\0&0&0&\ldots&1&0&1\\0&0&0&\ldots&0&1&0\end{pmatrix}$$

$$=(\boldsymbol{x}_2\quad\boldsymbol{x}_1+\boldsymbol{x}_3\quad\cdots\quad\boldsymbol{x}_{n-2}+\boldsymbol{x}_n\quad\boldsymbol{x}_{n-1})$$

である. したがって, 式 (3.3) より,

$$\begin{aligned}(A_m+E)\boldsymbol{x}_1&=\boldsymbol{x}_2\\(A_m+E)\boldsymbol{x}_2&=\boldsymbol{x}_1+\boldsymbol{x}_3\\&\vdots\\(A_m+E)\boldsymbol{x}_{i-1}&=\boldsymbol{x}_{i-2}+\boldsymbol{x}_i\\&\vdots\\(A_m+E)\boldsymbol{x}_{n-1}&=\boldsymbol{x}_{n-2}+\boldsymbol{x}_n\\(A_m+E)\boldsymbol{x}_n&=\boldsymbol{x}_{n-1}\end{aligned}$$

となる. $\boldsymbol{x}_0,\boldsymbol{x}_{n+1}$ をどちらも $\mathbf{0}$ として追加して, それぞれの式を整理すると, $2\le i\le n+1$ の各 i について $\boldsymbol{x}_i=(A_m+E)\boldsymbol{x}_{i-1}+\boldsymbol{x}_{i-2}$ が得られる. □

以後, この A_m+E を A_m^+ と表すことにする.

定義 3.2.4 $\mathbb{K}$ を体とし, 行列 $A\in M_n(\mathbb{K})$, 不定元 λ と n 次単位行列 E を用いて, $A-\lambda E$ を考えるとこれは λ に関する $\mathbb{K}$ 係数の多項式を成分とする行列である. この $A-\lambda E$ の行列式 $\det(A-\lambda E)\in\mathbb{K}[\lambda]$ を行列 A の**固有多項式**という. また, 行列 $A_m\in M_m(\mathbb{F}_2)$ の固有多項式を $P_m(\lambda)$ と表す. ただし $P_0(\lambda)=1$ とする.

命題 3.2.5 2以上の自然数nにおいて,

$$P_n(\lambda) = \lambda P_{n-1}(\lambda) + P_{n-2}(\lambda)$$

が成り立つ.

証明　$P_1(\lambda) = \lambda, P_0(\lambda) = 1$なので, $n = 2$のとき, $P_2(\lambda) = \lambda^2 + 1$より, $P_2(\lambda) = \lambda P_1(\lambda) + P_0(\lambda)$が成り立つ.

$n \geq 3$のとき, 実際に$P_n(\lambda)$を行列式の展開により計算していく. また, 簡単のために, 行列式の右下にその行列のサイズを$(n \times n)$というふうに記しておく.

$$\begin{aligned}
P_n(\lambda) &= |A_n - \lambda E_n| \\
&= \det \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 & 0 \\ 1 & \lambda & 1 & \dots & 0 & 0 \\ 0 & 1 & \lambda & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & \dots & 1 & \lambda \end{pmatrix}_{(n \times n)} \qquad \text{(第1行について展開する)} \\
&= \lambda \cdot \det \begin{pmatrix} \lambda & 1 & \dots & 0 & 0 \\ 1 & \lambda & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & \dots & 1 & \lambda \end{pmatrix}_{(n-1) \times (n-1)} \\
&\quad + 1 \cdot \det \begin{pmatrix} 1 & 1 & \dots & 0 & 0 \\ 0 & \lambda & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & \dots & 1 & \lambda \end{pmatrix}_{(n-1) \times (n-1)} \qquad \text{(第1列について展開する)} \\
&= \lambda P_{n-1}(\lambda) + 1 \cdot \det \begin{pmatrix} \lambda & 1 & \dots & 0 & 0 \\ 1 & \lambda & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & \dots & 1 & \lambda \end{pmatrix}_{(n-2) \times (n-2)} \\
&= \lambda P_{n-1}(\lambda) + P_{n-2}(\lambda)
\end{aligned}$$

となり, 示された. □

次にCayley-Hamiltonの定理と呼ばれる定理を示す.

定理 3.2.6 $\mathbb{K}$ を体とし, $n \geq 1$ に対して, 行列 $A \in M_n(\mathbb{K})$ の固有多項式 $P(\lambda)$ を

$$P(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0 \quad (a_i \in \mathbb{K})$$

とする. このとき,

$$A^n + a_{n-1}A^{n-1} + \cdots + a_1A + a_0E = O$$

が成り立つ.

証明 $n \times n$ 行列 $A - \lambda E$ を $B \in M_n(\mathbb{K})$ とし, B の余因子行列を $C \in M_n(\mathbb{K})$ とする. 余因子行列 C の成分は, もとの行列 B の $(n-1) \times (n-1)$ の小行列式で得られるため, C の成分は λ に関する高々 $(n-1)$ 次の多項式である. したがって, C は

$$C = \lambda^{n-1}C_{n-1} + \lambda^{n-2}C_{n-2} + \cdots + \lambda C_1 + C_0 \quad (C_i \in M_n(\mathbb{K}))$$

と表すことができる. ここで, $BC = \det(B)E = \det(A - \lambda E)E$ より,

$$(A - \lambda E)(\lambda^{n-1}C_{n-1} + \lambda^{n-2}C_{n-2} + \cdots + \lambda C_1 + C_0)$$

$$= (\lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0)E$$

である. ここで, 両辺を λ について係数比較すると,

$$\begin{aligned}
-C_{n-1} &= E \\
AC_{n-1} - C_{n-2} &= a_{n-1}E \\
AC_{n-2} - C_{n-3} &= a_{n-2}E \\
&\vdots \\
AC_2 - C_1 &= a_2E \\
AC_1 - C_0 &= a_1E \\
AC_0 &= a_0E
\end{aligned}$$

となる. これらの式の両辺に上から順に $A^n, A^{n-1}, A^{n-2}, \cdots, A^2, A, E$ を左からかけると,

$$\begin{aligned} -A^nC_{n-1} &= A^n \\ A^nC_{n-1} - A^{n-1}C_{n-2} &= a_{n-1}A^{n-1} \\ A^{n-1}C_{n-2} - A^{n-2}C_{n-3} &= a_{n-2}A^{n-2} \\ &\vdots \\ A^3C_2 - A^2C_1 &= a_2A^2 \\ A^2C_1 - AC_0 &= a_1A \\ AC_0 &= a_0E \end{aligned}$$

となる. 両辺それぞれに和をとると,

$$O = A^n + a_{n-1}A^{n-1} + a_{n-2}A^{n-2} + \cdots + a_2A^2 + a_1A + a_0E$$

を得る. □

一般に $\mathbb{F}_2$ を成分とする n 次正方行列 A と $\mathbb{F}_2$ を係数とする多項式

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

に対して, f に A を代入した行列とは

$$f(A) = a_nA^n + a_{n-1}A^{n-1} + \cdots + a_1A + a_0E$$

のことである. このとき, 定数項の取り扱いに注意を要する. この表現を用いると, $\mathbb{F}_2$ の元を成分とする行列の関する Cayley-Hamilton の定理は, n 次正方行列 A の固有多項式 $f(\lambda)$ の変数 λ に $A \in M_n(\mathbb{F}_2)$ を代入すると O 行列となることいいかえることができる.

補題 3.2.7 ${\mathbb{F}_2}^m$ 内の $n+2$ 個のベクトル $\boldsymbol{x}_0, \boldsymbol{x}_1, \cdots, \boldsymbol{x}_n, \boldsymbol{x}_{n+1}$ が

- $\boldsymbol{x}_0 = \boldsymbol{x}_{n+1} = \boldsymbol{0}$
- $\boldsymbol{x}_i = A_m^+\boldsymbol{x}_{i-1} + \boldsymbol{x}_{i-2} \quad (i = 2, \cdots, n+1)$

を満たすとき, 定義 3.2.4 の $P_i(\lambda)$ に関して,

$$\boldsymbol{x}_i = P_{i-1}(A_m^+)\boldsymbol{x}_1 \quad (i = 1, \cdots, n+1)$$

が成り立つ.

証明　$\boldsymbol{x}_i = P_{i-1}(A_m^+)\boldsymbol{x}_1$ が成り立つことを, i についての数学的帰納法で示す.

$i = 1$ のとき, $P_0(\lambda) = 1$ であるから, $P_0(A_m^+)\boldsymbol{x}_1 = E\boldsymbol{x}_1 = \boldsymbol{x}_1$ となり正しい.

$i = 2$ のとき, $\boldsymbol{x}_0 = \boldsymbol{0}, P_1(\lambda) = \lambda$ より,

$$\boldsymbol{x}_2 = A_m^+\boldsymbol{x}_1 + \boldsymbol{x}_0 = A_m^+\boldsymbol{x}_1 = P_1(A_m^+)\boldsymbol{x}_1$$

より正しい.

$k \geq 2$ とする. そして, $i \leq k$ のとき正しいと仮定して, $i = k+1$ のときを考える. 仮定より, $\boldsymbol{x_{k+1}} = A_m^+\boldsymbol{x_k} + \boldsymbol{x_{k-1}}$ が成り立っているので, 帰納法の仮定より

$$\begin{aligned}\boldsymbol{x_{k+1}} &= A_m^+P_{k-1}(A_m^+)\boldsymbol{x}_1 + P_{k-2}(A_m^+)\boldsymbol{x}_1 \\ &= \big(A_m^+P_{k-1}(A_m^+) + P_{k-2}(A_m^+)\big)\boldsymbol{x}_1\end{aligned}$$

となる. 命題 3.2.5 より,

$$P_k(A_m^+) = A_m^+P_{k-1}(A_m^+) + P_{k-2}(A_m^+)$$

であるから, $\boldsymbol{x_{k+1}} = P_n(A_m^+)\boldsymbol{x}_1$ が成り立つ. ゆえに $i = k+1$ のときも正しい. □

以下, 正方行列 $A \in M_n(\mathbb{F}_2)$ に対して, 写像 $f : \mathbb{K}^n \to \mathbb{K}^n$ を $f(\boldsymbol{x}) = A\boldsymbol{x}$ と定めたときの $\mathrm{Ker}f$ を単に $\mathrm{Ker}A$ と表すこととする.

定理 3.2.8　$P_{m,n}$ 上の特性写像 σ に関して, $\mathrm{Ker}\,\sigma \cong \mathrm{Ker}(P_n(A_m^+))$ が成り立つ.

証明　$\mathrm{Ker}\,\sigma$ から $\mathrm{Ker}(P_n(A_m^+))$ への写像 f を次のように定める.

まず, $X \in \mathrm{Ker}\,\sigma \subset M_{m,n}(\mathbb{F}_2)$ に対して, X を縦ベクトルに分けて $X = (\boldsymbol{x}_1, \cdots, \boldsymbol{x}_n)$ とし, $f(X) = \boldsymbol{x}_1$ とする.

この X に対して, 上記の $\boldsymbol{x}_1$ が $\mathrm{Ker}(P_n(A_m^+))$ の元となることを示す. 実際, $X \in \mathrm{Ker}\,\sigma$ であることから, $\boldsymbol{x}_1, \cdots, \boldsymbol{x}_n$ に $\boldsymbol{x}_0 = \boldsymbol{0}, \boldsymbol{x}_{n+1} = \boldsymbol{0}$ を加えると, 補題 3.2.7 より, $\boldsymbol{x}_{n+1} = P_n(A_m^+)\boldsymbol{x}_1 = \boldsymbol{0}$ となり $\boldsymbol{x}_1 \in \mathrm{Ker}(P_n(A_m^+))$ であることが分かる. したがってこの f は $\mathrm{Ker}\,\sigma$ から $\mathrm{Ker}(P_n(A_m^+))$ への写像となっている. またこの f が線型写像であることは容易に分かる.

次に, この写像 f が全射であることを示す. 任意の $\mathrm{Ker}(P_n(A_m^+))$ の元 $\boldsymbol{x}$ について, $X = (\boldsymbol{x}_1, \cdots, \boldsymbol{x}_n) \in M_{m,n}(\mathbb{F}_2)$ を次のように定める.

- $\boldsymbol{x}_1 = \boldsymbol{x}$
- $\boldsymbol{x}_i = A_m^+\boldsymbol{x}_{i-1} + \boldsymbol{x}_{i-2}$(ただし$i = 2, \cdots, n$及び$\boldsymbol{x}_0 = \boldsymbol{0}$とする)

すると, 補題3.2.7より, $A_m^+\boldsymbol{x}_n + \boldsymbol{x}_{n-1} = P_n(A_m^+)\boldsymbol{x}_1 = P_n(A_m^+)\boldsymbol{x} = \boldsymbol{0}$が成り立つ. したがって, 定理3.2.3より, $X = (\boldsymbol{x}_1, \cdots, \boldsymbol{x}_n)$は$\mathrm{Ker}\,\sigma$の元となり, $f(X) = \boldsymbol{x}_1$である. つまり, 任意の$\mathrm{Ker}(P_n(A_m^+))$の元$\boldsymbol{x}$に対して, $f(X) = \boldsymbol{x}$となる$X \in \mathrm{Ker}\,\sigma$が存在するので, fは全射である.

最後にfが単射であることを示す. $\mathrm{Ker}\,\sigma$の元X, Yをとり, それぞれ$X = (\boldsymbol{x}_1, \cdots, \boldsymbol{x}_n), Y = (\boldsymbol{y_1}, \cdots, \boldsymbol{y_n})$とする. このとき, $f(X) = f(Y)$とすると, $\boldsymbol{x}_1 = \boldsymbol{y_1}$である. X, Yは$\mathrm{Ker}\,\sigma$の元なので, 定理3.2.3より,

$$\boldsymbol{x}_i = A_m^+\boldsymbol{x}_{i-1} + \boldsymbol{x}_{i-2}$$

$$\boldsymbol{y_i} = A_m^+\boldsymbol{y_{i-1}} + \boldsymbol{y_{i-2}}$$

を満たす. したがって, $2 \leq i \leq n$において, $\boldsymbol{x}_i = \boldsymbol{y_i}$が得られる. ゆえに$f$は単射である.

以上より, $\mathrm{Ker}\,\sigma$と$\mathrm{Ker}(P_n(A_m^+))$は同型である. □

今までは$P_{m,n}$上のσゲームについて, これがσ可移であるかどうかの判定に, mn次元からmn次元への写像の$\mathrm{Ker}\,\sigma$を用いていたが, 定理3.2.8より, $\mathrm{Ker}\,\sigma$と$\mathrm{Ker}(P_n(A_m^+))$は同型であるので, これからはm次元からm次元への写像の$\mathrm{Ker}(P_n(A_m^+))$を考えればよい. これにより, 取り扱う次元が本来の$\dfrac{1}{n}$に抑えられたことになる.

定理 3.2.9 自然数m, nについて, $\mathrm{Ker}(P_n(A_m^+)) \cong \mathrm{Ker}(P_m(A_n^+))$が成り立つ.

証明　$P_{m,n}$上の特性写像σは$C_{m,n}$から$C_{m,n}$への写像であるが, $C_{m,n} \in M_{m,n}(\mathbb{F}_2)$の元を転置して$C_{n,m} \in M_{m,n}(\mathbb{F}_2)$の元にする写像$\tau$を考えると, $\tau : C_{m,n} \to C_{n,m}$は明らかにベクトル空間の同型写像である. ここで, $C_{n,m}$から$C_{n,m}$への写像σ'を

$$\sigma'(X) = A_nX + XA_m^+$$

とおくと, これは$P_{n,m}$の特性写像であるが, τ, σ, σ'について

$$\begin{aligned}\tau\sigma(X) &= {}^t(A_m^+X + XA_n)\\ &= A_n{}^tX + {}^tXA_m^+\\ &= \sigma'({}^tX)\\ &= \sigma'\tau(X)\end{aligned}$$

となることから, $\tau\sigma(X) = \sigma'\tau(X)$が成り立つ.

また, $\mathrm{Ker}\,\sigma$から$\mathrm{Ker}\,\sigma'$への写像τを考える. $X \in \mathrm{Ker}\,\sigma$に対して, $\sigma(X) = O$とすると, $\tau\sigma(X) = \sigma'\tau(X) = O$となるので, $\sigma'({}^tX) = O$である. したがって$\tau(X)$は$\mathrm{Ker}\,\sigma'$の元である.

次に写像τが全射であることを示す. $X' \in \mathrm{Ker}\,\sigma'$に対して, $\tau\sigma({}^tX') = \sigma'\tau({}^tX') = \sigma'(X') = O$である. したがって$\sigma({}^tX') = O$であるので, ${}^tX'$は$\mathrm{Ker}\,\sigma$の元であり, かつ$\tau({}^tX') = X'$である. ゆえに写像τは全射である.

最後に写像τが単射であることは明らかである.

よって$\mathrm{Ker}\,\sigma$と$\mathrm{Ker}\,\sigma'$はベクトル空間の同型である. 定理3.2.8より, $\mathrm{Ker}\,\sigma \cong \mathrm{Ker}(P_n(A_m^+))$及び$\mathrm{Ker}\,\sigma' \cong \mathrm{Ker}(P_m(A_n^+))$が成り立つので,

$$\mathrm{Ker}(P_n(A_m^+)) \cong \mathrm{Ker}(P_m(A_n^+))$$

が成り立つ. □

したがって, 定理3.2.8及び定理3.2.9をまとめると,

$$\dim \mathrm{Ker}\,\sigma = \dim \mathrm{Ker}(P_n(A_m^+)) = \dim \mathrm{Ker}(P_m(A_n^+))$$

がいえる.

3.3　A_m^+に関する計算

ここでは, 実際に$P_{m,n}$上のσゲームがσ可移であるかどうか調べていくために必要な, $A_m^+, P_n(\lambda)$等に関する計算結果を示す.

まず, $P_n(\lambda)$に関する計算から進める.

定理 3.3.1　$m \geq 0, n \geq 0$のとき,

$$P_{n+m}(\lambda) = P_n(\lambda)P_m(\lambda) + P_{n-1}(\lambda)P_{m-1}(\lambda)$$

が成り立つ. ただし$P_{-1}(\lambda) = 0$とする.

証明　m を固定して n に関する数学的帰納法で示す．$n = 0$ のとき，$P_{-1}(\lambda) = 0, P_0(\lambda) = 1$ より，

$$P_m(\lambda) = 1P_m(\lambda) + 0P_{m-1}(\lambda) = P_0(\lambda)P_m(\lambda) + P_{-1}(\lambda)P_{m-1}(\lambda)$$

となり正しい．また，$n = 1$ のとき，命題 3.2.5 より，

$$P_{m+1}(\lambda) = \lambda P_m(\lambda) + 1P_{m-1}(\lambda) = P_1(\lambda)P_m(\lambda) + P_0(\lambda)P_{m-1}(\lambda)$$

となり正しい．

次に，1 以上の k において，$n \leq k$ のとき正しいとして，$n = k+1$ のとき正しいことを示す．命題 3.2.5 より，

$$P_{k+1+m}(\lambda) = \lambda P_{k+m}(\lambda) + P_{k-1+m}(\lambda)$$

が成り立っているので，帰納法の仮定を用いて計算すると，

$$\begin{aligned} P_{k+1+m}(\lambda) &= \lambda P_{k+m}(\lambda) + P_{k-1+m}(\lambda) \\ &= \lambda(P_k(\lambda)P_m(\lambda) + P_{k-1}(\lambda)P_{m-1}(\lambda)) \\ &\quad + P_{k-1}(\lambda)P_m(\lambda) + P_{k-2}(\lambda)P_{m-1}(\lambda) \\ &= (\lambda P_k(\lambda) + P_{k-1}(\lambda))P_m(\lambda) \\ &\quad + (\lambda P_{k-1}(\lambda) + P_{k-2}(\lambda))P_{m-1}(\lambda) \\ &= P_{k+1}(\lambda)P_m(\lambda) + P_k(\lambda)P_{m-1}(\lambda) \end{aligned}$$

となり，$n = k+1$ のときも正しい．　□

定理 3.3.2　自然数 k について，

$$P_{2k-1}(\lambda) = \lambda(P_{k-1}(\lambda))^2$$

が成り立つ．

証明　実際に計算して求める．定理 3.3.1 から，以下のように式変形ができる．

$$\begin{aligned} P_{2k-1}(\lambda) &= P_k(\lambda)P_{k-1}(\lambda) + P_{k-1}(\lambda)P_{k-2}(\lambda) \\ &= P_{k-1}(\lambda)(P_k(\lambda) + P_{k-2}(\lambda)) \\ &= P_{k-1}(\lambda)(\lambda P_{k-1}(\lambda)) \\ &= \lambda(P_{k-1}(\lambda))^2 \end{aligned}$$

この計算の途中で，命題 3.2.5 を用いている．　□

定理 3.3.3 自然数nについて, $n=2^k-1$ならば,

$$P_n(\lambda)=\lambda^n$$

が成り立つ.

証明　まず, $k=1$のとき, $n=2^1-1=1$で, 実際に$P_1(\lambda)=\lambda^1$であるので正しい.

次に$n=2^k-1$のときの$P_{2^k-1}(\lambda)=\lambda^{2^k-1}$が成り立つと仮定して, $n=2^{k+1}-1$の場合を示す. 定理3.3.2を利用して, 次のように式変形できる.

$$\begin{aligned}P_{2^{k+1}-1}(\lambda)&=P_{2\cdot 2^k-1}(\lambda)\\&=\lambda(P_{2^k-1}(\lambda))^2\\&=\lambda(\lambda^{2^k-1})^2\\&=\lambda^{2^{k+1}-1}\end{aligned}$$

となるので, $n=2^{k+1}-1$のときも正しい.

□

定理 3.3.4 自然数nについて, $n=3\cdot 2^k-1$ならば,

$$P_n(\lambda)=\lambda^{2^k-1}(\lambda+1)^{2^{k+1}}$$

が成り立つ.

証明　kに関する数学的帰納法で示す.

$k=1$のとき, $n=3\cdot 2^1-1=5$であり, $P_3(\lambda)=\lambda P_2(\lambda)+P_1(\lambda)=\lambda^3$, $P_4(\lambda)=\lambda P_3(\lambda)+P_2(\lambda)=\lambda^4+\lambda^2+1$を用いると,

$$P_5(\lambda)=\lambda P_4(\lambda)+P_3(\lambda)=\lambda(\lambda^4+\lambda^2+1)+\lambda^3=\lambda^5+\lambda=\lambda^1(\lambda+1)^4$$

となり正しい.

$k\leq l$のとき正しいと仮定して, $k=l+1$のとき正しいことを示す. $P_{3\cdot 2^{l+1}-1}(\lambda)=P_{2\cdot 3\cdot 2^l-1}(\lambda)$であるので, 定理3.3.2を用いて, 次のように式変形できる.

$$\begin{aligned}P_{3\cdot 2^{l+1}-1}(\lambda)&=\lambda P_{3\cdot 2^l-1}(\lambda)^2\\&=\lambda\{\lambda^{2^l-1}(\lambda+1)^{2^{l+1}}\}^2\\&=\lambda\cdot\lambda^{2^{l+1}-2}(\lambda+1)^{2^{l+2}}\\&=\lambda^{2^{l+1}-1}(\lambda+1)^{2^{l+2}}\end{aligned}$$

となり, $k = l + 1$ のときも正しい. □

次に, A_m, A_m^+ の正則性について調べる.

定理 3.3.5 行列 A_m は, m が偶数ならば正則であり, m が奇数ならば, 非正則である.

証明　A_m の固有多項式 $P_m(\lambda)$ は

$$P_m(\lambda) = \det(A_m - \lambda E_m)$$

となるので, $\lambda = 0$ のとき $P_m(0) = \det(A_m)$ である. また, 定理 3.2.5 より $P_m(0) = P_{m-2}(0)$ が得られる. 特に, $P_0(0) = 1 \neq 0$ より, $P_{2k}(0) = P_0(0) \neq 0$ である. したがって, m が偶数のとき A_m は正則である. また, $P_{2k+1}(0) = P_1(0) = 0$ より, m が奇数のとき A_m は非正則である. □

定理 3.3.6 行列 A_m^+ は, $m \equiv 0, 1 \pmod 3$ ならば正則であり, $m \equiv 2 \pmod 3$ ならば非正則である.

証明　$A_m^+ = A_m + E_m$ より, $\lambda = 1$ とすると,

$$P_m(1) = \det(A_m - E_m) = \det(A_m^+)$$

となる. また, $P_n(\lambda) = \lambda P_{n-1}(\lambda) + P_{n-2}(\lambda)$ より,

$$P_n(1) = P_{n-1}(1) + P_{n-2}(1)$$

を得る. これを用いて計算すると,

$$\begin{aligned} P_{k+3}(1) &= P_{k+2}(1) + P_{k+1}(1) \\ &= (P_{k+1}(1) + P_k(1)) + P_{k+1}(1) \\ &= P_k(1) \end{aligned}$$

となる. $P_1(1) = 1, P_2(1) = 0$ なので, $P_3(1) = 1$ である. したがって, $m \equiv 0, 1 \pmod 3$ のとき A_m^+ は正則であり, $m \equiv 2 \pmod 3$ のとき A_m^+ は正則でない. □

3.4　$P_{m,n}$上のσゲームが解けるm,nの条件

3節で, $\mathrm{Ker}\,\sigma$は, $\mathrm{Ker}(P_n(A_m^+))$及び$\mathrm{Ker}(P_m(A_n^+))$と同型であることが分かった. また, $P_{m,n}$がσ可移であることの必要十分条件は, $\dim \mathrm{Ker}\,\sigma = 0$であることもわかった. 第4節では, m,nの具体的な値によって$P_{m,n}$がσ可移かどうかを調べていく.

まず, nを小さな値に固定して, mを変化させることを考える.

定理 3.4.1 長方形のグリッド$P_{m,1}$は, $m \equiv 0,1 \pmod 3$のときσ可移であり, $m \equiv 2 \pmod 3$のときσ可移でない.

証明　$P_1(\lambda) = \lambda$であるので, $P_1(A_m^+) = A_m^+$より, $P_1(A_m^+)$の正則条件はA_m^+の正則条件と同じである. したがって, 定理3.3.6より, $m \equiv 0,1 \pmod 3$のときσ可移であり, $m \equiv 2 \pmod 3$のときσ可移でない. □

定理 3.4.2 長方形のグリッド$P_{m,2}$は, mが偶数ならばσ可移であり, mが奇数ならばσ可移でない.

証明　$P_2(\lambda) = \lambda P_1(\lambda) + P_0(\lambda) = \lambda^2 + 1$であるので,

$$P_2(A_m^+) = (A_m^{+2} + E_m) = {A_m}^2 + E_m + E_m = {A_m}^2$$

より, $P_2(A_m^+)$の正則条件は${A_m}^2$の正則条件と同じである. したがって, 定理3.3.5よりmが偶数ならばσ可移であり, mが奇数ならばσ可移でない. □

定理 3.4.3 長方形のグリッド$P_{m,3}$は, $m \equiv 0,1 \pmod 3$のときσ可移であり, $m \equiv 2 \pmod 3$のときσ可移でない.

証明　$P_3(\lambda) = \lambda P_2(\lambda) + P_1(\lambda) = \lambda^3$であるので, $P_3(A_m^+) = A_m^{+3}$より, $P_3(A_m^+)$の正則条件はA_m^+の正則条件と同じである. したがって, 定理3.3.6より, $m \equiv 0,1 \pmod 3$のときσ可移であり, $m \equiv 2 \pmod 3$のときσ可移でない. □

定理 3.4.4 長方形のグリッド$P_{m,4}$は, $m \not\equiv 4 \pmod 5$のときσ可移であり, $m \equiv 4 \pmod 5$のときσ可移でない.

証明　$P_4(\lambda)=\lambda^4+\lambda^2+1=(\lambda+1)^4+(\lambda+1)^2+1$ より, A_4 の固有多項式と A_4^+ の固有多項式は一致する. ここで, $P_4(A_m^+)$ ではなくて, $P_m(A_4^+)$ を考える. $P_m(A_4^+)$ は, $m=(m-4)+4$ と考えれば, 定理3.3.1より,

$$P_m(A_4^+)=P_{m-4}(A_4^+)P_4(A_4^+)+P_{m-5}(A_4^+)P_3(A_4^+)$$

となる. $P_4(\lambda)$ は A_4 の固有多項式であり, A_4^+ の固有多項式でもあるから, 定理3.2.6より, $P_4(A_4^+)=O$ である. よって,

$$\begin{aligned}P_m(A_4^+)&=P_{m-5}(A_4^+)P_3(A_4^+)\\&=P_{m-5}(A_4^+)\cdot(A_4^+)^3\end{aligned}$$

となる. このことを使い, $m=5k+s(0\leq s\leq 4)$ とすると,

$$P_m(A_4^+)=P_s(A_4^+)\cdot(A_4^+)^{3k}$$

となる. $4\equiv 1 \pmod 3$ であるので, 定理3.3.6より, $(A_4^+)^{3k}$ は正則である. したがって, $P_m(A_4^+)$ が正則であることと, $P_s(A_4^+)$ が正則であることは同値である. 実際に計算すると, 次のことが分かる.

- $s=0$ のとき, $P_0(A_4^+)=E_4$ は正則である.
- $s=1$ のとき, $P_1(A_4^+)=A_4^+$ は正則である.
- $s=2$ のとき, $P_2(A_4^+)=(A_4^+)^2+E_4=(A_4)^2$ は正則である.
- $s=3$ のとき, $P_3(A_4^+)=(A_4^+)^3$ は正則である.
- $s=4$ のとき, $P_4(A_4^+)=O$ は非正則である.

よって, $P_m(A_4^+)$ が正則であるための必要十分条件は, $m\not\equiv 4 \pmod 5$ であることである. また, $m\equiv 4 \pmod 5$ のとき, $P_m(A_4^+)$ は非正則である. □

定理 3.4.5　長方形のグリッド $P_{m,5}$ は, m が自然数 k を用いて $m=6k$ もしくは $6k+4$ と表されるとき σ 可移であり, そうでないときは σ 可移でない.

証明　$P_5(\lambda)=\lambda^5+\lambda$ であるので,

$$P_5(A_m^+)=A_m^{+5}+A_m^+=A_m^+(A_m^{+4}+E_m)=A_m^+(A_m^4+E_m+E_m)=A_m^+A_m^4$$

となる. 定理1.4.16より, $P_5(A_m^+)$ が正則であるための必要十分条件は A_m^+ が正則かつ A_m が正則であることである. したがって, $m \equiv 0, 1 \pmod 3$ かつ m が偶数のとき, すなわち, m が自然数 k を用いて $m = 6k$ もしくは $6k+4$ と表されるとき σ 可移であり, そうでないときは σ 可移ではない. □

長方形のグリッド $P_{m,6}$ について, $P_6(\lambda) = P_3(\lambda)^2 + P_2(\lambda)^2 = \lambda^6 + \lambda^4 + 1$ であるので, $P_6(A_m^+)$ は

$$\begin{aligned} P_6(A_m^+) &= (A_m^+)^6 + (A_m^+)^4 + E_m \\ &= \left((A_m^+)^2\right)^3 + (A_m^4 + E_m) + E_m \\ &= (A_m^2 + E_m)^3 + A_m^4 \\ &= A_m^6 + 3A_m^4 + 3A_m^2 + E_m + A_m^4 \\ &= A_m^6 + A_m^2 + E_m \\ &= (A_m^3 + A_m + E_m)^2 \end{aligned}$$

となり, これ以上の因数分解はなく, $A_m^3 + A_m + E_m$ が正則であるための簡明な条件は得られなかった.

定理 3.4.6 長方形のグリッド $P_{m,7}$ は, $m \equiv 0, 1 \pmod 3$ のとき σ 可移であり, $m \equiv 2 \pmod 3$ のとき σ 可移でない.

証明　定理3.3.3より, $P_7(\lambda) = \lambda^7$ である. ゆえに $P_7(A_m^+) = {A_m^+}^7$ より, $P_7(A_m^+)$ の正則条件は A_m^+ の正則条件と同じである. したがって, $m \equiv 0, 1 \pmod 3$ のとき σ 可移であり, $m \equiv 2 \pmod 3$ のとき σ 可移でない. □

定理 3.4.7 長方形のグリッド $P_{m,8}$ は, m が奇数のときは σ 可移でない.

証明　$P_8(\lambda) = \lambda P_7(\lambda) + P_6(\lambda) = \lambda^8 + \lambda^6 + \lambda^4 + 1$ であるので, $P_8(A_m^+)$ は

$$\begin{aligned} P_8(A_m^+) &= {A_m^+}^8 + {A_m^+}^6 + {A_m^+}^4 + E_m \\ &= \left({A_m^+}^4\right)^2 + {A_m^+}^6 + {A_m^+}^4 + E_m \\ &= A_m^8 + E_m + A_m^6 + A_m^4 + A_m^2 + E_m + A_m^4 + E_m + E_m \\ &= A_m^8 + A_m^6 + A_m^2 \\ &= A_m^2(A_m^6 + A_m^4 + E_m) \end{aligned}$$

となり, A_m が非正則のときは $P_8(A_m^+)$ は非正則である. したがって, m が奇数のときは σ 可移でない. □

定理 3.4.8 長方形のグリッド $P_{m,9}$ は, $m \equiv 0,1 \pmod 3$ かつ, $m \not\equiv 4 \pmod 5$ のとき σ 可移であり, そうでないときは σ 可移でない.

証明 定理3.3.2より, $P_9(\lambda) = \lambda P_4(\lambda)^2 = \lambda(\lambda^4+\lambda^2+1)^2 = \lambda^9+\lambda^5+\lambda$ であるので, $P_9(A_m^+)$ は

$$\begin{aligned} P_9(A_m^+) &= {A_m^+}^9 + {A_m^+}^5 + A_m^+ \\ &= A_m^+({A_m^+}^8 + {A_m^+}^4 + E_m) \\ &= A_m^+(A_m^8 + E_m + A_m^4 + E_m + E_m) \\ &= A_m^+(A_m^4 + A_m^2 + E_m)^2 \\ &= A_m^+(P_4(A_m^+))^2 \end{aligned}$$

となる. 定理1.4.16より, A_m^+ が正則かつ $P_4(A_m^+)$ が正則のとき, $P_9(A_m^+)$ は正則である. したがって, 定理3.3.6及び定理3.4.4より, $P_9(A_m^+)$ が正則であるための必要十分条件は, $m \equiv 0,1 \pmod 3$ かつ $m \not\equiv 4 \pmod 5$ である. □

長方形のグリッド $P_{m,10}$ について,

$$P_{10}(\lambda) = \lambda P_9(\lambda)+P_8(\lambda) = \lambda(\lambda^9+\lambda^5+\lambda)+\lambda^8+\lambda^6+\lambda^4+1 = \lambda^{10}+\lambda^8+\lambda^4+\lambda^2+1$$

であるので, $P_{10}(A_m^+)$ は

$$\begin{aligned} P_{10}(A_m^+) &= (A_m^+)^{10} + (A_m^+)^8 + (A_m^+)^4 + (A_m^+)^2 + E_m \\ &= ((A_m^+)^2)^5 + (A_m^8 + E_m) + (A_m^4 + E_m) + (A_m^2 + E_m) + E_m \\ &= A_m^{10} + 5A_m^8 + 10A_m^6 + 10A_m^4 + 5A_m^2 + E_m + A_m^8 + A_m^4 + A_m^2 \\ &= A_m^{10} + A_m^4 + E_m \\ &= (A_m^5 + A_m^2 + E_m)^2 \end{aligned}$$

となり, これ以上の因数分解はなく, $A_m^5 + A_m^2 + E_m$ が正則であるための簡明な条件は得られなかった.

定理 3.4.9 長方形のグリッド $P_{m,11}$ は, m が自然数 k を用いて $m = 6k$ もしくは $6k+4$ と表されるとき σ 可移であり, そうでないときは σ 可移ではない.

証明　$11 = 3\cdot 2^2 - 1$であるので, 定理3.3.4より,

$$P_{11}(\lambda) = \lambda^3(\lambda+1)^8 = \lambda^{11} + \lambda^3$$

となる. $P_{11}(A_m^+)$は

$$\begin{aligned} P_{11}(A_m^+) &= {A_m^+}^{11} + {A_m^+}^3 \\ &= {A_m^+}^3({A_m^+}^8 + E_m) \\ &= {A_m^+}^3 {A_m}^8 \end{aligned}$$

であり, 定理1.4.16より, $P_{11}(A_m^+)$が正則であるための必要十分条件は, A_m^+が正則かつA_mが正則であることである. したがって, $m \equiv 0, 1 \pmod 3$かつmが偶数のとき, すなわち, mが自然数kを用いて$m = 6k$もしくは$6k+4$と表されるときσ可移であり, そうでないときはσ可移ではない. □

次に$P_n(\lambda)$を因数分解する方法で得られる結果について述べる.

定理 3.4.10　$n = 2k-1 (k \in \mathbb{N}), m \equiv 2 \pmod 3$のとき, $P_{m,2k-1}$はσ可移でない.

証明　定理3.3.2より, 自然数kについて$P_{2k-1}(A_m^+) = A_m^+(P_{k-1}(A_m^+))^2$が成り立つ. したがって, A_m^+が非正則ならば少なくとも$P_{2k-1}(A_m^+)$は非正則である. すなわち$m \equiv 2 \pmod 3$のとき, $P_{m,2k-1}$はσ可移でない. □

次は定理3.4.3及び定理3.4.6の証明を一般化したものである.

定理 3.4.11　$n = 2^k - 1 (k \in \mathbb{N})$とする. $m \equiv 0, 1 \pmod 3$ならば$P_{m,2^k-1}$はσ可移であり, $m \equiv 2 \pmod 3$ならば$P_{m,2^k-1}$はσ可移でない.

証明　定理3.3.3より, 自然数kについて$P_{2^k-1}(A_m^+) = (A_m^+)^{2^k-1}$が成り立つ. したがって, $P_{2^k-1}(A_m^+)$の正則条件はA_m^+の正則条件と同じである. すなわち$m \equiv 0, 1 \pmod 3$のとき, $P_{m,2^k-1}$はσ可移であり, $m \equiv 2 \pmod 3$のとき, $P_{m,2^k-1}$はσ可移でない. □

次は定理3.4.5及び定理3.4.9の証明を一般化したものである.

定理 3.4.12　$n = 3\cdot 2^k - 1$とする. $P_{m,3\cdot 2^k-1}$は, mが自然数lを用いて$m = 6l$もしくは$6l+4$と表されるときσ可移であり, そうでないときはσ可移ではない.

証明　定理3.3.4より, 自然数kについて$P_{3\cdot 2^{k-1}}(A_m^+) = (A_m^+)^{2^{k-1}}\cdot(A_m)^{2^{k+}}$が成り立つ. 定理1.4.16より, $P_{3\cdot 2^{k-1}}(A_m^+)$が正則であるための必要十分条件は, A_m^+が正則かつA_mが正則であることである. したがって, $m \equiv 0, 1 \pmod 3$かつmが偶数のとき, すなわち, mが自然数lを用いて$m = 6l$もしくは$6l+4$と表されるとき, $P_{m,3\cdot 2^{k-1}}$はσ可移であり, そうでないときはσ可移ではない. □

これまでに得た結果を$1 \le n \le 11$の範囲で表にまとめると以下のようになる.

	1	2	3	4	5	6	7	8	9	10	11
1	○	×	○	○	×	○	○	×	○	○	×
2	×	○	×	○	×	○	×	○	×	○	×
3	○	×	○	○	×	○	○	×	○	○	×
4	○	○	○	×	○	○	○	○	×	○	○
5	×	×	×	○	×	○	×	×	×	○	×
6	○	○	○	○	○		○		○		○
7	○	×	○	○	×	○	○	×	○	○	×
8	×	○	×	○	×		×		×		×
9	○	×	○	×	×	○	○	×	×	○	×
10	○	○	○	○	○		○		○		○
11	×	×	×	○	×	○	×	×	×	○	×

表 3.1: A_m^+の正則性

○のついているm, nの組み合わせについては, $P_{m,n}$がσ可移であり, ×の組み合わせでは$P_{m,n}$はσ可移でない. 空白のところは, 定理3.4.1から定理3.4.12ではσ可移かどうか決定できなかった組み合わせである. 表の空欄についても, 個々に$\det(P_n(A_m^+))$を計算すれば, σ可移かどうか決

定できる. 例えば, $P_6(A_6^+)$ を実際に計算すると

$$P_6(A_6^+) = (A_6^3 + A_6 + E_6)^2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

であり, $\det P_6(A_6^+) = 1$ となるので, $P_{6,6}$ はσ可移であることが分かる.

ここでは, $P_{m,n}$ がσ可移かどうかを決定するために $\mathbb{F}_2$ 上の線形代数, 特にrankや行列式といった初等的な線型代数の概念を用いてきた. 岩堀 [4] はさらに単因子論や環論といった代数的概念を応用して同じ問題を考察しており, $P_{m,n}$ がσ可移であるかどうかを, ある種の多項式の最大公約数の計算に帰着している. しかしながら, $P_{m,n}$ がσ可移であるかどうかを m, n の値から簡単に決定する方法は今のところ見つかっていないようである.

謝辞

本研究を進めるにあたり, 大学院入学当初からの3年間にわたる手厚い御指導をして頂いた, 指導教員の濱中裕明准教授に心より御礼申し上げます. 大学でしっかりと数学を学んでこなかった私に, 数学の基礎から丁寧に指導していただき, 理解が追い付かずに何度も何度もやり直した際も, 根気強くゼミを行って下さったことに, 大変感謝いたします. 濱中先生のご指導がなければ, 今の私はないといっても過言ではありません.

また, 兵庫教育大学にきてから, 同じ将来を目指す仲間と出会い, 日ごろから数学について考える機会が増えました. 特に3年間行動を共にした理数系教員養成特別プログラムの仲間とは, 授業や実習などで互いに意見を交わし, 切磋琢磨してきました. そんな中で私自身も成長できたと思います.

そして, 防衛大学校という将来を約束された進路から, 教師を目指す道に変えたにもかかわらず, 暖かく支援してくれた家族に心より御礼申し上げます.

平成24年12月20日

中原諒太

参考文献

[1] Rena Barua and S. Ramakrishnan, "σ^-game, σ^+game, and Two-dimensional Additive Cellular Automata", Theoretical Computer Science, Vol.154 Issue 2(1996).

[2] 齋藤正彦 『基礎数学 I 線型代数入門』東京大学出版会, (1966).

[3] K.Sutner "Linear cellular automata and the Gardens of Eden" THE MATHEMATICAL INTELLIGENCER VOL.11, NO.2, (1989), pp.49-53.

[4] 岩堀長慶 『ランプパターンの転移問題-単因子論の一応用-』Science reports of Tokyo Woman's Christian University 31(3), (1980) pp.623-635.

[5] 堀田良之 『数学シリーズ　代数入門 -群と加群』東京裳華房 (1987).